1-1-2015

A new bio-cryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion

Cai Li
University of New South Wales, Canberra

Jiankun Hu
University of New South Wales, Canberra

Josef Pieprzyk
Queensland University of Technology

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

A new bio-cryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion

Abstract

Biometric cryptosystems provide an innovative solution for cryptographic key generation, encryption as well as biometric template protection. Besides high authentication accuracy, a good biometric cryptosystem is expected to protect biometric templates effectively, which requires that helper data does not reveal significant information about the templates. Previous works predominantly follow an appropriate entropy definition to measure the security of biometric cryptosystems. In this paper, we point out limitations of entropy-based security analysis and propose a new security analysis framework that combines information-theoretic approach with computational security. In addition, we construct a fingerprint-based multibiometric cryptosystem using decision level fusion. Hash functions are employed in our construction to further protect each single biometric trait. The experimental results and security analysis demonstrate that the proposed multibiometric cryptosystem provides stronger security and better authentication accuracy compared to a cryptosystem based on single biometric.

Keywords

oriented, cryptosystem, decision, cryptosystems, level, fusion, multibiometric, analysis, framework, bio, security, implementation

Disciplines

Engineering | Science and Technology Studies

Publication Details

Li, C., Hu, J., Pieprzyk, J. & Susilo, W. (2015). A new bio-cryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion. IEEE Transactions on Information Forensics and Security, 10 (6), 1193-1206.

A New Bio-cryptosystem-oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion

Cai Li, Jiankun Hu, Josef Pieprzyk, Willy Susilo

***Abstract*—Biometric cryptosystems provide an innovative solution for cryptographic key generation, encryption as well as biometric template protection. Besides high authentication accuracy, a good biometric cryptosystem is expected to protect biometric templates effectively, which requires that helper data does not reveal significant information about the templates. Previous works predominantly follow an appropriate entropy definition to measure the security of biometric cryptosystems. In this paper, we point out limitations of entropy-based security analysis and propose a new security analysis framework that combines information-theoretic approach with computational security. In addition, we construct a fingerprint-based multibiometric cryptosystem using decision level fusion. Hash functions are employed in our construction to further protect each single biometric trait. The experimental results and security analysis demonstrate that the proposed multibiometric cryptosystem provides stronger security and better authentication accuracy compared to a cryptosystem based on single biometric.**

***Index Terms*—Biometric cryptosystems, min-entropy, Shannon-entropy, authentication accuracy, template protection, security.**

I. Introduction

Compared with traditional authentication techniques such as passwords and token cards, biometric-based techniques offer a non-repudiable, more universal and reliable option for individuals' authentication. A typical biometric-based authentication system is composed of two processes [1]: (1) the enrollment process, in which the system scans a user's biometric image, creates a biometric template of biometric features extracted from the image, and stores the template in databases; and (2) the authentication process, in which the system scans an individual's biometric data, extracts biometric features in the same manner and compares them with the template of the user the individual claims to be. The system will output a match if according to a pre-defined similarity measure, a query is sufficiently similar to the template or a mismatch if it is not.

However, widespread applications of biometrics have brought about new security challenges. As biometric templates are physically stored in databases or servers, raw images are able to be reconstructed once the templates are compromised by attackers [2]. Unlike traditional passwords or token cards, which can be reset or reissued, compromised biometric data is unlikely to be replaced due to the scarcity of biometric traits an individual possesses, which means a permanent loss of the chosen biometric features for authentication purposes. More seriously, since a biometric template is likely to be used repeatedly on different applications, a compromise of the template will put all these applications at risk and may lead to a great loss to the owner.

Over the past few years, there has been a great deal of work on how to protect biometric templates. Basically, biometric protection techniques use transformed data instead of original biometric data or feature-based templates to authenticate users. Proposed methods can be classified into two types: (1) feature transformations (or cancelable biometrics) [3]-[6], and (2) biometric cryptosystems [7]-[11]. The former applies non-invertible transformations to modify original biometric data. The transformed template is stored for matching. Once the transformed template is compromised, the system can reissue a new one using different transformation parameters. Biometric cryptosystems provide an innovative solution for cryptographic key generation, encryption as well as biometric template protection. In biometric cryptosystems, original templates are replaced by biometric-dependent information (referred to as helper data), which assists in recovering cryptographic keys. Matching is performed indirectly by verifying the validity of recovered keys.

Cai Li is with the School of Engineering and Information Technology, University of New South Wales at Canberra, Canberra, Australia. (e-mail: Cai.Li2@student.adfa.edu.au).

Jiankun Hu is with the School of Engineering and Information Technology, University of New South Wales at Canberra, Canberra, Australia. (e-mail: J.Hu@adfa.edu.au).

Josef Pieprzyk is with the School of Electrical Enginerring and Computer Science, Science and Engineering Faculty, Queensland University of Technology, Brisbane, Australia. (e-mail: josef.pieprzyk@qut.edu.au).

Willy Susilo is with the School of Computer Science and Software Engineering, University of Wollongong, Wollongong, Australia. (e-mail: wsusilo@uow.edu.au)

There exist two major criteria for judging the performance of a biometric cryptosystem: accuracy and security. The accuracy of biometric cryptosystems, similar to that of biometric authentication systems, is also measured by False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR is the probability of an imposter being accepted as an authorized user, while FRR is the probability of a legitimate user being rejected as an imposter. The security of biometric cryptosystems requires that helper data, once compromised by an attacker, should not reveal significant information about original biometric templates. A majority of papers in this field follows the average min-entropy of original biometric templates given helper data as a security metric [11]. However, Golic *et al.* [12] point out that the average min-entropy does not measure the statistical independence of random variables and introduced the conditional Shannon entropy instead. It is noteworthy that both the average min-entropy and the conditional Shannon entropy measure the security from the information-theoretic perspective, which merely reflects the probabilities rather than the actual values of biometric templates. Therefore, they cannot be completely equated with the security of biometric cryptosystems, especially those that are information-theoretically insecure but computationally secure. Unfortunately, this issue has not aroused due attention from researchers. What is worse, entropy measures are improperly employed in the security analysis of some biometric cryptosystems, especially in the case of fingerprint cryptosystems.

Although biometric cryptosystems applying single biometric (such as fingerprint, iris, face etc.) have been widely studied, the accuracy and security of single biometric cryptosystems (SBC) are limited, which leads to the theoretical work and practical applications of multibiometric cryptosystems (MBC). Compared to SBC, MBC offer higher authentication accuracy and flexibility, wider population coverage and stronger security. In general, MBC can be classified into two categories based on different fusion modes: (1) fusion at the feature level (also known as biometric level), and (2) fusion at the decision level (also known as cryptographic level) [13]. The former fuses biometric features from multiple sources into a single template for identification and verification. The latter performs authentication in each SBC separately and outputs final decisions based on specific rules (such as *n* out of *k* rule based fusion). Fu *et al*. [13] provide the theoretical accuracy analysis of MBCF (multibiometric cryptosystems based on feature level fusion) and MBCD (multibiometric cryptosystems based on decision level fusion). They conclude that both MBCF and MBCD (*MN*-split mode) have higher authentication accuracy (lower FAR and lower FRR) than SBC. However, we find their analysis is flawed and therefore reanalyze the accuracy of MBC. From our results, the accuracy of both MBCF and MBCD (*MN*-split mode) is not theoretically better than that of corresponding SBC but influenced by several practical factors, such as selected biometric traits, fusion algorithms, decision rules, etc.

Compared with MBCD, MBCF are more frequently proposed and studied in recent years since they can provide higher recognition accuracy as well as stronger security for single biometric templates [1], [14]-[16]. Sutcu *et al*. [1] design a combined template of fingerprint and face, and apply Pinsketch [11] for template protection. Nandakumar and Jain [15] adopt fuzzy vault to conceal a template fusing fingerprint and iris features among a host of chaff points. Camlikaya *et al*. [16] provide a template protection scheme by hiding fingerprint features among voice. However, as feature fusion transforms features from different biometric sources into the same universe, concatenation of these features can be arduous due to the inconsistency of different biometrics traits. Besides, the extendibility of MBCF is poor and may lead to the curse-of-dimensionality problem [17]. In contrast, implementation of MBCD avoids the difficulty of biometric feature unification and is more flexible in terms of choosing biometric sources and their corresponding cryptosystem constructions. These advantages motivate us to construct a practical MBCD.

This paper mainly consists of two parts: a new bio-cryptosystem-oriented security analysis framework and a practical fingerprint-based MBCD construction. Our work makes the following contributions. It

1. investigates the relations among different entropy measures and system security in depth under two common scenarios,
2. revisits the entropy-based security analysis of some popular fingerprint-based cryptosystems and points out the limitation of entropy for measuring the security of biometric cryptosystems,
3. proposes a new security analysis framework, which merges information-theoretic and computational security,
4. revisits the analysis of the authentication accuracy of MBCF and MBCD,
5. constructs a practical MBCD using fingerprints from multiple fingers of individuals.

The rest of this paper is organized as follows. Some preliminaries are presented in Section II, including basic concepts and terms used in the work. Section III concentrates on analyzing the correspondence between widely-applied entropy measures and systems security. In Section IV, we reanalyze the entropy-based security of several well-known fingerprint-related cryptosystems. A new security analysis framework for biometric cryptosystems is proposed in Section V. Section VI is dedicated to the accuracy analysis of MBC from a theoretical perspective, and a practical fingerprint-based MBCD construction is proposed in Section VII. Conclusions are given in Section VIII.

II. PRELIMINARY

A. Biometric Cryptosystems

Generally, based on how helper data is derived, biometric cryptosystems can be classified into two categories: key-binding systems and key generating systems [18]-[22].

1) Key-binding systems

Helper data is obtained by binding a chosen cryptographic key with a biometric template. During the matching/authentication process, the system attempts to recover the cryptographic key from the helper data using a biometric query (see Figure 1). The design of a key-binding biometric cryptosystem should always ensure that the key

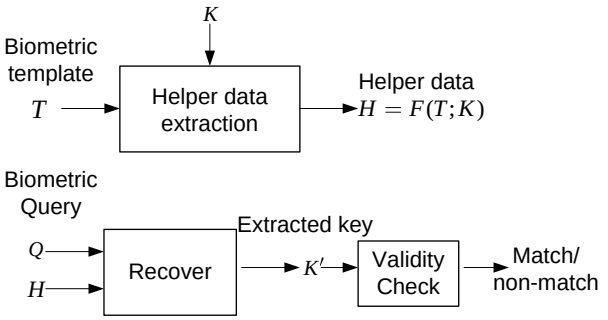

Fig. 1. The framework of key-binding systems

can be successfully recovered with overwhelming probability if the query is from a legitimate user.

2) Key generating systems

Helper data is derived only from the biometric template and the cryptographic key is generated from the helper data and the biometric query. If the template and query are from the same user, then the generated keys will be the same with overwhelming probability. Key generating systems are also referred to as "fuzzy extractor" or "secure sketch" (see Figure 2), both of which are formally-defined in [11]. In general, a fuzzy extractor is composed of a secure sketch and a strong extractor. The secure sketch uses helper data to recover original biometric templates while the strong extractor generates nearly uniform random keys from biometric data.

B. *Metric Spaces* (M)

Dodis *et al*. [11] define three metric spaces: Hamming metric, set difference metric and edit metric. The majority of biometric data falls into the first two metric spaces because a biometric template can always be represented as either a binary string or a set of features.

They also define distance functions in each metric space to measure the difference between the template and query. Definitions of Hamming distance and set distance are given as follows.

1) Hamming distance. Here $M = F^n$ for some alphabet F. For $x,\ x' \in F^n$, the distance between them, denoted by $dis(x, x')$, is the number of positions in which the strings x and x' differ.

2) Set difference distance. Here M consists of all subsets of a universe U and $|U| = n$. For $x, x' \in M$, $dis(x, x') = |x| + |x'| - 2|x \cap x'|$.

C. *Widely-Used Biometric Cryptosystem Constructions*

There are many constructions of biometric cryptosystems, among which fuzzy commitment, fuzzy vault and Pinsketch are most popular. Brief descriptions of them are given below. For more details, please refer to [9]-[11].

1) Fuzzy Commitment (Hamming Metric) [9]

This construction is made up of two algorithms: commitment and decommitment. To commit a template x that can be expressed by an n-bit string, the system selects a

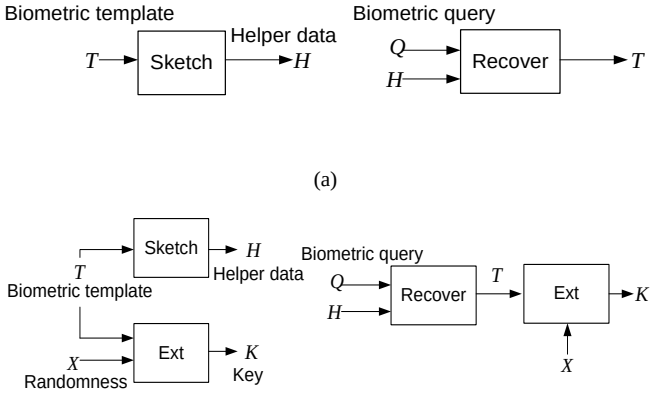

Fig.2. The frameworks of (a) a secure sketch and (b) a fuzzy extractor

random codeword c and sets $\partial = c + x$. Then $F(c, x) = (h(c), \partial)$ is stored in the system as a commitment, where h is a hash (or one-way) function [9]. To decommit a query x', $x' - \partial$ is calculated and mapped to the nearest codeword c', the decommitment is successful if $h(c') = h(c)$. For codewords with the minimum distance d, the decommitment can always succeed as long as $dis(x', x) \le t$, where $t = \lfloor d/2 \rfloor$.

2) Fuzzy Vault (Set Difference Metric) [10]

With a template that can be expressed by a set of biometric features: $x = \{x_1, x_2, ...x_s\} \in U^s$ and a cryptographic key $k = k_0 k_1 k_2 ... k_{m-1} \in U^m$ satisfying $m \le s$, a polynomial $p(x) = k_{m-1}x^{m-1} + k_{m-2}x^{m-2} + ... + k_1 x + k_0$ is constructed and evaluated at each point in x to generate a genuine set $\{x_i, p(x_i)\}_{i=1}^{s}$. Then a chaff point set $\{x_i, y_i\}_{i=s+1}^{r}$ is generated, where $x_i \notin \{x_1, x_2, ...x_{i-1}\}$ and $y_i \ne p(x_i)$. $\{x_i, p(x_i)\}_{i=1}^{s}$ and $\{x_i, y_i\}_{i=s+1}^{r}$ compose a vault $v = \{x_i, p(x_i)\}_{i=1}^{s} \bigcup \{x_i, y_i\}_{i=s+1}^{r}$ (helper data). It is commonly known that a polynomial of degree $m-1$ can be uniquely determined by m pairs of points, so if a query x' overlaps with x significantly, the polynomial p can be reconstructed. Further, both the key and template can be retrieved as well.

3) Pinsketch (Set Difference Metric) [11]

Pinsketch is a syndrome-based construction designed to deal with set difference. With a template $x = \{x_1, x_2, ...x_s\}$, the system generates helper data as

$$SS(x) = syn(x) = (s_1, s_3, ...s_{2t-3}, s_{2t-1}),$$

where $s_i = \sum_{j=1}^{s} x_j^{\,i}$ and t is the error tolerance. When a query $x' = \{x_1', x_2', ...x_s'\}$ is presented, the sketch generates the syndrome of x' as

$$syn(x') = (s_1', s_3', ...s_{2t-3}', s_{2t-1}'),$$

and retrieves the template x by

$$Rec(x', SS(x)) = supp(v)\Delta x',$$

where $supp(v)\Delta x' = supp(v) \cup x' - supp(v) \cap x'$ and $supp(v)$ denotes the positions in which v is nonzero, which can be computed through the syndrome of v:

$$syn(v) = (s_1' - s_1, s_3' - s_3, ...s_{2t-1}' - s_{2t-1})$$

The construction guarantees that if $dis(x', x) \le t$, $Rec(x', SS(x)) = x$.

D. Security of biometric cryptosystems

In biometric cryptosystems, physically-stored helper data is always assumed public to attackers and the security has been put into precise mathematical terms by defining the amount of information by appropriate entropy measures. Most papers in this field [1], [11], [15] have been following the average min-entropy of original biometric templates X given helper data Y, i.e., $\tilde{H}_\infty(X \mid Y)$, while some of them [12], [13], [23] use the conditional Shannon entropy, $H(X \mid Y)$. The entropy measures used in the paper are listed below.

$$H_\infty(X) = -\log \max_x \Pr(X = x) \quad (1)$$

$$H(X) = -\sum_{x \in X} \Pr(X = x) \log \Pr(X = x) \quad (2)$$

$$\begin{aligned} \tilde{H}_\infty(X \mid Y) &= -\log(E_{y \leftarrow Y}[\max_x \Pr(X = x \mid Y = y)]) \\ &= -\log(E_{y \leftarrow Y} 2^{-H_\infty(X|y)}) \end{aligned} \quad (3)$$

$$H(X \mid Y) = \sum_{y \in Y} \Pr(Y = y) H(X \mid Y = y) \quad (4)$$

III. Entropy And Security

It is a well-established fact that entropy reflects the amount of information. However, entropy is also very useful to characterize security of a system. When we analyze security, we often ask about how difficult it is to obtain secrets (such as passwords, private keys, biometric traits, etc.) by an attacker. A typical strategy of the attacker is to try to guess a secret. There are two possible scenarios that the attacker can apply [12]: (1) one-step guessing until success, and (2) multiple-guessing until success. In the first scenario, the attacker aims to guess one secret from a large collection of secrets. To be more specific, the attacker makes a guess and then browses the collection of secrets until a match is found. In the second scenario, the attacker targets a specific secret and keeps guessing until success. The two scenarios are illustrated below with an example of dicing game.

Dicing Game: Suppose there is an *n*-sided (label number *1~n*) loader dice. The number of the side facing upwards X follows a distribution: $\{\Pr(X = i) = p_i, \sum_{i=1}^{n} p_i = 1\}$, which is known by a player.

Now let us consider guessing the value of X in two different scenarios:

1) One-step guessing until success—toss the dice and let the player guess. If the player succeeds, game stops. Otherwise, repeat dicing and guessing until the player succeeds. How many trials are expected to guess the value of X ?
2) Multiple-guessing until success—toss the dice and let the player guess. If the player succeeds, game stops. Otherwise, the player is given another chance until he succeeds (no re-dicing). How many trials are expected to guess the value of X ?

For convenience, we denote the expected number of guessing trials under one-step guessing and that under multiple-guessing scenarios by ET_O and ET_M, respectively. Theorem 1 characterizes the relation between the entropy and the number of guessing trials under each scenario.

Theorem 1: Suppose a random variable X distributes over $U = \{u_1, u_2, ...u_n\}$ and $\{\Pr(X = u_i) = p_i, p_1 \ge p_2 ... \ge p_n\}$, then we have $ET_O = 2^{H_\infty(X)}$, $ET_M = \sum_{i=1}^{n} i p_i$, and $\frac{1}{2} + \frac{\lfloor ET_O \rfloor}{2} \le ET_M \le \frac{n+2}{2} - \frac{n}{2ET_O}$.

Proof: The best strategy for one-step guessing is to guess the most likely value every time. Hence we get

$$\begin{aligned} ET_O &= \sum_{i=1}^{\infty} (1 - \max_x \Pr(X = x))^{i-1} \max_x \Pr(X = x) i \\ &= 1 / \max_x \Pr(X = x) \\ &= 2^{-\log \max_x \Pr(X = x)} \\ &= 2^{-\log p_1} \\ &= 2^{H_\infty(X)} \end{aligned}$$

In terms of multiple-guessing, the best strategy is to guess the values of X in decreasing order of probability, so we have

$$ET_M = \sum_{i=1}^{n} i p_i$$

Since $n p_1 \ge \sum_{i=1}^{n} p_i = 1$, we can deduce $n \ge 1/p_1 = ET_O$. If $n = ET_O$, X is uniformly distributed over U and

$$ET_M = \sum_{i=1}^{n} i p_i = \sum_{i=1}^{n} \frac{i}{n} = \frac{1+n}{2} = \frac{1}{2} + \frac{ET_O}{2} = \frac{1}{2} + \frac{\lfloor ET_O \rfloor}{2}$$

If $n > ET_O$, ET_M approximates to the minimum value when $p_2 = p_3 = p_4 ... = p_{\lfloor 1/p_1 \rfloor} = p_1$, $p_{\lfloor 1/p_1 \rfloor + 1} \sim 1 - p_1 \lfloor 1/p_1 \rfloor$ and $p_{1/p_1+2}, p_{1/p_1+3}, ...p_n \sim 0$, and reaches the maximum value when $p_2 = p_3 = \ldots = p_n = (1 - p_1)/(n-1)$. Therefore, we have

$$\begin{aligned} ET_M &= \sum_{i=1}^{n} i p_i \\ &> p_1 \left\lfloor \frac{1}{p_1} \right\rfloor \left(1 + \left\lfloor \frac{1}{p_1} \right\rfloor\right)/2 + \left(1 - p_1 \left\lfloor \frac{1}{p_1} \right\rfloor\right)\left(1 + \left\lfloor \frac{1}{p_1} \right\rfloor\right) \\ &> \left(1 + \left\lfloor \frac{1}{p_1} \right\rfloor\right)/2 \\ &= \frac{1}{2} + \frac{\lfloor ET_O \rfloor}{2} \end{aligned}$$

And

$$ET_M = \sum_{i=1}^{n} i p_i \le p_1 + \frac{(1-p_1)}{n-1}\frac{(n+2)(n-1)}{2}$$
$$= \frac{1}{ET_O} + \frac{(1-1/ET_O)(n+2)}{2}$$
$$= \frac{n+2}{2} - \frac{n}{2ET_O}$$

Therefore, $\frac{1}{2} + \frac{\lfloor ET_O \rfloor}{2} \le ET_M \le \frac{n+2}{2} - \frac{n}{2ET_O}$.

According to Theorem 1, min-entropy $H_\infty(X)$ depends on the maximum probability of a random variable, and reflects ET_O very well. $H(X)$ measures ET_M to some extent [24] as both of them are influenced by the overall distribution (the more uniform the distribution is, the higher they are, and vice versa.). As far as biometric cryptosystems are concerned, helper data Y is stored in databases or servers instead of a biometric template X. Therefore, one-step guessing and multiple-guessing trials about the template are reflected by $\tilde{H}_\infty(X \mid Y)$ and $H(X \mid Y)$, respectively (assume Y is given).

IV. Entropy Analysis of Fingerprint-based Biometric Cryptosystems

It is assumed that for secure biometric cryptosystems, their helper data does not reveal too much information about original biometric templates. Consequently, they must retain high average min-entropy/conditional Shannon entropy. However, it has been found that the template entropy given helper data highly interacts with authentication accuracy. Buhan *et al*. [25] show that there is a relation between the template entropy given the helper data and the error rates of a biometric cryptosystem, which is defined as $H_\infty(X \mid y) \le -\log FAR$. Dodis *et al*. [11] give the upper bound of the average min-entropy $\tilde{H}_\infty(X \mid Y)$ of a secure sketch—when X is uniformly distributed over M, $\tilde{H}_\infty(X \mid Y) \le \log K(M,t)$, where $K(M,t)$ is the largest K for which there exists an (M,K,t) code (An (M,K,t) code is a subset $\{c_1, c_2, ...c_M\}$ of K elements of M that can correct up to t errors. More details can be found in [11]). For a *q-ary* block code C of length n (i.e. $M = Q^n, |Q| = q$), $K(M,t) \le q^n \Big/ \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$, which is called the Hamming bound, and we call C perfect if and only if it attains the Hamming bound. Obviously, the upper bound of entropy-based security is maximized when perfect codes are applied, but in real applications, error-correcting codes cannot always achieve the Hamming bound, e.g., it is impossible to construct a 6-bit perfect code which can correct up to 2-bit errors, so the entropy-based security of real systems may vary depending on different-sized error correcting codes used [26]. According to their work, it can be observed that the upper bound of template entropy given helper data depends on the error tolerance levels allowed during authentication. In particular, if the error tolerance level of a biometric cryptosystem is large, then the corresponding template entropy given helper data will be low as both $K(M,t)$ and FAR^{-1} are small, and vice versa. Therefore, it is unlikely that biometric traits suffering from high intra-class variation, such as fingerprints, can be applied to construct biometric cryptosystems which perform well in both authentication accuracy and entropy-based security. However, this issue has not gained deserved attention from experts specializing in fingerprint recognition. On one hand, they claim that their proposed fingerprint-based bio-cryptosystems are of high recognition accuracy (low FAR and FRR). On the other hand, they recommend these systems by demonstrating good entropy-based security. In this paper, we argue that some assumptions they make when analyzing entropy-based security are not well founded, which have produced confusing analysis results.

A number of fingerprint-based cryptosystems adopt fuzzy vault [10], which is proposed by Juels and Sudan for key encryption purpose. According to Juels and Sudan's analysis, suppose a fuzzy vault is made up of a biometric template $x \in U^s$, an encoding polynomial $p(x) = key_{m-1}x^{m-1} + key_{m-2}x^{m-2} + ... + key_0$, and a vault v of size r, then there are roughly $|U|^{m-s}\binom{r}{s}$ distinct polynomial candidates $p' \neq p$ that are able to produce v, i.e., $\tilde{H}_\infty(P \mid V) \approx \log(|U|^{m-s}\binom{r}{s} + 1)$ (p' is interpolated by exactly s points in v). Admittedly, the entropy-based security of fuzzy vault is high when m approximates s and the number of chaff points is large enough. However, with the increase of m, the error tolerance decreases, while excessive chaff points will consume much computer storage. Therefore, ideal parameters are unachievable in practice.

The polynomial reconstruction in fuzzy vault [10] is a special case of Reed-Solomon list decoding problem, and the best choice for decoding is generally the classical algorithm of Peterson-Berlekamp-Massey [27]-[29]. However, this algorithm takes the majority opinion among all possible solutions, and can tolerate only up to $s-m$ errors, which means the valid polynomial p can be found only when the number of discrepancies in the biometric data $|x-x'|$ is less than $(s-m)/2$. As is widely known, fingerprint data has large intra-class variability—fingerprint traits from the same user captured by different devices or at different time may vary significantly. Therefore, if Reed-Solomon decoding is directly used in fingerprint-based cryptosystems, it will result in many false rejects for genuine users [14].

To overcome this limitation, Nandakumar *et al*. [18] apply CRC (cyclic redundancy check) to fuzzy vault to help identify the correct polynomial from a set of candidates, thus improving the error tolerance up to $2(s-m)$. In their construction, the biometric features in the template are minutia attributes, which are represented as 16-bit binary strings, while s, m and r are set to 24, 9 and 224, respectively, for the best recognition performance. According to their parameters, we can roughly evaluate the number of polynomial candidates p' given a vault

v, which is $(2^{16})^{-15}\binom{224}{24} < \binom{224}{24}/10^{72} \approx 0$. That is to say, the only polynomial that can produce v is p itself. Consequently, we can deduce $\tilde{H}_{\infty}(K \mid V) \approx 0$ and further $\tilde{H}_{\infty}(X \mid V) \approx 0$ because x and k are bijective given v. They apply the same construction to multibiometric templates (fingerprint-iris) based on feature level fusion [15], and claim that the entropy-based security of the new vault could reach up to 49 bits (They assume the genuine and chaff points are uniformly distributed, thus concluding the entropy security corresponds to the security in the brute-force attack scenario). However, we find the assumption and conclusion unjustified. Even if all genuine and chaff points are distributed uniformly, the values of the encoding polynomial at genuine points, $p(x)$, are not uniform. To be more precise, not all the polynomials of degree $m-1$ constructed by interpolating m unique pairs of points from the vault can be the encoding polynomial as the valid polynomial should satisfy the condition that there are exactly s pairs of points in the vault falling on it. In fact, with the parameters they gave ($s=84, m=14, r=884$), we can calculate the actual average min-entropy $\tilde{H}_{\infty}(X \mid V) \approx \log((2^{16})^{-70}\binom{884}{84}+1) \approx 0$. This misleading entropy analysis is also adopted in [26].

Some other fingerprint-based cryptosystems require verification information, such as hash values to assist key recovery, but extra entropy loss is often neglected. Here, we take hash functions for example to help understand how hash values reduce entropy. Given any k-bit hash value $y = hash(x_j), x_j \in X, |X| = n$, the expected number of $x_i \in X, i \neq j$ being able to produce y can be expressed as:

$$N = \sum_{i=1}^{n-1} i\binom{n-1}{i} 2^{-ki}(1-2^{-k})^{n-i-1} = (n-1)/2^k,$$

Therefore, we can deduce $\tilde{H}_{\infty}(X \mid Y) \approx \log(1+(n-1)/2^k)$. When $H_{\infty}(X) = \log n$ (X is uniformly distributed), the entropy loss due to revealing hash values can be computed as: $H_{\infty}(X) - \tilde{H}_{\infty}(X \mid Y) \approx \log\left(\frac{2^k n}{2^k + n - 1}\right)$. For a fixed n, the entropy loss rises with the increase of the length of hash values, and the corresponding average min-entropy declines. Liu *et al*. [30] propose a fingerprint-based key-binding biometric cryptosystem which consists of three levels of secure sketch. The first two: wrap-round and Pinsketch, which deal with random errors and burst errors respectively, are essentially a type of soft two-level construction while the third level is a Shamir's secret sharing scheme. The output of the three levels of secure sketch, denoted by $\{\omega_i\}_{i=1}^N, \{\gamma_i\}_{i=1}^N, \{A_i\}_{i=1}^N, (A_0, SC_0)$, are stored explicitly for key recovery. Nevertheless, since Shamir's secret sharing scheme itself cannot identify the validity of recovered local structures, besides the three levels of sketch data, a collection of hash values of minutia structures, $\{h(SC_i)\}_{i=1}^N$, are required to be stored extra for verification purposes. For the sake of convenience, we denote the sum of the sketch data and the collection of hash values by $Y = \left\{\{\omega_i\}_{i=1}^N, \{\gamma_i\}_{i=1}^N, \{A_i\}_{i=1}^N, (A_0, SC_0), \{h(SC_i)\}_{i=1}^N\right\}$. Although the authors have shown the security of the system in two respects: Pinsketch security and hash security, the rigorous entropy-based security analysis of the overall system is not given. Actually, as they adopt SHA256 to encrypt each minutia structure, which is represented by a 108-bit binary string SC_i ($n=5$), based on the previous deduction, the remaining entropy of SC_i due to revealing $h(SC_i)$ can be computed as: $\tilde{H}_{\infty}(SC_i \mid h(SC_i)) \approx \log(1+(2^{108}-1)/2^{256}) \approx 0$. Further, we can deduce $\tilde{H}_{\infty}(NS_i \mid h(SC_i), \omega_i) \approx \tilde{H}_{\infty}(NS_i \mid SC_i, \omega_i) = 0$ since NS_i (raw biometric feature vector) is uniquely determined by SC_i and ω_i. The result can be extended to the entire system as: $\tilde{H}_{\infty}(\{NS_i\}_{i=1}^N \mid Y) \leq \tilde{H}_{\infty}(\{NS_i\}_{i=1}^N \mid \{h(SC_i)\}_{i=1}^N, \{\omega_i\}_{i=1}^N) \approx 0$ (Readers can look into [30] for details about the construction and the meanings of the symbols). Yang *et al*. [19] propose an alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures, in which the authors apply a two-level secure sketch (Pinsketch plus fuzzy vault) to tolerate errors as well as protect fingerprint templates. They claim that the entropy of their construction can reach 112 bits even if the Pinsketch is compromised by attackers. Nevertheless, similar to Liu *et al*.'s, their scheme also requires to store hash values of local structures for key recovery, which should be considered as a part of the helper data that may leak information about the templates. If we assume that SHA256 is adopted, their scheme has weak entropy-based security as well, i.e., $\tilde{H}_{\infty}(X_i \mid Y_i) \approx \log(1+(2^{8*14}-1)/2^{256}) \approx 0$, where X_i and Y_i are the binary representations of the *ith* local structure and its hash value, respectively. Admittedly, shorter hash values may decrease the entropy loss, but it meanwhile results in the degradation of authentication accuracy as more collisions occur.

V. A New Security Analysis Framework For Biometric Cryptosystems

Considering the low entropy (approximate to 0) of the above biometric cryptosystems, can we conclude that they are all insecure? The answer is no. As a matter of fact, entropy measures only reflect the information-theoretic security of a system, which assumes the attacker has unlimited computing power. Particularly, in biometric cryptosystems, entropy measures the guessing trials under the condition that given helper data, the possible corresponding values of biometric templates and their probabilities are known, ignoring the difficulty of deriving these values from the helper data. Admittedly, entropy is significant in measuring the amount of information and uncertainty. Besides biometric cryptosystems, entropy measures are also widely employed in many other security applications, especially network traffic analysis [31][32]. However, all attackers in practice are computationally limited. In this case, to measure the security of biometric cryptosystems more comprehensively, we should also consider the computational hardness of the derivation of biometric templates from helper data (referred to as computational security) besides related entropy. The current state of

knowledge has implied the decoding of Reed-Solomon codes, also known as the polynomial reconstruction, as a cryptographically hard problem when $s < \sqrt{rm}$ [33], [34]. Also, a good cryptographic hash function is always pre-image resistant, which means it is computationally difficult to get original messages given hash values. Therefore, even though the biometric cryptosystems listed above have no information-theoretic security, they are still computational secure.

There are some works in the literature dealing with computational security of bio-cryptosystems [14], [18]. However, the analysis is merely conducted on specific systems with known parameters rather than on general constructions. Also, the previous work considers either entropy-based security or computational security, while there are some cases in which entropy-based and computational security coexist. For instance, in some cryptographic scenarios that involve highly classified information, users concern more about FAR than FRR. That is, the systems target minimizing FAR to ensure that only valid users have access to the information. If a fingerprint-based fuzzy vault is applied, then it is supposed to only accept fingerprint queries that have high similarity to templates, which means a high value will be assigned to the degree of the polynomial m. As a result, the entropy will increase. To be more precise, if $|U| = 2^{16}$ and s, m, r are assigned 24, 20 and 224, respectively, the entropy will become $\log((2^{16})^{20-24}\binom{224}{24}+1) \approx 42.5$. Under this circumstance, the fuzzy vault construction has both entropy-based security and computational security as it is still time-consuming to search for 20-degree polynomials interpolated by 24 points in the vault. Considering the lack of a general security framework for bio-cryptosystems and the inability of conventional security analysis methodology in handling the above scenario, in this section, we propose a novel bio-cryptosystem-oriented security analysis framework, which jointly considers information-theoretic and computational security.

Without loss of generality, we consider a generalized biometric cryptosystem, which takes a biometric template $x \in X$ and generates helper data by $y = F(x)$, where F is an encoding algorithm. Given y, the decoding algorithm that finds out a value $x' \in X$ such that $F(x') = y$ is denoted by $F'(y)$ ($F(F'(y)) = y$) and the average number of elementary operations of F' is represented by $N(F'(y))$. The security analysis is given below under one-step guessing scenario and multiple-guessing scenario, respectively (For reasons of simplicity, we assume $H_\infty(X \mid y) = H(X \mid y)$, which means X is uniformly distributed over all values that may produce y).

Apparently, if x' is public to the attacker ($N(F'(y)) = 0$), under one-step guessing scenario, he can hold the value to browse a collection of the same systems and will succeed by average $2^{H_\infty(X|y)}$ guessing trials, and that is what min-entropy measures. However, in practical applications, the correlation between x' and y is not always transparent, which means the attacker has to perform decoding first to obtain x' from y and then conducts guess trials. If each guess trial is considered to be an elementary operation, then we can expect that the average number of elementary operations for success guess is $N(F'(y)) + 2^{H_\infty(X|y)}$. By replacing guessing trials with elementary operations for security measurement, we rewrite the security metric from $H_\infty(X \mid y) = \log 2^{H_\infty(X|y)}$ to $S_O(X \mid y) = \log(N(F'(y)) + 2^{H_\infty(X|y)})$. Correspondingly, we give the new security metric of the whole system under one-step guessing as follows.

Definition 1. Under one-step guessing scenario, the security of a biometric cryptosystem considering computational security can be measured by:

$$S_O(X \mid Y) = -\log(E_{y \leftarrow Y} 2^{-S_O(X|y)}) = -\log(E_{y \leftarrow Y} 2^{-\log(N(F'(y)) + 2^{H_\infty(X|y)})})$$

1) *If for any* $y_i, y_j \in Y, i \neq j$, $H_\infty(X \mid y_i) = H_\infty(X \mid y_j)$ and $N(F'(y_i)) = N(F'(y_j)) = N(F')$,
$$S_O(X \mid Y) = \log(N(F') + 2^{\tilde{H}_\infty(X|Y)}).$$
2) *If* $N(F'(y)) = 0$ *for any* $y \in Y$,
$$S_O(X \mid Y) = \tilde{H}_\infty(X \mid Y).$$
3) *If* $\tilde{H}_\infty(X \mid Y) = 0$,
$$S_O(X \mid Y) = -\log E_{y \leftarrow Y}(N(F'(y)) + 1)^{-1}.$$

In the multiple-guessing scenario, the case becomes more complicated as the attacker can perform multiple guessing trials that are inter-dependent. In particular, given $y = F(x)$, the attacker performs the decoding algorithm F' to get a value $x_1 \in X$ such that $F(x_1) = y$. If $x_1 = x$, the attacker succeeds and stops decoding, or he continues decoding to obtain the next value of X (x_2) that may produce y until he succeeds. If we assume the attacker succeeds at the *ith* guessing trial and denote the average number of elementary operations he conducts for decoding so far by $N(F'(i, y))$, then the average number of elementary operations of recovering X given y is $\sum_{i=1}^{n_y}(\Pr(x_i \mid y)(N(F'(i, y)) + i))$, where n_y represents the number of the values of X being able to generate y, and $\sum_{i=1}^{n_y}\Pr(x_i \mid y)i$ denotes the expected number of guessing trials. Since X is uniformly distributed over these n_y values, we can deduce $\Pr(x_i \mid y) = 1/n_y = 2^{-H(X|y)}$ and then rewrite the expression into $\sum_{i=1}^{2^{H(X|y)}}(2^{-H(X|y)}(N(F'(i, y)) + i))$, where $N(F'(i, y))$ also equals the average number of elementary operations the attacker needs to carry out to find i values from X that can produce y. Accordingly, the new security metric of the whole construction under multiple-guessing can be given as follows.

Definition 2. Under multiple-guessing scenario, the security of a biometric cryptosystem considering computational security can be measured by:

$$S_M(X \mid Y) = \log E_{y \leftarrow Y} \sum_{i=1}^{2^{H(X|y)}} 2^{-H(X|y)} (N(F'(i,y)) + i)$$

$$= \log E_{y \leftarrow Y} \left(2^{-H(X|y)} \sum_{i=1}^{2^{H(X|y)}} N(F'(i,y)) + (1 + 2^{H(X|y)})/2 \right)$$

1) *If* $N(F'(i,y)) = 0$ *for any* $y \in Y$,

$$S_M(X \mid Y) = \log E_{y \leftarrow Y} \sum_{i=1}^{2^{H(X|y)}} 2^{-H(X|y)} i = \log E_{y \leftarrow Y} ET_{M,y}.$$

Considering the similarity between $ET_{M,y}$ *and conditional Shannon entropy* $H(X \mid y)$ *(see section III),* $S_M(X \mid Y)$ *can be measured by* $H(X \mid Y)$ *to some extent in this case.*

2) *If* $H(X \mid Y) = 0$, $S_M(X \mid Y) = \log E_{y \leftarrow Y}(N(F'(1,y)) + 1)$

$= \log E_{y \leftarrow Y}(N(F'(y)) + 1)$.

From the new security analysis framework, it can be observed that the security of biometric cryptosystems is not only determined by the related entropy, but also influenced by the computational hardness of the decoding algorithm of each construction. In consequence, it is inappropriate to conclude that a fuzzy commitment of high entropy is more secure than a fuzzy vault of low entropy considering the decoding of the former is a simple XOR operator while that of the latter involves polynomial reconstruction, a much more complicated problem. As entropy (information-theoretic security) depends on the error tolerance of applied biometric, which is biologically determined and sometimes difficult to change artificially even by adopting different authentication algorithms [18], [19], [30], [35], to further improve the security of biometric cryptosystems, efficient, hard-inverse encoding algorithms can be employed when computational cost and time for encoding are relatively negligible.

VI. Accuracy Analysis Of MBC

Compared with single biometric cryptosystems, multibiometric cryptosystems can offer higher authentication accuracy and security, as well as larger population coverage. Therefore, they have been frequently studied in recent years. Based on previous work, Fu *et al*. [13] formulate the formal definition of MBC at two fusion levels: feature level (MBCF) and decision level (MBCD). To be more precise, the latter can be further divided into three sub-models: *MN*-split model (n out of k fusion rule), non-split model (OR rule) and package model (And rule). Fusion at feature level is a map $F_B : U^{b_1} \times U^{b_2} \times ... \times U^{b_m} \rightarrow U^b$, which transforms features from different biometric sources into the same universe and constructs a united template $x_T \in U^b$. Then x_T will be bound with a cryptographic key k and generate helper data. During the authentication process, if a query $x_Q \in U^b$ satisfies $dis(x_T, x_Q) \le t$, both x_T and k can be recovered. In a MBCD, a cryptographic key is bound with a biometric template set $\{x_{T,i}\}_{i=1}^m, x_{T,i} \in U^{b_i}$ consisting of templates from different biometric sources, and the recovery will succeed if at least n biometrics from a query set $\{x_{Q,i}\}_{i=1}^m, x_{Q,i} \in U^{b_i}$ and their counterparts in the template set satisfy $dis_i(x_{T,i}, x_{Q,i}) \le t_i$, where t_i is the error tolerance of the *ith* biometric.

Fu *et al*. [13] analyze both MBCF and MBCD theoretically in terms of security, privacy and accuracy. Although they conclude that both MBCF and MBCD (*MN*-split model) have lower FAR and FRR than SBC, we find there are theoretical flaws in their analysis.

Now let us consider the accuracy of MBCF. If we denote the query from the imposter and the legitimate user by x_{IM} and x_{LE}, respectively, the FAR and FRR of a MBCF can be expressed as:

$$FAR_{MBCF} = \Pr(dis(x_T, x_{IM}) \le t)$$

$$FRR_{MBCF} = \Pr(dis(x_T, x_{LE}) > t),$$

The accuracy improvement over the *ith* SBC can be computed by:

$$\begin{aligned} FAR_{reduction} &= FAR_{SBC_i} - FAR_{MBCF} \\ &= \Pr(dis(x_{T,i}, x_{IM,i}) \le t_i) - \Pr(dis(x_T, x_{IM}) \le t) \\ &= \Pr(dis(x_{T,i}, x_{IM,i}) \le t_i \ \&\ dis(x_T, x_{IM}) > t) \\ &\quad - \Pr(dis(x_{T,i}, x_{IM,i}) > t_i \ \&\ dis(x_T, x_{IM}) \le t) \\ FRR_{reduction} &= FRR_{SBC_i} - FRR_{MBCF} \\ &= \Pr(dis(x_{T,i}, x_{LE,i}) > t_i) - \Pr(dis(x_T, x_{LE}) > t) \\ &= \Pr(dis(x_{T,i}, x_{LE,i}) > t_i \ \&\ dis(x_T, x_{LE}) \le t) \\ &\quad - \Pr(dis(x_{T,i}, x_{LE,i}) \le t_i \ \&\ dis(x_T, x_{LE}) > t) \end{aligned}$$

According to the above equations, it is not theoretically guaranteed that the first probability on the right-hand exceeds the second one. Whether or not MBCF have higher authentication accuracy than SBC depends on the selected biometric sources, fusion algorithms, the error tolerance t, etc. As a matter of fact, inappropriate selection and concatenation of different biometric traits can even degrade the accuracy of the system.

In the case of MBCD, Fu *et al*. [13] express the FAR and FRR of *MN*-split model as:

$$FAR_{MBCD} = \prod_{i=1}^{n} FAR_{SBC_i}$$

$$FRR_{MBCD} = \prod_{i=1}^{m-n+1} FRR_{SBC_i},$$

and therefore they conclude that $FAR_{MBCD} \le FAR_{SBC_i}$ and $FRR_{MBCD} \le FRR_{SBC_i}, i = 1...n$. However, their accuracy analysis does not consider all the situations in which an imposter is accepted by the system and a legitimate user is rejected. We reanalyze the accuracy of *MN*-split model by Theorem 2.

Theorem 2. In a general construction of MN-split model, for m *biometrics* $X = \{X_i\}_{i=1}^m$, *the cryptographic key can be decrypted if at least* n *sub-keys are successfully decrypted by their corresponding biometrics. We have*

$$FAR_{MBCD} = \sum_{i=n}^{m} \sum_{j=1}^{\binom{m}{i}} \prod_{k \in C(m,i,j)} FAR_{SBC_k} \prod_{l \notin C(m,i,j)} (1 - FAR_{SBC_l})$$

$$FRR_{MBCD} = \sum_{i=m-n+1}^{m} \sum_{j=1}^{\binom{m}{i}} \prod_{k \in C(m,i,j)} FRR_{SBC_k} \prod_{l \notin C(m,i,j)} (1 - FRR_{SBC_l}),$$

where $C(m,i,j)$ denotes the jth combination of selecting i biometrics from m. In particular, if each biometric has the same FAR and FRR, then we can get

$$FAR_{MBCD} = \sum_{i=n}^{m} \binom{m}{i} FAR_{SBC}^{i} (1 - FAR_{SBC})^{m-i}$$

$$FRR_{MBCD} = \sum_{i=m-n+1}^{m} \binom{m}{i} FRR_{SBC}^{i} (1 - FRR_{SBC})^{m-i}$$

Proof: If an imposter attempts to recover the cryptographic key, he/she must successfully decrypt at least n sub-keys encrypted by the corresponding biometrics. Let $FAR_{MBCD,i}$ be the probability that the imposter gets the key by decrypting i sub-keys. Then we can calculate the FAR of *MN*-split model as follows.

$$\begin{aligned} FAR_{MBCD} &= FAR_{MBCD,n} + FAR_{MBCD,n+1} + ... + FAR_{MBCD,m} \\ &= \sum_{i=n}^{m} FAR_{MBCD,i} \end{aligned}$$

Since these i sub-keys can be any i ones from m, $FAR_{MBCD,i}$ can be expressed as

$$FAR_{MBCD,i} = \sum_{j=1}^{\binom{m}{i}} \prod_{k \in C(m,i,j)} FAR_{SBC_k} \prod_{l \notin C(m,i,j)} (1 - FAR_{SBC_l}),$$

and therefore

$$FAR_{MBCD} = \sum_{i=n}^{m} \sum_{j=1}^{\binom{m}{i}} \prod_{k \in C(m,i,j)} FAR_{SBC_k} \prod_{l \notin C(m,i,j)} (1 - FAR_{SBC_l}).$$

Similarly, if a legitimate user fails to decrypt the key, then it means the biometrics he/she presents can only decrypt at most $n-1$ sub-keys. In other words, he/she fails to decrypt at least $m-n+1$ sub-keys. Then the FRR of *MN*-split model can be computed in the same manner.

$$\begin{aligned} FRR_{MBCD} &= FRR_{MBCD,m-n+1} + FRR_{MBCD,m-n+2} + ... + FRR_{MBCD,m} \\ &= \sum_{i=m-n+1}^{m} FRR_{MBCD,i} \\ &= \sum_{i=m-n+1}^{m} \sum_{j=1}^{\binom{m}{i}} \prod_{k \in C(m,i,j)} FRR_{SBC_k} \prod_{l \notin C(m,i,j)} (1 - FRR_{SBC_l}), \end{aligned}$$

where $FRR_{MBCD,i}$ is the probability that the legitimate user fails to decrypt i sub-keys.

If we set $n=1$, then *MN*-split model becomes non-split model, and the FAR and FRR can be calculated as:

$$\begin{aligned} FAR_{MBCD} &= \sum_{i=1}^{m} \sum_{j=1}^{\binom{m}{i}} \prod_{k \in C(m,i,j)} FAR_{SBC_k} \prod_{l \notin C(m,i,j)} (1 - FAR_{SBC_l}) \\ &= 1 - \prod_{i=1}^{m} (1 - FAR_{SBC_i}) \\ &\geq FAR_{SBC_i} \end{aligned}$$

$$FRR_{MBCD} = \prod_{i=1}^{m} FRR_{SBC_i} \leq FRR_{SBC_i}$$

Similarly, the FAR and FRR of package model can be computed by setting $n = m$.

$$FAR_{MBCD} = \prod_{i=1}^{m} FAR_{SBC_i} \leq FAR_{SBC_i}$$

$$\begin{aligned} FRR_{MBCD} &= \sum_{i=1}^{m} \sum_{j=1}^{\binom{m}{i}} \prod_{k \in C(m,i,j)} FRR_{SBC_k} \prod_{l \notin C(m,i,j)} (1 - FRR_{SBC_l}) \\ &= 1 - \prod_{i=1}^{m} (1 - FRR_{SBC_i}) \\ &\geq FRR_{SBC_i} \end{aligned}$$

According to Theorem 2, we cannot conclude that MBCD (*MN*-split model) always have lower FAR and FRR than SBC. A simple case in point is $X = \{X_i\}_{i=1}^{3}$, in which $FAR_{SBC_1} = FRR_{SBC_1} = 0.4$, $FAR_{SBC_2} = FRR_{SBC_2} = 0.2$ and $FAR_{SBC_3} = FRR_{SBC_3} = 0.1$. Obviously, if n is set to 1 or 3, the *MN*-split model becomes non-split model or package model. Accordingly, $FAR_{MBCD}(\mathrm{n}=1) = FRR_{MBCD}(\mathrm{n}=3) = 0.568$ and $FAR_{MBCD}(\mathrm{n}=3) = FRR_{MBCD}(\mathrm{n}=1) = 0.008$. When n is set to 2, $FAR_{MBCD}(\mathrm{n}=2) = FRR_{MBCD}(\mathrm{n}=2) = 0.124$. No matter which value n takes, the corresponding MBCD does not provide lower FAR and FRR simultaneously than the 3rd SBC. In general, there are several factors that contribute to the accuracy of a MBCD, including the accuracy (FAR and FRR) of each SBC, the number of total biometrics m, and the threshold n. Theorem 3 shows a special case in which the resultant MBCD has lower FAR and FRR than the SBC composing it.

Theorem 3. (Major-vote-based [36], [37] MN-split model) For $m = 2n-1 \geq 3$ biometrics $X = \{X_i\}_{i=1}^{m}$, the cryptographic key can be decrypted if at least n sub-keys are successfully decrypted by corresponding biometrics. If

$$FAR_{SBC_1} = FAR_{SBC_2} ... = FAR_{SBC_m} = FAR_{SBC} < 1/2$$

$$FRR_{SBC_1} = FRR_{SBC_2} ... = FRR_{SBC_m} = FRR_{SBC} < 1/2,$$

then we have $FAR_{MBCD} < FAR_{SBC}$ and $FRR_{MBCD} < FRR_{SBC}$.

Proof: Let us consider the probability that an imposter fails to decrypt the key GRR_{MBCD} (Genuine Reject Rate), which can be expressed as

$$\begin{aligned} GRR_{MBCD} &= \sum_{i=m-n+1}^{m} \binom{m}{i} GRR_{SBC}^{i} (1 - GRR_{SBC})^{m-i} \\ &= \sum_{i=n}^{2n+1} \binom{2n+1}{i} GRR_{SBC}^{i} (1 - GRR_{SBC})^{2n+1-i} \end{aligned}$$

As $GRR_{SBC} = 1 - FAR_{SBC} > 1/2$, according to condorcet's jury theorem [38], [39], we can get $GRR_{MBCD} > GRR_{SBC}$ and therefore $FAR_{MBCD} < FAR_{SBC}$.

Similarly, the probability of a legitimate user successfully recovering the key (Genuine Accept Rate) is

$$GAR_{MBCD} = \sum_{i=n}^{m} \binom{m}{i} GAR_{SBC}^{i} (1 - GAR_{SBC})^{m-i}$$

Fig. 3. Delaunay triangulation of a fingerprint image.

$$= \sum_{i=n}^{2n+1} \binom{2n+1}{i} GAR_{SBC}^{i} (1 - GAR_{SBC})^{2n+1-i}$$

As $GAR_{SBC} = 1 - FRR_{SBC} > 1/2$, we can conclude that $GAR_{MBCD} > GAR_{SBC}$ and therefore $FRR_{MBCD} < FRR_{SBC}$.

VII. FINGERPRINT-BASED MBCD (*MN*-SPLIT MODEL)

Compared with MBCD, MBCF are stronger in terms of protecting single biometric templates, thus being more studied over the past few years [1], [14]-[16]. However, fusion at feature level also leads to some issues in practical applications, such as incompatibility of features from different biometric traits, entropy loss for fusion and the curse-of-dimensionality problem. In contrast, MBCD avoid the difficulty of biometric feature unification and can retain the advantages of each biometric and its corresponding cryptosystem construction. Moreover, MBCD are more extensible and can better meet the requirements of some scenarios [40] and applications. While Fu *et al*. [13] theoretically analyze the template privacy, key security and accuracy of MBCD, they do not propose a system implementation.

In the section, we present a practical MBCD construction based on *MN-split* model, which uses fingerprints from multiple fingers to secure cryptographic keys. A registration-free, Delaunay triangle-based matching algorithm proposed by Yang *et al*. [41] is adopted, which avoids authentication errors caused by inaccurate registration.

A. Delaunay Triangulation [41]

Triangulation is a process of dividing a region of space into multiple smaller triangular regions. Suppose a fingerprint image consists of n minutiae, which are denoted by $M = \{m_i\}_{i=1}^{n}$. The process to establish the Delaunay triangulation of M is composed of two steps, which are illustrated with Figure 3. Firstly, a Voronoi diagram of the minutiae set M is constructed, which partitions the whole image into n regions such that all the points in the *ith* region are closer to m_i than to any other minutia. Secondly, given the Voronoi diagram, we connect the minutiae in neighboring Voronoi regions and form the Delaunay triangulation net.

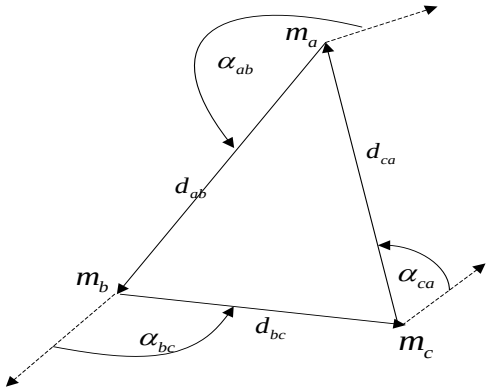

Fig. 4. A triangle and corresponding local features.

B. Features Extraction

We denote the *ith* triangle of a Delaunay triangulation net by $T_i = \{m_a, m_b, m_c\}, m_k|_{k\in\{a,b,c\}} = \{x_k, y_k, \theta_k, t_k\}$, where minutiae m_a, m_b, m_c are vertexes of the triangle, (x_k, y_k) is the coordinates of the minutia m_k , θ_k is the orientation of its associated edge, and $t_k \in \{0,1\}$ is the minutia type (0 corresponds to ridge ending while 1 corresponds to ridge bifurcation). Unlike [41], we do not use minutia type in our scheme due to its instability, so the feature vector of T_i is expressed by

$$FV_i = \{d_{ab}, d_{bc}, d_{ca}, \alpha_{ab}, \alpha_{bc}, \alpha_{ca}\}$$

$$d_{ab} = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$$

$$d_{bc} = \sqrt{(x_b - x_c)^2 + (y_b - y_c)^2}$$

$$d_{ca} = \sqrt{(x_c - x_a)^2 + (y_c - y_a)^2}$$

$$\alpha_{ab} = \tan^{-1}\left(\frac{y_a - y_b}{x_a - x_b}\right) - \theta_a$$

$$\alpha_{bc} = \tan^{-1}\left(\frac{y_b - y_c}{x_b - x_c}\right) - \theta_b$$

$$\alpha_{ca} = \tan^{-1}\left(\frac{y_c - y_a}{x_c - x_a}\right) - \theta_c$$

The triangle T_i and its features are demonstrated in Figure 4.

Suppose there are s triangles in the Delaunay triangulation net, then the fingerprint image can be expressed by a set of these s local feature vectors as $SV = \{FV_i\}_{i=1}^{s}$. In our construction, to reduce matching processing time, we choose the first 80 Delaunay triangles ($s = 80$) from the whole set in

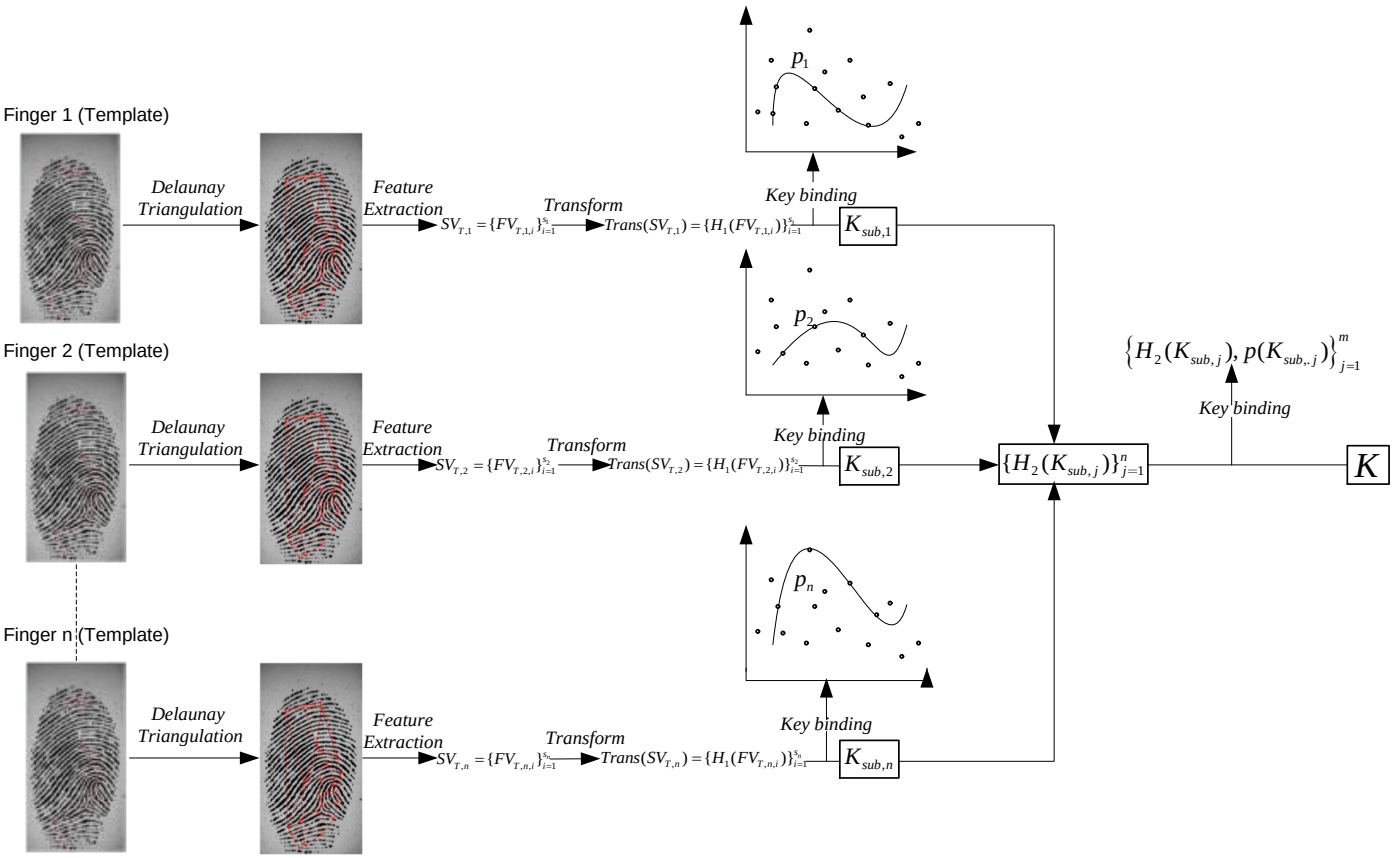

Fig. 5. The encryption procedure

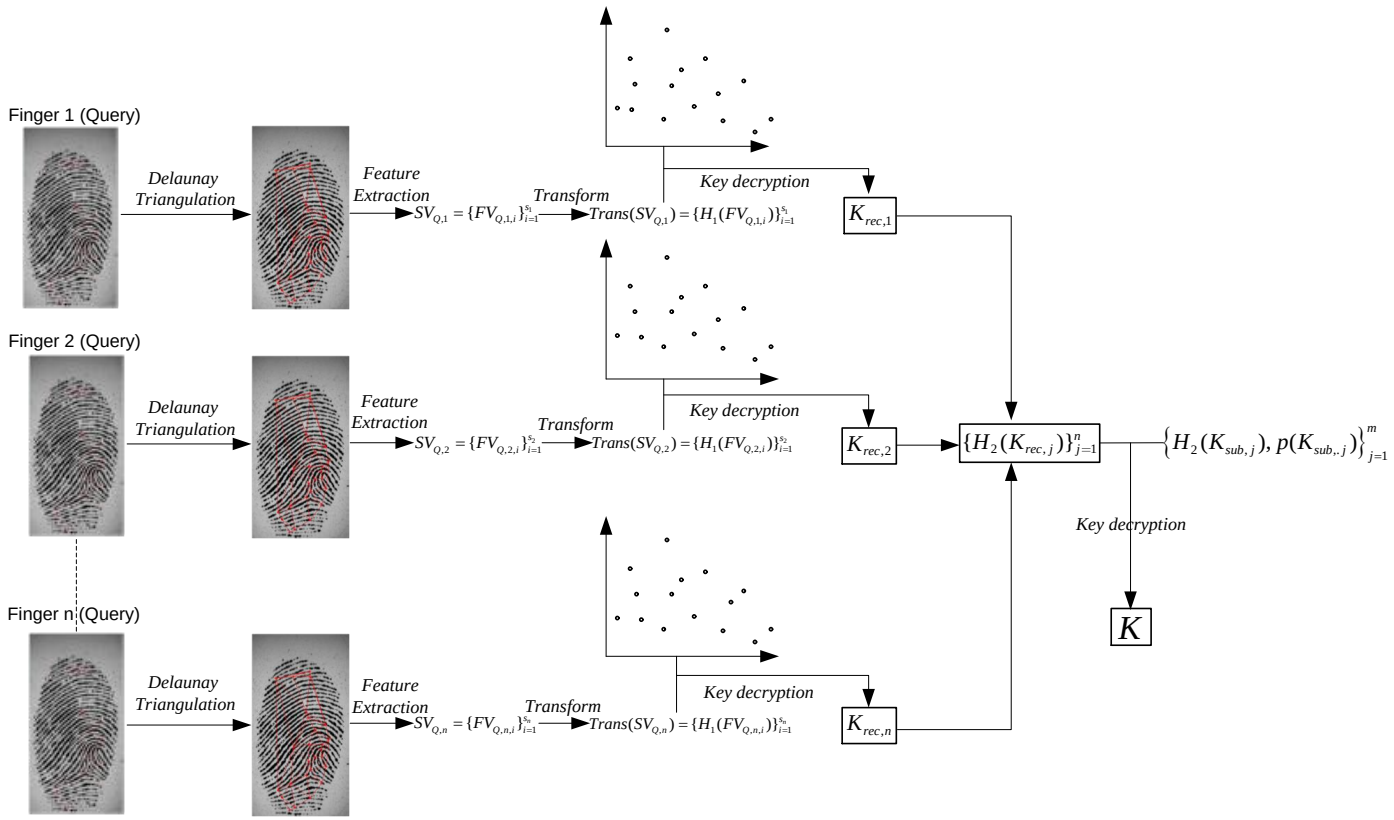

Fig. 6. The decryption procedure

ascending order of the distance between them and the singular point or the center of the fingerprint image. Both d and α are quantized and represented as bit strings of length 4, so FV_i can be represented by a 24-bit binary string.

C. Encryption

We use a two-level secure sketch to achieve error tolerance in our construction. The encryption procedure is shown in Figure 5 and the detailed steps are given below:

1) The first level encryption

Suppose the multibiometric template in our MBCD consists of templates from $m, 2 \le m \le 10$ different fingers, given the template of the *jth* finger $SV_{T,j} = \{FV_{T,j,i}\}_{i=1}^{s}$, we apply a hash function $H_1(.)$ to each $FV_{T,j,i}$ and form a transformed template $Trans(SV_{T,j}) = \{H_1(FV_{T,j,i})\}_{i=1}^{s}$. If the length of $H_1(.)$ is l, we can use fuzzy vault $V_{sub,j}$ to bind the transformed template $Trans(SV_{T,j})$ with a sub-key $K_{sub,j}$ of length ld_j bits. As the sub-keys will be used as the input of the second level secure sketch, we set $d_j = d$ for all fingers in our experiment to ensure all the sub-keys are of the same length. In addition, we compute the hash value of $K_{sub,j}$ ($H_2(K_{sub,j})$) for sub-key verification.

2) The second level encryption

The second level encryption is essentially the Shamir's secret sharing scheme. Given a cryptographic key K provided by the user, if we expect it to be decrypted successfully when at least n sub-keys are decrypted, then we can divide K into n segments $k_0, k_1, ...k_{n-1}$ and encode them into a polynomial p, i.e. $p(x) = k_{n-1}x^{n-1} + k_{n-2}x^{n-2} ... + k_0$. p x is evaluated at each sub-key $K_{sub,j}$ to generate a genuine set $\{K_{sub,j}, p(K_{sub,.j})\}_{j=1}^{m}$. In our construction, however, we store the hash values instead of the sub-keys themselves. Thus the output of the entire system which needs to be stored explicitly (the helper data) consists of $\{H_2(K_{sub,j}), p(K_{sub,.j})\}_{j=1}^{m}$ and $\{V_{sub,j}\}_{j=1}^{m}$.

D. Decryption

The decryption procedure is shown in Figure 6 and the detailed steps are explained in the following:

1) The first level decryption

Given the template of the *jth* finger from the query, we apply Delaunay Triangulation, feature extraction and hash function H_1 in a row and get $Tran(SV_{Q,j}) = \{H_1(FV_{Q,j,i})\}_{i=1}^{s}$. Then the sub-key is recovered (polynomial interpolation) by pairing $Tran(SV_{Q,j})$ and the elements in $V_{sub,j}$. If the recovered sub-key $K_{\text{rec},j}$ satisfies $H_2(K_{\text{rec},j}) = H_2(K_{sub,j})$, $(K_{rec,j}, p(K_{sub,j}))$ will be added into the unlocking set. Apparently, the sub-key $K_{sub,j}$ can always be decrypted from $V_{sub,j}$ as long as $SV_{T,j}$ and $SV_{Q,j}$ have at least d common elements.

2) The second level decryption

If at least n sub-keys are decrypted from the first level secure sketch—the size of the unlocking set is no less than n, the cryptographic key K can be decrypted.

E. Experimental Results

Our construction uses fingerprints from multiple fingers of an individual to encrypt the cryptographic key. Unfortunately, we cannot find any open, standard database to meet our requirements. Therefore, we collected fingerprint images from 150 cooperative subjects with balanced demographic characteristics including age, gender and nationality, using an optical sensor (CROSSMATCH Verifier 300 LC2.0) in our lab [42]. The subjects mainly consisted of students and staff in three Australian educational institutions: UNSW@ADFA, Deakin University and La Trobe University. The age distribution was as follows: (a) between the ages of 18 and 25: 45%, (b) between the ages of 25 and 35; 45%, and (c) older than 35 years: 10%. The gender distribution was almost balanced with only a 10% gap between females and males. In terms of the nationality distribution, 45% subjects are Asians, 45% are Indians or Bangladeshis, and the remaining 10% are Caucasians. Each subject was asked to provide images of ten fingers and we captured the image of each finger four times under different distortion. This database has been released publicly within a 3D fingerprint database package [43]. Note that most existing multimodal databases are combining biometric features from different persons. Such simulation databases have ignored the mutual dependency of different biometric features from the same person, which can produce misleading performance results [44].

The standard FVC protocol is applied in our experiment. In particular, each image from a finger of a subject is compared with other 3 images from the same finger of the subject to calculate FRR while the first image from a finger of a subject is compared with the first image from the corresponding finger of other subjects to calculate FAR. To avoid repeated comparison, if image 1 as the template has been already compared with image 2, then when image 2 is chosen as the template, it will not be compared with image 1 again. Since there are 4 images for each finger from 150 subjects, the total numbers of genuine test and imposter test are $((4\times3)/2)\times150 = 900$ and $(149+1)\times149/2 = 11175$, respectively.

Firstly, we test the matching accuracy of each finger using the Delaunay triangle-based algorithm. The corresponding FRR and FAR when $d = 9$ are shown in Table I, from which we can learn that single fingerprint cannot offer desirable performance in terms of identifying genuine users—the right thumb has the best FRR, which is still up to 7.44%. Then we use Theorem 2 in Section VI to analyze the accuracy of MBCD in two scenarios ($m = 4$ and $m = 10$). The theoretical results in Table II show that our MBCD can significantly lower FRR without compromising much on FAR when n is properly chosen, e.g., $n = 2$ in both scenarios. To further justify our theorem, we finally conduct experiments for these two scenarios. In the scenario $m = 4$, two index and two fingers are employed as the multibiometric template, the FRR/FAR of the

TABLE I
MATCHING PERFORMANCE ON EACH FINGER

Finger No	FRR	FAR
1 (right thumb)	0.0744	0.0001
2 (right index finger)	0.0744	0.0003
3 (right middle finger)	0.1244	0.0001
4 (right ring finger)	0.2244	0.0000
5 (right little finger)	0.3467	0.0000
6 (left thumb)	0.0900	0.0017
7 (left index finger)	0.1422	0.0002
8 (left middle finger)	0.1367	0.0001
9 (left ring finger)	0.2578	0.0002
10 (left little finger)	0.4044	0.0000

TABLE II
MBCD PERFORMANCE THEORETICAL ANALYSIS

MBCD	m=4 (FRR/FAR)	m=10(FRR/FAR)
n=1	0.0002/0.0007	0.0000/0.0027
n=2	0.0059/0.0000	0.0000/0.0000
n=3	0.0718/0.0000	0.0000/0.0000
n=4	0.3998/0.0000	0.0003/0.0000
n=5	NA	0.0031/0.0000
n=6	NA	0.0213/0.0000
n=7	NA	0.0971/0.0000
n=8	NA	0.3021/0.0000
n=9	NA	0.6429/0/0000
n=10	NA	0.9576/0.0000

proposed system when $n=2$ is 2.67%/0%, while the counterpart in the other scenario is 0.67%/0%. The ROC curves of the SBC (single fingerprint) and MBCD under both scenarios are shown and compared in Figure 7. Overall, the experimental results conform to the theoretical results in spite of the small FRR/FAR gap arising from the non-uniformity of experimental data.

F. *Security Analysis*

We analyze the security of our construction in two respects: single fingerprint protection and cryptographic key protection, under the condition that the helper data are compromised by the attacker. Similar to other fingerprint-based cryptosystems, our construction has no information-theoretic security either for low FRR. In particular, if we set $d=9$ and $|V_{sub,j}|=880$ (the number of chaff points is 10 times that of genuine points), the average min-entropy of the first level secure sketch (fuzzy vault) is $\tilde{H}_{\infty}(SV_{T,j}\,|\,V_{sub,j}) \approx \log((2^{24})^{9-80}\binom{880}{80}+1) \approx 0$. Therefore, the strength of our construction in terms of single fingerprint protection will degrade into the computational complexity $\log(N(F'(V_{sub,j}))+1)$. Given a sub-vault $V_{sub,j}$, the computational complexity to decrypt the fuzzy vault by brute force attack [18] can be computed as: $\binom{880}{9}\Big/\binom{80}{9} \approx 3.6e{+}09$. In addition, even if the sub-vault is decoded, the security of the template can still rely on the hash function. As each triangle is represented by a 24-bit binary string in the proposed system, if the attacker tries all 24-bit binary strings to find the pre-image of a given hash value, he/she will need to conduct average $(1+2^{24})/2$ hash operations, so the overall security now become $\log(3.6e{+}09+(1+2^{24})*9/2+1) \approx 32bits$. It is noteworthy that the security is evaluated by simply assuming polynomial interpolation and hashing to be only one elementary operation, while the real security can be much higher as both of them involves multiple computational elementary operations. By using different hash functions in diverse applications, the proposed construction can also resist the cross-matching attack.

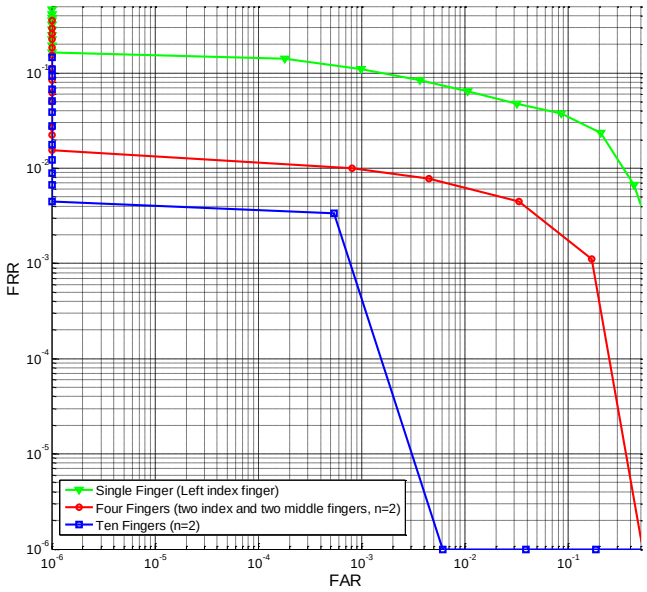

Fig. 7. ROC curves comparison.

As far as cryptographic key protection is concerned, the attacker has to decode at least n sub-vaults. Therefore, the computational security is $\log(\min_{1\le i\le C(m,n)} N_i+1)$, where N_i is the average number of elementary operations of the *ith* combination, which is generated by selecting n biometrics from m ones, denoted by $N_i=\sum_{j=1}^{n} N(F'(V_{sub,j}))$. Apparently, N_i is roughly n times $N(F'(V_{sub,j}))$, which is the average number of elementary operations required to decrypt the cryptographic key in the corresponding SBC.

VIII. CONCLUSION

Security and accuracy are two major factors influencing the performance of a biometric cryptosystem. The majority of work in this field uses average min-entropy or conditional Shannon entropy as the security metric. However, in this paper, we point out the limitation of entropy in measuring the security of biometric cryptosystems, and correct the entropy-based security analysis of some popular fingerprint-based cryptosystems. Then we propose a new security analysis framework, which jointly considers information-theoretic and computational security, thus being able to measure the security of biometric cryptosystems more comprehensively.

In terms of accuracy analysis, we reanalyze the accuracy of MBCF and MBCD from the theoretical perspective. The results show that better accuracy of MBC than SBC is not theoretically guaranteed. As a matter of fact, whether or not MBCF or

MBCD can offer an improvement of accuracy over SBC depends on several factors: selected biometric traits, fusion algorithms, decision rules, etc. Finally, we propose a practical MBCD construction, which uses fingerprints from multiple fingers to encrypt the cryptographic key. The experimental results and security analysis prove that the proposed construction provides stronger security and better authentication accuracy compared to the corresponding SBC.

REFERENCES

[1] Y. Sutcu, Q. Li, and N.Memon, "Secure biometric templates from fingerprint-face features," in *Proc. CVPR Workshop on Biometr.*, Minneapolis, MN, Jun. 2007, pp.1-6.

[2] A. Ross, J. Shah, and A. K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," IEEE Transaction on Pattern Analysis and Machine Intelligence, 2007, 29(4), pp. 544-560.

[3] S. Wang and J. Hu. "Alignment-Free Cancelable Fingerprint Template Design: A Densely Infinite-to-One Mapping (DITOM) Approach," *Pattern Recognition*, 2012, 45 (12), pp.4129-4137.

[4] T. Ahmad, J. Hu, and S. Wang. "Pair-polar coordinate based cancelable fingerprint templates," *Pattern Recognition*, 2011, 40(10-11), pp. 2555-2564.

[5] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating Cancelable Fingerprint Templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2007, 29 (4), pp. 561-572.

[6] C. Lee, J. Y. Choi, K. A. Toh, S. Lee, and J. Kim. "Alignment-Free Cancelable Fingerprint Templates Based on Local Minutiae Information," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 2007, 37 (4), pp. 980-992.

[7] A. Cavoukian and A. Stoianov, "Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy," Tech. Rep. Information and Privacy Commissioner, Ontario, Canada, 2007 [Online]. Available: www.ipc.on.ca

[8] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, Jun.2004.

[9] A. Juels and M. Wattenbeg, "A fuzzy commitment scheme," in *Proc.6th ACM Conf. Comput. Commun. Security*, Singapore, 1999, pp. 28–36.

[10] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes Cryptogr.*, Feb. 2006, 38(2), pp. 237-257.

[11] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Eurocrypt*, 2004, pp. 523–540.

[12] J. D. Golic and M. Baltatu, "Entropy analysis and new constructions of biometric key generation systems," *IEEE Trans. Inf. Theory*, May 2008, 54(5), pp. 2026–2040.

[13] B. Fu, S. X. Yang, J. Li, and D. Hu, "Multibiometric cryptosystem: Model structure and performance analysis," *IEEE Transactions on Information Forensics and Security*, December 2009, 4(4), pp.867-882.

[14] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature level fusion," *IEEE Transactions on Information Forensics and Security*, 2012, 7(1), pp.255–268.

[15] K. Nandakumar, and A. K. Jain, "Multibiometric template security using fuzzy vault," in *Proc. IEEE Int. Conf. Biometrics: Theory, Applications and Systems*, Arlington, VA, Sep. 2008, pp. 1–6.

[16] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multimodal biometric templates for verification using fingerprint and voice," in *SPIE Defense Security: Biometr. Technol. Human Identif. V*, Orlando, FL, Mar. 2008.

[17] A. Ross, and A. K. Jain, "Mutimodal Biometrics: An Overview," in *Proc. of 12th European Signal Processing Conference*, September 2004, pp. 1221-1224.

[18] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based Fuzzy Vault: Implementation and Performance," *IEEE Trans. on Info. Forensics and Security*, December 2007, 2(4), pp. 744–757.

[19] W. Yang, J. Hu, S. Wang, and M. Stojmenovic, "An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures," *Pattern Recognition*, March 2014, 47(3), pp. 1309-1320.

[20] G. Zheng, W. Li, and C. Zhan, "Cryptographic key generation from biometric data using lattice mapping," in *ICPR '06:Proceedings of the 18th International Conference on Pattern Recognition*, 2006, pp. 513–516.

[21] Y. J. Chang, W. Zhang, and T. Chen, "Biometrics-Based Cryptographic Key Generation," in *Proceedings of IEEE International Conference on Multimedia and Expo (ICME)*, 2004, volume 3, pp. 2203–2206.

[22] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice (extended abstract)," in *Proceeedings of the 2001 IEEE Symposium on Security and Privacy*, May 2001, pp. 12–25.

[23] J. D. Golic, and M. Baltatu, "Soft generation of secure biometric keys," in *Proceeding of the 12th Australasian conference on Information security and privacy*,2007, pp. 107-121.

[24] J. L. Massey, "Guessing and entropy," in *Proceedings of the 1994 IEEE International Symposium on Information Theory*, 1994, pp.204.

[25] I. R. Buhan, J. M. Doumen, P. H. Hartel, and R. N. J. Veldhuis, "Fuzzy Extractors for Continuous Distributions," in *Proceedings of ACM Symposium on Information, Computer and Communications Security*, Singapore, March 2007, pp. 353-355.

[26] A. Nagar, K. Nandakumar, and A. K. Jain, "A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates," *Pattern Recognition Letters*, 2010, 31(8), pp. 733–741.

[27] E. R. Berlekamp, "Algebraic Coding Theory," McGraw Hill, New York, 1968.

[28] J. L. Massey, "Shift register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, 1969, 15(1), pp.122-127.

[29] W. W. Peterson, "Encoding and error-correction procedures for Bose-Chaudhuri codes," *IRE Transactions on Information Theory*, IT-60 1960, pp.459-470.

[30] E. Liu, H.Zhao, J. Liang, L. Pang, M. Xie, H. Chen, Y. Li, P. Li, and J. Tian, "A key biding system based on n-nearest minutiae structure of fingerprint", *Pattern Recognition Letters*, 2011, 32(5), pp.666-675.

[31] J. Zhang, C. Chen, Y. Xiang, W. Zhou, and Y, Xiang, "Internet Traffic Classification by Aggregating Correlated Naïve Bayes Predictions," *IEEE Transactions on Information Forensics and Security*, 2013, 8(1), pp.5-15.

[32] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS Attacks Using Entropy Variations," *IEEE Trans. Parallel and Distributed Systems*, 2011, 22(3), pp. 412-425.

[33] A. Kiayias, and M. Yung, "Cryptographic Hardness based on the Decoding of Reed-solomn Codes," *IEEE Transaction on Information Theory*, 2008, 54(6), 2752-2769.

[34] V. Guruswami and M. Sudan, "Improved Decoding of Reed-Solomn and Algebratic-Geometric Codes," in the *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, 1998.

[35] K. Xi, J. Hu, and F. Han, "An alignment free fingerprint fuzzy extractor using near-equivalent dual layer structure check (NeDLSC) algorithm," in *Proceedings of the 6th IEEE Conference on Industrial Electronics and Applications (ICIEA)*,2011, pp. 1040–1045.

[36] J. M. Buchanan, "Simple Majority Voting, Game Theory, and Resource Use," *The Canadian journal of economics and political science : the journal of the Canadian Political Science Association*, 1961, 27(3), pp. 337-348.

[37] L. Lam and C. Y. Suen, "Application of Majority Voting to Pattern Recognition: An Analysis of Its Behavior and Performance," *IEEE Transaction on Systems, Man, and Cybernetics-Part A: Systems and Humans*, September 1997, 27(5), pp.553-568.

[38] K. K. Ladha, "The Condorcet Jury Theorem, Free Speech, and Correlated Votes," *American Journal of Political Science*, 1992, 36(3), pp.617-634.

[39] S. Berg, "Condorcet's Jury Theorem and the reliability of majority voting," *Group Decision and Negotiation*, 1996, 5(3), pp.229-238.

[40] C. Li, "Double layer secure sketch," in *Proceedings of AIP Conference, International Conference of Numerical Analysis and Applied Mathematics*, 2012, pp.1500-1505.

[41] W. Yang, J. Hu, and S. Wang, "A delaunay triangle-based fuzzy extractor for fingerprint authentication," in *Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2012, pp. 66–70.

[42] W. Zhou, J. Hu, S. Wang, I. Petersen, and M. Bennamoun, "Performance evaluation of a large 3D fingerprint database," *Electronics Letters*, 2014, 50(15), pp. 1060-1061.

[43] W. Zhou, J.Hu, I. Petersen, S. Wang, and M. Bennamoun, "3D fingerprint database and associated multimodal 2D fingerprint database," URL: http://seit.unsw.adfa.edu.au/staff/sites/hu/.

[44] W. Yang, J. Hu, S. Wang, C. Chen, "Mutual dependency of features in multimodal biometric systems," Electronics Letters, 2015, 51(3), pp. 234-235.

Cai Li received his B.S. degree from Nanjing University of Aeronautics and Astronautics, China in 2007 and his master degree of Information Technology from the University of Melbourne in 2009. Now he is currently working toward the PhD degree in the School of Engineering and Information Technology, University of New South Wales at Canberra (UNSW@Canberra), Australia. He is an IEEE Member. His research interests are biometric pattern recognition and biometric security.

Jiankun Hu is Full Professor and Research Director of Cyber Security Lab, School of Engineering and IT, University of New South Wales at the Australian Defence Force Academy (UNSW@ADFA), Canberra, Australia. He has obtained his BE from Hunan University, China in 1983; PhD in Control Engineering from Harbin Institute of Technology, China in 1993 and Masters by Research in Computer Science and Software Engineering from Monash University, Australia in 2000. He has worked in Ruhr University Germany on the prestigious German Alexander von Humboldt Fellowship 1995-1996; research fellow in Delft University of the Netherlands 1997-1998, and research fellow in Melbourne University, Australia 1998-1999.

Jiankun's main research interest is in the field of cyber security including biometrics security where he has published many papers in high-quality conferences and journals including IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI). He has served in the editorial board of up to 7 international journals and served as Security Symposium Chair of IEEE flagship conferences of IEEE ICC and IEEE Globecom. He has obtained 7 ARC (Australian Research Council) Grants and is now serving at the prestigious Panel of Mathematics, Information and Computing Sciences (MIC), ARC ERA (The Excellence in Research for Australia) Evaluation Committee.

Josef Pieprzyk is a Professor in School of Electrical Engineering and Computer Science at Queensland University of Technology. He is leading the Information Security Discipline in the School. His main research interest focus is Cryptology and Information Security and includes design and analysis of cryptographic algorithms (such as encryption, hashing and digital signatures), secure multiparty computations, cryptographic protocols, copyright protection, e-commerce, web security and cybercrime prevention.

Professor Pieprzyk is a member of the editorial boards for International Journal of Information Security, Journal of Mathematical Cryptology, International Journal of Applied Cryptography, Fundamental Informaticae, Journal of Research and Practice in Information Technology, International Journal of Security and Networks and International Journal of Information and Computer Security.

Professor Pieprzyk published 5 books, edited 10 books (conference proceedings published by Springer), 6 book chapters, and more than 200 papers in refereed journals and refereed international conferences.

Willy Susilo received the Ph.D. degree in computer science from the University of Wollongong, Wollongong, Australia. He is a Professor with the School of Computer Science and Software Engineering and the Director of Centre for Computer and Information Security Research, University of Wollongong. He has been awarded the prestigious ARC Future Fellow by the Australian Research Council. His main research interests include cryptography and information security. He has published numerous publications in the area of digital signature schemes and encryption schemes.