Privacy–Security Trade-Offs in Biometric Security Systems—Part II: Multiple Use Case

Lifeng Lai, *Member, IEEE*, Siu-Wai Ho, *Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—This is the second part of a two-part paper on the information theoretic study of biometric security systems. In this paper, the performance of reusable biometric security systems, in which the same biometric information is reused in *multiple* locations, is analyzed. The scenario in which the subsystems are jointly designed is first considered. An outer bound on the achievable trade-off between the privacy leakage of the biometric measurements and rates of keys generated at the subsystems is derived. A scheme that achieves the derived outer bound is then presented. Next, an incremental design approach is studied, in which the biometric measurements are reused while keeping the existing system intact. An achievable privacy–security trade-off region for this design approach is derived. It is shown that under certain conditions, the incremental design approach can achieve the performance of the joint design approach. Finally, examples are given to illustrate the results derived.**

***Index Terms*—Biometric security, incremental design, joint design, privacy–security trade-off, reusable biometrics.**

I. Introduction

BIOMETRIC security systems have been widely implemented. The biometrics-integrated fingerprint system employed at the U.S.'s 50 busiest land ports of entry for homeland security purposes is a representative one. Another example is the biometric passport system, in which a traveller's biometric information is stored in a chip embedded in the traveller's passport.

In the traditional implementation, biometric measurements are stored in a database in plain form. This creates a serious security threat. For example, it has been shown that it is possible to recover fingerprints from minutiae points stored in a database [2]. Unlike passwords, biometric characteristics cannot be changed. Hence, if the database is compromised, identity theft is possible. In recent years, there has been increasing research interest in addressing the privacy issue in biometric security systems. Several interesting approaches have been proposed. For example, a secure sketch approach was studied in [3]–[5]. In the secure sketch approach, one stores a hash of the biometric information along with certain helper data that assists the recovery of biometric information from noisy observations during the release stage. Using results from error correction coding, [6]–[9] developed practical coding schemes for the secure sketch approach. In [10], an irreversible transformation technique was applied to the cancelable biometric scheme, in which an irreversible transformation of the biometric measurements is stored in the database [11]. The security weaknesses of the secure sketch approach were studied in [12]. On the other hand, the fuzzy vault scheme, in which keys are extracted from the biometric information and then used to encrypt secret information in the database, has been studied in [13]–[17]. The information theoretic analyses of these schemes are provided in [18]–[21]. The use of a cryptographic approach to protect the biometric template is studied in [22]. Developments in this area are summarized in [23] and [24]. Based on an information theoretic perspective, the basic idea of these approaches is to generate a secret key and helper data during an initial enrollment stage. A hash of the key is stored in the database for authentication purposes. The helper data is stored in the database to assist key recovery during the release stage. Although the biometric measurements are not stored in the database in plain form anymore, the helper data stored in the database still contains certain information about the biometric measurements. To increase the security level of the biometric security system, we would like to make the key rate as large as possible. On the other hand, to preserve privacy, we need to ensure that information leakage about the biometric measurements themselves is as small as possible. In the first part of this two-part paper [25], by establishing an information theoretic foundation for biometric security systems, we characterize the fundamental trade-off between security and privacy in any biometric security system. The larger the key rate we aim for, the larger the privacy leakage we must accept. Here, we note that similar analysis was also independently presented in [26] and [27].

In this paper, we extend our analysis in [25], [28], and [29] to reusable biometric security systems, in which the same biometric information is used in *multiple* different locations. This is motivated by the fact that our biometric measurements are usually used in several systems. For example, our biometric measurements may be used not only in the biometric passport system but also in government databases for homeland security purposes. It is conceivable that an attacker will try to combine the data stored in different databases to gain information about either the biometric measurements or the generated keys. In this paper, we first consider a joint design approach. We derive an outer-bound on the achievable trade-off between the privacy

Manuscript received April 15, 2010; revised November 23, 2010; accepted December 04, 2010. Date of publication December 10, 2010; date of current version February 16, 2011. This work was supported in part by the National Science Foundation under Grant CCF-07-28208, Grant CNS-09-05398, and Grant CCF-10-16671, and in part by the Australian Research Council under an Australian Postdoctoral Fellowship. Some of the results in this paper were presented at the 35th International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Dallas, TX, March 14–19, 2010. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Arun Ross.

L. Lai is with the Department of Systems Engineering, University of Arkansas, Little Rock, AR 72204 USA (e-mail: lxlai@ualr.edu).

S.-W. Ho is with the Institute for Telecommunications Research, University of South Australia, Adelaide SA 5095, Australia (e-mail: SiuWai.Ho@unisa.edu.au).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

Digital Object Identifier 10.1109/TIFS.2010.2098873

level and the key rates of a jointly designed biometric system. We further design a scheme that achieves this outer bound. Next, for practical considerations, we study an incremental design approach. In the incremental design approach, we consider a situation in which there exists a legacy biometric security system. For cost considerations or backward compatibility, it is desirable to keep the legacy system intact when we reuse the biometric information. For this scenario, we provide a scheme that can reuse the biometric information without affecting the legacy system. The performance of this design approach is then analyzed. We also derive conditions under which the performance of the incremental design approach is the same as that of the joint design approach. This paper focuses only on deriving theoretical bounds. However, coupled with recent developments in the design of practical distributed source coding algorithms [30], [31], the achievable schemes presented in the paper do provide some valuable insights for the design of practical systems. One can adopt these practical codes to our setup. One potential challenge is that the length of biometric measurement is limited. In addition, this paper focuses on the information theoretic security analysis. This is different from another important line of work that focuses on cryptographic aspects of biometric security systems [10]–[12].

The rest of the paper is organized as follows. In Section II, we introduce our system model and notation. In Section III, we briefly review our results for the single-key system. Next, we derive an optimal security–privacy trade-off of the reusable biometric system achieved by a joint design in Section IV. We present our result for the incremental design approach in Section V. We then give an example in Section VI to illustrate the results obtained in this paper. Finally, in Section VII, we offer some concluding remarks.

II. Model

We denote the biometric measurements sampled during the enrollment stage for system j by X_j^n and the biometric measurements sampled during the verification stage for system j by Y_j^n. Here, we assume that X_j^n and Y_j^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 same joint distribution $P_{X^nY^n}(x^n, y^n)$, i.e.,

$$P_{X_j^nY_j^n}\left(x_j^n, y_j^n\right) = P_{X^nY^n}(x^n, y^n) = \prod_{i=1}^{n} P_{XY}(x_i, y_i).$$

Specific models for the distribution of the biometric measurements X, Y can be found, for example, in [6] or [32]. It is easy to see that the case with $X_1^n = X_2^n = X^n$ is the worst case scenario in the sense that it is the easiest for the attacker to learn the biometric information. Furthermore, one can use the generic notation Y^n to denote Y_1^n and Y_2^n since they have the same distribution. Hence in the paper, we will use only X^n to denote the biometric measurement during the enrollment stage (worst case scenario) and Y^n to denote the biometric measurement during the release stage (with the understanding that Y^n represents Y_j^n for system j).

We discuss the case in which the biometric measurements are used in two systems in detail. The results can be generalized to the scenario in which the biometric measurements are reused more than two times. During the enrollment stage, a key K_1 ranging in $\mathcal{K}_1$ and helper data V_1 ranging in $\mathcal{V}_1$ are generated for system one. A key K_2 ranging in $\mathcal{K}_2$ and helper data V_2 ranging in $\mathcal{V}_2$ are generated for system two. The helper data V_j, $j = 1, 2$, are stored in the database to assist the recovery of the respective key K_j, $j = 1, 2$, from the noisy measurements Y^n during the release stage. Regarding the generation of the key K_j, we consider two types of systems: namely nonrandomized systems and randomized systems. In the nonrandomized systems, V_j and K_j are generated from X^n by functions h_j and $\tilde{h}_j$, respectively, so that $V_j = h_j(X^n)$ and $K_j = \tilde{h}_j(X^n)$. In the randomized systems, a key K_j, which is independent with X^n, is randomly generated during the enrollment stage. Then V_j is generated from the randomly chosen key K_j and the biometric measurements X^n by a function h_j^* so that $V_j = h_j^*(X^n, K_j)$.

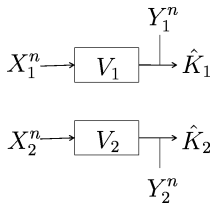


Fig. 1. Reusable biometric system when the biometric information is used in two separate subsystems.

During the release stage, by providing the noisy measurement Y^n and data stored in the database V_j, we generate an estimate $\hat{K}_j$ of the key. Let g_j be the recovery function, and thus $\hat{K}_j = g_j(Y^n, V_j)$. In order to perform authentication, we require an arbitrarily small error probability during the key recovery stage. Fig. 1 shows the biometric security system when the biometric information is used in two different subsystems.

We consider perfect key protection systems, in which we require that V_j does not contain any information about the generated key K_j. More specifically, in the two-key setup, we require that $n^{-1}I(K_1, K_2; V_1, V_2) \leq \epsilon$, since the attacker has the potential to access both sets of helper data. We further assume that systems generate keys independently, so that $n^{-1}I(K_1; K_2) \leq \epsilon$. This requirement guarantees that even if the attacker breaks one of the systems, the other system is still secure. The privacy of the biometric measurements is defined as the normalized equivocation rate $\Delta_{P,M} = H(X^n \,|\, V_1, V_2)/H(X^n)$, since both V_1 and V_2 are related to X^n. The larger this quantity, the greater the degree of privacy of the biometric measurements after the attacker accesses the data stored in both systems. If this quantity can be made arbitrarily close to 1, then we can achieve perfect privacy, which means that (V_1, V_2) does not leak any information about X^n, since $\Delta_{P,M} = 1$ implies $I(X^n; V_1, V_2) = 0$.

Definition 1: In a two-key biometric system with perfect key protection, a privacy–security triple $(\Delta_{P,M}, R_1, R_2)$ is said to be achievable, if for each $\epsilon > 0$, there exist an integer n, coding functions, namely h_j and $\tilde{h}_j$ in the nonrandomized systems (i.e., $K_j = \tilde{h}_j(X^n)$, $V_j = h_j(X^n)$) and h_j^* in the randomized systems (i.e., $V_j = h_j^*(X^n, K_j)$), and a decoding function, namely

g_j (i.e., $\hat{K}_j = g_j(V_j, Y^n)$), for $j = 1,2$, satisfying the following conditions:

$$n^{-1}H(K_j) \geq R_j \tag{1}$$

$$n^{-1}I(K_1; K_2) \leq \epsilon \tag{2}$$

$$H(X^n \,|\, V_1, V_2)/H(X^n) \geq \Delta_{P,M} \tag{3}$$

$$n^{-1}I(V_1, V_2; K_1, K_2) \leq \epsilon \tag{4}$$

and

$$\mathbb{P}[K_j \neq \hat{K}_j] \leq \epsilon. \tag{5}$$

III. Review of Single-Key Systems

To make this paper relatively self-contained, we first review results obtained in the first part of this paper [25] regarding the performance limits of single-key biometric security systems. The following proposition specifies the privacy–security pairs achievable in a single-key system by using either the randomized or the nonrandomized approaches.

Proposition 1 ([25]): Let $\mathcal{C}_1$ be the set of privacy–security pairs (Δ_P, R) satisfying the following conditions:

$$\Delta_P \leq 1 - \frac{I(U;X) - I(U;Y)}{H(X)} \tag{6}$$

and

$$R \leq I(U;Y) \tag{7}$$

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

The basic idea of achieving this region using the nonrandomized approach 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 with x^n and assign this u^n as the compressed version of x^n. We further reduce the information required to be stored in the database by using source coding with side-information [33], in which U^n serves as the source sequence at the encoder and Y^n serves as the side information present at the decoder. Roughly speaking, we divide these $2^{nI(U:X)}$ U^n sequences 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 its bin. We store the bin index in the database as the helper data, and set the key value as the index of U^n in each bin. Hence, the rate of the key is approximately $I(U;Y)$. The encoding process is illustrated in Fig. 2. 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 protection 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.

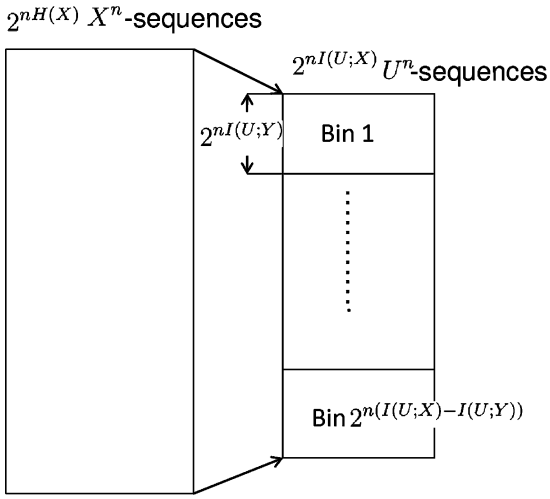


Fig. 2. Sketch of the coding scheme for single key systems: the bin index is the helper data; the index within each bin is the key value.

To achieve this region using the randomized approach, during the enrollment stage, we first use the scheme in the nonrandomized approach to generate a key Q, choosing from a set $\mathcal{Q}$ with size $|\mathcal{Q}|$. Then for a key K uniformly generated from a set $\mathcal{K}$, we store $Q \oplus K$ in the database, along with other information required to be stored in the nonrandomized scheme. Here $\oplus$ denotes mod-$|\mathcal{Q}|$ addition. If we set $\mathcal{K} = \mathcal{Q}$, $Q \oplus K$ will be approximately uniformly distributed over $\mathcal{Q}$ (please refer to [25] for rigorous meaning of these terms), 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 $\hat{Q}$ of Q using the same scheme as that of the nonrandomized system. We then recover K via $Q \oplus K \oplus \hat{Q}$. Since $\hat{Q} = Q$ with high probability, $\hat{K}$ is equal to K with high probability.

IV. Joint Design

In this section, we consider the situation in which we can design the two subsystems jointly by taking the security requirements specified in Definition 1 into consideration. We derive an outer-bound on the privacy–security trade-off of this joint design approach. We also present a scheme that achieves this outer-bound.

The following theorem characterizes the performance limits of the nonrandomized approach using a joint design.

Theorem 1: Let $\mathcal{C}_2$ be the set of privacy–security triples $(\Delta_{P,2}, R_1, R_2)$ satisfying the following conditions:

$$\Delta_{P,2} \leq 1 - \frac{I(U;X) - I(U;Y)}{H(X)} \tag{8}$$

and

$$R_1 + R_2 \leq I(U;Y) \tag{9}$$

for some auxiliary random variable U such that (U, X, Y) satisfies the Markov chain condition $U \rightarrow X \rightarrow Y$. Then a privacy–security triple $(\Delta_{P,2}, R_1, R_2)$ is achievable using the nonrandomized approach, if and only if $(\Delta_{P,2}, R_1, R_2) \in \mathcal{C}_2$.

Proof: (Outline) The basic idea to achieve this region is first to generate a key using the scheme in Proposition 1, then to

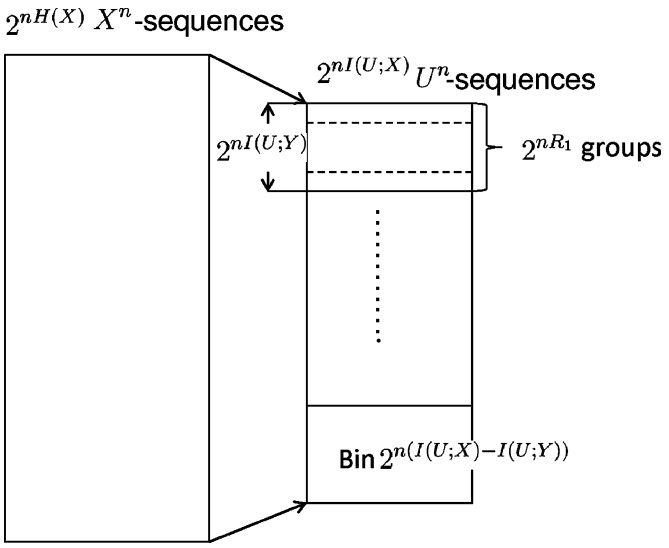


Fig. 3. Sketch of the coding scheme of the joint design approach: the bin index is the helper data, the group index is the key for the first system, and the index within each group is the key for the second system.

divide this key into two parts, one for each subsystem. A sketch of the coding scheme is shown in Fig. 3. We also provide converse proof showing that the privacy–security region achieved by this scheme is optimal. Please refer to Appendix A for details. ■

Similar to the single-key system, we can also achieve the same region using the randomized approach, in which the key in each system is randomly generated and is independent of the biometric measurements.

Theorem 2: Let $\mathcal{C}_{2R}$ be the set of privacy–security triples $(\Delta_{P,2R}, R_1, R_2)$ satisfying the following conditions:

$$\Delta_{P,2R} \leq 1 - \frac{I(U;X) - I(U;Y)}{H(X)} \tag{10}$$

and

$$R_1 + R_2 \leq I(U;Y) \tag{11}$$

for some auxiliary random variable U such that (U, X, Y) satisfies the Markov chain condition $U \rightarrow X \rightarrow Y$. Then a privacy–security triple $(\Delta_{P,2R}, R_1, R_2)$ is achievable using the randomized approach, if $(\Delta_{P,2R}, R_1, R_2) \in \mathcal{C}_{2R}$.

Proof: (Sketch) We first use the scheme in the nonrandomized approach to generate a key Q_j for system j (choosing from a set $\mathcal{Q}_j$ with size $|\mathcal{Q}_j|$) during the enrollment stage. Then for a uniformly generated key K_j from a set $\mathcal{K}_j$, we store $Q_j \oplus K_j$ in the database, along with other information required to be stored in the nonrandomized scheme. Here $\oplus$ denotes mod-$|\mathcal{Q}_j|$ addition. If we set $\mathcal{K}_j = \mathcal{Q}_j$, $Q_j \oplus K_j$ will be approximately uniformly distributed over $\mathcal{Q}_j$, 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 the biometric measurements. In the release stage, we first obtain an estimate $\hat{Q}_j$ of Q_j using the same scheme as that of the nonrandomized system. We then recover K_j via $Q_j \oplus K_j \oplus \hat{Q}_j$. Since $\hat{Q}_j = Q_j$ with high probability, K_j is equal to K_j with high probability. The detailed proof is omitted for conciseness. ■

The above results can be easily generalized to the scenario in which the biometric measurements are used more than twice. The following result characterizes the corresponding result.

Theorem 3: Let $\mathcal{C}_N$ be the set of privacy–security $N+1$-tuples $(\Delta_{P,N}, R_1, \ldots, R_N)$ satisfying the following conditions:

$$\Delta_{P,N} \leq 1 - \frac{I(U;X) - I(U;Y)}{H(X)} \tag{12}$$

and

$$\sum_{t=1}^{N} R_t \leq I(U;Y) \tag{13}$$

for some auxiliary random variable U such that (U, X, Y) satisfies the Markov chain condition $U \rightarrow X \rightarrow Y$. Then $(\Delta_{P,N}, R_1, \ldots, R_N)$ is achievable using either the randomized or nonrandomized approach in N-key biometric security systems, if and only if $(\Delta_{P,N}, R_1, \ldots, R_N) \in \mathcal{C}_N$.

Proof: (Outline) The basic idea to achieve this region is same as that of Theorem 1. That is we first generate a key using the scheme in Proposition 1, then to divide this key into N nonoverlapping parts, one for each subsystem. The proof is an extension of the proof of Theorem 1. It is omitted for brevity. ■

V. Incremental Design

The scheme that achieves the bound specified in Theorem 1 requires us to design two systems jointly. In certain scenarios, there already exists a legacy system. When we try to reuse the biometric measurements, we are not allowed to modify the legacy system (due, for example, to cost considerations or backward compatibility issue, etc.). Thus the joint design approach is not applicable for this situation. Now, the question is whether we can reuse the biometric information without any modifications of the legacy system while satisfying the conditions specified in Definition 1 or not.

Specifically, we assume that we have an existing system operating at point (Δ_P, R_1):

$$\begin{aligned} \Delta_P &= 1 - \frac{I(U_1;X) - I(U_1;Y)}{H(X)} \\ R_1 &= I(U_1;Y) \end{aligned} \tag{14}$$

for an auxiliary random variable U_1 that satisfies $U_1 \rightarrow X \rightarrow Y$. That is, in the existing system, we generate a key K_1 with rate R_1 from X^n, and store helper data V_1 in the database. Now, we want to reuse the biometric information to build another system while keeping the existing system intact. That is, we want to generate another key K_2 and helper data V_2 from X^n. And we use K_2 to secure the second system while storing V_2 in the database of the second system as helper data. Of course, now the attacker has access to both V_1 and V_2, and hence the privacy level of the biometric system will be reduced. The challenge is to satisfy other conditions specified in Definition 1, that is we need to guarantee that the newly generated key K_2 is independent of K_1, and the newly generated helper V_2 does not leak any information about K_1. Furthermore, we require that the attacker does not gain any information about K_1 and K_2 by combining V_1 and V_2. As discussed in Section IV, if we can make modifications to the legacy system, this can be done. The additional constraint that we cannot change the legacy system makes the problem more challenging. The following theorem shows an

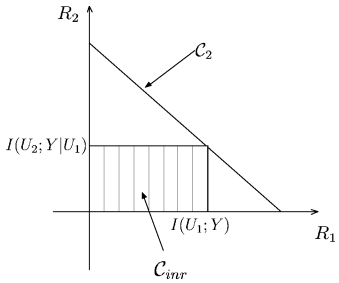


Fig. 4. Comparison of the performance achieved by the joint design approach and the incremental design approach.

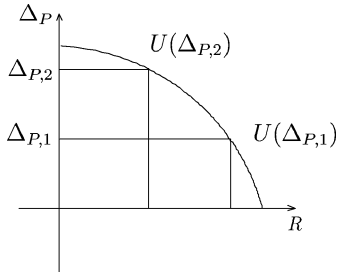


Fig. 5. Region $\mathcal{C}_1$ with an illustration of Δ_P and $U(\Delta_P)$.

achievable performance for the situation in which we keep the legacy system intact. To explain the basic idea behind this result, one can think of U_1^n as a projection of X^n onto a certain subspace. The basic idea is generate the key K_2 in the subspace orthogonal to the subspace in which U_1^n lies.

Theorem 4: If there is a legacy system operating at the point specified in (14), let $\mathcal{C}_{inr}$ be the set of privacy–security triples $(\Delta_{P,inr}, R_1, R_2)$ satisfying the following conditions:

$$\Delta_{P,inr} \le 1 - \frac{I(U_2;X) - I(U_2;Y)}{H(X)} \tag{15}$$

$$R_1 \le I(U_1;Y) \tag{16}$$

and

$$R_2 \le I(U_2;Y|U_1) \tag{17}$$

for an auxiliary random variable U_2 satisfying the following Markov chain condition:

$$U_1 \to U_2 \to X \to Y. \tag{18}$$

Then any triple $(\Delta_{P,inr}, R_1, R_2) \in \mathcal{C}_{inr}$ is achievable.

Proof: Please refer to Appendix B. ■

Remark 1: Similar to the joint design approach, the region in Theorem 4 can also be achieved using the randomization approach.

If we add R_1 and R_2 in (16) and (17), we have

$$\begin{aligned} R_1 + R_2 &= I(U_1;Y) + I(U_2;Y\,|\,U_1) \\ &= I(U_1U_2;Y) = I(U_2;Y) \end{aligned} \tag{19}$$

in which the last equality is due to the Markov chain relationship $U_1 \to U_2 \to Y$. Comparing (19) with (9), we see that the incremental approach achieves the sum rate that can be achieved using the joint design approach as specified in Theorem 1. On the other hand, this does not imply that the incremental design approach can achieve the same performance as that of the joint design approach. Compared with Theorem 1, we have three additional constraints, namely (16), (17), and the Markov chain relationship (18) in Theorem 4. Thus $\mathcal{C}_{inr}$ is a subset of $\mathcal{C}_2$. Fig. 4 illustrates a two-dimensional facet of the three-dimensional regions $\mathcal{C}_2$ and $\mathcal{C}_{inr}$ when we set both $\Delta_{P,2}$ and $\Delta_{P,inr}$ to be Δ.

We note that the region $\mathcal{C}_{inr}$ depends on the design of the legacy system, and more specifically depends on the choice of U_1. As discussed above, for each particular value of U_1, the region $\mathcal{C}_{inr}$ is a subset of $\mathcal{C}_2$. Let $\mathcal{C}_u$ be $\bigcup_{U_1} \mathcal{C}_{inr}$, that is $\mathcal{C}_u$ is the union of the triples that can be achieved using the incremental design approach for different choices of U_1. Obviously $\mathcal{C}_u \subseteq \mathcal{C}_2$; the question now is under what conditions are these two regions the same? To answer this question, we need to examine the boundary points of the region specified in Theorem 1, that is the boundary points of $\mathcal{C}_1$. Note that $\mathcal{C}_1$ is a two-dimensional region, which we show in Fig. 5. From Theorem 1, we know that for any predetermined privacy level Δ_P, the maximum key rate is given by

$$\begin{aligned} R = &\max_{P_{U\,|\,X}(u\,|\,x)} I(U;Y) \\ \text{s.t.}\quad &1 - \frac{I(U;X) - I(U;Y)}{H(X)} \le \Delta_P. \end{aligned} \tag{20}$$

For a different privacy level, the auxiliary random variable that solves the optimization problem in (20) is different. We use $U(\Delta_P)$ to denote the random variable that is optimal for privacy level Δ_P. We have the following result.

Corollary 1: If for any $\Delta_{P,1} < \Delta_{P,2}$, we have $U(\Delta_{P,2}) \to U(\Delta_{P,1}) \to X$, then $\mathcal{C}_u = \mathcal{C}_2$.

Proof: It is sufficient to show that under this condition $\mathcal{C}_2 \subseteq \mathcal{C}_u$. Let (Δ_P, R_1, R_2) be a point on the boundary of $\mathcal{C}_2$, with $U(\Delta_P)$ being the auxiliary random variable that achieves this point. That is, $R_1 + R_2 = I(U(\Delta_P);Y)$ and $\Delta_P = 1 - (I(U(\Delta_P);X) - I(U(\Delta_P);Y))/H(X)$. We show that there exist auxiliary random variables U_1 and U_2 such that $U_1 \to U_2 \to X \to Y$, $R_1 = I(U_1;Y)$, $R_2 = I(U_2;Y\,|\,U_1)$, and $\Delta_P = 1 - (I(U_2;X) - I(U_2;Y))/H(X) = 1 - (I(U(\Delta_P);X) - I(U(\Delta_P);Y))/H(X)$; that is $(\Delta_P, R_1, R_2) \in \mathcal{C}_u$.

First, we set U_2 to be $U(\Delta_P)$. We find U_1 using the following procedure. We increase Δ_P to $\Delta_{P,1}$, so that the solution to the problem

$$\begin{aligned} R = &\max I(U;Y) \\ \text{s.t.}\quad &1 - \frac{I(U;X) - I(U;Y)}{H(X)} \le \Delta_{P,1} \end{aligned} \tag{21}$$

is R_1. That is $I(U(\Delta_{P,1});Y) = R_1$ and $1 - (I(U(\Delta_{P,1});X) - I(U(\Delta_{P,1});Y))/(H(X)) \le \Delta_{P,1}$. Then we set U_1 to be $U(\Delta_{P,1})$.

Since $\Delta_{P,1} \ge \Delta_P$, from the assumption of the corollary, we have that $U_1 \to U_2 \to X$. Then from Theorem 5, we know that $(\Delta_P, R_1, R_2) \in \mathcal{C}_{inr}$ for this particular U_1, and hence $(\Delta_P, R_1, R_2) \in \mathcal{C}_u$, which implies that $\mathcal{C}_u = \mathcal{C}_2$. ■

The scheme developed in the Proof of Theorem 1 can also be generalized to the situation in which one will reuse the biometric information N times. The following theorem specifies the performance that one can achieve by the incremental design

approach. More specifically, we assume that we have a legacy system operating at the point as specified in (14). Now, we design system 2 without changing the legacy system. Later on, we need to reuse the biometric information, and hence, we design system 3 without changing the legacy system and system 2. More generally, when we design system i, we do not make any changes to systems designed before.

Theorem 5:

$$\begin{aligned}\Delta_{P,M} &\le 1 - \frac{I(U_N;X) - I(U_N;Y)}{H(X)}\\ R_1 &\le I(U_1;Y)\\ &\vdots\\ R_i &\le I(U_i;Y\,|\,U_1,\ldots,U_{i-1})\\ &\vdots\\ R_N &\le I(U_N;Y\,|\,U_1,\ldots,U_{N-1})\end{aligned}$$

with $U_1 \to U_2 \to \cdots \to U_N \to X \to Y$.

Proof: The proof follows the same steps as that of Theorem 4. ∎

Remark 2: We have

$$\begin{aligned}\sum_{i=1}^{N} R_i &= I(U_1;Y) + I(U_2;Y\,|\,U_2) + \cdots\\ &\quad + I(U_N;Y|U_1,\ldots,U_{N_1})\\ &= I(U_N;Y). \end{aligned} \tag{22}$$

Thus, as in the two keys case, we achieve the sum rate point achieved by the joint design approach.

VI. Example

Here, we give an example to illustrate the results in the paper. We consider the doubly symmetric binary source. In the doubly symmetric binary source, $\mathcal{X} = \mathcal{Y} = \{0,1\}$, $P(X=0) = 1/2$, and $Y = X \oplus N$, in which N is a Bernoulli random variable with $P(N=1) = p < 1/2$ and is independent of other random variables of interest.

We first examine the region $\mathcal{C}_1$ specified in Theorem 1. Since $H(X) = H(Y) = 1$, the region $\mathcal{C}_1$ is the same as

$$\Delta_P \le 1 - H(Y\,|\,U) + H(X\,|\,U) \tag{23}$$

$$R \le 1 - H(Y\,|\,U). \tag{24}$$

From Corollary 4 of [34], we know that if $H(X\,|\,U) = h(q)$ for some parameter $0 \le q \le 1/2$ with $h(q) = -q\log q - (1-q)\log(1-q)$, then $H(Y\,|\,U) \ge h(p*q)$, in which $a*b = a(1-b) + b(1-a)$. The equality is achieved when (U,X) is another doubly symmetric binary source with $P(U=X) = q$. Hence, $\mathcal{C}_1$ is further simplified to

$$\begin{cases}\Delta_P \le 1 - h(p*q) + h(q)\\ R \le 1 - h(p*q)\end{cases} \tag{25}$$

for $0 \le q \le 1/2$. From here, we know that any point on the boundary of $\mathcal{C}_1$ can be achieved using a binary auxiliary random variable U that can be parameterized by $0 \le q \le 1$ with $P(U = X) = q$. By changing the value of q, we obtain different points on the boundary.

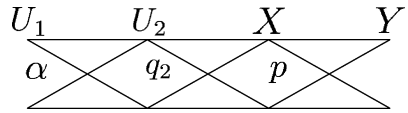


Fig. 6. Relations among U_2, U_1, X, and Y.

From Theorem 1, we know that $\mathcal{C}_2$ is characterized by

$$\begin{cases}\Delta_{P,2} \le 1 - h(p*q) + h(q)\\ R_1 + R_2 \le 1 - h(p*q)\end{cases} \tag{26}$$

for $0 \le q \le 1/2$.

We now show that the conditions in Corollary 1 are satisfied for the doubly symmetric binary source. And as a result, we have $\mathcal{C}_u = \mathcal{C}_2$. We define $f(q) = 1 - h(p*q) + h(q)$. Suppose $\Delta_{P,1} < \Delta_{P,2}$, let $q_1 = f^{-1}(\Delta_{P,1})$, and $q_2 = f^{-1}(\Delta_{P,2})$. Then the random variable U_1 that achieves the privacy level $\Delta_{P,1}$ while maximizing the key rate is a binary random variable with $P(U_1 = 1\,|\,X) = q_1$. Similarly, the random variable U_2 that achieves the privacy level $\Delta_{P,2}$ while maximizing the key rate is a binary random variable with $P(U_2 = 1\,|\,X) = q_2$. We also have $q_1 > q_2$. We can then find a parameter α, such that $q_1 = q_2(1-\alpha) + (1-q_2)\alpha$. That is we can find U_1 and U_2 such that $U_1 \to U_2 \to X$. Hence, the conditions specified in Corollary 1 are satisfied. The relationships among U_2, U_1, X and Y are shown in Fig. 6.

VII. Conclusion

Reusable biometric security systems, in which the same biometric information is reused for several systems, have been studied under a privacy–security trade-off framework. We have derived an outer bound on the trade-off among the rates of the generated keys and the level of privacy leakage for a joint design. We have further designed a scheme that achieves the derived bound. We have also considered the situation in which we are required to keep a legacy system intact, and we have designed a system that satisfies this requirement. We have also examined conditions under which the incremental design approach can achieve the performance of the joint design approach. For future work, it is of interest to design practical codes that achieve the derived theoretical bounds. It is also of interest to consider other performance metrics such as false accept rate (FAR) and false reject rate (FRR), which have been studied for the single-use case, in the multiple-use context. In addition, the design of schemes that combine benefits of both the information theoretic and computational security notions is of practical significance.

Appendix A
Proof of Theorem 1

A. Achievability

Here we show that for any auxiliary random variable U with $U \to X \to Y$, and any $\epsilon_1 > 0$, any triple $(\Delta_{P,M}, R_1, R_2)$ with

$$\Delta_{P,M} = 1 - \frac{I(U;X) - I(U;Y)}{H(X)} - \epsilon_1$$

and

$$R_1 + R_2 = I(U;Y) - \epsilon_1 \tag{27}$$

is achievable. That is, any triple in the region $\mathcal{C}_M$ is achievable.

For a given joint distribution $P_{UXY}(u,x,y) = P_{U|X}(u|x)P_{XY}(xy)$, we use a modification of a scheme used in the first part of this two-part paper [25] to achieve the promised performance.

1) Code Construction: Fix $\gamma > 0$ and $\eta > 0$, and let $\xi = \eta/3$. Randomly select $M = 2^{n(I(U;X)+\gamma)}$ sequences U^n from $T^n_{[U],\xi|\mathcal{X}|}$,[1] and divide them into $2^{n(I(U;X)-I(U;Y)+\gamma+\eta)}$ bins so that each bin contains $2^{n(I(U;Y)-\eta)}$ typical sequences. We further divide each bin into 2^{nR_1} subgroups, so that each subgroup has $2^{n(I(U;Y)-R_1-\eta)}$ typical sequences. We use L to denote the bin index, and hence L ranges in $\{1,\ldots,2^{n(I(U;X)-I(U;Y)+\gamma+\eta)}\}$. We use K_1, which ranges in $\{1,\ldots,2^{nR_1}\}$, to denote the index of the subgroup in which the sequence lies. We further use K_2, which ranges up to $2^{n(I(U;Y)-R_1-\eta)}$, to denote the index of the sequence within each subgroup.[2] Denote the set of these M sequences by $\mathcal{M}$. From the construction above, we can see that each sequence $u^n \in \mathcal{M}$ is uniquely identified by three indices $(l(u^n), k_1(u^n), k_2(u^n))$.

2) Enrollment Stage: For each $x^n \in \mathcal{X}^n$, we associate a sequence $u^n \in \mathcal{M}$ with it by the following procedure. First, we find a list of sequences in $\mathcal{M}$ that are jointly typical with x^n. If there is more than one sequence in the list, we set u^n to be the one with the smallest index (we first compare the bin indices and if there is a tie, we then compare the subgroup index within the bin; if there is again a tie, we then compare the index within the subgroup). If no such sequence exists, we set u^n to be the sequence with index $(l=1,k_1=1,k_2=1)$. Using this procedure, we associate every $x^n \in \mathcal{X}^n$ with a sequence $u^n \in \mathcal{M}$. We then store the bin index $l(u^n)$ in the database of both systems. We set the key value of system 1 as the subgroup index $k_1(u^n)$, and set the key value of system 2 as the index $k_2(u^n)$. Hence, in our scheme, $V_1 = V_2 = L$, $\mathcal{K}_1 = \{1,\ldots,2^{nR_1}\}$, and $\mathcal{K}_2 = \{1,\ldots,2^{n(I(U;Y)-R_1-\eta)}\}$. It then follows that

$$n^{-1}(\log|\mathcal{K}_1| + \log|\mathcal{K}_2|) \le I(U;Y) - \eta. \tag{28}$$

3) Release Stage: With the noisy measurement y^n, and the bin index l stored in each database, we obtain an estimate $\hat{k}_j$ of k_j for system j using the following procedure. For each system j, we first look for a list of sequences in bin l that are jointly typical with y^n. Then, we obtain an estimate $\hat{u}^n$ of u^n as follows: 1) if there is only one sequence in the list, we set $\hat{u}^n$ equal to this sequence; 2) if there is more than one sequence in the list, we randomly choose one sequence from the list and set $\hat{u}^n$ equal to this sequence; 3) if the list is empty, we set $\hat{u}^n$ to be the sequence in bin l with $k_1=1$ and $k_2=1$. Hence, each $y^n \in \mathcal{Y}^n$ has one $\hat{u}^n$ associated with it. Then for system 1, we obtain an estimate of the key $\hat{k}_1$ by setting it equal to the subgroup index of $\hat{u}^n$ in bin l. For system 2, we obtain an estimate of the key $\hat{k}_2$ by setting it equal to the index of the sequence in the subgroup with which it lies.

4) Error Probability Analysis: For each $j=1,2$, if $\hat{k}_j \neq k_j$, one of the following events must occur. 1) E_1: during the enrollment stage, there is no u^n that is jointly typical with x^n. 2) E_2: during the release stage, there exist $\tilde{u}^n \neq u^n$ in bin l that is jointly typical with y^n. 3) E_3: during the release stage, y^n is not jointly typical with u^n.

Using the union bound, we have

$$\mathbb{P}[\hat{K}_j \neq K_j] \le \mathbb{P}[E_1] + \mathbb{P}[E_2 \cap E_1^c] + \mathbb{P}[E_3 \cap E_1^c]. \tag{29}$$

Since there are $M = 2^{n(I(U;X)+\gamma)}$ typical sequences u^n, for any $\gamma > 0$, $\mathbb{P}[E_1]$ goes to zero as n increases [35]. In the following, we condition on the event that $(U^n, X^n) = (u^n, x^n) \in T^n_{[UX]\xi}$.

The probability of the second type of error can be bounded as follows:

$$\begin{aligned}
&\mathbb{P}[E_2 \cap E_1^c] \\
&\quad = \mathbb{P}\Big[\text{There exists } \tilde{u}^n \neq u^n \text{ in the bin } l \\
&\qquad\qquad \text{and} \quad (\tilde{u}^n, Y^n) \in T^n_{[UY]\delta}\Big] && (30)\\
&\quad \le \left(2^{n(I(U;Y)-\eta)} - 1\right)\left(2^{n(H(U|Y)+\delta)} - 1\right) \\
&\qquad \cdot 2^{-n(H(U)-\delta)} \\
&\quad \le 2^{n(I(U;Y)-\eta)} 2^{n(H(U|Y)+\delta)} \cdot 2^{-n(H(U)-\delta)} && (31)\\
&\quad = 2^{n(I(U;Y)-\eta)} 2^{-n(I(U;Y)-2\delta)} && (32)\\
&\quad = 2^{-\frac{n\eta}{3}} && (33)
\end{aligned}$$

which tends to 0 as $n \to \infty$.

Due to the Markov lemma [36], given $(u^n, x^n) \in T^n_{[UX]\xi}$, we have

$$\mathbb{P}\left[(u^n, x^n, Y^n) \in T^n_{[UXY]\xi}\right] > 1 - \xi \tag{34}$$

for n sufficiently large. Thus $\mathbb{P}[E_3 \cap E_1^c] \le \xi$.

Hence, for any $\epsilon > 0$, $\mathbb{P}[\hat{K}_j \neq K_j]$ can be made to be less than ϵ for all sufficiently large n.

5) Rate Analysis: For any u^n that is not the sequence with $l(u^n)=1, k_1(u^n)=1$ and $k_2(u^n)=1$, we have

$$\begin{aligned}
\mathbb{P}[U^n = u^n] &\le \sum_{x^n \in T^n_{[X|U],\xi}(u^n)} P_X^n(x^n) && (35)\\
&\le 2^{-n(I(U;X)-\zeta)} && (36)
\end{aligned}$$

in which ζ is a function of ξ, and goes to zero as ξ decreases.

Thus,

$$\begin{aligned}
H(U^n) &= \sum_{u^n \in \mathcal{M}} -\mathbb{P}[U^n = u^n]\log(\mathbb{P}[U^n = u^n]) \\
&\ge \sum_{u^n \in \mathcal{M}} \mathbb{P}[U^n = u^n] n(I(U;X) - \zeta) \\
&= n(I(U;X) - \zeta). && (37)
\end{aligned}$$

On the other hand, $H(V_1, V_2) = H(L) \le n(I(U;X) - I(U;Y) + \gamma + \eta)$, since L ranges from 1 to $2^{n(I(U;X)-I(U;Y)+\gamma+\eta)}$.

Combining the fact that $H(U^n) = H(K_1, K_2, L) = H(V) + H(K_1, K_2|L)$, we have

$$\begin{aligned}
n^{-1}H(K_1, K_2) &\ge n^{-1}H(K_1, K_2|L) \\
&= n^{-1}(H(U^n) - H(L)) \\
&\ge I(U;Y) - \zeta - \gamma - \eta. && (38)
\end{aligned}$$

[1]The notion of typicality and the definition of various typical sets used here follow from [35].

[2]In this development, we denote random variables by uppercase letters (for example, L) and realizations of random variables by corresponding lowercase letters (for example, l).

So

$$\begin{aligned} R_1 + R_2 &= n^{-1}(H(K_1) + H(K_2)) \\ &\geq n^{-1} H(K_1, K_2) \\ &\geq I(U;Y) - \zeta - \gamma - \eta. \end{aligned} \tag{39}$$

Hence the rate requirement is satisfied.

At the same time, we have

$$\begin{aligned} n^{-1} I(K_1; K_2) &= H(K_1) + H(K_2) - H(K_1, K_2) \\ &\leq R_1 + I(U;Y) - R_1 - \epsilon \\ &\quad - (I(U;Y) - \zeta - \gamma - \eta) \\ &\leq \zeta + \gamma + \eta - \epsilon \end{aligned} \tag{40}$$

satisfying the independence requirement (2).

6) Security Analysis: Now, we bound $I(K_1, K_2; V_1, V_2)$, the mutual information between the generated keys and the data stored in the two systems:

$$\begin{aligned} & n^{-1} I(K_1, K_2; V_1, V_2) \\ &\quad = n^{-1}(H(K_1, K_2) - H(K_1, K_2 \,|\, L)) \\ &\quad \leq I(U;Y) - \eta - (I(U;Y) - \zeta - \gamma - \eta) \\ &\quad \leq \gamma + \zeta \end{aligned} \tag{41}$$

where we have used (39) and the fact that K_1 ranges from 1 to 2^{nR_1}, and K_2 ranges from 1 to $2^{n(I(U;Y)-R_1-\eta)}$.

7) Privacy Analysis: We can write

$$\begin{aligned} & H(X^n \,|\, V_1, V_2) \\ &\quad = H(X^n, U^n \,|\, L) - H(U^n \,|\, L, X^n) \\ &\quad = H(U^n \,|\, L) + H(X^n \,|\, U^n, L) - H(U^n \,|\, X^n, L) \\ &\quad \overset{(a)}{\geq} nI(U;Y) - n(\zeta + \gamma + \eta) + H(X^n \,|\, U^n, L) \\ &\qquad - H(U^n \,|\, X^n) \\ &\quad \overset{(b)}{=} nI(U;Y) + H(X^n \,|\, U^n) \\ &\qquad - H(U^n \,|\, X^n) - n(\zeta + \gamma + \eta) \\ &\quad = nI(U;Y) + H(X^n) - H(U^n) - n(\zeta + \gamma + \eta) \\ &\quad \overset{(c)}{\geq} nI(U;Y) + nH(X) - nI(X;U) \\ &\qquad - n\gamma - n(\zeta + \gamma + \eta). \end{aligned} \tag{42}$$

Here, (a) is due to (39), since $H(U^n \,|\, L) = H(K_1, K_2, L \,|\, L) = H(K_1, K_2 \,|\, L)$; (b) is due to the fact that L is a function of U^n; and (c) is true since there are only $2^{n(I(U;X)+\gamma)}$ sequences of U^n in our codebook.

On defining $\epsilon_1 = \max\{(\zeta+2\gamma+\eta)/H(X), \zeta+\gamma+\eta, \gamma+\zeta\}$, from (28) (set size requirement), (29) (error probability requirement), (39) (rate requirement), (40) (independence requirement), (41) (security requirement), and (43) (privacy requirement), we have that the triple $(\Delta_{P,M}, R_1, R_2)$ with

$$\begin{aligned} \Delta_{P,M} &= \frac{H(X^n | V_1, V_2)}{H(X^n)} \\ &\geq 1 - \frac{I(U;X) - I(U;Y)}{H(X)} - \epsilon_1 \end{aligned}$$

and

$$R_1 + R_2 \geq I(U;Y) - \epsilon_1 \tag{43}$$

is achieved by the presented scheme. The proof of the achievability part is thus complete.

B. Converse

We now show the converse result that $\mathcal{C}_M$ is exactly the privacy–security region. To do so, we let $(\Delta_{P,M}, R_1, R_2)$ be a privacy–security triple achieved by using encoding functions h_j and $\tilde{h}_j$ and decoding function g_j. That is $V_j = h_j(X^n)$, $K_j = \tilde{h}_j(X^n)$, $n^{-1}\log |\mathcal{K}_j| \leq R_j + \epsilon$, $\mathbb{P}[K_j \neq g_j(Y^n)] \leq \epsilon$, and $n^{-1} I(K_1; K_2) \leq \epsilon$. In the following, we will show that there exists a random variable U with $U \to X \to Y$, such that

$$\Delta_{P,M} \leq 1 - \frac{I(U;X) - I(U;Y)}{H(X)} + \epsilon_n \tag{44}$$

and

$$R_1 + R_2 \leq I(U;Y) + \epsilon_n \tag{45}$$

in which ϵ_n approaches 0 as n increases. That is, $(\Delta_{P,M}, R_1, R_2) \in \mathcal{C}_M$.

First,

$$\begin{aligned} & \mathbb{P}[(K_1, K_2) \neq (g_1(Y^n), g_2(Y^n))] \\ &\qquad \leq \mathbb{P}[K_1 \neq g_1(Y^n)] + \mathbb{P}[K_2 \neq g_2(Y^n)] \end{aligned} \tag{46}$$

and combining with the conditions $\mathbb{P}[K_j \neq g_j(Y^n)] \leq \epsilon$ and $n^{-1}\log |\mathcal{K}_j| \leq R_j + \epsilon$, we have

$$\begin{aligned} & H(K_1, K_2 \,|\, Y^n, V_1, V_2) \\ &\quad = H(K_1, K_2 \,|\, g_1(Y^n, V_1), g_2(Y^n, V_2), Y^n, V_1, V_2) \\ &\quad \leq H(K_1, K_2 \,|\, g_1(Y^n, V_1), g_1(Y^n, V_1)) \\ &\quad \leq h(2\epsilon) + \epsilon \log |\mathcal{K}_1| + \epsilon \log |\mathcal{K}_2| \triangleq n\delta_n \end{aligned} \tag{47}$$

due to Fano's inequality. Here $h(2\epsilon) = -2\epsilon \log 2\epsilon - (1 - 2\epsilon)\log(1 - 2\epsilon)$, and δ_n goes to zero as n increases.

The equivocation can be bounded as follows:

$$\begin{aligned} & H(X^n \,|\, V_1, V_2) \\ &\quad = H(X^n) - I(X^n; V_1, V_2) \\ &\quad = H(X^n) - H(V_1, V_2) + H(V_1, V_2 \,|\, X^n) \\ &\quad = H(X^n) - H(V_1, V_2) \\ &\quad \leq H(X^n) - H(V_1, V_2 \,|\, Y^n) \\ &\quad = H(X^n) - H(V_1, V_2, K_1, K_2 | Y^n) \\ &\qquad + H(K_1, K_2 \,|\, V_1, V_2, Y^n) \\ &\quad \leq H(X^n) - H(V_1, V_2, K_1, K_2 \,|\, Y^n) + n\delta_n \end{aligned} \tag{48}$$

where (48) is due to (47).

By rewriting $H(V_1 V_2 K_1 K_2 \,|\, Y^n)$ as $H(Y^n \,|\, K_1 K_2 V_1 V_2) + H(K_1 K_2 V_1 V_2) - H(Y^n)$, we continue

$$\begin{aligned} & H(X^n \,|\, V_1 V_2) \\ &\quad \leq H(X^n) - H(Y^n \,|\, K_1 K_2 V_1 V_2) - H(K_1 K_2 V_1 V_2) \\ &\qquad + H(Y^n) + n\delta_n \\ &\quad \leq H(X^n) - \sum_{i=1}^{n} H(Y_i \,|\, K_1 K_2 V_1 V_2 Y^{i-1}) \\ &\qquad - I(K_1 K_2 V_1 V_2; X^n) + H(Y^n) + n\delta_n \\ &\quad \leq H(X^n) - \sum_{i=1}^{n} H(Y_i \,|\, K_1 K_2 V_1 V_2 Y^{i-1} X^{i-1}) \end{aligned}$$

$$
\begin{aligned}
&- I(K_1K_2V_1V_2;X^n) + H(Y^n) + n\delta_n \\
&\overset{(a)}{=} \sum_{i=1}^{n}\{H(X_i) - H(Y_i \,|\, K_1K_2V_1V_2X^{i-1}) \\
&\qquad - I(K_1K_2V_1V_2;X_i \,|\, X^{i-1}) + H(Y_i)\} + n\delta_n \\
&\overset{(b)}{=} \sum_{i=1}^{n}\{H(X_i) - H(Y_i|K_1K_2V_1V_2X^{i-1}) \\
&\qquad - I(K_1K_2V_1V_2X^{i-1};X_i) + H(Y_i)\} + n\delta_n \\
&= \sum_{i=1}^{n}\{H(X_i) + I(U_i;Y_i) - I(U_i;X_i)\} + n\delta_n \qquad (49)
\end{aligned}
$$

in which equality (a) is due to the fact that $Y^{i-1} \rightarrow (K_1, K_2, V_1, V_2, X^{i-1}) \rightarrow Y_i$ forms a Markov chain. To show this Markov chain relationship, we first have that $Y^{i-1} \rightarrow X^{i-1} \rightarrow X^nY_i$, which leads to $Y^{i-1} \rightarrow X^{i-1} \rightarrow X^nY_i \rightarrow (K_1, K_2, V_1, V_2, Y_i)$, and thus $Y^{i-1} \rightarrow (K_1, K_2, V_1, V_2, X^{i-1}) \rightarrow Y_i$. Equality (b) is due to the fact that $H(X_i \,|\, X^{i-1}) = H(X_i)$, while in the last equation, we set $U_i = K_1K_2V_1V_2X^{i-1}$.

On the other hand

$$
\begin{aligned}
&H(K_1, K_2, V_1, V_2) \\
&\quad = H(K_1, K_2) + H(V_1, V_2) - I(K_1, K_2; V_1, V_2) \\
&\quad \geq H(K_1, K_2) + H(V_1, V_2) - n\epsilon \qquad (50)
\end{aligned}
$$

due to the requirement that $I(K_1K_2; V_1V_2) \leq n\epsilon$, as specified in (4).

Now,

$$
\begin{aligned}
&H(K_1, K_2, V_1, V_2) \\
&\quad \overset{(a)}{=} I(K_1, K_2, V_1, V_2; X^n) \\
&\quad = \sum_{i=1}^{n} I(K_1, K_2, V_1, V_2; X_i \,|\, X^{i-1}) \\
&\quad = \sum_{i=1}^{n} I(K_1, K_2, V_1, V_2, X^{i-1}; X_i) \\
&\quad = \sum_{i=1}^{n} I(U_i; X_i) \qquad (51)
\end{aligned}
$$

in which (a) is due to the fact that K_1, K_2, V_1, and V_2 are functions of X^n.

Hence,

$$
H(K_1, K_2) \leq \sum_{i=1}^{n} I(U_i; X_i) - H(V_1, V_2) + n\epsilon + n\delta_n. \quad (52)
$$

Since V_1 and V_2 are functions of X^n, we have $H(V_1, V_2, X^n) = H(X^n)$. Together with (49), we obtain $H(V_1, V_2) \geq \sum_{i=1}^{n}[I(U_i; X_i) - I(U_i; Y_i)]$. It follows from (52) that

$$
H(K_1, K_2) \leq \sum_{i=1}^{n} I(U_i; Y_i) + n\epsilon + n\delta_n \qquad (53)
$$

where we have used (49).

Now

$$
\begin{aligned}
&H(K_1) + H(K_2) \\
&\quad = H(K_1, K_2) + I(K_1; K_2) \\
&\quad \overset{(a)}{\leq} \sum_{i=1}^{n} I(U_i; Y_i) + n\epsilon + n\delta_n + I(K_1; K_2) \\
&\quad \overset{(b)}{\leq} \sum_{i=1}^{n} I(U_i; Y_i) + n\epsilon + n\delta_n + n\epsilon \qquad (54)
\end{aligned}
$$

in which we use (53) in (a) and condition (2) in (b).

Now, by introducing a random variable T uniformly distributed over the set $\{1, \ldots, n\}$, and setting $U = (U_T, T)$, $X = X_T, Y = Y_T$ and $Z = Z_T$, we obtain the desired result by following the standard single-letter characterization technique [36].

Appendix B
Proof of Theorem 4

Here we show that for any $\epsilon_2 > 0$, the triple $(\Delta_{P,M}, R_1, R_2)$ with

$$
\begin{aligned}
\Delta_{P,M} &\leq 1 - \frac{I(U_2; X) - I(U_2; Y)}{H(X)} - \epsilon_2 \\
R_1 &\leq I(U_1; Y) - \epsilon_2 \qquad (55)
\end{aligned}
$$

and

$$
R_2 \leq I(U_2; Y \,|\, U_1) - \epsilon_2 \qquad (56)
$$

for auxiliary random variables U_1 and U_2 satisfying the following Markov chain $U_1 \rightarrow U_2 \rightarrow X \rightarrow Y$, is achievable.

For a given joint distribution $P_{U_1U_2XY}(u_1, u_2, x, y) = P_{U_1}(u_1)P_{U_2\,|\,U_1}(u_2 \,|\, u_1)P_{X\,|\,U_2}(x \,|\, u_2)P_{Y\,|\,X}(y \,|\, x)$, we use the following scheme to achieve the promised performance.

A. Legacy System

We keep the legacy system intact; that is, we use the same coding and decoding schemes as the single key system [25]. To assist the presentation, we give an overview of the design of the legacy system [25]. For a given joint distribution $P_{U_1XY}(u_1, x, y) = P_{U_1\,|\,X}(u_1 \,|\, x)P_{XY}(xy)$, the legacy system is designed using the following scheme.

1) Code Construction: Fix $\gamma > 0$ and $\eta > 0$, and let $\xi = \eta/3$. Randomly select $M_1 = 2^{n(I(U_1;X)+\gamma)}$ sequences U_1^n from $T^n_{[U_1],\xi|\mathcal{X}|}$, and divide them into $2^{n(I(U_1;X)-I(U_1;Y)+\gamma+\eta)}$ bins so that each bin contains $2^{n(I(U_1;Y)-\eta)}$ typical sequences. We use Q_1 to denote the bin index, and K_1 to denote the index of the sequence within each bin. Denote the set of these M_1 sequences by $\mathcal{M}_1$. From the construction above, we can see that each sequence $u_1^n \in \mathcal{M}_1$ is uniquely identified by two indices $(q_1(u_1^n), k_1(u_1^n))$.

2) Enrollment Stage: For each $x^n \in \mathcal{X}^n$, we associate a sequence $u_1^n \in \mathcal{M}_1$ with it by the following procedure. First, we find a list of sequences in $\mathcal{M}_1$ that are jointly typical with x^n. If there is more than one sequence in the list, we set u_1^n to be the one with the smallest index (we first compare the bin indices and if there is a tie, we then compare the index within the bin). If no such sequence exists, we set u_1^n to be the sequence with index $(q_1 = 1, k_1 = 1)$. Using this procedure, we associate every $x^n \in \mathcal{X}^n$ with a sequence $u_1^n \in \mathcal{M}_1$. We then store the bin index $q_1(u_1^n)$ in the database and set the key value as the index $k_1(u_1^n)$.

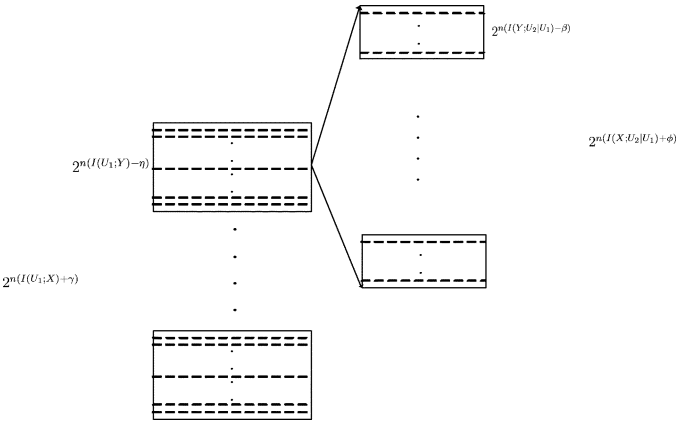


Fig. 7. Codebook used for the incremental design approach.

3) Release Stage: With the noisy measurement y^n, and the bin index q_1 stored in the database, we obtain an estimate $\hat{k}_1$ of k_1 using the following procedure. We first look for a list of sequences in bin q_1 that is jointly typical with y^n. Then, we obtain an estimate $\hat{u}_1^n$ of u_1^n as follows: 1) if there is only one sequence in the list, we set $\hat{u}_1^n$ equal to this sequence; 2) if there is more than one sequence in the list, we randomly choose one sequence from the list and set $\hat{u}_1^n$ equal to this sequence; 3) if the list is empty, we set $\hat{u}_1^n$ to be the first sequence in bin q_1. Hence, each $y^n \in \mathcal{Y}^n$ has one $\hat{u}_1^n$ associated with it. We then obtain an estimate of the key $\hat{k}_1$, by setting it equal to the index of $\hat{u}_1^n$ in bin q_1.

In [25], we show that for any ϵ, we have

$$n^{-1}H(K_1) \geq I(U_1;Y) - \epsilon \tag{57}$$

$$n^{-1}I(K_1;V_1) \leq \epsilon \tag{58}$$

for sufficiently large n.

B. New System

1) Code Construction: To construct the codebook of the new system, we need to use the codebook $\mathcal{M}_1$ of the legacy system. For each $u_1^n \in \mathcal{M}_1$, randomly select a set $\Lambda_{U_2}(u_1^n)$ of typical U_2^n sequences from $T^n_{[U_2\,|\,U_1]\delta'}(u_1^n)$ with size $|\Lambda_{U_2}(u_1^n)| = 2^{n(I(X;U_2\,|\,U_1)+\phi)}$. Since the size of the set $\mathcal{M}_1$ is $M_1 = 2^{n(I(U_1;X)+\gamma)}$, we have

$$\begin{aligned} &2^{n(I(U_1;X)+\gamma)}2^{n(I(X;U_2|U_1)+\phi)} \\ &\quad = 2^{n(I(U_1;X)+I(X;U_2|U_1)+\gamma+\phi)} \\ &\quad = 2^{n(I(X;U_2)+\gamma+\phi)} \end{aligned}$$

U_2^n sequences. We use $\mathcal{M}_2$ to denote these $2^{n(I(X;U_2)+\gamma+\phi)}$ U_2^n sequences. For each set $\Lambda_{U_2}(u_1^n)$, we divide these sequences into $2^{n(I(X;U_2\,|\,U_1)-I(Y;U_2\,|\,U_1)+\phi+\beta)}$ bins, so that each bin contains $2^{n(I(Y;U_2\,|\,U_1)-\beta)}$ typical sequences. We use Q_2 ranging from 1 to $2^{n(I(X;U_2\,|\,U_1)-I(Y;U_2\,|\,U_1)+\phi+\beta)}$ to denote the bin index, and use K_2 ranging from 1 to $2^{n(I(Y;U_2\,|\,U_1)-\beta)}$ to denote the index of the sequence within each bin. The codebook structure is shown in Fig. 7.

2) Enrollment Stage: For each $x^n \in \mathcal{X}^n$, we associate a sequence $u_2^n \in \mathcal{M}$ with it by the following procedure. First, we use the procedure in the old system to find u_1^n that is associated with x^n. As discussed in Subsection A of this appendix, this step can always be done. Then, we find a list of U_2^n sequences in $|\Lambda_{U_2}(u_1^n)|$ that are jointly typical with x^n. If there is more than one sequence in the list, we set u_2^n to be the one with the smallest index (we first compare the bin indices and if there is a tie, we then compare the index within the bin). If no such sequence can be found in $|\Lambda_{U_2}(u_1^n)|$, we randomly select a u_2^n from $|\Lambda_{U_2}(u_1^n)|$ using a uniform distribution. Using this procedure, we associate every $x^n \in \mathcal{X}^n$ with sequences u_1^n and u_2^n. We then store the bin indices $q_1(u_1^n)$ and $q_2(u_2^n)$ in the database of the new system. We set the key value of the new system to $k_2(u_2^n)$. Hence, in our scheme, $V_2 = (V_1, Q_2)$, $\mathcal{K}_2 = \{1, \ldots, 2^{n(I(U_2;Y\,|\,U_1)-\beta)}\}$.

3) Release Stage: With the noisy measurement y^n and the helper data $v_2 = (q_1, q_2)$, we obtain an estimate $\hat{k}_2$ of k_2 for the new system using the following procedure. We first obtain an estimate $\hat{u}_1^n$ using the release procedure of the legacy system as outlined in Subsection A of this appendix. And then, we find a list of u_2^n sequences in $|\Lambda_{U_2}(\hat{u}_1^n)|$ that are jointly typical with x^n. Then, we obtain an estimate $\hat{u}_2^n$ of u_2^n as follows: 1) if there is only one sequence in the list, we set $\hat{u}_2^n$ equal to this sequence; 2) if there is more than one sequence in the list, we set $\hat{u}_2^n$ to be the one with the smallest index (we first compare the bin indices and if there is a tie, we then compare the index within the bin); 3) if the list is empty, we randomly select a sequence from the set $\Lambda_{U_2}(\hat{u}_1^n)$ using a uniform distribution and set $\hat{u}_2^n$ to be this sequence. Hence, each $y^n \in \mathcal{Y}^n$ has $\hat{u}_1^n$ and $\hat{u}_2^n$ associated with it. We obtain an estimate of the key $\hat{k}_2$ by setting it equal to $k_2(\hat{u}_2^n)$.

4) Error Probability Analysis: This analysis is similar to that of the proof in Appendix A and is thus omitted.

5) Rate Analysis: For any u_2^n, we have

$$\mathbb{P}\left[U_2^n = u_2^n\right] \leq \sum_{x^n \in T^n_{[X\,|\,U_2],\xi}(u_2^n)} P_X^n(x^n) \tag{59}$$

$$\leq 2^{-n(I(U_2;X)-\zeta)} \tag{60}$$

in which ζ is a function of ξ, and goes to zero as ξ decreases.

Thus,

$$\begin{aligned} H\left(U_2^n\right) &= \sum_{u_2^n \in \mathcal{M}_2} -\mathbb{P}\left[U_2^n = u_2^n\right] \log(\mathbb{P}\left[U_2^n = u_2^n\right]) \\ &\geq \sum_{u_2^n \in \mathcal{M}_2} \mathbb{P}\left[U_2^n = u_2^n\right] n(I(U_2;X) - \zeta) \\ &= n(I(U_2;X) - \zeta). \end{aligned} \tag{61}$$

On the other hand,

$$\begin{aligned} &H(Q_1, Q_2) \\ &\quad \leq H(Q_1) + H(Q_2) \\ &\quad \overset{(a)}{\leq} n(I(U_1;X) - I(U_1;Y) + \gamma + \eta) \\ &\qquad + n(I(X;U_2\,|\,U_1) - I(Y;U_2\,|\,U_1) + \phi + \beta) \\ &\quad = n(I(X;U_1,U_2) - I(Y;U_1,U_2) + \gamma + \eta + \phi + \beta) \\ &\quad \overset{(b)}{=} n(I(X;U_2) - I(Y;U_2) + \gamma + \eta + \phi + \beta) \end{aligned} \tag{62}$$

where (a) is due to the fact that Q_1 ranges from 1 to $2^{n(I(U_1;X)-I(U_1;Y)+\gamma+\eta)}$ and Q_2 ranges from 1 to $2^{n(I(X;U_2\,|\,U_1)-I(Y;U_2\,|\,U_1)+\phi+\beta)}$. The equality (b) is true because $U_1 \to U_2 \to X \to Y$ forms a Markov chain.

Since each U_2^n in the codebook is uniquely identified by (Q_1, K_1, Q_2, K_2), and since $H(U_2^n) = H(Q_1, K_1, Q_2, K_2) = H(Q_1, Q_2) + H(K_1, K_2 \,|\, Q_1, Q_2)$, we have

$$\begin{aligned} & n^{-1}H(K_1, K_2) \\ & \quad \geq n^{-1}H(K_1, K_2 \,|\, Q_1, Q_2) \\ & \quad \geq n^{-1}\left(H\left(U_2^n\right) - H(Q_1, Q_2)\right) \\ & \quad \geq (I(U_2; X) - \zeta) \\ & \qquad - (I(X; U_2) - I(Y; U_2) + \gamma + \eta + \phi + \beta) \\ & \quad \geq I(Y; U_2) - \epsilon^{'} \end{aligned}$$

in which we set $\epsilon^{'} = \zeta + \gamma + \eta + \phi + \beta$. Hence

$$\begin{aligned} n^{-1}H(K_2) &= H(K_1, K_2) - H(K_1 \,|\, K_2) \\ &\geq H(K_1, K_2) - H(K_1) \\ &\geq I(Y; U_2) - \epsilon^{'} - I(Y; U_1) - \epsilon \\ &= I(Y; U_2|U_1) - \epsilon^{'} - \epsilon. \end{aligned} \tag{63}$$

Thus the rate requirement is satisfied.

6) Independence Analysis:

$$\begin{aligned} & n^{-1}I(K_1; K_2) \\ & \quad = n^{-1}(H(K_1, K_2) - H(K_1) - H(K_2)) \\ & \quad \overset{(a)}{\leq} I(U_1; Y) - \eta + I(U_2; Y \,|\, U_1) \\ & \qquad - \beta - H(K_1) - H(K_2) \\ & \quad \overset{(b)}{\leq} I(U_1; Y) - \eta + I(U_2; Y \,|\, U_1) - \beta \\ & \qquad - (I(U_1; Y) - \epsilon) - (I(Y; U_2|U_1) - \epsilon^{'} - \epsilon) \\ & \quad = 2\epsilon + \epsilon^{'} - \beta - \eta. \end{aligned} \tag{64}$$

Here, (a) is due to the fact that K_1 ranges from 1 to $2^{n(I(U_1;Y)-\eta)}$ and K_2 ranges from 1 to $2^{n(I(U_2;Y\,|\,U_1)-\beta)}$. And we use (57) and (63) for (b).

7) Security Analysis: From (63), we know that $H(K_1, K_2 \,|\, Q_1, Q_2) \geq n(I(Y; U_2) - \epsilon^{'})$, and hence

$$\begin{aligned} & n^{-1}I(K_1, K_2; V_1, V_2) \\ & \quad = I(K_1, K_2; Q_1, Q_2) \\ & \quad = n^{-1}(H(K_1, K_2) - H(K_1, K_2 \,|\, Q_1, Q_2)) \\ & \quad \leq I(U_1; Y) - \eta + I(U_2; Y|U_1) \\ & \qquad - \beta - (I(Y; U_2) - \epsilon^{'}) \\ & \quad \leq \epsilon^{'} + \eta + \beta. \end{aligned} \tag{65}$$

Thus, the helper data stored in both database does not provide any information about the generated keys.

8) Privacy Analysis:

$$\begin{aligned} & H(X^n \,|\, V_1 V_2) \\ & \quad = H(X^n \,|\, Q_1, Q_2) \\ & \quad = H\left(X^n U_2^n | \, Q_1, Q_2\right) - H\left(U_2^n | \, Q_1, Q_2, X^n\right) \\ & \quad = H\left(U_2^n | \, Q_1, Q_2\right) + H\left(X^n \,|U_2^n\right) \\ & \qquad - H\left(U_2^n | \, Q_1, Q_2, X^n\right) \\ & \quad \overset{(a)}{\geq} n(I(U_2; Y) - \epsilon^{'}) + H\left(X^n \,|U_2^n\right) - H\left(U_2^n | \, X^n\right) \\ & \quad = n(I(U_2; Y) - \epsilon^{'}) + H(X^n) - H\left(U_2^n\right) \\ & \quad \overset{(b)}{\geq} n(H(X) - (I(U_2; X) - I(U_2; Y)) - \epsilon^{'} - \gamma - \phi) \end{aligned} \tag{66}$$

in which (a) is due to (63), and (b) is due to the fact that in our codebook, U_2^n has at most $2^{n(I(X;U_2)+\gamma+\phi)}$ possible values.

On defining $\epsilon_2 = \max\{(\epsilon^{'} + \gamma + \phi)/H(X), \epsilon + \epsilon^{'}, 2\epsilon + \epsilon^{'} - \beta - \eta, \epsilon^{'} + \eta + \beta\}$, from (63) (rate requirement), (64) (independence requirement), (65) (security requirement), and (66) (privacy requirement), we have that

$$\begin{aligned} \Delta_{P,M} &\leq 1 - \frac{I(U_2; X) - I(U_2; Y)}{H(X)} - \epsilon_2 \\ R_1 &\leq I(U_1; Y) - \epsilon_2 \end{aligned} \tag{67}$$

and

$$R_2 \leq I(U_2; Y|U_1) - \epsilon_2 \tag{68}$$

is achieved by the presented scheme. The proof is thus complete.

REFERENCES

[1] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in reusable biometric security systems," in *Proc. IEEE Intl. Conf. Acoustics, Speech, and Signal Processing*, Dallas, TX, Mar. 2010.

[2] A. Ross, J. Shah, and A. K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 544–560, Apr. 2007.

[3] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 503–512, Sep. 2007.

[4] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates," in *Proc. Asiacrypt*, Shanghai, China, Dec. 2006, pp. 99–113.

[5] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in *Proc. IEEE Computer Society Workshop on Biometrics*, Minneapolis, MN, Jun. 2007.

[6] S. Draper, A. Khisti, E. Martinian, A. Vetro, and J. Yedidia, "Using distributed source coding to secure fingerprint biometrics," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Honolulu, HI, Apr. 2007, pp. 129–132.

[7] Y. Sutcu, S. Rane, J. S. Yedidia, S. Draper, and A. Vetro, "Feature transformation of biometric templates for secure biometric systems based on error correcting codes," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, Anchorage, AK, Jun. 2008.

[8] A. Vetro, S. Draper, S. Rane, and J. Yedidia, *Securing Biometric Data*. Amsterdam, The Netherlands: Elsevier, Jan. 2009.

[9] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identifications," in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, May 1998, pp. 148–157.

[10] J. Bringer, H. Chabannea, and B. Kindarji, "The best of both worlds: Applying secure sketches to cancelable biometrics," *Sci. Comput. Program.*, vol. 74, pp. 43–51, 2008.

[11] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[12] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches," in *Proc. IEEE Int. Symp. Security and Privacy*, May 2009, pp. 188–203.

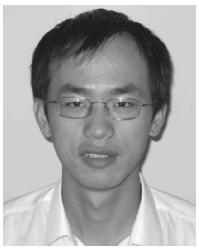
[13] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proc. ACM Conf. Computer and Communications Security*, New York, 2004, pp. 82–91, ACM Press.

[14] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Inf. Theory*, Lausanne, Switzerland, Jun./Jul. 2002, pp. 293–297.

[15] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," *Audio- and Video-Based Biometric Person Authentication*, pp. 310–319, Jul. 2005.

[16] U. Uludag and A. K. Jain, "Securing fingerprint template: Fuzzy vault with helper data," in *Proc. IEEE Workshop on Privacy Research in Vision*, New York, 2006.

[17] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Advances in Cryptology (EUROCRYPT)*, Interlaken, Switzerland, May 2004, pp. 523–540.
[18] G. Cohen and G. Zemor, "The wire-tap channel applied to biometrics," in *Proc. IEEE Int. Symp. Inf. Theory and its Applications*, Parma, Italy, Oct. 2004.
[19] T. Ignatenko and F. M. J. Willems, "On privacy in secure biometrics authentication systems," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Honolulu, HI, Apr. 2007, pp. 121–124.
[20] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," in *Biometric Authentication*. Berlin, Germany: Springer, 2004, pp. 158–170.
[21] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: A security analysis," in *Proc. SPIE, Electronic Imaging, Media Forensics and Security*, San Jose, Jan. 2010.
[22] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar, "Efficient biometric verification in encrypted domain," in *Proc. Int. Conf. Biometrics*, Sassari, Italy, 2009.
[23] P. Tuyls and J. Goseling, *Biometric Authentication*. Berlin, Germany: Springer, 2004.
[24] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Advances Signal Process.*, vol. 2008, pp. 1–17, Jan. 2008.
[25] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in biometric security systems—Part I: Single use case," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, Mar. 2011.
[26] T. Ignatenko and F. M. J. Willems, "Privacy leakage in biometric secrecy systems," in *Proc. Annu. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Sep. 2008.
[27] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.
[28] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in biometric security systems," in *Proc. 46th Annu. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Sep. 23–26, 2008.
[29] L. Lai, S.-W. Ho, and H. V. Poor, "An information theoretic framework for biometric security systems," in *Proc. Int. Conf. Biometrics*, Sassari, Italy, Jun. 2009.
[30] V. Stankovic, A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Design of Slepian-Wolf codes by channel code partitioning," in *Proc. IEEE Conf. Data Compression*, Snowbird, UT, Mar. 2004.
[31] S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," in *Proc. IEEE Conf. Data Compression*, Snowbird, UT, Mar. 1999.
[32] Y. Sutcu, S. Rane, J. S. Yedidia, S. Draper, and A. Vetro, "Feature extraction for a Slepian-Wolf biometric system using LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, Canada, Jul. 2008.
[33] R. Ahlswede and I. Csiszár, "Source coding with side information and a converse for the degraded broadcast channel," *IEEE Trans. Inf. Theory*, vol. 21, no. 6, pp. 629–637, Nov. 1975.
[34] A. D. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications: Part I," *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 769–777, Nov. 1973.
[35] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1981.
[36] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.



Lifeng Lai (M'07) received the B.E. and M.E. degrees from Zhejiang University, Hangzhou, China, in 2001 and 2004, respectively, and the Ph.D. degree from the Ohio State University at Columbus, OH, in 2007.

He was a postdoctoral research associate at Princeton University, Princeton, NJ, from 2007 to 2009. Since Aug. 2009, he has been an assistant professor at the University of Arkansas, Little Rock. His current research interests include network information theory, information theoretic security, statistical analysis of wireless networks, and biometric security systems.

Dr. Lai was a Distinguished University Fellow of the Ohio State University from 2004 to 2007. He coauthored a paper that received the Best Paper Award from the IEEE Global Communications Conference, 2008.

Siu-Wai Ho (S'05–M'07) was born in Hong Kong. He received the B.Eng., M.Phil., and Ph.D. degrees in information engineering from The Chinese University of Hong Kong in 2000, 2003, and 2006, respectively.

During 2006–2008, he was a Postdoctoral Research Fellow in the Department of Electrical Engineering, Princeton University, Princeton, NJ. Since 2009, he has been a Research Fellow at the Institute for Telecommunications Research (ITR), University of South Australia (UniSA), Adelaide, Australia, where he holds the ITR Director's Fellowship. His current research interests include Shannon theory, data communications and recording systems, and biometric security systems.

Dr. Ho was a recipient of the Croucher Foundation Fellowship for 2006–2008, the 2008 Young Scientist Award from the Hong Kong Institution of Science, UniSA Research SA Fellowship for 2010–2013, and the Australian Research Council Australian Postdoctoral Fellowship for 2010–2013.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in electrical engineering and computer science from Princeton University, Princeton, NJ, in 1977.

From 1977 to 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Dean of Engineering and Applied Science, and the Michael Henry Strater University Professor of Electrical Engineering. His research interests are in the areas of stochastic analysis, statistical signal processing and information theory, and their applications in wireless networks and related fields. Among his publications in these areas are *Quickest Detection* (Cambridge University Press, 2009), coauthored with Olympia Hadjiliadis, and *Information Theoretic Security* (Now Publishers, 2009), coauthored with Yingbin Liang and Shlomo Shamai.

Dr. Poor is a member of the National Academy of Engineering, a Fellow of the American Academy of Arts and Sciences, and an International Fellow of the Royal Academy of Engineering (U.K.). He is also a Fellow of the Institute of Mathematical Statistics, the Optical Society of America, and other organizations. In 1990, he served as President of the IEEE Information Theory Society, from 2004 to 2007 as the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY, and in 2009 as General Cochair of the IEEE International Symposium on Information Theory, held in Seoul, South Korea. He received a Guggenheim Fellowship in 2002 and the IEEE Education Medal in 2005. Recent recognition of his work includes the 2009 Edwin Howard Armstrong Achievement Award of the IEEE Communications Society, the 2010 IET Ambrose Fleming Medal for Achievement in Communications, and the 2011 IEEE Eric E. Sumner Award.