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

Vamoua Yachongka* Hideki Yagi† Hideki Ochiai*

*Dept. of Electrical and Computer Engineering, Yokohama National University, Yokohama, Kanagawa 240-8501 Japan.
†Dept. Computer and Network Engineering, The University of Electro-Communications, Chofu, Tokyo, 182-8585 Japan.

{yachongka-vamoua-fs, hideki}@ynu.ac.jp, h.yagi@uec.ac.jp

Abstract—Secret-key agreement based on biometric or physical identifiers is a promising security protocol for authenticating users or devices with small chips and has been extensively studied recently. Kittichokechai and Caire (2015) investigated the optimal trade-off in a secret-key agreement model with physical identifiers, where the structure of the authentication channels is similar to the wiretap channels, from information theoretic approaches. Later, the model was extended by Günlü et al. (2018) introducing noise in the enrollment phase and cost-constrained actions at the decoder. The results of these studies show that two auxiliary random variables are involved in the expressions of the optimal rate regions of secret-key, storage, and privacy-leakage rates. However, with these two auxiliary random variables, the complexity of computing the rate region may be prohibitively high. Due to this problem, we are interested in exploring channel structures of authentication channels that need only one auxiliary random variable in the capacity region expression for discrete source settings. The result shows for the class of degraded and less noisy authentication channels, a single auxiliary random variable is sufficient to express the capacity region of the model. As an example, we also derive the capacity region of secret-key, storage, and privacy-leakage rates for binary sources. Furthermore, the capacity region for scalar Gaussian sources is derived under Gaussian authentication channels.

Index Terms—Key agreement, physical identifiers, authentication, degraded channel, less noisy channel, strong secrecy.

I. INTRODUCTION

Biometric and physical identifiers can be used as information sources for secret-key-based authentications. Examples of biometric identifiers are fingerprints, irises, faces, etc. [1], and physical identifiers could be physical unclonable functions (PUFs), which make use of the randomness property of intrinsic manufacturing variations of the integrated circuit to produce source sequences [2]. Some well-known PUFs include, but not limited to ring oscillator PUF, static random access memory PUF, arbiter PUF, and so forth [3]. Though the generating processes are different, biometric data and PUFs have many common aspects, and nearly all assumptions and analyses for biometric identifiers can be applied to PUFs [4]. Secret-key agreement with biometric or physical identifiers, called authentication system in this paper, are generally designed to perform private authentication of users or devices based on secret keys generated from the identifiers. As the authentication is done on demand, it is safer and cheaper compared to key storage in non-volatile memories [5], [6]. Observing a measurement or output of the source sequence via a channel in the enrollment phase, the encoder generates a pair of a secret key and helper data. The helper data is shared with the decoder via a noiseless public channel to assist the reconstruction of the secret key. In the authentication phase, the decoder estimates the secret key using the helper data and another measurement observed through a channel in this phase [7], [8]. In this paper, the channels in the enrollment and authentication phases are called the enrollment channels (ECs) and authentication channels (ACs), respectively.

In [9], a model of the authentication systems, where the ECs are noiseless, known as visible source model (VSM), was investigated for discrete memoryless sources. In this model, the ACs are similar to the wiretap channels [10], and it is assumed that the eavesdropper can obtain both the helper data and a correlated sequence of the sources. The model can be viewed as the source model with one-way communication considered in [11], [12] with a privacy constraint to protect the information leakage from source sequences. In general, the analysis of the privacy constraint is elaborate, especially, for a hidden source model (HSM), where noise in the enrollment phase is taken into account [13]. An extension of the work [9] to an HSM with action costs at the decoder was conducted in [14]. The results provided in [9] and [14] involved two auxiliary random variables (RVs) in the capacity region expressions. However, with these two auxiliary RVs, the computational complexity for calculating the capacity region may be prohibitively high.

In distinct settings, the ECs and ACs are modeled as broadcast channels [15] to assume the correlated noises in the measurements in [16], [17]. These studies analyzed the capacity regions for some classes of the broadcast channels, e.g., physically degraded and less noisy channels [15]. In this paper, we also investigate the capacity regions of the authentication systems for similar classes of channels, but the model and the point to which we direct our attention are different from [16], [17]. More accurately, we deal with the model with separate measurements as in [14], and concentrate on the structure of the ACs, e.g., the main channel is less noisy than the eavesdropper’s channel or the eavesdropper’s channel is degraded with respect to (w.r.t.) the main channel, to simplify the expressions of the capacity regions with two auxiliary RVs.

We are interested in exploring classes of ACs that require only one auxiliary RV in the capacity region characterization of the authentication systems under a strong secrecy...
for secrecy-leakage. Unlike the techniques used in [9], [14], we apply information-spectrum methods [18] to derive our main results. An advantage of using this method is that the argument does not depend on the size of source alphabet, so it can also cover continuous sources. The obtained results clarify that for the class of degraded ACs and less noisy ACs [15], one auxiliary RV suffices to characterize the capacity region of secret-key, storage, and privacy-leakage rates. As an example, the optimal rate region for binary sources with less noisy channels is derived. To obtain this, we establish a new lemma to bound the binary entropy in the converse proof. Furthermore, motivated by the fact that the signals of the biometric and physical identifiers are basically in continuous forms, we extend the result of [19] to include noisy enrollment, whose proof of the optimal rate region becomes more intricate. Numerical calculations of the example for Gaussian sources are also given to capture the impact of the noise in the enrollment phase toward the capacity region, and to visualize the trade-off between secret-key and privacy-leakage rates in the VSM and HSM.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We basically use standard notation in [15]. The system model considered in this paper is depicted in Fig. 1. The sequences \((\tilde{X}^n, X^n, Y^n, Z^n)\) are independently and identically distributed (i.i.d.), and the joint distribution of the system is factorized as

\[
P_{\tilde{X}^n,X^n,Y^n,Z^n} = P_{\tilde{X}^n|X^n} \cdot P_{X^n} \cdot P_{Y^n|X^n} \cdot P_{Z^n|X^n}.
\]  

(1)

Let \(S = [1:M_S]\) and \(\mathcal{J} = [1:M_J]\) be the sets of secret keys and helper data, respectively. Random vectors \(\tilde{X}^n\) and \((Y^n, Z^n)\) denote the source input \(X^n\), generated from i.i.d. source \(P_X\), via the EC \((\mathcal{X}, P_{\tilde{X}|X}, \tilde{X})\) and AC \((\mathcal{X}, P_{Y,Z|X}, Y, Z)\), respectively. Assume that all alphabets \(\tilde{X}, X, Y, Z\) are finite, but this assumption will be relaxed in Sect. III-C. The encoder and decoder functions \((e, d)\) of the system are defined as

\[
e: \tilde{X}^n \rightarrow \mathcal{J} \times S, \quad d: Y^n \times \mathcal{J} \rightarrow S.
\]  

(2)

The system is composed of two phases, that is, enrollment and authentication phases. In the enrollment phase, observing \(\tilde{X}^n\), the encoder \(e\) generates a helper data \(J \in \mathcal{J}\) and a secret key \(S \in S; (J,S) = e(\tilde{X}^n)\). The helper data \(J\) is shared with the decoder via a noiseless public channel. In the authentication phase, seeing \(Y^n\), the decoder \(d\) estimates \(S\) from \(Y^n\) and the helper data \(J; \tilde{S} = d(Y^n, J)\). The eavesdropper has the helper data \(J\) and correlated source sequence \(Z^n\), and intends to learn about the source sequence \(X^n\) and the generated secret key \(S\).

Next, we formulate the achievability of the model.

Definition 1. A tuple of secret-key, storage, and privacy-leakage rates \((R_S, R_J, R_L)\) is achievable if for any small enough \(\delta > 0\) and large enough \(n\) there exists at least a pair of encoder and decoder satisfying

\[
Pr\{\tilde{S} \neq S\} \leq \delta, \quad \text{(error probability)}
\]  

(3)

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

(4)

\[
\log M_J \leq n(R_J + \delta), \quad \text{(storage)}
\]  

(5)

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

(6)

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

(7)

Also, let \(R\) be the closure of the set of all achievable rate tuples, called the capacity region.

To make things easier for the readers to grasp the difference between the expressions of the capacity region in the previous study and the one in this paper, we introduce the capacity region with two auxiliary RVs provided in [14] before presenting our main results.

Theorem 1. (Günlüt et al. [14, Theorem 3]) The capacity region of the authentication systems, denoted by \(\mathcal{R}'\), for general class of ACs is given by

\[
\mathcal{R}' = \bigcup_{P_U|X} \{ (R_S, R_J, R_L) \in \mathbb{R}^3_+ : \\
R_S \leq I(Y; U|V) - I(Z; U|V), \\
R_J \geq I(\tilde{X}; U|Y), \\
R_L \geq I(X; U, Y) - I(X; Y|V) + I(X; Z|V) \},
\]  

(8)

where auxiliary RVs \(U, V\) satisfy the Markov chain \(V - U - \tilde{X} - X - (Y, Z)\) and their cardinalities are limited to \(|V| \leq |\tilde{X}| + 3\) and \(|U| \leq (|\tilde{X}| + 3)(|\tilde{X}| + 2)\).

One can see that two auxiliary RVs \(U, V\) appear in the region \(\mathcal{R}'\). To calculate this region, we have to operate the transition probabilities of both test channels \(P_{U|X}\) and \(P_{V|U}\) together.

III. STATEMENT OF RESULTS

In this section, we state the capacity regions of the authentication systems when the ACs are physically or stochastically degraded and less noisy, and also give the optimal rate regions for binary and Gaussian sources. In order to simplify the statement of our results, we define three new rate regions.
\textbf{Definition 2.} Achievable rate regions of secret-key, storage, and privacy-leakage rates are defined as
\[ \mathcal{A}_1 = \bigcup_{p_{U|X}} \{(R_S, R_J, R_L) \in \mathbb{R}_+^3 : R_S \leq I(Y;U|Z),
R_J \geq I(\hat{X};U|Y),
R_L \geq I(X;U|Y) + I(X;Z)\}, \quad (9) \]
\[ \mathcal{A}_2 = \bigcup_{p_{U|X}} \{(R_S, R_J, R_L) \in \mathbb{R}_+^3 :
R_S \leq I(Y;U) - I(Z;U),
R_J \geq I(\hat{X};U|Y),
R_L \geq I(X;U|Y) + I(X;Z)\}, \quad (10) \]
where auxiliary RV \( U \) in the regions (9) and (10) satisfies the Markov chains \( U - \hat{X} - X - Y - Z \) and \( U - \hat{X} - X - (Y, Z) \), respectively, and the cardinality of the alphabet \( U \) of this auxiliary RV is constrained by \( |U| \leq |X| + 3 \) in both regions. Also, define
\[ \mathcal{A}_3 = \{(R_S, R_J, R_L) : R_S = 0, R_J \geq 0, R_L \geq I(X;Z)\}. \quad (11) \]

In the region \( \mathcal{A}_3 \), no auxiliary RV is involved in its expression.

\textbf{A. Discrete Sources With Degraded and Less Noisy ACs}

The physically and stochastically degraded channels, and less noisy channels are formally defined as follows [15, 20]:

\textbf{Definition 3.} (Physically degraded channel). \((A, P_{C|A}, X)\) is physically degraded w.r.t. \((A, P_{B|A}, B)\) if \( P_{B|A}(b,c|a) = P_{B|A}(b|a) \cdot P_{C|B}(c|b), \forall(a,b,c) \in A \times B \times C \) for some transition probabilities \( P_{C|B} \).

(Stochastically degraded channel). The channel \((A, P_{C|A}, X)\) is stochastically degraded w.r.t. \((A, P_{B|A}, B)\) if there exists a channel \((B, P_{C|B}, C)\) such that \( P_{C|A}(c|a) = \sum_{b \in B} P_{C|B}(c|b)P_{B|A}(b|a), \forall(a,c) \in A \times C \).

(Less noisy channel). \((A, P_{C|A}, X)\) is less noisy than \((A, P_{B|A}, B)\) if for every RV \( W \) such that \( W - A - (B, C) \), we have that \( I(B;W) \geq I(C;W) \).

The optimal rate regions for physically and stochastically degraded channels are stated below.

\textbf{Theorem 2.} Suppose that AC \( P_{Y|Z,X} \) has a structure such that the eavesdropper’s channel \( P_{Z|X,Y} \) is degraded w.r.t. the main channel \( P_{Y|X} \), meaning that the Markov chain \( X - Y - Z \) holds. The optimal trade-offs of secret-key, storage, and privacy-leakage rates are given by
\[ \mathcal{R} = \mathcal{A}_1. \quad (12) \]
Reciprocally, if the Markov chain \( X - Z - Y \) holds, the capacity region is characterized as
\[ \mathcal{R} = \mathcal{A}_3. \quad (13) \]
Theorem 2 can be proved similarly to Theorem 3, and therefore its proof is omitted.

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

The following theorem is the optimal trade-off of the authentication system for less noisy ACs.

\textbf{Theorem 3.} If AC \( P_{Y|Z,X} \) has a structure such that \( P_{Y|X} \) is less noisy than \( P_{Z|X} \), i.e., \( I(Y;W) \geq I(Z;W) \) for every RV \( W \) such that \( W - X - (Y, Z) \), we have that
\[ \mathcal{R} = \mathcal{A}_2. \quad (14) \]
For the case where \( P_{Z|X} \) is less noisy than \( P_{Y|X} \), i.e., \( I(Y;W) \leq I(Z;W) \) for every RV \( W \) such that \( W - X - (Y, Z) \), the capacity region of the system is provided by
\[ \mathcal{R} = \mathcal{A}_3. \quad (15) \]
The proof of Theorem 3 is available in [23, Appendix A]. By a similar method of [7, Section V-A], it can be checked that the region \( \mathcal{R} \) is convex. In case of no presence of Eve (Z is independent of other RVs), Theorems 2 and 3 naturally reduce to the results given in [13].

Note that the assumption of less noisy channels seen in Theorem 2, i.e., \( I(Y;U) \geq I(Z;U) \) (or \( I(Y;U) \leq I(Z;U) \)), is satisfied for every \( U \) satisfying the Markov chain \( U - \hat{X} - X - (Y, Z) \). This fact is utilized in the proof of Theorem 3.

As it was mentioned in the end of Section II, two auxiliary RVs with larger alphabet sizes involved in the region \( \mathcal{R} \) (cf. Theorem 1). On the other hand, the regions \( \mathcal{R} \) in Theorems 2 and 3 associate with one auxiliary RV, and we need to handle the transition probability of test channel \( P_{U|X} \) alone for simulating the capacity region. In this sense, compared to the region \( \mathcal{R} \), it may require less time and space complexity to simulate the capacity regions with one auxiliary RV in Theorems 2 and 3.

\textbf{Remark 2.} The class of more capable channels includes less noisy channels as a special case [15]. When the ACs are in the class of more capable channels, i.e., \( I(X;Y) \geq I(X;Z) \) or \( I(X;Y) \leq I(X;Z) \), it is not yet known whether the capacity region can be characterized by one auxiliary RV or not. More specifically, due to the impact of noise in the enrollment phase, the condition \( I(X;Y) \geq I(X;Z) \) does not guarantee that \( I(\hat{X};Y) \geq I(X;Z) \) and \( I(Y;U) \geq I(Z;U) \), making it hard to identify the values of of the right-hand sides of the secret-key rate constraint in (9) and (10). The same observation also applies to the case where \( I(X;Y) \leq I(X;Z) \).

In the typical wiretap channels [10], the fundamental limits, e.g., the capacity-equivocation regions, depend on the channels.
where $P_{YZ|X}$ only through the marginal distributions of the main channel $P_{Y|X}$ and the eavesdropper’s channel $P_{Z|X}$ [21]. For a VSM of the authentication systems, this conclusion may be applicable. However, for HSM settings, the capacity region of the model is hinged on by not only the AC $P_{YZ|X}$, but also the noise in the enrollment phase $P_{X|Z}$.

B. Binary Sources

In this section, we give a binary example of Theorem 3 for an HSM in the case where the main channel is less noisy than the eavesdropper’s channel, corresponding to (14). Such an example can be described as follows:

Consider $X \sim \text{Bern}(\frac{1}{2})$, $P_{X|Z}$ is a binary symmetric channel (BSC) with crossover probability $p \in [0, 1/2]$, $P_{Y|X}$ is a binary erasure channel with erasure probability $q \in [0, 1]$, and $P_{Z|X}$ is a BSC with crossover probability $\epsilon \in [0, 1/2]$. Note that if the relation of $\epsilon$ and $q$ is such that $2q < \epsilon < 4q(1-q)$, $P_{Y|X}$ is less noisy than $P_{Z|X}$, but $P_{Z|X}$ is not a degraded version of $P_{Y|X}$ [15, Chapter 5]. Let the test channel $P_{U|X}$ be a BSC with crossover probability $\beta \in [0, 1/2]$. The optimal rate region of the model for this case is given below.

**Theorem 4.** For binary sources where the main channel $P_{Y|X}$ is less noisy than the eavesdropper’s channel $P_{Z|X}$, the capacity region of the system is given by

$$
\mathcal{R} = \bigcup_{0 \leq p, q \leq 1/2} \left\{ (R_S, R_J, R_L) \in \mathbb{R}^3_+ : 
\begin{align*}
R_S &\leq H_b(\beta p + \epsilon) - (1 - q)H_b(\beta p) - q, \\
R_J &\geq q + (1 - q)H_b(\beta p) - H_b(\beta), \\
R_L &\geq 1 + q - qH_b(\beta p) - H_b(q) \right\},
\right.
$$

where $H_b(\cdot)$ denotes the binary entropy function and the convolution operator is defined as $p * q = p(1-q) + (1-p)q$. □

The proof of Theorem 4 is given in [23, Appendix C]. In [14], the optimal rate region of the authentication systems for binary sources was derived under the assumption that $X = X$ (EC is noiseless) and the eavesdropper’s channel $P_{Z|X}$ is physically degraded w.r.t. the main channel $P_{Y|X}$, i.e., $X - Y - Z$. Theorem 4 is provided under a more general setting, and the key idea for deriving this theorem is to apply Mrs. Gerber Lemma [24] to the reverse direction of the eavesdropper’s channel to obtain an upper bound on the conditional entropy $H(Z|U)$. However, the obtained bound is not yet tight. We establish a new lemma to acquire the optimal upper bound on $H(Z|U)$ in order to match the outer region with the inner region.

C. Gaussian Sources

Unlike the discrete sources, for Gaussian sources, we provide the capacity region of the system under general classes of ACs. Assume that the source $X \sim \mathcal{N}(0, 1)$, the EC $P_{X|Z}$, and the ACs (the main channel $P_{Y|X}$ and the eavesdropper’s channel $P_{Z|X}$) are modeled as

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

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

Using a converting technique introduced in [22] or covariance matrix transformations in [12, Appendix C.1], (17) can be converted to

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

where $N_x \sim \mathcal{N}(0, 1 - \rho_3^2)$.

It is well-known that the Gaussian wiretap channel is always degraded [15], and this fact is also valid for the authentication systems. We explain it briefly in the following.

By virtue of [12, Lemma 6], in the case where

$$
\rho_1^2 > \rho_3^2,
$$

there exist joint Gaussian RVs $(\tilde{X}, X', Y', Z')$ such that the Markov chain $\tilde{X}' - X' - Y' - Z'$ holds. Also, the marginal densities of $(\tilde{X}', Y')$, $(\tilde{X}', Z')$, and $(\tilde{X}', X', Z')$ coincide with the marginal densities of $(X, Y)$, $(X, Z)$, and $(X, X, Z)$, respectively. On the other hand, when the coefficient correlations of the main and eavesdropper’s channels are in the form of

$$
\rho_1^2 \leq \rho_3^2,
$$

there exist joint Gaussian RVs $(\tilde{X}', X', Y', Z')$ such that the Markov chain $\tilde{X}' - X' - Y' - Z'$ holds, and the marginal densities of $(\tilde{X}', Y')$, $(\tilde{X}', Z')$, and $(\tilde{X}', X', Z')$ coincide with the marginal densities of $(\tilde{X}, Y)$, $(\tilde{X}, Z)$, and $(\tilde{X}, X, Z)$, respectively.

Since the constraints (3), (6), and (7) depend on the marginal densities of $(\tilde{X}, Y)$, $(\tilde{X}, Z)$, $(\tilde{X}, X, Z)$, it suffices to derive the characterization of $\mathcal{R}$ for Gaussian sources under the joint sources $(X', X', Y', Z')$ instead of (17). For brevity, we just use $(\tilde{X}, X, Y, Z)$ to represent $(\tilde{X}', X', Y', Z')$ in the statement of result for Gaussian sources.

**Theorem 5.** Under the condition of (19), i.e., $\tilde{X} - X - Y - Z$, the capacity region for Gaussian sources is characterized as

$$
\mathcal{R} = \bigcup_{P_{U|X}} \left\{ (R_S, R_J, R_L) \in \mathbb{R}^3_+ : R_S \leq I(Y; U|Z), \\
R_J \geq I(\tilde{X}; U|Y), \\
R_L \geq I(X; U|Y) + I(X; Z) \right\},
$$

where unlike Theorems 2 and 3, auxiliary RV $U$ is a continuous RV and its cardinality is unbounded. In the case of (20), i.e., $\tilde{X} - X - Z - Y$, we have that

$$
\mathcal{R} = \mathcal{A}_3.
$$

For a proof of Theorem 5, the readers should refer to the proof of Theorem 3. We again omit the details since both proofs can be done in a similar way.

Due to the unbounded cardinality of alphabet $\mathcal{U}$ in (21), the region is not computable, so we want to derive a parametric expression for Theorem 5.
Corollary 1. The parametric form of (21) is given as
\[ R = \bigcup_{\alpha \in [0,1]} \left\{ (R_S, R_J, R_L) : \begin{array}{l}
R_S \leq \frac{1}{2} \log \left( \frac{\alpha \rho_1^2 \rho_3^2 + 1 - \rho_2^2 \rho_3^2}{\alpha \rho_1^2 \rho_3^2 + 1 - \rho_1^2 \rho_3^2} \right), \\
R_J \geq \frac{1}{2} \log \left( \frac{\alpha \rho_1^2 \rho_3^2 + 1 - \rho_1^2 \rho_2^2}{\alpha \rho_1^2 \rho_3^2 + 1 - \rho_1^2 \rho_2^2} \right), \\
R_L \geq \frac{1}{2} \log \left( \frac{1}{1 - \rho_3^2} \right) \end{array} \right\}, \] (23)
and that of (22) is given as
\[ R = \{(R_S, R_J, R_L) : R_S = 0, \ R_S \geq 0, \ R_L \geq \frac{1}{2} \log \left( \frac{1}{1 - \rho_3^2} \right) \}. \] (24)

The proof of Corollary 1 is given in [23, Appendix D]. When the EC is noiseless (i.e., \( \rho_3^2 \to 1 \)), Corollary 1 reduces to the result for the generated-secret VSM derived in [19, Corollary 1]. In addition, when the eavesdropper can only observe the helper data, corresponding to the case where \( Z \) is independent of other RVs (\( \rho_3^2 = 0 \)), Corollary 1 matches with a parametric expression of the generated-secret HSM provided in [22, Corollary 1].

We provide some numerical calculations of the region \( R \) in (23) for Gaussian sources. Figures 2 and 3 show the rate values of the secret-key and privacy-leakage rates for given storage rates. In these figures, the blue and red graphs illustrate the behaviors of the VSM and HSM, respectively. In the calculation, we set \( \rho_1^2 = \frac{2}{5}, \rho_2^2 = \frac{4}{5}, \) and \( \rho_3^2 = \frac{2}{5} \), where \( \rho_2^2 > \rho_3^2 \) is satisfied. Figure 2 depicts a relation of secret-key rate for a given storage rate for the VSM [19] and the HSM in this paper. Similarly, Fig. 3 is a relation between the privacy-leakage and storage rates. For the secret-key rate, Fig. 2 shows that the VSM offers better performance. On the other hand, in terms of privacy-leakage rate, Fig. 3 tells us that the amount of information leaked to the eavesdropper remarkably decreases for the HSM. From these figures, we can see that by introducing noise in the enrollment phase, the fundamental limits of the authentication systems change. Also, these behaviors reflect the trade-off of achieving high secret-key rate and low privacy-leakage rate at the same time for given storage rate as it is pointed out in [22] for Gaussian sources and channels. Moreover, similar to a conclusion for discrete sources given in [13], poor system design may lead to a vulnerable system; a major loss of privacy and secret-key generation with undesirably low rate could happen.

IV. Conclusion

In this paper, we revealed that only a single auxiliary RV was required in the expression of the capacity region of the authentication systems when the ACs are in the shapes of physically or stochastically degraded channels and less noisy channels. Moreover, the capacity regions of the authentication systems for both binary and Gaussian sources were derived. We also provided some numerical calculations concerning the Gaussian case to capture the impact of noise in the enrollment phase toward the capacity region, and to visualize the trade-off between secret-key and privacy-leakage rates. For future work, it may be of sufficient interest to investigate the classes of channels taking only a single auxiliary RV to characterize the capacity region for the joint-measurement-channel model [17].

ACKNOWLEDGMENTS

This work was supported in part by the Ministry of Internal Affairs and Communications, Japan, through the contract of “Research and development on new generation cryptography for secure wireless communication services” among “Research and Development for Expansion of Radio Wave Resources,” under Grant JPJ000254 and by JSPS KAKENHI Grant Numbers JP20K04462 and JP18H01438.
REFERENCES

[1] A.K. Jain, P. Flynn, A. Ross, Handbook of Biometrics, Springer: New York, NY, USA, 2009.
[2] C. Böhme and M. Hofer, Physical Unclonable Functions in Theory and Practice, New York, NY, USA: Springer, Oct. 2012.
[3] C. Herder, M. Yu, F. Koushanfar and S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial,” Proc. IEEE, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.
[4] O. Günülü, “Secret-key agreement with physical unclonable functions and biometric identifiers,” Ph.D. dissertation, TU Munich, Germany, Nov. 2018.
[5] R. Pappu, “Physical one-way functions,” Ph.D. dissertation, MIT, Cambridge, MA, USA, Mar. 2001.
[6] B. Gassend, “Physical random functions,” Master’s thesis, M.I.T., Cambridge, MA, Jan. 2003.
[7] T. Ignatenko and F. Willems, “Biometric systems: Privacy and secrecy aspects,” IEEE Trans. Inf. Forensics Secur., vol. 4, no. 4, pp. 956–973, Dec. 2009.
[8] 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 Secur., vol. 6, no. 1, pp. 122–139, Mar. 2011.
[9] 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.
[10] A. D. Wyner, “The wire-tap channel,” Bell Labs Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[11] I. Csiszár 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.
[12] S. Watanabe and Y. Oohama, “Secret key agreement from correlated Gaussian sources by rate limited public communication,” IEICE Trans. Fundamentals, vol. E93-A, no. 11, Nov. 2010.
[13] O. Günülü and G. Kramer, “Privacy, secrecy, and storage with multiple noisy measurements of identifiers,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 11, pp. 2872–2883, Nov. 2018.
[14] O. Günülü, K. Kittichokechai, R. F. Schaefer and G. Caire, “Controllable identifier measurements for private authentication with secret keys,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 8, pp. 1945–1959, Aug. 2018.
[15] A. El Gamal and Y.-H. Kim, Network Information Theory, Cambridge, U.K.: Cambridge Univ. Press, 2011.
[16] O. Günülü, R. F. Schaefer, and G. Kramer, “Private authentication with physical identifiers through broadcast channel measurements,” in Proc. IEEE Inf. Theory Workshop, Visby, Sweden, Aug. 2019, pp. 1–5.
[17] O. Günülü and R. F. Schaefer, “Controllable key agreement with correlated noise,” IEEE J. Sel. Areas Inf. Theory, vol. 2, no. 1, pp. 82–94, Mar. 2021.
[18] T.S. Han, Information-Spectrum Methods in Information Theory, Springer, 2003.
[19] V. Yachongka, H. Yagi, and Y. Oohama, “Secret key-based authentication with passive eavesdropper for scalar Gaussian sources,” in Proc. 2022 IEEE Int. Symp. Inf. Theory (ISIT), Espoo, Finland, Jun./Jul. 2022, pp. 2685–2690.
[20] M. Bloch and J. Barros, Physical-Layer Security, Cambridge, U.K.: Cambridge Univ. Press, 2011.
[21] Y. Liang, H. V. Poor, and S. Shamai (Shitz), Information-Theoretic Security, Now Publishers, 2009.
[22] V. Yachongka, H. Yagi, and Y. Oohama, “Biometric identification systems with noisy enrollment for Gaussian sources and channels,” Entropy, vol. 23, no. 1049, Aug. 2021.
[23] V. Yachongka, H. Yagi, and H. Ochiai, “Secret-key agreement with physical identifiers for degraded and less noisy authentication channels,” arXiv:2208.10478, Aug. 2022.
[24] A. Wyner and J. Ziv, “A theorem on the entropy of certain binary sequences and applications–I,” IEEE Trans. Inf. Theory, vol. 19, no. 6, pp. 769–772, Nov. 1973.