# Evaluation of Security for Biometric Guessing Attacks in Biometric Cryptosystem using Fuzzy Commitment Scheme

Seira HIDANO[1], Tetsushi OHKI[1], and Kenta TAKAHASHI[2,3]

[1]Faculty of Science and Engineering, Waseda University
3-4-1 Ohkubo, Shinjuku-ku, Tokyo, 169-8555, JAPAN
hidano@wiz.cs.waseda.ac.jp
ohki@suou.waseda.jp

[2]Yokohama Research Laboratory, Hitachi, Ltd.
292 Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa-ken, 244-0817, JAPAN
[3]Graduate School of Information Science and Technology, The University of Tokyo
7-3-1 Hongo, Bunkyo-ku, Tokyo, 113-8656, JAPAN
kenta.takahashi.bw@hitachi.com

**Abstract:** Biometric authentication based on template protection has attracted attention in the past decade. In the discussion on the security of these systems, however, the content of biometric information is assumed to be sufficiently large, and real conditions of biometric features have not yet been reflected. This paper focuses on a biometric cryptosystem using a fuzzy commitment scheme and demonstrates correlation between fingerprint bit strings by using our method for evaluating the content of biometric information. Additionally, attacks to guess biometric bit strings, which take advantage of correlation between them, are explained, and the security against these attacks is theoretically and experimentally discussed.

## 1 Introduction

Biometric authentication is convenient because users are freed from having to memorise something or keep hold of physical objects, so it has drawn attention as a method for implementing highly secure personal authentication for network services. However, biometric systems have specific vulnerabilities, which appear in their various components, including users, environmental conditions, operational conditions, biometric information, and biometrics devices. Since information unique to an individual is stored in the systems as a template and users cannot alter their own biometric characteristics, the privacy issues associated with information leaks are particularly weighty.

A number of technologies have already been proposed to prevent leakage of templates, and biometric authentication using these technologies is referred to as biometric authentication based on template protection. We focus on a biometric cryptosystem using a fuzzy commitment scheme (FCS) in this paper. Biometric cryptosystems incorporate functions that generate a secret key from auxiliary data only if a genuine user presents his/her biometric

information. These functions excel at concealing secret keys as well as protecting biometric templates, which enables these technologies to be applied to network authentication protocols using cryptographic techniques such as the challenge handshake authentication protocol (CHAP). On the other hand, in the FCS proposed by Juels and Wattenberg in 1999 [JW99], a commitment is created by binding biometric information with a codeword using a bitwise XOR operator after the codeword is generated from a secret key using an error-correcting encoder. This scheme can eliminate fluctuations of biometric information using an error-correcting decoder and can easily protect biometric templates, so its application is expected to be beneficial for biometric cryptosystems.

Additionally, since the FCS deals with quantised biometric information, there have been many studies on extracting bit strings from biometric samples [TAK+05, CV09]. Biometric bit strings have to meet the following requirement: Impostor bit strings should be i.i.d. in order to maximise the efforts to guess genuine ones. However, it is not easy to extract i.i.d. bit strings because biometric features strongly correlate, and most of those studies did not clearly state whether quantisers could eliminate the correlation or not.

Moreover, attempts have been made to theoretically analyse the security of the FCS from the viewpoint of information theory [STP09, WRDI11, KBK+11]. However, the content of biometric information is assumed to be sufficiently large, and it has not been considered that genuine bit strings can be easily guessed from compromised commitments due to the correlation between biometric bit strings.

We therefore discuss the security of the biometric cryptosystem using the FCS while taking into consideration the correlation between biometric bit strings. Zhou et al. analysed the correlation between iris bit strings and proposed an algorithm to recover an iris bit string from a compromised commitment by taking advantage of this correlation [ZKB12]. On the other hand, this paper does not focus on a particular characteristic, while taking a fingerprint bit string as an example. The rest of this paper is organised as follows. Sections 2 and 3 introduce the outlines of the biometric cryptosystem using the FCS and a method for evaluating the content of biometric information using quadratic Renyi entropy [HOKT10], respectively. Section 4 presents the evaluation of the information content in a fingerprint bit string using our method. Section 5 explains attacks to guess biometric bit strings, which take advantage of the correlation between them. Section 6 theoretically and experimentally discusses the security against these attacks.

## 2 Biometric cryptosystem using fuzzy commitment scheme

A fuzzy commitment scheme (FCS), proposed by Juels and Wattenberg in 1999 [JW99], is a type of cryptographic technology based on an error-correcting code. Figure 1 shows a client/server model of the biometric cryptosystem using the FCS.

**Enrolment process**

1. A user presents raw data on a biometric characteristic thorough a biometrics sensor,

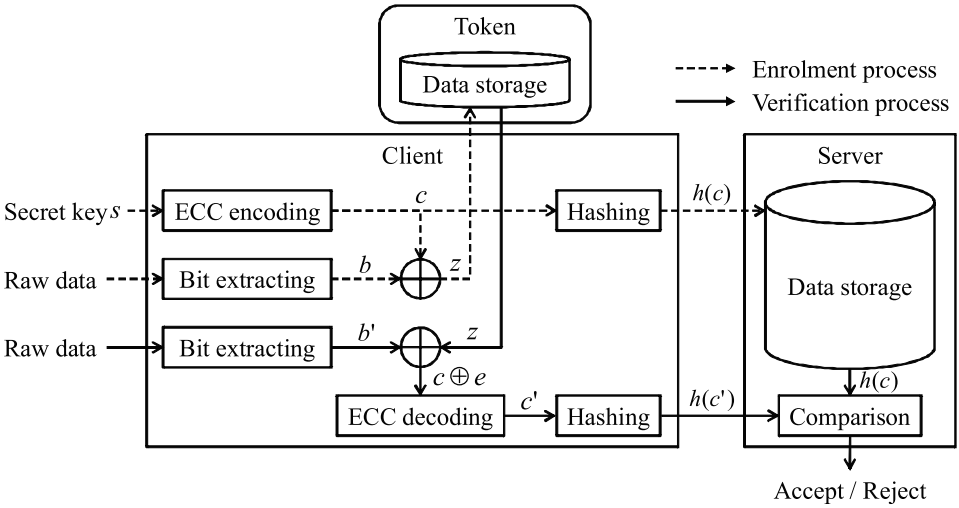


Figure 1: Biometric cryptosystem using fuzzy commitment scheme

and a client extracts a bit string, $b \in \mathcal{B} = \{0,1\}^n$, from the raw data. Note that $|\mathcal{B}| = 2^n$, where $|\cdot|$ denotes the number of members of a set.

2. The client generates a codeword, $c \in \mathcal{C}$, by passing a secret key, $s \in \{0,1\}^k$, chosen at random through an error-correcting encoder, and a commitment, $z$, is given by $b \oplus c$, where $\oplus$ denotes a bitwise XOR operator. We assume in this paper that $\mathcal{C}$ is an $(n, k, d_{min})$-linear error-correcting code, where $n$, $k$, and $d_{min}$ correspond to the codeword length, the number of information symbols, and the minimum distance. That is, $|\mathcal{C}| = 2^k$, and $t = (d_{min} - 1)/2$ or less bit errors can be corrected.

3. The client calculates the hash, $h(c)$, of $c$, and sends $h(c)$ to an authorisation server.

4. The server stores $h(c)$ in it's storage, and the client stores $z$ in user's token.

**Verification process**

1. The client extracts a bit string, $b' \in \mathcal{B}$, from raw data that a user presents as done with the enrolment process, and takes a stored $z$ from this user's token.

2. The client obtains $c'$ by passing $c \oplus e = b' \oplus z$ through an error-correcting decoder. Note that $e = b \oplus b'$; here, $c'$ corresponds to $c$ if $\| e \| \leq t$, where $\| \cdot \|$ denotes Hamming weights.

3. The client calculates the hash, $h(c')$, of $c'$, and sends $h(c')$ to the server.

4. The server compares $h(c')$ with $h(c)$ to determine whether the user is a genuine user or an impostor.

## 3 Method for evaluating content of biometric information

This section introduces a method for evaluating the content of biometric information using quadratic Renyi entropy [HOKT10]. To begin with, we will define the quadratic Renyi entropy of biometric information. Then, we will explain the procedure used to evaluate the quadratic Renyi entropy through inter-subject comparisons.

### 3.1 Quadratic Renyi entropy of biometric information

Let $B$ be a discrete random variable whose realisation is biometric information $b$ on possible values $\mathcal{B}$. We assume in our method that $b$ is represented by biometric features stored as a template in the system, e.g., an iris codeword [Dau03] or a set of fingerprint minutiae points.

The content of information obtained by observing a random variable following a certain probability distribution is often defined as Shannon entropy. The Shannon entropy of $B$ can be written as follows:

$$H(B) = -\sum_{b \in \mathcal{B}} p_B(b) \log_2 p_B(b), \tag{1}$$

where $p_B(b)$ is the probability mass function (PMF) of $B$. However, biometric features have some complex correlation, which cannot be simply modelled, and consequently it it difficult to theoretically estimate $p_B(b)$. It is also not easy to experimentally estimate $p_B(b)$ because the space of $b$ is generally high dimensional and a huge number of samples are required. $H(B)$ is thus not appropriate as a measure to evaluate the content of biometric information.

We therefore define the following quadratic Renyi entropy as a measure to evaluate the content of biometric information:

$$H_2(B) = -\log_2 \sum_{b \in \mathcal{B}} p_B(b)^2. \tag{2}$$

$H_2(B)$ is the case $\alpha = 2$ for the following Renyi entropy:

$$H_\alpha(B) = \frac{1}{1-\alpha} \log_2 \sum_{b \in \mathcal{B}} p_B(b)^\alpha, \tag{3}$$

where $\alpha \geq 0$, $\alpha \neq 1$. $H_2(B)$ indicates the possibility that two sets of biometric features will correspond, i.e., a measure to evaluate collision resistance.

Here, we consider the PMF, $p_D(d)$, of a discrete random variable $D$ whose realisation is the distance $d$ between two sets, $b$ and $b' \in \mathcal{B}$, of biometric features. Let $B$ and $B'$ be random variables whose realisations are respectively $b$ and $b'$, and $g$ be a distance function

such that $g : \mathcal{B} \times \mathcal{B} \to \mathbb{R}$. If it is assumed that $B$ and $B'$ are i.i.d. on $\mathcal{B}$, $p_D(d)$ can be written as follows:

$$\begin{aligned} p_D(d) &= P(g(B, B') = d) && (4) \\ &= \sum_{\substack{b,b' \in \mathcal{B}, \\ g(b,b')=d}} P(B = b, B' = b') && (5) \\ &= \sum_{\substack{b,b' \in \mathcal{B}, \\ g(b,b')=d}} p_B(b) p_B(b'). && (6) \end{aligned}$$

According to the identity of indiscernibles such that $d(b, b') = 0$ if and only if $b = b'$, which is a metric axiom, we obtain the following:

$$\begin{aligned} p_D(0) &= \sum_{\substack{b,b' \in \mathcal{B}, \\ b=b'}} p_B(b) p_B(b') && (7) \\ &= \sum_{b \in \mathcal{B}} p_B(b)^2. && (8) \end{aligned}$$

From Equation (2), therefore, $H_2(B)$ can also be written as follows:

$$H_2(B) = -\log_2 p_D(0). \quad (9)$$

The space of $d$ will be lower dimensional than that of $b$, while the amount of samples of $d$, which are obtained through inter-subject comparisons, can be quadratic in the number of samples of $b$. Accordingly, a sufficiently large number of samples of $d$ can be corrected, and $p_D(d)$ can be more easily estimated as compared to $p_B(b)$. If the collection of samples of $b$ and the comparisons follow the standard method of evaluating biometric accuracy, the estimation of distribution will be more reliable [MW02]. For this reason, $H_2(B)$ can be evaluated with Equation (9) and is considered to be a practicable measure for evaluating the content of biometric information.

### 3.2 Procedure to evaluate quadratic Renyi entropy

The quadratic Renyi entropy, $H_2(B)$, of biometric information can be evaluated with the following procedure:

1. Samples of the distance $d$ are obtained through inter-subject comparisons using a sufficient number of samples of biometric features $b$. As mentioned in Subsection 3.1, this step should follow the same procedure as that in the standard method for evaluating biometric accuracy.

2. The probability mass function, $p_D(d)$, of $d$ is estimated from the samples of $d$. Since $p_D(0)$, i.e., the probability that two sets of biometric features correspond, is considered to be an extremely small value, the observed value will be 0. Thus $p_D(0)$ should be calculated from the estimated distribution of $p_D(d)$. If the modelling of $p_D(d)$ is well investigated as it was with Daugman's model of iris authentication [Dau03], $p_D(d)$ is parametrically estimated from the samples of $d$ because it can be easily calculated. If the shape of $p_D(d)$ is not fully known, on the other hand, $p_D(d)$ is estimated using a nonparametric estimator that depends on training data.

3. $H_2(B)$ is calculated for the estimated value of $p_D(0)$ by using Equation (9).

# 4 Evaluation of information content in fingerprint bit string

Let us evaluate the information content in a fingerprint bit string on the basis of our method described in Section 3. To begin with, we will explain the application of our evaluation method to the biometric cryptosystem using the FCS. Then, we will present the results from experimentally estimating the information content using a fingerprint image set.

## 4.1 Quadratic Renyi entropy of biometric bit string

In the biometric cryptosystem using the FCS, biometric information $b$ is represented by an $n$-long bit string as described in Section 2, i.e., $b \in \mathcal{B} = \{0,1\}^n$, which allows the distance $d$ between two bit strings $b$, $b' \in \mathcal{B}$ to be written as follows:

$$d = \frac{\| b \oplus b' \|}{n}. \tag{10}$$

Given a random variable $D$ whose realisation is $d$, we assume that the PMF, $p_D(d)$, of $D$ can be modelled as the following binomial distribution $Bi(\theta, \hat{n})$:

$$p_D(d) = \frac{\hat{n}!}{(\hat{n}d)!(\hat{n}(1-d))!}\theta^{\hat{n}(1-d)}(1-\theta)^{\hat{n}d}. \tag{11}$$

This is because the definition of $b$ and $d$ is the same as that in Daugman's proposed model of iris authentication using an iris code [Dau03]. If $p_D(d)$ can be modelled as $Bi(\theta, \hat{n})$, $\theta$ means the correspondence probability for each bit, and $\hat{n}$ means the number of usable bits for discrimination. The expectation, $E(D)$, and the variance, $V(D)$, of $D$ can be written as follows:

$$E(D) = 1-\theta, \tag{12}$$

$$V(D) = \frac{\theta(1-\theta)}{\hat{n}}. \tag{13}$$

According to Equation (11), $p_D(0) = \theta^{\hat{n}}$, and hence the quadratic Renyi entropy of a random variable $B$ on $\mathcal{B}$ can be written as follows:

$$H_2(B) = -\log_2 \theta^{\hat{n}}. \tag{14}$$

$\theta$ and $\hat{n}$ therefore need to be estimated from samples of $d$ and Equations (12) and (13) to calculate $H_2(B)$, and the samples of $d$ to be obtained through inter-subject comparisons using samples of $b$.

Equation (14) can be considered to be a generalisation of Daugman's discrimination entropy [Dau03] in terms of quadratic Renyi entropy. Daugman did not refer to a sense of discrimination entropy for $\theta \neq 1/2$, while Equation (14) enable us to evaluate the correlation between biometric bit strings on the basis of the concept of information content for an arbitrary value of $\theta$.

### 4.2 Evaluation results

Taking up the biometric cryptosystem proposed by Tuyls et al. [TAK+05] as an example, we used 800 images in set A of FVC2002 DB1, in which the images consisted of eight images of each 100 fingers. Using six fingerprint images of each finger for registration and the remaining two images for verification, we generated $n = 127$-long fingerprint bit strings and performed inter-subject comparisons. The average value of distance scores between bit strings was 0.499, and the variance value was 0.00684. According to Equations (12) and (13), the estimated values for the correspondence probability, $\theta$, for each bit and the number, $\hat{n}$, of valid bits were 0.501 for the former and 37 for the latter, and then the quadratic Renyi entropy, $H_2(B)$, of a fingerprint bit string was 36 bits by using Equation (14). If fingerprint bit strings are uniformly distributed on $\mathcal{B} = \{0,1\}^{127}$, $H_2(B)$ will ideally be 127 bits, but the experimental value of $H_2(B)$ fell much below the ideal value. Consequently, we can say that fingerprint bit strings were correlated and thus this correlation will allow an adversary to perform the attacks explained in Section 5.

However, $p_D(d)$ cannot be always modelled as a binomial distribution because different types of correlation would occur according to the kind of biometric characteristic and extracted features. If the value of $H_2(B)$ needs to be more accurately evaluated, the modelling of $p_D(d)$ should be more carefully discussed, or nonparametric approaches should be adopted, as mentioned in Subsection 3.2.

## 5 Biometric guessing attacks

In this section, we consider practical guessing attacks taking advantage of the correlation between biometric bit strings, whose objective is that an adversary is incorrectly authenticated. To begin with, we will explain a biometric dictionary attack (BDA) as an attack in a normally running system where the commitment is not compromised, which only

takes advantage of the correlation between biometric bit strings. Next, we will explain an exhaustive codeword search attack (ECSA), which only takes advantage of the size of codeword space. This is because if the ECSA has a higher probability of success than the BDA, adversaries will carry out the ECSA when the system is running normally. Last, we propose a decodable biometric dictionary attack (DBDA) taking advantage of both the correlation between biometric bit strings and the size of codeword space.

### 5.1 Biometric dictionary attack (BDA)

The BDA is carried out with the following procedure:

1. An adversary prepares a number of samples, $DB = \{b_1, \ldots, b_N\}$, of the bit string on the biometric characteristic a targeted authentication system uses, which are obtained from real people, and then chooses a bit string $b^*$ at random from $DB$.
2. In step 1 of the verification process explained in Section 2, the adversary inputs $b^*$ as a genuine user.
3. If the authorisation server accepts the adversary in step 4 of the verification process, the attack is completed.

### 5.2 Exhaustive codeword search attack (ECSA)

If it is assumed that an adversary knows the system parameters that concern the error-correcting code and the generator polynomial, the ECSA is performed with the following procedure:

1. An adversary chooses a codeword $c^*$ at random from an error-correcting code $\mathcal{C}$ whose cardinality is $2^k$.
2. In step 3 of the verification process, the adversary inputs $c^*$ to the client as a genuine user.
3. If the authorisation server accepts the adversary in step 4 of the verification process, the attack is completed.

### 5.3 Decodable biometric dictionary attack (DBDA)

When a commitment, $z = b \oplus c$, of a certain user is compromised, the DBDA is conducted with the following procedure:

1. As with the first step of the BDA, an adversary prepares a number of samples, $DB = \{b_1, \ldots, b_N\}$, of the biometric bit string a targeted system uses.

2. The adversary passes $b_i \oplus z$ through an error-correcting decoder, where $b_i \in DB$. Then, $b_i \oplus z$ can be transformed into one of the codewords, or no codeword will be output due to the failure to decode.

3. In the second step above, if a codeword is obtained, the adversary adds $b_i$ to a new set $\overline{DB}$. The second and third steps are performed for every $b_i$.

4. The adversary chooses a bit string $b^*$ at random from $\overline{DB}$, and inputs $b^*$ as the user whose $z$ is compromised in the first step of the verification process. If the authorisation server accepts the adversary in step 4 of the verification process, the attack is completed.

Note that it is assumed that commitments are not revoked or reissued when they are compromised and the hash, $h(c)$, of $c$ is not leaked from the corresponding user's token.

Additionally, Simoens and Kelkboom both analysed a similar decodability attack based on cross-matching as the DBDA in terms of indistinguishability [STP09, KBK+11], and further Kelkboom proposed a countermeasure to the decodability attack by implementing a bit-permutation on the bit string. However, we note that this countermeasure cannot prevent the DBDA when the matrix for bit-permutation is public.

# 6 Security analysis

This section discusses the theoretical security for each attack explained in Section 5 and presents the results from experimentally evaluating the security. In the theoretical discussion, however, we consider a special case where correlation is caused by members with an extremely low probability of occurrence in the space of biometric bit strings.

## 6.1 Successful attack probability in normally running system

The successful attack probability of the BDA corresponds to the false accept rate ($FAR$), which is a standard measure for assessing biometric accuracy. Let a subspace, $\bar{\mathcal{B}}$, of the space, $\mathcal{B} = \{0,1\}^n$, of biometric bit strings be given by $\bar{\mathcal{B}} = \{b | p_B(b) > 0, b \in \mathcal{B}\}$, using the PMF, $p_B(b)$, of a random variable $B$ on $\mathcal{B}$. A random variable on $\bar{\mathcal{B}}$ is assumed to follow a uniform distribution. The value of $|\bar{\mathcal{B}}|$ will be less than that of $|\mathcal{B}|$ when information content in a biometric bit string falls below an ideal value due to some correlation, as described in Section 4. Given a word $x$ chosen from $\{0,1\}^n$ at random and the probability $P(x \in \bar{\mathcal{B}})$ that the $x$ is a member of $\bar{\mathcal{B}}$, $FAR$ can be written as follows:

$$FAR = \frac{|\bar{\mathcal{B}}_t(b)|}{2^n \cdot P(x \in \bar{\mathcal{B}})} \tag{15}$$

$$= \frac{|\bar{\mathcal{B}}_t(b)|}{|\bar{\mathcal{B}}|}, \tag{16}$$

where $\bar{\mathcal{B}}_t(b)$ denotes a set of bit strings in the hypersphere with centre $b \in \bar{\mathcal{B}}$ and radius $t$, i.e., $\bar{\mathcal{B}}_t(b) = \{b' | \parallel b \oplus b' \parallel \leq t, b' \in \bar{\mathcal{B}}\}$.

Then, given the space, $\mathcal{C}$, of codewords, the successful attack probability, $P_{ECSA}$, of the ECSA can be written as follows:

$$P_{ECSA} = \frac{1}{2^n \cdot P(x \in \mathcal{C})} \tag{17}$$

$$= \frac{1}{|\mathcal{C}|} = \frac{1}{2^k}. \tag{18}$$

The successful attack probability ($SAP$) in a normally running system can therefore be written as follows:

$$SAP = \max\{FAR, P_{ECSA}\}. \tag{19}$$

Function $\max$ returns the maximum value of all values.

### 6.2 Successful attack probability in system compromising commitment

When the commitment, $z$, of a certain user is compromised, the successful attack probability, $\overline{SAP}$, of the DBDA can be written as follows:

$$\overline{SAP} = \frac{|\bar{\mathcal{B}}_t(b)|}{2^n \cdot P(x \oplus z \in \bigcup_{c \in \mathcal{C}} \mathcal{C}_t(c), x \in \bar{\mathcal{B}})} \tag{20}$$

$$\approx \frac{|\bar{\mathcal{B}}_t(b)|}{2^n \cdot P(x \in \bigcup_{c \in \mathcal{C}} \mathcal{C}_t(c) \cap \bar{\mathcal{B}})} \tag{21}$$

$$\approx \frac{|\bar{\mathcal{B}}_t(b)|}{2^n \cdot P(x \in \bigcup_{c \in \mathcal{C}} \mathcal{C}_t(c)) P(x \in \bar{\mathcal{B}})} \tag{22}$$

$$= \frac{|\bar{\mathcal{B}}_t(b)|}{2^n \cdot |\mathcal{C}_t(c)| \cdot P(x \in \mathcal{C}) P(x \in \bar{\mathcal{B}})}, \tag{23}$$

where $\mathcal{C}_t(c)$ denotes a set of words that can be transformed into a certain codeword $c \in \mathcal{C}$ by an error-collecting decoder, i.e., $\mathcal{C}_t(c) = \{w | \parallel c \oplus w \parallel \leq t, w \in \{0,1\}^n\}$. Due to the properties of linear codes, we supposed in Equation (21) that the proportion of the words that can be transformed into codewords by an error-correcting decoder in $\bar{\mathcal{B}}$ nearly equals that of these words in the space such that $\bar{\mathcal{B}}$ is translated by $z$ [WRDI11]. Additionally, Equation (22) follows from the assumption that the proportion of members of $\bar{\mathcal{B}}$ in $\bigcup_{c \in \mathcal{C}} \mathcal{C}_t(c)$ nearly equals that of these members in $\{0,1\}^n$. If $|\bar{\mathcal{B}}_t(b)| = |\mathcal{C}_t(c)|$ is assumed, Equations (15) and (17) allow $\overline{SAP}$ to be written as follows:

$$\overline{SAP} \approx FAR \cdot \frac{1}{|\mathcal{C}_t(c)| \cdot P(x \in \mathcal{C})} \tag{24}$$

$$\approx P_{ECSA} \cdot \frac{1}{P(x \in \bar{\mathcal{B}})}. \tag{25}$$

Table 1: Successful attack probability

| $(n, k, d_{min})$ | (127,8,57) | (127,15,55) | (127,22,47) |
|---|---|---|---|
| $FRR$ | 0.0214 | 0.0267 | 0.0481 |
| $FAR$ | 0.00264 | 0.00232 | 0.00124 |
| $P_{ECSA}$ | 0.00391 | $3.05 \times 10^{-5}$ | $2.38 \times 10^{-7}$ |
| $SAP$ | 0.00391 | 0.00232 | 0.00124 |
| $\overline{SAP}$ | 0.228 | 0.216 | 0.135 |

Therefore, $\overline{SAP} \geq SAP$, which means that security of a system compromising a commitment is lower than that of a normally running system.

### 6.3 Evaluation results

As with the experiments explained in Subsection 4.2, we adopted the biometric cryptosystem using fingerprint bit strings proposed by Tuyls et al. [TAK+05]. We used a BCH code as a $(n, k, d_{min})$-linear code.

Table 1 lists the false reject rate ($FRR$), $FAR$, $P_{ECSA}$, $SAP$, and $\overline{SAP}$ for different BCH codes. If we take $(n, k, d_{min}) = (127, 22, 47)$ as an example, if fingerprint bit strings do not correlate and the PMF of a fingerprint bit string can be modelled as a uniform distribution, $FAR = \sum_{i=0}^{23} {}_{127}\mathrm{C}_i / 2^{127} = 8.48 \times 10^{-14}$, according to Equation (16). However, if we take the value of $FAR$ when $(n, k, d_{min}) = (127, 22, 47)$ in Table 1, the value is very different from the above ideal value, which means security deteriorates greatly due to the correlation between fingerprint bit strings. Moreover, in all BCH codes, the value of $\overline{SAP}$ is much greater than that of $SAP$, and the computational time for preparing a new set $\overline{DB}$ in steps 2 and 3 of the DBDA explained in Subsection 5.3 was negligibly small. We hence observed that the security of a system compromising a commitment is much lower than that of a normally running system.

## 7 Conclusion

This paper focused on a biometric cryptosystem using a fuzzy commitment scheme (FCS) and demonstrated the correlation between fingerprint bit strings by experimentally evaluating the information content in a fingerprint bit string. The security against attacks to guess biometric bit strings, which take advantage of this correlation, were theoretically discussed, and the results from quantifying the security in accordance with an experimental evaluation were presented. Consequently, we now know that the security of a system compromising a commitment is lower than that of a normally running system. In Subsections 6.1 and 6.2, however, since some ideal assumptions were used to develop successful attack probabilities, we will discuss the security of the FCS without these assumptions. We will also analyse theoretically and experimentally the security against a decodable biometric

dictionary attack (DBDA) in cases where not linear codes but other error-correcting codes are applied to the FCS.

## Acknowledgments

This paper contains some research achievements of a national project funded by the Ministry of Internal Affairs and Communications in Japan, Project #0155-0206.

## References

[CV09] C. Chen and R. Veldhuis. Binary biometric representation through pairwise polar quantization. In *Proceedings of the 3rd IAPR/IEEE International Conference on Biometrics (ICB2009)*, pages 72–81, 2009.

[Dau03] J. Daugman. The importance of being random: Statistical principles of iris recognition. *Pattern Recognition*, 36(2):279–291, 2003.

[HOKT10] Seira Hidano, Tetsushi Ohki, Naohisa Komatsu, and Kenta Takahashi. A metric of identification performance of biometrics based on information content. In *Proceedings of the 11th International Conference on Control, Automation, Robotics and Vision (ICARCV2010)*, pages 1274–1279, 2010.

[JW99] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS1999)*, pages 28–36, 1999.

[KBK+11] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis. Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Transactions on Information Forensics and Security*, 6(1):107–121, 2011.

[MW02] A. J. Mansfield and J. L. Wayman. Best practices in testing and reporting performance of biometric devices: Version 2.01. Technical report, Center for Mathematics and Scientific Computing, National Physical Laboratory, 2002.

[STP09] K. Simoens, P. Tuyls, and B. Preneel. Privacy weaknesses in biometric sketches. In *Proceedings of 2009 IEEE Symposium on Security and Privacy*, pages 188–203, 2009.

[TAK+05] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis. Practical biometric authentication with template protection. In *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA2005)*, pages 436–446, 2005.

[WRDI11] Y. Wang, S. Rane, S. C. Draper, and P. Ishwar. An information-theoretic analysis of revocability and reusability in secure biometrics. In *Proceedings of 2011 Information Theory and Applications Workshop (ITA2011)*, pages 1–10, 2011.

[ZKB12] X. Zhou, A. Kuijper, and C. Busch. Retrieving secrets from iris fuzzy commitment. In *Proceedings of the 5th IAPR International Conference on Biometrics (ICB2012)*, 2012.