

Biometric Identification Systems With Noisy Enrollment for Gaussian Source

Vamoua Yachongka*

Hideki Yagi*

Yasutada Oohama*

*Dept. of Network and Computer Engineering, The University of Electro-Communications,
1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585 Japan.

Email: {va.yachonka,h.yagi,oohama}@uec.ac.jp

Abstract—In the present paper, we investigate the fundamental trade-off of identification, secrecy, storage, and privacy-leakage rates in biometric identification systems for hidden or remote Gaussian sources. We introduce a technique for deriving the capacity region of these rates by converting the system to one where the data flow is in one-way direction. Also, we provide numerical calculations of three different examples for the generated-secret model. The numerical results imply that it seems hard to achieve both high secrecy and small privacy-leakage rates simultaneously. In addition, as special cases, the characterization coincides with several known results in previous studies.

I. INTRODUCTION

The identification capacity of biometric identification systems (BIS) was clarified in [1] for both discrete memoryless and Gaussian sources. For the discrete memoryless source (DMS), the fundamental performances of the BIS are extensively analyzed in [2], [3] for a visible source model (VSM) and in [4], [5] for a remote source model (RSM). However, the studies under Gaussian settings are still few. For example, the optimal trade-off between secrecy and privacy-leakage was clarified in [6] and in order to speed up search complexity, hierarchical identification was taken into account in [7]. A common stand in [6], [7] is that the VSM was assumed.

In this study, we extend the BIS assuming the RSM in [5] to Gaussian sources. This is motivated by the fact that the signal of biometric data (bio-data) is basically represented by vectors with continuous elements in real application and most communication links can be modeled as Gaussian channels. What is more, when the model is switched from the VSM to the RSM, the evaluation becomes more challenging [4], [5] and many existing techniques for deriving the results of the VSM are not directly applicable. Thus, the extension is of both theoretical and practical interest. Our goal is to find the optimal trade-off of identification and secrecy rates in the BIS under privacy and storage constraints. We demonstrate that an idea of converting the system to another one where the data flow of each user is in the same direction, which enables us to characterize the capacity region. More specifically, in establishing the outer bound of the region, the converted system allows us to use the well-known entropy power inequality (EPI) [8] twice in two opposite directions, and also its property facilitates the derivation of the inner bound. In [4], Mrs. Gerber's lemma was applied twice, too, to simplify the rate region of the RSM for binary sources without converting the BIS. That was possible due to the uniformity

of the source, and the backward channel of the enrollment channel is also the binary symmetric channel with the same crossover probability. However, this claim is no longer true in the Gaussian case, so it is necessary to formulate the general behavior of the backward channel. We also provide numerical calculations of three different examples. As a consequence, we may conclude that it is difficult to achieve high secrecy and small privacy-leakage rates at the same time. To achieve a small privacy-leakage rate, the secrecy rate is sacrificed somehow. Furthermore, as a by-product of our result, the capacity regions of the BIS analyzed in [4] (the BIS with a single user) is obtained, and as special cases, it can be checked that this characterization reduces to the results given in [1], [6].

II. SYSTEM MODEL AND CONVERTED SYSTEM

A. Notation and System Model

Upper-case A and lower-case $a \in \mathcal{A}$ denote random variable (RV) and its realization, respectively. $A^n = (A_1, \dots, A_n)$ represents a string of RVs and subscripts represent the position of a RV in the string. f_A denotes the probability density function (pdf) of RV A . For integers k and t such that $k < t$, $[k : t]$ denotes the set $\{k, k+1, \dots, t\}$. $\log x$ stands for the natural logarithm of $x > 0$. $\mathcal{A}_\epsilon^{(n)}(\cdot)$ denotes the weakly ϵ -typical set [9], and $\mathcal{B}_\epsilon^{(n)}(\cdot)$ is a modified ϵ -typical set, defined as follows.

Definition 1. (Modified ϵ -typical set [2, Appendix A-A])

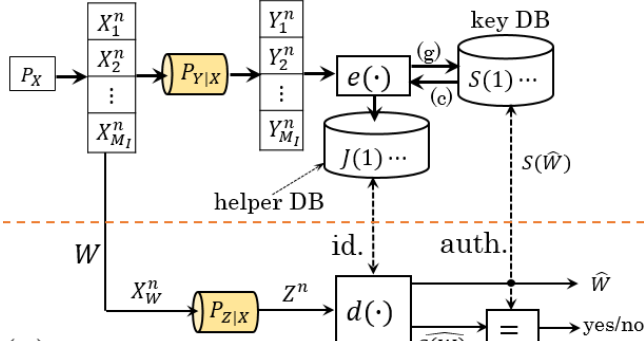
Consider that (X, Y, U) forms a Markov chain $X - Y - U$, i.e., $f_{XYU}(x, y, u) = f_{XY}(x, y)f_{U|Y}(u|y)$. The modified ϵ -typical set $\mathcal{B}_\epsilon^{(n)}(YU)$ is defined as

$$\mathcal{B}_\epsilon^{(n)}(YU) = \left\{ (y^n, u^n) : \Pr\{X^n \in \mathcal{A}_\epsilon^{(n)}(X|y^n, u^n) | (Y^n, U^n) = (y^n, u^n)\} \geq 1 - \epsilon \right\}, \quad (1)$$

where ϵ is small enough positive, and X^n is drawn i.i.d. from the transition probability $\prod_{k=1}^n f_{X|Y}(x_k|y_k)$. In addition, define $\mathcal{B}_\epsilon^{(n)}(U|y^n) = \{u^n : (u^n, y^n) \in \mathcal{B}_\epsilon^{(n)}(YU)\}$ for all y^n , and $\mathcal{B}_\epsilon^{(n)}(U|y^n)^c$ denotes the complementary set of $\mathcal{B}_\epsilon^{(n)}(U|y^n)$.

The generated-secret BIS model and chosen-secret BIS model considered in this study are depicted in Fig. 1. Arrows (g) and (c) indicate the directions of the secret key of the

(I) Enrollment Phases



(II) Identification Phase

Fig. 1. The generated- and chosen-secret BIS models

former and latter models. In the former model, the secret key is extracted from the bio-data sequence, while in the latter one, it is chosen independently. Let $\mathcal{I} = [1 : M_I]$, $\mathcal{S} = [1 : M_S]$, and $\mathcal{J} = [1 : M_J]$ be the sets of user's indexes, secret keys, and helper data, respectively. These sets are assumed to be finite. X_i^n , Y_i^n , and Z^n denote the bio-data sequence of user i generated from source P_X , the output of X_i^n via the enrollment channel $P_{Y|X}$, and the output of X_i^n via the identification channel $P_{Z|X}$, respectively. For $i \in \mathcal{I}$ and $k \in [1 : n]$, we assume $X_{ik} \sim \mathcal{N}(0, 1)$. Note that RV with unit variance can be obtained by applying a scaling technique. $P_{Y|X}$ and $P_{Z|X}$ are modeled as follows:

$$Y_{ik} = \rho_1 X_{ik} + N_1, \quad Z_k = \rho_2 X_{ik} + N_2, \quad (2)$$

where $|\rho_1| < 1$, $|\rho_2| < 1$ are the Pearson's correlation coefficients, and $N_1 \sim \mathcal{N}(0, 1 - \rho_1^2)$ and $N_2 \sim \mathcal{N}(0, 1 - \rho_2^2)$ are Gaussian RVs, independent of each other and bio-data sequences. From (2), Y and Z are Gaussian with zero mean and unit variance, and the Markov chain $Y - X - Z$ holds. Then, the pdf corresponding to the tuple (X_i^n, Y_i^n, Z^n) is given by

$$f_{X_i^n Y_i^n Z^n}(x_i^n, y_i^n, z_i^n) = \prod_{k=1}^n f_{XYZ}(x_{ik}, y_{ik}, z_{ik}), \quad (3)$$

where for $x, y, z \in \mathbf{R}$,

$$f_{XYZ}(x, y, z) = f_X(x) \cdot f_{Y|X}(y|x) \cdot f_{Z|X}(z|x), \quad (4)$$

$$= \frac{1}{\sqrt{(2\pi)^3(1-\rho_1^2)(1-\rho_2^2)}} \cdot \exp\left(-\left(\frac{x^2}{2} + \frac{(y-\rho_1x)^2}{2(1-\rho_1^2)} + \frac{(z-\rho_2x)^2}{2(1-\rho_2^2)}\right)\right). \quad (5)$$

In the generated-secret BIS model, upon observing Y_i^n , the encoder e generates secret key $S(i) \in \mathcal{S}$ and helper data $J(i) \in \mathcal{J}$ as $(S(i), J(i)) = e(Y_i^n)$. $J(i)$ is stored at position i in public database (helper DB) and $S(i)$ is saved in key DB, which is installed in a secure location. Seeing Z^n , the decoder d estimates $(\widehat{W}, \widehat{S}(\widehat{W}))$ from Z^n and all helper data in DB $\mathbf{J} \equiv \{J(1), \dots, J(M_I)\}$, i.e., $(\widehat{W}, \widehat{S}(\widehat{W})) = d(Z^n, \mathbf{J})$. In the chosen-secret BIS model, $S(i)$ is chosen uniformly from \mathcal{S} and independent of other RVs. The encoder forms the helper data by $J(i) = e(Y_i^n, S(i))$ for every individual. The decoder d owns the same functionality as the generated-secret model.

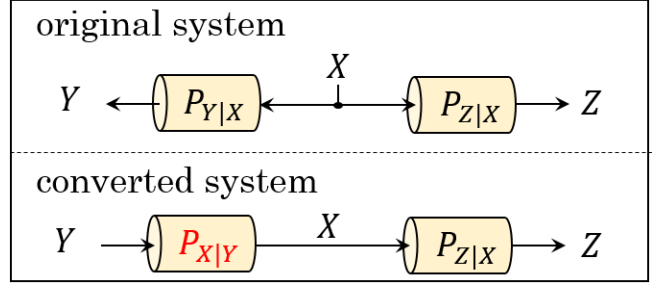


Fig. 2. The original (top) and converted (bottom) systems

B. Converted System

The original system, having X as input source and Y, Z as outputs, is in the top figure in Fig. 2. There are two main obstacles toward characterizing the capacity regions directly from this system. (I) In establishing the converse proof, an upper bound regarding RV Y for a fixed condition of RV X is needed, but it is laborious to pursue the desired bound since applying EPI to the first relation in (2) only produces a lower bound. (II) It seems difficult to prove the achievability part based on generating auxiliary sequences from edge X , e.g., the rate settings. To overcome these bottlenecks, we introduce an idea of converting the original system to a new one in which the data flow of each user is one-way from Y to Z without losing its general properties. The image of this idea is shown in the bottom figure of Fig. 2, where Y becomes input virtually. To achieve this objective, knowing the property of the backward channel $P_{X|Y}$, namely, how X correlates to the virtual input Y , is crucial and we explore that in the rest of this section.

Due to the Markov chain $Y - X - Z$, (4) can also be expanded in the following form.

$$f_{XYZ}(x, y, z) = f_Y(y) \cdot f_{X|Y}(x|y) \cdot f_{Z|X}(z|x). \quad (6)$$

Observe that

$$\begin{aligned} \frac{x^2}{2} + \frac{(y-\rho_1x)^2}{2(1-\rho_1^2)} &= \frac{x^2}{2} + \frac{y^2}{2(1-\rho_1^2)} - \frac{\rho_1xy}{1-\rho_1^2} + \frac{(\rho_1x)^2}{2(1-\rho_1^2)} \\ &= \frac{y^2}{2} + \frac{(x-\rho_1y)^2}{2(1-\rho_1^2)}. \end{aligned} \quad (7)$$

Without loss of generality, the exponential part in (5) can be rearranged as

$$-\left(\frac{y^2}{2} + \frac{(x-\rho_1y)^2}{2(1-\rho_1^2)} + \frac{(z-\rho_2x)^2}{2(1-\rho_2^2)}\right). \quad (8)$$

From (6) and (8), we may conclude that the following equations hold.

$$X_{ik} = \rho_1 Y_{ik} + N'_1, \quad (9)$$

$$Z_k = \rho_2 X_{ik} + N_2 = \rho_1 \rho_2 Y_{ik} + \rho_2 N'_1 + N_2 \quad (10)$$

with some RV $N'_1 \sim \mathcal{N}(0, 1 - \rho_1^2)$. Equation (9) describes the output of the backward channel with having Y as input. The above relations play key roles for solving the problem of the RSM, and indeed we use them in many steps during the analysis in this study. In [6] and [7], the concept of this

transformation is not seen because the enrollment channel does not exist due to the assumption of VSM as mentioned before.

Remark 1. In case there is no operation of scaling, equations (9) and (10) are settled as follows. Suppose that $X_{ik} \sim \mathcal{N}(0, \sigma_x^2)$, $Y_{ik} = X_{ik} + D_1$, and $Z_k = X_{ik} + D_2$, where $D_1 \sim \mathcal{N}(0, \sigma_1^2)$ and $D_2 \sim \mathcal{N}(0, \sigma_2^2)$ are Gaussian RVs, and independent of other RVs. By applying the arguments around (6)–(8), we obtain that

$$X_{ik} = \frac{\sigma_x^2}{\sigma_x^2 + \sigma_1^2} Y_{ik} + D'_1 \quad (11)$$

$$Z_k = X_{ik} + N'_2 = \frac{\sigma_x^2}{\sigma_x^2 + \sigma_1^2} Y_{ik} + D'_1 + D_2, \quad (12)$$

where $D'_1 \sim \mathcal{N}(0, \frac{\sigma_x^2 \sigma_1^2}{\sigma_x^2 + \sigma_1^2})$ is Gaussian and independent of other RVs. The capacity regions of the models considered in this study can also be characterized from (11) and (12). However, equation developments need more space and it does not look so neat. Herein, we pursue our results based on the method that RVs X , Y , and Z are standardized.

Now from (9) and (10), it is not difficult to calculate that

$$I(X; Y) = \frac{1}{2} \log \left(\frac{1}{1 - \rho_1^2} \right), \quad (13)$$

$$I(Z; Y) = \frac{1}{2} \log \left(\frac{1}{1 - \rho_1^2 \rho_2^2} \right), \quad (14)$$

where (14) is attained because the variance of the noise term $\rho_2 N'_1 + N_2$ in (10) is equal to $1 - \rho_1^2 \rho_2^2$.

III. STATEMENT OF RESULTS

In this section, we provide the formal definitions of both the generated- and chosen-secret BIS models, and state the main results.

A. Problem Formulation and Main Results

The achievability definition for the generated-secret BIS model is given below.

Definition 2. A tuple of identification, secrecy, storage, and privacy-leakage rates (R_I, R_S, R_J, R_L) is said to be achievable for a Gaussian source if for any $\delta > 0$ and large enough n there exist pairs of encoders and decoders satisfying

$$\max_{i \in \mathcal{I}} \Pr\{(\widehat{W}, \widehat{S(W)}) \neq (W, S(W)) | W = i\} \leq \delta, \quad (15)$$

$$\frac{1}{n} \log M_I \geq R_I - \delta, \quad (16)$$

$$\min_{i \in \mathcal{I}} \frac{1}{n} H(S(i)) \geq R_S - \delta, \quad (17)$$

$$\frac{1}{n} \log M_J \leq R_J + \delta, \quad (18)$$

$$\max_{i \in \mathcal{I}} \frac{1}{n} I(S(i); J(i)) \leq \delta. \quad (19)$$

$$\max_{i \in \mathcal{I}} \frac{1}{n} I(X_i^n; J(i)) \leq R_L + \delta. \quad (20)$$

Moreover, \mathcal{R}_G is defined as the set of all achievable rate tuples for the generated-secret BIS model, called the capacity region. \square

The achievability definition for the chosen-secret BIS model is provided as follows:

Definition 3. A tuple (R_I, R_S, R_J, R_L) is said to be achievable for a Gaussian source if there exist pairs of encoders and decoders that satisfy all the requirements in Definition 2 for any $\delta > 0$ and large enough n . In addition, \mathcal{R}_C is defined as the capacity region of the chosen-secret BIS model. \square

Note that the left-hand side of (17) is expressed as $\frac{1}{n} \log M_S$ because $S(i)$ is chosen uniformly from \mathcal{S} .

Remark 2. It is worthwhile to mention that it is not really suitable to call the rate of helper data the storage rate. In [5], it was called the template rate instead and the reason behind the scene is that there exist two databases in the BIS, namely, databases of secret keys and helper data or templates. The storage space of the database for storing the templates is minimized, while that for the secret keys is maximized. Thus, only a part of the entire storage space of the BIS is being minimized. In this paper, however, we also use this term because it is widely used in many previous works, e.g., [3], [4].

Now we are ready to present our main results.

Theorem 1. The capacity regions for the generated- and chosen-secret BIS models are given by

$$\begin{aligned} \mathcal{R}_G = \{ & (R_I, R_S, R_J, R_L) : \\ & R_I + R_S \leq \frac{1}{2} \log \left(\frac{1}{\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2} \right), \\ & R_J \geq \frac{1}{2} \log \left(\frac{\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2}{\alpha} \right) + R_I, \\ & R_L \geq \frac{1}{2} \log \left(\frac{\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2}{\alpha \rho_1^2 + 1 - \rho_1^2} \right) + R_I, \\ & R_I \geq 0, R_S \geq 0 \text{ for some } 0 < \alpha \leq 1 \}, \end{aligned} \quad (21)$$

$$\begin{aligned} \mathcal{R}_C = \{ & (R_I, R_S, R_J, R_L) : \\ & R_I + R_S \leq \frac{1}{2} \log \left(\frac{1}{\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2} \right), \\ & R_J \geq \frac{1}{2} \log \left(\frac{1}{\alpha} \right), \\ & R_L \geq \frac{1}{2} \log \left(\frac{\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2}{\alpha \rho_1^2 + 1 - \rho_1^2} \right) + R_I, \\ & R_I \geq 0, R_S \geq 0 \text{ for some } 0 < \alpha \leq 1 \}. \end{aligned} \quad (22)$$

\square

Similar to a conclusion in [5], the lower bound on R_J in \mathcal{R}_C is greater than the one in \mathcal{R}_G . This means the chosen-secret BIS model consumes more storage space. This is because the information related to the secret key chosen at the encoder must be saved together with the helper data in DB so as to aid the estimation of the key at the decoder. Unlike R_J , the bound on R_L remains unchanged in both models, and it rises in accordance with the increase of R_I .

As a by-product of Theorem 1, the following remark is obtained.

Remark 3. The capacity regions of the generated- and chosen-secret BIS models with a single user (the models con-

sidered in [4]) for Gaussian sources are given by substituting $R_I = 0$ into \mathcal{R}_G and \mathcal{R}_C , respectively.

The proofs of Remark 3 can be done similarly to the arguments in proving Theorem 1.

As special cases, when $R_S = 0$, and R_J and R_L are large enough ($R_J, R_L \rightarrow \infty$), the maximum value of R_I is $\frac{1}{2} \log(\frac{1}{1-\rho_1^2\rho_2^2})$. This value is exactly the identification capacity $I(Y; Z)$ (cf. (14)) derived in [1], and it is achieved when $\alpha \downarrow 0$. Moreover, when $R_I = 0$, $R_J \rightarrow \infty$, and the enrollment channel is noiseless ($\rho_1 = 1$), one can see that Theorem 1 naturally reduces to the characterizations of [6].

Remark 4. If there is no scaling as in (11) and (12) in Remark 1, the capacity regions of the generated- and chosen-secret BIS models \mathcal{R}'_G and \mathcal{R}'_C , respectively, are characterized as follows:

$$\begin{aligned} \mathcal{R}'_G = \{(R_I, R_S, R_J, R_L) : \\ R_I + R_S &\leq \frac{1}{2} \log \left(\frac{(\sigma_x^2 + \sigma_1^2)(\sigma_x^2 + \sigma_2^2)}{\alpha\sigma_x^4 + \sigma_x^2\sigma_1^2 + \sigma_1^2\sigma_2^2 + \sigma_2^2\sigma_x^2} \right), \\ R_J &\geq \frac{1}{2} \log \left(\frac{\alpha\sigma_x^4 + \sigma_x^2\sigma_1^2 + \sigma_1^2\sigma_2^2 + \sigma_2^2\sigma_x^2}{\alpha(\sigma_x^2 + \sigma_1^2)(\sigma_x^2 + \sigma_2^2)} \right) + R_I, \\ R_L &\geq \frac{1}{2} \log \left(\frac{\alpha\sigma_x^4 + \sigma_x^2\sigma_1^2 + \sigma_1^2\sigma_2^2 + \sigma_2^2\sigma_x^2}{(\alpha\sigma_x^2 + \sigma_1^2)(\sigma_x^2 + \sigma_2^2)} \right) + R_I, \\ R_I &\geq 0, R_S \geq 0 \text{ for some } 0 < \alpha \leq 1\}, \end{aligned} \quad (23)$$

$$\begin{aligned} \mathcal{R}'_C = \{(R_I, R_S, R_J, R_L) : \\ R_I + R_S &\leq \frac{1}{2} \log \left(\frac{(\sigma_x^2 + \sigma_1^2)(\sigma_x^2 + \sigma_2^2)}{\alpha\sigma_x^4 + \sigma_x^2\sigma_1^2 + \sigma_1^2\sigma_2^2 + \sigma_2^2\sigma_x^2} \right), \\ R_J &\geq \frac{1}{2} \log \left(\frac{1}{\alpha} \right), \\ R_L &\geq \frac{1}{2} \log \left(\frac{\alpha\sigma_x^4 + \sigma_x^2\sigma_1^2 + \sigma_1^2\sigma_2^2 + \sigma_2^2\sigma_x^2}{(\alpha\sigma_x^2 + \sigma_1^2)(\sigma_x^2 + \sigma_2^2)} \right) + R_I, \\ R_I &\geq 0, R_S \geq 0 \text{ for some } 0 < \alpha \leq 1\}. \end{aligned} \quad (24)$$

It can be verified that \mathcal{R}_G and \mathcal{R}_C are equivalent to \mathcal{R}'_G and \mathcal{R}'_C , respectively, if we set $\rho_1^2 = \frac{\sigma_x^2}{\sigma_x^2 + \sigma_1^2}$ and $\rho_2^2 = \frac{\sigma_x^2}{\sigma_x^2 + \sigma_2^2}$.

B. Examples

For the sake of succinct discussion, we only concentrate on the generated-secret BIS model at which $R_I = 0$. We first look over some special points of secrecy and privacy-leakage rates when storage rate becomes extremely low or large. We first define two rate functions

$$R_S^*(R_J) = \max_{(R_S, R_J, R_L) \in \mathcal{R}_G} R_S, \quad (25)$$

$$R_L^*(R_J) = \min_{(R_S, R_J, R_L) \in \mathcal{R}_G} R_L, \quad (26)$$

where (25) and (26) are the maximum secrecy rate and minimum privacy-leakage rate, respectively, for given R_J . Moreover, we define $R_J^\alpha = \frac{1}{2} \log(\frac{\alpha\rho_1^2\rho_2^2 + 1 - \rho_1^2\rho_2^2}{\alpha})$ so that we can write

$$R_S^*(R_J^\alpha) = \frac{1}{2} \log \left(\frac{1 - \rho_1^2\rho_2^2/2^{2(R_J^\alpha)}}{1 - \rho_1^2\rho_2^2} \right), \quad (27)$$

$$R_L^*(R_J^\alpha) = \frac{1}{2} \log \left(\frac{1 - \rho_1^2\rho_2^2}{1 - \rho_1^2 + \rho_1^2(1 - \rho_2^2)/2^{2(R_J^\alpha)}} \right). \quad (28)$$

As $R_J^\alpha \rightarrow \infty$ ($\alpha \downarrow 0$), the optimal asymptotic secrecy rate and the quantity of privacy-leakage approach to

$$\lim_{R_J^\alpha \rightarrow \infty} R_S^*(R_J^\alpha) = \frac{1}{2} \log \left(\frac{1}{1 - \rho_1^2\rho_2^2} \right) = I(Y; Z), \quad (29)$$

$$\begin{aligned} \lim_{R_J^\alpha \rightarrow \infty} R_L^*(R_J^\alpha) &= \frac{1}{2} \log \left(\frac{1 - \rho_1^2\rho_2^2}{1 - \rho_1^2} \right) \\ &= \frac{1}{2} \log \left(\frac{1}{1 - \rho_1^2} \right) - \frac{1}{2} \log \left(\frac{1}{1 - \rho_1^2\rho_2^2} \right) \\ &= I(X; Y) - I(Z; Y). \end{aligned} \quad (30)$$

The result (29) corresponds to the optimal asymptotic secrecy rate [6, Sect. III-B] and in order to achieve this rate, it is required to take the storage rate to infinity and leak the user's privacy up to rate $I(X; Y) - I(Z; Y)$.

In contrast, when $R_J \downarrow 0$, it is evident that R_S and R_L become zero as well, which does not carry much information. However, to investigate the BIS that achieves high secrecy and small privacy-leakage rates in the low storage rate regime, the zero-rate slopes of secrecy and privacy-leakage rates, namely, how fast they converge to zero, are important indicators. In views of (27) and (28), by a few steps of calculations, the slopes of secrecy and privacy-leakage rates at $R_J \downarrow 0$ can be determined as follows:

$$\left. \frac{dR_S^*(R_J^\alpha)}{dR_J^\alpha} \right|_{R_J^\alpha=0} = \frac{\rho_1^2\rho_2^2}{1 - \rho_1^2\rho_2^2}, \quad (31)$$

$$\left. \frac{dR_L^*(R_J^\alpha)}{dR_J^\alpha} \right|_{R_J^\alpha=0} = \frac{\rho_1^2(1 - \rho_2^2)}{1 - \rho_1^2\rho_2^2} = \frac{\rho_1^2\rho_2^2}{1 - \rho_1^2\rho_2^2} \cdot \frac{1 - \rho_2^2}{\rho_2^2}, \quad (32)$$

where (31) is equal to the signal-to-noise ratio of the compound channel from Y to Z . This value multiplied by the reverse of the signal-to-noise ratio of the channel $P_{Z|X}$ appears in the slope of privacy-leakage rate in (32).

Next, we give numerical computations of three different examples and take a look into behaviors of the special points.

Ex. 1: a) $\rho_1^2 = 3/4, \rho_2^2 = 2/3$, b) $\rho_1^2 = 7/8, \rho_2^2 = 2/3$,

c) $\rho_1^2 = 15/16, \rho_2^2 = 2/3$,

Ex. 2: a) $\rho_1^2 = 3/4, \rho_2^2 = 2/3$, b) $\rho_1^2 = 9/10, \rho_2^2 = 7/8$,

c) $\rho_1^2 = 15/16, \rho_2^2 = 11/12$,

Ex. 3: a) $\rho_1^2 = 3/4, \rho_2^2 = 2/3$, b) $\rho_1^2 = 3/4, \rho_2^2 = 8/9$,

c) $\rho_1^2 = 3/4, \rho_2^2 = 14/15$.

Note that as ρ_1^2, ρ_2^2 are large, the noises added to the bio-data sequences at encoder and decoder become small. Example 1 is the case where the noise at encoder is gradually small from a) to c), but the noise at the decoder stays constant for each round. Example 2 is the case in which the noises at both encoder and decoder are improved gradually from a) to c). Example 3 is opposite to Example 1. The calculated results of the secrecy and privacy-leakage rates for these cases are summarized in Table I and II, and Fig. 3–6.

It is ideal to keep the privacy-leakage rate small, while produce high secrecy rate, but Example 1 works out in the opposite way (cf. the rows of Ex. 1 in Table I and II), so this

TABLE I
THE SECRECY AND PRIVACY-LEAKAGE RATES WHEN $R_J \rightarrow \infty$.

Cases	Secrecy rate			Privacy-Leakage rate		
	a)	b)	c)	a)	b)	c)
Ex. 1	0.5	0.63	0.70	0.5	0.87	1.29
Ex. 2	0.5	1.12	1.41	0.5	0.54	0.59
Ex. 3	0.5	0.79	0.87	0.5	0.20	0.13

TABLE II
THE SLOPES OF SECRECY AND PRIVACY-LEAKAGE RATES AT $R_J \downarrow 0$.

Cases	Secrecy rate			Privacy-Leakage rate		
	a)	b)	c)	a)	b)	c)
Ex. 1	1.0	1.40	1.67	0.5	0.7	0.83
Ex. 2	1.0	3.71	6.11	0.5	0.53	0.56
Ex. 3	1.0	2.0	2.33	0.5	0.25	0.17

is not a preferable choice. Example 2 realizes a high secrecy rate, but the amount of privacy-leakage remains high at some level, too (cf. the rows of Ex. 2 in Table I and II, and Fig. 3 and 4). On the other hand, in Example 3, the privacy-leakage rate declines, but the secrecy rate becomes small compared to Example 3 (cf. the rows of Ex. 3 in Table I and II, and Fig. 5 and 6). From these behaviors, we may conclude that it is unmanageable to achieve both a high secrecy rate and small privacy-leakage at the same time. If one aims to achieve a high secrecy rate, it is important to diminish the noises at both encoder and decoder, e.g., deploying quantizers with high quality, but this could result in leaking more user's privacy. In different circumstances, to achieve a small privacy-leakage rate, it is preferable to maintain a certain level of noise at encoder and pay sufficient attention for processing the noise at decoder. In this way, however, the gain of the secrecy rate may be dropped.

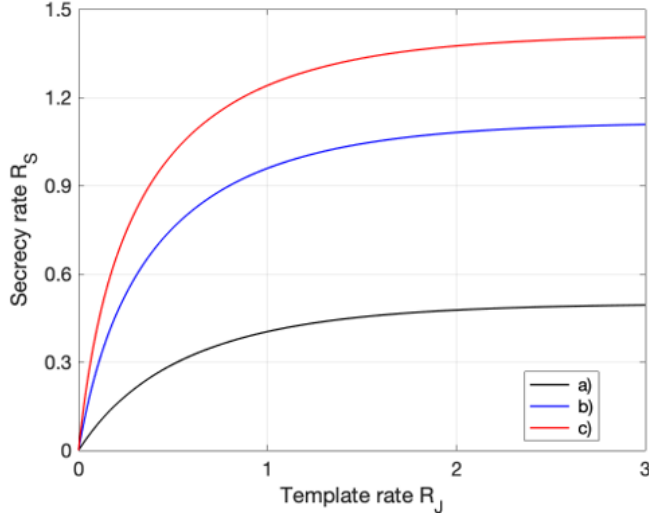


Fig. 3. The projection of the rate region onto $R_J R_S$ -plane for Ex. 2.

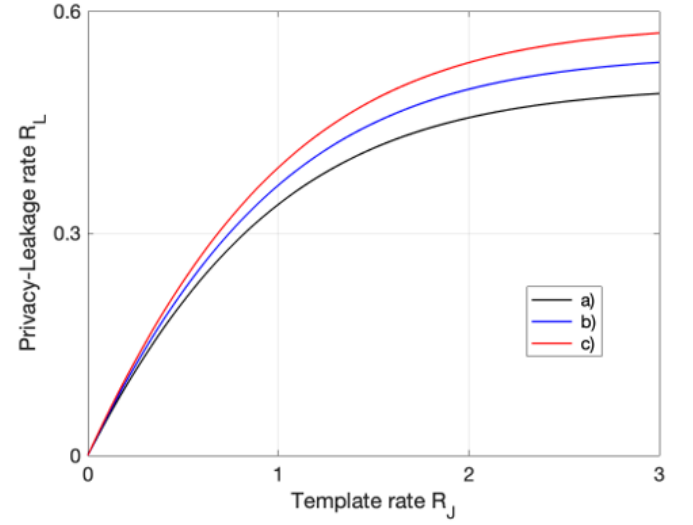


Fig. 4. The projection of the rate region onto $R_J R_L$ -plane for Ex. 2.

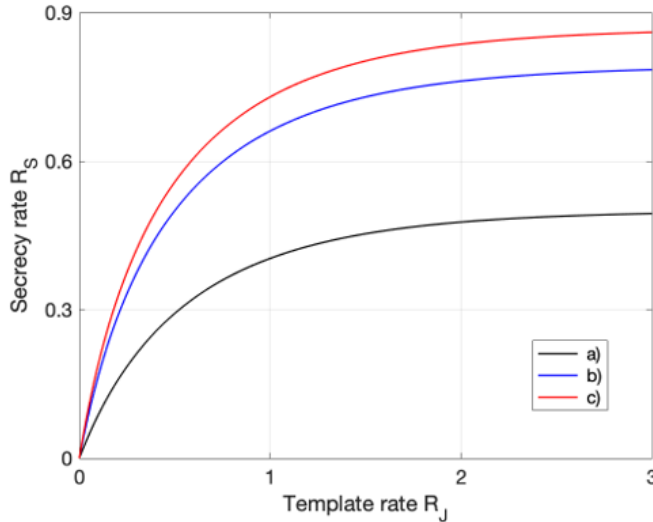


Fig. 5. The projection of the rate region onto $R_J R_S$ -plane for Ex. 3.

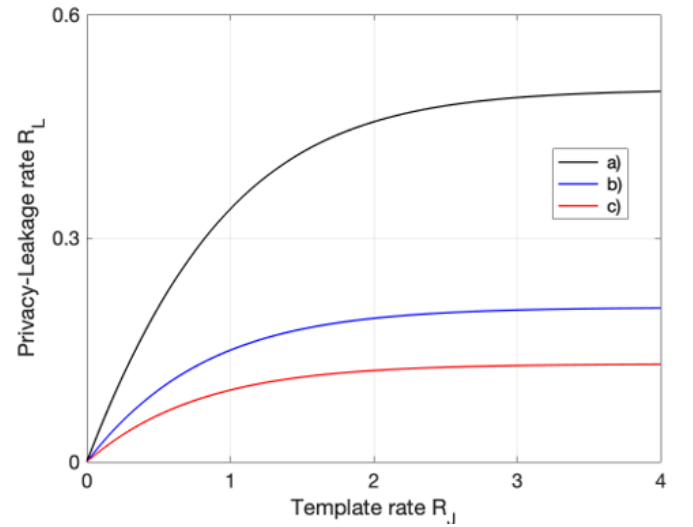


Fig. 6. The projection of the rate region into $R_J R_L$ -plane for Ex. 3.

IV. PROOF OF THE REGION \mathcal{R}_G

In this section, we give the proof of the capacity region of the generated-secret BIS model.

A. Converse Part

We consider a more relaxed case where W is uniformly distributed on \mathcal{I} , and (15) is replaced with the average error criterion $\Pr\{(\widehat{W}, \widehat{S(W)}) \neq (W, S(W))\} \leq \delta$. We shall show that the capacity region for this case, which contains \mathcal{R}_G , is contained in (21). We assume that a rate tuple (R_I, R_S, R_J, R_L) is achievable.

Analysis of Secrecy Rate: We begin with considering the joint entropy of W and $S(W)$ as

$$\begin{aligned}
& H(W, S(W)) \\
&= H(W, S(W)|Z^n, \mathbf{J}) + I(W, S(W); Z^n, \mathbf{J}) \\
&\stackrel{(a)}{=} H(W, S(W)|\widehat{W}, \widehat{S(W)}, Z^n, \mathbf{J}) + I(W, S(W); \mathbf{J}) \\
&\quad + I(W, S(W); Z^n|\mathbf{J}) \\
&\stackrel{(b)}{\leq} H(W, S(W)|\widehat{W}, \widehat{S(W)}) + I(W, S(W); J(W)) \\
&\quad + I(W, S(W); Z^n|J(W)) \\
&\stackrel{(c)}{\leq} n\delta_n + I(W; J(W)) + I(S(W); J(W)|W) \\
&\quad + I(W, S(W); Z^n|J(W)) \\
&\stackrel{(d)}{\leq} n(\delta_n + \delta) + h(Z^n|J(W)) - h(Z^n|J(W), S(W)) \\
&\stackrel{(e)}{\leq} n(\delta_n + \delta) + h(Z^n) - h(Z^n|J(W), S(W)), \quad (33)
\end{aligned}$$

where

- (a) holds since $(\widehat{W}, \widehat{S(W)})$ is a function of (Z^n, \mathbf{J}) ,
- (b) follows because conditioning reduces entropy, and only $J(W)$ is possibly dependent on Z^n and $S(W)$,
- (c) is due to Fano's inequality with $\delta_n = \frac{1}{n}(1 + \delta \log M_I M_S)$,
- (d) follows since W is independent of other RVs and (19) is applied,
- (e) follows because conditioning reduces entropy.

Also, since W is uniformly distributed on \mathcal{I} , we have that

$$\begin{aligned}
H(W, S(W)) &= H(W) + H(S(W)|W) \\
&\geq \log M_I + \min_{w \in \mathcal{I}} H(S(w)). \quad (34)
\end{aligned}$$

From (16), (17), (33), and (34), it yields that

$$R_I + R_S \leq h(Z) - \frac{1}{n}h(Z^n|J(W), S(W)) + 3\delta + \delta_n. \quad (35)$$

Analysis of Storage Rate:

$$\begin{aligned}
n(R_J + \delta) &\geq \log M_J \geq \max_{w \in \mathcal{I}} H(J(w)) \geq H(J(W)|W) \\
&= I(Y_W^n; J(W)|W) = I(Y_W^n, W; J(W)) \\
&= I(Y_W^n, W, S(W); J(W)) \\
&\quad - I(S(W); J(W)|Y_W^n, W) \\
&\stackrel{(f)}{=} h(Y_W^n, W, S(W)) - h(Y_W^n, W, S(W)|J(W)) \\
&\stackrel{(g)}{=} h(Y_W^n) + H(W) - H(W, S(W)|J(W)) \\
&\quad - h(Y_W^n|J(W), S(W)) \\
&\stackrel{(h)}{\geq} h(Y_W^n) + \log M_I - H(W, S(W)) \\
&\quad - h(Y_W^n|J(W), S(W)) \\
&\stackrel{(i)}{\geq} h(Z^n|J(W), S(W)) - h(Y_W^n|J(W), S(W)) \\
&\quad + nR_I - n(\delta_n + 2\delta), \quad (36)
\end{aligned}$$

where

- (f) hold as $(S(W), J(W))$ is a function of Y_W^n ,
- (g) follows since W is independent of other RVs, and $S(W)$ is a function of Y_W^n ,
- (h) follows because conditioning reduces entropy and W is uniformly distributed on \mathcal{I} ,
- (i) follows because $h(Y_W^n) = h(Z^n) = \frac{n}{2} \log(2\pi e)$, and (16) and (33) are applied.

Analysis of Privacy-Leakage Rate:

$$\begin{aligned}
n(R_L + \delta) &\geq \max_{w \in \mathcal{I}} I(X_w^n; J(w)) \geq I(X_W^n; J(W)|W) \\
&= I(X_W^n, W; J(W)) \\
&= I(X_W^n, W, S(W); J(W)) - I(S(W); J(W)|X_W^n, W) \\
&\geq h(X_W^n, W, S(W)) - h(X_W^n, W, S(W)|J(W)) \\
&\quad - H(S(W)|X_W^n) \\
&\geq h(X_W^n) + H(W) + H(S(W)|X_W^n) \\
&\quad - H(W, S(W)|J(W)) - h(X_W^n|J(W), S(W)) \\
&\quad - H(S(W)|X_W^n) \\
&\stackrel{(j)}{\geq} h(X_W^n) + \log M_I - H(W, S(W)) \\
&\quad - h(X_W^n|J(W), S(W)) \\
&\stackrel{(k)}{\geq} h(Z^n|J(W), S(W)) - h(X_W^n|J(W), S(W)) \\
&\quad + nR_I - n(\delta_n + 2\delta), \quad (37)
\end{aligned}$$

where

- (j) follows as conditioning reduces entropy and W is uniformly distributed on \mathcal{I} ,
- (k) follows because $h(X_W^n) = h(Z^n)$, and (16) and (33) are applied.

For further evaluations of (35)–(37), we scrutinize a lower bound on $h(Z^n|J(W), S(W))$ and an upper bound on $h(Y_W^n|J(W), S(W))$ with fixed $h(X_W^n|J(W), S(W))$ by applying the conditional EPI [10, Lemma II]. It is a key to set

$$\frac{1}{n}h(X_W^n|J(W), S(W)) = \frac{1}{2} \log(2\pi e(\alpha\rho_1^2 + 1 - \rho_1^2)) \quad (38)$$

with some $0 < \alpha \leq 1$. Indeed, this is reasonable setting because $\frac{1}{2} \log(2\pi e) \geq \frac{1}{n} h(X_W^n | J(W), S(W)) \geq \frac{1}{2} \log(2\pi e(1 - \rho_1^2))$. The lower bound is obtained from $\frac{1}{n} h(X_W^n | J(W), S(W)) \geq \frac{1}{n} h(X_W^n | Y_W^n, J(W), S(W)) = \frac{1}{n} h(X_W^n | Y_W^n)$ due to the fact that $(J(W), S(W))$ is a function of Y_W^n .

In the direction from X to Z , by applying the conditional EPI [10, Lemma II] to the first equality in (10), it follows that

$$\begin{aligned} e^{\frac{2}{n} h(Z^n | J(W), S(W))} &\geq e^{\frac{2}{n} h(\rho_2 X^n | J(W), S(W))} + e^{\frac{2}{n} h(N_2^n | J(W), S(W))}, \\ &\stackrel{(1)}{=} \rho_2^2 e^{\frac{2}{n} h(X^n | J(W), S(W))} + e^{\frac{2}{n} h(N_2^n)}, \\ &= \rho_2^2 (2\pi e(\alpha \rho_1^2 + 1 - \rho_1^2)) + 2\pi e(1 - \rho_2^2), \\ &= 2\pi e(\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2), \end{aligned} \quad (39)$$

where (1) holds as N_2^n is independent of $(J(W), S(W))$, and as a deduction,

$$\frac{1}{n} h(Z^n | J(W), S(W)) \geq \frac{1}{2} \log(2\pi e(\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2)). \quad (40)$$

In the opposite direction (from X to Y), by again applying the conditional EPI [10, Lemma II] to (9), we have that

$$e^{\frac{2}{n} h(X^n | J(W), S(W))} \geq e^{\frac{2}{n} h(\rho_1 Y^n | J(W), S(W))} + e^{\frac{2}{n} h(N_1'^n)}, \quad (41)$$

meaning that

$$2\pi e(\alpha \rho_1^2 + 1 - \rho_1^2) \geq \rho_1^2 e^{\frac{2}{n} h(Y^n | J(W), S(W))} + 2\pi e(1 - \rho_1^2) \quad (42)$$

and thus

$$e^{\frac{2}{n} h(Y^n | J(W), S(W))} \leq 2\pi e\alpha. \quad (43)$$

Hence, it follows that

$$\frac{1}{n} h(Y^n | J(W), S(W)) \leq \frac{1}{2} \log(2\pi e\alpha), \quad (44)$$

which is not derivable from the first equation in (2) of the original system. Now plugging (38), (40), and (44) into (35)–(37), we obtain that

$$R_I + R_S \leq \frac{1}{2} \log \left(\frac{1}{\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2} \right) + 3\delta + \delta_n, \quad (45)$$

$$R_J \geq \frac{1}{2} \log \left(\frac{\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2}{\alpha} \right) + R_I - (3\delta + \delta_n), \quad (46)$$

$$R_L \geq \frac{1}{2} \log \left(\frac{\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2}{\alpha \rho_1^2 + 1 - \rho_1^2} \right) + R_I - (3\delta + \delta_n). \quad (47)$$

Eventually, by letting $n \rightarrow \infty$ and $\delta \downarrow 0$, from (45)–(47), we can see that the capacity region is contained in the right-hand side of (21). \square

B. Achievability Part

Overviews:

The modified typical set (cf. Definition 1), giving the so-called Markov lemma for weak typicality, and Gaussian typicality [9, Section 8.2] help us show that the error probability of the BIS vanishes for large enough n . Though a more general version of the Markov lemma for Gaussian sources, including lossy reconstruction, is shown in [11], we found out that the two properties of the modified typical set are handy tools for checking all conditions in Definition 2, and thus we provide our proof of the achievability based on this set. For evaluating the uniformity of secret keys (17), secrecy-leakage (19), and privacy-leakage (20), we extend [12, Lemma 4] to include continuous RVs so that the extended one can be used to derive the upper bounds on conditional differential entropies of jointly typical sequences, appearing in these evaluations.

Let $0 < \alpha \leq 1$ and fix $\delta > 0$ (small enough positive), the block length n , and the joint pdf of (U, Y, X, Z) such that the Markov chain $U - Y - X - Z$ holds, where we let U be Gaussian with mean zero and variance $1 - \alpha$. Now consider that

$$Y = U + \Phi, \quad (48)$$

where Φ , independent of U , is Gaussian with mean zero and variance α . From (9) and (10) of the converted system, it yields that

$$X = \rho_1 U + \rho_1 \Phi + N_1', \quad (49)$$

$$Z = \rho_1 \rho_2 U + \rho_1 \rho_2 \Phi + \rho_2 N_1' + N_2. \quad (50)$$

Hence, we readily see that

$$\begin{aligned} I(Y; U) &= \frac{1}{2} \log \frac{1}{\alpha}, \quad I(X; U) = \frac{1}{2} \log \left(\frac{1}{\alpha \rho_1^2 + 1 - \rho_1^2} \right), \\ I(Z; U) &= \frac{1}{2} \log \left(\frac{1}{\alpha \rho_1^2 \rho_2^2 + 1 - \rho_1^2 \rho_2^2} \right). \end{aligned} \quad (51)$$

Now set $0 < R_I < I(Z; U)$, and

$$R_S = I(Z; U) - R_I - 2\delta, \quad (52)$$

$$R_J = I(Y; U) - I(Z; U) + R_I + 6\delta, \quad (53)$$

$$R_L = I(X; U) - I(Z; U) + R_I + 6\delta, \quad (54)$$

$$M_I = 2^{nR_I}, \quad M_S = 2^{nR_S}, \quad M_J = 2^{nR_J}, \quad (55)$$

where the values of $I(Y; U)$, $I(X; U)$, and $I(Z; U)$ are specified in (51). Also, remind that $\mathcal{I} = [1 : M_I]$, $\mathcal{S} = [1 : M_S]$, $\mathcal{J} = [1 : M_J]$.

Next we generate $2^{n(I(Y; U) + \delta)}$ sequences of $u^n(s, j)$, where each symbol of these sequences is i.i.d. Gaussian with mean zero and variance $1 - \alpha$, and $s \in \mathcal{S}$ and $j \in \mathcal{J}$.

Seeing y_i^n ($i \in \mathcal{I}$), the encoder finds $u^n(s, j)$ such that $(y_i^n, u^n(s, j)) \in \mathcal{B}_\delta^{(n)}(YU)$. If there are multiple pairs of such (s, j) , the encoder picks one at random. Otherwise, it declares error. We denote the chosen pair as $(s(i), j(i))$, where they are function of the index i . Template $j(i)$ is stored in the public DB and secret key $s(i)$ is saved in the key DB.

Observing z^n , the noisy sequence of the identified user x_w^n , the decoder looks for $u^n(s, j(i))$ such that $(z^n, u^n(s, j(i))) \in \mathcal{A}_\delta^{(n)}(ZU)$ for some $i \in \mathcal{I}$ and $s \in \mathcal{S}$. If a unique pair (i, s) is found, it outputs $(\widehat{w}, \widehat{s(w)}) = (i, s)$, or else it declares error. Finally, it compares $s(w)$ with $s(\widehat{w})$ in the key DB, and the authentication is successful if they match.

Let $(J(i), S(i))$ denote the index pair chosen at the encoder based on Y_i^n , i.e., $(Y_i^n, U^n(S(i), J(i))) \in \mathcal{B}_\delta^{(n)}(YU)$. Furthermore, we denote $U^n(S(i), J(i))$ as U_i^n for simplicity. Next, we check all conditions in Definition 2 hold for a random codebook $\mathcal{C}_n = \{U^n(s, j), s \in \mathcal{S} \text{ and } j \in \mathcal{J}\}$.

Analysis of Error Probability: For $W = i$, an error event possibly happens at the encoder is:

$\mathcal{E}_1 : \{(Y_i^n, U^n(s, j)) \notin \mathcal{B}_\delta^{(n)}(YU) \text{ for all } s \in \mathcal{S} \text{ and } j \in \mathcal{J}\}$, and those at the decoder are:

$\mathcal{E}_2 : \{(Z^n, U^n(J(i), S(i))) \notin \mathcal{A}_\delta^{(n)}(ZU)\}$,

$\mathcal{E}_3 : \{(Z^n, U^n(J(i), s')) \in \mathcal{A}_\delta^{(n)}(ZU) \text{ for some } \exists s' \neq S(i) (s' \in \mathcal{S})\}$.

$\mathcal{E}_4 : \{(Z^n, U^n(J(i'), s')) \in \mathcal{A}_\delta^{(n)}(ZU) \text{ for some } \exists i' \neq i (i' \in \mathcal{I}) \text{ and } s' \in \mathcal{S}\}$.

Note that the authentication process is guaranteed to be successful if the genuine index and secret key of the identified user are correctly estimated at the decoder, indicating that it is sufficient to focus on assessing the probability of incorrect estimation for the pair at the decoder. Then, the error probability can be further evaluated as

$$\begin{aligned} \Pr\{(\widehat{W}, \widehat{S(W)}) \neq (W, S(W)) | W = i\} \\ = \Pr\{\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3 \cup \mathcal{E}_4\} \\ \leq \Pr\{\mathcal{E}_1\} + \Pr\{\mathcal{E}_2 | \mathcal{E}_1^c\} + \Pr\{\mathcal{E}_3 \cup \mathcal{E}_4\}. \end{aligned} \quad (56)$$

By applying the similar arguments of [2, Appendix A-B], it can be shown that the entire error probability vanishes. Nonetheless, we provide the details for completeness of the proof.

The first term $\Pr\{\mathcal{E}_1\}$ can be evaluated as

$$\begin{aligned} \Pr\{\mathcal{E}_1\} \\ = \Pr\left[\bigcap_{s \in \mathcal{S}, j \in \mathcal{J}} (Y_i^n, U^n(s, j)) \notin \mathcal{B}_\delta^{(n)}(YU)\right] \\ = \prod_{s=1}^{|\mathcal{S}|} \prod_{j=1}^{|\mathcal{J}|} \Pr\{(Y_i^n, U^n(s, j)) \notin \mathcal{B}_\delta^{(n)}(YU)\} \\ \stackrel{(a)}{=} \int f_{Y_i^n}(y^n) \prod_{s=1}^{|\mathcal{S}|} \prod_{j=1}^{|\mathcal{J}|} \Pr\{U^n(s, j) \notin \mathcal{B}_\delta^{(n)}(U|y^n)\} dy^n \\ = \int f_{Y_i^n}(y^n) \left\{ \int_{\mathcal{B}_\delta^{(n)}(U|y^n)^c} f_{U^n}(u^n) du^n \right\}^{|\mathcal{S} \times \mathcal{J}|} dy^n \\ = \int f_{Y_i^n}(y^n) \left(1 - \int_{\mathcal{B}_\delta^{(n)}(U|y^n)} f_{U^n}(u^n) du^n\right)^{|\mathcal{S} \times \mathcal{J}|} dy^n \end{aligned}$$

$$\begin{aligned} &\stackrel{(b)}{\leq} \int f_{Y_i^n}(y^n) \left(1 - 2^{-n(I(U;Y)+3\delta)} \cdot \int_{\mathcal{B}_\delta^{(n)}(U|y^n)} f_{U^n|Y_i^n}(u^n|y^n) du^n\right)^{|\mathcal{S} \times \mathcal{J}|} dy^n \\ &\stackrel{(c)}{\leq} \int f_{Y_i^n}(y^n) \left(1 - \int_{\mathcal{B}_\delta^{(n)}(U|y^n)} f_{U^n|Y_i^n}(u^n|y^n) du^n + 2^{-|\mathcal{S} \times \mathcal{J}| \cdot 2^{-n(I(U;Y)+3\delta)}}\right) dy^n \\ &\stackrel{(d)}{=} \iint_{\mathcal{B}_\delta^{(n)}(U|y^n)^c} f_{U^n|Y_i^n}(u^n, y^n) du^n dy^n + 2^{-2^{n\delta}} \int f_{Y_i^n}(y^n) dy^n \\ &\stackrel{(e)}{\leq} 2\delta \end{aligned} \quad (57)$$

for large enough n , where

- (a) is due to the fact that Y_i^n and $U^n(s, j)$ are mutually independent,
- (b) is obtained by applying Property 1 of the modified δ -typical set [2], suggesting that if $(y^n, u^n) \in \mathcal{B}_\epsilon^{(n)}(YU)$, (y^n, u^n) is also a member of $\mathcal{A}_\epsilon^{(n)}(YU)$, and thus

$$\begin{aligned} f_{U^n}(u^n) &= f_{U^n|Y_i^n}(u^n|y^n) \frac{f_{U^n}(u^n) \cdot f_{Y_i^n}(y^n)}{f_{U^n|Y_i^n}(u^n, y^n)} \\ &\geq f_{U^n|Y_i^n}(u^n|y^n) \frac{2^{-n(h(U)+\delta)} \cdot 2^{-n(h(Y)+\delta)}}{2^{-n(h(Y,U)+\delta)}} \\ &= f_{U^n|Y_i^n}(u^n|y^n) 2^{-n(I(Y;U)+3\delta)}, \end{aligned} \quad (58)$$

- (c) follows because $(1-\alpha\beta)^m \leq 1-\alpha+2^{-m\beta}$ [9] is applied,
- (d) holds since $\frac{1}{2} \log |\mathcal{S}| + \frac{1}{2} \log |\mathcal{J}| = I(Y;U) + 4\delta$.
- (e) follows by applying Property 2 of the modified ϵ -typical set [2].

For the second term, it follows that

$$\begin{aligned} \Pr\{\mathcal{E}_2 | \mathcal{E}_1^c\} \\ = \Pr\{(Z^n, U_i^n) \notin \mathcal{A}_\delta^{(n)}(ZU) | (Y_i^n, U_i^n) \in \mathcal{B}_\delta^{(n)}(YU)\} \\ \leq \Pr\{(Z^n, Y_i^n, U_i^n) \notin \mathcal{A}_\delta^{(n)}(ZYU) | (Y_i^n, U_i^n) \in \mathcal{B}_\delta^{(n)}(YU)\} \\ = \iint_{\mathcal{B}_\delta^{(n)}(YU)} f_{Y_i^n U_i^n}(y^n, u^n) \cdot \Pr\{Z^n \notin \mathcal{A}_\delta^{(n)}(Z|y^n, u^n) | (Y_i^n, U_i^n) = (y^n, u^n)\} d(y^n, u^n) \\ \stackrel{(f)}{\leq} \delta \iint_{\mathcal{B}_\delta^{(n)}(YU)} f_{Y_i^n U_i^n}(y^n, u^n) d(y^n, u^n) \\ \leq \delta, \end{aligned} \quad (59)$$

where (f) follows from the definition of the modified δ -typical set due to the Markov chain $Z - Y - U$.

Finally, the last term $\Pr\{\mathcal{E}_3 \cup \mathcal{E}_4\}$ can be bounded as

$$\begin{aligned}
& \Pr\{\mathcal{E}_3 \cup \mathcal{E}_4\} \\
&= \Pr\left[\bigcup_{i' \in \mathcal{I}, s' \in \mathcal{S}} (Z^n, U^n(s', J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU)\right] \\
&\leq \sum_{i'=1}^{|\mathcal{I}|} \sum_{s'=1}^{|\mathcal{S}|} \Pr\{(Z^n, U^n(s', J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU)\} \\
&\leq \sum_{i'=1}^{|\mathcal{I}|} \sum_{s'=1}^{|\mathcal{S}|} 2^{-n(I(Z;U)-\delta)} \\
&= |\mathcal{I} \times \mathcal{S}| \cdot 2^{-n(I(Z;U)-\delta)} \\
&\stackrel{(g)}{=} 2^{-n\delta}, \tag{60}
\end{aligned}$$

where (g) follows as $\frac{1}{n} \log M_I + \frac{1}{n} \log M_S = I(Z;U) - 2\delta$.

Consequently,

$$\Pr\{(\widehat{W}, \widehat{S}(\widehat{W})) \neq (W, S(W)) | W = i\} \leq 4\delta \tag{61}$$

for large enough n .

Before proceeding further, we introduce a lemma that is often used in the sequel. Again recall that the index pair $(J(i), S(i))$ determines the chosen sequence U_i^n directly and thus the following lemma can be thought of an extended version of [12, Lemma 4], incorporating continuous RVs.

Lemma 1. *It holds that*

$$\frac{1}{n} h(Y_i^n | S(i), J(i), \mathcal{C}_n) \leq h(Y|U) + \delta_n, \tag{62}$$

$$\frac{1}{n} h(Y_i^n | X_i^n, J(i), S(i), \mathcal{C}_n) \leq h(Y|X, U) + \delta_n, \tag{63}$$

where $\delta_n \downarrow 0$ as $\delta \downarrow 0$ and $n \rightarrow \infty$.

Proof: The tie between the modified δ -typical set $\mathcal{B}_\delta^{(n)}(\cdot)$ and the weakly δ -typical set $\mathcal{A}_\delta^{(n)}(\cdot)$ is helpful for proving the above lemma. We first prove (62).

Define an RV T as follows:

$$T = \begin{cases} 1 & \text{if } (Y_i^n, U_i^n) \in \mathcal{B}_\delta^{(n)}(YU), \\ 0 & \text{otherwise.} \end{cases} \tag{64}$$

In the analysis of the error probability, we have already demonstrated that $P_T(0) \leq 2\delta$, or $(Y_i^n, U_i^n) \in \mathcal{B}_\delta^{(n)}(YU)$

with high probability. From the left-hand side of (62),

$$\begin{aligned}
& h(Y_i^n | J(i), S(i), \mathcal{C}_n) \\
&\stackrel{(h)}{=} h(Y_i^n | U_i^n, J(i), S(i), \mathcal{C}_n) \\
&\stackrel{(i)}{\leq} h(Y_i^n | U_i^n) \leq h(Y_i^n, T | U_i^n) \\
&\leq H(T) + h(Y_i^n | U_i^n, T) \\
&= 1 + P_T(0)h(Y_i^n | U_i^n, T=0) \\
&\quad + P_T(1)h(Y_i^n | U_i^n, T=1) \\
&\stackrel{(j)}{\leq} n\epsilon_n + h(Y_i^n | U_i^n, T=1) \\
&= n\epsilon_n + \iint_{\mathcal{B}_\delta^{(n)}(YU)} f_{Y_i^n U_i^n}(y^n, u^n) \\
&\quad \cdot \log \frac{\Pr\{(Y_i^n, U_i^n) \in \mathcal{B}_\delta^{(n)}(YU)\}}{f_{Y_i^n | U_i^n}(y^n | u^n)} d(y^n, u^n) \\
&\stackrel{(k)}{\leq} n\epsilon_n + n(h(Y|U) + 2\delta) \\
&\quad \cdot \iint_{\mathcal{B}_\delta^{(n)}(YU)} f_{Y_i^n U_i^n}(y^n, u^n) d(y^n, u^n) \\
&\leq n(h(Y|U) + 2\delta + \epsilon_n), \tag{65}
\end{aligned}$$

where

- (h) follows as $(J(i), S(i))$ determines U_i^n ,
- (i) follows because conditioning reduces entropy,
- (j) follows as $h(Y_i^n | U_i^n, T=0) \leq h(Y_i^n) = \frac{n}{2} \log(2\pi e)$, and we define $\epsilon_n = \frac{1}{n} + \delta \log(2\pi e)$,
- (k) follows since $\Pr\{(Y_i^n, U_i^n) \in \mathcal{B}_\delta^{(n)}(YU)\} \leq 1$, and from Property 1 of the modified δ -typical set [2], we have that $f_{Y_i^n | U_i^n}(y^n | u^n) = \frac{f_{Y_i^n U_i^n}(y^n, u^n)}{f_{U_i^n}(u^n)} \geq \frac{2^{-n(h(Y,U)+\delta)}}{2^{-n(h(U)-\delta)}} = 2^{-n(h(Y|U)+2\delta)}$.

Therefore, from (65), we obtain that

$$\frac{1}{n} h(Y_i^n | J(i), S(i), \mathcal{C}_n) \leq h(Y|U) + \delta_n, \tag{66}$$

where $\delta_n = 2\delta + \epsilon_n$ and $\delta_n \downarrow 0$ as $n \rightarrow \infty$ and $\delta \downarrow 0$.

Next, we briefly summarize how to show (63). The left-hand side of (63) can be developed as $h(Y_i^n | X_i^n, J(i), S(i), \mathcal{C}_n) = h(Y_i^n | X_i^n, U_i^n, J(i), S(i), \mathcal{C}_n) \leq h(Y_i^n | X_i^n, U_i^n, \mathcal{C}_n)$, where the first equality and second inequality follow due to the same reasons of (h) and (i) in (65), respectively. By the definition of the modified δ -typical set [2], it can be concluded that $\Pr\{(X_i^n, Y_i^n, U_i^n) \in \mathcal{A}_\delta^{(n)}(XYU)\} \rightarrow 1$ as $n \rightarrow \infty$ (cf. (59)) due to the Markov chain $X - Y - U$ and $(Y_i^n, U_i^n) \in \mathcal{B}_\delta^{(n)}(YU)$ with high probability. This implies $\Pr\{(X_i^n, U_i^n) \in \mathcal{A}_\delta^{(n)}(XU)\} \rightarrow 1$ and $\Pr\{Y_i^n \in \mathcal{A}_\delta^{(n)}(Y|x^n, u^n) | (X_i^n, U_i^n) = (x^n, u^n)\} \rightarrow 1$ as $n \rightarrow \infty$ as well. Based on this observation, the rest of proof for (63) can be done similarly by the arguments seen in [12, Appendix C], and therefore the details are omitted.

Analysis of Identification and Storage Rates:

Equations (16) and (18) obviously hold from the parameter settings.

Analysis of Secrecy Rate:

$$\begin{aligned}
H(S(i)|\mathcal{C}_n) &= h(Y_i^n, J(i), S(i)|\mathcal{C}_n) - H(J(i)|S(i), \mathcal{C}_n) \\
&\quad - h(Y_i^n|J(i), S(i), \mathcal{C}_n) \\
&\stackrel{(l)}{\geq} h(Y_i^n) - H(J(i)|\mathcal{C}_n) \\
&\quad - h(Y_i^n|J(i), S(i), \mathcal{C}_n) \\
&\stackrel{(m)}{\geq} nh(Y) - n(I(Y;U) - I(Z;U) + R_I + 6\delta) \\
&\quad - n(h(Y|U) + \delta_n) \\
&= n(I(Z;U) - R_I - 6\delta - \delta_n) \\
&= n(R_S - 4\delta - \delta_n). \tag{67}
\end{aligned}$$

where

- (l) follows because $(J(i), S(i))$ is a function of Y_i^n ,
- (m) follows as $\frac{1}{n}H(J(i)|\mathcal{C}_n) \leq I(Y;U) - I(Z;U) + R_I + 6\delta$ and (63) is applied.

Thus,

$$\frac{1}{n}H(S(i)|\mathcal{C}_n) \geq R_S - 5\delta = \frac{1}{n} \log M_S - 5\delta \tag{68}$$

for large enough n .

Analysis of Secrecy-Leakage:

$$\begin{aligned}
I(S(i); J(i)|\mathcal{C}_n) &= H(S(i)|\mathcal{C}_n) + H(J(i)|\mathcal{C}_n) - h(Y_i^n, S(i), J(i)|\mathcal{C}_n) \\
&\quad + h(Y_i^n|S(i), J(i), \mathcal{C}_n) \\
&\stackrel{(n)}{\leq} n(I(Z;U) - R_I - 2\delta + I(Y;U) - I(Z;U) + R_I + 6\delta) \\
&\quad - nh(Y) + n(h(Y|U) + \delta_n) \\
&= n(4\delta + \delta_n), \tag{69}
\end{aligned}$$

where (n) follows because $\frac{1}{n}H(S(i)|\mathcal{C}_n) \leq I(Z;U) - R_I - 2\delta$, $\frac{1}{n}H(J(i)|\mathcal{C}_n) \leq I(Y;U) - I(Z;U) + R_I + 6\delta$, and (63) is applied. Hence,

$$\frac{1}{n}I(S(i); J(i)|\mathcal{C}_n) \leq 5\delta \tag{70}$$

for sufficiently large n .

Analysis of Privacy-Leakage Rate: From the left-hand side of (20), we have that

$$\begin{aligned}
I(X_i^n; J(i)|\mathcal{C}_n) &= H(J(i)|\mathcal{C}_n) - H(J(i)|X_i^n, \mathcal{C}_n) \\
&\leq n(I(Y;U) - I(Z;U) + R_I + 6\delta) - H(J(i)|X_i^n, \mathcal{C}_n) \\
&= n(h(U|Z) - h(U|Y) + R_I + 6\delta) - H(J(i)|X_i^n, \mathcal{C}_n). \tag{71}
\end{aligned}$$

The last term in (71) can be further evaluated as

$$\begin{aligned}
H(J(i)|X_i^n, \mathcal{C}_n) &= h(Y_i^n, J(i)|X_i^n, \mathcal{C}_n) - h(Y_i^n|X_i^n, J(i), \mathcal{C}_n) \\
&= h(Y_i^n|X_i^n, \mathcal{C}_n) - h(Y_i^n|X_i^n, J(i), S(i), \mathcal{C}_n) \\
&\quad - H(S(i)|J(i), X_i^n, \mathcal{C}_n) \\
&\stackrel{(o)}{=} nh(Y|X) - h(Y_i^n|X_i^n, J(i), S(i), \mathcal{C}_n) \\
&\quad - H(S(i)|J(i), X_i^n, Z^n, \mathcal{C}_n) \\
&\stackrel{(p)}{\geq} nh(Y|X) - h(Y_i^n|X_i^n, J(i), S(i), \mathcal{C}_n) \\
&\quad - H(S(i)|\mathbf{J}, Z^n, \mathcal{C}_n) \\
&\stackrel{(q)}{\geq} nh(Y|X) - h(Y_i^n|X_i^n, J(i), S(i), \mathcal{C}_n) - n\delta''_n \\
&\stackrel{(r)}{\geq} nh(Y|X) - n(h(Y|X, U) + \delta_n) - n\delta''_n \\
&= n(I(Y;U|X) - \delta_n - \delta''_n) \\
&= n(h(U|X) - h(U|Y) - \delta_n - \delta''_n) \tag{72}
\end{aligned}$$

where

- (o) follows since Y_i^n and X_i^n are independent of \mathcal{C}_n and the Markov chain $S(i) - (J(i), X_i^n) - Z^n$ holds,
- (p) follows because conditioning reduces entropy and $S(i) - (J(i), Z^n) - \mathbf{J} \setminus J(i)$ is applied,
- (q) follows by applying Fano's inequality, and $\delta''_n \downarrow 0$ as $\delta \downarrow 0$ and $n \rightarrow \infty$,
- (r) is due to (63).

From (71) and (72), we have that

$$\begin{aligned}
\frac{1}{n}I(X_i^n; J(i)|\mathcal{C}_n) &\leq h(U|Z) - h(U|X) + R_I + 6\delta + \delta_n + \delta''_n \\
&= I(X;U) - I(Z;U) + R_I + 6\delta + \delta_n + \delta''_n \\
&\leq R_L + \delta \tag{73}
\end{aligned}$$

for sufficiently large n .

Finally, by using the selection lemma [13, Lemma 2.2], there exists at least a good codebook satisfying all the conditions in Definition 2 for large enough n . \square

V. PROOF SKETCH OF THE REGION \mathcal{R}_C

In this section, we highlight the proof of the chosen-secret BIS model. Some parts follow from the arguments in Section IV, so we omit the similarities.

A. Converse Part

As seen in the converse proof of the generated-secret BIS model, we also consider the case in which W is uniformly distributed on \mathcal{I} . Suppose that a pair (R_I, R_S, R_J, R_L) is achievable.

For the analyses of identification, secrecy, and privacy-leakage rates, the reader should refer to the discussions around (35) and (37). We argue only the bound of R_J , which is different from the one seen in the generated-secret BIS model.

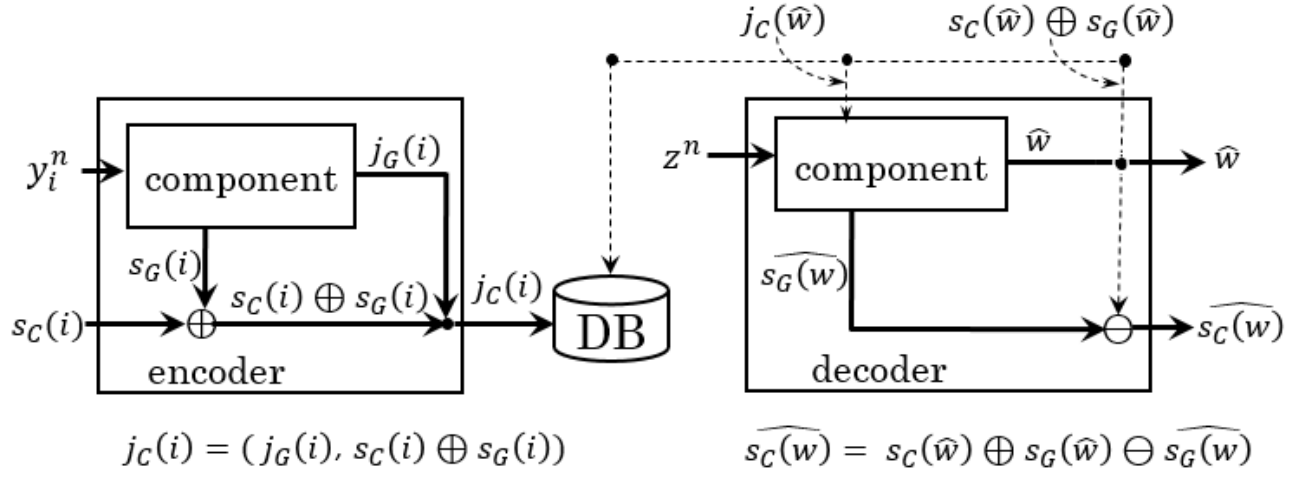


Fig. 7. Encoder and decoder of the chosen-secret BIS model

Analysis of Storage Rate:

$$\begin{aligned}
 n(R_J + \delta) &\geq \log M_J \geq \max_{w \in \mathcal{I}} H(w) \geq H(J(W)|W) \\
 &\stackrel{(a)}{=} I(Y_W^n, S(W); J(W)|W) \\
 &= h(Y_W^n, S(W)) - h(Y_W^n, S(W)|J(W)) \\
 &\stackrel{(b)}{=} h(Y_W^n) + H(S(W)) - H(S(W)|J(W)) \\
 &\quad - h(Y_W^n|J(W), S(W)) \\
 &\stackrel{(c)}{\geq} \frac{n}{2} \log(2\pi e) - \frac{n}{2} \log(2\pi e\alpha) \\
 &\geq \frac{n}{2} \log\left(\frac{1}{\alpha}\right), \tag{74}
 \end{aligned}$$

where

- (a) follows since $J(W)$ is a function of $(Y_W^n, S(W))$,
- (b) follows as $S(W)$ is chosen independently of Y_W^n ,
- (c) follows because conditioning reduces entropy and (44) is applied.

Then, we have that

$$R_J \geq \frac{1}{2} \log\left(\frac{1}{\alpha}\right) - \delta. \tag{75}$$

By letting $n \rightarrow \infty$ and $\delta \downarrow 0$, the capacity region of the chosen-secret BIS model is contained in the right-hand side of (22). \square

B. Achievability Part

In order to avoid confusion in the subsequent arguments, we define some new notations used only in this part. The pairs $(J_C(i), S_C(i))$ and $(J_G(i), S_G(i))$ denote the helper data and secret key of individual i for chosen- and generated-secret BIS models, respectively. Moreover, M_{J_C} and M_{J_G} denote the number of templates¹, and R_{J_G} and R_{J_C} denote the storage rates in the generated- and chosen-secret BIS models, respectively.

¹Normally, $J_C(i)$, $S_C(i)$, and M_{J_C} are denoted by $J(i)$, $S(i)$, and M_J in other sections of this paper.

Overviews:

The proof is an adapted version of the achievability proof of Section IV. The difference is that the encoder and decoder of the generated-secret BIS model are used as components inside the encoder and decoder of the chosen-secret BIS model as shown in Fig. 7. For encoding Y_i^n for each user $i \in \mathcal{I}$, the component encoder uses a masking layer (one-time pad operation) to mask $s_C(i)$ by using $s_G(i) \in \mathcal{S}$ as $s_C(i) \oplus s_G(i)$, where \oplus denotes the addition modulo M_S . The helper data $j_C(i)$ is the combined information of $j_G(i)$ and the masked data $s_C(i) \oplus s_G(i)$, i.e.,

$$j_C(i) = (j_G(i), s_C(i) \oplus s_G(i)). \tag{76}$$

For decoding the identified user w , it first uses the component decoder to estimate $(\widehat{w}, \widehat{s_G}(w))$ and then the secret key is retrieved by

$$\widehat{s_C}(w) = s_C(\widehat{w}) \oplus s_G(\widehat{w}) \ominus \widehat{s_G}(w), \tag{77}$$

where \ominus denotes the subtraction modulo M_S . This technique is also used in [2], [4], and [5].

Let $0 < \alpha \leq 1$. Fix a block length n and the joint pdf of (U, Y, X, Z) such that the Markov chain $U - Y - X - Z$ holds, where U is Gaussian with mean zero and variance $1 - \alpha$. The connection among the auxiliary RV U and (Y, X, Z) is exactly the same as the arguments around (48)–(51).

Now we fix $0 < R_I < I(Z; U)$, and

$$\begin{aligned}
 R_S &= I(Z; U) - R_I - 2\delta, \\
 R_{J_G} &= I(Y; U) - I(Z; U) + R_I + 6\delta, \\
 R_{J_C} &= I(Y; U) + 3\delta, \\
 R_L &= I(X; U) - I(Z; U) + R_I + 6\delta, \\
 M_I &= 2^{nR_I}, \quad M_S = 2^{nR_S}, \quad M_{J_G} = 2^{nR_{J_G}}, \tag{78}
 \end{aligned}$$

where $I(Y; U)$, $I(X; U)$, and $I(Z; U)$ are specified in (51).

Next we generate $2^{n(I(Y; U) + \delta)}$ sequences of $u^n(s, j)$, where each symbol of these sequences is i.i.d. Gaussian with mean zero and variance $1 - \alpha$, and $s \in \mathcal{S}$ and $j \in [1 : M_{J_G}]$.

Seeing y_i^n ($i \in \mathcal{I}$), the component encoder looks for $u^n(s, j)$ such that $(y_i^n, u^n(s, j)) \in \mathcal{B}_\delta^{(n)}(YU)$. If there are multiple pairs of such (s, j) , the encoder picks one at random. We denote the pair chosen by the component as $(s_G(i), j_G(i))$ and it is shared with the encoder. The encoder uses $s_G(i)$ to conceal the chosen secret key $s_C(i)$ by $s_C(i) \oplus s_G(i)$. This masked information is combined with $j_G(i)$ to form the helper data $j_C(i)$ as $j_C(i) = (j_G(i), s_C(i) \oplus s_G(i))$. If there does not exist such a pair, the component shares $(1, 1)$ with the encoder. In this case, the encoder declares error.

Observing z^n , the noisy version of x_w^n , the component decoder looks for $u^n(s, j(i))$ such that $(z^n, u^n(s, j(i))) \in \mathcal{A}_\delta^{(n)}(ZU)$ for all $i \in \mathcal{I}$ and some $s \in \mathcal{S}$. If a unique pair (i, s) is found, the component sets $(\widehat{w}, \widehat{s_G(w)}) = (i, s)$ and forwards this result to the decoder of the chosen-secret BIS model. The decoder detects $s_C(\widehat{w}) \oplus s_G(\widehat{w})$ from the public DB based on \widehat{w} , and outputs $\widehat{w} = i$ and $s_C(w) = s_C(\widehat{w}) \oplus s_G(\widehat{w}) \ominus s_G(w)$. In the final step, the estimated key $\widehat{s_C(w)}$ and $s_C(\widehat{w})$ in the key DB are compared, and if they are equal, the authentication is successful. If there is no such unique pair, the component shares $(1, 1)$ with the decoder and upon receiving these information, error is declared.

Analysis of Error Probability:

For individual $\widehat{W} = i$, the operation at the decoder (77) means that $\widehat{S_C(i)} = S_C(i)$ if and only if $\widehat{S_G(i)} = S_G(i)$. In (61), it was revealed that $\Pr\{(\widehat{W}, \widehat{S_G(W)}) \neq (W, S_G(W)) | W = i\} \leq 4\delta$. Therefore, the error probability of the chosen-secret BIS model can also be bounded by

$$\Pr\{(\widehat{W}, \widehat{S_C(W)}) \neq (W, S_C(W)) | W = i\} \leq 4\delta \quad (79)$$

for large enough n .

Analyses of Identification and Secrecy Rates:

Equations (16) and (17) are straightforward from the parameter settings.

Analysis of Storage Rate:

$$\begin{aligned} & \frac{1}{n} \log M_{J_C} \\ & \leq \frac{1}{n} \log M_{J_G} + \frac{1}{n} \log M_S \\ & = I(Y; U) - I(Z; U) + R_I + 6\delta + I(Z; U) - R_I - 2\delta \\ & = I(Y; U) + 4\delta = \frac{1}{2} \log \left(\frac{1}{\alpha} \right) + 4\delta \\ & = R_{J_C} + \delta. \end{aligned} \quad (80)$$

Analysis of Secrecy-Leakage: It holds that

$$\begin{aligned} & I(J_C(i); S_C(i) | \mathcal{C}_n) \\ & = I(J_G(i), S_C(i) \oplus S_G(i); S_C(i) | \mathcal{C}_n) \\ & = I(J_G(i); S_C(i) | \mathcal{C}_n) \\ & \quad + I(S_C(i) \oplus S_G(i); S_C(i) | J_G(i), \mathcal{C}_n) \\ & = I(J_G(i); S_C(i) | \mathcal{C}_n) + H(S_C(i) \oplus S_G(i) | J_G(i), \mathcal{C}_n) \\ & \quad - H(S_C(i) \oplus S_G(i) | J_G(i), S_C(i), \mathcal{C}_n) \\ & \leq I(J_G(i); S_C(i) | \mathcal{C}_n) + \log M_S \\ & \quad - H(S_G(i) | J_G(i), S_C(i), \mathcal{C}_n) \\ & \stackrel{(a)}{=} \log M_S - H(S_G(i) | J_G(i), \mathcal{C}_n) \\ & = I(J_G(i); S_G(i) | \mathcal{C}_n) + \log M_S - H(S_G(i) | \mathcal{C}_n), \end{aligned} \quad (81)$$

where (a) holds because $S_C(i)$ is chosen independently of $(S_G(i), J_G(i))$ for given \mathcal{C}_n . In (68) and (70) of Section IV, it was clarified that

$$H(S_G(i) | \mathcal{C}_n) \geq \log M_S - 5n\delta, \quad (82)$$

$$I(J_G(i); S_G(i) | \mathcal{C}_n) \leq 5n\delta \quad (83)$$

for large enough n . Substituting (82) and (83) into (81), the secrecy-leakage of the chosen-secret BIS model is bounded by

$$\frac{1}{n} I(J_C(i); S_C(i) | \mathcal{C}_n) \leq 10\delta \quad (84)$$

for large enough n .

Analysis of Privacy-Leakage Rate:

It can be proved that

$$I(X_i^n; J_C(i) | \mathcal{C}_n) = I(X_i^n; J_G(i) | \mathcal{C}_n). \quad (85)$$

To verify this, first one can easily see that

$$\begin{aligned} I(X_i^n; J_C(i) | \mathcal{C}_n) & = I(X_i^n; J_G(i), S_C(i) \oplus S_G(i) | \mathcal{C}_n) \\ & \geq I(X_i^n; J_G(i) | \mathcal{C}_n). \end{aligned} \quad (86)$$

Meanwhile, it can be shown that

$$\begin{aligned} & I(X_i^n; J_C(i) | \mathcal{C}_n) \\ & = I(X_i^n; J_G(i), S_C(i) \oplus S_G(i) | \mathcal{C}_n) \\ & = I(X_i^n; J_G(i) | \mathcal{C}_n) + I(X_i^n; S_C(i) \oplus S_G(i) | J_G(i), \mathcal{C}_n) \\ & = I(X_i^n; J_G(i) | \mathcal{C}_n) + H(S_C(i) \oplus S_G(i) | J_G(i), \mathcal{C}_n) \\ & \quad - H(S_C(i) \oplus S_G(i) | X_i^n, J_G(i), \mathcal{C}_n) \\ & \stackrel{(b)}{\leq} I(X_i^n; J_G(i) | \mathcal{C}_n) + \log M_S \\ & \quad - H(S_C(i) \oplus S_G(i) | X_i^n, J_G(i), S_G(i), \mathcal{C}_n) \\ & = I(X_i^n; J_G(i) | \mathcal{C}_n) + \log M_S \\ & \quad - H(S_C(i) | X_i^n, J_G(i), S_G(i), \mathcal{C}_n) \\ & \stackrel{(c)}{=} I(X_i^n; J_G(i) | \mathcal{C}_n) + \log M_S - \log M_S \\ & = I(X_i^n; J_G(i) | \mathcal{C}_n), \end{aligned} \quad (87)$$

where

(b) follows as conditioning reduces entropy,

(c) follows because $S_C(i)$ is chosen uniformly from \mathcal{S} and independent of other RVs.

From (86) and (87), (85) clearly holds. By invoking the result of (73), the privacy-leakage rate can also be made that

$$\frac{1}{n}I(X_i^n; J_C(i)|\mathcal{C}_n) \leq R_L + \delta \quad (88)$$

for large enough n .

Finally, by using the selection lemma [13, Lemma 2.2], there is at least one good codebook satisfying all the conditions in Definition 3 for large enough n . \square

VI. CONCLUSION AND FUTURE WORK

We characterized the capacity region of identification, secrecy, storage, and privacy-leakage rates for both generated- and chosen-secret BIS models under Gaussian sources. The models considered in this study are the RSM, namely, the enrollment channel is noisy. We showed that an idea for deriving the capacity regions is to convert the system to another one where the data flows of each user are in one-way direction. We also gave numerical computations of three different examples for the derived regions and from these results, it appeared that achieving high secrecy and small privacy-leakage rates simultaneously is unlikely manageable. For future work, we plan to extend this scenario to consider Gaussian vector sources and channels.

REFERENCES

- [1] F. Willems, T. Kalker, S. Baggen, and J. P. Linnartz, "On the capacity of a biometric identification system," in *Proc. IEEE Int. Symp. Inf. Theory*, Yokohama, Japan, p.82, Jun./Jul. 2003.
- [2] T. Ignatenko and F. Willems, "Fundamental limits for privacy-preserving biometric identification system that support authentication," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp.5583–5594, Oct. 2015.
- [3] 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, Nov. 2016.
- [4] 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, Nov. 2018.
- [5] V. Yachongka and H. Yagi, "A new characterization of the capacity region of identification systems under noisy enrollment," *54th Annu. Conf. Inf. Sci. Syst.*, Princeton, NJ, Mar. 2020.
- [6] F.M.J. Willems, T. Ignatenko, "Quantization effects in biometric systems," in *Proc. Inf. Theory and Appl. Workshop*, San Diego, CA, pp. 372–379, Feb. 2009.
- [7] M. T. Vu, T. J. Oechtering, and M. Skoglund, "Gaussian hierarchical identification with pre-processing," in *Proc. IEEE Data Compression Conf.*, Snowbird, UT, USA, pp. 277–286, Mar. 2018.
- [8] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 623–656, Oct. 1948.
- [9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed., John Wiley & Sons, New Jersey, 2006.
- [10] P. Bergmans, "A simple converse for broadcast channels with additive white Gaussian noise (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 20, no. 2, pp. 279–280, Mar. 1974.
- [11] Y. Oohama, "Gaussian multiterminal source coding," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1912–1923, Nov. 1997.
- [12] K. Kittichokechai, T. J. Oechtering, M. Skoglund, and Y.-K. Chia, "Secure source coding with action-dependent side information," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6444–6464, Dec. 2015.
- [13] M. Bloch and J. Barros, *Physical-Layer Security*, Cambridge, U.K.: Cambridge Univ. Press, 2011.