<http://www.diva-portal.org>

This is the published version of a paper published in .

Citation for the original published paper (version of record):

Zhou, L., Vu, M T., Oechtering, T J., Skoglund, M. (2021)
Two-Stage Biometric Identification Systems without Privacy Leakage
IEEE Journal on Selected Areas in Information Theory
<https://doi.org/10.1109/JSAIT.2021.3053368>

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

Permanent link to this version:

<http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-299943>

Two-Stage Biometric Identification Systems without Privacy Leakage

Linghui Zhou, *Student Member, IEEE*, Minh Thanh Vu,
Tobias J. Oechtering, *Senior Member, IEEE*, and Mikael Skoglund, *Fellow, IEEE*.

Abstract—We study two-stage biometric identification systems that allow authentication without privacy leakage. In the enrollment phase, secret keys and two layers of the helper data for each user are generated. Additional to the helper data and secret keys, we also introduce private keys in the systems. In the identification phase, an unknown but previously enrolled user is observed, and the user's private key is also presented to the system. The system firstly compares the user with the first layer helper database, outputs a list, and obtains a set of user indices. Then the system compares the observed user with the users in the set. Therefore, the identification procedure avoids an exhaustive search and only has to do a comparison with some part of the users in the system, which leads to a systematic reduction of the search complexity. Fundamental trade-offs among the identification rate, the secret key rate, the private key rate, the helper data rate, and the list size rate are derived in the imposed two-stage biometric identification systems without privacy leakage. Moreover, the obtained results show that a private key can boost the identification rate and the secret key rate, as well as preserve privacy.

Index Terms—Biometric, identification systems, privacy, secrecy.

I. INTRODUCTION

Biometrics are more and more used in various technologies and smart devices, such as biometric authentication and identification systems. Compared to traditional identification and authentication methods, which are knowledge-based (e.g. passwords) and token-based (e.g. ID cards), biometrics have the advantage that they are more stable, always carried with the person, and unique for each individual. Due to the uniqueness of biometrics, privacy should be taken into account when designing biometric systems. In the ideal case of a biometric identification system involving authentication, no or only a negligible amount of the information about both the secret keys and the biometrics is leaked. To reliably identify users and recover the secret keys, we have to store some data in the public database, which inevitably contains a certain amount of information about the biometrics and causes privacy issues. To solve this problem, we introduce additional private keys to enhance privacy.

We consider two-stage biometric identification systems that allow authentication without privacy leakage, where helper

data, secret keys, and private keys are involved. The helper data are stored in public databases and later used for identifying user indices and estimating secret keys. Secret keys are used for authentication and stored in a secure database or handed to the users. Private keys are handed to each user. Although external private keys are introduced, it is important that biometrics are also involved since the identification systems would be reduced to traditional knowledge or token-based keys without biometrics. Those key-only based systems have the disadvantage that the key can be guessed, lost, or stolen, which can lead to authorized access to the system. By enrolling both the biometrics and the private keys, the biometric systems have the advantage that it is more secure than traditional systems and at the same time the privacy is protected by external private keys. Moreover, we consider a two-stage setup, in which the helper data consist of two layers. When a user is trying to access the system, instead of doing an exhaustive search over all the users, the system firstly outputs a list of the first layer helper data and obtains a set of user indices. Then the system compares the user with the users in the set, and finally guesses the user index and estimates the corresponding secret key. A multi-stage identification procedure can be seen as an identification operation based on multiple features. Usually, biometric information contains multiple features. For simplicity, we consider the two-stage setup. In the enrollment phase, the system separates the features into two parts and stores them in two databases. In the identification phase, the system first compares the observed user with the first database and checks which users are matched with respect to the first part of the features. Then the system compares the observed user with the output users in terms of the second part of features and outputs a unique user that matches all the features. The principle of the search complexity reduction of the two-stage setting can be seen as a search procedure in a tree with two levels, where on the first level a decision is taken with respect to the first layer helper data entries and on the second level a decision is taken with respect to the second layer helper data entries of the potential users identified at the first stage. This principle can be straightforwardly extended.

In the proposed system, to reduce the hardware cost, we want to minimize the helper data rate and private key rate. Further, we want to maximize the secret key rate to increase the secrecy level and also maximize the identification rate to enroll and identify more users. We also want to minimize the rate of the output list such that fewer users are checked to reduce the search complexity. Therefore, we are interested in the fundamental trade-offs among the identification rate, secret

The work was partially supported by the Swedish Research Council under grant 2016-03853, the Digital Futures research center, and the Strategic Research Agenda Program, Information and Communication Technology - The Next Generation (SRA ICT - TNG), through the Swedish Government.

Linghui Zhou, Tobias J. Oechtering, and Mikael Skoglund are and Minh Thanh Vu was with the Division of Information Science and Engineering, KTH Royal Institute of Technology, 114 28 Stockholm, Sweden (e-mail: linghui@kth.se; oech@kth.se; skoglund@kth.se; mtvu@kth.se).

key rate, private key rate, helper data rates, and the list rate.

The capacity of biometric identification systems is characterized by Willems *et al.* in [1]. The capacity and storage trade-off in a multi-stage biometric identification system is studied by Tuncel *et al.* in [2]. Multi-stage biometric identification systems are further studied from the perspective of search complexity in [3], [4]. Hierarchical identification considering pre-processing is discussed in [5], it is assumed that there is a pre-processing step in the identification phase of a hierarchical identification.

Additional to the aforementioned concerns, biometric systems are also studied from the perspectives of privacy. Different frameworks for evaluating privacy have been proposed in the literature: reconstruction privacy constraint, privacy against statistical inference, privacy leakage [6], [7], etc. In [8], [9], reconstruction privacy constraint is studied in the lossy source coding problem under a privacy constraint that the reconstruction sequence at the decoder should be kept secret to a certain extent from an eavesdropper, which has access to both the compressed data and some side information. In this work, the process of generating helper data is related to the compression procedure in the source coding problem. However, in this work, we are interested in the privacy constraint only with respect to the compressed data, i.e., without additional side information or reconstruction operation. Based on the framework of privacy against statistical inference, the privacy-utility trade-off is studied extensively in [10]–[12], where it is assumed that a dataset is composed of both private and non-private information, and the privacy-utility guarantee aims at utilizing the dataset and at the same time satisfy a privacy level. The privacy-utility trade-off is closely related to this work because the objective of biometric identification without privacy leakage is to quantify and protect the privacy of personally identifiable biometric information as well as providing quantifiable utility, which is reliable identification and authentication in our problem scenario. Therefore, by studying the fundamental trade-offs involving privacy, identification, and authentication, we give specific operational meaning to the utility. By using mutual information as the measure of utility in the privacy-utility trade-off, perfect privacy of private latent variable with respect to revealed information is studied in [13]. In this work, perfect privacy is also achieved, but for the biometric source instead of the latent variable. As for the privacy-leakage, it refers to the amount of information leaked via public helper data about private information. Considering a biometric sequence as the source and private information, privacy leakage in biometric authentication and identification systems is characterized in [6], [7]. Their derived fundamental trade-offs use privacy leakage rate, which however is not required to be sufficiently small. In this work, we also use the privacy leakage rate to evaluate the privacy and use the masking approach to make the privacy leakage arbitrarily small.

Secrecy is another important concern when designing biometric systems involving authentication and the use of secret keys because compromised secret keys can lead to unauthorized access to the system. By taking both the privacy and secrecy into account, the privacy-secrecy trade-off in biometric

authentication systems is characterized in [6], [14], [15]. The privacy and secrecy aspects in biometric identification systems that allow authentication are investigated in [7], [16], [17]. In [18], [19], the authors additionally considered noisy enrollment in a privacy-preserving biometric identification system. Fundamental trade-offs among privacy, secrecy, and storage in biometric authentication systems with multiple measurements are characterized in [20], [21]. The problem of biometric authentication with controllable measurements is studied in [22], [23].

In [7], [16], the biometric identification system is characterized by a privacy constraint on the privacy leakage rate, which is not necessarily negligible. In this work, we study biometric identification systems that allow authentication with a more stringent privacy constraint than that in [7], [16]. Namely, the privacy leakage rate in our case is required to be sufficiently small, whereas the ones in [9] and [10] are not.

This work is an extension of our previous work [17]. Additional to the optimal trade-offs among the identification rate, secret key rate, and private key rate studied in [17], we also include the helper data rate and list rate in the optimal trade-offs in this work. The achievability is based on using the random binning and one-time padding masking methods. This proof scheme is shown to be optimal by a matching converse. Further, we perform this study for two cases based on how secret keys are produced. One scenario is that secret keys are generated from inputs to the system, i.e., biometric sequences and private keys. We call this setup the *generated secret key system*, which is depicted in Fig. 1. In the other scenario, chosen (or embedded) secret keys are produced from some random source independent of the biometric sequences and private keys. Then the secret keys are combined with inputs to the system to generate helper data. We call this setup the *chosen secret key system*, which is depicted in Fig. 2.

We summarize the main contributions as follows:

- This work deals with biometric information, and thus identification with zero privacy leakage of biometric data is an important extension. At the same time, the public database should not leak information about the secret key to maintain authentication performance. This zero leakage is achieved with an additional private key. Since a private key can be utilized in various ways in such a scenario, it is interesting to see how the key can be most efficiently employed and what fundamental trade-offs be achieved, i.e., finding matching converse to an achievability scheme is a challenge in a setting with many dimensions and choices.
- Since the proposed system requires to return both the user index and the corresponding secret key successfully, the error analysis in the achievability proof is challenging. Moreover, careful error analysis is necessary in such identification systems since we do not face a uniform distribution over the codewords when considering the case of a wrongly identified user. In particular, we deal with probabilities of an unselected codeword given the selected codeword and biometric information.
- The two-stage setup is closer to actual algorithmic implementations which are often based on feature extraction

Fig. 1: **Model for the generated secret key system.** In the enrollment phase, the enrollment mapping uses the biometric sequence $X^N(W)$ and private key P_W to generate the secret key S_W , a hash index (the first layer helper data) C_W , and the refinement data (the second helper data) J_W . In the identification phase, the first layer decoding $d_1(\cdot)$ maps the observation Y^N and private key P_W to a list of hash indices $\mathcal{L}$. Then the identification mapping $d_2(\cdot)$ guesses the user index and estimates the secret key using (Y^N, P_W) and $(\mathcal{J}_{\mathcal{L}}, \mathcal{B}_{\mathcal{L}}, \mathcal{L})$, where $\mathcal{B}_{\mathcal{L}}$ is defined as a set of user indices results in the hash indices in the list $\mathcal{L}$ and thus $(\mathcal{J}_{\mathcal{L}}, \mathcal{B}_{\mathcal{L}}, \mathcal{L}) = \{(J_w, w, c) | w \in \mathcal{B}(c), c \in \mathcal{L}\}$.

mechanism and successive processing. The principles and arguments presented here are ready to be extended to multiple stages, but are limited to two stages for a better exposition of the already involved setting. The complex fundamental regions can be simplified in several directions to recover existing results.

The rest of the paper is organized as follows. In Section II, we describe the problem formulation. In Section III, the main results are presented. In Section IV, the proofs are given. In Section V, a binary example is given to illustrate the trade-offs.

Notations: Let upper cases, lower cases and calligraphic letters denote random variables, their realizations and alphabets, respectively. Let a sequence $(X_m, \dots, X_n)$ be denoted by X_m^n . We use the short notation X^N for X_1^N . The terms $H(X)$, $I(X; Y)$, $Q_X(x)$ and $Q_{Y|X}(y|x)$ represent the entropy, mutual information, marginal and conditional probability mass function (p.m.f.), respectively. The strong typical set is denoted by $\mathcal{T}_\epsilon^N$. We use $|\mathcal{A}|$ to denote the cardinality of a set $\mathcal{A}$. the set $\{1, 2, \dots, M\}$ is denoted with $[1 : M]$.

II. THE IDENTIFICATION PROBLEM

A. Generated Secret Key System

A model of a generated secret key system without privacy leakage is presented in Fig. 1. Assume that there are M_I users enrolled in the system, where the users are indexed

Fig. 2: **Model for the chosen secret key system.** In the enrollment phase, the enrollment uses the biometric sequence $X^N(W)$, the private key P_W , and the secret key S_W to generate the first layer helper data C_W and the second layer helper data J_W . Similar to the generated secret key system, in the identification phase, the system firstly estimates a list of hashes $\mathcal{L}$ and then guesses the user identity and estimates the secret key use the observation (Y^N, P_W) and $(\mathcal{J}_{\mathcal{L}}, \mathcal{B}_{\mathcal{L}}, \mathcal{L})$.

by $w \in [1 : M_I]$. We further assume that for each user $w \in [1 : M_I]$, the biometric sequence $x^N(w)$ is identically independently distributed (i.i.d.) according to p.m.f. $Q_X(\cdot)$ on a finite alphabet $\mathcal{X}$.

In the enrollment phase, for each user $w \in [1 : M_I]$, the enrollment mapping $e_1(\cdot)$ uses the biometric sequence $x^N(w)$ and the user's private key p_w to generate a hash index $c_w \in [1 : M_C]$, i.e.,

$$c_w = e_1(x^N(w), p_w), \quad (1)$$

and puts the user index w inside the set $\mathcal{B}(c_w)$, which consists of user indices with hash index c_w . This hash index c_w is the first layer helper data, which is stored in the first layer public database at location w . Note that $\mathcal{B}(c_w)$ can be obtained from the first layer database. The private key for each user is assumed to be independent and uniformly distributed on $[1 : M_P]$. This private key is also accessible to the system in the identification phase when the user is trying to access the system.

Then the enrollment mapping $e_2(\cdot)$ uses the biometric sequence $x^N(w)$ and the user's private key p_w to generate the refinement data (the second layer helper data) $j_w \in [1 : M_J]$ and a secret key $s_w \in [1 : M_S]$, i.e.,

$$(j_w, s_w) = e_2(x^N(w), p_w), \quad (2)$$

where j_w is stored in the second layer public database.

In the identification phase, an unknown but previously enrolled user W is observed via a discrete memoryless channel (DMC) $Q_{Y|X}(\cdot)$ that generates an observation y^N , where W is uniformly distributed over $[1 : M_I]$. The observation y^N

together with the corresponding private key p_w are presented to the system. With (y^N, p_w) , the system first outputs a list of hash indices

$$\mathcal{L} = d_1(y^N, p_w) \subset [1 : M_C], \quad (3)$$

and then guesses the user index as well as estimates the secret key

$$(\hat{w}, \hat{s}) = d_2(y^N, (\mathcal{J}_L, \mathcal{B}_L, \mathcal{L}), p_w), \quad (4)$$

where $(\mathcal{J}_L, \mathcal{B}_L, \mathcal{L}) = \{(j_w, w, c) | w \in \mathcal{B}(c), c \in \mathcal{L}\}$. Since $\mathcal{L}$ is a subset of $[1 : M_C]$, we have that $|\mathcal{L}| \leq M_C$ holds.

We define the achievability of a rate tuple $(R_I, R_S, R_P, R_C, R_J, R_L)$ in a generated secret key system without privacy leakage as follows.

Definition 1: A tuple of identification rate R_I , secret key rate R_S , and private key rate R_P , the first layer helper data rate R_C , the second layer helper data rate R_J , and list rate R_L , $(R_I, R_S, R_P, R_C, R_J, R_L) \in \mathbb{R}_+^6$, is *achievable* if for all $\delta > 0$ there exists some $N_0(\delta) \geq 1$, as well as enrollment and identification mappings such that for any $N \geq N_0(\delta)$, the following conditions are satisfied

$$\Pr\{(\hat{W}, \hat{S}) \neq (W, S_W)\} \leq \delta, \quad (5a)$$

$$\Pr\{C_W \notin \mathcal{L}\} \leq \delta, \quad (5b)$$

$$\log M_I \geq N(R_I - \delta), \quad (5c)$$

$$H(S_W) + N\delta \geq \log M_S \geq N(R_S - \delta), \quad (5d)$$

$$\log M_P \leq N(R_P + \delta), \quad (5e)$$

$$\log M_C \leq N(R_C + \delta), \quad (5f)$$

$$\log M_C \leq H(C_W) + N\delta, \quad (5g)$$

$$\log M_J \leq N(R_J + \delta), \quad (5h)$$

$$\log M_L \leq N(R_L + \delta), \quad (5i)$$

$$I(S_W; C_W, J_W) + I(X^N(W); C_W, J_W) \leq N\delta. \quad (5j)$$

Moreover, we use $\mathcal{R}_g$ to denote the capacity region that contains *all* achievable rate tuples $(R_I, R_S, R_P, R_C, R_J, R_L)$ for a generated secret key system.

The inequalities in the definition above can be interpreted as follows: (5a) requires that the identification system should reliably return the true user index and the corresponding secret key; (5b) requires that the true hash index is included in the output list; (5c), (5d), (5e), (5f), (5g), (5h), (5i) and define the identification rate, the secret key rate private key rate, first layer helper data rate, second layer helper data rate, and list rate, respectively; (5d) and (5g) state that secret keys and the first layer hash indices are close to uniformly distributed; (5j) ensures the identification system is secrecy-preserving and privacy-preserving such that for each user, both first and second layer helper data leak only negligible information about the secret key and the biometric sequence.

We further explain the rates defined in (5c), (5d), (5e), (5f), (5h), and (5i) as follows. The identification rate R_I defined in (5c) relates to the number of users that can be reliably identified. The secret key rate R_S defined in (5d) relates to the length of the secret key. The private key rate R_P defined in (5e) relates to the length of the private key needed to protect the privacy of the biometrics. The first and second layer helper data rates R_C and R_J defined in (5f) and (5h) relate to the

length of the first and second layer helper data needed for reliable identification and authentication, respectively. The list rate R_L defined in (5i) relates to the size of the list in the first stage of the identification.

B. Chosen Secret Key System

Fig. 2 illustrates a chosen secret key system. In the enrollment phase, the enrollment mapping outputs a hash index c_w using inputs to the system $(x^N(w), p_w, s_w)$, i.e.,

$$c_w = e_1(x^N(w), p_w, s_w), \quad (6)$$

where the secret key s_w and private key p_w are chosen uniformly at random from $[1 : M_S]$ and $[1 : M_P]$, respectively. Moreover, similar to the generated secret key system, c_w is put in the first layer helper database at location w . Then the enrollment mapping uses $(x^N(w), p_w, s_w)$ to generate second layer helper data j_w , i.e.,

$$j_w = e_2(x^N(w), p_w, s_w). \quad (7)$$

In the identification phase, similar to (3) and (4) in the generated secret key system, the system firstly outputs a list of hash indices, and then estimates the user index and the secret key using the observation Y^N , the private key P_W and $(\mathcal{J}_L, \mathcal{B}_L, \mathcal{L})$.

We define the achievability of a rate tuple in a chosen secret key system as follows.

Definition 2: A tuple of identification rate R_I , chosen secret key rate R_S , and private key rate R_P , the first layer helper data rate R_C , the second layer helper data rate R_J , and list rate R_L , $(R_I, R_S, R_P, R_C, R_J, R_L) \in \mathbb{R}_+^6$, is *achievable* if for all $\delta > 0$ there exists some $N_0(\delta) \geq 1$, enrollment and identification mappings such that for any $N \geq N_0(\delta)$, (5a), (5b), (5c), (5e), (5f), (5h), (5i), (5j) and

$$\log M_S \geq N(R_S - \delta), \quad (8)$$

are satisfied. We use $\mathcal{R}_c$ to denote the capacity region that contains *all* achievable rate tuples $(R_I, R_S, R_P, R_C, R_J, R_L)$ for a two-stage biometric identification system using chosen secret key system without privacy leakage.

III. STATEMENT OF RESULTS

A. Main Results

Theorem 1: For a two-stage biometric identification system using generated secret keys without privacy leakage, the capacity region is given by

$$\begin{aligned} \mathcal{R}_g = \{ & (R_I, R_S, R_P, R_C, R_J, R_L) : \\ & R_I + R_S \leq R_P + I(U, V; Y), \\ & R_I + I(U, V; X) \leq R_P + I(U, V; Y), \\ & R_I + I(U, V; X) \leq R_C + R_J + I(U, V; Y), \\ & R_L \geq I(U; X) - I(U; Y), \\ & \text{for some } P_{UVXY} = Q_X Q_{Y|X} P_{V|X} P_{U|V}, \\ & \text{and } |\mathcal{U}| \leq |\mathcal{X}| + 3, |\mathcal{V}| \leq |\mathcal{U}||\mathcal{X}| + 1 \}. \end{aligned} \quad (9)$$

Theorem 2: For a two-stage biometric identification system using chosen secret keys without privacy leakage, the capacity region is given by

$$\begin{aligned} \mathcal{R}_c = \{ & (R_I, R_S, R_P, R_C, R_J, R_L) : \\ & R_I + R_S \leq R_P + I(U, V; Y), \\ & R_I + I(U, V; X) \leq R_P + I(U, V; Y), \\ & R_I + I(U, V; X) + R_S \leq R_C + R_J + I(U, V; Y), \\ & R_L \geq I(U; X) - I(U; Y), \\ & \text{for some } P_{UVXY} = Q_X Q_{Y|X} P_{V|X} P_{U|V}, \\ & \text{and } |\mathcal{U}| \leq |\mathcal{X}| + 3, |\mathcal{V}| \leq |\mathcal{U}||\mathcal{X}| + 1 \}. \end{aligned} \quad (10)$$

The proofs of Theorem 1 and Theorem 2 are given in Section IV. From the capacity regions for the generated and chosen secret key systems, we have the following remarks.

Remark 1: Comparing (9) and (10), it follows that to achieve the a rate tuple (R_I, R_S, R_P, R_L) , the chosen secret key system requires a larger helper data rate $R_C + R_J$.

Remark 2: If $R_J^1 \leq R_J^2$, then $\mathcal{R}_g(R_J^1) \subseteq \mathcal{R}_g(R_J^2)$ and $\mathcal{R}_c(R_J^1) \subseteq \mathcal{R}_c(R_J^2)$. Additionally, there exists a R_{J_0} such that for every $R_J \geq R_{J_0}$, $\mathcal{R}_g(R_J) = \mathcal{R}_c(R_J) = \mathcal{R}^*$.

If we increase the helper data rate, the capacity region is larger. If the storage can be sufficiently large, then the generated and chosen secret key systems achieve the same capacity region.

Remark 3: If we fix V , the capacity regions can be reduced to that of the single-stage [17].

This shows that the single-stage setting in [17] is a special case of the multi-stage setting. Moreover, compared to [17], this work additionally studies the helper data rate and list rate.

Remark 4: If we fix V and let $R_I = 0$, the capacity regions $\mathcal{R}_g$ and $\mathcal{R}_c$ can be reduced to the region $\mathcal{R}_1$ in [6].

This shows that the single-user setting in [6] is a special case of the multi-user setting in this work.

B. Complexity Discussion

In this section, we show that the two-stage setting results in lower search complexity. The following complexity analysis is based on the assumption that the search complexity is in the order of the total number of different entries in the database [3], [4]. Note that the number of different entries only depends on the length of the entries, which at each stage is shorter than in the single-stage identification setting (a special case of the two-stage setting).

To achieve some identification rate R_I , the system can do an exhaustive search on all enrolled users. This results in a search complexity in the order of the total number of enrolled user, i.e.,

$$S = \mathcal{O}(2^{NR_I}). \quad (11)$$

The corresponding complexity exponent is

$$S_e = R_I. \quad (12)$$

In this work, we design a two-stage identification scheme that avoids an exhaustive search. Upon observing an unknown user, the system searches among all 2^{NR_C} hash indices and outputs a list that includes 2^{NR_L} hash indices. Consequently,

the search complexity of the first-stage identification procedure is

$$S_1 = \mathcal{O}(2^{NR_C}). \quad (13)$$

In the second stage, the system compares the observed user with the users obtained in the first stage. As indicated in (5f), the hash indices are close to uniformly distributed. Therefore, approximately the same number of users result in a certain hash index, i.e., $2^{N(R_I - R_C)}$. To determine the user index, the system does $2^{N(R_I - R_C + R_L)}$ checks. Thus, this second stage identification procedure results in search complexity

$$S_2 = \mathcal{O}(2^{N(R_I - R_C + R_L)}). \quad (14)$$

As a consequence, the overall complexity exponent of the two-stage identification scheme is

$$S_{e2} = \limsup_{N \rightarrow \infty} \frac{\log(S_1 + S_2)}{N} = \max\{R_C, R_I - R_C + R_L\}. \quad (15)$$

Since $R_C \leq R_I$ and $R_C \geq R_L$ always hold, we obtain that $S_{e2} \leq S_e$. Eq (15) also implies that for some fixed R_C , when $R_L \geq 2R_C - R_I$, the overall complexity increases as the list rate R_L increases.

IV. PROOFS

A. Proof of Theorem 1

1) Achievability: Fix the conditional p.m.f. $P_{V|X}$ and $P_{U|V}$. The number of enrolled users is assumed to be $M_I = 2^{NR_I}$. Also fix some $\delta > 0$.

Codebook generation: Pick a rate tuple $(R_I, R_S, R_P, R_C, R_J, R_L) \in \mathcal{R}_g$ such that

$$\begin{aligned} R_P &\geq R_I + I(U, V; X) - I(U, V; Y) + 5\delta, \\ R_J &= R_I + I(U, V; X) - I(U, V; Y) + 5\delta - R_C, \\ R_S &= R_P - R_I + I(U, V; Y) - 3\delta, \\ R_C &> R_L = I(U; X) - I(U; Y) + 5\delta. \end{aligned} \quad (16)$$

Additionally, we fix auxiliary rates

$$\begin{aligned} R_1 &= I(U; X) - I(U; Y) + 2\delta, \\ R_2 &= I(U; Y) - \delta, \\ R_3 &= I(V; X|U) - I(V; Y|U) + 3\delta, \\ R_4 &= I(V; Y|U) - 2\delta. \end{aligned} \quad (17)$$

Randomly and independently generate $2^{N(R_1 + R_2)}$ i.i.d. codewords $u^N(k_1, m_1)$ according to P_U . Then we distribute the codewords into 2^{NR_1} bins indexed by $k_1 \in [1 : 2^{NR_1}]$. Each bin consists of 2^{NR_2} codewords indexed by $m_1 \in [1 : 2^{NR_2}]$. Furthermore, for each codeword $u^N(k_1, m_1)$, where $(k_1, m_1) \in [1 : 2^{NR_1}] \times [1 : 2^{NR_2}]$, randomly and independently generate $2^{N(R_3 + R_4)}$ codewords $v^N(k_1, m_1, k_2, m_2)$ according to $\prod_{i=1}^N P_{V|U=u_i(k_1, m_1)}$. We distribute the $2^{N(R_3 + R_4)}$ codewords into 2^{NR_3} bins indexed by $k_2 \in [1 : 2^{NR_3}]$. Each bin consists of 2^{NR_4} codewords indexed by $m_2 \in [1 : 2^{NR_4}]$.

Fig. 3: Illustration of generating helper data and secret keys in the generated secret key system.

Enrollment: For each user $w \in [1 : M_I]$, given the private key of this user p_w , we divide it into three parts, $\check{p}_w$, $\bar{p}_w$, and $\tilde{p}_w$, such that $p_w = (\check{p}_w, \bar{p}_w, \tilde{p}_w)$, $\check{p}_w \in [1 : 2^{NR_C}]$, $\bar{p}_w \in [1 : 2^{NR_J}]$ and $\tilde{p}_w \in [1 : 2^{N(R_P - R_C - R_J)}]$. For $\check{p}_w$ and $\bar{p}_w$, we further divide both of them into two parts as $\check{p}_w = (\check{p}_{1w}, \check{p}_{2w})$ and $\bar{p}_w = (\bar{p}_{1w}, \bar{p}_{2w})$, where $\check{p}_{1w} \in [1 : 2^{NR_1}]$, $\check{p}_{2w} \in [1 : 2^{N(R_C - R_1)}]$, $\bar{p}_{1w} \in [1 : 2^{NR_3}]$, $\bar{p}_{2w} \in [1 : 2^{N(R_J - R_3)}]$. For each user $w \in [1 : 2^{NR_I}]$, the enrollment mapping firstly looks for a codeword $u^N(k_{1w}, m_{1w})$ such that $(u^N(k_{1w}, m_{1w}), x^N(w)) \in \mathcal{T}_\epsilon^N$. If no such codeword exists, randomly choose a codeword index pair from $[1 : 2^{NR_1}] \times [1 : 2^{NR_2}]$. If there is more than one such codewords, randomly choose one from them. Then the enrollment mapping uses k_{1w} and the private key p_w to generate the first layer helper data c_w as $c_w = (k_{1w} \oplus \check{p}_{1w}, \check{p}_{2w})$, which is called hash index. We further put the user index w in a set of user indices, which is denoted by $\mathcal{B}(c_w)$. Secondly, the enrollment mapping looks for a codeword $v^N(k_{1w}, m_{1w}, k_{2w}, m_{2w})$ such that $(u^N(k_{1w}, m_{1w}), v^N(k_{1w}, m_{1w}, k_{2w}, m_{2w}), x^N(w)) \in \mathcal{T}_\epsilon^N$. If no such (k_{2w}, m_{2w}) exists, randomly choose one from $[1 : 2^{NR_3}] \times [1 : 2^{NR_4}]$. If there is more than one such (k_{2w}, m_{2w}) , randomly choose one from them. With the bin index k_{2w} and the private key p_w , the enrollment mapping generates the second layer helper data j_w as $j_w = (k_{2w} \oplus \bar{p}_{1w}, \bar{p}_{2w})$. Using the codeword index tuple $(k_{1w}, m_{1w}, k_{2w}, m_{2w})$ and the private key p_w , the secret key s_w is generated as $s_w = (k_{1w}, m_{1w}, k_{2w}, m_{2w}, \tilde{p}_w)$. Therefore, the three parts of the private key are used to generate the first layer helper data, the second layer helper data, and the secret key, respectively. The procedure of generating the helper data and secret keys is illustrated in Fig. 3. The codebooks and mappings are revealed to all parties.

Identification: Upon receiving the observation y^N and having access to the corresponding private key p_w of the observed user w , the system firstly looks for a list of hash indices $\mathcal{L}(y^N, p_w)$ such that for each hash index $c \in \mathcal{L}(y^N, p_w)$, there exists (k_1, m_1) that satisfies $c = (k_1 \oplus \check{p}_{1w}, \check{p}_{2w})$ and $(u^N(k_1, m_1), y^N) \in \mathcal{T}_\epsilon^N$. Next, the system checks users with index in $\{w : w \in \mathcal{B}(c), c \in \mathcal{L}\}$, which is denoted by $\mathcal{B}_\mathcal{L}$, and looks for a unique tuple $(\hat{w}, \hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2)$ that satisfies $c_{\hat{w}} \in \mathcal{L}(y^N, p_w)$, $c_{\hat{w}} = (\hat{k}_1 \oplus \check{p}_{1w}, \check{p}_{2w})$, $j_{\hat{w}} = (k_2 \oplus \bar{p}_{1w}, \bar{p}_{2w})$ and $(u^N(\hat{k}_1, \hat{m}_1), v^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), y^N) \sim \mathcal{T}_\epsilon^N$. The estimated secret key is $\hat{s} = (\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2, \tilde{p}_w)$.

Error Events Analysis: Assume that the user W is observed. Let $(K_{1W}, M_{1W}, K_{2W}, M_{2W})$ be the actual codeword index tuple determined by the enrollment mapping, C_W and J_W be the actual first layer helper data and second layer helper data, $P_W = (\check{P}_{1W}, \check{P}_{2W}, \bar{P}_{1W}, \bar{P}_{2W}, \tilde{P}_W)$ be the private key, and S_W be the actual secret key respectively. We firstly define the following event:

$$\begin{aligned} B(\hat{w}, \hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2) &= \{C_{\hat{w}} \in \mathcal{L}(Y^N, P_W), \\ C_{\hat{w}} &= (\hat{k}_1 \oplus \check{P}_{1W}, \check{P}_{2W}), J_{\hat{w}} = (\hat{k}_2 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ (U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) &\in \mathcal{T}_\epsilon^N\}. \end{aligned} \quad (18)$$

Then we have the following error events:

$$\begin{aligned} \mathcal{E}_1 &= \{(U^N(k_1, m_1), X^N(W)) \notin \mathcal{T}_\epsilon^N, \\ &\quad \forall (k_1, m_1) \in [1 : 2^{NR_1}] \times [1 : 2^{NR_2}]\}, \\ \mathcal{E}_2 &= \{(U^N(K_{1W}, M_{1W}), V^N(K_{1W}, M_{1W}, k_2, m_2)), \\ &\quad X^N) \notin \mathcal{T}_\epsilon^N, \forall (k_2, m_2) \in [1 : 2^{NR_3}] \times [1 : 2^{NR_4}]\}, \\ \mathcal{E}_3 &= \{(U^N(K_{1W}, M_{1W}), V^N(K_{1W}, M_{1W}, K_{2W}, M_{2W}), \\ &\quad Y^N) \notin \mathcal{T}_\epsilon^N\}, \\ \mathcal{E}_4 &= \{|\{c : \exists (k_1, m_1) \text{ such that } (U^N(k_1, m_1), Y^N) \in \mathcal{T}_\epsilon^N, \\ &\quad c = (k_1 \oplus \check{P}_{1W}, \check{P}_{2W})\}| > 2^{NR_L}\}, \\ \mathcal{E}_5 &= \bigcup_{\hat{w} \neq W} \bigcup_{\hat{k}_1} \bigcup_{\hat{m}_1} \bigcup_{\hat{k}_2} \bigcup_{\hat{m}_2} B(\hat{w}, \hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), \\ \mathcal{E}_6 &= \bigcup_{(\hat{m}_1, \hat{m}_2) \neq (M_{1W}, M_{2W})} B(W, K_{1W}, \hat{m}_1, K_{2W}, \hat{m}_2). \end{aligned} \quad (19)$$

The first two error events, $\mathcal{E}_1$ and $\mathcal{E}_2$, correspond to enrollment errors, i.e., there is no codeword jointly typical with the biometric sequence. The last four errors are errors that happen in the identification and authentication phase. The error event $\mathcal{E}_3$ is the case where the true codewords are not jointly typical with the observation Y^N . The error $\mathcal{E}_4$ is the event where in the first identification step are more than 2^{NR_L} hash indices satisfying the required conditions such that the true hash index might not be included in the output list $\mathcal{L}(Y^N, P_W)$. The error event $\mathcal{E}_5$ is the error that there exists another user index $\hat{w}$ that fulfills all conditions, which we call *identification error*. The error event $\mathcal{E}_6$ is the case where the user index is correctly identified but the estimated secret key is not the same as the true one, which we call *authentication error*. Note that the authentication error is under the condition that the user index is correctly identified, which implies that the true index pair (K_{1W}, K_{2W}) can be correctly estimated. Due to the construction of the secret key, the authentication error happens only when the true index pair (M_{1W}, M_{2W}) is not correctly estimated.

Due to the construction of helper data, the identification error $\mathcal{E}_5$ can be split in the following four cases

$$\begin{aligned} \mathcal{E}_{51} &= \bigcup_{\hat{w} \neq W} \bigcup_{\hat{k}_1 \neq K_{1W}} \bigcup_{\hat{m}_1} \bigcup_{\hat{m}_2} B(\hat{w}, \hat{k}_1, \hat{m}_1, K_{2W}, \hat{m}_2), \\ \mathcal{E}_{52} &= \bigcup_{\hat{w} \neq W} \bigcup_{\hat{m}_1} \bigcup_{\hat{k}_2 \neq K_{2W}} \bigcup_{\hat{m}_2} B(\hat{w}, K_{1W}, \hat{m}_1, \hat{k}_2, \hat{m}_2), \\ \mathcal{E}_{53} &= \bigcup_{\hat{w} \neq W} \bigcup_{\hat{k}_1 \neq K_{1W}} \bigcup_{\hat{m}_1} \bigcup_{\hat{k}_2 \neq K_{2W}} \bigcup_{\hat{m}_2} B(\hat{w}, \hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), \end{aligned}$$

$$\mathcal{E}_{54} = \bigcup_{\hat{w} \neq W} \bigcup_{\hat{m}_1} \bigcup_{\hat{m}_2} B(\hat{w}, K_{1W}, \hat{m}_1, K_{2W}, \hat{m}_2). \quad (20)$$

Similarly, the authentication error $\mathcal{E}_6$ can be split in the following three cases

$$\begin{aligned} \mathcal{E}_{61} &= \bigcup_{\hat{m}_1 \neq M_{1W}} B(W, K_{1W}, \hat{m}_1, K_{2W}, M_{2W}), \\ \mathcal{E}_{62} &= \bigcup_{\hat{m}_2 \neq M_{2W}} B(W, K_{1W}, M_{1W}, K_{1W}, \hat{m}_2), \\ \mathcal{E}_{63} &= \bigcup_{\hat{m}_1 \neq M_{1W}} \bigcup_{\hat{m}_2 \neq M_{2W}} B(W, K_{1W}, \hat{m}_1, K_{1W}, \hat{m}_2). \end{aligned}$$

The identification and authentication will be successful when none of the above error events happen. Hence, we have the following

$$\begin{aligned} \mathcal{E} &\subset \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3 \cup \mathcal{E}_4 \cup \mathcal{E}_{51} \\ &\quad \cup \mathcal{E}_{52} \cup \mathcal{E}_{53} \cup \mathcal{E}_{54} \cup \mathcal{E}_{61} \cup \mathcal{E}_{62} \cup \mathcal{E}_{63}. \end{aligned}$$

The probability $\Pr(\mathcal{E}_1) \rightarrow 0$ as $N \rightarrow \infty$ since $R_1 + R_2 > I(U; X)$ due to the covering lemma [24, Lemma 3.3]. Similarly, $\Pr(\mathcal{E}_1^c \cap \mathcal{E}_2) \rightarrow 0$ as $N \rightarrow \infty$ as $R_3 + R_4 > I(V; X|U)$ according to the covering lemma [24, Lemma 3.3]. $\Pr(\mathcal{E}_1^c \cap \mathcal{E}_2^c \cap \mathcal{E}_3) \rightarrow 0$ as $N \rightarrow \infty$ according to the Markov lemma [24, p.27].

Next, we consider the error event $\mathcal{E}_4$

$$\begin{aligned} \Pr(\mathcal{E}_4) &\stackrel{(a)}{\leq} \mathbb{E}\{|\{c : \exists(k_1, m_1) \text{ such that } c = (k_1 \oplus \check{P}_{1W}, \\ &\quad \check{P}_{2W}), (U^N(k_1, m_1), Y^N) \in \mathcal{T}_\epsilon^N(U, Y)\}|\} \frac{1}{2^{NR_L}} \\ &= \frac{1}{2^{NR_L}} \sum_c \sum_{k_1} \sum_{m_1} \Pr\{c = (k_1 \oplus \check{P}_{1W}, \check{P}_{2W})\} \\ &\quad \sum_{u^N} \Pr\{U^N(k_1, m_1) = u^N\} \\ &\quad \sum_{y^N} \Pr\{Y^N = y^N\} \mathbb{1}_{\mathcal{T}_\epsilon^N}(u^N, y^N) \\ &\stackrel{(b)}{\leq} 2^{N(R_1+R_2-R_L)} |\mathcal{T}_\epsilon^N(U, Y)| 2^{-N(H(U)+H(Y)-2\delta)} \\ &\leq 2^{N(I(U;X)-I(U;Y)-R_L+4\delta)}, \end{aligned} \quad (21)$$

where (a) follows from Markov inequality; (b) follows from the fact that for $\forall k_1$, $\sum_c \Pr\{c = (k_1 \oplus \check{P}_{1W}, \check{P}_{2W})\} \leq 1$ holds; $\mathbb{1}_{\mathcal{T}}(\cdot)$ is defined as the following indicator function:

$$\mathbb{1}_{\mathcal{T}}(t) = \begin{cases} 1 & t \in \mathcal{T}, \\ 0 & \text{otherwise.} \end{cases} \quad (22)$$

Since $R_L > I(U; X) - I(U; Y) + 4\delta$, we obtain that $\Pr(\mathcal{E}_4) \rightarrow 0$ as $N \rightarrow \infty$. Given $\Pr(\mathcal{E}_4) \rightarrow 0$ and $\Pr(\mathcal{E}_1^c \cap \mathcal{E}_2^c \cap \mathcal{E}_3) \rightarrow 0$ as $N \rightarrow \infty$, it follows that

$$\Pr(C_W \notin \mathcal{L}) \rightarrow 0, \text{ as } N \rightarrow \infty. \quad (23)$$

In the following analysis, due to symmetry and without loss of generality, we condition on the event $(W = 1, (K_{11}, M_{11}, K_{21}, M_{21}) = (1, 1, 1, 1))$, which is denoted with A . To defer some technical derivations, we include the following lemmas and claims. The two lemmas provide bounds on conditional probabilities based on the properties

of joint typicality. The first two claims provide bounds on conditional probabilities based on the use of the two lemmas. The third claim bounds the probability of both conditional probabilities and helper data.

Lemma 1 ([25]): Let $(U, Y) \sim p(u, y)$ and $\epsilon' > \epsilon > 0$. Let $Y^N \sim \prod_{i=1}^N p_Y(y_i)$ and $U^N(m), m \in [1 : 2^{NR}]$ be independently generated according to $\prod_{i=1}^N p_U(u_i)$, independent of Y^N . Let $\mathcal{I} = \{m \in [1 : 2^{NR}] : (U^N(m), Y^N) \in \mathcal{T}_\epsilon^{(n)}(U, Y)\}$ be a set of random indices and let $M \sim \text{Unif}(\mathcal{I})$, if $|\mathcal{I}| > 0$ and $M \sim \text{Unif}([1 : 2^{NR}])$, otherwise. Then, for every $(u^N, \tilde{u}^N, y^N)$,

$$\begin{aligned} \Pr\{U^N(2) = u^N \mid U^N(1) = \tilde{u}^N, Y^N = y^N, M = 1\} \\ \leq (1 + \epsilon') \cdot \prod_{i=1}^N p_U(u_i) \end{aligned} \quad (24)$$

for N sufficiently large.

Proof: The proof is given in [25, Appendix A].

The following lemma is an extension of Lemma 1.

Lemma 2 ([26]): Let $(U, V, X) \sim p(u, v, x)$ and $\epsilon' > \epsilon > 0$, where ϵ' is a fixed number and $\epsilon \rightarrow 0$ as $N \rightarrow \infty$. Assume that $(U^N, X^N) \sim p(u^N, x^N)$, which is not necessarily independent and identically distributed. For a given $X^N = x^N$, we generate 2^{NR_V} i.i.d. codewords $V^N \sim \prod_{i=1}^N p_{V|U}(v_i|u_i)$, which are also conditionally independent of U^N given $X^N = x^N$. Let $\mathcal{I} = \{m \in [1 : 2^{NR}] : (V^N(m), U^N, X^N) \in \mathcal{T}_\epsilon^{(n)}(V, U, X)\}$ be a random set of indices induced by the random codebook and random vectors U^N and X^N . Let $M \sim \text{Unif}(\mathcal{I})$ if $|\mathcal{I}| > 0$ and $M \sim \text{Unif}([1 : 2^{NR}])$ otherwise. Then, for sufficiently large N ,

$$\begin{aligned} \Pr\{V^N(2) = v^N \mid V^N(1) = \tilde{v}^N, U^N = u^N, \\ X^N = y^N, M = 1\} \leq (1 + \epsilon') \cdot \prod_{i=1}^N p_{V|U}(v_i|u_i). \end{aligned} \quad (25)$$

Proof: The proof is given in [26, Section IV].

Claim 1: For some $(\hat{k}_2, \hat{m}_2) \neq (1, 1)$, we have that

$$\begin{aligned} \Pr\{(U^N(1, 1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N|A\} \\ \leq (1 + \epsilon') 2^{-N(I(V;Y|U)-\delta)}, \end{aligned} \quad (26)$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$.

Proof: The proof is given in Appendix A-A.

Claim 2: For some $(\hat{k}_1, \hat{m}_1) \neq (1, 1)$, and $(\hat{k}_2, \hat{m}_2) \in [1 : 2^{NR_3}] \times [1 : 2^{NR_4}]$, we have that

$$\begin{aligned} \Pr\{(U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N|A\} \\ \leq (1 + \epsilon') 2^{-N(I(U,V;Y)-2\delta)}, \end{aligned} \quad (27)$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$.

Proof: The proof is given in Appendix A-B.

Claim 3: For some $\hat{w} \neq 1$ and $(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2) \in [1 : 2^{NR_1}] \times [1 : 2^{NR_2}] \times [1 : 2^{NR_3}] \times [1 : 2^{NR_4}]$, where $(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2)$ and Y^N are not necessarily independent, we have that

$$\begin{aligned} \Pr\{C_{\hat{w}} = (\hat{k}_1 \oplus \check{P}_{11}, \check{P}_{21}), J_{\hat{w}} = (\hat{k}_2 \oplus \bar{P}_{11}, \bar{P}_{21}), \\ (U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N|A\} \end{aligned}$$

$$\leq 2^{-N(R_C+R_J)} \cdot \Pr\{(U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N\}. \quad (28)$$

Proof: The proof is given in Appendix A-C. The probability $\Pr(\mathcal{E}_{51}|A)$ can be bounded as follows

$$\begin{aligned} \Pr(\mathcal{E}_{51}|A) &= \Pr\{C_{\hat{w}} = (\hat{k}_1 \oplus \check{P}_{1W}, \check{P}_{2W}), J_{\hat{w}} = (1 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ &\quad (U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \\ &\quad \text{for some } \hat{w} \neq 1, \hat{k}_1 \neq 1, \text{ and } (\hat{m}_1, \hat{m}_2)|A\} \\ &\stackrel{(a)}{\leq} \sum_{\hat{w} \neq 1} \sum_{\hat{k}_1 \neq 1} \sum_{\hat{m}_1} \sum_{\hat{m}_2} \Pr\{C_{\hat{w}} = (\hat{k}_1 \oplus \check{P}_{1W}, \check{P}_{2W}), \\ &\quad J_{\hat{w}} = (1 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ &\quad (U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N|A\} \\ &\stackrel{(b)}{\leq} (1 + \epsilon') 2^{-N(R_C+R_J+I(U,V;Y)-2\delta-R_I-R_1-R_2-R_4)} \\ &= (1 + \epsilon') 2^{-N(R_C+R_J-R_I+I(U;Y)-I(U;X)-\delta)}, \quad (29) \end{aligned}$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$; (a) follows from the union bound; (b) follows from Claim 2 and Claim 3. Since $R_C + R_J > R_I + I(U; X) - I(U; Y) + \delta$ due to (16), we obtain that $\Pr(\mathcal{E}_{51}|A) \rightarrow 0$ as $N \rightarrow \infty$.

For $\Pr(\mathcal{E}_{52}|A)$, we have that

$$\begin{aligned} \Pr(\mathcal{E}_{52}|A) &= \Pr\{C_{\hat{w}} = (1 \oplus \check{P}_{1W}, \check{P}_{2W}), J_{\hat{w}} = (\hat{k}_2 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ &\quad (U^N(1, \hat{m}_1), V^N(1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \\ &\quad \text{for some } \hat{w} \neq 1, \hat{k}_2 \neq 1, \text{ and } (\hat{m}_1, \hat{m}_2)|A\} \\ &\stackrel{(a)}{\leq} \Pr\{C_{\hat{w}} = (1 \oplus \check{P}_{1W}, \check{P}_{2W}), J_{\hat{w}} = (\hat{k}_2 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ &\quad (U^N(1, 1), V^N(1, 1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \\ &\quad \text{for some } \hat{w} \neq 1, \hat{k}_2 \neq 1, \text{ and } \hat{m}_2|A\} + \\ &\quad \Pr\{C_{\hat{w}} = (1 \oplus \check{P}_{1W}, \check{P}_{2W}), J_{\hat{w}} = (\hat{k}_2 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ &\quad (U^N(1, \hat{m}_1), V^N(1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \\ &\quad \text{for some } \hat{w} \neq 1, \hat{m}_1 \neq 1, \hat{k}_2 \neq 1, \text{ and } \hat{m}_2|A\} \\ &\stackrel{(b)}{\leq} (1 + \epsilon') 2^{-N(R_C+R_J+I(V;Y|U)-\delta-R_I)} \\ &\quad + \sum_{\hat{w} \neq 1} \sum_{\hat{m}_1 \neq 1} \sum_{\hat{k}_2 \neq 1} \sum_{\hat{m}_2} \Pr\{C_{\hat{w}} = (k_1 \oplus \check{P}_{11}, \check{P}_{21}), \\ &\quad J_{\hat{w}} = (\hat{k}_2 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ &\quad (U^N(k_1, \hat{m}_1), V^N(k_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N|A\} \\ &\stackrel{(c)}{\leq} (1 + \epsilon') 2^{-N(R_C+R_J-R_I+I(V;Y|U)-\delta)} \\ &\quad + (1 + \epsilon') 2^{-N(R_C+R_J+I(U,V;Y)-2\delta-R_I-R_2-R_3-R_4)} \\ &= (1 + \epsilon') 2^{-N(R_C+R_J-R_I+I(V;Y|U)-\delta)} \\ &\quad + (1 + \epsilon') 2^{-N(R_C+R_J-R_I+I(V;Y|U)-I(V;X|U)-2\delta)} \quad (30) \end{aligned}$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$; (a) follows by considering two cases of $\hat{m}_1$; (b) follows from the union bound, Claim 1 and Claim 3; (c) follows from Claim 2 and Claim 3. Since $R_C + R_J > R_I + I(V; X|U) - I(V; Y|U) + 2\delta$ due to (16), we obtain that $\Pr(\mathcal{E}_{52}|A) \rightarrow 0$ as $N \rightarrow \infty$.

The probability $\Pr(\mathcal{E}_{53}|A)$ can be bounded as

$$\begin{aligned} \Pr(\mathcal{E}_{53}|A) &= \Pr\{C_{\hat{w}} = (\hat{k}_1 \oplus \check{P}_{1W}, \check{P}_{2W}), J_{\hat{w}} = (\hat{k}_2 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ &\quad (U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \text{ for} \\ &\quad \text{some } \hat{w} \neq 1, \hat{k}_1 \neq 1, \hat{k}_2 \neq 1, \text{ and } (\hat{m}_1, \hat{m}_2)|A\} \\ &\stackrel{(a)}{\leq} \sum_{\hat{w} \neq 1} \sum_{\hat{k}_1 \neq 1} \sum_{\hat{m}_1} \sum_{\hat{k}_2 \neq 1} \sum_{\hat{m}_2} \Pr\{C_{\hat{w}} = (\hat{k}_1 \oplus \check{P}_{11}, \check{P}_{21}), \\ &\quad J_{\hat{w}} = (\hat{k}_2 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ &\quad (U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N|A\} \\ &\stackrel{(b)}{\leq} (1 + \epsilon') 2^{-N(R_C+R_J+I(U,V;Y)-2\delta-R_I-R_1-R_2-R_3-R_4)} \\ &= (1 + \epsilon') 2^{-N(R_C+R_J+I(U,V;Y)-R_I-I(U,V;X)-4\delta)} \quad (31) \end{aligned}$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$; (a) follows from the union bound; (b) follows from Claim 2 and Claim 3. Since $R_C + R_J > R_I + I(U, V; X) - I(U, V; Y) + 4\delta$ from (16), we obtain that $\Pr(\mathcal{E}_{53}|A) \rightarrow 0$ as $N \rightarrow \infty$.

Next we consider the probability $\Pr\{\mathcal{E}_{54}|A\}$

$$\begin{aligned} \Pr(\mathcal{E}_{54}|A) &= \Pr\{C_{\hat{w}} = (1 \oplus \check{P}_{1W}, \check{P}_{2W}), J_{\hat{w}} = (1 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ &\quad (U^N(1, \hat{m}_1), V^N(1, \hat{m}_1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \\ &\quad \text{for some } \hat{w} \neq 1, \text{ and } (\hat{m}_1, \hat{m}_2)|A\} \\ &\leq \sum_{\hat{w} \neq 1} \sum_{\hat{m}_1} \sum_{\hat{m}_2} \Pr\{C_{\hat{w}} = (1 \oplus \check{P}_{1W}, \check{P}_{2W}), \\ &\quad J_{\hat{w}} = (1 \oplus \bar{P}_{1W}, \bar{P}_{2W}), \\ &\quad (U^N(1, \hat{m}_1), V^N(1, \hat{m}_1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N|A\} \\ &\stackrel{(b)}{\leq} 2^{-N(R_C+R_J)} \sum_{\hat{w} \neq 1} \sum_{\hat{m}_1} \sum_{\hat{m}_2} \Pr\{(U^N(1, \hat{m}_1), \\ &\quad V^N(1, \hat{m}_1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N|A\} \\ &\stackrel{(c)}{\leq} 2^{-N(R_C+R_J)} \sum_{\hat{w} \neq 1} \left[\sum_{\hat{m}_1 \neq 1} \sum_{\hat{m}_2} \Pr\{(U^N(1, \hat{m}_1), \right. \\ &\quad V^N(1, \hat{m}_1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N|A\} \\ &\quad + \sum_{\hat{m}_2 \neq 1} \Pr\{(U^N(1, 1), V^N(1, 1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N|A\} \\ &\quad \left. + \Pr\{(U^N(1, 1), V^N(1, 1, 1, 1), Y^N) \in \mathcal{T}_\epsilon^N|A\} \right] \\ &\stackrel{(d)}{\leq} 2^{-N(R_C+R_J-R_I)} \left[(1 + \epsilon') 2^{N(R_2+R_4-I(U,V;Y)+2\delta)} \right. \\ &\quad \left. + (1 + \epsilon') 2^{N(R_4-I(V;Y|U)+\delta)} + 1 \right] \\ &= 2^{-N(R_C+R_J-R_I)} + 2(1 + \epsilon') 2^{-N(R_C+R_J-R_I+\delta)}, \quad (32) \end{aligned}$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$; (a) follows from the union bound; (b) follows from Claim 3; (c) follows from three cases of $(\hat{m}_1, \hat{m}_2)$; (d) follows from the union bound, Claim 1, and Claim 2. Since $R_C + R_J > R_I + \delta$ due to (16), we obtain that $\Pr(\mathcal{E}_{54}|A) \rightarrow 0$ as $N \rightarrow \infty$.

The probability $\Pr\{\mathcal{E}_{61}|A\}$ can be bounded as

$$\Pr(\mathcal{E}_{61}|A) = \Pr\{(U^N(1, \hat{m}_1), V^N(1, \hat{m}_1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \text{ for some } \hat{m}_1 \neq 1, \text{ and } \hat{m}_2|A\}$$

$$\begin{aligned}
&\stackrel{(a)}{\leq} \sum_{\hat{m}_1 \neq 1} \sum_{\hat{m}_2} \Pr\{(U^N(1, \hat{m}_1), \\
&\quad V^N(1, \hat{m}_1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N | A\} \\
&\stackrel{(b)}{\leq} (1 + \epsilon') 2^{-N(I(U, V; Y) - R_2 - R_4 - 2\delta)}, \quad (33)
\end{aligned}$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$; (a) follows from the union bound; (b) follows from Claim 2. As $R_2 + R_4 < I(U, V; Y) - 2\delta$ holds due to (16), we obtain that $\Pr(\mathcal{E}_{61} | A) \rightarrow 0$ as $N \rightarrow \infty$.

Consider the probability $\Pr(\mathcal{E}_{62} | A)$, which can be bounded as

$$\begin{aligned}
&\Pr(\mathcal{E}_{62} | A) \\
&= \Pr\{(U^N(1, 1), V^N(1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \\
&\quad \text{for some } \hat{m}_2 \neq 1 | A\} \\
&\stackrel{(a)}{\leq} \sum_{\hat{m}_2 \neq 1} \Pr\{(U^N(1, 1), V^N(1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N | A\} \\
&\stackrel{(b)}{\leq} (1 + \epsilon') 2^{-N(I(V; Y | U) - R_4 - \delta)}, \quad (34)
\end{aligned}$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$; (a) follows from the union bound; (b) follows from Claim 1. As $R_4 < I(V; Y | U) - \delta$ due to (16), we obtain that $\Pr(\mathcal{E}_{62} | A) \rightarrow 0$ as $N \rightarrow \infty$.

The probability of the last error event can be bounded as follows

$$\begin{aligned}
&\Pr(\mathcal{E}_{63} | A) = \Pr\{(U^N(1, \hat{m}_1), V^N(1, \hat{m}_1, 1, \hat{m}_2), \\
&\quad Y^N) \in \mathcal{T}_\epsilon^N, \text{ for some } \hat{m}_1 \neq 1, \hat{m}_2 \neq 1 | A\} \\
&\stackrel{(a)}{\leq} \sum_{\hat{m}_1 \neq 1} \sum_{\hat{m}_2 \neq 1} \Pr\{(U^N(1, \hat{m}_1), \\
&\quad V^N(1, \hat{m}_1, 1, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N | A\} \\
&\stackrel{(b)}{\leq} (1 + \epsilon') 2^{-N(I(U, V; Y) - R_2 - R_4 - 2\delta)}, \quad (35)
\end{aligned}$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$; (a) follows from the union bound; (b) follows from Claim 2. As $R_2 + R_4 < I(U, V; Y) - 2\delta$ due to (16), we obtain that $\Pr(\mathcal{E}_{63} | A) \rightarrow 0$ as $N \rightarrow \infty$.

Consequently, due to the union bound,

$$\Pr(\mathcal{E}) \rightarrow 0, \text{ as } N \rightarrow \infty. \quad (36)$$

Equations (23) and (36) imply that there exists a codebook and fixed mapping $e_1(\cdot)$, $e_2(\cdot)$, $d_1(\cdot)$ and $d_2(\cdot)$ such that conditioning on these (5a) and (5b) are fulfilled.

Total Leakage Analysis: For the fixed enrollment and identification mappings, the total leakage can be bounded as

$$\begin{aligned}
&I(S_W; C_W, J_W) + I(X^N(W); C_W, J_W) \\
&\leq 2I(S_W, X^N(W); C_W, J_W) \\
&\leq 2H(C_W) + 2H(J_W) - 2H(C_W, J_W | X^N(W), S_W) \\
&\leq 2N(R_C + R_J) - 2H(K_{1W} \oplus \tilde{P}_{1W}, \\
&\quad \tilde{P}_{2W}, K_{2W} \oplus \bar{P}_{1W}, \bar{P}_{2W} | X^N(W), S_W) \\
&\stackrel{(c)}{=} 2N(R_C + R_J) - 2H(\tilde{P}_{1W}, \tilde{P}_{2W}, \bar{P}_{1W}, \bar{P}_{2W} \\
&\quad | X^N(W), S_W, K_{1W}, K_{2W})
\end{aligned}$$

$$\stackrel{(d)}{=} 0, \quad (37)$$

where (c) follows from our coding scheme that given $X^N(W)$, (K_{1W}, K_{2W}) is known; (d) is valid since $(\tilde{P}_W, \bar{P}_W)$ is independent of $(X^N(W), S_W, K_{1W}, K_{2W})$.

Uniformity of Secret Key and Hash Index Analysis: We use the following lemma and the fact that the private key is uniformly distributed to show the uniformity of secret keys and hash indices.

Lemma 3: Given the chosen codebook $\mathcal{C}$, the index tuple $(K_{1W}, M_{1W}, K_{2W}, M_{2W})$ is close to uniformly distributed when N is sufficiently large:

$$\begin{aligned}
&H(K_{1W}, M_{1W}, K_{2W}, M_{2W}) \\
&\geq N(R_1 + R_2 + R_3 + R_4 - \beta) \quad (38)
\end{aligned}$$

where $\beta \rightarrow 0$ as $N \rightarrow \infty$. Consequently, each index K_{1W} , M_{1W} , K_{2W} , and M_{2W} , are also close to uniformly distributed.

Proof: The proof is given in Appendix A-D.

Since the secret key S_W is a combination of $(K_{1W}, M_{1W}, K_{2W}, M_{2W})$ and part of the private key P_W , combining with Lemma 3, it follows that the secret key is close to uniformly distributed.

Due to the construction of the hash index $C_W = (K_{1W} \oplus \tilde{P}_{1W}, \tilde{P}_{2W})$, where $(\tilde{P}_{1W}, \tilde{P}_{2W})$ is uniformly distributed and independent of K_{1W} , it follows that the hash index C_W is close to uniformly distributed.

Combining (16), (23), (36), (38), and (37), we complete the achievability proof of Theorem 1.

2) Converse: Define auxiliary random variables $U_n = (W, X^{n-1}(W), C_W, P_W)$ and $V_n = (W, X^{n-1}(W), C_W, P_W, S_W, J_W)$ for $n \in [1 : N]$. Let $\mathbf{J}$ denote $(J_i)_{i=1}^{M_I}$ and $\mathbf{C}$ denote $(C_i)_{i=1}^{M_I}$. Additionally, define $F = 1 + \Pr\{(\hat{W}, \hat{S}) \neq (W, S_W)\} \log(M_I M_S)$.

Before proceeding with the proofs, we include the following claims.

Claim 4: Given the fixed mapping $e_1(\cdot)$, $e_2(\cdot)$, $d_1(\cdot)$ and $d_2(\cdot)$, we have that

$$H(S_W, W | \mathbf{C}, \mathbf{J}, Y^N, P_W) \stackrel{(a)}{\leq} H(S_W, W | \hat{W}, \hat{S}) \stackrel{(b)}{\leq} F, \quad (39)$$

where (a) follows from the fact that $(\hat{W}, \hat{S})$ is a function of $(\mathbf{C}, \mathbf{J}, Y^N, P_W)$; (b) follows from Fano's inequality.

Claim 5: Given the fixed mapping $e_1(\cdot)$, $e_2(\cdot)$, $d_1(\cdot)$ and $d_2(\cdot)$, we have that

$$\begin{aligned}
&I(Y^N, P_W; S_W, W, \mathbf{C}, \mathbf{J}) \\
&= -I(X^N(W); P_W | S_W, W, C_W, J_W) \\
&\quad - H(P_W | X^N(W), S_W, W, C_W, J_W) \\
&\quad + I(Y^N; S_W, W, C_W, J_W, P_W) + H(P_W). \quad (40)
\end{aligned}$$

Proof: The proof is given in Appendix B-A.

Claim 6: It can be seen that

$$\begin{aligned}
&I(X^N(W); S_W, W, C_W, J_W, P_W) \\
&\quad - I(Y^N; S_W, W, C_W, J_W, P_W) \\
&\stackrel{(a)}{\geq} \sum_{n=1}^N I(X_n(W); U_n, V_n) - \sum_{n=1}^N I(Y_n; U_n, V_n),
\end{aligned}$$

where (a) holds due to the Markov chain $Y^{n-1} - (S_W, W, C_W, J_W, P_W, X^{n-1}(W)) - Y_n$.

Consider the following joint entropy

$$\begin{aligned}
H(W, S_W) &= I(W, S_W; P_W, \mathbf{C}, \mathbf{J}, Y^N) + H(W, S_W | P_W, \mathbf{C}, \mathbf{J}, Y^N) \\
&\stackrel{(a)}{\leq} I(W, S_W; P_W, \mathbf{C}, \mathbf{J}, Y^N) + F \\
&= I(W, S_W; \mathbf{C}, \mathbf{J}) + I(W, S_W; Y^N, P_W | \mathbf{C}, \mathbf{J}) + F \\
&\stackrel{(b)}{=} I(S_W; \mathbf{C}, \mathbf{J} | W) + I(W, S_W; Y^N, P_W | \mathbf{C}, \mathbf{J}) + F \\
&\stackrel{(c)}{\leq} I(S_W; C_W, J_W, W) + I(W, S_W; Y^N, P_W | \mathbf{C}, \mathbf{J}) + F \\
&\stackrel{(d)}{=} I(S_W; C_W, J_W) + I(W, S_W; Y^N, P_W | \mathbf{C}, \mathbf{J}) + F \\
&\leq N\delta + I(W, S_W; Y^N, P_W | \mathbf{C}, \mathbf{J}) + F \\
&= N\delta + I(W, S_W; P_W | \mathbf{C}, \mathbf{J}) \\
&\quad + I(W, S_W; Y^N | P_W, \mathbf{C}, \mathbf{J}) + F \\
&\leq N\delta + H(P_W) + I(W, S_W, \mathbf{C}, \mathbf{J}, P_W; Y^N) + F \\
&\stackrel{(e)}{=} N\delta + H(P_W) + I(Y^N; W, S_W, C_W, P_W, J_W) + F \\
&\leq N(2\delta + R_P) \\
&\quad + \sum_{n=1}^N I(Y_n; W, S_W, P_W, C_W, J_W, Y^{n-1}) + F \\
&\leq N(2\delta + R_P) + F \\
&\quad + \sum_{n=1}^N I(Y_n; W, S_W, P_W, C_W, J_W, Y^{n-1}, X^{n-1}(W)) \\
&\stackrel{(f)}{=} N(2\delta + R_P) + \sum_{n=1}^N I(Y_n; U_n, V_n) + F, \tag{41}
\end{aligned}$$

where (a) follows Claim 4; (b) holds since W is independent of $(\mathbf{C}, \mathbf{J})$; (c) is valid since given W , S_W is independent of the helper data of the other users; (d) follows from that W is independent of (C_W, J_W, S_W) ; (e) holds as Y^N only correlates to the helper data of the observed user in the database; (f) holds due to $Y^{n-1} - (W, S_W, P_W, C_W, J_W, X^{n-1}(W)) - Y_n$.

Combining the above results, we obtain that

$$\begin{aligned}
\log M_I M_S &\stackrel{(a)}{\leq} \log M_I + H(S_W) + N\delta \\
&\stackrel{(b)}{=} H(W) + H(S_W) + N\delta \stackrel{(c)}{=} H(W, S_W) + N\delta \\
&\leq N R_P + \sum_{n=1}^N I(Y_n; U_n, V_n) + F + 3N\delta, \tag{42}
\end{aligned}$$

where (a) follows from the uniformity of the secret key (5d); (b) follows from that W is uniformly distributed on $[1 : M_I]$; (c) follows from that W is independent of (X^N, P_W) , and thus independent of S_W . This gives

$$\begin{aligned}
R_I + R_S &\leq \frac{\log M_I M_S}{N} + 2\delta \\
&\leq R_P + \frac{1}{N} \sum_{n=1}^N I(Y_n; U_n, V_n) + \frac{F}{N} + 5\delta. \tag{43}
\end{aligned}$$

Now we consider the privacy leakage as follows

$$\begin{aligned}
I(X^N(W); C_W, J_W) &= I(X^N(W); \mathbf{C}, \mathbf{J} | W) \\
&\stackrel{(b)}{=} I(X^N(W), W; \mathbf{C}, \mathbf{J}) \\
&\geq H(X^N(W), W) - H(X^N(W), S_W, W | \mathbf{C}, \mathbf{J}) \\
&= H(W) + H(X^N(W)) - H(S_W, W | \mathbf{C}, \mathbf{J}, Y^N, P_W) \\
&\quad - [I(Y^N, P_W; S_W, W | \mathbf{C}, \mathbf{J}) \\
&\quad + H(X^N(W) | S_W, W, \mathbf{C}, \mathbf{J})] \\
&\stackrel{(c)}{\geq} H(W) + I(X^N(W); S_W, W, \mathbf{C}, \mathbf{J}) - F \\
&\quad - I(Y^N, P_W; S_W, W, \mathbf{C}, \mathbf{J}) \\
&\stackrel{(d)}{\geq} H(W) + I(X^N(W); S_W, W, C_W, J_W, P_W) \\
&\quad - F - I(Y^N; S_W, W, C_W, J_W, P_W) - H(P_W) \\
&\stackrel{(f)}{\geq} N(R_I - R_P - 2\delta) \\
&\quad + \sum_{n=1}^N I(X_n(W); U_n, V_n) - \sum_{n=1}^N I(Y_n; U_n, V_n) - F, \tag{44}
\end{aligned}$$

where (b) follows from that W is independent of $(\mathbf{C}, \mathbf{J})$; (c) follows from Claim 4 and the fact that the $X^N(W)$ and Y^N only correlate to the helper data (C_W, J_W) of user W in the database; (d) follows from Claim 5 and the fact that entropy $H(P_W | X^N(W), S_W, W, C_W, J_W)$ is non-negative; (f) follows from Claim 6.

Combining the above result with (5j), it follows that

$$\begin{aligned}
R_I + \frac{1}{N} \sum_{n=1}^N I(X_n(W); U_n, V_n) \\
\leq R_P + \frac{1}{N} \sum_{n=1}^N I(Y_n; U_n, V_n) - \frac{F - \delta}{N} + 2\delta. \tag{45}
\end{aligned}$$

Now we consider the list rate. Firstly, define a random variable E such that $E = 1$ when $C_W \in \mathcal{L}$ and $E = 0$ when $C_W \notin \mathcal{L}$. This implies that when $E = 1$, C_W can only take $|\mathcal{L}|$ values. Due to (5b), it follows that $\Pr(E = 0) \rightarrow 0$ as $N \rightarrow \infty$. Therefore, we have that

$$\begin{aligned}
H(C_W | \mathcal{L}) &= H(C_W | \mathcal{L}) + H(E | C_W, \mathcal{L}) \\
&= H(E, C_W | \mathcal{L}) = H(E | \mathcal{L}) + H(C_W | E, \mathcal{L}) \\
&\leq h_b(P_e) + \Pr(E = 0)H(C_W | E = 0, \mathcal{L}) \\
&\quad + \Pr(E = 1)H(C_W | E = 1, \mathcal{L}) \\
&\leq h_b(P_e) + P_e \log M_C + N(R_L + \delta) \\
&= N(R_L + \delta'), \tag{46}
\end{aligned}$$

where $\delta' \triangleq \frac{1}{N}(h_b(P_e) + P_e \log M_C) + \delta$ and $\delta' \rightarrow 0$ as $N \rightarrow \infty$. Thus we have that

$$\begin{aligned}
N(R_L + \delta') &\geq H(C_W | \mathcal{L}) \stackrel{(a)}{\geq} H(C_W | Y^N, P_W) \\
&= H(C_W | P_W) - I(C_W; Y^N | P_W) \\
&\geq I(X^N(W); C_W | P_W) - I(C_W, P_W; Y^N) \\
&\stackrel{(b)}{=} I(X^N(W); C_W, W, P_W) - I(C_W, P_W, W; Y^N)
\end{aligned}$$

$$\stackrel{(c)}{\geq} \sum_{n=1}^N I(X_n; U_n) - I(Y_n; U_n), \quad (47)$$

where (a) holds due to the fact that $\mathcal{L}$ is a function of (Y^N, P_W) ; (b) holds since $X^N(W)$ and P_W are independent, and W is independent of $(X^N(W), C_W, P_W, Y^N)$; (c) holds due to the Markov chain $Y^{n-1} - (C_W, W, X^{n-1}(W)) - Y_n$.

The helper data rate can be bounded as

$$\begin{aligned} N(R_C + R_J + \delta) &\geq H(C_W, J_W|W) \\ &= I(X^N(W); C_W, J_W|W) + H(C_W, J_W|X^N(W), W) \\ &\stackrel{(a)}{=} I(X^N(W); \mathbf{C}, \mathbf{J}|W) + H(C_W, J_W|X^N(W), W) \\ &= I(X^N(W), W; \mathbf{C}, \mathbf{J}) + H(C_W, J_W|X^N(W), W) \\ &= H(W) + H(X^N(W)) - \left[H(X^N(W), W, S_W|\mathbf{C}, \mathbf{J}) \right. \\ &\quad \left. - H(S_W|X^N(W), W, \mathbf{C}, \mathbf{J}) \right] \\ &\quad + H(C_W, J_W|X^N(W), W) \\ &= H(W) + I(X^N(W); S_W, W, C_W, J_W) \\ &\quad - \left[H(S_W, W|\mathbf{C}, \mathbf{J}, Y^N, P_W) \right. \\ &\quad \left. + I(Y^N, P_W; S_W, W|\mathbf{C}, \mathbf{J}) \right] + H(C_W, J_W|X^N(W), W) \\ &\quad + H(S_W|X^N(W), W, C_W, J_W) \\ &= H(W) + I(X^N(W); S_W, W, C_W, J_W) \\ &\quad - H(S_W, W|\mathbf{C}, \mathbf{J}, Y^N, P_W) \\ &\quad - I(Y^N, P_W; S_W, W|\mathbf{C}, \mathbf{J}) \\ &\quad + H(S_W, C_W, J_W|X^N(W), W) \\ &\stackrel{(b)}{\geq} H(W) + I(X^N(W); S_W, W, C_W, J_W) - F \\ &\quad - I(Y^N, P_W; S_W, W, \mathbf{C}, \mathbf{J}) \\ &\quad + H(S_W, C_W, J_W|X^N(W), W) \\ &\stackrel{(c)}{\geq} H(W) + I(X^N(W); S_W, W, C_W, J_W, P_W) - F \\ &\quad - I(Y^N; S_W, W, C_W, J_W, P_W) - H(P_W) \\ &\quad + \left[H(P_W|X^N(W), S_W, W, C_W, J_W) \right. \\ &\quad \left. + H(S_W, C_W, J_W|X^N(W), W) \right] \\ &= H(W) + I(X^N(W); S_W, W, J_W, C_W, P_W) - F \\ &\quad - I(Y^N(W); S_W, W, J_W, C_W, P_W) \\ &\quad - H(P_W) + \left[H(P_W|X^N(W), W) \right. \\ &\quad \left. + H(C_W, J_W, S_W|X^N(W), P_W, W) \right] \\ &\stackrel{(d)}{=} H(W) + I(X^N(W); S_W, W, J_W, C_W, P_W) \\ &\quad - I(Y^N(W); S_W, W, J_W, C_W, P_W) - F + \delta \\ &\stackrel{(e)}{\geq} N(R_I - \delta) - F \\ &\quad + \sum_{n=1}^N I(X_n(W); U_n, V_n) - \sum_{n=1}^N I(Y_n; U_n, V_n), \end{aligned} \quad (48)$$

where (a) follows from the fact that, given the user index W , the biometric sequence $X^N(W)$ is independent of the helper data of the other users; (b) follows from Claim 4 and the fact

Fig. 4: Illustration of generating helper data and secret keys in the chosen secret key system.

that $I(Y^N, P_W; \mathbf{C}, \mathbf{J})$ is non-negative; (c) follows from Claim 5; (d) follows from that P_W is independent of $(X^N(W), W)$, and the fact that given W , (C_W, S_W, J_W) is a function of $(X^N(W), P_W)$; (e) follows from Claim 6.

Combining (43), (45), (47), (48), and using the cardinality bounding argument, which is given in Appendix B-B, we complete the backward direction of the proof.

B. Proof of Theorem 2

The proof of Theorem 2 is based on that of Theorem 1, and uses the one-time padding method. For the sake of completeness, we provide detailed arguments in the following.

1) *Achievability*: Fix the conditional p.m.f. $P_{V|X}$ and $P_{U|V}$. The number of enrolled users is assumed to be $M_I = 2^{NR_I}$. Also fix some $\delta > 0$.

Codebook generation: Pick a rate tuple $(R_I, R_S, R_P, R_C, R_J, R_L) \in \mathcal{R}_c$ such that

$$\begin{aligned} R_P &\geq R_I + I(U, V; X) - I(U, V; Y) + 5\delta, \\ R_J &= R_S + R_I + I(U, V; X) - I(U, V; Y) + 5\delta - R_C, \\ R_S &= R_P - R_I + I(U, V; Y) - 3\delta, \\ R_C &> R_L = I(U; X) - I(U; Y) + 5\delta. \end{aligned} \quad (49)$$

Additionally, we fix auxiliary rates as in (17). Randomly and independently generate $2^{N(R_1+R_2)}$ i.i.d. codewords $u^N(k_1, m_1)$ according to P_U . Then we distribute the codewords into 2^{NR_1} bins indexed by $k_1 \in [1 : 2^{NR_1}]$. Each bin consists of 2^{NR_2} codewords indexed by $m_1 \in [1 : 2^{NR_2}]$. Furthermore, for each codeword $u^N(k_1, m_1)$, where $(k_1, m_1) \in [1 : 2^{NR_1}] \times [1 : 2^{NR_2}]$, randomly and independently generate $2^{N(R_3+R_4)}$ codewords $v^N(k_1, m_1, k_2, m_2)$ according to $\prod_{i=1}^N P_{V|U=u_i(k_1, m_1)}$. We distribute the $2^{N(R_3+R_4)}$ codewords into 2^{NR_3} bins indexed by $k_2 \in [1 : 2^{NR_3}]$. Each bin consists of 2^{NR_4} codewords indexed by $m_2 \in [1 : 2^{NR_4}]$.

Enrollment: For each user $w \in [1 : M_I]$, given the private key of this user p_w , we divide it into three parts, $\tilde{p}_w$, $\bar{p}_w$, and $\hat{p}_w$, such that $p_w = (\tilde{p}_w, \bar{p}_w, \hat{p}_w)$, $\tilde{p}_w \in [1 : 2^{NR_C}]$, $\bar{p}_w \in [1 : 2^{NR_J}]$ and $\hat{p}_w \in [1 : 2^{N(R_P-R_C-R_J)}]$. For $\tilde{p}_w$ and $\bar{p}_w$, we further divide both of them into two parts as $\tilde{p}_w = (\tilde{p}_{1w}, \tilde{p}_{2w})$ and $\bar{p}_w = (\bar{p}_{1w}, \bar{p}_{2w})$, where $\tilde{p}_{1w} \in [1 : 2^{NR_1}]$, $\tilde{p}_{2w} \in [1 : 2^{N(R_C-R_1)}]$, $\bar{p}_{1w} \in [1 : 2^{NR_3}]$, $\bar{p}_{2w} \in [1 : 2^{N(R_J-R_3)}]$. For each user $w \in [1 : 2^{NR_I}]$, the enrollment mapping firstly looks for a codeword $u^N(k_{1w}, m_{1w})$ such that

$(u^N(k_{1w}, m_{1w}), x^N(w)) \in \mathcal{T}_\epsilon^N$. If no such codeword exists, randomly choose a codeword index pair from $[1 : 2^{NR_1}] \times [1 : 2^{NR_2}]$. If there is more than one such codewords, randomly choose one from them. Then the enrollment mapping uses k_{1w} and the private key p_w to generate the first layer helper data c_w as $c_w = (k_{1w} \oplus \check{p}_{1w}, \check{p}_{2w})$, which is called hash index. We further put the user index w in a set of user indices, which is denoted by $\mathcal{B}(c_w)$. Secondly, the enrollment mapping looks for a codeword $v^N(k_{1w}, m_{1w}, k_{2w}, m_{2w})$ such that $(u^N(k_{1w}, m_{1w}), v^N(k_{1w}, m_{1w}, k_{2w}, m_{2w}), x^N(w)) \in \mathcal{T}_\epsilon^N$. If no such (k_{2w}, m_{2w}) exists, randomly choose one from $[1 : 2^{NR_3}] \times [1 : 2^{NR_4}]$. If there is more than one such (k_{2w}, m_{2w}) , randomly choose one from them. With the bin index k_{2w} and the private key p_w , the enrollment mapping generates the first part of second layer helper data as $j_w^g = (k_{2w} \oplus \bar{p}_{1w}, \bar{p}_{2w})$. Using the codeword index tuple $(k_{1w}, m_{1w}, k_{2w}, m_{2w})$ and the private key p_w , the the system generates additional data $s_w^g = (k_{1w}, m_{1w}, k_{2w}, m_{2w}, \tilde{p}_w)^1$. Then we use the chosen secret key s_w^c to mask the index s_w^g and generate the second part of the second layer helper data as $j_w^a = s_w \oplus s_w^g$. Thus the second layer helper is generated as $j_w = (j_w^g, j_w^a)$. Therefore, the three parts of the private key are used to generate the first layer helper data the second layer helper data. The procedure of generating the helper data and secret keys is illustrated in Fig. 4. The codebooks and mappings are revealed to all parties.

Identification: Upon receiving the observation y^N and having access to the corresponding private key p_w of the observed user w , the system firstly looks for a list of hash indices $\mathcal{L}(y^N, p_w)$ such that for each hash index $c \in \mathcal{L}(y^N, p_w)$, there exists (k_1, m_1) that satisfies $c = (k_1 \oplus \check{p}_{1w}, \check{p}_{2w})$ and $(u^N(k_1, m_1), y^N) \in \mathcal{T}_\epsilon^N$. Next, the system checks users with index in $\{w : w \in \mathcal{B}(c), c \in \mathcal{L}\}$, which is denoted by $\mathcal{B}_\mathcal{L}$, and looks for a unique tuple $(\hat{w}, \hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2)$ that satisfies $c_{\hat{w}} \in \mathcal{L}(y^N, p_w)$, $c_{\hat{w}} = (\hat{k}_1 \oplus \check{p}_{1w}, \check{p}_{2w})$, $j_{\hat{w}}^g = (\hat{k}_2 \oplus \bar{p}_{1w}, \bar{p}_{2w})$ and $(u^N(\hat{k}_1, \hat{m}_1), v^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), y^N) \sim \mathcal{T}_\epsilon^N$. An estimate of the chosen secret key is given as $\hat{s} = j_{\hat{w}}^a \oplus \hat{s}^g$, where $\hat{s}^g = (\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2, \tilde{p}_w)$.

Error Events Analysis: Follow the error events analysis of Theorem 1, we can obtain

$$\Pr\{C_W \in \mathcal{L}\} \leq \delta, \quad (50a)$$

$$\Pr\{(\hat{W}, \hat{S}^g) \neq (W, S_W^g)\} \leq \delta, \quad (50b)$$

where $\delta \rightarrow 0$ as $N \rightarrow \infty$. Due to the codebook generation scheme, assume that $\hat{W} = W$ holds, then $\hat{S}^c = S^c$ holds only if $\hat{S}^g = S^g$. Thus (50b) implies

$$\Pr\{(\hat{W}, \hat{S}^c) \neq (W, S_W^c)\} \leq \delta, \quad (51)$$

where $\delta \rightarrow 0$ as $N \rightarrow \infty$.

Equations (50a) and (51) imply that there exists a codebook and fixed mapping $e_1(\cdot)$, $e_2(\cdot)$, $d_1(\cdot)$ and $d_2(\cdot)$ such that conditioning on these (5a) and (5b) are fulfilled.

Uniformity of Hash Index Analysis: Follow the uniformity analysis in the proof of Theorem 1, we can obtain that the hash index C_W is close to be uniformly distributed, i.e.,

$$H(C_W) + N\delta = \log M_C \leq N(R_C + \delta), \quad (52)$$

¹Note that s_w^g corresponding to the generated secret key in the setting of Theorem 1.

where $\delta \rightarrow 0$ as $N \rightarrow \infty$.

Total Leakage Analysis: For the fixed enrollment and identification mappings, the secrecy leakage can be bounded as

$$\begin{aligned} I(S_W^c; C_W^c, J_W^c) &= I(S_W^c; C_W^g, J_W^g, J_W^a) = I(S_W^c; C_W^g, J_W^g, S_W^c \oplus S_W^g) \\ &= I(S_W^c; C_W^g, J_W^g) + I(S_W^c; S_W^c \oplus S_W^g | C_W^g, J_W^g) \\ &\stackrel{(a)}{=} H(S_W^c \oplus S_W^g) - H(S_W^c \oplus S_W^g | C_W^g, J_W^g, S_W^c) \\ &= \log M_S - H(S_W^g | C_W^g, J_W^g, S_W^c) \\ &\leq \log M_S - H(S_W^g) + I(S_W^g; C_W^g, J_W^g), \end{aligned} \quad (53)$$

where (a) follows from the fact that S_W^c is independent of (C_W^g, J_W^g) .

We bound the privacy leakage as follows

$$\begin{aligned} I(X^N(W); C_W^c, J_W^c) &= I(X^N(W); C_W^g, J_W^g, J_W^a) \\ &= I(X^N(W); C_W^g, J_W^g, S_W^c \oplus S_W^g) \\ &= I(X^N(W); C_W^g, J_W^g) \\ &\quad + I(X^N(W); S_W^c \oplus S_W^g | C_W^g, J_W^g) \\ &= I(X^N(W); C_W^g, J_W^g). \end{aligned} \quad (54)$$

Combining (53) and (54), the total leakage can be bounded as

$$\begin{aligned} I(S_W^c; C_W^c, J_W^c) + I(X^N(W); C_W^c, J_W^c) &\leq \log M_S - H(S_W^g) + I(S_W^g; C_W^g, J_W^g) \\ &\quad + I(X^N(W); C_W^g, J_W^g) \\ &\stackrel{(c)}{\leq} N\delta + I(S_W^g; C_W^g, J_W^g) + I(X^N(W); C_W^g, J_W^g), \end{aligned} \quad (55)$$

where (c) holds since the index S_W^g is close to uniformly distributed.

Combining (49), (50a), (51), (52), and (55), we complete the achievability proof of Theorem 2.

2) Converse: The converse for Theorem 2 is similar to that of Theorem 1. Define auxiliary random variables $U_n = (W, X^{n-1}(W), C_W)$ and $V_n = (W, X^{n-1}(W), C_W, S_W, J_W, P_W)$ for $n \in [1 : N]$. Let $\mathbf{J}$ denote $(J_i)_{i=1}^{M_I}$ and $\mathbf{C}$ denote $(C_i)_{i=1}^{M_I}$. Follow (41), (42) and (43), we can obtain that

$$R_I + R_S \leq R_P + \frac{1}{N} \sum_{n=1}^N I(Y_n; U_n, V_n) + \frac{F}{N} + 5\delta. \quad (56)$$

Similar to (44) and (45), we can obtain that

$$\begin{aligned} R_I + \frac{1}{N} \sum_{n=1}^N I(X_n(W); U_n, V_n) &\leq R_P + \frac{1}{N} \sum_{n=1}^N I(Y_n; U_n, V_n) - \frac{F - \delta}{N} + 2\delta. \end{aligned} \quad (57)$$

Similar to (46) and (47), we can obtain that

$$N(R_L + \delta') \geq \sum_{n=1}^N I(X_n; U_n) - I(Y_n; U_n), \quad (58)$$

where $\delta' \rightarrow 0$ as $N \rightarrow \infty$.

For the helper data rate, we have that

$$\begin{aligned}
N(R_C + R_J + \delta) &\geq H(C_W, J_W|W) \\
&\stackrel{(a)}{\geq} H(W) + I(X^N(W); S_W, W, J_W, C_W, P_W) - F \\
&\quad - I(Y^N(W); S_W, W, J_W, C_W, P_W) \\
&\quad - H(P_W) + \left[H(P_W|X^N(W), W) \right. \\
&\quad \left. + H(C_W, J_W, S_W|X^N(W), P_W, W) \right] \\
&\stackrel{(b)}{=} H(W) + I(X^N(W); S_W, W, J_W, C_W, P_W) \\
&\quad - I(Y^N(W); S_W, W, J_W, C_W, P_W) - F + H(S_W) \\
&\stackrel{(c)}{\geq} N(R_I + R_S - \delta) - F \\
&\quad + \sum_{n=1}^N I(X_n(W); U_n, V_n) - \sum_{n=1}^N I(Y_n; U_n, V_n), \quad (59)
\end{aligned}$$

where (a) follows from similar analysis in (48); (b) follows from the fact that (C_W, J_W) is a function of $(X^N(W), P_W)$ and S_W is independent of $(X^N(W), P_W, W)$; (c) follows from (5c) and the chosen secret key is uniformly distributed.

Similar to the converse proof of Theorem 1, we can use the cardinality bounding argument to complete the proof for the backward direction.

V. BINARY EXAMPLE

To illustrate the derived trade-offs, we next discuss a binary example. Assume the source is binary symmetric, i.e., $X \sim \text{Bernoulli}(1/2)$. Let the observation channel be a binary symmetric channel with crossover probability $q \in (0, \frac{1}{2})$. We choose V to be an output of a binary symmetric channel with crossover probability $p_1 \in (0, \frac{1}{2})$ and input X , and choose U to be an output of a binary symmetric channel with crossover probability $p_2 \in (0, \frac{1}{2})$ and input V . From Mrs. Gerber's lemma [27], we obtain that if $H(X|V) \geq h_2(p_1)$ for some $p_1 \in (0, \frac{1}{2})$, then $H(X|U) \geq h_2(p_1 * p_2)$, where $h_2(\cdot)$ denotes the binary entropy function and $*$ denotes the operation of $p_1 * p_2 = p_1(1 - p_2) + p_2(1 - p_1)$. Similarly, it holds that $H(Y|V) \geq h_2(p_1 * q)$ and $H(Y|U) \geq h_2(p_1 * p_2 * q)$.

In the following example, we fix the private key rate as $R_P = r$, then the capacity region of the generated secret key system $\mathcal{R}_g$ is

$$\mathcal{R}_g = \{(R_I, R_S, R_P, R_C, R_J, R_L) : \quad (60a)$$

$$R_I + R_S \leq r + 1 - h_2(p_1 * q), \quad (60a)$$

$$R_I - h_2(p_1) \leq r - h_2(p_1 * q), \quad (60b)$$

$$R_I - h_2(p_1) \leq R_C + R_J - h_2(p_1 * q), \quad (60c)$$

$$R_L \geq h_2(p_1 * p_2 * q) - h_2(p_1 * p_2), \quad (60d)$$

$$\text{for some } q, p_1, p_2 \in (0, \frac{1}{2})\},$$

The capacity region of the chosen secret key system is the region that satisfies (60a), (60b), (60d), and

$$R_I + R_S - h_2(p_1) \leq R_C + R_J - h_2(p_1 * q), \quad (61)$$

for some $q, p_1, p_2 \in (0, \frac{1}{2})$.

Fig. 5 illustrates trade-offs among $(R_I, R_S, R_C + R_J)$ when $q = 0.15$, $p_1 = 0.1$, $p_2 = 0.05$, and $R_P = 1$. For simplicity,

we consider the joint helper data rate $R_C + R_J$, i.e., the sum of the first and second layer helper data rates. Any rate tuples with smaller identification rate, smaller secret key rate, and larger joint helper data rate than the rate tuples on the boundaries are achievable. Comparing Fig. 5a and Fig. 5b, we observe that for the chosen secret key system, the joint helper data rate not only increases with a larger identification rate but also increases when the secret key rate increase. Therefore, to reliably identify the same number of users and including secret keys of the same length, the chosen secret key system requires more storage to store the helper data than the generated secret key system. Because to make the chosen secret keys secure, they have to be masked such that the masked data do not leak information about the secret keys. Then for reliable secret key reconstruction and authentication, the masked data must be stored in the database, which leads to more storage costs. Moreover, for both the generated secret key and chosen secret key systems, if we increase one of the secret key rate and the identification rate, the maximal achievable rate of the other one decreases. This means that we can only identify fewer users if we want to increase the security level by having longer secret keys, and vice versa.

We also depict the trade-off among the rate triple (R_C, R_J, R_L) in Fig. 6. Similar to the previous example, we set $q = 0.15$, $p_1 = 0.1$, $p_2 = 0.05$, and $R_P = 1$. Moreover, for simplicity, we pick an achievable rate pair $(R_I, R_S) = (0.7, 0.5)$. Any rate triples with larger first layer and second layer helper data rates, and larger list rate are achievable. Comparing Fig. 6a and Fig. 6b, we observe that for some fixed (R_C, R_L) , the chosen secret key system requires larger R_J (the border line between the yellow plane and blue plane is shifted). This observation implies that if the lengths of the first layer helper data are the same in both systems, then the chosen secret key system requires more storage to store the second layer helper data.

APPENDIX A

SUPPLEMENTARY PROOFS OF THE ACHIEVABILITY PROOF

A. Proof of Claim 1

For some $(\hat{k}_2, \hat{m}_2) \neq (1, 1)$, we have that

$$\begin{aligned}
&\Pr\{(U^N(1, 1), V^N(1, 1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N | A\} \\
&= \sum_{(u^N, \hat{v}^N, y^N) \in \mathcal{T}_\epsilon^N} \Pr\{U^N(1, 1) = u^N, \\
&\quad V^N(1, 1, \hat{k}_2, \hat{m}_2) = \hat{v}^N, Y^N = y^N | A\} \\
&= \sum_{(u^N, \hat{v}^N, y^N) \in \mathcal{T}_\epsilon^N} \sum_{x^N} \sum_{v^N} \Pr\{U^N(1, 1) = u^N, \\
&\quad V^N(1, 1, \hat{k}_2, \hat{m}_2) = \hat{v}^N, Y^N = y^N, X^N(1) = x^N, \\
&\quad V^N(1, 1, 1, 1) = v^N | A\} \\
&= \sum_{(u^N, \hat{v}^N, y^N) \in \mathcal{T}_\epsilon^N} \sum_{x^N} \sum_{v^N} \Pr\{(V^N(1, 1, \hat{k}_2, \hat{m}_2) = \hat{v}^N \\
&\quad | U^N(1, 1) = u^N, Y^N = y^N, X^N(1) = x^N, \\
&\quad V^N(1, 1, 1, 1) = v^N, A\} \\
&\quad \times \Pr\{U^N(1, 1) = u^N, Y^N = y^N, X^N(1) = x^N,
\end{aligned}$$

(a) Generated secret key system.

(b) Chosen secret key system.

Fig. 5: Trade-offs among $(R_I, R_S, R_C + R_J)$ with $q = 0.15$, $p_1 = 0.1$, $p_2 = 0.05$, and $R_P = 1$.

(a) Generated secret key system.

(b) Chosen secret key system.

Fig. 6: Trade-offs among rate triple (R_C, R_J, R_L) with $q = 0.15$, $p_1 = 0.1$, $p_2 = 0.05$, $R_P = 1$, $R_I = 0.7$, and $R_S = 0.5$.

$$\begin{aligned}
 & V^N(1, 1, 1, 1) = v^N | A \} \\
 \stackrel{(a)}{=} & \sum_{(u^N, \hat{v}^N, y^N) \in \mathcal{T}_\epsilon^N} \sum_{x^N} \sum_{v^N} \Pr\{V^N(1, 1, \hat{k}_2, \hat{m}_2) = \hat{v}^N \\
 & | U^N(1, 1) = u^N, X^N(1) = x^N, V^N(1, 1, 1, 1) = v^N, A\} \\
 & \times \Pr\{U^N(1, 1) = u^N, Y^N = y^N, X^N(1) = x^N, \\
 & V^N(1, 1, 1, 1) = v^N | A\}, \tag{62}
 \end{aligned}$$

where (a) holds since given $(X^N(1), W = 1)$, Y^N is independent of the other variables. Apply Lemma 2, we obtain that

$$\begin{aligned}
 & \Pr\{V^N(1, 1, \hat{k}_2, \hat{m}_2) = \hat{v}^N | U^N(1, 1) = u^N, \\
 & X^N(1) = x^N, V^N(1, 1, 1, 1) = v^N, A\} \\
 & \leq (1 + \epsilon') \prod_{i=1}^N P_{V|U}(\hat{v}_i | u_i). \tag{63}
 \end{aligned}$$

where $\epsilon' > 0$ is a fixed number. Combining (62) and (63), we obtain that

$$\begin{aligned}
 & \Pr\{(U^N(1, 1), V^N(1, 1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N | A\} \\
 & \leq (1 + \epsilon') 2^{-N(I(V; Y|U) - \delta)}, \tag{64}
 \end{aligned}$$

where $\epsilon' > 0$ is a fixed number.

B. Proof of Claim 2

For some $(\hat{k}_1, \hat{m}_1) \neq (1, 1)$, $(\hat{k}_2, \hat{m}_2) \in [1 : 2^{NR_3}] \times [1 : 2^{NR_4}]$, we have that

$$\begin{aligned}
 & \Pr\{(U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N | A\} \\
 & = \sum_{v^N \in \mathcal{T}_\epsilon^N(V|\hat{u}^N, y^N)} \sum_{(\hat{u}^N, y^N) \in \mathcal{T}_\epsilon^N} \\
 & \Pr\{V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2) = v^N | U^N(\hat{k}_1, \hat{m}_1) = \hat{u}^N, \\
 & Y^N = y^N, A\} \cdot \Pr\{U^N(\hat{k}_1, \hat{m}_1) = \hat{u}^N, Y^N = y^N | A\} \\
 \stackrel{(b)}{=} & \sum_{v^N \in \mathcal{T}_\epsilon^N(V|\hat{u}^N, y^N)} \sum_{(\hat{u}^N, y^N) \in \mathcal{T}_\epsilon^N} \\
 & \Pr\{V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2) = v^N | U^N(\hat{k}_1, \hat{m}_1) = \hat{u}^N, \\
 & W = 1\} \cdot \Pr\{U^N(\hat{k}_1, \hat{m}_1) = \hat{u}^N, Y^N = y^N | A\} \\
 & \leq 2^{-N(I(V; Y|U) - \delta)} \sum_{(\hat{u}^N, y^N) \in \mathcal{T}_\epsilon^N} \\
 & \Pr\{U^N(\hat{k}_1, \hat{m}_1) = \hat{u}^N, Y^N = y^N | A\}, \tag{65}
 \end{aligned}$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$; (b) follows from the fact that given $U^N(\hat{k}_1, \hat{m}_1) = \hat{u}^N$ for $(\hat{k}_1, \hat{m}_1) \neq (1, 1)$, $V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2)$ is independent of Y^N and $(K_{11}, M_{11}, K_{21}, M_{21})$, and thus i.i.d. distributed according to $\prod_{i=1}^N P_{V|U}(\cdot | u_i)$; (c) follows from the joint typicality

lemma [24, p.29]. The term $\sum_{(\hat{u}^N, y^N) \in \mathcal{T}_\epsilon^N} \Pr\{U^N(\hat{k}_1, \hat{m}_1) = \hat{u}^N, Y^N = y^N | A\}$ can be bounded as follows

$$\begin{aligned}
& \sum_{(\hat{u}^N, y^N) \in \mathcal{T}_\epsilon^N} \Pr\{U^N(\hat{k}_1, \hat{m}_1) = \hat{u}^N, Y^N = y^N | A\} \\
&= \sum_{(\hat{u}^N, y^N) \in \mathcal{T}_\epsilon^N} \sum_{u^N} \Pr\{U^N(\hat{k}_1, \hat{m}_1) = \hat{u}^N, \\
&\quad Y^N = y^N, U^N(1, 1) = u^N | A\} \\
&= \sum_{(\hat{u}^N, y^N) \in \mathcal{T}_\epsilon^N} \sum_{u^N} \Pr\{U^N(\hat{k}_1, \hat{m}_1) = \hat{u}^N | Y^N = y^N, \\
&\quad U^N(1, 1) = u^N, A\} \\
&\quad \times \Pr\{U^N(1, 1) = u^N, Y^N = y^N | A\} \\
&\stackrel{(*)}{\leq} \sum_{(\hat{u}^N, y^N) \in \mathcal{T}_\epsilon^N} \sum_{u^N} (1 + \epsilon') \prod_{i=1}^N P_U(\hat{u}_i) \\
&\quad \times \Pr\{U^N(1, 1) = u^N, Y^N = y^N | A\} \\
&\stackrel{(c)}{\leq} \sum_{y^N} \sum_{u^N} (1 + \epsilon) 2^{-N(I(U; Y) - \delta)} \\
&\quad \times \Pr\{U^N(1, 1) = u^N, Y^N = y^N | A\} \\
&= (1 + \epsilon') 2^{-N(I(U; Y) - \delta)}, \tag{66}
\end{aligned}$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$; (*) follows from Lemma 1. Combining (65), and (66), we obtain that

$$\begin{aligned}
& \Pr\{(U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N\} \\
&\leq (1 + \epsilon') 2^{-N(I(U, V; Y) - 2\delta)}, \tag{67}
\end{aligned}$$

where $\epsilon' > 0$ is a fixed number, and $\delta \rightarrow 0$ as $\epsilon \rightarrow 0$.

C. Proof of Claim 3

For some $\hat{w} \neq 1$, $(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2) \in [1 : 2^{NR_1}] \times [1 : 2^{NR_2}] \times [1 : 2^{NR_3}] \times [1 : 2^{NR_4}]$, we have that

$$\begin{aligned}
& \Pr\{(U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \\
&\quad C_{\hat{w}} = (\hat{k}_1 \oplus \check{P}_{11}, \check{P}_{21}), J_{\hat{w}} = (\hat{k}_2 \oplus \bar{P}_{11}, \bar{P}_{21}) | A\} \\
&\stackrel{(a)}{=} \sum_{\check{p}_1} \Pr\{\check{P}_{11} = \check{p}_1\} \sum_{\check{p}_2} \Pr\{\check{P}_{21} = \check{p}_2\} \\
&\quad \sum_{\bar{p}_1} \Pr\{\bar{P}_{11} = \bar{p}_1\} \sum_{\bar{p}_2} \Pr\{\bar{P}_{21} = \bar{p}_2\} \\
&\quad \Pr\{(U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \\
&\quad C_{\hat{w}} = (\hat{k}_1 \oplus \check{p}_1, \check{p}_2), J_{\hat{w}} = (\hat{k}_2 \oplus \bar{p}_1, \bar{p}_2) | A\} \\
&\stackrel{(b)}{=} \sum_{\check{p}_1} \Pr\{\check{P}_{11} = \check{p}_1\} \sum_{\check{p}_2} \Pr\{\check{P}_{21} = \check{p}_2\} \\
&\quad \sum_{\bar{p}_1} \Pr\{\bar{P}_{11} = \bar{p}_1\} \sum_{\bar{p}_2} \Pr\{\bar{P}_{21} = \bar{p}_2\} \\
&\quad \sum_{k_1} \sum_{k_2} \Pr\{K_{1\hat{w}} = k_1, \check{P}_{1\hat{w}} = \hat{k}_1 \oplus \check{p}_1 \ominus k_1, \check{P}_{2\hat{w}} = \check{p}_2, \\
&\quad K_{2\hat{w}} = k_2, \bar{P}_{1\hat{w}} = \hat{k}_2 \oplus \bar{p}_1 \ominus k_2, \bar{P}_{2\hat{w}} = \bar{p}_2, \\
&\quad (U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N | A\} \\
&\stackrel{(c)}{=} \sum_{\check{p}_1} \Pr\{\check{P}_{11} = \check{p}_1\} \sum_{\check{p}_2} \Pr\{\check{P}_{21} = \check{p}_2\}
\end{aligned}$$

$$\begin{aligned}
& \sum_{\bar{p}_1} \Pr\{\bar{P}_{11} = \bar{p}_1\} \sum_{\bar{p}_2} \Pr\{\bar{P}_{21} = \bar{p}_2\} \\
& \sum_{k_1} \sum_{k_2} \Pr\{\check{P}_{1\hat{w}} = \hat{k}_1 \oplus \check{p}_1 \ominus k_1\} \Pr\{\check{P}_{2\hat{w}} = \check{p}_2\} \\
& \Pr\{\bar{P}_{1\hat{w}} = \hat{k}_2 \oplus \bar{p}_1 \ominus k_2\} \Pr\{\bar{P}_{2\hat{w}} = \bar{p}_2\} \\
& \Pr\{(U^N(\hat{k}_1, \hat{m}_1), V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N, \\
&\quad K_{1\hat{w}} = k_1, K_{2\hat{w}} = k_2 | A\} \\
&= 2^{-N(R_C + R_J)} \cdot \Pr\{(U^N(\hat{k}_1, \hat{m}_1), \\
&\quad V^N(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2), Y^N) \in \mathcal{T}_\epsilon^N | A\}. \tag{68}
\end{aligned}$$

where (a) follows by expanding $\check{P}_{11}$, $\check{P}_{21}$, $\bar{P}_{11}$, and $\bar{P}_{21}$; (b) follows by expanding the term $(C_{\hat{w}}, J_{\hat{w}}, K_{1\hat{w}}, K_{2\hat{w}})$; (c) follows from the fact that $\check{P}_{1\hat{w}}$, $\check{P}_{2\hat{w}}$, $\bar{P}_{1\hat{w}}$, and $\bar{P}_{2\hat{w}}$ are uniformly distributed and independent of $(\hat{k}_1, \hat{m}_1, \hat{k}_2, \hat{m}_2, K_{1\hat{w}}, K_{2\hat{w}}, Y^N)$.

D. Proof of Lemma 3

Since W is uniformly distributed in $[1 : M_I]$, due to symmetry, it is sufficient to consider $W = 1$. For any codewords u^N and v^N , it holds that

$$\Pr\{(X^N(1), u^N, v^N) \in \mathcal{T}_\epsilon^N\} \leq 2^{-N(I(U, V; X) - \delta)}. \tag{69}$$

Let E_2 be a random variable such that $E_2 = 0$ when there exists a index tuple $(k_{11}, m_{11}, k_{21}, m_{21})$ satisfying $(x^N(1), u^N(k_{11}, m_{11}), v^N(k_{11}, m_{11}, k_{21}, m_{21})) \in \mathcal{T}_\epsilon^N$. If there is no such codeword index pair, then $E_2 = 1$. Let γ_2 denote $\Pr(E_2 = 1)$. Then according to the error events analysis, we can obtain that $\gamma_2 \rightarrow 0$ as $N \rightarrow \infty$. Now we consider the following joint entropy

$$\begin{aligned}
& H(K_{11}, M_{11}, K_{21}, M_{21}) \\
&= H(K_{11}, M_{11}, K_{21}, M_{21}, E_2) \\
&\quad - H(E_2 | K_{11}, M_{11}, K_{21}, M_{21}) \\
&\geq H(K_{11}, M_{11}, K_{21}, M_{21}, E_2) - H(E_2) \\
&\stackrel{(a)}{\geq} - \sum_{k_{11}} \sum_{m_{11}} \sum_{k_{21}} \sum_{m_{21}} \Pr(K_{11} = k_{11}, M_{11} = m_{11}, \\
&\quad K_{21} = k_{21}, M_{21} = m_{21}, E_2 = 0) \\
&\quad \times \log\{\Pr(x^N(1) \in \mathcal{T}_\epsilon^N(X | u^N(k_{11}, m_{11}), \\
&\quad v^N(k_{11}, m_{11}, k_{21}, m_{21})))\} - h_2(\Pr(E_2 = 0)) \\
&\geq \sum_{k_{11}} \sum_{m_{11}} \sum_{k_{21}} \sum_{m_{21}} \Pr(K_{11} = k_{11}, M_{11} = m_{11}, K_{21} = k_{21}, \\
&\quad M_{21} = m_{21}, E_2 = 0) N(I(U, V; X) - \delta) - h_2(\Pr(E_2 = 0)) \\
&= N(I(U, V; X) - \delta)(1 - \gamma_2) - h_2(1 - \gamma_2) \\
&= N(I(U, V; X) + 2\delta \\
&\quad - (3\delta + I(U, V; X)\gamma_2 - \delta\gamma_2 + \frac{1}{N}h_2(1 - \gamma_2))). \tag{70}
\end{aligned}$$

where the term $5\delta + I(U, V; X)\gamma_2 - \delta\gamma_2 + \frac{1}{N}h_2(1 - \gamma_2) \rightarrow 0$ as $N \rightarrow \infty$; (a) follows from that if $(K_{11} = k_{11}, M_{11} = m_{11}, K_{21} = k_{21}, M_{21} = m_{21}, E_2 = 0)$ holds, then $X^N(1) \in \mathcal{T}_\epsilon^N(X | u^N(k_{11}, m_{11}), v^N(k_{11}, m_{11}, k_{21}, m_{21}))$ is valid. Combining this result with $R_1 + R_2 + R_3 + R_4 = I(U, V; X) + 2\delta$, we have that $K_{1W}, M_{1W}, K_{2W}, M_{2W}$ are close to uniformly distributed.

APPENDIX B

SUPPLEMENTARY PROOF OF THE CONVERSE PROOF

A. Proof of Claim 5

Given the fixed mapping $e_1(\cdot)$, $e_2(\cdot)$, $d_1(\cdot)$ and $d_2(\cdot)$, we have that

$$\begin{aligned}
 I(Y^N, P_W; S_W, W, C, J) \\
 &= I(Y^N, P_W; S_W, W, C_W, J_W) \\
 &= I(P_W; S_W, W, C_W, J_W) + I(Y^N; S_W, W, C_W, J_W | P_W) \\
 &\stackrel{(a)}{=} I(P_W; S_W, W, C_W, J_W) + I(Y^N; S_W, W, C_W, J_W, P_W) \\
 &= -I(X^N(W); P_W | S_W, W, C_W, J_W) \\
 &\quad - H(P_W | X^N(W), S_W, W, C_W, J_W) \\
 &\quad + I(Y^N; S_W, W, C_W, J_W, P_W) + H(P_W), \tag{71}
 \end{aligned}$$

where (a) follows from that P_W is independent of Y^N .

B. Cardinality Bounds

Let us define the following $|\mathcal{X}| + 3$ continuous functions:

$$\begin{aligned}
 f_j(p(v|x)) &= \sum_{u \in \mathcal{U}} p(u, v|x), \quad j = 1, \dots, |\mathcal{X}| - 1, \\
 f_{|\mathcal{X}|}(p(v|x)) &= H(X|V, U = u), \\
 f_{|\mathcal{X}|+1}(p(v|x)) &= H(Y|V, U = u), \\
 f_{|\mathcal{X}|+2}(p(v|x)) &= H(X|U = u), \\
 f_{|\mathcal{X}|+3}(p(v|x)) &= H(Y|U = u). \tag{72}
 \end{aligned}$$

From the support lemma [24, Appendix C], we know that there exists a random variable U' on $\mathcal{U}'$ with $|\mathcal{U}'| \leq |\mathcal{X}| + 3$ to preserve Q_X , $H(X|U, V)$, $H(Y|U, V)$, $H(X|U)$ and $H(Y|U)$.

For each $u' \in \mathcal{U}'$, consider the following $|\mathcal{U}'| + 2$ continuous functions:

$$\begin{aligned}
 f_j(p(u', v|x)) &= p(u', v|x), \quad j = 1, \dots, |\mathcal{U}'| - 1, \\
 f_{|\mathcal{U}'|}(p(u', v|x)) &= H(X|U' = u', V = v), \\
 f_{|\mathcal{U}'|+1}(p(u', v|x)) &= H(Y|U' = u', V = v). \tag{73}
 \end{aligned}$$

From the support lemma [24, Appendix C], we know there exists a random variable $\{U' = u', V'\} | X \sim p(u', v'|x)$ on $\mathcal{V}'$ with $|\mathcal{V}'| \leq |\mathcal{X}| + 2$ to preserve $P_{U'|X}$, $H(X|U' = u', V)$, $H(Y|U' = u', V = v)$.

Therefore, we have shown that $U \in \mathcal{U}$ and $V \in \mathcal{V}$ can be equivalently replaced by $U' \in \mathcal{U}'$ and $V' \in \mathcal{V}'$ satisfying $|\mathcal{U}'| \leq |\mathcal{X}| + 3$, $|\mathcal{V}'| \leq |\mathcal{U}'| + 1$, and preserving the terms $H(X|U, V)$, $H(Y|U, V)$, $H(X|U)$ and $H(Y|U)$.

REFERENCES

- [1] F. Willems, T. Kalker, J. Goseling, and J. P. Linnartz, "On the capacity of a biometrical identification system," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*. IEEE, Jun. 2003, pp. 82–87.
- [2] E. Tuncel, "Capacity/storage tradeoff in high-dimensional identification systems," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*. IEEE, Jul. 2006, pp. 1929–1933.
- [3] F. M. J. Willems, "Searching methods for biometric identification systems: Fundamental limits," in *IEEE Int. Symp. Inf. Theory (ISIT)*. IEEE, 2009, pp. 2241–2245.
- [4] F. Farhadzadeh and F. M. J. Willems, "Identification rate, search and memory complexity tradeoff: Fundamental limits," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6173–6188, Nov. 2016.
- [5] M. T. Vu, T. J. Oechtering, and M. Skoglund, "Hierarchical identification with pre-processing," in *Proc. IEEE Int. Symp. Inf. Theory*. IEEE, Jun. 2017, pp. 2746–2750.
- [6] 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.
- [7] —, "Fundamental limits for privacy-preserving biometric identification systems that support authentication," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5583–5594, Oct. 2015.
- [8] K. Kittichokechai, T. J. Oechtering, and M. Skoglund, "Lossy source coding with reconstruction privacy," in *IEEE Int. Symp. Inf. Theory (ISIT)*. IEEE, 2014, pp. 386–390.
- [9] J. Villard and P. Piantanida, "Secure multiterminal source coding with side information at the eavesdropper," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3668–3692, 2013.
- [10] A. Makhdoomi, S. Salamatian, N. Fawaz, and M. Médard, "From the information bottleneck to the privacy funnel," in *IEEE Information Theory Workshop (ITW)*. IEEE, 2014, pp. 501–505.
- [11] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 838–852, 2013.
- [12] M. Diaz, H. Wang, F. P. Calmon, and L. Sankar, "On the robustness of information-theoretic privacy measures and mechanisms," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 1949–1978, 2020.
- [13] B. Rassouli and D. Gündüz, "On perfect privacy," in *IEEE Int. Symp. Inf. Theory (ISIT)*. IEEE, 2018, pp. 2551–2555.
- [14] L. Lai, S. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems—part i: Single use case," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 122–139, March 2011.
- [15] —, "Privacy–security trade-offs in biometric security systems—part ii: Multiple use case," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 140–151, March 2011.
- [16] K. Kittichokechai and G. Caire, "Secret key-based identification and authentication with a privacy constraint," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6189–6203, 2016.
- [17] L. Zhou, M. T. Vu, T. J. Oechtering, and M. Skoglund, "Fundamental limits for biometric identification systems without privacy leakage," in *57th Annu. Allerton Conf. Commun. Control Comput.* IEEE, Sep. 2019, pp. 1105–1112.
- [18] V. Yachongka and H. Yagi, "Identification, secrecy, template, and privacy-leakage of biometric identification system under noisy enrollment," *arXiv preprint arXiv:1902.01663*, 2019.
- [19] —, "A new characterization of the capacity region of identification systems under noisy enrollment," in *54th Annual. Conf. Inf. Sciences Systems*. IEEE, 2020, pp. 1–6.
- [20] O. Günlü, G. Kramer, and M. Skórski, "Privacy and secrecy with multiple measurements of physical and biometric identifiers," in *IEEE Conf. Commun. Network Security*. IEEE, 2015, pp. 89–94.
- [21] O. Günlü and G. Kramer, "Privacy, secrecy, and storage with multiple noisy measurements of identifiers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2872–2883, 2018.
- [22] O. Günlü, K. Kittichokechai, R. F. Schaefer, and G. Caire, "Controllable identifier measurements for private authentication with secret keys," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1945–1959, 2018.
- [23] O. Günlü, R. F. Schaefer, and H. V. Poor, "Biometric and physical identifiers with correlated noise for controllable private authentication," *arXiv preprint arXiv:2001.00847*, 2020.
- [24] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge university press, 2011.
- [25] P. Minero, S. H. Lim, and Y.-H. Kim, "A unified approach to hybrid coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 4, pp. 1509–1523, 2015.
- [26] M. T. Vu, T. J. Oechtering, M. Wiese, and M. Skoglund, "Cooperative successive refinement with side information," manuscript in preparation. [Online]. Available: <https://people.kth.se/%7Eoech/jnlp.pdf>
- [27] A. Wyner, "A theorem on the entropy of certain binary sequences and applications—i," *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 769–772, 1973.