Keyless Authentication and Authenticated Capacity

Wenwen Tu, *Student Member, IEEE,* and Lifeng Lai, *Member, IEEE*

***Abstract*—We consider the problem of keyless message authentication over noisy channels in the presence of an active adversary. Different from the existing models, in our model, the legitimate users do not have any pre-shared key for authentication. Instead, we use the noisy channel connecting the legitimate users for authentication. The main idea is to utilize the noisy channel connecting the legitimate users to distinguish a legitimate message from a fake message, by generating an output at the receiver that is difficult for the adversary to replicate through its noisy channel. By interpreting the message authentication as a hypothesis testing problem, we investigate the authentication exponent and the authenticated channel capacity of the noisy channel. In the authentication exponent problem, for a given message rate, we investigate the speed at which the optimal successful attack probability can be driven to zero. We fully characterize the authentication exponent for the zero-rate message case and provide both an upper bound and a lower bound on the exponent for the non-zero message rate case. In the authenticated capacity problem, we study the largest data transmission rate under which the attacker's optimal successful attack probability can still be made arbitrarily small. We establish an all or nothing result. In particular, we show that the authenticated channel capacity is the same as the classic channel capacity if a simulatability condition is not satisfied, while the authenticated capacity will be zero if this condition is satisfied. We also provide efficient algorithms to check this condition. We further show that our results are robust to modeling uncertainties about the eavesdropper's channels.**

***Index Terms*—Authentication, authenticated capacity, authentication exponent, hypothesis testing, K-L divergence, simulatability condition.**

I. Introduction

Message authentication is a fundamental concept in cryptography in the presence of an adversary who intends to deceive the legitimate receiver via sending fraudulent messages. It has been investigated intensively from different perspectives [2]–[14]. Most of existing works on authentication rely on a pre-shared secret (in the form of a shared key or shared randomness) between the transmitter and the legitimate receiver. The receiver uses this pre-shared secret to determine whether the received message is authentic or not. Under this shared key assumption, the authentication problem has been studied for both noiseless and noisy channel models.

The authentication model over a noiseless channel was developed by Simmons [5]. In this model, the communication channel is assumed to be noiseless, and the transmitter Alice and the receiver Bob share a secret key K. In order to send a message M to Bob, instead of transmitting M directly, Alice transmits a codeword $E = f(M, K)$ into the channel with f being the encoding function used by Alice. Upon receiving a codeword $\hat{E}$ ($\hat{E} = E$ if there is no attack; Otherwise, $\hat{E}$ is determined by the adversary), Bob first needs to check whether $\hat{E}$ is sent by Alice or not, based on the pre-shared key K. In [5], two types of attacks were considered. The first one is *impersonation attack*, in which the adversary Eve sends the fake codeword before Alice transmits anything. The impersonation attack is successful if the fake codeword is accepted by Bob. The successful attack probability of this attack is denoted by P_I. The second one is *substitution attack*, in which Eve initiates an attack after she observes the codeword sent by Alice. In particular, Eve intercepts the codeword sent by Alice (hence Bob does not receive this codeword), and replaces the intercepted codeword with her own attack codeword. The substitution attack is successful if the codeword from Eve is accepted by Bob and decoded into a message different from the message intended by Alice. The successful attack probability of the substitution attack is denoted as P_S. [5] also established lower bounds for P_I and P_S: $P_I \geq 2^{-I(K;E)}$, $P_S \geq 2^{-H(K|E)}$, where $I(\cdot;\cdot)$ is the mutual information between its arguments and $H(\cdot|\cdot)$ denotes the conditional entropy of its arguments. It is clear that there exists a tradeoff between making P_I and P_S smaller. To make P_I smaller, E should contain more information about the shared key K, that is $I(K;E)$ should be larger. However, this makes the substitution attack easier (i.e., $H(K|E)$ becomes smaller), as E will be overheard by Eve perfectly over the noiseless channel.

To overcome the tradeoff faced by the noiseless model in [5], as a natural extension, [3] extended Simmons's model to a noisy channel model, in which Alice and Eve (also Alice and Bob) are connected by noisy channels. The main idea is that the noisy channel between Alice and Eve may prevent Eve from learning information about K contained in E. In this way, we can embed more information about K in E to make the impersonation attack more difficult, while not making the substitution attack easier as the noisy channel between Alice and Eve may prevent Eve from learning information about K. Using this idea, [3] showed that one can make P_I and P_S to be simultaneously small under certain conditions. The model in [3] was further expanded in [15] to include noisy channel between Eve and Bob. The main observation is that the noisy channel between Alice and Bob and the noisy channel between Eve and Bob are different. And this difference can be exploited to facilitate the authentication of users, along with any pre-shared key.

W. Tu and L. Lai are with Department of Electrical and Computer Engineering, University of California, Davis, CA, 95616. Email: {wwtu,lflai}@ucdavis.edu. This work was supported by National Science Foundation under Grants CCF-1760889, CCF-1665073 and ECCS-1660140. This paper was presented in part at the Asilomar Conference on Signal, Systems, and Computers, Pacific Grove, CA, Nov. 2016 [1].

In this paper, we consider a similar model as [15]: Alice, Bob and Eve are all connected with one another by noisy channels. Here we assume that Alice and Bob *do not share any secret key*. We will mainly rely on the channel $W(Y|X)$ connecting Alice and Bob for authentication. In particular, for any input probability mass function (PMF) P_X generated by Alice, we produce an output distribution at Bob $P_Y = W(Y|X)P_X$. The main idea is to properly choose P_X so that the produced P_Y is difficult (precise meaning will be made clear in the sequel) for Eve to replicate through her noisy channel to Bob. In this way, after receiving a sequence Y^n, Bob can perform a hypothesis testing to check whether this sequence is generated from P_Y or not, which in return provides Bob evidences of whether the message is authentic or not. However, this hypothesis testing problem is more challenging than the classic hypothesis testing problems [16], in which each element of Y^n is typically assumed to be independently and identically generated from a certain PMF under each hypothesis. In our case, each element is not necessarily independent nor identically distributed. More importantly, the distribution under the alternative hypothesis, in which there is an attack, is totally controlled by the attacker (via the selection of the attack sequence) and can be arbitrary. Despite this challenge, we study and solve two closely related questions using this problem formulation.

In the first question, we focus on characterizing the optimal authentication exponent. In particular, for a given message rate, we investigate how to design the system so that the successful attack probability under Eve's optimal attack strategy is as smaller as possible. The speed at which the successful attack probability goes to zero is called the authentication exponent. We derive an upper bound as well as a lower bound on the authentication exponent. We show that the upper bound and the lower bound match in the zero-rate case. In the nonzero-rate scenario, we also identify some cases in which the upper and lower bound match. Hence the optimal authentication exponent is fully characterized in these cases.

In the second question, we focus on characterizing the authenticated capacity. In particular, we study what the largest data transmission rate is such that we can still design schemes to make Eve's successful attack probability arbitrarily small. We call such largest rate as the authenticated capacity. Compared with the classic definition of channel capacity, the authenticated capacity has an additional requirement that the decoded messages are guaranteed to come from the legitimate transmitter. We show an "all or nothing" result on the authenticated capacity. In particular, we show that if a "simulatability condition" is satisfied, the authenticated capacity is zero. On the other hand, if this condition is not satisfied, the authenticated capacity is the same as the classic notion of capacity. We also design efficient algorithms to check the simulatability condition for any given channels. We further extend our study to the authenticated secrecy capacity and show a similar "all or nothing" result.

We would like to mention that the case without any shared key is also briefly discussed in [15]. In addition, Our work is related to recent papers on authentication exploiting the channel intrinsic randomness as well as the properties of channel reciprocity [17]–[21]. These papers also studied the authentication problem without using any pre-shared key, and proposed various novel authentication schemes to exploit the different channel statistics associated with different channels for authentication. Compared with these interesting papers, in this paper, we characterize the fundamental limits of such systems by providing a more detailed and refined analysis.

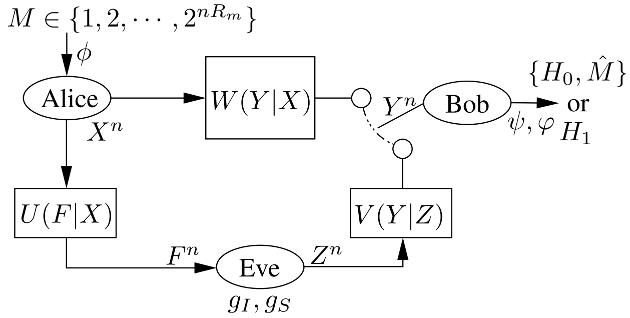


Fig. 1. System model

The remainder of the paper is organized as follows. In Section II, we introduce the system model. In Section III, we analyze the relationship between two types of attacks. In Section IV, we focus on characterizing the authentication exponent. In Section V, we characterize the authenticated capacity. Finally, in Section VI, we offer our concluding remarks.

Notation: We use X^n, Y^n and Z^n to denote the sequences generated or observed at Alice, Bob and Eve, respectively. Matrix $W(Y|X)$ is reserved as the channel statistics from Alice to Bob. $U(F|X)$ and $V(Y|Z)$ are defined in a similar manner. Furthermore, for any given sequence $X^n \in \mathcal{X}^n$, the relative frequencies $\left(\frac{n_1}{n},\cdots,\frac{n_{|\mathcal{X}|}}{n}\right)$ where $n_i, \forall i \in \mathcal{X}$ is the total number of indices $j \in [1:n]$ at which $X_j = i$, is called the type of X^n and is denoted by tp(X^n). We use P or Q to denote the PMF of a certain random variable, $\mathcal{T}_Y$ to denote the set of types of all sequences Y^n, and $\mathcal{T}_Y^n(P_Y)$ to denote the set of sequences Y^n with tp$(Y^n) = P_Y$. We use $\mathcal{P}$ to denote the set of all possible distributions. For example, $\mathcal{P}_X$ denotes the set of all possible distributions of random variable X. In addition, we denote $Q^n(A) := \Pr\{Y^n : Y^n \in A | Y \overset{iid}{\backsim} Q\}$, in which $Y \overset{iid}{\backsim} Q$ means that each component of Y^n is independently and identically distributed (i.i.d.) according to Q. Here, if $A = \mathcal{T}_Y^n(P_Y)$, we write it as $Q^n(P_Y)$ in short.

II. Preliminaries and Problem Setup

The model considered in this paper is illustrated in Fig.1. Two terminals, Alice and Bob, would like to communicate with each other in the presence of an active adversary Eve. Alice and Bob do not share any secret key. Let $\mathcal{X} =: \{1,\cdots,|\mathcal{X}|\}$, $\mathcal{Y} =: \{1,\cdots,|\mathcal{Y}|\}$, $\mathcal{Z} =: \{1,\cdots,|\mathcal{Z}|\}$, and $\mathcal{F} =: \{1,\cdots,|\mathcal{F}|\}$ be four finite discrete sets, which represent the input alphabet set of Alice, the output alphabet set of Bob, the input alphabet set and the output alphabet set of Eve, respectively. These three users are connected with one another by three *noisy discrete memoryless channels* $W(Y|X)$, $U(F|X)$ and $V(Y|Z)$, which connect Alice and Bob, Alice and Eve, as well as Eve and Bob respectively. Here, $W(Y|X)$ is an $|\mathcal{Y}| \times |\mathcal{X}|$ matrix, with each column i, denoted by $W(Y|i)$, representing the output distribution at Bob when the input is $X = i$. Other channel matrices are defined in a similar manner.

In this paper, we assume that $W(Y|X)$ is perfectly known. As it will be clear in the sequel, most of our schemes are universal with respect to Eve's channels $U(F|X)$ and $V(Y|Z)$. More specifically, with the exception of a particular scheme in Section V, most of our schemes do not depend on any knowledge about $U(F|X)$ and $V(Y|Z)$. Furthermore, we will show that the particular scheme in Section V is robust against the uncertainty of the knowledge of $V(Y|Z)$. Hence, even for that particular scheme, we do not need perfect knowledge of $V(Y|Z)$.

Alice would like to send a message $M \in [1 : |M|]$ to Bob. She will use an encoder ϕ to convert M to a certain codeword X^n and transmit it via the channel $W(Y|X)$. However, Eve is an active attacker, and is assumed to be able to intercept the transmission of X^n such that Bob does not receive Y^n from the channel $W(Y|X)$ if Eve initiates the attack. This is a typical assumption in the authentication literature [2]–[14] and represents the worst case scenario from the legitimate users' perspective. Furthermore, Eve can falsify messages and send them to Bob via the channel $V(Y|Z)$, based on her optimal strategy, to cheat Bob (details of the attacks considered will be made precise in the sequel). Thus, after observing a sequence Y^n, Bob first needs to check the identity of Y^n: whether it is transmitted from Alice or faked by Eve. In particular, Bob will use a tester ψ to determine which of the following hypothesis is true:

$$H_0 : Y^n \text{ comes from Alice, no attack occurs,} \quad (1)$$
$$H_1 : Y^n \text{ comes from Eve, an attack occurs.} \quad (2)$$

If Bob determines that H_0 is true, he will then use a decoder φ to decode Y^n and obtain a decoded message $\hat{M} = \varphi(Y^n)$.

In summary, the system consists of the following components:

$$\text{Encoder } \phi : M \to X^n, \quad (3)$$
$$\text{Tester } \psi : Y^n \to H_0 \text{ or } H_1, \quad (4)$$
$$\text{Decoder } \varphi \text{ (if Bob determines } H_0) : Y^n \to \hat{M}. \quad (5)$$

For a given ψ, the acceptance region is defined by

$$\mathscr{A}_n = \{y^n \in \mathcal{Y}^n : \psi(y^n) = H_0\}.$$

Following the existing work on authentication [2]–[10], two types of attacks are considered:

- *Impersonation attack* g_I: This attack occurs before Alice sends anything. In particular, Eve uses an attack strategy g_I to select a sequence Z^n and sends it into the channel $V(Y|Z)$ to cheat Bob. We use PV(Z^n) to denote the output at Bob when Eve sends Z^n. The impersonation attack is said to be successful if Bob decides H_0. We use P_I to denote the success probability of the impersonation attack, i.e., $P_I = \Pr(\text{PV}(Z^n) \in \mathscr{A}_n)$.
- *Substitution attack* g_S: This attack occurs after Alice sends a codeword $X^n = \phi(M)$. In this attack, Eve intercepts the communication between Alice and Bob such that Bob receives no sequence from the channel $W(Y|X)$. Then Eve sends a sequence $Z^n = g_S(F^n)$ to Bob via the channel $V(Y|Z)$ based on the observations F^n obtained from the channel $U(F|X)$ connecting Alice and Eve. The attack is successful if Bob decides H_0 and the decoded message is different from the message sent by Alice. We use P_S to denote the success probability of the substitution attack, i.e., $P_S = \Pr(\text{PV}(Z^n) \in \mathscr{A}_n \text{ and } \hat{M} \neq M)$.

The goal of the attacker is to design the attack strategies g_I and g_S to maximize its successful attack probability

$$P_{SA} := \max\{P_I, P_S\}. \quad (6)$$

If there is no attack (i.e., when H_0 is true), two classes of errors could occur at Bob. The first class is the false rejection error, in which Bob falsely determines that an attack has occurred. This error probability is denoted by $\Pr(H_1|H_0)$. The second class is that Bob correctly determines that there is no attack but incorrectly decodes the message. This error probability can be written as $\Pr\{\hat{M} \neq M, H_0|H_0\}$.

Definition 1. *A protocol (ϕ, ψ, φ) is called (ϵ, σ)-robust, if*

$$\max_M \Big\{ Pr\{\hat{M} \neq M, H_0|H_0\} + Pr(H_1|H_0) \Big\} \leq \epsilon, \quad (7)$$
$$\max_{g_I, g_S} P_{SA} \leq \sigma. \quad (8)$$

Furthermore, R_m is said to be achievable using an (ϵ, σ)-robust protocol, if

$$\frac{1}{n} \log |M| \geq R_m - \epsilon. \quad (9)$$

Here, (7) implies that, if there is no attack, the maximum error probability over all messages is required to be smaller than ϵ. At the same time, (8) implies that, if there is an attack, the success probability of Eve's optimal attack strategy is less than σ. In other words, if there is an attack, Bob should detect the presence of the attack with a probability larger than $1 - \sigma$. With these definitions, two related problems are considered in this paper:

- *Authentication Exponent:* For given R_m and ϵ, how fast can we make P_{SA} go to zero?
- *Authenticated Capacity:* What is the largest message rate R_m that a robust protocol can achieve?

A. Authentication Exponent

Define

$$\beta_n(R_m, \epsilon) = \min_{\phi, \psi, \varphi} \max_{g_I, g_S} P_{SA},$$

where ϕ, ψ and φ range over all possible functions satisfying (7) and (9). Furthermore, we define

$$\theta(R_m, \epsilon) = \liminf_{n\to\infty} -\frac{1}{n} \log \beta_n(R_m, \epsilon). \tag{10}$$

Here, $\theta(R_m, \epsilon)$ is the exponent (rate) at which the successful attack probability goes to zero as the block-length n increases.

Similarly, we can define

$$\beta_I(R_m, \epsilon) = \min_{\phi,\psi,\varphi} \max_{g_I} P_I, \tag{11}$$

$$\theta_I(R_m, \epsilon) = \liminf_{n\to\infty} -\frac{1}{n} \log \beta_I(R_m, \epsilon), \tag{12}$$

for the impersonation attack, and

$$\beta_S(R_m, \epsilon) = \min_{\phi,\psi,\varphi} \max_{g_S} P_S, \tag{13}$$

$$\theta_S(R_m, \epsilon) = \liminf_{n\to\infty} -\frac{1}{n} \log \beta_S(R_m, \epsilon), \tag{14}$$

for the substitution attack.

In this problem, our goal is to characterize $\theta(R_m, \epsilon)$.

B. Authenticated (Secrecy) Capacity

In the authenticated capacity problem, we would like to characterize the authenticated capacity of the channel $W(Y|X)$:

$$C^* = \sup_{\phi,\psi,\varphi} R_m,$$

in which the sup is taken over all ϕ, ψ, φ that satisfy (7) and (8) for arbitrarily small ϵ, σ. Compared with the classic definition of channel capacity C, the authenticated capacity has an additional requirement that the decoded messages are guaranteed to come from the legitimate transmitter. Clearly, we have that $C^* \leq C$.

In addition, we would also like to characterize the authenticated secrecy capacity C_S^*, which is defined as the largest achievable rate such that (7) and (8) are satisfied and

$$\frac{1}{n} I(M; F^n) \leq \epsilon.$$

Again, compared with the classic definition of secrecy capacity C_S [22], our definition of authenticated secrecy capacity has the additional requirement that the accepted messages are guaranteed to come from the legitimate transmitter. Hence, we also have $C_S^* \leq C_S$.

III. Impersonation Attack vs Substitution Attack

In this section, we first analyze the relationship between the success probabilities of the impersonation attack and the substitution attack. This analysis illustrates that we can focus only on the impersonation attack, which can greatly simplify the presentation of the paper.

Theorem 1. *If $|M| > 1$, we have*

$$\theta(R_m, \epsilon) = \theta_I(R_m, \epsilon) = \theta_S(R_m, \epsilon). \tag{15}$$

Proof: We first prove the second equality. For the substitution attack, suppose a sequence X^n is transmitted by Alice, and Eve observes a corresponding sequence F^n, then we have

$$\begin{aligned}
\beta_S(R_m, \epsilon) &= \min_{\phi,\psi,\varphi} \max_{g_S(F^n)} P_S \\
&= \min_{\phi,\psi,\varphi} \max_{g_S(F^n)} \Pr(\text{PV}(Z^n) \in \mathscr{A}_n, \hat{M} \neq M) \\
&\leq \min_{\phi,\psi,\varphi} \max_{g_S(F^n)} \Pr(\text{PV}(Z^n) \in \mathscr{A}_n) \\
&\leq \min_{\phi,\psi,\varphi} \max_{g_S(X^n)} \Pr(\text{PV}(Z^n) \in \mathscr{A}_n) \\
&\leq \min_{\phi,\psi,\varphi} \max_{X^n} \max_{g_S(X^n)} \Pr(\text{PV}(Z^n) \in \mathscr{A}_n) \\
&\overset{(a)}{\leq} \min_{\phi,\psi,\varphi} \max_{g_I} P_I \\
&= \beta_I(R_m, \epsilon).
\end{aligned} \tag{16}$$

Here, step (a) can be justified as follows. First, we note that the difference between the impersonation attack and the substitution attack lies in whether or not Eve observes the sequence F^n from the channel $U(F|X)$ before selecting the optimal attack sequence Z^n. Based on this observation, then for any given ϕ, ψ, φ and substitution attack strategy, we can construct a corresponding impersonation attack strategy as follows. Eve assumes that a codeword $\tilde{X}^n$ was transmitted by Alice and then generates $\tilde{F}^n$ using $U(F|X)$. With this $\tilde{F}^n$, Eve then makes the corresponding substitution attack. As Alice does not share a key with Bob in our model, Eve can generate $\tilde{X}^n$ in the same manner as Alice generates X^n (in the model with key considered in the existing work, Eve cannot do this as she does not know the key value shared by Alice and Bob), $\tilde{F}^n$ will have the same statistics as F^n. Since this is a particular impersonation attack strategy, we have

$$\begin{aligned}
&\max_{\tilde{X}^n} \max_{g_S(\tilde{X}^n)} \Pr(\text{PV}(Z^n) \in \mathscr{A}_n) \\
&\qquad\qquad \leq \max_{g_I} \Pr(\text{PV}(Z^n) \in \mathscr{A}_n),
\end{aligned}$$

which indicates

$$\begin{aligned}
&\min_{\phi,\psi,\varphi} \max_{X^n} \max_{g_S(X^n)} \Pr(\text{PV}(Z^n) \in \mathscr{A}_n) \\
&\leq \min_{\phi,\psi,\varphi} \max_{g_I} \Pr(\text{PV}(Z^n) \in \mathscr{A}_n) \\
&= \min_{\phi,\psi,\varphi} \max_{g_I} P_I.
\end{aligned}$$

Thus, we have

$$\theta_S(R_m, \epsilon) \geq \theta_I(R_m, \epsilon). \tag{17}$$

Now, we show the other direction. The following is a valid substitution attack strategy: Given ϕ, ψ and φ, no matter what F^n Eve observes from $U(F|X)$, she simply ignores F^n, and uses the corresponding optimal impersonation attack strategy to pick the attack sequence Z^n. We use P_S^* to denote the success probability of this particular substitution attack strategy, and we have

$$P_S^* = \left(1 - \frac{1}{|M|}\right) \max_{g_I} P_I,$$

with given ϕ, ψ and φ. Thus,

$$\begin{aligned}\beta_S(R_m,\epsilon) &= \min_{\phi,\psi,\varphi}\max_{g_S} P_S \\ &\geq \min_{\phi,\psi,\varphi} P_S^* \\ &= \left(1-\frac{1}{|M|}\right)\min_{\phi,\psi,\varphi}\max_{g_I} P_I \\ &= \left(1-\frac{1}{|M|}\right)\beta_I(R_m,\epsilon), \qquad (18)\end{aligned}$$

which implies

$$\theta_S(R_m,\epsilon) \leq \theta_I(R_m,\epsilon). \qquad (19)$$

Combining (17) with (19), we have

$$\theta_S(R_m,\epsilon) = \theta_I(R_m,\epsilon).$$

To show the first equality of (15), we have

$$\begin{aligned}\beta_n(R_m,\epsilon) &= \min_{\phi,\psi,\varphi}\max_{g_I,g_S} P_{SA} \\ &= \min_{\phi,\psi,\varphi}\max_{g_I,g_S}\max\{P_I,P_S\} \\ &= \min_{\phi,\psi,\varphi}\max\{\max_{g_I,g_S} P_I, \max_{g_I,g_S} P_S\} \\ &= \min_{\phi,\psi,\varphi}\max\{\max_{g_I} P_I, \max_{g_S} P_S\} \\ &\overset{(a)}{=} \min_{\phi,\psi,\varphi}\max_{g_I} P_I \\ &= \beta_I(R_m,\epsilon),\end{aligned}$$

where step (a) is true due to (16). Thus,

$$\theta(R_m,\epsilon) = \theta_I(R_m,\epsilon).$$

■

Remark 1. *This result shows that we can focus on analyzing the successful attack probability as well as its exponent based on the impersonation attack, as $\theta(R_m,\epsilon) = \theta_I(R_m,\epsilon) = \theta_S(R_m,\epsilon)$ and*

$$0 \leq \beta_I(R_m,\epsilon) - \beta_S(R_m,\epsilon) \leq \frac{1}{|M|}\beta_I(R_m,\epsilon), \qquad (20)$$

which is true due to (18). *The difference in* (20) *is a relatively small number, which has no influence on the authentication exponent analyzed in Section IV even when $|M|$ is finite. In addition, this difference will not affect the capacity result analyzed in Section V, since in that case $\beta_I(R_m,\epsilon)$ is an arbitrarily small number.*

Remark 2. *Here, we would like to compare this result with the result in the classic authentication setup [5], in which there exists a tradeoff between P_I and P_S as mentioned in the introduction: $P_I \geq 2^{-I(K;E)}$, $P_S \geq 2^{-H(K|E)}$. As discussed above, in the classic authentication setup, the authentication is based on the pre-shared key information. In the case with a shared key, the codeword E sent by Alice will contain information of K, which will be useful for Eve to carry out the substitution attack. In fact, the information about K contained in E is the main reason for the existence of a tradeoff between P_I and P_S in the classic setup. If E contains more information about K, the impersonation attack will be more difficult ($P_I \downarrow$) but the substitution attack will be easier ($P_S \uparrow$). Similarly, if E contains less information about K, $P_I \uparrow$ while $P_S \downarrow$. In our setup, there is no shared key, hence the codeword X^n sent by Alice does not carry any identification information and Eve can simply generate it by herself. In particular, when Alice sends nothing (thus the corresponding attack is an impersonation attack), Eve can construct an impersonation attack strategy by assuming a sequence $\tilde{X}^n$ was sent by Alice and using the corresponding substitution attack toward this $\tilde{X}^n$.*

We note that, when $M = 1$, there is no substitution attack as there is no any other message for the attacker to substitute with. In this case, $\beta_S(R_m,\epsilon) = 0$ and the corresponding $\theta_S(R_m,\epsilon)$ is not defined while $\beta_I(R_m,\epsilon)$ can still be positive with well defined $\theta_I(R_m,\epsilon)$. This case will be analyzed in Theorem 2 below. Furthermore, we can easily conclude that $\theta(R_m,\epsilon) = \theta_I(R_m,\epsilon)$ still holds.

IV. Authentication Exponent

In this section, for a given R_m and ϵ, we focus on characterizing the authentication exponent $\theta(R_m,\epsilon)$. We will first focus on the zero-rate case, in which $R_m = 0$, and then focus on the positive rate case.

A. Authentication of Zero-Rate Messages

To illustrate the main proof ideas, we first study the case of authentication for zero-rate messages: $|M|$ is finite, or infinite but

$$R_m = \frac{1}{n}\log|M| \to 0,$$

as $n \to \infty$. As discussed in Remark 1, it is sufficient to characterize $\theta_I(0,\epsilon)$.

Before deriving $\theta_I(0,\epsilon)$, we first analyze a special case: the case of single message, i.e., $|M| = 1$. In the single message case, the decoding step φ is not needed, hence the term $\Pr\{\hat{M} \neq M, H_0|H_0\}$ vanishes and (11) becomes

$$\beta_I(0_1,\epsilon) = \min_{\phi,\psi}\max_{g_I} P_I,$$

with 0_1 denoting the fact that $|M| = 1$. We also use $\theta_I(0_1,\epsilon)$ to denote the corresponding exponent.

We have the following three elements:

- From Alice's perspective, it needs to design ϕ. In this case, it is equivalent to deciding which X^n to use as the codeword.
- From Bob's perspective, it needs to design ψ for the following hypothesis testing problem:

$$\begin{aligned}H_0 &: Y^n \sim PW(X^n), \\ H_1 &: Y^n \sim PV(Z^n),\end{aligned}$$

  in which PW(X^n) denote the output at Bob when Alice sends X^n. However, it is more challenging than the classic hypothesis testing problem [16], in which $Y_i, i = 1, \cdots, n$ are typically assumed to be independently and identically generated from a certain PMF under each hypothesis. In our case, Y_i is not necessarily independent nor identically distributed for different i. More importantly, the distribution under H_1 is totally controlled by the attacker (via the selection of the attack sequence Z^n) and can be arbitrary.

- From Eve's perspective, its goal is to design g_I and the corresponding attack sequence Z^n to maximize the error probability.

Taking the above three elements into consideration, we have the following result.

Theorem 2.

$$\theta_I(0_1, \epsilon) = \max_{i \in \mathcal{X}} \min_{P_{Z,i} \in \mathcal{P}_Z} D(P_{Y,i} || Q_{Y,i}), \tag{21}$$

in which

$$P_{Y,i} = W(Y|i), \tag{22}$$

$$Q_{Y,i} = \sum_{j \in \mathcal{Z}} V(Y|j) P_{Z,i}(j), \tag{23}$$

$P_{Z,i}$ is some distribution of Z for each $i \in \mathcal{X}$, and $D(\cdot||\cdot)$ is the Kullback-Leibler (KL) distance between its arguments.

To simplify the presentation of the proof of Theorem 2, we first introduce a concept and its property from [23].

Definition 2 ([23]). *Let X be a random variable with PMF P. For a given $r \geq 0$, a sequence X^n is called a r-divergent sequence for P if*

$$D(tp(X^n)||P) \leq r.$$

We also denote the set of all r-divergent sequences for P as $S_r^n(P)$.

Lemma 1 ([23]). *Fix $r \geq 0$, then*

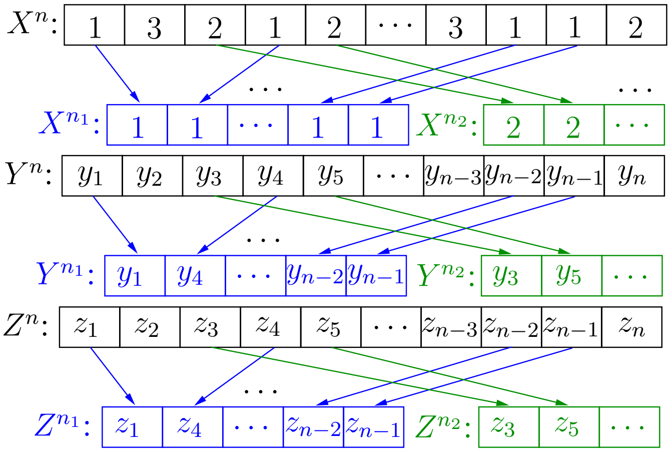
$$P^n(S_r^n(P)) \geq 1 - (n+1)^{|\mathcal{X}|} \exp(-nr).$$

Now, we proceed to our proof of Theorem 2.

Proof of Theorem 2: The proof has two major steps: 1) Step 1: For any given ϕ, we characterize the optimal ψ, g_I and the corresponding error exponent; 2) Step 2: Characterize the optimal ϕ.

Step 1: Characterizing optimal ψ and g_I for any given ϕ: In this step, we suppose ϕ is fixed (i.e., the codeword X^n for the message is given), and assume $\text{tp}(X^n) = P_X$. Analyzing this case involves two phases. In the first phase, we show that we can construct ψ such that $\beta_I(0_1, \epsilon)$ goes to zero exponentially with a rate $\min\limits_{\{P_{Z,i}\}_{i \in \mathcal{X}}} \sum\limits_i P_X(i) \cdot D(P_{Y,i}||Q_{Y,i})$. In the second phase, we show there is no scheme that can achieve an exponent larger than $\min\limits_{\{P_{Z,i}\}_{i \in \mathcal{X}}} \sum\limits_i P_X(i) \cdot D(P_{Y,i}||Q_{Y,i})$.

Step 1.1: For a given ϕ, construct a particular ψ and characterize the corresponding optimal attack strategy g_I: Fix a selected codeword X^n with type $\text{tp}(X^n) = P_X$. We need to characterize which attack sequences Z^n are optimal to minimize the error exponent. All our analysis is based on separating X^n into $|\mathcal{X}|$ sub-sequences such that each element within the same sub-sequence has the same realization. Thus, without any loss of generality, we assume $X^n = 1^{n_1} 2^{n_2} \cdots |\mathcal{X}|^{n_{|\mathcal{X}|}}$, in which $n_i = nP_X(i), i \in \mathcal{X}$. In the following, we denote the positions of i^{n_i} in X^n as the ith segment. For a general X^n, the sequence in the ith segment is denoted by X^{n_i}. And Y^{n_i} and Z^{n_i} are defined in the same manner, see Fig. 2.



X^n:
1 3 2 1 2 ··· 3 1 1 2
···
X^{n_1}:
1 1 ··· 1 1
X^{n_2}:
2 2 ···
Y^n:
y_1 y_2 y_3 y_4 y_5 ··· y_{n-3} y_{n-2} y_{n-1} y_n
···
Y^{n_1}:
y_1 y_4 ··· y_{n-2} y_{n-1}
Y^{n_2}:
y_3 y_5 ···
Z^n:
z_1 z_2 z_3 z_4 z_5 ··· z_{n-3} z_{n-2} z_{n-1} z_n
···
Z^{n_1}:
z_1 z_4 ··· z_{n-2} z_{n-1}
Z^{n_2}:
z_3 z_5 ···

Fig. 2. An illustration of the 1th segment for a general sequence X^n.

In the ith segment, since $X^{n_i} = i^{n_i}$ and that the channel $W(Y|X)$ is memoryless, Y^{n_i} obtained by passing X^{n_i} through the channel $W(Y|X)$ can be seen as generated i.i.d. according to $P_{Y,i} := W(Y|i)$. Now, we set the acceptance region, which in return determines ψ, as

$$\mathscr{A}_n(X^n) = \{Y^{n_1} \cdots Y^{n_{|\mathcal{X}|}} : Y^{n_i} \in \mathscr{A}_i, i \in \mathcal{X}\}, \tag{24}$$

in which

$$\mathscr{A}_i := S_r^{n_i}(P_{Y,i})$$

is defined in the ith segment with

$$r = \max_{i \in \mathcal{X}} -\frac{1}{n_i} \log \frac{\epsilon}{|\mathcal{X}|}(n_i+1)^{-|\mathcal{X}|}. \tag{25}$$

With this r, we have, according to Lemma 1, that

$$P_{Y,i}^{n_i}(S_r^{n_i}(P_{Y,i})) \geq 1 - \frac{\epsilon}{|\mathcal{X}|}, \forall i \in \mathcal{X}.$$

Then, we have

$$\Pr\{\mathscr{A}_n(X^n)|X^n\} \geq \prod_{i \in \mathcal{X}} \left(1 - \frac{\epsilon}{|\mathcal{X}|}\right) > 1 - \epsilon.$$

Thus,

$$\Pr(H_1|H_0) \leq \epsilon.$$

Hence using this particular ψ, the constraint (7) is satisfied.

In the following, we analyze the successful attack probability and characterize the optimal g_I (equivalently the optimal choice of the attack sequence Z^n) for this particular ψ. For any sequence Z_0^n selected by Eve, we denote the successful attack probability as $\Pr\{\mathscr{A}_n(X^n)|Z_0^n\}$. We realize that, due to the symmetric construction of $\mathscr{A}_n(X^n)$, we have

$$\Pr\{\mathscr{A}_n(X^n)|Z_0^n\} = \prod_{i\in\mathcal{X}} \Pr\{\mathscr{A}_i|Z_0^{n_i}\}.$$

To further analyze this probability, we need the following lemma whose proof is provided in Appendix B.

Lemma 2. *Set the acceptance region of a k length sequence Y^k as $S_r^k(P_Y)$, then the successful attack probability of any sequence Z_0^k via channel $V(Y|Z)$ is upper bounded by*

$$Pr\{S_r^k(P_Y)|Z_0^k\} \leq (k+1)^{|\mathcal{Y}|+|\mathcal{Z}|} 2^{-k(D(P_Y||Q_Y)-\delta(r))},$$

where $Q_Y = \sum\limits_{j\in\mathcal{Z}} V(Y|j)\cdot P_Z(j)$ with $P_Z := tp(Z_0^k)$.

Using Lemma 2 and let $\text{tp}(Z_0^{n_i}) = P_{Z,i}$, we have

$$\Pr\{\mathscr{A}_i|Z_0^{n_i}\} \leq n^{|\mathcal{Y}|+|\mathcal{Z}|} 2^{-n_i(D(P_{Y,i}||Q_{Y,i})-\delta(r))}. \tag{26}$$

Thus, we have

$$\begin{aligned}
&\Pr\{\mathscr{A}_n(x^n)|Z_0^n\} \\
&\quad\leq n^{|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{Z}|)} \prod_{i\in\mathcal{X}} 2^{-n_i(D(P_{Y,i}||Q_{Y,i})-\delta(r))} \\
&\quad= n^{|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{Z}|)} 2^{\sum_i -n_i(D(P_{Y,i}||Q_{Y,i})-\delta(r))} \\
&\quad= n^{|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{Z}|)} 2^{-n(\sum P_X(i)D(P_{Y,i}||Q_{Y,i})-\delta(r))}, \qquad (27)
\end{aligned}$$

which implies

$$\begin{aligned}
-\frac{1}{n}\log \Pr\{\mathscr{A}_n(x^n)|Z_0^n\} \geq \sum P_X(i)D(P_{Y,i}||Q_{Y,i}) \\
-\delta(r) - \frac{|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{Z}|)}{n}\log n. \qquad (28)
\end{aligned}$$

Inequality (28) implies that for our particular choice of ψ as specified in (24), the smallest exponent that Eve can hope for is

$$\min_{\{P_{Z,i}\}_{i\in\mathcal{X}}} \sum P_X(i)D(P_{Y,i}||Q_{Y,i}). \tag{29}$$

Now, we show that Eve can indeed achieve (29). Let $P_{Z^*,i}$ be the minimizer for (29) and $Q_{Y,i}^*$ be the corresponding value computed from (23). Similarly as (69), we also have, from Lemma 6 in Appendix A, that $\forall$ $\text{tp}(Y^{n_i})$: $\mathcal{T}_Y^{n_i}(\text{tp}(Y^{n_i})) \subseteq S_r^{n_i}(P_{Y,i})$,

$$D(\text{tp}(Y^{n_i})||Q_{Y,i}^*) \leq D(P_{Y,i}||Q_{Y,i}^*) + \delta(r),$$

in which $\delta(r)$ goes to zero as r decreases. Thus,

$$\begin{aligned}
Q_{Y,i}^{*,n_i}(\mathscr{A}_i) &\geq Q_{Y,i}^{*,n_i}(\text{tp}(Y^{n_i})) \\
&\overset{(a)}{\geq} \frac{1}{(n_i+1)^{|\mathcal{Y}|}} 2^{-n_i D(\text{tp}(Y^{n_i})||Q_{Y,i}^*)} \\
&\geq \frac{1}{(n+1)^{|\mathcal{Y}|}} 2^{-n_i(D(P_{Y,i}||Q_{Y,i}^*)+\delta(r))}, \qquad (30)
\end{aligned}$$

in which (a) is due to Theorem 11.1.4 in [24]. Now, consider a particular attack strategy g_I^*, in which Eve generates Z^{n_i} i.i.d. according to $P_{Z^*,i}$ in the ith segment, $\forall i \in \mathcal{X}$. With this particular attack strategy, from (30), the success probability is

$$P_I^* \geq \frac{1}{(n+1)^{|\mathcal{X}||\mathcal{Y}|}} 2^{-n(\sum\limits_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_{Y,i}^*)+\delta(r))}, \tag{31}$$

which implies that

$$\begin{aligned}
-\frac{1}{n}\log P_I^* \leq \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_{Y,i}^*) \\
+\delta(r) - \frac{|\mathcal{X}||\mathcal{Y}|}{n}\log n. \qquad (32)
\end{aligned}$$

As both $\delta(r)$ and $-\frac{|\mathcal{X}||\mathcal{Y}|}{n}\log n$ go to zero as n increases, we conclude that g_I^* achieves (29), the best Eve can hope for. Hence, for our particular choice of ψ, g_I^* is the optimal attack strategy.

Step 1.2: Show ψ constructed in Step 1.1 is optimal: Consider any acceptance region $\mathscr{A}_n$ with $\Pr\{\mathscr{A}_n|X^n\} \geq 1-\epsilon$, we will show that the particular attack strategy g_I^* discussed above will achieve an exponent specified in (29). Here $\Pr\{\mathscr{A}_n|X^n\} \geq 1-\epsilon$ is due to the fact that $\Pr\{\mathscr{A}_n|X^n\} = 1-\Pr(H_1|H_0)$ as well as the requirement defined by (7). We denote the set of the ith segment sequences of $Y^n \in \mathscr{A}_n$ by $\mathscr{A}_i, i \in \mathcal{X}$. Then we have

$$\begin{aligned}
1-\epsilon &\leq \Pr\{\mathscr{A}_n|X^n\} \\
&= \sum_{Y^n\in\mathscr{A}_n} \Pr\{Y^n|X^n\} \\
&= \sum_{Y^n\in\mathscr{A}_n} \prod_{i\in\mathcal{X}} \Pr\{Y^{n_i}|i^{n_i}\} \\
&= \sum_{Y^n\in\mathscr{A}_n} \prod_{i\in\mathcal{X}} P_{Y,i}^{n_i}(Y^{n_i}) \\
&= \sum_{Y^{n_k}\in\mathscr{A}_k} \sum_{Y^{n\setminus n_k}\in\mathscr{A}\setminus\mathscr{A}_k} P_{Y,k}^{n_k}(Y^{n_k}) \prod_{i\in\mathcal{X}\setminus k} P_{Y,i}^{n_i}(Y^{n_i}) \\
&= \sum_{Y^{n_k}\in\mathscr{A}_k} P_{Y,k}^{n_k}(Y^{n_k}) \sum_{Y^{n\setminus n_k}\in\mathscr{A}\setminus\mathscr{A}_k} \prod_{i\in\mathcal{X}\setminus k} P_{Y,i}^{n_i}(Y^{n_i}) \\
&\leq \sum_{Y^{n_k}\in\mathscr{A}_k} P_{Y,k}^{n_k}(Y^{n_k}) \\
&= \Pr\{\mathscr{A}_k|(X=k)^{n_k}\}.
\end{aligned}$$

Now, consider the attack strategy g_I^* discussed above. Using Lemma 7 in Appendix A, we have

$$Q_{Y,k}^{n_k}(\mathscr{A}_k) \geq (1-2\epsilon)2^{-n_k(D(P_{Y,k}||Q_{Y,k}^*)+\epsilon)}.$$

Then, it follows

$$\begin{aligned}
P_I^* &\geq \prod_{i\in\mathcal{X}} (1-2\epsilon)2^{-n_i(D(P_{Y,i}||Q_{Y,i}^*)+\epsilon)} \\
&= (1-2\epsilon)^{|\mathcal{X}|} 2^{\sum\limits_{i\in\mathcal{X}} -n_i(D(P_{Y,i}||Q_{Y,i}^*)+\epsilon)} \\
&= (1-2\epsilon)^{|\mathcal{X}|} 2^{-n\left(\sum\limits_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_{Y,i}^*)+\epsilon\right)}.
\end{aligned}$$

Since P_I^* is obtained by the particular attack strategy g_I^*, it must be less or equal to that from the optimal attack strategy (denote the optimal attack sequence by $Z^{\star n}$)with respect to $\mathscr{A}_n$, i.e. $\Pr\{\mathscr{A}_n|Z^{\star n}\} \geq P_I^*$. Thus, we have

$$\begin{aligned}
&-\frac{1}{n}\log \Pr\{\mathscr{A}_n|Z^{\star n}\} \\
&\leq \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_{Y,i}) + \epsilon - \frac{|\mathcal{X}|}{n}\log(1-2\epsilon). \quad (33)
\end{aligned}$$

Combining (28) and (33) with the fact that Eve can always select a Z^n with the optimal types $\{P_{Z,i}\}_{i\in\mathcal{X}}$ in corresponding segments, we conclude that the exponent of the successful attack probability when X^n is given, denoted by $\theta_I(X^n)$, is

$$\theta_I(X^n) = \min_{\{P_{Z,i}\}_{i\in\mathcal{X}}} \sum_i P_X(i)\cdot D(P_{Y,i}||Q_{Y,i}).$$

Step 2: Characterize the optimal ϕ: Now, we optimize over ϕ. We obtain

$$\begin{aligned}
\theta_I(0_1,\epsilon) &= \max_{X^n}\theta_I(X^n) = \max_{P_X}\theta_I(X^n) \\
&= \max_{P_X}\min_{\{P_{Z,i}\}_{i\in\mathcal{X}}}\sum_i P_X(i)\cdot D(P_{Y,i}||Q_{Y,i}) \\
&= \max_{i\in\mathcal{X}}\min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}),
\end{aligned}$$

in which the last step is true as $\sum\limits_i P_X(i)\cdot D(P_{Y,i}||Q_{Y,i})$ is a linear function of $P_X(i), i = 1,\cdots,|\mathcal{X}|$. This completes the proof. ■

Remark 3. *According to Theorem 2.7.2 of [24], $D(P_{Y,i}||Q_{Y,i})$ is convex in the pair $(P_{Y,i}, Q_{Y,i})$. Thus, for a fixed $P_{Y,i}$, we know that $D(P_{Y,i}||Q_{Y,i})$ is convex in $Q_{Y,i}$. In addition, $Q_{Y,i}$ is linear in $P_{Z,i}$ according to* (23)*, we can conclude that $D(P_{Y,i}||Q_{Y,i})$ is convex in $P_{Z,i}$ (See Chapter 2 in [25]). Hence, $\min\limits_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i})$ with constraints* (22) *and* (23) *is a convex optimization problem, which can be solved efficiently.*

Having obtained $\theta_I(0_1,\epsilon)$ of the single message case, we can easily generalize it to the case of multiple messages with zero-rate.

Theorem 3. *For the zero-rate case, we have*

$$\theta_I(0,\epsilon) = \theta_I(0_1,\epsilon).$$

Proof: First, we show

$$\theta_I(0,\epsilon) \leq \theta_I(0_1,\epsilon) = \max_{i\in\mathcal{X}}\min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}).$$

For the multiple messages case, we again require $\Pr(H_1|H_0) \leq \epsilon$. Meanwhile,

$$\Pr(H_1|H_0) = \sum_{i=1}^{|M|} P(M=i)\Pr(H_1|H_0, M=i).$$

As a result, there must exist at least one $m \in [1:|M|]$, such that $\Pr(H_1|H_0, M=m) \leq \epsilon$. If we focus on the message $M=m$, it has the same requirements as the single message case. Thus, we can conclude that

$$\theta_I(0,\epsilon) \leq \max_{i\in\mathcal{X}}\min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}).$$

In the following, we show that we can construct a scheme to achieve $\max\limits_{i\in\mathcal{X}}\min\limits_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i})$. Let $i_0 = \arg\max\limits_{i\in\mathcal{X}}\{\min\limits_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i})\}$. Since $\frac{1}{n}\log|M| \overset{n\to\infty}{\longrightarrow} 0$, there exist arbitrarily small nonnegative numbers $\{\epsilon_i\}_{i\in\mathcal{X}\setminus\{i_0\}}$, when n is sufficiently large, such that $2^{nI(X^*;Y)} > |M|$, where the distribution of X^* is given by

$$\begin{aligned}
P_X^* &:= [\epsilon_1,\cdots,\epsilon_{i_0-1}, 1-\epsilon_0, \epsilon_{i_0+1},\cdots,\epsilon_{|\mathcal{X}|}]^T, \\
&\qquad\qquad \text{with } \epsilon_0 := \sum_{i\neq i_0}\epsilon_i. \qquad (34)
\end{aligned}$$

Now, we use P_X^* defined above to do channel coding as that in [24, Chapter 7]: Generate $|M|$ sequences as codewords, and set the acceptance region be $\mathscr{A}_n := T_\epsilon^n(Y)$, in which the typical set is defined with respect to $P_Y = \sum\limits_{i\in\mathcal{X}} P_X^*(i)W(Y|i)$. Thus, we can easily verify that (7) is satisfied. For any sequence Z_0^n selected by Eve, we denote the successful attack probability as $\Pr\{\mathscr{A}_n|Z_0^n\}$. We realize that, for any given value $\epsilon > 0$, there exists an r, with r vanishing as ϵ goes to zero, such that

$$\mathscr{A}_n \subseteq S_r^n(P_Y),$$

which implies that

$$\Pr\{\mathscr{A}_n|Z_0^n\} \leq \Pr\{S_r^n(P_Y)|Z_0^n\}.$$

Using Lemma 2, we have

$$\Pr\{S_r^n(P_Y)|Z_0^n\} \leq (n+1)^{|\mathcal{Y}|+|\mathcal{Z}|}2^{-n(D(P_Y||Q_Y)-\delta(r))},$$

Thus, it follows that

$$\begin{aligned}
\theta_I(0,\epsilon) &\geq D(P_Y||Q_Y) - \delta(r) - \frac{|\mathcal{Y}|+|\mathcal{Z}|}{n}\log(n+1) \\
&:= \min_{P_Z} D(P_Y||Q_Y) - \epsilon' \\
&= D(P_Y||Q_Y^*) - \epsilon' \\
&\overset{(a)}{\geq} D(P_{Y,i_0}||Q_Y^*) - \delta(\epsilon') \\
&\geq \min_{P_Z} D(P_{Y,i_0}||Q_Y) - \delta(\epsilon') \\
&= \min_{P_{Z,i_0}} D(P_{Y,i_0}||Q_{Y,i_0}) - \delta(\epsilon') \\
&= \max_{i\in\mathcal{X}}\min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}) - \delta(\epsilon'),
\end{aligned}$$

where $Q_Y = \sum\limits_{j\in\mathcal{Z}} P_Z(j)V(Y|j)$, $Q_Y^* := \arg\min\limits_{Q_Y} D(P_Y||Q_Y)$, and (a) is true due to Lemma 6 in Appendix A, since $D(P_Y||P_{Y,i_0}) \leq \delta(\epsilon_0)$ because of (34).

Hence, we conclude that

$$\theta_I(0,\epsilon) = \max_{i\in\mathcal{X}}\min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}).$$

This completes the proof. ■

B. Authentication of Nonzero-Rate Messages

In this subsection, we deal with the case with $R_m > 0$, which is a much more complicated scenario compared to the single message case. We first provide an upper bound and a lower bound on the exponent of the successful attack probability. We then provide conditions under which the upper and the lower bounds match with each other.

Theorem 4. *Let* $P_Y = \sum_{i\in\mathcal{X}} P_X(i)W(Y|i)$ *and* $Q_Y = \sum_{j\in\mathcal{Z}} P_Z(j)V(Y|j)$*, we have*

$$\theta_I(R_m,\epsilon) \leq \min_{P_Z} \max_{P_X\in\mathcal{P}_R} D(P_Y||Q_Y), \tag{35}$$

$$\theta_I(R_m,\epsilon) \geq \max_{P_X\in\mathcal{P}_R} \min_{P_Z} D(P_Y||Q_Y), \tag{36}$$

in which

$$\mathcal{P}_R := \{P_X \in \mathcal{P}_X : I(X;Y) \geq R_m\}.$$

Proof:

This proof has two main parts: First, we will show that, $\min_{P_Z} \max_{P_X\in\mathcal{P}_R} D(P_Y||Q_Y)$ is an upper bound on the authentication exponent of any scheme; Second, we will construct a scheme to achieve an authentication exponent $\max_{P_X\in\mathcal{P}_R} \min_{P_Z} D(P_Y||Q_Y)$.

Upper-bounding the authentication exponent for any scheme by (35)**:** Consider an arbitrary triplet (ϕ,ψ,φ) that satisfy the conditions in (7) and (9). Suppose 2^{nR_m} sequences X^n are selected as the codewords by the encoder ϕ. Define the acceptance region determined by ψ as $\mathscr{A}_n$. As there are at most $(n+1)^{|\mathcal{X}|}$ different types of sequences X^n, there must exist at least $(n+1)^{-|\mathcal{X}|}2^{nR_m}$ codewords that have the same type. We denote this particular type as P_X and the set of these codewords as C_{P_X}.

For any arbitrary testing function ψ and decoding function φ, we define $A(X^n) \subset \mathcal{Y}^n$ as the set of sequences Y^n that are accepted and decoded to X^n with a probability larger than $\frac{1}{2}$. For each X^n, we must have $\Pr\{A(X^n)|X^n\} \geq 1-2\epsilon$, otherwise, the decoding error for X^n is larger than ϵ, which violates the condition (7). It is easy to see that

$$A(X^n) \cap A(\tilde{X}^n) = \emptyset,\ \forall\ X^n, \tilde{X}^n \in C_{P_X} : X^n \neq \tilde{X}^n. \tag{37}$$

In Appendix C, we show that we must have

$$R_m \leq I(X;Y), \tag{38}$$

in which the mutual information $I(X;Y)$ is computed from this particular P_X and $P_Y = \sum_{i\in\mathcal{X}} P_X(i)W(Y|i)$. Meanwhile, we also have

$$\mathscr{A}_n \supseteq \bigcup_{X^n\in C_{P_X}} A(X^n), \tag{39}$$

which follows from the fact that for any $Y^n \notin \mathscr{A}_n$, Y^n will be rejected by Bob, let alone be decoded to a codeword in C_{P_X}, and thus $Y^n \notin \bigcup_{X^n\in C_{P_X}} A(X^n)$.

Now suppose Eve initiates an impersonation attack by generating a sequence Z^n with each component generated i.i.d. according to some PMF P_Z, and define

$$Q_Y = \sum_{j\in\mathcal{Z}} P_Z(j)V(Y|j). \tag{40}$$

With this particular attack, the success probability is

$$\Pr\{\mathscr{A}_n|Z^n\} \overset{(a)}{\geq} \Pr\left\{ \bigcup_{X^n\in C_{P_X}} A(X^n)|Z^n \right\} \tag{41}$$

$$\overset{(b)}{=} \sum_{X^n\in C_{P_X}} \Pr\{A(X^n)|Z^n\}, \tag{42}$$

in which (a) follows from (39) and (b) is true due to (37).

On the other hand, according to the proof in Theorem 2 (in particular, the proof of (31)), we have, for each $X^n \in C_{P_X}$, that

$$\begin{aligned}\Pr\{A(X^n)|Z^n\} &\geq 2^{-n(\sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_{Y,i})+\varepsilon)}\\ &= 2^{-n(\sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y)+\varepsilon)},\end{aligned}$$

since $\Pr\{A(X^n)|X^n\} \geq 1-2\epsilon$. And the last step is true due to the fact that $\forall\ i \in \mathcal{X}$, $Q_{Y,i} = Q_Y$ is fixed under this attack ($P_{Y,i}$ and $Q_{Y,i}$ are defined in (22) and (23)). Thus, we have

$$\begin{aligned}\Pr\{\mathscr{A}_n|Z^n\} &\geq \sum_{x^n\in C_{P_X}} 2^{-n(\sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y)+\varepsilon)}\\ &\geq (n+1)^{-|\mathcal{X}|}2^{nR_m}2^{-n(\sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y)+\varepsilon)}\\ &= (n+1)^{-|\mathcal{X}|}2^{-n(\sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y)-R_m+\varepsilon)}.\end{aligned}$$

Since $\Pr\{\mathscr{A}_n|Z^n\}$ is obtained by one specific attack strategy, it must be less than or equal to the successful attack probability of the optimal attack strategy, $\Pr\{\mathscr{A}_n|Z^{\star n}\}$. Thus, we have

$$\begin{aligned}&-\frac{1}{n}\log\Pr\{\mathscr{A}_n|Z^{\star n}\}\\ &\leq \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m + \varepsilon + \frac{|\mathcal{X}|}{n}\log(n+1)\\ &= \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m + \varepsilon',\end{aligned} \tag{43}$$

where $\varepsilon' := \varepsilon + \frac{|\mathcal{X}|}{n}\log(n+1)$. From (38) and (43), we see that for any given (ϕ,φ,ψ) (thus P_X is given), Eve can select an arbitrary distribution $P_Z \in \mathcal{P}_Z$ to initiate an impersonation attack as described above, and the corresponding exponent of the successful attack probability is upper bounded by the right-hand side of (43). Thus, the largest exponent of the successful attack probability (corresponding to the smallest successful attack probability) Alice and Bob can expect in the worst case when Eve selects the optimal distribution P_Z based on the given P_X, is given by $\min_{P_Z}\sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m$. Hence, we conclude that

$$\theta_I(R_m,\epsilon) \leq \max_{P_X\in\mathcal{P}_R} \min_{P_Z} \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m,$$

since ε' is an arbitrarily small number as $n \to \infty$. And we have

$$\begin{aligned}\theta_I(R_m,\epsilon) &\leq \max_{P_X\in\mathcal{P}_R} \min_{P_Z} \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m\\ &\overset{(a)}{=} \min_{P_Z} \max_{P_X\in\mathcal{P}_R} \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m.\end{aligned} \tag{44}$$

Here, (a) is proved in Appendix D.

Given any $P_Z \in \mathcal{P}_Z$ (thus, Q_Y is given), we first focus on the maximization sub-problem:

$$\max_{P_X \in \mathcal{P}_R} \sum_{i\in\mathcal{X}} P_X(i) D(P_{Y,i}||Q_Y) - R_m, \tag{45}$$

In Appendix E, we show that, for the optimization problem (45), an optimizer P_X^* with $I(X^*;Y) = R_m$ can always be found. On the other hand, we have

$$\begin{aligned}
&\sum_i P_X(i) D(P_{Y,i}||Q_Y) - R_m \\
&= \sum_i P_X(i) \sum_Y P_{Y,i} \log \frac{P_{Y,i}}{Q_Y} - R_m \\
&= \sum_i P_X(i) \sum_Y W(Y|i) \log \frac{W(Y|i)}{Q_Y} - R_m \\
&= \sum_{i,Y} P_X(i) W(Y|i) \log \frac{W(Y|i)}{Q_Y} \frac{P_Y}{P_Y} - R_m \\
&= \sum_{i,Y} P_X(i) W(Y|i) \log \frac{P_Y}{Q_Y} \\
&\qquad + \sum_{i,Y} P_X(i) W(Y|i) \log \frac{W(Y|i)}{P_Y} - R_m \\
&= \sum_Y P_Y \log \frac{P_Y}{Q_Y} \\
&\quad + \sum_{i,Y} P_X(i) W(Y|i) \log \frac{P_X(i) W(Y|i)}{P_X P_Y} - R_m \\
&= D(P_Y||Q_Y) + \sum_{i,Y} P_{XY} \log \frac{P_{XY}}{P_X \cdot P_Y} - R_m \\
&= D(P_Y||Q_Y) + I(X;Y) - R_m.
\end{aligned}$$

Thus, (44) is equivalent to

$$\begin{aligned}
\theta_I(R_m,\epsilon) &\le \min_{P_Z} \max_{P_X \in \mathcal{P}_R} \sum_{i\in\mathcal{X}} P_X(i) D(P_{Y,i}||Q_Y) - R_m \\
&\overset{(a)}{=} \min_{P_Z} \max_{P_X \in \partial\mathcal{P}_R} D(P_Y||Q_Y) \\
&\overset{(b)}{=} \min_{P_Z} \max_{P_X \in \mathcal{P}_R} D(P_Y||Q_Y),
\end{aligned} \tag{46}$$

in which $\partial\mathcal{P}_R := \{P_X : I(X;Y) = R_m\}$. Here step (a) is true because as discussed above, the optimizer P_X^* satisfies $I(X^*;Y) = R_m$. Step (b) is true, because for any given P_Z, $D(P_Y||Q_Y)$ is convex in P_Y while P_Y is an affine function of P_X, then $D(P_Y||Q_Y)$ is convex in P_X, thus the optimal solution of $\max\limits_{P_X \in \mathcal{P}_R} D(P_Y||Q_Y)$ is obtained on the boundary $\partial\mathcal{P}_R$ [26].

Construct a scheme to achieve (36)**:** In this part, for any given P_X (thus P_Y is fixed), we will construct a scheme such that the successful attack probability of any attack strategy is less than $2^{-n(\min\limits_{P_Z} D(P_Y||Q_Y) - \varepsilon)}$.

Codebook construction: Fix P_X, generate 2^{nR_m} sequences X^n as the codewords, i.i.d. according to the PMF P_X, with $R_m \le I(X;Y)$. And each codeword is assigned to one message. We use $X^n(M)$ to denote the M-th codeword.

Encoder ϕ: If Alice needs to send a message M to Bob, she transmits $X^n(M)$ into the channel.

Testing function ψ: Upon receiving a sequence Y^n, Bob first determines whether Y^n is from Alice or not. He declares it to be from Alice if Y^n is P_Y-typical, in which $P_Y = \sum\limits_{i\in\mathcal{X}} P_X(i) W(Y|i)$ for the given P_X; Otherwise, Bob declares that the message is from Eve, and abandons it. Hence, the acceptance region is $\mathscr{A} = T_\epsilon^n(Y)$. It is easy to show that for any given ϵ, there exists an r such that

$$\mathscr{A} \subseteq S_r^n(P_Y). \tag{47}$$

Furthermore, r goes to zero as ϵ decreases.

Decoder φ: If Y^n is tested to be from Alice, Bob tries to find a unique sequence $X^n(\hat{M})$ from the codebook such that $(X^n(\hat{M}), y^n)$ are jointly typical according to $W(Y|X)P_X$. If there are more than one such sequences X^n, he randomly picks one and declares it as the transmitted message; If there is no such sequence, he declares an error.

Error analysis: Since the acceptance region is $\mathscr{A} = T_\epsilon^n(Y)$, and all Y^n sequences that are jointly typical with X^n are included in $\mathscr{A}$, thus, we can easily show that

$$\begin{aligned}
&\Pr\{\hat{M} \ne M, H_0|H_0\} \le \frac{\epsilon}{2}, \\
&\Pr\{H_1|H_0\} \le \frac{\epsilon}{2}.
\end{aligned}$$

Using similar argument as that of the proof of Theorem 7.7.1 [24], we can obtain that there exists at least one codebook such that (7) is satisfied.

Authentication exponent analysis: First, for any attack sequence Z^n with type P_Z chosen by Eve, we have

$$\Pr\{\mathscr{A}|Z^n\} \le \Pr\{S_r^n(P_Y)|Z^n\},$$

which is true due to (47). Furthermore, according to Lemma 2 we have

$$\begin{aligned}
\Pr\{S_r^n(P_Y)|Z^n\} &\le (n+1)^{|\mathcal{Y}|+|\mathcal{Z}|} 2^{-n(D(P_Y||Q_Y)-\delta(r))} \\
&\le (n+1)^{|\mathcal{Y}|+|\mathcal{Z}|} 2^{-n(\min\limits_{P_Z} D(P_Y||Q_Y)-\delta(r))}.
\end{aligned}$$

Thus, we have

$$\Pr\{\mathscr{A}|Z^n\} \le (n+1)^{|\mathcal{Y}|+|\mathcal{Z}|} 2^{-n(\min\limits_{P_Z} D(P_Y||Q_Y)-\delta(r))},$$

which indicates that

$$\begin{aligned}
-\frac{1}{n} \log \Pr\{\mathscr{A}|Z^n\} \ge \min_{P_Z} &D(P_Y||Q_Y) - \delta(r) \\
&- \frac{|\mathcal{Y}| + |\mathcal{Z}|}{n} \log(n+1).
\end{aligned}$$

Finally, we conclude that

$$\theta_I(R_m,\epsilon) \ge \max_{P_X \in \mathcal{P}_R} \min_{P_Z} D(P_Y||Q_Y), \tag{48}$$

and this completes the proof. ■

In general, (35) and (36) do not match with each other. However, there do exist scenarios where these two bounds match and hence the authentication exponent is fully characterized for these scenarios.

Corollary 1. *Let* $f(P_X) := \min_{P_Z} D(P_Y||Q_Y)$*, if* $f(P_X) + I(X;Y)$ *is convex with respect to* $P_X \in \mathcal{P}_R$*, then* (35) *and* (36) *match.*

Proof. First, from (44) and (46), we know that the upper bound (35) can be equivalently written as

$$\theta_I(R_m, \epsilon) \leq \max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X;Y) - R_m] \tag{49}$$

In the following, we will show that if $f(P_X) + I(X;Y)$ is convex with respect to $P_X \in \mathcal{P}_R$, then the lower bound in (36) can be equivalently written as

$$\theta_I(R_m, \epsilon) \geq \max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X;Y) - R_m], \tag{50}$$

which implies that the upper bound (35) matches with the lower bound (36).

Hence, to show this corollary, we only need to show (50). Towards that end, let

$$\begin{aligned} \hat{P}_X &= \arg\max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X;Y) - R_m], \\ \tilde{P}_X &= \arg\max_{P_X \in \mathcal{P}_R} f(P_X). \end{aligned} \tag{51}$$

Since $D(P_Y||Q_Y)$ is convex in (P_Y, Q_Y), and (P_Y, Q_Y) are affine functions of (P_X, P_Z), then $D(P_Y||Q_Y)$ is convex in (P_X, P_Z). Thus, according to [25], $f(P_X)$ is convex in P_X. Since $I(X;Y)$ is concave in P_X, then depending on $W(Y|X)$ and $V(Y|Z)$, the summation $f(P_X)+I(X;Y)$ can be convex, concave or neither. For the case when $f(P_X) + I(X;Y)$ is convex in $P_X \in \mathcal{P}_R$, then the optimal value of $\max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X;Y) - R_m]$ is obtained on the boundary [26], that is $I(\hat{X};Y) = R_m$. Thus, we have

$$\begin{aligned} f(\hat{P}_X) &= f(\hat{P}_X) + I(\hat{X};Y) - R_m \\ &= \max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X;Y) - R_m] \\ &\geq \max_{P_X \in \mathcal{P}_R} f(P_X) \\ &= f(\tilde{P}_X). \end{aligned}$$

On the other hand, according to the definition of $\tilde{P}_X$ as in (51), we have

$$f(\hat{P}_X) \leq \max_{P_X \in \mathcal{P}_R} f(P_X) = f(\tilde{P}_X).$$

Hence, it follows that

$$f(\hat{P}_X) = f(\tilde{P}_X).$$

Finally, if $f(P_X) + I(X;Y)$ is convex in $P_X \in \mathcal{P}_R$, the optimal value of the optimization problem (50) is same as

$$\max_{P_X \in \mathcal{P}_R} f(P_X),$$

which is (36). This finishes the proof. □

In the following, we provide an example for which the upper bound and lower bound match.

Example 1: Let

$$W(Y|X) = \begin{bmatrix} 1/3 & 1/4 \\ 2/3 & 3/4 \end{bmatrix}, V(Y|Z) = \begin{bmatrix} 2/5 & 2/3 \\ 3/5 & 1/3 \end{bmatrix},$$

and set $P_X = [\lambda_1, 1 - \lambda_1]^T,\ P_Z = [\lambda_2, 1 - \lambda_2]^T,\ \lambda_1, \lambda_2 \in [0:1]$. Then, we have

$$\begin{aligned} P_Y &= W(Y|X)P_X = \left[\frac{1}{4} + \frac{1}{12}\lambda_1, \frac{3}{4} - \frac{1}{12}\lambda_1\right]^T, \\ Q_Y &= V(Y|Z)P_Z = \left[\frac{2}{3} - \frac{4}{15}\lambda_2, \frac{1}{3} + \frac{4}{15}\lambda_2\right]^T. \end{aligned}$$

Define $\lambda_0 = \frac{1}{4} + \frac{1}{12}\lambda_1$, then

$$D(P_Y||Q_Y) = \lambda_0 \log \frac{\lambda_0}{\frac{2}{3} - \frac{4}{15}\lambda_2} + (1 - \lambda_0) \log \frac{1 - \lambda_0}{\frac{1}{3} + \frac{4}{15}\lambda_2}.$$

Following some simple calculations, we have

$$\begin{aligned} &\frac{\partial D(P_Y||Q_Y)}{\partial \lambda_2} \\ &= \frac{4}{15(\frac{2}{3} - \frac{4}{15}\lambda_2)\left(\frac{1}{3} + \frac{4}{15}\lambda_2\right)\ln 2} \left(\frac{4}{15}\lambda_2 + \lambda_0 - \frac{2}{3}\right). \end{aligned}$$

Since $\lambda_0 \in [\frac{1}{4} : \frac{1}{3}]$, we have

$$\frac{\partial D(P_Y||Q_Y)}{\partial \lambda_2} < 0,\ \forall \lambda_0 \in \left[\frac{1}{4} : \frac{1}{3}\right], \lambda_2 \in [0:1].$$

Thus, for any given P_Y, $D(P_Y||Q_Y)$ is a decreasing function of λ_2. Hence,

$$\lambda_2^* = \arg\min_{\lambda_2} D(P_Y||Q_Y) = 1,\ \forall \lambda_0 \in \left[\frac{1}{4} : \frac{1}{3}\right],$$

which is equivalent to

$$Q_Y^* = \arg\min_{Q_Y} D(P_Y||Q_Y) = \left[\frac{2}{5}, \frac{3}{5}\right]^T,\ \forall P_X \in \mathcal{P}_X. \tag{52}$$

Hence,

$$\begin{aligned} &f(P_X) + I(X;Y) \\ &= D(P_Y||Q_Y^*) + I(X;Y) \\ &= \sum_y P_Y \log \frac{P_Y}{Q_Y^*} + H(Y) - H(Y|X) \\ &= \sum_y P_Y \log \frac{P_Y}{Q_Y^*} - \sum_y P_Y \log P_Y - \sum_{i \in \mathcal{X}} P_X(i) H(Y|i) \\ &= \sum_y P_Y \log \frac{1}{Q_Y^*} - \sum_{i \in \mathcal{X}} P_X(i) H(Y|i). \end{aligned}$$

As $H(Y|X = i)$ are constants for either $i = 1$ or $i = 2$ and P_Y is an affine function of P_X, from the equation above, we have that $f(P_X) + I(X;Y)$ is linear (and hence convex) in P_X. Hence, for this example, we can conclude that

$$\max_{P_X \in \mathcal{P}_R} \min_{P_Z} D(P_Y||Q_Y) = \min_{P_Z} \max_{P_X \in \mathcal{P}_R} D(P_Y||Q_Y),$$

and hence the authentication exponent is fully characterized.

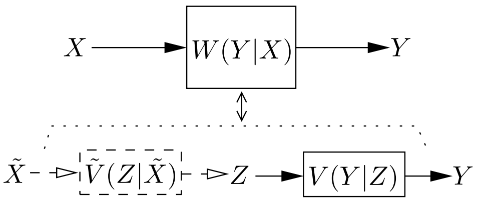


Fig. 3. Construct a virtual channel $\tilde{X} \to Y$ that has the same statistics as $X \to Y$

V. Authenticated (Secrecy) Capacity

In this section, we focus on characterizing the authenticated capacity C^* and the authenticated secrecy capacity C_S^*, defined in Section II-B.

A. Simulatability Condition and Authenticated (Secrecy) Capacity

We first introduce a concept named *simulatability condition* that plays an important role in our study. The simulatability condition was first defined under the source model in [9] for the study of key generation under unauthenticated public channel problems. Here, we extend the definition to the channel model. We note that [15] also introduced a similar concept for the channel model. We will show that our definition will lead to the definition given in [15].

Definition 3. *For given channels $W(Y|X)$ (the channel connecting Alice and Bob) and $V(Y|Z)$ (the channel connecting Eve and Bob), if for each $P_X \in \mathcal{P}_\mathcal{X}$, there exists some $P_Z \in \mathcal{P}_Z$ such that*

$$\sum_{j\in\mathcal{Z}} V(Y|j)\cdot P_Z(j) = \sum_{i\in\mathcal{X}} W(Y|i)\cdot P_X(i), \tag{53}$$

then, we say that the (channel) simulatability condition holds.

Remark 4. *The simulatability condition here means that no matter what P_X Alice uses, Eve can always find a P_Z, such that the received sequences Y^n at Bob from both channels have the same distribution.*

We have the following lemmas regarding the simulatability condition.

Lemma 3. *Given channels $W(Y|X)$ and $V(Y|Z)$, if the simulatability condition holds, then Eve can construct a virtual channel $\tilde{V}(Z|\tilde{X})$, such that*

$$V(Y|Z)\tilde{V}(Z|\tilde{X}) = W(Y|X). \tag{54}$$

Proof. The proof is given in Appendix F. □

As shown in Fig. 3, Lemma 3 means that if the simulatability condition holds, by concatenating $\tilde{V}(Z|\tilde{X})$ to $V(Y|Z)$, Eve can construct a channel from $\tilde{X}$ to Y that has the same statistics as the legitimate channel from X to Y. The definition of simulatability condition in [15] has the same interpretation as shown in Fig. 3.

Using Lemma 3, we can greatly simplify the simulatability condition as shown in the following lemma.

Lemma 4. *Given $W(Y|X)$ and $V(Y|Z)$, the simulatability condition holds if and only if $\forall i \in \mathcal{X}$, $\exists P_{Z,i} \in \mathcal{P}_Z$, s.t.*

$$V(Y|Z)P_{Z,i} = W(Y|i). \tag{55}$$

Proof. The proof is given in Appendix F. □

This lemma plays a key role in the proof of our main result on the authenticated capacity. It also facilitates us in the design of efficient algorithms for checking whether the simulatability condition holds or not for any given $W(Y|X)$ and $V(Y|Z)$. The design of efficient algorithms will be discussed in Section V-B.

Now, we state our result on C^* as follows.

Theorem 5. *Under the channel model when Eve is active, if the simulatability condition holds, $C^* = 0$; Otherwise, $C^* = C$.*

Suppose $P_X^\star = \arg\max_{P_X} I(X;Y)$ (the corresponding $P_Y := P_Y^\star$), then $C = I(X^\star;Y)$. If the simulatability condition does not hold and $\min_{P_Z} D(P_Y^\star||Q_Y) > 0$, the result $C^* = C = I(X^\star;Y)$ is obvious, as we can fix $P_X = P_X^\star$ and use the same scheme as that in the achievability in Section IV-B. Using this scheme, the successful attack probability is upper bounded as

$$\beta_n(Z_0^n) \le 2^{-n(\min_{P_Z} D(P_Y^\star||Q_Y)-\varepsilon)} \le \epsilon.$$

However, if the simulatability condition does not hold but $\min_{P_Z} D(P_Y^\star||Q_Y) = 0$, the above scheme does not work. In the following, we present a scheme such that, as long as the simulatability condition doesn't hold, we can guarantee that Alice can reliably transmit a message to Bob at a rate larger than $C-\epsilon$, meanwhile Bob can detect the attack by Eve with a probability larger than $1-\sigma$.

Proof of Theorem 5: The case when the simulatability condition holds is trivial: As shown in Lemma 3, if the simulatability condition holds, Eve can concatenate a virtual channel $\tilde{V}(Z|\tilde{X})$ to the channel $V(Y|Z)$ such that the concatenated channel from $\tilde{X}$ to Y has the same statistics as the legitimate channel from X to Y. Now, for any legitimate users' strategy ϕ, ψ, φ that satisfy (7), Eve can always generate the same codebook as Alice's codebook. When Eve conducts an impersonation attack, she only needs to randomly pick a codeword from the codebook and send it through the concatenated channel from $\tilde{X}$ to Y. Since this concatenated channel has the same statistics as that of the channel from X to Y, the successful attack probability equals the probability of that a message sent by Alice is accepted by Bob. As the latter probability is larger than $1-\epsilon$ due to (7), the successful attack probability will be larger than $1-\epsilon$. Thus, we have

$$C^* = 0.$$

For the case when the simulatability condition does not hold, we show that there exists a scheme such that Alice can reliably transmit the message to Bob at a rate larger than $C-\epsilon$ when Eve does not attack, meanwhile Bob can detect the attack by Eve with a probability larger than $1-\sigma$.

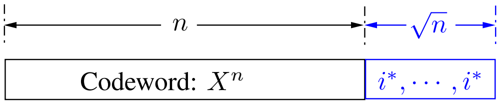


Fig. 4. Codeword $\hat{X}^{n+\sqrt{n}}$

According to Lemma 4, if the simulatability condition does not hold, then there exists $i^* \in \mathcal{X}$ s.t.

$$V(Y|Z)P_{Z,i^*} \neq W(Y|i^*),\ \forall P_{Z,i^*} \in \mathcal{P}_Z. \tag{56}$$

To show that $C^* = C$, it suffices to show that for any $P_X \in \mathcal{P}_X$, $R = I(X;Y) - \epsilon$ is achievable.

Codebook generation: Fix P_X, i.i.d generate 2^{nR_m} sequences X^n according to the PMF P_X with $R_m = I(X;Y) - \epsilon_0$. We then construct a sequence $i^{*\sqrt{n}}$, that is to repeat i^* for $\sqrt{n}$ times and append $i^{*\sqrt{n}}$ to each generated X^n. We denote the new $n + \sqrt{n}$ length sequence as $\hat{X}^{n+\sqrt{n}}$. As will be clear in the sequel, $i^{*\sqrt{n}}$ will be used as an authenticator. We then set the sequences $\hat{X}^{n+\sqrt{n}}$ as the codewords, and each $\hat{X}^{n+\sqrt{n}}$ is assigned to one message. We use $\hat{X}^{n+\sqrt{n}}(M)$ to denote the M-th codeword. Fig. 4 illustrates the codeword $\hat{X}^{n+\sqrt{n}}$.

Encoding: If Alice needs to send a message M to Bob, she transmits $\hat{X}^{n+\sqrt{n}}(M)$ into the channel.

Authentication: Upon receiving a sequence $Y^{n+\sqrt{n}}$, Bob first splits it into two parts: Y^n and $Y_{n+1}^{n+\sqrt{n}}$. Then he declares the signal to be from Alice if $Y_{n+1}^{n+\sqrt{n}}$ is P_{Y,i^*}-typical; Otherwise, he declares it to be from Eve and rejects it.

Decoding: If $Y^{n+\sqrt{n}}$ is authenticated to be from Alice, Bob tries to find a unique sequence $X^n(\hat{M})$ such that $(X^n(\hat{M}), Y^n)$ are jointly typical, and decodes the signal to $\hat{M}$. If there are more than one such sequence, he randomly picks one. If there is no such sequence, he declares an error.

Error analysis: Since the acceptance region is $\mathscr{A} = \mathcal{Y}^n \times T_\epsilon^{\sqrt{n}}(Y, i^*)$, and all X^n-jointly typical sequence Y^n is included in $\mathscr{A}$, thus we can easily obtain

$$\Pr\{\hat{M} \neq M, H_0 | H_0\} \leq \frac{\epsilon}{2},$$
$$\Pr\{H_1 | H_0\} \leq \frac{\epsilon}{2}.$$

Using the same argument as that in the proof of Theorem 7.7.1 in [24], we obtain that there exists at least one codebook such that (7) is satisfied.

Probability of successful attack: As discussed in Section III and (20) in particular, we only need to consider the impersonation attack. For this, we only need to focus on $Y_{n+1}^{n+\sqrt{n}}$. Since $Y_{n+1}^{n+\sqrt{n}}$ is i.i.d generated according to $P_{Y,i^*} = W(Y|i^*)$ when there is no attack, we have, based on Lemma 2, that

$$P_I \leq 2^{-\sqrt{n}(D(P_{Y,i^*}||Q_{Y,i^*}) - \delta(\epsilon_0))} \leq \sigma,$$

when n is sufficiently large.

Rate Per Channel Use:

$$\begin{aligned}
R = \frac{nR_m}{n+\sqrt{n}} &= \frac{n}{n+\sqrt{n}}(I(X;Y) - \epsilon_0) \\
&= I(X;Y) - \frac{\sqrt{n}}{n+\sqrt{n}} I(X;Y) - \frac{n}{n+\sqrt{n}}\epsilon_0 \\
&\geq I(X;Y) - \epsilon,
\end{aligned}$$

when n is large enough. ■

Using the same idea of appending an $\sqrt{n}$ length sequence as the authentication sequence, we can easily obtain the following result regarding the authenticated secrecy capacity.

Corollary 2. *Under the channel model when Eve is active, if the simulatability condition holds, $C_S^* = 0$; Otherwise, $C_S^* = C_S$.*

Proof. The proof follows similar steps as that of Theorem 5 and is omitted for brevity. □

Remark 5. *For the case when the simulatability condition holds, if Alice and Bob pre-share a secret key (even with a negligible rate), the authenticated (secrecy) capacity may not necessarily be zero, as Alice and Bob can utilize the pre-shared key to perform authentication such that the successful attack probability is upper bounded by σ. In this case, the channel $U(F|X)$ has effect on determining how much information Eve can learn about this secret key, and Eve can use this information to carry out the substitution attack. As our analysis relies on the assumption that the legitimate users do not have pre-share keys, the exact characterization of the authenticated (secrecy) capacity for the scenario with pre-share keys requires new analysis, which is left for further investigation.*

Note that the role of the simulatability condition in our setup is similar as that of the symmetrizability condition for an arbitrarily varying channel (AVC) as defined in [27]. For an AVC, the state of the channel can be viewed as being controlled by an adversary. If the AVC is symmetrizable, there exists a state sequence which the adversary can use, such that the decoder cannot distinguish the true codeword from a false codeword no matter what scheme is applied. On the other hand, if the AVC is not symmetrizable, there exists a scheme such that no matter what state the channel is, the decoder can correctly decode the codeword of positive rate with high probability. In this respect, the simulatability condition is weaker than the symmetrizability condition since the simulatability condition only involves in two separate channels and the channel from the encoder to the decoder remains the same while for the AVC, the channel statistics from the encoder to the decoder is determined by the state sequence and it can be arbitrarily changed.

B. Algorithm

As shown above, the simulatability condition plays an important role in our analysis. Hence, it is crucial to design efficient algorithms to check whether the simulatability condition holds or not for any given $W(Y|X)$ and $V(Y|Z)$. From Lemma 4, we know that to check the simulatability condition, we only need to check, for each $i \in \mathcal{X}$, whether there exists some $P_{Z,i} \in \mathcal{P}_Z$ such that (55) holds.

It is easy to see that if there exists a $P_{Z,i} \in \mathcal{P}_Z$ such that (55) holds, then the optimal value of the following optimization problem will be 0:

$$\begin{aligned} \min_{P_{Z,i}} \quad & ||V(Y|Z)P_{Z,i} - W(Y|i)||_1 \\ \text{s.t.} \quad & P_{Z,i} \succeq 0, \\ & \sum_{j \in \mathcal{Z}} P_{Z,i}(j) = 1, \end{aligned} \tag{57}$$

in which $|| \cdot ||_1$ is the ℓ_1 norm. At the same time, if the optimal value obtained from the optimization problem (57) is 0, the corresponding optimizer will satisfy (55). Hence, we conclude that (55) holds if and only if the optimal value obtained from (57) is 0. It is easy to check that (57) is a convex optimization problem, and hence can be solved efficiently. In fact, following similar steps as those in our recent work [28], the optimization problem (57) can be further simplified to be a linear programming problem. Details of those steps are omitted, as they are very similar to those in [28].

Finally, using Lemma 4, we know that we only need to solve $|\mathcal{X}|$ convex optimization problems as (57) to check the simulatability condition (53).

C. Channel Uncertainty

It is important to note that, although our model involves Eve's channels $U(F|X)$ and $V(Y|Z)$, most of our schemes (with one exception to be discussed below) in both Section IV and Section V are universal with respect to Eve's channels, in the sense that our schemes do not rely on the information on Eve's channels. However, in order to check the simulatability condition, we need to know the exact channel state information of $V(Y|Z)$, which is impractical. Nonetheless, we show that the simulatability condition here is not sensitive to modeling uncertainties, that is $V(Y|Z)$ does not need to be known perfectly.

Assume $W(Y|X)$ is perfectly known but $V(Y|Z)$ is known only to a certain precision. In particular, let the true channel between Eve and Bob to be $\hat{V}(Y|Z)$, but the legitimate users know only an estimate $V(Y|Z)$. Denote $\Delta V(Y|Z) = \hat{V}(Y|Z) - V(Y|Z)$, we assume $|\Delta V(Y|Z)|$ is bounded. In particular, we assume

$$|\Delta V(j|k)| \leq \delta, \ \forall j \in [1:|\mathcal{Y}|], k \in [1:|\mathcal{Z}|].$$

We clearly have

$$\sum_{j=1}^{|\mathcal{Y}|} \Delta V(j|k) = 0, \ \forall k \in [1:|\mathcal{Z}|].$$

Suppose that based on $V(Y|Z)$, Alice and Bob determine that $W(Y|X)$ is not simulatable, i.e., there exists a i^* such that $W(Y|i^*)$ satisfies

$$V(Y|Z)P_{Z,i^*} \neq W(Y|i^*), \ \forall P_{Z,i^*} \in \mathcal{P}_Z. \tag{58}$$

As discussed in the proof of Theorem 5, Alice and Bob will use i^* to design the authenticator. This is the only part of our scheme that depends on Eve's channel. Let

$$\begin{aligned} \rho = \min_{P_{Z,i^*}} & ||V(Y|Z)P_{Z,i^*} - W(Y|i^*)||_1 \\ \text{s.t.} \quad & P_{Z,i^*} \succeq 0, \ \sum_{j \in \mathcal{Z}} P_{Z,i^*}(j) = 1. \end{aligned} \tag{59}$$

From (58), we know $\rho > 0$.

We have the following result.

Lemma 5. *Suppose Eve can't simulate $W(Y|i^*)$ with regards to $V(Y|Z)$, then $\forall \delta < \frac{\rho}{|\mathcal{Y}|}$, Eve cannot simulate $W(Y|i^*)$ using $\hat{V}(Y|Z)$ neither.*

Proof. The proof is shown in Appendix F. □

This result means that, although Alice and Bob only have an estimate of Eve's channel $V(Y|Z)$, the authenticator $i^{*,\sqrt{n}}$ designed based on the estimated channel still works for the true channel $\hat{V}(Y|Z)$ as long as the difference between these two channels measured by δ is less than $\rho/|\mathcal{Y}|$. Hence, our scheme is robust to the uncertainty in Eve's channel.

Here, we provide an example to illustrate this result.

Example 2: Let

$$V(Y|Z) = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}, W(Y|i^*) = \begin{bmatrix} 2/3 \\ 1/3 \end{bmatrix}.$$

Then, we have

$$\begin{aligned} \rho \quad &:= \quad \min_{P_{Z,i^*}} ||V(Y|Z)P_{Z,i^*} - W(Y|i^*)||_1 \\ &= \quad \min_{P_{Z,i^*}} \left|\left| \begin{bmatrix} \frac{1}{2} - \frac{2}{3} \\ \\ \frac{1}{2} - \frac{1}{3} \end{bmatrix} \right|\right|_1 = 1/3. \end{aligned}$$

Now if

$$\delta < \frac{\rho}{|\mathcal{Y}|} = \frac{1}{2}\rho = \frac{1}{6}, \tag{60}$$

set $\hat{V}(Y|Z) = \begin{bmatrix} 1/2 + \delta_1 & 1/2 + \delta_2 \\ 1/2 - \delta_1 & 1/2 - \delta_2 \end{bmatrix}$, $|\delta_1| \leq \delta, |\delta_2| \leq \delta$ and $P_{Z,i^*} = \begin{bmatrix} \lambda_1 \\ 1 - \lambda_1 \end{bmatrix}$, then we have

$$\hat{V}P_{Z,i^*} = \begin{bmatrix} 1/2 + \delta_1\lambda_1 + \delta_2(1-\lambda_1) \\ 1/2 - \delta_1\lambda_1 - \delta_2(1-\lambda_1) \end{bmatrix}.$$

Since the first entry $1/2 + \delta_1\lambda_1 + \delta_2(1-\lambda_1) < 1/2 + 1/6\lambda_1 + 1/6(1-\lambda_1) = 2/3$, we can conclude

$$\hat{V}P_{Z,i^*} \neq W(Y|i^*), \ \forall P_{Z,i^*} \in \mathcal{P}_Z.$$

Hence, Eve can't simulate $W(Y|i^*)$ for any perturbed channel $\hat{V}(Y|Z)$ with constraint (60).

VI. Conclusion

In this paper, we have considered the problem of message authentication without any pre-shared key, in the presence of an active adversary over noisy channels. We have characterized the authentication exponent for the zero-rate case and provided both an upper bound and a lower bound on the exponent for the nonzero-rate case. We have shown an "all or nothing" result for the authenticated channel capacity, depending on a so called simulatability condition. We have further provided efficient algorithms to check the simulatability condition. We have also shown that our schemes are robust to modeling uncertainties about Eve's channels.

Appendix A

Lemma 6. *Let P^*, P and Q be three distributions on random variable X, and $r \geq 0$, then if $D(P^*||P) \leq r$ and $0 < D(P||Q) < \infty$, then*

$$\begin{aligned} D(P^*||Q) &\geq D(P||Q) - \delta(r), \\ D(P^*||Q) &\leq D(P||Q) + \delta(r). \end{aligned}$$

in which $\delta(r) \downarrow 0$ as $r \downarrow 0$.

In order to prove Lemma 6, techniques from [24] are utilized.

Lemma 7. *1. (Pinsker's Inequality, [24, Lemma 11.6.1]) Let P and Q be any two distributions on X, then*

$$D(P||Q) \geq \frac{1}{2\ln 2}||P-Q||_1^2,$$

in which $||P-Q||_1 = \sum_{x\in\mathcal{X}} |P(x)-Q(x)|$.

2. ([24, Lemma 11.8.1]) Let B_n be any set of sequences X^n, such that $P^n(B_n) > 1-\epsilon$. Let Q be any other distribution such that $D(P||Q) < \infty$, then

$$Q^n(B_n) > (1-2\epsilon)2^{-n(D(P||Q)+\epsilon)}.$$

Proof of Lemma 6. If $Q(i) = 0$ for some $i \in \mathcal{X}$, then $P(i) = 0$ and $P^*(i) = 0$, since $D(P||Q) < \infty$ and $D(P^*||P) \leq r$. Thus, the existence of $\{i \in \mathcal{X} : Q(i) = 0\}$ has no influence on the final result. Hence, to facilitate the presentation, we assume that $Q(i) > 0, \forall i \in \mathcal{X}$.

Since $r \geq D(P^*||P) \geq \frac{1}{2\ln 2}||P^*-P||_1^2$, then we have

$$\sum_{i\in\mathcal{X}} |P^*(i) - P(i)| \leq \sqrt{2\ln 2 \cdot r},$$

which indicates

$$|P^*(i) - P(i)| \leq \sqrt{2\ln 2 \cdot r}, \forall i \in \mathcal{X}.$$

Define a set $A := \{i \in \mathcal{X} : P(i) > Q(i) + \sqrt{2\ln 2 \cdot r}\}$, and $\bar{A} := \mathcal{X}\backslash A$. Then we have

$$\begin{aligned}
D(P^*||Q) &= \sum_{i\in\mathcal{X}} P^*(i)\log\frac{P^*(i)}{Q(i)} \\
&= \sum_{i\in A} P^*(i)\log\frac{P^*(i)}{Q(i)} + \sum_{i\in\bar{A}} P^*(i)\log\frac{P^*(i)}{Q(i)} \\
&\overset{(a)}{\geq} \sum_{i\in A}(P(i)-\sqrt{2r\ln 2})\log\frac{P(i)-\sqrt{2r\ln 2}}{Q(i)} \qquad (61) \\
&\qquad + \sum_{i\in\bar{A}}(P(i)+\sqrt{2r\ln 2})\log\frac{P(i)-\sqrt{2r\ln 2}}{Q(i)} \\
&= \sum_{i\in\mathcal{X}} P(i)\log\frac{P(i)-\sqrt{2r\ln 2}}{Q(i)} - \sqrt{2r\ln 2}\,\cdot \\
&\left(\sum_{i\in A}\log\frac{P(i)-\sqrt{2r\ln 2}}{Q(i)} - \sum_{i\in\bar{A}}\log\frac{P(i)-\sqrt{2r\ln 2}}{Q(i)}\right) \qquad (62) \\
&= \sum_{i\in\mathcal{X}} P(i)\log\frac{P(i)-\sqrt{2r\ln 2}}{Q(i)} - \delta'(r) \qquad (63) \\
&= \sum_{i\in\mathcal{X}} P(i)\log\frac{P(i)}{Q(i)} + \sum_{i\in\mathcal{X}} P(i)\log\frac{P(i)-\sqrt{2r\ln 2}}{P(i)} - \delta'(r) \\
&\overset{(b)}{\geq} D(P||Q) - \sum_{i\in\mathcal{X}} P(i)\frac{2\sqrt{2r\ln 2}}{P(i)\ln 2} - \delta'(r) \\
&= D(P||Q) - \delta_1(r),
\end{aligned}$$

in which step (a) follows from the facts that $\log(\cdot)$ is an increasing function of its argument, and that

$$\begin{aligned} \log\frac{P(i)-\sqrt{2r\ln 2}}{Q(i)} &> 0, \ \forall i \in A; \\ \log\frac{P(i)-\sqrt{2r\ln 2}}{Q(i)} &\leq 0, \ \forall i \in \bar{A}. \end{aligned}$$

In addition, step (b) is true due to the fact that $\ln(1-\gamma) \geq -2\gamma$ when γ $(\gamma \geq 0)$ is small enough. Then, we only need to show $\delta_1(r)$ vanishes as $r \to 0$, which is equivalent to show $\delta'(r) \downarrow 0$ as $r \downarrow 0$. From (62) to (63), $\delta'(r) := \varepsilon \cdot (\sum_{i\in A}\log\frac{P(i)-\varepsilon}{Q(i)} - \sum_{i\in\bar{A}}\log\frac{P(i)-\varepsilon}{Q(i)})$ by setting $\varepsilon = \sqrt{2r\ln 2}$. Since the sizes of sets A and $\bar{A}$ are finite, we only need to show $\log\frac{P(i)-\varepsilon}{Q(i)}$ is finite when ε is small enough. And that $\forall i \in \mathcal{X}, \log\frac{P(i)-\varepsilon}{Q(i)}$ is finite is obvious, because of the assumption that $P(i) > 0, Q(i) > 0$.

Following similar steps as above, we can also show that

$$D(P^*||Q) \leq D(P||Q) + \delta_2(r).$$

Finally, by setting $\delta(r) = \max\{\delta_1(r), \delta_2(r)\}$, we complete the proof. □

Appendix B
Proof of Lemma 2

According to the construction of $S_r^k(P_Y)$, all sequences Z^k with $\text{tp}(Z^k) = P_Z$ have the same success probability as that of Z_0^k:

$$\Pr\{S_r^k(P_Y)|Z^k\} = \Pr\{S_r^k(P_Y)|Z_0^k\},\ \forall Z^k : \text{tp}(Z^k) = P_Z. \quad (64)$$

Thus, we have

$$\begin{aligned}\Pr\{S_r^k(P_Y)|Z_0^k\} &= \sum_{Y^k \in S_r^k(P_Y)} \Pr\{Y^k|Z_0^k\}. \\ &= \sum_{Z^k \in \mathcal{T}_Z^k(P_Z)} \Pr\{Z^k|P_Z\} \sum_{Y^k \in S_r^k(P_Y)} \Pr\{Y^k|Z_0^k\} \\ &\overset{(a)}{=} \sum_{Z^k \in \mathcal{T}_Z^k(P_Z)} \Pr\{Z^k|P_Z\} \sum_{Y^k \in S_r^k(P_Y)} \Pr\{Y^k|Z^k\}, \quad (65)\end{aligned}$$

where $\Pr\{Z^k|P_Z\}$ can be any arbitrary conditional probability distribution of Z^k given $\text{tp}(Z^k) = P_Z$, and (a) holds due to (64).

To further analyze $\Pr\{S_r^k(P_Y)|Z_0^k\}$, we first investigate the relationship between $\Pr\{S_r^k(P_Y)|Z_0^k\}$ and $Q_Y^k(S_r^k(P_Y))$.

$$\begin{aligned}Q_Y^k(S_r^k(P_Y)) &= \sum_{Z^k \in \mathcal{Z}^k} P_Z^k(Z^k) \cdot \Pr\{S_r^k(P_Y)|Z^k\} \\ &= \sum_{Z^k \in \mathcal{Z}^k} P_Z^k(Z^k) \sum_{Y^k \in S_r^k(P_Y)} \Pr\{Y^k|Z^k\} \\ &= \sum_{\tilde{P}_Z \in \mathcal{T}_Z} \sum_{Z^k \in \mathcal{T}_Z^k(\tilde{P}_Z)} P_Z^k(Z^k|\tilde{P}_Z) P_Z^k(\mathcal{T}_Z^k(\tilde{P}_Z)) \\ &\qquad \cdot \sum_{Y^k \in S_r^k(P_Y)} \Pr\{Y^k|Z^k\} \\ &= \sum_{\tilde{P}_Z \in \mathcal{T}_Z} P_Z^k(\mathcal{T}_Z^k(\tilde{P}_Z)) \sum_{Z^k \in \mathcal{T}_Z^k(\tilde{P}_Z)} P_Z^k(Z^k|\tilde{P}_Z) \\ &\qquad \cdot \sum_{Y^k \in S_r^k(P_Y)} \Pr\{Y^k|Z^k\} \\ &\geq P_Z^k(\mathcal{T}_Z^k(P_Z)) \sum_{Z^k \in \mathcal{T}_Z^k(P_Z)} P_Z^k(Z^k|P_Z) \\ &\qquad \cdot \sum_{Y^k \in S_r^k(P_Y)} \Pr\{Y^k|Z^k\}. \\ &\overset{(a)}{=} P_Z^k(\mathcal{T}_Z^k(P_Z)) \cdot \Pr\{S_r^k(P_Y)|Z_0^k\}, \quad (66)\end{aligned}$$

where (a) is true because of (65). On the other hand, according to [24, Theorem 11.1.4], we have

$$\begin{aligned}P_Z^k(\mathcal{T}_Z^k(P_Z)) &\geq \frac{1}{(k+1)^{|\mathcal{Z}|}} \cdot 2^{-kD(P_Z||P_Z)} \\ &= \frac{1}{(k+1)^{|\mathcal{Z}|}}.\end{aligned}$$

Thus, we conclude that

$$\Pr\{S_r^k(P_Y)|Z_0^k\} \leq (k+1)^{|\mathcal{Z}|} Q_Y^k(S_r^k(P_Y)). \quad (67)$$

In the following, we bound $Q_Y^k(S_r^k(P_Y))$ from above. First, it follows

$$Q_Y^k(S_r^k(P_Y)) = \sum_{\text{tp}(Y^k):\mathcal{T}_Y^k(\text{tp}(Y^k)) \subseteq S_r^k(P_Y)} Q_Y^k(\text{tp}(Y^k)), \quad (68)$$

and by Lemma 6 in Appendix A, $\forall$ $\text{tp}(Y^k) : \mathcal{T}_Y^k(\text{tp}(Y^k)) \subseteq S_r^k(P_Y)$, we have

$$D(\text{tp}(Y^k)||Q_Y) \geq D(P_Y||Q_Y) - \delta(r), \quad (69)$$

with $\delta(r)$ goes to zero as r decreases. Thus,

$$\begin{aligned}Q_Y^k(\text{tp}(Y^k)) &\leq 2^{-kD(\text{tp}(Y^k)||Q_Y)} \\ &\leq 2^{-k(D(P_Y||Q_Y) - \delta(r))}. \quad (70)\end{aligned}$$

Combine (70) and (68), and we have

$$\begin{aligned}Q_Y^k(S_r^k(P_Y)) &\leq \sum_{\text{tp}(Y^k):\mathcal{T}_Y^k(\text{tp}(Y^k)) \in S_r^k(P_Y)} 2^{-k(D(P_Y||Q_Y) - \delta(r))} \\ &\leq (k+1)^{|\mathcal{Y}|} 2^{-k(D(P_Y||Q_Y) - \delta(r))}. \quad (71)\end{aligned}$$

Combining (71) and (67), we obtain

$$\Pr\{S_r^k(P_Y)|Z_0^k\} \leq (k+1)^{|\mathcal{Y}|+|\mathcal{Z}|} 2^{-k(D(P_Y||Q_Y) - \delta(r))}. \quad (72)$$

Appendix C
Proof of (38)

Proof. Given X^n, denote the conditionally ϵ-typical set of sequences Y^n by $T_\epsilon(Y^n|X^n)$ (the concept of ϵ-typicality and its property can be found in [29, Chapter 2]), and we have

$$\Pr\{T_\epsilon(Y^n|X^n)|X^n\} \geq 1 - \epsilon.$$

Thus,

$$\Pr\{A(X^n) \cap T_\epsilon(Y^n|X^n)|X^n\} \geq 1 - 3\epsilon.$$

In addition, for each $Y^n \in T_\epsilon(Y^n|X^n)$, we have

$$2^{-n(H(Y|X)+\epsilon)} \leq \Pr\{Y^n|X^n\} \leq 2^{-n(H(Y|X)-\epsilon)}.$$

Thus, we have

$$|A(X^n) \cap T_\epsilon(Y^n|X^n)| \geq (1 - 3\epsilon) 2^{n(H(Y|X)-2\epsilon)}.$$

Since for each $X^n \in C_{P_X}$, we have $T_\epsilon(Y^n|X^n) \subseteq T_\epsilon(Y^n)$, then,

$$T_\epsilon(Y^n) \supseteq \bigcup_{X^n \in C_{P_X}} A(X^n) \cap T_\epsilon(Y^n|X^n).$$

In addition, from (37), $\forall$ $X^n, \tilde{X}^n \in C_{P_X}, X^n \neq \tilde{X}^n$ we have

$$A(X^n) \cap T_\epsilon(Y^n|X^n) \bigcap A(\tilde{X}^n) \cap T_\epsilon(Y^n|\tilde{X}^n) = \emptyset.$$

Thus, we have

$$\begin{aligned}|T_\epsilon(Y^n)| &\geq \sum_{X^n \in C_{P_X}} |A(X^n) \cap T_\epsilon(Y^n|X^n)| \\ &\geq \sum_{X^n \in C_{P_X}} (1 - 3\epsilon) 2^{n(H(Y|X)-2\epsilon)} \\ &\geq (n+1)^{-|\mathcal{X}|} 2^{nR_m} (1 - 3\epsilon) 2^{n(H(Y|X)-2\epsilon)}.\end{aligned}$$

Since that $|T_\epsilon(Y^n)| \leq 2^{n(H(Y)+\epsilon)}$, we have

$$2^{n(H(Y)+\epsilon)} \geq (n+1)^{-|\mathcal{X}|}(1-3\epsilon)2^{n(H(Y|X)+R_m-2\epsilon)},$$

thus,

$$R_m \leq I(X;Y) + 4\epsilon + \frac{|\mathcal{X}|}{n}\log n(1-2\epsilon).$$

The proof is complete. □

Appendix D
Proof of (44)

Define

$$\begin{aligned} S &:= \{P_X : I(X;Y) \geq R_m\}, \\ T &:= \{Q_Y : Q_Y = \sum_{j\in\mathcal{Z}} P_Z(j)V(Y|j), \forall P_Z \in \mathcal{P}_Z\}. \end{aligned}$$

Since Q_Y is an affine function of P_Z, we can rewrite the $\max\min$ problem in (44) as

$$\max_{P_X\in S}\min_{Q_Y\in T} F(P_X, Q_Y),$$

where $F(P_X, Q_Y) := \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m$. Thus, we need to show

$$\max_{P_X\in S}\min_{Q_Y\in T} F(P_X, Q_Y) = \min_{Q_Y\in T}\max_{P_X\in S} F(P_X, Q_Y) \tag{73}$$

is true.

Before going further, we need to introduce Sion's minimax theorem as follows.

Lemma 8 (Sion's minimax theorem [30]). *Let B be a convex subset of a topological vector space and D a compact convex subset of a topological vector space. And f is a real-valued function defined on $B \times D$ with*
1. $f(b,\cdot)$ is lower semicontinuous and quasi-convex on D, $\forall b \in B$, and
2. $f(\cdot,d)$ is upper semicontinuous and quasiconcave on B, $\forall d \in D$.
Then

$$\max_{b\in B}\min_{d\in D} f(b,d) = \min_{d\in D}\max_{b\in B} f(b,d).$$

According to Sion's minimax theorem, in order to obtain (73), we need to prove
a) S and T are convex;
b) Given P_X, $F(P_X,\cdot)$ is convex on T;
c) Given Q_Y, $F(\cdot,Q_Y)$ is quasiconcave on S.
Now, we provide the proofs one by one.
Proof of a). That T is convex is obvious, since Q_Y is an affine function of P_Z, and $\mathcal{P}_Z$ is convex.

Then, we show S is convex. Suppose $P_{X1} \in S$ and $P_{X2} \in S$ (denote the corresponding mutual information by $I(X1;Y)$ and $I(X2;Y)$ respectively), thus we have

$$\begin{aligned} I(X1;Y) &\geq R_m, \\ I(X2;Y) &\geq R_m. \end{aligned}$$

Set $P_{X3} = \lambda P_{X1} + (1-\lambda)P_{X2}$ for arbitrary $\lambda \in [0,1]$. Since the conditional PMF $P_{Y|X}$ is fixed by the channel $W(Y|X)$ and that $I(X;Y)$ is concave in P_X for a fixed $P_{Y|X}$, we have

$$\begin{aligned} I(X3;Y) &\geq \lambda I(X1;Y) + (1-\lambda)I(X2;Y) \\ &\geq \lambda R_m + (1-\lambda)R_m \\ &= R_m. \end{aligned}$$

Thus, $P_{X3} \in S$. Then, we have that S is a convex set.
Proof of b). According to Theorem 2.7.2 of [24], $D(P_{Y,i}||Q_Y)$ is convex in $(P_{Y,i}, Q_Y)$. With a fixed $P_{Y,i}$, we obtain that $D(P_{Y,i}||Q_Y)$ is convex in Q_Y. Thus, suppose $Q_{Y1}, Q_{Y2} \in T$ and $Q_{Y3} = \lambda Q_{Y1} + (1-\lambda)Q_{Y2}$, and $\forall i \in \mathcal{X}$, we have

$$\begin{aligned} &P_X(i)D(P_{Y,i}||Q_{Y3}) \\ &\leq P_X(i)(\lambda D(P_{Y,i}||Q_{Y1}) + (1-\lambda)D(P_{Y,i}||Q_{Y2})). \end{aligned}$$

Thus

$$\begin{aligned} &\sum_i P_X(i)D(P_{Y,i}||Q_{Y3}) \\ &\leq \sum_i P_X(i)(\lambda D(P_{Y,i}||Q_{Y1}) + (1-\lambda)D(P_{Y,i}||Q_{Y2})) \\ &= \lambda\sum_i P_X(i)D(P_{Y,i}||Q_{Y1}) \\ &\qquad\qquad + (1-\lambda)\sum_i P_X(i)D(P_{Y,i}||Q_{Y2}). \end{aligned}$$

Then, we have

$$F(P_X, Q_{Y3}) \leq \lambda F(P_X, Q_{Y1}) + (1-\lambda)F(P_X, Q_{Y2}).$$

Thus, $F(P_X,\cdot)$ is convex on T.
Proof of c). Given Q_Y, we know $F(\cdot, Q_Y)$ is linear in P_X, thus, it's quasiconcave.

Appendix E
Proof of (45)

Proof. To assist the presentation, denote

$$\ell(P_X) := \sum_{i\in\mathcal{X}} P_X(i)h_i - R_m,$$

in which $h_i := D(P_{Y,i}||Q_Y)$. Since for each $i \in \mathcal{X}$, h_i is a constant, we have that $\ell(P_X)$ is linear in P_X.

Recall that $\mathcal{P}_R = \{P_X : I(X;Y) \geq R_m\}$. Suppose

$$P_X^* = \arg\max_{P_X\in\mathcal{P}_R} \ell(P_X), \tag{74}$$

and P_X^* is an interior point of $\mathcal{P}_R$, thus,

$$I(X^*;Y) > R_m.$$

Denote

$$\begin{aligned} S_I &:= \{i \in \mathcal{X} : P_X^*(i) \neq 0\}, \\ \hat{i} &= \arg\min_{i\in S_I} h_i. \end{aligned}$$

Then, we have

$$\begin{aligned}\ell(P_X^*) &= \sum_{i\in S_I} P_X^*(i)h_i - R_m\\ &= \sum_{i\in S_I\backslash\hat{i}} P_X^*(i)h_i + P_X^*(\hat{i})h_{\hat{i}} - R_m\\ &= \sum_{i\in S_I\backslash\hat{i}} P_X^*(i)h_i + \left(1-\sum_{i\in S_I\backslash\hat{i}} P_X^*(i)\right)h_{\hat{i}} - R_m\\ &= \sum_{i\in S_I\backslash\hat{i}} P_X^*(i)(h_i-h_{\hat{i}}) + h_{\hat{i}} - R_m.\end{aligned}$$

Now, construct $\tilde{P}_X$ as

$$\begin{aligned}&\tilde{P}_X(i) = P_X^*(i)+\epsilon, \qquad \forall\ i\in S_I\backslash\hat{i};\\ &\tilde{P}_X(i) = 0, \qquad\qquad\quad\ \forall\ i\in\mathcal{X}\backslash S_I;\\ &\tilde{P}_X(\hat{i}) = 1-\sum_{i\in S_I\backslash\hat{i}}\tilde{P}_X(i).\end{aligned}$$

Due to the continuity of $I(X;Y)$ in P_X, there exists some $\epsilon>0$ such that

$$I(\tilde{X};Y)\geq R_m.$$

However, for this $\tilde{P}_X$, we have

$$\begin{aligned}\ell(\tilde{P}_X) &= \ell(P_X^*) + \epsilon\sum_{i\in S_I\backslash\hat{i}}(h_i-h_{\hat{i}})\\ &\geq \ell(P_X^*),\end{aligned} \tag{75}$$

in which the equality holds only when $h_i = h_{\hat{i}}, \forall i\in S_I$. If the inequality in (75) is strict, then it contradicts the assumption in (74) that P_X^* is the maximizer for $\ell(P_X)$. Hence, the equality in (75) holds. In this case, all $\ell(P_X)$s with $P_X\in\{P_X:\forall i\in\mathcal{X}\backslash S_I, P_X(i)=0\}$ have the same value as $\ell(P_X^*)$. Now, due to the continuity of $I(X;Y)$ in P_X, it's easy to conclude that there exists a $\hat{P}_X\in\{P_X:\forall i\in\mathcal{X}\backslash S_I, P_X(i)=0\}$ such that $I(\hat{X};Y)=R_m$, as 1) $P_X^*\in\{P_X:\forall i\in\mathcal{X}\backslash S_I, P_X(i)=0\}$ and $I(X^*;Y)>R_m$ from the assumption; and 2) there exists a $P_X^\star\in\{P_X:\forall i\in\mathcal{X}\backslash S_I, P_X(i)=0\}$ (e.g. $P_X^\star$ is of the form $[0,\cdots,1,0,\cdots]$) such that $I(X^\star;Y)=0$.

Hence, the optimal value can always be obtained on the boundary defined as

$$\{P_X : I(X;Y)=R_m\}.$$

This completes the proof. □

Appendix F

Proof of Lemma 3. Denote channels $W(Y|X)$ and $V(Y|Z)$ by matrices W and V in short. Define $P_{X,i}^1 = [0,\cdots,0,1,0,\cdots,0]^T, i\in\mathcal{X}$, where 1 is on the ith row. Since the simulatability condition holds, there exists $P_{Z,i}^\Delta\in\mathcal{P}_Z$ such that

$$VP_{Z,i}^\Delta = WP_{X,i}^1,\ \forall i\in\mathcal{X}.$$

In addition, given an arbitrary $P_X\in\mathcal{P}_X$, we have

$$\begin{aligned}P_X &= [P_X(1),\cdots,P_X(|\mathcal{X}|)]^T\\ &= \sum_{i\in\mathcal{X}} P_X(i)P_{X,i}^1.\end{aligned}$$

Set a virtual channel $\tilde{V}_{Z|\tilde{X}}$ by

$$\tilde{V}_{Z|\tilde{X}} = [P_{Z,1}^\Delta, P_{Z,2}^\Delta,\cdots,P_{Z,|\mathcal{X}|}^\Delta],$$

then, we have

$$\begin{aligned}WP_X &= W\sum_{i\in\mathcal{X}}P_X(i)P_{X,i}^1 &(76)\\ &= \sum_{i\in\mathcal{X}}WP_X(i)P_{X,i}^1\\ &= \sum_{i\in\mathcal{X}}P_X(i)WP_{X,i}^1\\ &= \sum_{i\in\mathcal{X}}P_X(i)VP_{Z,i}^\Delta\\ &= V\sum_{i\in\mathcal{X}}P_X(i)P_{Z,i}^\Delta\\ &= V\tilde{V}_{Z|\tilde{X}}P_X. &(77)\end{aligned}$$

Since here $P_X\in\mathcal{P}_X$ is arbitrarily given, we have

$$W = V\tilde{V}_{Z|\tilde{X}}. \tag{78}$$

This completes the proof. □

Proof of Lemma 4. The conclusion that if the simulatability condition holds, then the equations defined by (55) hold is obvious, since $W(Y|i) = W(Y|X)P_{X,i}^1$, and $P_{X,i}^1\in\mathcal{P}_X$ ($P_{X,i}^1$ is defined in the proof of Lemma 3).

On the other hand, as we have shown from (76) to (77), if (55) holds, then $\forall P_X\in\mathcal{P}_X$, $P_Z = \sum_{i\in\mathcal{X}}P_X(i)P_{Z,i}^\Delta$ is always a valid choice. □

Proof of Lemma 5. It suffices to show

$$\min_{P_{Z,i^*}} ||\hat{V}(Y|Z)P_{Z,i^*} - W(Y|i^*)||_1 > 0$$

with constraints defined by (59).

$$\begin{aligned}&\min_{P_{Z,i^*}} ||\hat{V}(Y|Z)P_{Z,i^*} - W(Y|i^*)||_1\\ &\quad= \min_{P_{Z,i^*}} ||(V(Y|Z)+\Delta V(Y|Z))P_{Z,i^*} - W(Y|X)||_1\\ &\quad= \min_{P_{Z,i^*}} ||V(Y|Z)P_{Z,i^*} - W(Y|X) + \Delta V(Y|Z)P_{Z,i^*}||_1\\ &\quad\geq \min_{P_{Z,i^*}} ||V(Y|Z)P_{Z,i^*} - W(Y|X)||_1\\ &\qquad\qquad - \max_{P_{Z,i^*}} ||\Delta V(Y|Z)P_{Z,i^*}||_1\\ &\quad= \rho - \max_{P_{Z,i^*}} ||\Delta V(Y|Z)P_{Z,i^*}||_1\\ &\quad\overset{(a)}{\geq} \rho - |\mathcal{Y}|\delta\\ &\quad> 0,\end{aligned}$$

if $\delta < \frac{\rho}{|\mathcal{Y}|}$. (a) is true since the summation of each column of P_{Z,i^*} equals to 1. □

References

[1] W. Tu and L. Lai, “Keyless authentication over noisy channel,” in *Proc. Asilomar Conf. on Signals, Systems and Computers*, (Pacific Grove, CA), pp. 1665–1669, Nov. 2016.

[2] H. Koga and H. Yamamoto, “Coding theorems for secret-key authentication systems,” *IEICE Trans. Fundamentals*, vol. E83-A, pp. 1691–1703, Aug. 2000.

[3] L. Lai, H. El Gamal, and H. V. Poor, “Authentication over noisy channels,” *IEEE Trans. Inf. Theory*, vol. 55, pp. 906–916, Feb. 2009.

[4] U. Maurer, “Authentication theory and hypothesis testing,” *IEEE Trans. Inf. Theory*, vol. 46, pp. 1350–1356, Jul. 2000.

[5] G. J. Simmons, “Authentication theory/coding theory,” in *Proc. Advances in Cryptology*, (Linz, Austria), pp. 411–431, Apr. 1985.

[6] G. J. Simmons, “A survey of information authentication,” *Proc. IEEE*, vol. 76, pp. 603–620, May 1988.

[7] Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A distributed key management framework with cooperative message authentication in VANETs,” *IEEE J. Sel. Areas Commun.*, vol. 29, pp. 616–629, Mar. 2011.

[8] U. M. Maurer and S. Wolf, “Secret key agreement over a non-authenticated channel - Part I: Definitions and bounds,” *IEEE Trans. Inf. Theory*, vol. 49, pp. 822–831, Apr. 2003.

[9] U. M. Maurer and S. Wolf, “Secret key agreement over a non-authenticated channel - Part II: The simulatability condition,” *IEEE Trans. Inf. Theory*, vol. 49, pp. 832–838, Apr. 2003.

[10] U. M. Maurer and S. Wolf, “Secret key agreement over a non-authenticated channel - Part III: Privacy amplification,” *IEEE Trans. Inf. Theory*, vol. 49, pp. 839–851, Apr. 2003.

[11] T. Johansson, “Lower bounds on the probability of deception in authentication with arbitration,” *IEEE Trans. Inf. Theory*, vol. 40, pp. 1573–1585, Sep. 1994.

[12] M. Walker, “Information-theoretic bounds for authentication schemes,” *Journal of Cryptology*, vol. 2, pp. 131–143, Jan. 1990.

[13] B. Lampson, M. Abadi, M. Burrows, and E. Wobber, “Authentication in distributed systems: Theory and practice,” *ACM Transactions on Computer Systems*, vol. 10, pp. 265–310, Nov. 1992.

[14] T. Y. Woo and S. S. Lam, “Authentication for distributed systems,” *IEEE Computer Society*, pp. 39–52, Jan. 1992.

[15] O. Gungor and C. E. Koksal, “RF-fingerprint based authentication: Exponents and achievable rates,” in *Proc. IEEE Conf. on Communications and Network Security*, (San Francisco, CA), pp. 97–102, Oct. 2014.

[16] H. V. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1994.

[17] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, “Using the physical layer for wireless authentication in time-variant channels,” *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2571–2579, Jul. 2008.

[18] J. K. Tugnait, “Wireless user authentication via comparison of power spectral densities,” *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1791–1802, Aug. 2013.

[19] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, “Physical layer authentication for mobile systems with time-varying carrier frequency offsets,” *IEEE Trans. Commun.*, vol. 62, pp. 1658–1667, May 2014.

[20] H. Wen, P.-H. Ho, C. Qi, and G. Gong, “Physical layer assisted authentication for distributed ad hoc wireless sensor networks,” *IET inf. secur.*, vol. 4, pp. 390–396, Dec. 2010.

[21] X. Wu and Z. Yang, “Physical-layer authentication for multi-carrier transmission,” *IEEE Commun. Lett.*, vol. 19, pp. 74–77, Jan. 2015.

[22] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[23] T. S. Han and K. Kobayashi, “Exponential-type error probabilities for multiterminal hypothesis testing,” *IEEE Trans. Inf. Theory*, vol. 35, pp. 2–14, Jan. 1989.

[24] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: John Wiley & Sons, 2006.

[25] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge University Press, 2004.

[26] H. Tuy, *Convex analysis and global optimization*. Boston, MA: Springer Science & Business Media, 2013.

[27] I. Csiszár and P. Narayan, “The capacity of the arbitrarily varying channel revisited: Positivity, constraints,” *IEEE Trans. Inf. Theory*, vol. 34, pp. 181–193, Mar. 1988.

[28] W. Tu and L. Lai, “On the simulatability condition in key generation over a non-authenticated public channel,” in *Proc. IEEE Int. Symp. Inf. Theory*, (Hongkong, China), pp. 720–724, 2015.

[29] A. El Gamal and Y. Kim, *Network Information Theory*. New York: Cambridge University Press, 2011.

[30] M. Sion, “On general minimax theorems,” *Pacific J. Math*, vol. 8, pp. 171–176, Mar. 1958.

Wenwen Tu (S’16) received the B. E. degree from University of Science and Technology of China, Hefei, China in 2013. He was a PhD candidate at Worcester Polytechnic Institute from 2013 to 2016, a visiting graduate student research collaborator at Princeton University in 2016.

Mr. Tu is currently a Ph.D. candidate in the Department of Electrical and Computer Engineering, University of California, Davis. His research interests include information theory, stochastic learning and machine learning.

Lifeng Lai (M’07) received the B.E. and M. E. degrees from Zhejiang University, Hangzhou, China in 2001 and 2004 respectively, and the PhD degree from The Ohio State University at Columbus, OH, in 2007. He was a postdoctoral research associate at Princeton University from 2007 to 2009, an assistant professor at University of Arkansas, Little Rock from 2009 to 2012, and an assistant professor at Worcester Polytechnic Institute from 2012 to 2016. Since 2016, he has been an associate professor at University of California, Davis. Dr. Lai’s research interests include information theory, stochastic signal processing and their applications in wireless communications, security and other related areas.

Dr. Lai was a Distinguished University Fellow of the Ohio State University from 2004 to 2007. He is a co-recipient of the Best Paper Award from IEEE Global Communications Conference (Globecom) in 2008, the Best Paper Award from IEEE Conference on Communications (ICC) in 2011 and the Best Paper Award from IEEE Smart Grid Communications (SmartGridComm) in 2012. He received the National Science Foundation CAREER Award in 2011, and Northrop Young Researcher Award in 2012. He served as a Guest Editor for IEEE Journal on Selected Areas in Communications, Special Issue on Signal Processing Techniques for Wireless Physical Layer Security. He is currently serving as an Editor for IEEE Transactions on Wireless Communications, and an Associate Editor for IEEE Transactions on Information Forensics and Security.