Secret-Key Generation From Private Identifiers Under Channel Uncertainty

Vamoua Yachongka, *Member, IEEE*, and Rémi A. Chou, *Member, IEEE*

***Abstract*—This study investigates secret-key generation for device authentication using physical identifiers, such as responses from physical unclonable functions (PUFs). The system includes two legitimate terminals (encoder and decoder) and an eavesdropper (Eve), each with access to different measurements of the identifier. From the device identifier, the encoder generates a secret key, which is securely stored in a private database, along with helper data that is saved in a public database accessible by the decoder for key reconstruction. Eve, who also has access to the public database, may use both her own measurements and the helper data to attempt to estimate the secret key and identifier. Our setup focuses on authentication scenarios where channel statistics are uncertain, with the involved parties employing multiple antennas to enhance signal reception. Our contributions include deriving inner and outer bounds on the optimal trade-off among secret-key, storage, and privacy-leakage rates for general discrete sources, and showing that these bounds are tight for Gaussian sources.**

***Index Terms*—Capacity region, compound channels, multiple outputs, key generation, privacy leakage, PUFs.**

I. Introduction

THE Internet of Things (IoT) is a rapidly growing technology that enables numerous sensors and small-chip devices to interact and exchange information over the internet. However, ensuring security and privacy in IoT communications presents significant challenges compared to conventional networks due to the diverse range of applications and resource constraints of these devices [2]. To help address these difficulties, recent efforts have focused on developing security protocols at the physical layer for authenticating devices.

Secret-key generation using physical identifiers, such as responses from physical unclonable functions (PUFs), is a promising protocol for device authentication because it offers several advantages, including simple designs, low costs, and eliminating the need to save the secret key on the device [3]. A PUF is defined as a physical function that for a given input (challenge), provides an output (response) that serves as a unique identifier for each device [4], [5]. Some examples of PUFs are static random access memory (SRAM) PUFs and ring-oscillator (RO) PUFs.

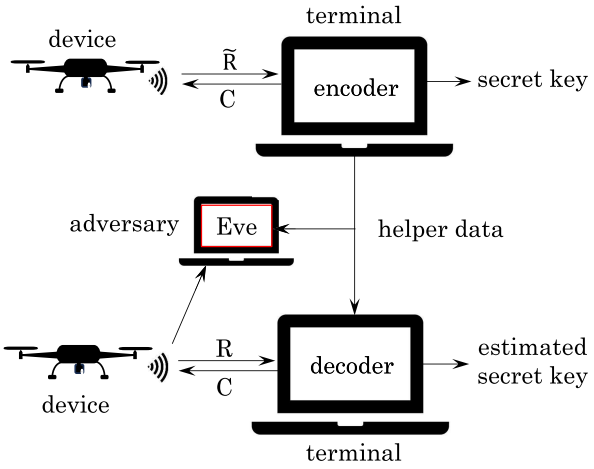

Fig. 1. An authentication scheme based on secret-key generation with PUFs. The eavesdropper (Eve) is a passive adversary who is interested in learning the secret key and the source identifier, but does not interfere with the communication mechanism of the system.

Secret-key authentication using PUFs is illustrated in Fig. 1 [6][1] and consists of an enrollment phase and an authentication phase. During the enrollment phase, the terminal (encoder) challenges the device, i.e., the PUF embedded in the device, with a challenge C and gets a response $\widetilde{R}$, from which the encoder generates a secret key and helper data. The secret key is securely stored in a private database, while the helper data are saved in a public database, which can be accessed by both the decoder and Eve. In the authentication phase, the terminal (decoder) challenges the device by sending the same challenge C, which produces a different response R due to noise effects. The decoder reconstructs the secret key based on both the response and helper data from the public database and then compares it with the one saved in the private database. If they match, the device is successfully authenticated; otherwise, the authentication fails.

In subsequent discussions, the response of a PUF unaffected by noise is referred to as the *source identifier*. The responses of a PUF observed at the terminals and Eve through communication channels are called the *observed identifiers*. It is worth

Received 11 March 2025; revised 4 August 2025 and 13 October 2025; accepted 15 October 2025. Date of publication 20 October 2025; date of current version 17 November 2025. This work was supported in part by NSF under Grant CCF-2425371. An earlier version of this paper was presented at the 2024 IEEE Information Theory Workshop (ITW) [DOI: 10.1109/ITW61385.2024.10806941]. The associate editor coordinating the review of this article and approving it for publication was Dr. Min Li. *(Corresponding author: Vamoua Yachongka.)*

The authors are with the Department of Computer Science and Engineering, The University of Texas at Arlington, Arlington, TX 76019 USA (e-mail: va.yachongka@ieee.org).

Digital Object Identifier 10.1109/TIFS.2025.3623929

[1] [6] does not consider the presence of Eve, but is included in the figure to facilitate understanding of our system model in Section II.

noting that the source identifiers are assumed to be fixed and thus the secret-key generation model considered in this paper corresponds to the source-type model, unlike the channel-type models, where the source distribution can be controlled [7].

A. Motivations

We study the capacity region of secret-key generation from source identifiers for a setup involving compound authentication channels with multiple outputs. The motivation for considering compound-channel settings is to capture a situation in which device authentication takes place in environments where the channel statistics may not be perfectly known. This contrasts with most previous studies, which assume that the encoder and decoder have perfect knowledge of the source and channel statistics of the systems.

For example, as shown in Fig. 1, consider a situation where the decoder needs to authenticate a flying drone. As the channel state information (CSI) of the channel from the drone to the decoder may fluctuate, it makes it difficult for the decoder to obtain the exact CSI. Additionally, Eve is unlikely to share her CSI with the legitimate terminals. Thus, compound channels are used to model the channels to the decoder and Eve. In this setting, the encoder and decoder do not possess precise CSI of the relevant channels but are aware that these channels belong to certain predefined sets.

Additionally, we consider multiple outputs for the channels to the encoder, decoder, and Eve to capture the circumstance where these parties may deploy multiple antennas to enhance signal reception. Note that having more antennas can increase the correlation between Eve's observation and the source identifier, giving her an advantage in learning the secret key and the source identifier. Hence, in this setting, we want to quantify the potential leakage to Eve from both security and privacy perspectives.

Finally, in practice, certain types of PUFs produce continuous-value identifiers. For example, the source of RO PUFs can be modeled as a Gaussian distribution [8]. Additionally, a number of communication channels are sometimes approximated as additive white Gaussian noise (AWGN) channels. This motivates us to study setups with Gaussian sources and AWGN channels.

B. Related Work

Secret-key generation using PUFs[2] has been studied from information-theoretic perspectives in [9] and [10]. Later, several extensions of this model were found in [11, Ch. 4] for Gaussian sources, [12] for separated and combined enrollments, and [13] for multiple rounds of enrollments and authentications. Limited storage rate was introduced to the model in [14]. Furthermore, the fundamental limits among secret-key, storage, and privacy-leakage rates when Eve also has a correlated sequence of the source were characterized in [15] for discrete sources and [16] for Gaussian sources. This model is similar to the key-agreement problem with forward communication only studied in [17], [18], and [19], but an additional privacy constraint is imposed in the problem formulation to limit information leakage on the source identifier.

More recent works have considered a setup that incorporates a noisy channel in the enrollment phase [20], [21], [22]. The channel is modeled to account for the noise introduced to the source identifier during the enrollment process, providing a more general framework, as signals generated by a PUF are inherently affected by noise. Further progress in this setting has been investigated in [23], [24], [25], and [26], addressing user identification.

Secret-key generation with PUFs for compound sources has been studied in [27] and [28] for the generated-secret (GS) model and the chosen-secret (CS) model. In the GS model, the secret key is generated using the observed identifier at the encoder. In contrast, the CS model assumes that the secret key is independently and uniformly chosen in advance. Relevant applications of the GS model include field-programmable gate array (FPGA) based key generation with PUFs [29], [30] and that of the CS model can be seen in key-binding biometric authentication [31] and fuzzy commitment schemes [32], [33]. Some extensions on this setting are explored in [34] and [35] to incorporate user identification. Similar problems can be found in [36] and [37], [38], [39] for key generation where the privacy constraint is not imposed and in [40], [41], [42], and [43] for compound wiretap channels. We note that the works [40], [41], [42], [43] focus on compound channels under the channel-type model, whereas our work addresses compound structure in the source-type model.

C. Main Challenges and Contributions

We begin by explaining challenges of proving the achievability part for general discrete sources. In [37], key generation for compound sources without the privacy constraint is investigated. While [37] derives a single-letter inner bound for discrete sources and a single-letter outer bound for degraded sources, we establish single-letter inner and outer bounds for discrete sources and also characterize the capacity region for Gaussian sources, which require different approaches from the discrete case. The key differences for inner-bound derivations between the work [37] and ours are twofold.

First, the techniques used for analyzing the secret-key uniformity and secrecy-leakage constraints are distinct. In [37, Th. 1], the secret key is derived from the shared randomness between encoder and decoder, and the analyses of the two constraints rely on extending the method proposed in [44] for non-compound sources. Our approach, in contrast, aligns with [21], where the secret key is generated through index mapping, and the analyses of the constraints build upon the technique used in [40] for analyzing the secrecy constraint in compound wiretap channels.

Second, the privacy-leakage constraint is not considered in [37]. In our problem formulation, as in [21] and [22], this constraint is imposed and quantified by the mutual information between the source identifier and the helper data, conditioned on Eve's observation. Its analysis is not straightforward because the helper data does not have an independent and identically distributed (i.i.d.) structure: although the encoder

[2]PUF and biometric identifiers share similar characteristics, and thus, the theoretical results developed for one can be applied to the other as well [3].

observes an i.i.d. identifier sequence, it generates the helper data based on the entire block rather than on individual symbols.

In the converse part, for a given channel state, the proofs of the GS and CS models mirror the ones in [21, Th. 3 and 4] with a proper modification for the privacy-leakage analysis as the definition is distinct. These results are then generalized to the compound-channel settings by taking the intersection over all possible channel states to establish the outer bounds. As a result, the inner region first involves an optimization carried over the distributions of auxiliary random variables, and then a minimization of the index pair for channel states. In contrast, the order of these two operations is reversed in the outer region. This leads to a gap between the inner and outer bounds, similar to the conclusion drawn in [40] for compound wiretap channels.

However, we show that, for a noiseless enrollment channel, our inner and outer regions coincide for Gaussian sources, providing a complete capacity characterization. The main challenging aspect arises in proving the converse part. Given the multiple-antenna settings at the legitimate terminals and Eve, the vector-form observations are not stochastically degraded in general [45]. We use sufficient statistics [46] to convert the vector problem into a scalar one. However, after this conversion, showing that all constraints of the original problem definition are preserved is challenging, and it is unclear whether the same expressions of the outer bounds for general discrete sources also hold for the scalar variables. Therefore, we cannot directly apply the technique in [47, Appx. B] to eliminate the second auxiliary random variable. In this paper, we instead derive new single-letter expressions of outer bounds for the Gaussian case using scalar random variables.

Another difficulty arises in proving the converse for the parametric expression of Gaussian sources. In the analysis of the model without side information at Eve [11, Appx. D], [48], the conditional entropy power inequality (EPI) plays an important role. However, the EPI is insufficient to prove the converse for all possible values of the optimization parameter in our problem. To overcome this issue, we adopt a distinct method introduced in [49, Sect. IV-C], using Fisher information. This approach enables us to derive the outer region that coincides with the inner one for any value of the optimization parameter.

Our main contributions are summarized as follows:

- We derive inner and outer bounds on the capacity regions of secret-key, storage, and privacy-leakage rates of the GS and CS models for discrete sources.
- We provide complete characterizations of the capacity regions of the GS and CS models for Gaussian sources by demonstrating the existence of a saddle point at which the inner and outer bounds coincide.
- We conduct numerical calculations for the Gaussian case to illustrate how the change of the number of antennas at the decoder and Eve affects the secret-key and storage rates. The results show that increasing the number of antennas at the decoder leads to a higher secret-key rate, while increasing antennas at Eve reduces the secret-key rate. Nevertheless, even if Eve has more antennas, a positive secret-key rate is still achievable as long as the worst channel power gain at the decoder is greater than the best channel power gain at Eve. Moreover, we compare the secret-key and privacy-leakage rates between the GS and CS models under the same values of storage rates. The results reveal that in the low storage-rate regime, the GS model outperforms the CS model in terms of secret-key rate, whereas the CS model provides better privacy-leakage performance. In the high storage-rate regime, the CS model is better suited as it can achieve the same secret-key rate as the GS model but with lower privacy leakage.

Our results recover, as special cases, results derived in previous works. For discrete sources, when only the channel to the decoder is compound and all channels have a single output, the inner and outer bounds match the preliminary result given in [1, Props. 1 and 2]. Additionally, the inner and outer bounds are tight for single-output and non-compound channels, and recover [21, Th. 3 and 4] without action cost. For Gaussian sources, as detailed in Section III-B, our results recover as special cases the capacity regions derived in [11, Ch. 4] and [22] for single-output and non-compound channels.

D. Modeling Assumptions

In general, PUF responses from devices are correlated. However, techniques such as transform coding-based algorithms [3] and principal component analysis [50] can be applied to convert these responses into a sequence with almost independent symbols. Therefore, we assume that each symbol in the source and observed identifier sequences is i.i.d. generated. Additionally, we assume that the database that stores helper data is public, e.g., in the cloud, and accessible to both the decoder and Eve. These modeling assumptions are consistent with those used in prior works [9], [10], [20], [21], [22].

E. Notation and Paper Organization

$\mathbb{R}_+$ is the set of non-negative real numbers. For any $a, b \in \mathbb{R}$, define $[a:b] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}$. Italic uppercase X and lowercase x denote a random variable and its realization, respectively. Boldface letters $\mathbf{X}$ and $\mathbf{x}$ represent a collection of random variables and its realization. X^n denotes the vector $(X_1, \ldots, X_n)$ and X_t represents the t-th element in the vector. X_k^t stands for a partial sequence $(X_k, \ldots, X_t)$ for any $[k:t] \subseteq [1:n]$. σ_X^2 and $\mathbf{\Sigma_Y}$ denote the variance of X and the covariance matrix of $\mathbf{Y}$. $\mathcal{N}(0, \sigma^2)$ denotes the Gaussian distribution with zero mean and variance σ^2. $\mathcal{T}_\delta^n(X)$ denotes the set of δ-strongly typical sequences according to P_X [51] and the random variable inside the parentheses is omitted, e.g., $\mathcal{T}_\delta^n$, when it is clear from the context. Additionally, the set of conditionally δ-typical sequences is denoted as $\mathcal{T}_\delta^n(XY|z^n) \triangleq \{(x^n, y^n) : (x^n, y^n, z^n) \in \mathcal{T}_\delta^n\}$ for a given $z^n \in \mathcal{Z}^n$.

The remainder of the paper is organized as follows. In Section II, we state the problem definitions for the GS and CS models. We present our main results in Section III. Proofs of our main results are available in the appendices. Finally, we provide concluding remarks and some future directions in Section IV.

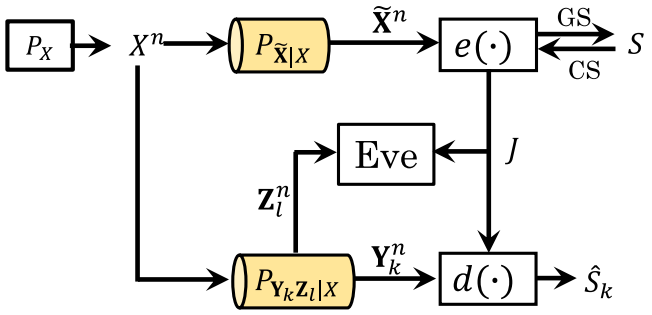

Fig. 2. Illustration of the system model in State (k, l).

II. Problem Statement

The source identifier X^n is i.i.d. according to P_X. The terminals do not have direct access to this identifier but can only observe its noisy versions. The encoder, decoder, and Eve are equipped with $(\Omega_{\tilde{X}}, \Omega_Y, \Omega_Z) \in \mathbb{N}^3$ receiver antennas, respectively. Furthermore, there are $|\mathcal{K}|$ possible states for the channel to the decoder $P_{\mathbf{Y}_k|X}$ with $k \in \mathcal{K}$, and $|\mathcal{L}|$ possible states for the channel to Eve $P_{\mathbf{Z}_l|X}$ with $l \in \mathcal{L}$ in the authentication phase.[3] When the channels are in State (k, l), the setting is depicted in Fig. 2. The vector-form random variables $\tilde{\mathbf{X}}^n \triangleq [\tilde{X}_1^n, \tilde{X}_2^n, \cdots, \tilde{X}_{\Omega_{\tilde{X}}}^n]^\intercal$, $\mathbf{Y}_k^n \triangleq [Y_{k1}^n, \cdots, Y_{k\Omega_Y}^n]^\intercal$, and $\mathbf{Z}_l^n \triangleq [Z_{l1}^n, \cdots, Z_{l\Omega_Z}^n]^\intercal$ denote the outputs of the source identifier X^n via the channel to the encoder, $(\mathcal{X}, P_{\tilde{\mathbf{X}}|X}, \tilde{\boldsymbol{\mathcal{X}}})$, and the channels to the decoder and Eve $(\mathcal{X}, P_{\mathbf{Y}_k\mathbf{Z}_l|X}, \boldsymbol{\mathcal{Y}}_k \times \boldsymbol{\mathcal{Z}}_l)$, respectively. The joint distribution of the system is

$$P_{\tilde{\mathbf{X}}^n X^n \mathbf{Y}_k^n \mathbf{Z}_l^n} \triangleq \prod_{t=1}^n P_{\tilde{\mathbf{X}}_t|X_t} \cdot P_{X_t} \cdot P_{\mathbf{Y}_{k,t}\mathbf{Z}_{l,t}|X_t}. \tag{1}$$

Secret-key generation strategies are formally defined below. Let $\mathcal{S} \triangleq [1 : 2^{nR_S}]$ and $\mathcal{J} \triangleq [1 : 2^{nR_J}]$.

Definition 1 (GS Model): For the GS model, a $(2^{nR_S}, n, R_J, R_L)$ secret-key generation strategy consists of:

- Encoding mapping $e : \tilde{\boldsymbol{\mathcal{X}}}^n \to \mathcal{J} \times \mathcal{S}$;
- Decoding mapping $d : \boldsymbol{\mathcal{Y}}_k^n \times \mathcal{J} \to \mathcal{S}$;

and operates as follows:

- The encoder observes $\tilde{\mathbf{X}}^n$ and generates the helper data $J \in \mathcal{J}$ and a secret key $S \in \mathcal{S}$, as $(J, S) \triangleq e(\tilde{\mathbf{X}}^n)$;
- The helper data J is stored in a public database, accessible to anyone;
- From $\mathbf{Y}_k^n$ and J, retrieved from the public database, the decoder estimates S as $\hat{S}_k \triangleq d(\mathbf{Y}_k^n, J)$.

Definition 2 (CS Model): For the CS model, a $(2^{nR_S}, n, R_J, R_L)$ secret-key generation strategy consists of:

- A secret key S, chosen uniformly at random in $\mathcal{S}$ and independently of $(\tilde{\mathbf{X}}^n, X^n, \mathbf{Y}_k^n, \mathbf{Z}_l^n)$;
- Encoding mapping $e : \tilde{\boldsymbol{\mathcal{X}}}^n \times \mathcal{S} \to \mathcal{J}$;
- Decoding mapping $d : \boldsymbol{\mathcal{Y}}_k^n \times \mathcal{J} \to \mathcal{S}$;

and operates as follows:

- From $\tilde{\mathbf{X}}^n$ and S, the encoder generates $J \triangleq e(\tilde{\mathbf{X}}^n, S)$;
- The helper data J is saved in a public database, accessible to anyone;
- From $\mathbf{Y}^n$ and J, the decoder estimates S as $\hat{S}_k \triangleq d(\mathbf{Y}_k^n, J)$.

In the following, we write $(\max_{k\in\mathcal{K}}, \min_{k\in\mathcal{K}})$ and $(\max_{l\in\mathcal{L}}, \min_{l\in\mathcal{L}})$ as $(\max_k, \min_k)$ and $(\max_l, \min_l)$, respectively, for simplicity.

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

$$\max_k \mathbb{P}\{\widehat{S}_k \neq S\} \leq \delta, \tag{2}$$

$$H(S) + n\delta \geq \log|\mathcal{S}| \geq n(R_S - \delta), \tag{3}$$

$$\log|\mathcal{J}| \leq n(R_J + \delta), \tag{4}$$

$$\max_l I(S; J, \mathbf{Z}_l^n) \leq n\delta, \tag{5}$$

$$\max_l I(X^n; J|\mathbf{Z}_l^n) \leq n(R_L + \delta). \tag{6}$$

$\mathcal{R}_{\mathrm{G}}$ is defined as the closure of the set of all achievable rate tuples for the GS model, and it is called the capacity region.

Definition 4 (CS Model): A tuple of secret-key, storage, and privacy-leakage rates $(R_S, R_J, R_L) \in \mathbb{R}_+^3$ is achievable for the CS model if, for sufficiently small $\delta > 0$ and large enough n, there exist pairs of encoders and decoders that satisfy all the conditions (2)–(6) with replacing (3) by $\log|\mathcal{S}| \geq n(R_S - \delta)$. Let $\mathcal{R}_{\mathrm{C}}$ be the capacity region of the CS model.

In Definition 3, (2) denotes the reliability constraint, (3) is the uniformity requirement of the generated secret key, (4) is the storage rate constraint, (5) is the secrecy-leakage constraint, evaluating the information about the secret key leaked to Eve, and (6) is the privacy-leakage constraint, quantifying the amount of information leaked to Eve regarding the source identifier via the helper data given Eve's side information.

III. Main Results

This section presents the inner and outer bounds for the GS and CS models with discrete sources, followed by the tight bounds for Gaussian sources and numerical results for both models.

A. Discrete Sources

Proposition 1 (Inner Bounds): We have

$$\begin{aligned}
\mathcal{R}_{\mathrm{G}} \supseteq \bigcup_{P_{V|U}, P_{U|\tilde{\mathbf{X}}}} \Big\{ & (R_S, R_J, R_L) \in \mathbb{R}_+^3 : \\
& R_S \leq \min_k I(\mathbf{Y}_k; U|V) - \max_l I(\mathbf{Z}_l; U|V), \\
& R_J \geq \max_k I(\tilde{\mathbf{X}}; U|V, \mathbf{Y}_k) + \max_k I(\tilde{\mathbf{X}}; V|\mathbf{Y}_k), \\
& R_L \geq \max_k I(\tilde{\mathbf{X}}; U|V, \mathbf{Y}_k) + \max_k I(\tilde{\mathbf{X}}; V|\mathbf{Y}_k) \\
& \quad - I(\tilde{\mathbf{X}}; U|X) + \min_k I(\mathbf{Y}_k; V) - \min_l I(\mathbf{Z}_l; V) \Big\}, \qquad (7) \\
\mathcal{R}_{\mathrm{C}} \supseteq \bigcup_{P_{V|U}, P_{U|\tilde{\mathbf{X}}}} \Big\{ & (R_S, R_J, R_L) \in \mathbb{R}_+^3 : \\
& R_S \leq \min_k I(\mathbf{Y}_k; U|V) - \max_l I(\mathbf{Z}_l; U|V), \\
& R_J \geq \max_k I(\tilde{\mathbf{X}}; U|V, \mathbf{Y}_k) + \max_k I(\tilde{\mathbf{X}}; V|\mathbf{Y}_k) \\
& \quad + \min_k I(\mathbf{Y}_k; U|V) - \max_l I(\mathbf{Z}_l; U|V), \\
& R_L \geq \max_k I(\tilde{\mathbf{X}}; U|V, \mathbf{Y}_k) + \max_k I(\tilde{\mathbf{X}}; V|\mathbf{Y}_k)
\end{aligned}$$

[3] Considering multiple states for the enrollment channel is unnecessary since its state could be estimated at the encoder and shared with the decoder through the helper data with a negligible cost.

$$- I(\tilde{\mathbf{X}}; U|X) + \min_k I(\mathbf{Y}_k; V) - \min_l I(\mathbf{Z}_l; V)\Big\}, \quad (8)$$

where auxiliary random variables V and U satisfy the Markov chain $V - U - \tilde{\mathbf{X}} - X - (\mathbf{Y}_k, \mathbf{Z}_l)$ for all $k \in \mathcal{K}$ and $l \in \mathcal{L}$, and $|\mathcal{V}| \leq |\tilde{\boldsymbol{\mathcal{X}}}| + 2(|\mathcal{K}| + |\mathcal{L}|) + 1$ and $|\mathcal{U}| \leq (|\tilde{\boldsymbol{\mathcal{X}}}| + 2(|\mathcal{K}| + |\mathcal{L}|) + 1)(|\tilde{\boldsymbol{\mathcal{X}}}| + |\mathcal{K}| + |\mathcal{L}| + 1)$.

Proof: The proof is available in Appendix A-A, where the random codebook is constructed based on two layered random coding techniques. The first layer consists of the auxiliary sequences V^n generated by P_V and the second layer consists of the auxiliary sequences U^n associated with $P_{U|V}$. The main challenge in the proof is to ensure that the secret-key uniformity (3) and the secrecy-leakage constraint (5) are satisfied for all possible receiver-eavesdropper states. To prove these constraints, the key idea is to introduce a random variable $\tilde{\mathbf{Z}}^n$ that jointly satisfies the equality $I(\tilde{\mathbf{Z}}; U|V) = \max_l I(\mathbf{Z}_l; U|V)$ and the Markov chain $V - U - \tilde{\mathbf{X}} - \tilde{\mathbf{Z}}$. The random variable $\tilde{\mathbf{Z}}^n$ plays a central role in analyzing the two constraints. This technique is not seen in the existing works [9], [21], [22] that study the secret-key generation with PUFs without compound channels. □

In Proposition 1, how each term in the constraints defining the regions $\mathcal{R}_{\mathrm{G}}$ and $\mathcal{R}_{\mathrm{C}}$ arises can be explained as follows. We begin with the region $\mathcal{R}_{\mathrm{G}}$. In the secret-key rate constraint, the term $\min_k I(\mathbf{Y}_k; U|V)$ represents the minimum rate required for reliably estimating the sequence U^n across all indices k, which in turn enables reliable reconstruction of the secret key since the key is extracted from U^n. On the other hand, the term $\max_l I(\mathbf{Z}_l; U|V)$ is the maximum rate at which Eve can gain information about U^n over all indices l. Therefore, the achievable secret-key rate is given by the difference $\min_k I(\mathbf{Y}_k; U|V) - \max_l I(\mathbf{Z}_l; U|V)$, similar to the one derived in [37, Th. 1] for compound sources. The terms $\max_k I(\tilde{\mathbf{X}}; V|\mathbf{Y}_k)$ and $\max_k I(\tilde{\mathbf{X}}; U|V, \mathbf{Y}_k)$ in the storage-rate constraint represents the rates of the bin indices at the first and second layers, respectively. In each layer, the maximum rate across all indices k must be shared between the encoder and decoder to ensure reliable reconstruction of the secret key at the decoder. For the privacy-leakage rate, note that we can expand the mutual information $\frac{1}{n}\max_l I(X^n; J|\mathbf{Z}_l^n)$ as $\frac{1}{n}H(J) - \frac{1}{n}H(J|X^n) - \frac{1}{n}\min_l I(\mathbf{Z}_l^n; J)$ by using the Markov chain $J - X^n - \mathbf{Z}_l^n$. In the constraint of the privacy-leakage rate, the first and second terms in the right-hand side represent the upper bound on the entropy $\frac{1}{n}H(J)$, the third term represents the upper bound on the conditional entropy $-\frac{1}{n}H(J|X^n)$, and the forth and fifth terms represent the upper bound on the mutual information $-\frac{1}{n}\min_l I(\mathbf{Z}_l^n; J)$.

For the region $\mathcal{R}_{\mathrm{C}}$, the codebook and coding scheme developed for proving the region $\mathcal{R}_{\mathrm{G}}$ are employed as a subsystem to prove the achievability part. One-time pad operation is applied to conceal the chosen secret key in the CS model by adding the secret key generated in the subsystem [9, Appx. B-C], which leads to the same achievable secret-key rate. However, the storage rate is different because the masked information must be saved in the public database together with the helper data generated by the subsystem, so that the chosen secret key can be reliably estimated at the decoder. Therefore, the storage rate of the CS model is the sum of the storage rate for the GS model (the subsystem) and the secret-key rate. Moreover, the privacy-leakage rate remains unchanged because the concealed information reveals no extra leakage to Eve after applying the one-time pad addition. Similar behaviors are reflected in the outer bound derived below in Proposition 2.

A special case of the GS model considered in this paper was investigated in [1]. One can check that, when $\Omega_{\tilde{X}} = \Omega_Y = \Omega_Z = |\mathcal{L}| = 1$, the region in (7) reduces to [1, Prop. 1].

Proposition 2 (Outer Bounds): We have

$$\begin{aligned}\mathcal{R}_{\mathrm{G}} \subseteq \bigcap_{k\in\mathcal{K}}\bigcap_{l\in\mathcal{L}}\bigcup_{P_{V|U},P_{U|\tilde{\mathbf{X}}}} \Big\{&(R_S, R_J, R_L) \in \mathbb{R}_+^3 : \\ &R_S \leq I(\mathbf{Y}_k; U|V) - I(\mathbf{Z}_l; U|V), \\ &R_J \geq I(\tilde{\mathbf{X}}; U|\mathbf{Y}_k), \\ &R_L \geq I(X; U|\mathbf{Y}_k) + I(\mathbf{Y}_k; V) - I(\mathbf{Z}_l; V)\Big\}, \quad (9)\\ \mathcal{R}_{\mathrm{C}} \subseteq \bigcap_{k\in\mathcal{K}}\bigcap_{l\in\mathcal{L}}\bigcup_{P_{V|U},P_{U|\tilde{\mathbf{X}}}} \Big\{&(R_S, R_J, R_L) \in \mathbb{R}_+^3 : \\ &R_S \leq I(\mathbf{Y}_k; U|V) - I(\mathbf{Z}_l; U|V), \\ &R_J \geq I(\tilde{\mathbf{X}}; U|\mathbf{Y}_k) + I(\mathbf{Y}_k; U|V) - I(\mathbf{Z}_l; U|V), \\ &R_L \geq I(X; U|\mathbf{Y}_k) + I(\mathbf{Y}_k; V) - I(\mathbf{Z}_l; V)\Big\}, \quad (10)\end{aligned}$$

where V and U satisfy the Markov chain $V - U - \tilde{\mathbf{X}} - X - (\mathbf{Y}_k, \mathbf{Z}_l)$, and $|\mathcal{V}| \leq |\tilde{\boldsymbol{\mathcal{X}}}| + 2(|\mathcal{K}| + |\mathcal{L}|) + 1$, $|\mathcal{U}| \leq (|\tilde{\boldsymbol{\mathcal{X}}}| + 2(|\mathcal{K}| + |\mathcal{L}|) + 1)(|\tilde{\boldsymbol{\mathcal{X}}}| + |\mathcal{K}| + |\mathcal{L}| + 1)$.

Proof: The proof is provided in Appendix A-B. For a fixed state (k, l), the proof is the same as that of [21, Th. 3 and 4] without considering the action cost. Therefore, we make use of the result of those theorems to derive Proposition 2 for the compound channel setting. However, due to the difference in the definition of the privacy-leakage rate, appropriate modifications are required. □

The region in (9) matches [1, Prop. 2] when $\Omega_{\tilde{X}} = \Omega_Y = \Omega_Z = |\mathcal{L}| = 1$. Moreover, in the non-compound settings, i.e., when $|\mathcal{K}| = 1 = |\mathcal{L}|$, the bounds in Propositions 1 and 2 match, yielding the following corollary.

Corollary 1 (Capacity Regions): When $|\mathcal{K}| = 1 = |\mathcal{L}|$, we have

$$\begin{aligned}\mathcal{R}_{\mathrm{G}} = \bigcup_{P_{V|U},P_{U|\tilde{\mathbf{X}}}} \Big\{&(R_S, R_J, R_L) \in \mathbb{R}_+^3 : \\ &R_S \leq I(\mathbf{Y}; U|V) - I(\mathbf{Z}; U|V), \\ &R_J \geq I(\tilde{\mathbf{X}}; U|\mathbf{Y}), \\ &R_L \geq I(X; U|\mathbf{Y}) + I(\mathbf{Y}; V) - I(\mathbf{Z}; V)\Big\}, \quad (11)\\ \mathcal{R}_{\mathrm{C}} = \bigcup_{P_{V|U},P_{U|\tilde{\mathbf{X}}}} \Big\{&(R_S, R_J, R_L) \in \mathbb{R}_+^3 : \\ &R_S \leq I(\mathbf{Y}; U|V) - I(\mathbf{Z}; U|V), \\ &R_J \geq I(\tilde{\mathbf{X}}; U|\mathbf{Y}) + I(\mathbf{Y}; U|V) - I(\mathbf{Z}; U|V), \\ &R_L \geq I(X; U|\mathbf{Y}) + I(\mathbf{Y}; V) - I(\mathbf{Z}; V)\Big\}, \quad (12)\end{aligned}$$

where (U, V) satisfy the same conditions as in Proposition 2.

Proof: We only sketch the proof of (11), as that of (12) follows similarly. When $|\mathcal{K}| = |\mathcal{L}| = 1$ and by dropping the indices k and l, the constraints in Proposition 1 become

$$R_S \le I(\mathbf{Y};U|V) - I(\mathbf{Z};U|V), \tag{13}$$

$$R_J \ge I(\tilde{\mathbf{X}};U|V,\mathbf{Y}) + I(\tilde{\mathbf{X}};V|\mathbf{Y}) \overset{(a)}{=} I(\tilde{\mathbf{X}};U|\mathbf{Y}), \tag{14}$$

$$\begin{aligned} R_L &\ge I(\tilde{\mathbf{X}};U|V,\mathbf{Y}) + I(\tilde{\mathbf{X}};V|\mathbf{Y}) \\ &\quad - I(\tilde{\mathbf{X}};U|X) + I(\mathbf{Y};V) - I(\mathbf{Z};V) \\ &= I(\tilde{\mathbf{X}};U|\mathbf{Y}) - I(\tilde{\mathbf{X}};U|X) + I(\mathbf{Y};V) - I(\mathbf{Z};V) \\ &\overset{(b)}{=} I(X;U|\mathbf{Y}) + I(\mathbf{Y};V) - I(\mathbf{Z};V), \end{aligned} \tag{15}$$

where (a) and (b) hold by the Markov chains $V - U - \tilde{\mathbf{X}} - \mathbf{Y}$ and $U - \tilde{\mathbf{X}} - X - \mathbf{Y}$, respectively. As $|\mathcal{K}| = |\mathcal{L}| = 1$, (13)–(15) match (9) in Proposition 2, and thus (11) is proved. □

Remark 1: The privacy-leakage rate in [21, Th. 3 and 4] without action cost is bounded as

$$\begin{aligned} R_L &\ge I(X;U,Y) - I(X;Y|V) + I(X;Z|V) \\ &= I(X;U|Y) + I(Y;V) - I(Z;V) + I(X;Z), \end{aligned} \tag{16}$$

where the equality holds by the Markov chain $V - X - (Y,Z)$. Compared to the privacy-leakage rate in (11) and (12), there is an extra term $I(X;Z)$, because the privacy-leakage rate constraint in [21, Ths. 3 and 4] is defined as $\frac{1}{n}I(X^n;J,Z^n) = \frac{1}{n}I(X^n;J|Z^n) + I(X;Z)$. Therefore, (11) and (12) coincide with [21, Ths. 3 and 4] (without action cost) if [21, eq. (5)] is replaced by (6).

In Propositions 1 and 2, the orders of the optimization (union) over the test channels $P_{V|U}, P_{U|\tilde{\mathbf{X}}}$ and the minimization (intersection) over the channel states (k,l) are reversed. Specifically, Proposition 1 requires one to choose test channels $P_{V|U}, P_{U|\tilde{\mathbf{X}}}$ that work simultaneously for all (k,l) pairs, whereas Proposition 2 allows one to choose different test channels $P_{V|U}, P_{U|\tilde{\mathbf{X}}}$ for a channel state pair (k,l), and then only keeps the intersection over what is achievable per channel state pair. Therefore, Proposition 1 imposes stronger requirements, and as a result, the regions in Proposition 2 may be potentially larger.

In the next subsection, we demonstrate that the regions in Propositions 1 and 2 match for Gaussian sources.

B. Gaussian Sources

In this subsection, we limit our discussion to a special case of setup in Section III-A where the enrollment channel is noiseless, i.e., $\tilde{\mathbf{X}} = X$. We consider $P_{X\mathbf{Y}_k\mathbf{Z}_l}$ the joint distribution of zero-mean Gaussian random variables with a non-singular covariance matrix. Suppose that the source $X \sim \mathcal{N}(0,\sigma_X^2)$, then it suffices to model the channels to the decoder and Eve as follows.

Lemma 1: Without loss of generality, one can write

$$\mathbf{Y}_k = \mathbf{H}_k X + \mathbf{N}_{\mathbf{Y}_k},\ \mathbf{Z}_l = \tilde{\mathbf{H}}_l X + \mathbf{N}_{\mathbf{Z}_l}, \tag{17}$$

where $\mathbf{H}_k \in \mathbb{R}^{\Omega_Y \times 1}$, $\tilde{\mathbf{H}}_l \in \mathbb{R}^{\Omega_Z \times 1}$, and $\mathbf{N}_{\mathbf{Y}_k} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_{\Omega_Y})$, and $\mathbf{N}_{\mathbf{Z}_l} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_{\Omega_Z})$ are independent of X. Here, $\mathbf{I}$ denotes the identity matrix.

Proof: See Appendix B. □

Remark 2: In the case where the enrollment channel is noisy, i.e., $\tilde{\mathbf{X}} \neq X$, the noise covariance matrices of the involved channels are not positive definite in general. This prevents the use of Cholesky decomposition to normalize them to identity matrices, and thus the channel models described in Lemma 1 may no longer be applicable.

Note that the single-letter expressions characterized in Propositions 1 and 2 can be extended to the channel model (17). To derive a closed-form analytical (parametric) expression for Gaussian sources, we directly leverage Proposition 1 to show the achievability. In the converse, we transform the problem in (17) into a scalar Gaussian problem using sufficient statistics [46, Ch. 2], which helps avoid the complexity of working with vector random variables. However, after the transformation, it is unclear whether all constraints in Definition 3, particularly (2), remain preserved under the scalar random variables. As a result, Proposition 2 may not hold when the vector random variables are replaced with scalar ones. To this end, as shown in the proof of Theorem 1, we derive new outer regions for the channel model (17) using scalar variables to establish the converse part of Theorem 1.

In the sequel, we define

$$k^* \in \arg\min_{k\in\mathcal{K}} \{\mathbf{H}_k^\intercal \mathbf{H}_k\}, \quad l^* \in \operatorname*{argmax}_{l\in\mathcal{L}} \{\tilde{\mathbf{H}}_l^\intercal \tilde{\mathbf{H}}_l\}. \tag{18}$$

To simplify the presentation of the results for Gaussian sources, we define the following rate constraints, where $\alpha \in (0,1]$ serves as a tuning parameter that adjusts the variance of the auxiliary Gaussian random variable. For further details, the reader is referred to (60).

$$R_S \le \frac{1}{2}\log\left(\frac{(\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1)(\alpha\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}+1)}{(\alpha\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1)(\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}+1)}\right), \tag{19}$$

$$R_J \ge \frac{1}{2}\log\left(\frac{\alpha\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1}{\alpha(\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1)}\right), \tag{20}$$

$$R_J \ge \frac{1}{2}\log\left(\frac{\alpha\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}+1}{\alpha(\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}+1)}\right), \tag{21}$$

$$R_L \ge \frac{1}{2}\log\left(\frac{\alpha\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1}{\alpha(\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1)}\right). \tag{22}$$

Theorem 1 (Capacity Regions): If $\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*} \ge \tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}$, then the capacity regions of the GS and CS models are

$$\mathcal{R}_{\mathrm{G}} = \bigcup_{0<\alpha\le 1} \{(R_S,R_J,R_L)\in\mathbb{R}_+^3 : \text{ (19), (20), and (22) are satisfied}\}, \tag{23}$$

$$\mathcal{R}_{\mathrm{C}} = \bigcup_{0<\alpha\le 1} \{(R_S,R_J,R_L)\in\mathbb{R}_+^3 : \text{ (19), (21), and (22) are satisfied}\}. \tag{24}$$

If $\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*} < \tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}$, then

$$\mathcal{R}_{\mathrm{G}} = \mathcal{R}_{\mathrm{C}} = \{(R_S,R_J,R_L) : R_S = 0, R_J \ge 0, R_L \ge 0\}. \tag{25}$$

Proof: The proof is provided in Appendix C and includes the achievability and converse parts. For the achievability, we set the test channel $P_{U|X}$ to be an AWGN channel and then apply Weinstein–Aronszajn Identity [52, Appx. B] to calculate the mutual information with vector random variables. Finally, we

use Lemma 5 to show that the optimal inner region is achieved when the indices of the channels to the decoder and Eve are k^* and l^*, respectively. For the converse, we begin by invoking the sufficient statistics [46] to convert vector variables to scalar ones. Next, we derive a single-letter characterization of the outer bound using these scalar variables, which is then used to determine the parametric expressions for the Gaussian case. The proof employs a technique based on Fisher information, introduced in [49]. In the final step, we again apply Lemma 5 to derive the outer region valid for an arbitrary pair (k, l), which is obtained when the decoder and Eve observe the channels indexed by k^* and l^* as well, coinciding with the optimal inner bound. □

In Theorem 1, the condition $\mathbf{H}_{k^*}^\intercal \mathbf{H}_{k^*} \geq \tilde{\mathbf{H}}_{l^*}^\intercal \tilde{\mathbf{H}}_{l^*}$ indicates that the channel power gain of the worst link to the decoder is at least as large as that of the best link to Eve. In the single-antenna case, i.e., $|\mathcal{K}| = 1 = |\mathcal{L}|$, this condition corresponds to physically degraded channels, where the channel to Eve is physically degraded with respect to the channel to the decoder.

Unlike the discrete sources, the inner and outer bounds for the Gaussian sources coincide. This is because, in the outer bound, the variable involved in the optimization is a scalar parameter, and rate constraints are given by logarithmic functions of the optimization parameter, α, and the values of channel power gains $\mathbf{H}_k^\intercal \mathbf{H}_k$ and $\tilde{\mathbf{H}}_l^\intercal \tilde{\mathbf{H}}_l$. These functions are monotonic with respect to the channel power gains for an arbitrary α. As a result, the order of intersection and union does not matter and can be swapped, which enable us to take the intersection over channel states (k, l) for each rate constraint and determine the saddle point (k^*, l^*) at which the outer bound matches the inner bound.

As a special case, when Ω_Y, Ω_Z, $|\mathcal{K}|$, and $|\mathcal{L}|$ are all one (let $\mathbf{H} = h$ and $\tilde{\mathbf{H}} = \tilde{h}$), the AWGN channels to the decoder and Eve reduce to $Y = hX + N_Y$ and $Z = \tilde{h}X + N_Z$, respectively, with $N_Y \sim \mathcal{N}(0,1)$ and $N_Z \sim \mathcal{N}(0,1)$. In this case, using the correlation coefficients of (X, Y), $\rho_{XY}^2 = \sigma_X^2 h^2/(\sigma_X^2 h^2 + 1)$ and that of (X, Z), $\rho_{XZ}^2 = \sigma_X^2 \tilde{h}^2/(\sigma_X^2 \tilde{h}^2 + 1)$, the regions (23) and (24) can be transformed as

$$\begin{aligned}
\mathcal{R}_{\mathrm{G}} = \bigcup_{0<\alpha\leq 1} \Big\{ & (R_S, R_J, R_L) \in \mathbb{R}_+^3 : \\
R_S &\leq \frac{1}{2}\log\frac{\alpha\rho_{XZ}^2 + 1 - \rho_{XZ}^2}{\alpha\rho_{XY}^2 + 1 - \rho_{XY}^2}, \\
R_J &\geq \frac{1}{2}\log\frac{\alpha\rho_{XY}^2 + 1 - \rho_{XY}^2}{\alpha}, \\
R_L &\geq \frac{1}{2}\log\frac{\alpha\rho_{XY}^2 + 1 - \rho_{XY}^2}{\alpha}\Big\},
\end{aligned} \tag{26}$$

$$\begin{aligned}
\mathcal{R}_{\mathrm{C}} = \bigcup_{0<\alpha\leq 1} \Big\{ & (R_S, R_J, R_L) \in \mathbb{R}_+^3 : \\
R_S &\leq \frac{1}{2}\log\frac{\alpha\rho_{XZ}^2 + 1 - \rho_{XZ}^2}{\alpha\rho_{XY}^2 + 1 - \rho_{XY}^2}, \\
R_J &\geq \frac{1}{2}\log\frac{\alpha\rho_{XZ}^2 + 1 - \rho_{XZ}^2}{\alpha}, \\
R_L &\geq \frac{1}{2}\log\frac{\alpha\rho_{XY}^2 + 1 - \rho_{XY}^2}{\alpha}\Big\}.
\end{aligned} \tag{27}$$

The regions in (26) and (27) align with [22, Cor. 1] when [22, eq. (5)] is replaced with (6) to eliminate the quantity $I(X; Z)$. Moreover, when the storage rate is not considered, i.e., (4) is not imposed, and Eve has no side information, i.e., $\rho_{XZ} = 0$, the regions in (26) and (27) simplify to [11, Th. 4.1 and 4.2].

C. Numerical Examples

We begin by presenting numerical calculations that illustrate the relationship between the secret-key and storage rates in the GS model, and then proceed to compare the secret-key and privacy-leakage rates of the GS and CS models under the same storage rate.

For investigating the relation of the secret-key and storage rates, we consider three cases, with the parameters summarized as follows: 1. $\Omega_Y = \Omega_Z = 1$ with $\mathbf{H}_{k^*}^\intercal = 0.95$ and $\tilde{\mathbf{H}}_{l^*}^\intercal = 0.8$, 2. $\Omega_Y = 3$ and $\Omega_Z = 1$ with $\mathbf{H}_{k^*}^\intercal = [0.95\ 0.95\ 0.95]$ and $\tilde{\mathbf{H}}_{l^*}^\intercal = 0.8$, and 3. $\Omega_Y = 3$ and $\Omega_Z = 4$ with $\mathbf{H}_{k^*}^\intercal = [0.95\ 0.95\ 0.95]$ and $\tilde{\mathbf{H}}_{l^*}^\intercal = [0.8\ 0.8\ 0.5\ 0.5]$. Moreover, we fix the variance of the source identifier as $\sigma_X^2 = 5$ for all cases.

For a given α, define the optimal storage rate $R_J(\alpha) = \frac{1}{2}\log\frac{\alpha\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1}{\alpha(\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1)}$, from which one can express α as

$$\alpha = \frac{1}{2^{2R_J(\alpha)} + (2^{2R_J(\alpha)} - 1)\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}}. \tag{28}$$

Substituting (28) into the right-hand side of (19), the optimal secret-key rate based on $R_J(\alpha)$ is given by $R_S(R_J(\alpha)) = \frac{1}{2}\log\left(\frac{\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}(1-2^{-2R_J(\alpha)})+\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}2^{-2R_J(\alpha)}+1}{\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}+1}\right)$. Note that if $R_J(\alpha) \to \infty$, $R_S^*(R_J(\alpha)) \to \frac{1}{2}\log\left(\frac{\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1}{\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}+1}\right)$.

Figure 3(a) depicts the relation of $(R_J(\alpha), R_S(R_J(\alpha)))$. In this figure, Case 2 (blue curve) shows a high secret-key rate compared to the other cases. This is due to an increase in the number of antennas at the decoder, which enhances the correlation between the source and observations at the terminal. On the other hand, in Case 3 (red curve), as the number of antennas at Eve increases, the secret-key rate drops compared to Case 2 because the stronger correlation with Eve reduces the key-generation rate. Also, Case 3 shows that even when Eve has more antennas, a positive secret-key rate is still achievable as long as $\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*} \geq \tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}$.

Figure 3(b) presents the secret-key and storage rates for a given α, focusing on Case 3, where the maximum secret-key rate reaches 0.2771 (cf. Fig. 3(a)). As $\alpha \to 0$, the storage rate grows unbounded, reflecting the absence of encoding, while the secret-key rate is maximized. In contrast, as $\alpha \to 1$, both rates approach zero. According to (60), this is because U is highly correlated with X when $\alpha \to 0$, leading to a high secret-key rate, whereas U becomes independent of X when $\alpha = 1$, resulting in zero secret-key rate.

Figures 3(c) and 3(d) respectively compare the secret-key and privacy-leakage rates between the GS and CS models for Case 2, under the same values of storage rates. In the low storage rate regime, the GS model results in a higher secret-key rate than the CS model, but at the cost of greater privacy leakage, highlighting a trade-off between these two security metrics. In the high storage rate regime, both models achieve the same secret-key rate, but the GS model still incurs greater privacy leakage than the CS model with the difference equal to the secret-key rate. This occurs because, in the CS

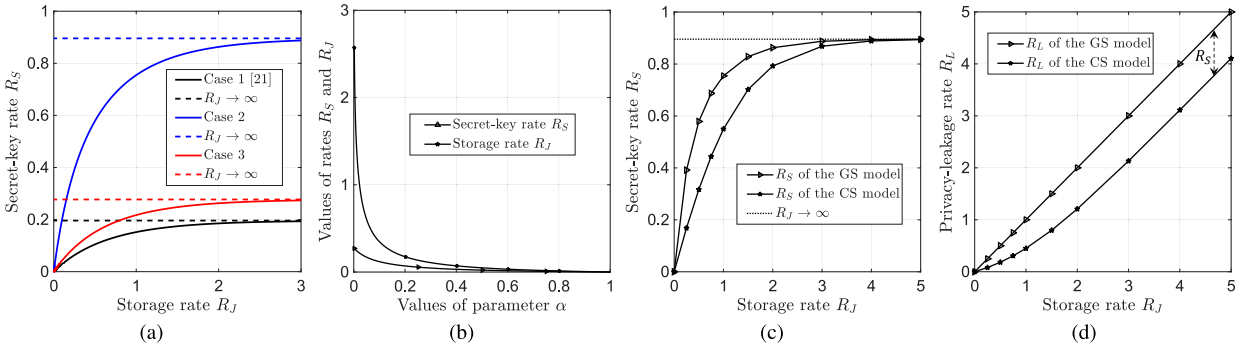

Fig. 3. (a) The relation of storage and secret-key rates in the GS model, (b) the secret-key and storage rates for a given value of α in the GS model, and for given a storage rate, a comparison of the secret-key and privacy-leakage rates in the GS and CS models are shown in (c) and (d), respectively.

model, the concealed data (with rate equal to the secret-key rate) reveals no information about the source identifier. These results suggest that in practical system designs, where the storage space is fixed, the GS model may be preferred in the low storage rate regime when maximizing the secret-key rate is important, while the CS model is preferable for minimizing privacy leakage. In the high storage rate regime, the CS model becomes the preferred option as it can achieve the same secret-key rate as the GS model but with lower privacy leakage.

IV. Concluding Remarks and Future Directions

We studied secret-key generation from private identifiers under channel uncertainty and multiple-output settings. This setup addresses authentication robustness against eavesdroppers in scenarios where the legitimate terminals lack exact CSI and Eve may use multiple antennas to improve signal reception. We derived inner and outer bounds for discrete sources and provided a full capacity characterization for Gaussian sources. The main technical contributions lie in proving the inner bound for discrete memoryless sources and the outer bound for the Gaussian case.

To prove the inner bound for discrete sources, we first extend the technique used in [40] for compound wiretap channels to ensure that the generated secret key is uniform and remains secret from Eve's observation for any channel state. For the outer bound in the Gaussian case, we first employ sufficient statistics to convert the vector problem into a scalar one, so that we can use the degraded property of the scalar Gaussian random variables to derive a single-letter characterization of the outer region. Then, we apply the single-letter characterization to derive the parametric expression for the Gaussian case with Fisher information-based techniques playing a crucial role in the derivation.

We also performed numerical evaluations for the Gaussian case to illustrate how changes in the number of antennas at the legitimate terminals and the eavesdropper affect the trade-offs between secret-key and storage rates, and to compare the secret-key and privacy-leakage rates of the GS and CS models under the same storage rate. The first set of results indicates that increasing the number of antennas at the decoder leads to a higher secret-key rate, while adding antennas at Eve reduces the secret-key rate. Nevertheless, even if Eve has more antennas, a positive secret-key rate remains achievable as long as the worst-case channel power gain at the decoder exceeds the best-case channel power gain at Eve. The second set of results shows that in the low storage-rate regime, the GS model achieves a higher secret-key rate, whereas the CS model offers better privacy-leakage performance. In contrast, in the high storage-rate regime, the CS model proves to be the more favorable choice as it provides the same secret-key rate as the GS model with lower privacy leakage.

A natural extension of this work is to characterize the capacity region for Gaussian sources under noisy enrollment channels. As noted in Lemma 2, since we may not be able to model the covariance matrices of the independent noises as identity matrices, the analysis will become more involved compared to that of Theorem 1. This arises because the scalar problem obtained by transforming the original vector problem using sufficient statistics results in more complicated forms than the expressions in Lemma 7. Extending the scenario to the case of vector Gaussian sources is also an interesting topic. Another possible avenue is to include user identification as studied in [23], [24], [25] and see how the identification rate influences the capacity region.

Appendix A
Proof of Propositions 1 and 2

A. Proof of Proposition 1

We only prove (7) since (8) follows similarly with an extra procedure, a one-time pad procedure to conceal the chosen secret key. As a result, an extra rate equal to the secret-key rate is needed for storing the concealed key information in the database, which appears in the constraint of the storage rate of the CS model.

Fix the test channels $P_{U|\tilde{\mathbf{X}}}$ and $P_{V|U}$ and let $\delta > 0$. In the following, we show that these rates are achievable

$$R_S \triangleq \min_k I(\mathbf{Y}_k; U|V) - \max_l I(\mathbf{Z}_l; U|V) - \delta, \tag{29}$$

$$R_J \triangleq \max_k I(\tilde{\mathbf{X}}; U|V, \mathbf{Y}_k) + \max_k I(\tilde{\mathbf{X}}; V|\mathbf{Y}_k) + 5\delta, \tag{30}$$

$$R_L \triangleq \max_k I(\tilde{\mathbf{X}}; U|V, \mathbf{Y}_k) + \max_k I(\tilde{\mathbf{X}}; V|\mathbf{Y}_k) - I(\tilde{\mathbf{X}}; U|X) + \min_k I(\mathbf{Y}_k; V) - \min_l I(\mathbf{Z}_l; V) + 4\delta. \tag{31}$$

For the random codebook construction, we also define

$$R_v \triangleq I(\tilde{\mathbf{X}}; V) + \delta, \quad R_{J_{v_1}} \triangleq \max_k I(\tilde{\mathbf{X}}; V|\mathbf{Y}_k) + 2\delta, \tag{32}$$

$$R_u \triangleq I(\tilde{\mathbf{X}}; U|V) + \delta, \quad R_{J_{u_1}} \triangleq \max_k I(\tilde{\mathbf{X}}; U|\mathbf{Y}_k, V) + 3\delta, \tag{33}$$

and the sets $\mathcal{J}_{v_1} \triangleq [1 : 2^{nR_{J_{v_1}}}]$, $\mathcal{J}_{v_2} \triangleq [1 : 2^{n(R_v - R_{J_{v_1}})}]$, $\mathcal{J}_{u_1} \triangleq [1 : 2^{nR_{J_{u_1}}}]$, $\mathcal{J}_{u_2} \triangleq [1 : 2^{nR_S}]$, $\mathcal{J}_{u_3} \triangleq [1 : 2^{n(\max_l I(\mathbf{Z}_l;U|V)-\delta)}]$. Note that $R_u = R_{J_{u_1}} + R_S + \max_l I(\mathbf{Z}_l; U|V) - \delta$.

Random Codebook: Generate i.i.d. sequences $v^n(j_{v_1}, j_{v_2})$ from P_{V^n}, where $(j_{v_1}, j_{v_2}) \in \mathcal{J}_{v_1} \times \mathcal{J}_{v_2}$. For every (j_{v_1}, j_{v_2}), generate i.i.d. sequences $u^n(j_{u_1}, j_{u_2}, j_{u_3}, j_{v_1}, j_{v_2})$, where $(j_{u_1}, j_{u_2}, j_{u_3}) \in \mathcal{J}_{u_1} \times \mathcal{J}_{u_2} \times \mathcal{J}_{u_3}$, according to $P_{U^n|V^n=v^n(j_{v_1},j_{v_2})}$. All the generated sequences $(V^n(j_{v_1}, j_{v_2}), U^n(j_{u_1}, j_{u_2}, j_{u_3}, j_{v_1}, j_{v_2}))$ form the codebook $\mathcal{C}_n$.

Encoding: Observing $\tilde{\mathbf{x}}^n$, the encoder first finds (j_{v_1}, j_{v_2}) such that $(\tilde{\mathbf{x}}^n, v^n(j_{v_1}, j_{v_2})) \in \mathcal{T}_\delta^n$. Then, it looks for $(j_{u_1}, j_{u_2}, j_{u_3})$ such that $(\tilde{\mathbf{x}}^n, u^n(j_{u_1}, j_{u_2}, j_{u_3}, j_{v_1}, j_{v_2})) \in \mathcal{T}_\delta^n(\tilde{\mathbf{X}}U|v^n(j_{v_1}, j_{v_2}))$. If a unique tuple $(j_{u_1}, j_{u_2}, j_{u_3}, j_{v_1}, j_{v_2})$ is found, the encoder assigns the helper data $j = (j_{v_1}, j_{u_1})$ and the secret key $s = j_{u_2}$. If multiple such tuples are found, the encoder selects one tuple uniformly at random and assigns $j = (j_{v_1}, j_{u_1})$ and $s = j_{u_2}$. In case no such tuple exists, the encoder sets all j_{v_1}, j_{v_2}, j_{u_1}, j_{u_2}, and j_{u_3} to be one and assigns $j = (1, 1)$ and $s = 1$.

Decoding: From $\mathbf{y}_k^n$ and (j_{u_1}, j_{v_1}), the decoder first looks for the unique index $\hat{j}_{v_2}$ such that $(\mathbf{y}_k^n, v^n(j_{v_1}, \hat{j}_{v_2})) \in \mathcal{T}_\delta^n$. Then, it looks for the unique pair $(\hat{j}_{u_2}, \hat{j}_{u_3})$ such that $(\mathbf{y}_k^n, u^n(j_{u_1}, \hat{j}_{u_2}, \hat{j}_{u_3}, j_{v_1}, \hat{j}_{v_2})) \in \mathcal{T}_\delta^n(\mathbf{Y}_k U|v^n(j_{v_1}, \hat{j}_{v_2}))$. If the indices $\hat{j}_{u_2}, \hat{j}_{u_3}$, and $\hat{j}_{v_2}$ are uniquely determined, then the decoder estimates $\hat{s} = \hat{j}_{u_2}$; otherwise, it sets $\hat{s} = 1$ and declares an error.

In the following, we write $V^n(J_{v_1}, J_{v_2})$ and $U^n(J_{u_1}, J_{u_2}, J_{u_3}, J_{v_1}, J_{v_2})$ as V^n and U^n for convenience.

Analysis of Error Probability: Possible error events at the encoder are

$$\mathcal{E}_1\colon \{(\tilde{\mathbf{X}}^n, V^n(j_{v_1}, j_{v_2})) \notin \mathcal{T}_\delta^n, \forall (j_{v_1}, j_{v_2}) \in \mathcal{J}_{v_1} \times \mathcal{J}_{v_2}\},$$
$$\mathcal{E}_2\colon \{(\tilde{\mathbf{X}}^n, U^n(j_{u_1}, j_{u_2}, j_{u_3}, J_{v_1}, J_{v_2})) \notin \mathcal{T}_\delta^n(\tilde{\mathbf{X}}U|V^n), \forall (j_{u_1}, j_{u_2}, j_{u_3}) \in \mathcal{J}_{u_1} \times \mathcal{J}_{u_2} \times \mathcal{J}_{u_3}\},$$

and those at the decoder are

$$\mathcal{E}_3\colon \{(\mathbf{Y}_k^n, U^n, V^n) \notin \mathcal{T}_\delta^n\},$$
$$\mathcal{E}_4\colon \{\exists j'_{v_2} \in \mathcal{J}_{v_2}, j'_{v_2} \neq J_{v_2} \text{ and } (\mathbf{Y}_k^n, V^n(J_{v_1}, j'_{v_2})) \in \mathcal{T}_\delta^n\},$$
$$\mathcal{E}_5\colon \{\exists (j'_{u_2}, j'_{u_3}) \in \mathcal{J}_{u_2} \times \mathcal{J}_{u_3}, (j'_{u_2}, j'_{u_3}) \neq (J_{u_2}, J_{u_3}) \text{ and } (\mathbf{Y}_k^n, U^n(J_{u_1}, j'_{u_2}, j'_{u_3}, J_{v_1}, J_{v_2})) \in \mathcal{T}_\delta^n(\mathbf{Y}_k U|V^n)\}.$$

Then, we have

$$\begin{aligned}&\max_k \mathbb{P}\{\hat{S}_k \neq S\} = \mathbb{P}\{\cup_{i=1}^5 \mathcal{E}_i\}\\ &\leq \mathbb{P}\{\mathcal{E}_1\} + \mathbb{P}\{\mathcal{E}_2\} + \mathbb{P}\{\mathcal{E}_3 \cap (\mathcal{E}_1 \cup \mathcal{E}_2)^c\} + \mathbb{P}\{\mathcal{E}_4\} + \mathbb{P}\{\mathcal{E}_5\}. \quad (34)\end{aligned}$$

The first and second terms vanish by the covering lemma [51, Lemma 3.3] since $R_v > I(\tilde{\mathbf{X}}; V)$ and $R_u > I(\tilde{\mathbf{X}}; U|V)$, respectively. The third term vanishes by Markov lemma [46, Lemma 15.8.1]. The last two terms vanish by the packing lemma [51, Lemma 3.1], since the rate of index $\hat{j}_{v_2}$ is less than $\min_k I(\mathbf{Y}_k; V)$ and that of index pair $(\hat{j}_{u_2}, \hat{j}_{u_3})$ is less than $\min_k I(\mathbf{Y}_k; U|V)$, respectively. Hence, we have

$$\lim_{n\to\infty} \max_k \mathbb{P}\{\hat{S}_k \neq S\} \to 0. \quad (35)$$

Before we analyze the constraints (3), (4), (5), and (6) in Definition 3, we state two lemmas. The first one, Lemma 2, is an extended version of [40, Lemma A.1] to incorporate conditional mutual information.

Lemma 2: If the inequality $I(\mathbf{Z}_l; U|V) < I(\mathbf{Z}_{l'}; U|V)$ holds for $l, l' \in \mathcal{L}$, then there exists a vector random variable $\mathbf{A}$ such that the equality $I(\mathbf{Z}_l, \mathbf{A}; U|V) = I(\mathbf{Z}_{l'}; U|V)$ and the Markov chain $V - U - \tilde{\mathbf{X}} - (\mathbf{Z}_l, \mathbf{Z}_{l'}) - \mathbf{A}$ are satisfied.

Proof: Let B be a binary random variable taking values l and l' with probabilities p and $1-p$, respectively, where $0 \leq p \leq 1$, and assume that B is independent of all other random variables. Define $\mathbf{A} \triangleq (\mathbf{Z}_B, B)$ and $\Gamma(p) = I(\mathbf{Z}_l, \mathbf{A}; U|V)$. Due to the independence of B, we have

$$\Gamma(p) = pI(\mathbf{Z}_l; U|V) + (1-p)I(\mathbf{Z}_l, \mathbf{Z}_{l'}; U|V). \quad (36)$$

Now observe that $\Gamma(1) < I(\mathbf{Z}_{l'}; U|V) \leq \Gamma(0)$, where the first inequality follows by the assumption $I(\mathbf{Z}_l; U|V) < I(\mathbf{Z}_{l'}; U|V)$. Due to the continuity of the function $\Gamma(p)$ for all $p \in [0, 1]$, there exists a $p^* \in [0, 1]$ such that $\Gamma(p^*) = I(\mathbf{Z}_{l'}; U|V)$, and thus the equality $I(\mathbf{Z}_l, \mathbf{A}; U|V) = I(\mathbf{Z}_{l'}; U|V)$ is satisfied with $\mathbf{A} = (\mathbf{Z}_{B^*}, B^*)$ and B^* taking the values l and l' with probabilities p^* and $1-p^*$, respectively. Also, this choice of $\mathbf{A}$ ensures that the Markov chain $V - U - \tilde{\mathbf{X}} - (\mathbf{Z}_l, \mathbf{Z}_{l'}) - \mathbf{A}$ is satisfied. □

Lemma 2 is used to show the existence of a random variable that achieves $\max_l I(\mathbf{Z}_l; U|V)$ and forms a Markov chain with $(V, U, \tilde{\mathbf{X}})$, as detailed in the following intermediate step.

Intermediate Step: For any $l \in \mathcal{L}$, by Lemma 2, there exists $\mathbf{A}$ such that for

$$\tilde{\mathbf{Z}} \triangleq (\mathbf{Z}_l, \mathbf{A}), \quad (37)$$

we have $I(\tilde{\mathbf{Z}}; U|V) = \max_l I(\mathbf{Z}_l; U|V)$ and

$$V - U - \tilde{\mathbf{X}} - \tilde{\mathbf{Z}}. \quad (38)$$

Moreover, define a binary random variable T, which takes 1 if $(U^n, \tilde{\mathbf{X}}^n, \tilde{\mathbf{Z}}^n) \in \mathcal{T}_\delta^n$ and 0 otherwise. For large enough n, it holds that

$$P_T(1) \geq 1 - \tilde{\delta}_n \quad (39)$$

with $\tilde{\delta}_n \downarrow 0$ as $\delta \downarrow 0$ and $n \to \infty$. This follows because the pair $(U^n, \tilde{\mathbf{X}}^n)$ is jointly typical with probability approaching one, as shown in (35), and $\tilde{\mathbf{Z}}^n$ is i.i.d. generated according to $\prod_{t=1}^n P_{\tilde{\mathbf{Z}}_t|\tilde{\mathbf{X}}_t}$ from (38), and thus (39) follows by applying the Markov lemma [46, Lemma 15.8.1]. Similarly, we have joint typicality of $(V^n, \tilde{\mathbf{Z}}^n)$ as $(V^n, \tilde{\mathbf{X}}^n)$ is jointly typical with high probability. These properties are applied in proving the next lemma, which plays a key role in the analyses of the secret-key uniformity and secrecy-leakage.

Lemma 3: For an arbitrary index $l \in \mathcal{L}$, we have

$$H(J_{u_2}|J_{u_1}, J_{v_1}, \mathbf{Z}_l^n, \mathcal{C}_n) \geq n(R_S - \xi_n), \quad (40)$$

where ξ_n goes to zero as $\delta \downarrow 0$ and $n \to \infty$.

Proof: We have

$$\begin{aligned}&H(J_{u_2}|J_{u_1}, J_{v_1}, \mathbf{Z}_l^n, \mathcal{C}_n)\\ &\geq H(J_{u_2}|J_{u_1}, J_{v_1}, J_{v_2}, \mathbf{Z}_l^n, \mathbf{A}^n, \mathcal{C}_n)\\ &\overset{(a)}{=} H(J_{u_2}|J_{u_1}, J_{v_1}, J_{v_2}, \tilde{\mathbf{Z}}^n, \mathcal{C}_n)\\ &= H(J_{u_1}, J_{u_2}, J_{u_3}, J_{v_1}, J_{v_2}, \tilde{\mathbf{Z}}^n|\mathcal{C}_n)\\ &\quad - H(J_{u_3}|J_{u_1}, J_{u_2}, J_{v_1}, J_{v_2}, \tilde{\mathbf{Z}}^n, \mathcal{C}_n)\\ &\quad - H(J_{u_1}, J_{v_1}, J_{v_2}, \tilde{\mathbf{Z}}^n|\mathcal{C}_n)\\ &\overset{(b)}{\geq} H(J_{u_1}, J_{u_2}, J_{u_3}, J_{v_1}, J_{v_2}, \tilde{\mathbf{Z}}^n|\mathcal{C}_n)\end{aligned}$$

$$
\begin{aligned}
&- H(J_{u_1}, J_{v_1}, J_{v_2}, \tilde{\mathbf{Z}}^n|\mathcal{C}_n) - n\delta_n \\
&\overset{(c)}{\geq} H(U^n, \tilde{\mathbf{Z}}^n|\mathcal{C}_n) - H(\tilde{\mathbf{Z}}^n|V^n, \mathcal{C}_n) \\
&\quad - H(J_{u_1}, J_{v_1}, J_{v_2}|\mathcal{C}_n) - n\delta_n \\
&\geq P_T(1)H(U^n, \tilde{\mathbf{Z}}^n|T=1, \mathcal{C}_n) - H(\tilde{\mathbf{Z}}^n|V^n, \mathcal{C}_n) \\
&\quad - H(J_{u_1}|\mathcal{C}_n) - H(J_{v_1}|\mathcal{C}_n) - H(J_{v_2}|\mathcal{C}_n) - n\delta_n \\
&\overset{(d)}{\geq} (1-\tilde{\delta}_n)H(U^n, \tilde{\mathbf{Z}}^n|T=1, \mathcal{C}_n) - H(\tilde{\mathbf{Z}}^n|V^n, \mathcal{C}_n) \\
&\quad - H(J_{u_1}|\mathcal{C}_n) - H(J_{v_1}|\mathcal{C}_n) - H(J_{v_2}|\mathcal{C}_n) - n\delta_n \\
&\overset{(e)}{\geq} n(1-\tilde{\delta}_n)(I(\tilde{\mathbf{X}}; U) + H(\tilde{\mathbf{Z}}|U) - 2\epsilon_\delta) - H(\tilde{\mathbf{Z}}^n|V^n, \mathcal{C}_n) \\
&\quad - H(J_{u_1}|\mathcal{C}_n) - H(J_{v_1}|\mathcal{C}_n) - H(J_{v_2}|\mathcal{C}_n) - n\delta_n \\
&\overset{(f)}{\geq} n(I(\tilde{\mathbf{X}}; U) + H(\tilde{\mathbf{Z}}|U) - H(\tilde{\mathbf{Z}}|V) - \gamma_n) \\
&\quad - H(J_{u_1}|\mathcal{C}_n) - H(J_{v_1}|\mathcal{C}_n) - H(J_{v_2}|\mathcal{C}_n) - n\delta'_n \\
&\overset{(g)}{\geq} n(I(\tilde{\mathbf{X}}; U) - I(\tilde{\mathbf{Z}}; U|V) - \gamma_n) \\
&\quad - n(\max_k I(\tilde{\mathbf{X}}; U|V, \mathbf{Y}_k) + 3\delta) \\
&\quad - n(\max_k I(\tilde{\mathbf{X}}; V|\mathbf{Y}_k) + 2\delta) \\
&\quad - n(\min_k I(\mathbf{Y}_k; V) - \delta) - n\delta'_n \\
&\overset{(h)}{=} n(I(\tilde{\mathbf{X}}; U) - I(\tilde{\mathbf{Z}}; U|V)) \\
&\quad - n(\max_k\{I(\tilde{\mathbf{X}}; U|V) - I(\mathbf{Y}_k; U|V)\}) \\
&\quad - n(\max_k\{I(\tilde{\mathbf{X}}; V) - I(\mathbf{Y}_k; V)\}) - n\min_k I(\mathbf{Y}_k; V) \\
&\quad - n(4\delta + \gamma_n + \delta'_n) \\
&\overset{(i)}{=} n(\min_k I(\mathbf{Y}_k; U|V) - \max_l I(\mathbf{Z}_l; U|V) - \delta - \xi_n) \\
&= n(R_S - \xi_n),
\end{aligned} \tag{41}
$$

where (a) holds from (37), (b) follows because the index J_{u_3} can be reliably estimated from $(J_{u_1}, J_{u_2}, J_{v_1}, J_{v_2}, \tilde{\mathbf{Z}}^n)$, as $\frac{1}{n}\log|\mathcal{J}_3| < \max_l I(\mathbf{Z}_l; U|V) = I(\tilde{\mathbf{Z}}; U|V)$, (c) holds because U^n and V^n are determined by the tuple $(J_{u_1}, J_{u_2}, J_{u_3}, J_{v_1}, J_{v_2})$ and the pair (J_{v_1}, J_{v_2}), respectively, (d) follows from (39), and (e) follows from

$$
\begin{aligned}
P_{\tilde{\mathbf{Z}}^n U^n}(\tilde{\mathbf{z}}^n, u^n) &\leq \sum_{\tilde{\mathbf{x}}^n \in \mathcal{T}_\delta^n(\tilde{\mathbf{X}}|\tilde{\mathbf{z}}^n, u^n)} P_{\tilde{\mathbf{X}}^n \tilde{\mathbf{Z}}^n}(\tilde{\mathbf{x}}^n, \tilde{\mathbf{z}}^n) \\
&\leq 2^{n(H(\tilde{\mathbf{X}}|\tilde{\mathbf{Z}}, U) - \epsilon_\delta)} \cdot 2^{-n(H(\tilde{\mathbf{X}}, \tilde{\mathbf{Z}}) - \epsilon_\delta)} \\
&= 2^{-n(I(\tilde{\mathbf{X}}; U) + H(\tilde{\mathbf{Z}}|U) - 2\epsilon_\delta)},
\end{aligned} \tag{42}
$$

(f) follows because, as shown in the intermediate step, $(V^n, \tilde{\mathbf{Z}}^n)$ is jointly typical with high probability and thus $H(\tilde{\mathbf{Z}}^n|V^n, \mathcal{C}_n) \leq n(H(\tilde{\mathbf{Z}}|V) + \gamma_n)$ (cf. [53, eq. (16)]) and $\delta'_n \triangleq \tilde{\delta}_n(I(\tilde{\mathbf{X}}; U) + H(\tilde{\mathbf{Z}}|U)) + 2(1-\tilde{\delta}_n)\epsilon_\delta + \delta_n$, (g) is due to the Markov chain (38) and $H(J_{u_1}|\mathcal{C}_n) \leq nR_{J_{u_1}}$, $H(J_{v_1}|\mathcal{C}_n) \leq nR_{J_{v_1}}$, $H(J_{v_2}|\mathcal{C}_n) \leq n(R_v - R_{J_{v_1}}) = n(\min_k I(\mathbf{Y}_k; V) - \delta)$, (h) is due to the Markov chain $V - U - \tilde{\mathbf{X}} - \mathbf{Y}_k$, (i) follows from $I(\tilde{\mathbf{Z}}; U|V) = \max_l I(\mathbf{Z}_l; U|V)$ and $\xi_n \triangleq 3\delta + \gamma_n + \delta'_n$. □

Analyses of Uniformity and Secrecy-Leakage: The constraints of (3) and (5) can be evaluated as

$$
\begin{aligned}
H(S|\mathcal{C}_n) &= H(J_{u_2}|\mathcal{C}_n) \\
&\geq H(J_{u_2}|J_{u_1}, J_{v_1}, \mathbf{Z}_l^n, \mathcal{C}_n) \\
&\geq n(R_S - \xi_n),
\end{aligned} \tag{43}
$$

and

$$
\begin{aligned}
\max_l I(S; J, \mathbf{Z}_l^n|\mathcal{C}_n) &= \max_l I(J_{u_2}; J_{u_1}, J_{v_1}, \mathbf{Z}_l^n|\mathcal{C}_n) \\
&= \max_l\{H(J_{u_2}|\mathcal{C}_n) - H(J_{u_2}|J_{u_1}, J_{v_1}, \mathbf{Z}_l^n, \mathcal{C}_n)\} \\
&\leq \max_l\{nR_S - n(R_S - \xi_n)\} = n\xi_n,
\end{aligned} \tag{44}
$$

where (43) and (44) follow from Lemma 3.

Analysis of Storage Rate: The helper data is $J = (J_{v_1}, J_{u_1})$, and thus the total storage rate is $\frac{1}{n}\log|\mathcal{J}_{v_1}||\mathcal{J}_{u_1}| = R_{J_{v_1}} + R_{J_{u_1}} = R_J$.

Analysis of Privacy-Leakage Rate: We have

$$
\begin{aligned}
&\max_l I(X^n; J|\mathbf{Z}_l^n, \mathcal{C}_n) = \max_l I(X^n; J_{u_1}, J_{v_1}|\mathbf{Z}_l^n, \mathcal{C}_n) \\
&= I(X^n; J_{u_1}, J_{v_1}|\mathcal{C}_n) - \min_l I(\mathbf{Z}_l^n; J_{u_1}, J_{v_1}|\mathcal{C}_n) \\
&\leq H(J_{u_1}|\mathcal{C}_n) + H(J_{v_1}|\mathcal{C}_n) - H(J_{u_1}, J_{v_1}|X^n, \mathcal{C}_n) \\
&\quad - \min_l I(\mathbf{Z}_l^n; J_{u_1}, J_{v_1}|\mathcal{C}_n) \\
&= H(J_{u_1}|\mathcal{C}_n) + H(J_{v_1}|\mathcal{C}_n) - H(\tilde{\mathbf{X}}^n, J_{u_1}, J_{v_1}|X^n, \mathcal{C}_n) \\
&\quad + H(\tilde{\mathbf{X}}^n|X^n, J_{u_1}, J_{v_1}, \mathcal{C}_n) - \min_l I(\mathbf{Z}_l^n; J_{u_1}, J_{v_1}|\mathcal{C}_n) \\
&\overset{(a)}{\leq} H(J_{u_1}|\mathcal{C}_n) + H(J_{v_1}|\mathcal{C}_n) - nH(\tilde{\mathbf{X}}|X) \\
&\quad + n(H(\tilde{\mathbf{X}}|X, U) + \epsilon'_n) - \min_l I(\mathbf{Z}_l^n; J_{u_1}, J_{v_1}|\mathcal{C}_n) \\
&\leq H(J_{u_1}|\mathcal{C}_n) + H(J_{v_1}|\mathcal{C}_n) - nI(\tilde{\mathbf{X}}; U|X) \\
&\quad - \min_l I(\mathbf{Z}_l^n; J_{v_1}|\mathcal{C}_n) + n\epsilon'_n \\
&\leq H(J_{u_1}|\mathcal{C}_n) + H(J_{v_1}|\mathcal{C}_n) - nI(\tilde{\mathbf{X}}; U|X) \\
&\quad - \min_l\{H(\mathbf{Z}_l^n) - H(\mathbf{Z}_l^n|J_{v_1}, J_{v_2}, \mathcal{C}_n)\} \\
&\quad + \max_l I(J_{v_2}; \mathbf{Z}_l^n|J_{v_1}, \mathcal{C}_n) + n\epsilon'_n \\
&\overset{(b)}{\leq} H(J_{u_1}|\mathcal{C}_n) + H(J_{v_1}|\mathcal{C}_n) - nI(\tilde{\mathbf{X}}; U|X) \\
&\quad - \min_l\{H(\mathbf{Z}_l^n) - H(\mathbf{Z}_l^n|V^n, \mathcal{C}_n)\} + H(J_{v_2}|\mathcal{C}_n) + n\epsilon'_n \\
&\overset{(c)}{\leq} H(J_{u_1}|\mathcal{C}_n) + H(J_{v_1}|\mathcal{C}_n) - nI(\tilde{\mathbf{X}}; U|X) \\
&\quad - n(\min_l\{H(\mathbf{Z}_l) - H(\mathbf{Z}_l|V)\}) + H(J_{v_2}|\mathcal{C}_n) + n\epsilon''_n \\
&\leq n(\max_k I(\tilde{\mathbf{X}}; V|\mathbf{Y}_k) + \max_k I(\tilde{\mathbf{X}}; U|V, \mathbf{Y}_k) + 4\delta \\
&\quad - I(\tilde{\mathbf{X}}; U|X) + \min_k I(\mathbf{Y}_k; V) - \min_l I(\mathbf{Z}_l; V) + \epsilon''_n) \\
&= n(R_L + \epsilon''_n),
\end{aligned} \tag{45}
$$

where (a) follows from (46), shown below, and the codebook $\mathcal{C}_n$ is independent of $(\tilde{\mathbf{X}}^n, X^n, \mathbf{Y}_k^n, \mathbf{Z}_l^n)$, (b) holds because V^n is a function of (J_{v_1}, J_{v_2}), and (c) follows because $H(Z_l^n|V^n, \mathcal{C}_n) \leq n(H(Z_l|V) + \gamma'_n)$ and $\epsilon''_n \triangleq \gamma'_n + \epsilon'_n$. For brevity, define $E \triangleq (J_{u_2}, J_{u_3}, J_{v_2})$, where the decoder can reliably estimate the index E for given $(\mathbf{Y}_k^n, J_{u_1}, J_{v_1})$. Observe that

$$
\begin{aligned}
&H(\tilde{\mathbf{X}}^n|X^n, J_{u_1}, J_{v_1}, \mathcal{C}_n) \\
&= H(\tilde{\mathbf{X}}^n|X^n, J_{u_1}, J_{v_1}, E, \mathcal{C}_n) + I(E; \tilde{\mathbf{X}}^n|X^n, J_{u_1}, J_{v_1}, \mathcal{C}_n) \\
&\overset{(a)}{\leq} H(\tilde{\mathbf{X}}^n|X^n, U^n, \mathcal{C}_n) + H(E|X^n, J_{u_1}, J_{v_1}, \mathcal{C}_n) \\
&\overset{(b)}{\leq} H(\tilde{\mathbf{X}}^n|X^n, U^n, \mathcal{C}_n) + H(E|\mathbf{Y}_k^n, J_{u_1}, J_{v_1}, \mathcal{C}_n) \\
&\overset{(c)}{\leq} H(\tilde{\mathbf{X}}^n|X^n, U^n, \mathcal{C}_n) + n\epsilon_n \\
&\overset{(d)}{\leq} n(H(\tilde{\mathbf{X}}|X, U) + \epsilon'_n),
\end{aligned} \tag{46}
$$

where (a) follows since U^n is a function of $(J_{u_1}, J_{u_2}, J_{u_3}, J_{v_1}, J_{v_2})$, (b) is due to the Markov chain $E - (X^n, J_{u_1}, J_{v_1}) - \mathbf{Y}_k^n$ and conditioning reduces entropy, (c) follows from Fano's inequality with $\epsilon_n \downarrow 0$ as $\delta \downarrow 0$ and $n \to \infty$, and (d) because $H(\tilde{\mathbf{X}}^n|X^n, U^n, \mathcal{C}_n) \le n(H(\tilde{\mathbf{X}}|X, U)+\gamma_n'')$ for jointly typical sequences (cf. [53, eq. (16)]) and $\epsilon_n' \triangleq \gamma_n'' + \epsilon_n$.

From (35), (43), (44), and (45), there must be at least one codebook satisfying all the conditions in Definition 3, so that the region in (7) is achievable.

B. Proof of Proposition 2

The cardinality bounds of the auxiliary random variables can be obtained from the support lemma [51, Lemma 3.4].

We show the proof for the GS model via a result derived in [21] in the absence of action cost. By replacing (6) with $I(X^n; J, \mathbf{Z}_l^n) \le n(R_L + \delta)$, the outer bound for a pair (k, l), denoted by $\mathcal{O}_{G_{kl}}$, is [21, Th. 3]

$$\begin{aligned}\mathcal{O}_{G_{kl}} \triangleq \bigcup_{P_{V|U}, P_{U|\tilde{\mathbf{X}}}} \{(R_S, R_J, R_L) \in \mathbb{R}_+^3 :\\ R_S \le I(\mathbf{Y}_k; U|V) - I(\mathbf{Z}_l; U|V),\ R_J \ge I(\tilde{\mathbf{X}}; U|\mathbf{Y}_k),\\ R_L \ge I(X; U, \mathbf{Y}_k) - I(X; \mathbf{Y}_k|V) + I(X; \mathbf{Z}_l|V)\},\end{aligned} \tag{47}$$

where V and U satisfy $V - U - \tilde{\mathbf{X}} - X - (\mathbf{Y}_k, \mathbf{Z}_l)$.

In Definition 3, the constraints on the secret-key and storage rates are the same as in [21, Def. 6], and the resulting bounds are given in the same form as in (47). For the privacy-leakage rate, we expand the right-hand side of R_L in (47) as

$$\begin{aligned}&I(X; U, \mathbf{Y}_k) - I(X; \mathbf{Y}_k|V) + I(X; \mathbf{Z}_l|V)\\ &= I(X; U|\mathbf{Y}_k) + I(\mathbf{Y}_k; V) - I(\mathbf{Z}_l; V) + I(X; \mathbf{Z}_l),\end{aligned} \tag{48}$$

where we use the Markov chain $V - X - (\mathbf{Y}_k, \mathbf{Z}_l)$. By (48), the privacy-leakage rate is lower bounded as

$$\begin{aligned}n(R_L + \delta) &\ge I(X^n; J|\mathbf{Z}_l^n) = I(X^n; J, \mathbf{Z}_l^n) - I(X^n; \mathbf{Z}_l^n)\\ &\ge n(I(X; U|\mathbf{Y}_k) + I(\mathbf{Y}_k; V) - I(\mathbf{Z}_l; V)).\end{aligned} \tag{49}$$

Therefore, an outer bound for a given (k, l) in Definition 3 is

$$\begin{aligned}\mathcal{O}_{G_{kl}} \triangleq \bigcup_{P_{V|U}, P_{U|\tilde{\mathbf{X}}}} \{(R_S, R_J, R_L) \in \mathbb{R}_+^3 :\\ R_S \le I(\mathbf{Y}_k; U|V) - I(\mathbf{Z}_l; U|V),\ R_J \ge I(\tilde{\mathbf{X}}; U|\mathbf{Y}_k),\\ R_L \ge I(X; U|\mathbf{Y}_k) + I(\mathbf{Y}_k; V) - I(\mathbf{Z}_l; V)\},\end{aligned} \tag{50}$$

where V and U satisfy $V - U - \tilde{\mathbf{X}} - X - (\mathbf{Y}_k, \mathbf{Z}_l)$. Hence,

$$\mathcal{R}_{\mathrm{G}} \subseteq \bigcap_{k \in \mathcal{K}} \bigcap_{l \in \mathcal{L}} \mathcal{O}_{G_{kl}}. \tag{51}$$

The proof for the CS model can be derived using the same reasoning from [21, Th. 4].

Appendix B
Proof of Lemma 1

Denote the covariance matrix of $(X, \mathbf{Y}_k, \mathbf{Z}_l)$ as $\mathbf{\Sigma}$, where

$$\mathbf{\Sigma} = \begin{bmatrix} \sigma_X^2 & \mathbf{\Sigma}_{X\mathbf{Y}_k} & \mathbf{\Sigma}_{X\mathbf{Z}_l} \\ \mathbf{\Sigma}_{\mathbf{Y}_k X} & \mathbf{\Sigma}_{\mathbf{Y}_k} & \mathbf{\Sigma}_{\mathbf{Y}_k\mathbf{Z}_l} \\ \mathbf{\Sigma}_{\mathbf{Z}_l X} & \mathbf{\Sigma}_{\mathbf{Z}_l\mathbf{Y}_k} & \mathbf{\Sigma}_{\mathbf{Z}_l} \end{bmatrix}. \tag{52}$$

Note that (2) depends on the marginal distribution of $(X, \mathbf{Y}_k)$, (3) depends on the marginal distribution of X, and (5) and (6) depend on the marginal distribution of $(X, \mathbf{Z}_l)$. Therefore, without loss of generality, using [54, Th. 3.5.2] and (52), it suffices to consider

$$\mathbf{Y}_k = \mathbf{\Sigma}_{\mathbf{Y}_k X}\sigma_X^{-2} X + \mathbf{N}_{\mathbf{Y}_k}, \tag{53}$$

$$\mathbf{Z}_l = \mathbf{\Sigma}_{\mathbf{Z}_l X}\sigma_X^{-2} X + \mathbf{N}_{\mathbf{Z}_l}, \tag{54}$$

where $\mathbf{N}_{\mathbf{Y}_k} \sim \mathcal{N}(0, \mathbf{\Sigma}_{\mathbf{N}_{\mathbf{Y}_k}})$ with $\mathbf{\Sigma}_{\mathbf{N}_{\mathbf{Y}_k}} = \mathbf{\Sigma}_{\mathbf{Y}_k} - \mathbf{\Sigma}_{\mathbf{Y}_k X}\sigma_X^{-2}\mathbf{\Sigma}_{X\mathbf{Y}_k}$, and $\mathbf{N}_{\mathbf{Z}_l} \sim \mathcal{N}(0, \mathbf{\Sigma}_{\mathbf{N}_{\mathbf{Z}_l}})$ with $\mathbf{\Sigma}_{\mathbf{N}_{\mathbf{Z}_l}} = \mathbf{\Sigma}_{\tilde{\mathbf{X}}} - \mathbf{\Sigma}_{\mathbf{Z}_l X}\sigma_X^{-2}\mathbf{\Sigma}_{X\mathbf{Z}_l}$, independent of X.

Since $\mathbf{\Sigma}$ is non-singular (positive definite), the sub-matrix $\begin{bmatrix} \sigma_X^2 & \mathbf{\Sigma}_{X\mathbf{Y}_k} \\ \mathbf{\Sigma}_{\mathbf{Y}_k X} & \mathbf{\Sigma}_{\mathbf{Y}_k} \end{bmatrix}$ is also positive definite. This implies that the matrix $\mathbf{\Sigma}_{\mathbf{N}_{\mathbf{Y}_k}}$ is positive definite as it is the Schur complement of σ_X^2 in the sub-matrix. By Cholesky decomposition, there exists an invertible matrix $\mathbf{C} \in \mathbb{R}^{\Omega_Y \times \Omega_Y}$ such that $\mathbf{\Sigma}_{\mathbf{N}_{\mathbf{Y}_k}} = \mathbf{C}\mathbf{C}^{\mathsf{T}}$. Then, we can reformulate (53) as

$$\mathbf{Y}_k' = \mathbf{A}_{\mathbf{Y}_k'} X + \mathbf{N}_{\mathbf{Y}_k}', \tag{55}$$

where $\mathbf{Y}_k' = \mathbf{C}^{-1}\mathbf{Y}_k$, $\mathbf{A}_{\mathbf{Y}_k'} = \mathbf{C}^{-1}\mathbf{\Sigma}_{\mathbf{Y}_k X}\sigma_X^{-2}$ and $\mathbf{N}_{\mathbf{Y}_k}' \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_{\Omega_Y})$. Similarly, the same approach can be applied to (54).

Appendix C
Proof of Theorem 1

This appendix consists of two parts, that is, the achievability part in Appendix C-A and the converse part in Appendix C-B.

A. Achievability Proof

Note that Proposition 1 was proved under finite source alphabets. However, the result can be extended to Gaussian sources as well by employing a fine quantization before encoding and decoding processes, similar to [55].

By choosing V as a constant in Proposition 1, the following regions are achievable.

$$\begin{aligned}R_G \ \supseteq\ \bigcup_{P_{U|X}} \Big\{&(R_S, R_J, R_L) \in \mathbb{R}_+^3 :\\ &R_S \le \min_k I(\mathbf{Y}_k; U) - \max_l I(\mathbf{Z}_l; U),\\ &R_J \ge I(X; U) - \min_k I(\mathbf{Y}_k; U),\\ &R_L \ge I(X; U) - \min_l I(\mathbf{Y}_k; U)\Big\},\end{aligned} \tag{56}$$

$$\begin{aligned}R_C \ \supseteq\ \bigcup_{P_{U|X}} \Big\{&(R_S, R_J, R_L) \in \mathbb{R}_+^3 :\\ &R_S \le \min_k I(\mathbf{Y}_k; U) - \max_l I(\mathbf{Z}_l; U),\\ &R_J \ge I(X; U) - \max_l I(\mathbf{Z}_l; U),\\ &R_L \ge I(X; U) - \min_l I(\mathbf{Y}_k; U)\Big\},\end{aligned} \tag{57}$$

where auxiliary random variable U satisfies the Markov chain $U - X - (\mathbf{Y}_k, \mathbf{Z}_l)$ for all $k \in \mathcal{K}$ and $l \in \mathcal{L}$.

Lemma 4 (Weinstein–Aronszajn Identity [52, Appx. B]): For any $a \in \mathbb{R}_+$ and matrix $\mathbf{H} \in \mathbb{R}^{\Omega \times 1}$, we have

$$\det(\mathbf{H}a\mathbf{H}^{\mathsf{T}} + \mathbf{I}_\Omega) = a\mathbf{H}^{\mathsf{T}}\mathbf{H} + 1, \tag{58}$$

where $\det(\cdot)$ denotes the determinant of a matrix.

Lemma 5: For given $\alpha \in (0,1]$, the function

$$f(\mathbf{H}^\intercal\mathbf{H}) = \log\left(\frac{\sigma_X^2\mathbf{H}^\intercal\mathbf{H}+1}{\alpha\sigma_X^2\mathbf{H}^\intercal\mathbf{H}+1}\right) \tag{59}$$

is monotonically increasing with respect to $\mathbf{H}^\intercal\mathbf{H}$.

Lemma 4 is applied in the calculation of mutual information with vector random variables for given k and l, and the role of Lemma 5 is to find the minimum and maximum values of the mutual information among all possible $k \in \mathcal{K}$ and $l \in \mathcal{L}$.

For $0 < \alpha \le 1$, consider

$$X \triangleq U + \Theta, \tag{60}$$

where $U \sim \mathcal{N}(0,(1-\alpha)\sigma_X^2))$ and $\Theta \sim \mathcal{N}(0,\alpha\sigma_X^2)$. This relation implies that

$$I(X;U) = \frac{1}{2}\log\left(\frac{1}{\alpha}\right). \tag{61}$$

From (17) and (60), it follows that

$$\mathbf{Y}_k = \mathbf{H}_k U + \mathbf{H}_k\Theta + \mathbf{N}_{\mathbf{Y}_k}, \tag{62}$$

$$\mathbf{Z}_l = \tilde{\mathbf{H}}_l U + \tilde{\mathbf{H}}_l\Theta + \mathbf{N}_{\mathbf{Z}_l}. \tag{63}$$

Using Lemma 4, we have

$$I(\mathbf{Y}_k;U) = \frac{1}{2}\log\frac{\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1}{\alpha\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1}, \tag{64}$$

$$I(\mathbf{Z}_l;U) = \frac{1}{2}\log\frac{\sigma_X^2\tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l+1}{\alpha\sigma_X^2\tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l+1} \tag{65}$$

for a fixed pair (k,l), and invoking Lemma 5 gives

$$\min_k I(\mathbf{Y}_k;U) = \frac{1}{2}\log\left(\frac{\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1}{\alpha\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1}\right), \tag{66}$$

$$\max_l I(\mathbf{Z}_l;U) = \frac{1}{2}\log\left(\frac{\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}+1}{\alpha\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}+1}\right). \tag{67}$$

Finally, substituting (61), (66), (67) into (56) and (57), gives (23) and (24).

B. Converse Proof

We will need the following lemmas. These lemmas convert vector observations in (17) into scalar Gaussian random variables using sufficient statistics [46, Sect. 2.9]. This transformation plays an important role in deriving the outer bound of Gaussian sources.

Lemma 6 ([56, Lemma 3.1]): Consider a channel with input W and output $\tilde{\mathbf{W}}$, namely, $\tilde{\mathbf{W}} \triangleq \mathbf{A}W + \mathbf{N}_{\tilde{\mathbf{W}}}$, where $\mathbf{A}$ is a matrix and $\mathbf{N}_{\tilde{\mathbf{W}}} \sim \mathcal{N}(\mathbf{0},\mathbf{\Sigma}_{\tilde{\mathbf{W}}})$. A sufficient statistic to correctly determine W from $\tilde{\mathbf{W}}$ is the following scalar

$$\bar{W} \triangleq \mathbf{A}^\intercal\Sigma_{\tilde{\mathbf{W}}}^{-1}\tilde{\mathbf{W}}. \tag{68}$$

Lemma 7: The vector equations in (17) can be rewritten as

$$\bar{Y}_k = \nu_{\bar{Y}_k}X + N_{\bar{Y}_k}, \bar{Z}_l = \nu_{\bar{Z}_l}X + N_{\bar{Z}_l}, \tag{69}$$

where $\nu_{\bar{Y}_k} \triangleq \mathbf{H}_k^\intercal\mathbf{H}_k$, $\nu_{\bar{Z}_l} \triangleq \tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l$, $N_{\bar{Y}_k} \sim \mathcal{N}(0,\nu_{\bar{Y}_k})$, and $N_{\bar{Z}_l} \sim \mathcal{N}(0,\nu_{\bar{Z}_l})$.

Proof: Applying Lemma 6 to our settings in (17), we have

$$\bar{Y}_k = \mathbf{H}_k^\intercal\mathbf{I}_{\Omega_Y}^{-1}\mathbf{Y}_k,\ \bar{Z}_l = \tilde{\mathbf{H}}_l^\intercal\mathbf{I}_{\Omega_Z}^{-1}\mathbf{Z}_l. \tag{70}$$

Now substituting (17) into (70), we have

$$\bar{Y}_k = \mathbf{H}_k^\intercal(\mathbf{H}_kX + \mathbf{N}_{\mathbf{Y}_k}) = \nu_{\bar{Y}_k}X + N_{\bar{Y}_k}, \tag{71}$$

$$\bar{Z}_l = \tilde{\mathbf{H}}_l^\intercal(\tilde{\mathbf{H}}_lX + \mathbf{N}_{\mathbf{Z}_l}) = \nu_{\bar{Z}_l}X + N_{\bar{Z}_l}, \tag{72}$$

where we denote $\nu_{\bar{Y}_k} \triangleq \mathbf{H}_k^\intercal\mathbf{H}_k$, $\nu_{\bar{Z}_l} \triangleq \tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l$, $N_{\bar{Y}_k} \triangleq \mathbf{H}_k\mathbf{N}_{\mathbf{Y}_k}$, and $N_{\bar{Z}_l} \triangleq \tilde{\mathbf{H}}_l\mathbf{N}_{\mathbf{Z}_l}$. Note that $N_{\bar{Y}_k}$ and $N_{\bar{Z}_l}$ are Gaussian random variables, and their variances are $\mathrm{Var}[\mathbf{H}_k^\intercal\mathbf{N}_{\mathbf{Y}_k}] = \mathbf{H}_k^\intercal\mathbf{H}_k$, and $\mathrm{Var}[\tilde{\mathbf{H}}_l^\intercal\mathbf{N}_{\mathbf{Z}_l}] = \tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l$. □

As $(X,\bar{Y}_k,\bar{Z}_l)$ are scalar Gaussian random variables, when the squared value of the correlation coefficient of $(X,\bar{Y}_{k^*})$ is greater than that of $(X,\bar{Z}_{l^*})$, i.e., $\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*} \ge \tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}$, implying that $\mathbf{H}_k^\intercal\mathbf{H}_k \ge \tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l$ for any pair (k,l), there exist Gaussian random variables $(X',\bar{Y}_k',\bar{Z}_l')$ such that $X'-\bar{Y}_k'-\bar{Z}_l'$ is satisfied, and the marginal distributions of $(X,\bar{Y}_k)$ and $(X',\bar{Y}_k')$ and that of $(X,\bar{Z}_l)$ and $(X',\bar{Z}_l')$ coincide [47, Lemma 6]. In the subsequent discussions, we denote $(X',\bar{Y}_k',\bar{Z}_l')$ as $(X,\bar{Y}_k,\bar{Z}_l)$ for brevity. This property is used in the derivation of the following lemma.

Lemma 8 (Outer Bounds): If $\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*} \ge \tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}$, the outer bounds of the GS and CS models are provided as

$$\mathcal{R}_{\mathrm{G}} \subseteq \bigcap_{k\in\mathcal{K}}\bigcap_{l\in\mathcal{L}}\bar{\mathcal{O}}_{G_{kl}},\quad \mathcal{R}_{\mathrm{C}} \subseteq \bigcap_{k\in\mathcal{K}}\bigcap_{l\in\mathcal{L}}\bar{\mathcal{O}}_{C_{kl}}, \tag{73}$$

where $\bar{\mathcal{O}}_{G_{kl}}$ and $\bar{\mathcal{O}}_{C_{kl}}$ are outer bounds of the GS and CS models for a given pair (k,l) and are defined as

$$\begin{aligned}\bar{\mathcal{O}}_{G_{kl}} \triangleq \bigcup_{P_{U|X}}\Big\{&(R_S,R_J,R_L)\in\mathbb{R}_+^3:\\ &R_S \le I(\bar{Y}_k;U) - I(\bar{Z}_l;U),\\ &R_J \ge I(X;U) - I(\bar{Y}_k;U),\\ &R_L \ge I(X;U) - I(\bar{Y}_k;U)\Big\},\end{aligned} \tag{74}$$

$$\begin{aligned}\bar{\mathcal{O}}_{C_{kl}} \triangleq \bigcup_{P_{U|X}}\Big\{&(R_S,R_J,R_L)\in\mathbb{R}_+^3:\\ &R_S \le I(\bar{Y}_k;U) - I(\bar{Z}_l;U),\\ &R_J \ge I(X;U) - I(\bar{Z}_l;U),\\ &R_L \ge I(X;U) - I(\bar{Y}_k;U)\Big\},\end{aligned} \tag{75}$$

and U satisfies the Markov chain $U-X-\bar{Y}_k-\bar{Z}_l$. If $\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*} < \tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}$, $\mathcal{R}_{\mathrm{G}} = \mathcal{R}_{\mathrm{C}} = \{(R_S,R_J,R_L) : R_S = 0, R_J \ge 0, R_L \ge 0\}$.

Proof: The proof is provided in Appendix D and follows standard converse proof techniques, where Fano's inequality and the introduction of auxiliary random variable are used. The key idea is to exploit the relationship in (70), which shows that $(\bar{Y}_k,\bar{Z}_l)$ and $(\mathbf{Y}_k,\mathbf{Z}_l)$ are mutually deterministic. This allows the vector random variables $(\mathbf{Y}_k,\mathbf{Z}_l)$ to be removed from the rate constraints during the analysis. □

Next, we utilize the single-letter expressions in Lemma 8 to derive the parametric forms for Gaussian sources. We begin with the proof of (74). Each rate constraint in (74) can be expanded as

$$\begin{aligned}R_S \le I(\bar{Y}_k;U) - I(\bar{Z}_l;U) &\overset{(a)}{=} \frac{1}{2}\log\frac{\mathbf{H}_k^\intercal\mathbf{H}_k(\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1)}{\tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l(\sigma_X^2\mathbf{H}_l^\intercal\mathbf{H}_l+1)}\\ &\quad + h(\bar{Z}_l|U) - h(\bar{Y}_k|U),\end{aligned} \tag{76}$$

$$R_J \ge I(X;U) - I(\bar{Y}_k;U) \overset{(b)}{=} \frac{1}{2}\log\frac{\sigma_X^2}{\mathbf{H}_k^\intercal\mathbf{H}_k(\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1)}$$

$$+ h(\bar{Y}_k|U) - h(X|U), \tag{77}$$

$$R_L \geq I(X;U) - I(\bar{Y}_k;U) \overset{(c)}{=} \frac{1}{2}\log\frac{\sigma_X^2}{\mathbf{H}_k^\intercal\mathbf{H}_k(\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1)} + h(\bar{Y}_k|U) - h(X|U), \tag{78}$$

where (a), (b), and (c) follow from (69).

From Lemma 7, we have

$$\begin{aligned}\frac{1}{2}\log\frac{\sigma_X^2+1/\nu_{\bar{Z}_l}}{\sigma_X^2+1/\nu_{\bar{Y}_k}} &= h\left(\frac{1}{\nu_{\bar{Z}_l}}\bar{Z}_l\right) - h\left(\frac{1}{\nu_{\bar{Y}_k}}\bar{Y}_k\right)\\ &\overset{(a)}{\leq} h\left(\frac{1}{\nu_{\bar{Z}_l}}\bar{Z}_l|U\right) - h\left(\frac{1}{\nu_{\bar{Y}_k}}\bar{Y}_k|U\right)\\ &\overset{(b)}{\leq} h\left(\frac{1}{\nu_{\bar{Z}_l}}\bar{Z}_l|X\right) - h\left(\frac{1}{\nu_{\bar{Y}_k}}\bar{Y}_k|X\right) = \frac{1}{2}\log\frac{1/\nu_{\bar{Z}_l}}{1/\nu_{\bar{Y}_k}},\end{aligned} \tag{79}$$

where (a) and (b) follow from the fact that $I(\bar{Y}_k;U|\bar{Z}_l)\geq 0$ and $I(\bar{Y}_k;X|U,\bar{Z}_l)\geq 0$, respectively. Thus, there must exist a parameter $\alpha\in(0,1]$ such that

$$h\left(\frac{1}{\nu_{\bar{Z}_l}}\bar{Z}_l|U\right) - h\left(\frac{1}{\nu_{\bar{Y}_k}}\bar{Y}_k|U\right) = \frac{1}{2}\log\frac{\alpha\sigma_X^2+1/\nu_{\bar{Z}_l}}{\alpha\sigma_X^2+1/\nu_{\bar{Y}_k}}. \tag{80}$$

Equation (80) also indicates that

$$\begin{aligned}h(\bar{Z}_l|U) - h(\bar{Y}_k|U) &= \frac{1}{2}\log\frac{\nu_{\bar{Z}_l}(\alpha\sigma_X^2\nu_{\bar{Z}_l}+1)}{\nu_{\bar{Y}_k}(\alpha\sigma_X^2\nu_{\bar{Y}_k}+1)}\\ &= \frac{1}{2}\log\frac{\tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l(\alpha\sigma_X^2\tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l+1)}{\mathbf{H}_k^\intercal\mathbf{H}_k(\alpha\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1)}.\end{aligned} \tag{81}$$

The conditional Fisher information of A is defined by $\mathbb{J}(A|U) = \mathbb{E}\left[\left(\frac{\partial\log f_{A|U}(a|u)}{\partial a}\right)^2\right]$, where the expectation is taken over (U,A) [49, Def. 1].

Lemma 9 ([49, Cor. 1]): Let W,A,B be random variables, and let the density for any combination of them exist. Moreover, assume that given W, A and B are independent. Then, we have

$$\frac{1}{\mathbb{J}(A+B|W)} \geq \frac{1}{\mathbb{J}(A|W)} + \frac{1}{\mathbb{J}(B|W)}. \tag{82}$$

We use Lemma 9 to establish a lower bound on the conditional Fisher information, as presented in Lemma 10. This lemma is then used to derive a lower bound on the difference $h(\bar{Y}_k|U) - h(X|U)$ given that $h(\bar{Z}_l|U) - h(\bar{Y}_k|U)$ is fixed.

Lemma 10: For $0\leq r\leq 1/\nu_{\bar{Y}_k}$, it holds that

$$\mathbb{J}(X+\sqrt{r}N|U) \geq \frac{1}{\alpha\sigma_X^2+r} \tag{83}$$

with an independent Gaussian random variable $N\sim\mathcal{N}(0,1)$.

Proof: From [49, Lemma 3], it follows that

$$h\left(\frac{1}{\nu_{\bar{Z}_l}}\bar{Z}_l|U\right) - h\left(\frac{1}{\nu_{\bar{Y}_k}}\bar{Y}_k|U\right) = \frac{1}{2}\int_{1/\nu_{\bar{Y}_k}}^{1/\nu_{\bar{Z}_l}} \mathbb{J}(X+\sqrt{t}\tilde{N}|U)dt \tag{84}$$

with an independent random variable $\tilde{N}\sim\mathcal{N}(0,1)$. Then,

$$\begin{aligned}&\frac{1}{2}\int_{1/\nu_{\bar{Y}_k}}^{1/\nu_{\bar{Z}_l}} \mathbb{J}(X+\sqrt{t}\tilde{N}|U)dt\\ &\overset{(a)}{=} \frac{1}{2}\int_{1/\nu_{\bar{Y}_k}}^{1/\nu_{\bar{Z}_l}} \mathbb{J}(X+\sqrt{r}N+\sqrt{t-r}N'|U)dt\\ &\overset{(b)}{\leq} \frac{1}{2}\int_{1/\nu_{\bar{Y}_k}}^{1/\nu_{\bar{Z}_l}} \left(\mathbb{J}(X+\sqrt{r}N|U)^{-1}+t-r\right)^{-1}dt\\ &= \frac{1}{2}\int_{1/\nu_{\bar{Y}_k}}^{1/\nu_{\bar{Z}_l}} \frac{\mathbb{J}(X+\sqrt{r}N|U)}{1+\mathbb{J}(X+\sqrt{r}N|U)(t-r)}dt\\ &= \frac{1}{2}\log\frac{1+\mathbb{J}(X+\sqrt{r}N|U)(1/\nu_{\bar{Z}_l}-r)}{1+\mathbb{J}(X+\sqrt{r}N|U)(1/\nu_{\bar{Y}_k}-r)},\end{aligned} \tag{85}$$

where (a) follows by picking a real number r in the range of $0\leq r\leq 1/\nu_{\bar{Y}_k}$ and using independent Gaussian random variables $N\sim\mathcal{N}(0,1)$ and $N'\sim\mathcal{N}(0,1)$, and (b) is due to Lemma 9. Lastly, comparing (80) and (85), we obtain (83). □

Observe that

$$\begin{aligned}h\left(\frac{1}{\nu_{\bar{Y}_k}}\bar{Y}_k|U\right) - h(X|U) &= \frac{1}{2}\int_0^{1/\nu_{\bar{Y}_k}} \mathbb{J}(X+\sqrt{r}N|U)dr\\ &\overset{(a)}{\geq} \frac{1}{2}\int_0^{1/\nu_{\bar{Y}_k}} \frac{1}{\alpha\sigma_X^2+r}dr = \frac{1}{2}\log\frac{\alpha\sigma_X^2+1/\nu_{\bar{Y}_k}}{\alpha\sigma_X^2},\end{aligned} \tag{86}$$

where (a) follows from Lemma 10, which implies that

$$\begin{aligned}h(\bar{Y}_k|U) - h(X|U) &\geq \frac{1}{2}\log\frac{\nu_{\bar{Y}_k}(\alpha\sigma_X^2\nu_{\bar{Y}_k}+1)}{\alpha\sigma_X^2}\\ &= \frac{1}{2}\log\frac{\mathbf{H}_k^\intercal\mathbf{H}_k(\alpha\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1)}{\alpha\sigma_X^2}.\end{aligned} \tag{87}$$

Substituting (81) and (87) into the rate constraints in (76)–(78), the outer bound for a fixed pair (k,l) is expressed as

$$\begin{aligned}\bar{\mathcal{O}}_{G_{kl}} \triangleq \bigcup_{0<\alpha\leq 1}\Bigg\{&(R_S,R_J,R_L)\in\mathbb{R}_+^3:\\ &R_S \leq \frac{1}{2}\log\frac{\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1}{\alpha\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1} - \frac{1}{2}\log\frac{\sigma_X^2\tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l+1}{\alpha\sigma_X^2\tilde{\mathbf{H}}_l^\intercal\tilde{\mathbf{H}}_l+1},\\ &R_J \geq \frac{1}{2}\log\frac{\alpha\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1}{\alpha(\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1)},\\ &R_L \geq \frac{1}{2}\log\frac{\alpha\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1}{\alpha(\sigma_X^2\mathbf{H}_k^\intercal\mathbf{H}_k+1)}\Bigg\}.\end{aligned} \tag{88}$$

Applying Lemma 5 to (73) and (88), the outer region of the GS model for all possible index pairs (k,l) is

$$\begin{aligned}\mathcal{R}_{\mathrm{G}} \subseteq \bigcup_{0<\alpha\leq 1}\Bigg\{&(R_S,R_J,R_L)\in\mathbb{R}_+^3:\\ &R_S \leq \frac{1}{2}\log\frac{(\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1)(\alpha\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}+1)}{(\alpha\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1)(\sigma_X^2\tilde{\mathbf{H}}_{l^*}^\intercal\tilde{\mathbf{H}}_{l^*}+1)},\\ &R_J \geq \frac{1}{2}\log\frac{\alpha\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1}{\alpha(\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1)},\\ &R_L \geq \frac{1}{2}\log\frac{\alpha\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1}{\alpha(\sigma_X^2\mathbf{H}_{k^*}^\intercal\mathbf{H}_{k^*}+1)}\Bigg\}.\end{aligned} \tag{89}$$

The outer region of the CS model in (24) can be shown similarly. □

Appendix D
Proof of Lemma 8

We only prove (74), the outer bound of the GS model for a given pair (k,l), as the proof of (8) follows by a similar manner. Assume that a rate tuple (R_S,R_J,R_L) is achievable with respect to Definition 3 for every pair $(k,l)\in\mathcal{K}\times\mathcal{L}$.

We begin by establishing the following Markov chains:

$$(J,S)-X^n-\mathbf{Y}_k^n-\bar{Y}_k^n,\ (J,S)-X^n-\bar{Y}_k^n-\mathbf{Y}_k^n, \tag{90}$$

$$(J,S)-X^n-\mathbf{Z}_l^n-\bar{Z}_l^n,\ \ (J,S)-X^n-\bar{Z}_l^n-\mathbf{Z}_l^n, \tag{91}$$

$$(J,S)-X^n-(\mathbf{Y}_k^n,\mathbf{Z}_l^n)-(\bar{Y}_k^n,\bar{Z}_l^n), \tag{92}$$

where the left-hand sides of (90) and (91), and (92) hold because $\bar{Y}_k^n$ and $\bar{Z}_l^n$ are functions of $\mathbf{Y}_k^n$ and $\mathbf{Z}_l^n$, respectively, by Lemma 7, and the right-hand sides of (90) and (91) are due to the sufficient statistic [46, Sect. 2.9]. In addition, for the scalar random variables $(X,\bar{Y}_k,\bar{Z}_l)$, the Markov chain $X^n-\bar{Y}_k^n-\bar{Z}_l^n$ holds for any pair (k,l) when $\mathbf{H}_{k^*}^{\mathsf{T}}\mathbf{H}_{k^*}\geq\tilde{\mathbf{H}}_{l^*}^{\mathsf{T}}\tilde{\mathbf{H}}_{l^*}$. Combining this with (92) gives

$$(J,S)-X^n-\bar{Y}_k^n-\bar{Z}_l^n. \tag{93}$$

Define auxiliary random variables

$$V_t=(J,\bar{Y}_{k,t+1}^n,\bar{Z}_l^{t-1}) \text{ and } U_t=(J,S,\bar{Y}_{k,t+1}^n,\bar{Z}_l^{t-1}), \tag{94}$$

which guarantee the Markov chain

$$V_t-U_t-X_t-\bar{Y}_{k,t}-\bar{Z}_{l,t}. \tag{95}$$

Also, we define

$$\delta_n=\frac{1}{n}\left(H_b(\delta)+\delta\log|\mathcal{S}|\right), \tag{96}$$

where $H_b(\cdot)$ denotes the binary entropy function, and $\delta_n\downarrow 0$ as $\delta\downarrow 0$ and $n\to\infty$.

Analysis of Secret-Key Rate: From (3),

$$\begin{aligned}
n(R_S-\delta)&\leq H(S)\\
&=H(S|J,\mathbf{Z}_l^n)+I(S;J,\mathbf{Z}_l^n)\\
&\overset{(a)}{\leq} H(S|J,\mathbf{Z}_l^n)-H(S|J,\mathbf{Y}_k^n)+n(\delta+\delta_n)\\
&\overset{(b)}{=} H(S|J,\mathbf{Z}_l^n,\bar{Z}_l^n)-H(S|J,\mathbf{Y}_k^n,\bar{Y}_k^n)+n(\delta+\delta_n)\\
&\overset{(c)}{=} H(S|J,\bar{Z}_l^n)-H(S|J,\bar{Y}_k^n)+n(\delta+\delta_n)\\
&=I(S;\bar{Y}_k^n|J)-I(S;\bar{Z}_l^n|J)+n(\delta+\delta_n)\\
&\overset{(d)}{=}\sum_{t=1}^n\{I(\bar{Y}_{k,t};U_t|V_t)-I(\bar{Z}_{l,t};U_t|V_t)\}+n(\delta+\delta_n)
\end{aligned} \tag{97}$$

$$\begin{aligned}
&\overset{(e)}{=}\sum_{t=1}^n\{I(\bar{Y}_{k,t};U_t)-I(\bar{Z}_{l,t};U_t)\\
&\quad-(I(\bar{Y}_{k,t};V_t)-I(\bar{Z}_{l,t};V_t))\}+n(\delta+\delta_n)\\
&\overset{(f)}{\leq}\sum_{t=1}^n\{I(\bar{Y}_{k,t};U_t)-I(\bar{Z}_{l,t};U_t)\}+n(\delta+\delta_n),
\end{aligned} \tag{98}$$

where (a) is due to (5) and Fano's inequality with δ_n defined in (96) as the secret key S can be reliably estimated from $(J,\mathbf{Y}_k^n)$, (b) follows from the left-hand sides of (90) and (91), (c) holds by the right-hand sides of (90) and (91), (d) follows by [7, Lemma 4.1], (e) follows from the Markov chains $V_t-U_t-\bar{Y}_{k,t}$ and $V_t-U_t-\bar{Z}_{l,t}$, and (f) is due to (95), which results in $I(\bar{Y}_{k,t};V_t)-I(\bar{Z}_{l,t};V_t)\geq 0$.

Analysis of Storage Rate: From (4),

$$\begin{aligned}
n(R_J+\delta)&\geq\log|\mathcal{J}|\geq H(J)=I(X^n;J)\\
&\overset{(a)}{\geq} I(X^n;J|\mathbf{Y}_k^n)\\
&\geq I(X^n;J,S|\mathbf{Y}_k^n)-H(S|\mathbf{Y}_k^n,J)\\
&\overset{(b)}{\geq} I(X^n;J,S|\mathbf{Y}_k^n)-n\delta_n\\
&=I(X^n;\bar{Y}_k^n|\mathbf{Y}_k^n)+I(X^n;J,S|\bar{Y}_k^n,\mathbf{Y}^n)\\
&\quad-I(X^n;\bar{Y}_k^n|J,S,\mathbf{Y}_k^n)-n\delta_n\\
&\overset{(c)}{=} I(X^n;J,S|\bar{Y}_k^n,\mathbf{Y}_k^n)-n\delta_n\\
&\overset{(d)}{=} I(X^n;J,S|\bar{Y}_k^n)-n\delta_n
\end{aligned} \tag{99}$$

$$\begin{aligned}
&\overset{(e)}{=}\sum_{t=1}^n\{h(X_t|\bar{Y}_{k,t})-h(X_t|J,S,X^{t-1},\bar{Y}_k^n,\bar{Z}_l^{t-1})\}-n\delta_n\\
&\overset{(f)}{\geq}\sum_{t=1}^n\{h(X_t|\bar{Y}_{k,t})-h(X_t|U_t,\bar{Y}_{k,t})\}-n\delta_n\\
&\overset{(g)}{=}\sum_{t=1}^n\{I(X_t;U_t)-I(\bar{Y}_{k,t};U_t)\}-n\delta_n,
\end{aligned} \tag{100}$$

where (a) is due to the Markov chain $J-X^n-\mathbf{Y}_k^n$, (b) follows by Fano's inequality with δ_n defined in (96), (c) follows because $\bar{Y}_k^n$ is a function of $\mathbf{Y}_k^n$, (d) holds from the left-hand side of (90), (e) holds due to the Markov chain $X_t-(J,S,X^{t-1},\bar{Y}_k^n,)-\bar{Z}_l^{t-1}$, (f) follows because conditioning reduces entropy, and (g) is due to $U_t-X_t-\bar{Y}_{k,t}$.

Analysis of Privacy-Leakage Rate: For a fixed l, we first show that the left-hand side of (6) is preserved when $(X^n,\mathbf{Z}^n)$ is replaced with $(X^n,\bar{Z}^n)$.

$$\begin{aligned}
I(X^n;J|\mathbf{Z}_l^n)&\overset{(a)}{=} I(X^n;J)-I(\mathbf{Z}_l^n;J)\\
&\overset{(b)}{=} I(X^n;J)-I(\mathbf{Z}_l^n,\bar{Z}_l^n;J)\\
&\overset{(c)}{=} I(X^n;J)-I(\bar{Z}_l^n;J)\\
&\overset{(d)}{=} I(X^n;J|\bar{Z}_l^n),
\end{aligned} \tag{101}$$

where (a), (b), (c), and (d) follow from the Markov chains $J-X^n-\mathbf{Z}_l^n$, $J-\mathbf{Z}_l^n-\bar{Z}_l^n$, $J-\bar{Z}_l^n-\mathbf{Z}_l^n$, and $J-X_l^n-\bar{Z}_l^n$, respectively, all of which are obtained as special cases of (91).

Therefore, we can evaluate the privacy-leakage rate as

$$\begin{aligned}
n(R_L+\delta)&\geq I(X^n;J|\mathbf{Z}_l^n)\\
&\overset{(a)}{=} I(X^n;J|\bar{Z}_l^n)\\
&=I(X^n;J,S,\mathbf{Y}_k^n|\bar{Z}_l^n)-I(X^n;\mathbf{Y}_k^n|J,\bar{Z}_l^n)\\
&\quad-I(X^n;S|J,\mathbf{Y}_k^n,\bar{Z}_l^n)\\
&\geq I(X^n;J,S,\mathbf{Y}_k^n|\bar{Z}_l^n)-I(X^n;\mathbf{Y}_k^n|J,\bar{Z}_l^n)-H(S|J,\mathbf{Y}_k^n)\\
&\geq I(X^n;J,S,\mathbf{Y}_k^n|\bar{Z}_l^n)-I(X^n;\mathbf{Y}_k^n|J,\bar{Z}_l^n)-n\delta_n\\
&\overset{(b)}{=} I(X^n;J,S,\bar{Y}_k^n,\mathbf{Y}_k^n|\bar{Z}_l^n)-I(X^n;\bar{Y}_k^n,\mathbf{Y}_k^n|J,\bar{Z}_l^n)-n\delta_n\\
&\overset{(c)}{=} I(X^n;J,S,\bar{Y}_k^n|\bar{Z}_l^n)-I(X^n;\bar{Y}_k^n|J,\bar{Z}_l^n)-n\delta_n\\
&\overset{(d)}{=} I(X^n;J,S|\bar{Y}_k^n,\bar{Z}_l^n)+I(X^n;\bar{Y}_k^n|\bar{Z}_l^n)\\
&\quad-(I(X^n;\bar{Y}_k^n|\bar{Z}_l^n)-I(\bar{Y}_k^n;J|\bar{Z}_l^n))-n\delta_n\\
&\geq I(X^n;J,S|\bar{Y}_k^n,\bar{Z}_l^n)-n\delta_n\\
&\overset{(e)}{=} I(X^n;J,S|\bar{Y}_k^n)-n\delta_n\\
&\overset{(f)}{\geq}\sum_{t=1}^n\{I(X_t;U_t)-I(\bar{Y}_{k,t};U_t)\}-n\delta_n,
\end{aligned} \tag{102}$$

where (a) is due to (101), (b) follows from (70), i.e., $\bar{Y}_k^n$ is a function of $\mathbf{Y}_k^n$, (c) holds because the Markov chain $X^n - (J, S, \bar{Y}_k^n, \bar{Z}_l^n) - \mathbf{Y}_k^n$ holds, from the right-hand side of (90), (d) and (e) are due to the Markov chain $(J, S) - X^n - \bar{Y}_k^n - \bar{Z}_l^n$, obtained from (93), and (e) follows by the same steps from (99) to (100).

For the case where $\mathbf{H}_{k^*}^\top \mathbf{H}_{k^*} < \tilde{\mathbf{H}}_{l^*}^\top \tilde{\mathbf{H}}_{l^*}$, the Markov chain $V_t - U_t - X_t - \bar{Z}_{l,t} - \bar{Y}_{k,t}$ holds. The secret-key rate follows from (97) since $I(\bar{Y}_{k,t}; U_t|V_t) \le I(\bar{Z}_{l,t}; U_t|V_t)$.

Finally, we introduce a time-sharing random variable $Q \sim \text{Unif}[1:n]$, independent of other random variables, and define $U = (U_Q, Q)$, $X = X_Q$, $\bar{Y}_k = \bar{Y}_{k,Q}$, and $\bar{Z}_l = \bar{Z}_{l,Q}$, so that the Markov chain $U - X - \bar{Y}_k - \bar{Z}_l$ holds. By letting $n \to \infty$ and $\delta \downarrow 0$, one can see that for a given pair (k, l), the outer bound of the GS model is given by (74). Hence, the outer bound valid for any pair (k, l) is given by (73). □

REFERENCES

[1] V. Yachongka and R. A. Chou, "Secret-key generation with PUFs and biometric identifiers for compound authentication channels," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Shenzhen, China, Nov. 2024, pp. 591–596.

[2] M. Ebrahimabadi, M. Younis, and N. Karimi, "A PUF-based modeling-attack resilient authentication protocol for IoT devices," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3684–3703, Mar. 2022.

[3] 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.

[4] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[5] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur.*, Washington DC, USA, Nov. 2002, pp. 148–160.

[6] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th Annu. Conf. Design Autom.*, San Diego, CA, USA, Jun. 2007, pp. 9–14.

[7] 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.

[8] F. Gebali and M. Mamun, "Review of physically unclonable functions (PUFs): Structures, models, and algorithms," *Frontiers Sensors*, vol. 2, pp. 1–15, Jan. 2022.

[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] T. Ignatenko, "Biometric security from an information-theoretical perspective," *Found. Trends Commun. Inform. Theory*, pp. 135–316, Feb. 2010.

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

[13] 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.

[14] 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.

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

[16] 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)*, Jun. 2022, pp. 2666–2671.

[17] 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.

[18] S. Watanabe and Y. Oohama, "Secret key agreement from vector Gaussian sources by rate limited public communication," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 541–550, Sep. 2011.

[19] 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.

[20] O. Gunlu 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.

[21] O. Gunlu, 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.

[22] V. Yachongka, H. Yagi, and H. Ochiai, "Key agreement using physical identifiers for degraded and less noisy authentication channels," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5316–5331, 2023.

[23] 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.

[24] K. Kittichokechai and G. Caire, "Secret key-based identification and authentication with a privacy constraint," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6189–6203, Nov. 2016.

[25] 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.

[26] 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.

[27] N. Tavangaran, S. Baur, A. Grigorescu, and H. Boche, "Compound biometric authentication systems with strong secrecy," in *Proc. SCC; 11th Int. ITG Conf. Syst., Commun. Coding*, Hamburg, Germany, Feb. 2017, pp. 1–5.

[28] A. Grigorescu, H. Boche, and R. Schaefer, "Robust biometric authentication from an information theoretic perspective," *Entropy*, vol. 19, no. 9, p. 480, Sep. 2017.

[29] B. Colombier, L. Bossuet, V. Fischer, and D. Hely, "Key reconciliation protocols for error correction of silicon PUF responses," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1988–2002, Aug. 2017.

[30] 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.

[31] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, no. 1, pp. 1–7, Apr. 2008.

[32] T. Ignatenko and F. M. J. Willems, "Information leakage in fuzzy commitment schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 337–348, Jun. 2010.

[33] O. Günlü, A. Belkacem, and B. C. Geiger, "Secret-key binding to physical identifiers with reliability guarantees," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–6.

[34] M. T. Vu, T. J. Oechtering, M. Skoglund, and H. Boche, "Uncertainty in identification systems," *IEEE Trans. Inf. Theory*, vol. 67, no. 3, pp. 1400–1414, Mar. 2021.

[35] L. Zhou, T. J. Oechtering, and M. Skoglund, "Uncertainty in biometric identification and authentication systems with strong secrecy," in *Proc. 58th Annu. Allert. Conf. Commun. Control Comput. Allert. (Allerton)*, Sep. 2022, pp. 1–6.

[36] R. A. Chou and M. R. Bloch, "Secret-key generation with arbitrarily varying eavesdropper's channel," in *Proc. IEEE Global Conf. Signal Inf. Process.*, Austin, TX, USA, Dec. 2013, pp. 277–280.

[37] N. Tavangaran, H. Boche, and R. F. Schaefer, "Secret-key generation using compound sources and one-way public communication," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 227–241, Jan. 2017.

[38] N. Tavangaran, R. F. Schaefer, H. V. Poor, and H. Boche, "Secret-key generation and convexity of the rate region using infinite compound sources," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2075–2086, Aug. 2018.

[39] R. Sultana and R. A. Chou, "Low-complexity secret sharing schemes using correlated random variables and rate-limited public communication," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 970–975.

[40] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, pp. 1–12, Dec. 2009.

[41] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy results for compound wiretap channel," *Probl. Inf. Transm.*, vol. 49, no. 1, pp. 73–98, Apr. 2013.
[42] A. Campello, C. Ling, and J.-C. Belfiore, "Semantically secure lattice codes for compound MIMO channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1572–1584, Mar. 2020.
[43] R. A. Chou, "Explicit wiretap channel codes via source coding, universal hashing, and distribution approximation, when the channels' statistics are uncertain," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 117–132, 2023.
[44] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[45] H. Weingarten, Y. Steinberg, and S. S. Shamai (Shitz), "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.
[46] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed., Hoboken, NJ, USA: Wiley, 2006.
[47] 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, Nov. 2010.
[48] 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.
[49] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.
[50] E. J. C. Kelkboom, G. Garcia 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.
[51] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[52] C. Pozrikidis, *An Introduction to Grids, Graphs, and Networks*. New York, NY, USA: Oxford Univ. Press, 2014.
[53] R. A. Chou and M. R. Bloch, "Separation of reliability and secrecy in rate-limited secret-key generation," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4941–4957, Aug. 2014.
[54] R. G. Gallager, *Stochastic Processes: Theory for Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2013.
[55] V. Rana, R. A. Chou, and H. M. Kwon, "Information-theoretic secret sharing from correlated Gaussian random variables and public communication," *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 549–559, Jan. 2022.
[56] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. Int. Symp. Inf. Theory*, Sep. 2005, pp. 2152–2155.

Vamoua Yachongka (Member, IEEE) received the Ph.D. degree in computer and network engineering from The University of Electro-Communications, Tokyo, Japan, in 2021. From 2021 to 2022, he was a Research Fellow with The University of Electro-Communications. He then joined Yokohama National University as a Post-Doctoral Researcher from 2022 to 2023. Since 2024, he has been a Post-Doctoral Research Associate with The University of Texas at Arlington. His research interests include information theory, information-theoretic security, and physical-layer security.

Rémi A. Chou (Member, IEEE) received the Engineering degree from Supélec, France, in 2011, and the Ph.D. degree in electrical engineering from Georgia Institute of Technology, Atlanta, GA, USA, in 2015. He was a Post-Doctoral Scholar with The Pennsylvania State University from 2015 to 2017, and an Assistant Professor with Wichita State University from 2017 to 2023. He is currently an Assistant Professor with the Computer Science and Engineering Department, The University of Texas at Arlington.