entropy

Article

User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks

Lavinia Mihaela Dinca * and Gerhard Hancke

Department of Computer Science, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong, China; gp.hancke@cityu.edu.hk

* Correspondence: lavinia.dinca@gmail.com

Academic Editor: James J. Park

Received: 30 November 2016; Accepted: 9 February 2017; Published: 21 February 2017

Abstract: Biometric data can be used as input for PKI key pair generation. The concept of not saving the private key is very appealing, but the implementation of such a system shouldn't be rushed because it might prove less secure then current PKI infrastructure. One biometric characteristic can be easily spoofed, so it was believed that multi-modal biometrics would offer more security, because spoofing two or more biometrics would be very hard. This notion, of increased security of multi-modal biometric systems, was disproved for authentication and matching, studies showing that not only multi-modal biometric systems are not more secure, but they introduce additional vulnerabilities. This paper is a study on the implications of spoofing biometric data for retrieving the derived key. We demonstrate that spoofed biometrics can yield the same key, which in turn will lead an attacker to obtain the private key. A practical implementation is proposed using fingerprint and iris as biometrics and the fuzzy extractor for biometric key extraction. Our experiments show what happens when the biometric data is spoofed for both uni-modal systems and multi-modal. In case of multi-modal system tests were performed when spoofing one biometric or both. We provide detailed analysis of every scenario in regard to successful tests and overall key entropy. Our paper defines a biometric PKI scenario and an in depth security analysis for it. The analysis can be viewed as a blueprint for implementations of future similar systems, because it highlights the main security vulnerabilities for bioPKI. The analysis is not constrained to the biometric part of the system, but covers CA security, sensor security, communication interception, RSA encryption vulnerabilities regarding key entropy, and much more.

Keywords: multi-modal key derivation; biometric PKI; biometric entropy; Wireless Sensor Security; user-centric security

1. Introduction

We are connecting an increasing amount of user devices to the Internet, driven by concept of Internet-of-Things and Machine-to-Machine communications [1]. Often we can interact with surrounding devices and collect sensor readings with our mobile devices [2]. In such settings, we still require security services to keep collected data confidential. As such, we are looking for new user-centric approaches of linking data to user devices [3]. While we can keep long term keys on our devices, even tamper resistant storage can be circumvented if the attacker is serious enough [4], and the ubiquitous nature of technology also makes it easier for attackers to interact with us [5]. Given this premise, we are looking for ways to generate and establish keys for security services from the user's characteristics. Biometric key derivation is one potential area that can be applied.

Biometrics are classified in [6]: *physical biometrics* unique human features like: face, biometrics found in hand (fingerprint, hand geometry, palm print, vein), *behavioural biometrics* unique actions performed by a person: signature, keystroke, gait and voice. Multi-modal is a term used to describe the use of two different biometric characteristics. There are many reasons one might use multi-modal systems, but two stand out: upper bound limitation and security. *Upper bound* is the maximum number of distinguishable patterns. This metric is essential for large biometric systems like: border control systems and biometric IDs. Using multi-modal biometrics increases the overall upper bound. Another issue in large population is lack of some biometrics. A person might have had an accident that resulted in a loss of a certain biometric characteristic, which might prevent him or her from enrolling into the biometric system.

Biometric *security* mostly deals with: renewability, template security and spoofing. A biometric characteristic can't be replaced or renewed, so if compromised that characteristics can be considered lost forever. Studies [7,8] proved that biometric data can be reconstructed from a stored template and a possible database breach could compromise biometric characteristics for many users. Ratha et al. [9] introduced the concept of cancelable biometrics which solves two of the security issues: renewability and template security. Cancelable biometrics were later divided intro two main groups: cancelable biometrics and biometric cryptosystems, as described in Table 1. The surveys [10,11] detail the large amount of cancelable and biometric cryptosystems, but for the scope of our paper we only need to differentiate between the two groups. Cancelable biometrics intentionally distort the biometric signals by applying transformation functions. The matching of templates is made in the transformed domain, the biometric template is never stored in clear. Biometric cryptosystems derive a key from the biometrics itself and use that key to encrypt the template. When matching is done the biometric template must be decrypted.

Table 1. Cancelable biometrics, as described by [9].

Type	Name	Description
Cancelable biometrics	Biometric salting	Adds a salt (randoms bits) to the key. If the biometric template is compromised it can be renewed and the user doesn't loose the biometric characteristic.
	Non-invertible transforms	The biometric data is transformed using a non-invertible function before being stored in the database. A template can be renewed by using a different transformation.
Biometric Cryptosystems	Key-binding schemes	The biometric template is binded by an encryption key and stored in the database.
	Key-generation schemes	The key is derived from the biometric template.

Biometric PKI (bioPKI) is a new biometric research field developing rapidly. 2011 was a dark year for PKI, because 3 CAs had their private keys stolen resulting in issuing of rogue certificates [12]. The same year a new breed of cyber-weapon named Stuxnet [13] was used to infect multiple targets. The malware was signed with genuine certificates from legitimate companies, that had their private keys stolen. Since then attackers have devised a new goal: breach companies and steal their private keys, which in turn will be used to sign and distribute malware. Unfortunately only some of attacks are reported [14,15], but most of them either aren't reported or are not even discovered.

PKI's weakest link is the private key. The latest available statistics from the world bank show there are over 120 million micro to small business [16] worldwide. Most companies need to file mandatory on-line tax reports forcing the entity to have a digital certificate. Projects like Stork [17] propose the implementation of eIDs including a recognised digital certificate for EU citizens. It reasonable to assume that in the not to distant future many countries will implement such initiatives and private key management will become a real issue. End users are known not to be technically proficient and if secure tokens are not safe guarded, they can easily be stolen. Some authors proposed the implementation of a distributed infrastructure to store the private key on multiple devices [18], but the user is still responsible for managing the key. It is safe to assume that if CAs were breached, the end user or the personnel from a small company won't be much of a challenge for a determined attacker.

The answer to PKIs pressing concerns might be found in biometrics. The goal is to eliminate the need for private key management, by not storing the private key. The use of multi-modal biometrics might be necessary because it might offer better security and key entropy. It was believed that multi-biometric authentication systems offer better security than their uni-modal counterpart, but studies [19–21] demonstrated the contrary.

The main contribution of our paper is proving an attacker can use spoofed biometrics to retrieve the private key and an in depth security analysis of the current vulnerabilities of bioPKI. We will run tests on both uni-modal systems comprised of: fingerprint and iris, and multi-modal with both characteristics. The reminder of this paper is organised as follows: Section 2 reviews current research into cryptographic key generation from biometric sources. Section 3 describes the implementation of our system. We will detail methods used for fingerprint and iris feature extraction, feature fusion, fuzzy extractor, RSA key generation. Section 4 details the experiments made, databases used, and interpretation of results related to successful tests and key entropy. Section 5 provides a detailed analysis on how a biometric system can be attacked, the impact of liveness detection, the importance of using good PRNG (pseudo number generator) for RSA key generation. This section can be considered a blueprint for the implementation of bioPKI system covering the full aspect of biometrics, PKI encryption security, and application security. Finally Section 6 concludes the paper.

2. Literature Review

There are many multi-biometric key binding schemes capable of generating cryptographic keys later used to encrypt the biometric template. Most notable template protection schemes are the Fuzzy Vault [22] and the Fuzzy commitment scheme [23]. This section concentrates on proposals related to the scope of our paper: key generation used for symmetric and asymmetric encryption.

Hao et al. [24] proposed a practical way to integrate iris into biometric applications. They detail a method for generating a repeatable string from iris biometrics. This issue is very important because an efficient algorithm should generate the same key from the same biometrics. Iris biometrics tends to have an ERR of 10% to 20%, if no error correcting is applied. To solve the problem the authors proposed a two layer correction system based on Hadamard and Reed-Solomon codes. The algorithm generates a 140 bits key and stores it on a tamper resistant hardware such as a token. This key is enough for 128 bit AES. Ballard et al. [25] introduced a new source of entropy in any biometric system by associating uncertainty with the biometric input. This approach requires a user to remember a low entropy password. The experiments show that 40% of users are able to generate keys that are 2 to 3 times stronger then normal passwords [25]. Jagadeesan et al. [26,27] generated cryptographic keys from feature level fusion of iris and fingerprint. They manage to derive 256 bit cryptographic keys. Kanade et al. [28] proposed a multi-modal regeneration scheme using feature level fusion of iris and face and obtained a long cryptographic key with high entropy. The system can generate 210 bit keys with 183 bit entropy, with FAR of 0% and FRR 0.91%. Abuguba et al. [29] described a method of generating cryptographic keys form face and iris using feature level fusion. The system can generate a 256 bit cryptographic key.

Sharma [30] extracts the fingerprint minutiae and uses it for input into a 64 bit key generation for DES algorithm. Kumar and Kumar [31] proposed a double encryption system to be used for communication. The system implements both: symmetric encryption and asymmetric encryption. The symmetric encryption encrypts the document, while asymmetric encryption is used for key exchange. The private key is stored in palm-print fuzzy vault. Arunachalam and Subramanian [32] proposes a multi-modal AES encryption system, where the encryption key is generated from fingerprint and Finger Knuckle Print (FKP). Minutiae points from fingerprint and key points from FKP are extracted and clustered using K-means algorithm. The resulting centroid is used as key for AES. The authors of [33] propose a multi-biometric system using feature level fusion from two different fingers as input for encryption algorithms. They system is tested on RSA, DES, 3DES and a Proposed Approach. The latter is the only one to offer revocability.

In case of PKI there are two main approaches: classic PKI with an additional security layer consisting of encrypting the private key with biometric data, and direct use of biometric data for RSA key pair generation. The first approach is very easy to implement and might offer better security then classic tokens, because the user doesn't need to remember a password. Various biometrics are used to accomplish this task such as: fingerprints [34], iris [35], two distinct fingerprints [36].

The following are examples of the second approach. Janbandhu and Siyal [37,38] proposed a method of generating keys from any biometrics. The template is XORed with a random number which is imputed through a one way hash function, then the closest prime number relative to $\phi(n)$ is found. Based on this number the RSA private key is found. The algorithm can generate various key sizes. Gong et al. [39] proposed a method of generating PKI keys based on left and right iris codes. Gabor filters method is used for iris feature encoding, then the image is normalised and a 1024 bit key is generated from each RGB channel. All three channels generate a 3072 bit key. The obtained code p is tested for prime using Rabin-Miller Probabilistic Primality Algorithm. If the number is not prime then the next number $p = p - 2$ is tested, if p is an odd number. The algorithm is repeated until a prime number is found. The same method is applied for the other iris code which will generate the q prime. The two large prime numbers p and q are used as input for RSA. Lakshmi and Kiran propose two methods of generation for PKI keys using iris and fingerprint as input. The first method [40] extracts the features from both modalities and performs feature fusion. The key is then generated based on the fused vector. The second method [41] generates a key from every feature, then two large primes are calculated based on the previous keys and used to generate RSA keys. Both methods were presented as a proof of concept and were not tested on large databases.

Next section details our bioPKI premise and tools used for system implementation including: feature extraction for both characteristics, fusion method, fuzzy extractor, RSA key generation.

3. System Implementation Details

We envision a bioPKI system with no need for storing private keys. The biometric data is the user's key. We propose the smartphone as the device used to acquire the biometric data for two main reasons. The latter is no additional devices are needed for biometric capture. Most users have a smartphone and they are accustomed to carrying it with them all the time, and most important take care who has physical access to it. The former is the smartphone's ability to capture many biometrics eliminating the need for multiple devices/sensors. A user will enroll into the bioPKI by providing their biometric data and will be required to install a specialised application on their smartphone. This application will be used for signing or signature verification when needed. The reminder of this section details the techniques and tools used in implementing the proposed system.

3.1. Fingerprint Feature Extraction

A close examination of fingerprints reveal they form a pattern comprised of ridges and valleys. The ridges either end abruptly or converge in different directions. The point where the ridges fluidity is interrupted is called minutiae point. For minutiae extraction we used the system proposed by Kussener [42]. The features extraction follows the steps detailed below:

- *Image pre-processing*, depicted in Figure 1a. Image enhancement is very important because the quality of the extraction process is dependant on the enhancement algorithm. Image enhancement is done by applying Gabor Filter to the image. Another important step in the preprocessing stage is limiting the search of the fingerprint extraction by only detecting and storing the position and orientation of bifurcations and terminations.
- *Image binarization*, depicted in Figure 1b. The purpose of this process is to differentiate between ridges marked with black and furrows marked with white.

- *Image thinning and minutiae extraction*, depicted in Figure 1c. The image is thinned so ridges are only one pixel wide, and all the redundant pixel information is eliminated. For minutiae extraction, the local neighbourhood of each pixel ridge is scanned using a 3 × 3 window. A pixel is either a termination (central pixel is 1 and 1 value neighbour), bifurcation (central pixel is 1 and 3 value neighbour), and usual pixel (central pixel is 1 and 2 value neighbour). The Terminations are marked with red and bifurcations with green.
- *Minutiae processing*, depicted in Figure 1d. This step eliminates minutiae that are too close together. If the distance between a termination and a bifurcation is smaller then a minimum accepted value d, then that minutiae is removed.
- *ROI*, depicted in Figure 1e. A Region of Interest is defined and based on that region the extra minutiae are omitted.
- *Orientation*, depicted in Figure 1f. When the minutiae extraction is complete, the orientation of each element, bifurcation, termination and their respective angles.
- *Binary template.* The extracted points are each binarised resulting in a binary biometric template.

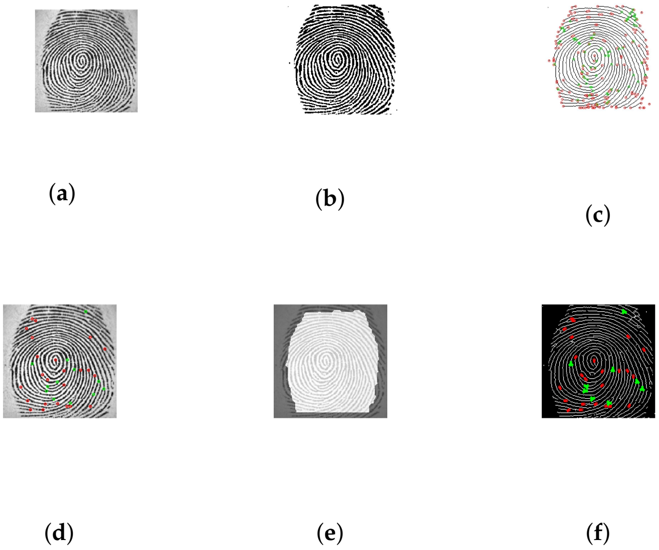


Figure 1. Fingerprint minutiae extraction process. (**a**) Enhanced fingerprint; (**b**) Binarized fingerprint; (**c**) Thinned with minutiae; (**d**) Selected minutiae; (**e**) ROI; (**f**) Minutiae with orientation.

3.2. Iris Feature Extraction

Iris is the coloured middle part of the eye formed during the first year of life. The pattern is random and it's not determined by genetics [43] making it unique even in twins. Iris features are extracted using the open source iris recognition system proposed by Masek [44]. The iris recognition steps are detailed below:

- *Segmentation.* Is the most important step and the success of this step determines the quality of the feature extraction. Image segmentation translates into isolating the iris image from the input image. Circular Hough transform is used to detect the boundaries of iris and pupil. Depending on the database quality specular reflections should be removed. The process is depicted in Figure 2a.
- *Normalisation.* This process creates fixed iris dimensions to allow comparisons, because no two iris images are alike due to different environmental factors when capturing the image, like: distance from the sensor, amount of light. Figure 2b,c depict normalised iris and noise corresponding to normalised image.

- *Feature encoding.* Feature encoding is done using 1D Log-Gabor wavelets, creating a iris bitwise template and a corresponding noise mask.

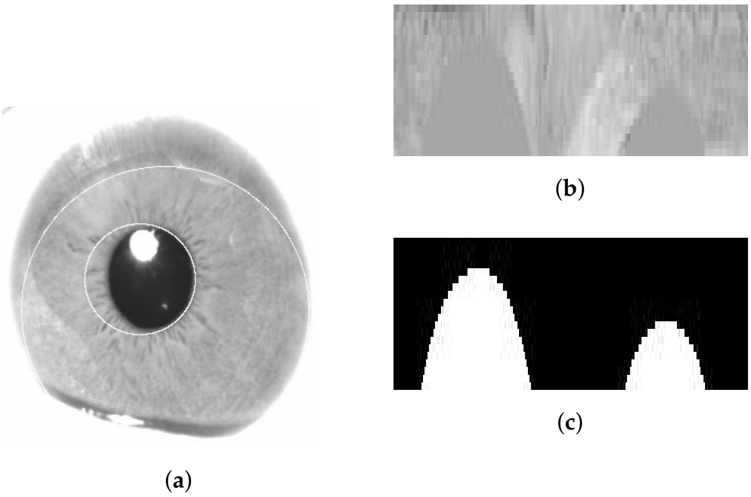


Figure 2. Iris features extraction process. (**a**) Iris segmentation; (**b**) Iris normalised; (**c**) Iris normalised noise.

3.3. Extraction oF Biometric Key

Cryptography needs uniform strings to generate keys, which translates to the ability to generate the same string from the biometric data. Dodis et al. [45] demonstrated that a fuzzy extractor can be generated based on a secure sketch (SS). A fuzzy extractor can be defined as a function which extracts a uniformly random string (key) R from a noisy input w. If the input changes w', but it is close to w, then the same R will be produced. The function produces helper data in the form of P used for recovering the initial input. P doesn't disclose any important information which might be used to recover the key. R doesn't need to be stored because it can be computed making it suitable to be used as seed for RSA. Dodis proposed constructs for different metrics like: hamming distance and set difference. Hamming distance calculates the number of bits changes between w to w'. This metric is considered the best for a multitude of different biometrics. Set difference is defined as the size of the symmetric difference between the two initial sets [45]. The authors demonstrate that in theory there can be optimal secure sketches constructed for this metric, but in practice there are two problems: finding optimal weight codes and sketch size which is directly proportional with the universe size. Due to the large size for these constructs we chose a construct based on hamming distance which will perform faster and better.

Our proposal uses the fuzzy extractor implemented in MATLAB by [46]. The fuzzy extractor will be constructed based on either the fingerprint template, iris template or fused template. Our fuzzy extractor works with a fixed length N = 4095. If the binary biometric vector has less bits then 4095, 1 will be added until the needed value is reached. The syndrome encoder will then output the *key* and $helperData$. The decoding procedure accepts the $nosiyData$ and $helperData$ as input, representing the new biometric sample and the stored helper data, respectively. The decoding procedure will output the new key, called the *noisyKey*. In case of the multi-modal system feature fusion will be performed by creating a fused template using XOR between iris and fingerprint template.

We have implemented RSA key generation in JAVA, using standard implementation. Listing 1 represents a short code snippet for RSA key generation function. The *key* generated by the fuzzy extractor, represented by $features$ parameter, is the seed for the one way hash function used to generate the keys pair. The one way hash function is a specialised Pseudo Number Generator (PRNG) that generates secure random numbers based on the biometric seed. Our RSA implementation generates keys of different lengths specified by the *size* parameter, which can be "512", "1024", "2048". The key pair is then saved in encoded format: x509 encoding for public key and pkcs8 encoding for private key.

Listing 1: Partial listing for RSA key generation.

```
public void generateKey(String features, int size, String fileName,
String path) {
try {
            byte[] featuresBytes = features.getBytes();
            SecureRandom random = SecureRandom.getInstance("SHA1PRNG");
            random.setSeed(featuresBytes);
            KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
            keyGen.initialize(size, random);
            KeyPair generatedKeyPair = keyGen.genKeyPair();
            saveEncodedKeyPair(generatedKeyPair, fileName, size, path);
} catch (Exception e) {
            e.printStackTrace();
            return;
        }
}
```

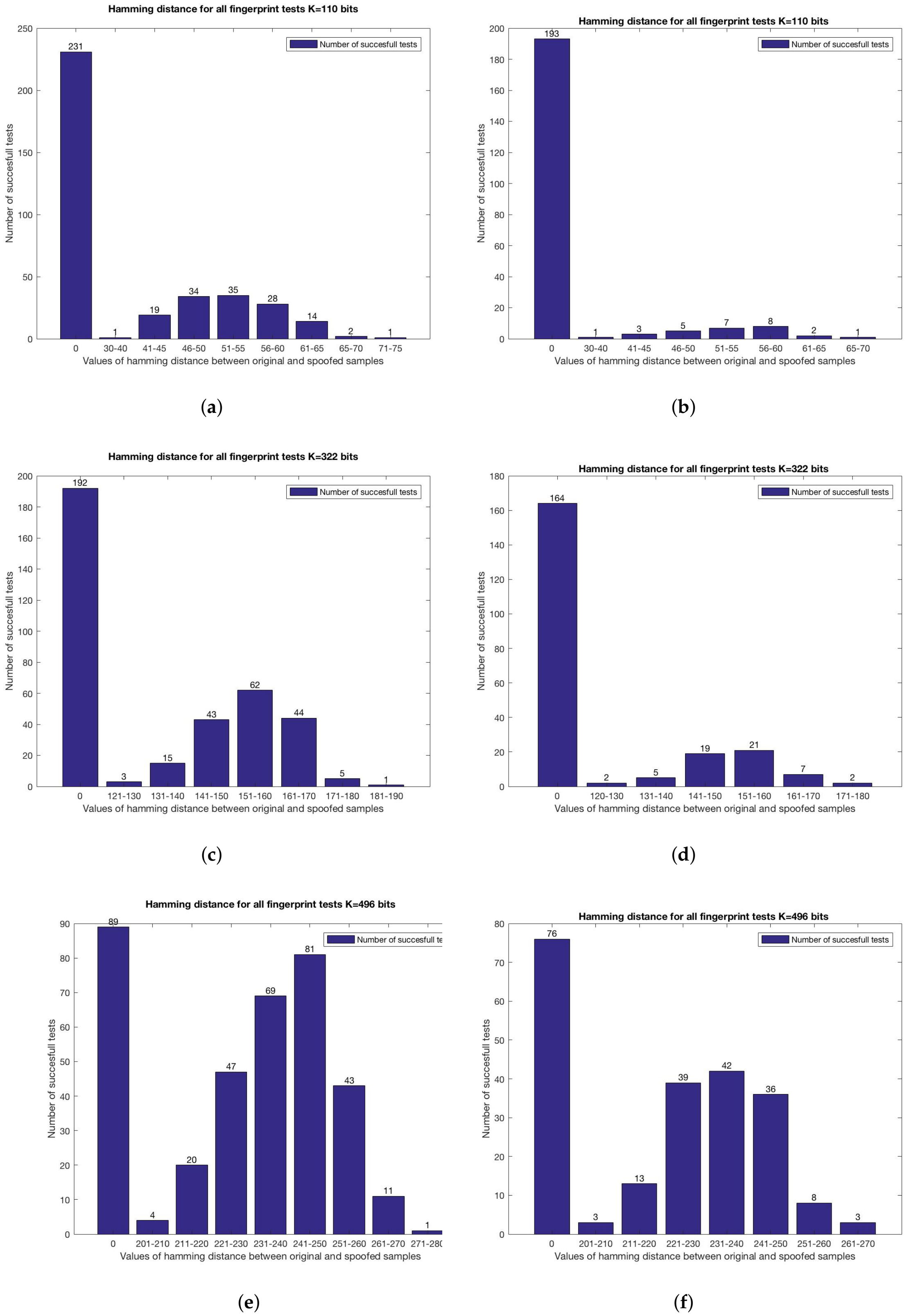
4. Experiments and Results

Biometric PKI's most important feature is not needing a token to store the private key, because the key it's the biometric itself. Biometrics have some important characteristics: they don't need to be remembered, can't be lost and should offer non-repudiation. The former is a requirement for a valid PKI transaction. Naturally a problem with bioPKI is the ease of capturing biometric data without user knowledge. There are ample examples of spoofing biometric characteristics. Many authors [47–51] demonstrated how artificial fingerprints, molded after a latent user fingerprint or a template, can be used to bypass fingerprint authentication systems. The same can be said by iris authentication system which are also susceptible to spoofing [52]. There are methods of detecting spoofed biometrics, but none of them are 100% efficient. For some time it was believed that using multi-modal systems will increase security. As stated in the introduction Section 1, recent studies proved the contrary, that it's enough to spoof only one biometric to have access to the authentication system.

For our tests we have used two databases: ATVS Fake fingerprint database (ATVS-FFp) [53] and ATVS-FIp [54]. We have created two sets of users. SET 1 consists of 25 users comprised of all users in the fingerprint database. The fingerprint database contains a total of 17 users with fake fingerprints obtained with cooperation and 16 users without cooperation, of which 8 same in both, so we chose the ones without cooperation. For the iris database we have chosen in order 25 users to match. SET 2 consists of what we can call a Best Case Scenario, where we have chosen 14 users with the best fake fingerprints and best fake irises. The attack scenario envisions an attacker who captures user's biometric data, and creates spoofed biometric samples to bypass the system. The attacker will provide the fake samples to the sensors in the hope of obtaining the right key.

4.1. Fingerprints

SET 1 consists of 25 users of which 9 sets with cooperation and 16 without cooperation. SET 2 consists of 14 users of which 6 sets with cooperation and 8 sets without cooperation. For both sets we have used the images from ft sensor (thermal). SET 1 contains 20 sets with 4 samples each (for original and fake biometric, 8 in total) and 5 sets with 3 samples each. We haven't been able to extract features from some of the fake samples, so we have limited the set to 3 samples each. SET 2 has only one set with 3 feature vectors. We know that SET 2 is basically a subset from SET 1, but because this is a worst case scenario it, the tests would be more successful, and we wanted to see the differences between what we might call a real life scenario (SET 1) and a worst case scenario like a very passionate attacker (SET 2).



(**a**)

(**b**)

(**c**)

(**d**)

(**e**)

(**f**)

Figure 3. Results for keys derived from fingerprint. (**a**) KEY length 110 bits—Fingerprint hamming distance SET 1 all tests; (**b**) KEY length 110 bits—Fingerprint hamming distance SET 2 all tests; (**c**) KEY length 322 bits—Fingerprint hamming distance SET 1 all tests; (**d**) KEY length 322 bits—Fingerprint hamming distance SET 2 all tests; (**e**) KEY length 496 bits—Fingerprint hamming distance SET 1 all tests; (**f**) KEY length 496 bits—Fingerprint hamming distance SET 2 all tests.

Different keys sizes in bits: 110, 322 and 496 were used for all sets. All the original keys were extracted and the helper data saved. Using the helper data and the fake biometric sample, a noisy key is extracted. This key is compared with the original key, by calculating the hamming distance. If the distance between two keys is 0, it means the key generated by the biometric system is the same. In this case the same key will be sent to the RSA seeder which will result in the same key pair (public and private key). The bigger the distance between the keys the better the key entropy. We run this test for every fake vector and every original key, consisting of 365 tests for SET 1 and 220 tests for SET 2.

For a key length of 110 bits most of the tests were successful, an attacker would have been able to receive the correct key. The results are presented in Figure 3a for SET 1 and Figure 3b for SET 2. SET 1 resulted in 231 tests which yielded a key distance of 0, meaning the reproduction function retrieved the same key as the original. SET 2 resulted in 193 successful tests. These results can be summarised as a success rate of 63.28% for SET 1 and 87.72% for SET 2. The hamming distance for the rejected tests follow the same distribution in both sets. SET 1 had 8 users for which all tests were successful and 2 users with no successful tests. For SET 2 the situation is worse, because all users had at least one successful test. This fact can be translated in at least one spoofed sample was accepted. All key distances for both sets was below 80 indicating the differences between the original and the fake samples are not high. The most disconcerting facts are the the overall successful tests percentages, indicating that running two tests will result in one retrieving the correct key.

The results suggest a key length of 110 for original samples is too low of a key size in the presence of spoofing. As such we have set a key size of 322 bits. The same trend applies for this key size, since most of the tests were successful. There were 192 successful tests for SET 1, representing 62.60% and 164 successful tests for SET 2 representing 74.54%, as depicted in Figure 1c,d. SET 1 had 5 users with all successful tests. The average hamming distance for the unsuccessful is larger then the previous tests and resides between 120 and 170. Both sets have the same distribution for the hamming distance. Even if the percentages for a successful key retrieval are lower, the same trend can be seen here: one in two tests is successful.

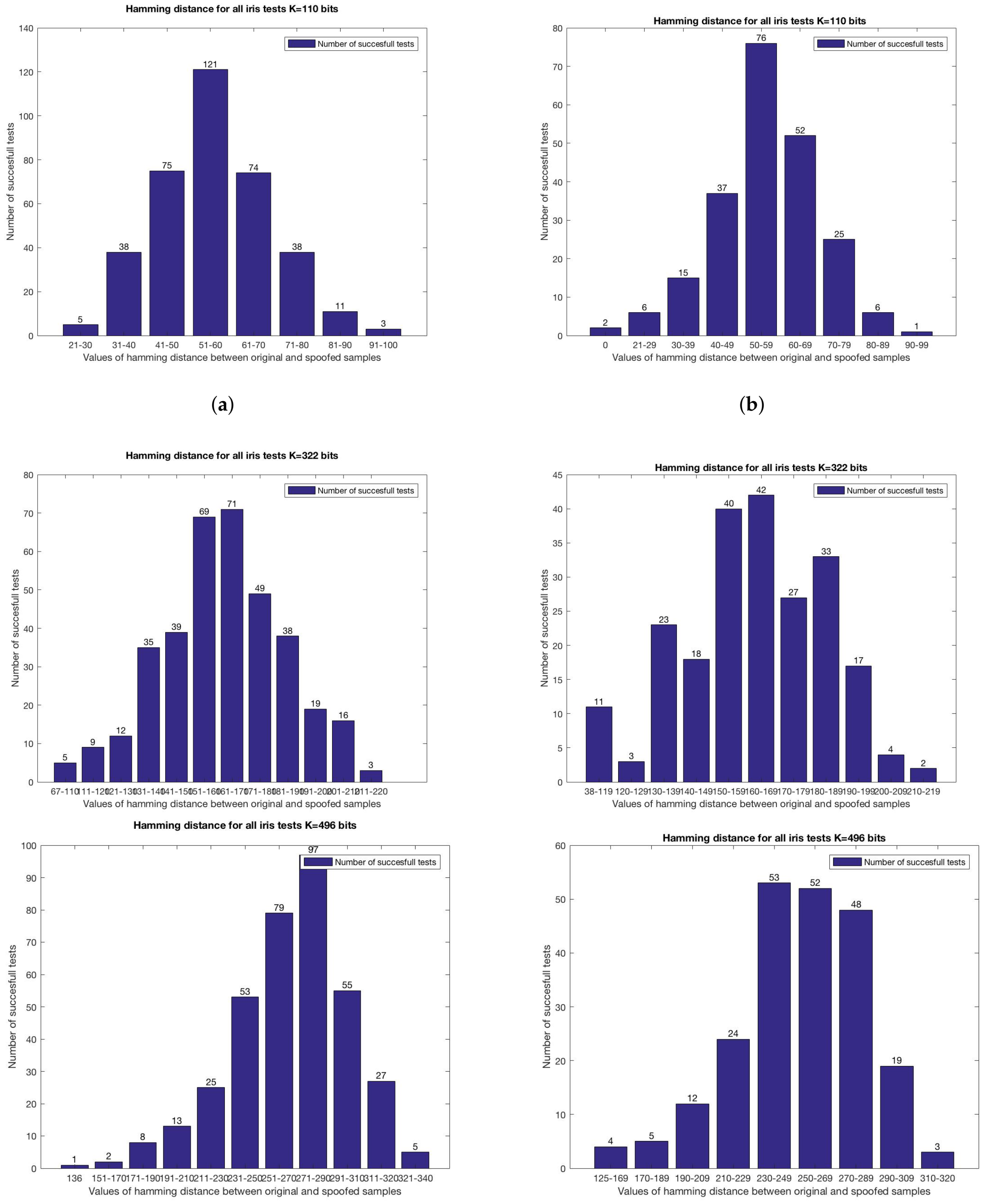
If key length is increased to 496 bits we can see a drastic change in successful key retrieval for spoofed samples, only 89 for SET 1 and 76 for SET 2, representing 24.38% and 34.54%, respectively. The same two users, for both sets, yielded a success rate of 100%, all samples passed. This result is due to very good image quality for both original and spoofed images. Most of the tests resulted in an average of 2 to 4 successful tests per user, for SET 1 and SET 2, respectively. The overall key distance for unsuccessful tests was between 200 and 270, meaning that the spoofed keys had more differences then the previous tests.

The above tests demonstrate what was expected: spoofing biometrics has a direct effect on key retrieval. The better the quality of the spoofed samples the better the chances of correct key retrieval. For the highest key length the average success rate is 1 in 4 tests, and 1 in 2 for the rest. This results are not encouraging because a persistent attacker might follow a victim for days and collect fingerprint samples from various objects the target has touched. It is reasonable to assume that when acquiring more then 40 samples some might good enough to obtain a good quality fake.

4.2. Iris

For iris the same number of samples were created for SET 1 and SET 2 and the same number of total tests were run. We can observe a massive improvement from fingerprint in the form of less successful tests. When the key size is 110 bits we had 0 successful tests for SET 1 and only two from SET 2, as shown in Figure 4a,b. Overall the key distance variation for all iris tests for this key size is between 0 and 100 for both sets.

Figure 4c,d, detail the overall results for key size of 322. There were no successful tests for both sets, but there were 5 and 11 samples from SET 1 and SET 2, respectively, with a variation below 100. Most tests however had a distance between $[150, 190]$ representing an improvement than the previous key length.



(**a**) (**b**)

(**e**) (**f**)

Figure 4. Results for keys derived from iris. (**a**) KEY length 110 bits—Iris hamming distance SET 1 all tests; (**b**) KEY length 110 bits—Iris hamming distance SET 2 all tests; (**c**) KEY length 322 bits—Iris hamming distance SET 1 all tests; (**d**) KEY length 322 bits—Iris hamming distance SET 2 all tests; (**e**) KEY length 496 bits—Iris hamming distance SET 1 all tests; (**f**) KEY length 496 bits—Iris hamming distance SET 2 all tests.

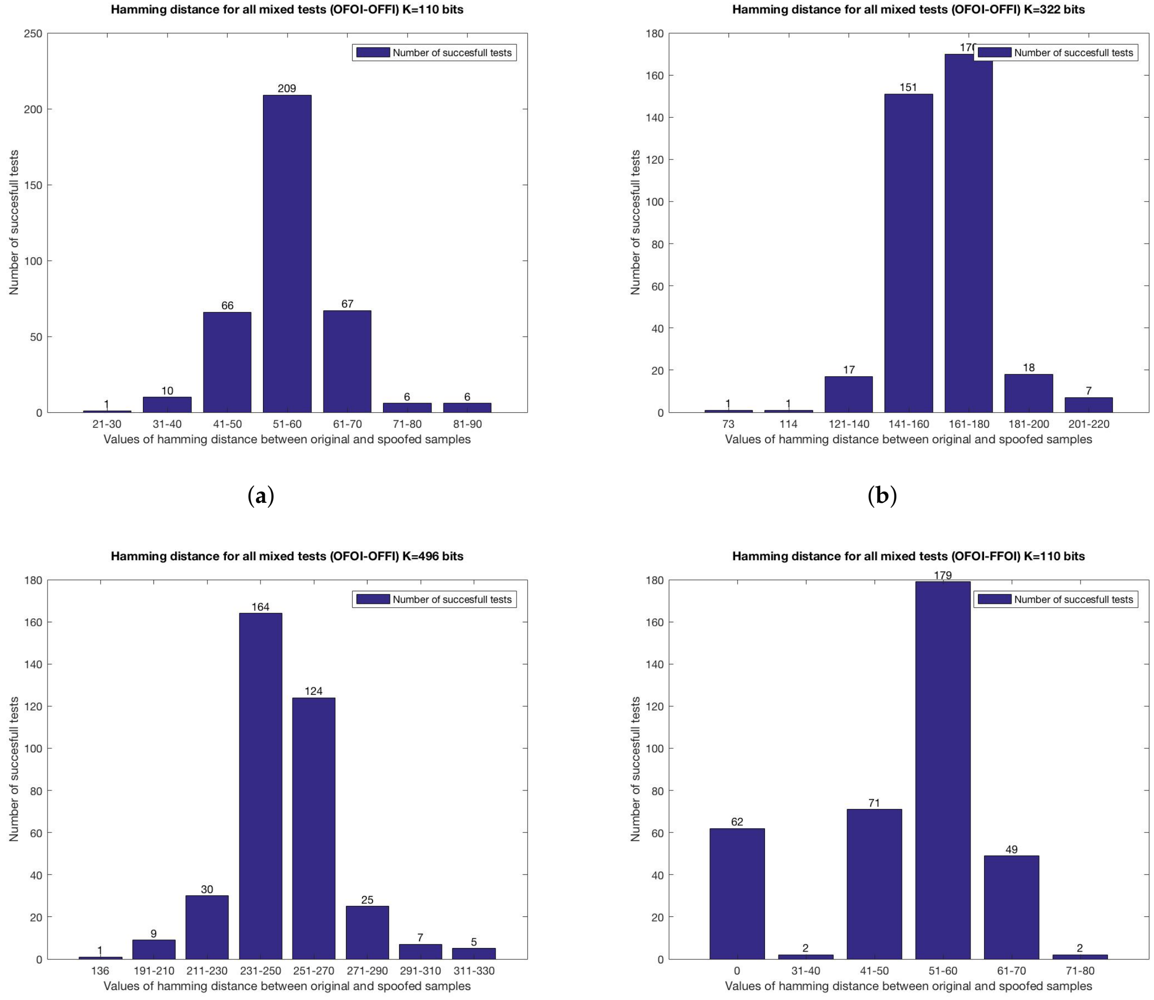
The same ascending key distance trend is seen when the key length is 496 bits, represented by Figure 4e,f. Both sets have a key distance between [230, 300]. As expected the iris biometric is harder to fake then fingerprint, which resulted in worse fake quality, hence worse results were obtained.

4.3. Multi-Biometrics

We have combined the templates for fingerprint and iris and obtained a fused set. SET 1 consists of 25 users and SET 2 of 14 users. In the interest of being concise we present only the graphics for SET 1, because the trend is the same. In case of multi-biometrics we have three different tests, for all three key lengths*:

- OFOI-OFFI Original samples against original fingerprint and fake iris sample.
- OFOI-FFOI Original samples against fake fingerprint and original iris sample.
- OFOI-FFFI Original samples against fake samples for both biometrics.

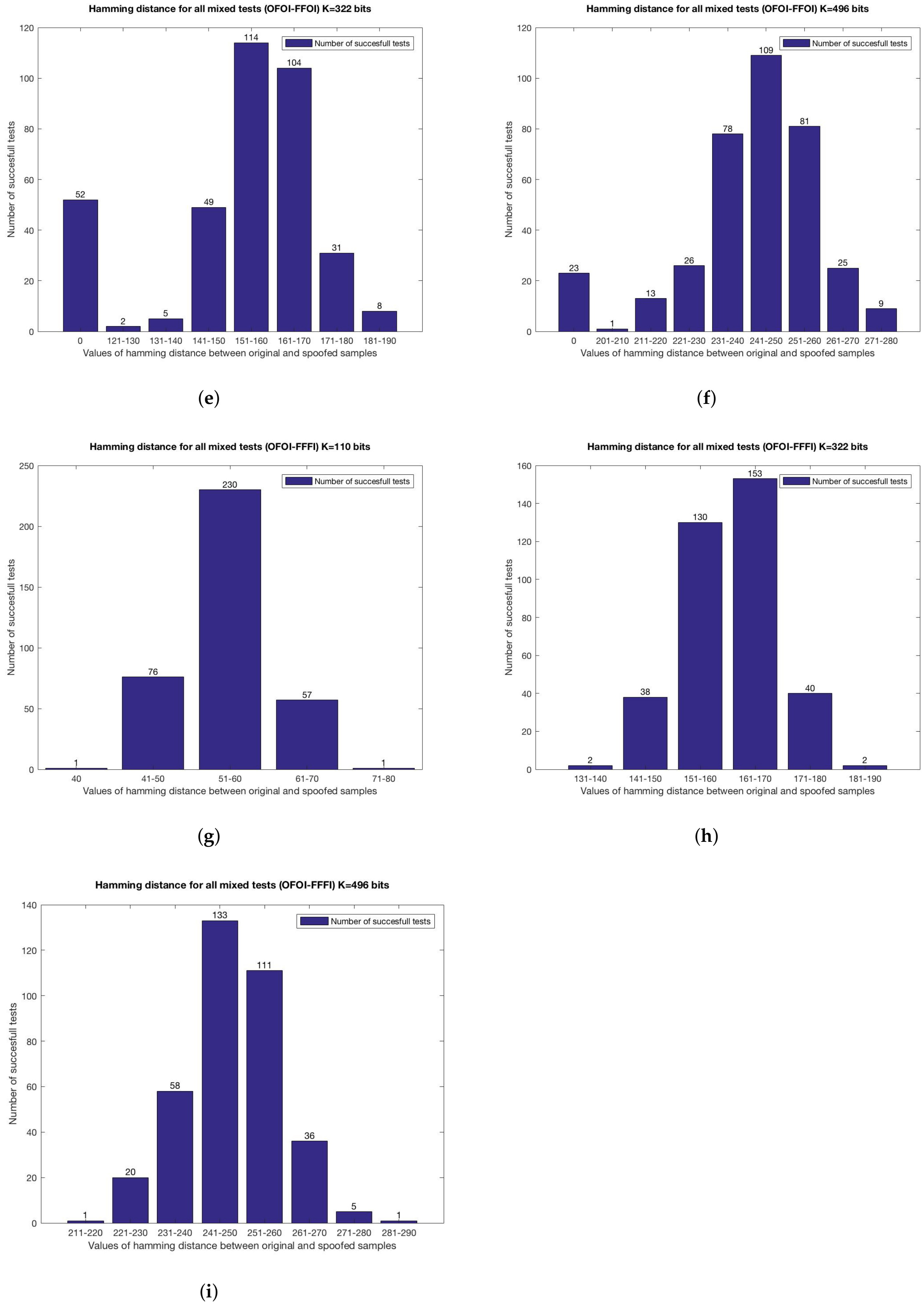
* we have used the following notations: OF (original fingerprint), FF (fake fingerprint), OI (original iris) and FI (fake iris).



(**a**) (**b**)

(**c**) (**d**)

Figure 5. *Cont.*



(**e**)

(**f**)

(**g**)

(**h**)

(**i**)

Figure 5. Comparative results for multi-biometric keys. (**a**) OFOI-OFFI all tests—Key 110 bits SET 1; (**b**) OFOI-OFFI all tests—Key 322 bits SET 1; (**c**) OFOI-OFFI all tests—Key 496 bits SET 1; (**d**) OFOI-FFOI all tests—Key 110 bits SET 1; (**e**) OFOI-FFOI all tests—Key 322 bits SET 1; (**f**) OFOI-FFOI all tests—Key 496 bits SET 1; (**g**) OFOI-FFFI all tests—Key 110 bits SET 1; (**h**) OFOI-FFFI all tests—Key 322 bits SET 1; (**i**) OFOI-FFFI all tests—Key 496 bits SET 1.

To facilitate the understanding we will only present the graphs for the overall tests for SET 1 in Figure 5. SET 1 obtained successful results only in the OFOI-FFOI scenario with 62, 54, and 23 successful tests for key sizes of 110, 322, 496. SET 2 obtained better results, managing to have 3 successful tests for OFOI-OFFI and OFOI-FFFI, and 56 successful tests for OFOI-FFOI, for a key of 110 bits. In both sets OFOI-FFOI tests performed the worst regardless of the key size and had 0 successful tests for all key sizes. The tests are consistent with the previous ones using single biometrics. The fingerprint biometrics performed the worst, that's why every time when FI is used in the mix the number of successful tests drops considerably. In the worst case scenario OFOI-FFOI for the multi-biometric system the results are better then for uni-modal fingerprint, where the success ratios are way higher as depicted in Figure 3. Overall hamming distances are higher in the case of multi-modal system then the fingerprint counter part regardless of the key size, but around the same values with different distribution when compared with the iris one.

We can confirm the findings of studies [19–21] which showed a multi-modal biometric system doesn't offer better security then their uni-modal counter parts. Faking only the fingerprint biometric yielded very good results, not as good as the uni-biometric fingerprint system, but it is still possible to obtain the same key in many cases. Faking only iris biometric and both characteristics the results are similar, meaning there isn't much improvement between the multi-modal biometric system and the iris one.

The next section makes an in-depth analysis of all the important points to have in mind when implementing such a system and creates a blueprint for implementation.

5. Security Analysis

The bioPKI scenario proposed by us has the following steps: a user applies to a CA for a key pair (private/public) and provides the CA with all the necessary documents and biometric data. The CA registers the user and creates and retains the secure sketch and Public key. In a bioPKI system the user never receives the private key, because this key will be derived from the user's biometrics whenever the need. The user will have to carry a device that has the necessary sensors to acquire the biometric data. In our scenario we proposed the smartphone as that device. This analysis relates to the bioPKI system as a whole and some points are not a direct result of the tests performed in Section 4. When implementing a system like the one described above the following issues should be taken into consideration:

5.1. Overall Biometric System Security

A biometric system can be attacked in 8 points depicted in Figure 6 and detailed below:

- *(a) Biometric spoofing*—the biometric characteristic is spoofed and presented to the sensor.
- *(b) Relaying stored signals*—a recorded signal is relayed to the system, overwriting the captured biometric data.
- *(c) Attacking feature extraction*—the feature extraction process itself is under attack, the intruder changes the extracted features with the desired set.
- *(d) Tampering with biometric features*—the extracted features are intercepted before going to the matcher module and replaced with the desired set.
- *(e) Attacking the matcher*—the matcher itself is under attack, meaning the intruder obtains the desired match scores.
- *(f) Attacking the stored templates*—penetrating the biometric database might allow an attacker to reconstruct the original biometric based on the template, or even worse replace a certain template with another one.
- *(g) Communication interception*—the communication between the database and the matcher might be intercepted by an intruder.
- *(h) Attacking the final decision*—an attacker will obtain the desired decision.

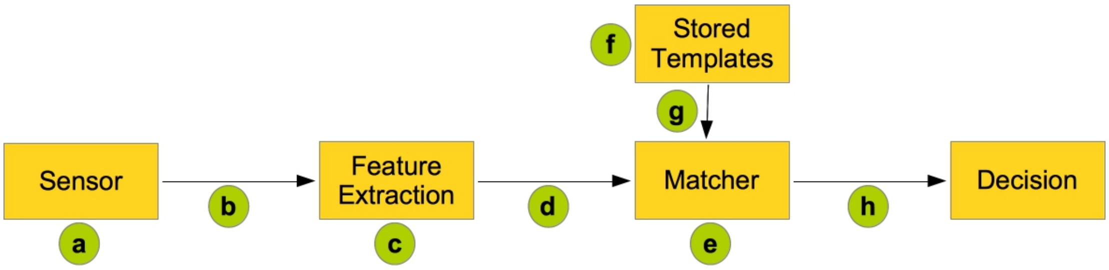


Figure 6. Biometric attack places, as defined by [55].

We can assume that items c to h are secure because they are performed by the CA. The template protection will be assured by the secure sketch. This point is very crucial, considering past attacks on CAs. In the case of a major breach the biometric data will be protected.

The biggest problems the system might face are items *a* (biometric spoofing) and *b* (relaying stored signals). The latter relates to the ability of the sensor or software to detect the fake biometric and the former the communication itself. The user might be tricked into sending his biometrics to a possible attacker or the user's phone might be under the perpetrator's control, which means the communication with the CA might be intercepted. These issues will be discussed in detail later on in our analysis.

5.2. Smartphone Application Security

The user will have to install an application received from the CA that will allow him/her to sign documents or to verify signatures. This application can help secure the bioPKI system against biometric spoofing and communication integrity. Installing the application might not be as easy as it sounds. There is a practice for intruders to masquerade a fake application as a legitimate one. The application store shows the manufactures name for every application, but the users rarely check. To avoid possible confusions the CA should send the link to the application installation in the form of a personalised QR code, and the installation process should make sure the user is who he's supposed to be. The application should have an activation process, and once activated the application should work only from that device and for that particular user. The application installation should be treated as receiving a cryptographic token, having a specialised secure procedure attached to it.

Smarphones are considered the most insecure devices, not because they lack security, but because of user behaviour. The core of a smartphone security system are permissions. A permission allows an application to access a certain phone feature. The problem with this approach is permissions are forever. When an application gains a certain permission no one knows how that permission is going to be used. Applications like Siri (for Apple), Google Now need many permissions, among them microphone. Once the two applications are activated they constantly record. This is a feature for voice recognition searching, but it is very often exploited by attackers.

Many smartphone application developers are misusing permissions. Most applications ask for more permissions than needed, because the producers sell the acquired data to advertisers. This is a practice among the developers of free applications. At first glance selling user data might seem innocent enough, but it might have important consequences in the context of our bioPKI system. The most misused permission is camera and microphone [56]. A smartphone's camera can capture the following biometrics: face, ear, retina, iris, voice and fingerprint if the user touched the back camera with his fingerprint. If this permission is misused by an intruder the user can loose all the biometrics we mentioned.

Over 40% of smartphone applications communicate unknown data to third parties [57]. Most worrisome is the fact that users don't understand the need to check for permissions and sometimes they will install an application that requires root access, translated into complete access to smarphone's features [58]. No one can monitor user behaviour, and a skilful attacker might make a potential victim install a nice game or an application that captures the user biometrics. Another tactic is to steal the smartphone. An attacker might follow a potential target, acquire his password through shoulder surfing or recording. In this case the bioPKI system can be considered compromised. Potential solutions for this problems are user awareness, which can be achieved by a leaflet the user receives when applying for the bioPKI, and a warning system implemented into the application delivered by the CA. The warning system should monitor overall applications behaviour and warn the user of suspicious activities. Being able to monitor everything will most likely require root level access, that might introduce additional vulnerabilities to the user. In the end the PKI application will have to have a balance between permissions and security.

5.3. Liveness Detection

Liveliness detection can be divided into: hardware and software. The former is embedded into the biometric sensor and aims to measure physical characteristics such as: temperature, blood pressure and circulation, skin texture, odor analysis, pulse, pupil dilation. The latter is embedded into the biometric system as software. Hardware liveness detection is very expensive, because it requires intervention at the physical sensor and can only be used for a certain biometrics. Smarphones sensors don't have hardware liveness detection nor it is to be introduced in the near future, mostly because of the increased costs, which will make the phone unattractive to perspective buyers.

There are many techniques for software liveliness detection and most are related to the biometric used. Because of the multitude of methods we have limited the citations to three for each group. Fingerprint liveness detection can be classified into 5 groups: perspiration, skin deformation, image quality, pore, and combined [59]. Perspiration methods rely on capturing multiple images from the same finger and try to determine the perspiration pattern based on various techniques [60–62]. Skin deformation aims in determining skin elasticity which is not present in fake materials used for spoofing [63–65]. The texture of a spoofed material is harsher then the real fingerprint and this fact can be revealed by analysing image quality [66–68]. Pore analysis tries to detect pores in fingerprints [69–71]. The combination group consists of mixing two or more methods from the first four groups [72–74]. Iris software detection uses specific methods mostly: variation in pupil size [75], pupil dynamics and light reflection from cornea [76], structured light that is used mainly for detecting contact lenses with another iris imprinted on them [77].

As stated there are many other techniques each available for the type of biometrics used. The liveness detection software should be installed at CA level, because of temper issues with the users smartphone. Even so, there is still a problem of an attacker installing a malicious software on user's smartphone and capturing live biometrics. This scenario should be prevented by the PKI application warning system.

5.4. Which Biometrics to Use

In the proposed scenario there are two limitations on which biometrics can be used. The first one relates to what sensors can be found on a smartphone. A smartphone can successfully perform 13 authentication types, of which 7 are physiological and 6 behavioural. The physiological ones are fingerprints, face, iris, retina, hand, ear and palmprint, and the behavioural ones voice, signature, gait, behaviour profiling, keystroke dynamics and touch dynamics. A smartphone has other biometric sensors that might be used to gather user data like: acceleration, gravity, gyroscope, magnetometer, rotation. This data can be acquired by monitoring the persons gait. Not all biometrics are alike. Hard biometrics are considered reliable for deriving biometric keys, others not so much. Behavioural biometrics are very easily spoofed, but they can be used for continuous user monitoring. We propose the following hard biometrics to be used for PKI (in order): ocular biometrics (iris and retina), ear—which is one of the most distinctive and non changeable human trait, fingerprint, hand, palmprint, and face.

The second limitation relates to the RSA algorithm itself. The system described uses a derived key extracted from user's biometric data. This key becomes the seed for RSA. It was demonstrated by [78] that hard biometrics can produce good seeds, the data needs to be random enough that it can't be predicted. Behavioural biometrics on the other hand doesn't produce enough random data to be securely used as seed.

Encryption systems need random numbers to generate encryption keys. Hardware random generators are very expensive, and usually used by military devices, so most software applications use specialised functions called Pseudo Number Generators (PRNG). PRNG are capable of generating a sequence of presumably random numbers based on a seed. The entropy and predictability of the seed is very important, because if the seed can be predicted the PRNG generated sequence can be guessed. In our implementation we have used an instance of "SHA1PRNG" secure random generator with the biometric characteristics as seed, as presented in code Listing 1. The standard implementation of a secure random generator generates different keys even when one single modification to the seed is made. The system implementation team must make sure to use a certified PRNG, not an in-house one. Usually the PRNGs implemented in major programming languages pass the entropy tests from the 3 major testing frameworks: (NIST) Statistical Testing Suite (STS) version 2.1.2, ENT test suites and Dieharder.

5.5. Which Fusion Method to Use

Biometric fusion levels are classified into two groups: before matching and after matching [79]. The later consists of: sensor level and feature level fusion, and the former of: score level, rank level and decision level fusion. Even if there are many classifications, experts agree this is the best because the information available reduces significantly after the matching is performed [80]. For biometric cryptosystems the input template must be represented as binary [81]. Feature level fusion is very robust and easy to create especially when applied with an embedding algorithm. The embedding algorithm creates a common representation of all features, in our case a binary representation, then the features are fused by various operations: concatenation, interlacing, XOR - the approach we have taken. A similar approach is proposed by Nagar [82], who creates a multi-biometric cryptosystem comprised of: iris, fingerprint and face. The features are fused together by concatenation of the binary feature representation and stored into a secure sketch. The system is implemented using both fuzzy vault and fuzzy commitment. Fuzzy commitment scheme (FCS) systems obtained through binary biometric concatenation are proposed by: Kelkboom et al. [23] for two 3D face recognition algorithms, and Sutch [83] for face and fingerprint.

Nandakumar [22] implemented a fuzzy vault, by transforming the elements from three biometric sources into Galois Field elements. The biometric sources used are: fingerprint minutia encoding and iris features. The author proposes three implementation of the multi biometric systems with different fusion techniques. The first one uses multiple impressions from the same finger, fuses them together through mosaicing resulting in a mosaiced template. The second proposal fuses through concatenation two instances of fingerprints (ex. right and left index). The third implementation combines the features of both fingerprint and iris. A new concept of hash-level fusion is introduced by [84]. The new proposal can be associated with decision level fusion using AND rule. Hash level fusion is not as flexible as decision level fusion, but obtains better error correction.

From the small review above we can see that there are many of choices available for fusion of biometric cryptosystems. There is no defacto choice, though the approach we have taken is very easy very widely used and very scalable, so the system is easily extendible. The proposed system has a weaknesses it treats every biometric the same, and this is the reason why most of the implementations fuse only hard biometrics.

5.6. No Access to Private Key

This point might seem redundant, since current PKI doesn't allow the user to have access to his private key. Even though there are tools to view the private key in clear, the user still needs a password to access it from the token. In the proposed system the keys are never stored, they are generated every time based on the user biometrics. Let's assume that an attacker provides spoofed data to the biometric system then he gets access to the fake key pair. Having access to a fake private key, which is close enough to the real one, might enable the attacker to know bits from the real key. Then the attacker might launch a partial key exposure attack on RSA [85,86]. When the hamming distance is very low, lets say smaller then 100, then the attacker might retrieve lots of bits from the private key. If an attacker has access to the biometric system and can retrieve the RSA pair generated by the system, the PKI keys might be compromised, even if the original private key is never stored. Depending on how good the fake samples are, the key entropy might be low enough to make the system susceptible to a partial key exposure attack.

6. Conclusions

This paper proposed a bioPKI system where the private key is never stored and it's derived form the user's biometrics. The device used to capture the biometric data is the smartphone. We studied the effect biometric spoofing has on RSA key generation. In case of fingerprint system an attacker can easily spoof biometric data and obtain the correct key. The iris biometric system is better at resisting spoofing. When the multi-modal biometric system is used performance increases significantly compared to uni-biometric counterpart. We have also confirmed the findings of different studies regarding multi-biometric authentication systems, that sometimes using a multi-modal biometric system doesn't increase security.

Our paper includes a detailed security analysis for proposed bioPKI. From the analysis we conclude that implementing a full scale bioPKI shouldn't be rushed, especially if the biometric data is captured by smarphone. Current PKI has it's vulnerabilities, but it's still better then introducing bioPKI now. The smarphone is not a suitable device to collect biometrics given all the security vulnerabilities mentioned in Section 5. A solution will be introducing certified temper resistant sensors, like cryptographic tokens. This solution is not desirable because it presents the same problem the current PKI faces with the cryptographic tokens storage. Such a device must be stored securely and not forgotten in a drawer.

Acknowledgments: The work described in the paper was partially supported by a grant from City University of Hong Kong (Project No. 7004473).

Author Contributions: Lavinia Mihaela Dinca put forward the original idea, performed all the experiments, and has written the paper. Gerhard Hancke reviewed the paper and provided useful comments. Both authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Potter, C.H.; Hancke, G.P.; Silva, B.J. Machine-to-Machine: Possible applications in industrial networks. In Proceedings of the 2013 IEEE International Conference on Industrial Technology (ICIT), Cape Town, South Africa, 25–28 February 2013; pp. 1321–1326.
2. Opperman, C.A.; Hancke, G.P. Using NFC-enabled phones for remote data acquisition and digital control. In Proceedings of the AFRICON 2011, Livingstone, Zambia, 13–15 September 2011; pp. 1–6.
3. Hancke, G.P.; Markantonakis, K.; Mayes, K.E. Security Challenges for User-Oriented RFID Applications within the "Internet of Things". *J. Internet Technol.* **2010**, *11*, 307–313.
4. Markantonakis, K.; Tunstall, M.; Hancke, G.; Askoxylakis, I.; Mayes, K. Attacking smart card systems: Theory and practice. *Inf. Secur. Tech. Rep.* **2009**, *14*, 46–56.

5. Francis, L.; Hancke, G.; Mayes, K.; Markantonakis, K. Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms. In Proceedings of the 2009 International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 9–12 November 2009; pp. 1–8.
6. AlMahafzah, H.; AlRwashdeh, M.Z. A Survey of Multibiometric Systems. *arXiv* **2012**, arXiv:1210.0829.
7. Ross, A.; Shah, J.; Jain, A.K. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Trans. Pattern Anal. Mach. Intell.* **2007**, *29*, 544–560.
8. Jain, A.K.; Nandakumar, K.; Nagar, A. Biometric template security. *EURASIP J. Adv. Signal Process.* **2008**, *2008*, 113.
9. Ratha, N.; Chikkerur, S.; Connell, J.; Bolle, R. Generating Cancelable Fingerprint Templates. *IEEE Trans. Pattern Anal. Mach. Intell.* **2007**, *29*, 561–572.
10. Rathgeb, C.; Uhl, A. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. Inf. Secur.* **2011**, *2011*, 1–25.
11. Patel, V.M.; Ratha, N.K.; Chellappa, R. Cancelable Biometrics: A review. *IEEE Signal Process. Mag.* **2015**, *32*, 54–65.
12. Prins, J.; Cybercrime, B.U. DigiNotar Certificate Authority breach "Operation Black Tulip". Available online: http://www.cs.ru.nl/ klaus/SiO2011/Assignments/rapport.pdf (accessed on 10 February 2017).
13. Farwell, J.P.; Rohozinski, R. Stuxnet and the future of cyber war. *Survival* **2011**, *53*, 23–40.
14. Goodin, D. Certificate Stolen from Malaysian Gov Used to Sign Malware. Available online: https://www.theregister.co.uk/2011/11/14/stolen_certificate_discovered/ (accessed on 13 February 2017).
15. Krebs, B. Signed Malware = Expensive "Oops" for HP — Krebs on Security, 2014. Available online: https://krebsonsecurity.com/2014/10/signed-malware-is-expensive-oops-for-hp/ (accessed on 13 February 2017).
16. Kushnir, K.; Mirmulstein, M.L.; Ramalho, R. *Micro, Small, and Medium Enterprises Around the World: How Many Are There, and What Affects the Count?* Technical Report; World Bank/IFC: Washington, DC, USA, 2010.
17. EU. Stork—What Is It? Available online: https://www.eid-stork.eu/index.php?option=com_content&task=view&id=37&Itemid=61 (accessed on 13 February 2017).
18. Dinca, L.; Hancke, G. A Framework for User-Centric Key Sharing in Personal Sensor Networks. In Proceedings of the INDIN 2016 IEEE International Conference on Industrial Informatics, Poitiers, France, 18–21 July 2016.
19. Rodrigues, R.N.; Kamat, N.; Govindaraju, V. Evaluation of biometric spoofing in a multimodal system. In Proceedings of the 2010 Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), Washington, DC, USA, 27–29 September 2010; pp. 1–5.
20. Akhtar, Z.; Alfarid, N. Robustness of Serial and Parallel Biometric Fusion against Spoof Attacks. In *Computer Networks and Intelligent Computing*; Venugopal, K.R., Patnaik, L.M., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 217–225.
21. Akhtar, Z.; Kale, S. Security Analysis of Multimodal Biometric Systems against Spoof Attacks. In *Advances in Computing and Communications*; Abraham, A., Mauri, J.L., Buford, J.F., Suzuki, J., Thampi, S.M., Eds.; Number 191 in Communications in Computer and Information Science; Springer: Berlin/Heidelberg, Germany, 2011; pp. 604–611.
22. Nandakumar, K.; Jain, A. Multibiometric Template Security Using Fuzzy Vault. In Proceedings of the 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington, DC, USA, 29 September–1 October 2008; pp. 1–6.
23. Kelkboom, E.J.C.; Zhou, X.; Breebaart, J.; Veldhuis, R.N.S.; Busch, C. Multi-algorithm Fusion with Template Protection. In Proceedings of the 3rd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS'09), Washington, DC, USA, 28–30 September 2009; pp. 222–229.
24. Hao, F.; Anderson, R.; Daugman, J. Combining Crypto with Biometrics Effectively. *IEEE Trans. Comput.* **2006**, *55*, 1081–1088.
25. Ballard, L.; Kamara, S.; Monrose, F.; Reiter, M.K. Towards Practical Biometric Key Generation with Randomized Biometric Templates. In Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS '08), Alexandria, VA, USA, 27–31 October 2008; pp. 235–244.
26. Jagadeesan, A.; Thillaikkarasi, T.; Duraiswamy, K. Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature. *Int. J. Comput. Appl.* **2010**, *2*, 16–26.
27. Jagadeesan, A.; Duraiswamy, K. Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris. *arXiv* **2010**, arXiv:1003.1458.

28. Kanade, S.; Petrovska-Delacrétaz, D.; Dorizzi, B. Obtaining cryptographic keys using feature level fusion of iris and face biometrics for secure user authentication. In Proceedings of the 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition—Workshops, San Francisco, CA, USA, 3–18 June 2010; pp. 138–145.
29. Abuguba, S.; Milosavljevic, M.M.; Macek, N. An Efficient Approach to Generating Cryptographic Keys from Face and Iris Biometrics Fused at the Feature Level. *Int. J. Comput. Sci. Netw. Secur.* **2015**, *15*, 6.
30. Sharma, R.K. Generation of Biometric Key for use in DES. *arXiv* **2012**, arXiv:1302.6424.
31. Kumar, A.; Kumar, A. A palmprint-based cryptosystem using double encryption. In Proceedings of the SPIE Defense and Security Symposium, Orlando, Florida, 16–21 March 2008; Volume 6944, pp. 69440D:1–69440D:9.
32. Arunachalam, M.; Subramanian, K. AES Based Multimodal Biometric Authentication using Cryptographic Level Fusion with Fingerprint and Finger Knuckle Print. *Int. Arab J. Inf. Technol.* **2015**, *12*, 431–440.
33. Marimuthu, M.; Kannammal, A. Dual Fingerprints Fusion for Cryptographic Key Generation. *Int. J. Comput. Appl.* **2015**, *122, 20–25.*
34. Nguyen, T.H.L.; Nguyen, T.T.H. An approach to protect Private Key using fingerprint Biometric Encryption Key in BioPKI based security system. In Proceedings of the 10th International Conference on Control, Automation, Robotics and Vision (ICARCV), Hanoi, Vietnam, 17–18 December 2008; pp. 1595–1599.
35. Boukhari, A.; Chitroub, S.; Bouraoui, I. Biometric Signature of Private Key by Reliable Iris Recognition Based on Flexible-ICA Algorithm. *Int. J. Commun. Netw. Syst. Sci.* **2011**, *4*, 778.
36. Dao, V.H.; Tran, Q.D.; Nguyen, T.H.L. A Multibiometric Encryption Key Algorithm Using Fuzzy Vault to Protect Private Key in BioPKI Based Security System. In Proceedings of the 2010 IEEE RIVF International Conference on Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), Hanoi, Vietnam, 1–4 November 2010; pp. 1–6.
37. Janbandhu, P.K.; Siyal, M.Y. Novel biometric digital signatures for internet based applications. *Inf. Manag. Comput. Secur.* **2001**, *9*, 205–212.
38. Janbandhu, P.K.; Siyal, M.Y. Modified Private Key Generation for Biometric Signatures. Available online: https://www.researchgate.net/publication/201599731 (accessed on 10 February 2017).
39. Gong, Y.; Deng, K.; Shi, P. PKI Key Generation Based on Iris Features. In Proceedings of the 2008 International Conference on Computer Science and Software Engineering, Wuhan, China, 12–14 December 2008; Volume 6, pp. 166–169.
40. Lakshmi, A.J.; Kiran, P.S. PKI Key Generation Based On Multimodal Biometrics. *IJCC* **2012**, *1*, 9–16.
41. Lakshmi, A.J.; Babu, R. PKI Key Generation Using Multimodal Biometrics Fusion of Fingerprint and Iris. *Int. J. Eng. Sci. Adv. Technol.* **2012**, *2*, 285–290.
42. Kussener, F. FingerPrint Application—File Exchange—MATLAB Central, 2007. Available online: https://www.mathworks.com/matlabcentral/fileexchange/16728-fingerprint-application (accessed on 13 February 2017).
43. Wildes, R.P. Iris recognition: An emerging biometric technology. *Proc. IEEE* **1997**, *85*, 1348–1363.
44. Masek, L. Recognition of Human Iris Patterns for Biometric Identification. Master's Thesis, The University of Western Australia, Perth, Australia, 2003.
45. Dodis, Y.; Reyzin, L.; Smith, A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In *Advances in Cryptology—EUROCRYPT 2004*; Cachin, C., Camenisch, J.L., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 523–540.
46. Kang, H.; Hori, Y.; Katashita, T.; Hagiwara, M. The Implementation of Fuzzy Extractor is Not Hard to Do: An Approach Using PUF Data. In Proceedings of the 30th Symposium on Cryptography and Information Security, Kyoto, Japan, 22–25 January 2013.
47. Matsumoto, T.; Matsumoto, H.; Yamada, K.; Hoshino, S. Impact of Artificial "gummy" Fingers on Fingerprint Systems. Available online: http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=878135# (accessed on 13 February 2017).
48. Espinoza, M.; Champod, C.; Margot, P. Vulnerabilities of fingerprint reader to fake fingerprints attacks. *Forensic Sci. Int.* **2011**, *204*, 41–49.
49. Galbally, J.; Cappelli, R.; Lumini, A.; Gonzalez-de Rivera, G.; Maltoni, D.; Fierrez, J.; Ortega-Garcia, J.; Maio, D. An evaluation of direct attacks using fake fingers generated from ISO templates. *Pattern Recogn. Lett.* **2010**, *31*, 725–732.

50. Galbally, J.; Cappelli, R.; Lumini, A.; Maltoni, D.; Fierrez, J. Fake fingertip generation from a minutiae template. In Proceedings of the 19th International Conference on Pattern Recognition (ICPR 2008), Tampa, FL, USA, 8–11 December 2008; pp. 1–4.
51. Cappelli, R.; Maio, D.; Lumini, A.; Maltoni, D. Fingerprint Image Reconstruction from Standard Templates. *IEEE Trans. Pattern Anal. Mach. Intell.* **2007**, *29*, 1489–1503.
52. Ruiz-Albacete, V.; Tome-Gonzalez, P.; Alonso-Fernandez, F.; Galbally, J.; Fierrez, J.; Ortega-Garcia, J. Direct Attacks Using Fake Images in Iris Verification. In *Biometrics and Identity Management*; Schouten, B., Juul, N.C., Drygajlo, A., Tistarelli, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 181–190.
53. Galbally, J.; Alonso-Fernandez, F.; Fierrez, J.; Ortega-Garcia, J. A high performance fingerprint liveness detection method based on quality related features. *Future Gener. Comput. Syst.* **2012**, *28*, 311–321.
54. Fierrez, J.; Ortega-Garcia, J.; Torre Toledano, D.; Gonzalez-Rodriguez, J. Biosec baseline corpus: A multimodal biometric database. *Pattern Recogn.* **2007**, *40*, 1389–1392.
55. Ratha, N.; Connell, J.; Bolle, R. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.* **2001**, *40*, 614–634.
56. Felt, A.P.; Chin, E.; Hanna, S.; Song, D.; Wagner, D. Android Permissions Demystified. In Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS '11), Chicago, IL, USA, 17–21 October 2011; pp. 627–638.
57. Labs, Z. 10% of Mobile Apps Leak Passwords, 40% Communicate with Third Parties | Cloud Security Solutions | Zscaler, 2012. Available online: https://www.zscaler.com/press/10-mobile-apps-leak-passwords-40-communicate-third-parties (accessed on 13 February 2017).
58. Zhou, Y.; Jiang, X. Dissecting Android Malware: Characterization and Evolution. In Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–23 May 2012; pp. 95–109.
59. Al-Ajlan, A. Survey on fingerprint liveness detection. In Proceedings of the 2013 International Workshop on Biometrics and Forensics (IWBF), Lisbon, Portugal, 4–5 April 2013; pp. 1–5.
60. DeCann, B.; Tan, B.; Schuckers, S. *A Novel Region Based Liveness Detection Approach for Fingerprint Scanners*; Advances in Biometrics; Springer: Berlin/Heidelberg, Germany, 2009; pp. 627–636.
61. Abhyankar, A.; Schuckers, S. Integrating a wavelet based perspiration liveness check with fingerprint recognition. *Pattern Recogn.* **2009**, *42*, 452–464.
62. Tan, B.; Schuckers, S. Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing. In Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), New York, NY, USA, 17–22 June 2006.
63. Zhang, Y.; Tian, J.; Chen, X.; Yang, X.; Shi, P. *Fake Finger Detection Based on Thin-Plate Spline Distortion Model*; Advances in Biometrics; Springer: Berlin/Heidelberg, Germany, 2007; pp. 742–749.
64. Jia, J.; Cai, L.; Zhang, K.; Chen, D. *A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis*; Advances in Biometrics; Springer: Berlin/Heidelberg, Germany, 2007; pp. 309–318.
65. Tan, B.; Schuckers, S. New approach for liveness detection in fingerprint scanners based on valley noise analysis. *J. Electron. Imaging* **2008**, *17*, doi:10.1117/1.2885133.
66. Nikam, S.B.; Agarwal, S. Ridgelet-based fake fingerprint detection. *Neurocomputing* **2009**, *72*, 2491–2506.
67. Nikam, S.B.; Agarwal, S. Curvelet-based fingerprint anti-spoofing. *Signal Image Video Process.* **2010**, *4*, 75–87.
68. Abhyankar, A.; Schuckers, S. Fingerprint Liveness Detection Using Local Ridge Frequencies and Multiresolution Texture Analysis Techniques. In Proceedings of the 2006 International Conference on Image Processing, Atlanta, GA, USA, 8–11 October 2006; pp. 321–324.
69. Marcialis, G.L.; Roli, F.; Tidu, A. Analysis of Fingerprint Pores for Vitality Detection. In Proceedings of the 2010 20th International Conference on Pattern Recognition, Istanbul, Turkey, 23–26 August 2010; pp. 1289–1292.
70. Espinoza, M.; Champod, C. Using the Number of Pores on Fingerprint Images to Detect Spoofing Attacks. In Proceedings of the 2011 International Conference on Hand-Based Biometrics, Hong Kong, China, 17–18 November 2011; pp. 1–5.
71. Memon, S.; Manivannan, N.; Balachandran, W. Active pore detection for liveness in fingerprint identification system. In Proceedings of the 2011 19th Telecommunications Forum (FOR) Proceedings of Papers, Belgrade, Serbia, 22–24 November 2011; pp. 619–622.
72. Tan, B.; Schuckers, S. Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. *Pattern Recogn.* **2010**, *43*, 2845–2857.

73. Jia, J.; Cai, L. *Fake Finger Detection Based on Time-Series Fingerprint Image Analysis*; Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues; Springer: Berlin/Heidelberg, Germany, 2007; pp. 1140–1150.
74. Marasco, E.; Sansone, C. An anti-spoofing technique using multiple textural features in fingerprint scanners. In Proceedings of the 2010 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, Taranto, Italy, 9 September 2010; pp. 8–14.
75. Bodade, R.; Talbar, S. Dynamic iris localisation: A novel approach suitable for fake iris detection. In Proceedings of the 2009 International Conference on Ultra Modern Telecommunications Workshops, St. Petersburg, Russia, 12–14 October 2009; pp. 1–5.
76. Pacut, A.; Czajka, A. Aliveness Detection for IRIS Biometrics. In Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology, Istanbul, Turkey, 11–15 June 2006; pp. 122–129.
77. Connell, J.; Ratha, N.; Gentile, J.; Bolle, R. Fake iris detection using structured light. In Proceedings of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 8692–8696.
78. Ballard, L.; Kamara, S.; Reiter, M.K. The Practical Subtleties of Biometric Key Generation. In Proceedings of the USENIX Security Symposium, SAN JOSE, CA, USA, 28–1 August 2008; pp. 61–74.
79. Sanderson, C.; Paliwal, K. *Information Fusion and Person Verification Using Speech & Face Information*; Technical Report; IDIAP Research Institute: Martigny, Switzerland, 2002.
80. Ross, A.; Nandakumar, K.; Jain, A. Introduction to Multibiometrics. In *Handbook of Biometrics*; Jain, A., Flynn, P., Ross, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 271–292.
81. Mai, G.; Lim, M.H.; Yuen, P.C. Fusing binary templates for multi-biometric cryptosystems. In Proceedings of the 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), Arlington, VA, USA, 8–11 September 2015; pp. 1–8.
82. Nagar, A.; Nandakumar, K.; Jain, A.K. Multibiometric Cryptosystems Based on Feature-Level Fusion. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 255–268.
83. Sutcu, Y.; Li, Q.; Memon, N. Secure Biometric Templates from Fingerprint-Face Features. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR '07), Minneapolis, MN, USA, 17–22 June 2007; pp. 1–6.
84. Merkle, J.; Kevenaar, T.; Korte, U. Multi-modal and multi-instance fusion for biometric cryptosystems. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG) (2012 BIOSIG), Darmstadt, Germany, 6–7 September 2012; pp. 1–6.
85. Boneh, D.; Durfee, G.; Frankel, Y. *An Attack on RSA Given a Small Fraction of the Private Key Bits*; In Advances in Cryptology—ASIACRYPT'98; Springer: Berlin/Heidelberg, Germany, 1998; pp. 25–34.
86. Blömer, J.; May, A. *New Partial Key Exposure Attacks on RSA*; Advances in Cryptology—CRYPTO 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 27–43.