Key Agreement Using Physical Identifiers for Degraded and Less Noisy Authentication Channels

Vamoua Yachongka, *Member, IEEE*, Hideki Yagi, *Member, IEEE*, and Hideki Ochiai, *Fellow, IEEE*

***Abstract*— Secret-key agreement using physical identifiers is a promising security protocol for the authentication of users and devices with small chips, owing to its lightweight security. In the previous studies, the fundamental limits of such a protocol were analyzed, and the results showed that two auxiliary random variables were involved in the capacity region expressions. However, with two auxiliary random variables, it is difficult to directly apply the expressions to derive the computable forms of the capacity regions for certain information sources such as binary and Gaussian sources, which hold importance in practical applications. In this paper, we explore the structure of authentication channels and reveal that for the classes of degraded and less noisy authentication channels, a single auxiliary random variable is sufficient to express the capacity regions. As specific examples, we use the expressions with one auxiliary random variable to derive the computable forms for binary and Gaussian sources. Numerical calculations for the Gaussian case show the trade-off between secret-key and privacy-leakage rates under a given storage rate, which illustrates how the noise in the enrollment phase affects the capacity region.**

***Index Terms*— Secret-key agreement, physical identifiers, degraded and less noisy channels, binary and Gaussian sources.**

I. Introduction

IN THE age of fast and momentous advancements in communication technologies, the number of Internet-of-Things (IoT) devices has increased remarkably. Since IoT devices equipped with small chips have resource-constrained capabilities, they may not be suitable for deploying high-profile cryptography schemes such as public-key encryption/decryption for device authentication. Lightweight security protocols handily feasible on physical layers have been receiving recent attention to a greater extent since they enable the devices to securely communicate with low latency as well as low power consumption [2].

Secret-key agreement in which physical identifiers are used as information sources to generate secret keys for authentication, called *authentication system* in this paper, has emerged as a promising candidate since it provides a low-complexity design, consumes less power, and preserves secrecy [3]. As authentication can be performed on demand, the cost is lower than that of key storage in non-volatile random access memories [4], [5]. Physical identifiers could be physical unclonable functions (PUFs), making use of intrinsic manufacturing variations of the integrated circuit to produce source sequences [6]. Several PUF designs have been proposed over the last few decades and can be largely classified into either strong PUFs or weak PUFs. We focus on weak PUFs such as static random-access memory (SRAM) PUFs and ring oscillator (RO) PUFs since they produce reliable challenge-response pairs that can be used as unique cryptographic keys for IoT device security [7]. Although generating processes are different, PUFs and biometric identifiers have several aspects in common, and nearly all assumptions and analyses of PUFs can be applied to biometric identifiers [8]. Thus, the theoretical results developed in this study should be applicable to the scenario where biometric identifiers are treated as sources.

A block diagram related to the data flows of an authentication system with PUFs is illustrated in Figure 1, and the system consists of two phases, i.e., enrollment (top) and authentication (bottom) phases. In the enrollment phase, observing a measurement of the source sequence via a channel, which is assumed to be noise-free in some previous studies, the encoder generates a pair of *secret key* and *helper data*. The helper data is shared with the decoder via a noiseless public channel to assist in the reconstruction of the secret key.[1] In the authentication phase, the decoder estimates the secret key using the helper data and another measurement observed through a channel in this phase [9], [10]. In this paper, the channels in the enrollment and the authentication phases are called the *enrollment channel* (EC) and *authentication channel* (AC), respectively. EC and AC are modeled to represent the

Manuscript received 9 October 2022; revised 12 March 2023, 4 June 2023, and 20 August 2023; accepted 20 August 2023. Date of publication 23 August 2023; date of current version 4 September 2023. This work was supported in part by the Ministry of Internal Affairs and Communications, Japan, through the Contract of "Research and Development on New Generation Cryptography for Secure Wireless Communication Services" Among "Research and Development for Expansion of Radio Wave Resources," under Grant JPJ000254; and in part by the Japan Society for the Promotion of Science (JSPS) through the Grants-in-Aid for Scientific Research (KAKENHI) under Grant JP21H04873, Grant JP20K04462, and Grant JP18H01438. An earlier version of this paper was presented in part at the 2022 IEEE Information Theory Workshop (ITW) in [DOI: 10.1109ITW54588.2022.9965800]. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Hossein Pishro-Nik. *(Corresponding author: Vamoua Yachongka.)*

Vamoua Yachongka and Hideki Ochiai are with the Department of Electrical and Computer Engineering, Yokohama National University, Yokohama, Kanagawa 240-8501, Japan (e-mail: yachongka-vamoua-fs@ynu.ac.jp; hideki@ynu.ac.jp).

Hideki Yagi is with the Department of Computer and Network Engineering, The University of Electro-Communications, Chofu, Tokyo 182-8585, Japan (e-mail: h.yagi@uec.ac.jp).

Digital Object Identifier 10.1109/TIFS.2023.3307976

[1] It is assumed that the secret key is stored in a secure database whose location is unknown to an eavesdropper; however, the eavesdropper eavesdrops on the helper data from the public database, which can be thought of as a public channel connecting the encoder and decoder, and utilizes it to examine the statistical behavior of the secret key.

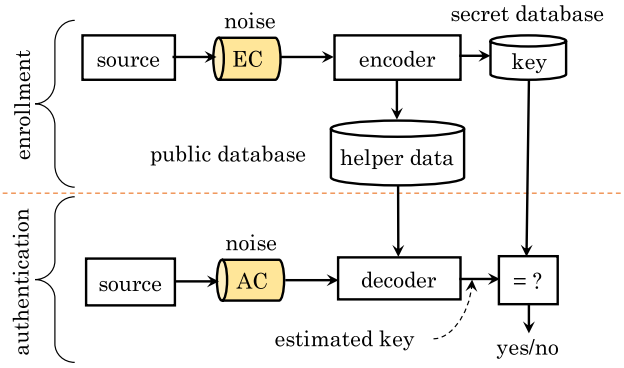

Fig. 1. A basic concept of secret-key agreement using physical and biometric identifiers [9].

noises added to the identifiers during the enrollment and authentication phases, respectively.

Relevant practical applications of the system described above include biometrics-based access control systems [11], fuzzy extractor schemes [12], [13], and field-programmable gate array (FPGA) based key generation with PUFs for IoT device authentication [14]. As a connection to physical layer security, PUFs are deployed to assist with key generation in poor scattering environments to enhance the randomness of bit sequences extracted from wireless channels, and it has been demonstrated that a higher secret-key generation rate is realizable [15].

A. Related Work

Seminal studies [9] and [10] independently investigated the fundamental limits of secret-key and privacy-leakage rates, called the *capacity region*, of the authentication systems. The capacity region elucidates the best possible trade-off between secret-key and privacy-leakage rates. The revealed trade-off may provide direct insights and serves as significant indicators for researchers seeking to design good practical codes that could achieve the largest achievable secret-key rate and the lowest implementable privacy-leakage rate for an authentication system.[2] In [9], eight different systems were taken into consideration, but among them, the generated-secret (GS) and chosen-secret (CS) models are the two major systems that are closely related to real-life applications and have been frequently analyzed in subsequent studies.[3]

The secret-key capacity increases for multiple rounds of enrollments and authentications in the GS model [16] and CS model [17] with static random-access memory PUFs (SRAM PUFs). The work [9] is extended to include a storage constraint [18], a multi-identifier scenario with joint and distributed encoding [19], and polar codes for achieving the fundamental limits [20]. All the theoretical results mentioned above [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20] are clarified under a common assumption, i.e., the EC is noiseless, and this particular model is known as a visible source model. Recently, the capacity regions of the GS and CS models have been characterized in a more realistic setting where EC is noisy [21], and this model is called a hidden source model. As an extended scenario of authentication systems, the GS and CS models that involve not only secret-key authentication but also user identification can be found in, e.g., [22], [23], and [24].

For practical code constructions on the authentication systems, some state-of-the-art approaches for binary source sequences are investigated in [25] for polar codes and in [26] for both Wyner-Ziv and nested polar codes. Compared to the simulation results in [25] and [26], better performance in terms of secret-key versus storage ratio is achieved by deploying nested randomized polar subcodes [27]. Lately, a model with non-binary sources is developed in [28] with multilevel coding, and its performance is also evaluated by taking coded modulation and shaping techniques into consideration [29].

The capacity region of a GS model with the structure of AC following the channel of the wiretap channels or two-receiver broadcast channels with confidential messages [30] was investigated in [31]. In this model, AC is composed of the channel to the encoder, referred to as the main channel, and the channel to the eavesdropper (Eve), referred to as Eve's channel. Eve can obtain not only the helper data transmitted over public channels but also a correlated sequence of the source identifiers via her channel. This setup can be viewed as the source model of key-agreement problems [32], [33], [34] with one-way communication only and a privacy constraint. The privacy constraint is imposed to minimize the information leakage of the identifiers, and in general, its analysis becomes challenging especially when the noise in the enrollment phase is taken into account [21]. An extension of the work [31] by considering noisy EC and action cost at the decoder was presented in [35], and in both [31] and [35], it was shown that the resulting expressions of the capacity regions involve two auxiliary random variables for a general class of ACs.

In a different setting, the GS and CS models with joint-measurement channels, where EC and AC are modeled as broadcast channels [36] to assume correlated noises in the measurements, were examined in [37]. Models with joint-measurement channels that incorporate Eve's channel can be found in [38]. These studies analyzed the capacity regions for some classes of broadcast channels, e.g., degraded and less noisy channels [36]. In a similar manner, we also investigate the capacity regions of the authentication systems for similar classes of channels, but the models and the point to which we direct our attention are different from those of [37] and [38]. More precisely, we deal with the models with separate measurements as in [35], and focus on the structure of AC, e.g., the main channel is less noisy than Eve's channel or Eve's channel is degraded with respect to the main channel, to simplify the expressions of the capacity regions with two auxiliary random variables that have been characterized in the paper.

[2]Note that when referring to the capacity region in the upcoming sections, it includes an extra dimension, the storage rate, along with the secret-key and privacy-leakage rates. To decrease memory usage in the public database, the storage rate should be minimized, similar to the privacy-leakage rate.

[3]The difference between the two models appears in the enrollment phases. In the GS model, the secret key is extracted from the measurement of identifiers observed at the encoder and does not need to be saved in the public database. By contrast, in the CS model, the secret key, chosen uniformly and independently of other random variables, is combined with the measurement. The combined information, which contains data relevant to the secret key but not the plain form of the key, is stored in the database so that the decoder can reliably estimate the secret key. Hence, compared with the GS model, the minimum amount of storage rate required for the CS model is larger in general. See [9, Section III] for a more comprehensive explanation.

B. Motivations

In real-life applications, the observations of PUFs and biometric identifiers are usually corrupted by noise. For instance, the measurements of PUFs' signals are affected by surrounding environments of integrated circuits such as temperature variation, change of supply voltage, and electronic noise [3], [8]. Likewise, a scanned picture of a fingerprint corresponds to a noisy version of its original image. Therefore, the assumption of the hidden source model as in [35] is considered to be a more realistic setting compared to that of the visible source model [31]. We thus adopt the setting of [35] on our model.

As we mentioned in the previous subsection, the expressions of the capacity regions of the GS and CS models characterized in [35] under a general class of AC involve two auxiliary random variables. Nevertheless, these expressions are impractical for developing the computable and tight bounds for some specific information sources and channels directly. Therefore, we explore and identify the classes of ACs that require only one auxiliary random variable for expressing the capacity regions, and use the simplified expressions to derive the computable forms for those specific sources and channels.

In this paper, we first investigate and characterize the capacity region with a single auxiliary random variable of the authentication systems for discrete sources and then apply this result to derive the capacity regions of GS and CS models for binary sources and channels. As an application of the systems with binary sources, it is well-known that SRAM-PUF responses are binary, and the outputs of sources and channels of SRAM PUFs can be modeled as binary bit sequences [16].

Furthermore, the measurements of the majority of PUFs are represented by continuous values. As an instance, the samples generated by RO PUFs obey a Gaussian distribution [39]. In addition, the noise in most communication channels is modeled as additive white Gaussian noise (AWGN). Motivated by this nature, we later extend the GS and CS models considered in [35] to characterize the capacity regions for Gaussian sources and channels.

C. Summary of Contributions

Unlike the technique used in [31] and [35], we apply information-spectrum methods [34], [40] to derive our main results. An advantage of leveraging these methods is that the argument does not depend on the size of the source alphabet, so it can also encompass continuous sources. The main contributions of this work are listed as follows:

- We demonstrate that one auxiliary random variable suffices to characterize the capacity regions of the GS and CS models when ACs are in the class of less noisy channels. Though less noisy ACs are a subclass of a general class of ACs, our results are not obtainable by a trivial reduction from the result derived in [35] under the general class of ACs.
- We apply the simplified expressions to derive the capacity regions for binary sources under less noisy ACs, which is a more general setting than the one discussed in [35, Section IV]. To obtain the tight regions, we establish a new lemma and use it to match the inner and outer bounds.
- The work [41] is extended to characterize the closed-form expressions of the capacity regions for a hidden source model. Also, numerical calculations of the Gaussian case are provided to demonstrate the trade-off between secret-key and privacy-leakage rates in the visible and hidden source models and to capture the effects of noise in the enrollment phase toward the capacity region.

D. Modeling Assumptions

We assume that each symbol in the source sequences is independently and identically distributed (i.i.d.). Techniques such as principal component analysis [42] and transform-coding-based algorithms [43] can be applied to convert biometric and physical identifiers into a vector having (nearly) independent components. However, under various environments and conditions, it may not be feasible to completely remove the correlations among symbols in the source sequence. For simplicity in the analysis, in this paper, we derive all the results under the assumption that every symbol of the source and measurement vectors is i.i.d. generated according to a joint distribution.

In principle, Eve can be classified as either a passive or active eavesdropper. In this paper, we only focus on a passive attack and do not address the issues of active attacks on PUFs, e.g., machine learning and side-channel attacks [35, Section IV]. The obtained results are analyzed under the common assumption that a PUF is capable of fending off these invasive attacks that may transform the physical features of PUF outputs permanently [8].

E. Notation and Organization

Italic uppercase A and lowercase a denote a random variable and its realization, respectively. $A^n = (A_1, \cdots, A_n)$ represents a string of random variables and subscript represents the position of a random variable in the string. $P_A(\cdot)$ denotes the probability mass function of the random variable A. $H(\cdot)$ and $H_b(\cdot)$ denote the Shannon entropy and the binary entropy function, respectively. For other notation, refer to Table I.

The rest of this paper is organized as follows: In Section II, we introduce the system models and formulate achievability definitions. Section III derives the capacity regions of the authentication systems with one auxiliary random variable, and Section IV focuses on binary and Gaussian examples. Finally, concluding remarks and future work are given in Section V.

II. System Models and Problem Formulations

A. System Models

The GS and CS models, with mathematical notations, are depicted in Figure 2. The sequences $(\tilde{X}^n, X^n, Y^n, Z^n)$ are i.i.d., and their joint distribution is factorized as $P_{\tilde{X}^n X^n Y^n Z^n} = \prod_{t=1}^n P_{\tilde{X}_t|X_t} \cdot P_{X_t} \cdot P_{Y_t Z_t|X_t}$.

Let $\mathcal{S}_n = [1 : M_S]$ and $\mathcal{J}_n = [1 : M_J]$ be the sets of secret keys and helper data, respectively. Here, M_S and M_J stand for the largest values in the sets from which secret key and helper data take values. The random vectors $\tilde{X}^n$ and (Y^n, Z^n) denote the measurements of the identifier X^n, generated from i.i.d.

TABLE I
LIST OF NOTATION

Notation	Descriptions
n	Block length
$\log x$	The natural logarithm for $x > 0$
$[k:t]$	Set $\{k, \cdots, t\}$ for integers k and t such that $k < t$
$[p, q]$	The closed interval from p to q for $p, q \in \mathbb{R}$
$p * q$	Convolution operator, defined as $p*q = p(1-q)+(1-p)q$ for $p \in [0,1]$ and $q \in [0,1]$
A_k^t	Partial sequence of A^n, i.e., $A_k^t = (A_k, \cdots, A_t)$, for any $[k:t] \subseteq [1:n]$
$I(A;B)$	Mutual information of random variables A and B
$A-B-C$	Markov chain, implying that random variables A and C are conditionally independent given B
$\mathcal{A}$, $\lvert\mathcal{A}\rvert$	A set $\mathcal{A}$, cardinality of the set $\mathcal{A}$
β	Parameter used in taking union on the capacity region for binary sources
α	Parameter used in taking union on the capacity region for Gaussian sources
ρ	Correlation coefficient between two random variables
δ, γ	Small enough positive numbers
$\mathrm{Bern}(0.5)$	Bernoulli distribution with outcome probability 0.5
$\mathcal{N}(0,\sigma^2)$	Gaussian distribution with zero mean and variance σ^2

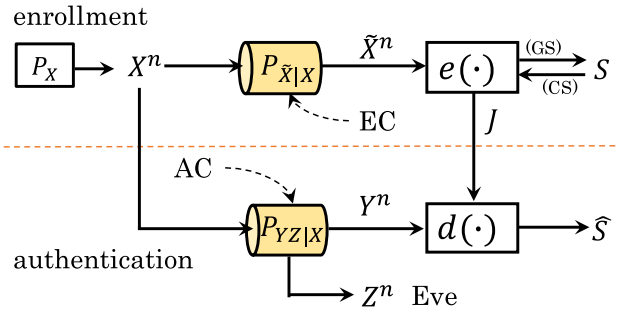

Fig. 2. System models in the presence of Eve: The arrows attached with (GS) and (CS) denote the directions of the secret keys in the GS and CS models, respectively.

source P_X, via EC $(\mathcal{X}, P_{\tilde{X}|X}, \tilde{\mathcal{X}})$ and AC $(\mathcal{X}, P_{YZ|X}, \mathcal{Y}\times\mathcal{Z})$, respectively. Assume that all alphabets $\tilde{\mathcal{X}}$, $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are finite, but this assumption will be relaxed in Section IV-B.

In the GS model, observing the measurement $\tilde{X}^n$, the encoder e generates a helper data $J \in \mathcal{J}_n$ and a secret key $S \in \mathcal{S}_n$; $(J, S) = e(\tilde{X}^n)$. The helper data J is shared with the decoder via a noiseless public channel. Detecting Y^n, the decoder d estimates the secret key generated at the encoder using Y^n and helper data J; $\widehat{S} = d(Y^n, J)$, where $\widehat{S}$ denotes an estimation of the secret key S. In the CS model, the secret key S is chosen uniformly from $\mathcal{S}_n$ and is independent of other random variables. It is embedded into the measurement $\tilde{X}^n$ to form the helper data J; $J = e(\tilde{X}^n, S)$. For the decoder, similar to the decoder of the GS model, the estimate is produced as $\widehat{S} = d(Y^n, J)$.

As the helper data J is sent over public channels, Eve can completely eavesdrop on this information. In addition to the helper data, Eve has a sequence Z^n, an output of the marginal channel $P_{Z|X}$, and both J and Z^n are exerted to learn the secret key S as well as the source identifier X^n. In essence, the information leaked to Eve regarding the identifier can not be made negligible because of the high correlation among X^n, J, and Z^n. However, it is possible to decelerate the distributions of S and (J, Z^n) and make them almost independent, so Eve may be able to recover only some insignificant bits but not the entire secret key based on the data available on her side.

B. Problem Formulations for the GS and CS Models

In this section, the formal achievability definitions of the GS and CS models are provided. We begin with the GS model.

Definition 1: A tuple of secret-key, storage, and privacy-leakage rates $(R_S, R_J, R_L) \in \mathbb{R}_+^3$ is said to be achievable for the GS model if for sufficiently small $\delta > 0$ and large enough n there exist pairs of encoders and decoders satisfying

$$\Pr\{\widehat{S} \neq S\} \leq \delta, \qquad \text{(error probability)} \quad (1)$$

$$H(S) + n\delta \geq \log M_S \geq n(R_S - \delta), \qquad \text{(secret-key)} \quad (2)$$

$$\log M_J \leq n(R_J + \delta), \qquad \text{(storage)} \quad (3)$$

$$I(S; J, Z^n) \leq \delta, \qquad \text{(secrecy-leakage)} \quad (4)$$

$$I(X^n; J, Z^n) \leq n(R_L + \delta). \qquad \text{(privacy-leakage)} \quad (5)$$

Also, $\mathcal{R}_G$ is defined as the closure of the set of all achievable rate tuples for the GS model, called the capacity region. □

The technical meaning of each constraint in Definition 1 can be interpreted as follows: Condition (1) evaluates the error probability of estimating the secret key. This is related to the reliability of the authentication systems and the probability must be bounded by a sufficiently small number δ. Equation (2) is the constraint on the secret-key rate, and the generated key should be forced to be nearly uniform in the entropy sense so as to extract as large a key size as possible. Constraint (3) is imposed to minimize the size of the local random codebook that is required for enrollment and authentication. The rate of the codebook must not exceed a given storage rate R_J.

Equation (4) measures the information leaked about the secret key to Eve, called secrecy leakage, and the secrecy leakage is evaluated under a strong secrecy criterion, which requires that the amount of leakage should be bounded by a small value regardless of the block length n. In other words, Eve can only obtain an ignorable amount of information regarding the secret key through the helper data and the correlated sequence. The last condition (5) assesses the amount of privacy leakage for the biometric or physical identifiers to Eve. In general, unlike the secrecy leakage (4), it is infeasible to make this amount vanish since the helper data itself are generated from $\tilde{X}^n$, a correlated sequence of X^n, and Z^n is also correlated to X^n. However, it is important to minimize this quantity to protect the sensitive data of users or the characteristics of PUFs embedded inside the integrated circuits of IoT devices.

The achievability definition of CS model is defined below.

Definition 2: A tuple of $(R_S, R_J, R_L) \in \mathbb{R}_+^3$ is said to be achievable for the CS model if for any $\delta > 0$ and large enough n there exist pairs of encoders and decoders satisfying all the requirements imposed in Definition 1 with replacing (2) by

$$\log M_S \geq n(R_S - \delta). \quad (6)$$

We define $\mathcal{R}_C$ as the capacity region of the CS model. □

The interpretations of the constraints in Definition 2 are the same as that in Definition 1; therefore, the details are omitted. In (6), the enforcement of the secret key to be uniform is no longer needed for the CS model as the secret key is uniformly chosen from the set $\mathcal{S}_n$.

There are other possible ways to define the secrecy-leakage and privacy-leakage in the authentication systems such as conditional entropy and variational distance. Nevertheless, in this paper, we adopt mutual information as the main metric, as in [31] and [35], so that it would be easy for us to connect our main results with those clarified in the previous studies.

C. The Capacity Regions With Two Auxiliary Random Variables

To facilitate the understanding of our main contributions in Section III, we highlight a complete characterization of the capacity regions of the GS and CS models (without action costs) derived in [35] for discrete sources.

Theorem 1 (Günlü et al. [35, Theorems 3 and 4]): The capacity regions of the GS and CS models under the general class of ACs are given by

$$\begin{aligned}\mathcal{R}_G = \bigcup_{P_{U|\tilde{X}}, P_{V|U}} \Big\{ & (R_S, R_J, R_L) \in \mathbb{R}_+^3 : \\ & R_S \le I(Y;U|V) - I(Z;U|V), \quad R_J \ge I(\tilde{X};U|Y), \\ & R_L \ge I(X;U,Y) - I(X;Y|V) + I(X;Z|V) \Big\}, \end{aligned} \tag{7}$$

$$\begin{aligned}\mathcal{R}_C = \bigcup_{P_{U|\tilde{X}}, P_{V|U}} \Big\{ & (R_S, R_J, R_L) \in \mathbb{R}_+^3 : \\ & R_S \le I(Y;U|V) - I(Z;U|V), \\ & R_J \ge I(\tilde{X};U|Y) + I(Y;U|V) - I(Z;U|V), \\ & R_L \ge I(X;U,Y) - I(X;Y|V) + I(X;Z|V) \Big\}, \end{aligned} \tag{8}$$

where auxiliary random variables U and V satisfy the Markov chain $V - U - \tilde{X} - X - (Y, Z)$ and their cardinalities are limited to $|\mathcal{V}| \le |\tilde{\mathcal{X}}| + 6$ and $|\mathcal{U}| \le (|\tilde{\mathcal{X}}| + 6)(|\tilde{\mathcal{X}}| + 5)$. □

The single-letter expressions of the regions above associate two auxiliary random variables U and V. Theorem 1 tells us that similar to the conclusion drawn in [33] for the key-agreement problem, two auxiliary random variables are required for expressing the capacity regions of the authentication systems for the general class of ACs.

In general, once the single-letter expressions for discrete sources are established, it is common to characterize a computable form of the capacity region for special cases via such expressions. However, it is challenging to directly employ the expressions in (7) and (8) so as to derive a computable form on the capacity regions for binary and Gaussian sources due to the difficulty of handling two auxiliary random variables. In the next section, we explore the classes of ACs such that the capacity regions can be expressed by one auxiliary random variable.

III. Statement of Main Results

As mentioned in the introduction, the structure of AC in the system model is similar to the channel of two-receiver broadcast channels with confidential messages. When it comes to the discussion on broadcast channels, degraded, less noisy, and more capable channels are three important classes of channels that are often discussed because the single-letter characterization for the capacity region of these types of broadcast channels is determinable [36, Chapter 5]. The class of degraded channels can be further subdivided into two classes: the classes of physically and statistically degraded channels. It is known that the latter class is larger than the former. In this section, we will take a look into each characterization of the capacity regions for these important channel classes.

Prior to the presentation of our main results, the formal definitions of physically and stochastically degraded channels, less noisy, and more capable channels [36] are defined. In order not to confuse with AC of the authentication systems, we denote the conditional probability of the channel of two-receiver broadcast channels as $P_{BC|A}(b,c|a)$ for $(a,b,c) \in \mathcal{A}\times\mathcal{B}\times\mathcal{C}$, and $P_{B|A}(b|a)$ and $P_{C|A}(c|a)$ correspond to the conditional marginal distributions of the broadcast channels.

Definition 3 Physically Degraded Channel: $(\mathcal{A}, P_{C|A}, \mathcal{C})$ *is physically degraded with respect to* $(\mathcal{A}, P_{B|A}, \mathcal{B})$ *if* $P_{BC|A}(b,c|a) = P_{B|A}(b|a) \cdot P_{C|B}(c|b)$ *for some transition probabilities* $P_{C|B}$.

(Stochastically Degraded Channel): We say that $(\mathcal{A}, P_{C|A}, \mathcal{C})$ *is stochastically degraded with respect to* $(\mathcal{A}, P_{B|A}, \mathcal{B})$ *if there exists a channel* $(\mathcal{B}, P_{C|B}, \mathcal{C})$ *such that* $P_{C|A}(c|a) = \sum_{b\in\mathcal{B}} P_{C|B}(c|b) P_{B|A}(b|a)$.

(Less Noisy Channel): $(\mathcal{A}, P_{B|A}, \mathcal{B})$ *is less noisy than* $(\mathcal{A}, P_{C|A}, \mathcal{C})$ *if* $I(B;W) \ge I(C;W)$ *for every random variables* W *such that* $W - A - (B,C)$.

(More Capable Channel): $(\mathcal{A}, P_{B|A}, \mathcal{B})$ *is more capable than* $(\mathcal{A}, P_{C|A}, \mathcal{C})$ *if* $I(A;B) \ge I(A;C)$ *for all* P_A. □

A clear relation among these classes of channels is that degraded channels are a subclass of less noisy channels, and less noisy channels are a subclass of more capable channels.

In some literature, e.g., [44], less noisy channels are called noisier channels. More precisely, it is said that $(\mathcal{A}, P_{C|A}, \mathcal{C})$ is noisier than $(\mathcal{A}, P_{B|A}, \mathcal{B})$ if for every random variables W such that $W - A - (B,C)$, we have that $I(B;W) \ge I(C;W)$. In this manuscript, we sometimes use the terms "less noisy channels" and "noisier channels" interchangeably.

In order to simplify the statement of our main results, we define five new rate regions. The following rate constraints are used in the newly defined rate regions.

$$R_S \le I(Y;U|Z), \tag{9}$$

$$R_S \le I(Y;U) - I(Z;U), \tag{10}$$

$$R_J \ge I(\tilde{X};U|Y), \tag{11}$$

$$R_J \ge I(\tilde{X};U|Z), \tag{12}$$

$$R_L \ge I(X;U|Y) + I(X;Z). \tag{13}$$

Definition 4: Rate regions of secret-key, storage, and privacy-leakage rates are defined as

$$\begin{aligned}\mathcal{A}_1 = \bigcup_{P_{U|\tilde{X}}} \Big\{ & (R_S, R_J, R_L) \in \mathbb{R}_+^3 : \text{ The auxiliary random} \\ & \text{variable } U \text{ satisfies (9), (11), and (13)} \Big\}, \end{aligned} \tag{14}$$

$$\mathcal{A}_2 = \bigcup_{P_{U|\tilde{X}}} \Big\{(R_S, R_J, R_L) \in \mathbb{R}_+^3 : \text{ The auxiliary random variable } U \text{ satisfies (9), (12), and (13)}\Big\}, \quad (15)$$

$$\mathcal{A}_3 = \bigcup_{P_{U|\tilde{X}}} \Big\{(R_S, R_J, R_L) \in \mathbb{R}_+^3 : \text{ The auxiliary random variable } U \text{ satisfies (10), (11), and (13)}\Big\}, \quad (16)$$

$$\mathcal{A}_4 = \bigcup_{P_{U|\tilde{X}}} \Big\{(R_S, R_J, R_L) \in \mathbb{R}_+^3 : \text{ The auxiliary random variable } U \text{ satisfies (10), (12), and (13)}\Big\}, \quad (17)$$

where auxiliary random variable U in the regions (14) and (15) satisfies the Markov chain $U - \tilde{X} - X - Y - Z$ and auxiliary random variable U in the regions (16) and (17) satisfies $U - \tilde{X} - X - (Y, Z)$. The cardinality of the alphabet $\mathcal{U}$ on the auxiliary random variables U in all regions above is constrained by $|\mathcal{U}| \leq |\tilde{\mathcal{X}}| + 3$. Also, define

$$\mathcal{A}_5 = \{(R_S, R_J, R_L) : \ R_S = 0, \ R_J \geq 0, \ R_L \geq I(X; Z)\}. \quad (18)$$

□

The regions $\mathcal{A}_1$ and $\mathcal{A}_2$ in Definition 4 correspond to the capacity regions of the GS and CS models when the AC is physically or statistically degraded, and the regions $\mathcal{A}_3$ and $\mathcal{A}_4$ are related to the capacity regions of the GS and CS models for less noisy ACs. The region $\mathcal{A}_5$ is used in a special case for degraded, less noisy, and Gaussian ACs, and no auxiliary random variable is involved in the expression in this region.

We start presenting our main results by showing a theorem when AC is degraded.

Theorem 2: Suppose that AC $P_{YZ|X}$ has a structure such that Eve's channel $P_{Z|X}$ is physically degraded with respect to the main channel $P_{Y|X}$, meaning that the Markov chain $X - Y - Z$ holds. The capacity regions among secret-key, storage, and privacy-leakage rates of the GS and CS models are given by

$$\mathcal{R}_G = \mathcal{A}_1, \qquad \mathcal{R}_C = \mathcal{A}_2. \quad (19)$$

Reciprocally, if the Markov chain $X - Z - Y$ holds, the regions are characterized as

$$\mathcal{R}_G = \mathcal{R}_C = \mathcal{A}_5. \quad (20)$$

□

The proof of Theorem 2 is similar to that of Theorem 3; therefore, it is omitted.

Remark 1: The capacity regions of physically and stochastically degraded ACs are given in the same form as in Theorem II-C. This is because the capacity region depends on the marginal distributions $(P_{\tilde{X}|X}, P_{Y|X}, P_{Z|X})$, and for the model considered in this paper, these distributions coincide for both physically and stochastically degraded ACs.

The following theorem states the capacity regions of the GS and CS models for less noisy ACs.

Theorem 3: If AC $P_{YZ|X}$ has a structure such that $P_{Y|X}$ is less noisy than $P_{Z|X}$, i.e., $I(Y; W) \geq I(Z; W)$ for every random variable W such that $W - X - (Y, Z)$, we have that

$$\mathcal{R}_G = \mathcal{A}_3, \qquad \mathcal{R}_C = \mathcal{A}_4. \quad (21)$$

For the case where $P_{Z|X}$ is less noisy than $P_{Y|X}$, i.e., $I(Y; W) \leq I(Z; W)$ for every W such that $W - X - (Y, Z)$, the capacity regions of the systems are provided by

$$\mathcal{R}_G = \mathcal{R}_C = \mathcal{A}_5. \quad (22)$$

□

The proof of Theorem 3 is available in Appendix A. By a similar method used in [9, Section V-A], it can be checked that both $\mathcal{R}_G$ and $\mathcal{R}_C$ are convex. In case of no presence of Eve (Z is independent of other random variables), Theorems 2 and 3 naturally reduce to the capacity regions given in [21].

Note that the assumption of less noisy channels seen in Theorem 3, i.e., $I(Y; U) \geq I(Z; U)$ (or $I(Y; U) \leq I(Z; U)$), is satisfied for every U satisfying the Markov chain $U - \tilde{X} - X - (Y, Z)$. This fact is utilized in the proof of this theorem.

Remark 2: The class of more capable channels includes less noisy channels as a special case [36]. When the AC is in the class of more capable channels, i.e., $I(X; Y) \geq I(X; Z)$ or $I(X; Y) \leq I(X; Z)$, it is not yet known whether the capacity region can be characterized by one auxiliary random variable. More specifically, due to the impact of noise on the enrollment phase, the condition $I(X; Y) \geq I(X; Z)$ does not guarantee that $I(Y; U) \geq I(Z; U)$ and $I(\tilde{X}; Y) \geq I(\tilde{X}; Z)$, making it difficult to identify the sign in the right-hand side of the secret-key rate constraint in (10). The same observation applies to the case in which $I(X; Y) \leq I(X; Z)$.

An observation from the theorems and remarks shown above is that in the wiretap channels, the fundamental limits, e.g, the capacity-equivocation regions, depend on the channel $P_{YZ|X}$ only through the marginal distributions of the main channel $P_{Y|X}$ and Eve's channel $P_{Z|X}$ [45]. This conclusion may be applicable to a visible source model of the authentication systems. However, for the settings of hidden source model, the capacity regions are hinged on by not only the marginal distributions of AC $P_{YZ|X}$ but also the EC $P_{\tilde{X}|X}$.

IV. Examples

A. Binary Sources

In this section, the characterization of a binary example for Theorem 3 in the case where Eve's channel is noisier than the main channel is presented.

Consider the source random variable $X \sim \text{Bern}(\frac{1}{2})$, $P_{\tilde{X}|X}$ is a binary symmetric channel with crossover probability $p \in [0, 1/2]$, $P_{Y|X}$ is a binary erasure channel with an erasure probability $q \in [0, 1]$, and $P_{Z|X}$ is a binary symmetric channel with crossover probability $\epsilon \in [0, 1/2]$. Note that if the relation of ϵ and q is such that $2q < \epsilon < 4q(1 - q)$, $P_{Y|X}$ is less noisy than $P_{Z|X}$, but $P_{Y|X}$ is not a degraded version of $P_{Z|X}$. An illustration of this setting is described in Figure 3.

Let the test channel $P_{U|\tilde{X}}$ be a binary symmetric channel with crossover probability $\beta \in [0, 1/2]$. The optimal rate regions of the GS and CS models in this case are given below.

Theorem 4: For binary sources when the main channel is less noisy than Eve's channel, the capacity regions of the GS

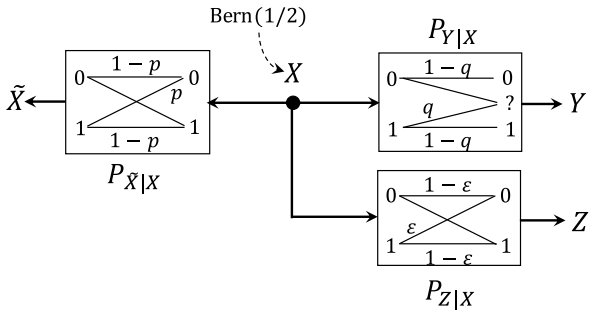

Fig. 3. Transition probabilities of each channel for binary example.

and CS models are given as

$$\mathcal{R}_G = \bigcup_{0\le\beta\le 1/2} \Big\{(R_S, R_J, R_L) \in \mathbb{R}_+^3 : R_S \le H_b(\beta * p * \epsilon) - (1-q)H_b(\beta * p) - q, \; R_J \ge q + (1-q)H_b(\beta * p) - H_b(\beta), \; R_L \ge 1 + q - qH_b(\beta * p) - H_b(\epsilon)\Big\}, \tag{23}$$

$$\mathcal{R}_C = \bigcup_{0\le\beta\le 1/2} \Big\{(R_S, R_J, R_L) \in \mathbb{R}_+^3 : R_S \le H_b(\beta * p * \epsilon) - (1-q)H_b(\beta * p) - q, \; R_J \ge H_b(\beta * p * \epsilon) - H_b(\beta), \; R_L \ge 1 + q - qH_b(\beta * p) - H_b(\epsilon)\Big\}, \tag{24}$$

where the convolution operation $*$ is defined as $x * y = x(1-y) + (1-x)y$ for $x \in [0,1]$ and $y \in [0,1]$. □

The proof of Theorem 4 is given in Appendix C. In [35], the rate region of the GS model for binary sources was derived under the assumptions that $\tilde{X} = X$ (EC is noiseless) and the AC is physically degraded, i.e., the Markov chain $X - Y - Z$ holds. Theorem 4 is provided under a more general setting, and the key idea for deriving this theorem is to apply Mrs. Gerber's Lemma [46] in the reverse direction of Eve's channel to obtain an upper bound on the conditional entropy $H(Z|U)$. However, the obtained bound is not yet tight. We establish a simple lemma (Lemma 3) to acquire the optimal upper bound on $H(Z|U)$ to match the outer region with the inner region.

B. Scalar Gaussian Sources

Unlike the discrete sources, for Gaussian sources, we provide the capacity regions of the system for a general class of Gaussian ACs. A picture of data flows for Gaussian sources is depicted at the top of Figure 4. Assume that the source is given by $X \sim \mathcal{N}(0,1)$, and the channels $P_{\tilde{X}|X}$, $P_{Y|X}$, and $P_{Z|X}$ are modeled as

$$\tilde{X} = \rho_1 X + N_1, \;\; Y = \rho_2 X + N_2, \;\; Z = \rho_3 X + N_3, \tag{25}$$

where $|\rho_1|, |\rho_2|, |\rho_3| < 1$ are the correlation coefficients of each channel, $N_1 \sim \mathcal{N}(0, 1-\rho_1^2)$, $N_2 \sim \mathcal{N}(0, 1-\rho_2^2)$, and $N_3 \sim \mathcal{N}(0, 1-\rho_3^2)$ are Gaussian random variables, and independent of each other and of other random variables.

Using a technique of transforming the exponent part of the joint distributions used in [47] or covariance matrix

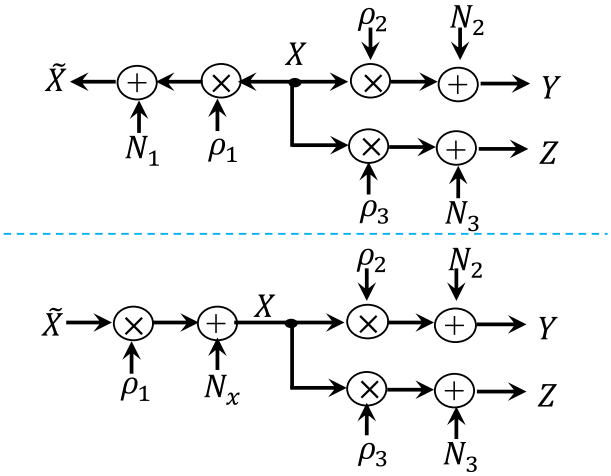

Fig. 4. Data flows of the original system model (top) and transformed one (bottom) for Gaussian sources and channels.

transformations in [34, Appnedix C.1], (25) can be rewritten as

$$X = \rho_1 \tilde{X} + N_x, \;\; Y = \rho_2 X + N_2, \;\; Z = \rho_3 X + N_3, \tag{26}$$

where $N_x \sim \mathcal{N}(0, 1-\rho_1^2)$ and is independent of other random variables. A depiction of the data flows for (26) is displayed at the bottom of Figure 4, and the capacity regions for Gaussian sources are derived via (26) instead of (25). The result is given below.

Theorem 5: Under the condition of $\rho_2^2 > \rho_3^2$, i.e., $\tilde{X} - X - Y - Z$ (cf. [34, Lemma 6]), the capacity regions of the GS and CS models for Gaussian sources are given by

$$\mathcal{R}_G = \bigcup_{P_{U|\tilde{X}}} \Big\{(R_S, R_J, R_L) \in \mathbb{R}_+^3 : \text{The auxiliary random variable } U \text{ satisfies (9), (11), and (13)}\Big\}, \tag{27}$$

$$\mathcal{R}_C = \bigcup_{P_{U|\tilde{X}}} \Big\{(R_S, R_J, R_L) \in \mathbb{R}_+^3 : \text{The auxiliary random variable } U \text{ satisfies (9), (12), and (13)}\Big\}, \tag{28}$$

where auxiliary random variable U satisfies the Markov chain $U - \tilde{X} - X - Y - Z$. Unlike Theorem 2, the random variable U is a continuous random variable and its cardinality is unbounded. For the case of $\rho_2^2 \le \rho_3^2$, i.e., $\tilde{X} - X - Z - Y$, the regions are characterized in the same form

$$\mathcal{R}_G = \mathcal{R}_C = \mathcal{A}_5. \tag{29}$$

□

Theorem 5 can be proved by a similar method for deriving Theorem 3, and thus we omit the detailed proof. In Theorems 2, 3, and 5, when the structure of ACs is such that the main channel is degraded with respect to Eve's channel or is noisier than Eve's one, the capacity regions of the GS and CS models are given in the same form. The secret-key generation at a positive rate is not possible, and the minimum value of the storage rates is zero, but that of the privacy-leakage rate can still be positive depending on the joint marginal densities of (X, Z). Even when the encoding procedure is not needed, e.g., U is set to be a constant, the

information leaked to Eve via her channel $P_{Z|X}$ is at minimum rate $I(Z;X)$, which is equal to the capacity of this channel. This quantity corresponds to an uncontrollable amount of the privacy-leakage rate at the encoder, and it is avoidable if the privacy-leakage rate is constrained by conditional mutual information, i.e., $I(X^n;J|Z^n)$, as in [48].

Note that due to the unbounded cardinality of the auxiliary random variable, the regions in (27) and (28) are not directly computable. Next, we show that the parametric forms, i.e., computable expressions, of Theorem 5 are determined by a single parameter. The parameter α which appears in the following corollary acts as an adjusting parameter for the variance of the auxiliary random variable U. Unlike random variables $(\tilde{X}, X, Y, Z)$, in which their variances are always one, the auxiliary random variable U could be any Gaussian random variable with a variance in the range $(0, 1]$.

Corollary 1: When the condition $\rho_2^2 > \rho_3^2$ is satisfied, we can compute the regions in (27) and (28) as

$$\begin{aligned}\mathcal{R}_G = \bigcup_{\alpha\in(0,1]} \Big\{&(R_S, R_J, R_L) \in \mathbb{R}_3^+ : \\ &R_S \le \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_3^2+1-\rho_1^2\rho_3^2}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}\right), \\ &R_J \ge \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{\alpha}\right), \\ &R_L \ge \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{(\alpha\rho_1^2+1-\rho_1^2)(1-\rho_3^2)}\right)\Big\}, \end{aligned} \tag{30}$$

$$\begin{aligned}\mathcal{R}_C = \bigcup_{\alpha\in(0,1]} \Big\{&(R_S, R_J, R_L) \in \mathbb{R}_3^+ : \\ &R_S \le \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_3^2+1-\rho_1^2\rho_3^2}{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}\right), \\ &R_J \ge \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_3^2+1-\rho_1^2\rho_3^2}{\alpha}\right), \\ &R_L \ge \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{(\alpha\rho_1^2+1-\rho_1^2)(1-\rho_3^2)}\right)\Big\}, \end{aligned} \tag{31}$$

respectively, and that of (29) is given as

$$\begin{aligned}\mathcal{R}_G = \mathcal{R}_C = \Big\{&(R_S, R_J, R_L) : \ R_S = 0, \quad R_J \ge 0, \\ &R_L \ge \frac{1}{2}\log\left(\frac{1}{1-\rho_3^2}\right)\Big\}. \end{aligned} \tag{32}$$

□

The full proof of Corollary 1 is available in [1, Appendix D] and the convexity of these regions is verified in [1, Appendix E]. When EC is noiseless (i.e., $\rho_1^2 \to 1$), Corollary 1 reduces to the parametric forms derived in [41, Corollary 1]. In addition, when Eve can observe only the helper data, corresponding to the case in which Z is independent of other random variables ($\rho_3^2 = 0$), Corollary 1 matches with the parametric expressions of the GS and CS models provided in [47, Corollary 1].

C. Behaviors of the Capacity Region for Gaussian Sources

In this section, we investigate the ultimate (asymptotic) limits of the secret-key and privacy-leakage rates and provide some numerical results under Gaussian sources. For brevity, we focus only on the GS model.

First, we find expressions for the optimal secret-key and privacy-leakage rates under a fixed condition of R_J for the hidden source model. Let us fix the storage rate

$$R_J^\alpha = \frac{1}{2}\log\left(\frac{\alpha\rho_1^2\rho_2^2+1-\rho_1^2\rho_2^2}{\alpha}\right), \tag{33}$$

equivalent to $\alpha = \frac{1-\rho_1^2\rho_2^2}{e^{2R_J^\alpha}-\rho_1^2\rho_2^2}$. Now define two rate functions

$$\begin{aligned} R_S^*(R_J^\alpha) &= \max_{(R_S,R_J^\alpha,R_L)\in\mathcal{R}_G} R_S, \\ R_L^*(R_J^\alpha) &= \min_{(R_S,R_J^\alpha,R_L)\in\mathcal{R}_G} R_L. \end{aligned} \tag{34}$$

Using the value of α, we can write that

$$\begin{aligned} R_S^*(R_J^\alpha) &= \frac{1}{2}\log\left(\frac{1-\rho_1^2\rho_3^2-\rho_1^2(\rho_2^2-\rho_3^2)e^{-2R_J^\alpha}}{1-\rho_1^2\rho_2^2}\right), \\ R_L^*(R_J^\alpha) &= \frac{1}{2}\log\left(\frac{1-\rho_1^2\rho_2^2}{(1-\rho_3^2)(1-\rho_1^2+\rho_1^2(1-\rho_2^2)e^{-2R_J^\alpha})}\right). \end{aligned} \tag{35}$$

The asymptotic limits of secret-key and privacy-leakage rates when R_J^α tends to infinity are given by

$$\begin{aligned} \lim_{R_J^\alpha\to\infty} R_S^*(R_J^\alpha) &= \frac{1}{2}\log\left(\frac{1-\rho_1^2\rho_3^2}{1-\rho_1^2\rho_2^2}\right) = I(Y;\tilde{X}|Z), \\ \lim_{R_J^\alpha\to\infty} R_L^*(R_J^\alpha) &= \frac{1}{2}\log\left(\frac{1-\rho_1^2\rho_2^2}{(1-\rho_1^2)(1-\rho_3^2)}\right) \\ &= I(X;\tilde{X}|Y) + I(X;Z). \end{aligned} \tag{36}$$

For the visible source model, the asymptotic limits of secret-key and privacy-leakage rates for a given storage rate are determinable by substituting $\rho_1^2 = 1$ into (36), i.e.,

$$\begin{aligned} \lim_{\tilde{R}_J^\alpha\to\infty} \tilde{R}_S^*(\tilde{R}_J^\alpha) &= \frac{1}{2}\log\left(\frac{1-\rho_3^2}{1-\rho_2^2}\right) = I(X;Y|Z), \\ \lim_{\tilde{R}_J^\alpha\to\infty} \tilde{R}_L^*(\tilde{R}_J^\alpha) &= \lim_{\tilde{R}_J^\alpha\to\infty}\left(\frac{1}{2}\log\left(\frac{1}{1-\rho_3^2}\right)+\tilde{R}_J^\alpha\right)\to\infty, \end{aligned} \tag{37}$$

where $\tilde{R}_J^\alpha = \frac{1}{2}\log\left(\frac{\alpha\rho_2^2+1-\rho_2^2}{\alpha}\right)$ and $\tilde{R}_S^*(\tilde{R}_J^\alpha)$ and $\tilde{R}_L^*(\tilde{R}_J^\alpha)$ are defined in the same manner as (34) and correspond to the maximum secret-key rate and the minimum privacy-leakage rate for this model under fixed $\tilde{R}_J^\alpha$. One can see that in the second equation of (37), the optimal value of the privacy-leakage rate increases linearly with the storage rate.

Next, we provide some numerical calculations of the region $\mathcal{R}_G$ in (30), and take a look into special points of both the visible source model ($\rho_1^2 = 1$) and hidden source model ($\rho_1^2 < 1$). The following two scenarios are considered.

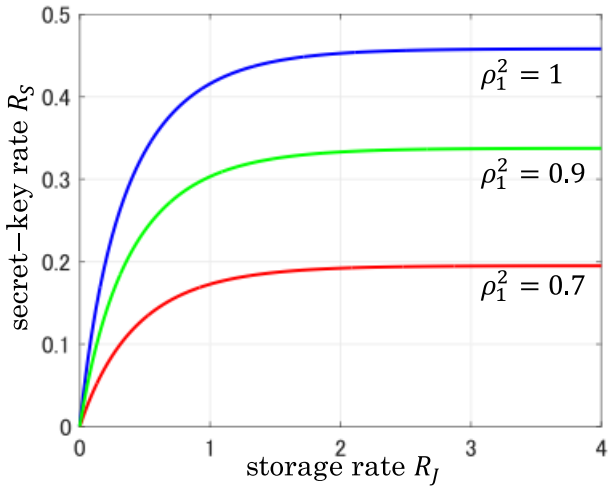

Fig. 5. Projection of the capacity region $\mathcal{R}_G$ in (30) with different ρ_1^2 onto $R_J R_S$-plane.

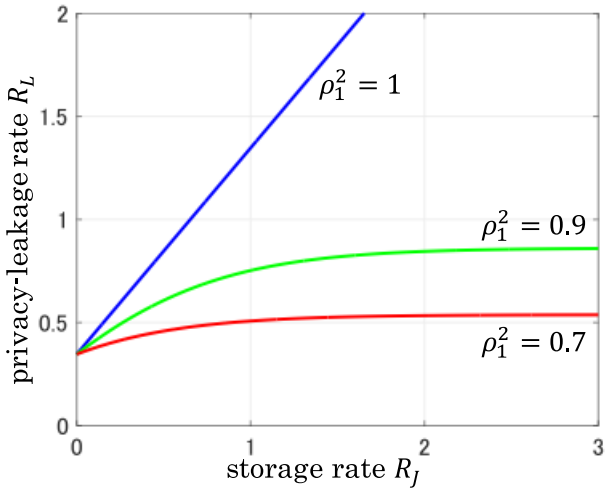

Fig. 6. Projection of the capacity region $\mathcal{R}_G$ in (30) with different ρ_1^2 onto $R_J R_L$-plane.

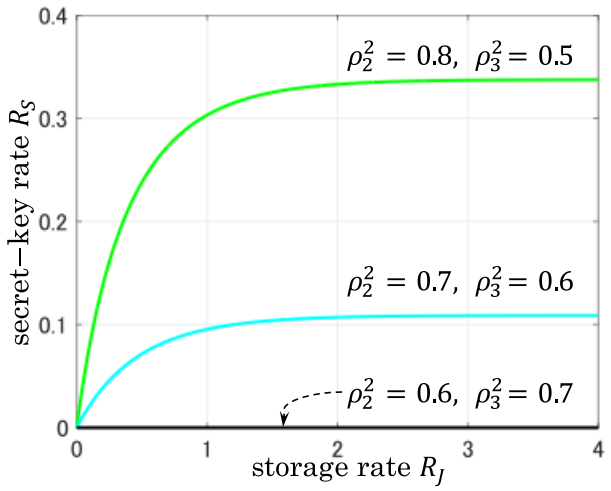

Fig. 7. Projection of the capacity region $\mathcal{R}_G$ in (30) with different ρ_2^2 and ρ_3^2 onto $R_J R_S$-plane.

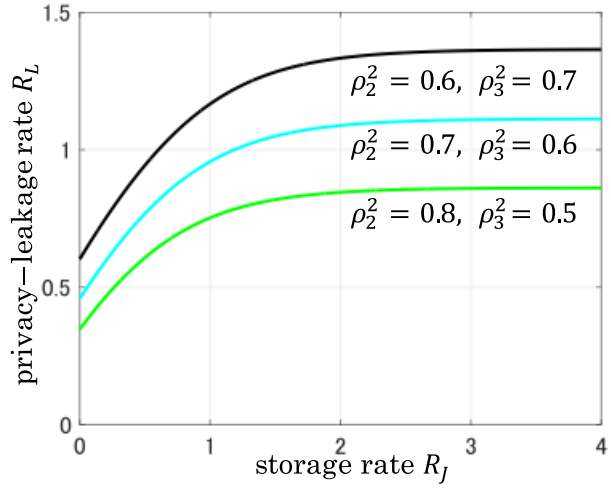

Fig. 8. Projection of the capacity region $\mathcal{R}_G$ in (30) with different ρ_2^2 and ρ_3^2 onto $R_J R_L$-plane.

1) ρ_1^2 varies over three values 1.0, 0.9, and 0.7, but (ρ_2^2, ρ_3^2) is fixed at (0.8, 0.5). This is the case where the probability of enrollment channel $P_{\tilde{X}|X}$ could be changed, but that of the authentication channel $P_{YZ|X}$ remains the same.
2) ρ_1^2 is fixed at 0.9, but (ρ_2^2, ρ_3^2) could be either one of the pairs (0.8, 0.5), (0.7, 0.6), or (0.6, 0.7). This is the opposite example of Scenario 1).

Figures 5 and 6 plot the optimal values between secret-key and storage rates $(R_J^\alpha, R_S^*(R_J^\alpha))$ and privacy-leakage and storage rates $(R_J^\alpha, R_L^*(R_J^\alpha))$, respectively, for Scenario 1). Figures 7 and 8 illustrate the relations of the same rate pairs for Scenario 2). These figures are obtained by calculating the values of R_J^α defined in (33), and $R_S^*(R_J^\alpha)$ and $R_L^*(R_J^\alpha)$ defined in (35) with respect to the parameter α. In this calculation, we set the step size of α to be 10^{-5}, which was found to be sufficiently small for numerical implementation.

From Figures 5 and 6, the visible source model produces a better secret-key rate but leaks more privacy of physical identifiers to Eve compared to the performances of the hidden source model. More precisely, the asymptotic values of secret-key rate are $\lim_{R_J^\alpha \to \infty} R_S^*(R_J^\alpha) = \frac{1}{2}\log(\frac{5}{2}) = 0.458$ nats, 0.338 nats, and 0.195 nats when ρ_1^2 is equal to 1.0, 0.9, and 0.7, respectively. This indicates that when ρ_1^2 decreases, implying that the noise introduced to the identifiers in the enrollment phase increases, the secret-key rate becomes smaller.

Conversely, in terms of the privacy-leakage rate, the asymptotic limits become $\lim_{R_J^\alpha \to \infty} R_L^*(R_J^\alpha) \to \infty$, 0.861 nats, and 0.538 nats when ρ_1^2 is equal to 1.0, 0.9, and 0.7, respectively. Evidently, when ρ_1^2 is low, less information about the identifiers leaks to Eve. By the reason that the noise in the enrollment phase serves as a fixed filter [49] to obscure the privacy of identifiers, when ρ_1^2 is small (the variance of noise added to the identifiers in the EC is large), the amount of information leaked to Eve is also small. By contrast, when ρ_1^2 approaches 1, the effectiveness of the filter is lessened, and the hidden source model behaves similarly to the visible source model. Thus, a larger amount of privacy of the identifiers could be leaked.

For Scenario 2), Figures 7 and 8 show that the achievable secret-key rate gradually decreases and the privacy-leakage rate rises as the value of ρ_2^2 declines and that of ρ_3^2 increases, which can explicitly be verified by comparing two distinct

values of the secret-key and privacy-leakage rates in (35) with different pairs (ρ_2^2, ρ_3^2) under the same storage rate. These behaviors suggest that when the noise variance of the measurements observed through the main channel is large, corresponding to the case where a low-quality quantizer, e.g., quantizer with few quantization levels, is deployed at the decoder, it leads to a small secret-key generation rate and a high privacy-leakage rate. This effect becomes particularly remarkable when Eve uses a high-quality quantizer.

In the authentication systems, it is favored for achieving a high secret-key rate while maintaining low storage and privacy-leakage rates, but these simulation results reflect the difficulty of achieving such a tuple simultaneously. Therefore, to prevent a circumstance such that a significant loss of privacy occurs, it may be important not only to focus on increasing the gain for the secret-key rate but also to weigh its balance with the storage and privacy-leakage rates as well when designing practical codes for an authentication system.

V. Conclusion

In this paper, we investigated the classes of ACs for which the capacity regions of the GS and CS models can be characterized by one auxiliary random variable. The obtained results revealed that only a single auxiliary random variable is required to characterize the capacity regions for degraded and less noisy ACs. Moreover, the capacity regions of the authentication systems for both binary and Gaussian sources were derived. All the expressions derived in this work are not only tight but also readily computable. They may serve as a performance benchmark when practical channel codes such as LDPC and polar codes are constructed for the authentication systems as in [25] for a visible source model. We also provided some numerical calculations for the Gaussian case to demonstrate the impact of noise in the enrollment phase on the capacity region as well as to examine the trade-off between secret-key and privacy-leakage rates for a given storage rate.

For future work, a natural extension of this work is to investigate whether polar codes can achieve all the rate points in the capacity region of binary sources. In fact, for the typical key-agreement problem [20], polar codes were shown to achieve the fundamental limits by exploiting the degraded and less noisy properties of the main and Eve's channels. Due to the similarities of the key-agreement problem and our model, it may be possible to demonstrate that the code achieves the fundamental limits of the authentication systems as well. Furthermore, extending the results in Section IV-B to vector Gaussian case is another interesting research topic.

Appendix A
Proof of Theorem 3

This appendix deals with the proof of the capacity regions for less noisy ACs. We only provide the proof of (21) since that of (22) follows similarly by simply setting the auxiliary random variable U to be constant. The entire proof is divided into two parts, namely, the converse and achievability parts. For the converse part, the derivation of each rate constraint for the GS and CS models is discussed in detail, while in the achievability part, only the key point is addressed.

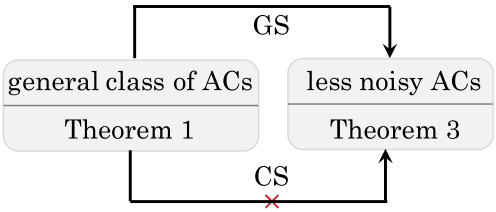

Fig. 9. The possibility of a reduction in Theorem 1 to obtain the outer regions of GS and CS models for less noisy ACs.

A. Converse Part

Note that following the same technique used in [35], the capacity regions derived under the general class of ACs also hold for less noisy ACs. Figure 9 illustrates the possibility of a direct deduction of the capacity regions of the GS and CS models for less noisy ACs via the expressions with two auxiliary random variables that we have seen in Theorem 1.

More specifically, it is possible to derive the outer region on $\mathcal{R}_G$ in Theorem 3 directly via the region in (7) by exploiting the long Markov chain $V - U - \tilde{X} - X - (Y, Z)$, as shown in Figure 10, and the property of less noisy channels, but the same approach cannot be applied to the CS model. In the proof, we demonstrate the proofs of the GS and CS models via different approaches. The proof begins with the GS model and follows by the detailed argument of the CS model.

Converse Proof of GS Model: Since the bounds on R_J in both the regions in (7) and (21) remain unchanged, we need to check the constraints on the secret-key and privacy-leakage rates. Transform the bound on the secret-key rate as follows:

$$\begin{aligned} R_S &\le I(Y;U|V) - I(Z;U|V) \\ &\overset{(a)}{=} I(Y;U) - I(Y;V) - (I(Z;U) - I(Z;V)) \\ &= I(Y;U) - I(Z;U) - (I(Y;V) - I(Z;V)) \\ &\overset{(b)}{\le} I(Y;U) - I(Z;U), \end{aligned} \tag{38}$$

where (a) follows by the Markov chains $V-U-Y$ and $V-U-Z$, derivable from the Markov chain $V - U - \tilde{X} - X - (Y, Z)$ (cf. Figure 10), and (b) follows because less noisy ACs fulfill the condition $I(Y;V) \ge I(Z;V)$ for every $V - X - (Y, Z)$.

Likewise, for the bound on the privacy-leakage rate, we have

$$\begin{aligned} R_L &\ge I(X;U,Y) - I(X;Y|V) + I(X;Z|V) \\ &\overset{(a)}{=} I(X;U,Y) - (I(X;Y) - I(Y;V)) \\ &\quad + I(X;Z) - I(Z;V) \\ &= I(X;U|Y) + I(X;Y) - (I(X;Y) - I(Y;V)) \\ &\quad + I(X;Z) - I(Z;V) \\ &= I(X;U|Y) + I(X;Z) + I(Y;V) - I(Z;V) \\ &\overset{(b)}{\ge} I(X;U|Y) + I(X;Z), \end{aligned} \tag{39}$$

where (a) is due to the Markov chain $V - X - (Y, Z)$ and (b) is due to the property that $I(Y;V) \ge I(Z;V)$ for less noisy ACs. Hence, the converse proof of the GS model is attained. □

Converse Proof of CS Model: Observe that the right-hand side of the storage rate of the CS model with two auxiliary

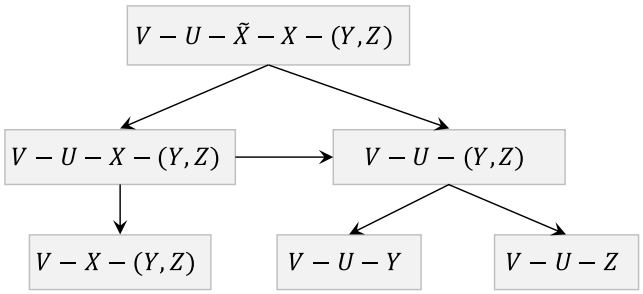

Fig. 10. Some shorter Markov chains that can be derived from the long Markov chain in Theorem 1.

random variables can be reshaped as

$$\begin{aligned} R_J &\geq I(\tilde{X};U|Y)+I(Y;U|V)-I(Z;U|V) \\ &\overset{(a)}{=} I(\tilde{X};U)-I(Y;U)+I(Y;U)-I(Y;V) \\ &\quad -(I(Z;U)-I(Z;V)) \\ &= I(\tilde{X};U)-I(Z;U)-(I(Y;V)-I(Z;V)) \\ &\overset{(b)}{=} I(\tilde{X};U|Z)-(I(Y;V)-I(Z;V)), \end{aligned} \tag{40}$$

where (a) is due to the Markov chains $U-\tilde{X}-Y$ and $V-U-(Y,Z)$, and (b) follows from the Markov chain $U-\tilde{X}-Z$.

In (40), since $I(Y;V)\geq I(Z;V)$ for less noisy ACs, this lower bound cannot be further reduced to the one seen in (12). We cannot apply the technique used for the GS model to derive the outer bound directly from the region with two auxiliary random variables (cf. eq. (8)) for the CS model, and thus an alternative approach is required. Here, we make use of a standard technique that relies on the assumption of auxiliary random variables and Fano's inequality.

Suppose that a rate tuple (R_S, R_J, R_L) is achievable, implying that there exists a pair of encoders and decoders such that all requirements in Definition 2 are satisfied for small enough $\delta>0$ and block length $n\geq n_0$ $(n_0\geq 1)$. For $t\in[1:n]$, define auxiliary random variables $U_t=(J,S,Y_{t+1}^n,Z^{t-1})$ and $V_t=(J,Y_{t+1}^n,Z^{t-1})$. Under these settings, it is easy to verify that the Markov chain $V_t-U_t-\tilde{X}_t-X_t-(Y_t,Z_t)$ is satisfied.

Analysis of Secret-key Rate: Define $\delta_n=\frac{1}{n}(1+\delta\log M_S)$, and this quantity is related to an upper bound of Fano's inequality. From (6), the secret-key rate can be bounded by

$$\begin{aligned} n(R_S-\delta) &\leq \log M_S = H(S) \\ &\overset{(a)}{\leq} \sum_{t=1}^{n}\{I(Y_t;U_t|V_t)-I(Z_t;U_t|V_t)\}+n(\delta_n+\delta) \\ &\overset{(b)}{=} \sum_{t=1}^{n}\{I(Y_t;U_t)-I(Z_t;U_t)-(I(Y_t;V_t) \\ &\qquad -I(Z_t;V_t))\}+n(\delta_n+\delta) \\ &\overset{(c)}{\leq} \sum_{t=1}^{n}\{I(Y_t;U_t)-I(Z_t;U_t)\}+n(\delta_n+\delta), \end{aligned} \tag{41}$$

where (a) is due to a similar argument in [21, eq. (40)], (b) holds since the Markov chains $V_t-U_t-Y_t$ and $V_t-U_t-Z_t$ are applied, and (c) follows from the Markov chain $V_t-U_t-(Y_t,Z_t)$ and the property of less noisy channels that $I(Y_t;V_t)\geq I(Z_t;V_t)$ for any random variable V_t such that $V_t-X_t-(Y_t,Z_t)$.

Analysis of Storage Rate: For the CS model, note that the secret key S is independent of random variables $(\tilde{X}^n,X^n,Y^n,Z^n)$, and the helper data J is a function of $(\tilde{X}^n,S)$. From (3), we have that

$$\begin{aligned} &n(R_J+\delta) \\ &\geq \log M_J \geq H(J)=I(\tilde{X}^n,S;J) \\ &= I(\tilde{X}^n,S;J,Z^n)-I(\tilde{X}^n,S;Z^n|J) \\ &\geq I(\tilde{X}^n;J,Z^n|S)-I(\tilde{X}^n;Z^n|J,S) \\ &\overset{(a)}{=} I(\tilde{X}^n;J,Z^n|S)-H(Z^n|J,S)+H(Z^n|\tilde{X}^n) \\ &\geq I(\tilde{X}^n;J,Z^n|S)-I(\tilde{X}^n;Z^n) \\ &= I(\tilde{X}^n;J|Z^n,S)+I(\tilde{X}^n;Z^n|S)-I(\tilde{X}^n;Z^n) \\ &= I(\tilde{X}^n;J|S,Z^n)=H(\tilde{X}^n|Z^n)-H(\tilde{X}^n|J,S,Z^n) \\ &= \sum_{t=1}^{n}\{H(\tilde{X}_t|Z_t)-H(\tilde{X}_t|\tilde{X}^{t-1},J,S,Z^n)\} \\ &\overset{(b)}{=} \sum_{t=1}^{n}\{H(\tilde{X}_t|Z_t)-H(\tilde{X}_t|\tilde{X}^{t-1},J,S,Z^n,Y_{t+1}^n)\} \\ &\overset{(c)}{\geq} \sum_{t=1}^{n}\{H(\tilde{X}_t|Z_t)-H(\tilde{X}_t|J,S,Y_{t+1}^n,Z^t)\} \\ &= \sum_{t=1}^{n}\{H(\tilde{X}_t|Z_t)-H(\tilde{X}_t|Z_t,U_t)\}=\sum_{t=1}^{n}I(\tilde{X}_t;U_t|Z_t), \end{aligned} \tag{42, 43}$$

where (a) is due to the Markov chain $Z^n-(\tilde{X}^n,S)-J$ and S is independent of other random variables, (b) is due to the Markov chain $\tilde{X}_t-(\tilde{X}^{t-1},J,S,Z^n)-Y_{t+1}^n$, and (c) follows because conditioning reduces entropy.

Analysis of Privacy-Leakage Rate: We can develop the right-hand side of (5) as

$$\begin{aligned} n(R_L+\delta) &\geq I(X^n;J,Z^n) \\ &= I(X^n;J,S,Z^n)-I(X^n;S|J,Z^n) \\ &\geq I(X^n;J,S,Z^n)-H(S) \\ &= I(X^n;J,S|Z^n)+nI(X;Z)-H(S) \\ &= I(X^n;J|S,Z^n)+nI(X;Z)-H(S) \\ &\overset{(a)}{\geq} \sum_{t=1}^{n}I(X_t;U_t|Z_t)+nI(X;Z)-H(S) \\ &\overset{(b)}{\geq} \sum_{t=1}^{n}I(X_t;U_t|Y_t)+nI(X;Z)-n(\delta_n+\delta), \end{aligned} \tag{44}$$

where (a) follows from similar steps between (42) and (43), and (b) follows since $H(S)$ is upper bounded by the last inequality in (41).

The proof wraps up with the standard argument for single letterization using a time-sharing random variable Q, where the random variable Q is uniformly distributed on $[1:n]$ and independent of other random variables. More specifically, define $X=X_Q$, $\tilde{X}=\tilde{X}_Q$, $Y=Y_Q$, $Z=Z_Q$, and $U=(U_Q,Q)$, so that $U-\tilde{X}-X-(Y,Z)$ forms a Markov chain, and finally, letting $n\to\infty$ and $\delta\downarrow 0$, from (41), (43), and (44), we obtain $\mathcal{R}_C\subseteq\mathcal{A}_4$.

For the cardinality bound on the set $\mathcal{U}$ of the auxiliary random variable U, we apply the support lemma [36, Lemma 3.4] to show that $|\mathcal{U}| \leq |\tilde{\mathcal{X}}| + 3$. More precisely, $|\tilde{\mathcal{X}}| - 1$ continuous functions suffice to preserve $H(\tilde{X})$, and other four more elements are necessary for preserving the conditional entropies $H(X|U)$, $H(\tilde{X}|U)$, $H(Y|U)$ and $H(Z|U)$. See [21, Appendix A] for a detailed discussion. Now the converse proof for the CS model is attained. □

B. Achievability Proof

In the proof, we provide only the main contribution of this part, which is the analysis of the privacy-leakage rate for the GS models, since other constraints can be proved by techniques developed in previous studies. As we have seen in the reduction of (39), the maximum lower bound on the privacy-leakage rate for less noisy ACs decreases compared to that of general ACs, so the important objective in the analysis is to check whether the decreased bound can be achieved or not. For the proof of the CS model, it follows similarly to that of the GS model with one-time pad operation to conceal the secret key, and thus it is omitted. The readers may refer to [1, Appendix A] for a detailed discussion.

Fix the test channel $P_{U|\tilde{X}}$ and let γ be small enough positive. Set $R_S = I(Y;U) - I(Z;U) - 6\gamma$, $R_J = I(\tilde{X};U|Y) + 4\gamma$, and $R_L = I(X;U|Y) + I(X;Z) + 7\gamma$, and the sizes of the set of helpers $|\mathcal{J}_n| = \exp\{nR_J\}$ and the set of secret keys $|\mathcal{S}_n| = \exp\{nR_S\}$. Define the sets

$$\mathcal{T}_n = \left\{(u^n, \tilde{x}^n) : \frac{1}{n}\log\frac{P_{U^n|\tilde{X}^n}(u^n|\tilde{x}^n)}{P_{U^n}(u^n)} \leq I(\tilde{X};U) + \gamma\right\},$$

$$\mathcal{A}_n = \left\{(u^n, y^n) : \frac{1}{n}\log\frac{P_{Y^n|U^n}(y^n|u^n)}{P_{Y^n}(y^n)} \geq I(Y;U) - \gamma\right\},$$

$$\mathcal{K}_n = \Bigg\{(u^n, \tilde{x}^n, x^n) : \frac{1}{n}\log\frac{P_{\tilde{X}^n|U^nX^n}(\tilde{x}^n|u^n, x^n)}{P_{\tilde{X}^n|X^n}(\tilde{x}^n|x^n)} \geq I(\tilde{X};U|X) - \gamma\Bigg\},$$

where $U^n \sim \prod_{t=1}^n P_{U_t}$ with $P_{U_t} = P_U$ for $t \in [1:n]$.

Next, we determine the codebook, and the enrollment (encoding) and authentication (decoding) procedures.

Random Code Generation: Generate $\exp\{n(I(\tilde{X};U)+2\gamma)\}$ i.i.d. sequences of $\tilde{u}^n$ from P_U and denote the set of these sequences as $\mathcal{Q}_n$. Let $g_n : \tilde{\mathcal{X}}^n \to \mathcal{Q}_n \subset \mathcal{U}^n$ be the mapping of measurement $\tilde{x}^n$ into $\tilde{u}^n$. The mapping rule is that it searches $\tilde{u}^n$ such that $(\tilde{u}^n, \tilde{x}^n) \in \mathcal{T}_n$. In case there are multiple such $\tilde{u}^n$, the encoder picks one at random. On the contrary, if there does not exist such a sequence, $\tilde{u}_1^n$ is chosen. Now prepare $M_J = e^{nR_J}$ bins. Assign each sequence $\tilde{u}^n \in \mathcal{Q}_n$ to one of M_J bins according to a uniform distribution on $\mathcal{J}_n$. This random assignment is denoted by $\phi_n(\tilde{u}^n)$. Let $j = \phi_n(\tilde{u}^n)$, $j \in \mathcal{J}_n$, denote the bin's index to which $\tilde{u}^n$ belongs. Also, let $\mathcal{F}_n$ be a universal hash family of functions [50] from $\mathcal{Q}_n$ to $\mathcal{S}_n$. A function $f_n : \mathcal{Q}_n \to \mathcal{S}_n$ is selected uniformly from $\mathcal{F}_n$ and satisfies that $P_{F_n}(\{f_n \in \mathcal{F}_n : f_n(\tilde{u}^n) = f_n(\widehat{u}^n)\}) \leq \frac{1}{|\mathcal{S}_n|}$ for any distinct sequences $\tilde{u}^n \in \mathcal{Q}_n$ and $\widehat{u}^n \in \mathcal{Q}_n$, where P_{F_n} is a uniform distribution on $\mathcal{F}_n$.

In the actual encoding and decoding processes, the set $\mathcal{Q}_n$ and the random functions ϕ_n and f_n are fixed.

Encoding: Observing $\tilde{x}^n$, the encoder first uses g_n to map this sequence to $\tilde{u}^n \in \mathcal{Q}_n$. It then determines the index j of the bin to which $\tilde{u}^n$ belongs, i.e., $j = \phi_n(\tilde{u}^n)$, and generates a secret key $s = f_n(\tilde{u}^n)$. The index j is shared with the decoder for authentication.

Decoding: Seeing y^n, the decoder looks for a unique $\widehat{u}^n$ such as $j = \phi_n(\widehat{u}^n)$ and $(\widehat{u}^n, y^n) \in \mathcal{A}_n$. If such a $\widehat{u}^n$ is found, then the decoder sets $\psi_n(j, y^n) = \widehat{u}^n$, and distills the secret key $\hat{s} = f_n(\widehat{u}^n)$. Otherwise, the decoder outputs $\hat{s} = f_n(\tilde{u}_1^n)$ and error is declared.

The random codebook $\mathcal{C}_n$ consists of the set $\mathcal{Q}_n = \{U_i^n : i \in [1 : \exp\{n(I(\tilde{X};U) + 2\gamma)\}]\}$ and the functions $(g_n, \phi_n, \psi_n, f_n)$, and it is revealed to all parties.

By a similar argument for evaluating the error probability for the Wyner-Ziv problem for general sources in [51], the error probability of the authentication systems averaged over the random codebook vanishes for large enough n. The bound on the storage rate is straightforward from the rate setting. The secret-key rate can be proved via [52, Lemma 3], and using [34, Lemma 12] and [52, Lemma 3] together, the secrecy-leakage can be made negligible for large enough n.

In the remainder of this proof, we evaluate the average performance of the privacy-leakage rate (5) over all possible $\mathcal{C}_n$. Before diving into the detailed analysis, we introduce some useful lemmas for the analysis.

Lemma 1: It holds that

$$\mathbb{E}_{\mathcal{C}_n}[\Pr\{(g_n(\tilde{X}^n), \tilde{X}^n, X^n) \notin \mathcal{K}_n\}] \leq \gamma \tag{45}$$

for large enough n, where $\mathbb{E}_{\mathcal{C}_n}[\cdot]$ denotes the expectation over the random codebook $\mathcal{C}_n$. □

By the definition of the set $\mathcal{K}_n$, the probability $\Pr\{(U^n, \tilde{X}^n, X^n) \notin \mathcal{K}_n\} \to 0$ for large enough n, and therefore using [51, Lemma 1], it guarantees that (45) holds. For detailed discussions of the above lemma, the readers may refer to the appendix in [51].

The following lemma is needed for the analysis of the privacy-leakage rate. The lemma was proved in [53, Lemma 4] for a strong typicality set [36] and [47, Lemma A4] for a modified-weak typicality set [9]. Here, a different proof, based on the information-spectrum methods, is given.

Lemma 2: We have that

$$H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), \mathcal{C}_n) \leq n(H(\tilde{X}|X,U) + 2\gamma + r_n), \tag{46}$$

where $r_n = 1/n(1 - \log(1-\gamma)) + \gamma\log|\tilde{\mathcal{X}}|$, and r_n tends to zero as n approaches infinity and $\gamma \downarrow 0$.

Proof: The proof is given in Appendix B. □

Analysis of Privacy-Leakage Rate: For (5), we have that

$$\begin{aligned} I(X^n; J, Z^n|\mathcal{C}_n) &= I(X^n; J|\mathcal{C}_n) + I(X^n; Z^n|J, \mathcal{C}_n) \\ &\overset{(a)}{=} I(X^n; J|\mathcal{C}_n) + H(Z^n|J, \mathcal{C}_n) - H(Z^n|X^n) \\ &\overset{(b)}{\leq} I(X^n; J|\mathcal{C}_n) + nI(X;Z), \end{aligned} \tag{47}$$

where (a) holds because for a given $\mathcal{C}_n$, the Markov chain $J - X^n - Z^n$ holds, and (X^n, Z^n) are independent of $\mathcal{C}_n$, and (b) follows because conditioning reduces entropy.

Next, we focus on bounding the term $I(X^n; J|\mathcal{C}_n)$ in (47):

$$\begin{aligned}
I(X^n; J|\mathcal{C}_n) &= H(J|\mathcal{C}_n) - H(J|X^n, \mathcal{C}_n) \\
&\le nR_J - H(J|X^n, \mathcal{C}_n) \\
&= nR_J - H(\tilde{X}^n, J|X^n, \mathcal{C}_n) + H(\tilde{X}^n|X^n, J, \mathcal{C}_n) \\
&\overset{(c)}{\le} nR_J - nH(\tilde{X}|X) + H(\tilde{X}^n|X^n, J, \mathcal{C}_n) \\
&\overset{(d)}{=} nR_J - nH(\tilde{X}|X) + H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), \mathcal{C}_n) \\
&\quad + I(\tilde{X}^n; g_n(\tilde{X}^n)|X^n, J, \mathcal{C}_n) \\
&= nR_J - nH(\tilde{X}|X) + H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), \mathcal{C}_n) \\
&\quad + H(g_n(\tilde{X}^n)|X^n, J, \mathcal{C}_n) \\
&\overset{(e)}{=} nR_J - nH(\tilde{X}|X) + H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), \mathcal{C}_n) \\
&\quad + H(g_n(\tilde{X}^n)|X^n, J, Y^n, \mathcal{C}_n) \\
&\overset{(f)}{\le} nR_J - nH(\tilde{X}|X) + H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), \mathcal{C}_n) \\
&\quad + H(g_n(\tilde{X}^n)|J, Y^n, \mathcal{C}_n) \\
&\overset{(g)}{\le} nR_J - nH(\tilde{X}|X) + H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), \mathcal{C}_n) + n\delta_n \\
&\overset{(h)}{\le} n(R_J - H(\tilde{X}|X) + H(\tilde{X}|X, U) + 2\gamma + r_n + \delta_n) \\
&= n(R_J - I(\tilde{X}; U|X) + 2\gamma + r_n + \delta_n) \\
&\overset{(i)}{=} n(R_J - (I(\tilde{X}; U) - I(X; U)) + 2\gamma + r_n + \delta_n) \\
&= n(I(X; U) - I(Y; U) + 6\gamma + r_n + \delta_n), \qquad (48)
\end{aligned}$$

where (c) holds as $(\tilde{X}^n, X^n)$ are independent of $\mathcal{C}_n$, (d) follows because J is a function of $g_n(\tilde{X}^n)$, i.e., $J = \phi(g_n(\tilde{X}^n))$, (e) is due to the Markov chain $g_n(\tilde{X}^n) - (X^n, J) - Y^n$, (f) follows because conditioning reduces entropy, (g) follows as the codeword $g_n(\tilde{X}^n)$ can be estimated from (J, Y^n) with high probability, and thus Fano's inequality is applied, (h) follows from Lemma 2, (i) is due to the Markov chain $U - \tilde{X} - X$, and the last equality holds as we set $R_J = I(\tilde{X}; U|Y) + 4\gamma$.

Merging (47) and (48), we obtain that

$$\begin{aligned}
I(X^n; J, Z^n|\mathcal{C}_n) &\le n(I(X; U|Y) + I(X; Z) + 8\gamma) \\
&= n(R_L + \gamma) \qquad (49)
\end{aligned}$$

for large enough n, which gives the desired bound on the privacy-leakage rate constraint (5) in Definition 1, and this also hints that the decreased lower bound on the privacy-leakage rate in (39) is achievable.

Finally, applying the selection lemma [44, Lemma 2.2], there exists at least one good codebook that satisfies all conditions in Definition 1.

Appendix B
Proof of Lemma 2

Define a binary random variable $T = \mathbf{1}\{(g_n(\tilde{X}^n), \tilde{X}^n, X^n) \in \mathcal{K}_n\}$, where $\mathbf{1}\{\cdot\}$ denotes the indicator function. When $T = 0$, using Lemma 1, it is straightforward that $\mathbb{E}_{\mathcal{C}_n}[P_T(0)] \le \gamma$.

In the rest of equation developments, let c_n and $\tilde{u}^n$ be realizations of the random codebook $\mathcal{C}_n$ and the mapping function $g_n(\tilde{X}^n)$, namely, $\tilde{u}^n = g_n(\tilde{x}^n)$, respectively. The conditional entropy on the left-hand side of (46) can be evaluated as

$$\begin{aligned}
&H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), \mathcal{C}_n) \\
&\le H(\tilde{X}^n, T|X^n, g_n(\tilde{X}^n), \mathcal{C}_n) \\
&\le H(T) + H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), T, \mathcal{C}_n) \\
&\le 1 + \mathbb{E}_{\mathcal{C}_n}[P_T(0)]H(\tilde{X}^n) \\
&\quad + \sum_{c_n} P_{T,\mathcal{C}_n}(1, c_n) H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), T = 1, \mathcal{C}_n = c_n) \\
&\le 1 + n\gamma \log|\tilde{\mathcal{X}}| \\
&\quad + \sum_{c_n} P_{T,\mathcal{C}_n}(1, c_n) H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), T = 1, \mathcal{C}_n = c_n), \qquad (50)
\end{aligned}$$

where the last inequality is due to Lemma 1. Next, we concentrate only on bounding the conditional entropy $H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), T = 1, \mathcal{C}_n = c_n)$ in (50). For a given $\mathcal{C}_n = c_n$, we define the following probability distribution

$$\begin{aligned}
&P_{g_n(\tilde{X}^n)\tilde{X}^n X^n|T}(\tilde{u}^n, \tilde{x}^n, x^n|1) \\
&= \begin{cases} \dfrac{P_{g_n(\tilde{X}^n)\tilde{X}^n X^n}(\tilde{u}^n, \tilde{x}^n, x^n)}{P_T(1)} & \text{if } (\tilde{u}^n, \tilde{x}^n, x^n) \in \mathcal{K}_n \\ 0 & \text{otherwise} \end{cases}, \qquad (51)
\end{aligned}$$

and $P_T(1) = \sum_{(\tilde{u}^n, \tilde{x}^n, x^n) \in \mathcal{K}_n} P_{g_n(\tilde{X}^n)\tilde{X}^n X^n}(\tilde{u}^n, \tilde{x}^n, x^n)$, which is obvious from the definition of the random variable T. For every tuple $(\tilde{u}^n, \tilde{x}^n, x^n) \in \mathcal{K}_n$, observe that

$$\begin{aligned}
&P_{\tilde{X}^n|X^n g_n(\tilde{X}^n) T}(\tilde{x}^n|x^n, \tilde{u}^n, 1) \\
&\overset{(a)}{=} \frac{P_{g_n(\tilde{X}^n)\tilde{X}^n X^n}(\tilde{u}^n, \tilde{x}^n, x^n)}{P_{g_n(\tilde{X}^n)X^n T}(\tilde{u}^n, x^n, 1)} \\
&\ge \frac{P_{g_n(\tilde{X}^n)\tilde{X}^n X^n}(\tilde{u}^n, \tilde{x}^n, x^n)}{P_{g_n(\tilde{X}^n)X^n}(\tilde{u}^n, x^n)} = P_{\tilde{X}^n|g_n(\tilde{X}^n)X^n}(\tilde{x}^n|\tilde{u}^n, x^n), \qquad (52)
\end{aligned}$$

where (a) is due to (51). Also, we have that

$$\begin{aligned}
&\log \frac{1}{P_{\tilde{X}^n|X^n g_n(\tilde{X}^n)}(\tilde{x}^n|x^n, \tilde{u}^n)} \\
&= \log \frac{P_{\tilde{X}^n|X^n U^n}(\tilde{x}^n|x^n, \tilde{u}^n)}{P_{\tilde{X}^n|X^n g_n(\tilde{X}^n)}(\tilde{x}^n|x^n, \tilde{u}^n)} \\
&\quad + \log \frac{P_{\tilde{X}^n|X^n}(\tilde{x}^n|x^n)}{P_{\tilde{X}^n|X^n U^n}(\tilde{x}^n|x^n, \tilde{u}^n)} + \log \frac{1}{P_{\tilde{X}^n|X^n}(\tilde{x}^n|x^n)} \\
&\overset{(b)}{\le} \log \frac{P_{\tilde{X}^n|X^n U^n}(\tilde{x}^n|x^n, \tilde{u}^n)}{P_{\tilde{X}^n|X^n g_n(\tilde{X}^n)}(\tilde{x}^n|x^n, \tilde{u}^n)} \\
&\quad - n(I(\tilde{X}; U|X) - \gamma) + n(H(\tilde{X}|X) + \gamma) \\
&= \log \frac{P_{\tilde{X}^n|X^n U^n}(\tilde{x}^n|x^n, \tilde{u}^n)}{P_{\tilde{X}^n|X^n g_n(\tilde{X}^n)}(\tilde{x}^n|x^n, \tilde{u}^n)} + n(H(\tilde{X}|X, U) + 2\gamma) \qquad (53)
\end{aligned}$$

for all large n, where (b) follows because the condition of the set $\mathcal{K}_n$ is applied to the second term, and using the law of large numbers, the i.i.d. property of $(\tilde{X}^n, X^n)$ guarantees that $\log \frac{1}{P_{\tilde{X}^n|X^n}(\tilde{x}^n|x^n)} \le n(H(\tilde{X}|X) + \gamma)$ for large enough n.

In light of (50), we have that

$$\begin{aligned}
&H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), T = 1, \mathcal{C}_n = c_n) \\
&\le H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), T = 1) \\
&= \sum_{(\tilde{u}^n, \tilde{x}^n, x^n) \in \mathcal{K}_n} P_{g_n(\tilde{X}^n)\tilde{X}^n X^n T}(\tilde{u}^n, \tilde{x}^n, x^n, 1)
\end{aligned}$$

$$\cdot \left(\log \frac{1}{P_{\tilde{X}^n|X^n g_n(\tilde{X}^n)T}(\tilde{x}^n|x^n, \tilde{u}^n, 1)} \right)$$

$$\overset{(c)}{\leq} \sum_{(\tilde{u}^n, \tilde{x}^n, x^n) \in \mathcal{K}_n} P_{g_n(\tilde{X}^n)\tilde{X}^n X^n T}(\tilde{u}^n, \tilde{x}^n, x^n, 1)$$

$$\cdot \left(\log \frac{1}{P_{\tilde{X}^n|X^n g_n(\tilde{X}^n)}(\tilde{x}^n|x^n, \tilde{u}^n)} \right)$$

$$\overset{(d)}{\leq} \sum_{(\tilde{u}^n, \tilde{x}^n, x^n) \in \mathcal{K}_n} P_T(1) \cdot P_{g_n(\tilde{X}^n)\tilde{X}^n X^n|T}(\tilde{u}^n, \tilde{x}^n, x^n|1)$$

$$\cdot \left(\log \frac{P_{\tilde{X}^n|X^n U^n}(\tilde{x}^n|x^n, \tilde{u}^n)}{P_{\tilde{X}^n|X^n g_n(\tilde{X}^n)}(\tilde{x}^n|x^n, \tilde{u}^n)} + n(H(\tilde{X}|X, U) + 2\gamma) \right)$$

$$\overset{(e)}{\leq} n(H(\tilde{X}|X, U) + 2\gamma) - \log(1 - \gamma), \tag{54}$$

where (c) and (d) follow from (52) and (53), respectively, and (e) is due to (55) shown below. To derive (55), we define $A^n = (g_n(\tilde{X}^n), \tilde{X}^n, X^n)$ and $a^n = (\tilde{u}^n, \tilde{x}^n, x^n)$ for brevity. From (51), it follows that $P_{g(\tilde{X}^n)\tilde{X}^n X^n}(\tilde{u}^n, \tilde{x}^n, x^n) = P_T(1) \cdot P_{A^n|T}(a^n|1)$, and thus we have that

$$\sum_{a^n \in \mathcal{K}_n} P_{A^n|T}(a^n|1) \log \frac{P_{\tilde{X}^n|X^n U^n}(\tilde{x}^n|x^n, \tilde{u}^n)}{P_{\tilde{X}^n|X^n g_n(\tilde{X}^n)}(\tilde{x}^n|x^n, \tilde{u}^n)}$$

$$\overset{(f)}{\leq} \log \left(\sum_{a^n \in \mathcal{K}_n} \frac{P_{A^n|T}(a^n|1) \cdot P_{\tilde{X}^n|X^n U^n}(\tilde{x}^n|x^n, \tilde{u}^n)}{P_{\tilde{X}^n|X^n g_n(\tilde{X}^n)}(\tilde{x}^n|x^n, \tilde{u}^n)} \right)$$

$$= \log \left(\sum_{a^n \in \mathcal{K}_n} \frac{P_{g_n(\tilde{X}^n)X^n}(\tilde{u}^n, x^n) \cdot P_{\tilde{X}^n|X^n U^n}(\tilde{x}^n|x^n, \tilde{u}^n)}{P_T(1)} \right)$$

$$\leq \log \left(\sum_{(\tilde{u}^n, x^n) \in \mathcal{Q}_n \times \mathcal{X}^n} P_{g_n(\tilde{X}^n)X^n}(\tilde{u}^n, x^n) \right.$$

$$\left. \cdot \left(\sum_{\tilde{x}^n \in \tilde{\mathcal{X}}^n} P_{\tilde{X}^n|X^n U^n}(\tilde{x}^n|x^n, \tilde{u}^n) \right) \right) - \log P_T(1)$$

$$\overset{(g)}{\leq} -\log(1 - \gamma), \tag{55}$$

where (f) is due to Jensen's inequality and (g) follows because Lemma 1, implying that $P_T(1) \geq 1 - \gamma$, is used.

Lastly, substituting (54) into (50), it follows that

$$H(\tilde{X}^n|X^n, g_n(\tilde{X}^n), \mathcal{C}_n) \leq n(H(\tilde{X}|X, U) + 2\gamma + r_n), \tag{56}$$

where $r_n = 1/n(1 - \log(1 - \gamma)) + \gamma \log|\tilde{\mathcal{X}}|$. □

Appendix C
Proof of Theorem 4

Note that due to the uniformity of the sources, the reverse channel $P_{X|\tilde{X}}$ also results in a binary symmetric channel with crossover probability p, and the entropies $H(\tilde{X})$, $H(X)$, and $H(Z)$ are all equal to one.

Achievability: We begin by proving the inner region of $\mathcal{R}_G$. Observe that each rate constraint in the region can be bounded as follows:

$$R_S \leq I(Y; U) - I(Z; U) \overset{(a)}{=} (1 - q)I(X; U) - I(Z; U)$$

$$= H(Z|U) - (1 - q)H(X|U) - q \tag{57}$$

$$\overset{(b)}{=} H_b(\beta * p * \epsilon) - (1 - q)H_b(\beta * p) - q, \tag{58}$$

$$R_J \geq I(\tilde{X}; U|Y) = I(\tilde{X}; U) - I(Y; U)$$

$$= I(\tilde{X}; U) - (1 - q)I(X; U)$$

$$= q + (1 - q)H(X|U) - H(\tilde{X}|U) \tag{59}$$

$$\overset{(c)}{=} q + (1 - q)H_b(\beta * p) - H_b(\beta), \tag{60}$$

$$R_L \geq I(X; U|Y) + I(X; Z) = qI(X; U) + I(X; Z)$$

$$= 1 + q - qH(X|U) - H(X|Z) \tag{61}$$

$$\overset{(d)}{=} 1 + q - qH_b(\beta * p) - H_b(\epsilon), \tag{62}$$

where (a) follows because $Y = X$ with probability $1 - q$, and (b), (c), and (d) are achieved by considering the test channel $P_{U|\tilde{X}}$ to be a binary symmetric channel with crossover probability β. For the CS model, we argue only for the storage rate as the others follow the same analysis seen in the GS model:

$$R_J \geq I(\tilde{X}; U|Z) \overset{(a)}{=} I(\tilde{X}; U) - I(Z; U)$$

$$= H(Z|U) - H(\tilde{X}|U) \tag{63}$$

$$= H_b(\beta * p * \epsilon) - H_b(\beta), \tag{64}$$

where (a) follows from the Markov chain $U - \tilde{X} - Z$. □

Converse Part: Before the proof, we introduce a simple lemma that will be used to match the inner and outer bounds of the capacity regions for binary sources.

Lemma 3: Given $p \in [0, \frac{1}{2}]$ and $\epsilon \in [0, \frac{1}{2}]$, and for any $\lambda \in [0, 1/2]$, it holds that

$$\frac{\lambda * p - \epsilon}{1 - 2\epsilon} \leq \lambda * p * \epsilon \leq \frac{1}{2}, \tag{65}$$

where the special case of $\epsilon = \frac{1}{2}$ for the fraction of the left-hand side in (65) should be interpreted as $\lim_{\epsilon \to \frac{1}{2}^-} \frac{\lambda * p - \epsilon}{1 - 2\epsilon}$.

Proof: First, the second inequality in (65) follows from the reason that for given p and ϵ, the function $\lambda * p * \epsilon$ is non-decreasing with respect to λ, and its peak is $1/2$ at the point $\lambda = 1/2$.

Next, the relation of the first inequality in (65) is verified. We begin by mentioning an extreme case where $\epsilon = \frac{1}{2}$. When ϵ approaches $\frac{1}{2}$, we consider other two subcases where ($p = \frac{1}{2}$, $\lambda \in [0, \frac{1}{2}]$) and ($p < \frac{1}{2}$, $\lambda \in [0, \frac{1}{2}]$). For the former subcase, the limit value $\lim_{\epsilon \to \frac{1}{2}^-} \frac{\lambda * p - \epsilon}{1 - 2\epsilon}$ is $\frac{1}{2}$ regardless of λ. The first inequality in (65) holds for this subcase as $\lambda * p * \epsilon = \frac{1}{2}$ for $p = \frac{1}{2}$. For the latter subcase, we have that

$$\lim_{\epsilon \to \frac{1}{2}^-} \frac{\lambda * p - \epsilon}{1 - 2\epsilon} = \begin{cases} -\infty & (\lambda < \frac{1}{2}) \\ \frac{1}{2} & (\lambda = \frac{1}{2}) \end{cases}. \tag{66}$$

Since $\lambda * p * \epsilon \geq 0$ and $\lambda * p * \epsilon = \frac{1}{2}$ at $\lambda = \frac{1}{2}$, the first inequality in (65) also holds for the latter subcase.

In the remaining of the proof, we focus on the range of $\epsilon \in [0, \frac{1}{2})$. Due to the same reason for the second inequality in (65), it is obvious that $\lambda * p \leq 1/2$ or $2(\lambda * p) \leq 1$, and since $\epsilon \geq 0$, it follows that $-2\epsilon(1 - \epsilon) \leq -4\epsilon(1 - \epsilon)(\lambda * p)$. Adding $\lambda * p$ to both sides of this inequality, we have that $-2\epsilon + 2\epsilon^2 + \lambda * p \leq -4\epsilon(\lambda * p) + 4\epsilon^2(\lambda * p) + \lambda * p$. Rearrange both sides as follows:

$$-\epsilon + \lambda * p \leq \epsilon - 2\epsilon^2 - 4\epsilon(\lambda * p) + 4\epsilon^2(\lambda * p) + \lambda * p$$

$$= (1-2\epsilon)(\epsilon - 2\epsilon(\lambda * p) + \lambda * p)$$
$$= (1-2\epsilon)(\lambda * p * \epsilon), \tag{67}$$

indicating that Lemma 3 holds. □

To derive the outer region of the GS model, we need to further bound (57), (59), and (61). In order to do so, we fix $H(X|U)$ and derive tight upper bounds for both $H(Z|U)$ and $H(\tilde{X}|U)$. Since $H_b(p) = H(X|\tilde{X}) \leq H(X|U) \leq H(X) = 1$, we fix $\lambda \in [0, 1/2]$ such that

$$H(X|U) = H_b(\lambda * p). \tag{68}$$

In the direction from Z to X, using Mrs. Gerber's Lemma [46], it follows that

$$H(X|U) \geq H_b(H_b^{-1}(H(Z|U)) * \epsilon). \tag{69}$$

Now substituting the value of $H(X|U)$ that we have set in (68) into the left-hand side of (69), we have that

$$H_b(\lambda * p) \geq H_b(H_b^{-1}(H(Z|U)) * \epsilon). \tag{70}$$

Since all $\lambda, p, \epsilon \leq \frac{1}{2}$ and the binary entropy function is monotonously increasing in the interval $[0, \frac{1}{2}]$, it follows that

$$\lambda * p \geq H_b^{-1}(H(Z|U)) * \epsilon \overset{(a)}{=} H_b^{-1}(H(Z|U))(1-2\epsilon) + \epsilon,$$

where (a) follows from the definition of the operator-$*$ defined in Table I, which implies that

$$H_b^{-1}(H(Z|U)) \leq \frac{\lambda * p - \epsilon}{1-2\epsilon} \leq \lambda * p * \epsilon, \tag{71}$$

where the second inequality follows because the first inequality in (65) is used, and thus

$$H(Z|U) \leq H_b(\lambda * p * \epsilon). \tag{72}$$

Likewise, in the direction from $\tilde{X}$ to X, again using Mrs. Gerber's Lemma, we have that $H(X|U) \geq H_b(H_b^{-1}(H(\tilde{X}|U)) * p)$. This equation implies that $\lambda * p \geq H_b^{-1}(H(\tilde{X}|U)) * p$. Since $0 \leq p \leq 1/2$, it follows that $H_b^{-1}(H(\tilde{X}|U)) \leq \lambda$ or equivalently,

$$H(\tilde{X}|U) \leq H_b(\lambda). \tag{73}$$

Plugging eqs. (68), (72), and (73) into eqs. (57), (59), and (61), we obtain that

$$R_S \leq H_b(\lambda * p * \epsilon) - (1-q)H_b(\lambda * p) - q, \tag{74}$$
$$R_J \geq q + (1-q)H_b(\lambda * p) - H_b(\lambda), \tag{75}$$
$$R_L \geq 1 + q - q\,H_b(\lambda * p) - H_b(\epsilon). \tag{76}$$

From (74)–(76), by varying λ over the range $[0, \frac{1}{2}]$ and taking the union, the inner and outer bounds on the capacity region match. Hence, the proof of the GS model is completed.

For the CS model, also fix λ such that (68) is satisfied. In the direction from X to Z, using Mrs. Gerber's Lemma [46] yields that

$$H(Z|U) \geq H_b(H_b^{-1}(H(X|U)) * \epsilon) = H_b(\lambda * p * \epsilon). \tag{77}$$

Substituting (73) and (77) into (63), one can derive that $R_J \geq H_b(\lambda * p * \epsilon) - H(\lambda)$, and by varying $\lambda \in [0, \frac{1}{2}]$, the optimal rate region of the CS model for binary sources is obtained. □

REFERENCES

[1] V. Yachongka, H. Yagi, and H. Ochiai, "Secret-key agreement using physical identifiers for degraded and less noisy authentication channels," 2022, *arXiv:2208.10478*.

[2] M. Bloch et al., "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.

[3] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[4] R. Pappu, "Physical one-way functions," Ph.D. dissertation, MIT, Cambridge, MA, USA, Oct. 2001.

[5] B. Gassend, "Physical random functions," Master's thesis, MIT, Cambridge, MA, USA, Jan. 2003.

[6] C. Böhm and M. Hofer, *Physical Unclonable Functions in Theory and Practice*. New York, NY, USA: Springer, Oct. 2012.

[7] J. Zhang, C. Shen, H. Su, M. T. Arafin, and G. Qu, "Voltage over-scaling-based lightweight authentication for IoT security," *IEEE Trans. Comput.*, vol. 71, no. 2, pp. 323–336, Feb. 2022.

[8] O. Günlü and R. F. Schaefer, "An optimality summary: Secret key agreement with physical unclonable functions," *Entropy*, vol. 23, no. 1, p. 16, Dec. 2020.

[9] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.

[10] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems—Part I: Single use case," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 122–139, Mar. 2011.

[11] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, "Secure biometrics: Concepts, authentication architectures, and challenges," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 51–64, Sep. 2013.

[12] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Jan. 2008.

[13] J. C. Bernal-Romero, J. M. Ramirez-Cortes, J. D. J. Rangel-Magdaleno, P. Gomez-Gil, H. Peregrina-Barreto, and I. Cruz-Vega, "A review on protection and cancelable techniques in biometric systems," *IEEE Access*, vol. 11, pp. 8531–8568, 2023.

[14] N. N. Anandakumar, M. S. Hashmi, and M. Tehranipoor, "FPGA-based physical unclonable functions: A comprehensive overview of theory and architectures," *Integration*, vol. 81, pp. 175–194, Nov. 2021.

[15] T. Assaf et al., "High-rate secret key generation using physical layer security and physical unclonable functions," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 209–225, 2023.

[16] L. Kusters and F. M. J. Willems, "Secret-key capacity regions for multiple enrollments with an SRAM-PUF," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2276–2287, Sep. 2019.

[17] L. Kusters and F. M. J. Willems, "Multiple observations for secret-key binding with SRAM PUFs," *Entropy*, vol. 23, no. 5, p. 590, May 2021.

[18] M. Koide and H. Yamamoto, "Coding theorems for biometric systems," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 2647–2651.

[19] R. A. Chou, "Biometric systems with multiuser access structures," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 807–811.

[20] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, Nov. 2015.

[21] O. Günlü and G. Kramer, "Privacy, secrecy, and storage with multiple noisy measurements of identifiers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2872–2883, Nov. 2018.

[22] T. Ignatenko and F. M. J. Willems, "Fundamental limits for privacy-preserving biometric identification systems that support authentication," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5583–5594, Oct. 2015.

[23] V. Yachongka and H. Yagi, "A new characterization of the capacity region of identification systems under noisy enrollment," in *Proc. 54th Annu. Conf. Inf. Sci. Syst. (CISS)*, Princeton, NJ, USA, Mar. 2020, pp. 1–6.

[24] L. Zhou, T. J. Oechtering, and M. Skoglund, "Fundamental limits-achieving polar code designs for biometric identification and authentication," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 180–195, 2022.

[25] B. Chen and F. M. J. Willems, "Secret key generation over biased physical unclonable functions with polar codes," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 435–445, Feb. 2019.

[26] O. Günlü, O. Iscan, V. Sidorenko, and G. Kramer, "Code constructions for physical unclonable functions and biometric secrecy systems," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2848–2858, Nov. 2019.

[27] O. Günlü, P. Trifonov, M. Kim, R. F. Schaefer, and V. Sidorenko, "Privacy, secrecy, and storage with nested randomized polar subcode constructions," *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 514–525, Jan. 2022.

[28] S. Müelich, H. Mandry, M. Ortmanns, and R. F. H. Fischer, "A multilevel coding scheme for multi-valued physical unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3814–3827, 2021.

[29] R. F. H. Fischer and S. Müelich, "Coded modulation and shaping for multivalued physical unclonable functions," *IEEE Access*, vol. 10, pp. 99178–99194, 2022.

[30] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[31] K. Kittichokechai and G. Caire, "Secret key-based authentication with a privacy constraint," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 1791–1795.

[32] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[33] I. Csiszar and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[34] S. Watanabe and Y. Oohama, "Secret key agreement from correlated Gaussian sources by rate limited public communication," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 93, no. 11, pp. 1976–1983, 2010.

[35] O. Günlü, K. Kittichokechai, R. F. Schaefer, and G. Caire, "Controllable identifier measurements for private authentication with secret keys," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1945–1959, Aug. 2018.

[36] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[37] O. Günlü, R. F. Schaefer, and G. Kramer, "Private authentication with physical identifiers through broadcast channel measurements," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Visby, Sweden, Aug. 2019, pp. 1–5.

[38] O. Günlü and R. F. Schaefer, "Controllable key agreement with correlated noise," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 82–94, Mar. 2021.

[39] F. Gebali and M. Mamun, "Review of physically unclonable functions (PUFs): Structures, models, and algorithms," *Frontiers Sens.*, vol. 2, Jan. 2022, Art. no. 751748.

[40] T. S. Han, *Information-Spectrum Methods in Information Theory*. Berlin, Germany: Springer, 2003.

[41] V. Yachongka, H. Yagi, and Y. Oohama, "Secret key-based authentication with passive eavesdropper for scalar Gaussian sources," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Espoo, Finland, Jun. 2022, pp. 2666–2671.

[42] E. J. C. Kelkboom, G. G. Molina, J. Breebaart, R. N. J. Veldhuis, T. A. M. Kevenaar, and W. Jonker, "Binary biometrics: An analytic framework to estimate the performance curves under Gaussian assumption," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 40, no. 3, pp. 555–571, May 2010.

[43] O. Günlü, O. Iscan, and G. Kramer, "Reliable secret key generation from physical unclonable functions under varying environmental conditions," in *Proc. IEEE Int. Workshop Inf. Forensics Security (WIFS)*, Rome, Italy, Nov. 2015, pp. 1–6.

[44] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[45] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information-theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2008.

[46] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications—I," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 6, pp. 769–772, Nov. 1973.

[47] V. Yachongka, H. Yagi, and Y. Oohama, "Biometric identification systems with noisy enrollment for Gaussian sources and channels," *Entropy*, vol. 23, no. 8, p. 1049, Aug. 2021.

[48] O. Günlü, R. F. Schaefer, H. Boche, and H. V. Poor, "Private key and decoder side information for secure and private source coding," *Entropy*, vol. 24, no. 12, p. 1716, Nov. 2022.

[49] L. Zhou, M. T. Vu, T. J. Oechtering, and M. Skoglund, "Privacy-preserving identification systems with noisy enrollment," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3510–3523, 2021.

[50] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.

[51] K. Iwata and J. Muramatsu, "An information-spectrum approach to rate-distortion function with side information," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 85, no. 6, pp. 1387–1395, 2002.

[52] M. Naito, S. Watanabe, R. Matsumoto, and T. Uyematsu, "Secret key agreement by soft-decision of signals in Gaussian Maurer's model," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 92, no. 2, pp. 525–534, 2009.

[53] 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.

Vamoua Yachongka (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in communication engineering and informatics from The University of Electro-Communications, Japan, in 2015, 2017, and 2021, respectively. From 2021 to 2022, he was a Post-Doctoral Research Fellow with The University of Electro-Communications. Since 2022, he has been a Post-Doctoral Research Fellow with Yokohama National University. His research interests include information-theoretic and physical layer security.

Hideki Yagi (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in industrial and management systems engineering from Waseda University, Tokyo, Japan, in 2001, 2003, and 2005, respectively. He was with the Media Network Center, Waseda University, as a Research Associate, from 2005 to 2007, and an Assistant Professor from 2007 to 2008. In winter 2008 and from July 2010 to January 2011, he was a Visiting Fellow with Princeton University. He is currently an Associate Professor with the Department of Computer and Network Engineering, The University of Electro-Communications, Tokyo. His research interests include information and coding theory and information theoretic security. He is a member of the Research Institute of Signal Processing.

Hideki Ochiai (Fellow, IEEE) received the B.E. degree in communication engineering from Osaka University, Osaka, Japan, in 1996, and the M.E. and Ph.D. degrees in information and communication engineering from The University of Tokyo, Tokyo, Japan, in 1998 and 2001, respectively. From 1994 to 1995, he was with the Department of Electrical Engineering, University of California at Los Angeles (UCLA), Los Angeles, CA, USA, under the Scholarship of the Ministry of Education, Science and Culture. From 2001 to 2003, he was a Research Associate with The University of Electro-Communications, Tokyo. Since April 2003, he has been with Yokohama National University, Yokohama, Japan, where he is currently a Professor. From 2003 to 2004, he was a Visiting Scientist with Harvard University, Cambridge, MA, USA. From 2019 to 2020, he was a Visiting Professor with the University of Waterloo, Waterloo, ON, Canada, and a Visiting Fellow with Princeton University, Princeton, NJ, USA. His research interests include wireless communications and networks. He served as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2007 to 2011 and the IEEE WIRELESS COMMUNICATIONS LETTERS from 2011 to 2016.