entropy

MDPI

Article

Biometric Identification Systems with Noisy Enrollment for Gaussian Sources and Channels †

Vamoua Yachongka [1,*], Hideki Yagi [2] and Yasutada Oohama [2]

[1] Advanced Wireless & Communication Research Center (AWCC), The University of Electro-Communications, 1-5-1 Chofugaoka, Tokyo 182-8585, Japan

[2] Department of Computer and Network Engineering, The University of Electro-Communications, 1-5-1 Chofugaoka, Tokyo 182-8585, Japan; h.yagi@uec.ac.jp (H.Y.); oohama@uec.ac.jp (Y.O.)

* Correspondence: va.yachongka@uec.ac.jp; Tel.: +81-42-443-5366

† A part of this paper was presented at the 2020 IEEE Information Theory Workshop, 11–15 April 2021. Available online: https://itw2020.it/ (accessed on 16 May 2020). The new contributions are that we provide a complete proof of Theorem 1, show that the characterized regions are convex, and add numerical calculations of the capacity regions.

Abstract: In the present paper, we investigate the fundamental trade-off of identification, secret-key, storage, and privacy-leakage rates in biometric identification systems for remote or hidden Gaussian sources. We use a technique of converting the system to one where the data flow is in one-way direction to derive the capacity region of these rates. Also, we provide numerical calculations of three different examples for the system. The numerical results imply that it seems hard to achieve both high secret-key and small privacy-leakage rates simultaneously.

Keywords: biometric identification system; noisy enrollment; privacy-leakage; entropy power inequality

check for updates

Citation: Yachongka, V.; Yagi, H.; Oohama, Y. Biometric Identification Systems with Noisy Enrollment for Gaussian Sources and Channels. *Entropy* **2021**, *23*, 1049. https://doi.org/10.3390/e23081049

Academic Editor: Boris Ryabko

Received: 30 June 2021
Accepted: 10 August 2021
Published: 15 August 2021

1. Introduction

Biometric identification indicates an automated process of recognizing an individual by matching the individual's biological data (bio-data) with the digital files stored in the system database [1]. Some unique bio-data that can be used for biometric identification include fingerprint, iris, face, voice, palm, and so on [2]. Compared to the traditional method such as password or smart card based identification, it provides higher convenience and security. However, the critical drawback for biometric identification is that the usable sources are limited [3], for instance, human has only two eyes and if their information are leaked, there is no alternative option to replace, and therefore it is important to protect users' privacy. Furthermore, the size of the storage should be minimized to reduce the memory space of the database [4], especially when the number of users becomes large.

From an information theoretic point of view, there are two major settings of the studies related to biometric identification systems (BISs), namely, the BIS with exponentially many users and the system with one user. The difference of these systems is that in the former setting, we are interested in finding the maximum number of users who are reliably identifiable, i.e., the maximum achievable identification rate at which the error probability of the BIS vanishes (the identification capacity). However, in the latter setting, the estimation of the user need not be considered since there exists only one user and it becomes redundant. For discrete memoryless sources (DMSs), the fundamental performance of the BIS was widely analyzed for both scenarios.

The BIS with multiple users was initially treated as a mathematical model in the seminal work [5], and the identification capacity of the BIS was clarified. In the model, it is assumed that every biometric identifier is enrolled via a noisy channel, and this type of model is known as a remote or hidden source model. The term the remote sources were used in [6,7], and hidden source model (HSM) is from [8]. In this paper, we use HSM as in [8] to represent the BIS with noisy enrollment. The encoding process was introduced in [9] to reduce the size of the storage. This work was extended to incorporate noisy reconstruction in [10]. The BIS with estimating both user's index and secret key for two classical models, namely, *generated-* and *chosen-secret* BIS models, was investigated in [11]. In this literature, a clear explanation of the difference of these models is given. Later, adopting the concept of the wiretap channel to assume that the adversary has side information of the identified user's bio-data sequence for the generated-secret BIS model was analyzed in [12]. Recently, a storage constraint and an HSM added to the model of [11] were studied in [13,14]. By using an additional private key, user's privacy-leakage can be made negligible [15,16]. Another scenario, that is, the BIS with one user, was extensively examined in [8,17–22]. More precisely, in [17,18], the relation of secret-key and privacy-leakage rates was analyzed. The optimal secret-key rate under privacy and storage constraints was characterized in [8,19] for non-vanishing and vanishing secrecy-leakage rate, respectively. It is worthwhile noting that in [8], a successful attempt for characterizing the capacity region of the BIS with one user for HSM was first made. The works of [8] was extended to constrain the action cost for the decoder in [20], and to consider two-enrollment systems for the same hidden source, where the encoders do not trust each other [21]. Moreover, in [22], the secret-key capacity of a multi-enrollment system, in which the decoder is required to estimate all secret keys generated in the earlier enrollments, was formulated.

Compared to the analyses of the BIS for DMSs, the results given under Gaussian sources are still few. For example, the optimal trade-off between secret-key and privacy-leakage rates was characterized in [23] and in order to speed up search complexity, hierarchical identification was taken into account in [24]. A common assumption in [23,24] is that the enrollment channel is noiseless, known as a visible source model (VSM). However, in real-life application, the signal of bio-data is basically represented with continuous values, and most communication links can be modeled as Gaussian channels [23]. What is more, the HSM is considered to be more realistic, e.g., captured picture of a finger via a scanner, and when the BIS is switched from the VSM to the HSM, the evaluation becomes more challenging [8] because many techniques used for deriving the results of the VSM are not directly applicable. These facts motivate us to extend the models in [13] to Gaussian sources and channels. Note that from the technical perspectives, this extension is not trivial since the technique for establishing Theorems 1 and 2 in [13] massively depends on the property that the alphabet sizes are finite, but unfortunately it cannot be applied to continuous sources. The technique used in this paper will be explained in Section 5 in details. Therefore, the extension is of both theoretical and practical interest. Although it is well-known that the bio-data is real-valued, as mentioned in [23], the validity of Gaussian assumption is not discussed in this paper and we leave this for further research. Here, we are interested in specifying the optimal trade-off of the BIS.

In this study, our goal is to find the optimal trade-off of identification and secret-key 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, 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 entropy power inequality (EPI) [25] doubly in two opposite directions, and also its property facilitates the derivation of the inner bound. In [8], Mrs. Gerber's lemma was applied twice, too, to simplify the rate region of the HSM for binary sources and symmetric channels 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 secret-key and small privacy-leakage rates at the same time. To achieve a small privacy-leakage rate, the secret-key rate must be sacrificed. Furthermore, as a by-product of our result, the capacity regions of the BIS analyzed in [8] for Gaussian sources and channels are obtained, and as special cases, it can be checked that this characterization reduces to the results given in [5,23].

The rest of this paper is organized as follows. In Section 2, we define the notation used in this paper, and describe our system model and the converted system. In Section 3, the formal definitions and main results are discussed in detail. We continue investigating the basic properties of the capacity regions, and provide there different examples in Section 4. The overviews of the proof of our main results are given in Section 5. The full proof is available in Appendices A and B. Finally, some concluding remark and future work are mentioned in Section 6.

2. System Model and Converted System

2.1. Notation and System Model

Upper-case A and lower-case a denote random variable (RV) and its realization, respectively. $A^n = (A_1, \cdots, A_n)$ represents a string of RVs and subscripts represent the position of an 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 $\{k, k+1, \cdots, t\}$. $\log x$ stands for the natural logarithm of $x > 0$.

The generated-secret BIS model and chosen-secret BIS model considered in this study are depicted in Figure 1. Arrows (g) and (c) indicate the directions of the secret key of the former and latter models. Let $\mathcal{I} = [1 : M_I]$, $\mathcal{S} = [1 : M_S]$, and $\mathcal{J} = [1 : M_J]$ be the sets of user's indices, secret keys, and helper data, respectively, where M_I, M_S, and M_J denote the numbers of users, 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 $X_{ik} \sim \mathcal{N}(0, 1)$, where $\mathcal{N}(0, 1)$ is a Gaussian RV with mean zero and variance one. Note that an RV with unit variance can be obtained by applying a scaling technique. $P_{Y|X}$ and $P_{Z|X}$ are additive Gaussian noise channels modeled as follows:

$$Y_{ik} = \rho_1 X_{ik} + N_1, \quad Z_k = \rho_2 X_{ik} + N_2, \qquad (k \in [1 : n]). \tag{1}$$

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 (1), Y_{ik} and Z_k are also 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

$$f_{X_i^n Y_i^n Z^n}(x_i^n, y_i^n, z^n) = \textstyle\prod_{k=1}^n f_{XYZ}(x_{ik}, y_{ik}, z_k), \tag{2}$$

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

$$f_{XYZ}(x, y, z) = f_X(x) \cdot f_{Y|X}(y|x) \cdot f_{Z|X}(z|x), \tag{3}$$

$$= \frac{1}{\sqrt{(2\pi)^3(1-\rho_1^2)(1-\rho_2^2)}} \exp\left(-\left(\frac{x^2}{2} + \frac{(y-\rho_1 x)^2}{2(1-\rho_1^2)} + \frac{(z-\rho_2 x)^2}{2(1-\rho_2^2)}\right)\right). \tag{4}$$

In the generated-secret BIS model, upon observing Y_i^n, the encoder $e(\cdot)$ generates secret key $S(i) \in \mathcal{S}$ and helper data $J(i) \in \mathcal{J}$ as $(S(i), J(i)) = e(Y_i^n)$. Then, $J(i)$ is stored at position i in the public database (helper DB) and $S(i)$ is saved in the key DB, which is installed in a secure location. Let W and $\widehat{W}$ denote the index of the identified user and its estimated value, respectively. Seeing Z^n, the decoder $d(\cdot)$ estimates $(\widehat{W}, \widehat{S(W)})$ from Z^n and all helper data in DB $\boldsymbol{J} \equiv \{J(1), \cdots, J(M_I)\}$, i.e., $(\widehat{W}, \widehat{S(W)}) = d(Z^n, \boldsymbol{J})$.

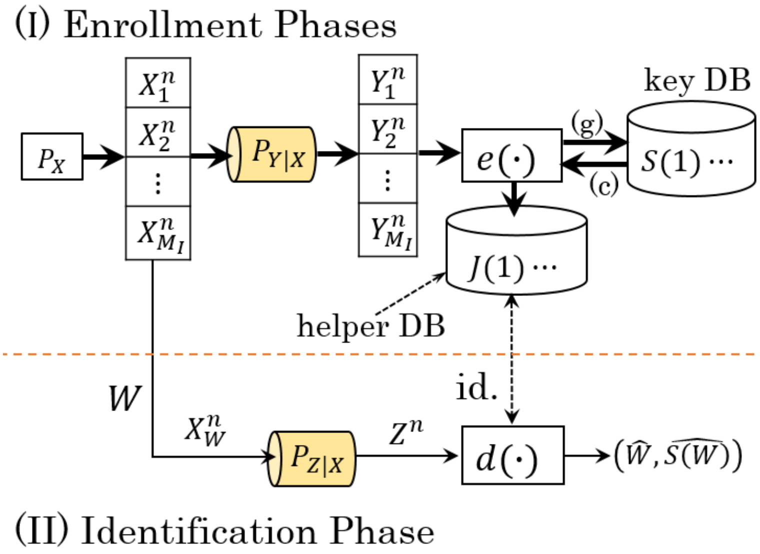

Figure 1. The generated- and chosen-secret BIS models.

In the chosen-secret BIS model, the secret key $S(i)$ is chosen uniformly from $\mathcal{S}$, i.e.,

$$P_{S(i)}(s) = 1/M_S \qquad (s \in \mathcal{S}), \tag{5}$$

and independent of other RVs. The encoder forms the helper data as $J(i) = e(Y_i^n, S(i))$ for every individual. The decoder $d(\cdot)$ owns the same functionality as in the generated-secret BIS model.

2.2. Converted System

The original system, having X as input source and Y, Z as outputs, is in the top figure in Figure 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 (1) produces only a lower bound. (II) It seems difficult to prove the achievability part by generating the codebook via a test channel due to the input X. To overcome these bottlenecks, we use 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 Figure 2, where Y becomes input virtually. To achieve this objective, knowing the statistics 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.

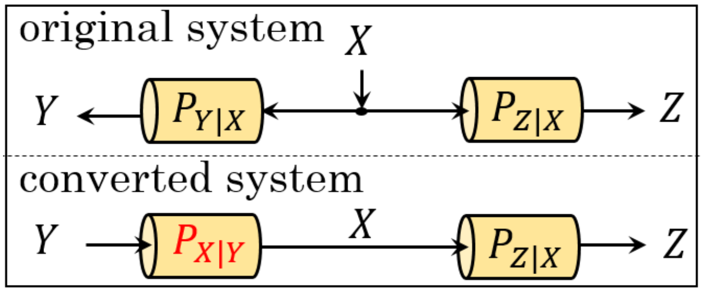

Figure 2. The original (**top**) and converted (**bottom**) systems

Due to the Markov chain $Y - X - Z$, Equation (3) can also be expanded in the following form.

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

Observe that

$$\frac{x^2}{2} + \frac{(y-\rho_1 x)^2}{2(1-\rho_1^2)} = \frac{x^2}{2} + \frac{y^2}{2(1-\rho_1^2)} - \frac{\rho_1 xy}{1-\rho_1^2} + \frac{(\rho_1 x)^2}{2(1-\rho_1^2)} = \frac{y^2}{2} + \frac{(x-\rho_1 y)^2}{2(1-\rho_1^2)}. \tag{7}$$

Without loss of generality, the exponential part in (4) can be rearranged as

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

From (6) and (8), we may conclude that the following relations hold with some RV $N_1' \sim \mathcal{N}(0, 1-\rho_1^2)$.

$$X_{ik} = \rho_1 Y_{ik} + N_1', \tag{9}$$

$$Z_k = \rho_2 X_{ik} + N_2 = \rho_1\rho_2 Y_{ik} + \rho_2 N_1' + N_2. \tag{10}$$

Equations (9) and (10) describe the outputs of the backward channel $P_{X|Y}$ and the combined channel $P_{Z|Y}$ of the virtual system. Actually, these relations can also be observed directly from the covariance matrix of RVs (X, Y, Z). However, we derive them based on the joint pdf for general readers' purpose. Moreover, this transformation is useful for the analysis of a non-standard source. The above relations play key roles for solving the problem of the HSM, and we use them in many steps during the analysis in this paper. In [23,24], the concept of this transformation is not seen because the enrollment channel is noiseless due to the assumption of VSM as mentioned before.

Remark 1. *In the case where there is no operation of scaling, Equations (9) and (10) are settled as follows. Suppose that $X_{ik} \sim \mathcal{N}(0,\sigma_x^2)$ with $\sigma_x^2 < \infty$, $Y_{ik} = X_{ik} + D_1$, 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 each other and other RVs. By applying the similar arguments around (6)–(8), we obtain that*

$$X_{ik} = \frac{\sigma_x^2}{\sigma_x^2+\sigma_1^2} Y_{ik} + D_1', \quad Z_k = X_{ik} + N_2' = \frac{\sigma_x^2}{\sigma_x^2+\sigma_1^2} Y_{ik} + D_1' + D_2, \tag{11}$$

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 paper can also be characterized via (11), and the results for this case will be mentioned in Remark 3. However, equation developments need more space and do 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 verify that

$$I(X;Y) = \frac{1}{2}\log\left(\frac{1}{1-\rho_1^2}\right), \quad I(Z;Y) = \frac{1}{2}\log\left(\frac{1}{1-\rho_1^2\rho_2^2}\right), \tag{12}$$

where the right equation in (12) is attained because the variance of the noise term $\rho_2 N_1' + N_2$ in (10) is equal to $1-\rho_1^2\rho_2^2$.

3. Problem Formulation and Main Results

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

Definition 1. *A tuple of identification, secret-key, public storage, and privacy-leakage rates (R_I, R_S, R_J, R_L) is said to be achievable for the generated-secret BIS model under a Gaussian source if for any $\delta > 0$ and large enough n there exist pairs of encoders and decoders satisfying*

$$\max_{i\in\mathcal{I}} \Pr\{(\widehat{W},\widehat{S(W)}) \neq (W,S(W))|W=i\} \leq \delta, \qquad \text{(error probability)} \tag{13}$$
$$\tfrac{1}{n}\log M_I \geq R_I - \delta, \qquad \text{(identification rate)} \tag{14}$$
$$\min_{i\in\mathcal{I}} \tfrac{1}{n}H(S(i)) \geq R_S - \delta, \qquad \text{(secret-key rate)} \tag{15}$$
$$\tfrac{1}{n}\log M_J \leq R_J + \delta, \qquad \text{(public storage rate)} \tag{16}$$
$$\max_{i\in\mathcal{I}} \tfrac{1}{n}I(S(i);J(i)) \leq \delta, \qquad \text{(secrecy-leakage rate)} \tag{17}$$
$$\max_{i\in\mathcal{I}} \tfrac{1}{n}I(X_i^n;J(i)) \leq R_L + \delta. \qquad \text{(privacy-leakage rate)} \tag{18}$$

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

For the chosen-secret BIS model, the definition is provided as follows:

Definition 2. *A tuple (R_I, R_S, R_J, R_L) is said to be achievable for the chosen-secret BIS model under a Gaussian source if there exist pairs of encoders and decoders that satisfy all the requirements in Definition 1 for any $\delta > 0$ and large enough n. Note that the left-hand side of (15) is expressed as $\frac{1}{n}\log M_S$ because the key is chosen uniformly from $\mathcal{S}$ (cf. (5)). In addition, $\mathcal{R}_C$ is defined as the capacity region for the chosen-secret BIS model.*

Remark 2. *Note that in the BIS, there are two databases, namely, databases of secret keys and helper data. The memory space of the database for storing the helper data (public database) is minimized, while that for the secret keys (secure database) should be maximized. This means only a part of the entire storage space of the BIS, which is the public database, is being compressed, and thus it is suitable to call this compression rate the public storage rate. However, we call the public storage rate just the storage rate as in [8] hereafter for brevity reason.*

Now we are ready to introduce our main results.

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

$$\begin{aligned}\mathcal{R}_G = \bigcup_{0<\alpha\leq 1}\Big\{(R_I,R_S,R_J,R_L) : R_I + R_S &\leq \frac{1}{2}\log\left(\frac{1}{\alpha\rho_1^2\rho_2^2 + 1 - \rho_1^2\rho_2^2}\right),\\ R_J &\geq \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2 + 1 - \rho_1^2\rho_2^2}{\alpha}\right) + R_I,\\ R_L &\geq \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2 + 1 - \rho_1^2\rho_2^2}{\alpha\rho_1^2 + 1 - \rho_1^2}\right) + R_I,\\ R_I &\geq 0,\ \ R_S \geq 0\Big\},\end{aligned} \tag{19}$$

$$\begin{aligned}\mathcal{R}_C = \bigcup_{0<\alpha\leq 1}\Big\{(R_I,R_S,R_J,R_L) : R_I + R_S &\leq \frac{1}{2}\log\left(\frac{1}{\alpha\rho_1^2\rho_2^2 + 1 - \rho_1^2\rho_2^2}\right),\\ R_J &\geq \frac{1}{2}\log\left(\frac{1}{\alpha}\right),\\ R_L &\geq \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2 + 1 - \rho_1^2\rho_2^2}{\alpha\rho_1^2 + 1 - \rho_1^2}\right) + R_I,\\ R_I &\geq 0,\ \ R_S \geq 0\Big\}.\end{aligned} \tag{20}$$

The proof of Theorem 1 is provided in Appendices A and B. It can be verified that the regions $\mathcal{R}_G$ and $\mathcal{R}_C$ are both convex, whose proofs are available in Appendix C. Unlike the approach taken in [23], based on investigating the second derivative of the rate region function, our proof makes use of the concavity of the logarithmic function. In both regions, $\alpha = 0$ is excluded by the reason that the point is not achievable, and this fact will be mentioned again in the converse proof of Equation (19).

For a fixed α, the optimal rate values for the regions $\mathcal{R}_G$ and $\mathcal{R}_C$ are shown in Figure 3. We begin with explaining Figure 3a. Suppose that $0 < R_I < \frac{1}{2}\log\left(\frac{1}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}\right)$. In the top band chart, $\frac{1}{2}\log\left(\frac{1}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}\right)$ is the maximum achievable rate that user's identities can be estimated correctly at the decoder. Since the index and the secret key of the identified user are reconstructed at the decoder, the sum of the optimal values for the identification and secret-key rates is equal to this value, implying the optimal secret-key rate is $R_S = \frac{1}{2}\log\left(\frac{1}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}\right) - R_I$. One can see that these rates are in a trade-off relation as the identification rate rises, the secret-key rate falls off. In the bottom one, $\frac{1}{2}\log\left(\frac{1}{\alpha}\right)$ is the entire rate that we need to generate auxiliary random sequences for encoding. The first part (blue part) represents the secret-key rate, and the second half $\left(\frac{1}{2}\log\left(\frac{1}{\alpha}\right) - R_S = \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{\alpha}\right) + R_I\right)$ is the rate of the sequences that are shared between the encoder and decoder to help estimation of the index and secret key, corresponding the storage rate. Storing the helper data at this rate results in leaking the user's privacy at least $\frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{\alpha\rho_1^2+1-\rho_1^2}\right) + R_I$, which is the optimal or minimum privacy-leakage for a given α.

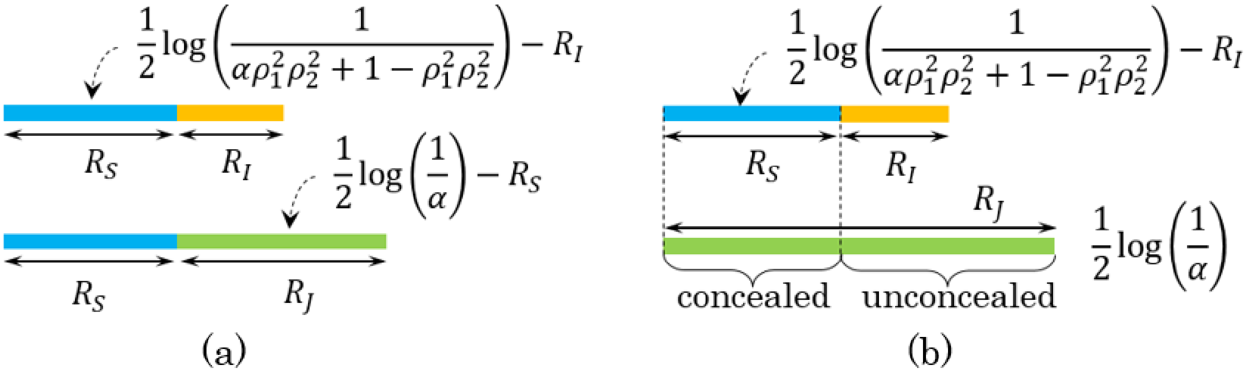
$\frac{1}{2}\log\left(\frac{1}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}\right)-R_I$
R_S
R_I
$\frac{1}{2}\log\left(\frac{1}{\alpha}\right)-R_S$
R_S
R_J
(a)
$\frac{1}{2}\log\left(\frac{1}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}\right)-R_I$
R_S
R_I
R_J
$\frac{1}{2}\log\left(\frac{1}{\alpha}\right)$
concealed
unconcealed
(b)

Figure 3. (**a**,**b**) are the explanations of the optimal values of identification, secret-key, storage, and privacy-leakage rates in the regions $\mathcal{R}_G$ and $\mathcal{R}_C$, respectively, for a fixed α.

For Figure 3b (the chosen-secret BIS model), the relation of the identification and secret-key rates is the same as in the generated-secret BIS model. However, the optimal storage rate becomes larger than the one seen in Figure 3a, equal to $\frac{1}{2}\log\left(\frac{1}{\alpha}\right)$ (the bottom band chart of Figure 3b), as the information related to the secret key chosen at the encoder (the concealed part) must be saved together with the helper data in DB to help the estimation of the key. For the privacy-leakage rate, the minimum values are not distinct in both models. This is because the unconcealed part of the storage at rate $\frac{1}{2}\log\left(\frac{1}{\alpha}\right) - R_S = \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{\alpha}\right) + R_I$, identical to the optimal storage rate of the generated-secret BIS model, is still exposed publicly, and thus the minimum privacy-leakage rates of the two models are the same.

Figure 4 shows a numerical example of the region $\mathcal{R}_G$ for $\rho_1^2 = 3/4$ and $\rho_2^2 = 2/3$. More specially, Figure 4a is a projection of the capacity region to the three-dimensional Euclidean space with X-axis R_J, Y-axis R_S, and Z-axis R_I. The black thick arrow indicates the direction of the achievable region for all rate tuples (R_J, R_S, R_I). Figure 4b is another projection of the capacity region to $R_J R_I$-plane. Red asterisks and circles correspond to the rate points (R_J, R_I) at which R_I is zero and R_I is optimal, respectively, for some $\alpha \in (0, 1]$. To explain the relation of the identification and storage rates, let us focus on the rightmost asterisk and circle pair in Figure 4b. When identification rate varies from zero to the optimal value, the rate point (R_J, R_I) moves from the asterisk point (in the bottom) to the circled point along the arrow. From this, it is clear that the value of the storage rate for the circled point is greater compared to the asterisk point, implying that the change of identification rate affects the storage rate.

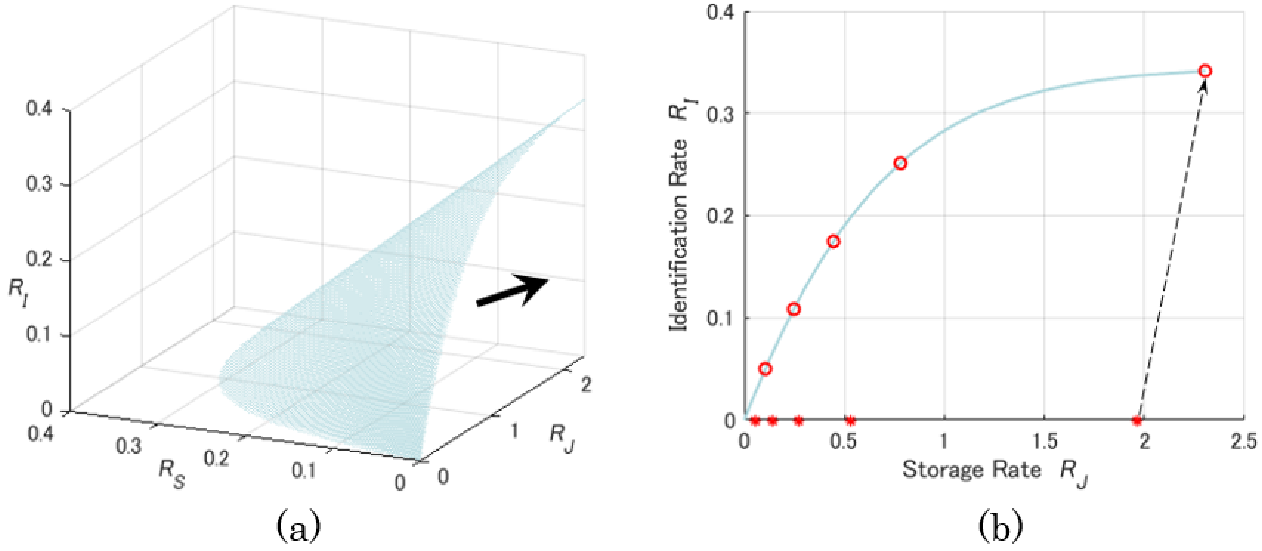

Figure 4. Projections of the capacity region $\mathcal{R}_G$ onto (**a**) $R_J R_S R_I$-space and (**b**) $R_J R_I$-plane.

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

Corollary 1. *The capacity regions of the generated- and chosen-secret BIS models with a single user (the models considered in* [8]*) for Gaussian sources are given by substituting $R_I = 0$ into the right-hand sides of* (19) *and* (20)*, respectively.*

Remark 3. *Let $\mathcal{R}'_G$ and $\mathcal{R}'_C$ denote the capacity regions of the generated-secret and chosen-secret BIS models characterized via* (11) *in Remark* 1*. The two regions are provided below.*

$$\begin{aligned}\mathcal{R}'_G = \bigcup_{0<\alpha\leq 1} \Big\{(R_I, R_S, R_J, R_L) : R_I + R_S &\leq \frac{1}{2}\log\left(\frac{(\sigma_x^2+\sigma_1^2)(\sigma_x^2+\sigma_2^2)}{\alpha\sigma_x^4+\sigma_x^2\sigma_1^2+\sigma_1^2\sigma_2^2+\sigma_2^2\sigma_x^2}\right), \\ R_J &\geq \frac{1}{2}\log\left(\frac{\alpha\sigma_x^4+\sigma_x^2\sigma_1^2+\sigma_1^2\sigma_2^2+\sigma_2^2\sigma_x^2}{\alpha(\sigma_x^2+\sigma_1^2)(\sigma_x^2+\sigma_2^2)}\right)+R_I, \\ R_L &\geq \frac{1}{2}\log\left(\frac{\alpha\sigma_x^4+\sigma_x^2\sigma_1^2+\sigma_1^2\sigma_2^2+\sigma_2^2\sigma_x^2}{(\alpha\sigma_x^2+\sigma_1^2)(\sigma_x^2+\sigma_2^2)}\right)+R_I, \\ R_I &\geq 0,\ \ R_S \geq 0\Big\}, \qquad (21)\end{aligned}$$

$$\begin{aligned}\mathcal{R}'_C = \bigcup_{0<\alpha\leq 1} \Big\{(R_I, R_S, R_J, R_L) : R_I + R_S &\leq \frac{1}{2}\log\left(\frac{(\sigma_x^2+\sigma_1^2)(\sigma_x^2+\sigma_2^2)}{\alpha\sigma_x^4+\sigma_x^2\sigma_1^2+\sigma_1^2\sigma_2^2+\sigma_2^2\sigma_x^2}\right), \\ R_J &\geq \frac{1}{2}\log\left(\frac{1}{\alpha}\right), \\ R_L &\geq \frac{1}{2}\log\left(\frac{\alpha\sigma_x^4+\sigma_x^2\sigma_1^2+\sigma_1^2\sigma_2^2+\sigma_2^2\sigma_x^2}{(\alpha\sigma_x^2+\sigma_1^2)(\sigma_x^2+\sigma_2^2)}\right)+R_I, \\ R_I &\geq 0,\ \ R_S \geq 0\Big\}. \qquad (22)\end{aligned}$$

It can be verified that $\mathcal{R}_G$ and $\mathcal{R}_C$ are equivalent to $\mathcal{R}'_G$ and $\mathcal{R}'_C$, respectively, if one sets $\rho_1^2 = \sigma_x^2/(\sigma_x^2+\sigma_1^2)$ and $\rho_2^2 = \sigma_x^2/(\sigma_x^2+\sigma_2^2)$, respectively. In addition, as a connection to the result in a previous study, when there is no secret-key generation or provision ($R_S = 0$), and R_J, R_L are large enough ($R_J, R_L \to \infty$), one can easily see that in $\mathcal{R}'_G$ and $\mathcal{R}'_C$, the maximum value of R_I

is $\frac{1}{2}\log\left(\frac{(\sigma_x^2+\sigma_1^2)(\sigma_x^2+\sigma_2^2)}{\sigma_x^2\sigma_1^2+\sigma_1^2\sigma_2^2+\sigma_2^2\sigma_x^2}\right) = \frac{1}{2}\log\left(1+\frac{\sigma_x^2}{\sigma_1^2+\sigma_2^2+\sigma_1^2\sigma_2^2/\sigma_x^2}\right)$*. This value is exactly the identification capacity of the BIS for non-standard Gaussian RVs shown in* [5] *(Equation (21)) and it is achieved when* $\alpha \downarrow 0$*.*

Another special case where $R_I = 0$ (only one user), $R_J \to \infty$ (the storage rate is sufficiently large), and $\rho_1 \to 1$ (the enrollment channel is noiseless), one can see that Theorem 1 naturally reduces to the characterizations of [23].

4. Behaviors of the Capacity Region

4.1. Optimal Asymptotic Rates and Zero-Rate Slopes

For the sake of succinct discussion, we concentrate on the generated-secret BIS model at which $R_I = 0$, and the capacity region for this case is denoted by $\mathcal{R}$, whose characterization is obtained by setting $R_I = 0$ in the right-hand side of (19). We first investigate some special points of secret-key and privacy-leakage rates when storage rate becomes extremely low or large. Define two rate functions of R_J as

$$R_S^*(R_J) = \max_{(R_S,R_J,R_L)\in\mathcal{R}} R_S, \qquad\qquad R_L^*(R_J) = \min_{(R_S,R_J,R_L)\in\mathcal{R}} R_L, \tag{23}$$

where the left and right equations in (23) are the maximum secret-key rate and the minimum privacy-leakage rate, respectively. 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

$$\begin{aligned} R_S^*(R_J^\alpha) &= \frac{1}{2}\log\left(\frac{1-\rho_1^2\rho_2^2/2^{2(R_J^\alpha)}}{1-\rho_1^2\rho_2^2}\right), \\ R_L^*(R_J^\alpha) &= \frac{1}{2}\log\left(\frac{1-\rho_1^2\rho_2^2}{1-\rho_1^2+\rho_1^2(1-\rho_2^2)/2^{2(R_J^\alpha)}}\right). \end{aligned} \tag{24}$$

As $R_J^\alpha \to \infty$ ($\alpha \downarrow 0$), the optimal asymptotic secret-key rate and the amount of privacy-leakage approach to

$$\lim_{R_J^\alpha\to\infty} R_S^*(R_J^\alpha) = \frac{1}{2}\log\left(\frac{1}{1-\rho_1^2\rho_2^2}\right) = I(Y;Z), \tag{25}$$

$$\begin{aligned} \lim_{R_J^\alpha\to\infty} R_L^*(R_J^\alpha) &= \frac{1}{2}\log\left(\frac{1-\rho_1^2\rho_2^2}{1-\rho_1^2}\right) = \frac{1}{2}\log\left(\frac{1}{1-\rho_1^2}\right) - \frac{1}{2}\log\left(\frac{1}{1-\rho_1^2\rho_2^2}\right) \\ &= I(X;Y) - I(Z;Y). \end{aligned} \tag{26}$$

The result (25) corresponds to the optimal asymptotic secret-key rate [23] (Sect. III-B), and in order to achieve this value, it is required to let the storage rate go 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 secret-key and small privacy-leakage rates in the low storage rate regime, the zero-rate slopes of secret-key and privacy-leakage rates, namely, how fast these rates converge to zero, are important indicators. In light of (24), by a few steps of calculations, the slopes of secret-key and privacy-leakage rates at $R_J \downarrow 0$ can be determined as follows:

$$\left.\frac{dR_S^*(R_J^\alpha)}{dR_J^\alpha}\right|_{R_J^\alpha=0} = \frac{\rho_1^2\rho_2^2}{1-\rho_1^2\rho_2^2}, \tag{27}$$

$$\left.\frac{dR_L^*(R_J^\alpha)}{dR_J^\alpha}\right|_{R_J^\alpha=0} = \frac{\rho_1^2(1-\rho_2^2)}{1-\rho_1^2\rho_2^2} = \frac{\rho_1^2\rho_2^2}{1-\rho_1^2\rho_2^2}\cdot\frac{1-\rho_2^2}{\rho_2^2}, \tag{28}$$

where (27) is equal to the signal-to-noise ratio (SNR) of the channel from Y to Z, and this value multiplied by the reverse of the SNR of the channel $P_{Z|X}$ appears in the slope of privacy-leakage rate in (28).

4.2. Examples

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 levels of noises (noises with smaller variances) added to the bio-data sequences at the encoder and decoder become small. Example 1 is the case where the level of noise at the encoder gradually decreases from (a) to (c), but the level of noise at the decoder stays constant for each round. Example 2 is the case in which the levels of noises at both the encoder and decoder are improved gradually from (a) to (c). Example 3 is opposite to Example 1. The calculated results of the secret-key and privacy-leakage rates for these cases are summarized in Tables 1 and 2, and Figure 5.

Table 1. The secret-key and privacy-leakage rates when $R_J \to \infty$.

Cases	The Optimal Secret-Key Rate			Privacy-Leakage Rate		
	(a)	**(b)**	**(c)**	**(a)**	**(b)**	**(c)**
Ex. 1	0.35	0.44	0.49	0.35	0.6	0.90
Ex. 2	0.35	0.77	0.98	0.35	0.38	0.41
Ex. 3	0.35	0.55	0.6	0.35	0.14	0.09

Table 2. The slopes of secret-key and privacy-leakage rates at $R_J \downarrow 0$.

Cases	The Slope of Secret-Key Rate			The Slope of 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

It is ideal to keep the privacy-leakage rate small while producing a high secret-key rate, but Example 1 works out in the opposite way (cf. the rows of Ex. 1 in Tables 1 and 2), so this is not a preferable choice. Example 2 realizes a high secret-key rate, but the amount of privacy-leakage remains high at some level, too (cf. the rows of Ex. 2 in Tables 1 and 2, and Figure 5a,b). On the other hand, in Example 3, the privacy-leakage rate declines, but the secret-key rate becomes smaller compared to Example 2 (cf. the rows of Ex. 3 in Tables 1 and 2, and Figure 5c,d). From these behaviors, we may conclude that it is unmanageable to achieve both high secret-key and small privacy-leakage rates at the same time. If one aims to achieve a high secret-key rate, it is important to diminish the levels of noises at both encoder and decoder, e.g., deploying quantizers with high quality, but this could result in leaking more users' privacy. In different circumstances, to achieve a small privacy-leakage rate, it is preferable to maintain a certain level of noise at the encoder and pay sufficient attention for processing the noise's level at the decoder. In this way, however, the gain of the secret-key rate may be dropped.

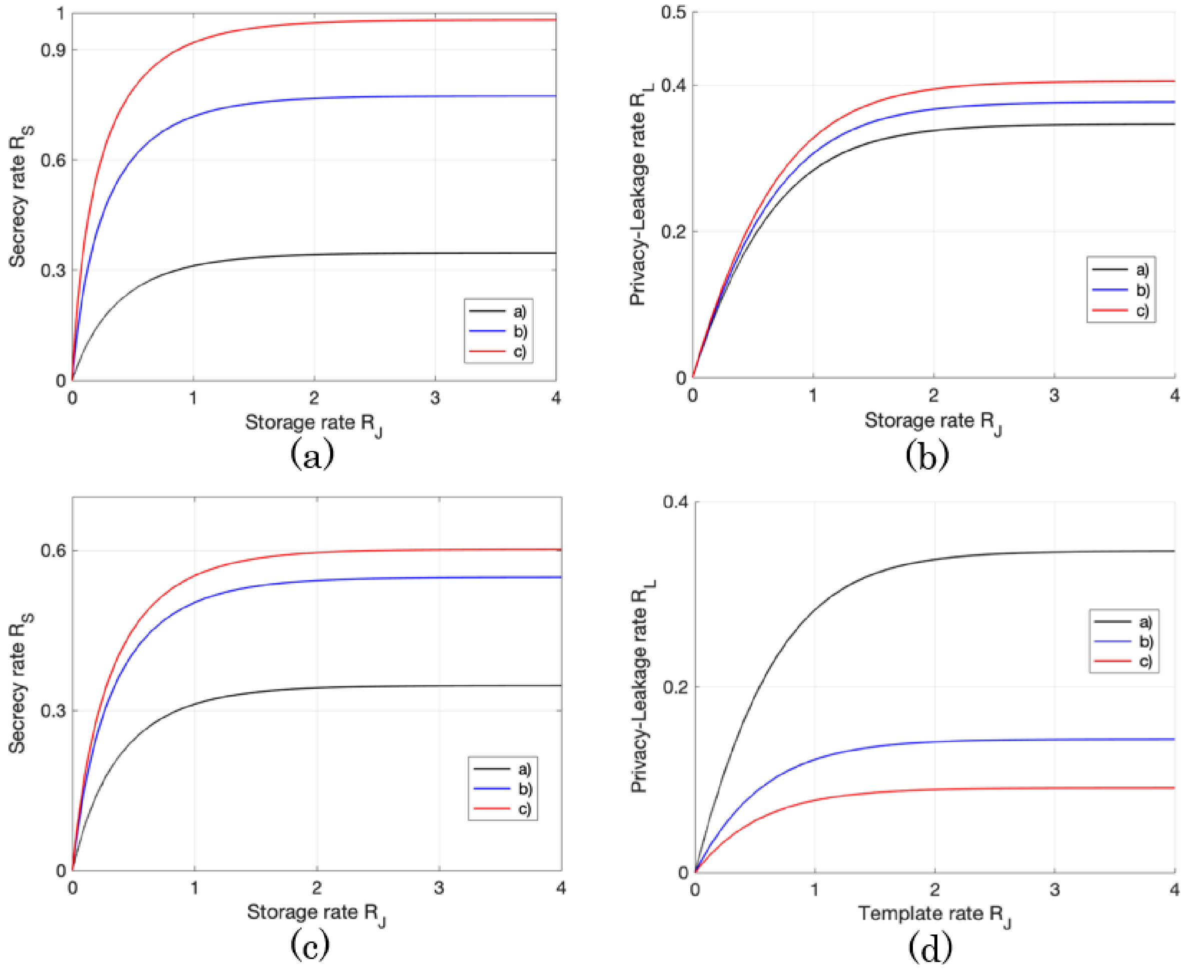

Figure 5. The projections of the capacity region $\mathcal{R}_G$ onto two dimension figures for Exs. 2 and 3. (**a**) is the boundary of the capacity region $\mathcal{R}_G$ onto $R_J R_S$-plane for Ex. 2. (**b**) is the boundary of the capacity region $\mathcal{R}_G$ onto $R_J R_L$-plane for Ex. 2. (**c**) is the boundary of the capacity region $\mathcal{R}_G$ onto $R_J R_S$-plane for Ex. 3. (**d**) is the boundary of the capacity region $\mathcal{R}_G$ into $R_J R_L$-plane for Ex. 3.

5. Overviews of the Proof of Theorem 1

The detailed proof of Theorem 1 is provided in Appendix A for $\mathcal{R}_G$ and Appendix B for $\mathcal{R}_C$. The regions $\mathcal{R}_G$ and $\mathcal{R}_C$ can be derived similarly, and the difference is that one-time pad is used to conceal the chosen secret key for secure transmission in the proof of $\mathcal{R}_C$. The proof of each region consists of two parts: achievability and converse parts. The converse proof follows by applying Fano's inequality [26], and the conditional version of EPI [27] doubly in two different directions. In the achievability part, the modified typical set [11], giving the so-called Markov lemma for weak typicality, helps us show that the error probability of the BIS vanishes since the so-called Markov lemma based on strong typicality can not be applied to the case of continuous RVs. Though a more general version of the Markov lemma for Gaussian sources, including lossy reconstruction, is shown in [28], we found that the two properties of the modified typical set are handy tools for checking all conditions in Definitions 1 and 2, and thus we provide our proof of the achievability based on this set. To evaluate the secret-key, secrecy-leakage, and privacy-leakage rates, we extend [29] (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.

6. Conclusions and Future Work

We characterized the capacity regions of identification, secret-key, storage, and privacy-leakage rates for both generated- and chosen-secret BIS models under Gaussian sources and channels. We showed that an idea for deriving the capacity regions of the BIS with HSM 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 generated-secret BIS model, and from these results, it appeared that achieving high secret-key and small privacy-leakage rates simultaneously is unlikely manageable.

For future work, a natural extension is to characterize the capacity regions of the BIS with Gaussian vector sources and channels. In the scalar Gaussian case, we showed that it suffices to use a single parameter to characterize the optimal trade-off of the BIS. However, for Gaussian vector sources, the optimal trade-off regions is generally in the form of the covariance matrix optimization problem, and solving the problem becomes more challenging as one may need to use the enhancement technique, introduced in [30], to characterize the capacity regions.

Another extension is to construct practical codes that can achieve the capacity regions. In the BIS with a single user, convolutional and turbo codes that control the privacy-leakage were investigated in [31] and applied to real-life application, Electroencephalograph, in [32]. In these studies, it was shown that by applying vector quantization at the encoder and soft-decision at the decoder for Gaussian sources, a lower privacy-leakage rate was realizable. However, to the best of our knowledge, there has not yet been any studies dealing with practical codes for the BIS with multiple users. This remains as an interesting research topic.

Author Contributions: The V.Y. author contributes to the conceptualization of the research goals and aims, the visualization/presentation of the works, the formal analysis of the results, and the review and editing. The H.Y. and Y.O. authors contribute to the conceptualization of the ideas, the validation of the results, and the supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported in part by JSPS KAKENHI Grant Numbers JP20K04462, JP19J13686, JP18H01438, and JP17K00020.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Proof of Equation (19)

In this appendix, we give the proof of the capacity region of the generated-secret BIS model. Before proceeding to the proof, we review the definitions of the weakly typical and modified typical sets, and some properties of these sets.

Appendix A.1. Weakly Typical Sets and Modified Typical Sets

The definition and property of weakly typical set hold for both discrete and continuous RVs, but here we provide only the continuous version.

Definition A1. *(Weakly ϵ-typical set for continuous RVs [26] (Chapter 8))*

Let $X_1, X_2, \cdots, X_k$ be a sequence of continuous RVs drawn i.i.d. according to the joint pdf $f_{X_1X_2\cdots X_k}(x_1, x_2, \cdots, x_k)$. For small enough $\epsilon > 0$, and any n, the weakly ϵ-typical set $\mathcal{A}_\epsilon^{(n)}(X_1X_2\cdots X_k)$ with respect to $f_{X_1X_2\cdots X_k}(x_1, x_2, \cdots, x_k)$ is defined as follows:

$$\mathcal{A}_\epsilon^{(n)}(X_1X_2\cdots X_k) = \left\{(x_1^n, x_2^n, \cdots, x_k^n) : \left|-\frac{1}{n}\log f_{S^n}(s^n) - h(S)\right| < \epsilon, \forall S \subseteq \{X_1, X_2, \cdots, X_k\}\right\}, \quad \text{(A1)}$$

where $s^n \subseteq \{x_1^n, x_2^n, \cdots, x_k^n\}$ *corresponding to RV* S *and* $f_{S^n}(s^n) = \prod_{t=1}^n f_{S_t}(s_t)$. *Moreover, the conditional* ϵ*-typical set is defined as* $\mathcal{A}_\epsilon^{(n)}(X_k|x_2^n, \cdots, x_{k-1}^n) = \left\{x_k^n : (x_1^n, x_2^n, \cdots, x_k^n) \in \mathcal{A}_\epsilon^{(n)}(X_1X_2\cdots X_k)\right\}$.

The weakly ϵ-typical set $\mathcal{A}_\epsilon^{(n)}(\cdot)$ has the following properties.

Lemma A1. *(Some properties of weakly* ϵ*-typical set* [26]*)*

1. *For* $\forall S \subseteq \{X_1, X_2, \cdots, X_k\}$ *and large enough* n*,*

$$\Pr\{\mathcal{A}_\epsilon^{(n)}(S)\} \geq 1 - \epsilon. \tag{A2}$$

2. *For* $\forall S, V \subseteq \{X_1, X_2, \cdots, X_k\}$ $(S \cap V = \emptyset)$*, we have that*

$$\mathrm{Vol}(\mathcal{A}_\epsilon^{(n)}(V|s^n)) \leq e^{n(h(V|S)+2\epsilon)}, \tag{A3}$$

where $\mathrm{Vol}(\cdot)$ *denotes the volume of a set.*

3. *Fix* $k = 2$*. If* $(\tilde{X}_1^n, \tilde{X}_2^n)$ *are independent sequences with the same marginals as* $f_{X_1^nX_2^n}(x_1^n, x_2^n)$*, then*

$$\Pr\{(\tilde{X}_1^n, \tilde{X}_2^n) \in \mathcal{A}_\epsilon^{(n)}(X_1X_2)\} \leq e^{-n(I(X_1;X_2)-2\epsilon)}. \tag{A4}$$

Moreover, for n large enough,

$$\Pr\{(\tilde{X}_1^n, \tilde{X}_2^n) \in \mathcal{A}_\epsilon^{(n)}(X_1X_2)\} \geq (1-\epsilon)e^{-n(I(X_1;X_2)+2\epsilon)}. \tag{A5}$$

Proof. See [26] (Section 15.2). □

Next, we provide the definition of the modified ϵ-typical set. This set gives the so-called Markov lemma for the weak typicality.

Definition A2. *(Modified* ϵ*-typical set* [11] *(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*

$$\mathcal{B}_\epsilon^{(n)}(YU) = \left\{(y^n, u^n) : \Pr\{X^n \in \mathcal{A}_\epsilon^{(n)}(X|y^n, u^n)|(Y^n, U^n) = (y^n, u^n)\} \geq 1 - \epsilon\right\}, \tag{A6}$$

where 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* $\mathcal{B}_\epsilon^{(n)}(U|y^n) = \{u^n : (y^n, u^n) \in \mathcal{B}_\epsilon^{(n)}(YU)\}$ *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 modified set induces two useful properties below.

Lemma A2. *(Properties of the modified set* [11] *(Appendix A-A))*

Property 1. If $(y^n, u^n) \in \mathcal{B}_\epsilon^{(n)}(YU)$ *then also* $(y^n, u^n) \in \mathcal{A}_\epsilon^{(n)}(YU)$*.*

Property 2. Assume that $(U^n, Y^n, X^n) \sim f_{U^nX^nY^n} = \prod_{t=1}^n f_{X_tY_t}f_{U_t|Y_t}$*. Then, for* $\epsilon \in (0, 1)$ *and n large enough,* $\sum_{(y^n,u^n)\in\mathcal{B}_\epsilon^{(n)}(YU)} P_{Y^nU^n}(y^n, u^n) \geq 1 - \epsilon$*.*

Proof. See [11] (Appendix A-A). □

Now we are at the position to present the detailed proofs of Equation (19).

Appendix A.2. Achievability Part

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. Let $U \sim \mathcal{N}(0, 1-\alpha)$, Gaussian RV with mean zero and variance $1-\alpha$. As shown in Figure A1, based on the converted system, consider that $Y_{ik} = U + \Phi$, where $\Phi \sim \mathcal{N}(0, \alpha)$, independent of U, is Gaussian with mean zero and variance α. From (9) and (10) of the converted system, it holds that

$$X_{ik} = \rho_1 U + \rho_1 \Phi + N_1', \qquad Z_k = \rho_1\rho_2 U + \rho_1\rho_2\Phi + \rho_2 N_1' + N_2. \tag{A7}$$

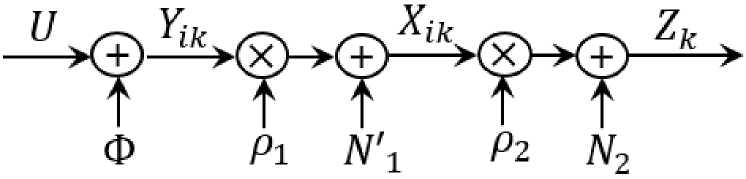

Figure A1. Relation among RVs (U, Y, X, Z).

Hence, we readily see that

$$I(Y;U) = \frac{1}{2}\log\left(\frac{1}{\alpha}\right), \quad I(X;U) = \frac{1}{2}\log\left(\frac{1}{\alpha\rho_1^2 + 1 - \rho_1^2}\right),$$
$$I(Z;U) = \frac{1}{2}\log\left(\frac{1}{\alpha\rho_1^2\rho_2^2 + 1 - \rho_1^2\rho_2^2}\right). \tag{A8}$$

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

$$R_S = I(Z;U) - R_I - 2\delta, \quad R_J = I(Y;U) - I(Z;U) + R_I + 6\delta, \tag{A9}$$
$$R_L = I(X;U) - I(Z;U) + R_I + 6\delta, \quad M_I = 2^{nR_I}, \quad M_S = 2^{nR_S}, \quad M_J = 2^{nR_J}, \tag{A10}$$

where the values of $I(Y;U), I(X;U)$, and $I(Z;U)$ are specified in (A8). Also, recall that $\mathcal{I} = [1 : M_I], \mathcal{S} = [1 : M_S]$, $\mathcal{J} = [1 : M_J]$.

Next we generate $e^{n(I(Y;U)+\delta)}$ sequences of $u^n(s, j)$ i.i.d. from pdf f_U, where $s \in \mathcal{S}$ and $j \in \mathcal{J}$.

Seeing y_i^n $(i \in \mathcal{I})$, the encoder finds $u^n(s, j)$ such that $(y_i^n, u^n(s, j)) \in \mathcal{B}_\delta^{(n)}(YU)$, denoting the modified set defined in Definition A2. If there are multiple pairs of such (s, j), the encoder picks one at random. If there are no such pairs, it declares error. We denote the chosen pair as $(s(i), j(i))$, where each element is a function of the index i. The helper $j(i)$ is stored in the helper DB and secret key $s(i)$ is saved in the key DB at location i, respectively.

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 $s \in \mathcal{S}$, where $\mathcal{A}_\delta^{(n)}(ZU)$ denotes the weakly δ-typical set. If a unique pair (i, s) is found, it outputs $(\widehat{w}, \widehat{s(w)}) = (i, s)$, or else it declares error.

Let $(S(i), J(i))$ 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 notational simplicity. Note that the pair $(S(i), J(i))$ can determine the sequence U_i^n precisely. Next, we check all conditions in Definition 1 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:

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

and those at the decoder are:

$\mathcal{E}_2 \ : \{(Z^n, U_i^n) \notin \mathcal{A}_\delta^{(n)}(ZU)\}$,

$\mathcal{E}_3$ $:\{(Z^n, U^n(s', J(i))) \in \mathcal{A}_\delta^{(n)}(ZU)$ for some $s' \in \mathcal{S},\ s' \neq S(i)\}$,
$\mathcal{E}_4$ $:\{(Z^n, U^n(s, J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU)$ for some $i' \in \mathcal{I},\ i' \neq i$, and $s \in \mathcal{S}\}$.

As usual, we use the random coding argument, and the ensemble average of the error probability can be evaluated as

$$\begin{aligned}\Pr\{(\widehat{W}, \widehat{S(W)}) \neq (W, S(W)) | W = i\} &= \Pr\{\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3 \cup \mathcal{E}_4\} \\ &\leq \Pr\{\mathcal{E}_1\} + \Pr\{\mathcal{E}_2 \cap \mathcal{E}_1^c\} + \Pr\{\mathcal{E}_3\} + \Pr\{\mathcal{E}_4\}, \quad \text{(A11)}\end{aligned}$$

where each of $\Pr\{\cdot\}$ on the right-hand side denotes the conditional probability given $W = i$.

Now let us focus on bounding each term individually. The first term of (A11) can be made arbitrarily small by a similar argument of [11] (cf. the analysis of First Term of Error Probability in Appendix A-B). The rest can be analyzed as follows. For the second term, it follows that

$$\begin{aligned}\Pr\{\mathcal{E}_2 \cap \mathcal{E}_1^c\} &= \Pr\{(Z^n, U_i^n) \notin \mathcal{A}_\delta^{(n)}(ZU) \cap (Y_i^n, U_i^n) \in \mathcal{B}_\delta^{(n)}(YU)\} \\ &\leq \Pr\{(Z^n, Y_i^n, U_i^n) \notin \mathcal{A}_\delta^{(n)}(ZYU) \cap (Y_i^n, U_i^n) \in \mathcal{B}_\delta^{(n)}(YU)\} \\ &= \iint_{\mathcal{B}_\delta^{(n)}(YU)} f_{Y_i^n U_i^n}(y^n, u^n) \Pr\{Z^n \notin \mathcal{A}_\delta^{(n)}(Z|y^n, u^n) | (Y_i^n, U_i^n) = (y^n, u^n)\} d(y^n, u^n) \\ &\overset{\text{(a)}}{\leq} \delta \iint_{\mathcal{B}_\delta^{(n)}(YU)} f_{Y_i^n U_i^n}(y^n, u^n) d(y^n, u^n) \leq \delta, \qquad \text{(A12)}\end{aligned}$$

where (a) follows from the definition of the modified δ-typical set due to the Markov chain $Z - Y - U$. To bound $\Pr\{\mathcal{E}_3\}$, due to the symmetry in the codebook generation, we can set $J(i) = 1$ and have that

$$\begin{aligned}\Pr\{\mathcal{E}_3\} &= \Pr\{(Z^n, U^n(s', 1)) \in \mathcal{A}_\delta^{(n)}(ZU) \ \text{ for some } s' \in \mathcal{S},\ s' \neq S(i)\} \\ &= \sum_{s \in \mathcal{S}} \Big(\Pr\{S(i) = s\} \cdot \Pr\{(Z^n, U^n(s', 1)) \in \mathcal{A}_\delta^{(n)}(ZU) \ \text{ for some } s' \in \mathcal{S},\ s' \neq s | S(i) = s\} \Big) \\ &= \sum_{s \in \mathcal{S}} \left(\Pr\{S(i) = s\} \cdot \Pr\left\{ \bigcup_{s' \in \mathcal{S} \backslash s} (Z^n, U^n(s', 1)) \in \mathcal{A}_\delta^{(n)}(ZU) \middle| S(i) = s \right\} \right) \\ &\leq \sum_{s \in \mathcal{S}} \left(\Pr\{S(i) = s\} \cdot \left(\sum_{s' \in \mathcal{S} \backslash s} \Pr\left\{ (Z^n, U^n(s', 1)) \in \mathcal{A}_\delta^{(n)}(ZU) \middle| S(i) = s \right\} \right) \right) \\ &\overset{\text{(b)}}{=} \sum_{s \in \mathcal{S}} \left(\Pr\{S(i) = s\} \cdot \left(\sum_{s' \in \mathcal{S} \backslash s} \Pr\{(Z^n, U^n(s', 1)) \in \mathcal{A}_\delta^{(n)}(ZU)\} \right) \right) \\ &\leq \sum_{s \in \mathcal{S}} \left(\Pr\{S(i) = s\} \cdot \left(\sum_{s' \in \mathcal{S} \backslash s} e^{-n(I(Z;U) - \delta)} \right) \right) \\ &\leq M_S \cdot e^{-n(I(Z;U) - \delta)} \leq e^{-n\delta}, \qquad \text{(A13)}\end{aligned}$$

where (b) holds because the event $\{(Z^n, U^n(s', 1)) \in \mathcal{A}_\delta^{(n)}(ZU)\}$, $s' \in \mathcal{S} \backslash s$ and the event $\{S(i) = s\}$ are mutually independent, and the last inequality in (A13) follows as $R_S < I(Z; U)$.

To evaluate $\Pr\{\mathcal{E}_4\}$, we define two new events $\mathcal{E}_4' = \{(Z^n, U^n(S(i), J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU)$ for some $i' \neq i,\ i' \in \mathcal{I}\}$ and $\mathcal{E}_4'' = \{(Z^n, U^n(s', J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU)$ for some $i' \neq i,\ i' \in \mathcal{I}$

and $s' \neq S(i)$, $s' \in \mathcal{S}\}$. Because $\mathcal{E}' \cap \mathcal{E}'' = \emptyset$, it follows that $\Pr\{\mathcal{E}_4\} = \Pr\{\mathcal{E}_4'\} + \Pr\{\mathcal{E}_4''\}$. For $\Pr\{\mathcal{E}_4'\}$, without loss of generality, we set $S(i) = 1$. Then, it follows that

$$\begin{aligned}\Pr\{\mathcal{E}_4'\} &= \Pr\{(Z^n, U^n(1, J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU) \ \text{ for some } i' \in \mathcal{I},\ i' \neq i\} \\ &\leq \sum_{i' \in \mathcal{I}\setminus i} \Pr\{(Z^n, U^n(1, J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU)\} \\ &\leq \sum_{i' \in \mathcal{I}\setminus i} e^{-n(I(Z;U)-\delta)} \leq M_I \cdot e^{-n(I(Z;U)-\delta)} \leq e^{-n\delta}, \end{aligned} \tag{A14}$$

where the last inequality in (A14) follows as $R_I < I(Z;U)$. For $\Pr\{\mathcal{E}_4''\}$, due to the statistical independence of Z^n and $U^n(s', J(i'))$, we have that

$$\begin{aligned}\Pr\{\mathcal{E}_4''\} &= \Pr\{(Z^n, U^n(s', J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU) \ \text{ for some } i' \neq i,\ i' \in \mathcal{I} \text{ and } s' \neq S(i),\ s' \in \mathcal{S}\} \\ &= \Pr\left\{ \bigcup_{i' \in \mathcal{I}\setminus i,\ s' \in \mathcal{S}\setminus S(i)} (Z^n, U^n(s', J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU) \right\} \\ &= \sum_{s \in \mathcal{S}} \left(\Pr\{S(i) = s\} \cdot \Pr\left\{ \bigcup_{i' \in \mathcal{I}\setminus i,\ s' \in \mathcal{S}\setminus s} (Z^n, U^n(s', J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU) \middle| S(i) = s \right\} \right) \\ &\leq \sum_{s \in \mathcal{S}} \left(\Pr\{S(i) = s\} \cdot \left(\sum_{i' \in \mathcal{I}\setminus i} \sum_{s' \in \mathcal{S}\setminus s} \Pr\left\{ (Z^n, U^n(s', J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU) \middle| S(i) = s \right\} \right) \right) \\ &= \sum_{s \in \mathcal{S}} \left(\Pr\{S(i) = s\} \cdot \left(\sum_{i' \in \mathcal{I}\setminus i} \sum_{s' \in \mathcal{S}\setminus s} \Pr\{(Z^n, U^n(s', J(i'))) \in \mathcal{A}_\delta^{(n)}(ZU)\} \right) \right) \\ &= \sum_{s \in \mathcal{S}} \left(\Pr\{S(i) = s\} \cdot \left(\sum_{i' \in \mathcal{I}\setminus i} \sum_{s' \in \mathcal{S}\setminus s} e^{-n(I(Z;U)-\delta)} \right) \right) \\ &\leq M_I \cdot M_S \cdot e^{-n(I(Z;U)-\delta)} = e^{-n\delta}, \end{aligned} \tag{A15}$$

where the last equality in (A15) holds as $\frac{1}{n}\log M_I + \frac{1}{n}\log M_S = I(Z;U) - 2\delta$. Hence, the error probability is bounded by

$$\Pr\{(\widehat{W}, \widehat{S(W)}) \neq (W, S(W)) | W = i\} \leq 4\delta \tag{A16}$$

for large enough n.

Before diving into the detailed analysis, we state lemmas that are important for the rest of the evaluations.

Lemma A3. *For given u^n and large enough n, we have that*

$$\mathrm{Vol}\Big(\mathcal{B}_\delta^{(n)}(Y|u^n)\Big) \leq \mathrm{Vol}\Big(\mathcal{A}_\delta^{(n)}(Y|u^n)\Big). \tag{A17}$$

Proof. This is a straightforward result from Property 1 of Lemma A2. □

The following lemma plays an essential role in bounding the secret-key, secrecy-leakage, and privacy-leakage rates of the BIS. Again recall that the index pair $(S(i), J(i))$ determines U_i^n directly, and therefore Lemma A4 can be thought of an extended version of [29] (Lemma 4) to incorporate continuous RVs. In [29], the lemma was proved by using the strongly typical set [33], and the literature, e.g., [8,13] demonstrated that it could be finely applied to establish the achievability part of the BIS under noisy enrollment for DMS settings. However, when the sources of the BIS becomes Gaussian, it is not trivial whether the claim of this lemma still holds or not. Here, we provide a full proof of the extended version of [29] (Lemma 4) for Gaussian RVs by using the connection between the modified δ-typical set $\mathcal{B}_\delta^{(n)}(\cdot)$ and the weakly δ-typical set $\mathcal{A}_\delta^{(n)}(\cdot)$.

Lemma A4. *It holds that*

$$h(Y_i^n|S(i),J(i),\mathcal{C}_n) \le n(h(Y|U)+\delta_n), \tag{A18}$$

$$h(Y_i^n|X_i^n,S(i),J(i),\mathcal{C}_n) \le n(h(Y|X,U)+\delta_n), \tag{A19}$$

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

Proof. We first prove (A18). Define a binary RV T taking value 1 if $(Y_i^n,U_i^n) \in \mathcal{B}_\delta^{(n)}(YU)$, and 0 otherwise. In the analysis of the error probability, it is guaranteed that $P_T(0) \le \delta$, i.e., $(Y_i^n,U_i^n) \in \mathcal{B}_\delta^{(n)}(YU)$ with high probability. The left-hand side of (A18) can be bounded as

$$\begin{aligned}
h(Y_i^n|S(i),J(i),\mathcal{C}_n) &\overset{\text{(c)}}{=} h(Y_i^n|U_i^n,S(i),J(i),\mathcal{C}_n)\\
&\overset{\text{(d)}}{\le} h(Y_i^n|U_i^n) \le h(Y_i^n,T|U_i^n) \le H(T)+h(Y_i^n|U_i^n,T)\\
&\le 1+P_T(0)h(Y_i^n|U_i^n,T=0)+P_T(1)h(Y_i^n|U_i^n,T=1)\\
&\overset{\text{(e)}}{\le} n\epsilon_n + h(Y_i^n|U_i^n,T=1)\\
&= n\epsilon_n + \int_{\mathbb{R}^n} h(Y_i^n|U_i^n=u^n,T=1)dF(u^n)\\
&= n\epsilon_n + \int_{\mathbb{R}^n}\int_{\mathcal{B}_\delta^{(n)}(Y|u^n)} P_{Y_i^n|U_i^n,T}(y^n|u^n,1)\log\frac{1}{P_{Y_i^n|U_i^n,T}(y^n|u^n,1)}dy^n dF(u^n)\\
&\overset{\text{(f)}}{\le} n\epsilon_n + \int_{\mathbb{R}^n}\log\left(\int_{\mathcal{B}_\delta^{(n)}(Y|u^n)} P_{Y_i^n|U_i^n,T}(y^n|u^n,1)\frac{1}{P_{Y_i^n|U_i^n,T}(y^n|u^n,1)}dy^n\right)dF(u^n)\\
&= n\epsilon_n + \int_{\mathbb{R}^n}\log\left(\int_{\mathcal{B}_\delta^{(n)}(Y|u^n)} dy^n\right)dF(u^n)\\
&= n\epsilon_n + \int_{\mathbb{R}^n}\log\left(\mathrm{Vol}\left(\mathcal{B}_\delta^{(n)}(Y|u^n)\right)\right)dF(u^n)\\
&\overset{\text{(g)}}{\le} n\epsilon_n + \int_{\mathbb{R}^n}\log\left(\mathrm{Vol}\left(\mathcal{A}_\delta^{(n)}(Y|u^n)\right)\right)dF(u^n)\\
&\overset{\text{(h)}}{\le} n\epsilon_n + n(h(Y|U)+\delta))\int_{\mathbb{R}^n} dF(u^n)\\
&= n(h(Y|U)+\delta+\epsilon_n),
\end{aligned} \tag{A20}$$

where

(c) follows as $(S(i),J(i))$ determines U_i^n,
(d) follows because conditioning reduces entropy,
(e) follows as $h(Y_i^n|U_i^n,T=0) \le h(Y_i^n) = \frac{n}{2}\log(2\pi e)$, and we define $\epsilon_n = \frac{1}{n}+\frac{\delta}{2}\log(2\pi e)$,
(f) follows by applying Jensen's inequality to the concave function $\phi(t) = -t\log t$,
(g) is due to (A17) in Lemma A3,
(h) is due to (A3) in Lemma A1.

Therefore, from (A20), we obtain that

$$\frac{1}{n}h(Y_i^n|S(i),J(i),\mathcal{C}_n) \le h(Y|U)+\delta_n, \tag{A21}$$

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

Next, we briefly summarize how to show (A19). The left-hand side of the inequality can be developed as $h(Y_i^n|X_i^n,S(i),J(i),\mathcal{C}_n) = h(Y_i^n|X_i^n,U_i^n,S(i),J(i),\mathcal{C}_n) \le h(Y_i^n|X_i^n,U_i^n)$, where the equality and inequality follow due to the same reasons of (c) and (d) in (A20), respectively. By the definition of the modified δ-typical set in Definition A2, it can be concluded that $\Pr\{(X_i^n, Y_i^n, U_i^n) \in \mathcal{A}_\delta^{(n)}(XYU)\} \to 1$ as $n \to \infty$ 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 $\Pr\{(X_i^n, U_i^n) \in \mathcal{A}_\delta^{(n)}(XU)\} \to 1$ and $\Pr\{Y_i^n \in \mathcal{A}_\delta^{(n)}(Y|x^n, u^n)|(X_i^n, U_i^n) = (x^n, u^n)\} \to 1$ as $n \to \infty$ as well. Based on this observation, the rest of the proof for (A19) can be done similarly by the arguments seen in [29] (Appendix C), and therefore the details are omitted. □

Note that Equations (14) and (16) obviously hold from the parameter settings. By applying Lemma A4, bounds on the secret-key and the secrecy-leakage rates can be derived as follows:

$$\frac{1}{n}H(S(i)|\mathcal{C}_n) \geq R_S - 5\delta = \frac{1}{n}\log M_S - 5\delta, \qquad \frac{1}{n}I(S(i);J(i)|\mathcal{C}_n) \leq 5\delta \tag{A22}$$

for large enough n. For detailed discussions, the readers may refer to [14] (Proof of Theorem 1).

Analysis of Privacy-Leakage Rate: From the left-hand side of (18), we have that

$$\begin{aligned} I(X_i^n; J(i)|\mathcal{C}_n) &= H(J(i)|\mathcal{C}_n) - H(J(i)|X_i^n, \mathcal{C}_n) \\ &\leq nR_J - H(J(i)|X_i^n, \mathcal{C}_n) \\ &= n(I(Y;U) - I(Z;U) + R_I + 6\delta) - H(J(i)|X_i^n, \mathcal{C}_n) \\ &= n(h(U|Z) - h(U|Y) + R_I + 6\delta) - H(J(i)|X_i^n, \mathcal{C}_n). \end{aligned} \tag{A23}$$

The last term in (A23) can be further evaluated as

$$\begin{aligned} H(J(i)|X_i^n, \mathcal{C}_n) &= h(Y_i^n, J(i)|X_i^n, \mathcal{C}_n) - h(Y_i^n|X_i^n, J(i), \mathcal{C}_n) \\ &= h(Y_i^n, J(i)|X_i^n, \mathcal{C}_n) - h(Y_i^n|X_i^n, J(i), S(i), \mathcal{C}_n) - I(Y_i^n; S(i)|X_i^n, J(i), \mathcal{C}_n) \\ &\overset{\text{(i)}}{=} h(Y_i^n|X_i^n, \mathcal{C}_n) - h(Y_i^n|X_i^n, J(i), S(i), \mathcal{C}_n) - H(S(i)|X_i^n, J(i), \mathcal{C}_n) \\ &\overset{\text{(j)}}{=} nh(Y|X) - h(Y_i^n|X_i^n, J(i), S(i), \mathcal{C}_n) - H(S(i)|X_i^n, J(i), Z^n, \mathcal{C}_n) \\ &\overset{\text{(k)}}{\geq} nh(Y|X) - h(Y_i^n|X_i^n, J(i), S(i), \mathcal{C}_n) - H(S(i)|\boldsymbol{J}, Z^n, \mathcal{C}_n) \\ &\overset{\text{(l)}}{\geq} nh(Y|X) - h(Y_i^n|X_i^n, J(i), S(i), \mathcal{C}_n) - n\delta_n' \\ &\overset{\text{(m)}}{\geq} nh(Y|X) - n(h(Y|X,U) + \delta_n) - n\delta_n' \\ &= n(I(Y;U|X) - \delta_n - \delta_n') \\ &= n(h(U|X) - h(U|Y) - \delta_n - \delta_n'), \end{aligned} \tag{A24}$$

where

(i) follows as $J(i)$ and $S(i)$ are functions of Y_i^n for given codebook $\mathcal{C}_n$,
(j) follows since (Y_i^n, X_i^n) are independent of $\mathcal{C}_n$, and the Markov chain $S(i) - (X_i^n, J(i)) - Z^n$ holds,
(k) follows because conditioning reduces entropy and $S(i) - (J(i), Z^n) - \boldsymbol{J}\backslash J(i)$ is applied,
(l) follows by applying Fano's inequality since $S(i)$ can be reliably reconstructed from $(\boldsymbol{J}, Z^n)$ for given codebook $\mathcal{C}_n$, and $\delta_n' \downarrow 0$ as $\delta \downarrow 0$ and $n \to \infty$,
(m) is due to (A19).

From (A23) and (A24), we have that

$$\begin{aligned}\frac{1}{n}I(X_i^n;J(i)|\mathcal{C}_n) &\le h(U|Z)-h(U|X)+R_I+6\delta+\delta_n+\delta_n' \\ &= I(X;U)-I(Z;U)+R_I+6\delta+\delta_n+\delta_n' \\ &\le R_L+\delta \end{aligned} \tag{A25}$$

for sufficiently large n.

Finally, by using the selection lemma [34] (Lemma 2.2), from, e.g., (A16) and (A25), there exists at least one good codebook satisfying all the conditions in Definition 1 for large enough n.

Appendix A.3. Converse Part

We consider a more relaxed case where W is uniformly distributed on $\mathcal{I}$, and (13), (15), (17) and (18) in Definition 1 are replaced by

$$\Pr\{(\widehat{W},\widehat{S(W)})\neq(W,S(W))\}\le\delta, \tag{A26}$$

$$\tfrac{1}{n}H(S(W)|W)\ge R_S-\delta, \tag{A27}$$

$$\tfrac{1}{n}I(S(W);J(W)|W)\le\delta, \tag{A28}$$

$$\tfrac{1}{n}I(X_W^n;J(W)|W)\le R_L+\delta, \tag{A29}$$

respectively. Other conditions remain unchanged. We shall show that even for this case the outer bound on $\mathcal{R}_G$ coincides with its inner bound where there is no assumption of the uniformity of W. A similar approach was also taken in [12]. We assume that a rate tuple (R_I,R_S,R_J,R_L) is achievable, implying there exists a pair of encoder and decoder (e,d) such that conditions (14), (16), and (A26)–(A29) are satisfied for any $\delta>0$ and large enough n.

Analysis of Identification and Secret-key Rates: The joint entropy of W and $S(W)$ can be developed as

$$\begin{aligned}H(W,S(W)) &= H(W,S(W)|Z^n,\boldsymbol{J})+I(W,S(W);Z^n,\boldsymbol{J}) \\ &\overset{\text{(a)}}{=} H(W,S(W)|\widehat{W},\widehat{S(W)},Z^n,\boldsymbol{J})+I(W,S(W);\boldsymbol{J})+I(W,S(W);Z^n|\boldsymbol{J}) \\ &\overset{\text{(b)}}{\le} H(W,S(W)|\widehat{W},\widehat{S(W)})+I(W,S(W);J(W))+I(W,S(W);Z^n|J(W)) \\ &\overset{\text{(c)}}{\le} n\delta_n+I(W;J(W))+I(S(W);J(W)|W)+I(W,S(W);Z^n|J(W)) \\ &\overset{\text{(d)}}{\le} n(\delta_n+\delta)+h(Z^n|J(W))-h(Z^n|J(W),S(W)) \\ &\overset{\text{(e)}}{\le} n(\delta_n+\delta)+h(Z^n)-h(Z^n|J(W),S(W)), \end{aligned} \tag{A30}$$

where

(a) holds since $(\widehat{W},\widehat{S(W)})$ is a function of $(Z^n,\boldsymbol{J})$,
(b) follows because conditioning reduces entropy, and only $J(W)$ is possibly dependent on $Z^n,S(W)$,
(c) is due to Fano's inequality with $\delta_n=\frac{1}{n}(1+\delta\log M_IM_S)$,
(d) follows since (A28) is applied, and W is independent of other RVs,
(e) follows because conditioning reduces entropy.

Due to the uniformity of W on $\mathcal{I}$, we have that

$$H(W,S(W))=H(W)+H(S(W)|W)=\log M_I+H(S(W)|W). \tag{A31}$$

From (14), (A27), and (A30), it yields that

$$R_I + R_S \leq h(Z) - \frac{1}{n}h(Z^n|J(W),S(W)) + 3\delta + \delta_n. \tag{A32}$$

Analysis of Storage Rate: From (16),

$$\begin{aligned} n(R_J+\delta) &\geq \log M_J \geq \max_{w\in\mathcal{I}} H(J(w)) \geq H(J(W)|W) \\ &= I(Y_W^n; J(W)|W) \overset{\text{(f)}}{=} h(Y_W^n) - h(Y_W^n|J(W),W) \\ &= h(Y_W^n) - h(Y_W^n|J(W),S(W),W) - I(S(W);Y_W^n|J(W),W) \\ &\overset{\text{(g)}}{=} h(Y_W^n) - h(Y_W^n|J(W),S(W)) - H(S(W)|J(W),W) \\ &\geq h(Y_W^n) - h(Y_W^n|J(W),S(W)) - H(S(W)|W) \\ &\overset{\text{(h)}}{\geq} h(Z^n|J(W),S(W)) - h(Y_W^n|J(W),S(W)) + n(R_I - (\delta_n + 2\delta)), \end{aligned} \tag{A33}$$

where

(f) holds as W is independent of Y_W^n,
(g) holds as W is independent of other RVs and $S(W)$ is a function of Y_W^n,
(h) follows because $h(Y_W^n) = h(Z^n) = \frac{n}{2}\log(2\pi e)$, and by combining (A30) and (A31), we obtain that $H(S(W)|W) \leq h(Z^n) - h(Z^n|J(W),S(W)) - n(R_I - (\delta_n + 2\delta))$.

Analysis of Privacy-Leakage Rate: From (A29),

$$\begin{aligned} n(R_L+\delta) &\geq I(X_W^n; J(W)|W) \overset{\text{(i)}}{=} h(X_W^n) - h(X_W^n|J(W),W) \\ &= h(X_W^n) - h(X_W^n|J(W),S(W),W) - I(S(W);X_W^n|J(W),W) \\ &\geq h(X_W^n) - h(X_W^n|J(W),S(W)) - H(S(W)|J(W),W) \\ &\geq h(X_W^n) - h(X_W^n|J(W),S(W)) - H(S(W)|W) \\ &\overset{\text{(j)}}{\geq} h(Z^n|J(W),S(W)) - h(X_W^n|J(W),S(W)) + n(R_I - (\delta_n + 2\delta)), \end{aligned} \tag{A34}$$

where

(i) holds as W is independent of X_W^n,
(j) follows because $h(X_W^n) = h(Z^n)$, and the same reason of (h) in (A33) is used.

For further evaluations of (A32)–(A34), 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 [27] (Lemma II). It is a key to set

$$\frac{1}{n}h(X_W^n|J(W),S(W)) = \frac{1}{2}\log\Big(2\pi e(\alpha\rho_1^2 + 1 - \rho_1^2)\Big) \tag{A35}$$

with some $0 < \alpha \leq 1$. Indeed, this is a 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. For $\alpha = 0$, it is not possible to achieve such point, and the reason will be explained right after Equation (A40).

In the direction from X to Z, by applying the conditional EPI [27] (Lemma II) to the first equality in (10), it follows that

$$\begin{aligned} e^{\frac{2}{n}h(Z^n|J(W),S(W))} &\geq e^{\frac{2}{n}h(\rho_2 X_W^n|J(W),S(W))} + e^{\frac{2}{n}h(N_2^n|J(W),S(W))} \\ &\overset{\text{(k)}}{=} \rho_2^2 e^{\frac{2}{n}h(X_W^n|J(W),S(W))} + e^{\frac{2}{n}h(N_2^n)} \\ &= \rho_2^2\Big(2\pi e(\alpha\rho_1^2+1-\rho_1^2)\Big) + 2\pi e(1-\rho_2^2) \\ &= 2\pi e(\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2), \end{aligned} \tag{A36}$$

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

$$\frac{1}{n}h(Z^n|J(W),S(W)) \geq \frac{1}{2}\log(2\pi e(\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2)). \tag{A37}$$

In the opposite direction (from X to Y), again applying the conditional EPI [27] (Lemma II) to (9), we have that

$$e^{\frac{2}{n}h(X_W^n|J(W),S(W))} \geq e^{\frac{2}{n}h(\rho_1 Y_W^n|J(W),S(W))} + e^{\frac{2}{n}h((N_1')^n)}, \tag{A38}$$

where the inequality holds as $(N_1')^n$ is also independent of $(J(W), S(W))$, meaning that

$$2\pi e(\alpha\rho_1^2+1-\rho_1^2) \geq \rho_1^2 e^{\frac{2}{n}h(Y_W^n|J(W),S(W))} + 2\pi e(1-\rho_1^2) \tag{A39}$$

and thus

$$\begin{aligned} e^{\frac{2}{n}h(Y_W^n|J(W),S(W))} &\leq 2\pi e\alpha, \\ \frac{1}{n}h(Y_W^n|J(W),S(W)) &\leq \frac{1}{2}\log(2\pi e\alpha), \end{aligned} \tag{A40}$$

which is not derivable from the first equation in (1) of the original system. As previously mentioned for the case in which $\alpha = 0$, in (A40), since RV Y has unit variance, it is required that the joint entropy $H(J(W), S(W))$ should be infinity, but this value is impossible to achieve for finite sets $\mathcal{S}$ and $\mathcal{J}$.

Now plugging (A35), (A37), and (A40) into (A32)–(A34), we obtain that

$$R_I + R_S \leq \frac{1}{2}\log\left(\frac{1}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}\right) + 3\delta + \delta_n, \tag{A41}$$

$$R_J \geq \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{\alpha}\right) + R_I - (3\delta+\delta_n), \tag{A42}$$

$$R_L \geq \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{\alpha\rho_1^2+1-\rho_1^2}\right) + R_I - (3\delta+\delta_n). \tag{A43}$$

Eventually, by letting $n \to \infty$ and $\delta \downarrow 0$, from (A41)–(A43), we can see that the capacity region is contained in the right-hand side of (19).

Appendix B. Proof Sketch of Equation (20)

In this section, we highlight the proof of the chosen-secret BIS model. The parts that follow directly from the same arguments in Appendix A are omitted.

Appendix B.1. Achievability Part

The proof slightly differs from the one in Appendix A, in which 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 Figure A2. In order to avoid confusion in the subsequent arguments, we define some new notation used only in this part. The pairs $(J_C(i), S_C(i))$ and $(J_G(i), S_G(i))$ denote the helper and secret key for individual i generated by the encoders of chosen- and generated-secret BIS models, respectively. To encode Y_i^n for $i \in \mathcal{I}$, the component inside the encoder first generates $(J_G(i), S_G(i))$ and then uses $S_G(i)$ to mask $S_C(i)$ by executing one-time pad operation $S_C(i) \oplus S_G(i)$, 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, i.e.,

$$J_C(i) = (J_G(i), S_C(i) \oplus S_G(i)). \tag{A44}$$

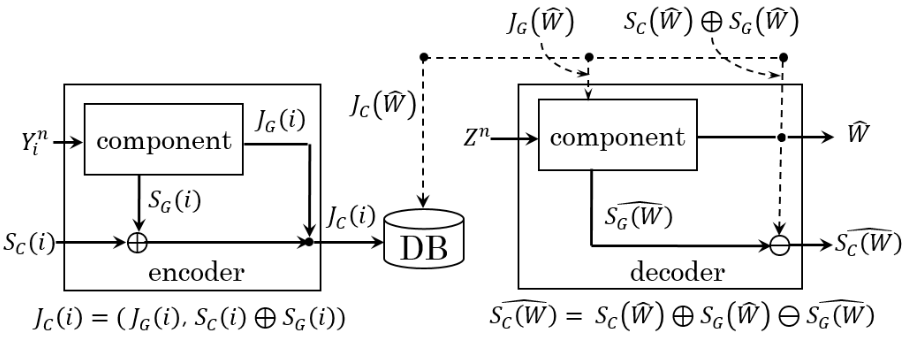
$J_G(\widehat{W})$
$S_C(\widehat{W}) \oplus S_G(\widehat{W})$
$J_C(\widehat{W})$
Y_i^n
component
$J_G(i)$
$S_G(i)$
$S_C(i)$
$J_C(i)$
encoder
DB
Z^n
component
$\widehat{W}$
$\widehat{S_G(W)}$
$\widehat{S_C(W)}$
decoder
$J_C(i) = (J_G(i), S_C(i) \oplus S_G(i))$
$\widehat{S_C(W)} = S_C(\widehat{W}) \oplus S_G(\widehat{W}) \ominus \widehat{S_G(W)}$

Figure A2. Encoder and decoder of the chosen-secret BIS model for achievability proof.

For decoding the identified user $W = i$, it first uses the component decoder to estimate $(\widehat{W}, \widehat{S_G(W)})$ and then the secret key is retrieved from

$$\widehat{S_C(W)} = S_C(\widehat{W}) \oplus S_G(\widehat{W}) \ominus \widehat{S_G(W)}, \tag{A45}$$

where $\ominus$ denotes the subtraction modulo M_S. This technique is also used in [8,11,13].

Analysis of Error Probability: For individual $W = i$, the operation at the decoder (A45) means that $(\widehat{W}, \widehat{S_C(W)}) = (W, S_C(W))$ if and only if $(\widehat{W}, \widehat{S_G(W)}) = (W, S_G(W))$. In (A16), it is 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

$$\Pr\{(\widehat{W}, \widehat{S_C(W)}) \neq (W, S_C(W)) | W = i\} \leq 4\delta \tag{A46}$$

for large enough n.

Analyses of Identification and Secret-key Rates: Equations (14) and (15) are straightforward from the parameter settings.

Analysis of Storage Rate: From (A44), the total storage rate is bounded by

$$\begin{aligned} \underbrace{I(Y;U) - I(Z;U) + R_I + 6\delta}_{\text{the rate of } J_G(i)} + \underbrace{I(Z;U) - R_I - 2\delta}_{\text{the rate of } S_C(i) \oplus S_G(i)} &= I(Y;U) + 4\delta \\ &= \frac{1}{2}\log\left(\frac{1}{\alpha}\right) + 4\delta. \end{aligned} \tag{A47}$$

Analysis of Secrecy-Leakage Rate: From the similar argument of [11] (Equation (48)), it was shown that

$$I(J_C(i);S_C(i)|\mathcal{C}_n) \le I(J_G(i);S_G(i)|\mathcal{C}_n) + \log M_S - H(S_G(i)|\mathcal{C}_n), \tag{A48}$$

and by substituting (A22) into (A48), the secrecy-leakage rate of the chosen-secret BIS model is bounded by

$$\frac{1}{n} I(J_C(i);S_C(i)|\mathcal{C}_n) \le 10\delta \tag{A49}$$

for large enough n.

Analysis of Privacy-Leakage Rate: It can be proved that

$$I(X_i^n;J_C(i)|\mathcal{C}_n) = I(X_i^n;J_G(i)|\mathcal{C}_n). \tag{A50}$$

To verify this, first one can easily see that

$$I(X_i^n;J_C(i)|\mathcal{C}_n) = I(X_i^n;J_G(i),S_C(i)\oplus S_G(i)|\mathcal{C}_n) \ge I(X_i^n;J_G(i)|\mathcal{C}_n). \tag{A51}$$

Meanwhile, by the same analogy to the development of ([11] Equation (49)), it also holds that

$$I(X_i^n;J_C(i)|\mathcal{C}_n) \le I(X_i^n;J_G(i)|\mathcal{C}_n). \tag{A52}$$

From (A51) and (A52), (A50) clearly holds. By invoking the result of (A25), from (A50), the privacy-leakage rate can also be made that

$$\frac{1}{n} I(X_i^n;J_C(i)|\mathcal{C}_n) \le R_L + \delta \tag{A53}$$

for large enough n.

Finally, by using the selection lemma [34] (Lemma 2.2), there is at least one good codebook satisfying all the conditions in Definition 2 for large enough n.

Appendix B.2. 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 and fix α such that the condition in (A35) is satisfied.

For the analyses of identification, secret-key, and privacy-leakage rates, the reader should refer to the discussions around (A32) and (A34). We argue only the bound on R_J, which is different from the one seen in the generated-secret BIS model.

Analysis of Storage Rate:

$$\begin{aligned} n(R_J+\delta) &\ge \log M_J \ge \max_{w\in\mathcal{I}} H(w) \ge H(J(W)|W) \\ &\overset{\text{(a)}}{=} I(Y_W^n, S(W); J(W)|W) = I(S(W);J(W)|W) + I(Y_W^n;J(W)|W,S(W)) \\ &\ge I(Y_W^n;J(W)|W,S(W)) \overset{\text{(b)}}{=} h(Y_W^n) - h(Y_W^n|J(W),S(W)) \\ &\overset{\text{(c)}}{\ge} \frac{n}{2}\log(2\pi e) - \frac{n}{2}\log(2\pi e\alpha) = \frac{n}{2}\log\left(\frac{1}{\alpha}\right), \end{aligned} \tag{A54}$$

where

(a) follows since $J(W)$ is a function of $(Y_W^n, S(W))$,
(b) follows as W is independent of other RVs and $S(W)$ is chosen independently of Y_W^n,
(c) follows because (A40) is applied.

Then, we have that

$$R_J \geq \frac{1}{2}\log\left(\frac{1}{\alpha}\right) - \delta. \tag{A55}$$

By letting $n \to \infty$ and $\delta \downarrow 0$, the capacity region of the chosen-secret BIS model is contained in the right-hand side of (20).

Appendix C. Convexity of the Regions $\mathcal{R}_G$ and $\mathcal{R}_C$

Here, we only verify that the region $\mathcal{R}_G$ is convex as the proof for $\mathcal{R}_C$ follows similarly. We begin with the case in which $\rho_1^2\rho_2^2 > 0$. We first define $\eta = \frac{1}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}$, and then it follows that $\alpha = \frac{1}{\rho_1^2\rho_2^2}\left(\frac{1}{\eta} - (1-\rho_1^2\rho_2^2)\right)$. Therefore, the constraints of R_J and R_L in (19) can be transformed as follows:

$$\begin{aligned} R_J &\geq \frac{1}{2}\log\left(\frac{\frac{1}{\rho_1^2\rho_2^2}\left(\frac{1}{\eta}-(1-\rho_1^2\rho_2^2)\right)\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{\frac{1}{\rho_1^2\rho_2^2}\left(\frac{1}{\eta}-(1-\rho_1^2\rho_2^2)\right)}\right)+R_I \\ &= \frac{1}{2}\log\left(\frac{\rho_1^2\rho_2^2}{1-(1-\rho_1^2\rho_2^2)\eta}\right)+R_I \\ &= -\frac{1}{2}\log\left(1-(1-\rho_1^2\rho_2^2)\eta\right)+\log|\rho_1\rho_2|+R_I, \end{aligned} \tag{A56}$$

and

$$\begin{aligned} R_L &\geq \frac{1}{2}\log\left(\frac{\frac{1}{\rho_1^2\rho_2^2}\left(\frac{1}{\eta}-(1-\rho_1^2\rho_2^2)\right)\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{\frac{1}{\rho_1^2\rho_2^2}\left(\frac{1}{\eta}-(1-\rho_1^2\rho_2^2)\right)\rho_1^2+1-\rho_1^2}\right)+R_I \\ &= \frac{1}{2}\log\left(\frac{\rho_2^2}{1-(1-\rho_2^2)\eta}\right)+R_I \\ &= -\frac{1}{2}\log\left(1-(1-\rho_2^2)\eta\right)+\log|\rho_2|+R_I. \end{aligned} \tag{A57}$$

Since $0 < |\rho_1|, |\rho_2| < 1$, and $0 < \alpha \leq 1$, it holds that $\frac{1-\rho_2^2}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2} < \frac{1-\rho_1^2\rho_2^2}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2} < 1$, indicating the values of $1-(1-\rho_1^2\rho_2^2)\eta$ and $1-(1-\rho_2^2)\eta$ are positive. Now the region in (19) can also be expressed as follows:

$$\begin{aligned} \mathcal{R}_G = \Big\{(R_I, R_S, R_J, R_L):\ & R_I + R_S \leq \frac{1}{2}\log\eta, \\ & R_J \geq -\frac{1}{2}\log\left(1-(1-\rho_1^2\rho_2^2)\eta\right)+\log|\rho_1\rho_2|+R_I, \\ & R_L \geq -\frac{1}{2}\log\left(1-(1-\rho_2^2)\eta\right)+\log|\rho_2|+R_I, \\ & R_I \geq 0,\ \ R_S \geq 0 \text{ for some } 1 \leq \eta < \frac{1}{1-\rho_1^2\rho_2^2}\Big\}. \end{aligned} \tag{A58}$$

Suppose that the rate tuples $\boldsymbol{R}^1 = (R_I^1, R_S^1, R_J^1, R_L^1)$ and $\boldsymbol{R}^2 = (R_I^2, R_S^2, R_J^2, R_L^2)$ are achievable tuples for η_1 and η_2, respectively. Without loss of generality, we assume that $1 \leq \eta_1 \leq \eta_2 < \frac{1}{1-\rho_1^2\rho_2^2}$. Next, let us consider linear combinations of these tuples. For $0 \leq \lambda \leq 1$, we have that

$$\begin{aligned}\lambda(R_I^1 + R_S^1) + (1-\lambda)(R_I^2 + R_S^2) &\leq \frac{1}{2}(\lambda \log \eta_1 + (1-\lambda)\log \eta_2)\\ &\overset{(a)}{\leq} \frac{1}{2}\log(\lambda\eta_1 + (1-\lambda)\eta_2)\\ &\overset{(b)}{=} \frac{1}{2}\log \eta', \end{aligned} \tag{A59}$$

where

(a) follows as $\log x$ $(x > 0)$ is a concave function,
(b) holds as we define $\eta' = \lambda\eta_1 + (1-\lambda)\eta_2$.

Now take a look into the bound on the storage rate

$$\begin{aligned}\lambda R_J^1 + (1-\lambda)R_J^2 &\geq -\lambda\frac{1}{2}\log\Big(1-(1-\rho_1^2\rho_2^2)\eta_1\Big) - (1-\lambda)\frac{1}{2}\log\Big(1-(1-\rho_1^2\rho_2^2)\eta_2\Big)\\ &\quad + \log|\rho_1\rho_2| + R_I\\ &\overset{(c)}{\geq} -\frac{1}{2}\log\Big(1-(1-\rho_1^2\rho_2^2)(\lambda\eta_1 + (1-\lambda)\eta_2)\Big) + \log|\rho_1\rho_2| + R_I\\ &= -\frac{1}{2}\log\Big(1-(1-\rho_1^2\rho_2^2)\eta'\Big) + \log|\rho_1\rho_2| + R_I, \end{aligned} \tag{A60}$$

where (c) follows because $f(x) = -\log(1-x)$ $(x < 1)$ is a convex function. Likewise, we can also show that

$$\lambda R_L^1 + (1-\lambda)R_L^2 \geq -\frac{1}{2}\log\Big(1-(1-\rho_2^2)\eta'\Big) + \log|\rho_2| + R_I. \tag{A61}$$

From (A59)–(A61), we see that there exists an η', where $\eta_1 \leq \eta' \leq \eta_2$, that satisfies $\lambda\boldsymbol{R}^1 + (1-\lambda)\boldsymbol{R}^2 \in \mathcal{R}_G$.

For the other case (when $\rho_1^2\rho_2^2 = 0$), the right-hand sides of each constraint in $\mathcal{R}_G$ become simpler forms, and it is easier to check that both regions are convex by applying Jensen's inequality to the logarithmic function. Accordingly, this concludes that the region $\mathcal{R}_G$ is convex.

References

1. Luis-Garcia, R.; Alberola-Lopez, C.; Aghzout, O.; Ruiz-Alzola, J. Biometric identification systems. *Signal Proces.* **2003**, *83*, 2539–2557. [CrossRef]
2. Jain, A. K.; Flynn, P.; Ross, A. *Handbook of Biometrics*; Springer: New York, NY, USA, 2009.
3. Schneier, B. Inside risks: The uses and abuses of biometrics. *Commun. ACM* **1999**, *42*, 136. [CrossRef]
4. Csisźar, I.; Narayan, P. Common randomness and secret key generation with a helper. *IEEE Trans. Inf. Theory* **2000**, *46*, 344–366. [CrossRef]
5. Willems, F.M.J.; Kalker, T.; Baggen, S.; Linnartz, J.P. On the capacity of a biometric identification system. In Proceedings of the 2003 IEEE International Symposium on Information Theory (ISIT), Yokohama, Japan, 29 June–4 July 2003; p. 82.
6. Berger, T. *Rate Distortion Theory*; Prentice-Hall: Upper Saddle River, NJ, USA, 1971.
7. Csiszár, I; Köner, J. *Information Theory—Coding Theorems for Discrete Memoryless Systems*, 2nd ed.; Cambridge University Press: Cambridge, UK, 2011.
8. Günlü, O.; Kramer, G. Privacy, Secrecy, and storage with multiple noisy measurements of identifiers. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2872–2883. [CrossRef]
9. Tuncel, E. Capacity/Storage tradeoff in high-dimensional identification systems. *IEEE Trans. Inf. Theory* **2009**, *55*, 2097–2016. [CrossRef]
10. Tuncel, E.; Gündüz, D. Identification and lossy reconstruction in noisy databases. *IEEE Trans. Inf. Theory* **2014**, *60*, 822–831. [CrossRef]
11. Ignatenko, T.; Willems, F.M.J. Fundamental limits for privacy-preserving biometric identification systems that support authentication. *IEEE Trans. Inf. Theory* **2015**, *61*, 5583–5594. [CrossRef]
12. Kittichokechai, K.; Caire, G. Secret key-based identification and authentication with a privacy constraint. *IEEE Trans. Inf. Theory* **2018**, *64*, 5879–5897. [CrossRef]

13. Yachongka, V.; Yagi, H. A new characterization of the capacity region of identification systems under noisy enrollment. In Proceedings of the 54th Annual Conference on Information Sciences and Systems (CISS), Princeton, NJ, USA, 18–20 March 2020.
14. Yachongka, V.; Yagi, H. Identification, secrecy, template, and privacy-leakage of biometric identification system under noisy enrollment. *arXiv* **2019**, arXiv: 1902.01663.
15. Zhou, L.; Vu, M.T.; Oechtering, T.J.; Skoglund, M. Two-stage biometric identification systems without privacy leakage. *IEEE J. Sel. Areas Inf. Theory* **2021**, *2*, 233–239. [CrossRef]
16. Zhou, L.; Vu, M.T.; Oechtering, T.J.; Skoglund, M. Privacy-preserving identification systems with noisy enrollment. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3510–3523. [CrossRef]
17. Ignatenko, T.; Willems, F.M.J. Biometric systems: Privacy and secrecy aspects. *IEEE Trans. Inf. Forensics Security* **2009**, *4*, 956–973. [CrossRef]
18. Lai, L.; Ho, S.-W.; Poor, H.V. Privacy-security trade-offs in biometric security systems–part I: single use case. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 122–139. [CrossRef]
19. Koide, M.; Yamamoto, H. Coding theorems for biometric systems. In Proceedings of the 2010 IEEE International Symposium on Information Theory (ISIT), Austin, TX, USA, 13–18 June 2010; pp. 2647–2651.
20. Günlü, O.; Kittichokechai, K.; Schaefer, R. F.; Caire, G. Controllable identifier measurements for private authentication with secret keys. *IEEE Trans. Inf. Forensics Secur.* **2018**, 13, 1945–1959. [CrossRef]
21. Günlü, O. Multi-entity and multi-enrollment key agreement with correlated noise. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1190–1202. [CrossRef]
22. Kusters, L.; Willems, F.M.J. Secret-key capacity regions for multiple enrollments with an SRAM-PUF. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2276–2287. [CrossRef]
23. Willems, F.M.J.; Ignatenko, T. Quantization effects in biometric systems. In Proceeding of Information Theory and Applications Workshop, San Diego, CA, USA, 8–13 February 2009; pp. 372–379.
24. Vu, M. T.; Oechtering, T. J.; and Skoglund, M. Hierarchical identification with pre-processing. *IEEE Trans. Inform. Theory* **2020**, *1*, 82–113. [CrossRef]
25. Shannon, C.E. A mathematical theory of communication. *Bell System Tech. J.* **1948**, *27*, 623–656. [CrossRef]
26. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*, 2nd ed.; John Wiley & Sons: Hoboken, NJ, USA, 2006
27. Bergmans, P. A simple converse for broadcast channels with additive white Gaussian noise. *IEEE Trans. Inf. Theory* **1978**, *20*, 279–280. [CrossRef]
28. Oohama, Y. Gaussian multiterminal source coding. *IEEE Trans. Inf. Theory* **1997**, *43*, 1912–1923. [CrossRef]
29. Kittichokechai, K.; Oechtering, T. J.; Skoglund, M.; Chia, Y.K. Secure source coding with action-dependent side information. *IEEE Trans. Inf. Theory* **2015**, *61*, 6444–6464. [CrossRef]
30. Weingarten, H.; Steinberg, Y.; Shamai (Shitz), S. The capacity region of the Gaussian MIMO broadcast channel. *IEEE Trans. Inf.Theory* **2006**, *52*, 3936–3964. [CrossRef]
31. Ignatenko, T.; Willems, F. M. J. Privacy-leakage codes for biometric authentication systems. In Proceeding of 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, Italy, 4–9 May 2014; pp. 1601–1605.
32. Yang, H.; Mihajlović, V.; Ignatenko, T. Private authentication keys based on wearable device EEG recordings. In Proceeding of 25th European Signal Processing Conference (EUSIPCO), Kos Island, Greece, 28 August–2 September 2017; pp. 956–960.
33. El Gamal, A.; Kim, Y.H. *Network Information Theory*; Cambridge University Press: Cambridge, UK, 2011
34. Bloch, M.; Barros, J. *Physical-Layer Security*; Cambridge University Press: Cambridge, UK, 2011.