Error Correction Codes for Biometric Cryptosystem: An Overview

Andrew Beng Jin Teoh, Jaihie Kim
Yonsei University

Abstract

In cryptographic applications, the key protection is either knowledge-based (passwords) or possession-based (tamper-proof device). Unfortunately, both approaches are easily forgotten or stolen, thus introducing various key management issues. By incorporating biometrics technologies which utilize the uniqueness of personal characteristics, the security of cryptosystems could be strengthened as authentication now requires the presence of the user. Biometric Cryptosystem (BC) encompasses the design of cryptographic keys protection methods by incorporating biometrics. BC involves either key-biometrics binding or direct key generation from biometrics. However, the wide acceptance and deployment of BC solutions are constrained by the fuzziness related with biometric data. Hence, error correction codes (ECCs) should be adopted to ensure that fuzziness of biometric data can be alleviated. In this overview paper, we present such ECC solutions used in various BCs. We also delineate on the important facts to be considered when choosing appropriate ECCs for a particular biometric based solution from accuracy performance and security perspectives.

I. Introduction

With widespread information exchange and access to resources over public network, cryptography has become an important and necessary mechanism for secure channel access and authentication. The aim of cryptography is to provide secure transmission of messages so that two or more persons can communicate in a way that guarantees to meet the desired subset of the following four goals – confidentiality, data integrity, authentication and non-repudiation [1]. However, there are some practical problems associated with the use of cryptosystem since the current methods authenticate the key instead of the user. The need for a proper and reliable key management mechanism is required in order to confirm that the listed keys actually belong to the given entities. Currently, a manual method of authentication using identification card, company number or license, is required for enrolment of public keys. In addition, the security depends on the large size of a cryptographic secret key generated, and it is not feasible to require user to remember such a long key. Thus a simple password is still required for key encryption which in turn leads to continuing potential hacker attack on the password to retrieve the cryptographic keys.

Biometrics is the science of using unique human characteristics for personal authentication based on a person's biological and behavioral characteristics[2]. Biological biometrics includes fingerprint, retina, face and iris features and the behavioral biometrics such as typing dynamic, signature and voice etc. Traditionally, biometrics based authentication for access into systems has always been yes/no decision-based depending on how "close" the test biometrics is to a stored template as shown in 〈Figure 1〉.

The template is usually obtained from the user during enrolment and is usually stored in a local or server-side storage. For local storage, normally a password is required for release of the template while for some challenge-response protocol needs to be in place to enable secure exchange of the biometric template. The decision of how "close" the test biometrics is to the template is determined

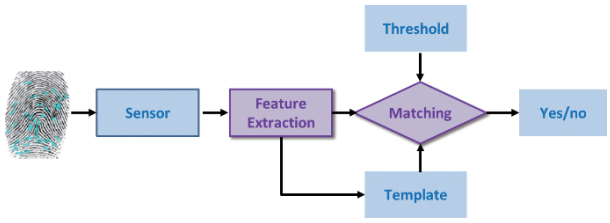

Figure 1. Conventional Biometric Authentication

empirically and entails tuning of a threshold.

Biometrics and cryptography have two very different objectives. The former is continuous and stochastics in nature, and its acceptance and rejection are governed by some empirically trained threshold. In contrast to biometrics, cryptography is discrete, and authentications are based on what is personally known like password and keys held in possession. Biometrics takes into consideration the physical presence of the user but however, suffers from permanently loss if compromised. On the other hand, cryptography has been used widely for securing transactions and access into systems without authenticating the physical presence of the user, and the keys used are replaceable. Both biometrics and cryptography are highly complementary, hence the motivation for their integrated application: Biometric Cryptosystems (BC) [3].

The notion of BC was first put forward in the mid-90s by Tomko et al [4] and also dubbed as "Biometric Encryption" [5]. BC either securely ***bind a digital key*** to a biometrics, or ***generate a digital key from the biometrics***, so that no biometric data is stored. What is stored is a piece of data coined as ***helper*** data. In general, helper data should be computationally difficult to retrieve either the key or the biometrics. That is, helper data should leak no or minimal information about key or biometrics. The key is recreated only if the correct biometric data is presented on verification. In literature, several dominant instances of BC are fuzzy vault, fuzzy commitment, secure sketch, fuzzy extractor etc.

However, the popularity of BC solutions are somewhat limited by the stochastics nature that associated with biometric data. For example, biometric data from an individual can vary during each capture due to acquisition noise and environmental condition. While providing evidence to the fact that biometric data cannot be encrypted simply as in cryptography. It is necessary to incorporate error tolerant mechanisms such as Error Correction Code (ECC) when dealing with biometric data to address the effect of noisy biometric inputs [6].

ECCs are commonly used to correct the errors in messages that are sent over noisy communication channels. ECCs can be defined as a set of ***codewords*** C, where each codeword $c \in C$ represents an n-bit sequence in which the k bit messages $m \in M$ $(n>k)$ are mapped to before transmission. The $(n-k)$ bits are dubbed as parity bits which used to restore the transmitted codeword from a corrupted received codeword. Denote size of error correcting capability as t, this implies that c can correct up to t errors, subject to the minimum distance of any two codewords in C is at least $2t+1$. An analogy can be established between the noisy communication channels and the fuzzy biometric system whereby biometric data can be perceived as corrupted codewords [6]. Several widely deployed ECCs in BC systems are Reed Solomon (RS) Codes [7], Hadamard Codes [8], Binary Bose-Chaudhuri-Hocquenghem (BCH) Codes [9], Low-Density Parity-Check (LDPC) Codes [10], Turbo Codes [11] or their combinations [8]. The choice of an ECC is one of the most crucial elements of BC scheme. The ECC must be able to remove the noise of biometric data, yet secure, i.e. not leaking information to an adversary.

In this paper, we outlined such ECC solution used in BC while explaining how they are deployed in several instances of BC. We will discuss the vital role of ECC plays in BC from accuracy performance and security perspectives.

II. Various ECCs Enabled Biometric Cryptosystems

1. Fuzzy Commitment

The fuzzy commitment scheme of Juels and Wattenberg

[13] is inspired from extension of a cryptographic bit commitment [14] but it allows some variability in the committed value via ECCs notion. In a bit commitment scheme, a sender commits an encrypted version of x bit, denote enc(x), an encrypted version of x, in such a way that the receiver unable to determine the true value from the encrypted commitment. Bit restoration is only possible if sender can validate that enc(x) is an encrypted version of x. On the other hand, the commitment cannot be de-commited by anyone else since the transformation of x to enc(x) is only recognized to the sender.

In biometric cryptosystem context, Juels and Wattenberg proposed a way of committing a bit string c which is an encoded version of digital key by using ECCs. Denote a set of n bit codewords C with a minimum distance among them of at least $2t+1$ and a same size biometric witness b. Then the fuzzy commitment, (d, $h(c)$) where, $d = cXORb$, cC, and $h(c)$ is a one-way hashed version of c. Ideally, the commitment does not reveal information on the biometric data, since $h(c)$ is a secure one-way function. In order to de-commit (d, $h(c)$), it is necessary to produce a biometric trait b' which is sufficiently close to b such as the hamming distance between b' and b, $Hm(b', b) \leq t$. In key production stage, we perform $c' = dXORb$ and if $h(c) = h(c')$, c will be decoded and a digital key k will be released else the process is terminated. The progression of fuzzy commitment can be found in 〈Figure 2〉.

Fuzzy commitment scheme is commonly applied to biometric data that is represented in binary ordered vector form such as iris [8], face [9], texture based fingerprint [12] etc. An early practical work of applying fuzzy commitment scheme on iris biometrics is demonstrated by Hao et al [8]. The authors used a combination of two ECCs, namely Hadamard and Reed-Solomon. The 2048-bit iris template is segmented into 32 blocks of 64 bits each. The blocks are the codewords of the (64, 7) Hadamard ECC which outputs a 7-bit word and can correct at least 15 random bit errors. The second ECC, Reed-Solomon code, removes the remaining block level (burst) errors. It works with the 7-bit words, so that 32 words decode 20 output words, thus producing a 140-bit key. The (32, 20) Reed-Solomon ECC can correct up to 6 erroneous 7-bit words. Despite Hao et al work depicts very promising results with low variability of iris data. However, when it was evaluated to the challenging ICE database, the key recovery rate is devastatingly deteriorated [15]. Subsequently, Bringer et al [15] proposed an ECC which is a product of two Reed-Muller ECCs, (64, 7) and (32, 6), and iterative soft decoding. This ECC significantly improved the accuracy of the fuzzy commitment scheme. Other works follows the same line of idea can be found in [16]-[18].

Fuzzy commitment is also particularly suitable for face biometrics as facial feature is typically presented in ordered feature vector form that can be easily binarized [19]-[21]. BCH codes, which are used for bit level error correction, are usually opted due to its simplicity. BCH codes have been used also by Tuyls P. et al. [22] in developing a fuzzy commitment scheme which concatenates two fingerprint texture vectors namely squared directional field and a finger-code obtained through Gabor filtering.

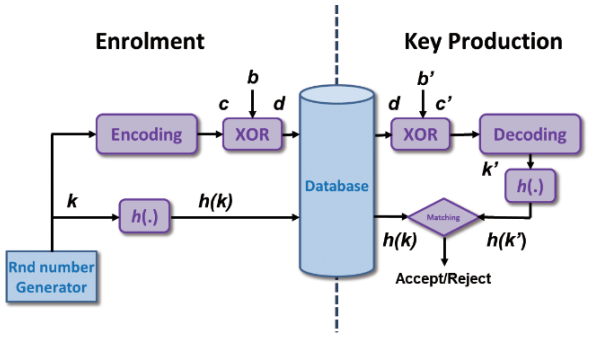

Figure 2. Fuzzy Commitment Scheme

2. Fuzzy Vault

Fuzzy vault is introduced by Juels A. et al. [23] which was inspired from the Shamir's secret sharing scheme. Fuzzy vault admits non-exactly ordered biometric representation such as minutiae-based fingerprint thus complement fuzzy commitment that incapable to handle this type of biometric data. The security of fuzzy vault relies completely upon the polynomial reconstruction problem.

Let consider a digital key k, and during vault construction it is encoded into coefficients of a polynomial P of degree d. Then, the vault V is constructed by projecting a user specific n element biometric set into the polynomial while including c element chaff set which does not lie on P. Furthermore, the k is restored through polynomial reconstruction after identifying possible $d+1$ out of n original points by presenting the biometric set during key production stage.

At enrolment, the secret message (or digital key in our context), k is encoded into coefficients of a secret sharing polynomial $P(x)$ of degree d. The genuine shares are represented as point $(x, y=P(x))$ with x being element in biometric set, and are collectively known as genuine set G and $|G|=n$. Then, another set of chaff points, $(a, b)\notin C$, which does not lie on $P(x)$ is generated randomly. The union set of G and C forms a vault V. During key production stage, the k can restored through polynomial reconstruction after identifying possible $d+1$ out of n genuine points by presenting the biometric set.

A practical fuzzy vault based on fingerprint minutiae set realized by [24] adopts Cyclic Redundancy Check (CRC), an error detecting coding scheme. During enrollment, let k of 128 bits be the digital key to be bounded with fingerprint data. The CRC checksum of k is then computed by means of 16-bit primitive generator polynomial $h(x) = x^{16}+x^{15}+x^2+1$. The resulting checksum is concatenated with k to generate a new key code, kc of 144 bits and encoded in 9 coefficients in Galois Field GF(2^{16}) of a polynomial P of degree $d = 8$. Each minutiae position (x, y) of n fingerprint minutiae is then quantized and coded into a 16 bit value r, in which the first 8 bits represents the x coordinate while y represents the rest. Thereafter, each r is projected into P and the genuine set $G = \{(r_i, P(r_i))|\ i=1,...n\}$ is generated. Subsequently, a set of Chaff points $C = \{(a_j, b_j)|\ j=1,...,m\}$ is produced in such a way that $a_j \neq r_j$ and b_j do not lie on P. Finally, the randomized list of points in $G \cup C$, $\{(r_j, s_j)|\ j=1,...,m+n\}$ and the degree of polynomial d are kept in vault V. The randomization is to conceal the information that vital for separating chaff and genuine points.

For key production, the minutiae is extracted from query fingerprint image, quantized and coded to create a set of 16 bit string $\{r'_i|i=1,...,n'\}$ which are to be used in polynomial reconstruction. Then, the subset of points that lie in both r'_i and s_j which is the abscissa of V is determined. Assuming q number of such points have been found $\{(r_i, s_i)|i = 1, 2, ..., q\}$; they are then divided into all possible $(d+1)$ combinations, since $(d+1)$ unique projection are required to decode a polynomial of degree d. Thereafter, for each such $(d+1)$ pair Lagrange interpolation polynomial is retrieved as well as from the coefficients the possible kc'. Then, the polynomial corresponding to kc' is divided by $h(x)$ to evaluate the CRC checksum and if the remainder is zero, no errors in kc' to be assumed. Finally, the k can be recovered from kc' by removing the bits corresponding to the checksum. Thus, the digital key can only be recovered if and only if $(d+1)$ points of query minutiae set match with the enrolled minutiae set.

Fuzzy vault security relies on the difficulty of separating genuine points on the vault which lie on the secretly embedded polynomial. If genuine points can be estimated, the digital key can be largely recovered from Lagrange interpolation. However, if the ordinate values of the vault is encrypted, it would forbid the vault decryption even having the correct set of points. This observation was exploited in [25] to improve the CRC based fuzzy fault by incorporating it with a BCH. Specifically, they quantized and coded fingerprint minutiae as afore described and then XORed with a set of BCH codewords, generated from the ordinate values of the vault to compute the fuzzy commitment. Therefore, key production is a two-step process of unwrapping the fuzzy commitment and thereafter the vault [6].

3. Secure Sketch and Fuzzy Extractor

Unlike key binding schemes such as fuzzy vault and fuzzy commitment, Dodis et al. [26] put forward a generic model of keys extraction from biometrics and other stochastic data. The model consists of two primitives, namely ***secure sketch*** and ***fuzzy extractor***. The former addresses the problem of compensating noise in biometrics, by producing a public helper data called

sketch SS(w) about the biometrics. Sketch is to be used to recover the original template w, from noisy input biometrics, w', provided both w and w' are sufficiently close. The latter addresses both the problem of noise compensation, along with the problem of non-uniformity of the resulting keys.

The strength in the Dodis's model is that the authors have defined the model in information-theoretic sense complete with the lower bound on the entropy for optimal security. Dodis et al also elucidated the fuzzy commitment and fuzzy vault using the fuzzy extractor model for Hamming metric (binary vector form) and set difference (unordered point set), respectively, and could verify the security ie. entropy lost via information theory. The model would not be directly applied to continuous metric though as with the model in Tuyls and Goseling [28], instead, a quantization process is required to convert a continuous feature vector into a discrete/binary vector form.

In general, four variants of secure sketch construction are discussed in [26]. For ***code-offset secure sketch*** implementation, we consider a set of n bit codewords C with a minimum distance at least $2t+1$ and a binary biometric vector w of the same size. They have defined the shift needed to get the codeword c from w as a secure sketch of w, $SS(w) = cXORw$. It is possible to recover w from w' if the $dis(w, w') \leq t$ where t is a threshold value. The recovery process requires the computation of $c' = SS(w)XORw'$ and decode c' to get c to generate w through $SS(w)XORc$ eventually. A realization in face biometrics can be found in [29].

In addition, code-offset secure sketch can be extended to a ***syndrome based secure sketch*** in which $SS(w)$ is re-defined as the syndrome of w, $syn(w) = Gw$, where G is the parity check matrix. The sketch can be restored by w' and $SS(w)$ by solving the unique error vector e with hamming weight $\leq t$, such that $syn(e) = syn(w')XORSS(w)$ and hence $w = w'XORe$. A practical implementation dubbed fuzzy syndrome hashing is demonstrated in [10] whereby syndromes of Low-Density Parity-Check (LDPC) codes are adopted for error correction on iris features.

Another variant of secure sketch, coined *Pin Sketch* is a primary instance for applying of BCH codes in secure sketch [26]. Pin Sketch adopts (n, k, d) binary BCH code where n is the number of bits in the codeword, k is the number of bits in the message while d denotes the minimum distance of the codewords for error correction. If w is the n bit biometric string to be protected, the secure sketch $SS(w)$ is constructed by taking the syndrome of w, $SS(w)=syn(w)$. When recovering w from a noisy biometrics w', $syn(w')$ is computed and thus difference set, $\delta = syn(w') - syn(w)$ can be obtained. Then BCH decoding is used to identify vector v such that $syn(v)=\delta$. If $Hm(w', w) \leq (d-1)/2$, w can be recovered by calculating $w'+v$. where $Hm(,)$ is Hamming distance [6].

Lastly, Reed-Solomon (RS) codes have also been deployed in secure sketch that admits fuzzy vault. Let $w= \{w_i | i=1,...,n\}$ be n minutia of fingerprint. Then, w is projected into a polynomial P of degree at most $(s-t-1)$ to compute s pairs $V=\{(w_i, P(w_i)) | i=1,...,s\}$. Finally the secure sketch $SS(w)$ is generated by adding $(r-s)$ chaff points to V that do not lie on the polynomial. In order to reconstruct the w from $SS(w)$ and w', first the points x_i w_1 that also lie in $SS(w)$ must be identified. Then, RS decoding can be performed to restore the P and hence the w.

As aforementioned, fuzzy extractor belongs to one of the primitives in Dodis's key extraction model [26]. The fuzzy extractor consists of a secure sketch and a strong extractor. During enrollment, output of the strong extractor with a biometric input w generates the ***uniformly random string*** R while the output of the sketch is stored as a helper data (similar to $SS(w)$) that publicly available. During authentication, the helper data along with a close enough noisy input w' could recover the R. The vital characteristic of such fuzzy extractor is that the R will not be stored; instead they are generated on-the-fly when required via w' which is sufficiently close to w.

Similar to secure sketch, fuzzy extractor admits both ordered binary feature vector and unordered point set biometrics such as iris, face, handwritten signature fingerprint etc. A handful realizations of fuzzy extractor include [31]-[34] in which they mostly applied on fingerprint minutia, iris and combination of multiple biometrics.

4. Others

Vetro et al. [35] proposed a secure sketch alike biometric cryptosystem based on distributed source coding. A Slepian-Wolf framework is used to store a secured biometric template during enrollment stage and recover the template at authentication stage. They demonstrated to use LDPC codes in combination with a hash function to provide secure iris template storage. Santos et al. [36] follow same line of design as in [35] and put forward a universal mask which selects only the 5142 most reliable bit positions of the 9600 bits in the iris templates to enhance the security of the system.

On the other hand, Nagar et al. [37] and Sutcu et al. [38] developed secure fingerprint systems by using syndromes of LDPC codes. In their systems, fingerprint minutiae maps are transformed into binary vectors which are suitable for LDPC coding. Syndromes obtained via LDPC coding of these binary vectors serve as secure biometrics. On top of providing very low false accept rates and low false reject rates, the design ensures that distributed biometric coding is information-theoretically secure.

A turbo code enabled keys extraction scheme that inspired by the code-offset sketches, along with constellation modulation is proposed recently[39]. The scheme allows to set the template size without constraint and to manage data characterized by a high intraclass variability of biometric data without exploiting specific characteristics of the biometrics of interest. These tasks are accomplished by utilizing turbo codes which allows to achieve high ECCs, while constellation modulations are used to let the codes operating in soft-decoding modality, thus further enhancing their correction capabilities and providing a highly flexible framework with different operating conditions. A real implementation of this scheme has been demonstrated through handwritten signature.

III. Impact of ECCs to Biometric Cryptosystems Performance

As evident from the literature, error-correcting codes indeed provide a powerful mechanism to cope with variations in biometric data. Quantitatively, the performance of biometric cryptosystems is commonly quantified via indicators such as False Acceptance rate (FAR) and False Rejection Rate (FRR). The FAR is the probability that the biometric system will incorrectly accept an unauthorized user. Likewise, the FRR is the probability that an authorized user is rejected. FAR/FRR is a trade-off and largely rely on the error correction capability with respect to bit error rate (BER) of the underlying ECCs used in the system. The error correcting capability must be sufficiently good to distinguish between intra-class and inter-class variability. Thus, before deciding on an ECC scheme it is vital to examine the genuine and imposter distance distribution, which respectively reflect intra-class and inter-class variability of the considered biometric information[40].

Linear codes such as BCH, Hadamard, RS, LDPC and their combinations were largely explored in the literature [7]-[12],[16]-[22],[25],[29],[31]-[34],[36],[38]. Unfortunately, these linear codes are inflexible[30]. Firstly, the application of linear block codes requires binary biometric vector having the same size of the employed codewords, thus some bits have to be discarded, or a bits-padding has to be performed. A loss in discriminability may occur in the former case, while in the latter case a severe leakage of information about codewords can result from the observation of the code-offset[48]. It is vital to adopt codewords whose length can be adjusted to the length of binary biometric vector, and not vice versa. A promising solution is by using Turbo code as reported in [39].

Secondly, linear block codes often incapable offer high satisfactory error correction capability to cope biometric data with significant intra-class variability, thus resulting in poor FRRs. Ideally the error correcting capability must be 100 % even for highest possible distance (or BER) while exhibiting 0% for inter-class BER [6]. This procedure would help in identifying the most suitable ECC for a BC in the early stage. Nevertheless, these ideal situations are highly unlikely be satisfied practically, hence fine tuning is necessary for the selected

ECC to ensure it can adequately differentiate between the two classes. As a remedy it could be possible to utilize known statistics about the existing differences of the considered biometrics to design a specific code adapted to the biometrics properties. This property has been exploited in [8], where Hadamard and Reed–Solomon codes are jointly employed to manage respectively the background and the burst differences deriving from the comparison of two iris templates. However, as observed in [15], the performance deteriorates when a more challenging iris dataset is examined.

In general, the impact of ECC on biometric cryptosystem performance relies on the type of the chosen ECCs as well as how to fine tune the selected ECC. The latter could be attained by altering the code rate (increasing or decreasing the amount of parity bits) included in the ECC. The effect on the error correcting capability with the code rate is known as the ***granular effect*** of an ECC. The finer it is possible to tune the ECC's correction capability, the more precisely it will be possible to adjust the FAR and FRR trade–off.

Furthermore, an ideal ECC should have a steep roll off characteristic with BER to allow a very high (close to 100%) error correction in a particular range and almost 0% in the other [6]. Hence, apart from the granularity property, the steepness property is also another important factor to be accounted. Interested readers on empirical study of granular effect and steepness properties of ECCs on biometric system are referred to [40].

IV. Impact of ECC to Biometric Cryptosystem Security

Despite biometric cryptosystems is provable secure in information theoretic sense, it is indeed vulnerable to several dreadful security and privacy attacks in practice. We refer curious readers on complete vulnerabilities of BC to [41]–[47]. Here we only describe a few attacks that have been attributed to ECCs.

Note ECCs security does not appear in most other ECC applications, such as data storage or communication system, but this is not the case for BC. For instance, ECC that is insecure for BC purposes is a trivial repetition code, when each key bit is encoded with an odd number of bits of the same parity [48]. As shown by [49], an adversary can generate a matching score and crack the BC helper data using a "hill climbing" attack despite BC is not supposed to have a score.

If we assume that the codeword c is chosen from an (n, k, t) ECC then k bits of biometric binary vector, b are protected by the k random bits in c due to the k bits of randomness in c. From information theoretic point of view, the helper data of BC, such as $d = cXORb$ in fuzzy commitment or $SS(w)$ in secure sketch will leak $n\text{-}k$ bits of information about b. It can be shown that if robustness against a certain number of bit errors in b is required, some leakage cannot be avoided [26]. Hence, in principle the adversary can set up a linear system of $n\text{-}k$ equations in n unknowns leaving him with k degrees of freedom. However, this theoretical leakage does not reveal to an adversary how this information can be exploited to learn specific information on b that was used to generate helper data.

A number of practical threats were reported in [46], [48] and [50] exploiting the use of linear ECCs and the fact that many practical ECCs are not perfect codes. In [46], the authors demonstrates that if two helper data $d1=c1XORb$ and $d2=c2XORb'$ of fuzzy commitment are retrieved, the adversary can compute $d1XORd2=c1XORc2XOR(bXORb')=c3XOR(bXORb')$ due to the ECC property that the sum of two codewords is again a codeword. If this can be decoded, it is highly possible that $b \simeq b'$, attributed to the non–perfectness of the ECC and the distribution of b. This observation thus implies bs are linkable across diverse applications or databases, which is one of the major concerns in privacy leakage.

Stoianov [48] illustrated zero insertion mechanism that proposed by Kanade et al [18] to improve the accuracy of IrisCode based fuzzy commitment [8] is indeed insecure. By learning the locations of only 7 zeros for each 32–bit block, an attacker can recover the full 198–bit key within a fraction of a second. Even if the scheme were

modified such that 12 zeros appended the IrisCode in each 32-bit block, for each block, the attacker would still be able to recover 5 out of 6 key bits. The remaining one bit ambiguity could be resolved in a matter of minutes by random trials and running a Reed-Solomon decoder. By and far, for an arbitrary linear ECC, the problem of cracking the zero insertion scheme is equivalent to solving a set of linear equations by using a syndrome decoding.

Despite a combination of codes could be useful for accuracy performance gain, eg. mix of Hadamard and RS codes in [8], it may also leave the system vulnerable to statistical attacks by exploiting the histograms of the computed offsets as revealed in [50]. The statistical attack based on ECCs is further examined in [52] in great detail whereby the authors reveal that binary biometric vectors, which exhibit sufficient entropy, bind cryptographic keys in a secure commitment is questionable. The study shows that fuzzy commitment can still be cracked. The structure of stored commitment is essential to the security of bound keys and biometric templates.

V. Summary

Error correction codes are an integrated part in most of the biometric cryptosystems to eliminate the fuzziness associated with biometric data. This overview paper delineates how ECCs are setup to achieve the accuracy performance requirements of various biometric cryptosystems. Depending upon the type of biometric data to be used and their associated error patterns, the ECCs must be selected attentively, considering the possible security and privacy breach of the underlying biometric cryptosystem. Moreover, error correcting capability characteristics and granularity of ECCs should also be considered when choosing the optimal coding scheme to achieve a desirable tradeoff between performance indicators FAR and FRR.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (2013006574)

References

[1]. B. Schneier. Applied Cryptography: Protocols Algorithms and Source Code in C. John Wiley and Sons, Inc. 1996.

[2] A.K. Jain, L. Hong, S. Pankanti. Biometrics Identification. Commun. ACM 43 (2) 91-98, 2000.

[3] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," Proceedings of the IEEE, vol. 92, no. 6, pp. 948-960, Jun. 2004.

[4] Tomko GJ, Soutar C, Schmidt GJ (1996) Fingerprint controlled pub Invalid source specified.lic key cryptographic sys-tem. US Patent 5541994, 30 July 1996 (Filing date: 7 Sept 1994).

[5] A. Cavoukian, M. Chibba, and A. Stoianov, "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment," Review of Policy Research, vol. 29, no. 1, pp. 37-61, Jan. 2012.

[6] Harsha S. Gardiyawasam Pussewalage, Jiankun Hu, and Josef Pieprzyk, "A Survey: Error Control Methods Used in Bio-Cryptography," presented at the 2014 10th International Conference on Natural Computation (ICNC 2014), 2014.

[7] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcardbased fingerprint authentication," in Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, 2003, pp. 45-52.

[8] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081-1088, Sep. 2006.

[9] 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, Berlin, Heidelberg, 2005, pp. 436 - 446.

[10] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani, "On fuzzy syndrome hashing with LDPC coding," in Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, New York, NY, USA, 2011, pp. 24:1 - 24:5.

[11] E. Maiorana, D. Blasi, and P. Campisi, "Biometric template protection using turbo codes and modulation constellations," in 2012 IEEE International Workshop on Information Forensics and Security (WIFS), 2012, pp. 25 - 30.

[12] Y. Imamverdiyev, A. B. J. Teoh, and J. Kim, "Biometric cryptosystem based on discretized fingerprint texture descriptors," Expert Systems with Applications, vol. 40, no. 5, pp. 1888 - 1901, 2013.

[13] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in Proceedings of the 6th ACM conference on Computer and communications security, New York, NY, USA, 1999, pp. 28 - 36.

[14] Giles Brassard, David Chaum, and Claude Crepeau, Minimum Disclosure Proofs of Knowledge Journal of Computer and System Sciences, vol. 37, pp. 156-189, 1988

[15] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, "Optimal iris fuzzy sketches", in IEEE First International Conference on Biometrics: Theory, Applications, and Systems, BTAS'07, 2007.

[16] R. Álvarez Mariño, F. Hernández Álvarez, and L. Hernández Encinas, "A crypto-biometric scheme based on iris-templates with fuzzy extractors," Information Sciences, vol. 195, pp. 91 - 102, Jul. 2012.

[17] S. Kanade, D. Petrovska-Delacretaz, and B. Dorizzi, "Cancelable Iris Biometrics and using Error Correcting Codes to reduce Variability in Biometric Data", in IEEE Conference on Computer Vision and Pattern Recognition, IEEE, pp. 120-127, Florida, USA, Jun. 2009.

[18] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacretaz, and B.Dorizzi, "Three Factor Scheme for Biometric-based Cryptographic Key Regeneration using Iris", in Biometrics Symposium, IEEE, pp. 59-64, Florida, USA, Sep. 2008.

[19] M. van der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and F. Zuo, "Face biometrics with renewable templates," Proceedings of SPIE, vol. 6072, no. 1, p. 60720J - 60720J - 12, Feb. 2006.

[20] E. J. C. Kelkboom, B. Gökberk, T. A. M. Kevenaar, A. H. M. Akkermans, and M. Veen, "3D Face": Biometric Template Protection for 3D Face Recognition," in Advances in Biometrics, vol. 4642, 2007, pp. 566 - 573.

[21] B. Chen and V. Chandran, "Biometric Based Cryptographic Key Generation from Faces," in 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, 2007, pp. 394 - 401.

[22] P. Tuyls, A. Akkermans, T. Kevenaar, G. Schrijen, and R. Veldhuis, "Practical Biometric Authentication with Template Protection", in Proceedings of 5 th International Conference on Audio-and Video-Based Biometric Person Authentication, Springer, pp. 436-446, New York, USA, Jul. 2005.

[23] A. Juels and M. Sudan, "A fuzzy vault scheme," in IEEE International Symposium on Information Theory, 2002. Proceedings, 2002.

[24] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy Vault for Fingerprints," in Audio- and Video-Based Biometric Person Authentication, 2005, pp. 310 - 319.

[25] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptors", in Proceedings of 19th International Conference on Pattern Recognition, IEEE, pp. 1-4, Florida, USA, Dec. 2008.

[26] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," SIAM J. Comput., vol. 38, no. 1, pp. 97 - 139, Mar. 2008.

[27] X. Boyen, "Reusable cryptographic fuzzy extractors," in Proceedings of the 11th ACM conference on Computer and communications security, New York, NY, USA, 2004, pp. 82 – 91.

[28] P. Tuyls and J. Goseling, Capacity and Examples of Template Protecting. BioAW 2004, LNCS 3087, 158 – 170, Prague, 2004.

[29] Yagiz Sutcu, Qiming Li, and N. Memon, "Protecting Biometric Templates With Sketch: Theory and Practice," IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 503 – 512, Sep. 2007.

[30] E. Maiorana, D. Blasi, and P. Campisi, "Biometric template protection using turbo codes and modulation constellations," in 2012 IEEE International Workshop on Information Forensics and Security (WIFS), 2012, pp. 25 – 30.

[31] A. Arakala, J. Jeffers, and K. J. Horadam, "Fuzzy Extractors for Minutiae-Based Fingerprint Authentication," in Advances in Biometrics, vol. 4642, S.-W. Lee and S. Z. Li, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 760 – 769.

[32] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, "Privacy-Aware Biometrics: Design and Implementation of a Multimodal Verification System," in Computer Security Applications Conference, 2008. ACSAC 2008. Annual, 2008, pp. 130 – 139.

[33] W. Yang, J. Hu, and S. Wang, "A Delaunay Triangle-Based Fuzzy Extractor for Fingerprint Authentication," in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 66 – 70.

[34] R. Álvarez Mariño, F. Hernández Álvarez, and L. Hernández Encinas, "A crypto-biometric scheme based on iris-templates with fuzzy extractors," Information Sciences, vol. 195, pp. 91 – 102, Jul. 2012.

[35] Anthony Vetro, Stark Draper, Shantanu Rane, and Jonathan Yedidia, "Securing Biometric Data," in DISTRIBUTED SOURCE CODING, Elsevier, 2009.

[36] T. Santos, L.D. Soares, P.L. Correia, "Iris Verification System with Secure Template Storage", European Signal Processing Conference (EUSIPCO), Aalborg, Denmark, August 2010.

[37] A. Nagar, S. Rane, and A. Vetro, "Privacy and security of features extracted from minutiae aggregates," in Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on, 2010, pp. 1826 – 1829.

[38] Y. Sutcu, S. Rane, J. S. Yedidia, S. C. Draper, and A. Vetro, "Feature extraction for a Slepian-Wolf biometric system using LDPC codes," in Information Theory, 2008. ISIT 2008. IEEE International Symposium on, 2008, pp. 2297 – 2301.

[39] E. Maiorana, D. Blasi, and P. Campisi, "Biometric template protection using turbo codes and modulation constellations," in 2012 IEEE International Workshop on Information Forensics and Security (WIFS), 2012, pp. 25 – 30.

[40] S. Noto, P. L. Correia, and L. D. Soares, "Analysis of error correcting codes for the secure storage of biometric templates," in EUROCON – International Conference on Computer as a Tool (EUROCON), 2011 IEEE, 2011, pp. 1 – 4.

[41] X. Zhou, A. Kuijper, R. Veldhuis, and C. Busch, "Quantifying privacy and security of biometric fuzzy commitment," in International Joint Conference on Biometrics (IJCB), 2011, pp. 1 – 8.

[42] W. J. Scheirer and T. E. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," in Biometrics Symposium, 2007, pp. 1 – 6.

[43] A. Kholmatov and B. Yanikoglu, "Realization of correlation attack against the fuzzy vault scheme," in Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 2008, pp. 68190O – 68190O – 7.

[44] H. Poon and A. Miri, "A Collusion Attack on the Fuzzy Vault Scheme," ISeCure: The ISC International Journal of Information Security, vol. 1, no. 1, pp. 27 – 34, Jan. 2009.

[45] L. Ballard, S. Kamara, and M. K. Reiter, "The practical subtleties of biometric key generation," in Proceedings of the 17th conference on Security symposium, Berkeley, CA, USA, 2008, pp. 61 – 74.

[46] K. Simoens, P. Tuyls, and B. Preneel, "Privacy Weaknesses in Biometric Sketches," in Proceedings of the 2009 30th IEEE Symposium on Security and Privacy, Washington, DC, USA, 2009, pp. 188–203.

[47] M. Blanton and M. Aliasgari, "Analysis of Reusability of Secure Sketches and Fuzzy Extractors," IEEE Transactions on Information Forensics and Security, vol. 8, no. 9, pp. 1433–1455, 2013.

[48] A. Stoianov, "Security of Error Correcting Code for biometric Encryption," in 2010 Eighth Annual International Conference on Privacy Security and Trust (PST), 2010, pp. 231–235.

[49] A. Adler, "Vulnerabilities in Biometric Encryption Systems", in Audio- and video-based Biometric Person Authentication (AVBPA2005), Tarrytown, New York, USA. Lecture Notes in Computer Science: Springer, v. 3546, 2005, pp. 1100–1109.

[50] A. Stoianov, T. Kevenaar, and M. V. der Veen, "Security issues of bio-metric encryption," in IEEE TIC-STH Symp. on Information Assurance, Biometric Security and Business Continuity, Toronto, Canada, 2009.

[51] E. Maiorana, P. Campisi, and A. Neri, "User adaptive fuzzy commitment for signature templates protection and renewability," SPIE Journal of Electronic Imaging, vol. 17, no. 1, March 2008.

[52] C. Rathgeb and A. Uhl, "Statistical attack against iris-biometric fuzzy commitment schemes," in 2011 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2011, pp. 23 –30.

약 력

Andrew Beng Jin Teoh

1999 National University of Malaysia
2003 National University of Malaysia
2003~2008 Multimedia University Senior Lecturer
2008~2012 Yonsei Univesity Assistant Professor
2012~Present Yonsei Univesity Associate Professor
Research Interest: Biometrics, Machine Learning, Information Security

Jaihie Kim

1979년 연세대학교 공과대학 전자공학과 학사
1984년 Case Western Reserve University, Electrical Eng. 인공지능, 영상인식 박사
1984년~현재 연세대학교 전기전자공학부 교수
2002년~현재 생체인식연구센터 소장
관심분야: 생체인식, 패턴인식, 영상인식