
# Strengthening trust in the identity life cycle

## Enhancing electronic machine readable travel documents due to advances in security protocols and infrastructure

**Dissertation**

zur Erlangung des Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)

am Fachbereich Mathematik und Informatik
der Freien Universität Berlin

vorgelegt von

Nicolas Buchmann

Berlin
August 2018

| | |
|---|---|
| **Erstgutachter:** | Prof. Dr. Marian Margraf |
| **Zweitgutachter:** | Prof. Dr. Harald Baier |
| **Tag der Disputation:** | 11.02.2019 |

# Erklärung

Ich versichere hiermit, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die im Literaturverzeichnis angegebenen Quellen benutzt habe.

Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder noch nicht veröffentlichten Quellen entnommen sind, sind als solche kenntlich gemacht.

Die Zeichnungen oder Abbildungen in dieser Arbeit sind von mir selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen.

Diese Arbeit ist in gleicher oder ähnlicher Form noch bei keiner anderen Prüfungsbehörde eingereicht worden.

Berlin August 2018

Nicolas Buchmann

**Abstract**

Travel documents have become an integral part of travelling into foreign countries and play a major role for border control. Today's electronic travel documents rely on electronic security protocols and infrastructure, which exhibit multiple shortcomings. On the one hand, utilised protocols and infrastructure are complex, partially not implemented, and have been found insecure in the presence of a large-scale quantum computer. On the other hand, electronic travel documents are only one part of the document life cycle, since a passport can be obtained with an insecure birth certificate.

Due to these shortcomings, focus is put on improving the security of birth certificates, simpler and post-quantum resistant security protocols, and infrastructure improvements in the identity life cycle. The security of birth certificates is strengthened by a blockchain based system and a 2D barcode which stores biometric information. Furthermore, simpler travel document protocols with less complex infrastructure requirements, fewer steps, and long-term post-quantum security achieved via hash-based cryptography and code-based cryptography are evaluated.

# Acknowledgement

At this point, I would like to thank Prof. Dr. Margraf and Prof. Dr. Baier for their supervision, support, and feedback during this thesis. Furthermore, I need to thank Prof. Dr. Busch and Dr. Christian Rathgeb for feedback and support in the field of biometrics. Special thanks go to Prof. Dr. Brown from the Stony Brook University, New York for proofreading and linguistic revision. Finally, I must express my gratitude to my parents for their support during my studies and this thesis.

# Contents

# List of Figures

# List of Tables

# List of Abbreviations

| | |
|---|---|
| AA | Active Authentication |
| ABC | Automated Border Control |
| AD | Auxiliary Data |
| AE | Authenticated Encryption |
| AES | Advanced Encryption Standard |
| AFIS | Automated Fingerprint Identification System |
| API | Application Programming Interface |
| ASCII | American Standard Code for Information Interchange |
| ASIC | Application Specific Integrated Circuit |
| ASM | Assembly |
| ATR | Answer To Reset |
| AVG | Average |
| AVX | Advanced Vector Extensions |
| BAC | Basic Access Control |
| BIG | Brussel Interoperability Group |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BTC | Bitcoin |
| CA | Certificate Authority or Chip Authentication |
| CAKE | Code-based Algorithm for Key Encapsulation |
| CAN | Card Access Number |
| CD-R | Compact Disc Recordable |
| CLAHE | Contrast Limited Adaptive Histogram Equalisation |
| CMAC | Cipher-based Message Authentication Code |
| CMSS | Chaining Merkle Signature Scheme |
| COM | Common Data Elements |
| CPU | Central Processing Unit |
| CRL | Certificate Revocation List |
| CSCA | Country Signing Certificate Authority |
| CUDA | Compute Unified Device Architecture |
| CVCA | Country Verifying Certificate Authority |
| dB | Decibel |
| DCT | Discrete Cosine Transform |
| DDoS | Distributed Denial of Service |
| DDR | Double Data Rate |
| DG | Data Group |
| DH | Diffie-Hellman |
| DNS | Domain Name System |

| | |
|---|---|
| DoS | Denial of Service |
| DS | Document Signer |
| DSA | Digital Signature Algorithm |
| DV | Document Verifier |
| DVD-R | Digital Versatile Disc Recordable |
| EAC | Extended Access Control |
| ECC | Elliptic Curve Cryptography or Error-Correcting Code |
| ECDLP | Elliptic Curve Discrete Logarithm Problem |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EER | Equal Error Rate |
| EF | Elementary File |
| eID | Electronic Identification |
| eIDAS | Electronic Identification, Authentication and Trust Services |
| eMRTD | Electronic Machine Readable Travel Document |
| ePassport | Electronic Passport |
| EU | European Union |
| EU-EAC | European Union Extended Access Control |
| FAR | False Acceptance Rate |
| FLD | Fisher Linear Discriminant |
| FMR | False Match Rate |
| FNMR | False Non-Match Rate |
| FPGA | Field Programmable Gate Array |
| FTS | Few-Time Signature Scheme |
| GB | Gigabyte |
| GCC | GNU Compiler Collection |
| GDDR | Graphics Double Data Rate |
| GHQ | General Headquarters |
| GmbH | Gesellschaft mit beschränkter Haftung |
| GMSS | Generalised Merkle Signature Scheme |
| GPGPU | General Purpose Computation on Graphics Processing Unit |
| GPU | Graphics Processing Unit |
| HD | Hamming Distance |
| HMAC | Keyed-Hash Message Authentication Code |
| HSM | Hardware Security Module |
| HSP | Hidden Subgroup Problem |
| IBC | Identity-Based Cryptography |
| ICAO | International Civil Aviation Organization |
| ID | Identity |
| IEC | International Electrotechnical Commission |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| IS | Inspection System |
| ISO | International Organization for Standardization |
| IT | Information Technology |

| | |
|---|---|
| J2K | Synonym for JPEG 2000 |
| JPEG | Joint Photographic Experts Group |
| JPEG 2000 | Joint Photographic Experts Group 2000 |
| JPG | Synonym for JPEG |
| KA | Key Agreement |
| kB | Kilobyte |
| KDF | Key Derivation Function |
| LD | Lamport-Diffie |
| LD-OTS | Lamport-Diffie One-Time Signature Scheme |
| LDS | Logical Data Structure |
| LG | Log Gabor |
| LMS | Leighton Micali Signature |
| LTE | Long-Term Evolution |
| MAC | Message Authentication Code |
| MB | Megabyte |
| MRTD | Machine Readable Travel Document |
| MRZ | Machine Readable Zone |
| MSS | Merkle Signature Scheme |
| MT | Multi Tree |
| NIR | Near-Infrared |
| NIST | National Institute of Standards and Technology |
| nPA | Neuer Personalausweis |
| NTP | Network Time Protocol |
| NTRU | N-Th Degree Truncated Polynomial Ring |
| OCR | Optical Character Recognition |
| OCSP | Online Certificate Status Protocol |
| OSEP | On-line Secure E-Passport Protocol |
| OTS | One-Time Signature Scheme |
| PACE | Password Authenticated Connection Establishment |
| PAPA | Popcount Add Popcount Add |
| PCA | Principal Component Analysis |
| PI | Pseudonymous Identifier |
| PIN | Personal Identification Number |
| PKD | Public Key Directory |
| PKI | Public Key Infrastructure |
| PPAA | Popcount Popcount Add Add |
| PQ | Post-Quantum |
| PRNG | Pseudo Random Number Generator |
| PSNR | Peak Signal-to-Noise Ratio |
| QC-MDPC | Quasicyclic Moderate Density Parity Check |
| QR | Quick Response |
| QSW | Quadratic Spline Wavelet |
| QUIC | Quick UDP Internet Connections |
| RAM | Random-Access Memory |

| | |
|---|---|
| RFC | Request for Comments |
| RFID | Radio-Frequency Identification |
| RLWE | Ring Learning With Errors |
| RSA | Rivest Shamir Adleman |
| SAC | Supplemental Access Control |
| SCVP | Server-Based Certificate Validation Protocol |
| SHA | Secure Hash Algorithm |
| SIGMA | Sign-and-Mac |
| SIMD | Single Instruction Multiple Data |
| SIS | Schengen Information System |
| SLTD | Stolen and Lost Travel Documents |
| SOD | Document Security Object |
| SPACE | Simplified PACE |
| SPI | Security Protocols and Infrastructures |
| SPOC | Single Point of Contact |
| SSE | Streaming SIMD Extensions |
| TCO | Total Cost of Ownership |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| TripleA | Accelerated Accuracy-Preserving Alignment |
| UMTS | Universal Mobile Telecommunications System |
| USB | Universal Serial Bus |
| USIT | University of Salzburg Iris Toolkit |
| VPN | Virtual Private Network |
| W-OTS | Winternitz One-Time Signature Scheme |
| XMSS | Extended Merkle Signature Scheme |

# Part I.

# Preface

# 1. Introduction

Travel documents have become an integral part of travelling into foreign countries and play a major role for border control and aviation. Today's electronic travel documents rely on electronic security protocols to ensure authenticity and integrity of the document holder's biometric data and originality of the document itself. The cryptographically protected (biometric) data is utilised to enable a link between the physical document and the document holder. Therefore, the two main security goals of any identity document are to ensure the document is unaltered and authentic, and that the physical document and document holder belong to each other.

The problems with today's security protocols are twofold. On the one hand, the protocols are very complex and therefore partially not implemented in practice after nearly 10 years of the EU's electronic passport introduction. On the other hand, the security protocols depend on the hardness of two mathematical problems, which have been found to be solvable in polynomial time in the presence of a large-scale quantum computer. Furthermore, electronic travel documents are only one part of the document life cycle, since today an electronic passport can be obtained with an unstandardised and insecure birth certificate. There is also no standardised mechanism to handle stolen passport terminals and since the terminal infrastructure is not fully deployed in the EU, terminals rely on low entropy face recognition instead of using the more secure fingerprints stored on the passport.

Due to these circumstances, the thesis focuses on five shortcomings of today's travel document protocols, their infrastructure and life cycle components:

- Improving the security of birth certificates.
- Simpler protocols with easier infrastructure requirements.
- Revocation mechanisms for stolen passport terminals.
- Post-Quantum secure cryptographic primitives for travel documents.
- Improvements regarding biometrics

These five topics are further outlined in the context of the identity life cycle in chapter 2 the life cycle introduction.

All shortcomings are discussed and solution candidates proposed. The security of birth certificates is strengthened by, on the one hand, a blockchain based system to ensure long-term authenticity and integrity of data and on the other hand, by a 2D barcode which stores biometric information of the document holder to create a link between birth certificate and document holder. Simpler travel document protocols are proposed

in the form of IBIHOP+ and BioPACE V2, which have less complex infrastructure requirements and fewer steps than the current security protocol suite. To eliminate the problem of stolen terminals a revocation mechanism based on the Network Time Protocol (NTP) and the Online Certificate Status Protocol (OCSP) was found as most suitable for the requirements of the travel document domain. Long-term post-quantum security of the travel document protocols is achieved by evaluating the most suitable post-quantum classes, in particular hash-based cryptography and code-based cryptography. Finally, improvements regarding biometrics are discussed, which on the one hand focus on suitable entropy for travel document biometrics and on the other hand, on techniques to speed up large-scale biometric comparisons (e.g., black-list checks and double enrolment checks).

The thesis first introduces the respective problem, gives an introduction into the underlying context, evaluates state-of the art proposals by the scientific community and finally evaluates and discusses the best solution candidates.

After this general introduction, the further structure is as follows: First, chapter 2 gives a more detailed introduction to the identity life cycle. Part II of the document focuses on the current travel document infrastructure in chapter 3, security protocols in chapter 4, and closes with chapter 5 a discussion of the shortcomings of the EU's Extended Access Control (EAC) infrastructure. These shortcomings were also the topic of several scientific publications, which are summarised and classified in the context of this work. Part III discusses the five introduced shortcomings and their solutions for future travel documents. These are birth certificate blockchain technologies in chapter 6, simpler and easier to deploy protocols in chapter 7, revocation for passport terminals in chapter 8, post-quantum cryptography for travel documents in chapter 9, and finally enhancements regarding biometrics in chapter 10. Part IV with chapter 11 concludes the thesis with a conclusion and summary of the achieved results in this work.

# 2. The Identity Life Cycle

Identity documents (ID documents) are physical documents, which are commonly used to identify a person or verify aspects of the document's holder (e.g., age or nationality). A German citizen usually comes into contact with at least three types of documents: birth certificates, ID cards and passports. Further situational documents (e.g., visa, child passport, provisional/temporary passport, death certificate) or documents which are non-legally binding, but commonly accepted as ID documents (e.g., driver's licence) exist but are out of scope for this document.

The issuance of a German birth certificate is initiated at the civil registry office with jurisdiction for the place of birth. By German law any birth must be reported to the local civil registry office within one week [53, §18]. In case the child was born in a hospital this is done directly by the staff, otherwise the parents or any witness is under duty to do so [53, §20]. Once the birth is reported to the local civil registry office a birth certificate is personalised, issued, and a registry entry is added at the local town hall.

There is no harmonisation of birth certificates in Germany and the document usually holds no security features or binding element to the document holder. The most common use cases for a birth certificate are the issuance of the first passport, the first ID card or in case of marriage.

The passport in Germany is called either ePassport or by its local short form ePass. In contrast to the passport issued before November 2005, the ePassport contains an electronic component for data storage and certain cryptographic security features. This is realised by a contactless RFID chip embedded into the booklet of the document.

From the age of 13 an ePassport can be issued, containing two mandatory biometric fingerprints as well as a facial image and is valid for a 10-year period [52, §4, §5]. The applicant has to present a birth certificate, an old passport or an ID card [52, §6]. Starting from the age of 16 any German citizen has to possess, but not carry, an ePassport or an ID card [51, §1]. The common use case for presenting an ePassport is travelling, thus crossing borders.

The German ID card can be requested at any age [51, §1] and the document applicant has to present an old document (e.g., a birth certificate, an ePassport or an ID card). ID cards are valid for six years under the age of 25 and ten years afterwards [51, §6]. In contrast to the ePassport, the enrolment of fingerprints is optional and only the facial image is mandatory [51, §5]. A contactless RFID chip is also embedded in the ID card, providing similar functionality as the ePassport, but also comprising two separate new applications, the so called eID function and the qualified electronic signature. Regardless of these two new applications the common use cases for the ID card are evidence of identity and travelling in the Schengen area.

Due to the limited validity period of ePassports and ID cards a recurring action in

the identity life cycle is the presentation of an ID document to get a new document. The identity life cycle is depicted in figure 2.1. In the first step, an existing document is presented during the enrolment for a new document. These documents are called breeder documents and defined as: "A document, genuine or fraudulent, that can serve as a basis to obtain other identification documents or benefits fraudulently." [224]. After enrolment of the applicant's information the data is sent to a document manufacturer for personalisation of a new electronic machine readable travel document (eMRTD) in step two. Following the manufacturing the document can be handed to the rightful document holder during the document issuance in step three. Step four is the presentation of the document during a border check to a border official, or an Automated Border Control (ABC) gate, and in step five the document is handed back to the document holder. The full round of the life cycle is complete if the document holder has to apply for a new identity document.

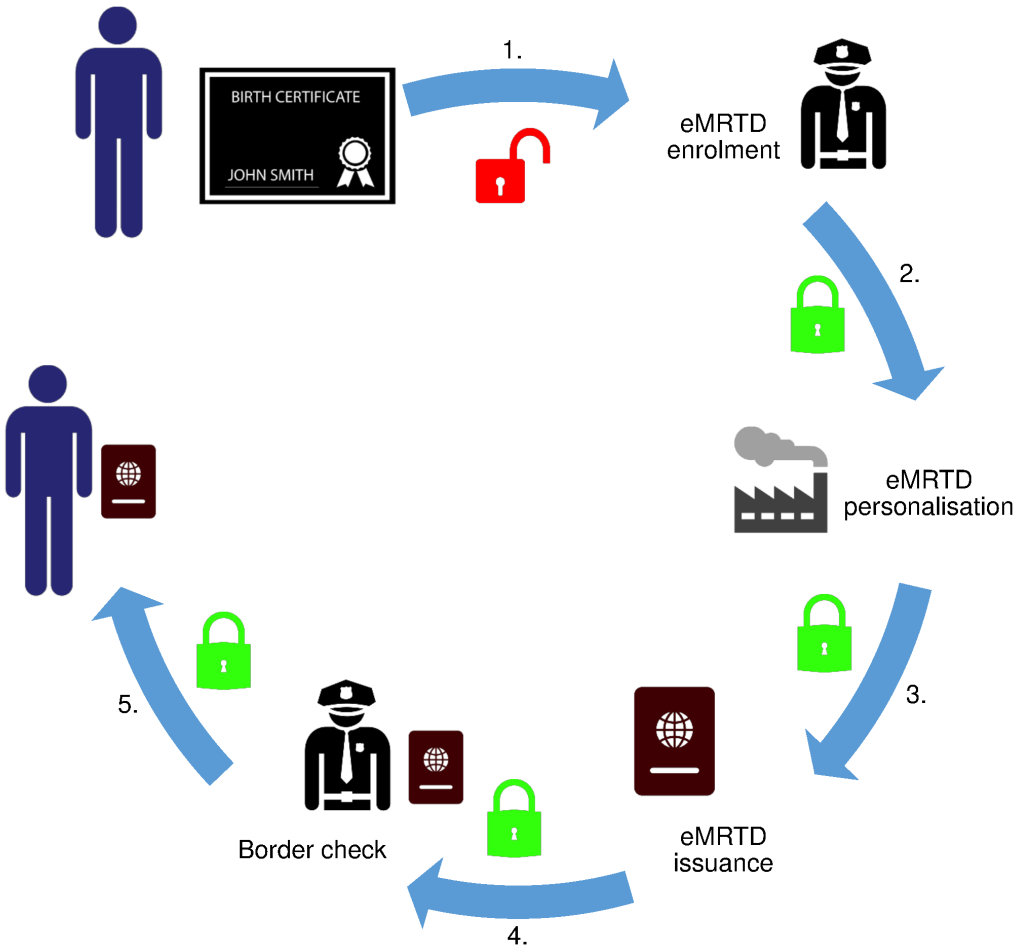



Figure 2.1.: The identity life cycle [223].

Further exceptional steps exist e.g., damaged, lost, and stolen travel documents, but these are country specific and out of scope for the thesis at hand. Nevertheless, a transnational project exists in form of Interpol's Stolen and Lost Travel Documents (SLTD) database, which is maintained by 174 countries [152]. The weakest link in the depicted life cycle is the first step, the presentation of the breeder document, since it can be besides an old ePassport or an old ID card, also a birth certificate, which is by general acknowledgement the most troublesome option [223, 142]. Today, birth certificates neither provide a reliable means to check for authenticity and integrity of data, nor a strong link to the document holder. Due to these shortcomings chapters 6 and section 10.2 of the thesis discuss possible improvements to birth certificates and their harmonisation.

Further emphasis is put on step four, the border check, and its underlying security protocols. Birth certificates cannot be used as travel documents and the underlying cryptographic eMRTD security protocols are considered more secure than the eMRTD enrolment. Nevertheless, a security discussion is necessary since on the one hand, the protocols rely on a complicated cross-border access control PKI without standardised revocation for the border terminals [123] (see chapter 8) and on the other hand, are not post-quantum secure. Therefore, improvements to the protocols performed by the RFID chip of the ePassport, which are on the one hand, beneficial to the ID document domain today (e.g., simpler infrastructure, higher entropy credentials, speed-ups) are discussed in separate chapter 7 and on the other hand, benefits which are considered relevant for the future (e.g., cryptography secure in the presence of a large scale quantum computer i.e., Post-Quantum cryptography) is further examined in chapter 9.

Even so the focus of the thesis is on the underlying technologies, best practices for the issuing processes [140, 222] harmonised employee training [91, 223], better exploitation of registers for authentic documents [90], and life cycle processes [101] are equally important for the overall domain security, but out of scope for the discussion.

Proposals for trustworthy life cycle management have also been published by the EU research project FIDELITY [54]. One of the main discussion points in the EU proposal is the harmonisation of a European birth certificate, including unified document security, verification, layout and data records, registers, and processes. The authors propose a layout for such a harmonised European birth certificate as well as the online back end system. In contrast, section 10.2 based on [46] specifically discusses an alternative layout as well as an offline approach. Chapter 10 as a whole comprises discussions for further biometric topics in the context of identity documents, which on the one hand, emphasise strengthening the link between the physical breeder document and the document holder in section 10.1. On the other hand, section 10.3 considers methods to speed up biometric comparisons. Table 2.1 gives an overview of the discussed identity life cycle shortcomings and examined proposals for future travel documents in the following chapters.

The importance of the identity life cycle is also emphasised by an action plan of the European commission to strengthen the response to travel document fraud [91]. Focus of the action plan are counter-measures and strategies towards the increasing problem of travel document fraud, which enables terrorism and organised crime. The authors of the action plan establish the rising demand of EU travel documents for fraud

Table 2.1.: Identity life cycle shortcomings and proposals of the following chapters.

| Shortcoming | Idea | Discussion |
|---|---|---|
| Breeder documents have no security feature to ensure authenticity and integrity of data. | A blockchain based system to ensure long-term authenticity and integrity of data. | Chapter 6 |
| Travel document security protocols are very complex and parts of the underlying infrastructure are unused. | Simpler protocols are proposed in the form of IBIHOP+ and BioPACE V2, which have less complex infrastructure requirements and fewer steps. | Chapter 7 |
| There is no global standardised revocation mechanism for stolen inspection systems. | A revocation mechanism based on NTP and OCSP was found as most suitable. | Chapter 8 |
| Travel document security protocols are not post-quantum secure. | Post-quantum classes, in particular hash/code-based cryptography are evaluated regarding long-term security. | Chapter 9 |
| Breeder documents have no biometric link to the document holder and travel documents commonly rely on a biometric link with low entropy. | Focus is put on suitable entropy for travel document biometrics and a 2D barcode which stores biometric information of the document holder. | Chapter 10 |

and the increase of fraudulent obtaining of genuine documents by 76% between Q1 of 2015 and Q1 of 2016. Recommended specific actions include the use of additional identity evidence sources (e.g., electoral rolls and social security records), if no reliable registration data is available. Furthermore, breeder documents shall become more fraud-resistant by adding a minimum set of security features and the possibility of biometric identifiers in population registers is discussed.

# Part II.

# Current Travel Document Infrastructure and Protocols

# 3. Travel Document Infrastructure

The main difference of the ePassport in contrast to the legacy passport is the integration of a smart card technology based radio frequency chip to enable data storage and discrete computations for cryptographic security protocols. These security protocols fulfil individual security goals which are discussed in subsequent sections and the data storage capabilities of the chip are mainly utilised for storage of the document holder's personal data and auxiliary data required by the protocols. In contrast to the recent rise of constructions like authenticated encryption (AE) [197], which combine several distinct security goals into one well-defined mechanism, the eMRTD protocols are based on the software development pattern of strong cohesion and loose coupling. Every protocol has a clear security goal and is mostly independent of the other security protocols. The latter enables the use of an adjusted protocol subset in different travel document families (e.g., ePassports, eVISAs, eID-cards and eIDAS tokens) [44]. Even though the protocols are mostly independent in their execution they can only be executed in a specified and well-defined order depending on the use case to guarantee security and eliminate user errors.

eMRTD security protocols are specified either by the International Civil Aviation Organization (ICAO) [144] or the EU/BSI [33], however these are no independent protocol sets since EU protocols proven as more effective or more secure can become an ICAO standard, as was the case with the PACE protocol, which will first supplement and later on replace the BAC protocol. All protocols relevant for this thesis are discussed in chapter 4, as well as the two related Public Key Infrastructures (PKI) in section 3.2 and the actual data on the chip in section 3.1, the so-called Logical Data Structure (LDS).

## 3.1. eMRTD Logical Data Structure

The LDS is a standardised data structure for global interoperability between ICAO countries and their inspection system terminals [143]. Furthermore, all data elements are flagged as mandatory, conditional or optional. The current LDS versions of travel documents in circulation are version 1.7 and 1.8, furthermore a future LDS 2.0 is discussed, which enables writing to the ePassport by authorised terminals to specified data groups [141]. Proposed LDS 2.0 use cases comprise digital entry/exit stamps, visa information, and additional biometrics for automated border clearance details [135]. At the moment of writing LDS 2.0 data groups have been removed from the current ICAO Doc 9303 version (see [135, 143]) and future LDS 2.0 developments are unclear.

An overview of the common data groups (DG) is depicted in figure 3.1. Only DG1, DG2, EF.SOD and EF.COM are mandatory for all ICAO compliant ePassports. For instance, the German ePassport contains DG1, DG2, DG3, DG14, EF.SOD and EF.COM

on its chip. The chip is specified to have a minimum storage capacity of 32 kB [143], however the facial image in DG2 already requires 15 kB to 20 kB, so if fingerprints shall be stored in DG3 a chip with more storage capacity is required. No upper limit for the storage capacity is specified.

*DG1* contains the same data as the Machine-Readable Zone (MRZ), the detailed data elements are listed in figure 3.1.

*DG2* - *DG4* contain biometric features of the document holder. *DG2*, the encoded facial image, is the only mandatory global interchange feature. *DG3* contains biometric references for the document holder's two index fingers, which is optional on a global level, but mandatory for ePassports issued within the EU [88]. *DG4* is reserved for pictures of the eyes to enable iris or retina based biometrics, but is currently not utilised.

*DG5* consists of additional non biometric facial portrait images to be displayed during the border check. As of today, it is mainly unused.

*DG7* can embed multiple recordings of the document holder's handwritten signature.

*DG14* is utilised for storing the so called *SecurityInfos* data structure for EU passports and the associated EAC protocols (see [143] for details).

*DG15* may shelter the public key of the Active Authentication protocol (see [143]).

*DG6, DG8, DG9, DG10, DG11, DG12, DG13, DG16* are either reserved for future use, currently not populated with actual data or available for temporary proprietary (state specific) use.

*EF.COM* contains version information of the LDS as well as a list of the present data groups. Since this file is not protected against modification, it is vulnerable to downgrade attacks on some terminals [9]. It is still a mandatory file, but the version information has also been added to the digitally signed *EF.SOD* container.

*EF.SOD* is the Document Security Object, which is a digitally signed structure including hash values of the available LDS data groups DG1 to DG16. The digital signature is created by the document issuing state's document signer during the personalisation phase of the document and verified as part of the Passive Authentication protocol with aid of the Country Signing PKI (see section 3.2 and chapter 4).

*EF.CardAccess* is only required if the document supports the currently optional PACE/SAC protocol (see chapter 4) and contains a *SecurityInfos* structure with protocol specific data.

*EF.CardSecurity* is similar to *EF.CardAccess* a conditional data structure that is only needed if the document supports the PACE/SAC protocol with Chip Authentication mapping (see [143]) and embeds a *SecurityInfos* structure for the protocols in question.

*EF.ATR/INFO* reports if the chip supports the conditional extended length mode specified in [154].

## 3.2. eMRTD Public Key Infrastructures

The PKI relevant for the ICAO security protocols is either called eMRTD PKI (in ICAO documents) or to distinguish it better from other eMRTD related PKIs Country Signing PKI. In this thesis it is referred to as Signing PKI. It is needed during Passive Authenti-

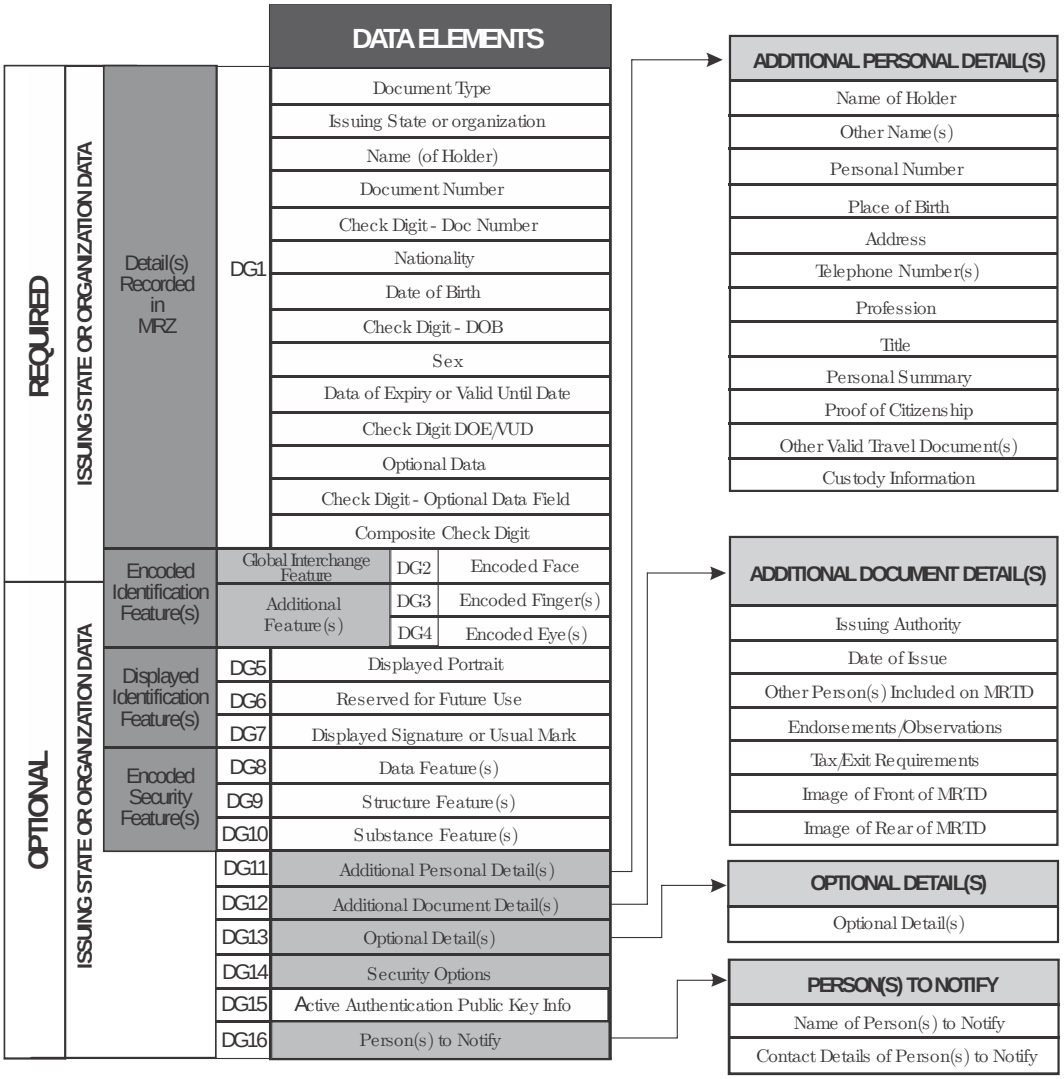



Figure 3.1.: eMRTD Logical Data Structure [143].

Table 3.1.: Distribution channels for Signing PKI certificates [145].

| | CSCA Certificates | DS Certificates |
|---|---|---|
| Primary | Bilateral | eMRTD chip |
| Secondary | Master Lists | ICAO PKD |

Table 3.2.: Key usage period for Signing PKI keys [145].

| | Use of Private Key | Public Key Validity (10-year valid passport) |
|---|---|---|
| CSCA | 3-5 years | 13-15 years |
| DS | Up to 3 months | $\approx$ 10 years |

cation to verify the digital signature of the Security Object *EF.SOD* on the eMRTD. The Signing PKI consists of two levels, which are the Country Signing Certificate Authority (CSCA) and the Document Signers (DS). For every state issuing an ICAO compliant ePassport there exists exactly one CSCA with a self-signed root certificate and the CSCA is the only CA in the infrastructure. The certificates used by the Signing PKI are X.509 compliant certificates [63, 278] and conform to the profile specified in [145]. According to ICAO multiple Document Signers per country are allowed, however the EU specified that only one DS per member state must exist.

On the one hand, the signing path results from the CSCA private key signing the DS public key and the DS private key signing the Document Security Object *EF.SOD* during the personalisation phase of the document. On the other hand, the verification path is derived from the Document Security Object's *EF.SOD* signature requiring the DS public key for verification and the DS certificate's signature depending on the CSCA self-signed certificate's public key for verification. The Signing PKI with the corresponding signing path and verification path is depicted in figure 3.2.

*EF.SOD* signatures must be verifiable for 5 to 10 years. The digital signature is commonly an RSA signature [254] or ECDSA signature [157], however DSA [97] is also part of the ICAO standard, but is currently (Aug. 2018) not used in practice . Currently the only allowed cryptographic hash functions are the algorithms from the SHA-2 family, i.e. SHA-224, SHA-256, SHA-384 and SHA-512 [95].

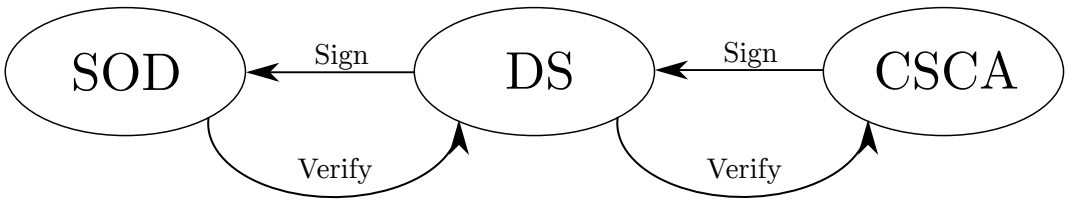



Figure 3.2.: The Signing PKI.

Common distribution channels for the certificates are specified in table 3.1. CSCA certificates are either distributed through bilateral diplomatic means or received via

the master lists e.g., ICAO PKD master list, BSI master list. DS certificates can be extracted from the eMRTD chip or downloaded from the ICAO PKD. Within the Signing PKI, Public Key and the corresponding Private Key have different validity periods; an overview is listed in table 3.2. On the one hand, the concrete validity period of the private key is specified by the individual country taking into account the number of documents signed with a private key per day. On the other hand, the validity of the public key is the sum of the private key validity period added with the validity period of the eMRTD issued [145].

Bilateral exchange as primary distribution mechanism is not fixed to a specific technology, e.g. it can be executed by diplomatic couriers or email exchange and depends on the issuing state's policies. In contrast to the bilateral exchange of certificates between eMRTD issuing states, the ICAO Public Key Directory (PKD) is openly accessible by anyone. Public access is limited to read access, for uploading (writing) certificates to the PKD an official, commercial ICAO PKD membership is necessary with out-of-band authentication. The initial ICAO PKD until 2015 was maintained by the Asian Nettrust Pte Ltd contractor, which hosted the primary directory in Singapore and the backup mirror in Bangkok Thailand [136], however today the ICAO PKD is maintained by the German D-Trust GmbH (Bundesdruckerei GmbH). The current primary mirror is hosted by D-Trust in Berlin, Germany and the secondary mirror is located in Abu Dhabi, United Arab Emirates and hosted by the Abu Dhabi Police GHQ [50]. As of May 2016, 52 countries are members of the ICAO PKD.

The second PKI required by the EU EAC protocol Terminal Authentication is the so-called Verifying PKI. EU EAC is used to provide an additional more secure access control mechanism for the sensitive biometric information stored on the eMRTD chip. Certificates of the Verifying PKI encapsulate the access rights for DG3 and can be used by an inspection system to request access to an ePassport supporting EU EAC. Similar to the Signing PKI, the Verifying PKI has one root CA per country, the so called Country Verifying Certificate Authority (CVCA) and multiple SubCAs the Document Verifiers (DV). Common DVs are the border police, e.g. at airport border control. The third PKI entity is the terminal certificate which inherits the access control from the DV certificate. The two biggest differences compared to the Signing PKI are on the one hand, the eMRTD chip has to verify the certificate chain itself, and on the other hand, the chip only knows the CVCA certificate from its issuing country and is unfamiliar with other member state certificates. Therefore, the DV needs a separate certificate chain ending with the eMRTD's known and trusted CVCA certificate for every EU member state. The required cross-border communication for certificate issuing and certificate request signing is one of the biggest drawbacks of EU EAC. The Verifying PKI and the cross-border communication is depicted in figure 3.3.

For issuing the terminal certificates the DV does not need to contact every country itself, but instead every country maintains a so-called Single Point of Contact (SPOC), which is responsible for transnational communications and cross-border certifications. Each country that issues an eMRTD with EAC support or wants to read an eMRTD needs its own SPOC. The protocols of the SPOC for operations across international borders have to handle the following use cases [56]:

- "A DV wants to send a certification request to a foreign CVCA."
- "A CVCA wants to send the issued certificate to the requesting DV."
- "DV and CVCA can request a list of valid certificates needed to read an eMRTD."
- "General messages can be exchanged between the national Verifying PKIs."

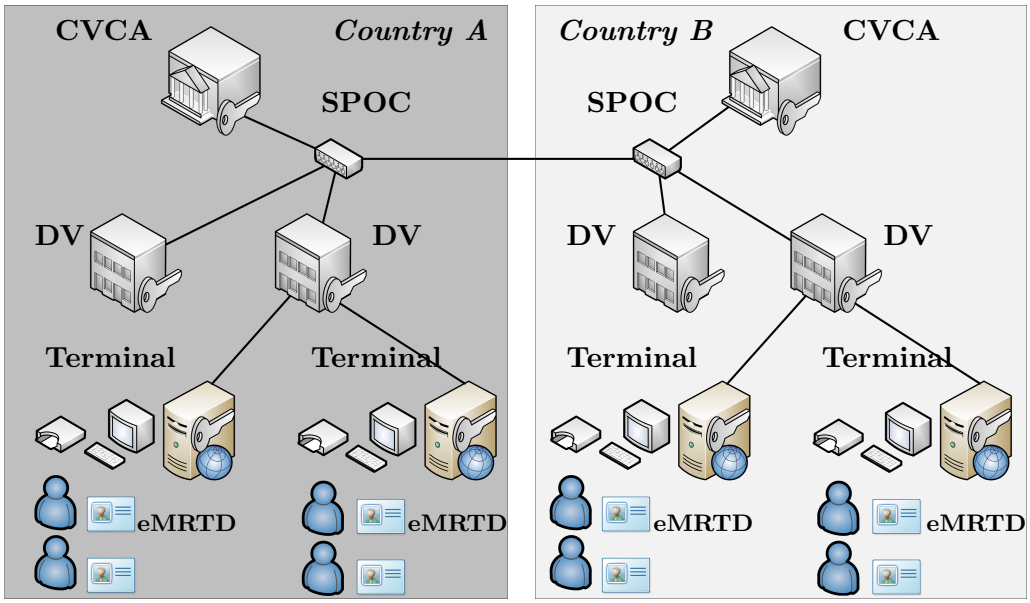



Figure 3.3.: The Verifying PKI and SPOC [41].

These operations are specified together with two designated operation channels. The first is based on a web service interface and the second relies on manual exchange of removable media like USB storage devices, CD-R, DVD-R media, or publication on the Internet. The web service is protected by at least TLS v1.0 [76] with Client and Server authentication. The manual out-of-band communication through diplomatic means specifies the structure of the exchanged media and which metadata has to be provided in form of hash values for the transported data.

# 4. eMRTD Security Protocols

This section describes the common security protocols for eMRTDs specified by ICAO [144] and the EU/BSI [33]. Table 4.1 summarises the cryptographic building blocks of the protocols, indicates if they are mandatory or optional following the ICAO standards and highlights their desired security goals. All protocols are described with a focus on their basic cryptographic mechanisms, so the actual implementation can differ slightly for technical reasons, but does not alter the underlying construction. A sequence diagram notation overview for the security protocols can be found in the appendix on page 167.

## 4.1. Passive Authentication

Passive Authentication is the only mandatory security protocol specified by ICAO [144], which ensures authenticity and integrity of the data stored on the chip. Therefore, the inspection system can ensure that the LDS data groups were created by an official document signer and have not been changed by a third party. The protocol relies on the Signing PKI, discussed in section 3.2 which has three main entities: the country signing certificate authority, the document signer and the digital signature on the eMRTD chip. The dependency of these three entities is depicted in figure 4.1.

The verification does not rely on computation power of the eMRTD chip, so the chip is passive during the authentication via the inspection system, hence the name passive authentication. To verify the digital signature stored in the document security object (SOD) against the LDS data groups on the chip, the following steps are mandatory during passive authentication and performed by the inspection system [144]:

1. Read the Document Security Object, which contains the DS certificate as well as the actual digital signature.

Table 4.1.: eMRTD security protocols summary [144, 33].

| Protocol | Security Goal | Mandatory | Mechanism |
|---|---|---|---|
| Passive Authentication | Data Authenticity | Yes | Digital signature |
| Active Authentication | Chip Originality | No | Challenge-response |
| Chip Authentication | Chip Originality | No | Diffie-Hellman |
| Basic Access Control | Access Control | No | Challenge-response |
| PACE | Access Control | No | Diffie-Hellman |
| Terminal Authentication | Access Control | No | Challenge-response |
| Secure Messaging | Confidentiality | No | Encryption |

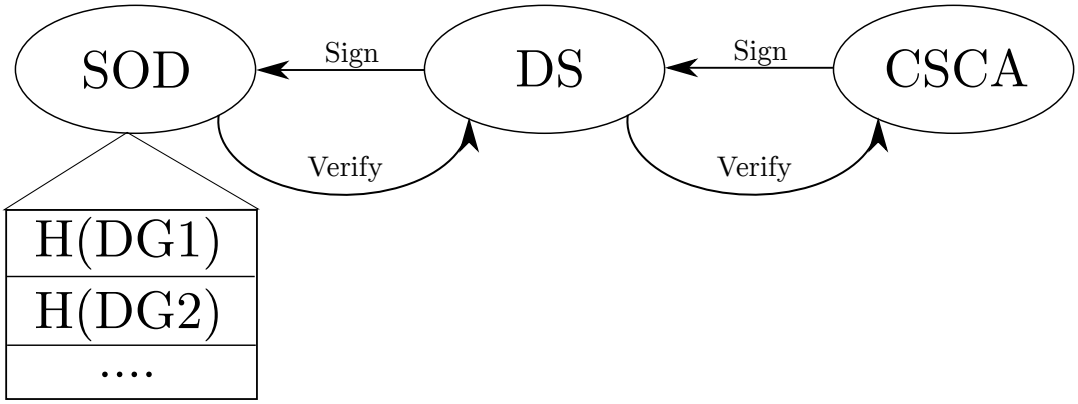



Figure 4.1.: The Passive Authentication protocol and the Signing PKI.

2. Verify the DS certificate with the appropriate trust anchor – i.e. the root CSCA certificate.
3. Extract the public key from the verified DS certificate to verify the digital signature embedded in the SOD.
4. Read Data Groups needed by the inspection system for further actions (e.g. biometric verification).
5. Hash the individual data groups and compare the hash values to those stored in the verified SOD.

Further steps are not mandatory for passive authentication, but are considered good practice to enhance the security:

1. Check if the DS certificate contains the *DocumentType* extension [145], if yes compare it to the document type stated in DG1 and the visual MRZ. If no suitable extension is found check if the *KeyUsage* extension [63] has the *digitalSignature* flag set and no *ExtendedKeyUsage* extension [63] is present.
2. Check consistency of the country code between DG1, the visual MRZ and the Subject-fields of the DS and CSCA certificates.
3. Compare the content of DG1 with the visual MRZ.
4. Check if the document's issuing date of the eMRTD is within the usage period of the DS certificate's private key usage period, specified in the *PrivateKeyUsagePeriod* extension [63] of the DS certificate.

These enhanced steps can detect chip substitution and according to [136] it further makes stolen blank eMRTDs useless. However, if the attacker is able to forge the physical document, a chip cloning can only be detected by Active Authentication or Chip Authentication. During the certificate chain validation all certificates of the certification path are also checked against corresponding CRL lists, e.g. from the ICAO PKD.

## 4.2. Active Authentication

Active Authentication (AA) is a protocol to counter chip cloning and chip substitution by ensuring the authenticity of the chip, which is also referred to as originality. If an eMRTD supports Active Authentication, DG15 is present and contains the Active Authentication Public Key. In contrast to Passive Authentication the eMRTD requires processing power to actively compute, therefore the protocol is called Active Authentication. The protocol is depicted in figure 4.2. Active Authentication is a classical challenge response protocol and consists of the following steps [144]:

1. The inspection system sends an 8 byte nonce M1 (challenge) to the eMRTD chip.
2. The eMRTD chip:
   a) Generates an algorithm specific message M2, which depends on the use of RSA oder ECDSA.
   b) M1 and M2 are concatenated and $h = H(M1|M2)$ is computed with an appropriate hash function $H$.
   c) Computes a digital signature according to [155] without $H$ enabling message recovery and sends the result to the inspection system.
3. The inspection system:
   a) Verifies the digital signature with the public key extracted from DG15.
   b) Checks that the eMRTD returned the correct nonce.
   c) The authenticity of the AA public key is verified beforehand via validating DG15 as part of Passive Authentication.

After these steps the inspection system can be sure that it is communicating with a genuine chip and if DG1 is compared to the visual MRZ it is established that the chip, the LDS data groups, and the physical document belong to each other. The AA Private Key used during signature generation is stored in a secure memory area of the eMRTD chip and not accessible by the inspection system. Therefore, the *AA Private Key* cannot be cloned in practice.

Active Authentication is an optional ICAO standard [144], but not used in Germany due to a potential privacy tracking issue referred to as challenge semantics, which is discussed in [33]. The privacy threat occurs due to the circumstance that the challenge is signed by the document without checking any semantics of the challenge. Therefore, the signature can be used to cryptographically prove to a third party that the eMRTD signed a specific value and thereby can be misused for tracking of the eMRTD. To summarise the Active Authentication protocol prevents cloning very efficiently but also provides non-repudiation in a use case where this security goal is undesired, thus the German ePassport uses Chip Authentication to prove chip originality instead.

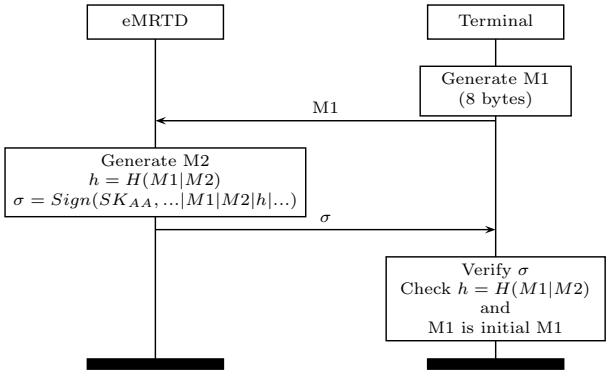



Figure 4.2.: The Active Authentication protocol.

## 4.3. Chip Authentication

Chip Authentication is designed to improve upon the shortcomings of Active Authentication, thereby not risking eMRTD tracking and providing strong session keys. Three versions of Chip Authentication exist for common document types, i.e. ePassport, eID and eIDAS token [33]. This section discusses a generic version since the details of the specific versions are neither important to the general protocol principal nor to the focus of the thesis.

The protocol is part of the EU Extended Access Control implemented in EU ePassports, but has also become a stand-alone protocol as ICAO standard [144]. Similar to Active Authentication Chip Authentication has a static key pair consisting of a private key stored in a memory region only accessible to the eMRTD chip and a public key stored as part of the *SecurityInfos* structure in DG14, which is protected by Passive Authentication against modification. Chip Authentication consists of an ephemeral-static Diffie-Hellmann key agreement and a final key derivation step for an encryption key and a MAC key.

The protocol is depicted in figure 4.3 and consists of the public key exchange and the Diffie-Hellmann key agreement. From the common secret $K$ both parties derive session keys for encryption and the MAC.

During the protocol no transferable signature is created by the eMRTD chip, so no transferable privacy or tracking issues exist. The derived session keys are used for the Secure Messaging protocol after Chip Authentication was successful. If the chip supports Chip Authentication, it is indicated by the presence of a Public Key *SecurityInfos* structure in DG14.

## 4.4. Basic Access Control (BAC)

BAC is a protocol recommended by ICAO, but not a mandatory component. It prevents eavesdropping (passive attacks) and skimming (active attacks) on the communication between eMRTD and inspection system (IS) to protect the document holder's privacy.

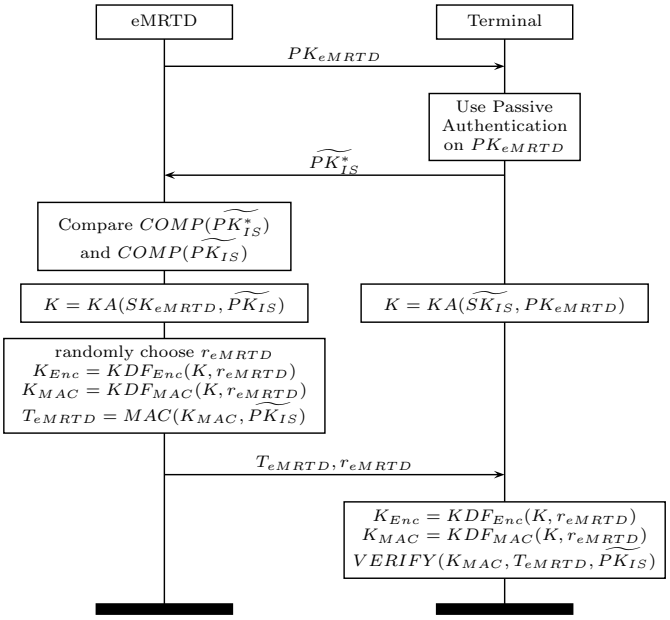



Figure 4.3.: The Chip Authentication protocol [44].

The protocol is a three-pass challenge response mutual authentication solely based on symmetric cryptography, namely 3DES [93] as block cipher and a MAC [156] also based on 3DES. 16 byte of keying material is generated whereof each party contributes 8 byte of random data. Out of this keying material a key derivation function (KDF) generates session keys to be used for *Secure Messaging* to establish a secure cryptographic channel between eMRTD and inspection system providing authenticity, integrity and confidentiality.

BAC ensures that the inspection system has optical access to the data page, because the shared secret is computed by reading values from the MRZ and hashing them. In detail document number, date of birth and date of expiration are read and concatenated, from the resulting string the SHA-1 hash is calculated and the most significant 16-byte of the resulting hash are used as seed for the KDF. Since the MRZ is only optical accessible if the ePassport booklet is open, the underlying idea is that access to the chip is only possible if the document holder knowingly offered the eMRTD to the inspection process.

The protocol is depicted in figure 4.4 and consists of the following steps [144]:

1. The inspection system requests a challenge $RND.eMRTD$ from the eMRTD.
2. The eMRTD sends a challenge $RND.eMRTD$ to the inspection system.
3. The inspection system:
   a) Generates a nonce $RND.IS$ and a random key part $K.IS$.
   b) Concatenates $S = RND.IS||RND.eMRTD||K.IS$.

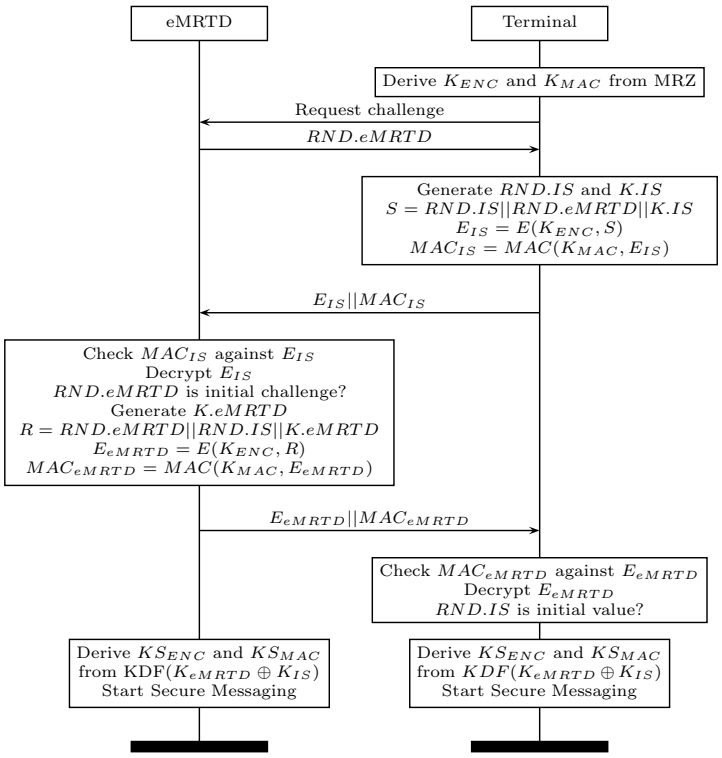



Figure 4.4.: The BAC protocol.

c) Encrypts $E_{IS} = E(K_{ENC}, S)$.

d) Calculates the checksum $MAC_{IS} = MAC(K_{MAC}, E_{IS})$.

e) Sends $E_{IS}||MAC_{IS}$ to the eMRTD.

4. The eMRTD chip:
   a) Checks the MAC $MAC_{IS}$ of $E_{IS}$.
   b) Decrypts $E_{IS}$.
   c) Extracts $RND.eMRTD$ and checks if it is equal to the initial challenge sent to the inspection system.
   d) Generates the random key part $K.eMRTD$.
   e) Concatenates $R = RND.eMRTD||RND.IS||K.eMRTD$.
   f) Encrypts $E_{eMRTD} = E(K_{ENC}, R)$.
   g) Calculates the checksum $MAC_{eMRTD} = MAC(K_{MAC}, E_{eMRTD})$.
   h) Sends $E_{eMRTD}||MAC_{eMRTD}$ to the inspection system.
5. The inspection system:
   a) Checks the MAC $MAC_{eMRTD}$ of $E_{eMRTD}$.
   b) Decrypts $E_{eMRTD}$.
   c) Extracts $RND.IS$ and checks if it is equal to the initial value.
6. Both parties derive Session keys $KS_{ENC}$ and $KS_{MAC}$ using a hash based KDF with $K_{eMRTD} \oplus K_{IS}$ as input.

The derived session keys are used to start Secure Messaging. BAC is subject to criticism in scientific publications (e.g. [109]), whereby the main concern is the low entropy of the static key retrieved from the MRZ. The maximum entropy of the key is ≈56bits [144] and is lower if the attacker can roughly guess the document holder's age or the document's issuing date. It is also possible to capture the handshake and brute-force the key on external more powerful hardware, a so called off-line brute-force attack. In the long-term the PACE protocol will replace the BAC protocol as default eMRTD access control mechanism [144]. Support for BAC is detected by the inspection system if the eMRTD does not support PACE and access to all LDS DGs is denied by the chip until BAC has been performed.

## 4.5. Password Authenticated Connection Establishment (PACE)

PACE is a more secure replacement for the BAC protocol, which fulfils the same security goals, but due to utilising asymmetric cryptography yields session keys with higher entropy and is resistant to off-line brute-force attacks [33]. It was first introduced in the

German eID card (i.e. nPA), but has since become an ICAO standard in the form of Supplemental Access Control (SAC). SAC shall supplement BAC until the end of 2017. So if an ePassport supports PACE it must also support BAC, but it is recommended to establish session keys with PACE in this scenario. ePassports utilising PACE without BAC are permitted starting January of 2018 [144]. In contrast to BAC, PACE does not rely on a fixed key agreement mechanism. Comparable to the TLS cipher suites an eMRTD presents its supported algorithms in the EF.CardAccess file. Based on this file the inspection system can decide if the presented eMRTD does support PACE/SAC in the first place. If the file is not available, the inspection system will fall back to BAC. PACE is also more flexible regarding its pre-shared key, since besides the MRZ information, a PIN known to the document holder, or a Card Access Number (CAN), which is a 6-digit numeric string printed on the document, can be served to the PACE mechanism. The concrete input depends on the eMRTD use case and support of the individual eMRTD, since only support for the MRZ key derivation is mandatory, which is similar to the BAC variant.

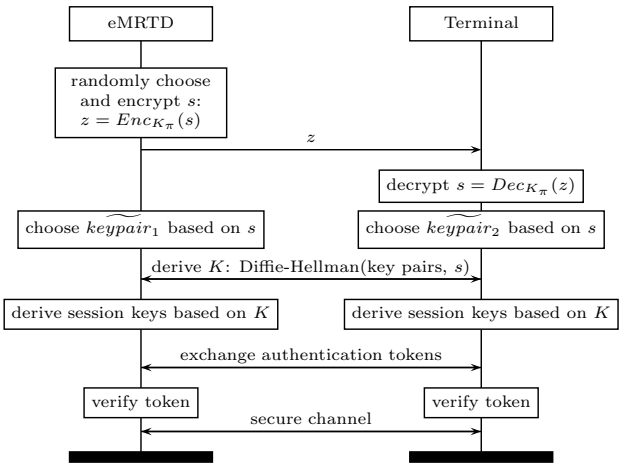



Figure 4.5.: The Password Authenticated Connection Establishment (PACE) protocol [44].

The PACE protocol is depicted in figure 4.5 and consists of the following steps [144]:

1. The eMRTD randomly generates a nonce s, encrypts it with the pre-shared secret $\Pi$, $z = E(K_\Pi, s)$ and sends the resulting ciphertext to the inspection system.

2. The inspection system decrypts the received ciphertext with a key derived from the shared secret $\Pi$, $s = D(K_\Pi, z)$.

3. Both parties:

   a) Exchange further data, if necessary, for the domain parameter mapping and compute the ephemeral domain parameters $\mathcal{D} = MAP(\mathcal{D}_{eMRTD}, s, ...)$.

b) Perform a Diffie-Hellman key agreement using the domain parameters and obtain the shared secret $K = KA(SK_{DH,eMRTD}, PK_{DH,IS}, \mathcal{D})$ $= KA(SK_{DH,IS}, PK_{DH,eMRTD}, \mathcal{D})$.

c) Ensure that $PK_{DH,eMRTD}$ and $PK_{DH,IS}$ are different.

d) Derives session keys $KS_{MAC} = KDF_{MAC}(K)$ and $KS_{ENC} = KDF_{ENC}(K)$.

e) Exchange and verify authentication tokens (i.e. MACs), $T_{IS}$ $= MAC(KS_{MAC}, PK_{DH,eMRTD})$ and $T_{eMRTD} = MAC(KS_{MAC}, PK_{DH,IS})$

4. The retrieved session keys are used to start secure messaging.

ICAO recommends the use of PACE/SAC as default access control mechanism for eMRTDs issued as of December 2014 [122]. A formal security proof for the PACE protocol was published by Bender *et al.* [13].

## 4.6. Terminal Authentication

Terminal Authentication is a protocol mainly used as part of the EU EAC to grant access to more sensitive data like the document holder's index finger images in DG3, using a two move challenge-response for explicit authentication of the terminal. The maintenance of the underlying PKI infrastructure, the so called Verifying PKI, is more complicated than the actual protocol [33].

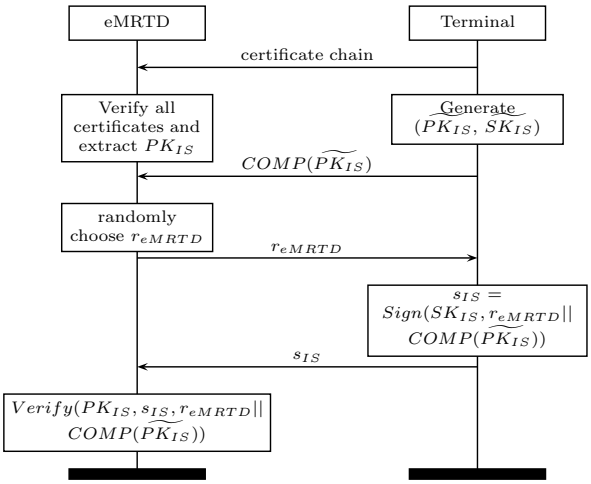



Figure 4.6.: The Terminal Authentication protocol [44].

Terminal Authentication is depicted in figure 4.6 and consists of the following steps:

1. The inspection system sends a certificate chain to the eMRTD, which ends with a certificate verifiable by the eMRTD's CVCA public key stored on the eMRTD. So the chain consists of an inspection system certificate and a document verifier certificate signed by the proper CVCA.

2. The eMRTD:
   a) Verifies all certificates and retrieves the inspection systems Public Key $PK_{IS}$.
   b) Sends a challenge $r_{eMRTD}$ to the inspection system.
3. The inspection system generates the signature $S_{IS} = Sign(SK_{IS}, ...||r_{eMRTD}||...)$ and sends it to the eMRTD.
4. The eMRTD verifies the signature $Verify(PK_{IS}, S_{IS}, ...||r_{eMRTD}||...) = True$ and grants access to the sensitive data groups according to the access control extension present in the inspection system certificate.

The actual access rights are decided upon and granted by the issuing state. Since Terminal Authentication grants access to the most sensitive data groups, the use of Secure Messaging is specified as mandatory.

## 4.7. Secure Messaging

Secure Messaging is the main data transport protocol which ensures authenticity, integrity and confidentiality of the transferred data between inspection system and eMRTD. As input the protocol receives one key for encryption $K_{ENC}$ and one key for MACs $K_{MAC}$. The keys can be retrieved during BAC, PACE or Chip Authentication and the session keys might be switched e.g. from PACE to Chip Authentication during the inspection process. It is comparable to the TLS record layer, but since it uses an encrypt-then-authenticate mode it is more similar to IPsec [173]. Secure Messaging is specified in [144].

## 4.8. Extended Access Control (EAC)

According to ICAO EAC is an access control mechanism that prevents unauthorised access to the additional biometrics (i.e. all besides the facial image). The official ICAO standard does provide an EAC specification proposing a separate EAC key access method similar to BAC, but leaves the concrete mechanism open to the issuing states. Therefore, multiple EAC variants exist, e.g. the EU EAC [33] and the Singapore EAC [139, 266]. The EU EAC consists of Terminal Authentication and Chip Authentication to protect access to the mandatory fingerprints present in EU ePassports, and was decided upon by the Brussel Interoperability Group (BIG) as well as specified for second generation ePassports in EU Article 6 [138]. These are all ePassports issued by the EU member states since June 28th 2009 [137]. The security of the EU EAC protocols was analysed by Dagdelen and Fischlin [66]. Singapore EAC in contrast to EU EAC is an access control mechanism, which ensures that all inspection systems in Singapore have access to the biometric data, but access control for other countries is not provided [139, 266]. Shortcomings of EU EAC are discussed in the next chapter 5.

# 5. Shortcomings of the current EU EAC and related work

## 5.1. Shortcomings

This EU EAC discussion is based on [40, 41]. Although the new protocols specified by the EU EAC standard [33] are sophisticated and thus enhance the security of former protocols, the current EAC standard still offers two unsolved weaknesses. They are linked to the Verifying PKI and the associated Terminal Authentication. First, the eMRTD has no access to a precise and authentic time source, so it can not accurately validate if a terminal certificate is still valid. Instead, a pseudo clock mechanism is used, which is described below. The second problem is that a certificate once issued stays valid until the expiration date no matter what happens. So no actual revocation mechanism is present, but instead to limit the value of a stolen inspection system the issued inspection system certificates have a very short validity period, usually only one day. On the one hand, this creates an enormous effort with respect to both generation of key pairs/certificates and their distribution and on the other hand, this strategy does not provide the same security level as a revocation, because of the pseudo clock mechanism an expired certificate can still be accepted as valid.

As announced above the missing time source is replaced by a pseudo clock mechanism, which works as follows:

The eMRTD stores a date $T_{eMRTD}$ in an internal register which gets updated during the Terminal Authentication. Initially $T_{eMRTD}$ is set during the chip personalisation to the personalisation date.

During the Terminal Authentication the eMRTD reads the "Expiration date" $T_{Cert,Expiration}$ field from all certificates and validates that $T_{Cert,Expiration}$ is not before $T_{eMRTD}$.

After every successful Terminal Authentication the eMRTD chip reads all certificates from the chain and checks which got the latest "Effective Date" $T_{Cert,Effective}$ field, which is the equivalent of the "Not Before" field from X.509 certificates. If $T_{Cert,Effective} > T_{eMRTD}$ then $T_{eMRTD}$ is set to $T_{Cert,Effective}$ and stored in the internal register [33][269].

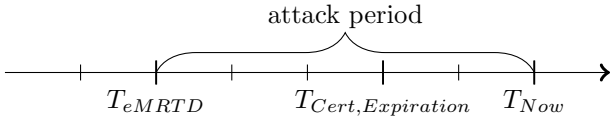



Figure 5.1.: Timeframe for stolen inspection system attack.

The problem which arises is that the eMRTD chip can only detect a past $T_{Cert,Expiration}$ value if it is used often, because then $T_{eMRTD}$ is relatively accurate. Nevertheless, an eMRTD chip cannot be sure if a terminal certificate is actually still valid, because if $T_{eMRTD} \leq T_{Cert,Expiration} < T_{Now}$ the eMRTD will not detect an expired certificate. The possible stolen inspection system attack period is shown in figure 5.1. So for a successful attack the attacker must already have a valid certificate, and can then expand the time period in which the terminal can read biometric data. This only works if the eMRTD's chip gets no accurate time update from another terminal.

Possible reasons why the eMRTD got no internal clock might be explained from the problems that arise if anyone tries to integrate a clock into an eMRTD, e.g. the missing power source.

## 5.2. Related work regarding EU EAC

This section summarises related contributions and evaluates their findings regarding EU EAC improvements:

### 5.2.1. Entrust

Moses [208] gives in the white paper from Entrust a comprehensive view on the weaknesses of the current Verifying PKI and proposes a workaround. Instead of revoking the certificates and providing a real-time clock, the author proposes to compensate this deficiency with strong confidential storage and restriction of using the reader's private key to authorised operators, e.g., due to a storage of the private key in the back office. His self-assessment of this solution is: "brittle, because there is no way to recover when it goes wrong" [208]. In contrast, solutions presented in section 8 also work if the terminal's private key has already been compromised. [208] states that the absence of a real-time clock makes revocation ineffective. Section 8 is in consent with this statement and only evaluates solutions that provide a real-time clock and revocation.

### 5.2.2. Vaudenay

Vaudenay and Vuagnoux [283] report the weaknesses of EAC and describe certain attack scenarios, but do not propose improvements for EAC.

Chaabouni and Vaudenay [58] introduce the idea to have identity checks when leaving a domestic country to have more frequent clock updates. To provide certificate revocation they propose a reputation-based trust mechanism where a threshold authentication proof is created by a collaboration of a certain number of neighbour terminals. The proposed additional identity check does indeed shorten the possible attack period, but it does not completely solve the problem, because during a long vacation an eMRTD's date is still not up-to-date. A reputation-based revocation system solves the problem of a single stolen terminal, but the authors present no detailed analysis how to integrate such a revocation system in the eMRTD infrastructure. An attacker still has the option to steal a sufficient number of terminals and compromise them to exceed the threshold for

the authentication proof. Section 8 proposes solutions that provide a real-time date and revocation independent of the number of stolen terminals by an attacker.

### 5.2.3. Chaabouni

Chaabouni extends the ideas from [58] in [57] by presenting an actual implementation for a t-out-of-l threshold signature scheme to augment terminal authentication. The scheme is based on RSA threshold signatures and the actual revocation check is performed by the neighbouring terminals. The main motivation for this approach given by the paper is the fact that terminals have a real clock embedded and more computational power than eMRTDs and are therefore better suited for checking the revocation status. Even though this is true and the steps from the theoretic idea [58] to an actual implementation [57] should be acknowledged the basic idea still suffers from the same problems as discussed for [58], and now with an actual implementation some new deficiencies surface. An attacker can still steal t-out-of-l terminals to exceed the threshold, which is a relevant problem simply because why should an attacker perform the illegal act of breaking and entering to only steal one terminal and not t terminals. Another problem with the threshold mechanism is that it does not consider small border check stations (or less affluent countries) with only two to three mobile terminals which make a threshold system nearly pointless. The biggest problem with the proposed scheme is that it relies on the assumption that Document Verifiers are trusted participants. This might be true for the majority of DVs, but should not be a general rule, because such a revocation mechanism is powerless against rogue DV certificates and trust issues towards DVs in countries with poor relations. A revocation mechanism in the eMRTD domain is only needed in rare special cases, but if it is needed it should be powerful enough to cover all use cases, which the proposed scheme does not fulfil.

### 5.2.4. Li

Li *et al.* [182] present an EAC scheme using identity-based cryptography (IBC) and compare it to the EU EAC system as well as the Singapore EAC scheme [139]. This new authorisation mechanism based on IBC introduces an authentication protocol between the eMRTD chip and a new entity the so called authorised smart card. Every terminal needs such an authorised smart card which stores its public identity information, and in the secure internal memory the terminal's private key. Instead of relying on the Verifying PKI the scheme needs an IBC server system for every eMRTD issuing country to provide the cryptographic services, and the authorisation information is now stored inside the authorised smart card instead of the terminal certificate. The attack scenario therefore shifts from stealing a terminal to stealing an authorised smart card. Therefore, the authors introduce the concept of smart card revocation lists which are stored in data group 13 of the eMRTD. Updating this revocation list is only allowed by a domestic terminal after a successful check. Even so the authors claim that their scheme is less complex than the EU EAC SPOC infrastructure the system relies on an on-line IBC server system to refresh the IBC information after expiration on the authorised smart

card. It is puzzling that this new EAC scheme relies on an on-line system, but the revocation system is constructed from a primitive off-line revocation list system. Since the updates of the revocation lists are only performed if the eMRTD is successfully checked by a domestic terminal, the document holder is not protected against stolen terminals during a stay abroad or the travel between two foreign airports. At first glance the proposed IBC EAC system might seem cheaper to maintain than EU EAC because no more Verifying PKI is needed, but on the one hand, the IBC servers have to be constantly on-line too, and on the other hand, every terminal now needs an authorised smart card. Together with the proposed primitive off-line revocation mechanism the biggest difference to the current EU EAC system is that the authors replace the current EU terminal authentication, which relies on the security of RSA signatures or ECDSA signatures, with an authentication protocol that relies on the security of the ECDLP and the bilinear Diffie-Hellman problem. This might be interesting from a cryptographic perspective, but does not solve the problem of stolen terminals.

### 5.2.5. Pasupathinathan

Pasupathinathan *et al.* [226] present a self-made protocol called On-line Secure E-Passport Protocol (OSEP Protocol). The authors claim to solve weaknesses of EAC. The OSEP protocol drops the access control flexibility of EAC and a terminal sends private information from the eMRTD to the country's embassy. In contrast to Pasupathinathan *et al.* [226] both facts raise privacy concerns: a terminal, which needs access to the document holder's name stored on the chip should not automatically get access to the sensitive fingerprints. Furthermore, countries, which may track travellers through their embassies, is a show-stopper for any travelling privacy. Comparable to [125] no other self-made protocol is needed where no practical experience data exists how the protocol performs in practice. It is not considered realistic that the EU will drop EAC, because of a practically untested, self-made protocol. With these characteristics, the OSEP protocol disqualifies itself and will not be evaluated against the proposals in section 8.

# Part III.

# Future Travel Document Infrastructure and Protocols

# 6. Enhancing eMRTD SPI via Blockchain Technology

This section presents the underlying ideas of blockchain technologies and how these can be integrated into the identity life cycle to strengthen its weakest links, the breeder documents. After introduction of the underlying technologies, this section presents a cost-efficient way to enhance the long-term security of breeder documents by utilising blockchain technology. A conceptual architecture to enhance breeder document long-term security and an introduction of the concept's constituting system components is presented.

The technical discussion is based on [215, 214] and the presented breeder document concept on [45]. Summarised Bitcoin is a cryptocurrency without a trusted central third party. Since Satoshi Nakamoto introduced the modern distributed blockchain protocol in the context of the Bitcoin currency [212], the blockchain basics are also introduced in the context of Bitcoin as they are strongly linked. Bitcoin and blockchain basics are introduced with the breeder document context and focus on security in mind. The linked economic, political and social dependencies of Bitcoin are not discussed since they are out of scope for breeder document security.

Bitcoin is currently the most prominent cryptocurrency, but many alternatives were forked from the prominent Bitcoin client. These alternative coin systems are referred to as Altcoins. Altcoins in general make changes to several properties of Bitcoin to achieve other or more specialised goals.

In the context of blockchain based cryptocurrencies, forks are categorised as soft forks and hard forks. On the one hand, hard forks can introduce new properties that were previously considered invalid, so a new version of the software recognises a block as valid that the old software would reject. On the other hand, soft forks add properties that make validation rules stricter to restrict the set of valid transactions or the set of valid blocks such that the old version would accept all blocks, whereas the new version would reject some blocks [215].

Some of these properties and motivations are:

- Stronger anonymity and privacy properties
- Alternative mining puzzles or strategies
- Different inter block time for higher transaction throughput
- Alternative scripting language e.g., for smart contracts or Turing completeness
- Different block size for higher transaction throughput

## 6.1. Cryptography and Data structures

### 6.1.1. Hash function properties

This section discusses the properties a cryptographic hash function needs to be suitable for a secure blockchain. In the context of blockchains, three basic hash function properties exist and three additional properties that make the hash function secure and practical for the domain at hand.

The basic properties for a blockchain hash function are:

1. It must be able to handle any input from any size.
2. It must produce an output of fixed size.
3. It must be computable in an efficient manner i.e., $\mathcal{O}(n)$ run time, while $n$ is the length of the input data.

The additional blockchain security properties are:

1. *Collision-resistance property:* It is infeasible for an attacker to find two inputs $x$ and $x'$, $(x \neq x')$ such that $\mathcal{H}(x) = \mathcal{H}(x')$.
2. *Hiding property:* If a value $r$ is chosen from a probability distribution with high entropy and an attacker is given $\mathcal{H}(r\|x)$ it must be infeasible to find the input value $x$. This property is related to the preimage resistance of secure cryptographic hash functions [171].
3. *Puzzle friendliness property:* For any given value $y$, if $k$ is chosen from a distribution with high entropy, it is infeasible for an attacker to find an $x$ that holds $\mathcal{H}(k\|x) = y$ in a manner that is significantly faster than brute-force. This property is important for constructing hash puzzles in the mining schemes.

The Bitcoin blockchain uses the SHA-256 hash function [95], which has a fixed 256-bit output and fulfils the given properties.

### 6.1.2. Data structures - Hash pointer, Hash list and Hash tree

A hash pointer is a basic data structure that is frequently used in blockchains and cryptocurrencies. Similar to a regular pointer in computer science a hash pointer points to a location where arbitrary data resides, but additionally provides a cryptographic hash of the data it points to. Therefore, besides retrieving the data a hash pointer makes it possible to verify if the obtained data has been changed. The hash pointer data structure is depicted in figure 6.1.

Main purpose of the hash pointer is to build data structures that are more sophisticated. In general all data structures which can be constructed out of regular pointers can also be built from hash pointers as long as they have no cycles (e.g., a linked list or a binary search tree).

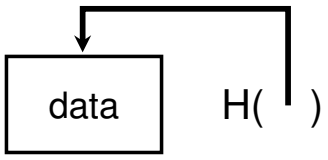



Figure 6.1.: A hash pointer points to data and provides a hash value of that data [215].

A linked list constructed out of hash pointers is referred to as blockchain, hash list, hash chain, hash log, tamper-evident log, or append only log and is the most prominent data structure for cryptocurrencies, which is depicted in figure 6.2. Due to the properties of the hash pointer, data can only be appended to the end of the blockchain data structure. If either a new data block is added to the blockchain in a position besides the end, or an existing data block is changed in the blockchain the hash pointers of all subsequent blocks will detect the modification. Therefore, the only way for an attacker to modify a block $X_i$ in the blockchain is to also manipulate all subsequent blocks $X_{i+1}$ to $X_n$. Since the hash of block $X_n$ is the head of the list, its hash is remembered by all applications and the manipulation would still be detected. Similar to the hash of block $X_n$ called head of the list, the first block $X_0$ has a special name and is referred to as genesis block.

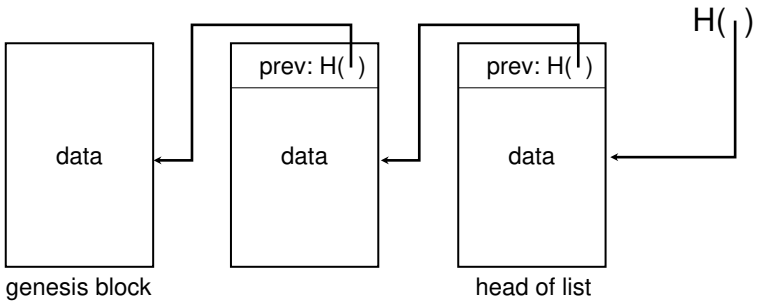



Figure 6.2.: A blochchain is a linked list built with hash pointers [215].

Another data structure that can be build using hash pointers is a binary tree. A binary tree with hash pointers is generally referred to as Merkle tree (depicted in figure 6.3) since it was invented and used most prominently by Ralph Merkle [201] in the context of digital signatures solely build from hash functions (see section 9). In the domain of cryptocurrencies, Merkle trees are usually utilised to efficiently handle verification of stored transactions in a blockchain block. Similar to the head of the list hash in the blockchain, storage of the root hash of the Merkle tree is sufficient to later check integrity of other blocks in the Merkle tree, since manipulation of one of the leaf data blocks makes hash pointers on higher levels of the tree invalid.

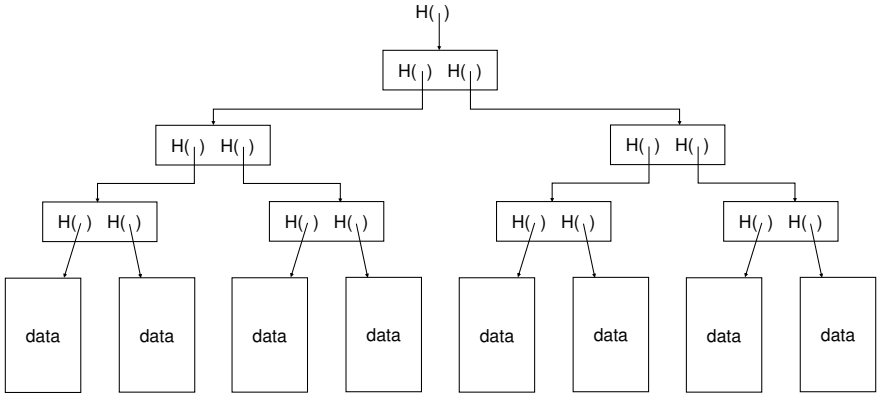



Figure 6.3.: A Merkle tree allows efficient integrity checks of transaction data [215].

## 6.2. Identities, Bitcoin structures and Script

### 6.2.1. Bitcoin Identities, Transactions and Blocks

Bitcoin uses ECDSA [97] as digital signature scheme to sign its transactions, furthermore identities in the Bitcoin network refer to the ECDSA public keys, necessary to verify transactions. Therefore, Bitcoins in a transaction are always sent to a specific public key (identity). The entity with the secret key corresponding to a public key controls the identity and its associated Bitcoins, because only the entity with the secret key can sign new transactions for linked Bitcoins. In Bitcoin these identities are referred to as addresses, so a transaction sends an arbitrary amount of Bitcoins to an address. The nodes in the network have no identity itself, instead identities are always bound to transactions. A block of the Bitcoin blockchain contains multiple transactions, simply for efficiency of validating the blockchain. The Bitcoin blockchain structure is a combination of a hash list and a Merkle tree, and is depicted in figure 6.4. A Merkle tree makes validating a single signature very efficient, since only the transaction path in the Merkle tree has to be validated and the block header solely has to store the Merkle tree root. Therefore, a client with limited storage space can store only the block headers and not the entire blocks of the blockchain. If needed all other data can be retrieved on demand from the other network nodes. Since the maximum Bitcoin block size is one Megabyte and the header size is only 80 byte this strategy saves roughly factor 1000 of storage space [215].

### 6.2.2. Bitcoin Script

All Bitcoin transactions are formulated in a programming language called Script or Bitcoin Script. Bitcoin Script is not Turing complete, but instead based on a simple stack based programming language called Forth [243]. The non-Turing-completeness is by design because it makes it easier to predict runtime and memory limits of the transaction scripts. Also, by omitting loops, no endless loops are possible. Even so

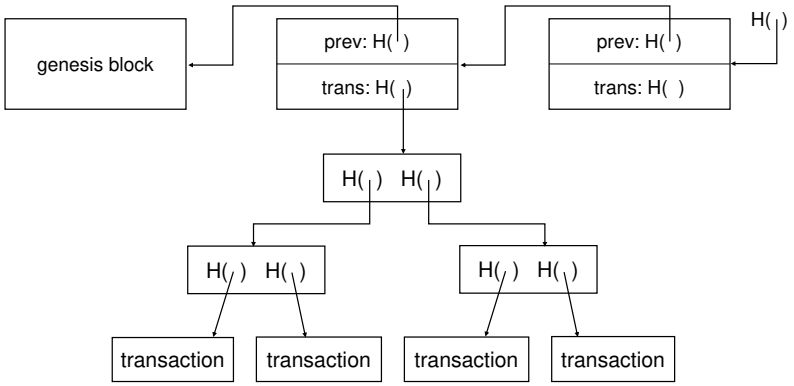



Figure 6.4.: The Bitcoin blockchain consists of a hash chain together with a Merkle tree per block for storing the transactions of the block [215].

Bitcoin Script is script based; the actual representation in the blockchain is a non-human readable binary format for efficiency. If an entire Script can be run without any errors, it is considered a valid transaction. To write arbitrary data in the Bitcoin blockchain a mechanism called proof of burn exists. Proof of burn proves that a certain amount of Bitcoins was destroyed (can never be redeemed), which concretely means that an error is created with the $OP\_RETURN$ command and all further data after the command in the script is ignored by the interpreter. To write arbitrary data into the blockchain usually a very small amount (i.e., a Satoshi, which is the smallest possible transaction value in Bitcoin, $10^{-8}$ BTC) of Bitcoins are burned. Another use case of proof of burn is to prove that a certain amount of Bitcoins were destroyed to redeem a volume of new coins in an Altcoin system. A possible reason for the later scenario would rise if Bitcoin someday became insecure and the current coin values had to be converted to a new secure cash system.

## 6.3. Decentralisation, Distributed consensus and Mining

### 6.3.1. Distributed consensus

Bitcoin does not rely on a central trusted third party, it is based on a peer-to-peer network in which every client has the same privileges and is open to anyone. Since there is no global register in the Bitcoin network, anyone can at any time create a new identity by generating an ECDSA key pair, which is also referred to as distributed identity management. The Bitcoin protocol implements a distributed consensus mechanism to achieve consensus between all genuine clients regarding consistent transactions, which also prevents double spending attacks, one of the core problems of digital cash systems. The distributed consensus ensures that all genuine clients see the same state of the Blockchain. The state of the entire network is independent of the presence of specific nodes, which means that a client is not required to be online to receive Bitcoins. Consensus is not found on individual transactions, but instead on a subset of the currently

open (i.e., unapproved) transactions. This transaction set becomes a new block in the blockchain after distributed consensus. In contrast to distributed databases, Bitcoin does not implement an absolute consent between the genuine nodes, but instead a probabilistic guarantee that increases over time, since new blocks are added to the blockchain. The common heuristic is that after the creation of six valid subsequent confirmation blocks a transaction is considered immutable and part of the long-term consensus blockchain. Since on average a new Bitcoin blockchain block is created every ten minutes this state is reached after roughly one hour. Protection against invalid transactions is enforced by digital signatures, but protection against double-spending is only prevented by the distributed consensus, which works because all genuine nodes will always extend the longest valid blockchain.

### 6.3.2. Mining as Proof of work

Bitcoin incentivises behaving honestly as a genuine node, by rewarding nodes that created new valid blockchain blocks. The overlying process for the distributed consensus is referred to as proof of work or mining and the concrete incentive is implemented via the block reward and the transaction fees. A block reward enables the block creator to insert a special Bitcoin transaction in the new block whose recipient address can be chosen freely. Usually the block creator will send the newly created Bitcoins to one of its own addresses. A block creator has an incentive that its newly created block becomes part of the long-term consensus blockchain, because it contains its reward. Block creation is the only mechanism to create new Bitcoins in the system. The voluntary transaction fees, a transaction creator can choose to make, build further incentive for the block creator, since the block creator receives all transaction fees of the embedded transactions in the block.

Block creators are not selected purely at random but instead by a process called proof of work, which in general is called mining. The proof of work implicitly selects nodes in proportion to its computing power, consequently nodes are competing with each other by their computing power. In Bitcoin the proof of work is accomplished by a hash puzzle. The Bitcoin hash puzzle is depicted in figure 6.5 and in general focuses on finding a nonce for the current block header that satisfies the following equation $\mathcal{H}(\mathcal{H}(block\_header)) < target\_space$ or in more detail:
$\mathcal{H}(\mathcal{H}(Version \| hashPrevBlock \| hashMerkleRoot \| Time \| Bits \| Nonce)) < target\_space$.
The current target space (June 2017) is defined as all double SHA-256 hashes with 72 leading zeros (i.e., difficulty $2^{72}$, and 40 Bitcoin difficulty since 32 leading zeros is the base value). The precise design decision of cascading the SHA-256 function two times in the mining function has never been specified by Satoshi Nakamoto and is open for speculation (e.g., security or speed). So the miner has to find a nonce, such that the double SHA-256 hash of the entire block header starts with the desired number of zeros. Since the Bitcoin hash function fulfils the puzzle friendliness property, miners have to search for a nonce by brute-force until they are successful and have no significant shortcuts. On the one hand, finding a nonce with such properties requires high computational power, but on the other hand, verifying if the nonce is valid is trivial, since a client simply has

to check if $\mathcal{H}(\mathcal{H}(block\_header)) < target\_space$ for the block proposed by the miner. The actual hardness (cost) of solving the hash puzzle (size of the target space) is automatically re-calculated every two weeks by the network to satisfy an average time of ten minutes per block creation. Therefore, the hardness of the mining in general depends on the collective computation power of all active miners. This is done for efficiency of the blockchain and for security, since an attack is infeasible as long as nodes, which follow the official protocol, control the majority of mining power. The opposite is referred to as a 51%-attack, which is possible if a hostile party controls at least 51% of the overall mining power. A 51%-attacker cannot create invalid transactions since the underlying signature scheme (ECDSA) would still be able to detect these invalid transactions, but instead can only censor specific transactions by ignoring them in the block creation. Instead of having one central block creator, all Bitcoin miners compete to create a new block by solving the current hash puzzle to retrieve the block reward and the transaction fees. Not all notes are Bitcoin miners, since solving the Proof of work has become very expensive, due to properties of the SHA-256 function, which are further discussed in more detail in section 6.5.

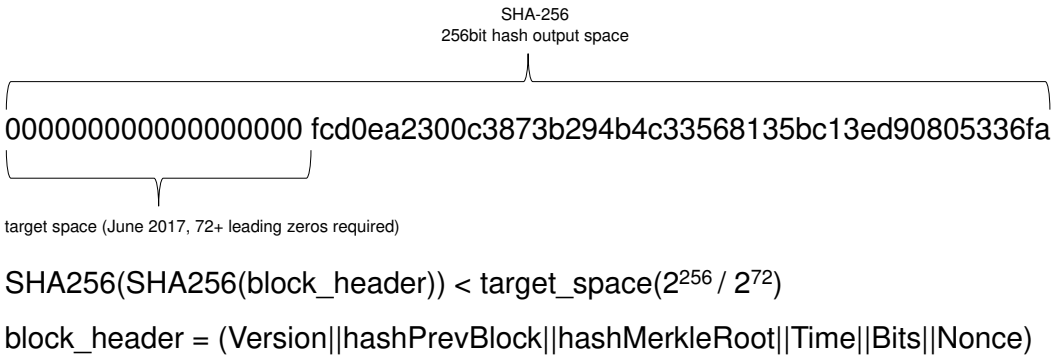



Figure 6.5.: The Bitcoin proof of work is a hash puzzle that involves finding a block nonce that yields a double SHA-256 hash value below the current target space [214].

## 6.4. Bootstrap

Difficulty of the proof of work significantly affects the security of the complete underlying blockchain ecosystem. As depicted in figure 6.6 this dependency is referred to as blockchain bootstrap. Security of the blockchain leads to a stable currency as well as a high value of the currency, since it is widely trusted. If value of the currency is high it is very attractive to start mining (i.e., solving the hash puzzles) for high value rewards, which leads to a healthy mining ecosystem. A healthy mining ecosystem enables high security of the blockchain since it is infeasible to attain the majority (i.e., referred to as 51%-attack) of mining power in the system to censor other transactions. The dependency of these three properties is critical for setting up a secure blockchain. The process

from having none to all three properties at once is referred to as blockchain bootstrap. All new Altcoins have to go through this bootstrap process.

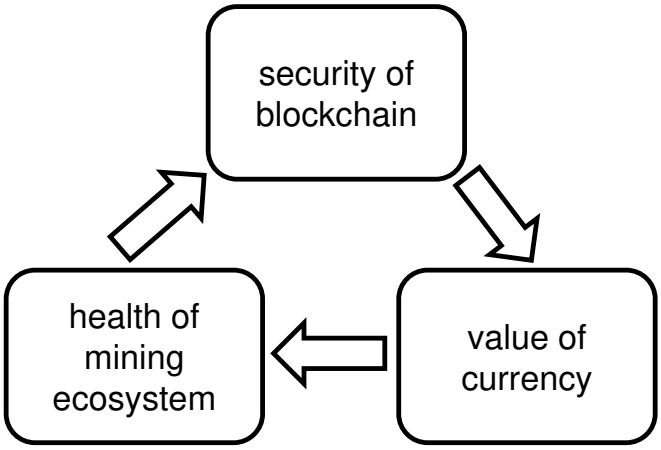



Figure 6.6.: Basic concept of the blockchain bootstrap [215].

## 6.5. Mining Alternatives

This section presents a selection of potential improvements to the Bitcoin proof of work, which are also relevant in case of breeder document blockchain adaption. The core obstacle involves the SHA-256 hash function, which is part of the SHA-2 family and a general purpose cryptographic hash function. SHA-256 today is considered secure, but has no specific optimisation for the Bitcoin mining use case. Since SHA-256 is computable very efficient in hardware, mining today is mostly done with specialised hardware (i.e., Application Specific Integrated Circuits (ASICs)) and not on general purpose PCs. On the one hand, Bitcoin is considered a decentralised cryptographic currency, but on the other hand, the need for specialised hardware in the mining process leads to a centralisation of the miners simply because it has become so expensive and inefficient on commodity hardware. Therefore, Altcoins in particular implement measures to prevent centralisation of the mining process and ASIC resistant hash functions can lower the barrier to the mining entry by reducing the gap between custom ASIC hardware and commodity devices.

### 6.5.1. Pooling resistance

Bitcoin miners mostly do not mine independently but as part of a mining pool to get any reward at all, due to the high computational effort. On the one hand, this is positive for the individual miners since they do not risk investing money in hardware that yields no reward at all, but on the other hand, leads to centralisation of mining power. Furthermore, single mining pools have in the past reached nearly 50% of total network computation power [262]. On the one hand, this could enable an 51%-attack and on the

other hand, these large pools of mining power become an attractive target for hacking, since their overall mining power is so viable. Since one of the core ideas of Bitcoin is decentralisation, the building of large mining pools should be inhibited. In the scientific community, this research field is referred to as pooling resistant proof of work. Most proposals rely on complex mining algorithms, which need more cryptographic building blocks than pure hashing. Miller *et al.* [203] discuss proof of work schemes that are not transferable. The basic idea is that if a mining pool operator would outsource the proof of work to several clients, each client would be able to steal the reward without the operator knowing. Since no honesty can be enforced in such a scheme, outsourcing and pooling become very unattractive, which motivates independent mining and decentralisation.

### 6.5.2. ASIC resistance

ASIC resistant mining puzzles are a new research field, which aims at finding suitable hash puzzles that revitalise the idea that regular users on commodity hardware (e.g., PCs, laptops and mobile phones) can re-join the mining process. Motivating more devices to join the mining process prevents centralisation of the mining ecosystem by big operators with server farms. Stronger decentralisation of the mining process also makes 51%-attacks less likely. The most prominent design for constructing ASIC resistant puzzles are the so-called memory hard puzzles.

One example for a memory hard hash function, which is widely used in Bitcoin Altcoins (e.g., Litecoin, Dogecoin and Auroracoin), is the Scrypt function [230]. It is commonly used as a strong key derivation function, but in the context of Altcoin mining serves as a hash function with constant time/memory trade-off. In other words if a system with less memory computes the hash function more CPU time is needed. One problem of Scrypt in the context of mining is that the verification of the blocks also has fixed time/memory trade-off requirements. Therefore, the Scrypt memory parameters can only be set to moderate requirements, since otherwise the Altcoin system becomes practically unusable for weak clients. In addition, the first ASICs for mining with the Scrypt function have been built and are commercially available [26], but the actual speed-up gap compared to commodity hardware is much smaller in contrast to SHA-256 ASICs.

Another mining strategy, which tries to be ASIC resistant, but is cheaper to verify than the actual puzzle solving is the cuckoo hash cycles system by Tromp [275]. The basic idea is to create a graph according to a deterministic formula and check if the graph has a cycle with $\mathcal{K}$ edges. On the one hand, algorithms to find cycles in big graphs require a lot of memory, but on the other hand, verification of such a cycle with $\mathcal{K}$ edges is very easy and has very moderate memory requirements

Further ASIC resistant concepts are:

- To chain multiple hash functions together, which makes hardware implementations very expensive e.g., the X11 hash function [79], which cascades eleven of the SHA-3 finalist hash functions.
- Moving target mining regularly changes the mining algorithm, which is no problem to commodity hardware since it only requires a software up-date, but makes

dedicated hardware completely infeasible since it becomes useless as soon as the mining strategy is changed [215].

### 6.5.3. Proof of Stake

In contrast to the proof of work used by Bitcoin the so called proof of stake is another distributed consensus mechanism, which focuses on getting rid of the high energy requirements of the proof of work mining. The basic idea is that instead of investing real money into new mining hardware to mine new blocks, money can be invested into the cryptocurrency directly for a higher "stake" to be picked as next block creator. Proof of stake is still subject to active research and has several open problems and drawbacks (i.e., nothing at stake problem [232, 215]). On the one hand, due to the technology still being immature, it is currently no relevant alternative to the proof of work for a breeder document blockchain and on the other hand, the focus being on an ideology rather than on enhanced security makes it out of scope for breeder document long-term security.

## 6.6. Privacy, Pseudonymity and Anonymity

This section discusses the privacy properties of Bitcoin, because on the one hand, the entire blockchain is available completely to the public, but on the other hand, Bitcoin has certain properties that could be interpreted as anonymity or pseudonymity.

Interacting without an entity's real name, but with a pseudonym is part of Bitcoin since transactions are not conducted between real people, but the public key addresses instead. In computer science, this property is called pseudonymity, since all interactions are made with the pseudonym and not the real identity. Bitcoin therefore fulfils the property of pseudonymity. In contrast, anonymity is defined as having pseudonymity with unlinkability between the single user interactions with the system at hand [215]. It is not possible to directly connect a Bitcoin address to a real world identity, but due to the blockchain it is possible to link together a Bitcoin address's activities over time and make conclusions based on these activities. Furthermore, common Bitcoin services require registration with the users real identity, which is also required for most exchange methods if the user wants to exchange the Bitcoins into a fiat money. Since the sender, receiver and Bitcoin value of a transaction are publicly available these informations can be used to further analyse the users behaviour and utilised in side-channel attacks to deanonymise the user. Deeper analysis of Bitcoin anonymity can be found in the scientific community [249, 199, 168], regarding anonymity models, anti money laundering, transactional graph analysis and Bitcoin deanonymisation algorithms. It is generally accepted that Bitcoin provides pseudonymity and no strong anonymity. The later has to be kept in mind when integrating the Bitcoin blockchain into the breeder document life cycle.

## 6.7. Main Breeder Document Architecture and Security Discussion

This section is mostly based on the concepts and discussion in [45]. The blockchain for storing the breeder document information can either be a private one or a publicly accessible blockchain. If it is publicly accessible, either a new dedicated breeder document blockchain is established or the information can be stored into an already established one.

Implementing a private blockchain between EU member states could be implemented via a virtual private network (VPN). Since only authorised government nodes could join the network, create transactions and mine for new blocks most of the underlying security ideas utilised in Bitcoin become pointless because all malicious clients are filtered via the VPN access. Furthermore, on the one hand, this concept does not provide any benefit over a regular distributed database between the EU member states running in a VPN. On the other hand, one of the main motivators was to be cost-efficient, which the idea of a dedicated private blockchain between the EU member states is not. Besides a similar EU wide IT project is the Verifying PKI between the EU member states to provide access control to ePassport fingerprints, which is not fully operational after more than 10 years [31] of existence. It is rather doubtful that this EU IT project could be established between all EU member states in a faster manner since birth certificates are in general considered less relevant than ePassports.

Similar properties apply for a public accessible blockchain between member states, since cost and Verifying PKI parallels remain independent of the lack of a VPN. Furthermore, it would be a very attractive target for hackers to perform DDoS attacks and inject dummy blocks, which happened to other Altcoin networks, which therefore failed in the bootstrap phase (see CoiledCoin [215]). Providing high computation power by the member states to prevent such attacks is also not realistic since this would also not be cost-efficient. Keeping in mind the properties of the bootstrap it is reasonable to assume that due to the low cost requirements of birth certificates it is rather unlikely to provide motivation for the miners to join a dedicated birth certificate blockchain network.

Therefore, the most secure and cost-efficient variant is to build on a well-established public blockchain with a healthy mining ecosystem. By utilising an already established blockchain system, initial difficulties similar to the EU Verifying PKI can be avoided. According to [61] the Bitcoin blockchain, is currently the blockchain with by far the most mining power and, hence, most suitable for the breeder document scenario, due to its healthy mining ecosystem and high security. The Altcoin follower Ethereum [86], according to market share, has useful properties, (e.g., smart contracts), but is currently no competitor for the breeder document scenario. All other Altcoins of the Top 100 market share charts [61] are currently in no position to practically compete with Bitcoin's mining security. Since all other Altcoin systems are in some form forked on the initial Bitcoin client, it is easy to establish that Bitcoin has the oldest Blockchain, best-analysed network, provides easy transaction deployment and has been proven secure longest.

### 6.7.1. Identity Declaration & Document Verification

The basic workflow of the proposed system architecture is depicted in figure 6.7. The identity declaration of a newborn must be done as soon as possible after birth by its parents and a government official, certifying the most relevant identity attributes (name of the newborn, date of birth, name of the parents etc.) in a birth certificate. Furthermore, biometric information are captured, features extracted and stored to the birth certificate e.g., via a 2D barcode (see section 10.2). Linking the birth certificate to the blockchain is done by computing a cryptographic hash over all document holder specific data elements of the document, including the biometric reference data, and storing the resulting hash value in the metadata of a Bitcoin transaction made by an official birth certificate issuer of the member state. Since Bitcoin transactions are implemented in the Bitcoin Script language, arbitrary data is usually written to the Bitcoin blockchain utilising the $OP\_RETURN$ opcode. In the proposed breeder document scenario the command would be: $OP\_RETURN < h1(data) \| h2(data) \| h3(data) >$.

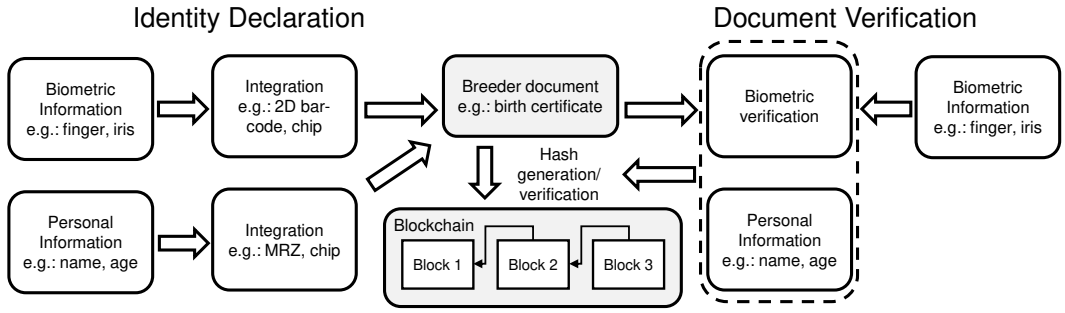



Figure 6.7.: Proposed architecture: breeder document is linked to a blockchain.

For later verification of the document, it can be distinguished between a verification by the same member state and a verification by another member state. In a national scenario, the member state knows its own public keys and therefore can verify if it conducted set Bitcoin transaction beforehand. For a cross-border member state verification the public keys could be shared on a public list i.e., no complex public key infrastructure is necessary. After several consecutive new blocks the transactions together with the birth certificate hashes are irreversibly part of the public blockchain, which can be used by anyone for authenticity and integrity verification of the document. After verification of authenticity and integrity of the birth certificate's data sets, embedded biometric reference data must be used to verify the link between document and document holder. Detailed specifications of operations, actors and roles have to be harmonised between EU member states as noted by [223].

### 6.7.2. Security Aspects

The security discussion considers the cryptographic building blocks of the presented concept regarding long-term security and post-quantum security. In case a birth certificate's cryptographic hash value is stored in the metadata of a Bitcoin transaction

($OP\_RETURN < h1(data)\|h2(data)\|h3(data) >$), security of these transactions is essential. A digital signature utilising the ECDSA algorithm [97] with the NIST P-256 curve [219] protects the transaction, which is considered secure at least until 2041 [214, 82]. ECDSA is not post-quantum secure and vulnerable to Shor's algorithm [263]. This issue does not only affect the presented breeder document scenario, but the entire Bitcoin ecosystem. Therefore, one option is to rely on the adaptation of the Bitcoin blockchain via a hard fork when the risk of quantum computers to common asymmetric cryptography becomes a viable threat. A more proactive measure would be to add an additional digital signature in the metadata created with a post-quantum resistant digital signature scheme e.g., XMSS [35] or SPHINCS [19] (see section 9.1). Both strategies are viable options depending on the requirements and further risk analysis by the member states. Similar to digital signatures used in ePassports, it is advised to regularly change the key pair for the digital signatures [144]. Since the individual blocks of the blockchain also contain a timestamp of creation time, an additional check can be implemented to check if the eligible public key was indeed used during implied creation time of the birth certificate and time of the linked block.

Besides the digital signature protecting the transaction, the hash function, which builds the basis for the hash puzzles of the blockchain is the remaining cryptographic primitive for discussion. Bitcoin constructs its hash puzzles with the SHA-256 [95] hash function. The impact of quantum computers is less foreseeable since according to current state of research, Shor's algorithm has no impact on hash functions and only Grover's algorithm [115, 116] has low impact on long-term post-quantum security of hash functions. Independent of advances in quantum computing research, the breeder document hash is not forced to use the same SHA-256 hash function for the blockchain proof of work, but can combine multiple hash functions to minimise impact due to advances in cryptanalysis regarding hash functions. Today three constructions for hash functions are most prominent i.e., Merkle-Damgård, HAIFA and Sponge [167]. Therefore, to be future-proof a SHA-3 finalist for all three constructions could be utilised (e.g., a combination of Grøstl, BLAKE, and Keccak [167]). Furthermore, it is not sufficient to find a collision attack against the hash function in question, but a second preimage must be found for a hash value stored in the metadata of the blockchain. The found second preimage must be a preimage for multiple hash functions and additionally be a biometric match for the attackers biometric modalities utilised in the underlying birth certificate. It is safe to say that from today's standpoint the existence of such an attack with relevant efficiency has negligible probability.

SHA-256 is not only used for the proof of work, but is also the hash function for the transaction hash tree in the Bitcoin blockchain. If an attacker wants to add a new breeder document transaction to the hash tree, this must be done without changing the Merkle root, since otherwise it would be easily detected due to the immutable long-term consensus property of the blockchain. Therefore, a second preimage attack against one of the existing tree nodes has to be executed with the boundary condition that the second preimage is the concatenated hash of two valid Bitcoin transactions (see figure 6.4). No such second preimage attack is known today against SHA-256 and even Grover's algorithm would reduce the security to at least 128 bits security, which remains secure,

since it is the same security level SHA-256 provides against a collision attack today. Even if such an attack would be theoretically possible, it is still very hard to achieve in practice. On the one hand, due to the nature of the peer-to-peer network it would be very hard to inject a manipulated old block to the network node verifying the birth certificate, since the node itself decides its communication partners and on the other hand, many blocks store the full blockchain and an old manipulated block would therefore be detectable. Furthermore, if an attacker can inject arbitrary transactions into the Bitcoin blockchain it breaks the entire Bitcoin system independent of the breeder document use case and is therefore out of scope.

The hypothetical scenario of the current Bitcoin blockchain becoming insecure can be compared to changing a country's fiat money to a new currency e.g., an EU member state's exchange of its legacy currency to the Euro currency. In contrast to a fiat currency, Bitcoins cannot simply be exchanged since they have no physical representation. Therefore, Bitcoin has the so-called proof of burn mechanism to cryptographically prove that arbitrary Bitcoins were destroyed, can never be redeemed and have no possible way to be spent. Conducting the proof of burn can be utilised to gain coins in a new post-quantum secure blockchain system if the current system becomes insecure.

## 6.8. Blockchain Discussion

Blockchain technology in the context of Bitcoin can indeed provide a strengthening of breeder document's long-term data authenticity and integrity in the identity life cycle, but the capabilities have to be estimated realistically. Today birth certificates have a validity for the complete life span of a human being (i.e., worst case 100 years); whereas neither today's cryptography, nor paper based birth certificates will be particular relevant in 100 years. Even planning 20 years in advance seems a bold choice and Bitcoin will change in the next years as well as the physical breeder documents. So planning a fixed architecture for 100 years in the future would be rather optimistic.

Nevertheless, what the proposed blockchain concept can provide is a direct short-term solution that can enhance the security of today's birth certificates by a software rollout, without establishment of an expensive separated infrastructure or severe extra hardware costs. The hardware already in use at local civil registry offices should be sufficient to make Bitcoin transactions or find Bitcoin transactions in the blockchain for a given address without further upgrades. Similar to ePassport or ID-card security, the overall security must be based on a multitude of security mechanisms and not on a single instance as the proposed concept. Long-term, the concept should be one of many building blocks to enhance the overall breeder document verification process security to make fraud and identity theft a tougher obstacle. Further building blocks can be stricter administration processes, better staff training, use of additional identity evidence sources (e.g., electoral rolls and social security records) [91], digital breeder records, and in the long-term maybe a validity period (i.e., 5-10 years) for breeder documents, which was already established for EU driving licences [92]. It is also a realistic estimation that a common piece of paper will never have the same security level as a dedicated integrated

circuit chip that was specifically designed to fulfil that security use case.

Bitcoin might not be considered the most modern blockchain cryptocurrency, but on the one hand, it has been proven secure for almost 10 years without the necessity for any security related hard forks and on the other hand, the mechanisms added to newer Altcoins do not enhance the security of the specific breeder document use case. The coming years will show if paper based breeder documents will be gradually replaced by a digital dataset, an id-document with fixed validity period, or if paper based documents are strengthened by additional measures, as the proposed blockchain architecture, to become established as the standard.

# 7. Enhancing eMRTD SPI via new Protocols

This chapter discusses advances of the scientific community in cryptographic security protocols aimed towards the eMRTD domain, which either enhance the established protocols discussed in chapter 4 or replace them for more efficient or more secure properties. First several protocols are introduced; their benefits examined, and in the second part of the chapter discussed which characteristics future eMRTD protocols should consider adopting. A sequence diagram notation overview for the security protocols can be found in the appendix on page 167.

## 7.1. BioPACE v1/v2

The BioPACE introduction and security analysis is based on [42] and presents, on the one hand, the BioPACE security protocol and its underlying idea as introduced by Deufel *et al.* in [75] and on the other hand, the BioPACE v2 protocol by Buchmann *et al.*[42, 43].

### 7.1.1. BioPACE v1

Deufel *et al.* present BioPACE as a pre-processing step to the PACE protocol. First the idea of BioPACE is sketched and then its two phases are described.

The underlying idea for the pre-processing step is to make use of biometric template protection based on the ISO/IEC 24745 standard for biometric information protection [158]. BioPACE does not favour a biometric modality, i.e., BioPACE may be implemented using the facial image, fingerprints, iris, etc. During personalisation of an eMRTD the biometric modality is enrolled and a feature extraction from the captured biometric sample results in a biometric reference comprising a pseudonymous identifier $PI$ and auxiliary data $AD$. The concrete specification of $PI$ and $AD$ with respect to size and structure is neither specified by the ISO/IEC 24745 standard nor by the authors of [75]. A verification consists of a new feature extraction from a fresh biometric sample and the previously enrolled $AD$. The verification results in a new pseudonymous identifier $PI^*$, which equals $PI$ if and only if the same person provided the biometric sample and therefore a biometric match occurs.

This subsection explains the two phases of BioPACE in more detail. The authors of [75] call these phases the *initialisation phase* and the *regular use phase*.

During the initialisation phase the biometric enrolment is conducted, which results in $PI$ and $AD$. Additionally, the eMRTD chip or a back-end system creates a random CAN or PIN, which serve as input for the regular PACE protocol after the pre-processing step

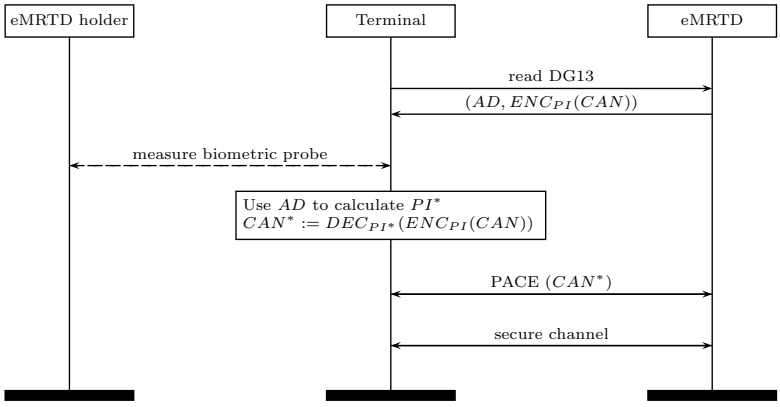



Figure 7.1.: The BioPACE v1 protocol [75].

of BioPACE. In what follows this random secret is denoted as CAN. The secret CAN is encrypted using $PI$ as encryption key resulting in $ENC_{PI}(CAN)$. Then $PI$ is discarded. The pair $(AD, ENC_{PI}(CAN))$ is then written to data group 13 (DG13) of the eMRTD logical data structure (LDS) [143]. DG13 is publicly accessible without any authentication. This is justified by [75] with the consideration that the tuple $(AD, ENC_{PI}(CAN))$ is not security sensitive, because it does not disclose biometric data of the enrolled person.

After the initialisation phase BioPACE is ready for regular use. This phase is depicted in figure 7.1. If an inspection system wants to perform BioPACE, it first has to read DG13 to receive $(AD, ENC_{PI}(CAN))$. The inspection system captures a biometric sample from the document holder and uses the received $AD$ from DG13 to compute $PI^*$. The inspection system then performs $DEC_{PI^*}(ENC_{PI}(CAN))$ to decrypt $ENC_{PI}(CAN)$ using $PI^*$ as decryption key to receive $CAN^*$, which will match $CAN$ if and only if $PI^*$ matches $PI$.

The secret value CAN is also known to the eMRTD chip, because it is stored in its internal memory and can therefore be used as input for the standard PACE protocol. After this pre-processing step, BioPACE uses the steps of the common PACE protocol.

### 7.1.2. Assessment of BioPACE v1

This section presents the security assessment of BioPACE with respect to common security features of an eMRTD and the identified weaknesses that are introduced when replacing PACE with BioPACE. Every subsection first presents a short assessment regarding a specific security aspect, and then proposes possible solutions, when applicable, on the basis of the found weaknesses.

#### No physical to electronic linkage.

Where PACE makes a link between the printed data page of the eMRTD and the chip inside the eMRTD, BioPACE makes a link between the eMRTD holder and the chip

inside the eMRTD. There is no more link between the printed data page of the eMRTD and the chip inside the eMRTD. As a consequence it cannot build further upon the prior established authenticity of the MRZ and CAN (by checking the optical security features on eMRTDs, such as special paper and printing techniques).

#### Tracking.

While PACE guarantees the unlinkability of eMRTD occurrences on the wireless channel, BioPACE does not. The authors of BioPACE justify that data group 13 can be read freely from the chip by claiming that it does not disclose any biometric data and as such is not security-sensitive. However, the data $(AD, ENC_{PI}(CAN))$ provides a unique identifier for every eMRTD and can be read out by anyone within communication range of the eMRTD making tracking possible.

A possible solution would be to print $(AD, ENC_{PI}(CAN))$ on the data page of the eMRTD, additionally ensuring the coupling between the data page of the eMRTD and the chip. However, this would require substantial changes in the eMRTD creation and verification processes, as opposed to reading out some extra values from the chip.

#### Usability degradation.

The aspect of better comfort is not proven in the paper [75]. It is doubtful that reading and processing a fingerprint is faster than performing OCR on a MRZ or CAN. Implementing BioPACE instead of PACE also means that the verifier needs biometric reader equipment, even if one only wants to read the chip's version of the holder's name, or to verify authenticity and integrity of the chip's data via passive authentication. At the end of the paper, it is suggested that one can always skip the biometric pre-processing step of BioPACE and fall back to the original PACE. However, if the biometric pre-processing step can be skipped, this raises questions about the benefits of BioPACE, especially towards the eMRTD holder.

#### Loss of access control flexibility.

As long as the sensitive biometric fingerprints are stored on the chip BioPACE should not be considered as EU EAC replacement, because it can only provide two possible authorisation levels: read every data group or read no data group. With EAC, one can provide a more fine-grained access control and the eMRTD receives an explicit authorisation from its issuing country that this terminal is indeed authorised to read certain data groups.

A possible solution is to replace the raw fingerprints by a biometric template that leaks no sensitive information.

#### Double biometric linkage goal.

The basic BioPACE protocol claims to provide access control and create a link between the eMRTD holder and the chip. In the current eMRTD security protocol pool these

goals are already achieved by BAC, PACE and EAC for the access control and the fingerprints stored on the chip for the biometric link. Achieving the same security goal twice has no benefit and only makes the border control check more lengthy.

Removing EAC and the raw fingerprints would justify the access control and linkage goal of BioPACE. Of course, this should only be considered if the eMRTD would contain no more sensitive biometric data.

#### Skimming.

BioPACE claims that no unauthorised data retrieval is possible. For eMRTDs that implement PACE, one requires access to the printed data page of the eMRTD to read the data on the chip. Handing the eMRTD over to an official for checking can be seen as an implicit authorisation from the eMRTD holder. For BioPACE to reach the same level of authorisation, eMRTD holders can only provide their fingerprint to the officials checking their eMRTDs. However, we leave our fingerprints everywhere. Anyone within wireless communication range that has access to the fingerprint of the eMRTD holder, can read out the data of the eMRTD without the holder even being aware. This makes skimming attacks easy, for example in airport bars (given that one can extract the fingerprint from a glass in a timely manner). One does not need to fool the terminal's fingerprint reader (which is difficult, since one has to make a dummy finger, possible liveness detection) but the raw image data is good enough for direct processing.

As boundary condition, the attacker also needs a terminal and the attack is only justified if a name or facial image to a corresponding fingerprint is the goal of the attacker.

By making a link to the printed data page of the eMRTD this attack can be mitigated, because the printed content is not revealed in airport bars.

#### Offline eMRTD holder guessing.

Because the CAN has low entropy, an offline guessing attack with respect to whom the eMRTD belongs to is possible. Assume that one wants to track a number of high profile individuals and one has access to their fingerprints (which are left behind on whatever the person in question happens to touch). From these fingerprints, together with $AD$ one can derive all possible $PI$'s. Only a subset of the corresponding $ENC_{PI}(CAN)$ will decrypt to a possible CAN (having low entropy). Of course this will not uniquely identify any one person, but it will narrow down the search space significantly.

A trivial solution would be to pad the CAN with some randomness before encryption, and discard the padding upon decryption. Note that this would not work when using the MRZ instead of the CAN. While the MRZ has typically more entropy than the CAN, it also has more structure that is preserved regardless of the random padding.

A side note worth mentioning: if $PI$ could provide a high enough entropy it could also make BAC attractive again, because the main complaint of BAC is the low entropy of the MRZ combined with its vulnerability to offline brute-force attacks. Still PACE is resistant against offline brute-force attacks and should therefore preferred over BAC.

### 7.1.3. An improved BioPACE v2

This subsection formalises the BioPACE v2 protocol. It aims at fixing the flaws identified by changing BioPACE according to the given proposals.

Figure 7.2 illustrates the protocol steps of the BioPACE v2 protocol. The improvement consists of two main changes compared to the basic version: First, $PI^*$ is used directly as input for the PACE protocol (and not as decryption key to get the low entropy CAN). Second, $AD$ is printed on the data page of the eMRTD to link the physical document to the chip instead of storing $AD$ on the chip.

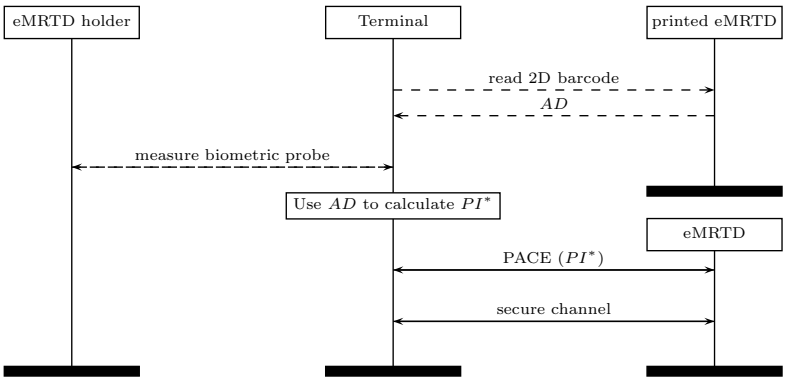



Figure 7.2.: The BioPACE v2 protocol [42].

There is no clear reason why one should encrypt a low entropy value (CAN or MRZ) if it does not need to be transferred manually/optically. Therefore, $PI^*$ is used directly as input for the PACE protocol. This also means that the value $ENC_{PI}(CAN)$ no longer needs to be transmitted from the eMRTD to the terminal via the wireless channel. Hence there is no initial access from the terminal to DG13 of the eMRTD. By removing the initial wireless access the issue of offline guessing of the eMRTD holder is avoided as well.

$AD$ is printed on the data page of the eMRTD in form of a 2D barcode (e.g., a QR code [162] or a Data Matrix code [160]), which is shown in figure 7.3. $PI$ is not publicly available, instead it is stored in the internal memory of the eMRTD chip and therefore only available to the chip itself, but not to the terminal. Since the chip does not need to transmit $(AD, ENC_{PI}(CAN))$, there is no longer a unique identifier for the eMRTD, resolving the tracking problem.

It was decided against integrating $AD$ into the present MRZ, because in common experience a 2D barcode is on the one hand, more reliable due to the integrated error correction code and on the other hand, more flexible for an $AD$ with variable size depending on the selected biometric modality. 2D barcodes become more and more popular in different areas of document security.

For instance, there is currently a discussion in the EU to integrate 2D barcodes to enhance the authenticity and integrity of non-electronic travel and ID documents (e.g., birth certificates, emergency passports, visas and driver licences). This EU discussion is

based on a new national standard, which is called the Digital Seal [32].

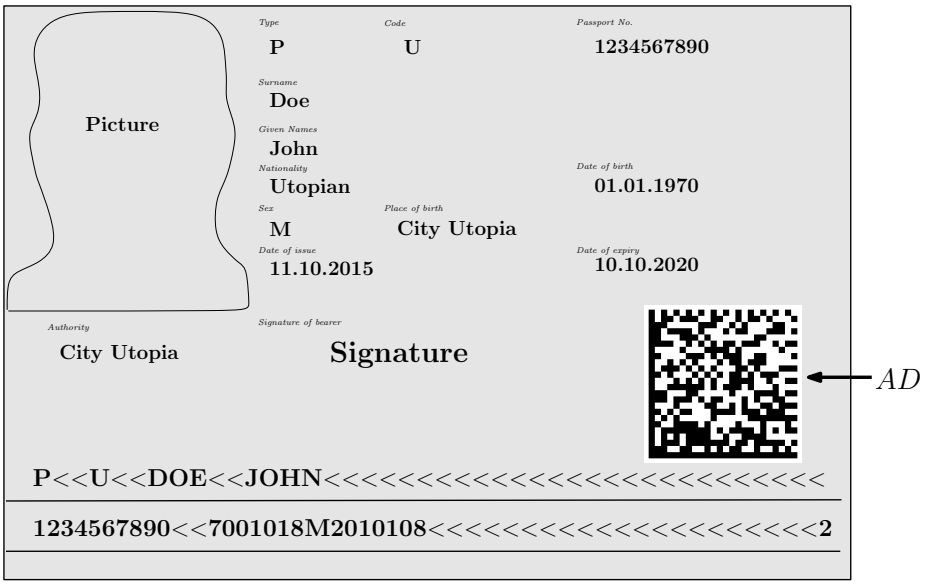



Figure 7.3.: The eMRTD data page with $AD$ printed as data matrix code [42].

By printing $AD$ on the data page the link between the physical eMRTD and the chip is recreated. Now a terminal needs optical access to the eMRTD to scan the 2D barcode and receive $AD$ to calculate $PI^*$. This will provide at least the same level of protection against skimming and sniffing attacks as PACE.

In the basic BioPACE protocol, matching $PI$ to $PI^*$ is done implicitly by decrypting the low-entropy $CAN$ with $PI^*$ and initialising PACE with the resulting $CAN^*$. The key space entropy of $PI$ is not specified by [75], but it is considered higher than the entropy of a numeric six digit CAN with an entropy of at most 20 bits (see section 10.1 for entropy of biometric data). Therefore, $PI^*$ is directly entered into PACE. Besides the higher entropy benefit, $PI^*$ is implicitly matched to $PI$ by the completion of the PACE protocol, because if $PI^*$ and $PI$ do not match the PACE protocol will fail.

The BioPACE v2 protocol fixes all the mentioned security problems. Now, it fulfils its duty as an access control mechanism and leaks no more unambiguous linkable data before the protocol successfully completes. To track a person and to read the data on the chip the attacker needs optical access to the data page. This equals the current security level of eMRTDs and does not constitute a security risk, because if an attacker gets access to the data page it can read all data in printed form anyway.

### 7.1.4. Replacing EAC and raw fingerprints by BioPACE v2

This subsection discusses the idea to replace the current infrastructure (i.e., the EAC protocols, the Verifying PKI, and the storage of raw fingerprints in data group 3) by the BioPACE v2 protocol. It contrasts the advantages with the disadvantages of the

approach and includes boundary conditions, which have to be fulfilled to make the BioPACE v2 protocol expedient.

Fundamental changes to an established infrastructure are a challenging task and require as a boundary condition both innovative ideas and enhanced security. It is considered that BioPACE v2 meets these demands as discussed below. In the context, for instance, a sample innovative idea is the Biocryptographic Key Infrastructure [256] to replace a common Public Key Infrastructure, yielding a higher security level. An example of enhancing an applied and proven protocol is the Biotokens [257] example, where biometric digital signatures and Bio-Kerberos increases security. Therefore, the redundant protocols have to be dropped, and the BioPACE v2 has to provide a significant enhancement to become a new eMRTD standard.

If BioPACE v2 is used without a subsequent EAC accomplishment, it has the following benefits:

1. **Faster verification:** If EAC is dropped and a $PI$ is used instead of raw fingerprints, it eliminates two bottlenecks: first, no more raw fingerprints have to be transferred from the chip to the terminal over the wireless interface. Second, the lack of terminal authentication resolves the need to verify certificate chains by the eMRTD chip. This will drastically speed up the eMRTD processing times at border checks.

2. **Enhanced practical security:** According to a recent EU border control study [89, D4.1] border control personnel does only perform an electronic check against eMRTD blacklists due to time constraints. Hence in practice the actual security level of the eMRTD chip and its infrastructure is mainly not used. A significant speed-up of the verification protocols will therefore not only make the verification more convenient for the travellers, but it will improve security, because the electronic security features will be actually used by border control personnel even under strict time schedule guidelines.

3. **Improving privacy:** Raw fingerprints are removed and replaced with a biometric template, which is stored in the eMRTD's internal memory and therefore only accessible by the chip. Hence, the privacy level is improved.

4. **Decreasing infrastructure costs:** If terminal authentication is abandoned, there is no more need to maintain the complicated Verifying PKI. As the further expenses remain constant (e.g., the costs for the biometric personalisation of eMRTDs), the costs of the whole eMRTD infrastructure will decrease significantly.

5. **Standardised data structures:** 2D barcodes are standardised, and their integration is already discussed for non-electronic travel documents based on the Digital Seal standard [32, 89, D6.1].

On the other hand, BioPACE v2 as a replacement for EAC yields the following downsides:

1. **Change of layout:** To establish the BioPACE v2 protocol in the eMRTD domain the creation and enrolment process has to be changed, because *AD* needs to be printed on the data page.

2. **Coarse-grained access control:** BioPACE v2 causes a loss of access control flexibility, however, if the sensitive JPEG fingerprints are removed from the chip no more sensitive data remains, which is worth protecting with a flexible access control scheme.

3. **Renounce of strong cohesion paradigm:** Security protocols often follow the software engineering paradigm of strong cohesion and loose coupling. Every protocol should have a very specific goal and depend on as few as possible other protocols. The proposal abandons this paradigm.

4. **Chip cloning:** Dropping EAC results in the loss of chip authentication and hence in giving up the current chip cloning protection. However, the physical protection through the printed AD on the document makes chip cloning useless from a practical point of view. Further electronic prevention approach of chip cloning is discussed below.

The improvement with respect to run-time, practical security, and costs are rated to be more important than the disadvantages to change the layout and the loss of fine-grained access control. Future attention should be paid to a sample specification of the PI scheme and to the integration of a chip cloning protection into the BioPACE v2 protocol. Bender *et al.* [12] present a protocol called PACE|AA, which combines PACE and Active Authentication to create a protocol which is more efficient than the single protocols and solves a security risk of Active Authentication.

## 7.2. PACE|AA and PACE|CA

This section discusses two protocols proposed by the German Federal Office for Information Security (BSI) PACE|AA [12] and PACE|CA [14], which combine the PACE protocol with an eMRTD anti cloning protocol. PACE|AA combines PACE with Active Authentication and PACE|CA combines PACE with Chip Authentication. Both variants focus on reducing the number of cryptographic primitive operations (i.e., elliptic curve operations) for better efficiency and fixing known flaws of the stand-alone protocols (i.e., Active Authentication's challenge semantics vulnerability).

### 7.2.1. PACE|AA

PACE|AA combines the PACE protocol with the optional Active Authentication protocol by re-using some part of the secret data computed during the PACE protocol in the AA protocol saving one exponentiation for the eMRTD chip. Bender *et al.* [12] formally prove that the combination of both protocols preserves the security goals of both protocols and fixes the challenge semantics weakness of the AA protocol. Combining

the protocols is also motivated by the fact that the optional AA chip cloning protection cannot be skipped anymore, hence enforcing a higher security during eMRTD checks. Bender *et al.* argue that their protocol combination provides "Active Authentication (almost) for free" [12] by saving the exponentiation for AA's challenge-response signature creation. PACE retrieves its initial low entropy password from the MRZ, CAN, or PIN, which is mapped to a random group element via a generic function called *Map2Point*. The scientific community [147, 29] proposes multiple versions of this mapping and two variants are standardised by ICAO [144], namely the integrated mapping and the generic mapping. The PACE|AA optimisation can only be implemented with the Diffie-Hellman based *Map2Point* generic mapping, which is also stated by [229]. PACE|AA aims at reusing the secret exponent of the *Map2Point* function, since the secret exponent $y_A$ of the first *Map2Point* call is reused during signature generation by the eMRTD chip in the anti-cloning step. The authors present two alternatives, one based on Schnorr signatures [258] and one using DSA signatures [97]. Security of the combined protocol is discussed and shown by a formal security proof that on the one hand, the individual security goals of the protocols are still achieved and on the other hand, sharing the secret between the two protocols still conserves the overall security properties. In contrast to Active Authentication's common signature scheme, that provides unwanted non-repudiation via potential challenge semantics, Bender *et al.* present a deniable Schnorr version that prevents creation of a cryptographic eMRTD interaction proof by the terminal for third parties. The authors call this property deniable authentication, define it formally and motivate it with higher privacy for the eMRTD holder. The PACE|AA protocol in Schnorr signature variant is depicted in figure 7.4.

### 7.2.2. PACE|CA

PACE|CA pursuits the same aims as the PACE|AA protocol to combine the Diffie-Hellman based key exchange protocol with a chip anti cloning protocol. Bender *et al.* [14] motivate the new protocol by strengthening the PACE key exchange with a mandatory chip authentication procedure, since they believe Active Authentication is omitted during the border control check due to efficiency reasons. Similar to PACE|AA [12] PACE|CA shall provide "active authentication almost for free" [14]. Starting point of the paper by Bender *et al.* is the discussion of an optimised protocol called simplified PACE|AA (SPACE|AA), which has been discussed by the BSI and independently introduced by Hanzlik *et al.* [119]. All three protocols, PACE|AA, SPACE|AA and PACE|CA, have the basic idea of reusing some randomised part of the PACE protocol during the chip authentication for an acceleration of the border check procedure. Main critic points by Bender *et al.* against the SPACE|AA protocol by Hanzlik *et al.* are on the one hand, that SPACE|AA slightly changes the PACE protocol itself and is therefore not compatible with the ICAO standard anymore and on the other hand, that their security proofs only consider passive attackers, which are eavesdropping, and no active attackers. These factors are the main motivation for the design of PACE|CA, namely PACE must remain ICAO compliant, resilience against active attackers, and implement the speed-up ideas of SPACE|AA in PACE|CA. [14] refers to the abbreviation CA as chip authentication,

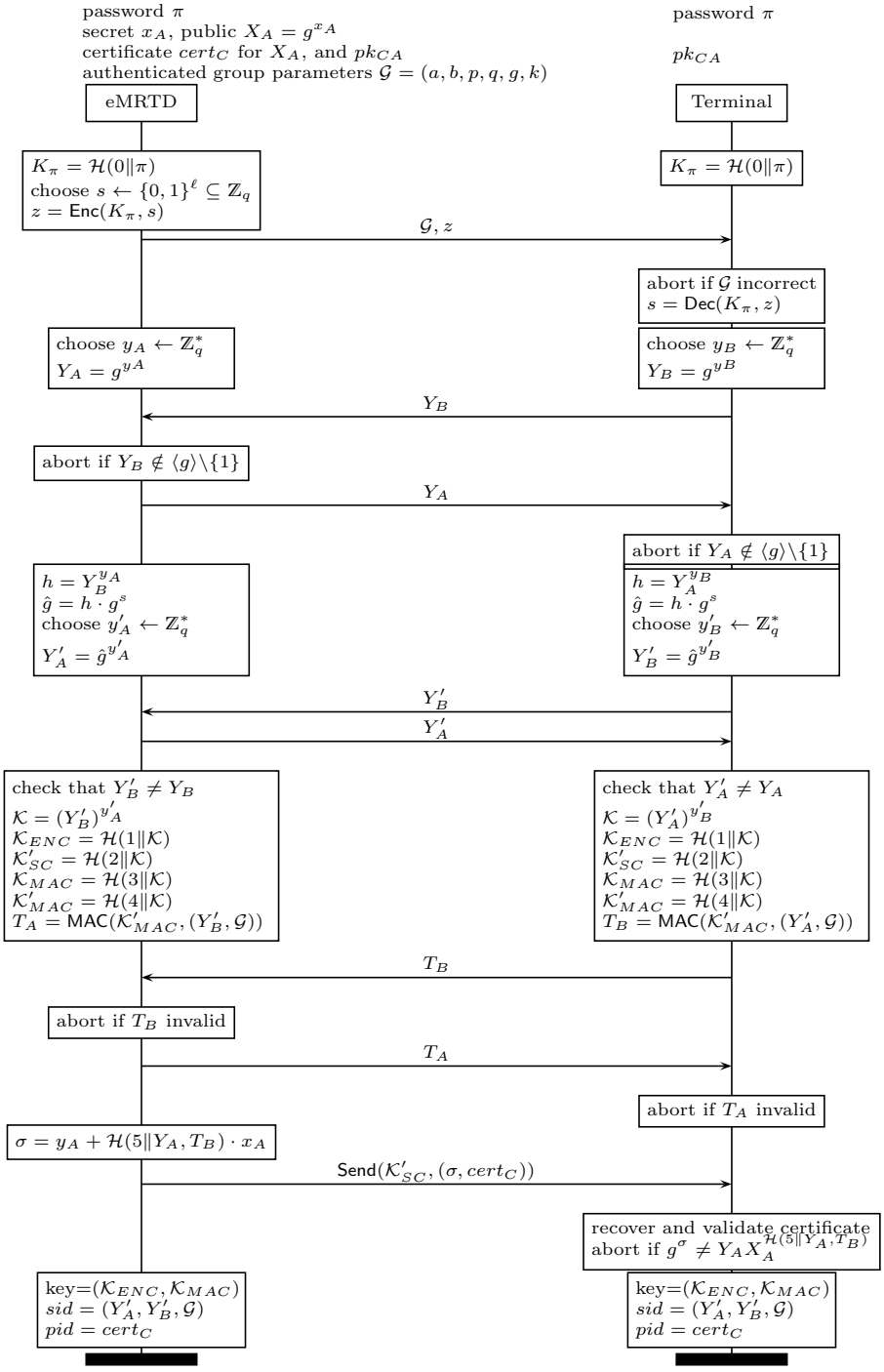



Figure 7.4.: The PACE|AA protocol [12].

but also uses card authentication as synonym. Bender *et al.* present an additive and multiplicative version of their PACE|CA protocol, the additive version is depicted in figure 7.5. Instead of relying on a DSA signature or Schnorr signature as in the PACE|AA protocol, which needs a hash function, modular multiplication and addition, PACE|CA only needs a subtraction modulo q, $\sigma = y_A - x_A$, for the chip anti cloning protocol step. This is the core change of the PACE|CA protocol to the PACE|AA protocol and discussed by Bender *et al.* in their security analysis. Similar to the PACE|AA protocol's requirements the PACE|CA combination only works if the Diffie-Hellman based generic mapping is used during the PACE protocol, which is the most used variant according to Bender *et al.* [14].

## 7.3. SIGMA-I and IBIHOP+

Peeters *et al.* [229] propose protocols to replace the PACE and EAC protocols. They proclaim a speed-up of 40%, better security and privacy guarantees than the current eMRTD protocols. For their speed-up estimation only the authentication procedure is considered and not the overall communication between ePassport and terminal. Since the biggest time expense is the transfer of biometrics and not the cryptographic protocols, the overall speed-up is considered less essential. The proposed authentication protocols are the SIGMA-I protocol [176], and the IBIHOP+ protocol which is a modification of the IBIHOP protocol [228]. Focus of both protocols is on the one hand, on directly using a mutual authentication protocol resulting in high entropy session keys instead of PACE's approach taking the MRZ as low entropy seed and on the other hand, to reduce the number of elliptic curve operations to speed up the authentication.

### 7.3.1. SIGMA-I

The first proposed protocol is the SIGMA-I protocol based on the SIGMA: 'SIGn-and-MAc' protocol family by Krawczyk [176], which discusses key exchange protocols based on Diffie-Hellman authenticated with digital signatures. Thereby perfect forward secrecy is provided. The SIGMA-I variant adds identity protection to the basic SIGMA protocol, hence the protocol initiator can delay disclosing its own identity until the other parties' identity has been authenticated. In this scenario the initiator is the ePassport thus verifying terminal has to authenticate itself first. Since the initiator receives more important consideration of its identity the protocol is called SIGMA-I. As an optimisation the protocol is modified with Schnorr's signature scheme [258] as authenticated encryption scheme, taking only one elliptic curve multiplication for signature generation. The SIGMA-I protocol is depicted in figure 7.6.

### 7.3.2. IBIHOP+

The extended IBIHOP protocol [228] originates from the space-efficient implementation on RFID tags, therefore the protocol is optimised for minimal circuit area and efficient hardware implementations. Focus of IBIHOP's design is to circumvent concerns of

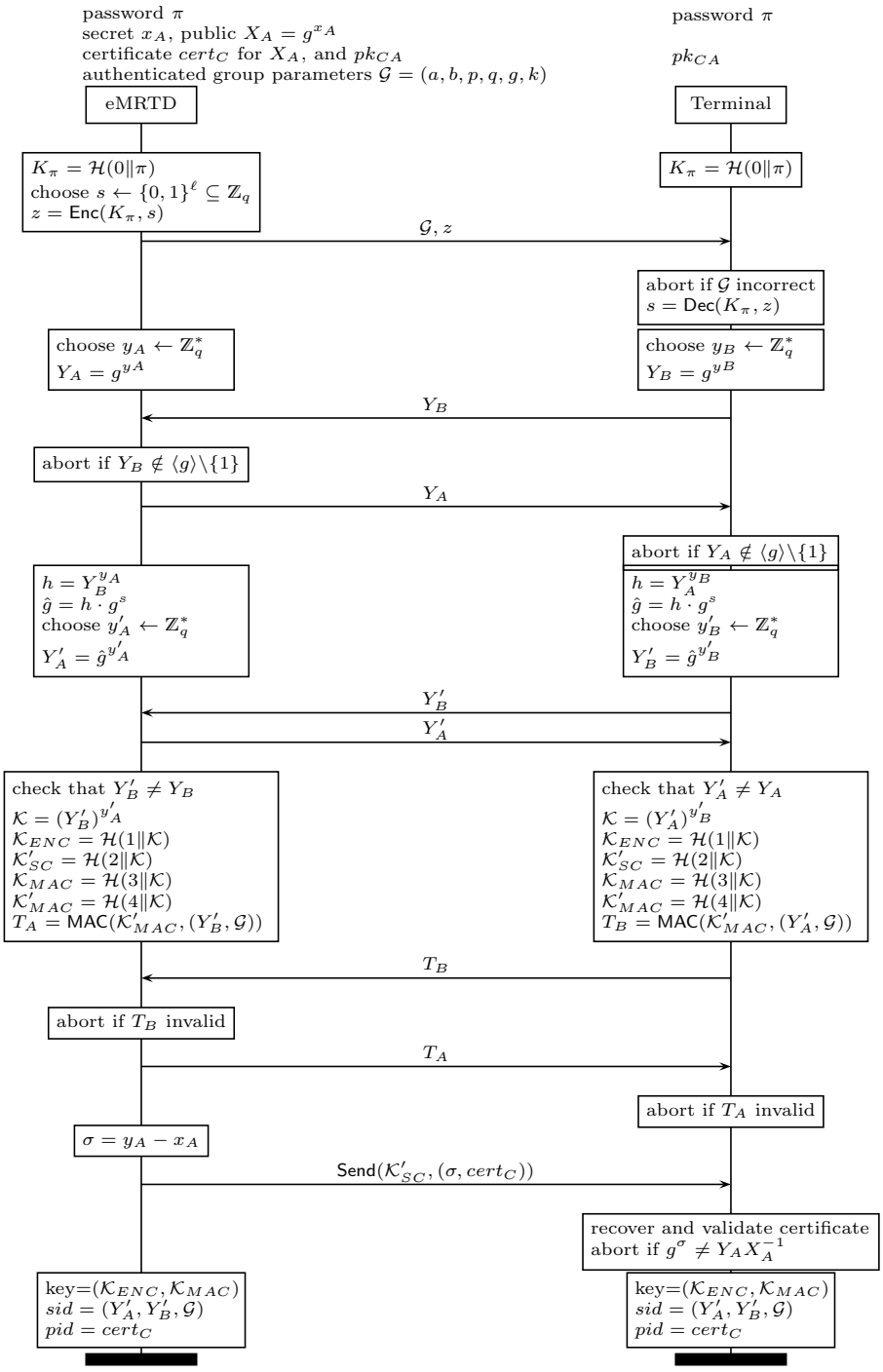



Figure 7.5.: The PACE|CA protocol [14].

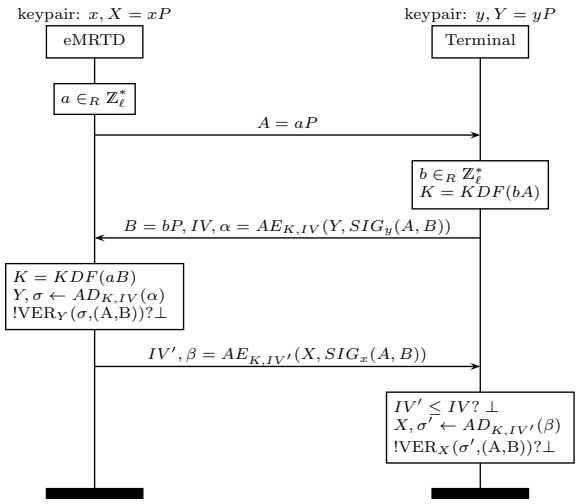



Figure 7.6.: The SIGMA-I protocol [176, 229].

RFID tags responding to any request by implementing mutual authentication between the tag and the reader, hence preserving the tag's privacy. With these requirements, the protocol is primarily designed for efficient mutual authentication and not for key agreement, resulting in the absence of forward security. IBIHOP+ adds a forward secure key agreement to the IBIHOP protocol by adding a full Diffie-Hellman key agreement.The IBIHOP+ protocol is depicted in figure 7.7.

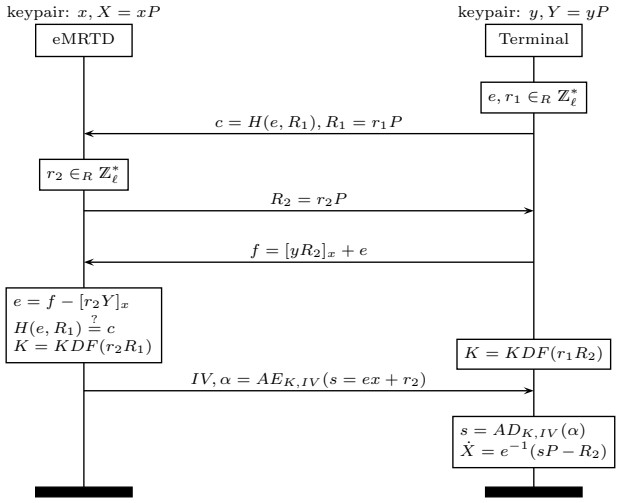



Figure 7.7.: The IBIHOP+ protocol [229].

Both protocols are discussed and evaluated regarding security, privacy and efficiency in accordance to the RFID privacy model by Hermans *et al.* [229]. Regarding privacy Peeters *et al.* show that SIGMA-I and IBIHOP+ are wide-strong private and PACE

has only wide-destructive privacy, since an attacker can correlate between a given secret and a PACE iteration. With respect to efficiency, both proposed protocols require less communication rounds and fewer elliptic curve operations than PACE. On the ePassport side IBIHOP+ needs less elliptic curve operations than the SIGMA-I protocol and is therefore the declared winner of both proposed protocols. Peeters *et al.* propose to spend the gained time on thoroughly verifying the biometrics of the document holder.

## 7.4. Zero Round-Trip Time EU EAC

Recently Google introduced the idea of security protocols with a zero round-trip time (0RTT) mode with its proposed QUIC protocol [118], furthermore 0RTT-supporting modes have been accommodated in recent drafts of the TLS 1.3 standardisation [250]. Brendel and Fischlin [28] propose a 0RTT mode enhancement for the EU EAC protocol, while remaining compliant to the current EU EAC standard and provide a security proof for their design. The basic idea of the 0RTT mode is the introduction of a so-called semi-static public key $g^s$. In contrast to an ephemeral key, which is only used for one session or a static key with permanent validity a semi-static key is only valid for a limited time only. The semi-static key $g^s$ is transferred from the server to the client during the first encounter of both entities. Thus, the first authenticated key agreement between client and server is a full Diffie-Hellman key exchange and only the second and further encounters between client and server can make use of the 0RTT mode. During the 0RTT mode the client uses a new ephemeral key $g^c$ and combines it with the servers semi-static key $g^s$ to directly receive $g^{cs}$ and immediately communicate via a secure channel with the server without any packet round-trip overhead, hence the name 0RTT mode. The EAC+0RTT mode proposed by Brendel and Fischlin is depicted in figure 7.8, in it $pk_T^{semi}$ refers to the beforehand transmitted semi-static public key of the Terminal.

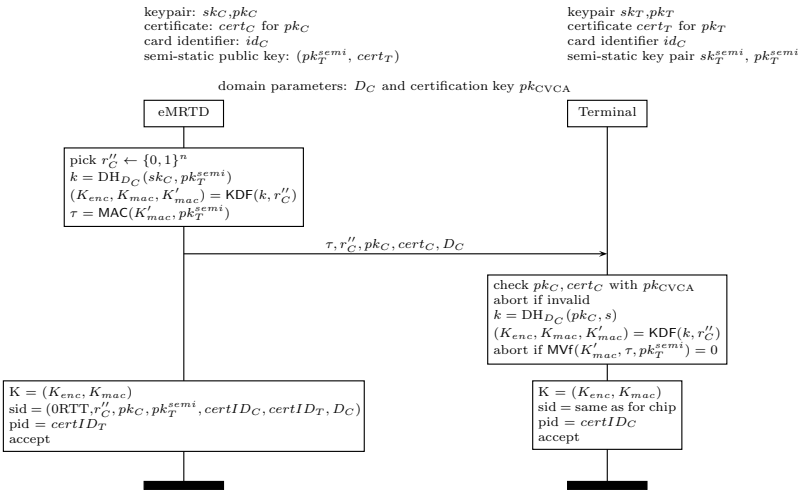



Figure 7.8.: The EAC+0RTT protocol mode [28].

Google introduced this mode in its QUIC protocol with the main use case in mind being the common daily web search behaviour of a user who uses the Google web search multiple times in a short time frame. Benefits of the 0RTT mode can only be fully exploited if the actual scenario utilises multiple connections between the client and server in a relatively short time frame. The authors Brendel and Fischlin motivate this circumstance with the increasing adoption of the EU EAC protocol in the smart card domain for secure transactions and physical access control. A concrete example discussed by the authors is the access to subway stations, which can be realised via the EU EAC protocol and is indeed a use case with multiple successive uses in a short period that relies on fast response times and short latencies to maximise the throughput to subway entries. Even so, the so-called EAC+0RTT protocol is an interesting proposal for this scenario, the classical border control scenario at an airport will most likely not benefit from the protocol enhancement since the probability of using an ePassport on the same terminal at the same airport is rather small. On the one hand, the route into an airplane is different than exiting an airplane at most airports and on the other hand, even if it would be the same route the border check commonly has multiple queues with different terminals where the traveller cannot always choose the preferred queue. Both factors make the repeated access to a terminal at an airport very unlikely. Therefore, the protocol enhancement is out of scope for this work.

## 7.5. Security Protocol Discussion

Directly evaluating the discussed protocols against each other cannot spawn a very fruitful discussion because the design goals are too different for the introduced protocols. Nevertheless, a trend of changes can be observed, discussed, and assessed towards future eMRTD requirements for the security protocols.

One of the design paradigms that applies to all new protocols besides EAC+0RTT is to renounce of strong cohesion and loose coupling and instead to combine multiple security goals in one monolithic security protocol similar to the Authenticated Encryption (AE) [197] design idea. Since the protocols are designed for a specific use case, the intended benefits of the software design pattern cannot exploit its strengths fully anyway. Benefits of the combined security goals in the discussed security protocols in contrast to the current eMRTD protocol suite are twofold. On the one hand, the number of round-trip time steps and elliptic curve operations is reduced, and on the other hand, fixing the protocol execution steps to one design reduces the source of errors for API calls compared to more flexible solutions as OpenSSL [169]. In context of eMRTD's reduction of round-trip time and elliptic curve operations does not have equal impact on overall border control time. On the one hand, the data transfer rates are slow in theory (i.e., 106 – 424 kbit/s [231]) and even slower in practice since transfer of the 15 kB DG2 facial image takes around 4 seconds to transfer. On the other hand, the cryptographic eMRTD FameXE coprocessor used in ePassport SmartMX [221] chips can compute elliptic curve operations much faster (i.e., 30 ms per ECC operation [220]). From a cryptographic research standpoint, reducing necessary scalar multiplications on the elliptic curve is an

interesting topic but the practical impact on border control is minimal due to the slow transfer rates of the wireless interface. Instead, reducing data transfers by consolidating multiple security goals into one security protocol for reduced round-trip times has more impact on the border control throughput times, which all discussed protocols in contrast to the current protocol stack fulfil.

In contrast to ICAO's optional Active Authentication recommendation most proposed protocols integrate a chip cloning protection. On the one hand, PACE|AA and PACE|CA add the chip cloning protection to the PACE protocol as a mandatory step and on the other hand, SIGMA-I and IBIHOP+ integrate it fluently as part of the mutual authentication process. So adding chip cloning as an inexpensive mandatory step should also be part of future ePassport protocols.

BioPACE v2 adds no mandatory chip cloning protection, but combines other security goals into one protocol. It combines the security goals of PACE, i.e., establishing a secure cryptographic channel between eMRTD and terminal, linking between printed document and the data on the chip, and providing a link between physical document and the document holder. Since BioPACE v2 uses implicit on chip comparison of the biometric data, it provides stronger data privacy, and does not require EAC with the Verifying PKI. An argument against BioPACE v2 is that the biometric data would only be accessible to the chip and not available for blacklist processing. In practice, this is not true since the individual person claiming to be the document holder is present in the ABC gate and a freshly taken biometric probe can be compared against the blacklist. This is sufficient and logical since the person trying to cross the border should be freshly checked against the blacklist and not the older biometric probes on the chip, which has also been identified by the EU action plan against travel document fraud [91]. Member States will start to integrate the automated fingerprint identification system (AFIS) to perform blacklist checks as part of the Schengen Information System (SIS) in 2018. The AFIS blacklist with BioPACE v2 can therefore fully replace the EAC protocols, the protected DG3 fingerprints and the Verifying PKI. Furthermore, since as of today EAC is not deployed at airports it would not be a replacement, but a supplement for a stronger link between document and the document holder. BioPACE v2 does provide a comprehensive security discussion, but no formal security proof. On the one hand, the BioPACE v2 protocol does not change the PACE core steps, but only introduces a pre step, which is independent of the existing security proof by Bender *et al.* [13]. On the other hand, the security proof is only for the more computationally expensive generic mapping and not for the faster integrated mapping, which is also stated by Peeters *et al.* [229].

The discussed protocols all provide some benefits over the currently used protocols and provide a foundation for the next eMRTD protocols for the future generation of ePassports.

# 8. Enhancing eMRTD SPI via Revocation

This chapter is based on and was published as [40] and [41].

As of today, the Verifying PKI neither supports CRLs nor OCSP [31]. Although the reason is not given in the policy [31] it is believed that it is due to the missing external connection of the eMRTD and memory restrictions on the eMRTD. Computing power increases through progress and the next generation of smart cards will support TCP/IP, therefore these are no longer obstacles [241, 177].

The following sections present potential Internet domain solution candidates to introduce a revocation mechanism to the Verifying PKI and discuss the practical feasibility, respectively. The starting point are protocols which are standardised for the Internet domain and thus thoroughly investigated.

Table 8.1 shows the three Internet domain candidates and their distinguishing characteristics as described in detail in the following sections.

Table 8.1.: Internet domain Candidates and Criteria.

| | candidates | | |
|---|---|---|---|
| criteria | CRL | OCSP | SCVP |
| storage requirement | high | none | none |
| memory requirement | high | low | low |
| computational amount | high | low | low |
| network traffic | high | low | low |
| real-time revocation | no | yes | yes |
| permanent connection | no | yes | yes |

## 8.1. Certificate Revocation List (CRL)

Certificate Revocation Lists (CRL) provide a mechanism to invalidate certificates before their actual expiration date. A reason for such an action can be for example the compromise of the private key or the release of a superseded certificate [276]. Besides completely revoking a certificate, a certificate can be put temporarily on hold until circumstances are clarified and the certificate can resume its validity period or become completely revoked. CRLs are specified in [127] as part of the X.509 PKI standard [276]. The CRL is a signed list of the revoked certificates and must be issued periodically by the Certificate Authority (CA). The CRL has a validity period itself and must be updated after the expiration. An advantage compared to other revocation techniques is

that after the CRL has been received no more external connection is necessary until the CRL expires. One key problem with CRLs is that their size increases monotonically, sometimes it grows arbitrary large after some time [294]. The bandwidth and storage requirements make CRLs not attractive for low memory and limited processing power environments. Instead of full CRLs the delta variant may be used in conjunction with the delta CRL extension to reduce bandwidth usage, but the required storage problems remain or even become larger through overhead [274].

In the context of the Verifying PKI a CRL has to be provided by the issuing country of the eMRTD, because a member state will not delegate this privilege to other member states. If the CRL is signed by the CVCA it can be verified with the certificate stored on the eMRTD chip. However, the eMRTD would need extra internal persistent memory to save the CRL. To check if it needs to download a new CRL the eMRTD chip would still need a clock. Without a clock the eMRTD chip needs to download the entire CRL during every Terminal Authentication. Depending on the size of the CRL this might be significant overhead and could immensely extend the validation time. Downloading the CRL would be the duty of the inspection system. Parsing through a big revocation list might also take unnecessarily long for the eMRTD chip [294].

## 8.2. OCSP

The Online Certificate Status Protocol (OCSP) provides an alternative to CRLs [211]. Besides real-time status, OCSP provides the benefit of lower bandwidth usage per request and no storage requirement compared to a CRL. Some OCSP responders present data simply fetched from a CRL, which results in an easy implementation, but is not better than the CRL in term of real-time revocation. CRLs should be avoided as direct data source and a modern database should be used instead to provide actual real-time revocation. A drawback is that the OCSP responder has to be available all the time [294].

Using OCSP as revocation mechanism in the Verifying PKI delivers many benefits over traditional CRLs. The eMRTD chip does not need additional internal memory for storing the list, the download size is smaller and simultaneously the eMRTD chip does not need to process an entire list of CRL entries. The eMRTD chip can get a direct response if the certificate has been revoked or is valid depending on its regular expiration date. Even so the paper by Chaabouni and Vaudenay [58] has a different focus; it favours OCSP to improve EAC. A time source is still needed, because the OCSP responder does not check the validity period of the certificate, but instead checks if it has been revoked (i.e., blacklist) and with the OCSP extension CertHash [23] also if the certificate has really been issued by the CVCA (i.e., whitelist). In this use case the validity period of the certificates will be verified by the eMRTD as part of Terminal Authentication and the OCSP responder should only send the status “good” (not revoked) or “revoked”. The “unknown” status is prohibited. For further evaluation and security discussion it is assumed an OCSP responder, which mimics this behaviour, uses the CertHash extension, and is supplied by a database which can be updated in real-time.

## 8.3. SCVP

The Server-Based Certificate Validation Protocol (SCVP) in contrast to OCSP provides a server based full validation of a certificate, with optional revocation [100]. The complete certificate path creation, validation and check for revocation is done by the SCVP server. If the client trusts the server, it can delegate nearly the complete PKI overhead to the SCVP server. This enables the use of a PKI for low-end devices. To check the validity status of a certificate the SCVP server uses either CRLs or OCSP. SCVP is not widely used yet, but has been tested on smart cards [225]. SCVP provides authenticity and integrity of the request and response messages, but does not ensure confidentiality. However, the SCVP standard suggests using the Transport Layer Security Protocol (TLS) if confidentiality is needed [76].

An eMRTD chip with support for the SCVP would not only benefit from the features of OCSP, but would also no longer depend on a clock. SCVP messages would be signed by the CVCA (or a dedicated SCVP service) and SCVP also provides measures against replay attacks. Despite the need for a transport protocol between inspection system and eMRTD chip, because of the missing Internet connection, SCVP is a promising solution with regard to created benefit.

## 8.4. Hoepman protocol

This sections discusses the Hoepman protocol, which is a security protocol, tailored for real-time eMRTD revocation. Hoepman *et al.* [125] present weaknesses and propose security improvements for a variety of eMRTD protocols. Relevant for this section are only the proposed improvements for EAC. Hoepman *et al.* [125] sketch an idea of a self-invented online terminal authentication (Hoepman protocol) and define certain boundary conditions (e.g., resistance to replay attacks). The proposed protocol is very similar, to the SCVP protocol (see section 8.3). It also delegates the actual terminal authentication to a trusted third-party called Application Authority ($AA$). However, in contrast to the SCVP proposal the Hoepman protocol separates the terminal access rights from the terminal certificates. Hoepman *et al.* [125] refer to the terminal certificate as $C_{AA}$ which contains the public key $K_{TA}$ and is signed by the $AA$. They describe their proposed protocol as such:

"First, the terminal sends the certificate $C_{AA}$ (containing its public key $K_{TA}$) to the chip. The chip and the terminal perform a challenge-response protocol in which the terminal proves to the chip that it owns the private key corresponding to $K_{TA}$. This establishes the identity of the terminal. Next, the chip sets up an authenticated channel between itself and the back office of the issuing country. It can do so using a country certificate that is stored in the chip during personalisation. The channel should not be vulnerable to replay attacks. It sends $C_{AA}$ (and $K_{TA}$) to the back-office. There, $C_{AA}$ is verified against the known application authorities (this validates that $K_{TA}$ was certified by such an authority) and $K_{TA}$ is checked against the list of all revoked terminals. If these checks pass, the access rights for $AA$ are sent back to the chip. If not, then the

empty set (i.e., no access rights) is sent back to the chip. The chip interprets the access rights it receives and grants access to the terminal accordingly. Because the channel is authentic and does not allow replay attacks, the access rights received by the chip correspond to the certificate it sent to the back office." [125]

Although this is a promising approach which provides real-time revocation, it suffers from two drawbacks: first, there is no detailed specification of the mechanism. Second it is a new protocol, which has to be investigated thoroughly. Solution candidates from the Internet domain, however, are mostly based on well-known and well-established Internet standard protocols that have been proven useful in other domains for a long time. Additionally, Hoepman *et al.* [125] do not provide an assessment methodology to evaluate solution candidates. Nevertheless, the Hoepman online terminal authentication is currently one of the most promising, self-created approaches from the scientific community and will therefore be evaluated against the other candidates.

## 8.5. Evaluation of Solution Candidates

For a revocation it is mandatory that the eMRTD chip can securely communicate with a trusted home server. This is not possible without extra infrastructure to handle the requests and the willingness of the inspection system to play the role as a network bridge between the Internet and the current simple smart card communication protocols. Due to the availability of UMTS or LTE this assumption even holds for mobile inspection systems. Mobile inspection systems without Internet access can fall back to the validation of the physical security features, face recognition or a manual validation with the picture printed on the data page. OCSP and SCVP both provide good solutions if the infrastructure obstacles (i.e., the high availability demands) can be handled. Both protocols effectively solve the problem of stolen terminals and their efficiency has been proven in other domains. The classical CRL is not suitable for the EAC revocation, because of the low-power eMRTD chip (see table 8.1).

This section introduces an evaluation scheme and applies it to the Network Time Protocol (NTP) [204] in combination with OCSP, SCVP and the Hoepman protocol [125]. NTP together with OCSP will from now on referred to as NTP+OCSP. The criteria are mostly based on the well-known Software Engineering non-functional requirements [290].

*Security* is the first criterion which the candidates are evaluated against. This criterion consists of the resistance against certain attacks like replay attacks, and man-in-the-middle attacks.

*Convenience and Acceptability* are the next criteria which reflect the end user's benefits and drawbacks which the respective solution provides.

The *Total Cost of Ownership (TCO)* is a criterion which not only depends on the new technology needed to provide the services, but also on the reusability of existing IT structures.

If another country wants to introduce a new technology and therefore the global number of users changes dramatically, then *Scalability* is the criterion which considers this.

The fifth criteria are *Reliability and Availability* which rate the dependence on other systems and if the systems are loosely coupled or if they heavily rely on other components.

*Feasibility* is the last criterion which also includes how likely it is that a certain technology will be integrated into an eMRTD.

Some criteria are not independent e.g., the scalability can influence the availability and therefore the user's acceptance and so on.

In the eMRTD domain *Security* and *Scalability* are considered the most important criteria. On the one hand, security is an absolute must, because of the embedded biometric data and on the other hand, scalability is very important, because in tourist seasons the passengers boarding airplanes can increase drastically and smooth operation of inspection systems must still be ensured. A higher security level at border checks is one of the main reasons why eMRTDs were introduced in the first place. Therefore, security is also one of the key factors for extending the current procedures. Another key factor why eMRTDs were introduced is the automation of border checks with so-called Automated Border Control gates (ABC gates) [102]. ABC gates can only make border checks faster if the underlying system properly scales with severe load scenarios like the holiday period. Therefore, *Security* and *Scalability* will weight double for the final score.

For every criterion the candidates are rated positive (+), neutral (∘) or negative (-) and for the final rank the individual ratings get points, these are then summed up to receive an end result. Table 8.2 presents a summary of the revocation protocol evaluation results.

### 8.5.1. Security

In this subsection all candidates are evaluated for potential weaknesses against common security attacks like replay attacks, and man-in-the-middle attacks.

The first item is the resistance against replay attacks. NTP, OCSP and SCVP all provide nonce support to individually link the unique request/response pairs, by default or via a protocol extension. The lightweight OCSP profile [74] should not be used, because it removes the nonce in favour of better scalability which is achieved by response pre-production and response message caching. To prevent replay attacks unique request/response pairs are essential.

The next topic is the resistance against man-in-the-middle attacks. NTP, OCSP and SCVP support the use of digital signatures for authenticity and therefore prevent man-in-the-middle attacks. Independent of the supported mechanisms, there is no direct use case for a man-in-the-middle attack, because confidentiality is no security goal, due to the fact that all time information and the revocation status are not considered confidential. A possible attack would be an Impersonation Attack in which the attacker tries to make the client believe that it is a legitimate server. This attack is also prevented by the same mechanisms as the man-in-the-middle attack.

A general security concern might be the introduction of TCP/IP itself, because it might open new attack vectors to the eMRTD. This can easily be mitigated by only allowing a one-to-one connection between the inspection system and the eMRTD with exactly one open socket. So with this careful design decision both protocols will provide

Table 8.2.: Revocation Protocol Evaluation Ratings.

| criterion | NTP+OCSP | SCVP | Hoepman |
|---|---|---|---|
| Security (replay & man-in-the-middle attack) | + | + | + |
| Convenience & Acceptability (border check time, privacy) | ∘ | + | + |
| TCO (hardware, software, reusability) | ∘ | - | - |
| Scalability (network load, home server load) | + | ∘ | - |
| Reliability & Availability (complexity, points of failure) | ∘ | ∘ | ∘ |
| Feasibility (economical) | + | - | ∘ |

a higher security increase than potential TCP/IP flaws a security decrease. Also, future eMRTDs supporting IP will most likely not communicate to the Internet directly, but always with assistance of the terminal as proxy to handle network subtleties like DNS or routing, which also makes implementation of complex network details easier and more robust. OCSP, the Hoepman protocol and SCVP specify TCP/IP as their default transport layer protocol. Even so a different transport layer protocol might be chosen, for a fair rating it is assumed that all application layer protocols rely on the same transport layer protocol TCP/IP. Therefore, this will not influence the rating.

From a security point the candidates from the Internet domain have no significant weaknesses. On the one hand, the fact that NTP+OCSP consist of two different protocols whose services must be provided by two different services, even if they are running on the same server, provide two potential weak points and SCVP only one. On the other hand, the independence of both services could also be treated positive, because it might be harder for an attacker to disturb both services. So this depends on the actual implementation and should not influence the rating. Therefore, both Internet domain candidates get a positive security rating.

For the *Security* criterion the Hoepman protocol only defines resistance to replay attacks as a boundary condition, but this should not be a practical problem, because comparable to SCVP this could be achieved with a unique request/response pair by nonce support. As a second requirement the Hoepman protocol creates an authentic channel from the chip to the back office. Since both entities have a common root certificate, setting up such a channel is possible with common cryptographic primitives and such a channel is also resistant against man-in-the-middle attacks. Therefore, the Hoepman protocol gets a positive rating.

### 8.5.2. Convenience and Acceptability

The user's convenience directly influences the acceptance of a certain technology. So a criterion must be how the new protocols influence the average border check time. A main benefit from the new protocols is better data privacy for the biometric data stored on the eMRTD.

The solution candidate's influence, on the border check processing time, shall be the first item for evaluation. NTP+OCSP has the disadvantage that it can only lengthen the eMRTD evaluation, because the EAC verifying card-verifiable certificate chain must still be validated by the chip and the additional steps for time acquisition and the certificate revocation cost additional time irrespective of how much. In contrast, SCVP can make the evaluation process shorter, require the same amount of time or even take longer.

For SCVP the certificate chain validation itself will take a shorter time, because the SCVP server has more computation power than a small smart card microprocessor. Two new potential time additions come to the verifying process on the SCVP server compared to current verification on the eMRTD. These are the acquisition of an accurate time and the certificate revocation mechanism. Both can be done independent of the certificate verification if NTP and automatic CRL download is used by the server. If OCSP is used by the server it would negatively influence the validation time and therefore a CRL

should be preferred. The SCVP validation process is expected to be faster than on the chip and the only variable remaining is the transmission of the request and response.

Calculating an exact transmission time is not possible, because it depends on at least the bandwidth and the distance to the home SCVP server.

The next item of consideration shall be how the data privacy benefits from the solution candidates. NTP+OCSP and SCVP both provide the same benefit that expired terminal certificates will always be rejected and that stolen or compromised terminal certificates can be revoked effectively. Both mechanisms provide the same benefit, but one question is if the protocols could leak private information or enable tracking of the document holder. Neither NTP, OCSP nor SCVP send travel document specific data to the home server. NTP does not send any privacy relevant data at all and OCSP/SCVP send only data identifying the inspection system to the home server. Therefore the only negligible privacy concern is that the home server's operator could learn that one of the country's million passports is currently presented to the terminal. The operator is not able to identify the document holder any further and therefore this is not considered a privacy risk.

So NTP+OCSP and SCVP only provide a benefit and pose no risk to the document holder's data privacy. Both Internet based solution candidates can provide convenience for the users and therefore boost their acceptance. NTP+OCSP provides all the benefits that SCVP does, but can only slow down the border check handling therefore it gets a neutral rating and SCVP a positive rating.

The Hoepman protocol is very similar to SCVP in regard to the fact that it delegates the certificate checks to a trusted third party server in the back office of the issuing country. Thus the Hopeman protocol is expected to provide a faster validation process than the current EAC Terminal Authentication, comparable to SCVP. Since the Hoepman protocol only sends the terminal certificate to the home server, the privacy concerns are as negligible as with SCVP. Therefore, the Hoepman protocol gets a positive rating for *Convenience and Acceptability*.

This analysis identifies that neither NTP, OCSP, SCVP nor the Hoepman protocol send travel document specific data to the home server. Nevertheless, if the transferred data must be considered confidential due to possible regulations this additional security goal can be achieved by using TLS. The impact of the confidential transport channel is equal for all protocols and will therefore not influence the evaluation results.

### 8.5.3. Total Cost of Ownership (TCO)

This chapter focuses on the expense necessary for the solution candidates. First, the necessary new hard- and software will be assessed. Furthermore, it is important which components of the already existent system can be reused or integrated directly or indirectly for example after a firmware update.

NTP, OCSP and SCVP have a relatively equal impact on the Verifying PKI and inspection system structure. The eMRTD chip is not upgradeable via a firmware update, so only the next generation of eMRTDs could support the new protocols. Whether the current chip is powerful enough to perform all three protocols is hard to tell, but

all of them have already been implemented on a regular smart card [225]. The current eMRTD chip is powerful enough to validate card-verifiable certificate chains, so it should be powerful enough to handle a time stamp package and an OCSP response or an SCVP response. Also neither of the protocols need any additional persistent storage space. So the financial impact on the eMRTD itself should be minimal from a hardware perspective. The software has to be changed of course to support the new protocols.

The next items to evaluate are the changes necessary to the inspection systems. The necessary modifications for the inspection systems operating system should be patchable with a new firmware. So only development costs occur, but no hardware upgrade costs. For NTP+OCSP and SCVP an Internet connection is necessary to communicate with the respective home server. The inspection system must already communicate with its DV and this DV must communicate with its country's SPOC. So some sort of network connection should already be present. Upgrading the broadband connection for the inspection system might be necessary as well as an upgrade for the SPOC to handle real time requests.

The last item for potential upgrade costs is at the home server. NTP+OCSP and SCVP need some sort of home server for every issuing country with a connection to the country's SPOC. The server must provide an NTP server and an OCSP responder or an SCVP server. To provide authenticity and integrity all three protocols support the use of digital signatures. The generation of the signatures could be accelerated by using Hardware Security Modules (HSM). Standard CPUs are also needed to handle the protocol request and the certificate chain creation and revocation for OCSP.

Even without exact figures SCVP and NTP+OCSP can be compared. On the one hand, NTP+OCSP cost two HSM runs for digital signature generation because they are two stand-alone protocols and SCVP only one, but on the other hand, SCVP needs more CPU time for the certificate chain building, revocation and verification than NTP+OCSP for a revocation and system clock lookup.

The bandwidth consumption of NTP+OCSP and SCVP should be minimal for both. NTP+OCSP might have higher development costs for the eMRTD chips software, the inspection system software and the SPOC's software. The development costs should be minimal compared to the required hardware costs for the home server. As already mentioned above, NTP+OCSP might require more HSM signing runs and less CPU power, than SCVP. For the actual NTP+OCSP specification it could be considered to drop the internal signatures and instead sign both responses together in one big response block. With such an optimisation only the CPU time remains, which is much higher per SCVP request than per OCSP request. So NTP+OCSP gets a neutral ranking and SCVP a negative ranking for the TCO, because of the higher CPU time costs.

As discussed before, from a technical standpoint the Hoepman protocol is very similar to the SCVP protocol. Even though it is not specified in detail it is reasonable to assume that the financial impact of the back office server is comparable to the SCVP server. Since it additionally manages dynamic access rights and is based on a practically untested and unoptimised protocol the *TCO* might be even worse than for SCVP, which already got a negative rating. So the Hoepman protocol also gets a negative rating.

### 8.5.4. Scalability

Scalability describes the system's behaviour if the requirements on supported user clients change drastically. The increased input can influence the performance because of higher resource requirements which depend on the complexity of the entire system. One criterion to evaluate is the load per request, which directly influences the system's scalability. The load on the home server and on the network between inspection system and home server can be differentiated.

To compare the network load of NTP+OCSP with the one from SCVP it must be taken into consideration that the protocols will most likely be implemented in a more lightweight form. The NTP network impact is minimal and therefore only OCSP and SCVP shall be compared. All certificates must be checked for revocation in case of OCSP. In case of SCVP all certificates need verification. The requests could contain all necessary certificates or just the serial numbers of the certificates which would result in a lower network usage.

For OCSP the serial number is always enough, because even if the OCSP responder does not know the associated certificate for the serial number, the certificate revocation status is considered good.

For SCVP a serial number certificate look up must always provide a result, because otherwise no verification of the complete chain is possible. The SCVP server can be easily provided with the CVCA certificate because it is present in the same country.

The DV certificate's signing requests are all handled by the SPOC which shall also be connected to the SCVP server. Therefore, an automatic supply of DV certificates should also be possible without requiring major effort. One problem however lies in the acquisition of the terminal certificates. They are created by the DV, for every terminal, on a daily basis and the serial number remains unknown for the SCVP server. So for SCVP the terminal certificate must be sent entirely instead of just the serial number.

SCVP would have a higher average bandwidth usage than NTP+OCSP. For the TCO scoring, it was already estimated that SCVP would have a higher CPU load per request. Therefore, NTP+OCSP gets a positive rating and SCVP a neutral one.

For the Hoepman protocol a transfer of the certificate is also always necessary, which makes the network impact higher than the impact of NTP+OCSP. Compared to SCVP it is an untested and unoptimised protocol, which therefore either performs similar to SCVP or worse. A difference to SCVP is that the back office server sets the access rights dynamically, which is in theory a nice feature but costs higher CPU load per request because of the decision logic than SCVP. Therefore, the Hoepman protocol gets a negative rating compared to the optimised and well-established Internet standards.

### 8.5.5. Reliability and Availability

Reliability and the linked availability are influenced by the solution candidates complexity and the resulting points of failure. A terminal not supporting the protocols or even a broken terminal always breaks the regular border control procedure and is out of scope for this evaluation. NTP+OCSP and SCVP need an Internet connection to

communicate with the home server. If the connection fails, all three protocols will not work. They also need the verifying country and issuing country SPOC to be online at all times. Both are points of failure as well as the home server of the issuing country. On the home server runs the NTP and OCSP services or the SCVP service to process the requests from the eMRTD. All of these are potential points of failure.

One small difference here is that for NTP+OCSP two services could stop working and for SCVP only one service, but again the purpose of NTP and OCSP is independent, so one service still running from two could also be considered as a better circumstance than a complete breakdown of a single service.

NTP+OCSP and SCVP have no big difference in their points of failure. It could be argued that the tasks of SCVP are more complicated and more prone to error, but this would involve potential implementation errors which are out of scope. Both candidates heavily rely on external systems and therefore both get a neutral rating.

The Hoepman protocol also relies on an external component, the back office server. As untested and more complex protocol (due to the dynamic access rights) the reliability can be considered worse or equal to SCVP. For NTP+OCSP and SCVP potential implementation errors are not considered and defined as out of scope. Therefore, the Hoepman protocol gets the same neutral rating as SCVP, because it also heavily relies on external systems.

### 8.5.6. Feasibility

Feasibility for the solution candidates can be divided into technical feasibility, financial feasibility, economical feasibility and the basic conditions concerning the existing infrastructure.

From a technical perspective all solution candidates are possible. OCSP and SCVP were implemented for some research projects on smart cards and can therefore be considered technical feasible on the eMRTD chip [225].

The financial part was already evaluated in, Section 8.5.3 therefore this shall not have an impact on the feasibility evaluation. The economical feasibility shall be the matter at hand. NTP+OCSP and SCVP both extend the EU EAC mechanism and provide effectively the same benefit. Financial factors aside both candidates require a certain amount of development effort. NTP+OCSP are two protocols, but do not automatically lead to the doubled development effort, because the protocols are older, simpler and most likely more common to the developers for the implementation on a smart card. What sets the difference is that NTP and OCSP could be more or less directly implemented on a smart card with little or no development effort for the home server. SCVP in the eMRTD would need an implementation with a single request response pair and the missing access to the terminal certificates for the home server would enlarge the request or require more effort for the DVs. That is why NTP+OCSP are considered more likely with this simple analysis than SCVP.

SCVP needs a more complicated home server, the protocol would have to be adjusted and would create more burden for the DVs. Therefore, NTP+OCSP gets a positive rating and SCVP a negative rating.

The Hoepman protocol is a theoretical concept and therefore it is only possible to speculate about its technical feasibility. It consists of common cryptographic primitives so it is very likely that it is technically feasible. From an economical perspective it is simply unlikely that the EU would select an untested new protocol, which provides no practical benefits compared to the competitors, instead of a well-established and tested protocol. This is why the Hoepman protocol gets a negative *Feasibility* rating.

## 8.6. Revocation Discussion

Table 8.2 shows a summary of the solution candidates evaluation results, and table 8.3 presents the final results. The positive rating gets two points, the neutral rating one point and the negative rating zero points. Additionally, the points for *Security* and *Scalability* will be doubled. NTP+OCSP ranks first with 13 points, SCVP second with 9 points and the Hoepman protocol last with 7 points. So the recommended solution for revocation is NTP+OCSP. Nevertheless, revocation for the Verifying PKI is only reasonable if EAC is actually used during border control. Since this is as of today not the case, the security protocols discussed in chapter 7 to replace EAC (i.e., BioPACE v2) are also a viable alternative.

Table 8.3.: Revocation Protocol Points and Result.

| criterion | NTP+OCSP | SCVP | Hoepman |
|---|---|---|---|
| Security (x2) | 4P | 4P | 4P |
| Convenience & Acceptability | 1P | 2P | 2P |
| TCO | 1P | 0P | 0P |
| Scalability (x2) | 4P | 2P | 0P |
| Reliability & Availability | 1P | 1P | 1P |
| Feasibility | 2P | 0P | 0P |
| Point Sum | 13P | 9P | 7P |
| Final Rank | 1 | 2 | 3 |

# 9. Enhancing eMRTD SPI via PQ Crypto

This chapter discusses the impact of quantum computers on the asymmetric cryptography used by eMRTDs today and potential post-quantum secure replacements suitable for the requirements of eMRTDs. The threat of quantum computers to today's asymmetric cryptography is known in the scientific community for more than 20 years, after the publication of a polynomial-time algorithm for prime factorisation and discrete logarithms on a quantum computer by Peter Wiliston Shor [264]. Recently multiple experts have warned [234, 20] of the practical construction of a large-scale quantum computer by secret intelligence services in the near future. Since eMRTDs rely on asymmetric cryptography, whose security is based on the discrete logarithm problem on elliptic curves and the factorisation problem, Shor's algorithm and the rising likelihood of a large-scale quantum computer also impact the future security of electronic travel documents.

All algorithms found today that are significantly faster (i.e., exponentially faster) on a quantum computer than on a classical computer are based on the quantum Fourier transform [264]. So is Shor's algorithm, which uses the quantum Fourier transform for finding the order of an element $x$ in the multiplicative group (mod n) and discusses how this can be applied for polynomial time integer factorisation and finding discrete logarithms in polynomial time. Shor states that this algorithm can make breaking RSA on a quantum computer faster than encrypting RSA on a classical computer [264]. In [27] Boneh and Lipton generalise the Shor algorithm for more relaxed requirements, namely a group that is abelian but not cyclic. Therefore, the Shor variant by Boneh and Lipton can also break elliptic curve cryptography, which is commonly based on additive groups. Ettinger *et al.* [87] further generalise the Shor algorithm to any problem that can be reduced to the hidden subgroup problem (HSP) (see [17]), effectively creating an algorithm which runs in polynomial time for an arbitrary finite group $\mathcal{G}$ [8]. A second quantum algorithm called Grover's algorithm by Lov Kumar Grover [115, 116] has impact on all cryptographic systems but can be compensated by selecting bigger key sizes. In contrast to quantum algorithms based on the quantum Fourier transform like the Shor algorithm, which are exponentially faster than their classical counterparts, the Grover algorithm only provides polynomial speed-up to the classical computer case. Grover [115, 116] presents a quantum search algorithm that can speed up search applications over unsorted data that only requires $\mathcal{O}(\sqrt{n})$ quantum steps instead of the $\mathcal{O}(n)$ steps on a classical computer [113].

The research field of finding and selecting algorithms that run on a classical computer, but are considered resistant to attacks by quantum computers (e.g., Shor's algorithm and Grover's algorithm), is called post-quantum cryptography. As of today six families (classes) of cryptographic algorithms are considered post-quantum secure by the cryptographic community, according to current state of research [17]. These cryptographic sys-

tems are: hash-based cryptography [201], code-based cryptography [196], lattice-based cryptography [126], multivariate cryptography [227], supersingular elliptic curve isogeny cryptography [165], and secret-key (symmetric) cryptography. From these six candidates not all are suitable (yet) for post-quantum secure travel documents. On the one hand, symmetric cryptography alone cannot provide efficient key-exchange mechanisms (see Merkle Puzzles [6]) and on the other hand, supersingular elliptic curve isogeny cryptography does provide a key exchange [165], but is a very new proposal without sufficient empirical research to currently recommend it for a high security domain like electronic travel documents. From the remaining four classes hash-based cryptography and code-based cryptography are the oldest and best researched candidates, which is backed up by the scientific community:

"Merkle's hash-tree public-key signature system and McEliece's hidden-Goppa code public-key encryption system were both proposed thirty years ago and remain essentially unscathed despite extensive cryptanalytic efforts." [17]

Furthermore, initial results of the PQCrypto Horizon 2020 EU project [233] recommend post-quantum cryptography variants that are based on code-based cryptography and hash-based cryptography for long-term security. Therefore, further discussion will first focus on hash-based cryptography and also take code-based cryptography into account.

## 9.1. Hash-based cryptography

Hash-based post-quantum cryptography focuses on digital signature schemes built from cryptographic hash functions. Hash-based digital signature schemes for creating many time signatures with only one key pair are constructed from either one-time signature schemes or few time signature schemes. Therefore, these schemes will be discussed first. The initial scheme descriptions are inspired by [17].

### 9.1.1. Lamport-Diffie one-time signature scheme

The Lamport-Diffie one-time signature scheme (LD-OTS) is one of the oldest purely hash-based signature schemes, which solely relies on the collision resistance of the underlying hash function used in the signature scheme. It was first introduced by Leslie Lamport and Whitfield Diffie in [178] and later extended by Ralph Merkle and Robert Winternitz in [202].

#### LD-OTS domain parameters

The LD-OTS requires a one-way function:

$$f : \{0,1\}^n \rightarrow \{0,1\}^n$$

where n is the security parameter of the signature scheme and a collision resistant cryptographic hash function:

$$g : \{0,1\}^* \rightarrow \{0,1\}^n$$

which maps the input document $M$ to length n.

### LD-OTS key generation

The LD-OTS key pair comprises a private key $X$, which consists of $2n$ bit strings of length $n$ that are chosen uniformly a random by the signer. So $X$ can be seen as a two-dimensional vector that yields $\{0,1\} \times n$ bit strings of length $n$.

$$X = (x_{n-1}[0], x_{n-1}[1], x_{n-2}[0], x_{n-2}[1], \ldots, x_1[0], x_1[1], x_0[0], x_0[1]) \in_R \{0,1\}^{(n,2n)}$$

The second part of the LD-OTS key pair is the public key $Y$, which also consists of $2n$ bit strings of length $n$. The values of $Y$ are calculated with the private key $X$ and the one way function $f$ accordingly:

$$\begin{aligned} Y &= (y_{n-1}[0], y_{n-1}[1], y_{n-2}[0], y_{n-2}[1], \ldots, y_1[0], y_1[1], y_0[0], y_0[1]) \\ &= (f(x_{n-1}[0]), f(x_{n-1}[1]), f(x_{n-2}[0]), f(x_{n-2}[1]), \ldots, f(x_1[0]), f(x_1[1]), f(x_0[0]), f(x_0[1])) \end{aligned}$$

### LD-OTS signature creation

The signature for an arbitrary document $M$ is created by first computing the digest $d$ with the hash function $g$:

$$g(M) = d = (d_{n-1}, \ldots, d_0)$$

After the digest creation the actual digital signature $\sigma$ is created from the digest $d$ of the document $M$ by selecting the corresponding fields of the private vector $X$, with $d$ as the index parameter:

$$\sigma = (x_{n-1}[d_{n-1}], x_{n-2}[d_{n-2}], \ldots, x_1[d_1], x_0[d_0]) \in \{0,1\}^{(n,n)}$$

The signature $\sigma$ therefore consists of $n$, $n$-bit strings and has length $n^2$. For position $i$ of the signature $\sigma$, the $i$-th bit of $d$ determines for 0 select $x_i[0]$ and for 1 $x_i[1]$ is chosen.

### LD-OTS signature verification

The verification of signature $\sigma$ through the verifier requires $Y$ and can be performed by first calculating the message digest $d$ with the hash function $g(M) = d = (d_{n-1}, \ldots, d_0)$ of document $M$ and subsequently verify if:

$$(f(\sigma_{n-1}), \ldots, f(\sigma_0)) = (y_{n-1}[d_{n-1}], \ldots., y_0[d_0])$$

If the condition holds for positions 0 to $n-1$ of signature $\sigma$ the signature is considered valid.

The key pair $X$ and $Y$ must only be used for the creation of one single signature $\sigma$, because if the key pair is used for a second signature $\sigma'$, an existential forgery for a third signature $\sigma''$ is trivial (see [17] for details).

### 9.1.2. Winternitz one-time signature scheme

The extension of the Lamport-Diffie one-time signature scheme from Robert Winternitz is commonly referred to as Winternitz one-time signature scheme (W-OTS) or Winternitz style signature scheme. The W-OTS is a generalisation of the LD-OTS and was first mentioned by Ralph Merkle in [202]. Merkle states that he received the idea by Robert Winternitz and the scheme is described in detail in [17, 78]. One of the main shortcomings of the LD-OTS is that the created signatures are rather big. While the LD-OTS only signs one bit per digest, the basic idea of the W-OTS is to sign multiple bits per digest, resulting in shorter signatures. To maintain the same security level as the LD-OTS more computations of the one-way function $f$ are necessary to securely sign multiple bits at once. The W-OTS therefore has a time-memory trade-off parameter, which controls the size of the created signatures in relation to the computation time for signature creation and verification. This parameter is referred to as the Winternitz parameter $w$.

#### W-OTS domain parameters

The W-OTS requires the same domain parameters as the LD-OTS. A one way-function:

$$f : \{0,1\}^n \rightarrow \{0,1\}^n$$

where n is the security parameter of the signature scheme and a collision resistant cryptographic hash function:

$$g : \{0,1\}^* \rightarrow \{0,1\}^n$$

which maps the input document $M$ to length n.

#### W-OTS key generation

The number of concurrent bits signed is controlled by the Winternitz parameter $w \geq 2$, which must be selected during key generation. $t_1$, $t_2$ and $t$ shall be computed to reflect signature size and checksum size.

$$t_1 = \left\lceil \frac{n}{w} \right\rceil, t_2 = \left\lceil \frac{\lfloor \log_2 t_1 \rfloor + 1 + w}{w} \right\rceil, t = t_1 + t_2$$

The private key $X$ consists of $t$ bit strings of length $n$ that are chosen uniformly at random by the signer and similar to the LD-OTS $X$ it can be seen as a two-dimensional vector.

$$X = (x_{t-1}, \ldots, x_1, x_0) \in_R \{0,1\}^{(n,t)}$$

The second part of the W-OTS key pair is the public key $Y$, which also consists of $t$ bit strings of length $n$. The values of $Y$ are calculated with the private key $X$ and the one way function $f$ by applying it $2^w - 1$ times to each bit string:

$$\begin{aligned} Y =& (y_{t-1}, \ldots, y_1, y_0) \\ =& (f^{2^w-1}(x_{t-1}), \ldots, f^{2^w-1}(x_1), f^{2^w-1}(x_0)) \end{aligned}$$

### W-OTS signature creation

The signature for an arbitrary document $M$ is created by first computing the digest $d$ with the hash function $g(M) = d = (d_{n-1}, \ldots, d_0)$. After the digest creation the digest $d$ is prepended with the minimum number of zeros, so it is dividable by $w$. The extended $d$ is split into $t_1$ blocks $b_{t-1}, \ldots, b_{t-t_1}$ of length $w$.

$$d = b_{t-1} \| \ldots \| b_{t-t_1}$$

These blocks are used to compute the checksum $c$ as follows:

$$c = \sum_{i=t-t_1}^{t-1} (2^w - b_i)$$

The resulting checksum $c$ is prepended by the minimum number of zeros until it is dividable by $w$ and afterwards split into $t_2$ blocks $b_{t_2-1}, \ldots, b_0$ of length $w$.

$$c = b_{t_2-1} \| \ldots \| b_0$$

The signature $\sigma$ of $M$ is computed by following term:

$$\sigma = \left( f^{b_{t-1}}(x_{t-1}), \ldots, f^{b_1}(x_1), f^{b_0}(x_0) \right)$$

The resulting W-OTS signature has size $t \cdot n$.

### W-OTS signature verification

The verification of signature $\sigma$ through the verifier requires $Y$ and computation of the blocks $b_{t-1}, \ldots, b_0$ as described in the signature creation. For signature verification, the verifier checks if:

$$\left( f^{2^w-1-b_{t-1}}(\sigma_{n-1}), \ldots, f^{2^w-1-b_0}(\sigma_0) \right) = (y_{n-1}, \ldots, y_0)$$

In case of a valid signature $\sigma_i = f^{b_i}(x_i)$ and therefore

$$f^{2^w-1-b_i}(\sigma_i) = f^{2^w-1}(x_i) = y_i$$

holds for all blocks $t-1,\ldots,0$.

### 9.1.3. Merkle signature scheme

One of the main drawbacks regarding one-time signature schemes is that every key pair can only be used once, because multiple use of the same key pair results in an existential forgery attack. This is not feasible in practice since on the one hand, a new key pair has to be generated every time a signature is needed and on the other hand, a public key has to be transferred to all verifiers in an authentic manner. The Merkle signature scheme (MSS), invented by Ralph Merkle [202], proposes a solution to this problem, which is described in detail in [17]. With a single transferred public key multiple signatures can be verified in the MSS. In contrast to RSA or ECDSA the MSS has a fixed number of signatures it can create and verify. The basic idea is to store the fixed number of one-time keys in a binary hash tree and ensure their validity via the tree's root, the public key of the MSS.

#### MSS domain parameters

The MSS requires a cryptographic hash function
$g : \{0,1\}^* \rightarrow \{0,1\}^n$ and a one-time signature scheme (e.g., LD-OTS or W-OTS) with its own specific domain parameters.

#### MSS key generation

For key generation a parameter $H \in \mathbb{N}, H \geq 2$, has to be selected, which reflects the height of the tree and therefore the number of signatures that can be processed. The global key pair of the MSS can sign and verify $2^H$ documents. A signer has to create $2^H$ one-time key pairs for the selected OTS, these are referred to as $(X_j, Y_j), 0 \leq j < 2^H$, while $X_j$ denotes a private key (signature key) and $Y_j$ a public key (verification key) of the OTS. Hash values of the OTS public keys $g(Y_j), 0 \leq j < 2^H$, form the leaves of the Merkle tree. All other nodes of the tree are computed by concatenating its left and right children nodes and computing the hash value $g(node_L \| node_R)$ of the concatenated bit string. The public key of the MSS is the root of the Merkle tree and the MSS private key is the sequence of all $2^H$ signature keys. A sample Merkle tree is depicted in figure 9.1.

#### MSS signature creation

Signature creation is performed by executing the steps of the selected OTS and using one of the one-time private (signature) keys $X_s, s \in \{0,\ldots,2^H-1\}$ generated during the Merkle tree setup, resulting in signature $\sigma_{OTS}$. The MSS signature contains the $\sigma_{OTS}$ one-time signature, the corresponding one-time public key $Y_s$, the index $s$ of the used key and an authentication path, which is a sequence $A_s = (a_0,\ldots,a_{H-1})$ of nodes in the Merkle tree. The index $s$ and the authentication path nodes $A_s$ enable the verifier to create a path from the leaf OTS key to the root of the Merkle tree. Computation of such an authentication path is depicted in figure 9.2.

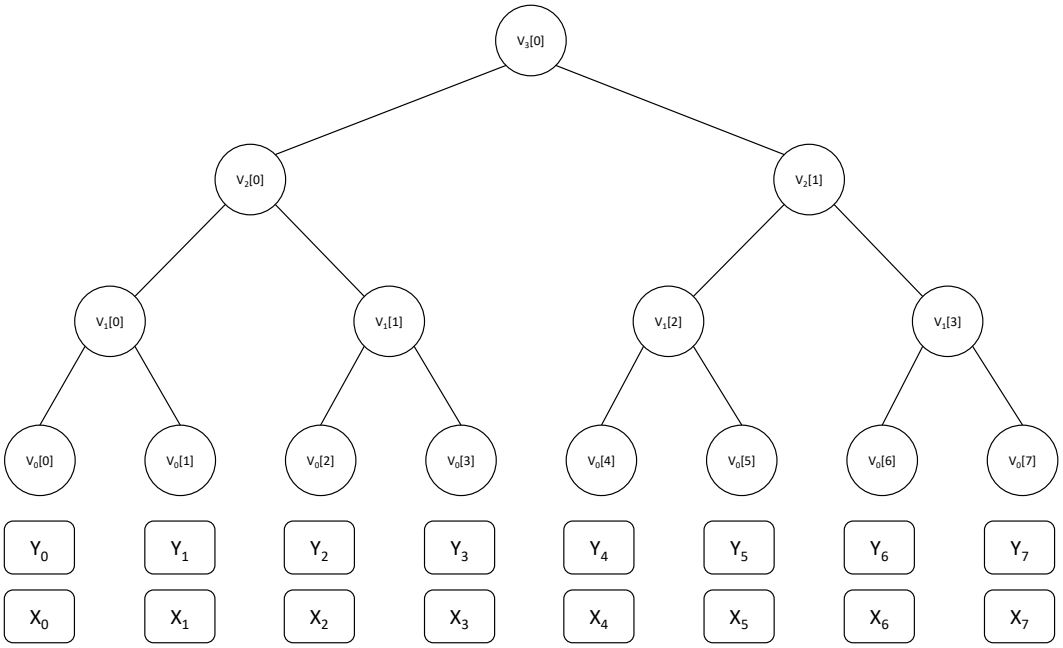



Figure 9.1.: A Merkle tree of height $H = 3$ [17].

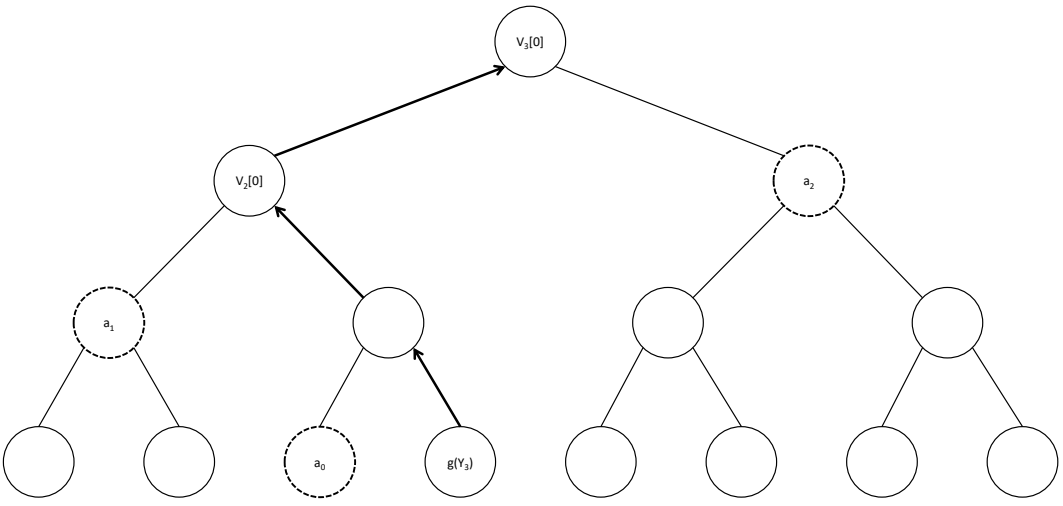



Figure 9.2.: Merkle authentication path for leaf $g(Y_3)$ [17].

#### MSS signature verification

MSS signature verification consists of two distinct steps. First, the selected OTS with the one-time verification key $Y_s$ as parameter shall be performed to verify the signature $\sigma_{OTS}$, as described for LD-OTS or W-OTS. The second step validates the authenticity of the utilised public key $Y_s$ constructing the path $(p_0, \ldots, p_H)$ from the selected leaf node to the root via the embedded authentication path $A_s$ and index $s$ of the MSS signature. Verification of the one-time public key $Y_S$ is considered successful if and only if the computed root $p_H$ equals the prior transferred MSS public key (Merkle root).

### 9.1.4. MSS generation using a PRNG

One of the biggest achievements of MSS compared to an OTS is the reduction of the public keys size to a practical capacity. In contrast, the private key for MSS consists of $2^N$ one-time signature keys and it is still unmanageable to store for a large $N$. [38] and [17] propose to save space by generating the one-time signature keys using a deterministic pseudo random number generator (PRNG) on demand and store only the seed of the PRNG as private key. For Merkle tree root (MSS public key) generation all one-time signature keys have to be generated once and later on during signing consecutively a single one-time signature key is generated. Since the MSS has to remember the current seed of the PRNG, the private key is updated after every signature generation with the new seed. MSS with a PRNG therefore is a key-evolving signature scheme as defined in [10].

#### MSS-PRNG domain parameters

The domain parameters are similar to the MSS, but additionally a cryptographically secure PRNG is needed that takes a seed $SEED_{in}$ as parameter and produces a random number $RAND$ as one-time key as well as an updated seed $SEED_{out}$ for storage in the private key.

$$\begin{aligned} \mathsf{PRNG} : \{0,1\}^n &\rightarrow \{0,1\}^n \times \{0,1\}^n \\ \mathsf{SEED_{in}} &\mapsto (\mathsf{RAND}, \mathsf{SEED_{out}}) \end{aligned}$$

#### MSS-PRNG key pair generation

The first seed of the PRNG $SEED_0$ has to be chosen uniformly at random. The sequence of one-time signature key seeds is referred to as $\mathsf{SEED_{OTS_j}}, 0 \leq j < 2^H$ and they are sequentially computed as such:

$$(\mathsf{SEED_{OTS_j}}, \mathsf{SEED_{j+1}}) = \mathsf{PRNG}(\mathsf{SEED_j}), 0 \leq j < 2^H$$

To generate private key $X_j$ only knowledge of $SEED_j$ is required, which is the current private key.

#### MSS-PRNG signature generation and verification

Signature creation for MSS-PRNG is equal to MSS besides the retrieval of the one-time signature key $X_j$ which has to be generated by the PRNG instead of obtained from memory. Signature verification is the same as specified for MSS.

### 9.1.5. MSS tree chaining

On the one hand, usage of a PRNG can drastically reduce the storage requirements for the MSS, but on the other hand, for MSS public key computation the complete Merkle tree still has to be computed once, to retrieve the MSS root. This process has to be done only once, but is very time-consuming and slows down the key pair generation. In [38, 17] Buchmann *et al.* propose to chain multiple smaller Merkle trees to solve this issue. The authors refer to this method as tree chaining and therefore the proposed system is referred to as chaining Merkle signature scheme (CMSS). The basic idea is that if multiple smaller trees are chained only the root of the top tree has to be computed during key setup for publishing the public key. All further tree computations can be divided to the signature generation calls. Therefore, CMSS speeds up the key setup drastically, but slows down the individual signature generation calls a little in contrast to pure MSS. In CMSS the number of trees is variable, but must be specified during key setup and is set as $T \geq 2$ for the tree layers. The individual trees are generated using a PRNG as described before. The root of the top layer 1 tree is the CMSS public key and the leaves of the bottom layer $T$ are the private keys to sign documents. All other leaf keys of the intermediate layers, $i, 1 \leq i < T$ sign the intermediate roots of trees on layer $i + 1$. Therefore, the CMSS signature consists of multiple MSS signatures, which is shown in equation 9.1.

$$\begin{aligned} \sigma = (s, & SIG_T, Y_T, AUTH_T \\ & SIG_{T-1}, Y_{T-1}, AUTH_{T-1} \\ & \vdots \\ & SIG_1, Y_1, AUTH_1) \end{aligned} \tag{9.1}$$

In equation 9.1 $SIG_T$ is the signature of the signed document, $Y_T$ the public key and $AUTH_T$ the authentication path, which enables the verifier to construct an authentication path from the public key $Y_T$ to the root of the bottom layer tree. Roots of the intermediate layer trees are not known by the verifier, which is solved by including signature $SIG_{T-1}$ up to $SIG_1$ in signature $\sigma$ to verify authenticity of the intermediate tree roots. All intermediate layer signatures also include an authentication path $AUTH_{T-x}$ as well as the corresponding public key $Y_{T-x}$.

Similar to MSS, CMSS can sign and verify $2^H$ documents where $H$ is the sum of individual tree levels: $H = H_1 + H_2 + \ldots + H_T$. For construction of the CMSS public key only the top layer tree must be computed with height $H1$, which is much faster

compared to MSS, which needs to construct a tree with height $H$. A CMSS sample tree is depicted in figure 9.3.

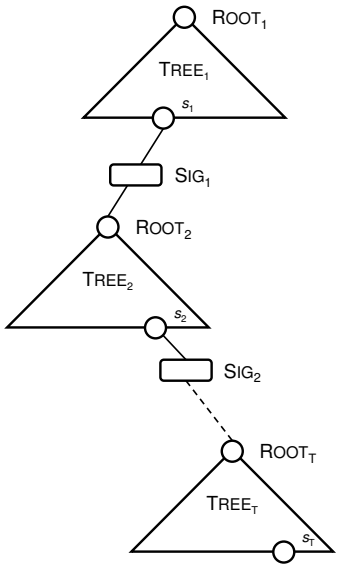



Figure 9.3.: The tree chaining method [17].

### Domain parameters

CMSS inherits the domain parameters from MSS as well as requiring a secure PRNG. The number of layers $T$ as well as the individual tree heights on layer $i$ i.e., $H_i, 1 \leq i \leq T$ must be specified.

### Key pair generation

One initial tree $TREE_i$ is generated for the individual layers. The CMSS public key is the root of the top tree $TREE_1$ and the secret key is the array of seeds used to construct the $T$ trees. Additionally, the one-time signatures of all generated roots are stored by the signer, which are generated with the respective signature on the next level.

### Signature generation

During signature generation, the signer already knows the current $TREE_i$ for each layer and the corresponding seeds $SEED_i$ to generate signature keys (private keys) for $i = 1, 2, \ldots, T$. The signature is generated as specified in section 9.1.4 for the document to be signed, the updated intermediate root signatures and the updated authentication path for the utilised one-time key index. In contrast to MSS, CMSS consists of $T$ MSS signatures and therefore results in signatures bigger by factor $T$. Computation of roots for subsequent intermediate trees as well as their signatures increases signature

generation time in comparison to common MSS. For further details regarding efficient authentication path creation and tree generation refer to [38, 17].

#### Signature verification

The signature $\sigma$ is verified by iteratively verifying the individual signatures $SIG_T$ to $SIG_1$. On the one hand, the public key $Y_T$ is utilised to verify $SIG_T$ and on the other hand, $Y_T$ is needed in combination with the authentication path $AUTH_T$ to construct the root of tree $T$. Root $T$'s signature is $SIG_{T-1}$ (see figure 9.3), which can be verified utilising $Y_{T-1}$. These steps are iteratively repeated until the root of layer 1 is produced, which must be equal to the CMSS public key, which was transferred beforehand. Only if all comparisons succeed $\sigma$ is considered valid, if any comparison fails the entire signature $\sigma$ is rejected.

### 9.1.6. Distributed signature generation

The idea of distributed signature generation was first introduced in [36] and is described in detail in [17]. CMSS introduces a significant speed-up in public key generation, but enlarges the signature size and slows down signature generation. The tree chaining of CMSS in combination with distributed signature generation is referred to as generalised Merkle signature scheme (GMSS) [36] and aims at improving upon the shortcomings of CMSS. GMSS's fundamental idea originates from the observation that root signatures and authentication paths in upper layer trees only change occasionally. As discussed in section 9.1.2 the Winternitz parameter $w$ controls the ratio between signature size and signature generation time. On the one hand, due to the mentioned observation higher layer trees shall use a big $w$ parameter, resulting in smaller overall signatures. On the other hand, GMSS proposes to distribute the operations for root signature creation and authentication path computation evenly across all document signature creations, which improves the worst case signature generation time in contrast to CMSS. GMSS introduces the notation for each tree layer $i \geq 2$, that $\text{TREE}_i$ is the currently active tree, the preceding tree on the same layer $\text{TREEPREV}_i$ and the future tree $\text{TREENEXT}_i$. Distributed signature generation ensures that when $\text{TREE}_i$ becomes the active signing tree, the root of $\text{TREENEXT}_i$ is already known, so the root can be signed while $\text{TREE}_i$ is used for signing. The root of $\text{TREENEXT}_i$ is computed while $\text{TREEPREV}_i$ was active.

#### Distributed root signing

Signature generation for the root of $\text{TREENEXT}_i$ is distributed across the leaves of $\text{TREE}_i$. If the first leave of $\text{TREE}_i$ is utilised the number of hash function evaluations and calls to the PRNG to generate a Winternitz signature is computed. These numbers are divided by the number of $\text{TREE}_i$ leaves to retrieve the amount of operations required per signing call. This distributed one-time signing is depicted in figure 9.4.

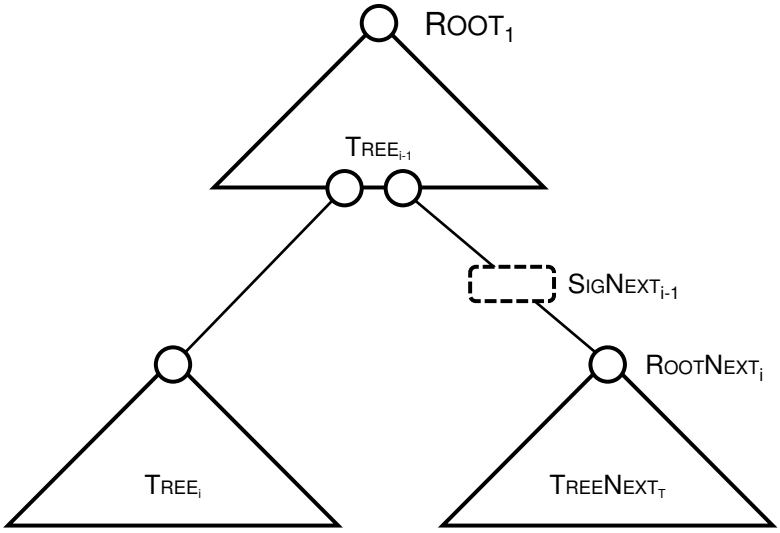



Figure 9.4.: Distributed generation of TREENEXT$_i$ root signature SIGNEXT$_{i-1}$ [17].

### Distributed root computation

Before signature creation of the TREENEXT$_i$ root ROOTNEXT$_i$, the root itself must be calculated. The computation is performed while TREEPREV$_i$ is active and since TREEPREV$_i$ and TREENEXT$_i$ have the same amount of leaves, a TREENEXT$_i$ leaf LEAF$_j$ is calculated when a TREEPREV$_i$ leaf LEAF$_j$ is used. If TREENEXT$_i$ is not the lowest tree, i.e., $i < T$ computation of the TREENEXT$_i$ leaves can be further distributed. Similar to the distributed root signing the number of hash function evaluations and calls to the PRNG must be determined and divided by the number of leaves of the tree below TREEPREV$_{i+1}$ to determine the number of computations per leaf. Thereby if TREENEXT$_i$ becomes TREE$_i$ the root is fully computed, which is depicted in figure 9.5.

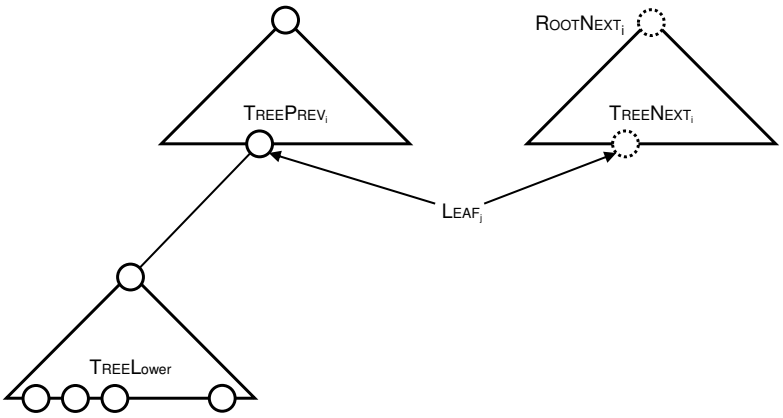



Figure 9.5.: Distributed computation of ROOTNEXT$_i$. LEAF$_j$ of of TREENEXT$_i$ is computed in TREELOWER while LEAF$_j$ of of TREEPREV$_i$ is used [17].

### Distributed authentication path computation

Distributed authentication path computation aims at computing the authentication path of the next leaf of the $\text{TREE}_i$ tree. Similar to distributed root computation the number of hash function evaluations and calls to the PRNG must be determined and divided by the number of leaves of the lower tree TREELOWER to determine the number of computations per leaf. So the computation of the authentication path is split between the $2^{H_{i+1}}$ leaves of the lower $\text{TREE}_{i+1}$. This process is depicted in figure 9.6 and for further details refer to [17].

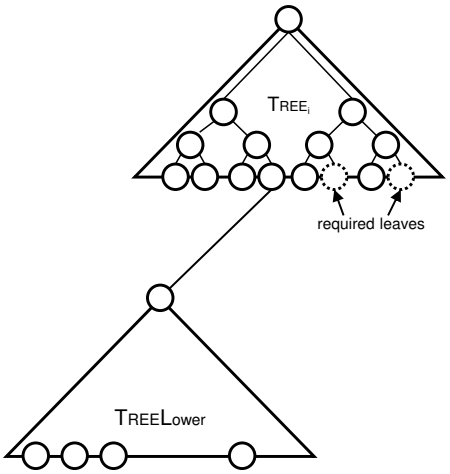



Figure 9.6.: Distributed authentication path computation computes the required leaves while TREELOWER is in use [17].

### GMSS key pair generation and domain parameters

The GMSS domain parameters are very similar to those of CMSS: $T$ specifies the number of trees (i.e., layers), the heights $H_1, \ldots, H_T$ has to be specified for all Merkle trees, and the Winternitz parameters $w_1, \ldots, w_T$ have to be selected. On the one hand, similar to CMSS the public key is the root $\text{ROOT}_1$ of the top layer tree i.e., $i = 1$. On the other hand, the GMSS private key consists of all values that define the current trees and their states, which are:

$$\begin{aligned}
&\text{SEED}_i, i = 1, \ldots, T, && \text{SEEDNEXT}_i, i = 2, \ldots, T \\
&\text{SIG}_i, i = 1, \ldots, T-1, && \text{ROOTNEXT}_i, i = 2, \ldots, T \\
&\text{AUTH}_i, i = 1, \ldots, T, && \text{AUTHNEXT}_i, i = 2, \ldots, T \\
&\text{STATE}_i, i = 1, \ldots, T, && \text{STATENEXT}_i, i = 2, \ldots, T
\end{aligned}$$

Most parameters have been introduced beforehand and for detailed descriptions of all components refer to [17].

#### GMSS signature generation/verification

GMSS signature generation consists of two parts. First, the document is signed similar to the described signature creation in CMSS. After the signature creation the distributed computation of the next roots, signatures of roots and authentication paths is performed as previously described. The full signature is depicted in equation 9.2.

$$\begin{aligned}\sigma = (s, & SIG_T, Y_T, AUTH_T \\ & SIG_{T-1}, Y_{T-1}, AUTH_{T-1} \\ & \vdots \\ & SIG_1, Y_1, AUTH_1)\end{aligned} \tag{9.2}$$

The main improvement of GMSS over CMSS is to distribute the signature generation, but the signature verification is equal to CMSS in GMSS.

### 9.1.7. eXtended Merkle Signature Scheme (XMSS)

The eXtended Merkle Signature Scheme (XMSS) was first described in [35], is based on GMSS but introduces new security improvements. On the one hand, the authors [35] of XMSS provide a formal security proof that XMSS is forward secure and existentially unforgeable under chosen message attacks. On the other hand, XMSS reduces the security requirements since it only requires a secure PRNG and a second preimage resistant function family. In contrast to prior introduced MSS improvements, the security of XMSS does not rely on collision resistance. Performance of XMSS is comparable to RSA for $H = 20$ to sign $2^{20}$ documents.

Removing the necessity for collision resistance is a big plus since even broken hash functions (e.g., MD5 and SHA1), which are not considered collision resistant for quite some time are still to this day second preimage resistant. Collision resistance for MD5 was first broken theoretically in 2004 [289] and later practically broken 2008 [268]. SHA1 suffered the same fate to be first theoretically broken in 2005 [288] and later even broken in practice 2017 [267]. Since MD5 and SHA1 are both Merkle-Damgård [200] constructions, they suffer from the widely known length extension attack [77] hence one practical collision leads to trivial computation of unlimited collision pairs by extending the found collision block pairs with the same blocks.

#### Domain parameters

The XMSS domain parameters as specified by the authors [35]:

- $n \in \mathbb{N}$, the security parameter,
- $w \in \mathbb{N}, w > 1$, the Winternitz parameter,

- $m \in \mathbb{N}$, the message length in bits,
- $F_n = \{f_K : \{0,1\}^n \to \{0,1\}^n | K \in \{0,1\}^n\}$ a function family,
- $H \in \mathbb{N}$, the tree height, XMSS allows to make $2^H$ signatures using one keypair,
- $h_K$, a hash function chosen randomly, with the uniform distribution from the family $\mathcal{H}_n = \{h_K : \{0,1\}^{2n} \to \{0,1\}^n | K \in \{0,1\}^n\}$,
- $x \in \{0,1\}^n$, chosen randomly with uniform distribution. The string $x$ is used to construct the one-time verification keys.

### XMSS improvements over GMSS

Second preimage resistance as sufficient requirement is achieved by two main changes to the (G)MSS. First the W-OTS is replaced by a slightly modified version, which was first proposed in [34] called W-OTS+. In contrast to W-OTS, which iteratively cascades (i.e., evaluates) a hash function resulting in an iterated walk through the function family, W-OTS+ performs a random walk through the function family. Everything else remains as specified in section 9.1.2. Since details of W-OTS+ are out of scope for the document at hand see [34] for more detailed information of W-OTS+. The second modification originates from Bellare and Rogaway [11], the idea being to replace necessity of a collision resistant hash function family with a second preimage resistant function family by utilising bitmasks. The resulting modification of the Merkle hash tree was first proposed in [67] and is depicted in figure 9.7.

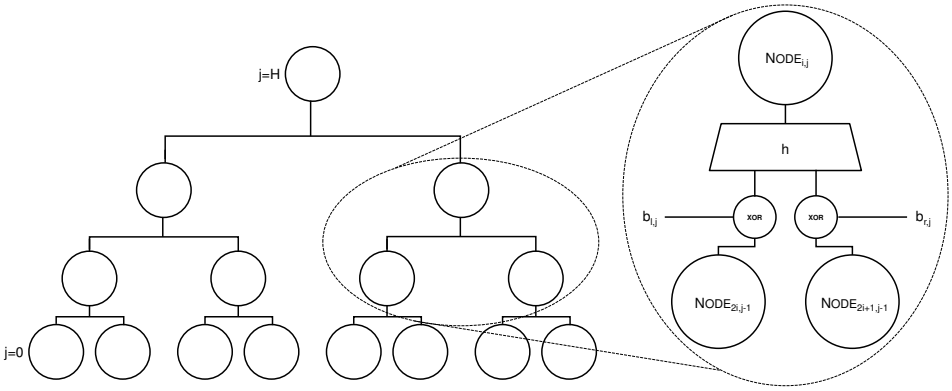



Figure 9.7.: The XMSS tree construction [35].

In common MSS any node is computed by concatenating and hashing its lower level nodes $\text{NODE}_{i,j} = h_K(\text{NODE}_{2i,j-1} \| \text{NODE}_{2i+1,j-1})$. In the XMSS tree a bitmask $(b_{l,j} \| b_{r,j}) \in \{0,1\}^{2n}$ is chosen uniformly at random for every node level $j, 0 \leq j \leq H$ and applied for node construction:

$$\text{NODE}_{i,j} = h_K((\text{NODE}_{2i,j-1} \oplus b_{l,j}) \| (\text{NODE}_{2i+1,j-1} \oplus b_{r,j})) \tag{9.3}$$

For more detailed information refer to [67, 35]. The $H$ bitmasks are stored together with the XMSS tree root in the public key.

Signature generation and signature verification are similar to GMSS.

#### XMSS standardisation as XMSS$^{MT}$ and XMSS-T

XMSS has become IETF standard as RFC 8391 [128], which was particular pushed by the XMSS authors. The RFC is based on XMSS but extends on the improvements introduced with XMSS$^{MT}$ [130] and XMSS-T [132].

XMSS$^{MT}$ stands for XMSS Multi Tree, was introduced in [130] and improves key and signature generation times by applying the tree chaining from CMSS [38] to XMSS. Furthermore Huelsing *et al.* [130] model the XMSS parameter selection as a linear problem to make the parameter selection of hash-based signature schemes more practical. Hence, the Simplex algorithm [174] is used to retrieve a provable optimal solution for a given parameter set. Huelsing *et al.* utilise the IBM Cplex solver (i.e., an implementation of the Simplex algorithm) [134] to find provable best possible domain parameter solutions for $2^{20}$ and $2^{80}$ uses of a single key pair for signature creation. The relevant concrete sizes will be reviewed in the discussion.

XMSS-T is described in [132] and builds upon the XMSS variant described in the XMSS IETF RFC 8391. Main difference to XMSS$^{MT}$ is the resistance to multi target attacks and an estimation of the quantum security of XMSS-T. To achieve multi target resistance XMSS-T introduces a new W-OTS+ variant called W-OTS-T and a new construction mechanism for the Merkle hash tree. In words of Huelsing *et al.*: "The main difference in the construction of XMSS$^{MT}$ and XMSS-T is the use of independent function keys and bitmasks for every call to a hash function inside of the hash trees or W-OTS-T. XMSS$^{MT}$ used a single fixed key per function family and the same bitmask per internal tree level or chain position." [132]. Similar to MSS-PRNG the values are generated pseudo-randomly utilising a hash-based pseudo-random function family. This mechanism keeps the public key small, because only the seed value has to be stored in the public key and no actual bitmasks.

W-OTS-T is based on W-OTS+ [34], but utilises fresh keys and bitmasks for each function call. Similar to the XMSS-T tree construction these values are derived by a pseudo-random generation mechanism and only the seed value is added as secret key.

Another hash based signature scheme sometimes mentioned in the context of XMSS$^{MT}$ is the Leighton Micali Signature (LMS) scheme [181] currently standardised by McGrew *et al.* [198]. Kampanakis and Fluhrer [170] compare XMSS$^{MT}$ and LMS, and conclude that XMSS$^{MT}$ has been proven in a tighter security model and provides smaller signature sizes. Therefore, LMS is not further discussed in detail is this work (see [55] LMS).

### 9.1.8. SPHINCS a stateless hash-based signature scheme

The paper SPHINCS: practical stateless hash-based signatures [19] by Bernstein *et al.* introduces the first practical stateless hash-based signature scheme. It is based on the XMSS ideas [35, 130] and the work by Goldreich [110], who proposed theoretical schemes

for stateless hash-based signatures. Similar to XMSS, SPHINCS provides a general construction with flexible parameters for different use cases, but the authors of SPHINCS also introduce a specific instantiation named SPHINCS-256. SPHINCS-256's parameter selection has two main goals. On the one hand, it shall provide $2^{128}$ long-term security against an attacker with a large-scale quantum computer. On the other hand, the authors seek a trade-off between speed and signature size. The security parameter $n = 256$ defines the name SPHINCS-256. Goldreich [110] proposed the idea of randomised leaf selection, which makes the signature scheme stateless, but it becomes insecure if the same leaf is selected twice. A sample MSS tree with 128 layers yields a probability of roughly $2^{-30}$ of leaf reuse. So the scheme gets presumably broken after $2^{50}$ signatures without a new key setup. SPHINCS-256 reuses this $2^{50}$ signatures threshold, but introduces new constructions to reduce the overall signature size, key sizes and computation time.

#### Few Time Signature Schemes

The first big change to the default XMSS system to increase the security for randomised index selection is to replace the hash-based OTS with a few-time signature scheme (FTS). The FTS is designed that a few index collisions are acceptable. In the case of SPHINCS-256, $2^9$ index collisions are compensated by the FTS. The big benefit of the FTS over the OTS is that the tree size can be reduced drastically while maintaining the same security level. For SPHINCS-256 the tree height is reduced from 256 to 60, while maintaining a $2^{128}$ security level. SPHINCS uses HORS [251] a few time signature with a tree modification called HORS with trees (HORST), which increases the runtime but reduces the public key size. The HORS tree stores the few time public keys in a binary hash tree similar to a Merkle tree and only publishes the root as long-term public key, for further details refer to [19].

#### Fast fixed size hashing

Previous XMSS designs either use cryptographic hash functions from the SHA-2 family or the block cipher AES to construct second preimage resistant function families. AES in particular is often chosen (see [35]) since it is implemented in hardware by modern CPUs resulting in much higher throughput than SHA-2. The authors of SPHINCS note that for example SHA-3 [22] is designed to have good performance for long inputs. In contrast most computations in the hash trees only compress $2n$ bit to $n$ bit, i.e., $H : \{0,1\}^{2n} \rightarrow \{0,1\}^n$. Bernstein *et al.* propose a faster design specifically for this use case, i.e., short-input performance based on ChaCha20 and Blake, which provides a speed-up over older designs. For further details refer to [19].

## 9.2. Code-based cryptography

The previous section 9.1 discussed hash-based cryptography and its ability to provide post-quantum resistant digital signatures for long-term security. Unfortunately, digital signatures are the sole forte of hash-based cryptography and more cryptographic

primitives are needed for security protocols, which as of this day hash-based cryptography cannot provide. Specifically post-quantum resistant public key encryption and key exchange are required to enhance current eMRTD security protocols.

Code-based cryptography has been similarly long in research as hash-based cryptography, but can provide multiple cryptographic primitives like key exchange and public key encryption. The roots of code-based cryptography originate in coding theory, which focuses on the design of error correcting codes to reliably transfer data over a faulty channel. A classic example is the communication from earth to outer space with a Mars rover or a space probe that have a transmission delay of multiple days and retransmission is not suitable or even possible. The problems in coding theory are being discussed since at least the 70s and are well understood formally [15]. This section first presents and discusses the classic McEliece scheme [196] and its variant the Niederreiter scheme [217] in the context of public key encryption and key exchange. Initial scheme descriptions are inspired by [17, 261].

Robert McEliece proposed parameters for the scheme to yield 64 bits of security and today roughly 60 bits [21] of security remain with state-of-the-art attacks, which can easily be compensated with adjusted parameters. In contrast to RSA and DSA the security level of the McEliece scheme has not changed much in nearly 40 years and the underlying problems remain of exponential complexity [16] and are not solvable subexponential as RSA and its factoring problem or DSA and its discrete logarithm problem [49, 62]. In context of post-quantum security the underlying coding theory problem of syndrome decoding [15] seems to be non-reducible to the Hidden Subgroup Problem (HSP), therefore Shor's algorithm is not applicable to code-based cryptography [17]. Grover's search algorithm has impact on code-based cryptography, but the exact impact is still open to research. However, the most recent assumption is that it cannot reduce the underlying bit security in more than half [16]. So parameters that provide 263 bits security in the McEliece scheme, can be reduced by Grover's algorithm below 263 bits, but remain above 131 bits security.

The main reason why the McEliece scheme or Niederreiter scheme have not found adaption in practice are the rather large key sizes. While RSA and DSA have key sizes of multiple 1000 bits, code-based schemes need key sizes of multiple kilobytes or even megabytes for adequate security levels. McEliece based the scheme on the work by Goppa [112] and the so-called Goppa codes, which remain secure today. Since in coding theory multiple efficient code types have been found, numerous code types were adapted to the McEliece scheme, to get more structure in the keys and therefore reduce their size. This includes Reed-Solomon codes [217], Concatenated codes [217], Reed-Muller codes [188], Algebraic-Geometry codes [164], Low-Density-Parity-Check-Codes [207], Convolutional codes [185], and so on. All these ideas have in common that they were broken a few years later [189, 259, 205, 65, 207, 179] and the McEliece scheme with Goppa codes remained as the only code-based secure alternative.

Recently a new type of codes for the McEliece scheme was introduced, the so-called quasicyclic moderate density parity check codes (QC-MDPC) [206]. The basic idea originates in lattice-based crypto schemes (e.g., NTRU [126], and Ring learning with errors (RLWE) [187]) to i.e., only store the first row of a matrix and further rows are

shifted permutations of the first row, which drastically reduces the key sizes. QC-MDPC codes are part of the discussion in this chapter since on the one hand, they are as of today the only alternative to Goppa codes with a security proof that remains valid and on the other hand, are already discussed as a candidate for long-term security by the PQCrypto EU project [234] and its initial recommendations [233].

The McEliece scheme has also been converted into a digital signature scheme by Courtois *et al.* [64], but since the parameters are very unattractive in comparison to hash-based digital signature schemes presented in section 9.1, these schemes are out of scope for this discussion.

### 9.2.1. McEliece scheme

The McEliece public-key encryption scheme was introduced by Robert McEliece in 1978 [196] (i.e., nearly 40 years ago), which follows the concept of using a linear error correcting code (i.e., Goppa code) and adding errors to it to receive the ciphertext. The generator matrix $G^{pub}$ represents the public key and the decoding algorithm $D_G$, matrix $S$, and permutation matrix $P$ form the secret key of the scheme. Without the secret key, the attacker has to solve the generic syndrome-decoding problem, which is considered hard [15] and remains hard for a quantum attacker [16]. The basic idea is depicted in figure 9.8.

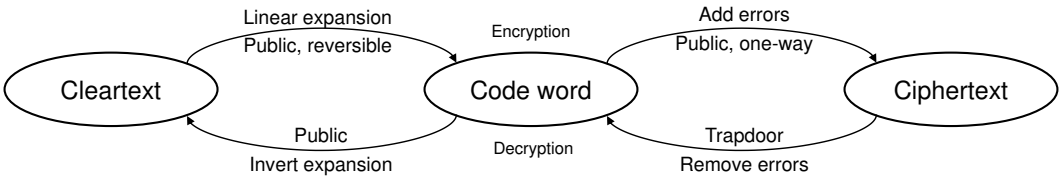



Figure 9.8.: The basic idea of code-based public-key encryption [261].

Subsequent paragraphs summarise the concrete McEliece scheme and are based on the more detailed description in [17].

#### Domain Parameters

$$n, t \in \mathbb{N}, t \ll n.$$

Where $n$ represents the basic security parameter and $t$ the number of errors introduced to the codeword.

#### Key Generation

$G : k \times n$, the generator matrix of dimension $k$.
$S : k \times k$, random binary non-singular matrix.
$P : n \times n$, random permutation matrix.

Compute the public-key: $G^{pub} = SGP$, thereby the full public key is set as $G^{pub}$ with $t$ and the secret key consists of $S$, $P$, and the decoding algorithm $D_G$.

#### Encryption and Decryption

The encryption function $E_{G^{pub},t}$ to encrypt a plaintext $m$, first chooses a random vector $z \in \mathbb{F}^k$ of hamming weight $t$ and secondly computes the ciphertext $c$ as:

$$c = mG^{pub} \oplus z.$$

The decryption function $D_{S,D_G,P}$ decrypts a ciphertext $c$ in multiple steps to receive the plaintext $m$:

$$\begin{aligned} cP^{-1} &= (mS)G \oplus zP^{-1} \\ mSG &= D_G(cP^{-1}) \\ m &= (mSG)(G)^{-1}(S)^{-1} \end{aligned}$$

#### Parameter selection for 128 bits security

For a common attacker the parameters $k = 3376, n = 4096, t = 60$ yield 128 bits security with a 303,840 bytes public key [261]. In case of a quantum attacker the parameters must be increased due to Grover's algorithm resulting in $k = 5413, n = 6960, t = 119$ and a 1,046,739 bytes public key for 128 bits post-quantum security [233].

### 9.2.2. Niederreiter scheme

The Niederreiter scheme proposed by Harald Niederreiter in 1986 [217] is a variant of the McEliece scheme, which was later shown to have equal security, i.e., if an attacker can break one of the schemes, the other scheme can be broken by the same attacker [184]. Instead of having the plaintext $m$ represented as a codeword, Niederreiter encodes the message into the error vector. For the encoding process a separated mapping function which converts binary strings into error vectors with constant hamming weight is required (see [99, 17] for sample functions).

Subsequent paragraphs summarise the concrete Niederreiter scheme and are based on the more detailed description in [17].

#### Domain Parameters

$$n, t \in \mathbb{N}, t \ll n.$$

The domain parameters are equal to the McEliece scheme.

### Key Generation

$$
\begin{aligned}
H &: (n-k) \times n, \text{ check matrix that can correct up to } t \text{ errors.} \\
S &: (n-k) \times (n-k), \text{ random binary non-singular matrix.} \\
P &: n \times n, \text{ random permutation matrix.}
\end{aligned}
$$

Compute the public-key: $H^{pub} = SHP$, and similar to the McEliece scheme $t$ is also part of the public key. The secret key consists of $S$, $P$, and the decoding algorithm $D_G$.

### Encryption and Decryption

The mapping function first converts a plaintext $m$ to an error vector $e \in \{0,1\}^n$ with hamming weight $t$ and the encryption function $E_{H^{pub},t}$ computes the ciphertext $s$ (i.e., syndrome) as such:

$$s = H^{pub} e^\top$$

The decryption function $D_{S,D_G,P}$ decrypts a ciphertext $s$ in multiple steps to receive the plaintext $m$:

$$
\begin{aligned}
S^{-1}s &= HPe^\top \\
D_G(HPe^\top) &= Pe^\top \\
e^\top &= P^{-1}Pe^\top.
\end{aligned}
$$

Finally $e$ has to be converted via the error vector mapping function to receive the plaintext $m$.

### Difference between McEliece and Niederreiter

On the one hand, an advantage of the Niederreiter scheme over the McEliece scheme is the reduced public-key size but on the other hand, the mapping function for constant hamming weight vectors slows down the encryption and decryption process. In practice both arguments are negligible since on the one hand, the McEliece Scheme's public-key $G$ matrix with $k \times n$ space can be converted into systematic form by Gaussian elimination [216], resulting in smaller $k \times (n-k)$ space requirement and marginal difference to the Niederreiter public-key. On the other hand, if the Niederreiter scheme is used for key establishment between two parties there is no need to decode $e$ via the mapping function since $e$ can be used directly as seed for a secure key derivation function, e.g., $k = h(e)$.

### 9.2.3. Block-circulant codes, QC-MDPC

McEliece's scheme and Niederreiter's scheme remain secure until this day, but have not found widespread use due to the unattractive public key sizes. Gaborit [105] first proposed a construction based on block-circulant matrices to significantly reduce public-key sizes. Later Sendrier [260] proved that the underlying security proof of code-based cryptography still holds with block-circulant matrices and the code-based cryptography community accepts, similar to the lattice-based cryptography community, that cyclic variants of the underlying problems remain hard if the code-family is chosen carefully [261]. The basic principle is depicted in figure 9.9, which exhibits the matrix consisting of multiple circulant blocks that are completely defined by its first row. Second row and all further rows rotate one element to the right of the proceeding row, and the index represents the number of circulant blocks per row in the block-circulant matrix. Since only the first row of each circulant block has to be stored, the public-key size drastically decreases.

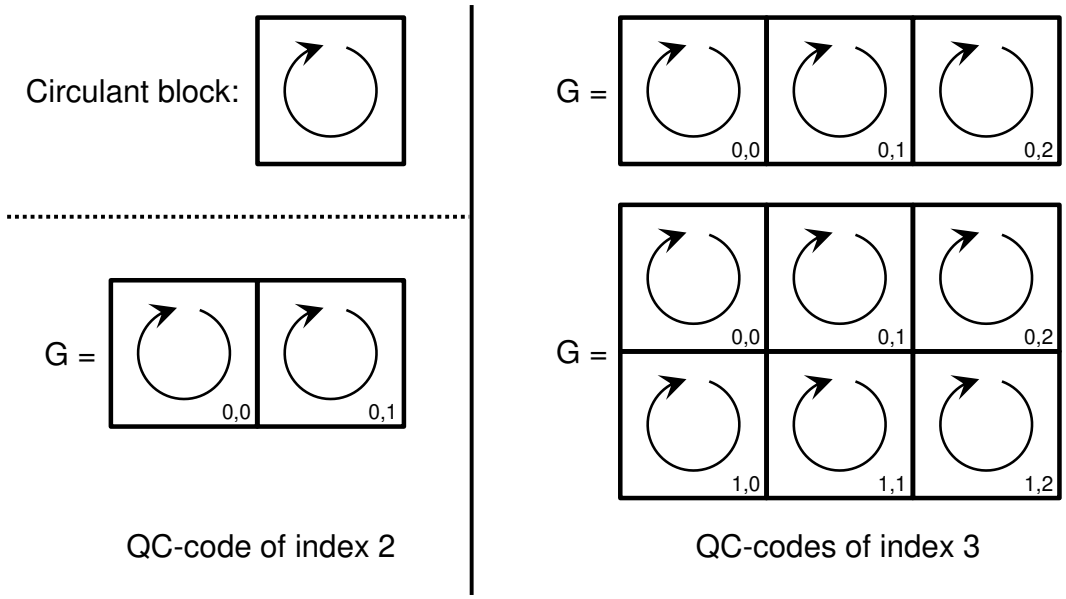



Figure 9.9.: The block-circulant matrices design [261].

#### Quasicyclic moderate density parity check codes (QC-MDPC)

One concrete code family proposal benefiting from block-circulant matrices is the quasicyclic moderate density parity check McEliece (QC-MDPC-McEliece) scheme by Misoczki *et al.* [206]. Using QC-MDPC codes with the McEliece scheme with index 2 for the block-circulant matrix, block size $p = 9857$, row weight $w = 142$, error count $t = 134$, and the resulting 1.2 kB public-key yield 128 bits security against a common attacker [261]. For the post-quantum era, the public-key grows to 4 kB in size, in contrast to

the roughly 1 MB public-key for the classical McEliece scheme with Goppa codes, to maintain 128 bits of security. QC-MDPC codes are already discussed as a candidate for long-term security by the EU PQ-Crypto project [233], but the status quo for security besides the classic Goppa codes was summarised by Tanja Lange during the PQCrypto 2016 winterschool with the following statement: "We are now in the area of exciting results, this is not what you want to use if your life depends on it, for that one use binary Goppa codes and deal with the key size, but we hope to be more confident soon." [180].

### QC-MDPC Key-Exchange

Since key-generation is simple for QC-MDPC-McEliece, Sendrier [261] proposed a key exchange protocol based on QC-MDPC codes. The protocol is depicted in figure 9.10 as sketch and is formally described by Barreto *et al.* [7] as the CAKE protocol (i.e., Code-based Algorithm for Key Encapsulation) in a SIGMA variant (see section 7.3.1) [81].

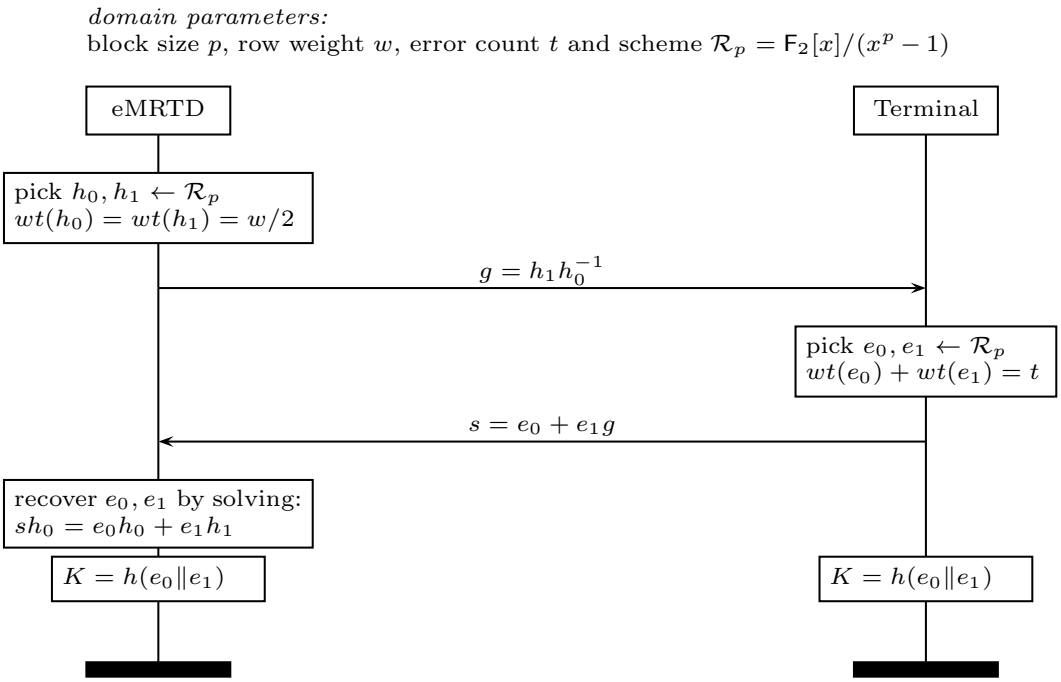



Figure 9.10.: The CAKE protocol sketch [7, 261].

## 9.3. Post-Quantum Cryptography Discussion

Since the impact of future quantum computer advances is hard to predict, upcoming eMRTD security protocols are expected to utilise cryptographic building blocks resisting quantum computer attacks introduced in this chapter. The cryptographic building blocks shall be split into three categories for discussion: symmetric building blocks (e.g.,

block ciphers, message authentication codes (MAC)), digital signatures based on hash-based cryptography, and public key cryptography (e.g., asymmetric encryption, and key exchange) based on code-based cryptography.

Symmetric building blocks used in eMRTD security protocols are twofold. On the one hand, block ciphers are utilised for confidentiality on the transport layer and on the other hand, MACs provide authenticity and integrity on the transport layer. Neither the standard block cipher (i.e., AES [94]) nor commonly used MACs (i.e., HMAC [96], and CMAC [80]) are impacted by Shor's algorithm. Therefore, only the post-quantum impact of Grover's algorithm has to be compensated [39]. Since Grover's algorithm can in the worst case reduce $\mathcal{O}(n)$ security to $\mathcal{O}(\sqrt{n})$ security, the numeric bit security has to be doubled. Hence, AES-128 has to be updated to AES-256 for block cipher and CMAC utilisation, and HMAC has to use a 256 bit cryptographic hash function (i.e., SHA-256). Consequently, the changes for symmetric post-quantum security are easy to deploy.

In contrast, digital signatures relying on hardness of the discrete logarithm problem or hardness of the factorisation problem have to be replaced, since they are susceptible to Shor's algorithm. eMRTD security protocols utilise digital signatures in two instances: On the one hand, Passive Authentication verifies a digital signature provided by the eMRTD on the inspection system. On the other hand, Active Authentication and Terminal Authentication rely on the processing of digital signatures on the eMRTD. Passive Authentication verifies the authenticity and integrity of the eMRTD data groups via a digital signature by verifying a digital signature created during document personalisation from the document signer, on the inspection system. Since the signature is only created once during the document's lifetime and the verification takes place on the inspection system, due to sufficient verification performance and uncritical creation time this use case is the most relaxed. In contrast, post-quantum digital signature processing on the eMRTD chip for Terminal Authentication and Active Authentication must be considered in detail due to the limited computation power of the eMRTD chip. Terminal Authentication proves the access rights of the inspection system to the eMRTD chip via verification of the Terminal certificate's digital signature on the eMRTD chip, which is harder since the chip has far less computation power than the inspection system. Nevertheless, the terminal certificate creation is performed in the back office and only the verification has to be performed on the eMRTD chip. Therefore, the most complex scenario is a post-quantum variant of Active Authentication, since it incorporates a digital signature for its challenge-response mechanism, which has to be created on the eMRTD chip and has to be different every time to prevent replay attacks.

As introduced in section 9.1, hash-based digital signature schemes are designed for a fixed number of signatures. For a travel document with 10 years validity, table 9.1 gives a worst-case approximation how many digital signatures can be created in this period.

Based on the results in table 9.1 a worst-case approximation of multiple uses a day but not every hour is reasonable for further discussion. Hence, a post-quantum secure digital signature scheme must be able to produce roughly $2^{12} - 2^{17}$ signatures in a 10 year period. Table 9.2 summarises the maximum signature count with the proposed sample parameters per scheme and table 9.3 presents implementations on special pur-

Table 9.1.: Number of digital signatures in a 10 year validity period of eMRTD uses.

| Granularity | Signatures |
|---|---|
| Once per week | $\approx 2^9$ |
| Once per day | $\approx 2^{12}$ |
| Once per hour | $\approx 2^{17}$ |
| Once per minute | $\approx 2^{23}$ |
| Once per second | $\approx 2^{29}$ |

Table 9.2.: Overview of hash-based digital signature schemes and their tested parameters.

| Scheme | Max Signatures | Reference |
|---|---|---|
| CMSS | $2^{40}$ | [38] |
| GMSS | $2^{80}$ | [36] |
| XMSS | $2^{20}$ | [35] |
| XMSS$^{MT}$ | $2^{80}$ | [130] |
| XMSS-T | $2^{60}$ | [132] |
| SPHINCS | (soft max) $2^{50}$ | [19] |

pose hardware, their applied scheme and the resulting maximum signature count. All schemes summarised in table 9.2 fulfil this requirement with proposed parameters of the respective authors, however all schemes were evaluated on powerful PCs, which even in the near future are not comparable to an embedded ePassport RFID chip in terms of computation power. Therefore, table 9.3 presents results for hash-based digital signature schemes implemented on low-end hardware. Fortunately, all listed special purpose implementations also fulfil the required signature count for a 10 year valid eMRTD.

Since the introduced schemes by the scientific community continuously integrate the improvements of former designs, only two schemes are candidates for future eMRTDs, namely XMSS-T and SPHINCS. On the one hand, XMSS-T combines all improvements of former hash-based signature schemes, resulting in short signatures and fast key generation times, furthermore it has become an IETF standard [128], which strengthens the overall trust in the design due to public review. On the other hand, SPHINCS has the

Table 9.3.: Overview of hash-based digital signature scheme implementations.

| Architecture | Scheme | Max Signatures | Reference |
|---|---|---|---|
| 8-bit smart card – ATMEL AT90SC | GMSS | $2^{16}$ | [252] |
| 16-bit smart card – Infineon SLE 78 | XMSS | $2^{20}$ | [129] |
| ATMEL AVR ATxmega128A1 | GMSS | $2^{20}$ | [83] |
| ARM Cortex M3 – ARMv7-M | XMSS$^{MT}$ | $2^{20}$ | [131] |
| ARM Cortex M3 – ARMv7-M | SPHINCS | (soft max) $2^{50}$ | [131] |

benefit of being stateless, which results in a design that can plug-and-play replace current digital signature designs without changes to the underlying hardware for the continuous state writing after every new signature. In contrast to XMSS-T, the statelessness of SPHINCS has the price of much larger signatures, specifically the SPHINCS-256 configuration results in 40 kB signatures and XMSS-T for a $2^{20}$ signature count results in 2.9 kB signatures, effectively being 14 times smaller than SPHINCS-256 signatures. For future eMRTDs it is hard to predict if the signature scheme state or bigger signatures are a tougher technical obstacle. On the one hand, as discussed in section 7.5 the transfer speed of current eMRTDs is very limited and big signatures would slow down the entire border control process, but on the other hand, transfer speed regular increases over time in all IT areas. Writing the state to the eMRTD would require a new hardware design, but on the one hand, the pseudo clock updates (see chapter 5) are already written every time EAC is used on the eMRTD. Additionally, on the other hand, LDS 2.0 (see chapter 3.1) already plans to save the passport stamps digitally on the ePassport [141] in the future, which also requires regular writes to the chip. Since both designs have been tested on low-end hardware [131] both are candidates for PQ resistant digital signatures on eMRTDs.

The final cryptographic building block public key encryption is only needed indirectly for key agreement between eMRTD and terminal. The introduced schemes are the McEliece scheme in the Niederreiter variant with Goppa codes and the QC-MDPC-McEliece scheme. Either a random value is encrypted with the asymmetric scheme and sent to the other party, similar to the TLS approach [76], or specific key exchange protocols as the CAKE protocol have to be considered. On the one hand, dedicated key agreement protocols like CAKE consider forward secrecy by design, but on the other hand, a new ephemeral key can be created for every new session and signed with a long-term key (i.e., XMSS-T or SPHINCS) to achieve perfect forward secrecy for all schemes. The latter is particularly suitable since the key setup is very fast for code-based systems [18]. QC-MDPC codes result in much smaller public key sizes (i.e., 1.2 kB) in contrast to Goppa codes (i.e., 1 Mb), but are currently not well enough researched to give a recommendation for a travel document with a 10 year validity period. In view of the significant public key size difference, both schemes are considered by the PQ-Crypto project [233], and since cryptanalysis regarding QC-MDPC is hard to predict, a soft introduction approach is most suitable.

Instead of waiting until the last minute when quantum computers become a critical threat to public key cryptography, a soft introduction in the next year's chips is more viable. Even if the new algorithms are not used directly they are important since a travel document issued today stays in circulation for 10 years. Therefore, the planning should consider the next ten years and not only today's security requirements.

Since the exact requirements are open to future discussion, a more high-level approach similar to the TLS cipher suites [76] might be most viable. Instead of relying on fixed algorithms implement the current schemes (i.e., RSA, DSA, and ECDSA) as well as future-proof schemes (i.e., SPHINCS, XMSS-T, Goppa-McEliece, and QC-MDPC-McEliece) and mandatorily activate the PQ schemes if required (i.e., when Quantum computers become a realistic threat). Since a connection to a trusted member state

home server or a reliable clock are currently still out of reach setting a fixed date is not an advisable strategy. Hence, arming the PQ resistant mode as well as deactivating certain algorithms must be done in hardware.

A technology to implement such behaviour securely is the so-called eFUSE [133], which represents similar to an electrical fuse a component that can be burned once and is permanently destroyed afterwards. In computer science this logically represents a bit field which can be arbitrarily read, but every bit can only be set once to burned and not changed afterwards. eFUSEs are commonly used to prevent firmware downgrading in consumer electronics, but could also be utilised to selectively deactivate algorithms in future eMRTDs. On the one hand, writing to the eFUSE of the eMRTD must only be allowed to trusted terminals that can prove their originality by a post-quantum secure digital signature and on the other hand, to furthermore prevent DoS attacks a minimum set of long-term secure algorithms (e.g., XMSS-T and Goppa-McEliece) must be usable independent of the eFUSE's status. Terminal and eMRTD are only to be allowed to use the schemes granted by the hardware eFUSE. Utilising a high-level approach similar to the TLS cipher suites can provide a soft approach for introduction of post-quantum resistant schemes into future eMRTDs.

# 10. Enhancements for the eMRTD SPI regarding Biometrics

Biometrics provide the primary means to link a person to its identity document. While the EU ePassports store two fingerprint images in DG3 and have the reserved DG4 for encoded eyes (i.e., iris), the primary link remains the face image in DG2, due to the discussed non-existent availability of EAC.

Common face recognition is troublesome since it has a very small Biometric entropy [71], cannot distinguish between full siblings, is prone to face morphing [98], prone to ageing effects [3], and has symmetry implications [111].

Similar to the classical birthday problem, only 38 randomly chosen people have to be assembled before it becomes more likely than not that at least two of them will have a biometric collision (False Match), and are considered doppelgängers [71].

This chapter first focuses on the entropy of different biometric characteristics reported in the scientific literature in section 10.1.

Barcodes represent a cost-efficient alternative to chip-based data storage. Section 10.2 investigates the feasibility of storing fingerprint and iris image data in compact 2D barcodes. In accordance to proposed standards different types of fingerprint and iris images are compressed employing cascades of lossy image and lossless data compression algorithms. Obtained results confirm that capacities of stacked 2D barcodes enable a standard-compliant chip-less embedding of biometric image data. Furthermore, custom-built compression techniques might allow for an even more compact storage of biometric data.

Section 10.3 analyses techniques to accelerate Hamming distance-based comparisons of binary biometric reference data, i.e., iris-codes, in large-scale iris recognition systems, which preserve the biometric performance. Focus is put on software-based optimisations, an efficient two-step iris-code alignment process referred to as *TripleA*, and a combination thereof. Benchmarking the throughput and identifying potential bottlenecks of a portable commodity hardware-based iris recognition system, is of particular interest. Based on conducted experiments the section points out practical boundaries of large-scale comparisons in CPU-based iris recognition systems, bridging the gap between the fields of iris recognition and software design.

To confirm an individual's identity accurately and reliably iris recognition systems analyse the texture that is visible in the iris of the eye. The rich random pattern of the iris constitutes a powerful biometric characteristic suitable for biometric identification in large-scale deployments. Identification attempts or deduplication checks require an exhaustive one-to-many comparison. Hence, for large-scale biometric databases with millions of enrollees the time required for a biometric identification is expected to sig-

nificantly increase.

## 10.1. Entropy of Biometric Data

This section is based on and was published as [43]. Biometric features must not be expected to be mutually independent, e.g. fingerprints underlie distinct structures (densities and orientations of minutiae). Focusing on data storage, binary biometric templates represent a favourable representation, enabling compact storage and rapid comparison. So far, numerous approaches have been proposed to extract binary feature vectors from diverse biometric characteristics. Without loss of generality this analysis will be restricted to entropy of biometric data according to a binary representation of biometric features.

A common way to estimate the average entropy ($\simeq$ amount of mutually independent bits) of biometric feature vectors is to measure the provided "degrees-of-freedom" which are defined by $d = p(1-p)/\sigma^2$, where $p$ is the mean Hamming distance ($HD$) and $\sigma^2$ the corresponding variance between comparisons of different pairs of binary feature vectors, shown in Figure 10.1. In case all bits of each binary feature vector of length $z$ would be mutually independent, comparisons of pairs of different feature vectors would yield a binomial distribution, $\mathcal{B}(z,p) = \binom{z}{k}p^k(1-p)^{z-k} = \binom{z}{k}0.5^z$ and the expectation of the $HD$ would be $1/z \cdot \mathbb{E}(X \oplus Y) = zp \cdot 1/z = p = 0.5$, where $X$ and $Y$ are two independent random variables in $\{0,1\}$. In reality $p$ decreases to $0.5-\epsilon$ while $HD$s remain binomially distributed with a reduction in $z$ in particular, $\mathcal{B}(d, 0.5)$ [287]. Reported entropy in literature of relevant biometric characteristics are summarised in Table 10.1. Estimated entropy can be directly transferred to $AD$ and $PI$s which are applied in further application. However, techniques which are employed to overcome biometric variance, e.g. severe quantisation, may reduce the entropy of resulting protected templates [1].

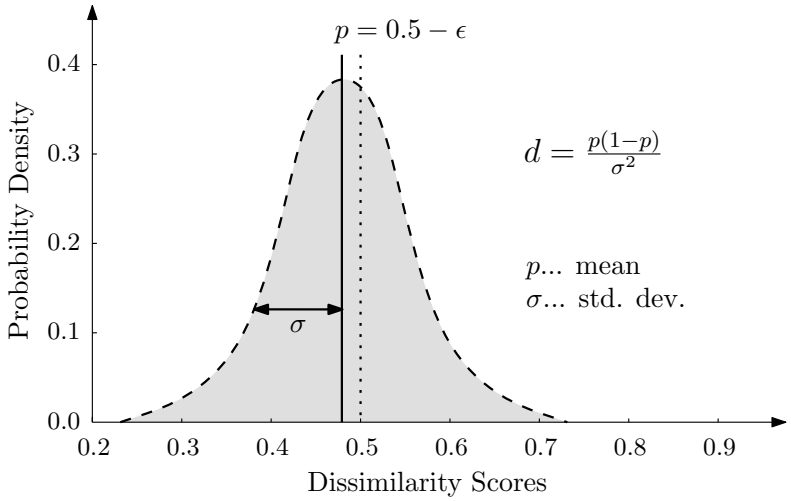



Figure 10.1.: Binomial distribution of scores between different pairs of vectors.

In addition, the amount of degrees-of-freedom can be directly derived from the false match rate (*FMR*) provided by a biometric (template protection) system. According to the ISO/IEC IS 19795-1 [163] the *FMR* defines the proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template. At a targeted false non-match rate (*FNMR*), the proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample, provided entropy (in bits) is estimated as $\log_2(FMR^{-1})$, which directly relates to entropy estimations which are frequently applied to passwords or PINs.

Table 10.1.: Entropy reported in literature for different biometric characteristics.

| Biometric characteristic | Feature extractor | Entropy (in bits) | Ref. |
|---|---|---|---|
| Fingerprint | Minutia-based | 84 | [242] |
| Iris | 2D Log-Gabor wavelets | 249 | [70, 69] |
| Face | Fusion of FLD and PCA | 56 | [1, 2] |

FLD ... Fisher linear discriminant PCA ... Principal component analysis

Most biometric cryptosystems aim at binding or generating keys long enough to be applied in a generic cryptographic system (e.g., 128-bit keys for AES). To prevent biometric keys from being guessed, these require sufficient entropy. While the issue of key entropy has been ignored in early approaches to biometric cryptosystems, recent works tend to provide key entropy estimations. In [48, 47], Buhan *et al.* point out a direct relation between the maximum length $k$ of cryptographic keys and the error rates of the biometric system. The authors define this relation as $k \leq -\log_2(FMR)$, as previously mentioned. This means that an ideal biometric cryptosystem would have to maintain an FAR $\leq 2^{-k}$ which appears to be a quite rigorous upper bound that may not be achievable in practice. Nevertheless, the authors emphasise the important fact that the recognition rates of a biometric system correlate with the amount of information which can be extracted, retaining maximum entropy. Based on their proposed quantisation scheme [286], Vielhauer *et al.* describe the issue of choosing significant features of online signatures and introduce three measures for feature evaluation [285]: intrapersonal feature deviation, interpersonal entropy of hash value components, and the correlation between both. By analysing the discriminativity of chosen features the authors show that the applied feature vector can be decreased by 45% maintaining error rates [255]. This example underlines the fact that biometric cryptosystems may generate arbitrary long keys while inter-class distances (i.e., Hamming distance between keys) remain low.

Ballard *et al.* [4, 5] propose a new measure to analyse the security of a biometric cryptosystem, termed guessing distance. The guessing distance defines the number of guesses a potential imposter has to perform in order to retrieve either the biometric data or the cryptographic key. Thus, the guessing distance directly relates to intra-class distances of biometric systems and, therefore, provides a more realistic measure of the entropy of biometric keys. Kelkboom *et al.* [172] analytically obtained a relationship between the maximum key size and a target system performance. An increase of maximum key

size is achieved in various scenarios, e.g. when applying several biometric templates at enrolment and authentication or when increasing the desired false rejection rates. In theory-oriented work Tuyls *et al.* [284, 277] estimate the capacity and entropy loss for fuzzy commitment schemes and shielding functions, respectively. Similar investigations have been done in [183, 271] providing a systematic approach of how to examine the relative entropy loss of any given scheme, which bounds the number of additional bits that could be extracted if optimal parameters were used.

## 10.2. Storing Fingerprint and Iris Image Data in 2D Barcodes

This section is based on and was published as [46]. With the introduction of the e-passport, and its physical as well as logical security mechanisms, protection against travel document forgery has been greatly improved. Moreover, embedded biometric information provides a reliable link between the travel document and its holder. In contrast, birth certificates are nowadays either printed using common office printers or hand written on pre-printed templates. Generally neither physical nor electronic security features are utilised. On the one hand, this keeps the production costs low and is reasonable since the document is rarely used and not contained in the specification of Machine Readable Travel Documents (MRTD) as defined by the International Civil Aviation Organization (ICAO). On the other hand, a birth certificate can be used as an evidence of identity and enables the application for a travel document like an ePassport. Hence, the requirements are contradictory in regard to document protection level and financial cost. For a document holder the motivation to pay a higher price for a birth certificate is expected to be rather low, since it cannot be used as a travel document. Nevertheless, equipping birth certificates with biometric information could close the aforementioned security gap, eliminating one weak link in the e-passport document life cycle, where the link between a document and its holder via biometrics has to be created with these boundary conditions in mind. Therefore a cheap 2D barcode might represent the primary choice for future birth certificates in contrast to more expensive embedded RFID chips, since 2D barcodes can be generated completely by software and no expensive document manufacturing equipment is required.

The International Organization for Standardization (ISO/IEC JTC1) and the ICAO specify biometric interchange data to be stored in governmental documents, e.g. passports, in image form, rather than in form of extracted biometric feature vectors [153, 146]. On the one hand, such deployments benefit from future improvements which can be easily incorporated, without re-enrolment of registered subjects. On the other hand, since biometric templates may depend on patent-registered algorithms, images achieve more interoperability, vendor neutrality, and allow for visual inspection by human experts. Focusing on birth certificates' potential ageing effects represent a crucial factor for the stability of biometric characteristics. While certain characteristics are influenced by age factors, e.g. face, a level of permanence which enables reliable long-term biometric recognition has been confirmed for fingerprints and iris [292, 114].

This study investigates the feasibility of storing fingerprint and iris image data in

2D barcodes. For this purpose a two-stage compression strategy is employed based on lossy image compression stage and lossless data compression stage. In accordance with relevant ISO/IEC standard practical lossy image compression profiles are identified in the first stage. In the second stage the potential of diverse lossless data compressors is investigated. Based on this preliminary study initial conclusions with respect to the storage of biometric images in 2D barcodes are drawn and promising directions for future research stated. This chapter is organised as follows: In section 10.2.1 the proposed system architecture is described in detail. Experiments are presented in section 10.2.2 and conclusions are drawn in section 10.2.3.

## 10.2.1. Storage of Biometric Image Data in 2D Barcodes

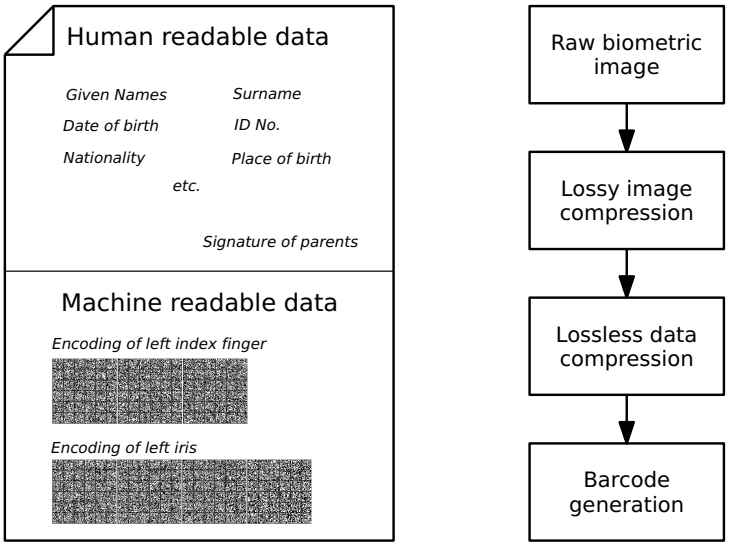
Since the cost of future birth certificates shall be kept to a minimum it is proposed to stick to the standard paper format of common office printers, e.g. DIN A4 or letter. Today the complete birth certificate is human readable. For efficient and fault tolerant processing of the biometric data the future layout shall be divided into a human readable zone and a machine readable zone. Figure 10.2(a) depicts the envisioned layout. The human readable zone stores the same data as today's birth certificates and the machine readable zone comprising a 2D barcode containing the data from the human readable zone as well as the biometric data of the document holder. The biometric data can be encrypted to ensure confidentiality and data privacy of sensitive biometric data and the complete data can be digitally signed for validation of authenticity and integrity of the data. These cryptographic mechanisms are out of scope for the chapter at hand. Nevertheless, these mechanisms would not have a high impact on the storage requirements of the used barcode in contrast to the biometric data (see [32]). The backside of the birth certificate could either contain a multi lingual description of the data fields used in the human readable zone, or be empty for cheaper non-duplex printer requirements.

Figure 10.2(b) illustrates the processing chain of the proposed study. In order to obtain compact biometric records, raw biometric images are compressed in two stages, employing lossy image compression as well as lossless data compression techniques. Finally, 2D barcodes are extracted from the resulting data records.

### 2D Barcodes

2D barcodes are commonly used in logistics, merchandise tagging or advertisement. One of the most popular barcodes is the Quick Response Code [162], which is usually called QR code. QR codes have four levels of error correction which allow a reconstruction of barcodes with 7% to 30% unreadable surface. The capacity depends on the version, the error correction level, and the data type. The biggest QR code specified in ISO/IEC 18004 is the $177 \times 177$ pixel version 40-L with a maximum character storage capacity of 7089 numeric only characters, 4296 alphanumeric values, 2953 binary bytes or 1817 kanji with minimal error correction level of 7%.

Another commonly used 2D barcode standard is the data matrix code standardised in ISO/IEC 16022 [160]. Modern data matrix codes, called ECC200, utilise Reed Solomon




(a) document layout (b) processing chain

Figure 10.2.: Proposed birth certificate layout and overview of the processing chain of this study. Sizes of barcodes in figure 10.2(a) correspond to the approximated storage requirement for the compressed biometric sample.

codes for error correction and allow the recovery of barcodes with up to 25% damaged surface. The maximum standardised character capacity for the $144 \times 144$ pixel data matrix code is 1556 byte, 3116 numeric digits or 2335 ASCII values.

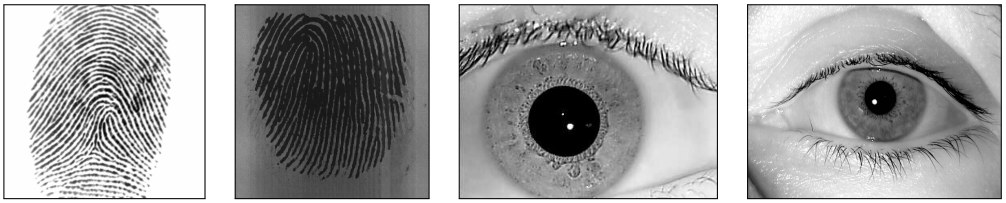
Other 2D barcode standards are the PDF417 code which is used in a wide range of applications e.g. plane tickets, standardised under ISO/IEC 15438 [159] and the AZTEC code utilised in the transport industries, e.g. railway companies and standardised under ISO/IEC 24778 [161]. Common 2D barcodes are not intended for the storage of big data. Therefore, biometric data on birth certificates will probably be split onto multiple stacked barcodes.

### Lossy Biometric Image and Lossless Data Compression

Image compression represents a well-studied field in biometric research. Recommendations on compression algorithms as well as compression ratios are provided in ISO/IEC IS 19794 on "Biometric data interchange format" in particular, Part 4 on "Finger image data" and Part 6 on "Iris image data" [153]. Both standards advise against the usage of the popular DCT-based JPEG (JPG) compression method specified ISO/IEC 10918-1, i.e. it is only retained to encode legacy data. The wavelet-based JPEG 2000 (J2K) standard specified in ISO/IEC 15444-1, which provides a more efficient compression, is recommended for lossless/lossy compression of (high-resolution) fingerprint and iris image data, where compression ratios should be limited to a 15:1 compression for fingerprint and a 10:1 compression for iris (in verification mode). For using 8-bit grayscale images

Table 10.2.: Overview of relevant parameters of employed databases.

| Characteristic | Name | Sensor | Format | Image resolution | File size |
|---|---|---|---|---|---|
| Fingerprint | FVC02 DB1 | TouchView II (optical) | Finger-image | 388×374 px | 142 kB |
| | FVC02 DB3 | 100 SC (capacitive) | Finger-image | 300×300 px | 88 kB |
| Iris | IITDv1 | JPC1000 (NIR) | Cropped | 320×240 px | 75 kB |
| | BioSecure | IrisAccess 3000 (NIR) | Uncropped | 640×480 px | 300 kB |



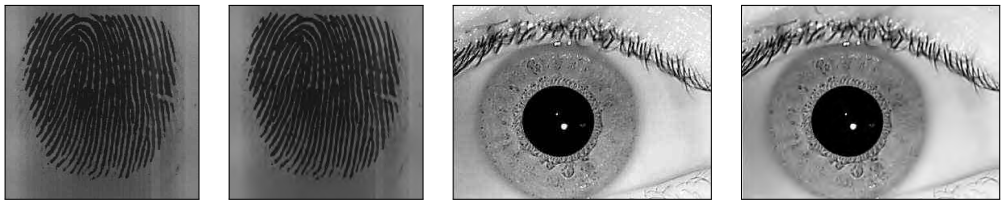
(a) FVC'02 DB1 (b) FVC'02 DB3 (c) IITDv1 (d) BioSecure

Figure 10.3.: Uncompressed image samples (images correspond to the first instance of the first subject).

this would result in a compression rate of 0.5 and 0.8 bits per pixel (bpp), respectively.

Recommendations of ISO/IEC are backed by diverse proposed studies. In [104, 193] it is found that, at same compression rates, J2K compression generally causes less effects on the recognition accuracy of a fingerprint recognition system compared to JPG, i.e. the peak signal-to-noise ratio (PSNR) serves as a predictor of biometric performance. Similar findings have been reported for compression of iris image data [238, 73, 248]. For both, fingerprint and iris image data, it has been shown that compression ratios, which yield PSNR values above 30 dB, cause only a negligible decrease in recognition accuracy [104, 248]. Hence, relevant compression profiles are chosen according to these findings. Note that, it is generally conceded that visual lossless compression is achieved at PSNR values above 40 dB.

In contrast to ePassports and other travel documents the birth certificate has no fast processing requirements like border crossing in lines where time is a significant factor to maximise passenger processing throughput. Therefore, the required memory size and computation time is secondary for the analysed compression algorithms and the compression rate is key. The investigated data compression programs are either common compressors used on Linux systems or taken from state-of-the-art benchmark results for data compression. The following 32 programs were tested for the four specified lossy image compression profiles: zip, gzip, bzip2, rar, 7zip, xz, lz4, lzop, arj, ncompress, lrzip, balz, jpgcrush, lpaq8, lzip, lzma_alone, pcompress, quad, jpegoptim, zoo, zpaq, zstd, packJPG, NanoZip, yzx, zcm, rejpeg, paq8pxd_v4, fp8_v3, paq8pxd_v16, paq8pxd_v16_sk4 and cmix. For details on utilised compressors the reader is referred to [191].



(a) *JPG-F* (b) *J2K-F* (c) *JPG-I* (d) *J2K-I*

Figure 10.4.: Samples for compression profiles for (a)-(b) fingerprint and (c)-(d) iris image data.

### 10.2.2. 2D Barcode Experiments

Experiments are conducted on four publicly available image databases, the DB1 and the DB3 of the Second Fingerprint Verification Competition [280], the IIT Dehli Version 1.0 [24] and BioSecure [25] iris database. Relevant information about the employed datasets are summarised in Table 10.2, sample images are depicted in figure 10.3.

Compression experiments are performed on the first instance of the first one hundred subjects of each dataset. For JPG compression quality parameters are iteratively configured in order to obtain desired bit-rates using the ImageMagick software *convert* [150]. For J2K compression the *JJ 2000* software [84] is employed as conversion tool which allows for explicit rate control.

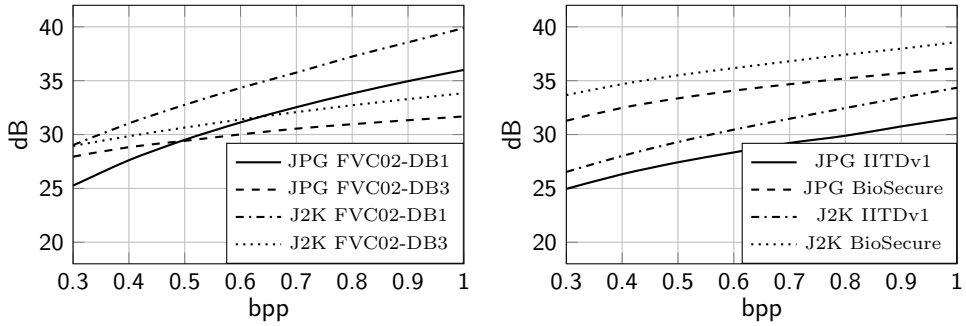
#### Lossy Image Compression Profiles

Obtained file sizes (in kB) for different compression rates for all datasets are summarised in Table 10.3. File headers (general and representation), which are required by ISO/IEC formats, cause negligible additional storage cost (∼64 byte). Corresponding PSNR values (in dB) for JPG and J2K compression are plotted in figure 10.5. As expected, in terms of PSNR J2K outperforms JPG across all datasets and compression rates. Focusing on fingerprint image data, PSNR values above 30 dB are achieved for compression rates down to 0.4 bpp in case of J2K, yielding file sizes of 7.1 kB and 4.4 kB for FVC'02 DB1 and DB3, respectively. With respect to iris image data higher PSNR values are obtained on the BioSecure database, however, images in this dataset are stored in un-cropped format. Thus, images are significantly larger, compared to the cropped images of the IITDv1 database, as these comprise a large region around the eye. Hence, considering obtained file sizes, cropped images compressed at 0.6 bpp using J2K appear preferable, resulting in images of size 5.6 kB. Note that recent advances in the field of sclera and periocular biometric recognition [218] might depreciate the use of the cropped and masked format suggested in [73], which is not considered in this study.

If JPG compression is applied, significantly higher compression rates have to be chosen to obtain images of comparable quality (in terms of PSNR). In order to receive images which exhibit PSNR values above 30 dB, compression rates of 0.6 and 0.8 bpp should be chosen for fingerprint and cropped iris images, yielding file sizes of 6.6 kB and 7.5 kB,

Table 10.3.: File sizes (kB) obtained on all datasets for different compression rates.

| Database | Compression rate (bpp) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **1.0** | **0.9** | **0.8** | **0.7** | **0.6** | **0.5** | **0.4** | **0.3** |
| FVC02 DB1 | 17.7 | 15.9 | 14.2 | 12.4 | 10.6 | 8.9 | 7.1 | 5.3 |
| FVC02 DB3 | 11.0 | 9.9 | 8.8 | 7.7 | 6.6 | 5.5 | 4.4 | 3.3 |
| IITDv1 | 9.4 | 8.4 | 7.5 | 6.6 | 5.6 | 4.7 | 3.75 | 2.8 |
| BioSecure | 37.6 | 33.6 | 30.0 | 26.4 | 22.4 | 18.8 | 15.0 | 11.2 |




(a) fingerprint (b) iris

Figure 10.5.: PSNR (dB) obtained on all datasets for different compression rates.

respectively. Based on the obtained results four relevant profiles are identified for JPG and J2K compression of fingerprint images of FVC'02 DB3 and iris images of IITDv1, which are summarised in Table 10.4. Compressed sample images for different profiles for the original uncompressed images of figure 10.3 (a) and (c) are shown in figure 10.4.

### Lossless Data Compression

The considered compressors can be divided into three groups. *Group-1* of the compressors does not compress the specified image data in the profiles at all or results in even bigger data. *Group-2* does compress the data but with a negligible compression rate of more than 95%. *Group-3* of the compressors can compress a lossy compressed image below 95%.

JPG and J2K pictures are data of high entropy and are generally considered hard to compress. Therefore, for JPG most compressor candidates are in *Group-1* or *Group-2*. Only some compressors can significantly lossless compress JPG pictures even further. Table 10.5 shows these *Group-3* results for the profiles *JPG-F* and *JPG-I* by their average compression rate as well as lower quartile and upper quartile. For J2K images nearly all compressors are in *Group-1*, only very few are in *Group-2* and *Group-3* is empty. The best compressors can compress J2K data to around 99.5% of its source size, which is negligible for the discussed use case.

There are at least two explanations for this behaviour. Either J2K images are of such

Table 10.4.: Profiles for JPG and J2K compression of fingerprint and iris image data.

| Name | Characteristic | Database | Compression | Rate | File size |
|---|---|---|---|---|---|
| *JPG-F* | Fingerprint | FVC'02 DB3 | JPG | 0.6 bpp | 6.6 kB |
| *J2K-F* | | | J2K | 0.4 bpp | 4.4 kB |
| *JPG-I* | Iris | IITDv1 | JPG | 0.8 bpp | 7.5 kB |
| *J2K-I* | | | J2K | 0.6 bpp | 5.6 kB |

Table 10.5.: Compression rate (%) obtained on JPG-F and JPG-I profiles for different compressors.

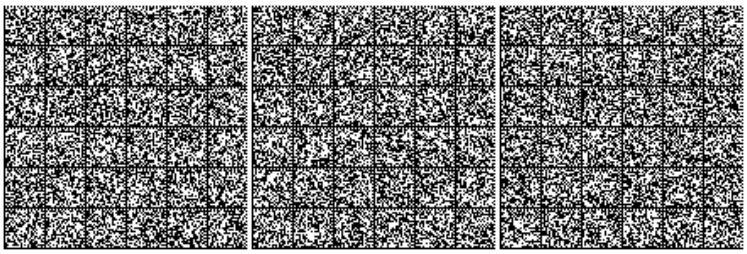
| Compressor | *JPG-F* | | | *JPG-I* | | |
|---|---|---|---|---|---|---|
| | u.Q. | AVG | l.Q. | u.Q. | AVG | l.Q. |
| cmix | 80.83 | 80.59 | 78.70 | 87.79 | 87.21 | 86.93 |
| packJPG | 82.74 | 82.04 | 81.36 | **83.59** | **82.99** | **82.56** |
| rejpeg | 87.19 | 86.34 | 85.50 | 94.01 | 93.06 | 92.33 |
| paq8pxd_v4 | 79.77 | 79.60 | 77.64 | 86.99 | 86.42 | 86.06 |
| fp8_v3 | **79.77** | **79.58** | **77.63** | 87.02 | 86.44 | 86.08 |
| paq8pxd_v16 | 81.95 | 81.82 | 79.85 | 89.24 | 88.61 | 88.29 |
| paq8pxd_v16_sk4 | 81.95 | 81.82 | 79.85 | 89.24 | 88.61 | 88.29 |

high entropy that they simply are not compressible or J2K images are still considered unimportant in other common domains that compression research does not focus on this particular image format. It is believed the latter is the case and this is considered a topic of future work. The benchmarks for lossless data compression mostly build their data corpus file sets out of data formats used in the Internet domain like JPG. These compressors detect the JPG format and usually follow a common strategy to compress it even further. The lossless Huffmann compression of the JPG data gets decompressed and the DCT coefficients get recompressed by a more efficient compression algorithm.

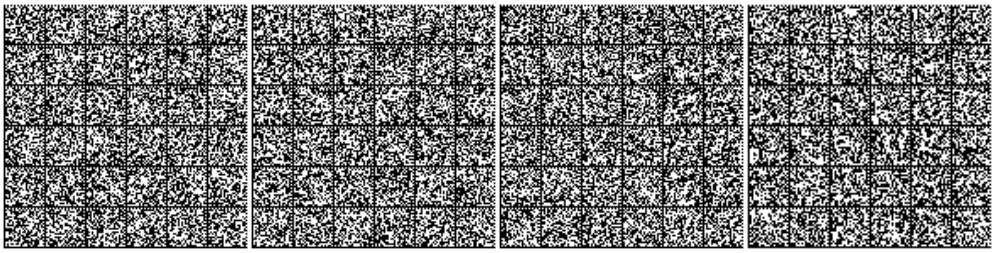
There exist no models for J2K data in these compressors and it is handled as binary data instead, which might explain the low compression results. Therefore, currently the lossless compression step for profiles *J2K-F* and *J2K-I* brings no further benefits. For the *JPG-F* profile the average file size can be reduced to 5.2 kB and the *JPG-I* profile to 6.2 kB.

As final step the compressed biometric data is divided and stored in multiple 2D barcodes. Figure 10.6 depicts an example for data matrix codes with the J2K profiles. For the *J2K-F* face profile three codes are necessary and for the *J2K-I* iris profile four codes are needed.

A single data matrix code has $144 \times 144$ pixel therefore the iris barcode has $576 \times 144$ pixel. Using a letter or DIN A4 layout with 300 dpi negligible space is required on the document and the barcode can be upscaled for more reliable optical readings. Even multiple instances of iris and finger images can be stored on a birth certificate.



(a) fingerprint



(b) iris

Figure 10.6.: Stacked data matrix codes for (a) the image of figure 10.4(b) and (b) the image of figure 10.4(d).

### 10.2.3. 2D Barcode Conclusions and Future Work

Current security gaps in the life cycle of travel documents stress an integration of biometric data into breeder documents, i.e. birth certificates, in order to achieve a strong link between the document and its holder. It has been shown that 2D barcode technologies can be utilised to store biometric data in a cost-efficient way with realistic space requirements. The best compression rates are achieved by employing a serial combination of lossy image and lossless data compression algorithms.

It is observed that specifically designed lossless data compression methods are capable of further reducing the size of high-entropy image data. Compression techniques based on machine learning, e.g. deep auto-encoders or content mixing utilising neural networks, might obtain even further gains in the narrow field of biometric data compression, which is subject to future research.

## 10.3. Accelerating CPU-based Iris Recognition Systems

This section is based on and was published as [245]. The rich random structure of the iris, and hence its resistance to false matches, constitutes one of the most powerful biometric characteristics [69]. Following Daugman's approach [69], which represents the core of most public operational deployments, four processing components form an iris recognition system: (1) *acquisition*, where most current deployments require subjects to fully cooperate with the system in order to capture images of sufficient quality; (2)

*pre-processing*, which includes the detection of the pupil and the outer iris boundary. Subsequently, the iris (approximated in the form of a ring) is normalised to a rectangular texture. To complete the preprocessing, parts of the iris texture which are occluded by eye-lids, eye-lashes or reflections are detected and stored in an according noise-mask; (3) *feature extraction*, in which an iris-code is generated by convolving local regions of the pre-processed iris texture with filters and encoding responses into bits. This binary data representation enables compact storage and rapid (4) *comparison*, which is based on the estimation of Hamming distance (*HD*) scores between pairs of iris-codes and corresponding masks. In the comparison stage circular bit shifts are applied to iris-codes and *HD* scores are estimated at $K$ different shifting positions, i.e. relative tilt angles. The minimal obtained *HD*, which corresponds to an optimal alignment, represents the final score. It is important to note, that the number of shifting positions employed to determine an appropriate alignment between pairs of iris-codes may vary depending on the application scenario. Some public deployments of iris recognition go as far as $K = 21$ shifting positions when handheld cameras are used for which it is more difficult to ensure an upright capture orientation [72]. Hence, score distributions are skewed towards lower *HD* scores, which (for a given threshold) increases the probability of a false match by the factor $K$ [72].

Nowadays iris recognition technologies are already deployed in numerous nation-wide projects. Simplicity in design and development as well as the usage of commodity hardware are driving factors behind the deployment of large-scale biometric systems, e.g. the Indian Aadhaar project [279] in which thousands of CPU cores are processing millions of transactions on a daily basis. In such systems identification attempts or de-duplication checks might represent a bottleneck, since these require an exhaustive $1 : N$ comparison where $N$ represents the number of subjects registered with the system. In particular, comparison time represents a crucial factor, which dominates the overall computational workload in any large-scale biometric identification system, especially if large values of $K$ are unavoidable.

### 10.3.1. Contribution of Section

In this section focus is put on an iris recognition system, which performs a CPU-based exhaustive search for each authentication attempt. The presented study represents a more common scenario, in contrast to proposed studies, which analyse hardware-specific acceleration of iris recognition systems. The analyses include a comparative study of the most efficient ways to count disagreeing bits between iris-codes. Potential of manual loop-unrolling as well as different extensions to the x86 instruction set architecture for microprocessors are analysed. In addition, multi-threading techniques and statistical optimisation of micro-operations are considered. Furthermore, the inter-relation between throughput and rotation compensation provided by an iris recognition system is estimated. In order to further accelerate a single pair-wise comparison of iris-codes, the study builds upon the work of [246], where a novel technique for comparing pairs of iris-codes is proposed, which is referred to as Accelerated Accuracy-preserving Alignment – *TripleA*. This method focuses on the alignment process, in which an adjustable

two-step search-procedure is employed in order to efficiently determine alignments between iris-codes. Within this procedure only a fraction of $K$ shifting positions has to be considered during a single pair-wise comparison, while covering the same range of possible tilt angles. This work, enhances the *TripleA* scheme by applying it to an optimised CPU-based iris recognition scheme and shows that the *TripleA* method can be seamlessly integrated, such that the resulting system takes full advantage of *TripleA* on top of software-based optimisations. In summary, this work provides a detailed guidance of how to substantially accelerate large-scale iris biometric systems on commodity hardware in an accuracy-preserving manner, by combining software-based optimisations with a technique for efficient iris-code alignment. Moreover, summarised key observations might as well provide explanations for anomalies reported in existing studies.

### 10.3.2. Organisation of Section

This section is organised as follows: related works are discussed in subsection 10.3.3. In subsection 10.3.4 the employed iris recognition system is summarised. A detailed analysis of software-based acceleration techniques is given in subsection 10.3.5 and the *TripleA* method is described in subsection 10.3.6. Experimental results are presented in subsection 10.3.7. Finally, conclusions are drawn in subsection. 10.3.8.

### 10.3.3. Hamming Distance Related Work

To circumvent the bottleneck of an exhaustive $1 : N$ comparison, different concepts have been proposed in order to reduce the workload in an iris biometric (identification) system. These concepts might be differentiated between four key concepts: (1) coarse classification or "binning", (2) a serial combination of a computationally efficient and a conventional system, (3) indexing schemes, and (4) hardware-based acceleration.

By binning an iris biometric database into several classes, the workload can be divided by the number of classes, given that irises of registered subjects are equally distributed among them. Natural features to be utilised include eye position (left or right) [272] or eye colour [236, 103]. Recent advances in the field of soft biometrics suggest further possible classification based on gender [273], age groups [85], or ethnicity [237, 270] (for further details on soft biometrics the reader is referred to [68]). Instead of creating tangible, human-understandable classes, it is also possible to rely on distinct iris texture features [293, 253, 213]. Binning is equivalent to the combination of biometric systems. Hence, classification errors might significantly increase the false non-match rate (FNMR) of the overall system. Moreover, the potential benefit of binning is limited by the number of bins which determines the factor by which the database size can be reduced.

Within serial combinations computationally efficient biometric systems are used to extract a short-list, i.e. small fraction, of most likely candidates. This procedure might be referred to as pre-screening. While generic iris recognition systems already provide a rapid comparison, more efficient biometric comparators can be obtained by employing compressed versions of original iris-codes during pre-screening [108, 107]. Further, a rotation-invariant iris recognition scheme can be applied in the pre-screening step [175].

Similar to binning approaches, a serial combination of a computationally efficient and an accurate (but more complex) scheme might increase the FNMR of the overall system. However, a serial combination enables a more accurate operation of the resulting trade-off between computational effort and accuracy by choosing an adequate size for the short-list.

Indexing schemes aim at constructing hierarchical search structures for iris biometric data, which tolerate a certain amount of biometric variance. Such schemes substantially reduce the overall workload of a biometric identification, e.g. $\log N$ in case of a binary search tree. Such search structures might be designed for iris-codes [120, 244] as well as iris images [209, 106, 235]. While the majority of works report hit/ penetration rates on distinct datasets, required computational efforts are frequently omitted. The application of complex search structures on rather small datasets may as well cloud the picture about actual gains in terms of speed and leaves the scalability of some approaches questionable.

Adapting comparison procedures to adequate hardware, e.g. multiple cores within a CPU, allows for parallelisation [240]. By simultaneously executing a number of threads the workload can be significantly reduced since a $1 : N$ comparison can be performed in parallel on various subsets of equal size. Also, the estimation of *HD* scores at various shifting positions during alignment can be parallelised. Moreover, iris-code comparisons can be efficiently performed on the GPU using GPGPU or CUDA [282], FPGA [240, 186], or other specialised hardware like CELL processors [239].

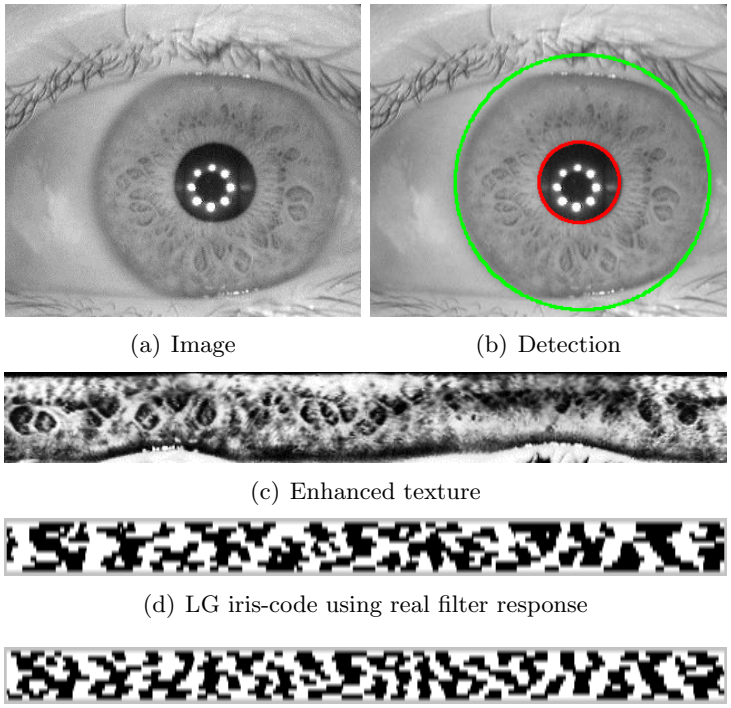
Apart from hardware-based acceleration, most of presented schemes either fail to provide a significant acceleration, or they suffer from a significant decrease in recognition accuracy. Hence, existing approaches often obtain a trade-off between biometric performance (recognition accuracy) and speed-up, compared to a traditional iris recognition system. In practice most concepts do not allow for a seamless integration into a conventional identification system. The majority of hardware-specific acceleration techniques of iris recognition systems is custom-built, which makes it difficult to derive generally applicable methodologies or concepts. Moreover, anomalies in runtime tests are frequently left uncommented.

### 10.3.4. Iris Recognition System

The following subsections summarise the key components of the employed iris recognition systems.

#### Preprocessing and Feature Extraction

In the employed iris recognition system, which builds upon common processing components, the iris of a given sample image is detected and transformed to a rectangular texture of 512×64 pixels applying a contrast-adjusted Hough transform. The enhanced texture is obtained by applying contrast limited adaptive histogram equalisation (CLAHE). In the feature extraction stage the enhanced texture is divided into stripes resulting in 10 one-dimensional signals, each one averaged from the pixels of 5 adjacent rows (the upper 512×50 rows are analysed). The first feature extraction method follows the Daugman-



(a) Image (b) Detection

(c) Enhanced texture

(d) LG iris-code using real filter response

(e) QSW iris-code using a single wavelet subband

Figure 10.7.: Common iris biometric processing chain for image S1008L02 of the CASIAv4-Interval iris database.

like 1D-LogGabor feature extraction algorithm of Masek [194] (LG) and the second follows the algorithm proposed by Ma *et al.* [190] (QSW) based on a quadratic spline wavelet transform. Both feature extraction techniques generate an iris-code $IC$, which consists of of $B$=512×10=5,120 bits. Figure 10.7 illustrates the described processing chain for a sample iris image. Custom implementations of employed segmentation and feature extractors are freely available in the University of Salzburg Iris Toolkit (USIT) [281]. For further details on the employed feature extraction algorithms the reader is referred to [247]. Note that a compression of iris-codes, e.g. to 2,048 bits as suggested in [69], might cause a decrease in biometric performance [108], especially in challenging unconstrained scenarios.

### Iris-Code Comparison

In the comparison stage circular bit shifts are applied to iris-codes and $HD$ scores are estimated at $K$ different shifting positions, i.e. relative tilt angles. In the used scheme a 1-bit shift equals 0.7° of rotation. Let $f(IC, i)$ denote an iris-code shifted by $i$ bits. Assuming that blocks of $L$ bits are processed at a time, the final comparison score between a query and a reference iris-code, $IC_Q$ and $IC_R$, and their corresponding noise

masks, $M_Q$ and $M_R$, is estimated as:

$$\min_{i \in K} \frac{\sum_{j=1}^{B/L} \|(IC_{Q_j} \oplus f(IC_R, i)_j) \cap M_{Q_j} \cap f(M_R, i)_j\|}{\sum_{j=1}^{B/L} \|M_{Q_j} \cap f(M_R, i)_j\|}. \tag{10.1}$$

Since iris-codes can be shifted prior to comparison and only a single division is required, the workload for calculating scores between iris-codes is dominated by the following three (per-block) processing steps:

1. *XOR:* the exclusive or ($\oplus$) detects disagreeing bits between two $L$-bit blocks, resulting in bit block of same size where 1s indicate differing bits.
2. *POPCNT:* the population count ($\|\cdot\|$), or Hamming weight, counts the number of 1s in the vector extracted in the first step, i.e. the amount of detected differences.
3. *ADD:* the amount of disagreeing bits is added up ($\sum$) for all $L$-bit blocks.

Of these processing steps, *POPCNT* represents the most complex one and most of presented software-based optimisations will focus on speeding up its calculation (see section 10.3.5). Nevertheless, the other two steps are also analysed where appropriate.

### 10.3.5. Software-based Optimisations

From a practical point of view, seven settings were identified as most relevant, *S-1* to *S-7*, which are described in the following subsections.

#### Look-up Tables, Intrinsics and Loop-Unrolling

*Look-up table (S-1):* the population count of $L = 8$ bit blocks is stored in a pre-computed look-up table. An 8-bit look-up table has a small memory footprint (256 byte) and is universally applicable in contrast to a register-sized look-up table, e.g. 64-bit (∼16.7 million terabyte), which is far too big even for common memory sizes in the foreseeable future. For the *XOR* and *ADD* step common arithmetics are used.

*Hardware POPCNT (S-2):* intrinsics are used to calculate the population count with the SSE4 *POPCNT* CPU instruction. Experiments are performed in 32-bit and 64-bit operation mode.

*Assembler POPCNT (S-3):* instead of high level intrinsics the *POPCNT* command is directly invoked via inline assembler code in a C++ function.

*Manual loop-unrolling (S-4):* even though loop-unrolling is activated for the compiler, this experiment measures the impact on the overall duration regarding the (manually adjusted) number of bit blocks processed per loop iteration.

*SSE2 and AVX (S-5): (S-5)* also considers calculating *XOR* for 128-bit blocks with the Streaming SIMD Extensions 2 (SSE2) instruction *PXOR*, the Advanced Vector Extensions (AVX) 256-bit equivalents *VXORPD*, the AVX2 256-bit version *VPXORPD* and measure the impact of addition trees using the AVX2 8-bit and 16-bit vectoring commands *VPADDB* and *VPADDW*. The latter operations can add 32 8-bit packed integers and 16 16-bit packed integers with one operation, respectively.

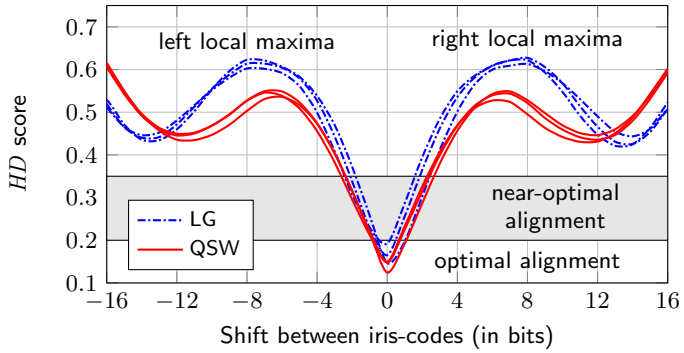



Figure 10.8.: Sample HD-scores obtained from three genuine pairs of iris-codes at various shifting positions.

#### Multithreading and Statistical Micro-Ops Optimisation

*Multithreading (S-6):* iris-code comparisons are split upon multiple threads. Like in the previous settings, *S-2* to *S-5*, *POPCNT* and *ADD* operations are performed alternatingly (*PAPA*). First a given query iris-code is compared to all pre-shifted versions of stored reference iris-codes. Hence, no shifting operations have to be performed at the time of comparison, while storage requirement, which is usually not a crucial factor, increases. In an alternative implementation the *query* iris-code is shifted prior to comparison against all stored non-shifted *reference* iris-codes. Both settings, which are referred to as $PAPA_R$ and $PAPA_Q$, describe the same transposed algorithm and result in the same amount of bit comparisons.

*Statistical micro-ops optimisation (S-7):* static data dependency, latency and throughput analysis are utilised to minimise latencies of micro-operations. The resulting strategies, which are referred to as $PPAA_R$ and $PPAA_Q$, perform all *POPCNT* operations first and add up all intermediate results afterwards.

### 10.3.6. Accelerated Accuracy-preserving Alignment

The following subsections present an analysis of *HD* scores estimated from genuine iris-code comparisons across various shifting positions, which motivates the adjustable two-step search-procedure, referred to as *TripleA* [246].

#### Iris-Code Analysis

For both feature extractors figure 10.8 shows the *HD* scores across different shifting positions for three genuine comparisons of iris-codes. It can be seen that, for each feature extraction algorithm the *HD* scores of the three genuine comparisons seem almost identical. Within a certain range *HD* scores constantly decrease towards the minimum (best) score. This range is enclosed by local maxima resulting in *HD* scores significantly beyond 0.5. For the sample *HD* scores in Figure 10.8 these local maxima can be detected

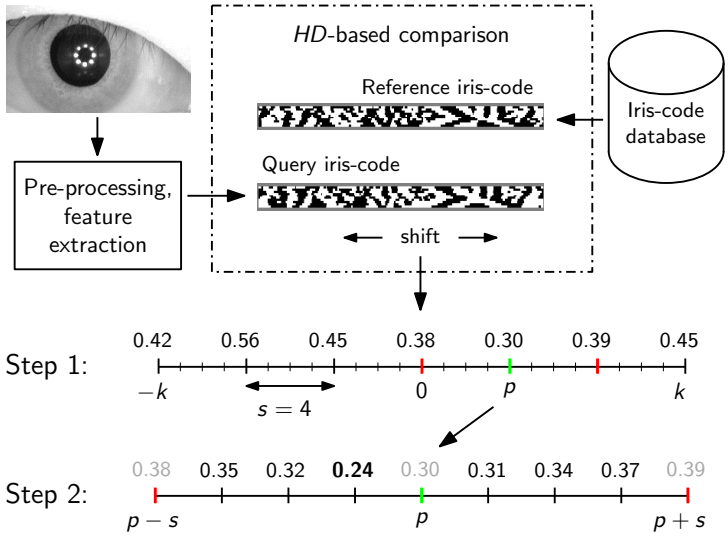



Figure 10.9.: Example of the *TripleA* procedure: In the first step comparisons between a query and reference iris-code are performed at $2\lceil k/s \rceil + 1 = 7$ positions according to the reference's step size $s = 4$. After detecting the near-optimal shifting position $p = 4$, the final score (marked bold) is detected in the interval $[p - s + 1 = 1; p + s - 1 = 7]$ at a shifting position of 3. *HD* scores are estimated at a total number of 13 shifting positions compared to $K = 25$ in a linear search [246].

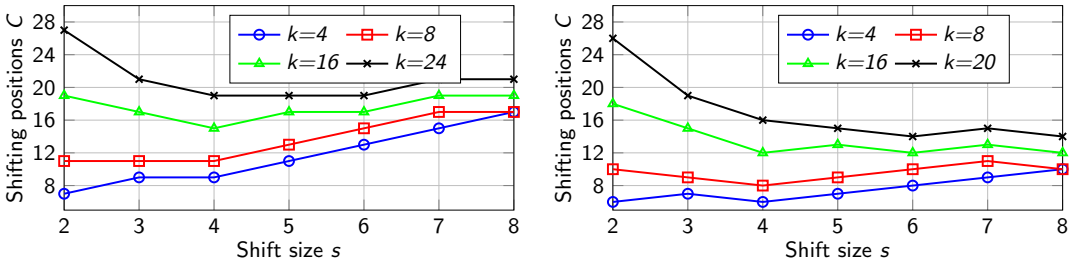
at shifting positions of ±8 bits for LG and ±6 bits for QSW. A detailed analysis of this phenomenon is provided in [246].

Intuitively, the distance between the shifting position resulting in a minimum *HD* score and those of surrounding local *HD* score maxima might be approximated by the average length of 1-bit and 0-bit sequences $\mu$, as $\pm\mu$ bit shifts are expected to cause the most drastic misalignment. The sequence of *HD* scores between genuine iris-codes across various shifting positions might be interpreted as an oscillation which decreases its amplitude with the distance to the minimum score. For such a signal it can be empirically verified that distances between consecutive vertices are virtually the same for a constant value of $\mu$ even in case of large standard deviations.

### TripleA

The *TripleA* approach [246] comprises the following two key steps: (1) estimation of near-optimal alignment and (2) estimation of subset-minimum. An example of the approach is illustrated in figure 10.9.

In the first step the range of $K = 2k+1$ shifting positions $[-k; k]$ is divided into $2\lceil k/s \rceil$ intervals, where $s$ denotes the employed *step-size*. Then *HD* scores are estimated at interval boundaries, i.e. for a subset of $2\lceil k/s \rceil + 1$ shifting positions. In other words, the




(a) *TripleA* (b) *TripleA-SS*

Figure 10.10.: Number of shifting positions to be considered $C$ using *TripleA* and *TripleA-SS* for different values of $k$ and $s$.

sequence of scores, interpreted as signal, is sampled every $s$ bits. For a genuine comparison a sampling with at most the average length of 1-bit and 0-bit sequences, $s < \mu$, is expected to detect a minimum score which represents a near-optimal alignment. In this work an alignment is considered as near-optimal if the corresponding shifting position is close enough to the optimal alignment revealing a *HD* score, which is significantly smaller compared to remaining sampling positions. For the sample comparisons of Figure 10.8 near-optimal alignments would be found in the range of approximately $\pm 2$ bit shifts.

After detecting a near-optimal alignment at shifting position $p$ the interval $[p - s + 1; p + s - 1]$ is considered for the second step. Note that the scores for positions $p \pm s$ have already been estimated in the first step. Based on a linear search the second step detects a minimum *HD* score for a subset of $2(s-1)$ shifting positions. That is, the number of shifting positions to be considered is reduced to $C = 2\lceil k/s \rceil + 1 + 2(s-1)$. To further accelerate the *TripleA* alignment procedure it is suggested to process only half of the subset detected in the first step during the second step. This bisected interval is defined by $p$ and minimum of surrounding *HD* scores at $p \pm s$. Hence, the number of shifting positions is further reduced to $C = 2\lceil k/s \rceil + s$. In the example of figure 10.9 the interval $[p - s + 1, p - 1]$ would be chosen for the linear search of the second step, since the *HD* score at shifting position $p - s$ is smaller than that at $p + s$. This derivation is referred to as *TripleA-Single-Sided*. In figure 10.10 the number of shifting positions $C$ is plotted for different values of $k$ and $s$. To obtain a maximum speed-up $C$ has to be minimised, such that $s = \sqrt{2k}/\sqrt{2}$ and $s = \sqrt{2k}$ represent the theoretical optimal step-size in terms of speed-up for *TripleA* and *TripleA-SS*, respectively.

In [246] it was shown that, $\mu$ can be dynamically estimated from a single reference iris-code during enrolment, however, this dynamic estimation was not found to yield any significant gains in terms of performance are obtained. Hence, this work restricts itself to applying static values of $s$ for each comparison performed by the system. In this case $\mu$ can be averaged from a training set of extracted iris-codes.

### 10.3.7. Hamming Distance Experiments

The following subsections describe the experimental setup and summarise results obtained by the presented approaches.

#### Experimental Setup and Methodology

Experimental evaluations are carried out on the CASIAv4-Interval iris database [60]. The database consists of $N$=2,639 good-quality 320×280 pixel NIR iris images of 249 subjects. This work considers two types of experiments, where in both experiments an iris-code is compared against $K$ shifted versions of another one:

*Experiment 1 (E-1):* the maximum number of $N(N-1)/2 = 3,480,841$ iris-code cross-comparisons is performed. Based on obtained scores it is identified an adequate trade-off between biometric performance and provided rotation compensation. Subsequently, diverse settings with the aim of accelerating these iris-code cross-comparisons are compared and the best setting is identified. For time measurements a total number of 40 iterations is executed and the obtained median time elapsed is reported. The considered number of iterations minimises the influence of outliers with respect to time measurements, which assures significance of relative improvements or degradations in comparison speed. This experiment might reflect a de-duplication check on an iris-code database with $N$ registered subjects.

*Experiment 2 (E-2):* the dataset is partitioned into a reference set of 2,500 iris-codes and a query set of 139 iris-codes. To simulate identification attempts on a large-scale database the reference set is extended to a large-scale dataset by replicating the subset 20,000 times, resulting in a set of $N$=2,500×20,000=50,000,000 iris-codes. Note that the obtained set is used for runtime experiments only. For the best setting of *E-1*, in terms of throughput, all 139 identification attempts (1:$N$) are performed and the obtained median time elapsed is reported for various degrees of rotation compensation. Subsequently, the *TripleA* method is applied with different parameter configurations on top of the best setting of *E-1* in order to obtain further speed-ups.

The main difference between these experiments is that, while in *E-1*, the de-duplication experiment, a total number of $N$ query iris-codes are successively compared against the database, in *E-2*, the identification experiment, a single query iris-code is compared against a huge database.

Biometric performance is estimated in terms of FNMR at a target false match rate (FMR) and equal error rate (EER) obtained from *E-1*. The test system for measuring the duration of *E-1* and *E-2* with different settings uses an x86_64 Linux operating system with kernel version 4.4 and GCC 5.3.0 as C++ compiler. While other CPU-types, e.g. ARM-based, have been analysed with respect to the required operations [265], focusing on large-scale biometric systems x86_64 hardware is considered as most relevant. The utilised CPU is an Intel Core i7-6700 with sufficient DDR4-SDRAM 2133.

In order to identify an appropriate degree of rotation compensation in *E-1*, this work first calculates EERs and FNMRs at a FMR of 0.01%, denoted as $\text{FNMR}_{0.01}$, considering $\pm k$ shifting positions during alignment. The progress in terms of EER and $\text{FNMR}_{0.01}$

Table 10.6.: Progression of EERs and $FNMR_{0.01}$s in relation to rotation compensation (the selected setting for the used iris recognition system is marked bold).

| Rot. comp. | LG | | QSW | |
|---|---|---|---|---|
| $\pm k$ bits | EER | $FNMR_{0.01}$ | EER | $FNMR_{0.01}$ |
| 0 | 6.81 | 11.98 | 16.14 | 20.35 |
| 1 | 5.65 | 10.73 | 11.51 | 15.12 |
| 2 | 5.01 | 10.18 | 8.22 | 11.33 |
| 4 | 2.78 | 9.89 | 3.03 | 6.24 |
| 8 | 1.04 | 2.26 | 0.94 | 1.46 |
| 12 | 1.01 | 2.23 | 0.79 | 1.28 |
| **16** | **0.80** | **1.75** | **0.74** | **1.06** |
| 20 | 0.80 | 1.75 | 0.73 | 1.05 |
| 24 | 0.79 | 1.71 | 0.70 | 1.01 |

with respect to rotation compensation is shown in Table 10.6. As can be seen, the majority of misalignments is compensated by ±8 bit shifts (∼6°) while biometric performance converges at approximately ±16 bit shifts (∼11°). Focusing on recognition accuracy versus required bit-shifting $k = \pm 16$ is chosen, resulting in $2k + 1 = 33$ shifting positions, is considered as reasonable trade-off for the used iris recognition systems resulting in an EER of 0.80% and a $FNMR_{0.01}$ of 1.75% for LG and an EER of 0.74% and a $FNMR_{0.01}$ of 1.06% for QSW.

#### Software-based Optimisations

Table 10.7 summarises time measurements for all settings in experiment *E-1*. Since time measurements might highly depend on hardware components of a system, emphasis should be placed on relative improvements obtained by according optimisation techniques. Optimal parameters of each setting are preserved in subsequent settings where appropriate.

With over two minutes runtime the 8-bit look-up table of *S-1* turns out to be by far the slowest implementation. Nevertheless, it represents a baseline for a hardware independent implementation.

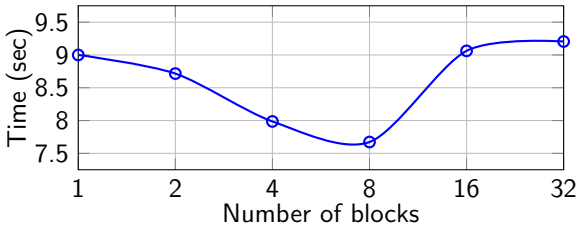
Without any optimisation the 32-bit population count implementation in *S-2*, using intrinsics to invoke the SSE4 *POPCNT* instruction provides a tenfold speed-up compared to *S-1*. The 64-bit version can double the data processing per instruction and is therefore even faster. It is not twice as fast as the 32-bit implementation due to overhead of the bigger 64-bit address handling for data access and pointer dereferencing. Based on this observation subsequent settings process blocks of $L = 64$ bits.

The inline assembler of *S-3* also provides a clear speed-up over high level *POPCNT* intrinsic calls used in *S-2*.

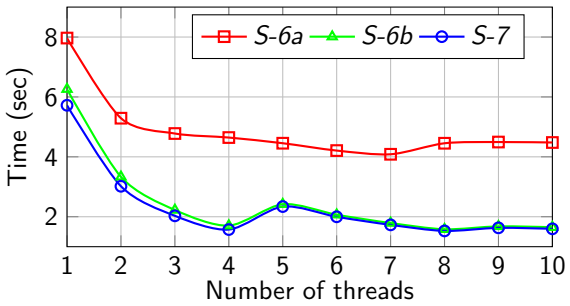
Focusing on *S-4*, figure 10.11(a) shows that the preferred number of $L$-bit blocks processed per loop iteration is 8. The analysis identifies two reasons to justify this behaviour: on the one hand, 8 64-bit blocks fit very well in the general purpose registers

Table 10.7.: Overview of time measurements (in seconds) obtained for different settings in experiment *E-1* performing all 3,480,841 iris-code cross-comparisons at 33 shifting positions.

| Setting | | Time | Setting | | Time |
|---|---|---|---|---|---|
| ID | Description | | ID | Description | |
| S-1 | 8-bit Look-up table | 157.95 | S-6a | 3 Threads $PAPA_R$ | 4.78 |
| S-2 | POPCNT 32-bit | 14.98 | | 4 Threads $PAPA_R$ | 4.62 |
| | POPCNT 64-bit | 9.16 | | 5 Threads $PAPA_R$ | 4.46 |
| S-3 | POPCNT ASM | 8.16 | | 6 Threads $PAPA_R$ | 4.21 |
| S-4 | 2 Blocks | 8.71 | | 7 Threads $PAPA_R$ | 4.09 |
| | 4 Blocks | 7.98 | | 8 Threads $PAPA_R$ | 4.45 |
| | 8 Blocks | 7.65 | | 9 Threads $PAPA_R$ | 4.50 |
| | 10 Blocks | 9.54 | | 10 Threads $PAPA_R$ | 4.47 |
| | 16 Blocks | 9.05 | S-6b | 1 Thread $PAPA_Q$ | 6.24 |
| | 32 Blocks | 9.21 | | 2 Threads $PAPA_Q$ | 3.33 |
| S-5a | 2 Blocks SSE2 | 12.08 | | 3 Threads $PAPA_Q$ | 2.21 |
| | 4 Blocks SSE2 | 12.43 | | 4 Threads $PAPA_Q$ | 1.70 |
| | 8 Blocks SSE2 | 10.26 | | 5 Threads $PAPA_Q$ | 2.42 |
| | 16 Blocks SSE2 | 9.37 | | 6 Threads $PAPA_Q$ | 2.06 |
| | 32 Blocks SSE2 | 8.33 | | 7 Threads $PAPA_Q$ | 1.79 |
| S-5b | 4 Blocks AVX | 10.76 | | 8 Threads $PAPA_Q$ | 1.58 |
| | 8 Blocks AVX | 12.34 | | 9 Threads $PAPA_Q$ | 1.68 |
| | 16 Blocks AVX | 8.01 | | 10 Threads $PAPA_Q$ | 1.65 |
| | 32 Blocks AVX | 8.05 | S-7 | 1 Thread $PPAA_Q$ | 5.73 |
| S-5c | 4 Blocks AVX2 | 11.90 | | 2 Threads $PPAA_Q$ | 3.02 |
| | 8 Blocks AVX2 | 12.32 | | 3 Threads $PPAA_Q$ | 2.03 |
| | 16 Blocks AVX2 | 8.00 | | 4 Threads $PPAA_Q$ | 1.57 |
| | 32 Blocks AVX2 | 8.06 | | 5 Threads $PPAA_Q$ | 2.33 |
| S-5d | AVX2 8-bit ADD | 9.63 | | 6 Threads $PPAA_Q$ | 1.99 |
| | AVX2 16-bit ADD | 9.32 | | 7 Threads $PPAA_Q$ | 1.72 |
| S-5e | SSSE3 | 20.66 | | 8 Threads $PPAA_Q$ | 1.54 |
| S-6a | 1 Thread $PAPA_R$ | 7.96 | | 9 Threads $PPAA_Q$ | 1.63 |
| | 2 Threads $PAPA_R$ | 5.31 | | 10 Threads $PPAA_Q$ | 1.58 |




(a) S-4




(b) S-6 and S-7

Figure 10.11.: Time measurements (in seconds) obtained for (a) setting *S-4* and (b) settings *S-6* and *S-7* in experiment *E-1* performing all 3,480,841 iris-code cross-comparisons at 33 shifting positions.

of the x86_64 processor and no memory access is needed for the *XOR*, *POPCNT*, *ADD* operation, see figure 10.12(b) lines 20-36; on the other hand, $8 \times 64$ bit are exactly 64 byte which is the same size as one CPU cache line. Since a cache line copied from memory is exactly 64 byte it is preferable to process the complete cache line resulting in a favourable cache hit/miss ratio. It is therefore recommended to process the data in 64 byte blocks and storing it as a continuous array for an optimal exploitation of the CPU caches. Hence, in settings *S-6* and *S-7* a total number of 8 64-bit blocks are processed per loop iteration.

Settings *S-5a*, *S-5b* and *S-5c* make use of SSE2, AVX and AVX2 instructions to process bigger data chunks with the *XOR* operation. However, no significant speed-up over the common x86 64-bit *XOR* instruction is obtained. The reason for this is very straightforward, since SSE works on specific registers, the so called 128-bit XMM registers and AVX on the 256-bit YMM registers. Data has to be loaded to and retrieved from these registers before it can be used with SSE/AVX instructions. In contrast, the SSE4 *POPCNT* command operates on 64-bit general purpose registers of a CPU. Therefore, a transfer between these registers is necessary where the overhead for these transfers is higher than a straightforward processing by the common *XOR* command which operates on the same registers as the *POPCNT* instruction. SSE and AVX are optimised for algorithms which do a lot of operations on a comparably low amount data. Calculating a great amount of iris-code comparisons, which requires only very few operations on extreme amounts of data, is no such problem. Settings *S-5d* and *S-5e*, which

```
buf[0]=ic[x].dat[k][i]^ic[y].dat[i];
buf[1]=ic[x].dat[k][i+1]^ic[y].dat[i+1];
buf[2]=ic[x].dat[k][i+2]^ic[y].dat[i+2];
buf[3]=ic[x].dat[k][i+3]^ic[y].dat[i+3];
buf[4]=ic[x].dat[k][i+4]^ic[y].dat[i+4];
buf[5]=ic[x].dat[k][i+5]^ic[y].dat[i+5];
buf[6]=ic[x].dat[k][i+6]^ic[y].dat[i+6];
buf[7]=ic[x].dat[k][i+7]^ic[y].dat[i+7];

asm(".intel_syntax noprefix\n");

__asm__(
"popcnt %1, %1  \n\t"
"popcnt %2, %2  \n\t"
"popcnt %3, %3  \n\t"
"popcnt %4, %4  \n\t"
"popcnt %5, %5  \n\t"
"popcnt %6, %6  \n\t"
"popcnt %7, %7  \n\t"
"popcnt %8, %8  \n\t"

"add %0, %1     \n\t"
"add %0, %2     \n\t"
"add %0, %3     \n\t"
"add %0, %4     \n\t"
"add %0, %5     \n\t"
"add %0, %6     \n\t"
"add %0, %7     \n\t"
"add %0, %8     \n\t"

: "+r" (dist)
: "r" (buf[0]), "r" (buf[1]),
: "r" (buf[2]), "r" (buf[3]),
: "r" (buf[4]), "r" (buf[5]),
: "r" (buf[6]), "r" (buf[7])
);
```

(a) C++ / Inline ASM

```
prefetcht0 ptr [r13+r11*1]
prefetcht0 ptr [r13]
xor edi, edi ; XOR
mov rax, qword ptr [r12]
mov rdx, qword ptr [r12+0x8]
xor rax, qword ptr [r13-0x138]
xor rdx, qword ptr [r13-0x130]
mov rcx, qword ptr [r12+0x10]
mov r8, qword ptr [r12+0x18]
xor rcx, qword ptr [r13-0x128]
xor r8, qword ptr [r13-0x120]
mov r9, qword ptr [r12+0x20]
mov r10, qword ptr [r12+0x28]
xor r9, qword ptr [r13-0x118]
xor r10, qword ptr [r13-0x110]
mov rbx, qword ptr [r12+0x30]
mov rsi, qword ptr [r12+0x38]
xor rbx, qword ptr [r13-0x108]
xor rsi, qword ptr [r13-0x100]
popcnt rax, rax ; POPCNT
popcnt rdx, rdx
popcnt rcx, rcx
popcnt r8, r8
popcnt r9, r9
popcnt r10, r10
popcnt rbx, rbx
popcnt rsi, rsi
add rdi, rax ; ADD
add rdi, rdx
add rdi, rcx
add rdi, r8
add rdi, r9
add rdi, r10
add rdi, rbx
add rdi, rsi
mov rcx, rdi ; final result
```

(b) ASM

Figure 10.12.: Comparison between (a) C++ code using Inline Assembler and (b) corresponding Assembler code for setting *S-7*.

implement the AVX2 vector addition, are slower for the same reasons. Note that the SSSE3 implementation tested in *S-5e* is considered the fasted *POPCNT* implementation by experts in the field [210]. In contrast, it is observed that the hardware *POPCNT* instruction used in *S-2* to *S-4*, is clearly superior to the SSSE3 implementation. Still, for older CPUs where no *POPCNT* instruction is available, this could still be of interest since it is faster than an 8-bit look-up table.

The common idea to compare a freshly extracted query iris-code to a large pre-shifted database of reference iris-codes is represented in *S-6a*. As shown in figure 10.11(b) for 1 to 3 threads this setting behaves as expected, but starting from 4 threads the runtime stagnates at roughly 4 seconds, i.e. dividing the workload in more threads provides no further speed-up. As one iris-code consists of 512×20 bits (1280 byte), 3,480,841 comparisons have to be performed and for each comparison a new iris-code has to be loaded from memory, resulting in roughly 137 GB of data transferred from memory to the CPU. The experiment computer uses DDR4-2133 RAM with a speed of 17.0 GB/s per channel according to specification [166]. The experiment uses a common dual channel setup and, hence has a maximum RAM bandwidth of 34 GB/s. Hence, transferring 137 GB from memory to CPU takes at least 4 seconds. In this setup the execution speed of the implemented algorithm is interfered by the relatively slow RAM to CPU interface. The RAM as bottleneck is a common problem for highly multithreaded tasks

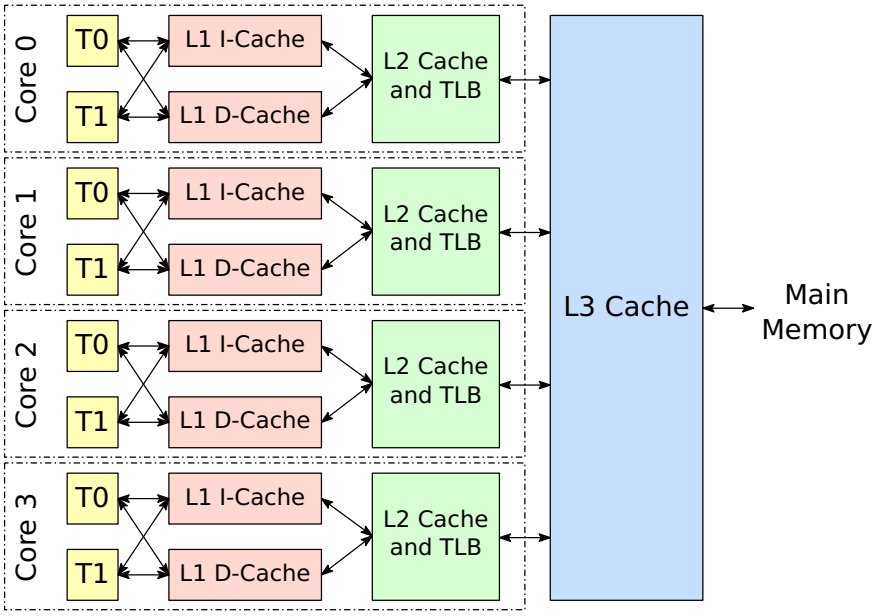



Figure 10.13.: Cache hierarchy of the Intel Core i7-6700 CPU in the employed test system [151].

performing a few operations on a big amount of data [121]. The bottleneck gets enhanced by the fact that this biometric scenario floods the CPU caches with all new data and is practically not using them at all, resulting in a very poor cache hit/miss ratio. In *S-6b* $K$ shifted versions of the given query iris-code are computed and compared to $N$ non-shifted reference iris-codes of the database. From a computational perspective, this setup seems less intuitive because the shifted versions have to be computed before the actual comparison can start, but the $K$ iris-codes can stay in the CPU caches across all comparisons and only one 1,280 byte block has to be loaded for each comparison, resulting in much less actual memory access since the CPU caches have a high hit count for the shifted iris-codes [151]. Therefore, *S-6b* scales much better with multiple threads as highlighted in figure 10.11(b). Hence, the subsequent setting will be based on this strategy. Moreover, in *S-6b* the effect that 5 threads are actually slower than 4 threads is observed. The Intel Core i7-6700 processor used has 4 physical cores of which each can process 2 threads at once due to hyper threading [192]. As depicted in figure 10.13, in case 5 threads are used 2 threads have to share the L1 and L2 cache on one core. Therefore, the iris-code prefetching, see figure 10.12(b) lines 1-2, is not as effective as if one thread uses the complete cache. This effect occurs since both threads are working on completely independent parts of the iris-code database. Due to this aspect 8 threads are only negligibly faster than 4 threads.

Setting *S-7* implements the results obtained by the Intel Architecture Code Analyzer [124] which suggests the *PPAA* strategy instead of the *PAPA* strategy of previous settings (see section 10.3.5), as shown in figure 10.12. As can be seen in Table 10.7 and

Table 10.8.: EERs and $FNMR_{0.01}$ for different settings of *TripleA* for the LG and QSW feature extraction (LG baseline: EER=0.80%, $FNMR_{0.01}$=1.75%; QSW baseline: EER=0.74%, $FNMR_{0.01}$=1.06%).

| Step size | *TripleA* | | | | *TripleA-SS* | | | |
|---|---|---|---|---|---|---|---|---|
| | LG | | QSW | | LG | | QSW | |
| | EER | $FNMR_{0.01}$ | EER | $FNMR_{0.01}$ | EER | $FNMR_{0.01}$ | EER | $FNMR_{0.01}$ |
| 2 | 0.80 | 1.75 | 0.74 | 1.05 | 0.80 | 1.75 | 0.74 | 1.05 |
| 3 | 0.79 | 1.75 | 0.74 | 1.06 | 0.80 | 1.75 | 0.74 | 1.06 |
| 4 | 0.80 | 1.78 | 0.77 | 1.14 | 0.80 | 1.78 | 0.77 | 1.14 |
| 5 | 0.78 | 1.76 | 0.77 | 1.10 | 0.81 | 1.78 | 0.77 | 1.13 |
| 6 | 0.88 | 2.70 | 0.80 | 1.31 | 1.09 | 4.08 | 0.91 | 1.70 |
| 7 | 0.82 | 1.98 | 1.58 | 2.07 | 0.92 | 2.80 | 3.91 | 7.79 |
| 8 | 0.80 | 1.75 | 0.89 | 1.29 | 0.82 | 1.84 | 1.73 | 5.43 |

figure 10.11(b), this results in minor speed-up which would be more significant for larger databases. That is, optimising the order of the instruction sequence for the used microarchitecture by a static code analyser can still improve the overall performance even in case modern CPUs support out-of-order execution, which should (in theory) do this automatically.

The presented results are obtained using a Linux operating system. It is important to note that identical performance rates are achieved on other types of operating systems (OS), since basic memory operations, in particular cache management, is independent of the used OS.

### Accelerated Accuracy-preserving Alignment

For different configurations of *TripleA* using static step-sizes, Table 10.8 summarises obtained EERs and $FNMR_{0.01}$s. Regarding the general approach it can be observed that biometric performance is maintained across most step-size settings. In case of both feature extractors the *TripleA-SS* approach causes no drastic decrease in accuracy while providing further speed-up as will be shown in the following subsection.

### Simulation of Large Scale Identification

For *E-2* a large scale identification scenario, the best setting $PPAA_Q$ resulting from *E-1* is selected as baseline. Figure 10.14 presents the absolute number of iris-code comparisons per second. Again, emphasis should be placed on relative difference in throughput rates of different configurations. Due to the efficient CPU caches the comparisons per second depend on how well the shifted iris-codes fit into the caches and the break even point from 4 to 5 threads, can similarly be observed as in the $1 : N$ identification scenario, due to 2 threads sharing one cache. Therefore, having 8 threads reveals no significant speed-up over 4 threads. Both setups roughly compare 4.6 million iris-codes per second using $\pm 8$ bit shifts ($\simeq$ 80 million comparisons per second without shifting).

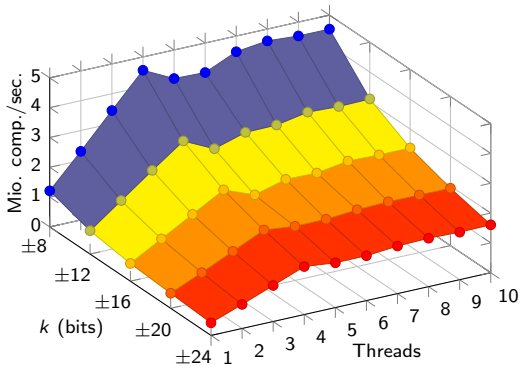



Figure 10.14.: Throughput (in millions of iris-code comparisons per second) in *E-2* in relation to shift size and number of threads.

Table 10.9.: Overview of time measurements (in seconds) for different settings in experiments *E-2* performing an identification with $N = 50,000,000$ at 33 shifting positions using $s = 4$.

| Method | Number of threads | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Baseline | 84.10 | 42.24 | 28.21 | 21.17 | 25.52 | 22.24 | 22.49 | 20.89 | 21.13 | 21.13 |
| *TripleA* | 34.36 | 18.04 | 12.15 | 9.26 | 10.06 | 9.64 | 9.64 | 9.03 | 9.26 | 9.26 |
| *TripleA-SS* | 30.65 | 16.40 | 11.03 | 8.37 | 9.65 | 8.82 | 8.69 | 8.26 | 8.37 | 8.32 |

Based on the findings depicted in Table 10.6 and Table 10.8 further scenarios in *E-2* utilising *TripleA* and *TripleA-SS* are performed with the parameters $k = 16$, $s = 4$ as step-size and $\text{PPAA}_Q$ as core *HD* score comparator. These experiment results are summarised in Table 10.9 and depicted in figure 10.15.

From a theoretical standpoint the expected speed-up can be approximated by comparing the number of shifted iris-code comparisons to the baseline algorithm $\text{PPAA}_Q$. The baseline algorithm has to process all $K$ shifting positions, resulting in 33 comparisons. *TripleA* with the selected parameters does 9 comparisons in Step 1 and in general 6 more in Step 2. In the special case of Step 1 yielding $-k$ or $k$ as result only 3 comparisons are performed in Step 2. This is considered negligible for an approximation and *TripleA* is considered performing 15 comparisons per iris-code. The special case of *TripleA* is the regular case of *TripleA-SS* since only a single side is considered during Step 2. Therefore, the baseline does 33 comparisons, *TripleA* 15 comparisons and *TripleA-SS* 12 comparisons, which results in an approximation of *TripleA* taking 45% and *TripleA-SS* only 36% of the time compared to the baseline. These theoretical considerations match the observed results in Table 10.9 taking measuring tolerance into account. It means in effect *TripleA* and *TripleA-SS* scale linearly to the number of comparisons relative to the baseline algorithm $\text{PPAA}_Q$ and all further $k$ and $s$ combinations can be effectively

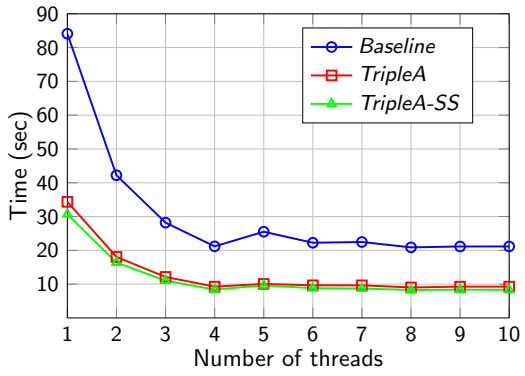



Figure 10.15.: Illustration of time measurements (in seconds) for different settings in experiments *E-2* performing an identification with $N = 50,000,000$ at 33 shifting positions using $s = 4$.

approximated using the results from *E-2*. figure 10.15 further depicts that *TripleA* and *TripleA-SS* yield no further anomalies that were not present in the $\text{PPAA}_Q$ baseline algorithm.

### 10.3.8. Hamming Distance Conclusions

This section analysed commodity hardware-based iris recognition systems, which perform a CPU-based exhaustive comparison on a large-scale database. The experiments showed that utilising the *POPCNT* hardware instruction can significantly speed up biometric comparisons based on the Hamming distance. It was identified that taking the CPU caches into consideration during the algorithm design is the most efficient way to circumvent potential RAM bottlenecks. Especially when making use of multithreading ignoring these caches will lead to bottlenecks and even make the actual comparison algorithm secondary since the greatest share of time is claimed by the RAM to CPU data transfer and not the actual execution of the algorithm. This observation also impacts the reflection of iris-code comparisons based on GPGPU/CUDA since their speed-up is not only explained due to the high number of cores (hardware shaders), but also the higher memory bandwidth of Video RAM (GDDR) compared to common RAM (DDR). Therefore, GPGPU/CUDA implementations have to deal to a lesser extent with memory bottlenecks. Awareness of cache line sizes on the target system can also greatly improve the data throughput since it maximises cache hits, particular in hotspot loops. Taking into account the aforementioned issues, it is shown that an optimised conventional CPU-based iris-biometric comparator can achieve a hundredfold speed-up compared to a naïve baseline comparator. As the $1 : N$ results with different shifts sizes show, the number of comparisons alone is no sufficient statement, since the fitting of all shifted iris-code versions into the CPU cache is a high performance factor, independent of the actual algorithm or achieved comparisons per second. Further, the results show that by combining the *TripleA* algorithm with a fast multithreaded *POPCNT* implementation

response times of large scale biometric systems can be further decreased, achieving a more than two-hundredfold overall speed-up. Finally, it is important to point out that these findings may also be exploited in other software-based acceleration techniques, e.g., [107].

## 10.4. Biometrics Discussion

This chapter presents several areas of improvement for eMRTDs regarding biometrics. First, the entropy of common face based biometrics for linking the travel document to the document holder is not sufficient to be considered secure. Either the finger images already stored on the ePassport in DG3 must be utilised to strengthen the link or iris based systems can provide a more secure alternative. Furthermore, breeder documents (e.g., birth certificates) currently have no biometric link at all between the physical document and the document holder, which is a risk to the entire document life cycle. A cost-effective solution was found in the form of standardised 2D barcodes, which are able to store sufficient data for finger or iris recognition. Furthermore, 2D barcodes provide an easy way to make breeder documents machine-readable, which can speed up civil obligations and lower the burden for governmental staff. In contrast to a dedicated RFID chip, 2D barcodes can be integrated into breeder documents without expensive dedicated hardware costs. Naturally, a 2D barcode cannot provide the same security level as an RFID chip since it cannot perform self-contained computations. Therefore, 2D barcodes can provide a short-term solution for establishing a link between holder and breeder document, but for long-term security, further mechanisms are recommended (see section 6.8). Finally, hardware instruction set extensions can significantly improve performance of large-scale biometric applications, e.g. double enrolment checks and black list checks. Since ABC gates are becoming more and more frequent at airports, performance and security of biometric verifications and identifications should be considered regarding the presented results.

# Part IV.

# Conclusion

# 11. Conclusion

Multiple shortcomings of the identity life cycle, breeder documents, and electronic travel documents were analysed, and solutions assessed and discussed. This section summarises the proposed enhancements regarding future travel document infrastructure and protocols, illustrates their impact on forthcoming applications, and future work.

The proposed breeder document blockchain concept demonstrates that blockchain technology in the context of Bitcoin can indeed provide a strengthening of breeder document's long-term data authenticity and integrity in the identity life cycle. It grants a direct enhancement to the security of today's birth certificates by a pure software rollout, without establishment of an expensive separated infrastructure or severe extra hardware costs. Long-term, the concept grants one important building block to enhance the overall breeder document verification process security to make fraud and identity theft a tougher obstacle.

In context of eMRTD's data transfer rates are very slow, therefore, reducing data transfers by consolidating multiple security goals into one security protocol for reduced round-trip times has a positive impact on the border control throughput times, which all discussed protocols fulfil. Furthermore, adding chip cloning as an inexpensive mandatory step should be part of future eMRTD protocols. BioPACE v2 uses implicit on chip comparison of the biometric data, provides stronger data privacy, and does not require EAC with the Verifying PKI. Accordingly, the AFIS blacklist with BioPACE v2 can fully replace the EAC protocols, the protected DG3 fingerprints and the Verifying PKI. Since as of today EAC is not deployed at airports BioPACE v2 would not be a replacement, but a supplement for a stronger link between document and the document holder. The discussed protocols provide a foundation for the next eMRTD protocols for the future generation of eMRTD's.

Multiple thoroughly investigated Internet domain solution candidates to introduce a revocation mechanism to the Verifying PKI were discussed regarding practical feasibility, respectively. The recommended solution for Verifying PKI revocation is NTP+OCSP. Nevertheless, revocation for the Verifying PKI is only reasonable if EAC is actually used during border control. Since as of today this is not the case, BioPACE v2 is a viable alternative.

Upcoming eMRTD security protocols are expected to utilise cryptographic building blocks resisting quantum computer attacks. Digital signature schemes shall be based on hash-based cryptography, namely either XMSS-T or SPHINCS. On the one hand, XMSS-T has short stateful signatures and fast key generation times, but on the other hand, SPHINCS has the benefit of being stateless with the price of much larger signatures. For key agreement between eMRTD and terminal code-based cryptography, specifically the McEliece scheme with either Goppa codes or QC-MDPC codes, provides

a post-quantum secure solution. QC-MDPC codes result in much smaller public key sizes in contrast to Goppa codes, but are currently not well enough researched to give a recommendation for a travel document. On the one hand, for future eMRTDs in the case of XMSS-T or SPHINCS it is hard to predict if the signature scheme's statefulness or bigger signatures are a tougher technical obstacle. On the other hand, future security analysis of the more attractive QC-MDPC codes over Goppa codes is hard to predict as well. Therefore, the recommendation is to utilise a high-level mechanism similar to the TLS cipher suites, which provide a soft approach for introduction of post-quantum resistant schemes into future eMRTDs.

Linking a travel document and its holder solely on low entropy face based biometrics is not sufficient and should be supplemented by either the finger images already stored on the ePassport in DG3 or iris based biometrics. Breeder documents need a biometric link between the physical document and the document holder, hence a cost-effective solution was found in the form of standardised 2D barcodes to store biometric data. On the one hand, 2D barcodes provide an easy way to make breeder documents machine-readable to speed up governmental processes. On the other hand, 2D barcodes can be integrated without expensive hardware costs. Finally, hardware instruction set extensions can significantly improve performance of large-scale Biometric applications, e.g. double enrolment checks and black list checks.

It was demonstrated that multiple enhancements for electronic machine readable travel documents are achievable due to advances in security protocols and infrastructure to strengthen the overall trust in the identity life cycle. The next generation of breeder documents and electronic travel documents can directly benefit from the proposed measures. Future work can focus on prototyping, practical application, and more fine-grained testing in the field of the introduced procedures. Overall, the concrete enhancements have the potential and may eventually lead to a next generation identity cycle and more secure electronic travel documents.

# Bibliography


[1] A. Adler, R. Youmaran, and S. Loyka. Towards a measure of biometric information. In *Proceedings of the Canadian Conference on Electrical and Computer Engineering, CCECE 2006, May 7-10, 2006, Ottawa Congress Centre, Ottawa, Canada*, pages 210–213. IEEE, 2006.

[2] A. Adler, R. Youmaran, and S. Loyka. Towards a measure of biometric feature information. *Pattern Anal. Appl.*, 12(3):261–270, 2009.

[3] Z. Akhtar, A. Rattani, A. Hadid, and M. Tistarelli. Face recognition under ageing effect: A comparative analysis. In A. Petrosino, editor, *Image Analysis and Processing - ICIAP 2013 - 17th International Conference, Naples, Italy, September 9-13, 2013, Proceedings, Part II*, volume 8157 of *Lecture Notes in Computer Science*, pages 309–318. Springer, 2013.

[4] L. Ballard, S. Kamara, F. Monrose, and M. Reiter. On the Requirements of Biometric Key Generators. *Technical Report TR-JHU-SPAR-BKMR-090707*, 2007. Submitted and available as JHU Department of Computer Science Technical Report.

[5] L. Ballard, S. Kamara, and M. K. Reiter. The practical subtleties of biometric key generation. In P. C. van Oorschot, editor, *Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA*, pages 61–74. USENIX Association, 2008.

[6] B. Barak and M. Mahmoody-Ghidary. Merkle puzzles are optimal - an $O(n^2)$-query attack on any key exchange from a random oracle. In Halevi [117], pages 374–390.

[7] P. S. L. M. Barreto, S. Gueron, T. Gueneysu, R. Misoczki, E. Persichetti, N. Sendrier, and J. Tillich. CAKE: Code-based Algorithm for Key Encapsulation. *IACR Cryptology ePrint Archive*, 2017:757, 2017.

[8] S. Beauregard. Circuit for Shor's algorithm using 2n+3 qubits. *Quantum Information & Computation*, 3(2):175–185, 2003.

[9] J. van Beek. eCLOWN. online, `http://www.dexlab.nl`, retrieved December 2017, 1 2009.

[10] M. Bellare and S. K. Miner. A forward-secure digital signature scheme. In M. J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19,*

*1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 431–448. Springer, 1999.

[11] M. Bellare and P. Rogaway. Collision-resistant hashing: Towards making uowhfs practical. In B. S. K. Jr., editor, *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, volume 1294 of *Lecture Notes in Computer Science*, pages 470–484. Springer, 1997.

[12] J. Bender, Ö. Dagdelen, M. Fischlin, and D. Kügler. The PACE|AA Protocol for Machine Readable Travel Documents, and Its Security. In A. D. Keromytis, editor, *Financial Cryptography and Data Security - 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers*, volume 7397 of *Lecture Notes in Computer Science*, pages 344–358. Springer, 2012.

[13] J. Bender, M. Fischlin, and D. Kügler. Security Analysis of the PACE Key-Agreement Protocol. In P. Samarati, M. Yung, F. Martinelli, and C. A. Ardagna, editors, *Information Security, 12th International Conference, ISC 2009, Pisa, Italy, September 7-9, 2009. Proceedings*, volume 5735 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 2009.

[14] J. Bender, M. Fischlin, and D. Kügler. The PACE|CA Protocol for Machine Readable Travel Documents. In R. Bloem and P. Lipp, editors, *Trusted Systems - 5th International Conference, INTRUST 2013, Graz, Austria, December 4-5, 2013, Proceedings*, volume 8292 of *Lecture Notes in Computer Science*, pages 17–35. Springer, 2013.

[15] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Information Theory*, 24(3):384–386, 1978.

[16] D. J. Bernstein. Grover vs. McEliece. In N. Sendrier, editor, *Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings*, volume 6061 of *Lecture Notes in Computer Science*, pages 73–80. Springer, 2010.

[17] D. J. Bernstein, J. Buchmann, and E. Dahmen, editors. *Post-Quantum Cryptography*. Springer Berlin Heidelberg, 2009.

[18] D. J. Bernstein, T. Chou, and P. Schwabe. McBits: Fast Constant-Time Code-Based Cryptography. In G. Bertoni and J. Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *Lecture Notes in Computer Science*, pages 250–272. Springer, 2013.

[19] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn. SPHINCS:

Practical Stateless Hash-Based Signatures. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 368–397. Springer, 2015.

[20] D. J. Bernstein and T. Lange. Post-quantum cryptography - dealing with the fallout of physics success. *IACR Cryptology ePrint Archive*, 2017:314, 2017.

[21] D. J. Bernstein, T. Lange, and C. Peters. Attacking and Defending the McEliece Cryptosystem. In Buchmann and Ding [37], pages 31–46.

[22] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche. Keccak. In T. Johansson and P. Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 313–314. Springer, 2013.

[23] H.-J. Bickenbach, J. Brauckmann, G. Alfred, T. Horváth, and H.-J. Knobloch. Common PKI Specifications for interoperable Applications. online, `http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf`, retrieved December 2017, 1 2009. v2.0.

[24] Biometrics Research Laboratory at IIT Delhi. IIT Dehli Iris Database Version 1.0 (IITDv1): `http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm`. retrieved December, 2017.

[25] BioSecure Association. BioSecure Multi-modal Database (BioSecure): `http://biosecure.wp.tem-tsp.eu/biosecure-database/`. retrieved December, 2017.

[26] BitcoinWare.net. BitcoinWare - The Canadian Cryptocurrency Store - ASIC Miners in Stock - Scrypt ASIC Miners. online, `https://bitcoinware.net/collections/gridseed-dual-ltc-and-btc-miner`, retrieved December 2017, 2017.

[27] D. Boneh and R. J. Lipton. Quantum cryptanalysis of hidden linear functions (extended abstract). In D. Coppersmith, editor, *Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27-31, 1995, Proceedings*, volume 963 of *Lecture Notes in Computer Science*, pages 424–437. Springer, 1995.

[28] J. Brendel and M. Fischlin. Zero Round-Trip Time for the Extended Access Control Protocol. In S. N. Foley, D. Gollmann, and E. Snekkenes, editors, *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part I*, volume 10492 of *Lecture Notes in Computer Science*, pages 297–314. Springer, 2017.

[29] E. Brier, J. Coron, T. Icart, D. Madore, H. Randriam, and M. Tibouchi. Efficient Indifferentiable Hashing into Ordinary Elliptic Curves. In T. Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*, pages 237–254. Springer, 2010.

[30] A. Brömme and C. Busch, editors. *BIOSIG 2014 - Proceedings of the 13th International Conference of the Biometrics Special Interest Group, 10.-12. September 2014, Darmstadt, Germany*, volume 230 of *LNI*. GI, 2014.

[31] BSI. *Certificate Policy für die ePass-Anwendung der hoheitlichen Dokumente.* Bundesamt für Sicherheit in der Informationstechnik (BSI), 10 2010.

[32] BSI. *Technical Guideline TR-03137 Optically Verifiable Cryptographic Protection of non-electronic Documents (Digital Seal).* Bundesamt für Sicherheit in der Informationstechnik (BSI), 1.0 edition, 2013.

[33] BSI. *Technical Guideline TR-03110-1 Advanced Security Mechanisms forMachine Readable Travel Documents and eIDAS Token - Part 1 - eMRTDs with BAC/PACEv2 and EACv1.* Bundesamt für Sicherheit in der Informationstechnik (BSI), 2.20 edition, 2 2015.

[34] J. A. Buchmann, E. Dahmen, S. Ereth, A. Hülsing, and M. Rückert. On the Security of the Winternitz One-Time Signature Scheme. In A. Nitaj and D. Pointcheval, editors, *Progress in Cryptology - AFRICACRYPT 2011 - 4th International Conference on Cryptology in Africa, Dakar, Senegal, July 5-7, 2011. Proceedings*, volume 6737 of *Lecture Notes in Computer Science*, pages 363–378. Springer, 2011.

[35] J. A. Buchmann, E. Dahmen, and A. Hülsing. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In Yang [291], pages 117–129.

[36] J. A. Buchmann, E. Dahmen, E. Klintsevich, K. Okeya, and C. Vuillaume. Merkle Signatures with Virtually Unlimited Signature Capacity. In J. Katz and M. Yung, editors, *Applied Cryptography and Network Security, 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007, Proceedings*, volume 4521 of *Lecture Notes in Computer Science*, pages 31–45. Springer, 2007.

[37] J. A. Buchmann and J. Ding, editors. *Post-Quantum Cryptography, Second International Workshop, PQCrypto 2008, Cincinnati, OH, USA, October 17-19, 2008, Proceedings*, volume 5299 of *Lecture Notes in Computer Science*. Springer, 2008.

[38] J. A. Buchmann, L. C. C. García, E. Dahmen, M. Döring, and E. Klintsevich. CMSS - An Improved Merkle Signature Scheme. In R. Barua and T. Lange, editors, *Progress in Cryptology - INDOCRYPT 2006, 7th International Conference on Cryptology in India, Kolkata, India, December 11-13, 2006, Proceedings*, volume 4329 of *Lecture Notes in Computer Science*, pages 349–363. Springer, 2006.

[39] J. A. Buchmann, K. E. Lauter, and M. Mosca. Postquantum Cryptography - State of the Art. *IEEE Security & Privacy*, 15(4):12–13, 2017.

[40] N. Buchmann and H. Baier. Towards a more secure and scalable verifying PKI of eMRTD. In S. K. Katsikas and I. Agudo, editors, *Public Key Infrastructures, Services and Applications - 10th European Workshop, EuroPKI 2013, Egham, UK, September 12-13, 2013, Revised Selected Papers*, volume 8341 of *Lecture Notes in Computer Science*, pages 102–118. Springer, 2013.

[41] N. Buchmann and H. Baier. Towards a more secure and scalable verifying PKI of eMRTD. *Journal of Computer Security*, 22(6):1025–1049, 2014.

[42] N. Buchmann, R. Peeters, H. Baier, and A. Pashalidis. Security considerations on extending pace to a biometric-based connection establishment. In *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)*, pages 1–13, Sept 2013.

[43] N. Buchmann, R. Peeters, C. Rathgeb, and H. Baier. BioPACE: Biometric-Protected Authentication Connection Establishment. In D. Chek and L. Ngo, editors, *Biometric Security*, chapter 6, pages 198–223. Cambridge Scholars Publishing, unabridged edition, 2015.

[44] N. Buchmann, C. Rathgeb, H. Baier, and C. Busch. Towards Electronic Identification and Trusted Services for Biometric Authenticated Transactions in the Single Euro Payments Area. In B. Preneel and D. Ikonomou, editors, *Privacy Technologies and Policy - Second Annual Privacy Forum, APF 2014, Athens, Greece, May 20-21, 2014. Proceedings*, volume 8450 of *Lecture Notes in Computer Science*, pages 172–190. Springer, 2014.

[45] N. Buchmann, C. Rathgeb, H. Baier, C. Busch, and M. Margraf. Enhancing Breeder Document Long-Term Security Using Blockchain Technology. In S. Reisman, S. I. Ahamed, C. Demartini, T. M. Conte, L. Liu, W. R. Claycomb, M. Nakamura, E. Tovar, S. Cimato, C. Lung, H. Takakura, J. Yang, T. Akiyama, Z. Zhang, and K. Hasan, editors, *41st IEEE Annual Computer Software and Applications Conference, COMPSAC 2017, Turin, Italy, July 4-8, 2017. Volume 2*, pages 744–748. IEEE Computer Society, 2017.

[46] N. Buchmann, C. Rathgeb, J. Wagner, C. Busch, and H. Baier. A Preliminary Study on the Feasibility of Storing Fingerprint and Iris Image Data in 2D-Barcodes. In A. Brömme, C. Busch, C. Rathgeb, and A. Uhl, editors, *2016 International Conference of the Biometrics Special Interest Group, BIOSIG 2016, Darmstadt, Germany, September 21-23, 2016*, volume 260 of *LNI*, pages 1–5. GI / IEEE, 2016.

[47] I. R. Buhan, J. Doumen, P. Hartel, and R. N. J. Veldhuis. Constructing practical fuzzy extractors using QIM. Technical report, Centre for Telematics and Information Technology, University of Twente, Netherland Technical Report TR-CTIT-07-52, 2007.

[48] I. R. Buhan, J. M. Doumen, P. H. Hartel, and R. N. J. Veldhuis. Fuzzy extractors for continuous distributions. Technical report, University of Twente, 2006.

[49] J. P. Buhler, H. W. Lenstra, and C. Pomerance. *Factoring integers with the number field sieve*, pages 50–94. Springer Berlin Heidelberg, Berlin, Heidelberg, 1993.

[50] Bundesdruckerei GmbH. Press Release – Bundesdruckerei makes global travel more secure. online, `https://www.bundesdruckerei.de/de/system/files/dokumente/pdf/Press-release-bundesdruckerei-makes-global-travel-more-secure.pdf.pdf`, retrieved December 2017, 7 2015.

[51] Bundestag. Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG). online, `https://www.gesetze-im-internet.de/pauswg/index.html`, retrieved December 2017, 7 2017. BGBl. I S. 2745.

[52] Bundestag mit Zustimmung des Bundesrates. Paßgesetz (PaßG). online, `https://www.gesetze-im-internet.de/pa_g_1986/`, retrieved December 2017, 7 2017. BGBl. I S. 537.

[53] Bundestag mit Zustimmung des Bundesrates. Personenstandsgesetz (PStG). online, `https://www.gesetze-im-internet.de/pstg/index.html`, retrieved December 2017, 7 2017. BGBl. I S. 122.

[54] C. Busch, B. Yang, U. Seidel, O. Henniger, M. Butt, C. Rathgeb, J. Hermans, G. Schumacher, J. Loeschner, E. Springmann, U. Rabeler, and A. Wolf. FIDELITY project – Trustworthy lifecycle management for public documents White Paper. online, `http://www.fidelity-project.eu/media/download_pictures/WP_FIDELITY_EC_1.0-RC.pdf`, retrieved December 2017, 2015.

[55] D. Butin. Hash-based signatures: State of play. *IEEE Security & Privacy*, 15(4):37–43, 2017.

[56] CESKÁ TECHNICKÁ NORMA. CSN 36 9791 ed. A – Information technology - Country Verifying Certification Authority Key Management Protocol for SPOC, 12 2009.

[57] R. Chaabouni. Solving Terminal Revocation in EAC by Augmenting Terminal Authentication. In A. Brömme and C. Busch, editors, *2013 BIOSIG - Proceedings of the 12th International Conference of Biometrics Special Interest Group, Darmstadt, Germany, September 4-6, 2013*, volume 212 of *LNI*, pages 273–280. GI, 2013.

[58] R. Chaabouni and S. Vaudenay. The extended access control for machine readable travel documents. In A. Brömme, C. Busch, and D. Hühnlein, editors, *BIOSIG 2009 - Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 17.-18. September 2009 in Darmstadt, Germany*, volume 155 of *LNI*, pages 93–103. GI, 2009.

[59] C. Cheng, K. Chung, G. Persiano, and B. Yang, editors. *Public-Key Cryptography - PKC 2016 - 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I*, volume 9614 of *Lecture Notes in Computer Science*. Springer, 2016.

[60] Chinese Academy of Sciences' Institute of Automation. CASIA Iris Image Database V4.0 — Interval. online, `http://biometrics.idealtest.org`, retrieved December 2017, 2012.

[61] CoinMarketCap. Cryptocurrency market capitalizations,. online, `https://coinmarketcap.com/`, retrieved March 2017, 2017.

[62] A. Commeine and I. A. Semaev. An algorithm to solve the discrete logarithm problem with the number field sieve. In M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, editors, *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings*, volume 3958 of *Lecture Notes in Computer Science*, pages 174–190. Springer, 2006.

[63] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280, RFC Editor, May 2008. online, `http://www.rfc-editor.org/rfc/rfc5280.txt`, retrieved December 2017.

[64] N. Courtois, M. Finiasz, and N. Sendrier. How to Achieve a McEliece-Based Digital Signature Scheme. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 157–174. Springer, 2001.

[65] A. Couvreur, I. M. Corbella, and R. Pellikaan. Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and Their Subcodes. *IEEE Trans. Information Theory*, 63(8):5404–5418, 2017.

[66] Ö. Dagdelen and M. Fischlin. Security Analysis of the Extended Access Control Protocol for Machine Readable Travel Documents. In M. Burmester, G. Tsudik, S. S. Magliveras, and I. Ilic, editors, *Information Security - 13th International Conference, ISC 2010, Boca Raton, FL, USA, October 25-28, 2010, Revised Selected Papers*, volume 6531 of *Lecture Notes in Computer Science*, pages 54–68. Springer, 2010.

[67] E. Dahmen, K. Okeya, T. Takagi, and C. Vuillaume. Digital signatures out of second-preimage resistant hash functions. In Buchmann and Ding [37], pages 109–123.

[68] A. Dantcheva, P. Elia, and A. Ross. What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. *IEEE Trans. Information Forensics and Security*, 11(3):441–467, 2016.

[69] J. Daugman. How iris recognition works. *IEEE Trans. Circuits Syst. Video Techn.*, 14(1):21–30, 2004.

[70] J. Daugman. Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons. *Proceedings of the IEEE*, 94(11):1927–1935, 2006.

[71] J. Daugman. Biometric entropy: searching for doppelgängers and the rare entropod uniquorns, 2016. ICB-2016: the 9th IAPR Conference on Biometrics - Halmstad, Sweden.

[72] J. Daugman. Information Theory and the IrisCode. *IEEE Trans. Information Forensics and Security*, 11(2):400–409, 2016.

[73] J. Daugman and C. Downing. Effect of Severe Image Compression on Iris Recognition Performance. *IEEE Trans. Information Forensics and Security*, 3(1):52–61, 2008.

[74] A. Deacon and R. Hurst. The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments. RFC 5019, RFC Editor, September 2007. `http://www.rfc-editor.org/rfc/rfc5019.txt`, retrieved December 2017.

[75] B. Deufel, C. Mueller, G. Duffy, and T. Kevenaar. BioPACE – Biometric passwords for next generation authentication protocols for machine-readable travel documents. *Datenschutz und Datensicherheit - DuD*, 37(6):363 – 366, 2013.

[76] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246, RFC Editor, August 2008. online, `http://www.rfc-editor.org/rfc/rfc5246.txt`, retrieved December 2017.

[77] Y. Dodis, T. Ristenpart, and T. Shrimpton. Salvaging Merkle-Damgård for Practical Applications. In A. Joux, editor, *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*, pages 371–388. Springer, 2009.

[78] C. Dods, N. P. Smart, and M. Stam. Hash based digital signature schemes. In N. P. Smart, editor, *Cryptography and Coding, 10th IMA International Conference, Cirencester, UK, December 19-21, 2005, Proceedings*, volume 3796 of *Lecture Notes in Computer Science*, pages 96–115. Springer, 2005.

[79] E. Duffield and D. Diaz. Dash: A Privacy-Centric Crypto-Currency. online, `https://github.com/dashpay/dash/wiki/Whitepaper`, retrieved December 2017, 2014.

[80] M. Dworkin. *NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation - The CMAC Mode for Authentication.* National Institute of Standards and Technology, May 2005. (Updated 10/6/2016).

[81] E. Eaton, M. Lequesne, A. Parent, and N. Sendrier. QC-MDPC: A timing attack and a CCA2 KEM. In T. Lange and R. Steinwandt, editors, *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, volume 10786 of *Lecture Notes in Computer Science*, pages 47–76. Springer, 2018.

[82] ECRYPT consortium. ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012). Technical report, ECRYPT II – European Network of Excellence in Cryptology, EU FP7, ICT-2007-216676, 2012.

[83] T. Eisenbarth, I. von Maurich, and X. Ye. Faster Hash-Based Signatures with Bounded Leakage. In T. Lange, K. E. Lauter, and P. Lisonek, editors, *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, volume 8282 of *Lecture Notes in Computer Science*, pages 223–243. Springer, 2013.

[84] D. Engel. JJ 2000, 2016. online, `http://www.wavelab.at/sources/`, retrieved December 2017.

[85] M. Erbilek, M. C. Fairhurst, and M. C. D. C. Abreu. Improved age prediction from biometric data using multimodal configurations. In Brömme and Busch [30], pages 179–186.

[86] Ethereum Foundation. Ethereum. online, `https://ethereum.org/`, retrieved December 2017, Zug, Switzerland, 2017.

[87] M. Ettinger, P. Høyer, and E. Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Inf. Process. Lett.*, 91(1):43–48, 2004.

[88] EU. Integration of biometric features in passports and travel documents - regulation (ec) 2252/2004, 2004.

[89] European Commission. Fidelity project. online, `http://www.fidelity-project.eu/page/project/deliverables.php`, retrieved December 2017.

[90] European Commission. False and Authentic Documents Online (FADO), 12 1998. Joint Action 98/700/JHA concerning the setting up of a European image-archiving system.

[91] European Commission. Action plan to strengthen the European response to travel document fraud, 12 2016. COM(2016) 790 final.

[92] European Parliament and European Council. Directive 2006/126/EC on driving licences, 12 2006.

[93] Federal Information Processing Standards Publication (FIPS PUB). *FIPS PUB 46-3: Data Encryption Standard (DES)*. National Institute of Standards and Technology, October 1999.

[94] Federal Information Processing Standards Publication (FIPS PUB). *FIPS PUB 197: Advanced Encryption Standard (AES)*. National Institute of Standards and Technology, November 2001.

[95] Federal Information Processing Standards Publication (FIPS PUB). *FIPS PUB 180-2: Secure Hash Standard*. National Institute of Standards and Technology, August 2002.

[96] Federal Information Processing Standards Publication (FIPS PUB). *FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC)*. National Institute of Standards and Technology, July 2008.

[97] Federal Information Processing Standards Publication (FIPS PUB). *FIPS PUB 186-4: Digital Signature Standard (DSS)*. National Institute of Standards and Technology, July 2013. Supersedes FIPS PUB 186-3 dated June 2009.

[98] M. Ferrara, A. Franco, and D. Maltoni. The magic passport. In *IEEE International Joint Conference on Biometrics, Clearwater, IJCB 2014, FL, USA, September 29 - October 2, 2014* [149], pages 1–7.

[99] J. Fischer and J. Stern. An Efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding. In Maurer [195], pages 245–255.

[100] T. Freeman, R. Housley, A. Malpani, D. Cooper, and W. Polk. Server-Based Certificate Validation Protocol (SCVP). RFC 5055, RFC Editor, December 2007. online, `http://www.rfc-editor.org/rfc/rfc5055.txt`, retrieved December 2017.

[101] Frontex — European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. Operational and Technical security of Electronic Passports, 7 2011.

[102] Frontex — European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. Best practice operational guidelines for Automated Border Control (ABC) systems, 8 2012.

[103] J. Fu, H. J. Caulfield, S. Yoo, and V. Atluri. Use of Artificial Color filtering to improve iris recognition and searching. *Pattern Recognition Letters*, 26(14):2244–2251, 2005.

[104] W. Funk, M. Arnold, C. Busch, and A. Munde. Evaluation of image compression algorithms for fingerprint and face recognition systems. In *6th Systems, Man Cybernetics Information Assurance Workshop (SMC-IAW'06)*, pages 72–78, 2005.

[105] P. Gaborit. Shorter keys for code based cryptography. In *Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)*, pages 81–90, 2005.

[106] R. B. Gadde, D. A. Adjeroh, and A. Ross. Indexing iris images using the burrows-wheeler transform. In *2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010, Seattle, WA, USA, December 12-15, 2010* [148], pages 1–6.

[107] J. Gentile, N. Ratha, and J. Connell. An efficient, two-stage iris recognition system. In *Proc. 3rd Int'l Conf. on Biometrics: Theory, Applications, and Systems (BTAS)*, 2009.

[108] J. Gentile, N. Ratha, and J. Connell. SLIC: Short-length iris codes. In *Poc. of 3rd Int'l Conf. on Biometrics: Theory, Applications, and Systems (BTAS)*, 2009.

[109] B. Gipp, J. Beel, and I. Rössling. *ePassport - The World's New Electronic Passport: A Report about the ePassport's Benefits, Risks and its Security*. CreateSpace Independent Publishing Platform, 2007.

[110] O. Goldreich. *The Foundations of Cryptography - Volume 2, Basic Applications*. Cambridge University Press, 2004.

[111] M. Gomez-Barrero, C. Rathgeb, K. Raja, R. Raghavendra, and C. Busch. Biometric symmetry: Implications on template protection. In *25th European Signal Processing Conference, EUSIPCO 2016, Kos island, Greece, August 28 - September 2, 2017*. IEEE, 2017.

[112] V. D. Goppa. A Rational Representation of Codes and $(L, g)$-Codes. *Problems of Information Transmission*, 7(3):223–229, 1971.

[113] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt. Applying Grover's algorithm to AES: quantum resource estimates. In T. Takagi, editor, *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, volume 9606 of *Lecture Notes in Computer Science*, pages 29–43. Springer, 2016.

[114] P. Grother, J. R. Matey, E. Tabassi, G. Quinn, and M. Chumakov. IREX VI: temporal stability of iris recognition accuracy. *NIST, Tech. Rep., interagency Report 7948*, 2013.

[115] L. K. Grover. A fast quantum mechanical algorithm for database search. In G. L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996.

[116] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, jul 1997.

[117] S. Halevi, editor. *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*. Springer, 2009.

[118] R. Hamilton, J. Iyengar, I. Swett, and A. Wilk. QUIC: A UDP-Based Secure and Reliable Transport for HTTP/2. Internet-Draft draft-hamilton-early-deployment-quic-00, IETF Secretariat, July 2016. online, `http://www.ietf.org/internet-drafts/draft-hamilton-early-deployment-quic-00.txt`, retrieved December 2017.

[119] L. Hanzlik, L. Krzywiecki, and M. Kutylowski. Simplified PACE|AA Protocol. In R. H. Deng and T. Feng, editors, *Information Security Practice and Experience - 9th International Conference, ISPEC 2013, Lanzhou, China, May 12-14, 2013. Proceedings*, volume 7863 of *Lecture Notes in Computer Science*, pages 218–232. Springer, 2013.

[120] F. Hao, J. Daugman, and P. Zielinski. A fast search algorithm for a large fuzzy database. *IEEE Trans. Information Forensics and Security*, 3(2):203–212, 2008.

[121] I. S. Haque, V. S. Pande, and W. P. Walters. Anatomy of High-Performance 2D Similarity Calculations. *Journal of Chemical Information and Modeling*, 51(9):2345–2351, 2011.

[122] V. Heino and Gemalto. Moving to the third generation of electronic passports. online, `https://silicontrust.wordpress.com/2011/04/08/moving-to-the-third-generation-of-electronic-passports/`, retrieved December 2017, 10 2016.

[123] J. Hermans, R. Peeters, and N. Buchmann. ePassport Protocols and Certificate Architecture. Technical report, FIDELITY EU FP7 WP9 & WP10 management, 12 2015. online, `https://www.esat.kuleuven.be/cosic/publications/article-2596.pdf`, retrieved December 2017.

[124] I. Hirsh and Intel. Intel Architecture Code Analyzer. v3.0, online, `https://software.intel.com/en-us/articles/intel-architecture-code-analyzer`, retrieved December 2017, June 2012.

[125] J. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R. W. Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. In H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, and S. Kawamura, editors, *Advances in Information and Computer Security, First International Workshop on Security, IWSEC 2006, Kyoto, Japan, October 23-24, 2006, Proceedings*, volume 4266 of *Lecture Notes in Computer Science*, pages 152–167. Springer, 2006.

[126] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. In J. Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceed-*

*ings*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

[127] R. Housley, W. Polk, W. Ford, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, RFC Editor, April 2002. online, `http://www.rfc-editor.org/rfc/rfc3280.txt`, retrieved December 2017.

[128] A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen. XMSS: eXtended Merkle Signature Scheme. RFC 8391, RFC Editor, May 2018. `http://www.rfc-editor.org/rfc/rfc8391.txt`, retrieved August 2018.

[129] A. Hülsing, C. Busold, and J. A. Buchmann. Forward secure signatures on smart cards. In L. R. Knudsen and H. Wu, editors, *Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers*, volume 7707 of *Lecture Notes in Computer Science*, pages 66–80. Springer, 2012.

[130] A. Hülsing, L. Rausch, and J. A. Buchmann. Optimal parameters for XMSS MT. In A. Cuzzocrea, C. Kittl, D. E. Simos, E. R. Weippl, and L. Xu, editors, *Security Engineering and Intelligence Informatics - CD-ARES 2013 Workshops: MoCrySEn and SeCIHD, Regensburg, Germany, September 2-6, 2013. Proceedings*, volume 8128 of *Lecture Notes in Computer Science*, pages 194–208. Springer, 2013.

[131] A. Hülsing, J. Rijneveld, and P. Schwabe. Armed SPHINCS - computing a 41 KB signature in 16 KB of RAM. In Cheng et al. [59], pages 446–470.

[132] A. Hülsing, J. Rijneveld, and F. Song. Mitigating multi-target attacks in hash-based signatures. In Cheng et al. [59], pages 387–416.

[133] IBM. IBM Introduces Chip Morphing Technology – Self-Managing Semiconductors Physically Reconfigure Themselves, 7 2004. online, `https://www-304.ibm.com/jct03001c/press/us/en/pressrelease/7246.wss`, retrieved December 2017.

[134] IBM. CPLEX Optimizer - High-performance mathematical programming solver for linear programming, mixed integer programming, and quadratic programming, 8 2017. online, `https://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/`, retrieved December 2017.

[135] ICAO. *Doc 9303 - Part 1 Machine Readable Passports - Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability*. International Civil Aviation Organization (ICAO), 6 edition, 2006.

[136] ICAO. ICAO MRTD Report - Inaugural Issue - Vol. 1, No. 1. online, `https://www.icao.int/publications/Pages/MRTD-Report.aspx`, retrieved December 2017, 3 2006.

[137] ICAO. ICAO MRTD Report - ICAO PKD - Vol. 2, No. 1. online, `https://www.icao.int/publications/Pages/MRTD-Report.aspx`, retrieved December 2017, 4 2007.

[138] ICAO. ICAO MRTD Report - Stressing Security - Vol. 2, No. 2. online, `https://www.icao.int/publications/Pages/MRTD-Report.aspx`, retrieved December 2017, 11 2007.

[139] ICAO. Technical Advisory Group on Machine Readable Travel Documents (TAG-MRTD) – Seventeenth Meeting – Extended Access Control. online, `http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-17/TagMrtd17_WP011.pdf`, retrieved December 2017, 3 2007.

[140] ICAO. Guide for Assessing Security of Handling and Issuance of Travel Documents. V3.4, online, `https://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/tcm/Assessment-Guide-PART1-Best-Practices-Jan-2010.pdf`, retrieved December 2017, 1 2010.

[141] ICAO. Technical Advisory Group on Machine Readable Travel Documents (TAG-MRTD) – Twenty-first Meeting – Revision of the Logical Data Structure Technical Report. online, `https://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-21/Tag-Mrtd21_WP06.pdf`, retrieved December 2017, 12 2012.

[142] ICAO. ICAO MRTD Report - ID Management - Vol. 9, No. 3. online, `https://www.icao.int/publications/Pages/MRTD-Report.aspx`, retrieved December 2017, 10 2014.

[143] ICAO. *Doc 9303 - Machine Readable Travel Documents - Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*. International Civil Aviation Organization (ICAO), 7 edition, 2015.

[144] ICAO. *Doc 9303 - Machine Readable Travel Documents - Part 11: Security Mechanisms for MRTDs*. International Civil Aviation Organization (ICAO), 7 edition, 2015.

[145] ICAO. *Doc 9303 - Machine Readable Travel Documents - Part 12: Public Key Infrastructure for MRTDs*. International Civil Aviation Organization (ICAO), 7 edition, 2015.

[146] ICAO. *Doc 9303 - Machine Readable Travel Documents - Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs*. International Civil Aviation Organization (ICAO), 7 edition, 2015.

[147] T. Icart. How to hash into elliptic curves. In Halevi [117], pages 303–316.

[148] IEEE. *2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010, Seattle, WA, USA, December 12-15, 2010*. IEEE, 2010.

[149] IEEE. *IEEE International Joint Conference on Biometrics, Clearwater, IJCB 2014, FL, USA, September 29 - October 2, 2014*. IEEE, 2014.

[150] ImageMagick. Imagemagick software, 2016. online, `http://www.imagemagick.org/download/`, retrieved December 2017.

[151] Intel Corporation. Intel 64 and IA-32 Architectures Optimization Reference Manual. online, `https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-optimization-manual.pdf`, retrieved December 2017, June 2016.

[152] International Criminal Police Organization-INTERPOL. Stolen and Lost Travel Documents database: `https://www.interpol.int/en/INTERPOL-expertise/Border-management/SLTD-Database`. retrieved December, 2017.

[153] Int'l Organization for Standardization and Int'l Electrotechnical Committee. *ISO/IEC IS 19794:2011. Information Technology – Biometric Data Interchange Format – Part 4: Finger image data, Part 6: Iris image data*, 2011.

[154] ISO/IEC JTC 1/SC 17. Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange – ISO/IEC 7816-4, 4 2013.

[155] ISO/IEC JTC 1/SC 27. ISO/IEC 9796-2 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, 12 2010.

[156] ISO/IEC JTC 1/SC 27. ISO/IEC 9797-1:2011 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, 3 2011.

[157] ISO/IEC JTC 1/SC 27. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General – ISO/IEC 15946-1, 7 2016.

[158] ISO/IEC JTC 1/SC 27 - Security Techniques. Information Technology – Security Techniques – Biometric Information Protection. ISO/IEC 24745:2011, 2011.

[159] ISO/IEC JTC 1/SC 31 - Automatic Identification and Data Capture Techniques. Information Technology – Automatic Identification and Data Capture Techniques – PDF417 Bar Code Symbology Specification. ISO/IEC 15438:2005, 2005.

[160] ISO/IEC JTC 1/SC 31 - Automatic Identification and Data Capture Techniques. Information Technology – Automatic Identification and Data Capture Techniques – Data Matrix Bar Code Symbology Specification. ISO/IEC 16022:2006, 2006.

[161] ISO/IEC JTC 1/SC 31 - Automatic Identification and Data Capture Techniques. Information Technology – Automatic Identification and Data Capture Techniques – Aztec Code Bar Code Symbology Specification. ISO/IEC 24778:2008, 2008.

[162] ISO/IEC JTC 1/SC 31 - Automatic Identification and Data Capture Techniques. Information Technology – Automatic Identification and Data Capture Techniques – QR Code Bar Code Symbology Specification. ISO/IEC 18004:2015, 2015.

[163] ISO/IEC JTC 1/SC 37 Biometrics. *ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*. International Organization for Standardization and International Electrotechnical Committee, 2006.

[164] H. Janwa and O. Moreno. McEliece Public Key Cryptosystems Using Algebraic-Geometric Codes. *Des. Codes Cryptography*, 8(3):293–307, 1996.

[165] D. Jao and L. D. Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Yang [291], pages 19–34.

[166] JC-42.3. *DDR4 SDRAM Standard - JESD79-4A*, 2013. online, `https://www.jedec.org/standards-documents/docs/jesd79-4a`, retrieved December 2017.

[167] S. jen Chang, R. Perlner, W. E. Burr, M. S. Turan, J. M. Kelsey, S. Paul, L. E. Bassham, S. jen Chang, R. Perlner, W. E. Burr, M. S. Turan, J. M. Kelsey, S. Paul, L. E. Bassham, R. M. Blank, and A. Secretary. Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition, 2012.

[168] D. Kaminsky. Black Ops of TCP/IP - BitCoin: Network Manipulation for Fun And (Literal) Profit, Black Hat, 2011.

[169] P. Kamp. Please Put OpenSSL Out of Its Misery. *ACM Queue*, 12(3):20–23, 2014.

[170] P. Kampanakis and S. R. Fluhrer. LMS vs XMSS: A comparison of the stateful hash-based signature proposed standards. *IACR Cryptology ePrint Archive*, 2017:349, 2017.

[171] J. Katz and Y. Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2007.

[172] E. J. C. Kelkboom, J. Breebaart, I. Buhan, and R. N. J. Veldhuis. Analytical template protection performance and maximum key size given a gaussian modeled biometric source. In *Proc. of SPIE defense, security and sensing*, 2010.

[173] S. Kent and K. Seo. Security architecture for the internet protocol. RFC 4301, RFC Editor, December 2005. `http://www.rfc-editor.org/rfc/rfc4301.txt`.

[174] V. Klee. Linear Programming and Extensions. George B. Dantzig. Princeton University Press, Princeton, N.J., 1963. xviii + 625 pp. Illus. *Science*, 146(3651):1572–1572, 1964.

[175] M. Konrad, H. Stögner, A. Uhl, and P. Wild. Computationally efficient serial combination of rotation-invariant and rotation compensating iris recognition algorithms. In P. Richard and J. Braz, editors, *VISAPP 2010 - Proceedings of the Fifth International Conference on Computer Vision Theory and Applications, Angers, France, May 17-21, 2010 - Volume 1*, pages 85–90. INSTICC Press, 2010.

[176] H. Krawczyk. SIGMA: the 'sign-and-mac' approach to authenticated diffie-hellman and its use in the ike-protocols. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 400–425, 2003.

[177] L. Kyrnitszke, T. Ravishankar, and T. Violleau. Java Card 3 Platform – White paper. online, `http://www.oracle.com/technetwork/articles/javase/javacard3-whitepaper-149761.pdf`, retrieved December 2017, 9 2008. Sun Microsystems, Inc.

[178] L. Lamport. Constructing digital signatures from a one way function. Technical report, SRI International, October 1979.

[179] G. Landais and J. Tillich. An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional Codes. In P. Gaborit, editor, *Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings*, volume 7932 of *Lecture Notes in Computer Science*, pages 102–117. Springer, 2013.

[180] T. Lange. Code-based cryptography. *Technische Universiteit Eindhoven, Post-Quantum Cryptography Winter School*, 2016. presentation – Fukuoka, Japan.

[181] F. Leighton and S. Micali. Large provably fast and secure digital signature schemes based on secure hash functions, July 11 1995. US Patent 5,432,852.

[182] C. H. Li, X. F. Zhang, H. Jin, and W. Xiang. E-passport EAC scheme based on identity-based cryptography. *Inf. Process. Lett.*, 111(1):26–30, 2010.

[183] Q. Li, Y. Sutcu, and N. D. Memon. Secure Sketch for Biometric Templates. In X. Lai and K. Chen, editors, *Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3-7, 2006, Proceedings*, volume 4284 of *Lecture Notes in Computer Science*, pages 99–113. Springer, 2006.

[184] Y. Li, R. H. Deng, and X. Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Trans. Information Theory*, 40(1):271–273, 1994.

[185] C. Löndahl and T. Johansson. A New Version of McEliece PKC Based on Convolutional Codes. In T. W. Chim and T. H. Yuen, editors, *Information and Communications Security - 14th International Conference, ICICS 2012, Hong Kong,*

*China, October 29-31, 2012. Proceedings*, volume 7618 of *Lecture Notes in Computer Science*, pages 461–470. Springer, 2012.

[186] M. López, J. Daugman, and E. Cantó. Hardware-software co-design of an iris recognition algorithm. *IET Information Security*, 5(1):60–68, 2011.

[187] V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning with Errors over Rings. *J. ACM*, 60(6):43:1–43:35, 2013.

[188] S. V. M. *Discrete Mathematics and Applications*, volume 4, chapter A public-key cryptosystem based on binary Reed-Muller codes, page 191. Walter de Gruyter GmbH, 2017 1994. 3.

[189] S. V. M. and S. S. O. *Discrete Mathematics and Applications*, volume 2, chapter On insecurity of cryptosystems based on generalized Reed-Solomon codes, page 439. Walter de Gruyter GmbH, 2017 1992. 4.

[190] L. Ma, T. Tan, Y. Wang, and D. Zhang. Efficient iris recognition by characterizing key local variations. *IEEE Trans. Image Processing*, 13(6):739–750, 2004.

[191] M. Mahoney. Data compression programs, 2016. online, `http://www.mattmahoney.net/dc/`, retrieved December 2017.

[192] D. T. Marr, F. Binns, D. L. Hill, G. Hinton, D. A. Koufaty, J. A. Miller, and M. Upton. Hyper-threading technology architecture and microarchitecture. *Intel Technology Journal*, 1(Q1), 2002.

[193] A. Mascher-Kampfer, H. Stögner, and A. Uhl. Comparison of compression algorithms' impact on fingerprint and face recognition accuracy. In *Proc. of SPIE Visual Communications and Image Processing (VCIP'07)*, pages 1–12, 2006.

[194] L. Masek. Recognition of human iris patterns for biometric identification. Master's thesis, Univ. of Western Australia, 2003.

[195] U. M. Maurer, editor. *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*. Springer, 1996.

[196] R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. Technical Report 44, Jet Propulsion Lab., CA, 1978.

[197] D. McGrew. An Interface and Algorithms for Authenticated Encryption. RFC 5116, RFC Editor, January 2008. online, `http://www.rfc-editor.org/rfc/rfc5116.txt`, retrieved December 2017.

[198] D. McGrew, M. Curcio, and S. Fluhrer. Hash-based signatures. Internet-Draft draft-mcgrew-hash-sigs-08, IETF Secretariat, October 2017. online, `http:`

//www.ietf.org/internet-drafts/draft-mcgrew-hash-sigs-08.txt, retrieved December 2017.

[199] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. A fistful of bitcoins: characterizing payments among men with no names. *Commun. ACM*, 59(4):86–93, 2016.

[200] R. C. Merkle. *Secrecy, Authentication, and Public Key Systems.* PhD thesis, Stanford University, Stanford, CA, USA, 1979. AAI8001972.

[201] R. C. Merkle. A digital signature based on a conventional encryption function. In C. Pomerance, editor, *Advances in Cryptology - CRYPTO '87, A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, August 16-20, 1987, Proceedings*, volume 293 of *Lecture Notes in Computer Science*, pages 369–378. Springer, 1987.

[202] R. C. Merkle. A certified digital signature. In G. Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 218–238. Springer, 1989.

[203] A. Miller, A. E. Kosba, J. Katz, and E. Shi. Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions. In I. Ray, N. Li, and C. Kruegel, editors, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*, pages 680–691. ACM, 2015.

[204] D. Mills, J. Martin, J. Burbank, and W. Kasch. Network Time Protocol Version 4: Protocol and Algorithms Specification. RFC 5905, RFC Editor, June 2010. http://www.rfc-editor.org/rfc/rfc5905.txt, retrieved December 2017.

[205] L. Minder and A. Shokrollahi. Cryptanalysis of the Sidelnikov Cryptosystem. In M. Naor, editor, *Advances in Cryptology - EUROCRYPT 2007, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings*, volume 4515 of *Lecture Notes in Computer Science*, pages 347–360. Springer, 2007.

[206] R. Misoczki, J. Tillich, N. Sendrier, and P. S. L. M. Barreto. MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. In *Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013*, pages 2069–2073. IEEE, 2013.

[207] C. Monico, J. Rosenthal, and A. Shokrollahi. Using low density parity check codes in the McEliece cryptosystem. In *2000 IEEE International Symposium on Information Theory (Cat. No.00CH37060)*, pages 215–, 2000.

[208] T. Moses. Protecting Biometric Data with Extended Access Control – Securing biometric datasets in electronic identification documents. online, `https://www.entrust.com/wp-content/uploads/2010/01/WP_Entrust_ePassport-Biometrics_Aug2014.pdf`, retrieved December 2017, 1 2010. Entrust, Inc.

[209] R. Mukherjee and A. Ross. Indexing iris images. In *19th International Conference on Pattern Recognition (ICPR 2008), December 8-11, 2008, Tampa, Florida, USA*, pages 1–4. IEEE Computer Society, 2008.

[210] W. Mula. SSSE3: fast popcount, 2008. online, `http://wm.ite.pl/articles/sse-popcount.html`, retrieved December 2017.

[211] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560, RFC Editor, June 1999. online, `http://www.rfc-editor.org/rfc/rfc2560.txt`, retrieved December 2017.

[212] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. online, `http://bitcoin.org/bitcoin.pdf`, retrieved December 2017.

[213] P. R. Nalla and K. M. Chalavadi. Iris classification based on sparse representations using on-line dictionary learning for large-scale de-duplication applications. *SpringerPlus*, 4:1–10, 2015.

[214] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. Bitcoin and Cryptocurrency Technologies - Coursera Online Course, Princeton University, 2016.

[215] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press, Princeton, NJ, USA, 2016.

[216] R. Niebuhr, M. Meziani, S. Bulygin, and J. A. Buchmann. Selecting parameters for secure McEliece-based cryptosystems. *Int. J. Inf. Sec.*, 11(3):137–147, 2012.

[217] H. Niederreiter. Knapsack type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15:157–166, 01 1986.

[218] I. Nigam, M. Vatsa, and R. Singh. Ocular biometrics: A survey of modalities and fusion approaches. *Information Fusion*, 26:1–35, 2015.

[219] NIST: National Institute of Standards and Technology. *Recommended elliptic curves for federal government use*, 1999.

[220] NXP Semiconductors. P5Cx009/P5Cx072 – Secure triple, dual and contact PKI smart card controller, 2 2010. Rev. 01, Product short data sheet, online, `http://datasheet.datasheetarchive.com/originals/library/Datasheets-EDS6/DSAEDA000114095.pdf`, retrieved December 2017.

[221] NXP Semiconductors. NXP Secures Next-gen SAC ePassports for Germany and Switzerland, 4 2014. online, `https://nxp-rfid.com/nxp-secures-next-gen-sac-epassports-germany-switzerland/`, retrieved December 2017.

[222] Organization for Security and Co-operation in Europe (OSCE). Addressing the Link between Travel Document Security and Population Registration/Civil Registration Documents and Processes. online, `http://www.osce.org/secretariat/110610`, retrieved December 2017, 11 2013.

[223] ORIGINS consortium. ORIGINS project. `http://www.origins-project.eu`, retrieved December 2017, 2017.

[224] Oxford Living Dictionaries. Definition of breeder document in US English. `https://en.oxforddictionaries.com/definition/us/breeder_document`, retrieved December 2017.

[225] K. Papapanagiotou, C. Markantonakis, Q. Zhang, W. G. Sirett, and K. Mayes. On the Performance of Certificate Revocation Protocols Based on a Java Card Certificate Client Implementation. In R. Sasaki, S. Qing, E. Okamoto, and H. Yoshiura, editors, *Security and Privacy in the Age of Ubiquitous Computing, IFIP TC11 20th International Conference on Information Security (SEC 2005), May 30 - June 1, 2005, Chiba, Japan*, volume 181 of *IFIP*, pages 551–564. Springer, 2005.

[226] V. Pasupathinathan, J. Pieprzyk, and H. Wang. An on-line secure e-passport protocol. In L. Chen, Y. Mu, and W. Susilo, editors, *Information Security Practice and Experience, 4th International Conference, ISPEC 2008, Sydney, Australia, April 21-23, 2008, Proceedings*, volume 4991 of *Lecture Notes in Computer Science*, pages 14–28. Springer, 2008.

[227] J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In Maurer [195], pages 33–48.

[228] R. Peeters, J. Hermans, and J. Fan. IBIHOP: proper privacy preserving mutual RFID authentication. In *Radio Frequency Identification System Security - RFIDsec'13 Asia Workshop Proceedings, Guangzhou, China, November 27, 2013*, pages 45–56, 2013.

[229] R. Peeters, J. Hermans, and B. Mennink. Speedup for european epassport authentication. In Brömme and Busch [30], pages 39–50.

[230] C. Percival. Stronger Key Derivation via Sequential Memory-Hard Functions. online, `https://www.tarsnap.com/scrypt/scrypt.pdf`, retrieved December 2017, May 2009.

[231] Philips Semiconductors. P5CT072 – Secure Dual Interface PKI Smart Card Controller, 10 2004. Rev. 1.3, Short Form Specification, online, `http://www.win.tue.nl/pinpasjc/docs/cards-docs/jcop41/sfs085513.pdf`, retrieved December 2017.

[232] A. Poelstra. Distributed Consensus from Proof of Stake is Impossible. online, `https://download.wpsoftware.net/bitcoin/old-pos.pdf`, retrieved December 2017, May 2014.

[233] PQCRYPTO consortium. Initial recommendations of long-term secure post-quantum systems. online, `https://pqcrypto.eu.org/docs/initial-recommendations.pdf`, retrieved December 2017, March 2015.

[234] PQCRYPTO consortium. PQCRYPTO EU Project ICT-645622. online, `https://pqcrypto.eu.org/`, retrieved December 2017, 2017.

[235] H. Proença. Iris biometrics: Indexing and retrieving heavily degraded data. *IEEE Trans. Information Forensics and Security*, 8(12):1975–1985, 2013.

[236] N. B. Puhan and N. Sudha. Coarse indexing of iris database based on iris colour. *Int'l J. on Biometrics*, 3(4):353–375, 2011.

[237] X. Qiu, Z. Sun, and T. Tan. Global texture analysis of iris images for ethnic classification. In D. Zhang and A. K. Jain, editors, *Advances in Biometrics, International Conference, ICB 2006, Hong Kong, China, January 5-7, 2006, Proceedings*, volume 3832 of *Lecture Notes in Computer Science*, pages 411–418. Springer, 2006.

[238] S. Rakshit and D. M. Monro. An evaluation of image sampling and compression for human iris recognition. *IEEE Trans. Information Forensics and Security*, 2(3-2):605–612, 2007.

[239] R. N. Rakvic, H. T. Ngo, R. P. Broussard, and R. W. Ives. Comparing an FPGA to a Cell for an image processing application. *EURASIP J. Adv. Sig. Proc.*, 2010, 2010.

[240] R. N. Rakvic, B. J. Ulis, R. P. Broussard, R. W. Ives, and N. Steiner. Parallelizing iris recognition. *IEEE Trans. Information Forensics and Security*, 4(4):812–823, 2009.

[241] W. Rankl and W. Effing. *Smart Card Handbook*. Wiley, New York, 4 edition, 8 2010.

[242] N. K. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In J. Bigün and F. Smeraldi, editors, *Audio- and Video-Based Biometric Person Authentication, Third International Conference, AVBPA 2001 Halmstad, Sweden, June 6-8, 2001, Proceedings*, volume 2091 of *Lecture Notes in Computer Science*, pages 223–228. Springer, 2001.

[243] E. D. Rather and C. H. Moore. The FORTH approach to operating systems. In J. A. Gosden and O. G. Johnson, editors, *Proceedings of the 1976 Annual Conference, Houston, Texas, USA, October 20-22, 1976*, pages 233–240. ACM, 1976.

[244] C. Rathgeb, H. Baier, C. Busch, and F. Breitinger. Towards bloom filter-based indexing of iris biometric data. In *International Conference on Biometrics, ICB 2015, Phuket, Thailand, 19-22 May, 2015*, pages 422–429. IEEE, 2015.

[245] C. Rathgeb, N. Buchmann, H. Hofbauer, H. Baier, A. Uhl, and C. Busch. Methods for Accuracy-preserving Acceleration of Large-Scale Comparisons in CPU-based Iris Recognition Systems. *IET Biometrics*, 2017.

[246] C. Rathgeb, H. Hofbauer, A. Uhl, and C. Busch. TripleA: Accelerated accuracy-preserving alignment for iris-codes. In *International Conference on Biometrics, ICB 2016, Halmstad, Sweden, June 13-16, 2016*, pages 1–8. IEEE, 2016.

[247] C. Rathgeb, A. Uhl, and P. Wild. *Iris Recognition: From Segmentation to Template Security*, volume 59 of *Advances in Information Security*. Springer Verlag, 2013.

[248] C. Rathgeb, A. Uhl, and P. Wild. Effects of severe image compression on iris segmentation performance. In *IEEE International Joint Conference on Biometrics, Clearwater, IJCB 2014, FL, USA, September 29 - October 2, 2014* [149], pages 1–6.

[249] F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system. In *PASSAT/SocialCom 2011, Privacy, Security, Risk and Trust (PASSAT), 2011 IEEE Third International Conference on and 2011 IEEE Third International Conference on Social Computing (SocialCom), Boston, MA, USA, 9-11 Oct., 2011*, pages 1318–1326. IEEE, 2011.

[250] E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. Internet-Draft draft-ietf-tls-tls13-21, IETF Secretariat, July 2017. online, `http://www.ietf.org/internet-drafts/draft-ietf-tls-tls13-21.txt`, retrieved December 2017.

[251] L. Reyzin and N. Reyzin. Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying. In L. M. Batten and J. Seberry, editors, *Information Security and Privacy, 7th Australian Conference, ACISP 2002, Melbourne, Australia, July 3-5, 2002, Proceedings*, volume 2384 of *Lecture Notes in Computer Science*, pages 144–153. Springer, 2002.

[252] S. Rohde, T. Eisenbarth, E. Dahmen, J. A. Buchmann, and C. Paar. Fast Hash-Based Signatures on Constrained Devices. In G. Grimaud and F. Standaert, editors, *Smart Card Research and Advanced Applications, 8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8-11, 2008. Proceedings*, volume 5189 of *Lecture Notes in Computer Science*, pages 104–117. Springer, 2008.

[253] A. Ross and M. S. Sunder. Block based texture analysis for iris classification and matching. In *IEEE Conference on Computer Vision and Pattern Recognition, CVPR Workshops 2010, San Francisco, CA, USA, 13-18 June, 2010*, pages 30–37. IEEE Computer Society, 2010.

[254] J. Schaad, B. Kaliski, and R. Housley. Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 4055, RFC Editor, June 2005. online, `http://www.rfc-editor.org/rfc/rfc4055.txt`, retrieved December 2017.

[255] T. Scheidat and C. Vielhauer. Biometric hashing for handwriting: entropy-based feature selection and semantic fusion. In E. J. D. III, P. W. Wong, J. Dittmann, and N. D. Memon, editors, *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, San Jose, CA, USA, January 27, 2008*, volume 6819 of *SPIE Proceedings*, page 68190N. SPIE, 2008.

[256] W. J. Scheirer, W. Bishop, and T. E. Boult. Beyond PKI: the biocryptographic key infrastructure. In *2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010, Seattle, WA, USA, December 12-15, 2010* [148], pages 1–6.

[257] W. J. Scheirer and T. E. Boult. Bio-cryptographic protocols with bipartite biotokens. In *Biometrics Symposium*, pages 9–16, 2008.

[258] C. Schnorr. Efficient signature generation by smart cards. *J. Cryptology*, 4(3):161–174, 1991.

[259] N. Sendrier. On the Concatenated Structure of a Linear Code. *Appl. Algebra Eng. Commun. Comput.*, 9(3):221–242, 1998.

[260] N. Sendrier. On the use of structured codes in code based cryptography. *Coding Theory and Cryptography III, The Royal Flemish Academy of Belgium for Science and the Arts*, 2010.

[261] N. Sendrier. Code-Based Cryptography: State of the Art and Perspectives. *IEEE Security & Privacy*, 15(4):44–50, 2017.

[262] S. Shanafelt. Miners flee GHash.io after near 51% scenario. online, `http://www.bitcoinx.com/miners-flee-ghash-io-after-near-51-scenario/`, retrieved December 2017, 2014.

[263] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 124–134. IEEE Computer Society, 1994.

[264] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[265] V. Sklyarov, I. Skliarova, and J. P. S. da Silva. On-Chip Reconfigurable Hardware Accelerators for Popcount Computations. *Int. J. Reconfig. Comp.*, 2016:11, 2016.

[266] SPRING Singapore. Singapore Standard SS 529: 2006 – Specifications for Smart-Card ID – ICS 35.240.15, 12 2006.

[267] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov. The first collision for full SHA-1. In J. Katz and H. Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 570–596. Springer, 2017.

[268] M. Stevens, A. Sotirov, J. Appelbaum, A. K. Lenstra, D. Molnar, D. A. Osvik, and B. de Weger. Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate. In Halevi [117], pages 55–69.

[269] T. Straub, M. Hartl, and M. Ruppert. Digitale Reisepässe in Deutschland - Prozesse und Sicherheitsinfrastruktur. In J. Dittmann, editor, *Sicherheit 2006: Sicherheit - Schutz und Zuverlässigkeit, Beiträge der 3. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.v. (GI), 20.-22. Februar 2006 in Magdeburg*, volume 77 of *LNI*, pages 233–243. GI, 2006.

[270] Z. Sun, H. Zhang, T. Tan, and J. Wang. Iris Image Classification Based on Hierarchical Visual Codebook. *IEEE Trans. Pattern Anal. Mach. Intell.*, 36(6):1120–1133, 2014.

[271] Y. Sutcu, Q. Li, and N. D. Memon. How to protect biometric templates. In E. J. D. III and P. W. Wong, editors, *Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, CA, USA, January 28, 2007*, volume 6505 of *SPIE Proceedings*, page 650514. SPIE, 2007.

[272] T. Tan, X. Zhang, Z. Sun, and H. Zhang. Noisy iris image matching by using multiple cues. *Pattern Recognition Letters*, 33(8):970–977, 2012.

[273] J. E. Tapia and C. A. Perez. Gender Classification Based on Fusion of Different Spatial Scale Features Selected by Mutual Information From Histogram of LBP, Intensity, and Shape. *IEEE Trans. Information Forensics and Security*, 8(3):488–499, 2013.

[274] H. C. A. van Tilborg and S. Jajodia, editors. *Encyclopedia of Cryptography and Security, 2nd Ed.* Springer, 2011.

[275] J. Tromp. Cuckoo cycle: A memory bound graph-theoretic proof-of-work. In M. Brenner, N. Christin, B. Johnson, and K. Rohloff, editors, *Financial Cryptography and Data Security - FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers*, volume 8976 of *Lecture Notes in Computer Science*, pages 49–62. Springer, 2015.

[276] S. Tuecke, V. Welch, D. Engert, L. Pearlman, and M. Thompson. Internet x.509 public key infrastructure (pki) proxy certificate profile. RFC 3820, RFC Editor,

June 2004. online, `http://www.rfc-editor.org/rfc/rfc3820.txt`, retrieved December 2017.

[277] P. Tuyls and J. Goseling. Capacity and examples of template-protecting biometric authentication systems. In D. Maltoni and A. K. Jain, editors, *Biometric Authentication, ECCV 2004 International Workshop, BioAW 2004, Prague, Czech Republic, May 15, 2004, Proceedings*, volume 3087 of *Lecture Notes in Computer Science*, pages 158–170. Springer, 2004.

[278] I. T. Union. ITU-T X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[279] Unique Identification Authority of India. Aadhaar: `http://uidai.gov.in/`. retrieved December, 2017.

[280] University of Bologna – BioLab. Fingerprint Verification Competition (FVC'02): `http://bias.csr.unibo.it/fvc2002/`. retrieved December, 2017.

[281] University of Salzburg. USIT – University of Salzburg iris toolkit. `http://www.wavelab.at/sources/Rathgeb16a`. Version 2.0, retrieved December 2017.

[282] N. A. Vandal and M. Savvides. CUDA accelerated iris template matching on graphics processing units (GPUs). In *Fourth IEEE International Conference on Biometrics: Theory Applications and Systems, BTAS 2010, Washington, DC, USA, 27-29 September, 2010*, pages 1–7. IEEE, 2010.

[283] S. Vaudenay and M. Vuagnoux. About machine-readable travel documents. *Journal of Physics: Conference Series*, 77(1), 2007.

[284] E. Verbitskiy, P. Tuyls, D. Denteneer, and J. P. Linnartz. Reliable biometric authentication with privacy protection. *presented at the SPIE Biometric Technology for Human Identification Conf., Orlando, FL*, 2004.

[285] C. Vielhauer and R. Steinmetz. Handwriting: Feature correlation analysis for biometric hashes. *EURASIP J. Adv. Sig. Proc.*, 2004(4):542–558, 2004.

[286] C. Vielhauer, R. Steinmetz, and A. Mayerhöfer. Biometric hash based on statistical features of online signatures. In *16th International Conference on Pattern Recognition, ICPR 2002, Quebec, Canada, August 11-15, 2002.*, pages 123–126. IEEE Computer Society, 2002.

[287] R. Viveros, K. Balasubramanian, and N. Balakrishnan. Binomial and negative binomial analogues under correlated bernoulli trials. *The American Statistician*, 48(3):243–247, 1984.

[288] X. Wang, Y. L. Yin, and H. Yu. Finding collisions in the full SHA-1. In V. Shoup, editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceed-*

*ings*, volume 3621 of *Lecture Notes in Computer Science*, pages 17–36. Springer, 2005.

[289] X. Wang and H. Yu. How to break MD5 and other hash functions. In R. Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 19–35. Springer, 2005.

[290] K. E. Wiegers. *Software Requirements, Second Edition (Pro-Best Practices)*. Microsoft Press, 0002 edition, 3 2003.

[291] B. Yang, editor. *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings*, volume 7071 of *Lecture Notes in Computer Science*. Springer, 2011.

[292] S. Yoon and A. K. Jain. Longitudinal study of fingerprint recognition. *Proceedings of the National Academy of Sciences*, 112(28):8555–8560, 2015.

[293] L. Yu, D. Zhang, K. Wang, and W. Yang. Coarse iris classification using box-counting to estimate fractal dimensions. *Pattern Recognition*, 38(11):1791–1798, 2005.

[294] D. H. Yum and P. J. Lee. Separable implicit certificate revocation. In C. Park and S. Chee, editors, *Information Security and Cryptology - ICISC 2004, 7th International Conference, Seoul, Korea, December 2-3, 2004, Revised Selected Papers*, volume 3506 of *Lecture Notes in Computer Science*, pages 121–136. Springer, 2004.

# Appendices

## Security Protocols Sequence Diagram Notation

| Notation | Description |
|---|---|
| $SHA256(data)$ | Calculate SHA-256 hash value of *data*. |
| $h = H(data)$ | Calculate a cryptographic hash value of *data* with function $H()$. |
| $s = Sign(SK, data)$ | Sign *data* with the secret key $SK$ utilising an asymmetric signature scheme to retrieve $s$. |
| $Verify\ s$ | Verify the signature $s$ by utilising an asymmetric signature scheme. |
| $Verify(PK, s, data)$ | Verify signature $s$ with the public key $PK$ utilising an asymmetric signature scheme. |
| $Ver_{PK}(s, data)$ | Verify Signature $s$ of *data* with public key $PK$ utilising function $Ver()$. |
| $COMP(PK)$ | Calculate the compressed public key $PK$. |
| $KA(SK, PK)$ | Perform a Key Agreement utilising the own secret key $SK$ and the other parties public key $PK$. |
| $DH(SK, PK)$ | Perform a Diffie-Hellman Key Agreement utilising the own secret key $SK$ and the other parties public key $PK$. |
| $K_{Type} = KDF_{Type}(K, r)$ | Utilise the key derivation function $KDF()$ in mode $Type$ and random value $r$ to retrieve a session key $K_{Type}$ based on $K$. |
| $K_{Session} = KDF(K)$ | Utilise the key derivation function $KDF()$ to retrieve a session key $K_{Session}$ based on $K$. |
| $T = MAC(K, data)$ | Calculate the message authentication code $T$ (token) utilising function $MAC()$ with symmetric key $K$ of *data*. |
| $Verify(K_{MAC}, T, data)$ | Verify the message authentication code $T$ utilising function $Verify()$ with key $K_{MAC}$ and *data*. |
| MVf($T$) | Verify the message authentication code token $T$ utilising function MVf(). |
| $E(K, data)$ / $Enc_K(data)$ | Encrypt *data* with a symmetric encryption scheme utilising function $E()$ / $Enc()$ with key $K$. |
| $D(K, data)$ / $Dec_K(data)$ | Decrypt *data* with a symmetric encryption scheme utilising function $D()$ / $Dec()$ with key $K$. |
| $AE_K()$ | Authenticated Encryption with key $K$ |
| $AD_K()$ | Authenticated Decryption with key $K$ |
| $PACE(CAN)$ | Perform a Password Authenticated Connection Establishment with the Card Access Number $CAN$. |
| $wt(data)$ | Calculate the hamming weight of *data*. |

## curriculum vitae

The CV is not included in the online version due to privacy protection.

## Zusammenfassung der Dissertation

Reisedokumente sind ein fester Bestandteil von Reisen ins Ausland und spielen eine wichtige Rolle für die Grenzkontrolle und den Luftverkehr. Die heutigen elektronischen Reisedokumente basieren auf elektronischen Sicherheitsprotokollen und -infrastrukturen, um die Authentizität und Integrität der biometrischen Daten des Dokumenteninhabers und die Originalität des Dokuments selbst zu gewährleisten. Die kryptographisch geschützten biometrischen Daten werden genutzt, um eine Verbindung zwischen dem physischen Dokument und dem Dokumenteninhaber herzustellen. Die beiden wichtigsten Sicherheitsziele eines jeden Ausweisdokuments sind daher, sicherzustellen, dass das Dokument unverändert und authentisch ist und dass das physische Dokument und der Dokumenteninhaber zueinander gehören. Die derzeitigen Sicherheitsprotokolle und -infrastrukturen für Reisedokumente weisen zahlreiche Mängel auf.

Einerseits sind die verwendeten Protokolle und Infrastrukturen komplex, teilweise nach fast 10 Jahren Einführung des elektronischen Reisepasses der EU in der Praxis nicht implementiert und wurden in Gegenwart eines Quantencomputers als unsicher eingestuft. Andererseits sind elektronische Reisedokumente nur ein Teil des Dokumentenlebenszyklus, da ein Reisepass mit einer nicht standardisierten und unsicheren Geburtsurkunde beantragt werden kann. Darüber hinaus gibt es keinen standardisierten Mechanismus für gestohlene Passterminals, und da die Terminalinfrastruktur in der EU nicht vollständig genutzt wird, verlassen sich die Terminals auf Gesichtserkennung mit geringer Entropie, anstatt die zuverlässigeren Fingerabdrücke, welche im Pass gespeichert sind, zu verwenden.

Aufgrund dieser Mängel liegt der Schwerpunkt dieser Dissertation auf der Verbesserung der Sicherheit von Geburtsurkunden, einfacheren und postquantumresistenten Sicherheitsprotokollen und Infrastrukturverbesserungen im Identitätslebenszyklus.

Die Sicherheit von Geburtsurkunden wird einerseits durch ein Blockchain basiertes System zur Sicherstellung der langfristigen Authentizität und Integrität der Daten und andererseits durch einen 2D-Barcode, der biometrische Informationen des Dokumenteninhabers speichert und so eine Verbindung zwischen Geburtsurkunde und Dokumenteninhaber herstellt, erhöht.

Darüber hinaus werden einfachere Reisedokumentenprotokolle mit weniger komplexen Infrastrukturanforderungen, weniger Schritten als die aktuelle Sicherheitsprotokoll-Suite vorgeschlagen, und langfristige Postquantum-Sicherheit wird durch die Evaluierung der am besten geeigneten Postquantum-Klassen, insbesondere der hashbasierten Kryptographie und der codebasierten Kryptographie, erreicht.

Um das Problem der gestohlenen Terminals zu beseitigen, wurde ein Revokationsmechanismus basierend auf dem Network Time Protocol (NTP) und dem Online Certificate Status Protocol (OCSP) als am besten geeignet für die Anforderungen der Reisedokumenten-Domäne erachtet.

Schließlich werden Verbesserungen in Bezug auf die verwendete Biometrie diskutiert, die sich einerseits auf die geeignete Entropie für die Biometrie von Reisedokumenten konzentrieren und andererseits auf Techniken zur Beschleunigung großflächiger biometrischer Vergleiche (z.B. Black-List-Checks und Double-Enrollment-Checks).