

Privacy-Security Tradeoffs in Biometric Security Systems

Lifeng Lai, Siu-Wai Ho and H. Vincent Poor
 {llai,siuho,poor}@princeton.edu

Abstract—Biometric security systems are analyzed from an information theoretic perspective. A fundamental tradeoff between 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, is 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 upper bounds on the privacy-security tradeoff are derived in this case.

I. INTRODUCTION

Biometric security systems have widespread applications. One typical example is a biometric encryption system, in which secret messages are encrypted using biometric characteristics, and are decrypted by presenting the same biometric measurements. Biometric characteristics are unique and do not change dramatically over time. The employment of biometric systems relieves the burden of selecting, memorizing and protecting passwords.

There are usually two stages in a biometric encryption system: an enrollment stage and a release stage. In the enrollment stage, biometric characteristics, such as fingerprints, are sampled. The biometric measurements themselves or a transformation of the biometric measurements are used to encrypt the document. In the release stage, the biometric characteristics are sampled again. The newly sampled biometric measurements are then used for decryption. 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. Another issue in a biometric encryption system is *privacy*. Biometric characteristics are stored in a certain form in the database, which creates a security threat. For example, it has been shown that it is possible to recover fingerprints from minutiae points stored in the database [1]. Unlike passwords, biometric characteristics cannot be changed. Hence, if the database is compromised, irreversible identity theft is possible.

The authors are with the Department of Electrical Engineering at Princeton University. This research was supported in part by the National Science Foundation under Grants ANI-03-38807, CNS-06-25637 and CCF-07-28208. Some of the results in this paper were presented at the Forty-Sixth Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, September 23-26, 2008.

In recent years, there has been increasing research interest in addressing these issues. A number of interesting approaches have been proposed (see, e.g., [2]–[7] and [8] for an overview.). 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 syndrome 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 [9]. From an information theoretic perspective, these existing approaches can be modelled as a problem of generating a secret key from common randomness [10]–[12], and hence the largest rate of the key can be characterized [13]. 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. It has been shown that in the existing approaches, the mutual information between the biometric measurements and the data stored in the database is $nH(X|Y)$ [14], where n is the length of the biometric measurement, X and Y are the biometric measurements taken during enrollment and release stages, respectively and $H(\cdot|\cdot)$ denotes conditional entropy.

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?¹ In this paper, by establishing an information theoretic foundation 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

¹A line of related work is the key generation problem with rate constraint considered in [15]. Our work, on the other hand, can be viewed as key generation problem with privacy constraints.

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 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 randomized and non-randomized systems are equivalent in terms of 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. Both randomized and non-randomized approaches are considered. Inner and outer bounds on the privacy-security region are derived for these situations. These bounds are shown to match under certain conditions of interest.

The rest of the paper is organized as follows. In Section II, we introduce our system model and notation. Section III is devoted to the perfect security scenario. Next, we discuss the perfect privacy scenario in Section IV. The situation in which the attack has side information is analyzed in Section V. Finally, in Section VI, we offer some concluding remarks. For the sake of readability, we describe the basic ideas behind our results in the main body of the paper, while providing detailed proofs in appendices.

II. MODEL

We denote the biometric measurements taken during the enrollment stage by X^n and the biometric measurements taken during the release 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. Assume these measurements are generated according to a joint distribution

$$P_{X^n Y^n}(x^n, y^n) = \prod_{i=1}^n P_{XY}(x_i, y_i).$$

Specific models for the distribution of biometric measurements can be found, for example, in [14].

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 encrypt messages. 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 recover stage.

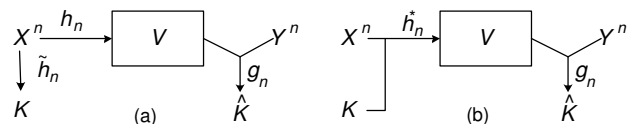


Fig. 1: Two different approach for generating key in biometric encryption systems: (a) non-randomized approach; (b) randomized approach.

A. Perfect security systems

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 any $\epsilon > 0$, $n^{-1}I(K; V) \leq \epsilon$ for sufficiently large n . 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 $R = n^{-1}H(K)$. 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:

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

$$H(X^n|V)/H(X^n) \geq \Delta_P, \quad (2)$$

$$n^{-1}I(V; K) \leq \epsilon \quad \text{and} \quad (3)$$

$$\mathbb{P}[K \neq \hat{K}] \leq \epsilon. \quad (4)$$

Additionally, we require that

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

Along with (1), this condition guarantees that the key is nearly uniformly generated, in the sense that the rate of the generated key is arbitrarily close to that of a uniformly generated key. We note that one can impose more stronger notion of uniformity, but in the current paper, we only consider the uniformity defined above.

B. Perfect privacy system

In a perfect privacy system, we require that the data stored in the database does not leak any information about 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 generalize the requirement on the generated key, that is 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:

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

$$I(X^n; V) \leq \epsilon, \quad (7)$$

$$H(K|V)/H(K) \geq \Delta_s, \quad (8)$$

$$\mathbb{P}\{K \neq \hat{K}\} \leq \epsilon \quad \text{and} \quad (9)$$

$$n^{-1} \log |\mathcal{K}| \leq R + \epsilon. \quad (10)$$

C. Side-information

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 $P_{X^n Y^n Z^n}(x^n, y^n, z^n) = \prod_{i=1}^n P_{XYZ}(x, y, z)$.

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 the 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:

$$n^{-1}H(K) \geq R, \quad (11)$$

$$H(X^n|VZ^n)/H(X^n) \geq \Delta_P, \quad (12)$$

$$n^{-1}I(VZ^n; K) \leq \epsilon, \quad (13)$$

$$\mathbb{P}\{K \neq \hat{K}\} \leq \epsilon \quad \text{and} \quad (14)$$

$$n^{-1} \log |\mathcal{K}| \leq R + \epsilon. \quad (15)$$

III. PERFECT KEY CASE

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

A. Non-randomized System

As discussed in Section II, 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 [3] and [5] and the coding approach in [14], belong to this category. The theorem below establishes the performance limits of this biometric security system. The basic idea of the achievability scheme behind of 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 (rigorous procedure will be given in the proof) a u^n that is jointly typical 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 [16], 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: bin index and index among each bin. We store the bin index in the database as helper data, and set the key value as the index of U^n in each bin. Hence, the rate of the key is approximately $I(U; Y)$. 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 the different choices of U , we control the leakage of information about the biometric measurements and the rate of the generated key. We note that similar scheme was also used in [15], in which the purpose of selection of U is to satisfy the rate constraints, while in our case the choices of U is to reduce the privacy leakage. We also 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:

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

$$R \leq I(U; Y), \quad (17)$$

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 $(\Delta_P, R) \in \mathcal{C}_N$.

Proof: Please refer to Appendix I². ■

Remark 1: 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 [13], [19], [20].

Remark 2: In order to achieve both perfect privacy and perfect security, the auxiliary random variable U in (16) should be chosen such that $I(U; X) = I(U; Y)$. The maximal rate achievable is then

$$\begin{aligned} & \max_U I(U; Y) \\ \text{s.t. } & U \rightarrow X \rightarrow Y \text{ and } I(U; X) = I(U; Y). \end{aligned} \quad (18)$$

B. Randomized Approach

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 [2] and [4] 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 achievability 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 in Theorem 1. Here \oplus denotes mod- $|\mathcal{J}|$ addition. If we set $\mathcal{K} = \mathcal{J}$, $J \oplus K$ will be approximately uniformly (these terms will be made rigorous in the proof) 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 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:

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

$$R \leq I(U; Y), \quad (20)$$

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 $(\Delta_P, R) \in \mathcal{C}_R$.

Proof: Please refer to Appendix II. ■

Remark 3: From here, we can see that $\mathcal{C}_N = \mathcal{C}_R$, and hence, randomized does not increase the region. But one advantage of this randomized approach is that the system is revocable.

²Here, we note that the result of Theorem 1, which the authors first presented in [17], also appeared independently and concurrently in [18] in a different form.

IV. PERFECT PRIVACY FOR BIOMETRIC MEASUREMENTS

In this section, we consider the perfect privacy case, in which we require that the mutual information between the data stored in the database and biometric measurements should be arbitrarily small. This models the situation in which privacy is of primary concern. As discussed in Remark 2 in Section III, 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 a suitable auxiliary random variable U , as specified in (18). 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 Remark 2 in Section III. Therefore, it is sufficient to discuss only randomized systems in the remainder of this section.

In this section, we make the technical assumption that

$$\log |\mathcal{V}| = O(n). \quad (21)$$

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

Definition 4: For two random processes X^n and Y^n , there exists 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

$$\mathbb{P}[\psi_n(X^n) \neq \phi_n(Y^n)] \leq \eta \quad \text{and} \quad (22)$$

$$n^{-1}H(\psi_n(X^n)) \geq \alpha - \eta. \quad (23)$$

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 measurement, 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 there exists a common random process between X^n and Y^n with entropy rate not less than $R\Delta_s$.

Proof: For any $\eta > 0$, there exist $\psi_n(X^n)$ and $\phi_n(Y^n)$ such that (22) and (23) are satisfied. Let $\alpha = n^{-1}H(\psi_n(X^n)) \geq R\Delta_s - \eta$. If $R \leq \alpha$, let $K = \psi_n(X^n)$, $\hat{K} = \phi_n(Y^n)$ and V be a constant. Then $n^{-1}H(K) \geq R$ and

$\frac{H(K|V)}{H(K)} = 1 \geq \Delta_s$. If $R > \alpha$, then let $\beta = R - \alpha$. Choose V independent of X^n such that $n^{-1}H(V) = \beta$. Let $K = (\psi_n(X^n), V)$ and $\hat{K} = (\phi_n(Y^n), V)$. Then $n^{-1}H(K) = \alpha + \beta = R$ and

$$\frac{H(K|V)}{H(K)} = \frac{n^{-1}H(\psi_n(X^n))}{n^{-1}H(K)} \geq \frac{R\Delta_s - \eta}{R} = \Delta_s - \frac{\eta}{R}. \quad (24)$$

In both cases, it is obvious that $I(X^n; V) = 0$ and $\mathbb{P}[K \neq \hat{K}] = \mathbb{P}[\psi_n(X^n) \neq \phi_n(Y^n)] \leq \eta$. Since $\eta > 0$ is arbitrary, the privacy-rate pair (R, Δ_s) is achievable. ■

The following theorem provides a converse.

Theorem 4: If (R, Δ_s) is achievable for X^n and Y^n , then there exist a common random process between X^n and Y^n with entropy rate not less than $R\Delta_s$.

Proof: Please refer to Appendix III. ■

This theorem says that if there exists a scheme that provides (R, Δ_s) , we can always find functions $\psi_n(X^n)$ and $\phi_n(Y^n)$ so that the entropy of $\psi_n(X^n)$ or $\phi_n(Y^n)$ is not less than $nR\Delta_s$. And hence, we can construct another scheme that is solely based on common information as that of Theorem 3 and can still achieve (R, Δ_s) . Thus, the scheme presented in Theorem 3 is optimal. Therefore, 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 $R\Delta_s$.

V. SIDE-INFORMATION AT THE ATTACKER

In this section, we consider a situation in which, besides the data V stored in the database, the 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.

A. Non-randomized approach

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 U^n s 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 [21], 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 (in this case,

the key is the the subset index). 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 recover sequence U^n . Using information inequalities, we also provide an upper bound on the performance achievable by any scheme.

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

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

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

$$\Delta_P \leq 1 - \frac{I(X;UZ) - I(U;Y) + I(U;Z|W)}{H(X)} \quad \text{and} \\ R \leq I(U;Y|W) - I(U;Z|W), \quad (26)$$

in which W and U are auxiliary random variables such that (W, U, X, Y, Z) satisfies the following Markov chain condition $W \rightarrow U \rightarrow X \rightarrow (Y, Z)$.

Any pair in $C_{s,in}$ is achievable, while any pair outside of $C_{s,out}$ is not achievable.

Proof: Please refer to Appendix IV. ■

Remark 4: In general, these two bounds do not match. If the attacker does not have side information, that is $Z = \Phi$, then the lower bound does match the upper-bound. Furthermore, the result recovers that of Theorem 1, since, if $Z = \Phi$, the lower bound becomes

$$\Delta_P \leq 1 - \frac{I(X;U) - I(U;Y|W)}{H(X)} \quad \text{and} \quad (27)$$

$$R \leq I(U;Y|W), \quad (28)$$

and the upper bound becomes

$$\Delta_P \leq 1 - \frac{I(X;U) - I(U;Y)}{H(X)} \quad \text{and} \quad (29)$$

$$R \leq I(U;Y|W). \quad (30)$$

Since $W \rightarrow U \rightarrow Y$, we have $I(U;Y|W) \leq I(U;Y)$, in which the equality can be achieved by setting W to be a constant. Thus, choosing W as a constant maximizes both R and Δ_P simultaneously in both the lower and upper-bounds. Furthermore, when we choose W to be a constant, these two bounds match.

B. Randomized approach

Same as Section III-B, during the enrollment stage, the key K is randomly generated and is 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 5. 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 in Theorem 5. Here \oplus denotes mod- $|\mathcal{J}|$ addition. If we set $\mathcal{K} = \mathcal{J}$, $J \oplus K$ will be approximately uniformly (these terms will be made rigorous in the proof) 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 scheme as that of Theorem 5. 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 also provide an upper-bound on the achievable privacy-security pairs.

Theorem 6: Let $C_{sr,in}$ be the set of (Δ_P, R) pairs satisfying the following conditions:

$$\begin{aligned} \Delta_P &\leq 1 - \frac{I(X;UZ) - I(U;Y|W) + I(U;Z|W)}{H(X)} \quad \text{and} \\ R &\leq I(U;Y|W) - I(U;Z|W), \end{aligned} \quad (31)$$

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

$$\begin{aligned} \Delta_P &\leq 1 - \frac{I(X;Z|U) - I(U;Y|W) + I(U;Z|W)}{H(X)} \quad \text{and} \\ R &\leq I(U;Y|W) - I(U;Z|W), \end{aligned} \quad (32)$$

in which W and U are auxiliary random variables such that (W, U, X, Y, Z) satisfies the following Markov chain condition $W \rightarrow U \rightarrow X \rightarrow (Y, Z)$.

Then any pair in $C_{sr,in}$ is achievable, while any pair outside of $C_{sr,out}$ is not achievable.

Proof: Please refer to Appendix VI. \blacksquare

VI. CONCLUSIONS

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. More specifically, an upper-bound on the privacy-security pair achievable by any scheme has been derived. Moreover, a scheme has been proposed to achieve this upper bound. For the scenario in which the attacker has side-information about the biometric measurements, inner and upper bounds on the privacy-security region have been derived.

Several interesting open questions arise from our work. Designing practical codes that achieve the derived theoretical bounds is a natural next step. Deriving a tighter bounds for the side-information case is also of interest.

APPENDIX I

PROOF OF THEOREM 1

Achievability

Here we show that for any auxiliary random variable U with $U \rightarrow X \rightarrow Y$, and any $\epsilon_1 > 0$, the pair (Δ_P, R) with

$$\begin{aligned} \Delta_P &= 1 - \frac{I(U;X) - I(U;Y)}{H(X)} - \epsilon_1 \quad \text{and} \\ R &= I(U;Y) - \epsilon_1 \end{aligned} \quad (33)$$

is achievable. That is, any pair in the region \mathcal{C}_N is achievable.

For a given joint distribution $P_{UXY}(u, x, y) = P_{U|X}(u|x)P_{XY}(xy)$, we use the following scheme.

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 $T_{[U],\xi|\mathcal{X}}^n$ ³, 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 use L to denote the bin index, and K to denote the index of the sequence within each bin⁴. 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 two indices $(l(u^n), k(u^n))$.

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 are 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 index within the bin). If no such sequence exists, we set u^n to be the sequence with index $(l = 1, k = 1)$. 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, and set the key value as the index $k(u^n)$. Hence, in our scheme, $V = L$, and $\mathcal{K} = \{1, \dots, 2^{n(I(U;Y)-\eta)}\}$. It then follows that

$$n^{-1} \log |\mathcal{K}| \leq I(U;Y) - \eta. \quad (34)$$

3) Release stage. With the noisy measurement y^n , and the bin index l stored in the database, we obtain an estimate \hat{k} of k using the following procedure. 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 are 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 first sequence in bin l . Hence, each $y^n \in \mathcal{Y}^n$ has one \hat{u}^n associated with it. We then obtain an estimate of the key \hat{k} , by setting it equal to the index of \hat{u}^n in bin l .

4) Error probability analysis. If $\hat{k} \neq k$, 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 $\hat{u}^n \neq u^n$ 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

$$\mathbb{P}[\hat{K} \neq K] \leq \mathbb{P}[E_1] + \mathbb{P}[E_2 \cap E_1^c] + \mathbb{P}[E_3 \cap E_1^c]. \quad (35)$$

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 [22]. In the following, we condition on the event that $(U^n, X^n) = (u^n, x^n) \in T_{[UX],\xi}^n$.

³In this paper, the notion of typicality and the definition of various typical sets follow from [22].

⁴In the development, we denote random variables by upper-case letters (for example L) and realizations of random variables by corresponding lower-case letters (for example l).

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

$$\mathbb{P}[E_2 \cap E_1^c] = \mathbb{P}[\text{There exists } \tilde{u}^n \neq u^n \text{ in the bin } l \text{ and } (\tilde{u}^n, Y^n) \in T_{[UY]\delta}^n] \quad (36)$$

$$\leq \left(2^{n(I(U;Y)-\eta)} - 1\right) \left(2^{n(H(U|Y)+\delta)} - 1\right) \cdot 2^{-n(H(U)-\delta)} \quad (37)$$

$$\leq 2^{n(I(U;Y)-\eta)} 2^{n(H(U|Y)+\delta)} \cdot 2^{-n(H(U)-\delta)} \quad (38)$$

$$= 2^{n(I(U;Y)-\eta)} 2^{-n(I(U;Y)-2\delta)} \quad (39)$$

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

Due to the Markov lemma [23], given $(u^n, x^n) \in T_{[UX]\xi}^n$, we have

$$\mathbb{P}[(u^n, x^n, Y^n) \in T_{[UXY]\xi}^n] > 1 - \xi \quad (40)$$

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

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

5) Rate analysis. For any u^n with $l(u^n) \neq 1$ and $k(u^n) \neq 1$, we have

$$\mathbb{P}[U^n = u^n] \leq \sum_{x^n \in T_{[X|U],\xi}^n(u^n)} P_X^n(x^n) \quad (41)$$

$$\leq 2^{-n(I(U;X)-\zeta)}, \quad (42)$$

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

Thus,

$$\begin{aligned} H(U^n) &= \sum_{u^n \in \mathcal{M}} -\mathbb{P}[U^n = u^n] \log(\mathbb{P}[U^n = u^n]) \\ &\geq \sum_{u^n \in \mathcal{M}} \mathbb{P}[U^n = u^n] n(I(U;X) - \zeta) \\ &= n(I(U;X) - \zeta). \end{aligned} \quad (43)$$

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

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

$$\begin{aligned} R = n^{-1}H(K) &\geq n^{-1}H(K|V) \\ &= n^{-1}(H(U^n) - H(V)) \\ &\geq I(U;Y) - \zeta - \gamma - \eta. \end{aligned} \quad (44)$$

So the rate of the key in our scheme is larger than $I(U;Y) - \zeta - \gamma - \eta$.

6) Security analysis. Now, we bound $I(K;V)$, the mutual information between the generated key and the data stored in the database:

$$\begin{aligned} n^{-1}I(K;V) &= n^{-1}(H(K) - H(K|V)) \\ &\leq I(U;Y) - \eta - (I(U;Y) - \zeta - \gamma - \eta) \\ &\leq \gamma + \zeta, \end{aligned} \quad (45)$$

where we have used (44) and the fact that K ranges from 1 to $2^{n(I(U;Y)-\eta)}$.

7) Privacy analysis.

We can write

$$\begin{aligned} H(X^n|V) &= H(X^n, U^n|V) - H(U^n|V, X^n) \\ &= H(U^n|V) + H(X^n|U^n, V) - H(U^n|X^n, V) \\ &\stackrel{(a)}{\geq} nI(U;Y) - n(\zeta + \gamma + \eta) + H(X^n|U^n, V) \\ &\quad - H(U^n|X^n) \\ &\stackrel{(b)}{=} nI(U;Y) + H(X^n|U^n) - H(U^n|X^n) \\ &\quad - n(\zeta + \gamma + \eta) \\ &= nI(U;Y) + H(X^n) - H(U^n) - n(\zeta + \gamma + \eta) \\ &\stackrel{(c)}{\geq} nI(U;Y) + nH(X) - nI(X;U) \\ &\quad - n\gamma - n(\zeta + \gamma + \eta). \end{aligned} \quad (46)$$

Here, (a) is due to (44), since $H(U^n|V) = H(K, V|V) = H(K|V)$; (b) is due to the fact that V 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 (34) (set size requirement), (35) (error probability requirement), (44) (rate requirement), (45) (security requirement) and (46) (privacy requirement), we have that the pair (Δ_P, R) with

$$\begin{aligned} \Delta_P &= \frac{H(X^n|V)}{H(X^n)} \geq 1 - \frac{I(U;X) - I(U;Y)}{H(X)} - \epsilon_1 \quad \text{and} \\ R &\geq I(U;Y) - \epsilon_1 \end{aligned} \quad (47)$$

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

Converse

We now show the converse result that \mathcal{C}_N is exactly the privacy-security region. To do so, we let (Δ_P, R) be a privacy-security pair achieved by using encoding functions h_n and \tilde{h}_n and decoding function g_n . That is $V = h_n(X^n)$, $K = \tilde{h}_n(X^n)$, $n^{-1} \log |\mathcal{K}| \leq R + \epsilon$ and $\mathbb{P}[K \neq g_n(Y^n)] \leq \epsilon$. In the following we will show that there exists a random variable U with $U \rightarrow X \rightarrow Y$, such that

$$\Delta_P \leq 1 - \frac{I(U;X) - I(U;Y)}{H(X)} + \epsilon_n \quad \text{and} \quad (48)$$

$$R \leq I(U;Y) + \epsilon_n, \quad (49)$$

in which ϵ_n approaches to 0 as n increases. That is $(\Delta_P, R) \in \mathcal{C}_N$.

First, from the conditions $\mathbb{P}[K \neq g_n(Y^n)] \leq \epsilon$ and $n^{-1} \log |\mathcal{K}| \leq R + \epsilon$, we have

$$\begin{aligned} H(K|Y^n, V) &= H(K|g_n(Y^n, V), Y^n, V) \\ &\leq H(K|g_n(Y^n, V)) \\ &\leq h(\epsilon) + \epsilon \log |\mathcal{K}| \triangleq n\delta_n, \end{aligned} \quad (50)$$

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

The privacy leakage can be bounded as follows:

$$\begin{aligned}
H(X^n|V) &= H(X^n) - I(X^n; V) \\
&= H(X^n) - H(V) + H(V|X^n) \\
&= H(X^n) - H(V) \\
&\leq H(X^n) - H(V|Y^n) \\
&= H(X^n) - H(V, K|Y^n) + H(K|V, Y^n) \\
&\leq H(X^n) - H(V, K|Y^n) + n\delta_n, \quad (51)
\end{aligned}$$

where (51) is due to (50).

By rewriting $H(VK|Y^n)$ as $H(Y^n|KV) + H(KV) - H(Y^n)$, we continue

$$\begin{aligned}
H(X^n|V) &\leq H(X^n) - H(Y^n|KV) - H(KV) \\
&\quad + H(Y^n) + n\delta_n \\
&\leq H(X^n) - \sum_{i=1}^n H(Y_i|KVY^{i-1}) \\
&\quad - I(KV; X^n) + H(Y^n) + n\delta_n \\
&\leq H(X^n) - \sum_{i=1}^n H(Y_i|KVY^{i-1}X^{i-1}) \\
&\quad - I(KV; X^n) + H(Y^n) + n\delta_n \\
&\stackrel{(a)}{=} \sum_{i=1}^n \{H(X_i) - H(Y_i|KVX^{i-1}) \\
&\quad - I(KV; X_i|X^{i-1}) + H(Y_i)\} + n\delta_n \\
&\stackrel{(b)}{=} \sum_{i=1}^n \{H(X_i) - H(Y_i|KVX^{i-1}) \\
&\quad - I(KVX^{i-1}; X_i) + H(Y_i)\} + n\delta_n \quad (52) \\
&= \sum_{i=1}^n \{H(X_i) + I(U_i; Y_i) - I(U_i; X_i)\} + n\delta_n,
\end{aligned}$$

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

On the other hand

$$\begin{aligned}
H(K, V) &= H(K) + H(V) - I(K; V) \\
&\geq H(K) + H(V) - n\epsilon, \quad (53)
\end{aligned}$$

due to the requirement that $I(K; V) \leq n\epsilon$, as specified in (3).

Now,

$$\begin{aligned}
H(K, V) &\stackrel{(a)}{=} I(K, V; X^n) \\
&= \sum_{i=1}^n I(K, V; X_i|X^{i-1}) \\
&= \sum_{i=1}^n I(K, V, X^{i-1}; X_i) \\
&= \sum_{i=1}^n I(U_i; X_i), \quad (54)
\end{aligned}$$

in which (a) is due to the fact that K and V are functions of X^n .

Hence,

$$H(K) \leq \sum_{i=1}^n I(U_i; X_i) - H(V) + n\epsilon + n\delta_n. \quad (55)$$

Since V is a function of X^n , we have $H(V, X^n) = H(X^n)$. Together with (52), we get $H(V) \geq \sum_{i=1}^n [I(U_i; X_i) - I(U_i; Y_i)]$. It follows from (55) that

$$H(K) \leq \sum_{i=1}^n I(U_i; Y_i) + n\epsilon + n\delta_n, \quad (56)$$

where we used (52).

Now, by introducing a random variable T uniformly distributed over the set $\{1, \dots, n\}$, and setting $U = (U_T, T)$, $X = X_T$, $Y = Y_T$ and $Z = Z_T$, we obtained the desired result by following the standard single-letter characterization technique [23].

APPENDIX II PROOF OF THEOREM 2

Achievability

Here we show that for any auxiliary random variable U with $U \rightarrow X \rightarrow Y$, and any $\epsilon_1 > 0$, the pair (Δ_P, R) with

$$\begin{aligned}
\Delta_P &= 1 - \frac{I(U; X) - I(U; Y)}{H(X)} - \epsilon_1 \quad \text{and} \\
R &= I(U; Y) - \epsilon_1 \quad (57)
\end{aligned}$$

is achievable. That is, any pair in the region \mathcal{C}_R is achievable.

For a given joint distribution $P_{U, X, Y}(u, x, y) = P_{U|X}(u|x)P_{XY}(xy)$, we use the following scheme.

1) Code construction. Fix $\gamma > 0$, $\eta > 0$ and $\xi > 0$. Randomly select $M = 2^{n(I(U; X) + \gamma)}$ sequences U^n from $T_{[U], \xi, \mathcal{X}}^n$, 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 use L to denote the bin index, and J to denote the index of the sequence within each bin. 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 two indices $(l(u^n), j(u^n))$.

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 are 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 index within the bin). If no such sequence exists, we set u^n to be the sequence with index $(l = 1, j = 1)$. Using this procedure, we associate every $x^n \in \mathcal{X}^n$ with a sequence $u^n \in \mathcal{M}$. Now, we randomly generate a key $K = k$ from the set $\mathcal{K} = \{1, \dots, 2^{n(I(U; Y) - \eta)}\}$ with a uniform distribution. We then store the bin index $l(u^n)$ and $j(u^n) \oplus k$ in the database, in which $j(u^n)$ denotes the index of u^n in bin $l(u^n)$. Here \oplus denotes mod- $2^{n(I(U; Y) - \eta)}$ addition. Hence, in this particular scheme $V = (L, J \oplus K)$. Also, we have

$$n^{-1} \log |\mathcal{K}| \leq I(U; Y) - \eta. \quad (58)$$

3) Release stage. With the noisy measurement y^n , and the data stored in the database $(l, j \oplus k)$, we obtain an estimate \hat{k} of k using the following procedure. 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 are more than one sequence in the list, we randomly choose one sequence from the list and set \hat{u}^n equal to this sequence; and (3) if the list is empty, we set \hat{u}^n to be the first sequence in bin l . Hence, for any $y^n \in \mathcal{Y}^n$, we have one \hat{u}^n associated with it. We then set $\hat{k} = \hat{j} \oplus (j \oplus k)$.

4) Error probability analysis. It is easy to see that $\mathbb{P}[\hat{K} \neq K] = \mathbb{P}[\hat{J} \neq J]$. The probability that \hat{J} is not equal to J can be analyzed exactly the same as the corresponding analysis in the proof of Theorem 1, which we thus omit.

5) Rate analysis. Since in our scheme, K is generated from $\mathcal{K} = \{1, \dots, 2^{n(I(U;Y)-\eta)}\}$ with a uniform distribution, the rate of the key is

$$R = I(U; Y) - \eta. \quad (59)$$

6) Security analysis. For any u^n with $l(u^n) \neq 1$ and $j(u^n) \neq 1$, we have

$$\mathbb{P}[U^n = u^n] \leq \sum_{x^n \in \mathcal{T}_{[X|U], \xi}^n(u^n)} P_X^n(x^n) \quad (60)$$

$$\leq 2^{-n(I(U;X)-\zeta)}, \quad (61)$$

in which ζ is a function of ξ , and approaches to zero as ξ decreases. Hence, we have

$$n^{-1}H(U^n) \geq I(U; X) - \zeta \quad (62)$$

based on the same argument of (43).

We also have

$$H(L) \leq n(I(U; X) - I(U; Y) + \gamma + \eta), \quad (63)$$

since the value of l ranges from 1 to $2^{n(I(U;X)-I(U;Y)+\gamma+\eta)}$.

From the fact that $H(U^n) = H(L, J) = H(L) + H(J|L)$, we have

$$\begin{aligned} H(J) &\geq H(J|L) \\ &= H(U^n) - H(L) \\ &\geq n(I(U; Y) - \zeta - \gamma - \eta), \end{aligned} \quad (64)$$

in which we have used (62) and (63).

Thus we have

$$\begin{aligned} n^{-1}I(K; V) &= n^{-1}I(K; L, K \oplus J) \\ &= n^{-1}(H(L, K \oplus J) - H(L, K \oplus J|K)) \\ &= n^{-1}(H(L) + H(K \oplus J|L) - H(L|K) \\ &\quad - H(K \oplus J|K, L)) \\ &= n^{-1}(H(K \oplus J|L) - H(J|L)) \\ &\leq I(U; Y) - \eta - (I(U; Y) - \zeta - \gamma - \eta) \\ &\leq \gamma + \zeta, \end{aligned} \quad (65)$$

where we have used (64) and the fact that the value of $k \oplus j$ ranges from 1 to $2^{n(I(U;Y)-\eta)}$.

7) Privacy analysis.

We can write

$$\begin{aligned} &H(X^n|L, J \oplus K) \\ &= H(X^n, U^n|L, J \oplus K) - H(U^n|X^n, L, J \oplus K) \\ &= H(U^n|L, J \oplus K) + H(X^n|U^n, L, J \oplus K) \\ &\quad - H(U^n|X^n, L, J \oplus K) \\ &\stackrel{(a)}{=} H(L, J|L, J \oplus K) + H(X^n|U^n, L, J \oplus K) \\ &\stackrel{(b)}{\geq} nI(U; Y) - 2n(\zeta + \gamma + \eta) + H(X^n|U^n, L, J \oplus K) \\ &\stackrel{(c)}{\geq} nI(U; Y) + H(X^n|U^n, J \oplus K) - 2n(\zeta + \gamma + \eta) \\ &= nI(U; Y) + H(X^n|U^n) - I(X^n; J \oplus K|U^n) \\ &\quad - 2n(\zeta + \gamma + \eta) \\ &\stackrel{(d)}{=} nI(U; Y) + H(X^n) - H(U^n) - 2n(\zeta + \gamma + \eta) \\ &\stackrel{(e)}{\geq} nI(U; Y) + nH(X) - nI(U; X) - n\gamma \\ &\quad - 2n(\zeta + \gamma + \eta). \end{aligned} \quad (66)$$

Here (a) is due to the fact that there is a one-to-one correspondence between U^n and (L, J) , and $H(U^n|X^n, L, J \oplus K) = 0$, since in our scheme U^n is a function of X^n ; (b) is due to the fact that $H(L, J|L, J \oplus K) = H(J|L, J \oplus K) = H(J|L) - I(J; J \oplus K) \geq nI(U; Y) - 2n(\zeta + \gamma + \eta)$, due to (64) and the fact that $I(J; J \oplus K) \leq n(\zeta + \gamma + \eta)$, which can be easily shown; (c) is due to the fact that L is a function of U^n ; (d) is due to the fact that $H(X^n|U^n) = H(X^n, U^n) - H(U^n) = H(X^n) - H(U^n)$, since in our scheme U^n is a function of X^n , and the fact that $I(X^n; J \oplus K|U^n) = H(J \oplus K|J, L) - H(J \oplus K|X^n, J, L) = 0$; and (e) is due to the fact that U^n takes at most $2^{n(I(U;X)+\gamma)}$ different values in our codebook.

On defining $\epsilon_1 = \max\{(\gamma + 2(\zeta + \gamma + \eta))/H(X), \eta, \gamma + \zeta\}$, from (58) (key size requirement), (59) (rate requirement), (65) (security requirement) and (66) (privacy requirement), we have that the pair (Δ_P, R) with

$$\begin{aligned} \Delta_P &= \frac{H(X^n|V)}{H(X^n)} \geq 1 - \frac{I(U; X) - I(U; Y)}{H(X)} - \epsilon_1 \quad \text{and} \\ R &\geq I(U; Y) - \epsilon_1 \end{aligned} \quad (67)$$

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

Converse

We now show the converse result that \mathcal{C}_R is the exactly the privacy-security region. To do so, we let (Δ_P, R) be a privacy-security pair achieved by using encoding functions h_n^* and decoding function g_n . That is $V = h_n^*(X^n, K)$, $n^{-1} \log |\mathcal{K}| \leq R + \epsilon$ and $\mathbb{P}[K \neq g_n(Y^n)] \leq \epsilon$. In the following we will show that there exists a random variable U with $U \rightarrow X \rightarrow Y$, such that

$$\Delta_P \leq 1 - \frac{I(U; X) - I(U; Y)}{H(X)} + \epsilon_n \quad \text{and} \quad (68)$$

$$R \leq I(U; Y) + \epsilon_n, \quad (69)$$

in which ϵ_n approaches to 0 as n increases. That is $(\Delta_P, R) \in \mathcal{C}_R$.

First, similarly to (50), there exists a sequence of δ_n that approaches 0 as n increases, such that

$$H(K|Y^n, V) \leq n\delta_n. \quad (70)$$

Now, we bound the privacy leakage as follows:

$$\begin{aligned} H(X^n|V) &\leq H(X^n, K|V) \\ &= H(X^n, K) - I(X^n, K; V) \\ &= H(X^n) + H(K) - H(V) \\ &\quad + H(V|X^n, K). \end{aligned} \quad (71)$$

Now

$$\begin{aligned} 0 &\geq H(V|Y^n) - H(V) \\ &= H(V, K|Y^n) - H(K|V, Y^n) - H(V) \\ &\geq H(V, K|Y^n) - H(V) - n\delta_n \\ &= H(Y^n|V, K) + H(V, K) - H(Y^n) - H(V) - n\delta_n \\ &= H(Y^n|V, K) + H(K|V) - H(Y^n) - n\delta_n \\ &= H(Y^n|V, K) + H(K) - H(Y^n) - I(K; V) - n\delta_n \\ &\geq H(Y^n|V, K) + H(K) - H(Y^n) - n\delta_n - n\epsilon, \end{aligned} \quad (72)$$

due to the requirement that $I(K; V) \leq n\epsilon$.

Thus, subtracting (72) from (71), we have

$$\begin{aligned} H(X^n|V) &\leq H(X^n) + H(Y^n) - H(Y^n|V, K) \\ &\quad - H(V) + n\delta_n + n\epsilon. \end{aligned} \quad (73)$$

We also have

$$\begin{aligned} H(V) &\geq I(V; X^n, K) \\ &= H(X^n, K) - H(X^n, K|V) \\ &= H(X^n, K) - H(K|V) - H(X^n|K, V) \\ &\geq H(X^n) - H(X^n|K, V) \\ &= \sum_{i=1}^n \{H(X_i) - H(X_i|X^{i-1}, K, V)\} \\ &= \sum_{i=1}^n \{H(X_i) - H(X_i|X^{i-1}, Y^{i-1}, K, V)\}, \end{aligned}$$

which is due to the fact that $Y^{i-1} \rightarrow (X^{i-1}, K, V) \rightarrow X_i$. To show this Markov chain relationship, we first note that $Y^{i-1} \rightarrow (X^{i-1}, K) \rightarrow (X^n, K, X_i)$, from which we have $Y^{i-1} \rightarrow (X^{i-1}, K) \rightarrow (X^n, K, X_i) \rightarrow (V, X_i)$, because $V = f(X^n, K)$. Now, we have $Y^{i-1} \rightarrow (X^{i-1}, K) \rightarrow (V, X_i)$, which leads to $Y^{i-1} \rightarrow (X^{i-1}, K, V) \rightarrow X_i$.

We continue as follows

$$\begin{aligned} H(V) &\geq \sum_{i=1}^n \{H(X_i) - H(X_i|X^{i-1}, Y^{i-1}, K, V)\} \\ &\geq \sum_{i=1}^n \{H(X_i) - H(X_i|Y^{i-1}, K, V)\} \\ &= \sum_{i=1}^n I(Y^{i-1}, K, V; X_i). \end{aligned} \quad (74)$$

Hence

$$\begin{aligned} H(X^n|V) &\leq H(X^n) + H(Y^n) - H(Y^n|V, K) - H(V) \\ &\quad + n\delta_n + n\epsilon \\ &\stackrel{(a)}{\leq} \sum_{i=1}^n \{H(X_i) + H(Y_i) - H(Y_i|V, K, Y^{i-1}) \\ &\quad - I(Y^{i-1}, K, V; X_i)\} + n\delta_n + n\epsilon \\ &= \sum_{i=1}^n \{H(X_i) + I(V, K, Y^{i-1}; Y_i) \\ &\quad - I(Y^{i-1}, K, V; X_i)\} + n\delta_n + n\epsilon \\ &\stackrel{(b)}{=} \sum_{i=1}^n \{H(X_i) + I(U_i; Y_i) - I(U_i; X_i)\} \\ &\quad + n\delta_n + n\epsilon, \end{aligned} \quad (75)$$

Here, in (a), we have used (74), and in (b) we have set $U_i = (Y^{i-1}, K, V)$.

Moreover, we have

$$\begin{aligned} H(K) &= I(K; VY^n) + H(K|VY^n) \\ &\stackrel{(a)}{\leq} I(K; VY^n) + n\delta_n \\ &= I(K; V) + I(K; Y^n|V) + n\delta_n \\ &\leq n\epsilon + n\delta_n + \sum_{i=1}^n I(K; Y_i|Y^{i-1}V) \\ &\leq n\epsilon + n\delta_n + \sum_{i=1}^n I(K, Y^{i-1}, V; Y_i) \\ &= n\epsilon + n\delta_n + \sum_{i=1}^n I(U_i; Y_i), \end{aligned} \quad (76)$$

in which (a) is due to (70).

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

APPENDIX III PROOF OF THEOREM 4

Consider a coding scheme (h_n^*, g_n, P_K) which achieves the pair (R, Δ_s) so that (6)–(9) are satisfied. For simplicity, we assume $P_V(v) > 0$ for all v . We will show that a common random process exists between X^n and Y^n with entropy rate $R\Delta_s$. We show this by explicitly constructing the functions $\psi_n(X^n)$ and $\phi_n(Y^n)$ from the coding scheme (h_n^*, g_n, P_K) .

Note that the joint distribution of X^n , K and V is given by

$$P_{X^n, K, V}(x^n, k, v) = P_{X^n}(x^n)P_K(k)\mathbf{1}\{v = h_n^*(x^n, k)\}. \quad (77)$$

Let

$$f_n(x^n, v) = \operatorname{argmax}_{k^*} \sum_{y^n} P_{Y^n|X^n}(y^n|x^n)\mathbf{1}\{k^* = g_n(y^n, v)\}, \quad (78)$$

and

$$K^* = f_n(X^n, V). \quad (79)$$

Then

$$\mathbb{P}[K \neq K^*] \leq \mathbb{P}[K \neq \hat{K}] \leq \epsilon, \quad (80)$$

where the last inequality follows from (9).

Let \tilde{V} be an auxiliary random variable that has the same distribution as V but is independent of all the above named variables. Let $\tilde{K} = f_n(X^n, \tilde{V})$. Then

$$P_{\tilde{K}\tilde{V}}(kv) = \sum_{x^n: f_n(x^n, v)=k} P_{X^n}(x^n)P_V(v), \quad (81)$$

and

$$P_{K^*V}(kv) = \sum_{x^n: f_n(x^n, v)=k} P_{X^nV}(x^n v). \quad (82)$$

Therefore,

$$\begin{aligned} & \sum_{kv} |P_{K^*V}(kv) - P_{\tilde{K}\tilde{V}}(kv)| \\ &= \sum_{kv} \left| \sum_{x^n: f_n(x^n, v)=k} P_{X^nV}(x^n v) \right. \\ & \quad \left. - \sum_{x^n: f_n(x^n, v)=k} P_{X^n}(x^n)P_V(v) \right| \\ &\leq \sum_{kv} \sum_{x^n: f_n(x^n, v)=k} |P_{X^nV}(x^n v) - P_{X^n}(x^n)P_V(v)| \\ &= \sum_{x^n v} |P_{X^nV}(x^n v) - P_{X^n}(x^n)P_V(v)| \quad (83) \\ &\leq \sqrt{2I(X^n; V) \ln 2} \quad (84) \\ &\leq \sqrt{2\epsilon \ln 2}, \quad (85) \end{aligned}$$

where (84) follows from Pinsker's inequality [23] and (85) follows from (7). Hence,

$$\begin{aligned} & n^{-1} \left| H(K^*|V) - H(\tilde{K}|\tilde{V}) \right| \\ &= n^{-1} \left| H(K^*V) - H(\tilde{K}\tilde{V}) \right| \quad (86) \end{aligned}$$

$$\leq n^{-1} \left(h \left(\frac{\sqrt{2\epsilon \ln 2}}{2} \right) + \frac{\sqrt{2\epsilon \ln 2}}{2} \log(|\mathcal{K}||\mathcal{V}|) \right) \quad (87)$$

$$\leq h \left(\frac{\sqrt{2\epsilon \ln 2}}{2} \right) + \frac{\sqrt{2\epsilon \ln 2}}{2n} \log(|\mathcal{K}||\mathcal{V}|), \quad (88)$$

where (87) follows from (85) and [24, Theorem 7]. Therefore,

$$\begin{aligned} & n^{-1} H(\tilde{K}|\tilde{V}) \\ &\geq n^{-1} H(K^*|V) - h \left(\frac{\sqrt{2\epsilon \ln 2}}{2} \right) - \frac{\sqrt{2\epsilon \ln 2}}{2n} \log(|\mathcal{K}||\mathcal{V}|) \\ &\geq n^{-1} I(K; K^*|V) - h \left(\frac{\sqrt{2\epsilon \ln 2}}{2} \right) - \frac{\sqrt{2\epsilon \ln 2}}{2n} \log(|\mathcal{K}||\mathcal{V}|) \\ &\geq n^{-1} (H(K|V) - H(K|K^*)) - h \left(\frac{\sqrt{2\epsilon \ln 2}}{2} \right) \\ & \quad - \frac{\sqrt{2\epsilon \ln 2}}{2n} \log(|\mathcal{K}||\mathcal{V}|) \\ &\geq n^{-1} H(K|V) - h \left(\frac{\sqrt{2\epsilon \ln 2}}{2} \right) \\ & \quad - \frac{\sqrt{2\epsilon \ln 2}}{2n} \log(|\mathcal{K}||\mathcal{V}|) - n^{-1} \delta, \quad (89) \end{aligned}$$

where

$$\delta = h(\epsilon) + \epsilon \log |\mathcal{K}| \quad (90)$$

and the last inequality follows from (80) and Fano's inequality [23]. For any $\mu > 0$, let

$$\Gamma_\mu = \{v : n^{-1} H(\tilde{K}|\tilde{V} = v) \geq n^{-1} H(\tilde{K}|\tilde{V}) - \mu\}, \quad (91)$$

and

$$v^* = \operatorname{argmin}_{v^* \in \Gamma_\mu} \sum_{x^n y^n} P_{X^n Y^n}(x^n y^n) \mathbf{1} \{f_n(x^n, v^*) \neq g_n(y^n, v^*)\}. \quad (92)$$

Now we consider a pair of random variables $(f_n(X^n, v^*), g_n(Y^n, v^*))$. Note that

$$n^{-1} H(f_n(X^n, v^*)) \quad (93)$$

$$= n^{-1} H(\tilde{K}|\tilde{V} = v^*) \quad (94)$$

$$\geq n^{-1} H(\tilde{K}|\tilde{V}) - \mu \quad (95)$$

$$\begin{aligned} & \geq n^{-1} H(K|V) - h \left(\frac{\sqrt{2\epsilon \ln 2}}{2} \right) \\ & \quad - \frac{\sqrt{2\epsilon \ln 2}}{2n} \log(|\mathcal{K}||\mathcal{V}|) - \mu - n^{-1} \delta, \quad (96) \end{aligned}$$

where (95) follows from the fact that $v^* \in \Gamma_\mu$, and (96) follows from (89).

Since $Y^n \rightarrow X^n \rightarrow V$ and $I(X^n; V) \leq \epsilon$, we have $I(X^n Y^n; V) \leq \epsilon$. Together with Pinsker's inequality, we have

$$\begin{aligned} & \sqrt{2\epsilon \ln 2} \\ &\geq \sum_{x^n y^n v} |P_{X^n Y^n}(x^n y^n)P_V(v) - P_{X^n Y^n V}(x^n y^n v)| \\ &\geq \sum_v P_V(v) \sum_{x^n y^n} |P_{X^n Y^n}(x^n y^n) - P_{X^n Y^n|V}(x^n y^n|v)| \\ &\geq \sum_v P_V(v) \sum_{x^n y^n} |P_{X^n Y^n}(x^n y^n) - P_{X^n Y^n|V}(x^n y^n|v)| \\ & \quad \mathbf{1} \{f_n(x^n, v) \neq g_n(y^n, v)\} \\ &\geq \sum_v P_V(v) \sum_{x^n y^n} (P_{X^n Y^n}(x^n y^n) - P_{X^n Y^n|V}(x^n y^n|v)) \\ & \quad \mathbf{1} \{f_n(x^n, v) \neq g_n(y^n, v)\}. \quad (97) \end{aligned}$$

From (78), we can see that

$$\begin{aligned} & \mathbb{P}[K^* = \hat{K} | X^n = x^n, V = v] \\ &= \sum_{y^n} P_{Y^n|X^n}(y^n|x^n) \mathbf{1} \{f_n(x^n, v) = g_n(y^n, v)\} \\ &\geq \sum_{y^n} P_{Y^n|X^n}(y^n|x^n) \mathbf{1} \{k = g_n(y^n, v)\} \\ &= \mathbb{P}[K = \hat{K} | X^n = x^n, V = v, K = k]. \quad (98) \end{aligned}$$

Therefore, $\mathbb{P}[K^* = \hat{K}] \geq \mathbb{P}[K = \hat{K}]$. Together with the requirement that $\mathbb{P}[K \neq \hat{K}] \leq \epsilon$, we get

$$\begin{aligned} \epsilon &\geq \mathbb{P}[K \neq \hat{K}] \\ &\geq \mathbb{P}[K^* \neq \hat{K}] \\ &= \sum_v P_V(v) \sum_{x^n y^n} P_{X^n Y^n|V}(x^n y^n|v) \\ & \quad \mathbf{1} \{f_n(x^n, v) \neq g_n(y^n, v)\}. \quad (99) \end{aligned}$$

Together with (97), we have

$$\begin{aligned}
\sqrt{2\epsilon \ln 2} + \epsilon &\geq \sum_v P_V(v) \sum_{x^n y^n} P_{X^n Y^n}(x^n y^n) \\
&\quad \mathbf{1}\{f_n(x^n, v) \neq g_n(y^n, v)\} \\
&\geq \sum_{v \in \Gamma_\mu} P_V(v) \sum_{x^n y^n} P_{X^n Y^n}(x^n y^n) \\
&\quad \mathbf{1}\{f_n(x^n, v) \neq g_n(y^n, v)\} \\
&\geq \left(\sum_{v \in \Gamma_\mu} P_V(v) \right) \sum_{x^n y^n} P_{X^n Y^n}(x^n y^n) \\
&\quad \mathbf{1}\{f_n(x^n, v^*) \neq g_n(y^n, v^*)\}. \quad (100)
\end{aligned}$$

The proof can be completed if we can find a lower bound on $\left(\sum_{v \in \Gamma_\mu} P_V(v)\right)$. Note that

$$\begin{aligned}
n^{-1}H(\tilde{K}|\tilde{V}) &= n^{-1} \sum_{v \in \Gamma_\mu} P_V(v)H(\tilde{K}|\tilde{V} = v) \\
&\quad + n^{-1} \sum_{v \in \Gamma_\mu^c} P_V(v)H(\tilde{K}|\tilde{V} = v) \\
&< n^{-1} \sum_{v \in \Gamma_\mu} P_V(v)H(X^n) \\
&\quad + \sum_{v \in \Gamma_\mu^c} P_V(v)(n^{-1}H(\tilde{K}|\tilde{V}) - \mu).
\end{aligned}$$

After rearranging the terms, we obtain

$$\begin{aligned}
\sum_{v \in \Gamma_\mu} P_V(v) &\geq \frac{\mu}{n^{-1}H(X^n) - n^{-1}H(\tilde{K}|\tilde{V}) + \mu} \\
&\geq \frac{\mu}{n^{-1}H(X^n) + \mu} \\
&\geq \frac{\mu}{\log |\mathcal{X}| + \mu}. \quad (101)
\end{aligned}$$

Together with (100), we have

$$\begin{aligned}
\sum_{xy} P_{X^n Y^n}(x^n y^n) \mathbf{1}\{f_n(x^n, v^*) \neq g_n(y^n, v^*)\} \\
\leq \frac{(\sqrt{2\epsilon \ln 2} + \epsilon)(\log |\mathcal{X}| + \mu)}{\mu}. \quad (102)
\end{aligned}$$

Finally, for any $\eta > 0$, we take

$$\mu = \frac{\eta}{2}.$$

Due to (5) and (21), there exists a sufficiently small ϵ such that

$$\max \left\{ h \left(\frac{\sqrt{2\epsilon \ln 2}}{2} \right) + \frac{\sqrt{2\epsilon \ln 2}}{2n} \log(|\mathcal{K}||\mathcal{V}|) + n^{-1}\delta, \frac{(\sqrt{2\epsilon \ln 2} + \epsilon)(\log |\mathcal{X}| + \mu)}{\mu} \right\} \leq \frac{\eta}{2} \quad (103)$$

even though $|\mathcal{K}|$ and $|\mathcal{V}|$ may be increasing as ϵ decreasing. At the same time, $n^{-1}\delta \rightarrow 0$ as $\epsilon \rightarrow 0$.

Finally, let $\psi_n(X^n) = f_n(X^n, v^*)$ and $\phi_n(Y^n) = g_n(Y^n, v^*)$. Then

$$\begin{aligned}
n^{-1}H(\psi_n(X^n)) &= n^{-1}H(f_n(X^n, v^*)) \\
&\geq n^{-1}H(K|V) - \eta \quad (104)
\end{aligned}$$

$$\geq R\Delta_s - \eta, \quad (105)$$

where (104) follows from (96), and (105) follows from (6) and (8). At the same time, the relationship

$$\mathbb{P}[\psi_n(X^n) \neq \phi_n(Y^n)] = \mathbb{P}[f_n(X^n, v^*) \neq g_n(Y^n, v^*)] \leq \eta \quad (106)$$

follows from (102) and (103).

Thus, we have successfully constructed $\psi_n(X^n)$ and $\phi_n(Y^n)$, and hence there is a common random process between X^n and Y^n with entropy rate $R\Delta_s$.

APPENDIX IV PROOF OF THEOREM 5

Achievability

Here we show that for any auxiliary random variable W and U with $W \rightarrow U \rightarrow X \rightarrow YZ$, and any $\epsilon^* > 0$, the pair (Δ_P, R) with

$$\begin{aligned}
\Delta_P &= 1 - \frac{I(X;UZ) - I(U;Y|W) + I(U;Z|W)}{H(X)} - \epsilon^*, \\
R &= I(U;Y|W) - I(U;Z|W) - \epsilon^* \quad (107)
\end{aligned}$$

is achievable. That is, any pair in the region $\mathcal{C}_{s,in}$ is achievable.

Fix a joint distribution $P_{WUXYZ}(wuxyz) = P_W(w)P_{U|W}(u|w)P_{X|U}(x|u)P_{YZ|X}(yz|x)$, we use the following scheme.

1) Code construction. We fix $\phi, \gamma, \eta, \delta$ and ν to be positive real numbers. Randomly select a set $\Lambda_W \subset T_{[W]^\delta}^n$ of typical sequence w^n with size $|\Lambda_W| = 2^{n(I(X;W)+\phi)}$. We arbitrarily order the sequences in Λ_W , and give an index, ranging from 1 to $2^{n(I(X;W)+\phi)}$, to each sequence. We also denote the sequence with index 1 by w_1^n . For each $w^n \in \Lambda_W$, randomly select a set $\Lambda_U(w^n) \subset T_{[U|W]^\delta}^n(w^n)$ of sequences u^n with size $|\Lambda_U(w^n)| = 2^{n(I(X;U|W)+\gamma)}$. For each set $\Lambda_U(w^n)$, we divide these sequences into $2^{n(I(U;X|W)-I(U;Y|W)+\gamma+\eta)}$ bins so that each bin contains $2^{n(I(U;Y|W)-\eta)}$ typical sequences. We further divide each bin into $2^{n(I(U;Y|W)-I(U;Z|W)-\eta+\nu)}$ subsets so that each subset contains $2^{n(I(U;Z|W)-\nu)}$ typical sequences. We use Q as the bin index, K as the index of the subset within each bin, and L as the index of the sequence within each subset. Then each sequence U^n can be uniquely identified by three indices (Q, K, L) and W^n .

2) Enrollment stage. For each $x^n \in \mathcal{X}^n$, we associate a u^n sequence with it using the following procedure. First, we find a sequence $w^n \in \Lambda_W$ such that (w^n, x^n) is jointly typical. If there are more than one sequence, we select w^n to be the one with the smallest index. If no such sequence exists, we choose w_1^n . After finding w^n , we find a list of $u^n \in \Lambda_U(w^n)$ such that (u^n, x^n) is jointly typical. If the list has more than one sequence, we select the one with the smallest index and associate it with x^n (we first compare Q ; if there is a tie, then we compare K ; if there is still a tie, then compare L). If the list is empty, we set u^n as the sequence with index $(q = 1, k = 1, l = 1)$ in $\Lambda_U(w_1^n)$, and associate it with x^n . After this procedure, each $x^n \in \mathcal{X}^n$ has a u^n associated with it. We set the key value to be the subset index k in which the sequence u^n falls. Hence, in this scheme $\mathcal{K} = \{1, \dots, 2^{n(I(U;Y|W)-I(U;Z|W)-\eta+\nu)}\}$, thus

$$n^{-1} \log |\mathcal{K}| \leq I(U;Y|W) - I(U;Z|W) - \eta + \nu. \quad (108)$$

We store w^n and the bin index q in the database. Hence, in this particular scheme $V = (W^n, Q)$.

3) Release stage. With the noisy measurement y^n , and the data stored in the database (w^n, q) , we obtain an estimate \hat{k} of k using the following procedure. we first look for a list of sequences in bin q of $\Lambda_U(w^n)$ 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 are more than one sequence in the list, we randomly choose one sequence from the list and set \hat{u}^n equal to this sequence; and (3) if the list is empty, we set \hat{u}^n to be the first sequence in bin q of $\Lambda_U(w^n)$. Hence, for any $y^n \in \mathcal{Y}^n$, we have a \hat{u}^n associated with it. We then obtain an estimate of the key \hat{k} , by setting it as the subset index of \hat{u}^n in the bin q of $\Lambda_U(w^n)$.

4) Rate analysis. For any u^n that is not the first sequence in $\Lambda_U(w_1^n)$, we have

$$\mathbb{P}[U^n = u^n] \leq \sum_{x^n \in T_{[X|UW], \xi}^n(u^n, w^n)} P_X^n(x^n) \quad (109)$$

$$\leq \exp^{(-n(I(WU; X) + \varsigma_\xi))}, \quad (110)$$

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

Hence, there exists a $\zeta > 0$, which is again a function of ξ and goes to zero as ξ decreases, such that

$$n^{-1}H(U^n) \geq I(WU; X) - \zeta. \quad (111)$$

On the other hand, $H(W^n) \leq n(I(X; W) + \phi)$, since the codebook contains only $2^{n(I(X; W) + \phi)}$ different w^n s. Similarly, we have $H(Q) \leq n(I(U; X|W) - I(U; Y|W) + \gamma + \eta)$, and $H(L) \leq n(I(U; Z|W) - \nu)$. Thus, we have

$$\begin{aligned} R &= n^{-1}H(K) \\ &\geq n^{-1}H(K|W^n, Q, L) \\ &= n^{-1}(H(W^n, K, Q, L) - H(W^n, Q, L)) \\ &\stackrel{(a)}{\geq} n^{-1}(H(U^n) - H(W^n, Q, L)) \\ &\geq n^{-1}(H(U^n) - H(W^n) - H(Q) - H(L)) \\ &\geq I(WU; X) - \zeta - (I(X; W) + \phi) \\ &\quad - (I(U; X|W) - I(U; Y|W) + \gamma + \eta) \\ &\quad - (I(U; Z|W) - \nu) \\ &= I(U; Y|W) - I(U; Z|W) \\ &\quad - \zeta - \phi - \gamma - \eta + \nu, \end{aligned} \quad (112)$$

in which (a) is due to the fact that there is a one-to-one correspondence between U^n and (W^n, Q, K, L) . From (112), it follows that the rate of the key is larger than $I(U; Y|W) - I(U; Z|W) - \epsilon$ for a suitable parameter ϵ .

5) Error probability analysis. The argument is similar to the corresponding one in the proof of Theorem 1; so it is omitted here.

6) Security analysis. In the following, we bound

$I(K; VZ^n)$. First, we have

$$\begin{aligned} &H(K|VZ^n) \\ &= H(K, V, Z^n) - H(VZ^n) \\ &= H(K, V, Z^n, U^n) - H(U^n|K, V, Z^n) - H(VZ^n) \\ &= H(K, V, U^n) + H(Z^n|U^n, K, V) - H(U^n|K, V, Z^n) \\ &\quad - H(VZ^n) \\ &\stackrel{(a)}{=} H(U^n) + H(Z^n|U^n) - H(U^n|K, V, Z^n) - H(V) \\ &\quad - H(Z^n|V) \\ &\geq H(U^n) + H(Z^n|U^n) - H(U^n|K, V, Z^n) - H(V) \\ &\quad - H(Z^n|W^n) \\ &\stackrel{(b)}{\geq} n(I(X; UW) - \zeta) + n(H(Z|U) - \varsigma) - n\delta_n \\ &\quad - n(I(X; W) + I(U; X|W) - I(U; Y|W) + \phi + \gamma + \eta) \\ &\quad - n(H(Z|W) + \epsilon_n) \\ &\stackrel{(c)}{=} n(I(U; Y|W) - I(U; Z|W) - \epsilon). \end{aligned} \quad (113)$$

Here (a) is due to the fact that K and V are functions of U^n . And (b) is due to the following facts: (1) $H(U^n) \geq n(I(WU; X) - \zeta)$, which was shown in (111); (2) $H(U^n|K, V, Z^n) \leq n\delta_n$, which will be shown in Lemma 1 of Appendix V; (3) $H(V) \leq H(W^n) + H(Q) \leq n(I(X; W) + I(U; X|W) - I(U; Y|W) + \phi + \gamma + \eta)$; (4) $H(Z^n|W^n) \leq n(H(Z|W) + \epsilon_1)$ with ϵ_1 goes to 0 as n increases, which will be shown in the Lemma 2 of Appendix V; and (5) $H(Z^n|U^n) \geq n(H(Z|U) - \varsigma)$ which can be shown similarly as in Lemma 3 of Appendix V. In (c), we define $\epsilon = \zeta + \varsigma + \delta_n + \epsilon_n + \phi + \gamma + \eta$.

Thus

$$\begin{aligned} n^{-1}I(K; VZ^n) &= n^{-1}(H(K) - H(K|VZ^n)) \\ &\stackrel{(a)}{\leq} I(U; Y|W) - I(U; Z|W) - \eta + \nu \\ &\quad - (I(U; Y|W) - I(U; Z|W) - \epsilon) \\ &= \nu - \eta + \epsilon, \end{aligned} \quad (114)$$

in which (a) follows from (113) and the fact that the value of K ranges from 1 to $2^{n(I(U; Y|W) - I(U; Z|W) - \eta + \nu)}$.

7) Privacy analysis

We have

$$\begin{aligned} &H(X^n|V, Z^n) \\ &= H(X^n, U^n|V, Z^n) - H(U^n|V, X^n, Z^n) \\ &= H(U^n|V, Z^n) + H(X^n|U^n, V, Z^n) - H(U^n|X^n, V, Z^n) \\ &\stackrel{(a)}{\geq} n(I(U; Y|W) - I(U; Z|W) - \epsilon) + H(X^n|U^n, V, Z^n) \\ &\stackrel{(b)}{\geq} n(I(U; Y|W) - I(U; Z|W)) + H(X^n|U^n, Z^n, W^n) - n\epsilon \\ &\stackrel{(c)}{\geq} n((1 - \delta_n)H(X) - ((1 - \delta_n)I(X; UZW) \\ &\quad - (I(U; Y|W) - I(U; Z|W)))) - 2n\delta_n - n\epsilon \\ &\stackrel{(d)}{=} n((1 - \delta_n)H(X) - ((1 - \delta_n)I(X; UZ) \\ &\quad - I(U; Y|W) + I(U; Z|W))) - 2n\delta_n - n\epsilon. \end{aligned} \quad (116)$$

Here, (a) is due to 1) the inequality $H(U^n|VZ^n) \geq H(K|VZ^n)$ and (113) and 2) the fact that U^n is a function of X^n in our scheme; (b) is due to the fact that $V = (W^n, Q)$

where Q is a function of U^n ; (c) is due to Lemma 3 of Appendix V; and (d) is due to the Markov chain relationship $W \rightarrow U \rightarrow X$.

On defining $\epsilon^* = (2 + H(X))\delta_n + \epsilon$, from (108) (key size requirement), (112) (rate requirement), (113) (security requirement) and (116) (privacy requirement), we have that the pair (Δ_P, R) with

$$\begin{aligned} \Delta_P &\geq 1 - \frac{I(X;UZ) - I(U;Y|W) + I(U;Z|W)}{H(X)} - \epsilon^*, \\ R &\geq I(U;Y|W) - I(U;Z|W) - \epsilon^* \end{aligned} \quad (117)$$

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

Converse

Here we show that $C_{s,out}$ is an upper-bound on the privacy-security pair achieved by any scheme. To do this, we let (Δ_P, R) be a privacy-security pair achieved by using encoding functions h_n and \tilde{h}_n and decoding function g_n . That is $V = h_n(X^n)$, $K = \tilde{h}_n(X^n)$, $\log |\mathcal{K}| \leq n(R + \epsilon)$ and $\mathbb{P}[K \neq g_n(Y^n)] \leq \epsilon$. In the following we will show that there exist random variables W and U with $W \rightarrow U \rightarrow X \rightarrow (Y, Z)$, such that

$$\begin{aligned} \Delta_P &\leq 1 - \frac{I(X;UZ) - I(U;Y) + I(U;Z|W)}{H(X)} + \epsilon_n \quad \text{and} \\ R &\leq I(U;Y|W) - I(U;Z|W) + \epsilon_n, \end{aligned} \quad (118)$$

in which ϵ_n approaches to 0 as n increases. That is $(\Delta_P, R) \in C_{s,out}$.

Again, similarly to (50), we have

$$H(K|Y^n, V) \leq n\delta_n. \quad (119)$$

We proceed as follows:

$$\begin{aligned} H(K) &= H(K|VZ^n) + I(K;VZ^n) \\ &\stackrel{(a)}{\leq} H(K|VZ^n) - H(K|VY^n) + n\delta_n + n\epsilon \\ &= I(K;Y^n|V) - I(K;Z^n|V) + n\delta_n + n\epsilon \\ &\stackrel{(b)}{=} \sum_{i=1}^n [I(K;Y_i|VY^{i-1}Z_{i+1}^n) - I(K;Z_i|VY^{i-1}Z_{i+1}^n)] \\ &\quad + n\delta_n + n\epsilon \\ &= \sum_{i=1}^n [I(KVY^{i-1}Z_{i+1}^n; Y_i|VY^{i-1}Z_{i+1}^n) \\ &\quad - I(KVY^{i-1}Z_{i+1}^n; Z_i|VY^{i-1}Z_{i+1}^n)] + n\delta_n + n\epsilon \\ &= \sum_{i=1}^n [I(U_i; Y_i|W_i) - I(U_i; Z_i|W_i)] + n\delta_n + n\epsilon, \end{aligned} \quad (120)$$

in which we have defined

$$W_i = (V, Y^{i-1}, Z_{i+1}^n), U_i = (K, V, Y^{i-1}, Z_{i+1}^n). \quad (121)$$

Here (a) follows from (119) and the requirement that $I(K;VZ^n) \leq n\epsilon$, and (b) can be obtained by using Lemma 7 of [25].

In the following, we bound $H(X^n|VZ^n)$:

$$\begin{aligned} H(X^n|VZ^n) &= H(X^n) - I(X^n;VZ^n) \\ &= H(X^n) - I(X^n;V) - I(X^n;Z^n|V) \\ &= H(X^n) - H(V) + H(V|X^n) - I(X^n;Z^n|V) \\ &= H(X^n) - H(V) - H(Z^n|V) + H(Z^n|X^nV), \end{aligned}$$

because V is a function of X^n .

We continue as follows

$$\begin{aligned} H(X^n|VZ^n) &= H(X^n) - H(V) - H(Z^n|V) + H(Z^n|X^nV) \\ &= \sum_{i=1}^n \{H(X_i) - H(Z_i|VZ_{i+1}^n) + H(Z_i|VX^nZ_{i+1}^n)\} \\ &\quad - H(V) \\ &\leq \sum_{i=1}^n \{H(X_i) - H(Z_i|VY^{i-1}Z_{i+1}^n) + H(Z_i|VX^nZ_{i+1}^n)\} \\ &\quad - H(V) \\ &\stackrel{(a)}{=} \sum_{i=1}^n \{H(X_i) - H(Z_i|VY^{i-1}Z_{i+1}^n) + H(Z_i|VKX^nZ_{i+1}^n)\} \\ &\quad - H(V) \\ &\stackrel{(b)}{=} \sum_{i=1}^n \{H(X_i) - H(Z_i|VY^{i-1}Z_{i+1}^n) \\ &\quad + H(Z_i|VKX^nY^{i-1}Z_{i+1}^n)\} - H(V) \\ &\leq \sum_{i=1}^n \{H(X_i) - H(Z_i|VY^{i-1}Z_{i+1}^n) \\ &\quad + H(Z_i|VKX_iY^{i-1}Z_{i+1}^n)\} - H(V) \\ &\leq \sum_{i=1}^n \{H(X_i) - I(X_iK; Z_i|VY^{i-1}Z_{i+1}^n)\} - H(V) \\ &= \sum_{i=1}^n \{H(X_i) - I(X_iKVY^{i-1}Z_{i+1}^n; Z_i|VY^{i-1}Z_{i+1}^n)\} \\ &\quad - H(V), \end{aligned} \quad (122)$$

in which (a) is due to the fact that K is a function of X^n , and (b) is due to the Markov chain relationship

$$Y^{i-1} \rightarrow VKX^nZ_{i+1}^n \rightarrow Z_i. \quad (123)$$

To show this, we have that $Y^{i-1}Z_{i+1}^n \rightarrow X^n \rightarrow Z_i$, which leads to $Y^{i-1} \rightarrow Z_{i+1}^nVKX^n \rightarrow Z_i$, since VK is a function of X^n .

Now,

$$\begin{aligned} H(V) &\geq H(V|Y^n) \\ &= H(VK|Y^n) - H(K|VY^n) \\ &\geq H(VK|Y^n) - n\delta_n \\ &= H(VK|Y^n) - H(VK|X^n) - n\delta_n \\ &= I(VK;X^n) - I(VK;Y^n) - n\delta_n \\ &= \sum_{i=1}^n \{I(VK; X_i|X_{i+1}^nY^{i-1}) - I(VK; Y_i|X_{i+1}^nY^{i-1})\} \\ &\quad - n\delta_n, \end{aligned} \quad (124)$$

in which we have used Lemma 7 of [25].

We continue as follows:

$$\begin{aligned}
& H(V) \\
& \geq \sum_{i=1}^n \{I(VKX_{i+1}^n Y^{i-1}; X_i) - I(VKX_{i+1}^n Y^{i-1}; Y_i)\} \\
& \quad - n\delta_n \\
& \stackrel{(a)}{=} \sum_{i=1}^n \{I(VKX_{i+1}^n Y^{i-1} Z_{i+1}^n; X_i) \\
& \quad - I(VKX_{i+1}^n Y^{i-1} Z_{i+1}^n; Y_i)\} - n\delta_n \\
& = \sum_{i=1}^n \{I(VKZ_{i+1}^n Y^{i-1}; X_i) - I(VKZ_{i+1}^n Y^{i-1}; Y_i)\} \\
& \quad + \sum_{i=1}^n \{I(X_{i+1}^n; X_i | VKY^{i-1} Z_{i+1}^n) \\
& \quad - I(X_{i+1}^n; Y_i | VKY^{i-1} Z_{i+1}^n)\} - n\delta_n \\
& \stackrel{(b)}{\geq} \sum_{i=1}^n \{I(VKZ_{i+1}^n Y^{i-1}; X_i) - I(VKZ_{i+1}^n Y^{i-1}; Y_i)\} \\
& \quad - n\delta_n, \tag{125}
\end{aligned}$$

in which (a) is due to the Markov chain relationship $Z_{i+1}^n \rightarrow VKX_{i+1}^n Y^{i-1} \rightarrow X_i Y_i$, which can be shown similarly to (123), and (b) is due to the fact that

$$I(X_{i+1}^n; X_i | VKY^{i-1} Z_{i+1}^n) = I(X_{i+1}^n; X_i Y_i | VKY^{i-1} Z_{i+1}^n),$$

which is due to the Markov chain relationship $X_{i+1}^n \rightarrow VKY^{i-1} Z_{i+1}^n X_i \rightarrow Y_i$. Combining (122) with (125), we have

$$\begin{aligned}
& H(X^n | VZ^n) \\
& \leq \sum_{i=1}^n \{H(X_i) - I(X_i K V Y^{i-1} Z_{i+1}^n; Z_i | V Y^{i-1} Z_{i+1}^n)\} \\
& \quad - H(V) + n\delta_n \\
& \leq \sum_{i=1}^n \{H(X_i) - I(X_i K V Y^{i-1} Z_{i+1}^n; Z_i | V Y^{i-1} Z_{i+1}^n) \\
& \quad - I(VKZ_{i+1}^n Y^{i-1}; X_i) + I(VKZ_{i+1}^n Y^{i-1}; Y_i)\} + n\delta_n \\
& = \sum_{i=1}^n \{H(X_i) - I(X_i U_i; Z_i | W_i) - I(U_i; X_i) \\
& \quad + I(U_i; Y_i)\} + n\delta_n \\
& = \sum_{i=1}^n \{H(X_i) - I(U_i; Z_i | W_i) - I(X_i; Z_i | W_i U_i) \\
& \quad - I(U_i; X_i) + I(U_i; Y_i)\} + n\delta_n \\
& \stackrel{(a)}{=} \sum_{i=1}^n \{H(X_i) - I(U_i; Z_i | W_i) - I(X_i; Z_i | U_i) \\
& \quad - I(U_i; X_i) + I(U_i; Y_i)\} + n\delta_n \\
& = \sum_{i=1}^n \{H(X_i) - I(X_i; U_i Z_i) - I(U_i; Z_i | W_i) \\
& \quad + I(U_i; Y_i)\} + n\delta_n, \tag{126}
\end{aligned}$$

Here W_i and U_i are defined in (121) and (a) is due to the Markov chain condition $W \rightarrow U \rightarrow X \rightarrow (Y, Z)$.

Now, by introducing a random variable T uniformly distributed over the set $\{1, \dots, n\}$, and setting $W = (W_T, T)$, $U = (U_T, T)$, $X = X_T$, $Y = Y_T$ and $Z = Z_T$, we

get the desired result by following the standard single-letter characterization technique.

APPENDIX V

LEMMAS FOR THE PROOF OF THEOREM 5

In this section, we state and prove several lemmas used in Appendix IV (the proof of Theorem 5).

Lemma 1: For the coding scheme in Theorem 5, we can write $H(U^n | K, V, Z^n) \leq n\delta_n$, where $\delta_n \rightarrow 0$ as n increases.

Proof: With knowledge of k and v , the attacker can obtain an estimate \tilde{u}^n of u^n by looking for a sequence in the subset k , bin i of $\Lambda_U(w^n)$ that is jointly typical with z^n . Based on a similar error probability analysis as to that given in the proof of Theorem 1, one can show that the probability that $\tilde{U}^n \neq U^n$ goes to zero as n increases. Thus, using Fano's inequality, we have $H(U^n | K, V, Z^n) \leq n\delta_n$ for a suitable choice of δ_n , which approaches to 0 as n increases. ■

Lemma 2: For the coding scheme in Theorem 5, we have

$$H(Z^n | W^n) \leq nH(Z | W) + n\epsilon_n,$$

in which ϵ_n goes to zero as n increases.

Proof: For each w^n , we define \hat{z}^n as following

$$\hat{z}^n = \begin{cases} z^n, & \text{if } z^n \in T_{[Z|W]\delta}^n(w^n) \\ z_t^n, & \text{if } z^n \notin T_{[Z|W]\delta}^n(w^n) \end{cases} \tag{127}$$

in which z_t^n is an arbitrary sequence in \mathcal{Z}^n .

We have

$$\begin{aligned}
H(Z^n | W^n) & \leq H(Z^n, \hat{Z}^n | W^n) \\
& = H(Z^n | \hat{Z}^n, W^n) + H(\hat{Z}^n | W^n) \\
& \leq H(Z^n | \hat{Z}^n) + H(\hat{Z}^n | W^n). \tag{128}
\end{aligned}$$

From the Markov lemma [23], (Z^n, W^n) are jointly typical with high probability. Hence $Z^n = \hat{Z}^n$ with high probability, and thus we have

$$H(Z^n | \hat{Z}^n) \leq n\epsilon'_n, \tag{129}$$

for a suitable choice of ϵ'_n that approaches to 0 as n increases, due to Fano's inequality [23].

At the same time, for any $w^n \in \Lambda_W \subset T_{[W]\delta}^n$, we have

$$H(\hat{Z}^n | w^n) \leq \log |T_{[Z|W]\delta}^n(w^n)| \leq n(H(Z | W) + \epsilon''_n), \tag{130}$$

for a suitable choice of ϵ''_n that approaches to 0 as n increases [22].

Hence

$$\begin{aligned}
H(Z^n | W^n) & \leq H(Z^n | \hat{Z}^n) + H(\hat{Z}^n | W^n) \\
& \leq n\epsilon_n + \sum_{w^n \in \Lambda_W} \mathbb{P}(W^n = w^n) H(\hat{Z}^n | W^n = w^n) \\
& \leq n\epsilon'_n + n(H(Z | W) + \epsilon''_n). \tag{131}
\end{aligned}$$

On defining $\epsilon_n = \epsilon'_n + \epsilon''_n$, which approaches zero as n increases, the claim is proved. ■

Lemma 3: For any $\epsilon > 0$, there exists a sufficiently large n such that $H(X^n | U^n, Z^n, W^n) \geq (1 - \epsilon)nH(X | UZ) - 2n\epsilon$.

Proof: Consider

$$\begin{aligned}
& H(X^n|U^n, Z^n, W^n) \\
& \geq - \sum_{(x^n, u^n, z^n, w^n) \in T_{[XUZW]\epsilon}^n} P_{X^n, U^n, Z^n, W^n}(x^n, u^n, z^n, w^n) \\
& \quad \log P_{X^n|U^n, Z^n, W^n}(x^n|u^n, z^n, w^n) \\
& \geq \sum_{(x^n, u^n, z^n, w^n) \in T_{[XUZW]\epsilon}^n} P_{X^n, U^n, Z^n, W^n}(x^n, u^n, z^n, w^n) \\
& \quad n(H(X|UZW) - 2\epsilon) \\
& = \mathbb{P}[(X^n, W^n, U^n, Z^n) \in T_{[XWUZ]\epsilon}^n] \\
& \quad n(H(X|UZW) - 2\epsilon) \\
& \stackrel{(a)}{\geq} (1 - \epsilon)n(H(X|UZW) - 2\epsilon) \\
& \geq (1 - \epsilon)nH(X|UZW) - 2n\epsilon. \tag{132}
\end{aligned}$$

Here for each $\epsilon > 0$, (a) is true for sufficiently large n [23]. ■

APPENDIX VI PROOF OF THEOREM 6

Achievability

Here we show that for any auxiliary random variable W and U with $W \rightarrow U \rightarrow X \rightarrow YZ$, and any $\epsilon^* > 0$, the pair (Δ_P, R) with

$$\begin{aligned}
\Delta_P &= 1 - \frac{I(X;UZ) - I(U;Y|W) + I(U;Z|W)}{H(X)} - \epsilon^*, \\
R &= I(U;Y|W) - I(U;Z|W) - \epsilon^* \tag{133}
\end{aligned}$$

is achievable. That is, any pair in the region $\mathcal{C}_{sr,in}$ is achievable.

Fix a joint distribution $P_{WUXYZ}(wuxyz) = P_W(w)P_{U|W}(u|w)P_{X|U}(x|u)P_{YZ|X}(yz|x)$, we use the following scheme.

1) Code construction. Fix $\phi, \gamma, \eta, \delta$ and ν to be positive real numbers. Randomly select a set $\Lambda_W \subset T_{[W]\delta}^n$ of typical sequences w^n with size $|\Lambda_W| = 2^{n(I(X;W)+\phi)}$. We arbitrarily order the sequences in Λ_W , and give an index ranging from 1 to $2^{n(I(X;W)+\phi)}$ to each sequence. We also denote the sequence with index 1 by w_1^n . For each $w^n \in \Lambda_W$, randomly select a set $\Lambda_U(w^n) \subset T_{[U|W]\delta'}^n(w^n)$ of sequences u^n with size $|\Lambda_U(w^n)| = 2^{n(I(X;U|W)+\gamma)}$. For each set $\Lambda_U(w^n)$, we divide the sequences into $2^{n(I(U;X|W)-I(U;Y|W)+\gamma+\eta)}$ bins so that each bin contains $2^{n(I(U;Y|W)-\eta)}$ typical sequences. We further divide each bin into $2^{n(I(U;Y|W)-I(U;Z|W)-\eta+\nu)}$ subsets so that each subset contains $2^{n(I(U;Z|W)-\nu)}$ typical sequences. We use Q as the bin index, J as the index of the subset within each bin, and L as the index of the sequence within each subset. Then each sequence U^n can be uniquely identified by three indices (Q, J, L) and W^n .

2) Enrollment stage. For each $x^n \in \mathcal{X}^n$, we associate a u^n sequence with it using the following procedure. First, we find a sequence $w^n \in \Lambda_W$ such that (w^n, x^n) is jointly typical. If there are more than one sequence, we select w^n to be the one with the smallest index. If no such sequence exists, we choose w_1^n . After finding w^n , we find a list of $u^n \in \Lambda_U(w^n)$ such that (u^n, x^n) is jointly typical. If the list has more than

one sequence, we select the one with the smallest index and associate it with x^n (we first compare Q ; if there is a tie, then we compare J ; if there is still a tie, then compare L). If the list is empty, we set u^n as the sequence with index $(q = 1, j = 1, l = 1)$ in $\Lambda_U(w_1^n)$, and associate it with x^n . After this procedure, each $x^n \in \mathcal{X}^n$ has a u^n associated with it. We now randomly generate a key K from the set $\mathcal{K} = \{1, \dots, 2^{n(I(U;Y|W)-I(U;Z|W)-\eta+\nu)}\}$ with a uniform distribution. We store W^n , bin index Q and $J \oplus K$ in the database. Here \oplus denotes $\text{mod-}2^{n(I(U;Y|W)-I(U;Z|W)-\eta+\nu)}$ addition. Hence, in this particular scenario $V = (W^n, Q, J \oplus K)$.

3) Release stage. With the noisy measurement y^n , and the data stored in the database $(w^n, q, j \oplus k)$, we obtain an estimate \hat{k} of k using the following procedure. we first look for a list of sequences in bin q of $\Lambda_U(w^n)$ 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 are more than one sequence in the list, we randomly choose one sequence from the list and set \hat{u}^n equal to this sequence; and (3) if the list is empty, we set \hat{u}^n to be the first sequence in bin q of $\Lambda_U(w^n)$. Hence, for any $y^n \in \mathcal{Y}^n$, we have one \hat{u}^n associated with it. We then obtain an estimate of the key \hat{k} , namely $\hat{k} = \hat{j} \oplus (j \oplus k)$, in which \hat{j} is the subset index of \hat{u}^n in the bin q of $\Lambda_U(w^n)$.

The error probability, rate, security and privacy analysis follow similarly those in the proofs of Theorem 2 and Theorem 5, and we omit them for the sake of compactness.

Converse

Here we show that $\mathcal{C}_{sr,out}$ is an upper-bound on the privacy-security pair achieved by any scheme. To do this, we let (Δ_P, R) be a privacy-security pair achieved by using encoding functions h_n and \hat{h}_n , and decoding function g_n . That is $V = h_n(X^n)$, $K = \hat{h}_n(X^n)$, $n^{-1} \log |\mathcal{K}| \leq R + \epsilon$ and $\mathbb{P}[K \neq g_n(Y^n)] \leq \epsilon$. In the following we will show that there exist random variables W and U with $W \rightarrow U \rightarrow X \rightarrow (Y, Z)$, such that

$$\begin{aligned}
\Delta_P &\leq 1 - \frac{I(X;Z|U) - I(U;Y) + I(U;Z|W)}{H(X)} + \epsilon_n, \\
R &\leq I(U;Y|W) - I(U;Z|W) + \epsilon_n, \tag{134}
\end{aligned}$$

in which ϵ_n approaches to zero as n increases. That is $(\Delta_P, R) \in \mathcal{C}_{sr,out}$.

Again, similarly to (50), we have $H(K|Y^n, V) \leq n\delta_n$.

We first bound the privacy leakage, as follows:

$$\begin{aligned}
H(X^n|VZ^n) &\leq H(X^n, K|VZ^n) \\
&= H(X^n, K) - I(X^n, K; VZ^n) \\
&= H(X^n) + H(K) - I(X^n, K; V) \\
&\quad - I(X^n, K; Z^n|V) \\
&= H(X^n) + H(K) - H(V) + H(V|X^n, K) \\
&\quad - H(Z^n|V) + H(Z^n|X^n, K, V) \\
&= H(X^n) - H(Z^n|V) + H(Z^n|X^n, K, V) \\
&\quad + H(K) - H(V) \tag{135}
\end{aligned}$$

since V is a function of (X^n, K) . We continue:

$$\begin{aligned}
& H(X^n|VZ^n) \\
& \leq \sum_{i=1}^n \{H(X_i) - H(Z_i|Z_{i+1}^n, V) \\
& \quad + H(Z_i|Z_{i+1}^n, X^n, K, V)\} + H(K) \\
& \leq \sum_{i=1}^n \{H(X_i) - H(Z_i|Z_{i+1}^n, V, Y^{i-1}, K) \\
& \quad + H(Z_i|Z_{i+1}^n, X^n, K, V)\} + H(K) \\
& \stackrel{(a)}{\leq} \sum_{i=1}^n \{H(X_i) - H(Z_i|Z_{i+1}^n, V, Y^{i-1}, K) \\
& \quad + H(Z_i|Z_{i+1}^n, Y^{i-1}, X^n, K, V)\} + H(K) \\
& \leq \sum_{i=1}^n \{H(X_i) - H(Z_i|Z_{i+1}^n, V, Y^{i-1}, K) \\
& \quad + H(Z_i|X_i, Z_{i+1}^n, Y^{i-1}, K, V)\} + H(K) \\
& \leq \sum_{i=1}^n \{H(X_i) - I(X_i; Z_i|Z_{i+1}^n, V, Y^{i-1}, K)\} + H(K).
\end{aligned}$$

In the derivation above, (a) is due to the Markov chain relationship $Y^{i-1} \rightarrow (Z_{i+1}^n, X^n, K, V) \rightarrow Z_i$, which can be easily shown.

At the same time, we have

$$\begin{aligned}
H(K) &= H(K|VZ^n) + I(K; VZ^n) \\
&\stackrel{(a)}{\leq} H(K|VZ^n) - H(K|VY^n) + n\delta_n + n\epsilon \\
&= I(K; Y^n|V) - I(K; Z^n|V) + n\delta_n + n\epsilon \\
&\stackrel{(b)}{=} \sum_{i=1}^n [I(K; Y_i|VY^{i-1}Z_{i+1}^n) \\
& \quad - I(K; Z_i|VY^{i-1}Z_{i+1}^n)] + n\delta_n + n\epsilon \\
&= \sum_{i=1}^n [I(KVY^{i-1}Z_{i+1}^n; Y_i|VY^{i-1}Z_{i+1}^n) \\
& \quad - I(KVY^{i-1}Z_{i+1}^n; Z_i|VY^{i-1}Z_{i+1}^n)] + n\delta_n + n\epsilon \\
&= \sum_{i=1}^n [I(U_i; Y_i|W_i) - I(U_i; Z_i|W_i)] + n\delta_n + n\epsilon,
\end{aligned}$$

in which we define

$$W_i = (V, Y^{i-1}, Z_{i+1}^n), U_i = (K, V, Y^{i-1}, Z_{i+1}^n). \quad (136)$$

Here (a) follows from Fano's inequality and the requirement that $I(K; VZ^n) \leq n\epsilon$, and (b) can be obtained by using Lemma 7 of [25].

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

REFERENCES

- [1] A. Ross, J. Shah, and A. Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, pp. 544–560, Apr. 2007.
- [2] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Intl. Symposium on Information Theory*, (Lausanne, Switzerland), pp. 293–297, June–July 2002.
- [3] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Trans. Inf. Forensics and Security*, vol. 2, pp. 503–512, Sept. 2007.
- [4] W. J. Scheirer and T. E. Boulton, "Cracking fuzzy vaults and biometric encryption," in *Proc. IEEE Biometrics Symposium*, (Baltimore, MD), pp. 1–6, Sept. 2007.
- [5] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates," in *Asiacrypt*, (Shanghai, China), pp. 99–113, Dec. 2006.
- [6] P. Tuyls and J. Goseling, *Biometric Authentication*. Berlin: Springer, 2004.
- [7] X. Boyen, "Reusable cryptographic fuzzy extractors," in *ACM Conference on Computer and Communications Security—CCS 2004*, pp. 82–91, New-York: ACM Press, 2004.
- [8] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, pp. 1–17, Jan. 2008.
- [9] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.
- [10] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, May 1993.
- [11] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, pp. 1121–1132, July 1993.
- [12] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part II: CR capacity," *IEEE Trans. Inf. Theory*, vol. 44, pp. 225–240, Jan. 1998.
- [13] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," in *In ECCV Workshop BioAW*, pp. 158–170, 2004.
- [14] S. Draper, A. Khisti, E. Martinian, A. Vetro, and J. Yedidia, "Using distributed source coding to secure fingerprint biometrics," in *Proc. IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing*, (Honolulu, HI), pp. 129–132, Apr. 2007.
- [15] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, pp. 344–366, Mar. 2000.
- [16] R. Ahlswede and I. Csiszár, "Source coding with side information and a converse for the degraded broadcast channel," *IEEE Trans. Inf. Theory*, vol. 21, pp. 629–637, Nov. 1975.
- [17] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in biometric security systems," in *Proc. 46th Annual Allerton Conf. on Communication, Control, and Computing*, (Monticello, IL), Sep. 23–26, 2008.
- [18] T. Ignatenko and F. Willems, "Privacy leakage in biometric secrecy systems," in *Proc. 46th Annual Allerton Conf. on Communication, Control, and Computing*, (Monticello, IL), Sep. 23–26, 2008.
- [19] G. Cohen and G. Zemor, "The wire-tap channel applied to biometrics," in *Proc. IEEE Intl. Symposium on Information Theory and its Applications*, (Parma, Italy), Oct. 2004.
- [20] T. Ignatenko and F. Willems, "On privacy in secure biometrics authentication systems," in *Proc. IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing*, (Honolulu, HI), pp. 121–124, Apr. 2007.
- [21] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.
- [22] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic Press, 1981.
- [23] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
- [24] S.-W. Ho and R. W. Yeung, "The interplay between entropy and variational distance," in *Proc. IEEE Intl. Symposium on Information Theory*, (Nice, France), pp. 491–495, July 2007.
- [25] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.