A Survey of the Security and Privacy Measures for Anonymous Biometric Authentication Systems

Ileana Buhan
Information and Systems Security
Philips Research Laboratories
ileana.buhan@philips.com

Emile Kelkboom
Information and Systems Security
Philips Research Laboratories
emile.kelkboom@philips.com

Koen Simoens
ESAT/COSIC
Katholieke Universiteit Leuven and IBBT
koen.simoens@esat.kuleuven.be

***Abstract*—The challenge in applying the known information theoretical measures for biometric authentication systems is that on one hand these measures are defined in a specific context and on the other hand there are several constructions known for the protection of biometric information. The goal of this work is to organize and conceptualize the existing knowledge in the area of security of biometrics and build a bridge between the formal model of cryptography and the practical view of the signal processing area. It is the scope of this paper to build and present the framework where results from both cryptography and signal processing can be integrated.**

I. Introduction

Biometric security systems that verify a persons identity by scanning fingerprints, irises or faces are becoming more and more common. Authentication with biometrics requires comparing a registered or enrolled biometric sample (biometric template or identifer) against a newly captured biometric sample (for example, a fingerprint captured during a login). Biometric authentication is not perfect and the output of a biometric authentication system can be subject to errors due to imperfections of the classification algorithm, poor quality of biometric samples, or an adversary who has tampered with the biometric authentication systems. Although biometric authentication is intended primarily to enhance security, storing biometric information in a database introduces new security and privacy risks. Anonymous biometric authentication techniques allow the authentication of users without requiring the server to store a biometric reference information [4]. They were proposed to mitigate the risk of storing biometric information. The main challenge in building anonymous biometric authentication is the unpredictable nature of the biometric data. Security and privacy measures for anonymous biometric authentication estimate the chances of success of an adversary who is not honest and behaves maliciously. Security and privacy for anonymous biometric authentication is studied from two different, complementary and sometimes conflicting angles. On the one hand, cryptography offers elegant theoretical models, which transform noisy, non-uniform strings into reproducible, uniform strings suitable for cryptographic purposes. These models have to offer precise formalisms and concrete adversarial models while making minimal assumptions. The problem is that due to the minimal assumptions, results are mostly of theoretical interest. The signal processing area deals mostly with the practical aspects of the recognition process, like algorithms for detecting the reliable features in a biometric sample, pattern recognition techniques, etc. The emphasis is put on the building blocks and their performance trade-offs with models that are less formally defined compared to cryptography. Although security and privacy are recognized as being important, their analysis is mostly superficial often missing the specification for the adversarial model.

It is the scope of this paper to build and present the framework where results from both cryptography and signal processing can be integrated. A common starting point to present results is beneficial for both. Practical results from the signal processing area would benefit by the formalisms that cryptography has to offer, while taking a closer look at the more realistic data models and authentication scenarios could lead to new, exciting results. The challenges in building the common frame to present results are twofold. Firstly, there are several methods, which can achieve anonymous biometric authentication and that are conceptually different. For example, the fuzzy extractor [1] constructs during enrollment a reproducible, uniform string from the biometric sample collected during enrollment that is reconstructed during authentication only if the biometric sample presented during authentication is close in terms of a predefined distance to the enrollment biometric sample. Cancelable biometrics applies a transformation function on the biometric sample collected during enrollment and during authentication [3]. Authentication is achieved if the transformed biometric samples are close with respect to a pre-defined distance measure. Secondly, security and privacy measures are defined for a specific theoretical construction (fuzzy extractor, fuzzy sketch, etc.) and for a given model of the input data (biometric data can be represented as discrete variable or as continuous variables).

Our contributions are threefold: firstly, we propose a model for authentication that is general to all the known models of anonymous biometric authentication. Secondly we propose a generic enrollment function that is composed from four generic building blocks that cover most of the transformations that can be applied to transform the biometric data into suitable input to cryptographic purposes. Thirdly, we present the known measures for security and privacy in the context and constraints in which they were defined.

II. Biometric Authentication and Anonymous Biometric Authentication

A. Biometric Authentication

A biometric authentication system is a computational process that involves two parties: a user (Alice) and a biometric server (Bob). Bob is assumed to have a database $\mathcal{D} = \{b_1, b_2, ..b_M\}$ of M biometric signals. Authentication with biometrics is a two step process. The first step is enrollment. During enrollment Bob learns the identity of Alice and stores a reference of her identity, b_A in database $\mathcal{D}$. The second step is verification. During verification Alice provides b'_A to Bob who verifies whether the biometric measurement of the claimed identity (b_A) matches b'_A. It is an established fact that two biometric measurements collected from the same person are almost never exactly the same. Therefore Bob uses a distance function d to asses whether b_A and b'_A are within a pre-defined range. Biometric measurements collected from the same person are, in most cases, closer ($d(b_A, b'_A) \leq t$) than biometric measurements collected from different persons ($d(b, b'_A) > t$).

Definition 1 (BAS): A $(\mathcal{D}, d, t)$-biometric authentication system (BAS) is a computational protocol between two parties, Bob who has access to biometric database $\mathcal{D}$, and Alice with a probe b_A such that at the end of the protocol, Bob can compute $v = 1$ if $(\exists) b^* \in \mathcal{D}$ such that $d(b_A, b^*) \leq t$ and $v = 0$ otherwise.

We note that a biometric authentication system can run in two modes. The first is *verification* when Alice claims an identity $b_i \in \mathcal{D}$ and Bob verifies the claim by computing the distance between the claimed identity b_i and the provided sample b_A. The second is *identification* where Alice makes no identity claim and Bob matches b_A against all biometric identities in the database $\mathcal{D}$. In this paper by authentication we refer to the verification scenario.

B. Anonymous Biometric Authentication

Biometric information is classified as highly sensitive because it might *reveal sensitive information*, such as ethnic origin, gender or medical condition. Some of these attributes are disregarded when the biometric measurements are processed and biometric templates are generated. Nonetheless, these kinds of results indicate a potential exposure of sensitive information in current biometric systems and give Bob additional, unnecessary information about Alice. Also biometric data is relatively unique and stable over time, both qualities being essential for authentication purposes. However, biometric data cannot be reissued. If Bob's database is compromised and the information in the database is revealed, Alice cannot use her biometrics for the purpose of authentication. Another privacy threat spurred by the widespread use of biometric applications is the *ability to track users* across applications by comparing biometric references facilitated by the uniqueness and persistence of biometric characteristics. To model this scenario we assume Bob, the biometric server has access to set of databases $\mathbf{D} = \{\mathcal{D}_1, \mathcal{D}_2, \cdots \mathcal{D}_N\}$. Each biometric database corresponds to a service or an application. To access service i, Alice has to prove to Bob that her identity is stored in database $\mathcal{D}_i$. As opposed to BAS authentication, Alice will not present the probe b^*, but an authentication secret g^* derived from b_A. Similarly, Bob will not store biometric samples but the secret $g*$ derived from them. We emphasis that Bob never receives $b*$ but only the secret g^*.

Definition 2 (ABAS): A $(\mathbf{D}, T, d, t)$ anonymous biometric authentication system (ABAS) is a computational protocol between two parties, Bob the biometric server who owns a set of databases $\mathbf{D} = \{\mathcal{D}_1, \mathcal{D}_2, \cdots \mathcal{D}_N\}$ and Alice with an authentication secret g derived from the probe b_A with the following properties at the end of the protocol:

1) Bob can compute $T(g, g*) = 1$ if $(\exists) g^* \in \mathcal{D}_i$ derived from a probe b^* such that $d(b_A, b^*) \leq t$;
2) Except for the authentication result $v = T(g, g^*)$ for $g^* \in \mathcal{D}_i$ Bob has negligible knowledge about the probes b_A, b^* (to try and reconstruct them) and insufficient knowledge about the comparison results between $d(b_A, b^*)$ to conduct, e.g. a hill-climbing attack;
3) Except for the authentication result $v = T(g, g^*)$ of the $(g^* \in \mathcal{D}_i)$ Bob cannot obtain any verification result $v' = T(g, g')$ of the $(g' \in \mathcal{D}_j)$ for $(\forall) j \neq i$;

In the following section we look at the known constructions for the realization of an ABAS.

III. Generic construction for ABAS systems

The enrollment and authentication in an ABAS involves a non-invertible transformation of the biometric signal during enrollment that allows the reconstruction of a secret value when a similar biometric is presented during authentication. There are several known generic constructions (summarized in table I) that Bob can use to construct an ABAS. These construction vary on the accepted input (discrete vs continuous signals), the reconstructed secret and the security guarantees that can be offered.

When using a *fuzzy sketch*, during enrollment Bob applies function F on the biometric x and the output is $F(x) = p$, which is public. Bob stores p. During authentication function G is applied on the biometric x' presented by Alice and the stored p. If x' is close enough, function G will output $G(x', p) = x$. A fuzzy sketch reconstructs the biometric signal recorded during enrollment. An alternative to the fuzzy sketch is a *fuzzy extractor*. A fuzzy extractor transforms a noisy, non-uniform biometric measurement into a uniform

Table I
OVERVIEW OF KNOWN CONSTRUCTIONS FOR BIOMETRIC TEMPLATE PROTECTION.

Definition	Enrollment	Authentication	Test	Public Information
Fuzzy Sketch [1]	$F(x) = p$	$G(x', p) = x^*$	$T(x, x^*) \in \{0, 1\}$	$p, h(x), F, G, T$
Fuzzy Extractor [1]	$F(x, r) = (p, s)$	$G(x', p, r) = s^*$	$T(s, s^*) \in \{0, 1\}$	$p, r, h(s), h(r)F, G, T$
Fuzzy Embeder [2]	$F(x, k) = p$	$G(x', p) = k^*$	$T(k, k^*) \in \{0, 1\}$	$p, h(k), F, G, T$
Cancelable Biometrics [3]	$F(x, k) = p$	$G(x', k) = p^*$	$T(p, p^*) \in \{0, 1\}$	p, k, F, G, T

and reproducible sequence. During enrollment, Bob applies function F on the biometric x and on the explicit random parameter r that extracts a public sketch p and a secret s. The goal of the authentication stage is to reconstruct the secret s by applying function G on the biometric sample presented by Alice and the public sketch p. A *fuzzy embedder* binds the biometric to a binary string k, generated externally. When using a fuzzy embedder Bob applies function F to the biometric input x and key k and stores the result $F(x, k) = p$ in the database. The goal of the authentication stage is to reconstruct the binary string k using function G on input x' provided by Alice and public sketch p provided by Bob. When using *cancelable biometrics* Bob applies function F on the biometric measurement x of Alice. The function F has to be probabilistic therefore Bob adds an explicit parameter r to function F. The transformed biometric $F(x, r) = p$ is stored in the database. During authentication the same transformation is applied to the biometric measurement provided by Alice x' and Bob compares whether the two transforms are close enough. Generically, we can model the enrollment as a function F that Bob applies on inputs: x-the biometric sample, r-the explicit random value and k-the external source of randomness. The result of the enrollment stage is $F(x, r, k) = (p, s)$ is a public sketch p and a secret value s. The parameters of the authentication function vary according to the specifics of each particular construction, but generically it is applied on: x'- the noisy version of biometric, p-the public sketch and r-the random value when F is a probabilistic function. The result of the authentication stage is $G(x', p, r) = g^*$ where $g^* \in \{h(x), h(s), h(k)\}$ the *authentication secret* can be either x the biometric measurement collected during enrollment, s-the noise free, uniform biometric sequence or k the external source of randomness. Part of the authentication process is also the binary test function T that compares the result of the enrollment and authentication process. The test function T will not work on the values x, s and k directly, but on transformed values $h(x), h(s)$ and $h(k)$, where h is a collision-free one-way function that does not reveal any data about its input. In practice, such functions are implemented by cryptographic hash functions, which we assume leak no information on their input. Generically we write $T(h(x), h(s), h(k), g^*) = 1$ if Bob can authenticate Alice and $T(h(x), h(s), h(k), g^*) = 0$ if Bob fails to authenticate Alice. Definition 3 formalizes the construction of an $ABAS$ as described above.

Definition 3 (Construction ABAS): An $(\mathbf{D}, F, G, T, d)$-ABAS is a construction of an $(\mathbf{D}, T, d)$-ABAS between Bob, the biometric server and Alice who wants to be authenticated, which proceeds as:

1) During enrollment Alice computes $F(x, r, k) = (p, s)$ and gives Bob the value p and $g \in \{h(x), h(s), h(k)\}$.
2) During authentication Alice computes the authentication secret $G(x', r, p) = g^*$ where $g^* \in \{h(x), h(s), h(k)\}$ and Bob verifies the authentication secret by using the test function $T(h(x), h(s), h(k), g^*)$, which returns 1 when $d(x, x') \leq t$.

In the following sections we establish the terminology with respect to the meaning of security and privacy in the context of anonymous biometric authenticators.

IV. SECURITY AND PRIVACY ATTRIBUTES FOR BIOMETRIC KEY AUTHENTICATORS

Before the various security and privacy threats can be described in more detail, one first needs to define what security and privacy mean in the context of biometrics. To formalize the concepts of privacy and security, Breebart, *et. al* [4] introduce the concept of Trusted Biometric System (TBS). The TBS takes as inputs a biometric characteristic and an identity claim, and as outcome produces the verification decision. Hence the TBS represents the ideal biometric system, where for example all the components function as expected and the various components inside the TBS are not accessible to fraudulent attackers. The security of a TBS can be understood as the difficulty to obtain a false accept. Similarly, privacy can be understood as the level of protection against an attacker that tries to obtain any other information than a verification decision from the stored verification information and a claimed identity.

In the context of biometric authentication systems Ye, *et. al* [5] classify adversarial behaviors broadly in two classes: semi-honest and malicious. A semi-honest adversary follows the protocol faithfully but attempts to find out additional information about the other parties involved in the protocol. A malicious adversary can change private inputs and even attempt to disrupt the protocol by premature termination. Security in the context of ABAS can be understood as the difficultly for Charlie, a malicious adversary, to convince Bob that he is Alice. Charlie knows the public parameters, the functions used during enrollment and authentication and can change private inputs in the functions used during authentication. Charlie cannot control the enrollment process and cannot change the information stored by Bob in the database. Privacy in the context of ABAS is defined in the presence of a semi-honest Bob, who can use the information stored in the database to learn more information about Alice. An example in this sense is the race, gender, medical condition of Alice but also the types and frequency of application and services that Alice uses.

V. Security Measures against a computationally unbounded adversary

We note that our purpose is to illustrate the known measures for security and privacy in the context and constraints in which they are defined. The key element in this sense is the enrollment function F that determines the properties of the authentication secret, the amount of tolerated noise and the amount of information that is leaked to an adversary. In the following section we propose an enrollment function that is constructed using four generic building blocks (quantization, error correction, extractor and randomization), which takes as input a noisy, non-unifom, continuously represented biometric measurement and transforms it into a reproducible, uniform binary feature vector. The building blocks form a logical decomposition, a typical enrollment function must not use all blocks in figure 1, some can use only quantization, others error correction and/or randomization, etc. Moreover the order of the blocks can be different compared to Figure 1 or some blocks can overlap. We argue, however that each of the four blocks solves a well defined problem and in the following we take a closer look at the purpose and requirements for each of the four blocks.

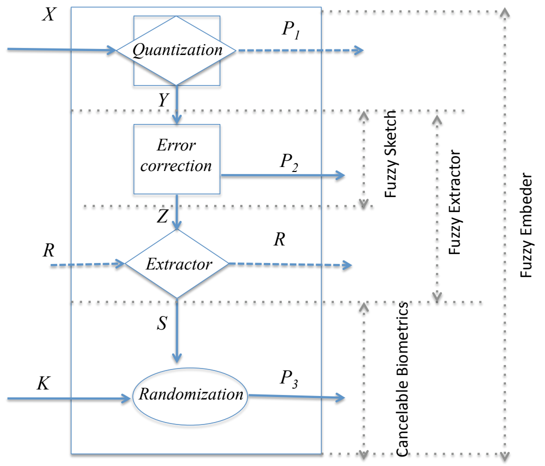

Figure 1. Building blocks for a generic enrollment function F. The shape of the building block is a code for its function: square blocks can do error correction, rhombus blocks do distribution shaping and the round block does randomization.

A. *Building blocks for the enrollment function*

The enrollment function described in figure 1 shows the building blocks for a generic enrollment function $F(x, r, k) = (p, s)$ that transforms a continuous variable X into a discrete random variable Y by quantization, transforms the noisy variable Y into a reproducible sequence Z, extracts all randomness from Z into the uniform variable S and diversifies the reproducible, uniform sequence S with the help of an external source of randomness K. We argue that the model described in figure 1 covers most of the work done in the area of construction of cryptographic keys from noisy data. Theoretical work in the area usually covers the error correction block and randomness extraction [1], [6] whereas others, look at more practical aspects like quantization [7], [8] or randomization [10].

QUANTIZATION. The quantization block is used to transform continuously distributed data X with probability density function $f_X(x)$ into discretely distributed data Y with discrete probability density $f_Y(y)$. This block can shape the probability density function distribution $f_X(x)$ into $f_Y(y)$ and changes the continually distributed data into discretely distributed data. Gersho, [11] describes quantization as a mechanism whereby information is thrown away, keeping only as much as is really needed to reconstruct the original value to within a desired accuracy as measured by some fidelity criterion. Formally, a quantizer is a function $Q : X \rightarrow Y$ that maps $x \in X$ into a *reconstruction point* $y \in Y$ by $Q(x) = \min_{y \in Y} d(x, y)$ where d is the distance measure defined on X.

A "known trick" to improve the performance of a quantizer is to store *user specific information*, which is computed during enrollment and used during authentication. Common types of user specific information are: the error offset for a specific user $e_{\mathcal{X}} = Q(\mathcal{X}) - \mathcal{X}$ [12], [2] or information regarding the distinguishability of a feature component [13]. User-specific quantization functions are superior in terms of the false accept vs. false reject trade-off compared to user-independent quantization function. However the former will leak user information (P_1 in figure 1) while the latter will leak no information.

ERROR CORRECTION. The error correction block adds redundant information to the input variable Y to increase the probability that its values are correctly reproduced. The input variable $Y = (Y_1, Y_2, \cdots Y_n)$ is represented as a n-dimensional vector and its elements Y_i are called feature vectors. There are two types of noise that can occur in Y. The first is *additive noise* where elements of Y_i are perturbed by noise and the second is *replacement noise* where some features of Y can disappear and new features can appear between two consecutive measurements. To perform error

Table II
INFORMATION THEORETICAL MEASURES OF SECURITY AND PRIVACY.

Notation	Description
Charlie has no information about Alice	
$H(Y); H(S); H(K)$	**Shannon entropy.** Measures the probability Charlie guesses $Y = y$ in an *average case* scenario (the probability of y is close to the probability of the expected value of the distribution of Y). The same measure can be used to evaluate the strength of S and K.
$H^{\delta}_{\infty}(Y)$	**Smooth min-entropy.** Measures the probability that Charlie guesses $Y = y$ in an *almost worst case* scenario (the probability of g is δ-smaller compared to the element with the maximum probability in $f_Y(y)$). It cannot be applied to S and K because both are assumed to be uniformly distributed, therefore there is need to eliminate δ-entropy.
$H_{\infty}(Y); H_{\infty}(S); H_{\infty}(K)$	**Min-entropy.** Measures the chance that Charlie guesses the value of $Y = y$ in a *worst case* scenario (y is the element with the highest probability in the probability distribution associated to Y). Min-entropy represents the probability that Charlie guesses the value of the key from 1 trial. It can be used also for variables S and K.
$G(Y); G(S); G(K)$	**Guessing entropy.** Represents the average *number of guesses* needed to guess the authentication secret when Charlie is using the optimal strategy. Can be applied to any discrete variable, so it makes sense to use it on Y, S, K.
$SD(Z, U)$	**Statistical distance.** It measures how close the distribution of Z is to the uniform distribution U. This is a measure of distinguishability; any system in which U is replaced by Z will behave exactly the same as the original with probability 1-$SD(Z, U)$.
Charlie knows the public sketch $P = (P_1, P_2, P_3)$	
$H(Y\|P_2)$,$H(K\|P_3)$	**Conditional entropy.**Measure the chances of Charlie predicting Y (average case) when P_2 is known to Charlie. It can also be used to measure the chance of Charlie predicting K when he knows P_3.
$\tilde{H}_{\infty}(Y\|P_2)$,$\tilde{H}_{\infty}(K\|P_3)$	**Average min-entropy.** Measures, for random P_2 and P_3 the average chances of Charlie predicting Y or K (worst case), when P_2 or P_3 respectively is known to him.
Measures the amount of information Bob knows	
$I(X; P_1)$	**Mutual Information.** Measures the amount of common information between P_1 and X.
$H_{\infty}(Y) - \tilde{H}_{\infty}(Y\|P_2)$,$H_{\infty}(K) - \tilde{H}_{\infty}(K\|P_3)$	**Entropy loss.** It is used as a performance measure and measures the amount of entropy that is lost by making the sketch public. Can be used on both Y and K variables.
$H^{Q}_{\infty}(Y) - H^{Q}_{\infty}(Y\|P_2)$	**Relative entropy loss.**The measure represents the number of additional bits that could have been extracted if an optimal quantization function is used. It makes sense to use it when entropy is evaluated for a variable obtained after a quantization function is used.

correction a *public sketch* (also called *helper data*) is computed for Y. If the helper data is made public, which is the case in most scenarios, it reveals information about the variable Y. Error correction schemes which correct additive noise where proposed by several authors among which [12] while error correction schemes for replacement noise can be found in [10], [14]. The performance of an error correction scheme is measured in terms of *errors correction* and *information leakage*.

EXTRACTORS. This block is used to transform *any* probability density function $f_Y(y)$ into a *uniform* probability function $f_Z(z)$, which is desirable for a cryptographic algorithm. A randomness extractor is used to "purify" the randomness coming from an imperfect source of randomness, it can efficiently convert a distribution that contains some entropy (but is also biased and far from uniform) Y into an almost uniform random variable Z. The performance of a randomness extractor is measured in terms of the statistical distance between the distribution of the output variable Z and the distribution of a uniform random variable R, in figure 1. In the process of randomness extraction an external source of randomness must be present. Reducing the randomness in the external source and producing outputs, which are as close as possible to a uniform distribution is the main research topic in this area [15], [16].

RANDOMIZATION. When biometrics is used as a noisy source, the purpose of randomization is the protection of privacy. For example, from one fingerprint only one reproducible, uniform string can be extracted. The randomization ensures that from one fingerprint multiple random sequences can be produced. Randomization can be done by xor-ring the uniform, reproducible binary biometric (S in figure 1) with another binary sequence (K in figure 1), as in the code-offset construction introduced by Dodis, *et. al* [1], by asking a random, binary, question to each feature and store the answer [17], adding chaff points [10] or by applying a transformation function as in the case of cancelable biometric schemes [3].

B. Information theoretic measures of security and privacy

The challenge in describing the known information theoretical measures is that on one hand not all enrollment function use all blocks and on the other hand not every measure can be used in any context, for instance, min-entropy cannot be used on continuously distributed random variable. We found about a dozen measures, see table II. for both security and privacy, each capturing a different aspect and measure of protection against a semi-honest and malicious adversary. In the context of security we are interested in the probability that Charlie predicts a random value, in this case the authentication secret. For Charlie we model two scenarios, in the first scenario Charlie has no information about Alice while in the second scenario Charlie knows the public sketch of Alice. Information theoretical measures for Charlie consider the probability of the value he has to guess within the probability distribution of the variable to be predicted. In the context of privacy common measures in the literature define the amount of information that Bob can learn about the input data.

When using table I as a guide for which measures to use in the context of a given enrollment function, we first recommend to look at three aspects (1) the goal of the adversary (2) the properties of the variable to be guessed, in other words the type of authentication secret that is used (biometric, binary biometric sequence or an external random sequence see table I) and (3) the building blocks of the enrollment function, which gives an indication of the trade-offs that have to made and choose the ones that are relevant.

Acknowledgement

This work was sponsored in part by the EU project TURBINE, which is funded by the European Community's Seventh Framework Program (FP7/2007-2013) under the grant agreement nb. ICT-2007-216339. Also we would like to thank the anonymous reviuwers for their suggestion to improve this paper.

References

[1] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data." in *EUROCRYPT 2004, Interlaken, Switzerland*, ser. LNCS, vol. 3027. Springer, May 2004, pp. 523–540.

[2] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Embedding renewable cryptographic keys into continuous noisy data," in *10th International Conference on Information and Communications Security (ICICS)*, ser. LNCS, vol. 5308. Birmingham, UK: Springer-Verlag, Oct. 2008, pp. 294–310.

[3] N. Ratha, S.Chikkerur, J.H.Connell, and R.Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on pattern analysis and machine intellingence*, vol. 29, no. 4, April 2007.

[4] J. Breebaart, B. Yang, I. Buhan, and C. Busch, "Biometric template protection – the need for open standards," in *Datenschutz und Datensicherheit – DuD*, vol. 33, no. 5, 2009, pp. 299–304.

[5] R. Wei and D. Ye, "Delegate predicate encryption and its application to anonymous authentication," in *Proceedings of the 2009 ACM, ASIACCS 2009, Sydney, Australia,*. ACM, 2009, pp. 372–375.

[6] Y. Dodis and A. Smith, "Correcting errors without leaking partial information," in *STOC, Baltimore, MD, USA*, ACM, May 2005, pp. 654–663.

[7] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Fuzzy extractors for continuous distributions," in *ACM, ASIACCS, Singapore*, R. Deng and P. Samarati, Eds. New York: ACM, March 2007, pp. 353–355

[8] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates." in *ASIACRYPT 2006, Shanghai, China*, ser. LNCS, vol. 4284. Springer, December 2006, pp. 99–113.

[9] W. Zhang, Y. Chang, and T. Chen, "Optimal thresholding for key generation based on biometrics," in *Proceedings of the IEEE 2004 International Conference on Image Processing (ICIP 2004), Singapore*. IEEE Computer Society, October 2004, pp. 3451–3454.

[10] E. Chang and Q. Li, "Hiding secret points amidst chaff," in *EUROCRYPT, 2006 Saint Petersburg, Russia*, ser. LNCS,vol. 4004. Springer, May 2006, pp. 59–72.

[11] A. Gersho, "Priciples of quantization," *IEEE Transactions on Circuits and Systems*, vol. CAS-25, no. 7, pp. 16–29, September 1978.

[12] J. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates." in *4th International Conference on Audio-and Video-Based Biometrie Person Authentication (AVBPA 2003), Guildford, UK*, ser. LNCS, vol. 2688. Springer, June 2003, pp. 393–402.

[13] P. Tuyls, A. Akkermans, T. Kevenaar, G. Schrijen, A. Bazen, and R. Veldhuis, "Practical biometric authentication with template protection." in *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA 2005), Hilton Rye Town, NY, USA*, ser. LNCS, vol. 3546. Springer, July 2005, pp. 436–446.

[14] U. Uludag, S. Pankanti, and A. Jain, "Fuzzy vault for fingerprints," in *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication, (AVBPA 2005) Hilton Rye Town, NY, USA*, ser. LNCS, T. Kanade, A. K. Jain, and N. K. Ratha, Eds., vol. 3546. Springer, July 2005, pp. 310–319.

[15] B. Barak, R. Impagliazzo, and A. Wigderson, "Extracting randomness using few independent sources," *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS'04), Roma, Italy*, vol. 45, pp. 384–393, October 2004.

[16] L. Trevisan and S. Vadhan, "Extracting randomness from samplable distributions," in *Proceedings of the 41st Annual Symposium on Foundations of Computer Science,Redondo Beach, CA, USA*, vol. 41. IEEE Computer Society, 2000, pp. 32–42.

[17] Y. Sutcu, S. Rane, J.Yedidia, S. Draper, and A. Vetro, "Feature transformation of biometric templates for secure biometric systems based on error correcting codes," in *Computer Vision and Pattern Recognition Workshops, 2008. CVPRW '08. IEEE Computer Society Conference on*, 2008, pp. 1–6.

[18] R. Renner and S. Wolf, "Simple and tight bounds for information reconciliation and privacy amplification," in *Advances in Cryptology ASIACRYPT*, ser. LNCS, B. Roy, Ed., vol. 3788. Springer, December 2005, pp. 199–216.

[19] U.Uludag, S.Pankanti, and A. Jain, "Fuzzy vault for fingerprints," in *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication, (AVBPA 2005) Hilton Rye Town, NY, USA*, ser. LNCS, vol. 3546. Springer, July 2005, pp. 310–319.