Analytical Template Protection Performance and Maximum Key Size given a Gaussian Modeled Biometric Source

Emile J. C. Kelkboom[a], Jeroen Breebaart[a], Ileana Buhan[a], and Raymond N. J. Veldhuis[b]

[a]Philips Research, High Tech Campus 34, 5656 AE, Eindhoven, The Netherlands;
[b]University of Twente, Hogekamp 9250, 7500 AE, Enschede, The Netherlands

ABSTRACT

Template protection techniques are used within biometric systems in order to protect the stored biometric template against privacy and security threats. A great portion of template protection techniques are based on extracting a key from or binding a key to a biometric sample. The achieved protection depends on the size of the key and its closeness to being random. In the literature it can be observed that there is a large variation on the reported key lengths at similar classification performance of the same template protection system, even when based on the same biometric modality and database. In this work we determine the analytical relationship between the system performance and the theoretical maximum key size given a biometric source modeled by parallel Gaussian channels. We consider the case where the source capacity is evenly distributed across all channels and the channels are independent. We also determine the effect of the parameters such as the source capacity, the number of enrolment and verification samples, and the operating point selection on the maximum key size. We show that a trade-off exists between the privacy protection of the biometric system and its convenience for its users.

Keywords: Template protection, Binary biometrics, Biometric security, Biometric privacy

1. INTRODUCTION

A biometric system consist of an enrolment and verification phase. In the enrolment phase, a biometric sample is captured from which a reference template is created and stored. In the verification phase, a new biometric sample is captured and compared with the stored reference template. The user is considered as being genuine if the new biometric sample is similar to the stored reference template. In recent years, the interest in biometric systems has significantly increased. Examples are the planned introduction of the United Kingdom National Identity Card based on biometrics required by the Identity Cards Act 2006[1] or the recommendation by the International Civil Aviation Organization (ICAO)[2] to adopt the ePassport that also includes biometric data. The widespread use of biometrics and its necessity of storing a reference template introduces new security and privacy risks such as (i) *identity theft* where an adversary steals the stored reference template and impersonates the genuine user of the system by some spoofing mechanism, (ii) *non-renewability* where it is not possible to renew a compromised reference template due to the limited number of biometric instances (for example we only have one face, two irises or retinas, and ten fingers), (iii) *cross-matching* where it is possible to link reference templates of the same subject across databases of different applications, and (iv) *sensitive medical information* where it is known that your biometric data may reveal the presence of certain diseases.

The field of template protection is focussing on mitigating these privacy risks by developing template protection techniques that provide (i) *irreversibility* where it is impossible or at least very difficult to retrieve the original biometric sample from the reference template, (ii) *renewability* where it is possible to renew the reference template when necessary, and (iii) *unlinkability* where it is impossible to link reference templates from the same subject across databases of multiple applications. The field of template protection is relatively young, however

Further author information: (Send correspondence to Emile Kelkboom)
Emile Kelkboom: E-mail: emile.kelkboom@philips.com
Jeroen Breebaart: E-mail: jeroen.breebaart@philips.com
Ileana Buhan: E-mail: ileana.buhan@philips.com
Raymond Veldhuis: E-mail: r.n.j.veldhuis@utwente.nl

there is a significant interest to successfully develop and implement these techniques as shown by their prominent position within the European projects 3DFace[3] and TURBINE (TrUsted Revocable Biometric IdeNtitiEs)[4] from the 6th and 7th Framework Programme, respectively, and the great interest from privacy offices such as the Office of the Information and Privacy Commissioner of Ontario.[5]

As described in Jain et al. (2008),[6] the template protection techniques proposed in the literature can be divided into two categories, namely (i) *feature transformation* and (ii) *biometric encryption*. The most common technique based on feature transformation is known as *Cancellable Biometrics*.[7,8] Biometric encryption techniques can be sub-divided into (1) *key binding* and (2) *key generation* methods.

In the enrolment phase, the key binding techniques combines the key with a biometric sample into auxiliary data as such that the same key can be successfully released in the verification phase. The key release process in the verification phase uses a new biometric sample and the stored auxiliary data. Examples of the key binding techniques are the *Fuzzy Commitment Scheme* (FCS),[9] the *Helper Data System* (HDS),[10] the *Fuzzy Vault*,[11] and *Secure Sketches*.[12]

Key generation techniques extract a robust key from the biometric sample in the enrolment phase, with auxiliary data if necessary. In the verification phase the same key has to be extracted using a new biometric sample and, when available, the auxiliary data. *Fuzzy Extractors*[12] are the most common key generation techniques.

For both the key binding and key generation techniques, an adversary could retrieve biometric information from the protected template when having correctly guessed the key. Therefore, the achieved privacy and security protection depends on the size and randomness of the key: the larger the key and the closer it is to uniform random the more protection can be provided. However, a general trend observed in the literature is that extracting larger keys also influences the classification performance of the template protection system. In the remainder of this work we refer to the classification performance of the template protection system as the system performance. The system performance can be expressed by the *false match rate* (FMR) and the *false non-match rate* (FNMR). The FMR is the probability of incorrectly classifying the biometric samples from two different subjects as similar and genuine, hence leading to a false match, while the FNMR is the probability of incorrectly classifying two biometric samples from the same subject as different or imposter, thus leading to a false non-match. The FNMR is seen as the convenience factor of the biometric system, because it determines the probability that users have to repeat the verification process which is considered as an unpleasant user experience.

In the literature, there is a significant variation on the reported key size with respect to the system performance. Table 1 shows an overview of the reported system performance and key size for different template protection techniques, databases and feature extraction methods. It is difficult to find a relationship between the system performance and the key size. For example, consider the cases 6 and 11 that use the same template protection technique and modality, and a similar database. While having similar reported performance, the key size in case 11 is almost three times larger than in case 6. Likewise, when comparing the cases 2c and 10a with similar template protection technique, modality, and database, the key size reported in case 10a is almost double of the one of case 2c. As last example, the separate cases 7 and 10 show that using exactly the same template protection technique on the same modality but different database may lead to a different performance at an equal key size as in case 7 or different key sizes at similar performance as in case 10. *Hence, in practice there seems no clear relationship between the system performance and the key size.*

Contribution: In this work we present three contributions. Firstly, we analytically determine the classification performance of the Fuzzy Commitment Scheme where the input is a biometric source modeled by parallel Gaussian channels. We also include the number of enrolment and verification samples. Secondly, we analytically determine the theoretical maximum key size, bounded by Shannon's theory, at the operating point determined by the target FNMR. Finally, we investigate the effect of the parameters such as the Gaussian capacity of the biometric source, the number of enrolment and verification samples, and the target FNMR on the maximum key size.

The outline of this paper is as follows. We briefly describe the FCS construction in Section 2. In Section 3 we present the analytical framework that models the biometric source as parallel Gaussian channels. Furthermore, we derive the analytical system performance and the theoretical maximum key size. Section 4 illustrates the effect of the parameters on the maximum key size and our final remarks and conclusions are given in Section 5.

Table 1. Overview of the key size and the classification performance of different template protection techniques, modalities and databases found in the literature.

Work	Case	Method	Modality	Database (# samples / instance)	FMR	FNMR	Key size [bits]
Arakala et al.[13]	1	fuzzy extractors	fingerprint	FVC2000 DB1a (800/100)	0.15	0.15	34
Bringer et al.[14]	2a	FCS	iris	ICE 2005 (2953/244)	$< 10^{-5}$	0.0562	42
	2b	FCS	iris	CASIA (756/108)	≈ 0	0.0665	42
	2c	FCS	fingerprint	FVC2000 DB2a (800/100)	0.0553	0.0273	42
Change et al.[15]	3	FCS	fingerprint	NIST 4 (4000/2000)	≈ 0.001	≈ 0.10	10
Clancy et al.[16]	4	fuzzy vault	fingerprint	-	-	0.20-0.30	69
Hao et al.[17]	5	code-offset	iris	private (700/70)	≈ 0	0.0047	140
Kelkboom et al.[18]	6	HDS	3D face	FRGC v2 subset (2347/145)	0.0019	0.16	35
Kevenaar et al.[19]	7a	HDS	2D face	FERET (> 948/237)	≈ 0	0.35	58
	7b	HDS	2D face	Caltech (> 209/19)	≈ 0	0.035	58
Nandakumar et al.[20]	8a	fuzzy vault	fingerprint	FVC2000 DB2a (800/100)	$\approx 10^{-4}$	0.09	≈ 40
	8b	fuzzy vault	fingerprint	MSU-DBI (640/160)	$\approx 2 \cdot 10^{-4}$	0.175	≈ 40
Sutcu et al.[21]	9	FCS	fingerprint	Mitsubishi (1035/69)	$1.19 \cdot 10^{-4}$	0.11	30
Tuyls et al.[22]	10a	HDS	fingerprint	FVC2000 DB2a&b (880/110)	0.052	0.054	76
	10b	HDS	fingerprint	Univ. Twente (2500/500)	0.035	0.054	40
Zhou et al.[23]	11	HDS	3D face	FRGC v1 subset (> 396/99)	0.004	0.12	107

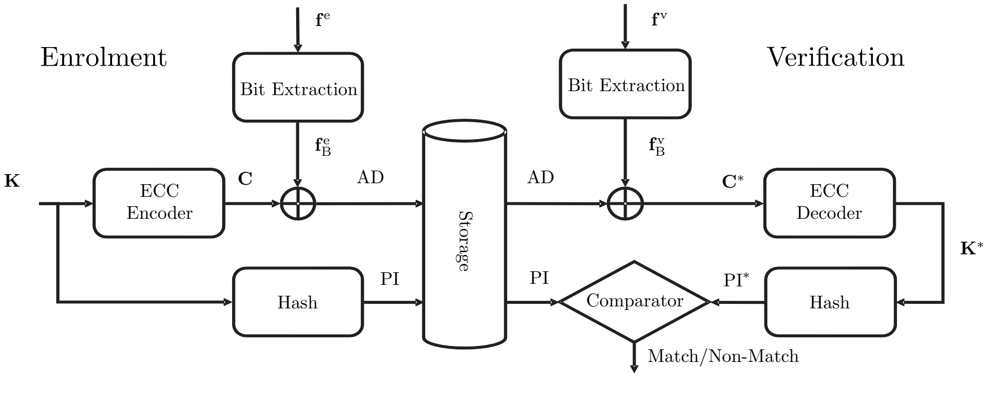


Figure 1. The FCS construction combined with a *Bit Extraction* module.

2. FUZZY COMMITMENT SCHEME

The FCS construction combined with a *Bit Extraction* module is depicted in Fig. 1. Note that the FCS is considered as a key-binding technique. In the enrolment phase the real-valued column *feature vector* $\mathbf{f}^{\mathrm{e}} \in \mathbb{R}^{N_{\mathrm{F}}}$ is extracted from each N_{e} biometric enrolment sample by the feature extraction algorithm. A single binary column vector $\mathbf{f}^{\mathrm{e}}_{\mathrm{B}} \in \{0,1\}^{N_{\mathrm{F}}}$ is created from the mean of the N_{e} feature vectors within the *Bit Extraction* module, which we will discuss in Section 3. Furthermore, a random key $\mathbf{K} \in \{0,1\}^{k_{\mathrm{c}}}$ is created and encoded by the *ECC Encoder* module into a codeword $\mathbf{C} \in \mathcal{C}$ of size $\{0,1\}^{n_{\mathrm{c}}}$, where $\mathcal{C}$ is the ECC codebook (the set of codewords). As the key-binding method, the codeword is XOR-ed with the binary vector $\mathbf{f}^{\mathrm{e}}_{\mathrm{B}}$ creating the helper data AD also referred to as the *Auxiliary Data* in Breebaart et al. (2008).[24] AD is stored as part of the protected template together with the hash of $\mathbf{K}$, which is referred to as the *Pseudonymous Identifier* (PI). The terminology is in line with standardization activities in ISO.[25] Because of the XOR operation and the fact that a single bit is extracted from each feature component, it implies that $n_{\mathrm{c}} = N_{\mathrm{F}}$ and in the remainder of this work we will only use n_{c}.

In the verification phase or the key-release process, the binary vector $\mathbf{f}^{\mathrm{v}}_{\mathrm{B}}$ is created by quantizing the mean of the N_{v} verification feature vectors $\mathbf{f}^{\mathrm{v}}$. Hereafter, the auxiliary data AD is XOR-ed with $\mathbf{f}^{\mathrm{v}}_{\mathrm{B}}$ resulting into the possibly corrupted codeword $\mathbf{C}^{*}$. Decoding $\mathbf{C}^{*}$ by the *ECC Decoder* module leads to the candidate secret $\mathbf{K}^{*}$.

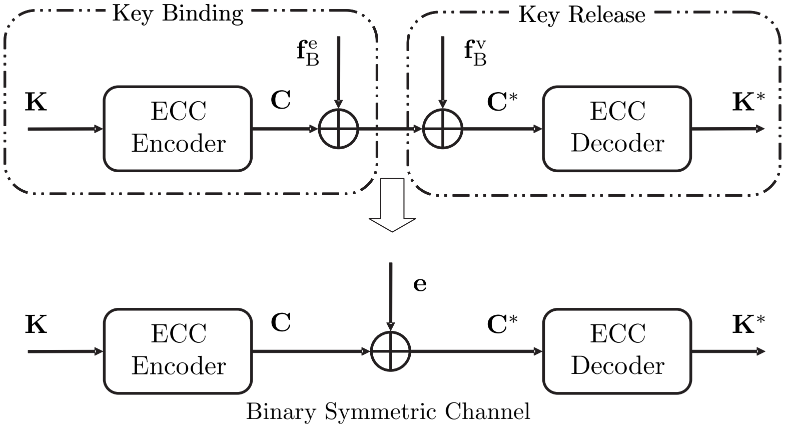


Figure 2. Modeling the key binding and release process by a Binary Symmetric Channel.

The candidate pseudo identity PI* is obtained by hashing $\mathbf{K}^*$. A match is given by the *Comparator* module if PI and PI* are equal, which occurs only when $\mathbf{K}$ and $\mathbf{K}^*$ are equal, i.e. the key-released process was successful.

The key-binding and key-release process can be modeled by a binary symmetric channel (BSC) as portrayed in Fig. 2, where the error pattern $\mathbf{e} = \mathbf{f}_{\mathrm{B}}^{\mathrm{e}} \oplus \mathbf{f}_{\mathrm{B}}^{\mathrm{v}}$ of weight $\epsilon = ||\mathbf{e}|| = d_{\mathrm{H}}(\mathbf{f}_{\mathrm{B}}^{\mathrm{e}}, \mathbf{f}_{\mathrm{B}}^{\mathrm{v}})$ corrupts the original codeword used in the key-binding process. The bit-error probability P_{e}, which is the probability that a bit of $\mathbf{e}$ is '1', determines the number of bit-errors that have to be corrected by the *ECC Decoder* and therefore also the system performance. The bit-error probability depends on the quantization method being used and is different at imposter and genuine comparisons. The following section includes the computation of P_{e} at both imposter and genuine comparisons.

3. THE ANALYTICAL FRAMEWORK

In this section we present the analytical framework for modeling the biometric source, quantization method, system performance, and the maximum key size that can be extracted. An overview of this framework is depicted in the Fig. 3. The *Source Modeling* module models the biometric source from which the enrolment and verification feature vectors $\mathbf{f}$ are derived. Given the input capacity C_{in} and the number of feature components n_{c} as its parameters the *Source Modeling* module outputs the feature quality of each component defined by the within-class and between-class variances ratio $\frac{\sigma_{\mathrm{b}}}{\sigma_{\mathrm{w}}}$. With the quantization method, the number of enrolment N_{e} and verification N_{v} samples, and the feature quality $\frac{\sigma_{\mathrm{b}}}{\sigma_{\mathrm{w}}}$, the *Quantization* module estimates the bit-error probability of the extracted bits at genuine $P_{\mathrm{e}}^{\mathrm{ge}}$ and imposter $P_{\mathrm{e}}^{\mathrm{im}}$ comparisons. Knowing the bit-error probabilities the *Performance Estimation* module estimates the analytical system performance defined by the false match rate (FMR) $\alpha(T)$ and the false non-match rate (FNMR) $\beta(T)$ at the operating point T. Given the system performance and the target FNMR β_{tar}, the maximum extracted key size is determined in the *Maximum Key Size* module. In the remainder of this section we discuss each module in more detail.

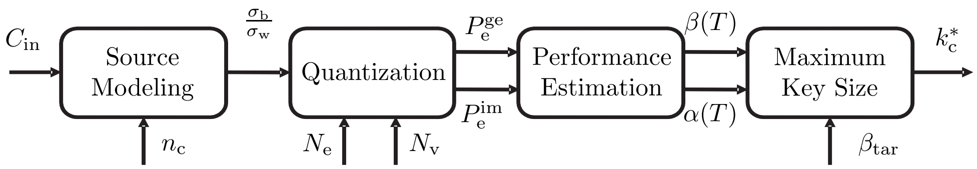
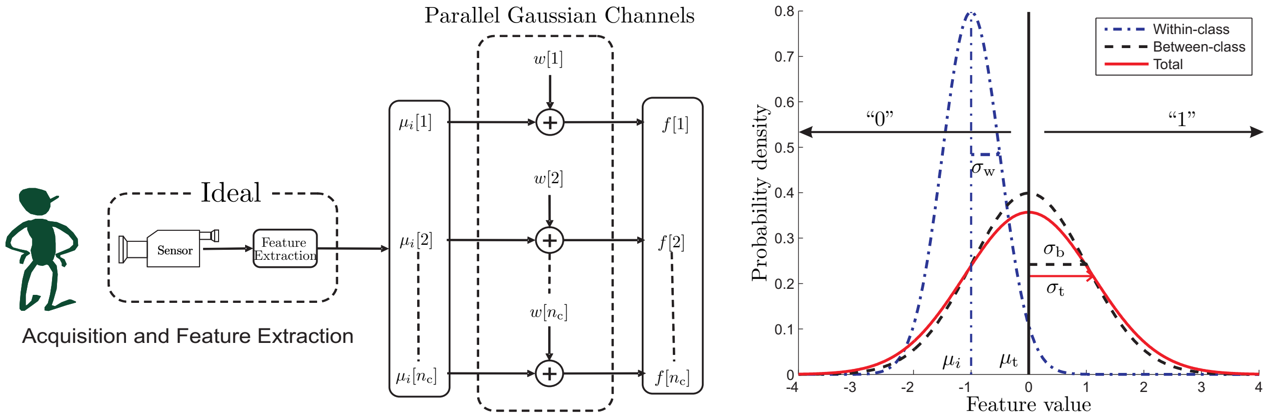


Figure 3. An overview of the framework used to model the biometric source, determine the corresponding performance and the maximum key size that can be extracted.



(a) (b)

Figure 4. (a) The Parallel Gaussian Channels modeling the real-valued features and (b) the within-class, between-class and the total density and the quantization method based on thresholding.

3.1 Biometric Source Modeling with Parallel Gaussian Channels

The input of the FCS template protection system is a real-valued feature vector $\mathbf{f} = [f[1], f[2], \ldots, f[n_c]]'$ of dimension n_c, where ' $'$ ' is the transpose operator. The feature vector $\mathbf{f}$ is extracted from a biometric measurement by the feature extractor and is likely to be different between two measurements, even if they are acquired immediately after each other. Causes for this difference include sensor noise, environment conditions and biometric variabilities.

To model these variabilities, we use the Parallel Gaussian Channels (PGC) as portrayed in Fig. 4(a). This approach has been successfully used on estimating the performance of two biometric databases in Kelkboom et al. (2009).[26] We assume an ideal Acquisition and Feature-Extraction module which always produces the same feature vector $\boldsymbol{\mu}_i$ for subject i. Such ideal module is thus robust against all aforementioned variabilities. However, the variability of component j is modeled as an additive zero-mean Gaussian noise $w[j]$ with its pdf $p_{\mathrm{w[j]},i} \sim \mathcal{N}(0, \sigma^2_{\mathrm{w},i}[j])$. Adding the noise $w[j]$ with the mean $\mu_i[j]$ results into the noisy feature component $f[j]$, in vector notation $\mathbf{f} = \boldsymbol{\mu}_i + \mathbf{w}$. The observed variability within one subject is characterized by the variance of the *within-class* pdf and is referred to as within-class variability. We assume that each subject has the same within-class variance, i.e. homogeneous within-class variance $\sigma^2_{\mathrm{w},i}[j] = \sigma^2_{\mathrm{w}}[j], \forall i$. We also assume the noise to be independent. Hence, the feature vector extracted from each biometric sample is equivalent to retransmitting $\boldsymbol{\mu}_i$ over the same PGC channels.

Across the population we assume the mean $\mu_i[j]$ to be another Gaussian random variable with density $p_{\mathrm{b}[j]} \sim \mathcal{N}(\mu_{\mathrm{b}}[j], \sigma^2_{\mathrm{b}}[j])$. The variability of $\mu_i[j]$ across the population is referred to as the *between-class* variability. Fig. 4(b) shows an example of the within-class and between-class pdfs for a specific component and a given subject. The *total* pdf describes the observed real-valued feature value $f[j]$ across the whole population and is also Gaussian with $p_{\mathrm{t}[j]} \sim \mathcal{N}(\mu_{\mathrm{t}}[j], \sigma^2_{\mathrm{t}}[j])$, where $\mu_{\mathrm{t}}[j] = \mu_{\mathrm{b}}[j]$ and $\sigma^2_{\mathrm{t}}[j] = \sigma^2_{\mathrm{w}}[j] + \sigma^2_{\mathrm{b}}[j]$. For simplicity but without loss of generality we consider $\mu_{\mathrm{t}}[j] = \mu_{\mathrm{b}}[j] = 0$.

The capacity of each channel is given by the Gaussian channel capacity $C_{\mathrm{G}}[j]$ as defined in Cover and Thomas (1991)[27]

$$C_{\mathrm{G}}[j] = \tfrac{1}{2}\log_2\left(1 + \left(\tfrac{\sigma_{\mathrm{b}}[j]}{\sigma_{\mathrm{w}}[j]}\right)^2\right), \tag{1}$$

which in fact states that a maximum of $C_{\mathrm{G}}[j]$ bits can be send per transmission. Note that the Gaussian channel capacity only depends on the ratio $\frac{\sigma_{\mathrm{b}}[j]}{\sigma_{\mathrm{w}}[j]}$ and in Section 3.2 we will also show that the bit-error probability P_{e} depends on this ratio. Therefore, we can define the $\frac{\sigma_{\mathrm{b}}[j]}{\sigma_{\mathrm{w}}[j]}$ as the feature quality of component j. Given the capacity per channel, we can define the total capacity of the input biometric source C_{in} as the sum of the capacity of each channel

$$C_{\mathrm{in}} = \sum_{j=1}^{n_{\mathrm{c}}} C_{\mathrm{G}}[j]. \tag{2}$$

In this work, we consider the capacity of each channel to be equal, consequently given the input capacity C_{in} the Gaussian capacity of each channel $C_{\mathrm{G}}[j]$ is equal to $\frac{C_{\mathrm{in}}}{n_{\mathrm{c}}}$. The distribution of C_{in} over n_{c} channels may simulate feature extraction algorithms where the number of features extracted from the biometric sample can be varied. The input capacity C_{in} thus represents the amount of discriminating information in a biometric sample across the whole population.

By substituting $C_{\mathrm{G}}[j] = \frac{C_{\mathrm{in}}}{n_{\mathrm{c}}}$ in (2) and taking its inverse, the feature quality parameter $\frac{\sigma_{\mathrm{b}}}{\sigma_{\mathrm{w}}}$ is defined by C_{in} and n_{c} according to

$$\frac{\sigma_{\mathrm{b}}}{\sigma_{\mathrm{w}}} = \sqrt{2^{\frac{2C_{\mathrm{in}}}{n_{\mathrm{c}}}} - 1}, \tag{3}$$

and is equal for each component. Thus, (3) gives the relationship between the input and output parameters of the *Source Modeling* module.

3.2 Quantization Module based on Thresholding

Fig. 4(b) depicts the quantization method we consider, which is a binarization method based on thresholding, where the mean of the total density μ_{t} is taken as the threshold.[18, 19, 22] If the real-valued feature is larger than the threshold, then a bit of value '1' is allocated, otherwise '0'. To estimate the analytical system performance we need to estimate the bit-error probability P_{e} at imposter and genuine comparisons. In this section we analytically estimate P_{e} given the quantization scheme, the feature quality $\frac{\sigma_{\mathrm{b}}}{\sigma_{\mathrm{w}}}$, and the number of enrolment N_{e} and verification N_{v} samples.

3.2.1 Imposter Bit-Error Probability $P_{\mathrm{e}}^{\mathrm{im}}$

At imposter comparisons, each bit is compared with the bit extracted from a randomly selected feature value from total density. Because μ_{t} is the binarization threshold, there is a 50% probability that a randomly selected bit from the whole population will be equal, hence $P_{\mathrm{e}}^{\mathrm{im}} = 0.5$. Note that both the number of enrolment and verification samples do not have an influence on $P_{\mathrm{e}}^{\mathrm{im}}$.

3.2.2 Genuine Bit-Error Probability $P_{\mathrm{e}}^{\mathrm{ge}}$

At genuine comparisons the analytical bit-error probability $P_{\mathrm{e}}^{\mathrm{ge}}$ has been derived in Kelkboom et al. (2008),[28] namely

$$P_{\mathrm{e}}^{\mathrm{ge}} = \frac{1}{2} - \frac{1}{\pi}\arctan\left(\frac{\sigma_{\mathrm{b}}\sqrt{N_{\mathrm{e}}N_{\mathrm{v}}}}{\sigma_{\mathrm{w}}\sqrt{N_{\mathrm{e}}+N_{\mathrm{v}}+\left(\frac{\sigma_{\mathrm{b}}}{\sigma_{\mathrm{w}}}\right)^{-2}}}\right), \tag{4}$$

where it can be seen that the ratio of the variances $\frac{\sigma_{\mathrm{b}}}{\sigma_{\mathrm{w}}}$ (the feature quality) determines $P_{\mathrm{e}}^{\mathrm{ge}}$. Note that $P_{\mathrm{e}}^{\mathrm{ge}}$ is the average bit-error probability across the population. Some subjects have a larger bit-error probability because their mean $\mu_i[j]$ is closer to the quantization threshold $\mu_{\mathrm{t}}[j]$, while others have a smaller bit-error probability because their mean is further away. However, for estimating the genuine Hamming distance pmf it is only necessary to compute the average bit-error probability as shown in.[26] Because the input capacity C_{in} is divided equally over all n_{c} channels, the feature quality $\frac{\sigma_{\mathrm{b}}}{\sigma_{\mathrm{w}}}$ is equal for each component and therefore $P_{\mathrm{e}}^{\mathrm{ge}}$ is equal for each extracted bit. By substituting (3) into (4) we obtain

$$P_{\mathrm{e}}^{\mathrm{ge}} = \frac{1}{2} - \frac{1}{\pi}\arctan\left(\frac{\sqrt{\left(2^{\frac{2C_{\mathrm{in}}}{n_{\mathrm{c}}}}-1\right)N_{\mathrm{e}}N_{\mathrm{v}}}}{\sqrt{N_{\mathrm{e}}+N_{\mathrm{v}}+\left(2^{\frac{2C_{\mathrm{in}}}{n_{\mathrm{c}}}}-1\right)^{-1}}}\right). \tag{5}$$

With (5) it is easy to show that $P_{\mathrm{e}}^{\mathrm{ge}}$ for the $N_{\mathrm{e}} = N_{\mathrm{v}} = 2X$ case converges to the $\{N_{\mathrm{e}} = \infty, N_{\mathrm{v}} = X\}$ case when $\frac{C_{\mathrm{in}}}{n_{\mathrm{c}}}$ becomes larger as such that $\left(2^{\frac{2C_{\mathrm{in}}}{n_{\mathrm{c}}}} - 1\right)^{-1} \ll X$. Fig. 5 depicts $P_{\mathrm{e}}^{\mathrm{ge}}$ as a function of $\frac{C_{\mathrm{in}}}{n_{\mathrm{c}}}$ for different settings of N_{e} and N_{v}. By increasing N_{e}, $P_{\mathrm{e}}^{\mathrm{ge}}$ decreases because the bits extracted in the enrolment phase are more stable. However, when increasing N_{e} further to infinity, $P_{\mathrm{e}}^{\mathrm{ge}}$ stays close to the $N_{\mathrm{e}} = N_{\mathrm{v}} = 2$ case and converges when $\frac{C_{\mathrm{in}}}{n_{\mathrm{c}}}$ increases. To further decrease $P_{\mathrm{e}}^{\mathrm{ge}}$ it is thus necessary to also increase N_{v}.

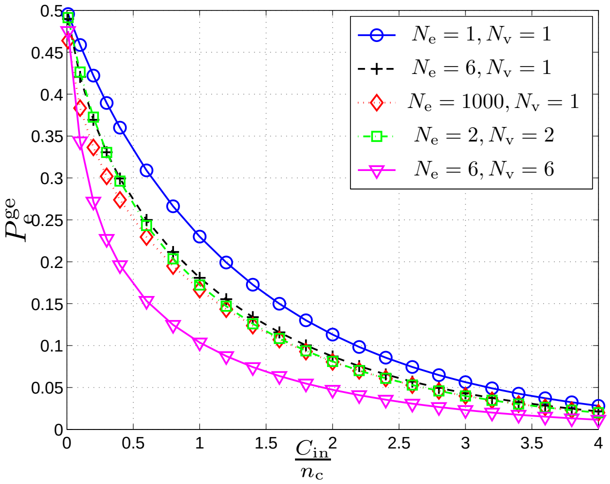


Figure 5. The genuine bit-error probability $P_{\mathrm{e}}^{\mathrm{ge}}$ as a function of the Gaussian capacity per channel $\frac{C_{\mathrm{in}}}{n_{\mathrm{c}}}$ and different values of the enrolment N_{e} and verification N_{v} samples.

3.3 Analytical System Performance

In Section 2 we have modeled the FCS template protection system as a BSC channel with bit-error probability P_{e}. The bit-error probability determines the probability mass function (pmf) of the number of bit errors or Hamming distance $\epsilon = d_{\mathrm{H}}(\mathbf{f}_{\mathrm{B}}^{\mathrm{e}}, \mathbf{f}_{\mathrm{B}}^{\mathrm{v}})$. As presented in Daugman (2003),[29] under the random bits assumption, the imposter Hamming distance pmf can be modeled by a binomial distribution

$$P_{\mathrm{b}}(d; N, p) \overset{\mathrm{def}}{=} \binom{N}{d} p^d (1-p)^{(N-d)} \tag{6}$$

with the degrees of freedom N and probability p. Because we assume the bits to be independent, the degrees of freedom is equal to the number of components, $N = n_{\mathrm{c}}$. In Daugman's experimental results the extracted binary string of 2048 bits are dependent. Therefore, they obtained a smaller number of degrees of freedom, namely 249 bits.

3.3.1 False Match Rate

The FMR depends on the pmf of ϵ at imposter comparisons, therefore the binomial probability p is equal to $P_{\mathrm{e}}^{\mathrm{im}}$. Hence, the FMR at the operating point T, $\alpha(T)$, is the probability that ϵ is smaller or equal to T, namely

$$\begin{aligned} \alpha(T) &\overset{\mathrm{def}}{=} \mathcal{P}\{\epsilon \le T \mid \text{imposter comparisons}\} \\ &= \sum_{i=0}^{T} P_{\mathrm{b}}(i; n_{\mathrm{c}}, P_{\mathrm{e}}^{\mathrm{im}}) \\ &= 2^{-n_{\mathrm{c}}} \sum_{i=0}^{T} \binom{n_{\mathrm{c}}}{T}. \end{aligned} \tag{7}$$

3.3.2 False Non-Match Rate

Because $P_{\mathrm{e}}^{\mathrm{ge}}$ is equal for each bit, the pmf of ϵ at genuine comparisons can also be described by a binomial distribution, however with $p = P_{\mathrm{e}}^{\mathrm{ge}}$. The false non-match rate at the operating point T, $\beta(T)$, is the probability that ϵ is larger than T, namely

$$\begin{aligned} \beta(T) &\overset{\mathrm{def}}{=} \mathcal{P}\{\epsilon > T \mid \text{genuine comparisons}\} \\ &= \sum_{i=T+1}^{n_{\mathrm{c}}} P_{\mathrm{b}}(i; n_{\mathrm{c}}, P_{\mathrm{e}}^{\mathrm{ge}}). \end{aligned} \tag{8}$$

3.4 Maximum Key Size at the Target Operating Point

In this section, we determine the theoretical maximum key size or message length that can be transmitted given the BSC depicted in Fig. 2 with bit-error probability P_{e} and assuming an ECC operating at Shannon's bound. With the code rate R equal to the ratio of the key size and the codeword size, $\frac{k_{\mathrm{c}}}{n_{\mathrm{c}}}$, Shannon's theorem shows that there exists a decoding technique that can decode the corrupted codeword with a bit-error rate p with an arbitrary small probability of error when

$$R < C(p) \tag{9}$$

for a large enough value of n_{c}, where $C(p)$ is the channel capacity defined as

$$C(p) = 1 - H(p), \tag{10}$$

with $H(p)$ being the binary entropy function

$$H(p) = -p\log_2 p - (1-p)\log_2(1-p). \tag{11}$$

Hence, the key size k_{c} is bounded by Shannon's bound with $p = P_{\mathrm{e}}^{\mathrm{ge}}$ as

$$k_{\mathrm{c}} = n_{\mathrm{c}}R < n_{\mathrm{c}}C(P_{\mathrm{e}}^{\mathrm{ge}}). \tag{12}$$

Note that the decoding error probability can be made arbitrarily small if n_{c} is large enough. In practice, however, n_{c} is not large enough and in order to still achieve a small decoding error probability more bits have to be corrected. Instead of correcting $t_{\mathrm{c}} = n_{\mathrm{c}}P_{\mathrm{e}}^{\mathrm{ge}}$ bits, we will correct $t_{\mathrm{c}} = T_{tar}$ bits, where T_{tar} is the operating point in order to reach the target FNMR β_{tar} and is computed with (8) according to

$$T_{tar} = \arg\min_{T}(|\beta(T) - \beta_{\mathrm{tar}}|). \tag{13}$$

Hence, the theoretical maximum key size assuming an ECC at Shannon's bound with $p = \frac{T_{tar}}{n_{\mathrm{c}}}$ is then equal to

$$k_{\mathrm{c}}^{*} \overset{\mathrm{def}}{=} n_{\mathrm{c}}C\left(\tfrac{T_{tar}}{n_{\mathrm{c}}}\right) = n_{\mathrm{c}}\left(1 - H\left(\tfrac{T_{tar}}{n_{\mathrm{c}}}\right)\right). \tag{14}$$

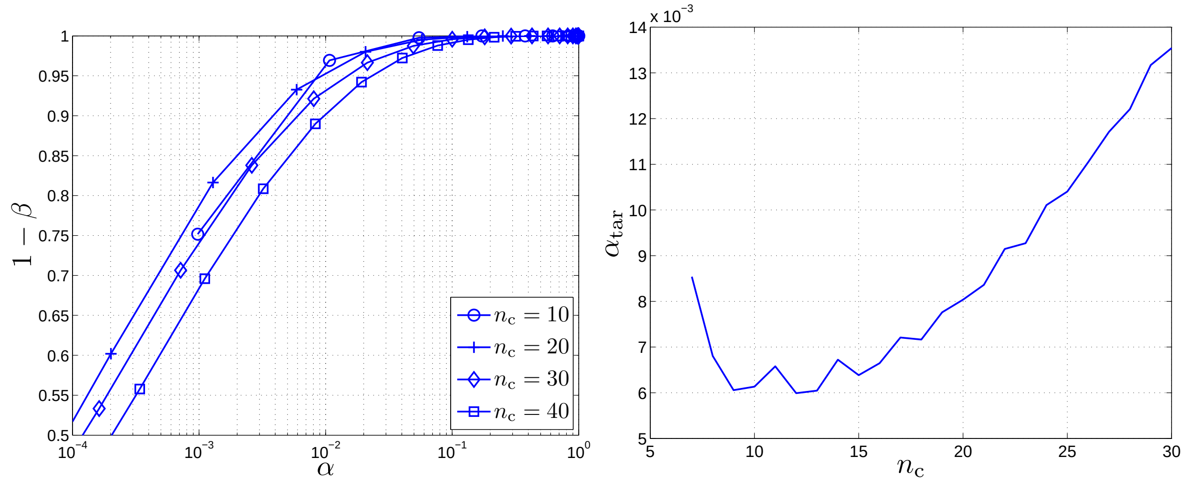
Because $\frac{T_{tar}}{n_{\mathrm{c}}}$ is larger than $P_{\mathrm{e}}^{\mathrm{ge}}$ and will not exceed $\frac{1}{2}$, we know that k_{c}^{*} will be smaller than $n_{\mathrm{c}}C(P_{\mathrm{e}}^{\mathrm{ge}})$. Note that a similar approach with Shannon's theorem is used in the work of Bringer et al. (2008),[14] however in its inverse. Namely, given a key size and the empirically obtained Hamming distances and the number of erasures at genuine and imposter comparison, they derived the best FNMR and worst FMR that could be achieved.

In the next section, we study the effect of the parameters of the framework shown in Fig. 3 on the theoretical maximum key size k_{c}^{*}.

4. THE EFFECT OF THE SYSTEM PARAMETERS ON THE SYSTEM PERFORMANCE AND THE MAXIMUM KEY SIZE

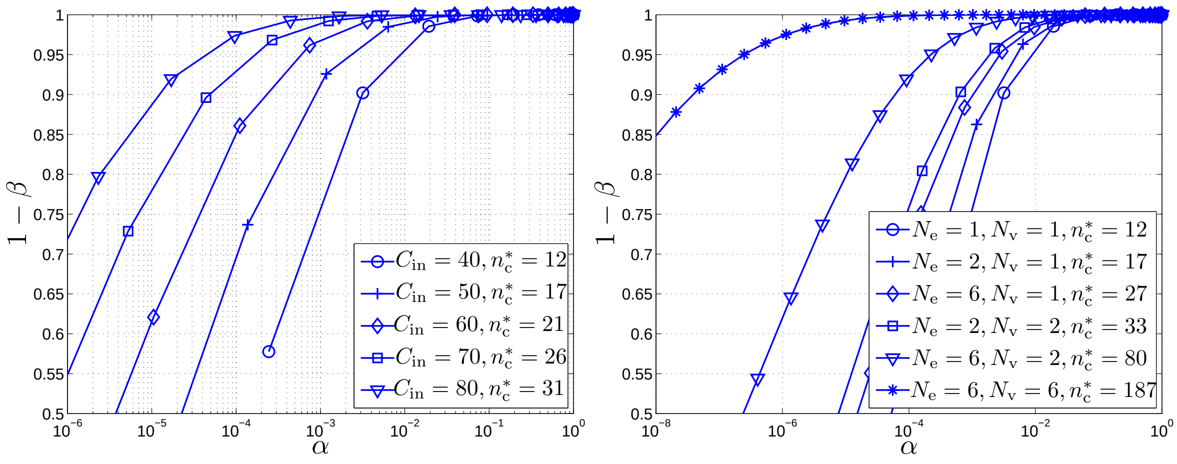
In this section we illustrate the effect of the system parameters on both the system performance and the theoretical maximum key size k_{c}^{*}. As the system parameters we have the input capacity C_{in}, the number of Gaussian channels n_{c}, the number of enrolment N_{e} and verification N_{v} samples, and the target FNMR β_{tar}.

First, we will illustrate the effect of distributing the source capacity C_{in} over n_{c} channels on the system performance. We present the system performance with the receiver operating characteristics (ROC) curve. For different settings of n_{c}, Fig. 6(a) portrays the ROC curves obtained for the case when $C_{\mathrm{in}} = 40$ bits and Fig. 6(b) depicts the obtained α_{tar} at $\beta_{\mathrm{tar}} = 5\%$. The figures show that the system performance depends on n_{c}. If n_{c} is too large or small the performance deteriorates. At smaller n_{c} values, the genuine bit-error probability $P_{\mathrm{e}}^{\mathrm{ge}}$ will be smaller, however the number of subjects that can be distinguished reduces. In a perfect system where $P_{\mathrm{e}}^{\mathrm{ge}} = 0$, it is only possible to distinguish $2^{n_{\mathrm{c}}}$ subjects without any errors. As a consequence, the system performance will degrade. On the other hand, at larger n_{c} values it is possible to distinguish more subjects, however $P_{\mathrm{e}}^{\mathrm{ge}}$ increases with a system performance deterioration as its consequence. Consequently, for each $\{C_{\mathrm{in}}, N_{\mathrm{e}}, N_{\mathrm{v}}\}$



(a) (b)

Figure 6. For different n_c settings, (a) the obtained ROC curves with $C_{in} = 40$ bits and $N_e = N_v = 1$, and (b) the obtained α_{tar} at $\beta_{tar} = 5\%$.



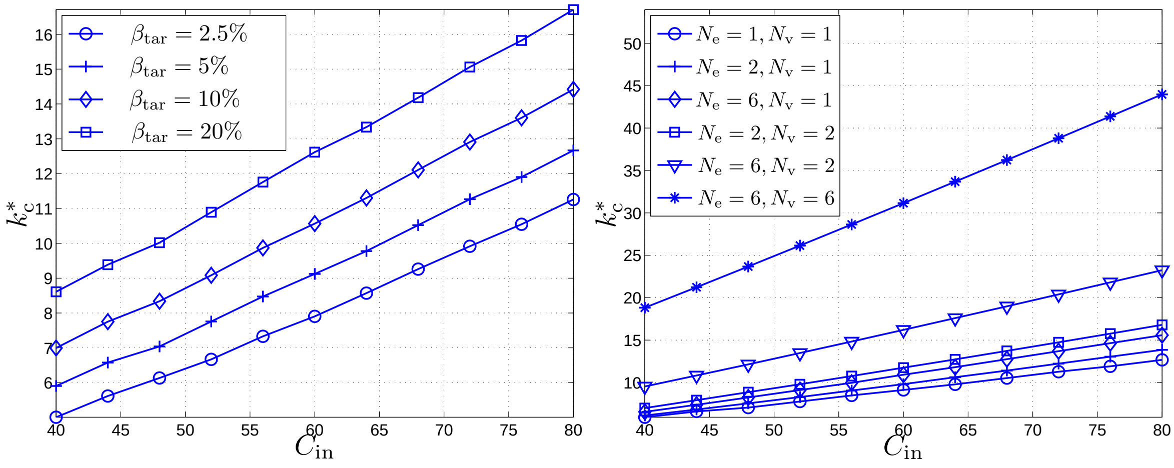
(a) (b)

Figure 7. (a) ROC curve for $C_{in} \in \{40, 50, 60, 70, 80\}$ settings and (b) the the ROC curve for different $\{N_e, N_v\}$ settings with $C_{in} = 50$.

setting we determine n_c^* leading to the optimum α_{tar} and use the corresponding ROC curve for comparison between different settings.

With the optimum number of channels n_c^* determined, Fig. 7(a) depicts the ROC curve at different C_{in} settings, while Fig. 7(b) shows the ROC curve at different $\{N_e, N_v\}$ settings with $C_{in} = 40$. The figures show that the ROC improves when either increasing C_{in}, N_e, or N_v. The most significant performance improvement is obtained when increasing both N_e and N_v.

Having shown the effect of the $\{C_{in}, n_c, N_e, N_v\}$ parameters on the ROC performance curve, we will now illustrate the effect of the $\{C_{in}, N_e, N_v, \beta_{tar}\}$ parameters on the maximum key size k_c^*. Fig. 8(a) portrays the effect of β_{tar} and C_{in} on k_c^* with $N_e = N_v = 1$. The results show that k_c^* increases when either C_{in} or β_{tar} is increased. Doubling β_{tar} from 10% to 20% on average adds around 2 bits to k_c^*, but from 2.5% to 5% on average adds 1 bit. Furthermore, doubling C_{in} roughly doubles k_c^* for the case when $\beta_{tar} = 20\%$ and almost triples when $\beta_{tar} = 2.5\%$. Fig. 8(b) depicts the effect of the $\{N_e, N_v, C_{in}\}$ parameters on k_c^*. The effect of C_{in} is similar as illustrated in Fig. 8(a). Increasing either N_e or N_v leads to an increase of k_c^*. By increasing N_e from one to



(a)

(b)

Figure 8. Under the assumption of a Shannon bounded ECC, the maximum key size k_{c}^{*} for different (a) β_{tar} and C_{in} settings, and (b) N_{e}, N_{v}, and C_{in} settings.

six samples, k_{c}^{*} will increase with 0.6 bits at $C_{\mathrm{in}} = 40$ bits and 2.9 bits at $C_{\mathrm{in}} = 80$ bits. Keeping $N_{\mathrm{e}} = 6$ and increasing N_{v} from one to two samples increases k_{c}^{*} with 3.0 bits at $C_{\mathrm{in}} = 40$ and 7.6 bits at $C_{\mathrm{in}} = 80$ bits. The increase of N_{v} from two to six samples increases k_{c}^{*} with 9.3 bits at $C_{\mathrm{in}} = 40$ and 20.8 bits at $C_{\mathrm{in}} = 80$ bits.

5. DISCUSSION AND CONCLUSION

We have analytically determined the classification performance of the Fuzzy Commitment Scheme given an input biometric source modeled by parallel Gaussian channels. The input capacity is thus defined by the Gaussian channel capacity and we assumed the input capacity to be evenly distributed across all channels and the channels to be independent. Furthermore, we assumed a single bit is extracted per channel using a binarization scheme based on thresholding. We also included the number of enrolment and verification samples.

We have shown that the optimum performance given an input capacity depends on the number of channels. Both the performance and optimum number of channels do increase when increasing the input capacity. The performance can be further improved by increasing the number of enrolment and verification samples. The greatest improvement is obtained when increasing both together. We have also shown that having an infinite enrolment samples with X verification samples approximates the performance when both are equal to $2X$, if the capacity per channel is large enough.

Furthermore, we determined the theoretical maximum key size k_{c}^{*}, bounded by Shannon's theory, at the target FNMR. With this relationship, we have shown the effect of the system parameters such as the input capacity, the number of enrolment and verification samples, and the target FNMR on the maximum key size. Doubling the input capacity roughly tripled the key size at a target FNMR of 2.5%, while doubling the target FNMR from 2.5% to 5% on average added around 1 bit. Increasing the number of enrolment samples from one to six could add 2.9 bits. With six enrolment samples and increasing the number of verification samples from one to two added 7.6 bits, while increasing from two to six samples added 20.8 bits.

By adding one bit to the key the search space of randomly selecting the key doubles. Thus, if the users of the biometric system have no issue with a less convenient system where the target FNMR has doubled we could create a protected template that is four times more difficult to break by an adversary. Moreover, switching from a single to six enrolment and verification samples increases the search space by almost 2^{32}. Supplying six sample during enrolment seems acceptable, because it only needs to be done once. Although capturing six samples during verification may be considered inconvenient, it still gives a good insight in what can be achieved by such a system.

We can thus conclude that we analytically obtained the relationship between the system performance and the maximum key size given the system parameters. Furthermore, we revealed the trade-off between the convenient use of the biometric system and the maximum key size determining the privacy and security protection. Essentially, if desired, more protection can be achieved by sacrificing some convenience.

As future work, we could consider the case where the input capacity is not evenly distributed across all channels. Hence, simulating a more realistic scenario where components do differ in discriminating power. Furthermore, relaxing the independent channel assumption is of interest.

REFERENCES

[1] Identity Cards Act 2006. `http://www.opsi.gov.uk/acts/acts2006/ukpga_20060015_en_1`.

[2] ICAO, "International Civil Aviation Organization." `http://www.icao.int`.

[3] 3DFace, "3DFace EU Project." `http://www.3dface.org/home/welcome`.

[4] TURBINE, "TrUsted Revocable Biometric IdeNtitiEs EU Project." `ttp://www.turbine-project.eu/`.

[5] Cavoukian, A. and Stoianov, A., "A positive-sum technology that achieves strong authentication, security and privacy," (March 2007).

[6] Jain, A. K., Nandakumar, K., and Nagar, A., "Biometric template security," *EURASIP Journal on Advances in Signal Processing* (2008).

[7] Ratha, N. K., Connell, J. H., and Bolle, R. M., "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal* **40**(3), 614–634 (2001).

[8] Yang, B., Busch, C., Bours, P., and Gafurov, D., "Robust minutiae hash for fingerprint template protection," in [*Proc. SPIE Vol. 7541*], (2010).

[9] Juels, A. and Wattenberg, M., "A fuzzy commitment scheme," in [*6th ACM Conference on Computer and Communications Security*], 28–36 (November 1999).

[10] Linnartz, J.-P. and Tuyls, P., "New shielding functions to enhance privacy and prevent misuse of biometric templates," in [*4th Int. Conf. on AVBPA*], 393 – 402 (2003).

[11] Juels, A. and Sudan, M., "A fuzzy vault scheme," *Designs, Codes and Cryptography* **38**, 237–257 (February 2006).

[12] Dodis, Y., Ostrovsky, R., Reyzin, L., and Smith, A., "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing* **38**(1), 97 – 139 (2008).

[13] Arakala, A., Jeffers, J., and Horadam, K. J., "Fuzzy extractors for minutiae-based fingerprint authentication," in [*International Conference on Biometrics*], 760–769 (2007).

[14] Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., and Zemor, G., "Theoretical and practical boundaries of binary secure sketches," *IEEE Transactions on Information Forensics and Security* **3**(4), 673–683 (2008).

[15] Chang, E.-C. and Roy, S., "Robust extraction of secret bits from minutiae," in [*Int. Conf. on Biometrics*], 750–759 (August 2007).

[16] Clancy, T., Kiyavash, N., and Lin, D., "Secure smartcard-based fingerprint authentication," in [*Proc. 2003 ACM SIGMM Workshop Biometrics Methods and Application (WBMA)*], 45 – 52 (2003).

[17] Hao, F., Anderson, R., and Daugman, J., "Combining crypto with biometrics effectively," *IEEE Transactions on Computers* **55**, 1081–1088 (September 2006).

[18] Kelkboom, E. J. C., Gökberk, B., Kevenaar, T. A. M., Akkermans, A. H. M., and van der Veen, M., ""3D face": Biometric template protection for 3d face recognition," in [*Int. Conf. on Biometrics*], 566–573 (August 2007).

[19] Kevenaar, T. A. M., Schrijen, G.-J., Akkermans, A. H. M., van der Veen, M., and Zuo, F., "Face recognition with renewable and privacy preserving binary templates," in [*4th IEEE workshop on AutoID*], 21–26 (October 2005).

[20] Nandakumar, K., Nagar, A., and Jain., A. K., "Hardening fingerprint fuzzy vault using password.," in [*Proceedings of Second International Conference on Biometrics*], 927 – 937 (August 2007).

[21] Sutcu, Y., Rane, S., Yedidia, J. S., Draper, S. C., and Vetro, A., "Feature extraction for a slepian-wolf biometric system using ldpc codes," in [*IEEE International Symposium on Information Theory, 2008. ISIT 2008.*], *Information Theory, 2008. ISIT 2008. IEEE International Symposium on* , 2297–2301 (2008).

[22] Tuyls, P., Akkermans, A. H. M., Kevenaar, T. A. M., Schrijnen, G.-J., Bazen, A. M., and Veldhuis, R. N. J., "Pratical biometric authentication with template protection," in [*5th International Conference, AVBPA*], (July 2005).

[23] Zhou, X., "Template protection and its implementation in 3d face recognition systems," in [*In Proceedings of SPIE 07, Biometric Technology for Human Identification IV*], (2007).

[24] Breebaart, J., Busch, C., Grave, J., and Kindt, E., "A reference architecture for biometric template protection based on pseudo identities," in [*BIOSIG*], (September 2008).

[25] "ISO/IEC JTC1 SC27. CD 24745 - information technology - security techniques - biometric template protection," (2009).

[26] Kelkboom, E. J. C., Garcia Molina, G., Breebaart, J., Veldhuis, R. N. J., Kevenaar, T. A. M., and Jonker, W., "Binary biometrics: An analytic framework to estimate the performance curves under gaussian assumption," *IEEE Transactions on Systems, Man and Cybernetics Part A, Special Issue on Advances in Biometrics: Theory, Applications and Systems (accepted)* (2010).

[27] Cover, T. M. and Thomas, J. A., [*Elements of Information Theory*], John Wiley & Sons, Inc. (1991).

[28] Kelkboom, E. J. C., Garcia Molina, G., Kevenaar, T. A. M., Veldhuis, R. N. J., and Jonker, W., "Binary biometrics: An analytic framework to estimate the bit error probability under gaussian assumption," in [*2nd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS '08)*], 1–6 (2008).

[29] Daugman, J., "The importance of being random: statistical principles of iris recognition," *Pattern Recognition* **36**(2), 279–291 (2003).