BioPACE: Biometric-Protected Authentication Connection Establishment

Nicolas Buchmann[*], Christian Rathgeb[*], Roel Peeters[†], Harald Baier[*] and Christoph Busch[*]

[*]da/sec Biometrics and Internet Security Research Group
Hochschule Darmstadt, Darmstadt, Germany
firstname.lastname@h-da.de

[†]KU LEUVEN, ESAT/COSIC & iMinds, Belgium
firstname.lastname@esat.kuleuven.be

December 13, 2013

0.1 Introduction

The regulations of the European Union (EU) Council in 2004 form the basis for the deployment of electronic passports within the EU [21, 22]. Since then EU member states adopt the format and the access protocols to further electronic machine readable travel documents (eMRTD) like national electronic ID cards and electronic residence permits, respectively. Currently issued ePassports feature an embedded radio frequency chip which contains sensitive biometric data. Typically the ePassport holder's facial image and fingerprints of two index fingers [28]. The electronic storage and wireless communication channel lead to several risks which have to be addressed with appropriate security protocols. Access control mechanisms protect the privacy of the ePassport holder's fingerprints, i.e. only trusted parties may access them and confidentiality of the transferred data is achieved by encrypting all communication between the travel document's chip and the inspection system. Further security protocols ensure authenticity and integrity of all data read from the chip, as well as the chip's originality.

Security protocols used in the eMRTD domain follow the paradigm of strong cohesion and loose coupling, i.e. each protocol fulfils a very specific security goal and the security protocols hardly depend on each other, if there is a dependency at all. This paradigm is well established in the software engineering community [30, 35]. Due to this principle further chip equipped cards (e.g., electronic ID cards) with similar security goals can utilize a subset of the ePassports' security protocols and replace an ePassport protocol by a new one where appropriate. This does not only create a benefit for the electronic ID cards, but instead a mutual gain, because if an improved security protocol is favoured in the electronic ID card domain it might replace the ePassport counterpart in the long term. This is currently the case for the Password Authenticated Connection Establishment (PACE, [9]), which is expected to replace the Basic Access Control (BAC) protocol by the PACE-based Supplemental Access Control (SAC) in 2018 [29].

The recently introduced BioPACE protocol proposes to replace the knowledge-based shared 'secret' of PACE by a biometric-based secret instead [20, 11]. This protocol represents the centre of our discussions, where the goal of this book chapter is twofold:

1. we evaluate the BioPACE protocol and perform a security assessment. We highlight design decisions which strengthen the protocol against common attacks and

2. we discuss state-of-the-art biometric template protection schemes as well as the entropy provided by different biometric characteristics which are most suitable to integrate BioPACE into the eMRTD domain.

We sketch the idea of replacing the expensive Extended Access Control (EAC) protocols and their related Country Verifying Public Key Infrastructure (CV PKI) by BioPACE. An initial evaluation reveals that BioPACE actually has the potential to serve as replacement, if some of the conveniences of EAC are considered to be dispensable (e.g., fine-grained authorisation levels to different data groups).

The remainder of this chapter is organised as follows: Section 0.2 describes the eMRTD security protocols and their security goals, which are relevant for the subsequent discus-

sion of BioPACE. Fundamentals of biometric template protection and state-of-the-art schemes are discussed in Section 0.3. Section 0.4 is about the PACE protocol, which represents the basis building block for the BioPACE protocol. In Section 0.5 the concept and underlying idea of BioPACE is introduced. The security assessment of BioPACE is presented in Section 0.6. Entropy of different biometric characteristics is the focus of Section 0.7. Section 0.8 presents a future perspective to replace EAC with our BioPACE, and discusses the expediency of our BioPACE in the eMRTD domain. In Section 0.9 conclusions are drawn and the achievements of BioPACE are summarised.

0.2 eMRTD protocols and their security goals

Each eMRTD security protocol fulfils a very specific security goal, as summarised in table 0.1. The protocols are either specified by the International Civil Aviation Organisation (ICAO) [28] or the German Federal Office for Information Security (BSI) [9], and are well described in [41].

Table 0.1: eMRTD security protocols and their security goals.

Protocol name	**Security goal**	**Cryptographic method**
Passive Authentication	Authenticity/Integrity of eMRTD data	PKI/Digital Signature
Basic Access Control	Authorisation/Session key establishment	Shared Secret/Encryption
Active Authentication	Originality of the chip	Challenge/Response
Chip Authentication	Originality of the chip	Diffie-Hellman
Terminal Authentication	Terminal access validation	PKI/Challenge Response

Passive Authentication is the only protocol, which is specified as mandatory by the ICAO [28]. It provides authenticity and integrity of the data stored on the chip. Therefore a cryptographic hash is calculated for every data group stored on the chip, and this hash list is electronically signed by the eMRTD issuer with a digital signature. The hash list and the digital signature are stored on the chip in a special file termed Document Security Object, which can be read by the terminal, after performing BAC/PACE, in order to validate the authenticity and integrity of the read data groups, by verifying the digital signature. Passive Authentication depends on the so-called *Signing PKI*.

Basic Access Control (BAC) provides protection against unauthorised access to the data stored on the chip [28]. Unauthorised means access to the data without the eMRTD owner handing over the document. To get access to the chip the terminal needs optical access to the data page in order to read the Machine Readable Zone (MRZ). The terminal authenticates itself to the chip with the data read from the MRZ, and both entities agree

on session keys during BAC to establish a secure channel which provides authenticity, integrity and confidentiality of the transferred data by means of the *Secure Messaging* sub-protocol.

To protect the sensitive data groups, which contain biometric data, BAC is not sufficient. Therefore *Extended Access Control* (EAC) protects data group 3 (DG3), which contains the fingerprints. EAC consists of *Terminal Authentication* and *Chip Authentication* [9]. After performing EAC the terminal can read the fingerprints, capture a biometric sample from the eMRTD holder, and compare the biometric data to check if the current eMRTD holder is the legitimate owner, i.e. the linkage security goal is achieved.

To prevent chip cloning, two protocols exist in the eMRTD domain. *Active Authentication* (AA) specified by the ICAO [28] and as part of EAC *Chip Authentication* (CA) specified by the BSI [9]. Both protocols prove the authenticity of the chip (originality) to the terminal. AA achieves this goal with a challenge-response protocol and CA establishes a strong secure channel based on the Diffie-Hellman protocol to implicitly prove the originality of the chip.

Terminal Authentication (TA) is part of EAC and is a protocol by which a terminal can prove to a chip its access right to the sensitive biometric data [9]. The chip forces every terminal to prove its authorisation to DG3 before granting access to the fingerprints. TA is based on a PKI for terminals called the *Country Verifying PKI*.

0.3 Fundamentals of biometric template protection

The industry has long claimed that one of the primary benefits of biometric templates is that original biometric signals acquired to enrol a data subject cannot be reconstructed from stored reference data (templates). Several techniques, e.g. [14, 50], have proven this claim wrong. Since most biometric characteristics are largely immutable, a compromise of raw biometric data or biometric templates might result in a situation that a subject's biometric characteristics are essentially *burned* and not usable any longer from the security perspective. Biometric template protection technologies offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at a high security level.

0.3.1 Categorization

Biometric template protection schemes are commonly categorized as,

1. *Biometric cryptosystems*, also referred to as helper data-based schemes and
2. *Cancelable biometrics*, also referred to as feature transformation.

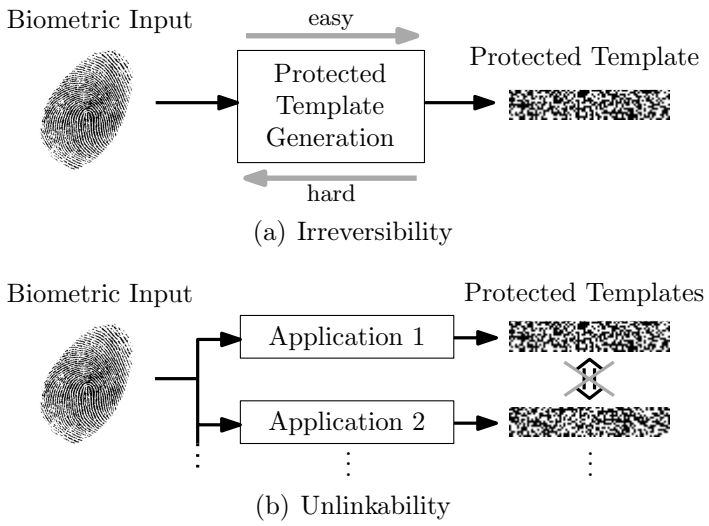
Biometric cryptosystems are designed to securely bind a digital key to a biometric or generate a digital key from a biometric [15], offering solutions to biometric-dependent

key-release (Biocryptographic Key Infrastructure [53]) and biometric template protection [16, 36]. Cancelable biometrics consist of intentional, repeatable distortions of biometric representations (i.e., templates) based on transforms which provide a comparison of biometric templates in the transformed domain [46]. In accordance with the ISO/IEC IS 24745 [31] based on biometric information protection, technologies of biometric template protection are designed to meet two major requirements:

1. *Irreversibility*, i.e. it should be computationally hard to reconstruct the original biometric template from the stored reference data (protected template), while it should be easy to generate the protected biometric template;

2. *Unlinkability*, i.e. different versions of protected biometric templates can be generated based on the same biometric data (renewability), while protected templates should not allow cross-matching (diversity).

Schematic illustrations of both properties are shown in Figure 0.1(a) and Figure 0.1(b).



(a) Irreversibility

(b) Unlinkability

Figure 0.1: Template protection: security properties required by ISO/IEC IS 24745.

0.3.2 Advantages

Biometric cryptosystems and cancelable biometrics offer several advantages over generic biometric systems. Most important advantages are summarized in table 0.2 on the next page. These major advantages over conventional biometric systems call for several applications. With respect to the design goals, biometric cryptosystems and cancelable biometrics offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at an high security level. Several new issues and challenges arise deploying these technologies [16].

Table 0.2: Major advantages of technologies of biometric template protection.

Advantage	**Description**
Privacy protection	Within biometric cryptosystems and cancelable biometrics the original biometric template is obscured such that a reconstruction is hardly feasible.
Secure key release	Biometric cryptosystems provide key release mechanisms based on biometrics.
Pseudonymous authentication	Authentication is performed in the encrypted domain and, thus, the biometric reference is a pseudonymous identifier.
Revocability and renewability of templates	Several instances of secured templates can be generated.
Increased security	Biometric cryptosystems and cancelable biometrics prevent from several traditional attacks against biometric systems.
More social acceptance	Biometric cryptosystems and cancelable biometrics are expected to increase the social acceptance of biometric applications.

0.3.3 Issues

One fundamental challenge, regarding template protection, represents the issue of alignment, which significantly effects recognition performance. Biometric templates are obscured within both technologies, i.e. alignment of obscured templates without leakage is highly non-trivial. For instance, if iris biometric textures or templates (iris-codes) are transformed in a non-row-wise manner, e.g. block permutation of preprocessed textures or a permutation of iris-code bits. Consequentially, additional information, which must not lead to template reconstruction, has to be stored [49].

Focusing on biometric template protection technologies it is not actually clear which biometric characteristics to apply in which type of application. In addition, stability of biometric features is required to limit information leakage of stored helper data [55]. In addition, feature adaptation schemes that preserve accuracy have to be utilized in order to obtain common representations of arbitrary biometric characteristics. Several approaches to extract fixed-length binary fingerprint templates have been proposed, e.g. [8, 67].

As a variety of different approaches to biometric cryptosystems and cancelable biometrics has been proposed a large number of pseudonyms and acronyms have been dispersed across literature such that attempts to represented biometric template protection schemes in unified architectures have been made [6]. Standardization on biometric tem-

plate protection has been achieved in the ISO/IEC IS 24745 [31], providing guidance on the protection of an individual's privacy during the processing of biometric information.

0.3.4 State-of-the-art

Focusing on the current state-of-the-art in biometric template protection key approaches to biometric cryptosystems and cancelable biometrics are summarized in table 0.3 on the following page. Representing one of the simplest key binding approaches the fuzzy commitment scheme [38] has been successfully applied to iris recognition [27] (and other biometrics). The fuzzy vault scheme [37] which represents one of the most popular biometric cryptosystem has frequently been applied to fingerprints. Early approaches, e.g. [17], which required a pre-alignment of biometric templates, have demonstrated the potential of this concept. Several techniques, e.g. [60, 45], to overcome the shortcoming of pre-alignment have been proposed. Quantization schemes, e.g. [63, 57], have been applied to several physiological and behavioural biometrics, while focusing on reported performance rates, these schemes require further studies in order to improve accuracy. Besides, approaches which aim at "salting" existing passwords with biometric features have been proposed [44]. Within the BioHashing approach [24] biometric features are projected onto secret domains applying user-specific tokens prior to a key-binding process. Variants of this approach have been exposed to reveal impractical performance rates under the stolen-token scenario [40]. With respect to recognition rates, the vast majority of biometric template protection schemes are by no means comparable to conventional biometric systems. While numerous approaches to biometric cryptosystems generate rather short keys at unacceptable performance rates, several enrolment samples may be required as well, e.g. four samples in [17]. Approaches which report practical recognition rates are tested on rather small datasets, e.g. 70 persons in [27], which must not be interpreted as significant. In addition, the introduction of additional tokens, be it random numbers or secret PINs, often clouds the picture of reported results.

First approaches to non-invertible transforms [46] (representing an instance of cancelable biometrics), which have been applied to face and fingerprints, include block-permutation and surface-folding. Diverse proposals, e.g. [68, 26], have shown that recognition performance decreases noticeably compared to original biometric systems. Additionally, it is doubtable if sample images of transformed biometric images are non-invertible. BioHashing [24] (without key-binding) represents the most popular instance of biometric salting yielding a two-factor authentication scheme. Since additional tokens have to be kept secret, e.g. [51, 65], result reporting turns out to be problematic. Perfect recognition rates have been reported, e.g. in [25] while the opposite was found to be true [40] within the stolen-token scenario.

Table 0.3: Experimental results of key approaches to template protection schemes.

Author(s)	Applied technique	Modality	FRR / FAR (%)	Remarks
[27]	Fuzzy commitment	Iris	0.42 / 0.0	small test set
[7]			5.62 / 0.0	short key
[17]	Fuzzy vault	Fingerprints	20-30 / 0.0	pre-alignment, >1 enroll sam.
[45]			4.0 / 0.004	>1 enroll sam.
[66]		Iris	5.5 / 0.0	–
[23]	Quantization	Online sig.	28.0 / 1.2	>1 enroll sam.
[63]			7.05 / 0.0	short key
[44]	Password-hardening	Voice	>2.0 / 2.0	short key
[58]	BioHashing	Face	0.0 / 0.0	non-stolen token
[47]	Block permutation, Surface folding	Fingerprints	$\sim$35 / 10^{-4}	–
			$\sim$15 / 10^{-4}	
[43]	BioConvolving	Online Sig.	10.81 EER	–
[25]	BioHashing	Face	0.0002 EER	non-stolen token

0.4 PACE: Password authentication connection establishment

The *Password Authenticated Connection Establishment* (PACE) fulfils the same security goals as BAC, but provides strong session keys even in the presence of low-entropy passwords, and contrary to BAC is resistant against off-line brute-force attacks [9]. The shared password is denoted by π and can either be received from the MRZ, a PIN, or the Card Access Number (CAN), which is printed on the data page of the eMRTD and consists of a six digit number. PACE is based on symmetric and asymmetric cryptography, while BAC is based solely on symmetric cryptography. PACE is depicted in Figure 0.2 and roughly consists of the following steps:

1. First the eMRTD chip randomly chooses a nonce s and encrypts it with K_π which is derived from the shared password π. The chips sends the ciphertext $z = Enc_{K_\pi}(s)$ to the terminal.

2. The terminal recovers s with the shared password π and receives $s = Dec_{K_\pi}(z)$.

3. Chip and terminal both create ephemeral key pairs, and perform a Diffie-Hellman key agreement protocol based on these key pairs and the generated shared secret s. By performing Diffie-Hellman both entities agree on a new shared secret K.

4. Based on K both parties derive session keys.

5. Chip and terminal exchange and verify authentication tokens based on a Message Authentication Code.

6. After successfully performing PACE the *Secure Messaging* sub-protocol is started with the derived session keys to establish a secure channel, which provides authenticity, integrity and confidentiality.

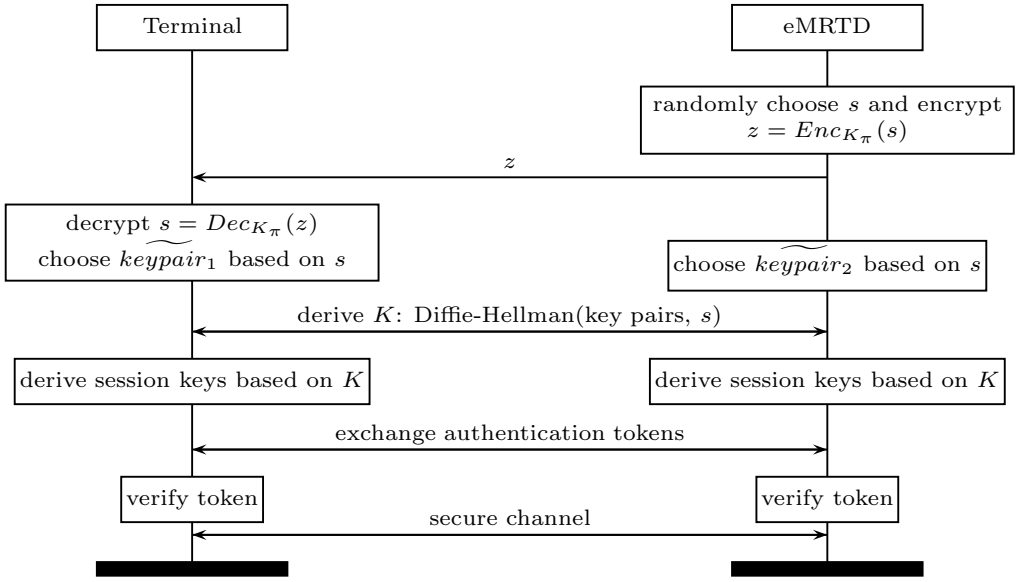


Figure 0.2: Basic operation mode of the PACE protocol.

PACE represents the constituent building block for the BioPACE protocol introduced in the next section.

0.5 BioPACE: Biometric-protected authenticated connection establishment

The idea of BioPACE was first introduced in [20] and later extended in [11] in the form of BioPACE version 2. Since version 2 fixes a tracking issue and adds diverse useful security properties which will be discussed in section 0.6 on page 11, in this work we will from now on refer to BioPACE version 2 as BioPACE.

BioPACE is a pre-processing step to the PACE protocol which replaces the commonly used knowledge-based shared secret by a biometric-based secret. In [20] the idea to make use of biometric template protection based on the ISO/IEC IS 24745 [31] is introduced (see Section 0.3). BioPACE does not favour a biometric characteristic, i.e. BioPACE may be implemented using the facial image, fingerprints, iris, etc. The BioPACE protocol consists of two phases:

1. *Initialisation phase* and

2. *Regular use phase.*

For every eMRTD the initialisation phase has to be conducted before the manufacturer can personalise the eMRTD. During the application of an eMRTD a user is enrolled and feature extraction is applied to the captured biometric sample, resulting in a biometric reference consisting of a pseudonymous identifier PI and auxiliary data AD.

Figure 0.3: The eMRTD with AD printed as data matrix code.

After the biometric enrolment AD is printed on the eMRTD in form of a 2D barcode (e.g., a QR code [33] or a Data Matrix code [32]), which is shown as part of Figure 0.3. PI is not publicly available, instead it is stored in the internal memory of the eIDAS token chip and is therefore only available to the chip itself, but not to the eMRTD terminal.

After initialisation BioPACE is ready for the regular use phase which consists of a new feature extraction from a biometric sample and an optical scan of previously enrolled AD. An eMRTD terminal requires optical access to the eMRTD in order to scan the 2D barcode and receive AD to calculate PI^*, which equals PI if and only if the same person provided the biometric sample and therefore a biometric match occurs, this phase is depicted in Figure 0.4 on the next page.

After this pre-processing step PI^* is used as input for the PACE protocol. PI^* is implicitly compared to PI by the completion of the PACE protocol, because if PI^* and PI do not match the PACE protocol will fail. With respect to provided entropy biometric-based PIs exhibit sufficient entropy, cf. Table 0.4 on page 15, compared to a PACE-based six digit numeric PIN which provides $\log_2(10^6) \simeq 20$ bits entropy.

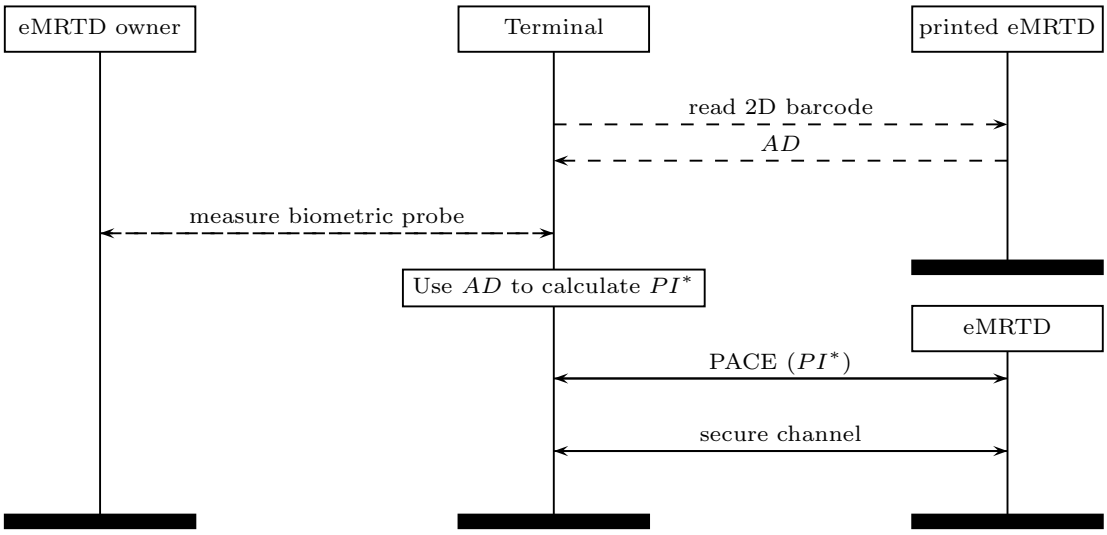


Figure 0.4: Basic operation mode of the BioPACE protocol.

0.6 Assessment of BioPACE

Our security assessment of BioPACE was conducted with respect to common security features of an eMRTD. Every paragraph first presents a short assessment regarding a specific security aspect, and then explains specific design decisions, when applicable.

0.6.1 Physical to electronic linkage

Where PACE makes a link between the printed data page of the eMRTD and the chip inside the eMRTD, by comparing the MRZ to DG1, BioPACE makes a link between the eMRTD owner and the chip inside the eMRTD. There usually would be no more link between the printed data page of the eMRTD and the chip inside the eMRTD. As a consequence it could not build further upon the prior established authenticity of the MRZ and CAN (by checking the optical security features on eMRTDs, such as special paper and printing techniques). Therefore AD is printed on the data page of the eMRTD in form of a 2D barcode. By printing AD on the data page we create a link between the physical eMRTD and the chip. Now a terminal needs optical access to the eMRTD to scan the 2D barcode and receive AD to calculate PI^*. This will provide at least the same level of protection against skimming and sniffing attacks as PACE.

0.6.2 No Tracking

PACE guarantees the unlinkability of eMRTD occurrences on the wireless channel, BioPACE does not destroy this property even so it relies on two unique identifiers PI and AD. On the one hand PI is never directly transferred over the wireless channel, instead it is used to encrypt a random value and matched on the eMRTD chip and on the other hand AD is not wirelessly transferred at al, but instead optically read from

the printed 2D barcode making no tracking possible via sniffing the BioPACE communication between an eMRTD and an eMRTD terminal.

0.6.3 Usability enhancement

By introducing BioPACE usability is enhanced is several ways:

1. the shared secret PI has a much higher entropy, than the currently utilised secrets (PIN, PUK, CAN or MRZ) and therefore BioPACE provides a higher security level for any further transferred data, which strengthens the user's data privacy;

2. in contrast to a knowledge based secret like a PIN, a biometric feature can not be forgotten by the document holder which enhances the user experience.

3. in some jurisdictions (e.g. in Germany) the eID-law prohibits photocopies of the e-ID card in order not to disseminate CAN, which is printed on the card. This regulation is intentionally or unintentionally ignored as it is widely unknown. BioPACE and the abolition of the printed would thus enable to return to the legal regulation that allows photocopies of eID cards.

0.6.4 Impeded skimming

With BioPACE no unauthorised data retrieval is possible. For eMRTDs that implement PACE or BioPACE, one requires access to the printed data page of the eMRTD to read the data on the chip. Handing the eMRTD over to an official for checking can be seen as an implicit authorisation from the eMRTD owner. If BioPACE would only require the eMRTD holders to provide their fingerprint to the officials checking their eMRTDs it would not reach the same level of authorisation, because we leave our fingerprints everywhere. Anyone within wireless communication range that has access to the fingerprint of the eMRTD holder, could read out the data of the eMRTD without the owner even being aware. This would make skimming attacks easy, for example in airport bars (given that one can extract the fingerprint from a glass in a timely manner). One does not need to fool the terminal's fingerprint reader (which is hard, since one has to make a dummy finger, possible liveness detection) but the raw image data is good enough for direct processing. As boundary condition, the attacker also needs a terminal and the attack is only justified if a name or facial image to a corresponding fingerprint is the goal of the attacker. By making a link to the printed data page of the eMRTD this attack is mitigated, because the printed content is not revealed in airport bars.

0.6.5 No off-line eMRTD owner guessing

Because the biometric feature has high entropy, an off-line guessing attack with respect to whom the eMRTD belongs to is not possible. Assume that one wants to track a number of high profile individuals and one has access to their fingerprints (which are left behind on whatever the person in question happens to touch). From these fingerprints, together

with AD one can derive all possible PI's. This would narrow down the search space significantly. Since PI is a high entropy value this attack is not feasible for BioPACEand one could conclude it would also make BAC suitable again, because the main complaint against BAC is the low entropy of the MRZ combined with its vulnerability to off-line brute-force attacks. Still PACE is resistant against off-line brute-force attacks and should therefore preferred over BAC.

0.6.6 Biometric linkage goal

The BioPACE protocol provides access control and creates a link between the eMRTD holder and the chip. In the current eMRTD security protocol pool these goals are already achieved by BAC, PACE and EAC for the access control and the fingerprints stored on the chip for the biometric link. Achieving the same security goal twice has no benefit and only makes the border control check more lengthy. Therefore removing EAC and the raw fingerprints would justify the access control and linkage goal of BioPACE. Of course this should only be considered if the eMRTD would contain no more sensitive biometric data. This is discussed in section 0.8 on page 16.

0.6.7 Access control flexibility

As long as the sensitive biometric fingerprints are stored on the chip BioPACE should not be considered as EU EAC replacement, because it can only provide two possible authorisation levels:

1. read every data group or
2. read no data group.

With EAC, one can provide a more fine grained access control and the eMRTD receives an explicit authorisation from its issuing country that this terminal is indeed authorised to read certain data groups. A possible solution is to replace the raw fingerprints by a protected biometric template that leaks no sensitive information.

0.7 Entropy of biometric data

Biometric features must not be expected to be mutually independent, e.g. fingerprints underlie distinct structures (densities and orientations of minutiae). Focusing on data storage, binary biometric templates represent a favourable representation, enabling compact storage and rapid comparison. So far, numerous approaches have been proposed to extract binary feature vectors from diverse biometric characteristics, i.e. without loss of generality we will restrict to analyse entropy of biometric data according to a binary representation of biometric features.

A common way to estimate the average entropy ($\simeq$ amount of mutually independent bits) of biometric feature vectors is to measure the provided "degrees-of-freedom" which

are defined by $d = p(1-p)/\sigma^2$, where p is the mean Hamming distance (HD) and σ^2 the corresponding variance between comparisons of different pairs of binary feature vectors, shown in Figure 0.5. In case all bits of each binary feature vector of length z would be mutually independent, comparisons of pairs of different feature vectors would yield a binomial distribution, $\mathcal{B}(z,k) = \binom{z}{k} p^k (1-p)^{z-k} = \binom{z}{k} 0.5^z$ and the expectation of the HD would be $1/z \cdot \mathbb{E}(X \oplus Y) = zp \cdot 1/z = p = 0.5$, where X and Y are two independent random variables in $\{0,1\}$. In reality p decreases to $0.5 - \epsilon$ while HDs remain binomially distributed with a reduction in z in particular, $\mathcal{B}(d, 0.5)$ [64]. Reported entropy in literature of relevant biometric characteristics are summarised in Table 0.4 on the next page. Estimated entropy can be directly transferred to AD and PIs which are applied in further application. However, techniques which are employed to overcome biometric variance, e.g. severe quantisation, may reduce the entropy of resulting protected templates [1].

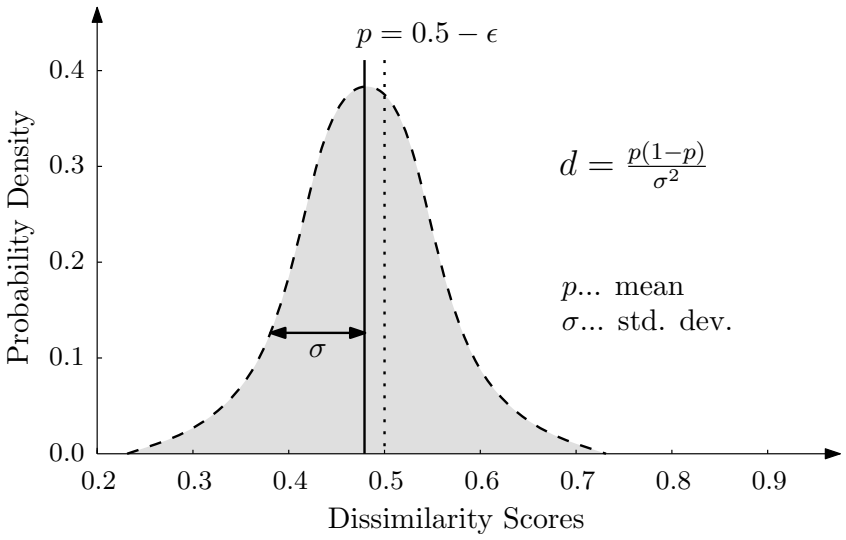


Figure 0.5: Binomial distribution of scores between different pairs of vectors.

In addition the amount of degrees-of-freedom can be directly derived from the false match rate (FMR) provided by a biometric (template protection) system. According to the ISO/IEC IS 19795-1 [34] the FMR defines the proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template. At a targeted false non-match rate ($FNMR$), the proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample, provided entropy (in bits) is estimated as $\log_2(FMR^{-1})$, which directly relates to entropy estimations which are frequently applied to passwords or PINs.

Most biometric cryptosystems aim at binding or generating keys, long enough to be applied in a generic cryptographic system (e.g. 128-bit keys for AES). Obviously, to prevent a biometric keys from being guessed, these need to exhibit sufficient entropy. While the issue of key entropy has been ignored in early approaches to biometric cryptosystems,

Table 0.4: Entropy reported in literature for different biometric characteristics.

Biometric characteristic	Feature extractor	Entropy (in bits)	Ref.
Fingerprint	Minutia-based	84	[48]
Iris	2D Log-Gabor wavelets	249	[19]
Face	Fusion of FLD and PCA	56	[1]

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

recent works tend to provide key entropy estimations. In [13, 12], Buhan *et al.* point out a direct relation between the maximum length k of cryptographic keys and the error rates of the biometric system. The authors define this relation as $k \leq -\log_2(FMR)$, as previously mentioned. This means that an ideal biometric cryptosystem would have to maintain an FAR $\leq 2^{-k}$ which appears to be a quite rigorous upper bound that may not be achievable in practice. Nevertheless, the authors emphasise on the important fact that the recognition rates of a biometric system correlate with the amount of information which can be extracted, retaining maximum entropy. Based on their proposed quantization scheme [63], Vielhauer *et al.* describe the issue of choosing significant features of on-line signatures and introduce three measures for feature evaluation [62]: intrapersonal feature deviation, interpersonal entropy of hash value components and the correlation between both. By analysing the discriminativity of chosen features the authors show that the applied feature vector can be reduced by 45% maintaining error rates [52]. This example underlines the fact that BCSs may generate arbitrary long keys while inter-class distances (=Hamming distance between keys) remain low. Ballard *et al.* [2, 3] propose a new measure to analyse the security of a BCS, termed guessing distance. The guessing distance defines the number of guesses a potential imposter has to perform in order to retrieve either the biometric data or the cryptographic key. Thus, the guessing distance directly relates to intra-class distances of biometric systems and, therefor, provides a more realistic measure of the entropy of biometric keys. Kelkboom *et al.* [39] analytically obtained a relationship between the maximum key size and a target system performance. A increase of maximum key size is achieved in various scenarios, e.g. when applying several biometric templates at enrolment and authentication or when increasing the desired false rejection rates. In theory-oriented work Tuyls *et al.* [61, 59] estimate the capacity and entropy loss for fuzzy commitment schemes and shielding functions, respectively. Similar investigations have been done in [42, 56] providing a systematic approach of how to examine the relative entropy loss of any given scheme, which bounds the number of additional bits that could be extracted if optimal parameters were used.

0.8 Replacing EAC and fingerprint images by BioPACE

We discuss the idea to replace the current infrastructure (i.e., the EAC protocols, the Country Verifying PKI, and the storage of index finger images in data group 3) by BioPACE. We analyse advantages and disadvantages of our approach and include boundary conditions, which have to be fulfilled to make BioPACE expedient. Fundamental changes to an established infrastructure are a challenging task and require as a boundary condition both innovative ideas and enhanced security. We consider BioPACE to meet these demands as discussed below. In our context, for instance, a sample innovative idea is the Biocryptographic Key Infrastructure [53] to replace a common Public Key Infrastructure, yielding a higher security level. An example of enhancing an applied and proven protocol is the Biotokens [54] approach, where biometric digital signatures and Bio-Kerberos increases security. Therefore the redundant protocols have to be dropped, and the BioPACE has to provide a significant enhancement to become a new eMRTD standard.

If BioPACE is used without a subsequent EAC accomplishment, we see the following benefits:

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

2. **Enhanced practical security:** According to a recent EU border control study [18, D4.1] border control personnel does only perform an electronic check against eMRTD blacklists due to time constraints. Hence in practice the actual security level of the eMRTD chip and its infrastructure is mainly not used. A significant speed-up of the verification protocols will therefore not only make the verification more convenient for the travellers, but it will improve security, because the electronic security features will be actually used by border control personnel even under strict time schedule guidelines.

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

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

5. **Standardised data structures:** 2D barcodes are standardised, and their integration is already discussed for non-electronic travel documents based on the Digital Seal standard [10, 18, D6.1].

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

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

2. **Coarse-grained access control:** As discussed in Section 0.6 BioPACE causes a loss of access control flexibility. However, if the sensitive JPEG fingerprints are removed from the chip no more sensitive data remains, which is worth protection with a flexible access control scheme. Currently the EU EAC only protects DG2 so the only actual flexibility is access or no access to DG2, which is gone anyway in our future proposal.

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

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

To conclude we rate the improvement with respect to run-time, practical security, and costs to be more important than the disadvantages to change the layout and the loss of fine-grained access control. Future attention should be paid to the integration of a chip cloning protection into the BioPACE. Bender *et al.* [5] present a protocol called PACE|AA, which combines PACE and Active Authentication to create a protocol, which is more efficient than the single protocols and solves a security risk of Active Authentication.

The future BioPACE could be a merged protocol with the benefits of the BioPACE and the PACE|AA protocol. This combination would create a monolithic protocol that fulfils all security goals currently achieved by the eMRTD protocols and requirements of a biometric system regarding privacy protection and security [55], save the EU a lot of money because the CV PKI could be shut down, data privacy concerns would be mitigated and border gate checks would become faster.

0.9 Summary and conclusion

This chapter presented an assessment of the BioPACE protocol, pointed out strengths and evaluated its expediency for the eMRTD domain. We came to the conclusion that

it is expedient in its proposed form only with the drastic approach to completely drop EAC and remove the raw fingerprint images from DG2, which then makes BioPACE very attractive since the expensive CV PKI can be shut down. If BioPACE gets merged with the PACE|AA protocol to also get a chip cloning protection it could become a perfectly tailored monolithic security protocol for the eMRTD domains requirements. Our discussions about the entropy of different biometric characteristics as well as state-of-the-art biometric template protection schemes demonstrate that BioPACE is no abstract concept, but rather a practical security protocol which simplifies the eMRTD infrastructure and strengthens the key exchange between chip and terminal. BioPACE also provides an enhanced border control user experience by on the one hand making the inspection faster since no more big raw finger fingerprint images have to be transferred over the slow wireless channel and no more on-chip certificate chain validation is necessary; and on the other hand by enhancing the data privacy of the sensitive biometric information since the raw fingerprint images are replaced by a biometric template protection mechanism and by using implicit biometric on-chip comparison during BioPACE.

We presented the theoretical idea of merging BioPACE with the PACE|AA protocol, therefore future work will focus on a formal security proof for this protocol based on the model proposed by Bellare *et al.* [4].

Acknowledgement

This work was supported by the European Commission through the FIDELITY EU-FP7 project (Grant No. SEC-2011-284862), CASED and the Research Council KU Leuven: GOA TENSE (GOA/11/007).

Bibliography

[1] A. Adler, R. Youmaran, and S. Loyka. Towards a measure of biometric information. In *Canadian Conference on Electrical and Computer Engineering, (CCECE'06).*, pages 210–213, 2006.

[2] L. Ballard, S. Kamara, F. Monrose, and M. Reiter. On the requirements of biometric key generators. *Technical Report TR-JHU-SPAR-BKMR-090707*, 2007. Submitted and available as JHU Department of Computer Science Technical Report.

[3] L. Ballard, S. Kamara, and M. K. Reiter. The practical subtleties of biometric key generation. In *SS'08: Proc. of the 17th Conf. on Security symposium*, pages 61–74, 2008.

[4] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 139–155. Springer, 2000.

[5] Jens Bender, Özgür Dagdelen, Marc Fischlin, and Dennis Kügler. The pace|aa protocol for machine readable travel documents, and its security. In *Financial Cryptography and Data Security*, volume 7397 of *LNCS*, pages 344–358. Springer, 2012.

[6] J. Breebaart, C. Busch, J. Grave, and E. Kindt. A reference architecture for biometric template protection based on pseudo identities. In *Proc. of the BIOSIG 2008: Biometrics and Electronic Signatures*, pages 25–38, 2008.

[7] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor. Optimal iris fuzzy sketches. *in Proc. 1st IEEE Int. Conf. on Biometrics: Theory, Applications, and Systems.*, pages 1–6, 2007.

[8] J. Bringer and V. Despiegel. Binary feature vector fingerprint representation from minutiae vicinities. In *Proc. of the 4th IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTAS'10)*, pages 1–6, 2010.

[9] BSI. *Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2.05 edition, 2010.

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

[11] Nicolas Buchmann, Roel Peeters, Harald Baier, and Andreas Pashalidis. Security considerations on extending PACE to a biometric-based connection establishment. In *Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the*, pages 1–13, 2013.

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

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

[14] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(9):1489–1503, 2007.

[15] A. Cavoukian and A. Stoianov. Biometric encryption. In *Encyclopedia of Biometrics*. Springer Verlag, 2009.

[16] A. Cavoukian and A. Stoianov. Biometric encryption: The new breed of untraceable biometrics. In *Biometrics: fundamentals, theory, and systems*. Wiley, 2009.

[17] T. C. Clancy, N. Kiyavash, and D. J. Lin. Secure smartcard-based fingerprint authentication. *Proc. ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop*, pages 45–52, 2003.

[18] European Commission. Fidelity project. online, http://www.fidelity-project.eu/page/project/deliverables.php.

[19] J. Daugman. Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. *Proc. of the IEEE*, 94(11):1927–1935, 2006.

[20] Bernhard Deufel, Carsten Mueller, Gavan Duffy, and Tom Kevenaar. BioPACE – Biometric passwords for next generation authentication protocols for machine-readable travel documents. *Datenschutz und Datensicherheit - DuD*, 37(6):363 – 366, 2013.

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

[22] EU. Commission decision c(2005)409. Online, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-visas/document-security/index_en.htm, 2005.

[23] H. Feng and C. C. Wah. Private key generation from on-line handwritten signatures. *Information Management and Computer Security*, 10(18):159–164, 2002.

[24] A. Goh and D. C. L. Ngo. Computation of cryptographic keys from face biometrics. In *Communications and Multimedia Security (LNCS: 2828)*, pages 1–13, 2003.

[25] A. Goh, A. B. J. Teoh, and D. C. L. Ngo. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Trans. Pattern Anal. Mach. Intell.*, 28(12):1892–1901, 2006.

[26] J. Hämmerle-Uhl, E. Pschernig, , and A.Uhl. Cancelable iris biometrics using block re-mapping and image warping. *In Proc. of the Information Security Conf. 2009 (ISC'09) LNCS: 5735*, pages 135–142, 2009.

[27] F. Hao, R. Anderson, and J. Daugman. Combining Cryptography with Biometrics Effectively. *IEEE Transactions on Computers*, 55(9):1081–1088, 2006.

[28] ICAO. *Doc 9303 Part 1 Machine Readable Passports Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability*. International Civil Aviation Organization (ICAO), 6 edition, 2006.

[29] ICAO. *SUPPLEMENT to Doc 9303*. International Civil Aviation Organization (ICAO), 12 edition, 2013.

[30] IEEE Std 610.12-1990 – Glossary of Software Engineering Terminology, 1990.

[31] ISO/IEC JTC 1/SC 27 - Security Techniques. Information technology – security techniques – biometric information protection. ISO/IEC 24745:2011, 2011.

[32] ISO/IEC JTC 1/SC 31 - Automatic identification and data capture techniques. Information technology – automatic identification and data capture techniques – data matrix bar code symbology specification. ISO/IEC 16022:2006, 2006.

[33] ISO/IEC JTC 1/SC 31 - Automatic identification and data capture techniques. Information technology – automatic identification and data capture techniques – qr code 2005 bar code symbology specification. ISO/IEC 18004:2006, 2006.

[34] ISO/IEC TC JTC1 SC37 Biometrics. *ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*. International Organization for Standardization and International Electrotechnical Committee, March 2006.

[35] ISO/IEC TR 19759:2005 – Software Engineering – Guide to the Software Engineering Body of Knowledge (SWEBOK), 9 2005.

[36] A. K. Jain, A. Ross, and U. Uludag. Biometric template security: Challenges and solutions. *in Proc. of European Signal Processing Conf. (EUSIPCO)*, 2005.

[37] A. Juels and M. Sudan. A fuzzy vault scheme. *Proc. 2002 IEEE Int. Symp. on Information Theory*, page 408, 2002.

[38] A. Juels and M. Wattenberg. A fuzzy commitment scheme. *6th ACM Conf. on Computer and Communications Security*, pages 28–36, 1999.

[39] E. J. C. Kelkboom, J. Breebaart, I. Buhan, and R. N. J. Veldhuis. Analytical template protection performance and maximum key size given a gaussian modeled biometric source. In *Proc. of SPIE defense, security and sensing*, 2010.

[40] A. Kong, K.-H. Cheunga, D. Zhanga, M. Kamelb, and J. Youa. An analysis of BioHashing and its variants. *Pattern Recognition*, 39:1359–1368, 2006.

[41] Dennis Kügler and Ingo Naumann. Sicherheitsmechanismen für kontaktlose chips im deutschen reisepass. *Datenschutz und Datensicherheit - DuD*, 31(3):176–180, 2007.

[42] Q. Li, Y. Sutcu, and N. Memon. Secure sketch for biometric templates. *Advances in Cryptology - ASIACRYPT 2006 (LNCS:4284)*, pages 99–113, 2006.

[43] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri. Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *Trans. on System, Man, and Cybernetics-Part A: Systems and Humans*, 40(3):525–538, 2010.

[44] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel. Using Voice to Generate Cryptographic Keys. *Proc. 2001: A Speaker Odyssey, The Speech Recognition Workshop*, 2001. 6 pages.

[45] K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint-based Fuzzy Vault: Implementation and Performance. *in IEEE Transactions on Information Forensics And Security*, 2:744–757, 2007.

[46] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40:614–634, 2001.

[47] N. K. Ratha, J. H. Connell, and S. Chikkerur. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572, 2007.

[48] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. An analysis of minutiae matching strength. In *AVBPA '01: Proc. of the Third Int. Conf. on Audio- and Video-Based Biometric Person Authentication*, pages 223–228, 2001.

[49] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(3), 2011.

[50] Arun Ross, Jidnya Shah, and Anil K. Jain. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):544–560, 2007.

[51] M. Savvides, B.V.K.V. Kumar, and P.K. Khosla. Cancelable biometric filters for face recognition. *ICPR '04: Proc. of the Pattern Recognition, 17th Int. Conf. on (ICPR'04)*, 3:922–925, 2004.

[52] T. Scheidat and C. Vielhauer. Biometric hashing for handwriting : Entropy based feature selection and semantic fusion. In *Proc. of SPIE*, volume 6819, pages 68190N.1–68190N.12, 2008.

[53] Walter Scheirer, Bill Bishop, and Terrance Boult. Beyond pki: The biocryptographic key infrastructure. In *Workshop Information Forensics and Security*, pages 1–6. IEEE, 2010.

[54] Walter Scheirer and Terrance Boult. Bio-cryptographic protocols with bipartite biotokens. In *Biometrics Symposium*, pages 9–16, 2008.

[55] K. Simoens, J. Bringer, H. Chabanne, and S. Seys. A framework for analyzing template security and privacy in biometric authentication systems. *IEEE Transactions on Information Forensics and Security*, 7(2):833–841, 2012.

[56] Y. Sutcu, Q. Li, and N. Memon. How to Protect Biometric Templates. *SPIE Conf. on Security, Steganography and Watermarking of Multimedia Contents IX*, 6505, 2007. Proc. of SPIE, 11 pages.

[57] Y. Sutcu, H. T. Sencar, and N. Memon. A secure biometric authentication scheme based on robust hashing. *MMSec '05: Proc. of the 7th Workshop on Multimedia and Security*, pages 111–116, 2005.

[58] A. B. J. Teoh, D. C. L. Ngo, and A. Goh. Personalised cryptographic key generation based on FaceHashing. *Computers And Security*, 2004(23):606–614, 2004.

[59] P. Tuyls and J. Goseling. Capacity and examples of template-protecting biometric authentication systems. *in Proc. ECCV Workshop BioAW (LNCS)*, 3087:158 – 170, 2004.

[60] U. Uludag and A. K. Jain. Fuzzy fingerprint vault. *Proc. Workshop: Biometrics: Challenges Arising from Theory to Practice*, pages 13–16, 2004.

[61] E. Verbitskiy, P. Tuyls, D. Denteneer, and J. P. Linnartz. Reliable biometric authentication with privacy protection. *presented at the SPIE Biometric Technology for Human Identification Conf., Orlando, FL*, 2004.

[62] C. Vielhauer and R. Steinmetz. Handwriting: feature correlation analysis for biometric hashes. *EURASIP J. Appl. Signal Process.*, 2004(1):542–558, 2004.

[63] C. Vielhauer, R. Steinmetz, and A. Mayerhöfer. Biometric hash based on statistical features of online signatures. In *ICPR '02: Proc. of the 16 th Int. Conf. on Pattern Recognition (ICPR'02) Volume 1*, page 10123, 2002.

[64] R. Viveros, K. Balasubramanian, and N. Balakrishnan. Binomial and negative binomial analogues under correlated bernoulli trials. *The American Statistician*, 48(3):243–247, 1984.

[65] Y. Wang and K.N. Plataniotis. Face based biometric authentication with changeable and privacy preservable templates. In *Proc. of the IEEE Biometrics Symposium 2007*, pages 11–13, 2007.

[66] X. Wu, N. Qi, K. Wang, and D. Zhang. A Novel Cryptosystem based on Iris Key Generation. *Fourth Int. Conf. on Natural Computation (ICNC'08)*, pages 53–56, 2008.

[67] H. Xu and R. N.J. Veldhuis. Binary representations of fingerprint spectral minutiae features. In *Proc. of the 20th Int. Conf. on Pattern Recognition (ICPR'10)*, pages 1212–1216, 2010.

[68] J. Zuo, N. K. Ratha, and J. H. Connel. Cancelable iris biometric. *In Proc. of the 19th Int. Conf. on Pattern Recognition 2008 (ICPR'08)*, pages 1–4, 2008.