An Information Theoretic Framework for Biometric Security Systems*

Lifeng Lai[1], Siu-Wai Ho[2], and H. Vincent Poor[1]

[1] Department of Electrical Engineering,
Princeton University, Princeton, NJ, 08512. USA
{llai,poor}@princeton.edu
[2] Department of Information Engineering,
The Chinese University of Hong Kong, Shatin, N.T., Hong Kong
swho@ie.cuhk.edu.hk

Abstract. An information theoretic framework is established to analyze the performance of biometric security systems. Two performance metrics, namely privacy, measured by the normalized equivocation rate of the biometric measurements, and security, measured by the rate of the key generated from the biometric measurements, are first defined. A fundamental tradeoff between these two metrics is then identified. The scenario in which a potential attacker does not have side information is considered first. The privacy-security region, which characterizes the above-noted tradeoff, is derived for this case. An important role of common information among random variables is revealed in perfect privacy biometric security systems. The scenario in which the attacker has side information is then considered. Inner and outer bounds on the privacy-security tradeoff are derived in this case.

Keywords: Biometric, Entropy, Mutual Information, Privacy, Security.

1 Introduction

Addressing reliability and privacy issues properly is important for the widespread application of biometric security systems. Due to measurement noise or other factors such as aging or injury, two measurements of the same biometric characteristics will not produce the same result. Hence, biometric measurements cannot be directly used for encryption in the same way that a secret key would typically be used. The issue of *privacy* arises from the fact that biometric characteristics are stored in a certain form in database, which creates a security threat. Unlike passwords, biometric characteristics cannot be changed. Hence, if the database is compromised, irreversible identity theft is possible.

In recent years, there has been increasing research interest in addressing these issues. A number of interesting approaches have been proposed (see, e.g., [1,2]

* This research was supported in part by the National Science Foundation under Grants CNS-06-25637 and CCF-07-28208.

M. Tistarelli and M.S. Nixon (Eds.): ICB 2009, LNCS 5558, pp. 879–888, 2009.

and [3] for overviews). The basic idea of these approaches is to generate a secret key and helper data during the initial enrollment stage. The key is used for encryption. The helper data is stored in the database. In the release stage, by combining the noisy measurements with the helper data, one can recover the key which is then used to decrypt the message. The helper data can be viewed as the parity-check bits of an error correcting code, and the effects of noise can be mitigated by such error correction. The existing approaches focus on maximizing the rate of the key that can be recovered successfully from the noisy measurements. This approach is motivated by the fact that in an encryption system, the equivocation of the encrypted message is limited by the entropy of the key [4]. From an information theoretic perspective, these existing approaches can be modelled as a problem of generating a secret key from common randomness [5], and hence the largest rate of the key can be characterized [6]. On the other hand, although the biometric measurements are not stored in the database in plain form, the helper data still contains information about the biometric measurements.

While the existing approaches maximize the key rate, they do not address the privacy issue adequately. In practice, the protection of the biometric measurements themselves is at least as important as maximizing the key rate. To increase the security level of the encrypted messages, we would like to make the key rate as large as possible. On the other hand, to preserve the privacy, we need to ensure that information leakage about the biometric measurements themselves is as small as possible. One question naturally arises: can we maximize the rate of the generated key while simultaneously minimizing the information leakage? In this paper, by establishing an information theoretic foundation[1] for biometric security systems, we show that there exists a fundamental tradeoff between security, measured by the rate of the generated key, and privacy, measured by the normalized equivocation of the biometric measurements, in any biometric security system. Thus, we cannot achieve both goals simultaneously. More specifically, we first rigorously formulate the privacy-security tradeoff in biometric security systems. We then identify and characterize this fundamental tradeoff for several different scenarios. In the first scenario, we require perfect security (rigorous definition will be given in the sequel) of the generated key. In this scenario, we consider two systems differentiated by whether the user is allowed to select the key or not. In each system, we characterize the security-privacy tradeoff. Furthermore, we propose schemes that fully achieve any particular point on the tradeoff curve. We show that the performance of the existing approach is one particular point on the derived tradeoff curve. We further show that the freedom of selecting a key does not affect the privacy-security tradeoff. In the second scenario, we require perfect privacy of the biometric measurements. We identify a close relationship between the common randomness between the biometric characteristics obtained during the enrollment and release stages and the rate of a secret key that can be generated. Finally, we study the scenario in which an attacker has side information about the biometric measurements. Again both types of systems are considered. Inner and outer bounds on the privacy-security

[1] Please refer to [7] for basic background on information theory.

region are derived for these situations. These bounds are shown to match under certain conditions of interest.

Due to space limitations, we include only the outline of the proofs of our results. Details of these proofs can be found in [8].

2 Model

We denote the biometric measurements taken during the enrollment stage by X^n and the biometric measurements taken during the verification stage by Y^n. Here, we assume that X^n and Y^n are sequences with length n taking values from n-fold product sets $\mathcal{X}^n$ and $\mathcal{Y}^n$, respectively. We assume that these measurements are generated according to a joint distribution $P_{X^nY^n}(x^n, y^n) = \prod_{i=1}^{n} P_{XY}(x_i, y_i)$. Specific models for the distribution of biometric measurements can be found, for example, in [9].

During the enrollment stage both the key K, ranging over $\mathcal{K}$, and the helper data V, ranging over $\mathcal{V}$, are generated. The key K is used to perform various tasks, such as message encryption. The helper data V is stored in the database to assist the recovery of the key from the noisy measurements Y^n during the release stage. Regarding the generation of key K, we consider two types of systems: namely non-randomized systems and randomized systems. In non-randomized systems, as shown in Figure 1 (a), both V and K are generated from X^n by functions h_n and $\tilde{h}_n$, respectively, so that $V = h_n(X^n)$ and $K = \tilde{h}_n(X^n)$. In randomized systems, a key K, which is independent with X^n, is randomly generated during the enrollment stage. Then V is generated from the randomly chosen key K and the biometric measurements X^n by a function h_n^* so that $V = h_n^*(X^n, K)$. The randomized system is illustrated in Figure 1 (b).

During the release stage, by providing the noisy measurement Y^n and data stored in the database V, we generate an estimate $\hat{K}$ of the key. Let g_n be the recovery function, and thus $\hat{K} = g_n(Y^n, V)$. In order to perform decryption, we require an arbitrarily small error probability during the key recovery stage.

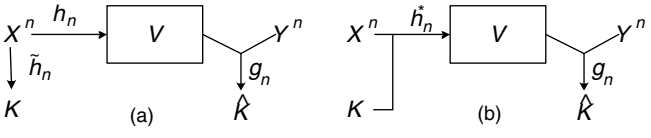

Fig. 1. Two different approaches for generating keys in biometric encryption systems: (a) a non-randomized approach; (b) a randomized approach

We first consider perfect security systems, in which we require that V does not contain any information about the generated key. More specifically we require that for every $\epsilon > 0$, $n^{-1}I(K;V) \leq \epsilon$ for sufficiently large n. Here $I(\cdot;\cdot)$ denotes

the mutual information between its two arguments. As mentioned before, the security level of the encrypted message is related to the rate of the generated key, and hence we measure the security level of the system by $R = n^{-1}H(K)$. Here $H(\cdot)$ denotes the entropy of its argument. The privacy of the biometric measurements is defined as the normalized equivocation rate $\Delta_P = H(X^n|V)/H(X^n)$. The larger this quantity, the greater the degree of privacy of the biometric measurements. If this quantity can be made arbitrarily close to 1, then we can achieve perfect privacy, which means that V does not leak any information about X^n, since $\Delta_P = 1$ implies $I(X^n; V) = 0$.

Definition 1 (perfect security system). *In a perfect security biometric encryption system, a privacy-security pair (Δ_P, R) is said to be achievable if, for each $\epsilon > 0$, there exist an integer n, coding functions, namely h_n and $\tilde{h}_n$ in non-randomized systems (i.e. $K = \tilde{h}_n(X^n)$, $V = h_n(X^n)$) and h_n^* in randomized systems (i.e., $V = h_n^*(X^n, K)$), and a decoding function, namely g_n (i.e., $\hat{K} = g_n(V, Y^n)$), satisfying the following conditions:*

$$n^{-1}H(K) \geq R, \tag{1}$$

$$H(X^n|V)/H(X^n) \geq \Delta_P, \tag{2}$$

$$n^{-1}I(V; K) \leq \epsilon, \tag{3}$$

$$\mathbb{P}[K \neq \hat{K}] \leq \epsilon \quad \textit{and} \tag{4}$$

$$n^{-1}\log|\mathcal{K}| \leq R + \epsilon. \tag{5}$$

Here, we offer some explanations of this definition. In this definition, (1) implies that the rate of the key should be larger than R; (2) implies that the privacy level of the system should be at least Δ_P; (3) says that the data stored in the database does not leak any information about the generated key; (4) implies that we can recover the key with high probability; and the combination of (1) and (5) says that the key is nearly uniformly generated.

For the second scenario, we consider a perfect privacy system, in which we require that the data stored in the database does not leak any information about the biometric measurements, that is for each $\epsilon > 0$, we require $I(X^n; V) \leq \epsilon$ for sufficiently large n. At the same time, we relax the requirement on the generated key, namely to allow $I(V; K)$ to range from 0 to $H(K)$. Of course, the smaller $I(V; K)$ the better. We measure the performance of a perfect privacy system by 1) the rate of the generated key $n^{-1}H(K)$, and 2) the normalized equivocation of the generated key $\Delta_s = H(K|V)/H(K)$. If $\Delta_s = 1$, we have $I(V; K) = 0$.

Definition 2 (perfect privacy system). *In a perfect privacy biometric security system, a rate-equivocation pair (R, Δ_s) is achievable if, for any $\epsilon > 0$, there exist an integer n, coding functions, namely h_n and $\tilde{h}_n$ in non-randomized systems (i.e. $K = \tilde{h}_n(X^n)$, $V = h_n(X^n)$) and h_n^* in randomized systems (i.e., $V = h_n^*(X^n, K)$), and a decoding function, namely g_n (i.e., $\hat{K} = g_n(V, Y^n)$), satisfying the following conditions:*

$$n^{-1}H(K) \geq R, \tag{6}$$

$$I(X^n;V) \le \epsilon, \tag{7}$$
$$H(K|V)/H(K) \ge \Delta_s, \tag{8}$$
$$\mathbb{P}[K \ne \hat{K}\} \le \epsilon \quad and \tag{9}$$
$$n^{-1}\log|\mathcal{K}| \le R + \epsilon. \tag{10}$$

Another situation of interest is that in which, besides the data V stored in the database, an attacker of the system has side-information about the biometric characteristics. This models the situation in which the attacker obtains side-information from other sources, such as biometric characteristics stored in other databases or biometric characteristics from the relatives of the user. We denote the side observation at the attacker by Z^n, ranging in the set $\mathcal{Z}^n$, and assume that it is correlated with (X^n, Y^n). Furthermore, we assume $P_{X^nY^nZ^n}(x^n, y^n, z^n) = \prod_{i=1}^{n} P_{XYZ}(x, y, z)$. Since the attacker has both V and Z^n, the privacy level is now measured as $H(X^n|VZ^n)/H(X^n)$, and the generated key is required to be independent of V and Z^n.

Definition 3 (side-information at attacker). *In a biometric system with side-information Z^n available to an attacker, a privacy-security pair (Δ_P, R) is said to be achievable if, for any $\epsilon > 0$, there exist an integer n, coding functions, namely h_n and $\tilde{h}_n$ in non-randomized systems (i.e. $K = \tilde{h}_n(X^n)$, $V = h_n(X^n)$) and h_n^* in randomized systems (i.e., $V = h_n^*(X^n, K)$), and a decoding function, namely g_n (i.e., $\hat{K} = g_n(V, Y^n)$), satisfying the following conditions:*

$$n^{-1}H(K) \ge R, \tag{11}$$
$$H(X^n|VZ^n)/H(X^n) \ge \Delta_P, \tag{12}$$
$$n^{-1}I(VZ^n;K) \le \epsilon, \tag{13}$$
$$\mathbb{P}[K \ne \hat{K}\} \le \epsilon \quad and \tag{14}$$
$$n^{-1}\log|\mathcal{K}| \le R + \epsilon. \tag{15}$$

3 Perfect Key Case

In this section, we study perfect security systems, in which the data stored in the database contains limited information about the generated key. Our goal is to characterize the relationship between the key size and the information leakage about the biometric measurements.

We first consider non-randomized systems. As discussed in Section 2, in a non-randomized system, both the key K and data V are generated from the biometric measurements X^n. Some existing schemes, for example, the secure sketch approach of [2] and the coding approach of [9], belong to this category. The theorem below establishes the performance limits of this type of biometric security system. The basic idea of the achievability scheme behind this theorem is to construct a compressed version U^n of X^n, and then generate the key K and helper data V as functions of U^n. Roughly speaking, we generate approximately $2^{nI(U:X)}$ U^n sequences. For each $x^n \in \mathcal{X}^n$, we find a u^n that is jointly

typical (in this paper, we use strong typicality defined in [7]) with x^n and assign this u^n as the compressed version of x^n. Since the number of X^n sequences is approximately $2^{nH(X)}$, which is larger than the number of U^n sequences in the codebook, each U^n will correspond to more than one X^n. We further reduce the information required to be stored in the database by using source coding with side-information [7], in which U^n is the source sequence at the encoder and Y^n is the side information present at the decoder. Roughly speaking, we divide all sequences U^n into approximately $2^{n(I(U;X)-I(U;Y))}$ bins, each containing approximately $2^{nI(U;Y)}$ sequences. Thus, each U^n sequence has two indices: a bin index and an index within each bin. We store the bin index in the database as helper data, and set the key value as the index of U^n within each bin. Hence, the rate of the key is approximately $I(U;Y)$. With the bin index and noisy measurements Y^n, we can recover U^n during the release stage with high probability. We can then further recover the key. Furthermore, it can be shown that the mutual information between the data stored in the database (i.e. the bin index) and the key (i.e. the index of the sequence within the bin) can be made arbitrarily small. Thus this scheme guarantees the perfect security of the generated key. By different choices of U, we control the leakage of information about the biometric measurements and the rate of the generated key. Furthermore, we are able to prove a converse result, and thus show that the above mentioned scheme is optimal.

Theorem 1. *Let $\mathcal{C}_N$ be the set of the privacy-security pairs (Δ_P, R) satisfying the following conditions:*

$$\Delta_P \leq 1 - \frac{I(U;X) - I(U;Y)}{H(X)} \quad \textit{and} \tag{16}$$

$$R \leq I(U;Y), \tag{17}$$

for some auxiliary random variable U such that (U, X, Y) satisfies the Markov chain condition $U \to X \to Y$. Then a privacy-security pair (Δ_P, R) is achievable if and only if $(\Delta_P, R) \in \mathcal{C}_N$.

We note that a similar scheme was used in [10] with a different purpose. From this theorem, we know that in order to maximize the rate of the key, we should set $U = X$. The rate of the key is then $I(X;Y)$. Correspondingly, the privacy level is $1 - H(X|Y)/H(X)$. This recovers the existing results of [11,12]. On the other hand, in order to achieve perfect privacy, the auxiliary random variable U in (16) should be chosen such that $I(U;X) = I(U;Y)$. The maximal rate achievable is then

$$\max_U I(U;Y) \quad s.t. \quad U \to X \to Y \quad \textit{and} \quad I(U;X) = I(U;Y). \tag{18}$$

In randomized systems, during the enrollment stage, users have the freedom to choose the values of the keys but they are not required to remember them. For example, the fuzzy vault scheme studied in [1] belongs to this category. Here, the key K can be viewed as a source of additional randomness. It is reasonable

to conjecture that this additional randomness could help in achieving better performance, at least for the privacy of the biometric measurements. The theorem below disproves this conjecture. The basic idea of the achievablity scheme is as follows. We first use the scheme in the proof of Theorem 1 to generate a key J, choosing from a set $\mathcal{J}$ with size $|\mathcal{J}|$. Then for a uniformly generated key K from a set $\mathcal{K}$, we store $J \oplus K$ in the database, along with other information required to be stored for the achievability scheme described above Theorem 1. Here $\oplus$ denotes mod-$|\mathcal{J}|$ addition. If we set $\mathcal{K} = \mathcal{J}$, $J \oplus K$ will be approximately uniformly distributed over $\mathcal{J}$, and is independent of other random variables of interest. Hence, this additional information stored in the database will not provide any information about the generated key and biometric measurements. In the release stage, we first obtain an estimate $\hat{J}$ of J using the same achievability scheme as that of Theorem 1. We then recover K via $J \oplus K \oplus \hat{J}$. Since $\hat{J} = J$ with high probability, $\hat{K}$ is equal to K with high probability. We show in the converse that the performance of the above mentioned scheme is optimal.

Theorem 2. *Let $\mathcal{C}_R$ be the set of the privacy-security pairs (Δ_P, R) satisfying the following conditions:*

$$\Delta_P \leq 1 - \frac{I(U;X) - I(U;Y)}{H(X)} \quad \textit{and} \tag{19}$$

$$R \leq I(U;Y), \tag{20}$$

for some auxiliary random variable U such that (U, X, Y) satisfies the Markov chain condition $U \to X \to Y$. Then a privacy-security pair (Δ_P, R) is achievable if and only if $(\Delta_P, R) \in \mathcal{C}_R$.

From here, we can see that $\mathcal{C}_N = \mathcal{C}_R$, and hence, the additional randomization does not increase the region. But one advantage of this randomized approach is that the system is revocable.

4 Perfect Privacy for Biometric Measurements

In this section, we consider the perfect privacy case. As discussed in Section 3, if we consider both perfect privacy and perfect secrecy, i.e. both $I(X^n;V)$ and $n^{-1}I(V;K)$ can be made arbitrarily small, the problem can be solved by looking for suitable auxiliary random variables U. Thus in this section we generalize the requirement on the generated key by allowing $I(V;K)$ to be nonzero, as specified in Definition 2.

First consider non-randomized systems, in which $H(K|X^n) = 0$ since K is a function of X^n. Thus in this case, $I(X^n;V) \leq \epsilon$ implies that $I(K;V) \leq \epsilon$. Hence in non-randomized systems, perfect privacy means perfect security. This case has been considered in Section 3. Therefore, it is sufficient to discuss only randomized systems in the remainder of this section.

In the following, we show a close relationship between perfect privacy and common random information, which is defined as follows.

Definition 4. *For two random processes X^n and Y^n, there exists a common random process between them with entropy rate not less than α if for each $\eta > 0$, there exist n and functions ψ_n of X^n and ϕ_n of Y^n such that*

$$\mathbb{P}[\psi_n(X^n) \neq \phi_n(Y^n)] \leq \eta \quad \textit{and} \tag{21}$$

$$n^{-1}H(\psi_n(X^n)) \geq \alpha - \eta. \tag{22}$$

This definition says that if X^n and Y^n have a common random process with entropy rate α, then one can generate two random variables: $\psi_n(X^n)$ solely based on X^n and $\phi_n(Y^n)$ solely based on Y^n, with the property that each of these two random variables has entropy $n\alpha$ and equals to the other one with high probability. Now, if there exists a common random process between the biometric measurements X^n and Y^n with entropy rate R, we can construct a system with perfect privacy. We first generate a random variable $J = \psi_n(X^n)$ during the enrollment stage, and store a function $f(K, J)$ in the database. Now, as long as $H(K) \geq nR$, there exists a function f such that $I(X^n; f(K, J)) = 0$, which means that there is no privacy leakage. During the release stage, based on the biometric measurements, we can first generate $\hat{J} = \phi_n(Y^n)$, and then recover the key K. Based on Definition 4, $\hat{J} = J$ with high probability, and hence $K = \hat{K}$ with high probability. The following theorem makes these ideas precise.

Theorem 3. *A privacy-rate pair (R, Δ_s) is achievable if and only if there exists a common random process between X^n and Y^n with entropy rate not less than $R\Delta_s$.*

5 Side-Information at an Attacker

In this section, we consider a situation in which, besides the data V stored in the database, an attacker has side-information about the biometric characteristics. This models the situation in which the attacker obtains side-information from other sources, such as biometric characteristics stored in other databases or biometric characteristics from the relatives of the user.

We first consider the non-randomized approach, in which both V and K are functions of the biometric measurements X^n, i.e., $V = h_n(X^n)$ and $K = \tilde{h}_n(X^n)$. We begin with a scheme that provides an inner bound on the set of all achievable privacy-security pairs. The basic idea is based on that of Theorem 1. We first generate a compressed version U^n of X^n, and then perform source coding with side information (U^n as the source sequence at the source coding encoder, and Y^n as the side information present at the decoder). That is we divide the U^ns into bins, and store the bin index in the database. In Theorem 1, we set the key value as the index of U^n in each bin. Now the attacker has additional information, the key rate should be reduced accordingly in order to guarantee that the attacker does not obtain any information about the generated key. We fulfill this goal by further partitioning each bin into subsets. We set the key value as the subset index. Using ideas from the analysis of the wiretap channel [13], it can

be shown that there exists a partition such that even with the side information at the attacker and bin index, the attacker will not be able to infer too much information about the generated key. We then characterize the privacy leakage of this scheme. With the bin index and noisy information Y^n, we can recover U^n, and then recover the key by looking at the subset index of the recovered sequence U^n. Using information inequalities, we also provide an upper bound on the performance achievable by any scheme.

Theorem 4. *Let $C_{s,in}$ be the set of (Δ_P, R) satisfying the following conditions:*

$$\Delta_P \leq 1 - \frac{I(X;UZ) - I(U;Y|W) + I(U;Z|W)}{H(X)} \quad \textit{and} \tag{23}$$

$$R \leq I(U;Y|W) - I(U;Z|W), \tag{24}$$

and $C_{s,out}$ be the set of (Δ_P, R) satisfying the following conditions:

$$\Delta_P \leq 1 - \frac{I(X;UZ) - I(U;Y) + I(U;Z|W)}{H(X)} \quad \textit{and} \tag{25}$$

$$R \leq I(U;Y|W) - I(U;Z|W), \tag{26}$$

in which W and U are auxiliary random variables such that (W, U, X, Y, Z) satisfies the following Markov chain condition $W \to U \to X \to (Y, Z)$. Any pair in $C_{s,in}$ is achievable, while any pair outside of $C_{s,out}$ is not achievable.

Now consider randomized systems, in which K is randomly generated and independent of X^n. The helper data V is a function of K and X^n; that is $V = h_n^*(K, X^n)$. An achievable region is described by the following scheme. The basic idea is to first generate a key J, choosing from a set $\mathcal{J}$ with size $|\mathcal{J}|$, using the scheme in the proof of Theorem 4. Then for a randomly generated key K, we store $J \oplus K$ in the database, along with other information required to be stored in Theorem 4. Here $\oplus$ denotes mod-$|\mathcal{J}|$ addition. If we set $\mathcal{K} = \mathcal{J}$, $J \oplus K$ will be approximately uniformly (these terms can be made rigorous, but these details are omitted here due to space limitations) distributed over $\mathcal{J}$, and is independent of other random variables of interest. In the release stage, we first obtain an estimate $\hat{J}$ of J using the same scheme as that of Theorem 4. We then recover K via $J \oplus K \oplus \hat{J}$. Since $\hat{J} = J$ with high probability, $\hat{K}$ is equal to K with high probability. Using information theoretic inequalities, we provide an upper-bound on the achievable privacy-security pairs.

Theorem 5. *Let $C_{sr,in}$ be the set of (Δ_P, R) pairs satisfying the following conditions:*

$$\Delta_P \leq 1 - \frac{I(X;UZ) - I(U;Y|W) + I(U;Z|W)}{H(X)} \quad \textit{and} \tag{27}$$

$$R \leq I(U;Y|W) - I(U;Z|W), \tag{28}$$

and let $C_{sr,out}$ be the set of (Δ_P, R) pair satisfying the following conditions:

$$\Delta_P \leq 1 - \frac{I(X;Z|U) - I(U;Y|W) + I(U;Z|W)}{H(X)} \quad \textit{and} \tag{29}$$

$$R \leq I(U;Y|W) - I(U;Z|W), \tag{30}$$

in which W and U are auxiliary random variables such that (W, U, X, Y, Z) satisfies the following Markov chain condition $W \to U \to X \to (Y, Z)$. Then any pair in $C_{sr,in}$ is achievable, while any pair outside of $C_{sr,out}$ is not achievable.

6 Conclusions

An information theoretic framework has been established to study the performance of biometric security systems. More specifically, biometric security systems have been studied under a privacy-security tradeoff framework. Two different scenarios, in which the attacker either has side-information about the biometric measurements or not, have been considered. In the scenario for which the attacker does not have side-information, we have considered two cases of perfect security and perfect privacy. In both cases, the complete privacy-security region has been identified. For the scenario in which the attacker has side-information about the biometric measurements, the perfect security case has been considered, for which inner and upper bounds on the privacy-security region have been derived.

References

1. Juels, A., Sudan, M.: A fuzzy vault scheme. In: Proc. IEEE Intl. Symposium on Information Theory, pp. 293–297 (2002)
2. Sutcu, Y., Li, Q., Memon, N.: Protecting biometric templates with sketch: Theory and practice. IEEE Trans. Inf. Forensics and Security 2, 503–512 (2007)
3. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP Journal on Advances in Signal Processing, 1–17 (2008)
4. Shannon, C.E.: Communication theory of secrecy systems. Bell System Technical Journal 28, 656–715 (1949)
5. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory 39, 733–742 (1993)
6. Tuyls, P., Goseling, J.: Biometric Authentication. Springer, Berlin (2004)
7. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley, New York (1991)
8. Lai, L., Ho, S.-W., Poor, H.V.: Privacy-security tradeoffs in biometric security systems. IEEE Trans. on Inf. Theory (submitted, 2008)
9. Draper, S., Khisti, A., Martinian, E., Vetro, A., Yedidia, J.: Using distributed source coding to secure fingerprint biometrics. In: Proc. IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing, pp. 129–132 (2007)
10. Csiszár, I., Narayan, P.: Common randomness and secret key generation with a helper. IEEE Trans. Inf. Theory 46, 344–366 (2000)
11. Cohen, G., Zemor, G.: The wire-tap channel applied to biometrics. In: Proc. IEEE Intl. Symposium on Information Theory and its Applications (2004)
12. Ignatenko, T., Willems, F.: On privacy in secure biometrics authentication systems. In: Proc. IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing, pp. 121–124 (2007)
13. Wyner, A.D.: The wire-tap channel. Bell System Technical Journal 54, 1355–1387 (1975)