Keyless Authentication and Authenticated Capacity

Wenwen Tu and Lifeng Lai

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 generate an output at the receiver that is difficult for the adversary to replicate through his noisy channel, and then use this output to distinguish legitimate messages from fake messages. By interpreting the message authentication as a hypothesis testing problem, we investigate the authentication exponent and authenticated channel capacity of a 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 a broad class of non-zero message rate cases. 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 modelling uncertainties in 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 providing the evidence to the receiver that the received message is sent by the transmitter, in the presence of an adversary who intends to deceive legitimate receiver via sending fraudulent messages to the receiver. It has been investigated intensively from different perspectives [1]–[13]. 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, who 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 noiseless channel was developed by Simmons [4]. 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 the receiver, instead of transmitting $M$ directly, Alice transmits a codeword $E = f(M, K)$ into the channel. Upon receiving a codeword $\hat{E}$ ($E = \hat{E}$ 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 [4], two types of attacks were considered. The first one is impersonation attack, in which the adversary Eve sends fake codewords before Alice transmits anything. The impersonation attack is successful if the fake codewords are 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 it observes the codeword sent by Alice. In particular, Eve intercepts the codeword sent by Alice (hence Bob does not receive the codeword sent by Alice), and replaces the intercepted codeword with its own. 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 denoted as $P_S$. [4] 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 augments and $H(\cdot)$ denotes the conditional entropy of its augments. It is clear that there is a tradeoff between making $P_I$ and $P_S$ small. To make $P_I$ small, we should contain more information about the shared key $K$ in $E$, that is to make $I(K; E)$ larger. However, this makes the impersonation attack easier (i.e., $H(K|E)$ smaller), as $E$ will be overheard by Eve perfectly over the noiseless channel.

To overcome the tradeoff faced by the noiseless model in [4], as a natural extension, [2] extended Simmons’s model to the 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, [2] showed that one can make $P_I$ and $P_S$ to be simultaneously small under certain conditions. The model in [2] was further expanded in [14] 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 Bob and Eve are different. This difference can be exploited to facilitate the authentication of users, along with any pre-shared key.

In this paper, we consider a similar model as [14]: Alice, Bob and Eve are all connected by noisy channels. However, unlike all existing work on authentication, 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 paper) for Eve to replicate through his noisy channel to Bob. In this way, after receiving noisy observations $Y^n$ from the channel, Bob can perform a hypothesis testing to check whether it is generated from $P_Y$ or not, which in turn can give Bob the evidence of whether the message is authentic or not. However, this hypothesis testing problem is more challenging than classic hypothesis testing problems [15], in which each element of $Y^n$ is typically assumed to be independently and identically generated from certain PMF under both hypotheses. 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 small 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 lower bound match in the zero-rate case, and in a broad class of nonzero-rate cases. 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 is the largest data transmission rate such that we can still design schemes to guarantee that the successful attack probability of Eve can still be made 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 legitimated transmitter. We show an “all or nothing” result. 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 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 [14]. In this paper, we provide a more detailed and refined analysis.

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 the authentication exponent. In Section V, we characterize the authenticated capacity. Finally, in Section VI, we offer our concluding remarks.

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 $\mathcal{X} = \{1, \ldots , |\mathcal{X}|\}$, $\mathcal{Y} = \{1, \ldots , |\mathcal{Y}|\}$, $\mathcal{Z} = \{1, \ldots , |\mathcal{Z}|\}$, and $\mathcal{F} = \{1, \ldots , |\mathcal{F}|\}$ be four finite discrete sets, which represent the input alphabet sets of Alice, the output alphabet set of Bob, the input alphabet of Eve and the output alphabet of Eve respectively. These three users are connected by three noisy 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 $X = i$. Other channel matrices are defined in a similar manner.

In this paper, we assume that $W(Y|X)$ is perfectly known. As 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 $M \in \{1, \ldots , 2^nR_m\}$ to Bob. He will use an encoder $\phi$ to convert $M$ to codeword $X^n$ and transmit it via channel $W(Y^n|X^n)$. However, Eve is an active attacker, who can intercept the transmission of $X^n$ and falsify some messages via the channel $V(Y|Z)$, based on his optimal strategy to cheat Bob (details of the attacks considered will be made precisely 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 $\psi$ 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 \( \phi \) to decode and obtain \( \hat{M} = \phi(Y^n) \).

In summary, the system consists of the following components:

Encoder \( \phi : M \rightarrow X^n \),

Tester \( \psi : Y^n \rightarrow H_0 \) or \( H_1 \),

Decoder \( \phi \) (if Bob determines \( H_0 \) : \( Y^n \rightarrow \hat{M} \)).

(5)

For a given \( \psi \), the acceptance region is defined by

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

Following the existing work on authentication [1]–[9], 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 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 will be successful if Bob decides \( H_0 \). We use \( P_I \) to denote the success probability of the impersonation attack, i.e., \( P_I = \Pr(\psi(PV(Z^n)) \in \mathcal{A}_n) \).

- **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, and sends a sequence \( Z^n = g_S(F^n) \) based on the observation \( F^n \) 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., \( P_S = \Pr(\psi(PV(Z^n)) \in \mathcal{A}_n \) and \( \hat{M} \neq M \)).

We note that in the substitution attack, Bob does not receive any signal from Alice directly, which is a standard assumption in the existing literature on authentication [1]–[4], [6], [7], [9] and represents the worst case scenario for the legitimate users.

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

\[ P_{SA} \triangleq \max \{ P_I, P_S \}. \] (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 \( \Pr(H_1|H_0) \). 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 \( (\phi, \psi, \varphi) \) is called \((\epsilon, \sigma)\)-robust, if

\[ \max_M \left\{ \Pr(\hat{M} \neq M, H_0|H_0) + \Pr(H_1|H_0) \right\} \leq \epsilon, \] (7)

\[ \max_{g_I, g_S} P_{SA} \leq \sigma. \] (8)

Furthermore, \( R_m \) is said to be achievable using an \((\epsilon, \sigma)\)-robust protocol, if

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

Here, (7) implies that, if there is no attack, the maximum error probability over all messages is required to be smaller than \( \epsilon \). At the same time, (8) implies that, if there is an attack, the success probability of Eve’s optimal attack strategy is less than \( \sigma \). 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 a given \( R_m \), 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 \( \phi, \psi \) and \( \varphi \) range over all possible functions satisfying (7) and (9). Furthermore, we define

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

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

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

for the impersonation attack, and

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

\[ \theta_S(R_m, \epsilon) = \liminf_{n \to \infty} -\frac{1}{n} \log \beta_S(R_m, \epsilon), \] (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 channel \( W(Y|X) \):

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

in which the sup is taken over all \( \phi, \psi, \varphi \) that satisfy (7) and (8) for arbitrarily small \( \epsilon, \sigma \). 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 \( C^* \leq C \).
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 $C_S$ [16], 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 $C_S^* \leq C_S$.

**Notations:** Following [17], for any given sequence $x^n \in \mathcal{X}^n$, the relative frequencies $\left(\frac{n_1}{n}, \ldots, \frac{n_k}{n}\right)$ where $n_i \in \mathcal{X}$ 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 $\hat{P}(x^n)$. We use $P$ or $Q$ to denote the PMF of a random variable, $\mathcal{T}_X$ to denote the set of all types of all sequences $Y^n$s, and $T^n_\Psi(P_Y)$ to denote the set of all sequences $Y^n$s with $\hat{P}(Y^n) = P_Y$. In addition, we denote $Q^n(A) \triangleq \Pr\{Y^n : Y^n \in A[Y \stackrel{iid}{\sim} Q]\}$, in which $Y \stackrel{iid}{\sim} Q$ means that each component of $Y^n$ is independent and identically distributed (i.i.d.) according to $Q$. If $A = T^n_\Psi(P_Y)$, we write it as $Q^n(P_Y)$ in short.

**III. Impersonation vs Substitution Attack**

In this section, we first analyze the relationship between the success probabilities of the impersonation attack and 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.**

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

(15)

**Proof:** We have

$$\beta_S(R_m, \epsilon) = \min_{\phi, \psi, \varphi} \max_{g_1, g_2} P_S$$

$$= \min_{\phi, \psi, \varphi} \max_{g_1, g_2} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n)$$

$$\leq \min_{\phi, \psi, \varphi} \max_{g_1, g_2} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n)$$

$$\leq \min_{\phi, \psi, \varphi} \max_{X^n \sim g_1(X^n)} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n)$$

$$\leq \min_{\phi, \psi, \varphi} \max_{g_1} P_I$$

$$= \beta_I(R_m, \epsilon).$$

(16)

Here, step (a) can be justified as follows. For any given $\phi, \psi, \varphi$, the following attack strategy is a valid impersonation attack strategy: Eve simply assumes a codeword $X^n$ was transmitted by Alice, and he makes an substitution attack towards $X^n$. As this is a particular impersonation attack strategy, we have

$$\min_{X^n \sim g_1(X^n)} \max_{\phi, \psi, \varphi} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n)$$

$$\leq \max_{g_1} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n),$$

which indicates

$$\min_{\phi, \psi, \varphi} \max_{g_1} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n)$$

$$\leq \min_{\phi, \psi, \varphi} \max_{g_1} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n)$$

$$= \min_{\phi, \psi, \varphi} \max_{g_1} P_I.$$

From (16), we have

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

(17)

Now, we show the other direction. The following is a valid substitution attack strategy: No matter what $F^n$ Eve observes from $U(F|X)$, it simply ignores $F^n$, and uses an impersonation attack strategy to pick the attack sequence $Z^n$. For this substitution attack strategy, the success probability

$$P_S \geq \left(1 - \frac{1}{|M|}\right) P_I.$$  

Thus,

$$\beta_S(R_m, \epsilon) \geq \left(1 - \frac{1}{|M|}\right) \beta_I(R_m, \epsilon),$$

(18)

which implies

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

(19)

Combining (17) with (19), we have

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

Now, from (16), we have

$$\beta_n(R_m, \epsilon) = \min_{\phi, \psi, \varphi} \max_{g_1, g_2} \Pr_S$$

$$= \min_{\phi, \psi, \varphi} \max_{g_1, g_2} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n)$$

$$\leq \min_{\phi, \psi, \varphi} \max_{g_1} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n)$$

$$\leq \min_{\phi, \psi, \varphi} \max_{g_1} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n)$$

$$\leq \min_{\phi, \psi, \varphi} \max_{g_1} \Pr(\psi(\mathcal{PV}(Z^n)) \in \mathcal{A}_n)$$

$$\leq \min_{\phi, \psi, \varphi} \max_{g_1} P_I$$

$$= \beta_I(R_m, \epsilon).$$

(16)

Thus, we have

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

And this completes the proof. □

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

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

(20)

which is true due to (16) and (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 value.
Remark 2. Here, we would like to compare this result with the result in the classic authentication setup [4], in which there exists a tradeoff between $P_1$ and $P_S$ as mentioned in the introduction: $P_1 \geq 2^{-I(K;E)}$, $P_S \geq 2^{-R(K;E)}$. 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 $K$ is the main reason for the existence of a tradeoff between $P_1$ and $P_S$ in the classic setup. If $E$ contains more information about $K$, the impersonation attack will be more difficult ($P_1 \downarrow$) but the substitution attack will be easier ($P_S \uparrow$). Similarly, if $E$ contains less information about $K$, $P_1 \uparrow$ while $P_S \downarrow$. In our setup, there is no shared key, hence the codeword $X^n$ sent by Alice is not very useful for Eve. The tradeoff between $P_1$ and $P_S$ does not necessarily exist anymore, and hence it is possible to design schemes to make both probabilities simultaneously small in our setup.

IV. AUTHENTICATION EXPONENT

In this section, for a given $R_m$ and $\epsilon$, 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

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

as $n \rightarrow \infty$. As discussed in Remark 1, it is sufficient to characterize $\theta_1(0, \epsilon)$.

Before deriving $\theta_1(0, \epsilon)$, we first analyze a special case: the case of single message, i.e., $|M| = 1$. In the single message case, the decoding step $\phi$ is not needed, hence the term $\Pr\{M \neq M, H_0|H_0\}$ vanishes and (11) becomes

$$\beta_1(0, \epsilon) = \min_{\phi, \psi} \max_{g_1} P_I,$$

with $0_1$ denoting the fact that $|M| = 1$. We also use $\theta_1(0, \epsilon)$ to denote the corresponding exponent.

We have the following three elements:

- From Alice’s perspective, it needs to design $\phi$. In this case, it is equivalent to deciding which $x^n$ to use for the message.
- From Bob’s perspective, it needs to design $\psi$ for the following hypothesis testing problem:

  $$H_0 : Y^n \sim PW(X^n),$$
  $$H_1 : Y^n \sim PV(Z^n),$$

in which $PW(X^n)$ denote the output distribution at Bob when Alice sends $X^n$. However, this is more challenging than classic hypothesis testing problem [15], in which $Y_i, i = 1, \cdots, n$ are typically assumed to be independent and identically generated from certain PMF under both hypotheses. In our case, $Y_i$ are 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 $g_1$ 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.

$$\theta_1(0, \epsilon) = \max_{i \in X} \min_{P_{Z,i} \in P_Z} D(P_{Y,i}||Q_{Y,i}),$$

in which

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

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

For the proof of Theorem 2, the following definition and properties of $r$-divergent sequence from [18] are useful.

Definition 2 ([18]). Let $X$ be a r.v. 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 $S^r_P$.

Lemma 1 ([18]). Fix $r \geq 0$, then

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

Now we can begin our proof for Theorem 2.

Proof of Theorem 2: The proof has two major steps: 1) Step 1: For any given $\phi$, we characterize the optimal $\psi, g_1$ and the corresponding error exponent; 2) Step 2: Characterize the optimal $\phi$.

Step 1: Characterizing optimal $\psi$ and $g_1$ for any given $\phi$:

In this step, we suppose $\phi$ is fixed such that the codeword for the message is $x^n$ with $tp(x^n) = P_X$. Analyzing this case involves two phases. In the first phase, we show that we can construct $\psi$ such that $\beta_1(0, \epsilon)$ goes to zero exponentially with a rate

$$\min_{\{P_{Z,i}\}_{i \in X}} \sum_{i \in X} P_X(i) \cdot D(P_{Y,i}||Q_{Y,i}).$$

In the second phase, we show there is no scheme that can achieve an error exponent larger than

$$\min_{\{P_{Z,i}\}_{i \in X}} \sum_{i \in X} P_X(i) \cdot D(P_{Y,i}||Q_{Y,i}).$$

Step 1.1: For a given $\phi$, construct a particular $\psi$ and characterize the corresponding optimal attack strategy $g_1$:

Fix a selected codeword $x^n$ with type $tp(x^n) = P_X$. We need to characterize what attack sequences $Z^n(s)$ is (are) optimal to minimize the error exponent. All our analysis is based on
separating $x^n$ in to $|X|$ small sequences with the same realization values, thus, without any loss of generality, we assume $x^n = 1^n 2^n \cdots |X|^n$, in which $n_1 = n_P(x(i), i \in X)$. In the following, we denote the positions of $i^n$ in $x^n$ as the $i$th segment. For $X^n$, the sequences in the $i$th segment is denoted by $X^n_i$, $Y^n_i$ and $Z^n_i$ are defined in the same manner, see Fig. 2.

In the $i$th segment, since $X^n_i = i^n$ and that the channel $W(Y|X)$ is memoryless, $Y^n_i$ obtained by passing $X^n_i$ through $W(Y|X)$ can be seen as i.i.d generated with distribution $P_{Y|i}$ being $W(Y|i)$. Now, we set the acceptance region, which in turn determines $\psi_i$ as

$$
\mathcal{A}_n(x^n) = \{y^n_1, \ldots, y^n_{|X|} : y^n_i \in \mathcal{A}_i, i \in X\},
$$

in which

$$
\mathcal{A}_i := S_n^{P_{Y|i}}(P_{Y|i}),
$$

is defined on the $i$th segment with

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

With this choice of $r$, using Lemma 1, we have that

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

Then, we have

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

Thus,

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

Hence using this particular $\psi$, the constraint (7) is satisfied.

In the following, we analyze the successful attack probability and characterize the optimal $g_1$ (equivalently the optimal choice of the attack sequence $Z^n$) for this particular $\psi$. For any sequence $Z^n = z^n_0$ selected by Eve, we denote the successful attack probability as $\Pr\{\mathcal{A}_n(x^n)|z^n_0\}$. We realize that, due to the construction of $\mathcal{A}_n(x^n)$, we have

$$
\Pr\{\mathcal{A}_n(x^n)|z^n_0\} = \prod_{i \in X} \Pr\{\mathcal{A}_i|z^n_0\}.
$$

Suppose $tp(z^n_0) = P_{Z,i}$, then according to the construction of $\mathcal{A}_i$, all $Z^n_i$s with $tp(Z^n_i) = P_{Z,i}$ result in the same success probability:

$$
\Pr\{\mathcal{A}_i|z^n_0\} = \Pr\{\mathcal{A}_i|z^n_0\}, \forall z^n_i, \text{ with } tp(z^n_i) = P_{Z,i}.
$$

Thus, we have

$$
\Pr\{\mathcal{A}_i|z^n_0\} = \sum_{y^n_i \in \mathcal{A}_i} \Pr\{y^n_i|z^n_0\},
$$

$$
= \sum_{z^n_i \in T^n_{Z,i}(P_{Z,i})} \Pr\{z^n_i|P_{Z,i}\} \sum_{y^n_i \in \mathcal{A}_i} \Pr\{y^n_i|z^n_i\}.
$$

where $\Pr\{Z^n_i|P_{Z,i}\}$ can be an arbitrary conditional probability distribution of $Z^n_i$ given $tp(Z^n_i) = P_{Z,i}$. And (b) holds due to (26).

To analyze $\Pr\{\mathcal{A}_i|z^n_0\}$ further, we first investigate the relationship between $\Pr\{\mathcal{A}_i|z^n_0\}$ and $Q_{Y,i}(\mathcal{A}_i)$, in which

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

with $P_{Z,i} = tp(z^n_0)$. Thus, $Q_{Y,i}$ is equivalent to being the distribution of corresponding $Y$ if Eve i.i.d generates $Z^n_i$ according to $P_{Z,i}$.

We can decompose $Q_{Y,i}(\mathcal{A}_i)$ as follows

$$
Q_{Y,i}^{n_i}(\mathcal{A}_i) = \sum_{z^n_i \in Z^n_i} P_{Z,i}(z^n_i) \cdot \Pr\{\mathcal{A}_i|z^n_i\}
$$

$$
= \sum_{z^n_i \in Z^n_i} P_{Z,i}(z^n_i) \sum_{y^n_i \in \mathcal{A}_i} \Pr\{y^n_i|z^n_i\}
$$

$$
= \sum_{\tilde{P}_{Z,i} \in T^n_{Z,i}(P_{Z,i})} \sum_{z^n_i \in T^n_{Z,i}(\tilde{P}_{Z,i})} P_{Z,i}(z^n_i|\tilde{P}_{Z,i}) P_{Z,i}(\tilde{P}_{Z,i}) \sum_{y^n_i \in \mathcal{A}_i} \Pr\{y^n_i|z^n_i\}
$$

$$
\geq P_{Z,i}(T^n_{Z,i}(P_{Z,i})) \sum_{z^n_i \in T^n_{Z,i}(P_{Z,i})} \sum_{y^n_i \in \mathcal{A}_i} \Pr\{y^n_i|z^n_i\}
$$

$$
\leq P_{Z,i}(T^n_{Z,i}(P_{Z,i})) \cdot \Pr\{\mathcal{A}_i|z^n_0\}.
$$

(29)
(c) is true because of (27). Then, according to Theorem 11.1.4 of [19], we have
\[
P_{Z,i}^{n_i}(T_{Z}^{n_i}(P_{Z,i})) \geq \frac{1}{(n_i + 1)|Z|^i} \cdot 2^{-n_i D(P_{Z,i}||P_{Z,i})}
= \frac{1}{(n_i + 1)|Z|^i}.
\]

Thus, we have
\[
\Pr\{\mathcal{A}_{i}|z_0^{n_i}\} \leq (n_i + 1)|Z|^i Q_{Y,i}^{n_i}(\mathcal{A}_{i}).
\]

In the following, we bound $Q_{Y,i}^{n_i}(\mathcal{A}_{i})$ from above.
\[
Q_{Y,i}^{n_i}(\mathcal{A}_{i}) = \sum_{\mathcal{A}^{(n_i)):T^{(n_i)}(\mathcal{A})}} Q_{Y,i}^{n_i}(\mathcal{A})^{(n_i)},
\]
and by Lemma 5 in Appendix A, \(\forall \mathcal{A}(Y^{n_i}) : T^{(n_i)}(\mathcal{A}) \subseteq S^{(n_i)}(P_{Y,i})\), we have
\[
D(\mathcal{A}(Y^{n_i})||Q_{Y,i}) \geq D(P_{Y,i}||Q_{Y,i}) - \delta(r),
\]
with $\delta(r)$ goes to zero as $r$ decreases. Thus,
\[
Q_{Y,i}^{n_i}(\mathcal{A}) \leq 2^{-n_i D(\mathcal{A}(Y^{n_i})||Q_{Y,i})} \leq 2^{-n_i (D(P_{Y,i}||Q_{Y,i}) - \delta(r))}.
\]

After combining (33) and (31), we have
\[
Q_{Y,i}^{n_i}(\mathcal{A}) \leq \sum_{\mathcal{A}^{(n_i)):T^{(n_i)}(\mathcal{A})}} 2^{-n_i (D(P_{Y,i}||Q_{Y,i}) - \delta(r))}
\leq (n_i + 1)|Z|^i 2^{-n_i (D(P_{Y,i}||Q_{Y,i}) - \delta(r))}.
\]

Combining (34) and (30), we obtain
\[
\Pr\{\mathcal{A}_{i}|z_0^{n_i}\} \leq (n_i + 1)|Z|^i 2^{-n_i (D(P_{Y,i}||Q_{Y,i}) - \delta(r))}
\leq n|\mathbb{Y}||Z| 2^{-n_i (D(P_{Y,i}||Q_{Y,i}) - \delta(r))}.
\]

Thus, we have
\[
\Pr\{\mathcal{A}_{i}(x^n)|z_0^n\} \leq n|\mathbb{Y}||\mathbb{Z}| 2^{-n_i (D(P_{Y,i}||Q_{Y,i}) - \delta(r))}
= n|\mathbb{Y}||\mathbb{Z}| 2^{-n_i (D(P_{Y,i}||Q_{Y,i}) - \delta(r))}
= n|\mathbb{Y}||\mathbb{Z}| 2^{-n_i (D(P_{Y,i}||Q_{Y,i}) - \delta(r))}
\]
which implies
\[
-\frac{1}{n} \log \Pr\{\mathcal{A}_{i}(x^n)|z_0^n\} \geq \sum_{i \in \mathcal{X}} P_X(i) D(P_{Y,i}||Q_{Y,i})
- \delta(r) - \frac{|\mathbb{Y}||\mathbb{Z}|}{n} \log n.
\]

As both $\delta(r)$ and $-\frac{|\mathbb{Y}||\mathbb{Z}|}{n} \log n$ go to zero as $n$ increases, we conclude that $g^*_T$ achieves (38), the best Eve can hope for. Hence, for our particular choice of $\psi$, $g^*_T$ is the optimal attack strategy.

**Step 1.2: Show $\psi$ constructed in Step 1.1 is optimal:**
Consider any acceptance region $\mathcal{A}_{n}$ with $\Pr\{\mathcal{A}_{n}|x^n| \geq 1 - \epsilon$, we will show that the particular attack strategy $g^*_T$ discussed above will achieve an error exponent specified in (38). Here $\Pr\{\mathcal{A}_{n}|x^n| \geq 1 - \epsilon$ is due to the fact that $\Pr\{\mathcal{A}_{n}|x^n| = 1 - \Pr(H_1|H_0)$ as well as the requirement defined by (7). We denote $\mathcal{A}_{i}, i \in \mathcal{X}$ be the set of the ith segment sequences of $Y^n \in \mathcal{A}_{n}$ Then we have
\[
1 - \epsilon \leq \Pr\{\mathcal{A}_{n}|x^n| \geq \sum_{y^n \in \mathcal{A}_{n}} \prod_{i \in \mathcal{X}} \Pr\{y^n|i^n\}
= \sum_{y^n \in \mathcal{A}_{n}} \prod_{i \in \mathcal{X}} \Pr\{y^n|i^n\}
= \sum_{y^n \in \mathcal{A}_{n}} \prod_{i \in \mathcal{X}} P_{Y,i}^{n_i}(y^{n_i})
= \sum_{y^n \in \mathcal{A}_{n}} \sum_{y^{n_k} \in \mathcal{A}_{n} \setminus \mathcal{A}_{i}^{n_i}} P_{Y,i}^{n_k}(y^{n_k}) \prod_{i \in \mathcal{X} \setminus k} P_{Y,i}^{n_i}(y^{n_i})
\]
which implies
\[
\min_{x \in \mathcal{X}} \sum_{P_{X}(i) D(P_{Y,i}||Q_{Y,i})}.
\]

Now, we show that Eve can indeed achieve (38). Let $P_{Z,i}^{n_i}$ be the minimizer for (38) and $Q_{Y,i}^{n_i}$ be the corresponding value computed from (23). Similar as (32), from Lemma 5 in Appendix A, we also have that, \(\forall \mathcal{A}(Y^{n_i}) : T^{(n_i)}(\mathcal{A}) \subseteq S^{(n_i)}(P_{Y,i})\),
\[
D(\mathcal{A}(Y^{n_i})||Q_{Y,i}) \leq D(P_{Y,i}||Q_{Y,i}^*) + \delta(r),
\]
in which $\delta(r)$ goes to zero as $r$ decreases. Thus,
\[
Q_{Y,i}^{n_i}(\mathcal{A}) \geq Q_{Y,i}^{n_i}(\mathcal{A}|Y^{n_i})) \geq \frac{1}{(n_i + 1)|Z|^i} 2^{-n_i D(P_{Y,i}||Q_{Y,i}^*) + \delta(r)},
\]
in which $\delta(r)$ is due to Theorem 11.1.4 in [19]. Now, consider a particular attack strategy $g^*_T$, in which Eve generates $Z^n$ i.i.d. according to $P_{Z,i}^{n_i}$ in the ith segment for $i \in \mathcal{X}$. With this particular attack strategy, from (39), the success probability is
\[
\frac{1}{n} \log P_i \leq \sum_{i \in \mathcal{X}} P_X(i) D(P_{Y,i}||Q_{Y,i}^*)
+ \delta(r) - \frac{|\mathbb{Y}||\mathbb{Z}|}{n} \log n.
\]

As both $\delta(r)$ and $-\frac{|\mathbb{Y}||\mathbb{Z}|}{n} \log n$ go to zero as $n$ increases, we conclude that $g^*_T$ achieves (38), the best Eve can hope for.
Now, consider the attack $g_i^*$ discussed above. Using Lemma 6 in Appendix A, we have
\[ Q_{Y,i,k}^{n_h}(\omega_{k,i}) \geq (1 - 2\epsilon)2^{-n_k(D(P_{Y,i},|Q_{Y,i})+\epsilon)}. \]
Then, we have
\[ P_{i}^* \geq \prod_{i \in X} (1 - 2\epsilon)^{|X|/|X|}2^{-n_i(D(P_{Y,i},|Q_{Y,i})+\epsilon)} \]
\[ = (1 - 2\epsilon)^{|X|/|X|}2^{-n_i(D(P_{Y,i},|Q_{Y,i})+\epsilon)} \]
\[ = (1 - 2\epsilon)^{|X|/|X|}2^{-n_i(P_X(i)D(P_{Y,i},|Q_{Y,i})+\epsilon)} \]
\[ \leq \sum_{i \in X} P_X(i)D(P_{Y,i},|Q_{Y,i}) + \epsilon - \frac{|X|}{n}\log(1 - 2\epsilon). \] (42)
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 with respect to $\omega_N$. By Theorem 3, we have
\[ \theta_i(0,\epsilon) = \max_{x^n} \min_{i \in X} \sum_{i \in X} P_X(i)D(P_{Y,i},|Q_{Y,i}) \]
\[ \geq \frac{1}{|X|}\log \Pr \{\omega_{i,n}^{n} \mid \omega_{i}^{n} \} \geq P_{i}^*. \]
Thus, we have
\[ \theta_i(0,\epsilon) \leq \theta_i(0,\epsilon) \leq \max_{i \in X} \min_{i \in X} D(P_{Y,i},|Q_{Y,i}). \]

**Proof:** First, we show
\[ \theta_i(0,\epsilon) \leq \theta_i(0,\epsilon) = \max_{i \in X} \min_{i \in X} D(P_{Y,i},|Q_{Y,i}). \]
For the multiple messages case, we again require $\Pr(H_1|H_0) \leq \epsilon$. Meanwhile,
\[ \Pr(H_1|H_0) = \sum_{i=1}^{|M|} (P = i) \Pr(H_1|H_0, M = i). \]
As the 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 $M = m$, it has the same requirements as the single message case. Thus, we can conclude that
\[ \theta_i(0,\epsilon) \leq \max_{i \in X} \min_{i \in X} D(P_{Y,i},|Q_{Y,i}). \]
In the following, we show that we can construct a scheme to achieve $\max_{i \in X} \min_{i \in X} D(P_{Y,i},|Q_{Y,i})$. Let $k = \arg \max \min_{i \in X} D(P_{Y,i},|Q_{Y,i})$. Since $\frac{1}{n}\log |M| \overset{n \to \infty}{\to} 0$, there exists an arbitrary small numbers $\{\epsilon_i\}_{i \in X} \subset [k]$, such that $2^n(\sum x_i) > |M|$, in which
\[ P_{i}^* \triangleq \epsilon_1, \epsilon_2, \cdots, \epsilon_{k-1}, 1 - \epsilon_0, \epsilon_{k+1}, \cdots, \epsilon_{|X|} \]
\[ \epsilon_0 = \sum_{i \neq k} \epsilon_i. \] (43)
Now, use $P_{i}^*$ defined above to do randomly coding: Generate $|M|$ sequences as codewords, and set the acceptance region be $\omega_N = T_{i}^n(Y)$, in which the typical set is defined with respect to $P_Y = \sum_{i \in X} P_X(i)W(Y|i)$. When $n$ is sufficiently large, we have $|M| < 2^{n(\sum x_i)}$. Thus, (7) can be easily satisfied. Following similar steps as the derivation of (35), we have
\[ 2^{-n\theta_i(0,\epsilon)} \leq 2^{-n(\min_{i \in X} D(P_{Y,i},|Q_{Y,i}) - \epsilon)} \]
\[ \leq 2^{-n(\min_{i \in X} D(P_{Y,i},|Q_{Y,i}) - \delta(\epsilon))} \]
\[ = 2^{-n\min_{i \in X} D(P_{Y,i},|Q_{Y,i}) - \delta(\epsilon)} \]
\[ = 2^{-n\min_{i \in X} D(P_{Y,i},|Q_{Y,i}) - \delta(\epsilon)}, \]
where $Q_Y = \sum_{i \in X} P_{j}^* j W(Y|i)$, and $\epsilon$ is true due to Lemma 5 in Appendix A, since $D(P_{Y,i},|Q_{Y,i}) \leq \delta(\epsilon)$ because of (43).
Thus, we have $\theta_i(0,\epsilon) \geq \max_{i \in X} \min_{i \in X} D(P_{Y,i},|Q_{Y,i}) - \delta(\epsilon)$. Hence,
\[ \theta_i(0,\epsilon) = \max_{i \in X} \min_{i \in X} D(P_{Y,i},|Q_{Y,i}). \]
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 lower bounds match each other.

**Theorem 3.**
\[ \theta_i(0,\epsilon) = \max_{i \in X} \min_{i \in X} D(P_{Y,i},|Q_{Y,i}), \]
where $P_{Y,i}$ and $Q_{Y,i}$ are defined by (22) and (23).
Theorem 4. Let \( P_Y = \sum_{i \in X} P_X(i)W(Y|i) \) and \( Q_Y = \sum_{j \in Z} P_Z(j)V(Y|j) \), we have

\[
\theta_1(R_m, \epsilon) \leq \min_{P_Z} \max_{P_X \in P_R} D(P_Y||Q_Y), \quad (44)
\]

\[
\theta_1(R_m, \epsilon) \geq \max_{P_X \in P_R} \min_{P_Z} D(P_Y||Q_Y), \quad (45)
\]

in which

\[
P_R := \{ P_X \in P_X : I(X;Y) \geq R_m \}.
\]

Proof:

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

Upper-bounding the error exponent for any scheme by (44): Consider an arbitrary \((\phi, \psi, \varphi)\) that satisfies conditions in (7) and (9). Suppose \( 2^nR_m \) sequences \( X^n \)s are selected by the encoder \( \phi \) as codewords to transmit messages. Define the acceptance region determined by \( \psi \) as \( \mathcal{A}_n \). As there are at most \((n+1)^{|X|}\) different types of \( X^n \)s, there must exist at least \((n+1)^{-|X|}2^{-nR_m}\) codewords that have a 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 \( \psi \) and decoding function \( \varphi \), we define \( A(x^n) \subset \mathcal{Y} \) as the set of \( y^n \)s 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 \( \epsilon \), which will violate the condition (7). It is easy to see that

\[
A(x^n) \cap A(\tilde{x}^n) = \emptyset, \quad \forall \; x^n, \tilde{x}^n \in C_{P_X}, \; x^n \neq \tilde{x}^n. \quad (46)
\]

In Appendix B, we show that we must have

\[
R_m \leq I(X;Y), \quad (47)
\]

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

\[
\mathcal{A}_n \supseteq \bigcup_{x^n \in C_{P_X}} A(x^n). \quad (48)
\]

This is true, because for any \( y^n \notin \mathcal{A}_n \), \( y^n \) will be rejected by Bob, let alone be decoded to a codeword in \( C_{P_X} \). And this contradicts the definition of \( A(x^n) \), 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 i.i.d. generated according to some PMF \( P_Z \), and define

\[
Q_Y = \sum_{j \in Z} P_Z(j)V(Y|j). \quad (49)
\]

With this particular attack, the success probability is

\[
\Pr\{x^n | Z^n\} \overset{(f)}{=} \Pr\left\{ \bigcup_{x^n \in C_{P_X}} A(x^n) \right\} \geq \sum_{x^n \in C_{P_X}} \Pr\{A(x^n)\} \quad (50)
\]

in which \((f)\) is due to (48) and \((g)\) is due to (46).

On the other hand, according to the proof in Theorem 2 (in particular, the proof of (40)), for each \( x^n \in C_{P_X} \), since \( \Pr\{A(x^n)|x^n\} \geq 2^{-n} \), we have

\[
\Pr\{x^n | Z^n\} \geq 2^{-n} \Pr\{A(x^n)\} \geq 2^{-2n} \Pr\{A(x^n)\} \geq 2^{-2n} \Pr\{A(x^n)\} \geq 2^{-2n} \Pr\{A(x^n)\}. \quad (51)
\]

The last step is true, as \( \forall \; x^n \in C_{P_X} \), we have \( Q_{Y,i} = Q_Y \) (\( P_{Y,i} \) and \( Q_{Y,i} \) are defined in Section IV-A).

Thus, we have

\[
\Pr\{x^n | Z^n\} \overset{(g)}{=} \sum_{x^n \in C_{P_X}} \Pr\{A(x^n)\} \geq 2^{-2n} \Pr\{A(x^n)\} \geq 2^{-2n} \Pr\{A(x^n)\} \geq 2^{-2n} \Pr\{A(x^n)\}. \quad (52)
\]

Since \( \Pr\{x^n | Z^n\} \) is obtained by one specific attack strategy, it must be less than or equal to the successful attack probability of the optimal attack strategy, \( \Pr\{x^n | z^n_0\} \). Thus, we have

\[
\frac{1}{n} \log \Pr\{x^n | z^n_0\} \leq \sum_{i \in X} P_X(i)D(P_{Y,i}|Q_Y) - R_m + \frac{|X|}{n} \log(n + 1)
\]

\[
= \sum_{i \in X} P_X(i)D(P_{Y,i}|Q_Y) - R_m + \varepsilon'. \quad (52)
\]

Combining (47) and (52), and since \( \varepsilon' := \varepsilon + \frac{|X|}{n} \log(n + 1) \) is an arbitrary small number as \( n \to \infty \), we have

\[
\theta_1(R_m, \epsilon) \leq \max_{P_X \in P_R} \min_{P_Z} \sum_{i \in X} P_X(i)D(P_{Y,i}|Q_Y) - R_m, \quad (53)
\]

This optimization problem is equivalent to

\[
\theta_1(R_m, \epsilon) \leq \min_{P_Z} \max_{P_X \in P_R} \sum_{i \in X} P_X(i)D(P_{Y,i}|Q_Y) - R_m \quad (h)
\]

\[
= \min_{P_Z} \max_{P_X \in P_R} \sum_{i \in X} P_X(i)D(P_{Y,i}|Q_Y) - R_m. \quad (53)
\]

Here, \((h)\) is proved in Appendix C.

Given any \( P_Z \in P_Z \) (thus, \( Q_Y \) is given), we first focus on the maximization sub-problem:

\[
\max_{P_X \in P_R} \sum_{i \in X} P_X(i)D(P_{Y,i}|Q_Y) - R_m. \quad (54)
\]

In Appendix D, we show that, for the optimization problem (54), the optimizer \( P_X \) must satisfy \( I(X;Y) = R_m \).
On the other hand, we have
\[
\sum_i P_X(i) D(P_{Y,i}||Q_Y) - R_m = 
\sum_i P_X(i) \sum_y P_{Y,i} \log \frac{P_{Y,i}}{Q_Y} - R_m = 
\sum_i P_X(i) \sum_y W(y|i) \log \frac{W(y|i)}{Q_Y} - R_m = 
\sum_i P_X(i) W(y|i) \log \frac{P_Y}{Q_Y} - R_m + \sum_i P_X(i) W(y|i) \log \frac{W(y|i)}{P_Y} - R_m = 
\sum_y P_Y \log \frac{P_Y}{Q_Y} + \sum_{i,y} P_X(i) W(y|i) \log \frac{P_Y}{P_X} - R_m = 
D(P_Y||Q_Y) + I(X;Y) - R_m.
\]
Thus, (53) is equivalent to
\[
\theta_1(R_m, \epsilon) \leq \min_{P_Z} \max_{P_X \in \mathcal{P}_R} \sum_i P_X(i) D(P_{Y,i}||Q_Y) - R_m = 
\min_i \max_{P_X \in \mathcal{P}_R} D(P_{Y,i}||Q_Y) = 
\min_i D(P_{Y,i}||Q_Y),
\]
in which \(\mathcal{P}_R := \{P_X : I(X;Y) = R_m\}\). Here (i) is true because as discussed above, the optimizer \(P_X\) must satisfy \(I(X;Y) = R_m\). In addition, (j) is true since given any \(P_Z\), \(D(P_Y||Q_Y)\) is convex in \(P_Y\) while \(P_Y\) is an affine function of \(P_X\), then \(D(P_Y||Q_Y)\) is convex in \(P_Y\) and \(D(P_Y||Q_Y)\) is obtained on the boundary \(\partial P_R\) [21].

**Construct a scheme to achieve (45):** 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 \(2^{-n \epsilon(R_m) - \epsilon} \).

**Codebook construction:** Fix \(P_X\), i.i.d. generates \(2^n R_m\) sequences \(X^n\)'s as codewords, according to PMF \(P_X\). Here \(R_m \leq I(X;Y)\). Each codeword is assigned to one message. And we use \(X^n(m)\) to denote the \(m\)th codeword.

**Encoder \(\phi\):** If Alice needs to send a message \(M = m\) to Bob, she transmits \(X^n(m)\) into the channel.

**Testing function \(\psi\):** 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 \(P_Y = \sum_{i \in X} P_X(i) W(Y|i)\) computed from the given \(P_X\); Otherwise, Bob declares that the message is from Eve, and abandons it. Hence, the acceptance region is \(\mathcal{A} = T^n_e(Y)\). It is easy to show that for any given \(\epsilon\), there exists an \(r\) such that
\[
\mathcal{A} \subseteq S^n_e(P_Y).
\]
Furthermore, \(r\) goes to zero as \(\epsilon\) decreases.

**Decoder \(\varphi\):** If \(y^n\) is authenticated to be from Alice, Bob tries to find a unique sequence \(x^n\) from the codebook such that \((x^n, y^n)\) are jointly typical and set \(\hat{m}\) as the index of this \(x^n\). If there are more than one such sequence \(x^n\)'s, randomly picks one \(X^n(\hat{m})\) and declares \(\hat{m}\) as the transmitted message; If there is no such sequence, declares an error.

**Error analysis:** Since the acceptance region is \(\mathcal{A} = T^n_e(Y)\), and all \(Y^n\) sequences that are jointly typical with \(X^n\) are included in \(\mathcal{A}\), thus, we can easily show that
\[
\Pr\{\hat{M} \neq M, H_0|H_0\} \leq \epsilon
\]
and
\[
\Pr\{H_1|H_0\} \leq \epsilon.
\]
Using similar argument as that of the proof of Theorem 7.7.1 [19], we can obtain that there exists at least one codebook such that (7) is satisfied.

**Error exponent analysis:** For any attack sequence \(z^n_0\) with type \(P_Z\) chosen by Eve, we have
\[
\Pr\{\mathcal{A}^c|z^n_0\} \leq \Pr\{S^n(P_Z)|z^n_0\},
\]
which is true due to (56).

Following the same derivation of (35) (here we have only one segment, the whole sequence), we have
\[
\Pr\{S^n(P_Z)|z^n_0\} \leq n|X| + |Z| \frac{2^{-n(D(P_Y||Q_Y) - \delta(r))}}{2^{-n\min_{P_Z} D(P_Y||Q_Y) - \delta(r))}}.
\]
Thus, we have
\[
\Pr\{\mathcal{A}^c|z^n_0\} \leq n|X| + |Z| \frac{2^{-n\min_{P_Z} D(P_Y||Q_Y) - \delta(r))}}{2^{-n\min_{P_Z} D(P_Y||Q_Y) - \delta(r))}}.
\]

Finally, we have
\[
\theta_1(R_m, \epsilon) \geq \max_{P_X \in \mathcal{P}_R} \min_{P_Z} D(P_Y||Q_Y),
\]
This completes the proof.

**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 (44) and (45) match.
Proof. First, from (55), we know that the upper bound (44) can be equivalently written as
\[ \theta_1(R_m, \epsilon) \leq \max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X; Y) - R_m] \] (58)

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 (45) can be equivalently written as
\[ \theta_1(R_m, \epsilon) \geq \max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X; Y) - R_m], \] (59)

which implies that the upper bound (44) matches with the lower bound (45).

Hence, to show this corollary, we only need to show (59). Towards that end, let
\[ \hat{P}_X = \arg \max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X; Y) - R_m], \]
\[ \tilde{P}_X = \arg \max_{P_X \in \mathcal{P}_R} f(P_X). \] (60)

Since \( D(P_Y || Q_Y) \) is convex in pair \((P_Y, Q_Y)\) and \((P_X, Q_Y)\) are affine functions of \((P_X, P_Z)\), then \( D(P_Y || Q_Y) \) is convex in \((P_X, P_Z)\). Thus, according to [20], \( f(P_X) \) 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 [21], that is \( I(\hat{X}; Y) = R_m \). Hence, we have
\[ f(\hat{P}_X) = \max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X; Y) - R_m] \]
\[ \geq \max_{P_X \in \mathcal{P}_R} f(P_X) \]
\[ = f(\hat{P}_X). \]

On the other hand, from (60), we have \( f(\tilde{P}_X) \leq f(\hat{P}_X) \). Thus,
\[ f(\hat{P}_X) = f(\tilde{P}_X). \]
Hence, if \( f(P_X) + I(X; Y) \) is convex in \( P_X \in \mathcal{P}_R \), the optimal value of the optimization problem (59) is same as
\[ \max_{P_X \in \mathcal{P}_R} f(P_X), \]
which is (45). This finishes the proof. \( \square \)

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

Example 1: Let
\[ W(Y|X) = \begin{bmatrix} 1/3 & 1/4 \\ 2/3 & 3/4 \end{bmatrix}, \quad V(Y|X) = \begin{bmatrix} 2/5 & 2/3 \\ 3/5 & 1/3 \end{bmatrix}, \]
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
\[ P_Y = W(Y|X)P_X = \begin{bmatrix} 1 + \frac{1}{12} \lambda_1, 3 - \frac{1}{12} \lambda_1 \\ 2/5 + \frac{4}{15} \lambda_2, 1/3 + \frac{4}{15} \lambda_2 \end{bmatrix}^T, \]
\[ Q_Y = V(Y|X)P_Z = \begin{bmatrix} 2/3 - \frac{4}{15} \lambda_2, 1/3 + \frac{4}{15} \lambda_2 \\ 1 + \frac{1}{12} \lambda_1, 3/4 - \frac{1}{12} \lambda_1 \end{bmatrix}^T. \]

Define \( \lambda_0 = \frac{1}{4} + \frac{1}{12} \lambda_1 \), then
\[ D(P_Y || Q_Y) = \lambda_0 \log \frac{\lambda_0}{R} \quad \text{and} \quad (1 - \lambda_0) \log \frac{1 - \lambda_0}{R}. \]
Following simple calculations, we have
\[ \frac{\partial D(P_Y || Q_Y)}{\partial \lambda_2} = \frac{4}{15} \left( \frac{2}{15} - \frac{4}{15} \lambda_2 \right) \left( \frac{4}{15} \lambda_2 + 2 \right) \ln 2 \left( \frac{4}{15} \lambda_2 + 2 \right). \]
Since \( \lambda_0 \in [\frac{1}{4} : \frac{1}{3}] \), we have
\[ \frac{\partial D(P_Y || Q_Y)}{\partial \lambda_2} < 0, \quad \forall \lambda_0 \in \left[ \frac{1}{4} : \frac{1}{3} \right], \lambda_2 \in [0 : 1]. \]
Thus, for any given \( P_Y \), \( D(P_Y || Q_Y) \) is a decreasing function of \( \lambda_2 \). Hence,
\[ \lambda_2^* = \arg \min_{\lambda_2} D(P_Y || Q_Y) = 1, \quad \forall \lambda_0 \in \left[ \frac{1}{4} : \frac{1}{3} \right], \]
which is equivalent to
\[ Q_Y^* = \arg \min_{Q_Y} D(P_Y || Q_Y) = \begin{bmatrix} 2/5, 3/5 \end{bmatrix}^T, \quad \forall P_X \in \mathcal{P}_X. \] (61)
Hence,
\[ f(P_X) + I(X; Y) \]
\[ = D(P_Y || Q_Y^*) + I(X; Y) \]
\[ = \sum_y P_Y \log \frac{P_Y}{Q_Y^*} + H(Y) - H(Y|X) \]
\[ = \sum_y P_Y \log \frac{P_Y}{Q_Y^*} - \sum_y P_Y \log P_Y - \sum_{i \in X} P_X(i) H(Y|i) \]
\[ = \sum_y P_Y \log \frac{1}{Q_Y^*} - \sum_{i \in X} P_X(i) H(Y|i). \]
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.

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 the simulatability condition that plays an important role in our study. The simulatability condition was first defined under the source model in [8] for the study of key generation under unauthenticated public channel problems. Here, we extend the definition to the channel model. We note that [14] also introduced a similar concept for the channel.
model. We will show that our definition will lead to the definition given in [14].

**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 $P_X \in \mathcal{P}_X$, there exists some $P_Z \in \mathcal{P}_Z$ such that
\[
\sum_{j \in Z} V(Y|j) \cdot P_Z(j) = \sum_{i \in X} W(Y|i) \cdot P_X(i),
\]
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 $Y^n$s from both channels have the same distribution.

We have the following lemmas regarding the simulatability condition.

**Lemma 2.** Given channels $W(Y|X)$ and $V(Y|Z)$, if the simulatability condition holds, then Eve can construct a virtual channel $\tilde{V}(Z|\hat{X})$, such that
\[
V(Y|Z)\tilde{V}(Z|\hat{X}) = W(Y|X).
\]

**Proof.** The proof is given in Appendix E.

![Diagram](image)

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

As shown in Fig. 3, Lemma 2 means that if the simulatability condition holds, by concatenating $\tilde{V}(Z|\hat{X})$ to $V(Y|Z)$, Eve can construct a channel $\tilde{X} \rightarrow Y$ that has the same statistics as the legitimate channel $X \rightarrow Y$. The definition of simulatability condition in [14] has the same interpretation as shown in Fig. 3.

Using Lemma 2, we can greatly simplify the simulatability condition as shown in the following lemma.

**Lemma 3.** Given $W(Y|X)$ and $V(Y|Z)$, the simulatability condition holds if and only if for all $i \in X$, there exists $P_{Z|i} \in \mathcal{P}_Z$, s.t.
\[
V(Y|Z)P_{Z|i} = W(Y|i).
\]

**Proof.** The proof is given in Appendix E.

This lemma plays a key role in the proof of our main result on the authenticated capacity. It will also facilitate 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 $P_X^* = \arg \max I(X;Y)$ (the corresponding $P_Y = P_Y^*$), then $C = I(X^*;Y^*)$. If the simulatability condition doesn’t hold and $\min_{P_Z} D(P_X^*||Q_Y) > 0$, the result $C^* = C = I(X^*;Y^*)$ is obvious, as we can fix $P_X = P_X^*$ and use the same scheme as in the achievability in Section IV-B. Using this scheme, the successful attack probability is upperbounded as
\[
\beta_n(Z^n) \leq 2^{-n(\min_{P_Z} D(P_X^*||Q_Y) - \epsilon)} \leq \epsilon.
\]

However, if the simulatability condition doesn’t hold but $\min_{P_Z} D(P_X^*||Q_Y) = 0$, 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 messages 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 2, if the simulatability condition holds, Eve can concatenate a virtual channel $\tilde{V}(Z|\hat{X})$ to the channel $V(Y|Z)$ such that the concatenated channel $\tilde{X} \rightarrow Y$ has the same statistics as the legitimate channel $X \rightarrow Y$. Now, for any legitimate users’ strategy $\phi, \psi, \phi_e$ that satisfy (7), Eve can always generate the same codebook as Alice’s codebook. When Eve conducts an impersonation attack, he only needs to randomly pick a codeword from the codebook and sends it through the concatenated channel $\tilde{X} \rightarrow Y$. Since this concatenated channel has the same statistics as that of $X \rightarrow Y$, the successful attack probability will be the same as the probability of the message being accepted by Bob as if the message was sent by Alice. 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 doesn’t hold, we’ll show that there exists a scheme such that Alice can reliably transmit some 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 $1 - \sigma$.

According to Lemma 3, if the simulatability condition doesn’t hold, then there exists $i^* \in X$ s.t.
\[
V(Y|Z)P_{Z,i^*} \neq W(Y|i^*), \forall P_Z \in \mathcal{P}_Z.
\]

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 $X^n$s according to PMF $P_X$ with $R_m = I(X;Y) - \epsilon_0$.

We then construct a sequence $i^*\sqrt{n}$, that is to repeat $i^*\sqrt{n}$ times and append $i^*\sqrt{n}$ to each generated $X^n$. We denote the new $n + \sqrt{n}$ length sequence as $X^{n+\sqrt{n}}$. As will be clear in the sequel, $i^*\sqrt{n}$ will be used as an authenticator. We then set
\( \hat{X}^{n+\sqrt{n}} \) as codewords, and each \( \hat{X}^{n+\sqrt{n}}(m) \) is assigned to one message. We use \( \hat{X}^{n+\sqrt{n}}(m) \) to denote the \( m \)th codeword. Fig. 4 illustrates the codeword \( \hat{X}^{n+\sqrt{n}} \).

![Codeword: \( \hat{X}^{n} \) is assigned to one message](image)

**Fig. 4. Codeword \( \hat{X}^{n+\sqrt{n}} \)**

**Encoding:** If Alice needs to send a message \( M = m \) 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, 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 joint typical, and decodes the signal to \( \hat{m} \). If there are more than one such sequence, randomly picks one. If there is no such sequence, declares an error.

**Error analysis:** Since the acceptance region is \( \mathcal{U} = Y^{n} \times T^\sqrt{n}(Y, i^{*}) \), and all \( X^{n} \)-joint typical sequence \( Y^{n} \) is included in \( \mathcal{U} \), 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 argument as in the proof of Theorem 7.7.1 [19], 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, according to the achievability proof of Theorem 2, we have

\[
P_{I} \leq 2^{-\sqrt{n}(D(P_{Y,i,*}||Q_{Y,i,*})-\epsilon_{0})} \leq \sigma,
\]

when \( n \) is sufficiently large.

**Rate Per Channel Use:**

\[
R = \frac{nR_{mn}}{n + \sqrt{n}} = \frac{n}{n + \sqrt{n}}(I(X; Y) - \epsilon_{0}) \\
= I(X; Y) - \frac{\sqrt{n}}{n + \sqrt{n}}I(X; Y) - \frac{n}{n + \sqrt{n}}\epsilon_{0} \\
\geq I(X; Y) - \epsilon,
\]

when \( n \) is large.

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, \( C_{S}^{E} = 0 \); Otherwise, \( C_{S}^{E} = C_{S} \).

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

**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 3, we know that to check the simulatability condition, we only need to check, for each \( i \), whether there exists some \( P_{Z,i} \in \mathcal{P}_{Z} \) such that (64) holds.

It is easy to see that if there exists \( P_{Z,i} \in \mathcal{P}_{Z} \) such that (64) holds, then the optimal value of the following optimization problem will be:

\[
\min_{P_{Z,i}} \|V(Y|Z)P_{Z,i} - W(Y|i)\|_{1} \quad (66) \\
\text{s.t.} \quad P_{Z,i} \geq 0, \\
\sum_{j \in \mathcal{Z}} P_{Z,i}(j) = 1,
\]

in which \( \| \cdot \|_{1} \) is the \( \ell_{1} \) norm. At the same time, if the optimal value obtained from the optimization problem (66) is 0, the corresponding optimizer will satisfy (64). Hence, we conclude that (64) holds if and only if the optimal value obtained from (66) is 0. It is easy to check that (66) is a convex optimization problem, and hence can be solved efficiently. In fact, following similar steps as those in our recent work [22], the optimization problem (66) can be further simplified to be a linear programming problem. Details of those steps are omitted, as they are very similar to those in [22].

Finally, using Lemma 3, we know that we only need to solve \( |\mathcal{X}| \) convex optimization problems as (66) to check the simulatability condition (62).

**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, similar to the sensitive analysis in [22], we will show that the simulatability condition here is not sensitive to modelling 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

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

We clearly have

\[
\sum_{j=1}^{|\mathcal{Y}|} \Delta V(j|k) = 0, \quad \forall k \in [1 : |\mathcal{Z}|].
\]
Suppose based on $V(Y|Z)$, Alice and Bob determine that $W(Y|X)$ is not simulatable, i.e., there exists $i^*$ such that $W(Y|i^*)$ satisfies

$$V(Y|Z)P_Z \neq W(Y|i^*), \forall P_Z \in \mathcal{P}_Z. \tag{67}$$

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

$$\rho = \min_{P_{Z,i^*}} ||V(Y|Z)P_{Z,i^*} - W(Y|i^*)||_1 \tag{68}$$

s.t. $P_{Z,i^*} \geq 0$, $\sum_{j \in Z} P_{Z,i^*}(j) = 1$.

From (67), we know $\rho > 0$.

We have the following result.

**Lemma 4.** Suppose Eve can’t simulate $W(Y|i^*)$ with regards to $V(Y|Z)$, then $\forall \delta < \frac{\delta}{|\mathcal{Y}|}$, Eve cannot simulate $W(Y|i^*)$ using $\hat{V}(Y|Z)$ neither.

**Proof.** The proof is shown in Appendix E. \hfill \square

This result means that, although Alice and Bob only have an estimate of Eve’s channel $V(Y|Z)$, the authenticator $i^*\sqrt{\pi}$ 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 $\delta$ 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

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

Then, we have

$$\rho = \min_{P_{Z,i^*}} ||V(Y|Z)P_{Z,i^*} - W(Y|i^*)||_1 = \min_{P_{Z,i^*}} \left| \left[ \frac{1}{2} - \frac{2}{3} \right] \right|_1 = 1/3.$$ 

Now if

$$\delta < \frac{\rho}{|\mathcal{Y}|} = \frac{1}{2} \rho = \frac{1}{6}, \tag{69}$$

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 (69).

**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 channel. We have characterized the authentication exponent for the zero-rate case and a broad class of nonzero-rate cases. 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 modelling uncertainties in Eve’s channels.

**APPENDIX A**

**Lemma 5.** Let $P^*$, $P$ and $Q$ be three distributions related to $X$, and $r \geq 0$, then if $D(P^*||P) \leq r$ and $0 < D(P||Q) < \infty$, then

$$D(P^*||Q) \geq D(P||Q) - \delta(r),$$

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

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

In order to prove Lemma 5, techniques from [19] are utilized.

**Lemma 6 ([19]).** 1. (Pinsker’s Inequality) Let $P$ and $Q$ be any two distributions related to $X$, then

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

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

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

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

Define a set $A := \{i \in \mathcal{X} : P(i) > Q(i)\}$, and $\bar{A} := \mathcal{X} \setminus A$. 

14
Then we have

$$D(P^*||Q) = \sum_{i \in A} P^*(i) \log \frac{P^*(i)}{Q(i)}$$

$$= \sum_{i \in A} P^*(i) \log \frac{P^*(i)}{Q(i)} + \sum_{i \in A} P^*(i) \log \frac{P^*(i)}{Q(i)}$$

$$\geq \sum_{i \in A} (P(i) - \sqrt{2r \ln 2}) \log \frac{P(i) - \sqrt{2r \ln 2}}{Q(i)}$$

$$+ \sum_{i \in A} (P(i) + \sqrt{2r \ln 2}) \log \frac{P(i) + \sqrt{2r \ln 2}}{Q(i)}$$

$$= \sum_{i \in A} P(i) \log \frac{P(i) - \sqrt{2r \ln 2}}{Q(i)}$$

$$- \delta'(r) \quad (70)$$

$$\geq \sum_{i \in A} P(i) \log \frac{P(i) - \sqrt{2r \ln 2}}{Q(i)} - \delta'(r)$$

$$= D(P||Q) - \sum_{i \in A} P(i) \frac{2\sqrt{2r \ln 2}}{P(i) \ln 2} - \delta'(r)$$

$$= D(P||Q) - \delta_1(r),$$

where (l) is true due to the fact that \(\ln(1 - \gamma) \geq -2\gamma\) when \(\gamma \geq 0\) is small enough. Then, we only need to show \(\delta_1(r)\) vanishes as \(r \rightarrow 0\), which is equivalent to show \(\delta'(r) \downarrow 0\) as \(r \downarrow 0\). From (71) to (72), \(\delta'(r) := \varepsilon \cdot (\sum \log \frac{P(i) - \varepsilon}{Q(i)} - \sum \log \frac{P(i)}{Q(i)})\) by setting \(\varepsilon = \sqrt{2r \ln 2}\). Since the sizes of sets \(A\) and \(\tilde{A}\) are finite, we only need to show \(\log \frac{P(i) - \varepsilon}{Q(i)}\) is finite when \(\varepsilon\) is small enough. And that \(\forall i \in A, \log \frac{P(i) - \varepsilon}{Q(i)}\) 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 (47)**

**Proof.** According to the conditional typicality property, we have

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

Thus,

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

In addition, for each \(y^n \in T_x(Y^n|x^n)\), we have

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

Thus, we have

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

Since for each \(x^n \in C_{P_x}\), we have \(T_x(Y^n|x^n) \subseteq T_x(Y^n)\), then,

$$T_x(Y^n) \supseteq \bigcup_{x^n \in C_{P_x}} A(x^n) \cap T_x(Y^n|x^n).$$

In addition, from (46), \(\forall x^n, \tilde{x}^n \in C_{P_x}, x^n \neq \tilde{x}^n\) we have

$$A(x^n) \cap T_x(Y^n|x^n) \cap T_x(Y^n|x^n) = \emptyset.$$ 

Thus, we have

$$\Pr\{A(x^n) \cap T_x(Y^n|x^n)\} \leq \sum_{x^n \in C_{P_x}} \Pr\{A(x^n) \cap T_x(Y^n|x^n)\}$$

$$\geq \sum_{x^n \in C_{P_x}} (1 - 3\epsilon)2^{n(H(Y|X)-2\epsilon)}$$

Since that \(\Pr\{T_x(Y^n)\} \leq 2^n(H(Y)+\epsilon)\), we have

$$2^{n(H(Y)+\epsilon)} \geq (n + 1)^{-|X|2^{nR_m}(1 - 3\epsilon)2^n(H(Y|X)-2\epsilon)}.$$ 

Thus,

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

The proof is complete. 

**APPENDIX C**

**Proof of (53)**

Define

$$S := \{P_x : I(X;Y) \geq R_m\}$$

$$T := \{Q_Y : Q_Y = \sum_{j \in Z} P_Z(j)V(Y|j), \forall P_Z \in P_Z\}.$$ 

Since \(Q_{Y|X}\) is an affine function of \(P_Z\), we can rewrite the max problem in (53) as

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

where \(F(P_x, Q_Y) := \sum_{i \in X} P_x(i)D(P_y||Q_Y) - R_m\). Thus, we need to show

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

(73) is true.

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

**Lemma 7** (Sion’s minimax theorem [23]). 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 \(B\),
Thus, it’s quasiconcave. Given 

\[ P_X = \text{arg max}_{P_X} \, f(P_X), \]

and that \( I \) is concave in \( P_X \) for a fixed \( P_{Y\mid X} \), we have

\[ I(X; Y) \geq R_m, \]
\[ I(X2; Y) \geq R_m. \]

Thus, \( P_{X3} \in S \). Then, we have that \( S \) is a convex set.

Proof of \( b \). According to Theorem 2.7.2 of [19], \( D(P_{Y\mid X}) \) is convex in the pair \( (P_{Y\mid X}, P_Y) \). With a fixed \( P_{Y\mid X} \), we obtain that \( D(P_{Y\mid X}) \) is convex in \( P_Y \). Thus, suppose \( Q_{Y1}, Q_{Y2} \in T \) and \( Q_{Y3} = \lambda Q_{Y1} + (1-\lambda) Q_{Y2} \), and \( \forall i \in X \), we have

\[ P_X(i)D(P_{Y\mid X})|Q_{Y3}) \leq P_X(i)(\lambda D(P_{Y\mid X})|Q_{Y1}) + (1-\lambda) D(P_{Y\mid X})|Q_{Y2}). \]

Thus,

\[ \sum_{i} P_X(i)D(P_{Y\mid X})|Q_{Y3}) \leq \sum_{i} P_X(i)(\lambda D(P_{Y\mid X})|Q_{Y1}) + (1-\lambda) D(P_{Y\mid X})|Q_{Y2}) \]
\[ = \lambda \sum_{i} P_X(i)D(P_{Y\mid X})|Q_{Y1}) \]
\[ + (1-\lambda) \sum_{i} P_X(i)D(P_{Y\mid X})|Q_{Y2}) \]

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 D**

**PROOF OF (54)**

**Proof.** To assist the presentation, denote

\[ f(P_X) := \sum_{i \in X} P_X(i)h_i - R_m, \]

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

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

\[ P_X^* = \text{arg max}_{P_X \in \mathcal{P}_R} f(P_X), \quad (74) \]

and \( P_X^* \) is an interior point of \( S \), thus,

\[ I(X^*; Y) > R_m. \]

Denote

\[ S_I := \{ i \in X : P_X^*(i) \neq 0 \}, \]
\[ \hat{i} = \text{arg min}_{i \in S_I} h_i. \]

Then, we have

\[ f(P_X^*) = \sum_{i \in S_I} P_X^*(i)h_i - R_m \]
\[ = \sum_{i \in S_I \setminus \hat{i}} P_X^*(i)h_i + P_X^*(\hat{i})h_{\hat{i}} - R_m \]
\[ = \sum_{i \in S_I \setminus \hat{i}} P_X^*(i)h_i + \left(1 - \sum_{i \in S_I \setminus \hat{i}} P_X^*(i)\right) h_{\hat{i}} - R_m \]
\[ = \sum_{i \in S_I \setminus \hat{i}} P_X^*(i)(h_i - h_{\hat{i}}) + h_{\hat{i}} - R_m. \]

Now, construct \( \tilde{P}_X \) as

\[ \tilde{P}_X(i) = P_X^*(i) + \epsilon, \quad \forall i \in S_I \setminus \hat{i}; \]
\[ \tilde{P}_X(i) = 0, \quad \forall i \in X \setminus S_I; \]
\[ \tilde{P}_X(\hat{i}) = 1 - \sum_{i \in S_I \setminus \hat{i}} \tilde{P}_X(i). \]

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

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

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

\[ f(\tilde{P}_X) = f(P_X^*) + \epsilon \sum_{i \in S_I \setminus \hat{i}} (h_i - h_{\hat{i}}) \]
\[ \geq f(P_X^*), \quad (75) \]

and “=” is true when \( h_i = h_{\hat{i}}, \forall i \in S_I \). In this case, all \( f(P_X) \) has the same value as \( f(P_X^*) \), if we set \( P_X \) as the same as \( P_X^* \) \( (\forall i \in X, P_X(i) = 0 \text{ if } P_X^*(i) = 0) \). Hence, there exists a \( P_X \) such that \( I(X; Y) = R_m \).

If “=” is not true in (75), it contradicts the assumption (74).

Thus the optimal value must be obtained on the boundary of \( S \), in which the boundary is defined as

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

This completes the proof. \( \square \)
APPENDIX E

Proof of Lemma 2. Denote channels $W(Y|X)$ and $V(Y|Z)$ by matrices $W$ and $V$ in short. Define $P^{1}_{X,i} = [0, \cdots, 0, 1, 0, \cdots, 0]^{T}$, $i \in \mathcal{X}$, where 1 is on the $i$th row. Since the simulatability condition holds, there exists $P_{Z,i}^{*} \in \mathcal{P}_{Z}$ such that

$$V P_{Z,i}^{*} = W P^{1}_{X,i}, \forall i \in \mathcal{X}.$$ 

In addition, given an arbitrary $P_{X} \in \mathcal{P}_{X}$, we have

$$P_{X} = \sum_{i \in \mathcal{X}} P_{X}(i) P^{1}_{X,i}.$$ 

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

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

then we have

$$WP_{X} = W \sum_{i \in \mathcal{X}} P_{X}(i) P^{1}_{X,i} \tag{76}$$
$$= \sum_{i \in \mathcal{X}} WP_{X}(i) P^{1}_{X,i}$$
$$= \sum_{i \in \mathcal{X}} P_{X}(i) WP^{1}_{X,i}$$
$$= \sum_{i \in \mathcal{X}} P_{X}(i) V P_{Z,i}^{\hat{X}}$$
$$= V \sum_{i \in \mathcal{X}} P_{X}(i) P_{Z,i}^{\hat{X}}$$
$$= V \hat{V}_{Z|\hat{X}} P_{X}. \tag{77}$$

Since here $P_{X} \in \mathcal{P}_{X}$ is arbitrarily given, we have

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

This completes the proof.

Proof of Lemma 3. The conclusion that if the simulatability condition holds, then the equations defined by (64) 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 2).

On the other hand, as we have shown from (76) to (77), if (64) holds, then $VP_{X} \in \mathcal{P}_{X}$, $P_{Z} = \sum_{i \in \mathcal{X}} P_{X}(i) P_{Z,i}^{\hat{X}}$ is always a valid choice.

Proof of Lemma 4. It suffices to show

$$\min_{P_{Z,i}^{*}} \|\hat{V}(Y|Z) P_{Z,i}^{*} - W(Y|i^{*})\|_{1} > 0$$

with constraints defined by (68).

$$\min_{P_{Z,i}^{*}} \|\hat{V}(Y|Z) P_{Z,i}^{*} - W(Y|i^{*})\|_{1} = \min_{P_{Z,i}^{*}} \|\hat{V}(Y|Z) + \Delta V(Y|Z) P_{Z,i}^{*} - W(Y|X)\|_{1}$$
$$= \min_{P_{Z,i}^{*}} \|V(Y|Z) P_{Z,i}^{*} - W(Y|X) + \Delta V(Y|Z) P_{Z,i}^{*}\|_{1}$$
$$\geq \min_{P_{Z,i}^{*}} \|V(Y|Z) P_{Z,i}^{*} - W(Y|X)\|_{1} - \max_{P_{Z,i}^{*}} \|\Delta V(Y|Z) P_{Z,i}^{*}\|_{1}$$
$$= \rho - \max_{P_{Z,i}^{*}} \|\Delta V(Y|Z) P_{Z,i}^{*}\|_{1} \tag{m}$$
$$\geq \rho - |\mathcal{Y}| \delta$$
$$> 0,$$

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

REFERENCES


