Strongly Secure Multiuser Communication and Authentication With Anonymity Constraints

Rémi A. Chou, *Member, IEEE*, and Aylin Yener, *Fellow, IEEE*

***Abstract*— We consider authentication of messages sent from transmitters to a receiver over a multiple access channel, where each transmitter shares a secret key with the legitimate receiver. Additionally, there exists a computationally unbounded opponent who has access to noisy observations of the messages transmitted and can initiate impersonation or substitution attacks. We require that the legitimate receiver must be able to authenticate the messages he receives with respect to predetermined groups of transmitters, but at the same time must be kept ignorant of the transmitter's identity of a given message in a given group. We propose an information-theoretic formulation of these anonymity constraints as well as an authentication coding scheme for which the asymptotic probability of successful attack is shown to optimally scale with the length of the secret keys shared between each transmitter and the legitimate receiver. Our results quantify the positive impact of the multiple access setting compared to the single-user setting on the probability of successful attack.**

***Index Terms*— Authentication, anonymity, impersonation attack, substitution attack, multiple access wiretap channel.**

I. Introduction

AUTHENTICATION aims at preventing the receiver of a message from being deceived by a falsely claimed authorship of the message. Early work by Simmons [2] considers a transmitter T and a receiver R, which are the legitimate users, an opponent, whose computational power is unbounded, and the following model for the authentication problem. The transmitter T wishes to send $M' = f(K, M)$ to the receiver R over a noiseless channel, where f is an encoding function, K is a secret key shared with R, and M is a message. f is designed such that R is able to recover M from (M', K). However, R could receive $\widetilde{M}$, a modified version of M', if an opponent performs a *substitution attack*, i.e., intercepts M' and sends $\widetilde{M}$ to R. The substitution attack is successful if R decodes $\widetilde{M}$ in $\widehat{M} \neq M$ and decides that $\widehat{M}$ has been authored by T. R could also be subject to an *impersonation attack*, for which the opponent generates and sends to R a message M'' before T initiates any communication. The impersonation attack is successful if R decides that the message he decodes has been authored by T. P_I and P_S, the probabilities of successful impersonation and substitution attacks, respectively, are lower bounded in function of the size of the secret key K shared by the legitimate users in [2], specifically, $P_I \geqslant 2^{-I(K;M)}$ and $P_S \geqslant 2^{-H(K|M)}$. A review of subsequent works related to this model can be found in [3], [4], as well as [5], in which a simplified and unified proof of several results via hypothesis testing is proposed.

While the model described above considers authentication over noiseless channels, several more recent works have studied authentication over noisy channels, including [6]–[11], see also [12] for a review. The closest counterpart to Simmons' noiseless authentication model described above is [11]. Instead of decoupling the problem of authentication over noisy channel to channel coding and authentication over noiseless channel, which has been shown to be detrimental in general [8], [9], reference [11] has proposed combining these two tasks to take *advantage* of the channel noise. Specifically, [11] has provided the lower bound $\max(P_I, P_S) \geqslant 2^{-H(K)}$, as well as an asymptotically matching upper bound for a coding scheme based on wiretap codes for strong secrecy [13].

In this paper, we build upon the premise of taking advantage of the physical channel for providing information-theoretic security and consider multiuser authentication with anonymity constraints. In particular, we consider an authentication problem for *multiple legitimate transmitters* who wish to communicate *strongly secure* messages to a legitimate receiver over a multiple access channel in the presence of an opponent. As in [2], [5], [11], we consider impersonation and substitution attacks by the opponent. Additionally, we enforce *anonymity constraints* which protect the identity of the individual transmitters with respect to a predefined transmitter group structure while simultaneously allowing the legitimate receiver to authenticate the integrity of the messages sent through the multiple access channel. A precise problem statement will be provided in the next section, however, we can already provide three motivating examples for transmitter group structures that will be covered by our model.

1) *Multiuser authentication in one-to-one correspondence*: Consider the case of a base station that receives signals from a number of legitimate cellular users and wishes to authenticate each signal individually. In this case, each group has one member and no anonymity is desired.

Manuscript received January 14, 2018; revised April 22, 2019; accepted September 1, 2019. Date of publication October 8, 2019; date of current version December 23, 2019. This work was supported in part by NSF under Grant CIF-1319338 and Grant CNS-1314719. This article was presented in part at the 2016 IEEE International Symposium on Information Theory (ISIT).

R. A. Chou is with the Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS 67260 USA (e-mail: remi.chou@wichita.edu).

A. Yener is with the Department of Electrical Engineering, Pennsylvania State University, University Park, PA 16802 USA (e-mail: yener@ee.psu.edu).

Communicated by A. Khisti, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2019.2946252

2) *Multiuser authentication with complete anonymity*: Consider the case of a legitimate receiver who must validate the group of transmitters for the messages he decodes but should be kept uninformed of the identity of the transmitter of a particular message. This case could correspond, for instance, to a secret ballot, or an anonymous review among a set of known reviewers.
3) *Multiuser authentication with group anonymity*: Consider several groups of people involved in clinical trials. Assume that each group is assigned a different drug. At the end of the trial, each participant submits a report of his/her experience to the principal investigator. Upon receiving all the reports, the latter must identify the group $\mathcal{G}$ associated with a particular report but the identity of the person who wrote the report should be kept anonymous among the group $\mathcal{G}$.

The contributions of this paper are fourfold. (i) We propose a metric to assess anonymity in multiuser authentication over noisy channels. (ii) We provide an authentication scheme relying on multiple access wiretap channel codes for strong secrecy, and prove that its probability of successful attack *optimality* scales with the length of the secret keys shared by the legitimate users. (iii) We quantify the impact of anonymity constraints on the probability of successful attack. (iv) We quantify the impact of the multi-transmitter setting on the probability of successful attack compared to the single-user case in [11]. Preliminary results were presented in [1].

The remainder of the paper is organized as follows. We describe the model under consideration in Section II. We propose a coding scheme in Section III. We derive a lower bound on the probability of successful attack, valid for any authentication scheme, in Section IV. We derive in Section V an upper bound on the probability of successful attack for the coding scheme of Section III. We summarize our main results in Section VI. We end the paper with concluding remarks in Section VII.

Notation: Throughout the paper, let $[\![a,b]\!] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}$, and let $\mathbb{1}\{\omega\}$ denote the indicator function, which is equal to 1 if the predicate ω is true and 0 otherwise. Define $[x]^+ \triangleq \max(0,x)$ for any $x \in \mathbb{R}$. Let $\mathbb{R}_+ \triangleq \{x \in \mathbb{R} : x > 0\}$ be the set of strictly positive real numbers. Unless specified otherwise, capital letters designate random variables, whereas lowercase letters designate realizations of associated random variables, e.g., x is a realization of the random variable X. For two sequences of bits l_1 and l_2, let $l_1 \| l_2$ denote the concatenation of l_1 and l_2. Given a sequence of t sequences of bits $(l_i)_{i \in [\![1,t]\!]}$, let $\|_{i \in [\![1,t]\!]} l_i$ denote $l_1 \| l_2 \| \dots \| l_t$. Finally, for any finite set $\mathcal{S}$, we denote the symmetric group on $\mathcal{S}$ by $\mathfrak{S}(\mathcal{S})$.

II. Problem Statement

A. Model Constituents

We first describe the principal constituents of our model depicted in Figure 1.

Parties. Consider a set $\mathcal{L} \triangleq [\![1,L]\!]$ of $L \in \mathbb{N}^*$ transmitters, a legitimate receiver, and an opponent. The transmitters form groups according to a partition $\mathcal{P} \triangleq \{\mathcal{G}_q : q \in \mathcal{Q}\}$ of $\mathcal{L}$, where

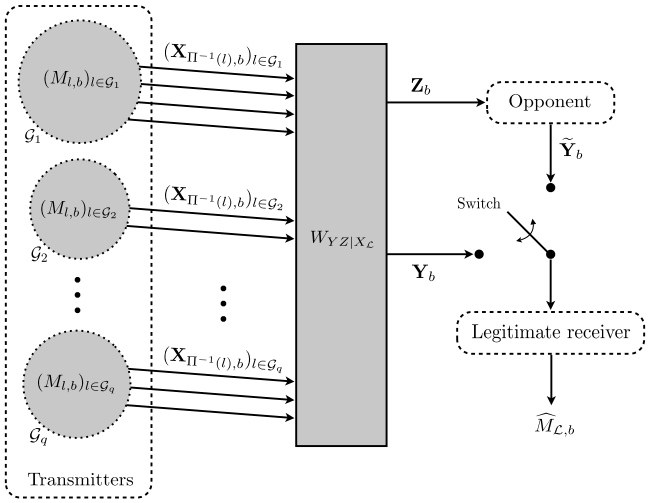

Fig. 1. Multiuser authentication with anonymity constraints: The L transmitters are grouped according to the partition $\mathcal{P} \triangleq \{\mathcal{G}_q\}_{q\in\mathcal{Q}}$ of $\mathcal{L}$, so that anonymity of transmitters among each group must be preserved. The switch models a potential attack initiated by the opponent in Block $b \in \mathcal{B}$. When the switch is connected to $\mathbf{Y}_b$ there is no attack, whereas when the switch is connected to $\widetilde{\mathbf{Y}}_b$, there is an impersonation attack or a substitution attack, depending on whether or not the transmitters are silent.

$\mathcal{Q} \triangleq [\![1,Q]\!]$, $Q \in \mathbb{N}^*$, i.e., $\forall q_1 \in \mathcal{Q}, \forall q_2 \in \mathcal{Q}\backslash\{q_1\}, \mathcal{G}_{q_1} \neq \emptyset, \mathcal{G}_{q_1} \cap \mathcal{G}_{q_2} = \emptyset$, and $\bigcup_{q\in\mathcal{Q}} \mathcal{G}_q = \mathcal{L}$. The partition $\mathcal{P}$ is known to all parties. Additionally, we define $\mathcal{C} \triangleq \{|\mathcal{G}_q| : q \in \mathcal{Q}\}$ as the set of lengths taken by the parts of $\mathcal{P}$. For convenience, we define $(c_d)_{d\in\mathcal{D}}$ as the sorted (in increasing order) sequence of the elements of $\mathcal{C}$, where $\mathcal{D} \triangleq [\![1,D]\!]$ with $D \triangleq |\mathcal{C}|$. We also define for $d \in \mathcal{D}$, n_d as the number of parts of $\mathcal{P}$ with length c_d. We thus have $\sum_{d\in\mathcal{D}} n_d c_d = L$ and $\sum_{d\in\mathcal{D}} n_d = Q$. For instance, if $L = 6$ and $\mathcal{P} = \{\{1\},\{2\},\{3\},\{4,5,6\}\}$, then $Q = 4$, $D = 2$, $c_1 = 1$, $c_2 = 3$, $n_1 = 3$, $n_2 = 1$.

Communication Channel. We consider a discrete memoryless multiple access channel $\left(\mathcal{X}_\mathcal{L}, W_{YZ|X_\mathcal{L}}, \mathcal{Y}\times\mathcal{Z}\right)$, where $\mathcal{X}_\mathcal{L}$, $\mathcal{Y}$, and $\mathcal{Z}$ are finite alphabets and $X_\mathcal{L} \triangleq (X_l)_{l\in\mathcal{L}}$. To model the absence of a priori knowledge of the legitimate receiver about how the transmitters are associated with the different inputs of the channel, we introduce a permutation Π chosen uniformly at random over $\mathfrak{S}(\mathcal{L})$ such that Input $l \in \mathcal{L}$ of the channel is used by Transmitter $\Pi(l)$. For instance, when $L = 3$, if Π is defined by $(\Pi(1),\Pi(2),\Pi(3)) \triangleq (3,1,2)$, then Input 1 is used by Transmitter 3, Input 2 is used by Transmitter 1, and Input 3 is used by Transmitter 2. Π is assumed fixed for the entire communication protocol, and *unknown* to the legitimate receiver and the opponent. Assume that the transmission over the channel is over $B \in \mathbb{N}^*$ blocks and define $\mathcal{B} \triangleq [\![1,B]\!]$. For $b \in \mathcal{B}$, let $\mathbf{Y}_b$ and $\mathbf{Z}_b$ denote the observations of the legitimate receiver and the opponent in Block b, respectively, when $\mathbf{X}_{\mathcal{L},b} \triangleq (\mathbf{X}_{l,b})_{l\in\mathcal{L}}$ is the input of the channel with $\mathbf{X}_{l,b}$ a codeword of length N emitted by Transmitter $\Pi(l) \in \mathcal{L}$. We also define $\mathbf{X}_\mathcal{L}^B \triangleq (\mathbf{X}_{\mathcal{L},b})_{b\in\mathcal{B}}$, $\mathbf{Y}^B \triangleq (\mathbf{Y}_b)_{b\in\mathcal{B}}$, and $\mathbf{Z}^B \triangleq (\mathbf{Z}_b)_{b\in\mathcal{B}}$.

Secret keys. For the purpose of authentication, we assume that the legitimate receiver and each transmitter share a

secret key uniformly distributed over the same alphabet $\mathcal{K} = \{0,1\}^{\log|\mathcal{K}|}$, where the logarithm is base 2 and $|\mathcal{K}|$ is a power of 2. Let K_l denote the key shared between Transmitter $l \in \mathcal{L}$ and the legitimate receiver, and define $K_{\mathcal{L}} \triangleq (K_l)_{l\in\mathcal{L}}$. The keys K_l's are assumed mutually independent, i.e., their joint probability distribution factorizes as $p_{K_{\mathcal{L}}} = \prod_{l\in\mathcal{L}} p_{K_l}$, and private in the sense that Transmitter l does not share K_l with any other transmitter.

Remark 1. *If the transmitters share with the legitimate receiver private keys that do not have the same length, then the transmitters can truncate their keys to the length of the smallest key.*

B. Definition of an authentication protocol

We describe in Section II-B.1 a generic scheme for authentication. We describe in Section II-B.2 the impersonation and substitution attacks to which an authentication scheme can be subject. We describe and motivate in Section II-B.3 the requirements we propose for an authentication scheme. We also show in Section II-B.3 that our model subsumes the model in [11].

1) We first introduce a general definition for authentication schemes and describe how it operates:

Definition 1. *Let $L, N, B, Q \in \mathbb{N}^*$. Let $\mathcal{P} \triangleq \{\mathcal{G}_q\}_{q\in\mathcal{Q}}$ be a partition of $\mathcal{L}$. Define the sequences $\mathcal{R}_{\mathcal{L}} \triangleq \left(R_l^{(S)}\right)_{l\in\mathcal{L}}$, $\mathcal{R}_{\mathcal{Q}} \triangleq (R_q)_{q\in\mathcal{Q}}$, and the sequence $\mathcal{T} \triangleq (\tau_b)_{b\in\mathcal{B}} \in \mathcal{Q}^B$. An $(L, N, B, \mathcal{K}, \mathcal{R}_{\mathcal{L}}, \mathcal{R}_{\mathcal{Q}}, \mathcal{P}, \mathcal{T})$ authentication scheme for a discrete memoryless multiple access channel $(\mathcal{X}^L, W_{YZ|X_{\mathcal{L}}}, \mathcal{Y}\times\mathcal{Z})$ consists of*

- *B communication blocks of length N.*
- *For $q \in \mathcal{Q}$, a message set $\mathcal{M}_q \triangleq [\![1, 2^{NR_q}]\!]$.*
- *For $q \in \mathcal{Q}$, an alphabet $\mathcal{F}_q$ and a function $\upsilon_q : \mathcal{K}^{|\mathcal{G}_q|} \to \mathcal{F}_q$, which maps $K_{\mathcal{G}_q} \triangleq (K_l)_{l\in\mathcal{G}_q}$ to $F_q \in \mathcal{F}_q$. In the following, we refer to F_q as the authentication sequence for the group $\mathcal{G}_q$.*
- *For each transmitter $l \in \mathcal{L}$,*
  - *(i) a private key $K_l \in \mathcal{K}$ shared with the legitimate receiver as described in Section II-A;*
  - *(ii) a message set $\mathcal{M}_l^{(S)} \triangleq [\![1, 2^{NR_l^{(S)}}]\!]$. $M_{l,b} \in \mathcal{M}_l^{(S)}$ denotes the message that Transmitter l wishes to secretly communicate to the legitimate receiver over Block $b \in \mathcal{B} \triangleq [\![1, B]\!]$, i.e., $M_{l,b}$ must be kept secret from the opponent. We make the assumption that the messages $(M_{l,b})_{l\in\mathcal{L}}$ are mutually independent in each block $b \in \mathcal{B}$. Let $M_{\mathcal{L},b} \triangleq (M_{l,b})_{l\in\mathcal{L}}$ denote all the messages sent over Block b, and define $M_{\mathcal{L}}^B \triangleq (M_{\mathcal{L},b})_{b\in\mathcal{B}}$.*
  - *(iii) an encoder $h_l : \mathcal{K}\times\mathcal{M}_l^{(S)}\times\mathcal{M}_q \to \mathcal{X}^N_{\Pi^{-1}(l)}$, where q is such that $l \in \mathcal{G}_q$.*
- *A decoder $g : \mathcal{Y}^N \to \bigtimes_{l\in\mathcal{L}} \mathcal{M}_l^{(S)}$ that maps for any $b \in \mathcal{B}$, $\mathbf{Y}_b$ to an estimate $\widehat{M}_{\mathcal{L},b}$ of $M_{\mathcal{L},b}$.*
- *For $q \in \mathcal{Q}$, a decision function $d_q : \mathcal{Y}^N \times \mathcal{F}_q \to \{0,1\}$, which maps for any $b \in \mathcal{B}$, $(\mathbf{Y}_b, F_q)$ to $D_q \in \{0,1\}$. If the receiver has recovered the messages sent by the transmitters in $\mathcal{G}_q$ and decides that the messages come from the transmitters in $\mathcal{G}_q$ then $D_q = 1$, otherwise $D_q = 0$. Note that d_q describes how this decision is made by the receiver, and that it is left unspecified in this definition in all generality. We provide examples for the decision functions $(d_q)_{q\in\mathcal{Q}}$ in Examples 1 and 5 in Section II-B.3.*

An $(L, N, B, \mathcal{K}, \mathcal{R}_{\mathcal{L}}, \mathcal{R}_{\mathcal{Q}}, \mathcal{P}, \mathcal{T})$ authentication scheme for a discrete memoryless multiple access channel $(\mathcal{X}^L, W_{YZ|X_{\mathcal{L}}}, \mathcal{Y}\times\mathcal{Z})$ operates as follows.

- For $q \in \mathcal{Q}$, transmitters in $\mathcal{G}_q$ communicate over a noiseless private channel that all the transmitters in $\mathcal{G}_q$ can have access to. The overall information communicated over this channel is denoted by M_q and its rate by R_q. At the end of the communication, the individual keys of the transmitters must still be private as explained in Section II-A.

  Remark 2. *It is unclear at this point whether this extra communication among the members of a group is necessary. We will later discuss why R_q should be strictly positive in general. We will also show that R_q can be chosen vanishing to zero as $N \to \infty$.*

- For $b \in \mathcal{B}$, Transmitter $l \in \mathcal{L}$ encodes his messages $M_{l,b}$, uniformly distributed over $\mathcal{M}_l^{(S)}$ as $h_l\left(K_l, M_{l,b}, M_q\right)$, where q is such that $l \in \mathcal{G}_q$, and send the resulting codeword $\mathbf{X}_{\Pi^{-1}(l),b}$ over the channel in Block b, i.e., Transmitter l uses Input $\Pi^{-1}(l)$ of the multiple access channel as described in Section II-A. We also assume that $(M_{\mathcal{L}}^B, (M_q)_{q\in\mathcal{Q}})$ is independent of Π.
- For $b \in \mathcal{B}$, upon observing $\mathbf{Y}_b$ in Block b, the legitimate receiver computes $\widehat{M}_{\mathcal{L},b}$ with decoder g. The legitimate receiver decides then whether to authenticate the messages or not in the following manner. Let $\lambda \triangleq \sum_{q\in\mathcal{Q}} \mathbb{1}\{D_q\}$. If $\lambda < \tau_b$, then the legitimate receiver refuses all the messages. If $\lambda \geqslant \tau_b$, then the legitimate receiver accepts all the messages from $\mathcal{G}_q$, where $q \in \mathcal{Q}$ is such that $D_q = 1$, as authentic, and refuses all the other messages.

  Remark 3. *If one chooses $\tau_b = Q$, $b \in \mathcal{B}$, then either the legitimate receiver authenticates all the received messages or none of them. If one choose $\tau_b < Q$, $b \in \mathcal{B}$, then one allows the legitimate receiver to authenticate some messages and reject others in a given block. Hence, the potential advantage of choosing $\tau_b < Q$ is to avoid a waste of bandwidth. The choice of τ_b, $b \in \mathcal{B}$, and its relationship with the probability of a successful attack is further discussed in Section II-B.3, where we describe the requirements for the authentication scheme.*

2) We next describe the attack model: The opponent can choose an arbitrary block index $b \in \mathcal{B}$ and initiate one of the following. Note that without loss of generality [11], we assume the channel between the opponent and the legitimate receiver to be noiseless.

- **Impersonation attack**: The opponent sends $\widetilde{\mathbf{Y}}_b$ to the receiver when the transmitters are silent, and where $\widetilde{\mathbf{Y}}_b$ is

a function of all observations of the opponent, i.e, $\mathbf{Z}^{b-1} \triangleq (\mathbf{Z}_i)_{i\in[\![1,b-1]\!]}$.

- **Substitution attack**: The opponent blocks the transmission of the b-th block between the transmitters and the legitimate receiver while observing $\mathbf{Z}_b$. The opponent then sends $\widetilde{\mathbf{Y}}_b$, to the legitimate receiver, where $\widetilde{\mathbf{Y}}_b$ is a function of all observations of the opponent, i.e, $\mathbf{Z}^b \triangleq (\mathbf{Z}_i)_{i\in[\![1,b]\!]}$.

An impersonation or a substitution attack is successful if $\lambda \geqslant \tau_b$, where λ is defined in Section II-B.1, and if there exists $q_0 \in \mathcal{Q}$ such that $D_{q_0} = 1$ and the messages decoded by the legitimate receiver associated with $\mathcal{G}_{q_0}$ differ from the messages sent by $\mathcal{G}_{q_0}$. We denote the probability of a successful impersonation and the probability of a successful substitution attack in Block b by $P_{I,b}(\tau_b)$ and $P_{S,b}(\tau_b)$, respectively. For any $(L, N, B, \mathcal{K}, \mathcal{R}_\mathcal{L}, \mathcal{R}_\mathcal{Q}, \mathcal{P}, \mathcal{T})$ authentication scheme $\mathcal{S}_N$, we define the probability of a successful attack by the opponent as

$$P_A(\mathcal{S}_N) \triangleq \max_{b\in\mathcal{B}} \max\left(P_{I,b}(\tau_b), P_{S,b}(\tau_b)\right). \tag{1}$$

3) We now introduce the requirements for an authentication scheme as described in Section II-B.1 under the attack model desribed in Section II-B.2: A sequence $(\mathcal{S}_N)_{N\in\mathbb{N}}$ of $(L, N, B, \mathcal{K}, \mathcal{R}_\mathcal{L}, \mathcal{R}_\mathcal{Q}, \mathcal{P}, \mathcal{T})$ authentication schemes must satisfy the following constraints.

- **Reliability**: $M_\mathcal{L}^B$ must be reconstructed reliably by the legitimate receiver, i.e.,

$$\lim_{N\to\infty} \mathbb{P}\left[\widehat{M}_\mathcal{L}^B \neq M_\mathcal{L}^B | \{\text{Absence of attack}\}\right] = 0, \tag{2}$$

  where $\widehat{M}_\mathcal{L}^B$ denotes the estimate of $M_\mathcal{L}^B$.
- **Strong Secrecy**: $M_\mathcal{L}^B$ must be kept secret from the opponent in the sense that

$$\lim_{N\to\infty} I\left(M_\mathcal{L}^B; \mathbf{Z}^B\right) = 0. \tag{3}$$

- **Anonymity**: For all $b \in \mathcal{B}$, for all $q \in \mathcal{Q}$, we require anonymity of the transmitters in the group $\mathcal{G}_q$, i.e., for any $l \in \mathcal{L}$, the legitimate receiver can determine from which group of transmitters $\mathcal{G}_q$, the message $\widehat{M}_{l,b}$ has been sent but must not be able to determine from which transmitter in $\mathcal{G}_q$, $\widehat{M}_{l,b}$ has been sent. We formalize the requirement as follows.
  For $q \in \mathcal{Q}$, define the restriction of Π to $\mathcal{G}_q$ as Π_q, define Im_q as the image of Π_q, and let $\mathfrak{S}(\mathcal{G}_q, \mathrm{Im}_q)$ be the set of all bijections from $\mathcal{G}_q$ to Im_q. While the sets Im_q can be determined by the decoder for all $q \in \mathcal{Q}$, the anonymity constraint is written as
  $\forall N, B \in \mathbb{N}^*, \forall \mathbf{y}^B \in \mathcal{Y}^{NB}, \forall q \in \mathcal{Q}, \forall \sigma \in \mathfrak{S}(\mathcal{G}_q, \mathrm{Im}_q)$,

$$\mathbb{P}\left[\Pi_q = \sigma | \mathbf{Y}^B = \mathbf{y}^B\right] = \frac{1}{|\mathcal{G}_q|!}. \tag{4}$$

- **Attack Resilience**: The asymptotic probability of a successful attack by the opponent $\lim_{N\to\infty} P_A(\mathcal{S}_N)$ should be arbitrarily small for sufficiently long keys, i.e., we require

$$\lim_{|\mathcal{K}|\to\infty} \lim_{N\to\infty} P_A(\mathcal{S}_N) = 0. \tag{5}$$

Remark 4. *This requirement raises several questions. Is there an authentication scheme that meets this constraint? Is it possible to determine a convergence rate for* $\lim_{|\mathcal{K}|\to\infty} \lim_{N\to\infty} P_A(\mathcal{S}_N) = 0$ *in function of* $|\mathcal{K}|$*? Is it possible to determine an optimal convergence rate for* $\lim_{|\mathcal{K}|\to\infty} \lim_{N\to\infty} P_A(\mathcal{S}_N) = 0$ *in function of* $|\mathcal{K}|$*, over all the possible sequences* $(\mathcal{S}_N)_{N\in\mathbb{N}}$ *of* $(L, N, B, \mathcal{K}, \mathcal{R}_\mathcal{L}, \mathcal{R}_\mathcal{Q}, \mathcal{P}, \mathcal{T})$ *authentication schemes? What particular choices for* F_q *and* d_q*,* $q \in \mathcal{Q}$*, would allow achievability of this optimal convergence rate? How does the choice of the sequence of thresholds* $\mathcal{T}$ *influence the probability of successful attack? The goal of our study is to address these questions.*

We now provide some settings covered by our model.

Example 1 (Single-user authentication [11])**.** *Choose* $L = Q = 1$*, for all* $b \in \mathcal{B}$*,* $\tau_b = Q$*, and* $\mathcal{R}_\mathcal{Q} = \emptyset$*. Note that the anonymity constraint is irrelevant since* $L = 1$*. This case recovers the setting in [11]. Moreover, the authors in [11] choose in Definition 1,* $F_1 = K_1$ *and choose the decision rule* d_1 *such that* $d_1 = 1$ *if* F_1 *is present at the beginning of the decoded message, and* $d_1 = 0$ *otherwise. It is also proved in [11] that there exists a sequence* $(\mathcal{S}_N)_{N\in\mathbb{N}}$ *of authentication schemes such that the probability of successful attack satisfies* $\lim_{N\to\infty} P_A(\mathcal{S}_N) \overset{|\mathcal{K}|\to\infty}{\sim} \frac{1}{|\mathcal{K}|}$*, and that this convergence rate is optimal over all possible sequences of authentication schemes. This result will be recovered by our results.*

Example 2 (Multiuser authentication in one-to-one correspondence)**.** *Consider a partition* $\mathcal{P}$ *of* $\mathcal{L}$ *with* $Q = L$*, i.e.,* $\mathcal{P}$ *is the set of singletons* $\{\{l\} : l \in \mathcal{L}\}$*. In this case, there is no anonymity constraint, i.e., the legitimate receiver must find a bijection between the* L *decoded messages and the* L *transmitters. This case could corresponds to Point 1 described in the introduction.*

Example 3 (Multiuser authentication with complete anonymity)**.** *Consider a partition* $\mathcal{P}$ *of* $\mathcal{L}$ *with* $Q = 1$*, i.e.,* $\mathcal{P}$ *is the singleton* $\{\mathcal{L}\}$*. In this case, the legitimate receiver must authenticate the group of transmitters as* $\mathcal{L}$ *for the* L *decoded messages but should be kept uninformed of the identity of the transmitter of a particular message. This case is illustrated by Point 2 in the introduction.*

Example 4 (Multiuser authentication with group anonymity)**.** *Consider a partition* $\mathcal{P}$ *of* $\mathcal{L}$ *with* $Q \in [\![2, L-1]\!]$*. This case could corresponds to Point 3 in the introduction, where the partition of* $\mathcal{L}$ *represents the different groups of people.*

We now illustrate with a simple coding scheme our model.

Example 5. *Consider* $L = 2$*,* $B = 1$*,* $Q = 1$*,* $\mathcal{P} = \{\{1, 2\}\}$*. Define* $F_1 \triangleq K_1 \oplus K_2$*, note that* F_1 *is known at the receiver. Assume that Transmitter* l*,* $l \in \mathcal{L}$*, draws* R_l *a sequence of uniformly distributed bits over* $\mathcal{K}$*, and sends* $R_l \oplus K_l$ *to the other transmitter over their private noiseless channel. Hence, by doing these one-time pads the transmitters do not disclose their keys to each other - see Lemma 6 in Appendix A. The transmitters also exchange a random bit* C

over their private channel such that C is unknown to the legitimate receiver. Define $(H_1||H_2) \triangleq K_1 \oplus K_2 \oplus R_1 \oplus R_2$, where $|H_1| = |H_2|$ and $||$ denotes concatenation (for simplicity, we assume in this example that the length of the keys is even). Then, Transmitter $l \in \{1,2\}$ encodes $(\bar{H}_l(C), R_l, M_l)$ and sends the result $\mathbf{X}_{\Pi^{-1}(l)}$ over the channel, where $\bar{H}_l(C) \triangleq H_l$ if $C = 1$ and $\bar{H}_l(C) \triangleq H_{3-l}$ if $C = 0$. We assume that the transmitters use a code for multiple access wiretap channels [14], which ensures that reliability and secrecy hold. Upon observing the channel output $\mathbf{Y}$, the legitimate receiver can compute an estimate of the pair $\left((M_i, R_i, \bar{H}_i(C))\right)_{i\in\{1,2\}}$ (without knowing how to map the elements of the pair to the indices 1 and 2), and can compute an estimate of the pair $((\bar{H}_1(C)||\bar{H}_2(C)) \oplus R_1 \oplus R_2, (\bar{H}_2(C)||\bar{H}_1(C)) \oplus R_1 \oplus R_2)$. The decision rule d_1 to authenticate the messages is then the following: if either the estimate of $(\bar{H}_1(C)||\bar{H}_2(C)) \oplus R_1 \oplus R_2$ or the estimate of $(\bar{H}_2(C)||\bar{H}_1(C)) \oplus R_1 \oplus R_2$ is equal to F_1, then accept the estimates of the messages M_1, M_2 as authentic, otherwise reject all the messages. By construction, for any $\sigma \in \mathfrak{S}(\mathcal{L})$, for any $\mathbf{y}$, $\mathbb{P}[\Pi = \sigma|\mathbf{Y} = \mathbf{y}] = \mathbb{P}[C = 1] = \mathbb{P}[C = 0] = 1/2$, i.e., the anonymity constraint is satisfied.

Note that this simple coding scheme raises many questions that our study will address. What is the probability of successful attack by an opponent for this scheme and how does it scale with $|\mathcal{K}|$? What is the optimal scaling with $|\mathcal{K}|$ of the probability of successful attack for this setting? Is the private channel between the trasmitters necessary? Is the choice of F_1 optimal in terms probability of successful attack? Is the decision rule d_1 optimal in terms of probability of successful attack?

Remark 5. *As illustrated in Example 5, note that the legitimate receiver cannot authenticate a strict subset of messages from a given group $\mathcal{G}_q$, $q \in \mathcal{Q}$. Indeed, by the anonymity requirement, the receiver could not know which messages have not been correctly authenticated for the group $\mathcal{G}_q$.*

Remark 6. *Our setting only considers partitions of $\mathcal{L}$ for the purpose of anonymity. The reason is the following. Consider three transmitters that form two overlapping groups, for instance, $\mathcal{G}_1 \triangleq \{1,2\}$ and $\mathcal{G}_2 \triangleq \{2,3\}$, such that anonymity should be preserved in $\mathcal{G}_1$ and $\mathcal{G}_2$. Assume that the legitimate receiver estimates the messages sent by the transmitters as I, J, K, and decides (correctly) that (I, J) are the messages coming from $\mathcal{G}_1$, and that (J, K) are the messages coming from $\mathcal{G}_2$. The receiver can then deduce that Transmitter 2 has sent J, Transmitter 1 has sent I, and Transmitter 3 has sent K, and no anonymity is possible for the transmitters.*

Section III is dedicated to the design of a coding scheme that meets the objectives described in this section.

III. Coding Scheme Design

In Section III-A, we provide guidelines for the design of authentication schemes as defined in Section II-B. In Section III-B, we construct an authentication scheme in light of Section III-A.

A. Design guidelines

Observe that the authentication scheme design should aim at maximizing $H(F_q)$, for all $q \in \mathcal{Q}$, to make an attack more difficult to succeed. Indeed, the probability of a successful attack by an opponent is lower bounded by the probability of the opponent correctly guessing F_q, $q \in \mathcal{Q}$ at random, which, ideally, we would also like to be the best possible strategy for the opponent. Since F_q is a function of $K_{\mathcal{G}_q}$, we could potentially choose F_q such that $H(F_q) = H(K_{\mathcal{G}_q})$, however, it raises the question of whether such a choice is compatible with the other requirements described in Section II-B. This question is addressed in this section. We also determine in this section that the communication rates R_q, $q \in \mathcal{Q}$, in Definition 1, must be strictly positive in general.

Specifically, we first show that any authentication scheme as defined in Section II-B must satisfy Property 1 to minimize the probability of a successful attack by an opponent. We then provide in Lemma 1 a necessary condition to ensure the anonymity requirement (4). We develop consequences of Lemma 1 in Lemma 2, which provides an upper-bound on $H(F_q)$, $q \in \mathcal{Q}$, and in Lemma 3, which shows that the communication rates R_q, $q \in \mathcal{Q}$, in Definition 1, must be strictly positive in general.

Property 1. *To minimize the probability of a successful attack by an opponent, an authentication scheme, as defined in Section II-B, must be such that in the absence of attack*

$$\forall b \in \mathcal{B}, \forall q \in \mathcal{Q}, I(\mathbf{Y}_b; F_q) = H(F_q). \tag{6}$$

Indeed, for any authentication scheme, there exists a strategy for the opponent to successfully attack the messages associated with the group of transmitters $\mathcal{G}_q$ with probability at least $2^{-I(\mathbf{Y}_b;F_q)}$, which is minimized when (6) holds to yield the probability of successfully guessing F_q at random, i.e., $2^{-H(F_q)}$.

Proof: The proof is an application of [5, Section IV]. Assume that the opponent forms a fraudulent signal $\widetilde{\mathbf{Y}}_b$ according to the distribution $p_{\widetilde{\mathbf{Y}}_b} \triangleq p_{\mathbf{Y}_b}$. Note that $p_{\mathbf{Y}_b}$ is known to the opponent because it is independent of the specific key $K_{\mathcal{L}}$ shared by the legitimate users. Upon observing $\widetilde{\mathbf{Y}}_b$, when the legitimate receiver authenticates the messages associated with $\mathcal{G}_q$, $q \in \mathcal{Q}$, he has to decide whether $\widetilde{\mathbf{Y}}_b$ has been generated from $p_{F_q\mathbf{Y}_b}$ (Hypothesis H_0), or from $p_{F_q}p_{\widetilde{\mathbf{Y}}_b}$, (Hypothesis H_1). The probability that the legitimate receiver accepts the messages in $\mathcal{G}_q$, i.e., the probability of accepting Hypothesis H_0 whereas Hypothesis H_1 holds, is lower bounded by [5, Lemma 1], $2^{-\mathbb{D}\left(p_{F_q\mathbf{Y}_b}\middle\|p_{F_q}p_{\widetilde{\mathbf{Y}}_b}\right)} = 2^{-I(\mathbf{Y}_b;F_q)}$, where $\mathbb{D}(\cdot||\cdot)$ denotes the Kullback-Leibler divergence. ∎

In light of Property 1, in the remainder of this section, we will consider authentication schemes as defined in Section II-B that in addition satisfy in the absence of attack

$$I(\mathbf{Y}_b; F_q) = H(F_q), \tag{7}$$

for all $b \in \mathcal{B}$, for all $q \in \mathcal{Q}$.

We now provide a necessary condition to ensure the anonymity requirement (4) that we will use to derive an upper-bound on $H(F_q)$, $q \in \mathcal{Q}$, in Lemma 2.

Lemma 1. *If the anonymity requirement* (4) *holds, then*

$$\forall N, B \in \mathbb{N}^*, \forall q \in \mathcal{Q}, \quad \max_{\substack{\mathcal{G}\subset\mathcal{G}_q \\ \text{s.t. } |\mathcal{G}|=|\mathcal{G}_q|-1}} I\left(\mathbf{Y}^B; K_{\mathcal{G}}\right) = 0. \quad (8)$$

Proof: By contradiction, assume that (8) does not hold, i.e., there exists $N \in \mathbb{N}^*$, $B \in \mathbb{N}^*$, $q \in \mathcal{Q}$, $\mathcal{G} \subset \mathcal{G}_q$ such that $|\mathcal{G}| = |\mathcal{G}_q| - 1$, and

$$I\left(\mathbf{Y}^B; K_{\mathcal{G}}\right) \neq 0. \quad (9)$$

For notation convenience, define $\mathcal{H} \triangleq \Pi^{-1}(\mathcal{G})$, $\mathcal{I} \triangleq \Pi^{-1}(\mathcal{G}_q)\backslash\Pi^{-1}(\mathcal{G})$, and $\mathcal{J} \triangleq \mathcal{L}\backslash\Pi^{-1}(\mathcal{G}_q)$ such that $\{\mathcal{H}, \mathcal{I}, \mathcal{J}\}$ forms a partition of $\mathcal{L}$. We have

$$\begin{aligned}
&I\left(\mathbf{X}_{\mathcal{H}}^B M_q \Pi; K_{\mathcal{G}}\right) \\
&= I\left(\mathbf{X}_{\mathcal{H}}^B M_q \Pi; K_{\mathcal{G}}\right) + I\left(K_{\mathcal{G}_q\backslash\mathcal{G}}; K_{\mathcal{G}} M_q\right) && (10a)\\
&= I\left(\mathbf{X}_{\mathcal{H}}^B M_q \Pi; K_{\mathcal{G}}\right) + I\left(K_{\mathcal{G}_q\backslash\mathcal{G}}; K_{\mathcal{G}} \mathbf{X}_{\mathcal{H}}^B M_q \Pi\right) && (10b)\\
&\geqslant I\left(\mathbf{X}_{\mathcal{H}}^B M_q \Pi; K_{\mathcal{G}}\right) + I\left(K_{\mathcal{G}_q\backslash\mathcal{G}}; K_{\mathcal{G}} | \mathbf{X}_{\mathcal{H}}^B M_q \Pi\right) && (10c)\\
&= I\left(\mathbf{X}_{\mathcal{H}}^B M_q \Pi K_{\mathcal{G}_q\backslash\mathcal{G}}; K_{\mathcal{G}}\right) && (10d)\\
&= I\left(\mathbf{X}_{\mathcal{L}}^B M_q \Pi K_{\mathcal{G}_q\backslash\mathcal{G}}; K_{\mathcal{G}}\right) - I\left(\mathbf{X}_{\mathcal{I}}^B; K_{\mathcal{G}} | \mathbf{X}_{\mathcal{H}}^B M_q \Pi K_{\mathcal{G}_q\backslash\mathcal{G}}\right) \\
&\quad - I\left(\mathbf{X}_{\mathcal{J}}^B; K_{\mathcal{G}} | \mathbf{X}_{\mathcal{H}\cup\mathcal{I}}^B M_q \Pi K_{\mathcal{G}_q\backslash\mathcal{G}}\right) && (10e)\\
&\geqslant I\left(\mathbf{X}_{\mathcal{L}}^B; K_{\mathcal{G}}\right) - I\left(\mathbf{X}_{\mathcal{I}}^B; K_{\mathcal{G}} | \mathbf{X}_{\mathcal{H}}^B M_q \Pi K_{\mathcal{G}_q\backslash\mathcal{G}}\right) \\
&\quad - I\left(\mathbf{X}_{\mathcal{J}}^B; K_{\mathcal{G}_q} \mathbf{X}_{\mathcal{H}\cup\mathcal{I}}^B M_q | \Pi\right) && (10f)\\
&= I\left(\mathbf{X}_{\mathcal{L}}^B; K_{\mathcal{G}}\right) - I\left(\mathbf{X}_{\mathcal{J}}^B; K_{\mathcal{G}_q} \mathbf{X}_{\mathcal{H}\cup\mathcal{I}}^B M_q | \Pi\right) && (10g)\\
&= I\left(\mathbf{X}_{\mathcal{L}}^B; K_{\mathcal{G}}\right) && (10h)\\
&\geqslant I\left(\mathbf{Y}^B; K_{\mathcal{G}}\right) && (10i)\\
&> 0, && (10j)
\end{aligned}$$

where (10a) holds because the keys of the transmitters in $\mathcal{G}_q\backslash\mathcal{G}$ must remain secret from the transmitters in $\mathcal{G}$ after the exchange of M_q, i.e., $I(K_{\mathcal{G}_q\backslash\mathcal{G}}; K_{\mathcal{G}} M_q) = 0$, (10b) holds because $K_{\mathcal{G}_q\backslash\mathcal{G}} - (M_q, K_{\mathcal{G}}) - (\mathbf{X}_{\mathcal{H}}^B, \Pi)$ forms a Markov chain, (10c), (10d), (10e), (10f) hold by the chain rule, (10g) holds because $\mathbf{X}_{\mathcal{I}}^B - (\mathbf{X}_{\mathcal{H}}^B, M_q, \Pi, K_{\mathcal{G}_q\backslash\mathcal{G}}) - K_{\mathcal{G}}$ forms a Markov chain, (10h) holds because $\mathbf{X}_{\mathcal{J}}^B - \Pi - (K_{\mathcal{G}_q}, \mathbf{X}_{\mathcal{H}\cup\mathcal{I}}^B, M_q)$ forms a Markov chain, (10i) holds by the data processing inequality, (10j) holds by (9).

Since $I\left(\mathbf{X}_{\mathcal{H}}^B M_q \Pi; K_{\mathcal{G}}\right)$ does not depend on the specific realization of Π, it can be assumed known to the legitimate receiver. Hence, by (10j), there exists $\mathcal{G}' \subset \mathcal{G}_q$ and $\mathcal{H}' \subset \Pi^{-1}(\mathcal{G}_q)$ such that $|\mathcal{H}'| = |\mathcal{G}'| = |\mathcal{G}_q| - 1$, and the legitimate receiver can determine that

$$I\left(\mathbf{X}_{\mathcal{H}'}^B M_q \Pi; K_{\mathcal{G}'}\right) > 0. \quad (11)$$

Then, note that there exists $a \in \mathcal{G}'$ such that $\Pi^{-1}(a) \in \mathcal{H}'$, otherwise $\Pi(\mathcal{H}') \cap \mathcal{G}' = \emptyset$, and

$$\begin{aligned}
I\left(\mathbf{X}_{\mathcal{H}'}^B M_q \Pi; K_{\mathcal{G}'}\right) &= I\left(\mathbf{X}_{\mathcal{H}'}^B \Pi; K_{\mathcal{G}'} | M_q\right) && (12a)\\
&= 0, && (12b)
\end{aligned}$$

where (12a) holds by the key privacy requirement, i.e., $I(M_q; K_{\mathcal{G}'}) = 0$, (12b) holds because $(\mathbf{X}_{\mathcal{H}'}^B, \Pi) - M_q - K_{\mathcal{G}'}$ forms a Markov chain when $\Pi(\mathcal{H}') \cap \mathcal{G}' = \emptyset$, and (12b) would contradict (11). Finally, since $\Pi^{-1}(a) \in \mathcal{H}'$, the anonymity requirement (4) is not satisfied because for any $\mathbf{y}^B \in \mathcal{Y}^{NB}$, $\mathbb{P}[\Pi_q = \sigma | \mathbf{Y}^B = \mathbf{y}^B] = 0$, where $\sigma \in \mathfrak{S}(\mathcal{G}_q, \mathrm{Im}_q)$ and is such that $\sigma^{-1}(a) \in \Pi^{-1}(\mathcal{G}_q)\backslash\mathcal{H}' \neq \emptyset$. ∎

Lemma 2. *For any authentication scheme, as defined in Section II-B, we have*

$$\forall q \in \mathcal{Q}, H(F_q) \leqslant \log|\mathcal{K}|. \quad (13)$$

Proof: Let $b \in \mathcal{B}$, let $q \in \mathcal{Q}$. We have

$$\begin{aligned}
&I(\mathbf{Y}_b; F_q) \\
&\leqslant I\left(\mathbf{Y}_b; K_{\mathcal{G}_q}\right) && (14a)\\
&= I\left(\mathbf{Y}_b; K_{l^*} | K_{\mathcal{G}_q\backslash\{l^*\}}\right) + I\left(\mathbf{Y}_b; K_{\mathcal{G}_q\backslash\{l^*\}}\right) && (14b)\\
&= I\left(\mathbf{Y}_b; K_{l^*} | K_{\mathcal{G}_q\backslash\{l^*\}}\right) && (14c)\\
&\leqslant H(K_{l^*}) && (14d)\\
&= \log|\mathcal{K}|, && (14e)
\end{aligned}$$

where (14a) holds by the data processing inequality due to the Markov chain $\mathbf{Y}_b - K_{\mathcal{G}_q} - F_q$, in (14b) l^* is an arbitrary element of $\mathcal{G}_q$, (14c) holds by (8) or because $|\mathcal{G}_q| = 1$. Hence, by (7), $H(F_q) = I(\mathbf{Y}_b; F_q) \leqslant \log|\mathcal{K}|$. ∎

Finally, we show that the communication rates R_q, $q \in \mathcal{Q}$, in Definition 1, must be strictly positive in general.

Lemma 3. *Consider an authentication scheme, as defined in Section II-B. Let $q \in \mathcal{Q}$ be such that $|\mathcal{G}_q| > 1$. If the transmitters in $\mathcal{G}_q$ are not allowed to communicate with each other, then there exists multiple access channels, $(\mathcal{X}^m, W_{Y|X_{\mathcal{M}}}, \mathcal{Y})$, for which it is necessary to have $\max_{\upsilon_q} H(F_q) = 0$, where the maximum is taken over all the function υ_q of $K_{\mathcal{G}_q}$, as defined in Definition 1.*

Proof: Let $b \in \mathcal{B}$. Consider a channel such that the legitimate receiver observes $\mathbf{Y}_b \triangleq \left(\mathbf{Y}_b^{(1)}, \mathbf{Y}_b^{(2)}\right)$, and such that there exists $q \in \mathcal{Q}$ and $l^* \in \mathcal{G}_q$ with $|\mathcal{G}_q| > 1$ such that $\mathbf{Y}_b^{(1)}$ only depends on the codeword sent by the transmitter $l^* \in \mathcal{G}_q$, and $\mathbf{Y}_b^{(2)}$ only depends on the codewords sent by the transmitters in $\mathcal{L}\backslash\{l^*\}$. Consider an authentication scheme as defined in Definition 1 with arbitrary functions $(\upsilon_q)_{q\in\mathcal{Q}}$. We then have,

$$\begin{aligned}
I(\mathbf{Y}_b; F_q) &\leqslant I\left(\mathbf{Y}_b; K_{l^*} | K_{\mathcal{G}_q\backslash\{l^*\}}\right) && (15a)\\
&= I\left(\mathbf{Y}_b^{(1)}; K_{l^*} | K_{\mathcal{G}_q\backslash\{l^*\}}\right) \\
&\quad + I\left(\mathbf{Y}_b^{(2)}; K_{l^*} | K_{\mathcal{G}_q\backslash\{l^*\}} \mathbf{Y}_b^{(1)}\right) && (15b)\\
&\leqslant I\left(\mathbf{Y}_b^{(1)}; K_{l^*} | K_{\mathcal{G}_q\backslash\{l^*\}}\right) \\
&\quad + I\left(\mathbf{Y}_b^{(2)} K_{\mathcal{G}_q\backslash\{l^*\}}; K_{l^*} \mathbf{Y}_b^{(1)}\right) && (15c)\\
&= I\left(\mathbf{Y}_b^{(1)}; K_{l^*} | K_{\mathcal{G}_q\backslash\{l^*\}}\right) && (15d)\\
&= I\left(\mathbf{Y}_b^{(1)}; K_{l^*}\right) && (15e)\\
&\leqslant I(\mathbf{Y}_b; K_{l^*}) && (15f)\\
&= 0, && (15g)
\end{aligned}$$

where (15a) holds by the proof of Lemma 2, (15e) holds by independence between $(\mathbf{Y}_b^{(1)}, K_{l^*})$ and $K_{\mathcal{G}_q\backslash\{l^*\}}$, (15g) holds by (8) because $|\mathcal{G}_q| > 1$. Hence, by (7) and (15g), $H(F_q) = I(\mathbf{Y}_b; F_q) = 0$. ∎

B. Proposed coding scheme

The basis of our coding scheme is a multiple access wiretap code for strong secrecy [14]. Hence, we briefly recall the definition and known results concerning this model in Section III-B.1. We then describe our encoding and decoding scheme in Section III-B.2. We only study the reliability, strong secrecy, and anonymity constraints in this section, and postpone the analysis of successful probability of attack to Sections IV and V.

1) Multiple access wiretap channel codes:

Codes for the multiple access wiretap channel are formally defined as follows.

Definition 2. *A code $\mathcal{C}_N$ for a multiple access wiretap channel $(\mathcal{X}_{\mathcal{L}}, W_{YZ|X_{\mathcal{L}}}, \mathcal{Y}\times\mathcal{Z})$ consists of*

- *L encoders, $f_l : \mathcal{M}_l^{(S)} \to \mathcal{X}_l^N$, $l \in \mathcal{L}$, which maps a message M_l of Transmitter l uniformly distributed over $\mathcal{M}_l^{(S)} \triangleq [\![1, 2^{NR_l^{(S)}}]\!]$ to a codeword of length N. Moreover, we define $M_{\mathcal{L}} \triangleq (M_l)_{l\in\mathcal{L}}$;*
- *One decoder, $g : \mathcal{Y}^N \to \bigtimes_{l\in\mathcal{L}} \mathcal{M}_l^{(S)}$, which maps a sequence of N channel output observations to an estimate $\widehat{M}_{\mathcal{L}}$ of $M_{\mathcal{L}}$.*

Definition 3. *A rate L-tuple $\left(R_l^{(S)}\right)_{l\in\mathcal{L}}$ is achievable, if there exists a sequence of codes $(\mathcal{C}_N)_{N\in\mathbb{N}^*}$, such that*

$$\lim_{N\to\infty} \mathbb{P}\left[\widehat{M}_{\mathcal{L}} \neq M_{\mathcal{L}}\right] = 0 \text{ (reliability)}, \tag{16a}$$

$$\lim_{N\to\infty} I\left(M_{\mathcal{L}}; \mathbf{Z}\right) = 0 \text{ (strong secrecy)}, \tag{16b}$$

where $\mathbf{Z}$ is the channel output observed by the eavesdropper.

The next result characterizes a set of known achievable rates.

Theorem 1. *Let Conv $(\cdot)$ denotes the convex hull of a set. The region $\mathcal{R} \triangleq$ Conv $\left(\bigcup_{p_{X_{\mathcal{L}}}=\prod_{l\in\mathcal{L}} p_{X_l}} \mathcal{R}(p_{X_{\mathcal{L}}})\right)$ is achievable, where we have defined*

$$\mathcal{R}(p_{X_{\mathcal{L}}}) \triangleq \Bigg\{ \left(R_l^{(S)}\right)_{l\in\mathcal{L}} : \forall \mathcal{A} \subseteq \mathcal{L}, \sum_{l\in\mathcal{A}} R_l^{(S)} \leqslant \left[I(X_{\mathcal{A}}; Y|X_{\mathcal{A}^c}) - I(X_{\mathcal{A}}; Z)\right]^+ \Bigg\}. \tag{17}$$

Note that Theorem 1 has been established for weak secrecy in [15] and extended to strong secrecy in [14], [16]. Note also that when $L = 2$, Theorem 1 can be obtained with a low-complexity and explicit coding scheme [17].

2) Proposed encoding and decoding algorithms:

For $q \in \mathcal{Q}$, we choose F_q in Definition 1 as

$$F_q \triangleq \bigoplus_{l\in\mathcal{G}_q} K_l, \tag{18}$$

where $\bigoplus$ denotes the modulo-2 addition. We define for any $q \in \mathcal{Q}$,

$$\overline{K}_{q,i} \triangleq F_q\left[[\![1 + (i-1)n^*, i\ n^*]\!]\right], \forall i \in [\![1, |\mathcal{G}_q|]\!], \tag{19}$$

where for any $\mathcal{A} \subseteq [\![1, \log|\mathcal{K}|]\!]$, $F_q[\mathcal{A}]$ denote the bits of F_q in positions indexed by $\mathcal{A}$, n^* is known by all parties and such that $n^* = o(\log(|\mathcal{K}|))$ and $\lim_{|\mathcal{K}|\to\infty} n^* = +\infty$. As seen in Lemma 3, in general, communication among transmitters is required to allow authentication. Algorithm 1 describes the communication process among the transmitters. After the communication process described in Algorithm 1,

Algorithm 1 Communication Among Transmitters

1: **for** $q \in \mathcal{Q}$ **do**
2: **for** $l \in \mathcal{G}_q$ **do**
3: Transmitter l draws a binary sequence R_l uniformly distributed over $\mathcal{K}$ and sends $K_l \oplus R_l$ to all transmitters in $\mathcal{G}_q$
4: Transmitter l sends $K_l[[\![1, |\mathcal{G}_q|n^*]\!]]$ to all transmitters in $\mathcal{G}_q$
5: **end for**
6: All the transmitters in $\mathcal{G}_q$ can compute
$$\overline{\Gamma}_q \triangleq \bigoplus_{l'\in\mathcal{G}_q} (K_{l'} \oplus R_{l'})$$
7: All the transmitters in $\mathcal{G}_q$ can compute $\overline{K}_{q,i}, \forall i \in [\![1, |\mathcal{G}_q|]\!]$, defined in (19)
8: An arbitrary transmitter in $\mathcal{G}_q$ sends to all transmitters in $\mathcal{G}_q$ a permutation Σ_q uniformly chosen at random in $\mathfrak{S}([\![1, |\mathcal{G}_q|]\!])$
9: **end for**

Transmitter $l \in \mathcal{G}_q$, $q \in \mathcal{Q}$, has leaked to other group members $K_l[[\![1, |\mathcal{G}_q|n^*]\!]]$, however, this amount of key leaked is negligible since $n^* = o(\log|\mathcal{K}|)$ and no information has been leaked about $K_l[[\![|\mathcal{G}_q|n^* + 1, \log|\mathcal{K}|]\!]]$ – see Lemma 6 in Appendix A. The corresponding communication rate R_q, $q \in \mathcal{Q}$, in Definition 1 is thus

$$R_q = \frac{|\mathcal{G}_q| \log|\mathcal{K}| + \log(|\mathcal{G}_q|!) + o(\log|\mathcal{K}|)}{NB}, \tag{20}$$

where we have used $n^* = o(\log|\mathcal{K}|)$.

Note that the probability that all the elements of the sequence $(\overline{K}_{q,i})_{q\in\mathcal{Q}, i\in[\![1,|\mathcal{G}_q|]\!]}$ are distinct is $\prod_{i=1}^{L-1}\left(1 - \frac{i}{2^{n^*}}\right) \xrightarrow{|\mathcal{K}|\to\infty} 1$.

Remark 7. *The exchange of the sequences defined in* (19) *described in Algorithm 1 is meant to simplify the presentation of our coding scheme and the decoding rule. Specifically, in Algorithm 3, the decoder can easily determine how to combine the decoded messages from all transmitters to form the left-hand side in* (23)*.*

Remark 8. *Communication among transmitters is not needed when $Q = L$.*

For any group $\mathcal{G}_q$, $q \in \mathcal{Q}$, we then divide $\overline{\Gamma}_q$, obtained in Algorithm 1, in $|\mathcal{G}_q|$ parts as follows. $\forall i \in [\![1, |\mathcal{G}_q| - 1]\!]$,

$$\overline{\Gamma}_{q,i} \triangleq \overline{\Gamma}_q\left[[\![|\mathcal{G}_q|n^* + 1 + (i-1)\Delta_q, |\mathcal{G}_q|n^* + i\Delta_q]\!]\right], \tag{21a}$$

$$\overline{\Gamma}_{q,|\mathcal{G}_q|} \triangleq \overline{\Gamma}_q\left[[\![|\mathcal{G}_q|n^* + 1 + (|\mathcal{G}_q| - 1)\Delta_q, \log|\mathcal{K}|]\!]\right], \tag{21b}$$

where

$$\Delta_q \triangleq \left\lceil \frac{\log|\mathcal{K}| - n^*|\mathcal{G}_q|}{|\mathcal{G}_q| - 1} - 1 \right\rceil, \tag{22}$$

and for any $\mathcal{A} \subseteq [\![1, \log|\mathcal{K}|]\!]$, $\overline{\Gamma}_q[\mathcal{A}]$ denote the bits of $\overline{\Gamma}_q$ in positions indexed by $\mathcal{A}$. The transmitters then encode their messages as described in Algorithm 2, and the legitimate receiver decodes its observations as described in Algorithm 3.

Algorithm 2 Encoding at the Transmitters

for Block $b \in \mathcal{B}$ **do**
  for $q \in \mathcal{Q}$ **do**
    for $l \in \mathcal{G}_q$ **do**
      Define $\Gamma_l^{(1)} \triangleq \overline{\Gamma}_{q,\Sigma_q(l)}$, $\Gamma_l^{(2)} \triangleq \overline{K}_{q,\Sigma_q(l)}$. Transmitter l encodes $\left(M_{l,b}, R_l, \Gamma_l \triangleq \left[\Gamma_l^{(1)}, \Gamma_l^{(2)}\right]\right)$ as his secret message with the multiple access wiretap codes of Theorem 1
    end for
  end for
end for

Algorithm 3 Decoding at the Legitimate Receiver

for Block $b \in \mathcal{B}$ **do**
  For all $l \in \mathcal{L}$, the legitimate receiver forms the estimate $\left(\widehat{M}_{l,b}, \widehat{R}_{l,b}, \widehat{\Gamma}_{l,b}\right)$ of $(M_{l,b}, R_l, \Gamma_l)$, using the decoder of Theorem 1 associated with the encoders used in Algorithm 2. Let $(\widehat{\Gamma}_l^{(1)})_{l\in\mathcal{L}}$, $(\widehat{\Gamma}_l^{(2)})_{l\in\mathcal{L}}$ denote the estimates of $(\Gamma_l^{(1)})_{l\in\mathcal{L}}$, $(\Gamma_l^{(2)})_{l\in\mathcal{L}}$, respectively
  for $q \in \mathcal{Q}$ **do**
    if all the elements of $(\overline{K}_{q,i})_{i\in[\![1,|\mathcal{G}_q|]\!]}$ appears exactly once in $(\widehat{\Gamma}_{l,b}^{(2)})_{l\in\mathcal{L}}$ in positions indexed by $(l_{i,q})_{i\in[\![1,|\mathcal{G}_q|]\!]} \in \mathcal{L}^{|\mathcal{G}_q|}$, and

$$\widehat{R}_q \oplus \left(\left(\mathop{||}_{i\in[\![1,|\mathcal{G}_q|]\!]} \widehat{\Gamma}^{(2)}_{l_{i,q},b}\right) || \left(\mathop{||}_{i\in[\![1,|\mathcal{G}_q|]\!]} \widehat{\Gamma}^{(1)}_{l_{i,q},b}\right)\right) = F_q, \tag{23}$$

    where $||$ denotes concatenation, and $\widehat{R}_q$ is defined as the sum $\bigoplus_{i\in[\![1,|\mathcal{G}_q|]\!]} \widehat{R}_{l_{i,q},b}$ with the first $|\mathcal{G}_q|n^*$ bits replaced by zeros **then**
      The decoder decides that the messages $\left(\widehat{M}_{l_{i,q},b}\right)_{i\in[\![1,|\mathcal{G}_q|]\!]}$ comes from the transmitters in $\mathcal{G}_q$ and sets $D_q = 1$
    else
      The decoder sets $D_q = 0$
    end if
  end for
  if $\sum_{q\in\mathcal{Q}} \mathbb{1}\{D_q = 1\} \geqslant \tau_b$ **then**
    The legitimate receiver accepts as authenticated all the messages of Group $\mathcal{G}_q$ if q is such that $D_q = 1$, $q \in \mathcal{Q}$, and refuse all the other messages
  else
    The legitimate receiver refuses all the messages
  end if
end for

The following proposition summarizes the properties satisfied by our proposed scheme. As alluded to earlier, we postpone the analysis of the probability of successful attack to Sections IV and V.

Proposition 1. *For any rate L-tuple* $\left(R_l^{(S)}\right)_{l\in\mathcal{L}} \in \mathcal{R} \cap \mathbb{R}_+^L$, *where* $\mathcal{R}$ *is defined in Theorem 1, for* $\mathcal{R}_{\mathcal{Q}} \triangleq (O(|\mathcal{G}_q|\log|\mathcal{K}|)/NB)_{q\in\mathcal{Q}}$, *the authentication scheme defined by Algorithms 1, 2, and 3 satisfies strong secrecy, anonymity, and reliability. Note also that* (7) *is asymptotically satisfied, and that* (13) *holds with equality.*

Proof: Reliability holds by Theorem 1. Strong secrecy is shown as follows. Define for $b \in \mathcal{B}$, $\mathcal{V}_{\mathcal{L},b} \triangleq (M_{l,b}, R_l, \Gamma_l)_{l\in\mathcal{L}}$ and $\mathcal{V}_{\mathcal{L}}^B \triangleq (\mathcal{V}_{\mathcal{L},b})_{b\in\mathcal{B}}$. We have

$$\begin{aligned}
I\left(\mathcal{V}_{\mathcal{L}}^B; \mathbf{Z}^B\right) &= \sum_{b\in\mathcal{B}} I\left(\mathbf{Z}_b; \mathcal{V}_{\mathcal{L}}^B | \mathbf{Z}^{b-1}\right) && \text{(24a)}\\
&\leqslant \sum_{b\in\mathcal{B}} I\left(\mathbf{Z}_b; \mathcal{V}_{\mathcal{L}}^B \mathbf{Z}^{b-1}\right) && \text{(24b)}\\
&= \sum_{b\in\mathcal{B}} I\left(\mathbf{Z}_b; \mathcal{V}_{\mathcal{L}}^B\right) && \text{(24c)}\\
&= \sum_{b\in\mathcal{B}} I\left(\mathbf{Z}_b; \mathcal{V}_{\mathcal{L},b}\right) && \text{(24d)}\\
&\leqslant \sum_{b\in\mathcal{B}} \delta(N) && \text{(24e)}\\
&= B\delta(N), && \text{(24f)}
\end{aligned}$$

where (24c) holds because for any $b \in \mathcal{B}$, we have $\mathbf{Z}_b - \mathcal{V}_{\mathcal{L}}^B - \mathbf{Z}^{b-1}$, (24d) holds because $\mathbf{Z}_b - \mathcal{V}_{\mathcal{L},b} - (\mathcal{V}_{\mathcal{L},b'})_{b'\in\mathcal{B}\setminus\{b\}}$, (24e) holds by Algorithm 2 and Theorem 1 and where $\delta(N)$ denotes a generic function that vanishes to zero exponentially fast as $N \to \infty$.

We now verify that the anonymity constraints hold. Consider an arbitrary bijection β between $\mathfrak{S}(\mathcal{G}_q, \mathrm{Im}_q)$ and $\mathfrak{S}([\![1, |\mathcal{G}_q|]\!])$. By construction of F_q, we have, $\forall N, B \in \mathbb{N}^*, \forall q \in \mathcal{Q}, \forall \mathbf{y}^B \in \mathcal{Y}^{NB}, \forall \sigma \in \mathfrak{S}(\mathcal{G}_q, \mathrm{Im}_q)$,

$$\mathbb{P}\left[\Pi_q = \sigma | \mathbf{Y}^B = \mathbf{y}^B\right] = \mathbb{P}\left[\Sigma_q = \beta(\sigma)\right] = \frac{1}{|\mathcal{G}_q|!}. \tag{25}$$

■

IV. Characterization of the Probability of a Successful Attack: Lower Bound

We derive in Section IV-B a lower bound on the probability of successful attack valid for any authentication scheme, as defined in Section II-B, that satisfies Equation (7) and Equation (13) with equality. We will then provide in Section V an upper bound on the probability of successful attack for the coding scheme proposed in Section III-B and compare it to the lower bound found in this section. We first introduce additional definitions in Section IV-A.

A. Additional definitions

Define

$$\mathbf{B}(L, B, \mathcal{K}, \mathcal{P}, \mathcal{T})$$

$$\triangleq \max_{b\in\mathcal{B}} \left(\frac{\max\limits_{\boldsymbol{\epsilon}\in\mathcal{E}} \sum\limits_{\mathbf{l}_b\in\Lambda_b} \prod\limits_{d\in\mathcal{D}} \binom{n_d}{l_{d,b}} \binom{\epsilon_d}{l_{d,b}} l_{d,b}!}{|\mathcal{K}|^{\tau_b}} \right), \quad (26)$$

where we have defined the sets

$$\mathcal{E} \triangleq \left\{ \boldsymbol{\epsilon} \triangleq (\epsilon_d)_{d\in\mathcal{D}} \in \mathbb{N}^D : \sum_{d\in\mathcal{D}} \epsilon_d c_d \leqslant L \right\}, \quad (27)$$

$\forall b \in \mathcal{B}$,

$$\Lambda_b \triangleq \left\{ \mathbf{l}_b \triangleq (l_{d,b})_{d\in\mathcal{D}} \in \bigtimes_{d\in\mathcal{D}} [\![1, n_d]\!] : \sum_{d\in\mathcal{D}} l_{d,b} = \tau_b \right\}, \quad (28)$$

and with the convention $\binom{x}{y} \triangleq 0$ when $x, y \in \mathbb{N}$ are such that $y > x$. Finally, define

$$b^* \text{ as any element of } \arg\min_{b\in\mathcal{B}} \tau_b, \quad (29)$$

such that

$$\mathbf{B}(L, B, \mathcal{K}, \mathcal{P}, \mathcal{T}) \overset{|\mathcal{K}|\to\infty}{\sim} \frac{\max\limits_{\boldsymbol{\epsilon}\in\mathcal{E}} \sum\limits_{\mathbf{l}_{b^*}\in\Lambda_{b^*}} \prod\limits_{d\in\mathcal{D}} \binom{n_d}{l_{d,b^*}} \binom{\epsilon_d}{l_{d,b^*}} l_{d,b^*}!}{|\mathcal{K}|^{\tau_{b^*}}}. \quad (30)$$

B. Lower bound on the probability of a successful attack

In this section, we consider any authentication scheme as defined in Section II-B that satisfies Equation (7) and Equation (13) with equality. As explained in Section III-A, an authentication scheme should be designed to satisfy Equation (7) and Equation (13) with equality to make an attack of the opponent more difficult. To lower bound the probability of a successful attack by an opponent, one can consider any strategy and study its probability of success, since the later represents the probability of success that an opponent can at least yield. In the following proposition, we study the case where the opponent tries to guess at random the sequences $(F_q)_{q\in\mathcal{Q}}$.

Proposition 2. *Let $L, N, B, Q \in \mathbb{N}^*$. Let $\mathcal{P} \triangleq \{\mathcal{G}_q\}_{q\in\mathcal{Q}}$ be a partition of $\mathcal{L}$, and let $\mathcal{T} \triangleq (\tau_b)_{b\in\mathcal{B}} \in \mathcal{Q}^B$ be a sequence of decision thresholds. For any sequence $(\mathcal{S}_N)_{N\in\mathbb{N}}$ of $(L, N, B, \mathcal{K}, \mathcal{R}_\mathcal{L}, \mathcal{R}_\mathcal{Q}, \mathcal{P}, \mathcal{T})$ authentication schemes, the probability of a successful attack $P_A(\mathcal{S}_N)$ is lower bounded by a term equivalent, as $|\mathcal{K}| \to \infty$, to $\mathbf{B}(L, B, \mathcal{K}, \mathcal{P}, \mathcal{T})$, defined in Section IV-A.*

Proof: The strategy of the opponent is the following. For $b \in \mathcal{B}$, the opponent successively guesses at random with ϵ_d tries for each $d \in \mathcal{D}$, some authentication sequence F_q associated with the groups of size c_d. We assume that for a given $d \in \mathcal{D}$, the opponent can redraw sequences that he has already drawn for previous d's, i.e., the opponent draws with replacement for different d's. Note that the number of tries ϵ_d, $d \in \mathcal{D}$, are limited by the constraint $\sum_{d\in\mathcal{D}} \epsilon_d c_d \leqslant L$. For instance, if $L = 6$ and $\mathcal{G}_1 = \{1\}$, $\mathcal{G}_2 = \{2\}$, $\mathcal{G}_3 = \{3\}$, $\mathcal{G}_4 = \{4, 5, 6\}$, then the attacker could try to impersonate $\mathcal{G}_1$, $\mathcal{G}_2$, or $\mathcal{G}_3$ with 6 tries, or $\mathcal{G}_4$ with 2 tries as there are 6 transmitters. Define for $\boldsymbol{\epsilon} \in \mathcal{E}$, $\mathbf{l}_b \in \Lambda_b$, and for $d \in \mathcal{D}$, the events

$$\mathcal{A}_d(\boldsymbol{\epsilon}, \mathbf{l}_b) \triangleq \{\text{Correctly guess exactly } l_{d,b} \text{ authentication sequences for the groups of size } c_d \text{ in } \epsilon_d \text{ tries}\}, \quad (31)$$

and

$$\mathcal{A}(\boldsymbol{\epsilon}, \mathbf{l}_b) \triangleq \bigcap_{d\in\mathcal{D}} \mathcal{A}_d(\boldsymbol{\epsilon}, \mathbf{l}_b). \quad (32)$$

For a given $\boldsymbol{\epsilon} \in \mathcal{E}$, the probability that the opponent correctly guesses at least τ_b authentication sequences is lower bounded by

$$\mathbb{P}\left[\bigcup_{\mathbf{l}_b\in\Lambda_b} \mathcal{A}(\boldsymbol{\epsilon}, \mathbf{l}_b) \right] = \sum_{\mathbf{l}_b\in\Lambda_b} \mathbb{P}\left[\mathcal{A}(\boldsymbol{\epsilon}, \mathbf{l}_b)\right] \quad (33a)$$

$$= \sum_{\mathbf{l}_b\in\Lambda_b} \prod_{d\in\mathcal{D}} \mathbb{P}[\mathcal{A}_d(\boldsymbol{\epsilon}, \mathbf{l}_b)] \quad (33b)$$

$$= \sum_{\mathbf{l}_b\in\Lambda_b} \prod_{d\in\mathcal{D}} \frac{\binom{n_d}{l_{d,b}} \binom{|\mathcal{K}| - n_d}{\epsilon_d - l_{d,b}}}{\binom{|\mathcal{K}|}{\epsilon_d}} \quad (33c)$$

$$= f(|\mathcal{K}|, \boldsymbol{\epsilon}, b), \quad (33d)$$

where (33a) holds because the events $(\mathcal{A}(\boldsymbol{\epsilon}, \mathbf{l}_b))_{\mathbf{l}_b\in\Lambda_b}$ are mutually disjoint, (33b) holds because the draws of the opponent are independent of each other and with replacement for different group sizes, in (33c) observe that we have an hypergeometric distribution: for $d \in \mathcal{D}$, there are n_d correct sequences among $2^{\log|\mathcal{K}|} = |\mathcal{K}|$ possible sequences and the opponent must guess $l_{d,b}$ correct sequences in ϵ_d tries without replacement, in (33d) we have defined

$$f(|\mathcal{K}|, \boldsymbol{\epsilon}, b) \triangleq \sum_{\mathbf{l}_b\in\Lambda_b} \prod_{d\in\mathcal{D}} \frac{\binom{n_d}{l_{d,b}} \binom{\epsilon_d}{l_{d,b}} l_{d,b}! \prod\limits_{k=0}^{\epsilon_d - l_{d,b} - 1} (|\mathcal{K}| - n_d - k)}{\prod\limits_{k=0}^{\epsilon_d - 1} (|\mathcal{K}| - k)}. \quad (34)$$

Finally, the opponent chooses $b \in \mathcal{B}$ and $\boldsymbol{\epsilon} \in \mathcal{E}$ to maximize his probability of success, so that the probability of a successful attack is lower bounded by $\max\limits_{b\in\mathcal{B}} \max\limits_{\boldsymbol{\epsilon}\in\mathcal{E}} f(|\mathcal{K}|, \boldsymbol{\epsilon}, b)$. As shown in Appendix B, we have

$$\max_{b\in\mathcal{B}} \max_{\boldsymbol{\epsilon}\in\mathcal{E}} f(|\mathcal{K}|, \boldsymbol{\epsilon}, b) \overset{|\mathcal{K}|\to\infty}{\sim} \max_{b\in\mathcal{B}} \max_{\boldsymbol{\epsilon}\in\mathcal{E}} g(|\mathcal{K}|, \boldsymbol{\epsilon}, b), \quad (35)$$

where

$$g(|\mathcal{K}|, \boldsymbol{\epsilon}, b) \triangleq \sum_{\mathbf{l}_b\in\Lambda_b} \frac{\prod\limits_{d\in\mathcal{D}} \binom{n_d}{l_{d,b}} \binom{\epsilon_d}{l_{d,b}} l_{d,b}!}{|\mathcal{K}|^{\tau_b}}. \quad (36)$$

■

V. Characterization of the Probability of a Successful Attack: Upper Bound

We now provide an upper bound on the probability of successful attack for the coding scheme proposed in Section III-B and show that it asymptotically matches the lower bound derived in Section IV.

A. Preliminary definitions

We consider an arbitrary attack strategy, denoted by e, performed by the opponent. Recall that an attack from the opponent consists in forming a fraudulent signal $\widetilde{\mathbf{Y}}_b$, which is function of all his knowledge in Block $b \in \mathcal{B}$, that will be sent to the legitimate receiver. Let

$$\widetilde{m}_{\mathcal{L},b}(e) \triangleq (\widetilde{m}_{l,b})_{l\in\mathcal{L}}\,, \tag{37}$$

$$\widetilde{r}_{\mathcal{L},b}(e) \triangleq (\widetilde{r}_{l,b})_{l\in\mathcal{L}}\,, \tag{38}$$

$$\widetilde{\gamma}_{\mathcal{L},b}(e) \triangleq (\widetilde{\gamma}_{l,b})_{l\in\mathcal{L}} = \left([\widetilde{\gamma}^{(1)}_{l,b}, \widetilde{\gamma}^{(2)}_{l,b}]\right)_{l\in\mathcal{L}}\,, \tag{39}$$

be the messages decoded in Block b by the legitimate receiver upon decoding $\widetilde{\mathbf{Y}}_b$ with Algorithm 3 and where $\left(\widetilde{\gamma}^{(1)}_{l,b}\right)_{l\in\mathcal{L}}$, $\left(\widetilde{\gamma}^{(2)}_{l,b}\right)_{l\in\mathcal{L}}$ correspond to the estimate of $\left(\gamma^{(1)}_{l,b}\right)_{l\in\mathcal{L}}$, $\left(\gamma^{(2)}_{l,b}\right)_{l\in\mathcal{L}}$, respectively.

For $q \in \mathcal{Q}$, if all the elements of $(\overline{k}_{q,i})_{i\in[\![1,|\mathcal{G}_q|]\!]}$ appears exactly once in $(\widetilde{\gamma}^{(2)}_{l,b})_{l\in\mathcal{L}}$ in positions indexed by $(\widetilde{l}_{i,q})_{i\in[\![1,|\mathcal{G}_q|]\!]} \in \mathcal{L}^{|\mathcal{G}_q|}$, then define

$$\widetilde{\sigma}_{\widetilde{l}_{i,q},b} \triangleq \widetilde{r}_q \oplus \left(\left(\mathop{||}_{i\in[\![1,|\mathcal{G}_q|]\!]} \widetilde{\gamma}^{(2)}_{\widetilde{l}_{i,q},b}\right) || \left(\mathop{||}_{i\in[\![1,|\mathcal{G}_q|]\!]} \widetilde{\gamma}^{(1)}_{\widetilde{l}_{i,q},b}\right)\right), \tag{40}$$

where $\widetilde{r}_q$ is defined as the sum $\bigoplus_{i\in[\![1,|\mathcal{G}_q|]\!]} \widetilde{r}_{\widetilde{l}_{i,q},b}$ with the first $|\mathcal{G}_q|n^*$ bits replaced by zeros. Let

$$m_{\mathcal{L},b} \triangleq (m_{l,b})_{l\in\mathcal{L}}\,, \tag{41}$$

$$r_{\mathcal{L}} \triangleq (r_l)_{l\in\mathcal{L}}\,, \tag{42}$$

$$\gamma_{\mathcal{L}} \triangleq (\gamma_l)_{l\in\mathcal{L}}\,, \tag{43}$$

be the messages encoded by the legitimate transmitters in Block $b \in \mathcal{B}$. For $q \in \mathcal{Q}$, let $(l_{i,q})_{i\in[\![1,|\mathcal{G}_q|]\!]} \in \mathcal{L}^{|\mathcal{G}_q|}$ be such that $||_{i\in[\![1,|\mathcal{G}_q|]\!]} \gamma^{(2)}_{l_{i,q}} = f_q[[\![1,|\mathcal{G}_q|n^*]\!]]$. We define for $q \in \mathcal{Q}$,

$$\overline{\gamma}_q \triangleq \left(\mathop{||}_{i\in[\![1,|\mathcal{G}_q|]\!]} \gamma^{(2)}_{l_{i,q}}\right) || \left(\mathop{||}_{i\in[\![1,|\mathcal{G}_q|]\!]} \gamma^{(1)}_{l_{i,q}}\right), \tag{44}$$

$$\overline{\sigma}_q \triangleq r_q \oplus \overline{\gamma}_q = f_q, \tag{45}$$

where r_q is defined as the sum $\bigoplus_{l\in\mathcal{G}_q} r_l$ with the first $n^*|\mathcal{G}_q|$ bits replaced by zeros.

The opponent chooses his strategy to maximize his success, given its observations $\mathbf{Z}^{b-1}$ for an impersonation attack, or given its observations $\mathbf{Z}^b$ for a substitution attack. Hence, averaging over the opponent's observations the probabilities of successful impersonation and substitution attacks are

$$P_{I,b}(\tau_b) = \mathbb{E}_{\mathbf{Z}^{b-1}} \sup_e \left\{ \sum_{\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b}} \mathbb{1}\left\{\mathcal{A}(e)\right\} p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b} \middle| \mathbf{z}^{b-1}\right) \right\}, \tag{46}$$

$$P_{S,b}(\tau_b) = \mathbb{E}_{\mathbf{Z}^{b}} \sup_e \left\{ \sum_{\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b}} \mathbb{1}\left\{\mathcal{A}(e)\right\} p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b} \middle| \mathbf{z}^{b}\right) \right\}, \tag{47}$$

where we have defined for any $\gamma_{\mathcal{L}}$, for any $r_{\mathcal{L}}$, for any $m_{\mathcal{L},b}$, for any opponent's attack e, the set

$$\mathcal{I}_{\sigma,\widetilde{\sigma}} \triangleq \{q \in \mathcal{Q} : \overline{\sigma}_q \text{ appears exactly } |\mathcal{G}_q| \text{ times in } (\widetilde{\sigma}_{l,b})_{l\in\mathcal{L}}\}, \tag{48}$$

and the event

$$\mathcal{A}(e) \triangleq \left\{ |\mathcal{I}_{\sigma,\widetilde{\sigma}}| \geqslant \tau_b \text{ and } \exists q_0 \in \mathcal{I}_{\sigma,\widetilde{\sigma}}, (\widetilde{m}_{l,b})_{l\in\mathcal{G}_{q_0}} \neq (m_{l,b})_{l\in\mathcal{G}_{q_0}} \right\}. \tag{49}$$

The realization of the event $\mathcal{A}(e)$ means that at least τ_b groups of messages in $\mathcal{P}$, are accepted as authentic and at least one message has been modified among all the messages accepted by the receiver.

B. Upper bound

We show the following upper bound on the probability of successful attack for the authentication scheme defined in Section III-B.

Proposition 3. *Consider a sequence $(\mathcal{S}_N)_{N\in\mathbb{N}}$ of authentication schemes as defined in Section III-B. For any $\mathcal{R}_{\mathcal{L}} \in \mathcal{R} \cap \mathbb{R}^L_+$, where $\mathcal{R}$ is defined in Theorem 1, the asymptotic probability of a successful attack $\lim_{N\to\infty} P_A(\mathcal{S}_N)$ is upper bounded by a term equivalent, as $|\mathcal{K}| \to \infty$, to $\mathbf{B}(L, B, \mathcal{K}, \mathcal{P}, \mathcal{T})$, defined in Section IV-A.*

Proof: Let $b \in \mathcal{B}$. We define for any opponent's attack e, the event,

$$\mathcal{A}'(e) \triangleq \{|\mathcal{I}_{\sigma,\widetilde{\sigma}}| \geqslant \tau_b\}\,, \tag{50}$$

hence, by (46) and since $\mathbb{1}\{\mathcal{A}'(e)\} \geqslant \mathbb{1}\{\mathcal{A}(e)\}$, we have

$$P_{I,b}(\tau_b) \leqslant \mathbb{E}_{\mathbf{Z}^{b-1}} \sup_e \sum_{\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b}} \mathbb{1}\left\{\mathcal{A}'(e)\right\} p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b} \middle| \mathbf{z}^{b-1}\right). \tag{51}$$

Then, for any opponent's attack e, for any $i \in [\![\tau_b, Q]\!]$, define the event

$$\mathcal{A}'_i(e) \triangleq \{|\mathcal{I}_{\sigma,\widetilde{\sigma}}| = i\}\,, \tag{52}$$

so that

$$\mathbb{1}\left\{\mathcal{A}'(e)\right\} = \mathbb{1}\left\{\bigcup_{i=\tau_b}^{Q} \mathcal{A}'_i(e)\right\} = \sum_{i=\tau_b}^{Q} \mathbb{1}\left\{\mathcal{A}'_i(e)\right\}. \tag{53}$$

We thus obtain from (51)

$$\begin{aligned} &P_{I,b}(\tau_b) \\ &\leqslant \sum_{i=\tau_b}^{Q} \mathbb{E}_{\mathbf{Z}^{b-1}} \sup_{e} \sum_{\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b}} \mathbb{1}\left\{\mathcal{A}'_i(e)\right\} p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b} \middle| \mathbf{z}^{b-1}\right). \end{aligned} \tag{54}$$

We next upper bound the first term in the sum in the right-hand side of (54) in Lemma 4 when $N \to \infty$. The other terms of the sum in the right-hand side of (54) will be upper bounded in Lemma 5.

Lemma 4. *An upper bound on*

$$\lim_{N\to\infty} \mathbb{E}_{\mathbf{Z}^{b-1}} \sup_{e} \sum_{\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b}} \mathbb{1}\left\{\mathcal{A}'_{\tau_b}(e)\right\} p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b} \middle| \mathbf{z}^{b-1}\right)$$

is $\frac{\max_{\boldsymbol{\epsilon}\in\mathcal{E}} h(\boldsymbol{\epsilon}, b)}{|\mathcal{K}|^{\tau_b}}$, *where*

$$h(\boldsymbol{\epsilon}, b) \triangleq \sum_{\mathbf{l}_b \in \Lambda_b} \prod_{d\in\mathcal{D}} \binom{n_d}{l_{d,b}} \binom{\epsilon_d}{l_{d,b}} l_{d,b}!. \tag{55}$$

Proof: See Appendix C. ∎

Similar to (87e) in the proof of Lemma 4, we have the following lemma.

Lemma 5. *For* $i \in [\![\tau_b + 1, Q]\!]$,

$$\lim_{N\to\infty} \mathbb{E}_{\mathbf{Z}^{b-1}} \sup_{e} \sum_{\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b}} \mathbb{1}\left\{\mathcal{A}'_i(e)\right\} p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b} \middle| \mathbf{z}^{b-1}\right)$$

is upper bounded by a term in $O(|\mathcal{K}|^{-i})$.

Hence, by (54), Lemma 4, and Lemma 5, $\lim_{N\to\infty} P_{I,b}(\tau_b)$ is upper bounded by a term equivalent, as $|\mathcal{K}| \to \infty$, to $\frac{\max_{\boldsymbol{\epsilon}\in\mathcal{E}} h(\boldsymbol{\epsilon}, b)}{|\mathcal{K}|^{\tau_b}}$. Replacing $\mathbf{Z}^{b-1}$ by $\mathbf{Z}^b$ in the proof of Lemmas 4, 5, we obtain the same upper bound for $\lim_{N\to\infty} P_{S,b}(\tau_b)$. We thus have, similar to Appendix B,

$$\begin{aligned} &\lim_{N\to\infty} \max_{b\in\mathcal{B}} \max\left(P_{I,b}(\tau_b), P_{S,b}(\tau_b)\right) \\ &= \max_{b\in\mathcal{B}} \max\left(\lim_{N\to\infty} P_{I,b}(\tau_b), \lim_{N\to\infty} P_{S,b}(\tau_b)\right) && \text{(56a)} \\ &\leqslant \max_{b\in\mathcal{B}} \left(\frac{\max_{\boldsymbol{\epsilon}\in\mathcal{E}} h(\boldsymbol{\epsilon}, b)}{|\mathcal{K}|^{\tau_b}} + o\left(\frac{1}{|\mathcal{K}|^{\tau_b}}\right)\right) && \text{(56b)} \\ &\overset{|\mathcal{K}|\to\infty}{\sim} \max_{b\in\mathcal{B}} \left(\frac{\max_{\boldsymbol{\epsilon}\in\mathcal{E}} h(\boldsymbol{\epsilon}, b)}{|\mathcal{K}|^{\tau_b}}\right). && \text{(56c)} \end{aligned}$$

∎

VI. Results and Discussion

The following result provides an asymptotically optimal characterization of the probability of a successful attack by combining Proposition 2 and Proposition 3.

Theorem 2. *For any* $L, N, B, Q \in \mathbb{N}^*$, *for any partition* $\mathcal{P} \triangleq \{\mathcal{G}_q\}_{q\in\mathcal{Q}}$ *of* $\mathcal{L}$, *for any sequence of decision thresholds* $\mathcal{T} \triangleq (\tau_b)_{b\in\mathcal{B}} \in \mathcal{Q}^B$, *for any* $\mathcal{R}_{\mathcal{L}} \in \mathcal{R} \cap \mathbb{R}_+^L$, *where* $\mathcal{R}$ *is defined in Theorem 1,*

(i) The sequence $(\mathcal{S}_N)_{N\in\mathbb{N}}$ *of* $(L, N, B, \mathcal{K}, \mathcal{R}_{\mathcal{L}}, \mathcal{R}_{\mathcal{Q}}, \mathcal{P}, \mathcal{T})$ *authentication schemes as defined in Section III-B is such that the probability of a successful attack satisfies*

$$\begin{aligned} &\lim_{N\to\infty} P_A(\mathcal{S}_N) \\ &\qquad \overset{|\mathcal{K}|\to\infty}{\sim} \frac{\max_{\boldsymbol{\epsilon}\in\mathcal{E}} \sum_{\mathbf{l}_{b^*}\in\Lambda_{b^*}} \prod_{d\in\mathcal{D}} \binom{n_d}{l_{d,b^*}} \binom{\epsilon_d}{l_{d,b^*}} l_{d,b^*}!}{|\mathcal{K}|^{\tau_{b^*}}}, \end{aligned} \tag{57}$$

where b^*, $\mathcal{E}$, *and* Λ_{b^*} *are defined in Section IV-A.*

(ii) Moreover, the convergence rate of the probability of a successful attack with respect to $|\mathcal{K}|$ *is optimal.*

In the following, we write $\lim_{N\to\infty} P_A$ instead of $\lim_{N\to\infty} P_A(\mathcal{S}_N)$ to simplify notation, where $(\mathcal{S}_N)_{N\in\mathbb{N}}$ is defined in Theorem 2. We obtain the following corollary.

Corollary 1. *Theorem 2 simplifies as follows in special cases.*

(i) Assume that there exists $b_0 \in \mathcal{B}$ *such that* $\tau_{b_0} = 1$, *i.e.,* $\tau_{b^*} = 1$. *Then,*

$$\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{\max_{\boldsymbol{\epsilon}\in\mathcal{E}} \sum_{d\in\mathcal{D}} \epsilon_d n_d}{|\mathcal{K}|}. \tag{58}$$

(ii) Assume that for any $b \in \mathcal{B}$, $\tau_b = Q$, *i.e.,* $\tau_{b^*} = Q$. *Then,*

$$\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{\prod_{d\in\mathcal{D}} n_d!}{|\mathcal{K}|^{Q}}. \tag{59}$$

(iii) Assume that all parts of $\mathcal{P}$ *have same size, i.e.,* $|\{|\mathcal{G}_q|\}_{q\in\mathcal{Q}}| = 1$. *Then,*

$$\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{\binom{Q}{\tau_{b^*}}^2 \tau_{b^*}!}{|\mathcal{K}|^{\tau_{b^*}}}. \tag{60}$$

Proof: Observe that

(i) When $\tau_{b^*} = 1$, l_{b^*} is a sequence of $D-1$ zeros and one 1, hence, in (57), $(D-1)$ terms in the product $\prod_{d\in\mathcal{D}}$ are equal to 1 and $|\Lambda_{b^*}| = D$.

(ii) When $\tau_{b^*} = Q$, Λ_{b^*} is the singleton $\{(n_d)_{d\in\mathcal{D}}\}$, hence, in (57), the sum $\sum_{\mathbf{l}_{b^*}\in\Lambda_{b^*}}$ has only one term.

(iii) When $|\{|\mathcal{G}_q|\}_{q\in\mathcal{Q}}| = 1$, in (57), the product $\prod_{d\in\mathcal{D}}$ has only one term, Λ_{b^*} is the singleton $\{\tau_{b^*}\}$, and the maximum over $\mathcal{E}$ is achieved for $\boldsymbol{\epsilon} = Q$.

∎

From Theorem 2, we observe a trade-off between the acceptance parameter τ_b and the probability of a successful attack. If τ_b is large, the receiver might refuse up to $\tau_b - 1$ correctly authenticated groups of messages (which might not

be desirable since it represents wasted transmissions), on the other hand, if τ_b is small the probability of a successful attack increases by a factor $|\mathcal{K}|$ each time τ_b is decreased by one.

Observe also that the decay of the probability of successful attack with respect to $|\mathcal{K}|$, is independent of the choice of the partition $\mathcal{P}$, and only depends on the minimum value τ_{b^*} in $\mathcal{T}$. The choice of $\mathcal{P}$ does, however, influence the constant coefficient, i.e., the numerator, in (57). We thus remark that except for the cases $Q = 1$, for which $\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{1}{|\mathcal{K}|}$, and the case $\tau_{b^*} = 1$, for which

$$\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{\max\limits_{\boldsymbol{\epsilon}\in\mathcal{E}} \sum\limits_{d\in\mathcal{D}} \epsilon_d n_d}{|\mathcal{K}|},$$

all the transmitters benefit from a multiuser setting compared to a single-user setting, for which the probability of successful attack scales at best as $\frac{1}{|\mathcal{K}|}$ as N goes to infinity [11].

Finally, assuming $\tau_{b^*} = Q$, remark that the anonymity constraints benefit the opponent since Q is maximal and equal to L when no anonymity constraint holds.

Example 6. *Consider Examples 2–5 with the assumption* $\tau_{b*} = 1$.

- *For Example 2, we have*

$$\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{L^2}{|\mathcal{K}|}. \tag{61}$$

- *For Examples 3 and 5, we have*

$$\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{1}{|\mathcal{K}|}. \tag{62}$$

- *For Example 4, assume that* $\mathcal{P} \triangleq \{\mathcal{G}_1, \mathcal{G}_2\}$. *We then have*

$$\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{(1 + \mathbb{1}\{|\mathcal{G}_1| = |\mathcal{G}_2|\}) \left\lfloor \frac{L}{\min(|\mathcal{G}_1|, |\mathcal{G}_2|)} \right\rfloor}{|\mathcal{K}|}. \tag{63}$$

Example 7. *Consider Examples 2–5 with the assumption* $\tau_{b*} = Q$.

- *For Example 2, we have*

$$\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{L!}{|\mathcal{K}|^L}. \tag{64}$$

- *For Examples 3 and 5, we have*

$$\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{1}{|\mathcal{K}|}. \tag{65}$$

- *For Example 4, assume that* $\mathcal{P} \triangleq \{\mathcal{G}_1, \mathcal{G}_2\}$. *We then have*

$$\lim_{N\to\infty} P_A \overset{|\mathcal{K}|\to\infty}{\sim} \frac{1 + \mathbb{1}\{|\mathcal{G}_1| = |\mathcal{G}_2|\}}{|\mathcal{K}|^2}. \tag{66}$$

Note that we also recover the case $L = 1$, *i.e., authentication when there is only one transmitter [11], for which the probability of successful attack scales as* $\frac{1}{|\mathcal{K}|}$ *when* N *goes to infinity.*

Remark 9. *If one chooses* $\log|\mathcal{K}| = \omega_N$, *where* $\lim_{N\to\infty} \omega_N = +\infty$ *and* $\lim_{N\to\infty} \frac{\omega_N}{N} = 0$, *then in Section III-B the rates* $(R_q)_{q\in\mathcal{Q}}$ *all go to zero as* N *goes to infinity.*

VII. Conclusion

We have considered authentication of multiple messages sent by L transmitters over a noisy multiple access channel, where each transmitter shares a secret key with the legitimate receiver. The presence of a computationally unbounded opponent able to perform a substitution or impersonation attacks is assumed. Our model also considers anonymity constraints, i.e., when groups of individuals must remain anonymous despite being authenticated. Our main result is the design of an authentication scheme for the proposed model, associated with the derivation of an asymptotic characterization of the probability of successful attack, that optimally scales with the length of the secret keys shared between each transmitter and the legitimate receiver.

Appendix A
One-Time Pad

Lemma 6. *Consider the random variables* A, B, C, *defined over* $\{0,1\}^N$, $N \in \mathbb{N}$. *Assume that* $I(AB;C) = 0$ *and* $H(C) = N$, *i.e.,* C *is uniformly distributed. We then have* $I(AB; B \oplus C) = 0$.

Proof: We have

$$\begin{aligned} I(AB; B\oplus C) &= H(B\oplus C) - H(B\oplus C|AB) && \text{(67a)}\\ &\leqslant N - H(B\oplus C|AB) && \text{(67b)}\\ &= N - H(C|AB) && \text{(67c)}\\ &= N - H(C) && \text{(67d)}\\ &= 0. && \text{(67e)} \end{aligned}$$

■

Appendix B
Proof of (35)

For $|\mathcal{K}|$ large enough, we have

$$b^* \in \arg\max_{b\in\mathcal{B}} \left(\max_{\boldsymbol{\epsilon}\in\mathcal{E}} g(|\mathcal{K}|, \boldsymbol{\epsilon}, b) \right), \tag{68}$$

where b^* is defined in (29), hence,

$$\max_{b\in\mathcal{B}} \max_{\boldsymbol{\epsilon}\in\mathcal{E}} g(|\mathcal{K}|, \boldsymbol{\epsilon}, b) = \frac{\max\limits_{\boldsymbol{\epsilon}\in\mathcal{E}} h(\boldsymbol{\epsilon}, b^*)}{|\mathcal{K}|^{\tau_{b^*}}}, \tag{69}$$

where we have defined

$$h(\boldsymbol{\epsilon}, b) \triangleq \sum_{\mathbf{l}_b\in\Lambda_b} \prod_{d\in\mathcal{D}} \binom{n_d}{l_{d,b}} \binom{\epsilon_d}{l_{d,b}} l_{d,b}!. \tag{70}$$

Then,

$$\lim_{|\mathcal{K}|\to\infty} \frac{\max\limits_{b\in\mathcal{B}} \max\limits_{\boldsymbol{\epsilon}\in\mathcal{E}} f(|\mathcal{K}|, \boldsymbol{\epsilon}, b)}{\max\limits_{b\in\mathcal{B}} \max\limits_{\boldsymbol{\epsilon}\in\mathcal{E}} g(|\mathcal{K}|, \boldsymbol{\epsilon}, b)}$$

$$= \lim_{|\mathcal{K}|\to\infty} \frac{\max_{b\in\mathcal{B}} \max_{\boldsymbol{\epsilon}\in\mathcal{E}} (f(|\mathcal{K}|,\boldsymbol{\epsilon},b)|\mathcal{K}|^{\tau_{b^*}})}{\max_{\boldsymbol{\epsilon}\in\mathcal{E}} h(\boldsymbol{\epsilon},b^*)} \tag{71a}$$

$$= \frac{\max_{b\in\mathcal{B}} \max_{\boldsymbol{\epsilon}\in\mathcal{E}} \lim_{|\mathcal{K}|\to\infty} (f(|\mathcal{K}|,\boldsymbol{\epsilon},b)|\mathcal{K}|^{\tau_{b^*}})}{\max_{\boldsymbol{\epsilon}\in\mathcal{E}} h(\boldsymbol{\epsilon},b^*)} \tag{71b}$$

$$= \frac{\max_{b\in\mathcal{B}} \max_{\boldsymbol{\epsilon}\in\mathcal{E}} h(\boldsymbol{\epsilon},b^*)}{\max_{\boldsymbol{\epsilon}\in\mathcal{E}} h(\boldsymbol{\epsilon},b^*)} \tag{71c}$$

$$= 1, \tag{71d}$$

where (71a) holds by (69), (71b) holds because, provided that the limits exist, for a finite subset $\mathcal{J}$ of $\mathbb{N}$, and for convergent sequences $\left((a_n^{(j)})_{n\in\mathbb{N}}\right)_{j\in\mathcal{J}}$,

$$\lim_{n\to\infty} \max_{j\in\mathcal{J}} a_n^{(j)} = \max_{j\in\mathcal{J}} \lim_{n\to\infty} a_n^{(j)}, \tag{72}$$

which is obtained by induction from the case $|\mathcal{J}| = 2$, which in turn is obtained by continuity remarking that $\max\left(a_n^{(1)}, a_n^{(2)}\right) = \frac{1}{2}(a_n^{(1)} + a_n^{(2)} + |a_n^{(1)} - a_n^{(2)}|)$, (71c) holds because for any $b \in \mathcal{B}$, $\sum_{d\in\mathcal{D}} l_{d,b} = \tau_b \geqslant \tau_{b^*}$.

Appendix C
Proof of Lemma 4

We start by showing the following upper bound.

Lemma 7. *For any $b \in \mathcal{B}$, for any $\mathbf{z}^{b-1}$, for any opponent's strategy e, we have*

$$\sum_{\gamma_{\mathcal{L}}} \sum_{r_{\mathcal{L}}} \sum_{m_{\mathcal{L},b}} \mathbb{1}\left\{\mathcal{A}'_{\tau_b}(e)\right\} p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b} \middle| \mathbf{z}^{b-1}\right)$$
$$\leqslant |\mathcal{K}|^{n(\mathbf{v}^*)} \max_{\gamma_{\mathbf{v}^*}, r_{\mathbf{v}^*}} p\left(\gamma_{\mathbf{v}^*}, r_{\mathbf{v}^*} \middle| \mathbf{z}^{b-1}\right) \max_{\boldsymbol{\epsilon}\in\mathcal{E}} h(\boldsymbol{\epsilon}, b), \tag{73}$$

where we have defined

- *Λ_b, $\mathcal{E}$ as in* (27), (28) *in Section IV-A;*
- *For $\mathbf{l}_b \in \Lambda_b$,*

$$v(\mathbf{l}_b) \triangleq \left(v_{l_{d,b}}\right)_{d\in\mathcal{D}}, \tag{74}$$

  where for $d \in \mathcal{D}$, $v_{l_{d,b}}$ is a set of $l_{d,b}$ distinct elements of $\{q \in \mathcal{Q} : |\mathcal{G}_q| = c_d\}$. We let $\mathcal{V}(\mathbf{l}_b)$ be the set of all possible $v(\mathbf{l}_b)$;
- *For $\mathbf{l}_b \in \Lambda_b$, for $v(\mathbf{l}_b) \in \mathcal{V}(\mathbf{l}_b)$,*

$$n(v(\mathbf{l}_b)) \triangleq \sum_{d\in\mathcal{D}} l_{d,b} c_d, \tag{75}$$

$$\gamma_{v(\mathbf{l}_b)} \triangleq (\gamma_l)_{l\in\mathcal{G}_q, q\in v_{l_{d,b}}, d\in\mathcal{D}}, \tag{76}$$

$$r_{v(\mathbf{l}_b)} \triangleq (r_l)_{l\in\mathcal{G}_q, q\in v_{l_{d,b}}, d\in\mathcal{D}}; \tag{77}$$

- *And*

$$(\mathbf{l}^*, \mathbf{v}^*) \in \arg\max_{\mathbf{l}_b, v(\mathbf{l}_b)} \left(|\mathcal{K}|^{n(v(\mathbf{l}_b))} \max_{\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)}} p\left(\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)} \middle| \mathbf{z}^{b-1}\right) \right). \tag{78}$$

Proof: Define for any $c_d \in \mathcal{C}$, the set

$$\mathcal{I}_{\sigma,\widetilde{\sigma}}(c_d) \triangleq \{q \in \mathcal{Q} : |\mathcal{G}_q| = c_d \text{ and } \overline{\sigma}_q \text{ appears exactly } |\mathcal{G}_q| \text{ times in } (\widetilde{\sigma}_{l,b})_{l\in\mathcal{L}}\}. \tag{79}$$

Define the set $\widetilde{\Sigma}_b \triangleq \bigtimes_{d\in\mathcal{D}} \widetilde{\Sigma}_{d,b}$, where $\bigtimes$ denotes the Cartesian product, for $d \in \mathcal{D}$, $\widetilde{\Sigma}_{d,b}$ is the set of sequences made of $l_{d,b}$ distinct elements that appear exactly c_d times in $(\widetilde{\sigma}_{l,b})_{l\in\mathcal{L}}$. Let $\mathbf{a}_b \triangleq (a_{d,b})_{d\in\mathcal{D}}$ denote an element of $\widetilde{\Sigma}_b$. From these definitions and (74), we first show (80e) and (81d). The set Λ_b defined in Section IV-A will be used to indicate how many groups of size c_d are accepted. We have for any $\gamma_{\mathcal{L}}$, for any $r_{\mathcal{L}}$, for any opponent's attack e,

$$\mathbb{1}\left\{\mathcal{A}'_{\tau_b}(e)\right\} \tag{80a}$$

$$= \mathbb{1}\left\{ \bigcup_{\mathbf{l}_b} \bigcap_{c_d} \{|\mathcal{I}_{\sigma,\widetilde{\sigma}}(c_d)| = l_{d,b}\} \right\} \tag{80b}$$

$$= \mathbb{1}\left\{ \bigcup_{\mathbf{l}_b} \bigcup_{v(\mathbf{l}_b)} \bigcap_{c_d} \{\mathcal{I}_{\sigma,\widetilde{\sigma}}(c_d) = v_{l_{d,b}}\} \right\} \tag{80c}$$

$$= \mathbb{1}\left\{ \bigcup_{\mathbf{l}_b} \bigcup_{v(\mathbf{l}_b)} \bigcup_{\mathbf{a}_b} \bigcap_{c_d} \left\{ (\overline{\sigma}_q)_{q\in v_{l_{d,b}}} = a_{d,b} \text{ and } |\mathcal{I}_{\sigma,\widetilde{\sigma}}(c_d)| = l_{d,b} \right\} \right\} \tag{80d}$$

$$\leqslant \sum_{\mathbf{l}_b} \sum_{v(\mathbf{l}_b)} \sum_{\mathbf{a}_b} \mathbb{1}\left\{ \bigcap_{c_d} \left\{ (\overline{\sigma}_q)_{q\in v_{l_{d,b}}} = a_{d,b} \right\} \right\}, \tag{80e}$$

where in (80b) the union is over $\mathbf{l}_b \in \Lambda_b$ and the intersection is over $c_d \in \mathcal{C}$, in (80c) we have used the definition in (74) and the union is over $v(\mathbf{l}_b) \in \mathcal{V}(\mathbf{l}_b)$, in (80d) the union is over $\mathbf{a}_b \in \widetilde{\Sigma}_b$. Then, for any $\mathbf{l}_b \in \Lambda_b$, for any $v(\mathbf{l}_b) \in \mathcal{V}(\mathbf{l}_b)$, for any $\mathbf{a}_b \in \widetilde{\Sigma}_b$, using the definitions in (76) and (77) for $(\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)})$, we have

$$\sum_{\gamma_{v(\mathbf{l}_b)}} \sum_{r_{v(\mathbf{l}_b)}} \mathbb{1}\left\{ \bigcap_{c_d\in\mathcal{C}} \left\{ (\overline{\sigma}_q)_{q\in v_{l_{d,b}}} = a_{d,b} \right\} \right\} \times p\left(\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)} \middle| \mathbf{z}^{b-1}\right)$$
$$= \sum_{\gamma_{v(\mathbf{l}_b)}} \sum_{r_{v(\mathbf{l}_b)}} \mathbb{1}\left\{ \bigcap_{c_d\in\mathcal{C}} \left\{ (\overline{\gamma}_q)_{q\in v_{l_{d,b}}} = a_{d,b} \oplus (r_q)_{q\in v_{l_{d,b}}} \right\} \right\} \times p\left(\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)} \middle| \mathbf{z}^{b-1}\right) \tag{81a}$$

$$\leqslant \sum_{r_{v(\mathbf{l}_b)}} \max_{\gamma_{v(\mathbf{l}_b)}} p\left(\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)} \middle| \mathbf{z}^{b-1}\right) \tag{81b}$$

$$\leqslant \sum_{r_{v(\mathbf{l}_b)}} \max_{\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)}} p\left(\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)} \middle| \mathbf{z}^{b-1}\right) \tag{81c}$$

$$= |\mathcal{K}|^{n(v(\mathbf{l}_b))} \max_{\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)}} p\left(\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)} \middle| \mathbf{z}^{b-1}\right), \tag{81d}$$

where (81a) holds because by (45) $(\overline{\sigma}_q)_{q\in v_{l_{d,b}}} = \left(\overline{\gamma}_q \oplus r_q\right)_{q\in v_{l_{d,b}}}$, (81b) holds by definition of $\gamma_{v(\mathbf{l}_b)}$ and because at most one term is non zero in the sum $\sum_{\gamma_{v(\mathbf{l}_b)}}$ for a fixed $r_{v(\mathbf{l}_b)}$, (81d) holds by (75).

Define for an opponent's strategy e, the sequence $\boldsymbol{\epsilon} \triangleq (\epsilon_d)_{d\in\mathcal{D}}$, where for $d \in \mathcal{D}$, ϵ_d, is the number of elements of $(\widetilde{\sigma}_{l,b})_{l\in\mathcal{L}}$ that appears exactly c_d times. $\boldsymbol{\epsilon}$ is an element

of $\mathcal{E}$ defined in Section IV-A. We now use (80e) and (81d) as follows. For any $b \in \mathcal{B}$, for any $\mathbf{z}^{b-1}$, for any opponent's strategy e, we have

$$\sum_{\gamma_{\mathcal{L}}} \sum_{r_{\mathcal{L}}} \sum_{m_{\mathcal{L},b}} \mathbb{1}\left\{\mathcal{A}'_{\tau_b}(e)\right\} p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b} \middle| \mathbf{z}^{b-1}\right)$$

$$= \sum_{\gamma_{\mathcal{L}}} \sum_{r_{\mathcal{L}}} \mathbb{1}\left\{\mathcal{A}'_{\tau_b}(e)\right\} p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}} \middle| \mathbf{z}^{b-1}\right) \tag{82a}$$

$$\leqslant \sum_{\gamma_{\mathcal{L}}} \sum_{r_{\mathcal{L}}} \sum_{\mathbf{l}_b} \sum_{v(\mathbf{l}_b)} \sum_{\mathbf{a}_b} \mathbb{1}\left\{\bigcap_{c_d}\left\{(\overline{\sigma}_q)_{q \in v_{l_{d,b}}} = a_{d,b}\right\}\right\} \times p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}} \middle| \mathbf{z}^{b-1}\right) \tag{82b}$$

$$= \sum_{\mathbf{l}_b} \sum_{v(\mathbf{l}_b)} \sum_{\mathbf{a}_b} \sum_{\gamma_{v(\mathbf{l}_b)}} \sum_{r_{v(\mathbf{l}_b)}} \mathbb{1}\left\{\bigcap_{c_d}\left\{(\overline{\sigma}_q)_{q \in v_{l_{d,b}}} = a_{d,b}\right\}\right\} \times p\left(\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)} \middle| \mathbf{z}^{b-1}\right) \tag{82c}$$

$$\leqslant \sum_{\mathbf{l}_b} \sum_{v(\mathbf{l}_b)} \sum_{\mathbf{a}_b} |\mathcal{K}|^{n(v(\mathbf{l}_b))} \max_{\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)}} p\left(\gamma_{v(\mathbf{l}_b)}, r_{v(\mathbf{l}_b)} \middle| \mathbf{z}^{b-1}\right) \tag{82d}$$

$$\leqslant \sum_{\mathbf{l}_b} \sum_{v(\mathbf{l}_b)} \sum_{\mathbf{a}_b} |\mathcal{K}|^{n(\mathbf{v}^*)} \max_{\gamma_{\mathbf{v}^*}, r_{\mathbf{v}^*}} p\left(\gamma_{\mathbf{v}^*}, r_{\mathbf{v}^*} \middle| \mathbf{z}^{b-1}\right) \tag{82e}$$

$$= |\mathcal{K}|^{n(\mathbf{v}^*)} \max_{\gamma_{\mathbf{v}^*}, r_{\mathbf{v}^*}} p\left(\gamma_{\mathbf{v}^*}, r_{\mathbf{v}^*} \middle| \mathbf{z}^{b-1}\right) \times \sum_{\mathbf{l}_b} \prod_{d \in \mathcal{D}} \binom{n_d}{l_{d,b}} \binom{\epsilon_d}{l_{d,b}} l_{d,b}! \tag{82f}$$

$$\leqslant |\mathcal{K}|^{n(\mathbf{v}^*)} \max_{\gamma_{\mathbf{v}^*}, r_{\mathbf{v}^*}} p\left(\gamma_{\mathbf{v}^*}, r_{\mathbf{v}^*} \middle| \mathbf{z}^{b-1}\right) \times \max_{\boldsymbol{\epsilon} \in \mathcal{E}} \sum_{\mathbf{l}_b} \prod_{d \in \mathcal{D}} \binom{n_d}{l_{d,b}} \binom{\epsilon_d}{l_{d,b}} l_{d,b}!, \tag{82g}$$

where (82a) holds by marginalization over $m_{\mathcal{L},b}$ since $\mathcal{A}'_{\tau_b}(e)$ is independent of $m_{\mathcal{L},b}$, (82b) holds by (80e), (82c) holds by marginalization over $\gamma_{\mathcal{L}} \backslash \gamma_{v(\mathbf{l}_b)}$, and $r_{\mathcal{L}} \backslash r_{v(\mathbf{l}_b)}$, (82d) holds by (81d), in (82e) we have used the Definition in (78), (82f) holds because

$$|\mathcal{V}(\mathbf{l}_b)| = \prod_{d \in \mathcal{D}} \binom{n_d}{l_{d,b}}, \quad |\widetilde{\Sigma}_b| = \prod_{d \in \mathcal{D}} \frac{\epsilon_d!}{(\epsilon_d - l_{d,b})!} \mathbb{1}\{\epsilon_d \geqslant l_{d,b}\}, \tag{83}$$

in (82g) we maximize the right hand side over $\boldsymbol{\epsilon} \in \mathcal{E}$ to obtain an upper bound valid for any opponent's strategy e. ∎

We now use Lemma 8 to simplify the upper bound found in Lemma 7 when $N \to \infty$.

Lemma 8. *Let A and B be two randoms variables over the finite alphabets $\mathcal{A}$ and $\mathcal{B}$, jointly distributed according to p_{AB}. For any $\epsilon \geqslant 0$, if $I(A;B) \leqslant \epsilon$, then*

$$0 \leqslant 2^{-H_\infty(A|B)} - 2^{-H_\infty(A)} \leqslant 2\left(2 \ln 2\right)^{1/4} \epsilon^{1/4}, \tag{84}$$

where $H_\infty(A) \triangleq -\log\left(\max_{a \in \mathcal{A}} p_A(a)\right)$ is the min-entropy of A, and $H_\infty(A|B) \triangleq -\log\left(\sum_{b \in \mathcal{B}} p_B(b) \max_{a \in \mathcal{A}} p_{A|B}(a|b)\right)$ is the average min-entropy of A given B.

Proof: See Appendix D. ∎

Consider $\mathbf{v}^*$ in Definition (78), we write it as $\mathbf{v}^* = v^*(\mathbf{l}_b^*)$ with $\mathbf{l}_b^* = (l_{d,b}^*)_{d \in \mathcal{D}}$, and define

$$\Gamma_{\mathbf{v}^*} \triangleq (\Gamma_l)_{l \in \mathcal{G}_q, q \in v^*_{l^*_{d,b}}, d \in \mathcal{D}}, \tag{85}$$

$$R_{\mathbf{v}^*} \triangleq (R_l)_{l \in \mathcal{G}_q, q \in v^*_{l^*_{d,b}}, d \in \mathcal{D}}. \tag{86}$$

We then have

$$\mathbb{E}_{\mathbf{Z}^{b-1}}\left[\sup_e \left\{\sum_{\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b}} \mathbb{1}\left\{\mathcal{A}'_{\tau_b}(e)\right\} p\left(\gamma_{\mathcal{L}}, r_{\mathcal{L}}, m_{\mathcal{L},b} \middle| \mathbf{z}^{b-1}\right)\right\}\right]$$

$$\leqslant \mathbb{E}_{\mathbf{Z}^{b-1}}\left[|\mathcal{K}|^{n(\mathbf{v}^*)} \max_{\gamma_{\mathbf{v}^*}, r_{\mathbf{v}^*}} p\left(\gamma_{\mathbf{v}^*}, r_{\mathbf{v}^*} \middle| \mathbf{z}^{b-1}\right) \max_{\boldsymbol{\epsilon} \in \mathcal{E}} h(\boldsymbol{\epsilon}, b)\right] \tag{87a}$$

$$= |\mathcal{K}|^{n(\mathbf{v}^*)} 2^{-H_\infty\left(\Gamma_{\mathbf{v}^*} R_{\mathbf{v}^*} \middle| \mathbf{Z}^{b-1}\right)} \max_{\boldsymbol{\epsilon} \in \mathcal{E}} h(\boldsymbol{\epsilon}, b) \tag{87b}$$

$$\leqslant |\mathcal{K}|^{n(\mathbf{v}^*)} \left(2^{-H_\infty(\Gamma_{\mathbf{v}^*} R_{\mathbf{v}^*})} + 2\left(2 \ln 2\right)^{1/4} \delta(N)^{(1/4)}\right) \times \max_{\boldsymbol{\epsilon} \in \mathcal{E}} h(\boldsymbol{\epsilon}, b) \tag{87c}$$

$$= \left(\frac{1}{|\mathcal{K}|^{\tau_b}} + 2\left(2 \ln 2\right)^{1/4} \delta(N)^{(1/4)} |\mathcal{K}|^{n(\mathbf{v}^*)}\right) \max_{\boldsymbol{\epsilon} \in \mathcal{E}} h(\boldsymbol{\epsilon}, b) \tag{87d}$$

$$\xrightarrow{N \to \infty} \frac{\max_{\boldsymbol{\epsilon} \in \mathcal{E}} h(\boldsymbol{\epsilon}, b)}{|\mathcal{K}|^{\tau_b}}, \tag{87e}$$

where (87a) holds by Lemma 7, (87c) holds by Lemma 8 and strong secrecy – see (24f) in the proof of Proposition 1, (87d) holds because $\Gamma_{\mathbf{v}^*}$ contains $\sum_{d \in \mathcal{D}} l_{d,b}^* = \tau_b$ independent sequences uniformly distributed over $\mathcal{K}$, which are independent of $R_{\mathbf{v}^*}$, which in turn, is a sequence of $\sum_{d \in \mathcal{D}} l_{d,b}^* c_d = n(\mathbf{v}^*)$ sequences uniformly distributed over $\mathcal{K}$.

Appendix D
Proof of Lemma 8

We define the variational distance between p_{AB} and $p_A p_B$ as $\mathbb{V}(p_{AB}, p_A p_B) \triangleq \sum_{a \in \mathcal{A}, b \in \mathcal{B}} |p_{AB}(a,b) - p_A(a) p_B(b)|$. For any $b \in \mathcal{B}$, define $v(b) \triangleq \sum_{a \in \mathcal{A}} |p(a|b) - p(a)|$ so that $\mathbb{V}(p_{AB}, p_A p_B) = \mathbb{E}_B[v(b)]$. Note that, for any $\alpha > 0$, by Markov's inequality, we have

$$\mathbb{P}[v(B) \geqslant \alpha] \leqslant \frac{\mathbb{V}(p_{AB}, p_A p_B)}{\alpha}. \tag{88}$$

We then have

$$2^{-H_\infty(A|B)}$$

$$= \sum_{b \in \mathcal{B}} p(b) \max_{a \in \mathcal{A}} p(a|b) \tag{89a}$$

$$= \sum_{\substack{b \in \mathcal{B} \\ v(b) < \alpha}} p(b) \max_{a \in \mathcal{A}} p(a|b) + \sum_{\substack{b \in \mathcal{B} \\ v(b) \geqslant \alpha}} p(b) \max_{a \in \mathcal{A}} p(a|b) \tag{89b}$$

$$\leqslant \sum_{\substack{b \in \mathcal{B} \\ v(b) < \alpha}} p(b) \left(v(b) + \max_{a \in \mathcal{A}} p(a)\right) + \sum_{\substack{b \in \mathcal{B} \\ v(b) \geqslant \alpha}} p(b) \tag{89c}$$

$$\leqslant \alpha + 2^{-H_\infty(A)} + \frac{\mathbb{V}(p_{AB}, p_A p_B)}{\alpha} \tag{89d}$$

$$\leqslant 2\mathbb{V}(p_{AB}, p_A p_B)^{1/2} + 2^{-H_\infty(A)} \tag{89e}$$

$$\leqslant 2\left(\sqrt{2 \ln 2} \sqrt{\mathbb{D}(p_{AB} || p_A p_B)}\right)^{1/2} + 2^{-H_\infty(A)} \tag{89f}$$

$$= 2\left(2 \ln 2\right)^{1/4} I(A;B)^{1/4} + 2^{-H_\infty(A)}, \tag{89g}$$

where (89c) holds because $\forall b, |p(a^*|b) - p(a^*)| \leqslant v(b)$ where $a^* \in \arg\max_{a \in \mathcal{A}} p(a|b)$, and because $\forall a, b, p(a|b) \leqslant 1$,

(89d) holds because $\sum_{\substack{b\in\mathcal{B}\\ v(b)<\alpha}} p(b) \leqslant 1$ and by (88), (89e) is obtained by choosing the α that minimizes $\alpha + \frac{\mathbb{V}(p_{AB},p_Ap_B)}{\alpha}$, i.e, $\alpha = \mathbb{V}(p_{AB}, p_Ap_B)^{1/2}$, (89f) holds by Pinsker's inequality and letting $\mathbb{D}(\cdot||\cdot)$ denote the Kullback-Leibler divergence. Finally, to show $0 \leqslant 2^{-H_\infty(A|B)} - 2^{-H_\infty(A)}$, we remark that

$$H_\infty(A|B) = -\log\left(\sum_{b\in\mathcal{B}} p(b)\max_{a\in\mathcal{A}} p(a|b)\right) \tag{90a}$$

$$\leqslant -\log\left(\max_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}} p(b)p(a|b)\right) \tag{90b}$$

$$= H_\infty(A). \tag{90c}$$

REFERENCES

[1] R. A. Chou and A. Yener, "Multiuser authentication with anonymity constraints over noisy channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 2439–2443.

[2] G. J. Simmons, "Authentication theory/coding theory," in *Advances in Cryptology*. Berlin, Germany: Springer, 1985, pp. 411–431.

[3] M. Walker, "Information-theoretic bounds for authentication schemes," *J. Cryptol.*, vol. 2, no. 3, pp. 131–143, 1990.

[4] U. Rosenbaum, "A lower bound on authentication after having observed a sequence of messages," *J. Cryptol.*, vol. 6, no. 3, pp. 135–156, 1993.

[5] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1350–1356, Jul. 2000.

[6] E. Martinian, G. W. Wornell, and B. Chen, "Authentication with distortion criteria," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2523–2542, Jul. 2005.

[7] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[8] C. G. Boncelet, "The NTMAC for authentication of noisy messages," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 35–42, Mar. 2006.

[9] Y. Liu and C. Boncelet, "The CRC–NTMAC for noisy message authentication," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 4, pp. 517–523, Dec. 2006.

[10] 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, no. 7, pp. 2571–2579, Jul. 2008.

[11] L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 906–916, Feb. 2009.

[12] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proc. IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.

[13] I. Csiszár, "Almost independence and secrecy capacity," *Problems Inf. Transmiss.*, vol. 32, no. 1, pp. 40–47, Jan./Mar. 1996.

[14] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. IEEE Inf. Theory Workshop*, Aug. 2010, pp. 1–5.

[15] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[16] A. J. Pierrot and M. R. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 595–605, Sep. 2011.

[17] R. A. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 64, no. 12, pp. 7903–7921, Dec. 2018.

Rémi A. Chou (M'17) received the Engineering degree from Supélec, Gif-sur-Yvette, France, in 2011, and the Ph.D. degree in Electrical Engineering from the Georgia Institute of Technology, Atlanta, GA, in 2015. From 2015 to 2017, he was a postdoctoral scholar at The Pennsylvania State University, University Park, PA. He is now an Assistant Professor in the Electrical Engineering and Computer Science Department at Wichita State University, Wichita, KS.

Aylin Yener (S'91–M'01–SM'14–F'15) received the B.Sc. degree in electrical and electronics engineering and the B.Sc. degree in physics from Bogazici University, Istanbul, Turkey, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Wireless Information Network Laboratory (WINLAB), Rutgers University, New Brunswick, NJ, USA. She is a Distinguished Professor of Electrical Engineering at The Pennsylvania State University, University Park, PA, USA, where she joined the faculty as an assistant professor in 2002. Since 2017, she is also a Dean's Fellow in the College of Engineering at The Pennsylvania State University. She was a visiting professor of Electrical Engineering at Stanford University in 2016-2018 and a visiting associate professor in the same department in 2008-2009. Her current research interests are in information security, green communications, caching systems, and more generally in the fields of information theory, communication theory and networked systems. She received the NSF CAREER Award in 2003, the Best Paper Award in Communication Theory from the IEEE International Conference on Communications in 2010, the Penn State Engineering Alumni Society (PSEAS) Outstanding Research Award in 2010, the IEEE Marconi Prize Paper Award in 2014, the PSEAS Premier Research Award in 2014, the Leonard A. Doggett Award for Outstanding Writing in Electrical Engineering at Penn State in 2014, the IEEE Women in Communications Engineering Outstanding Achievement Award in 2018, and the IEEE Communications Society Best Tutorial Paper Award in 2019. She is a distinguished lecturer for the IEEE Information Theory Society (2019-2020), the IEEE Communications Society (2018-2020) and the IEEE Vehicular Technology Society (2017-2021).

Dr. Yener is serving as the vice president of the IEEE Information Theory Society in 2019. Previously she was the second vice president (2018), member of the Board of Governors (2015-2018) and the treasurer (2012-2014) of the IEEE Information Theory Society. She served as the Student Committee Chair for the IEEE Information Theory Society (2007-2011), and was the co-Founder of the Annual School of Information Theory in North America in 2008. She was a Technical (Co)-Chair for various symposia/tracks at the IEEE ICC, PIMRC, VTC, WCNC, and Asilomar in 2005, 2008-2014 and 2018. Previously, she served as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS (2009-2012), an Editor for the IEEE TRANSACTIONS ON MOBILE COMPUTING (2017-2018), and an Editor and an Editorial Advisory Board Member for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS (2001-2012). She also served as a Guest Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY in 2011, and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS in 2015. Currently, she serves as a Senior Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS and is on the inaugural Senior Editorial Board of the IEEE JOURNAL ON SELECTED AREAS IN INFORMATION THEORY.