This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

Physical Layer based Message Authentication with Secure Channel Codes

Dajiang Chen, *Member, IEEE*, Ning Zhang, *Member, IEEE*, Nan Cheng, *Member, IEEE*, Kuan Zhang, *Member, IEEE*, Zhiguang Qin, *Member, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—In this paper, we investigate physical (PHY) layer message authentication to combat adversaries with infinite computational capacity. Specifically, a PHY-layer authentication framework over a wiretap channel (W_1, W_2) is proposed to achieve information-theoretic security with the same key. We develop a theorem to reveal the requirements/conditions for the authentication framework to be information-theoretic secure for authenticating a polynomial number of messages in terms of n. Based on this theorem, we design an authentication protocol that can guarantee the security requirements, and prove its authentication rate can approach infinity when n goes to infinity. Furthermore, we design and implement a feasible and efficient message authentication protocol over binary symmetric wiretap channel (BSWC) by using *Linear Feedback Shifting Register* based (LFSR-based) hash functions and strong secure polar code. Through extensive simulations, it is demonstrated that the proposed protocol can achieve high authentication rate, with low time complexity and authentication error rate.**

***Index Terms*—Physical layer security, Message authentication, Wiretap channel, Polar codes, LFSR-based hash functions, Strong secure channel coding.**

I. Introduction

Confidentiality, *Integrity*, and *Authentication* are the fundamental requirements for information security. Confidentiality ensures information is not available to unauthorized entities, integrity protects information accuracy and completeness during transmission, while authentication mainly assures the source of information. To provision those security functions, the typical approach is through upper-layer cryptographic algorithms/protocols, which usually provides computational security and might be comprised as the computation power of adversaries keeps increasing.

This work is an extension of our previous work in IEEE MASS 2017 [1]. This work is jointly supported by Natural Sciences and Engineering Research Council (NSERC) of Canada, NSFC (No. 61502085, No. 61520106007, No. 61472064), and China Postdoctoral Science Foundation funded project (No. 2015M570775).

Dajiang Chen and Zhiguang Qin are with the School of information and software engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China (Email: dajiang.chen@uwaterloo.ca; qinzg@uestc.edu.cn)

Ning Zhang is with the Department of Computing Science, Texas A&M University-Corpus Christi, Corpus Christi, TX 78412, USA (e-mail: ning.zhang@tamucc.edu)

Nan Cheng and Xuemin (Sherman) Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: n5cheng@uwaterloo.ca; sshen@uwaterloo.ca)

Kuan Zhang is with Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Omaha, NE 68182, USA (e-mail: kuan.zhang@unl.edu)

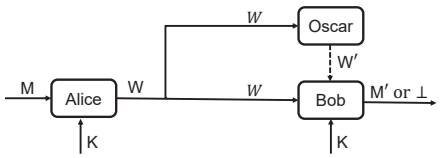


Fig. 1. The authentication model over noiseless channels.

As a complement, there is a flurry of research to provision information-theoretic security from the physical (PHY) layer [2]–[6]. Information-theoretic security can ensure the aforementioned security attributes, even though adversaries have infinite computational capabilities. Based on the security objective, PHY-layer security can be roughly divided into two categories: PHY-layer secure transmission and PHY-layer message authentication, where the former targets confidentiality while the latter focuses on message integrity and sender authentication. In the literature, the two research areas are usually separately studied. In addition, there is extensive research on PHY-layer secure message transmission, aiming to improve the secrecy rate at which message can be securely delivered [7]–[14]. In contrast, PHY-layer message authentication is inadequately studied, and needs further investigation.

In the line of PHY-layer message authentication, the pioneering work by Simmons [16] proposes an authentication model over noiseless channels, as shown in Fig. 1. Alice intends to send a message M to Bob, while an adversary Oscar might launch two different types of man-in-the-middle attacks: 1) *impersonation attack*: forge the sender of the message; or 2) *substitution attack*: modify or replace the message. It is assumed that Alice and Bob share a common secret key K in advance, which helps Bob identify the source of the message. The message M and the key K have distributions P_M over message space $\mathcal{M}$ and P_K over key space $\mathcal{K}$, respectively. Alice maps a pair (M, K) to a codeword W, and sends W over the noiseless channel. The adversary succeeds if Bob decodes the adversary's message and accepts it as a valid message from Alice. When performing multiple-message authentication, it is found that this model causes an entropy loss of the key. In fact, after l times of authentication, the probability for successful attacks is at least $2^{-H(K)/(l+1)}$, which approaches 1 quickly as l increases [17], where $H(K)$ is the entropy of K.

In this paper, we aim to i) achieve information-theoretic security for multiple messages authentication with the same key; and ii) bridge the two separate areas of research in PHY-layer security. We propose a multi-message authentication

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

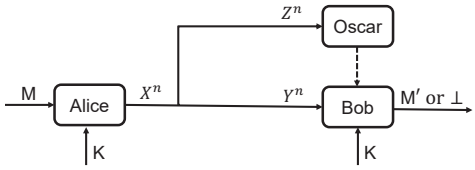


Fig. 2. The authentication model over noise channels.

framework over wiretap channel (as shown in Fig. 2), which integrates existing secure channel coding to achieve a high authentication rate. Specifically, Alice first encodes M to X^{ν} using an error-correcting code, where ν is the length of the error-correcting code. Then, Alice generates a message tag S of M using a hash function and employs a secure channel coding to encode S to X^n, where n is the length of the secure channel coding. Finally, Alice transmits (X^{ν}, X^n) over wiretap channel (W_1, W_2). Suppose that $< X^{\nu}, X^n >$ arrives at Bob as $< Y^{\nu}, Y^n >$, where Bob decodes Y^{ν} to M' by the decoding function of the error-correcting code and decodes Y^n to S' with the secure channel decoder. Bob decides to accept or reject the message by verifying the consistency of $< M', S' >$ (i.e., whether S' is the tag of M'). To achieve information-theoretical security for a polynomial number of messages and attacks, we obtain a theorem (i.e., Theorem 1), which states the requirements/conditions for a authentication protocol to be information-theoretic secure to authenticate a polynomial number of messages. Furthermore, based on this theorem, an authentication protocol with high efficiency is proposed. The authentication rate of the proposed authentication protocol approaches infinity when n goes to infinity.

Based on theoretical analysis, we construct a feasible and efficient authentication protocol over binary symmetric wiretap channel (BSWC) by using Linear Feedback Shifting Register based (LFSR-based) hashing functions and strong secure polar codes. Moreover, we evaluate the proposed protocol via extensive experiments. The results demonstrate that, 1) by decreasing the secure rate, the strong secure coding scheme can provide the reliability of the main channel; and 2) the proposed authentication scheme has low time cost, high authentication rate, and low authentication error rate.

The main contributions of this paper is summarized as follows.

- A multiple message authentication framework with the same secret key K is proposed over wiretap channels. A theorem on the conditions for the authentication protocols to be information-theoretical secure is provided, with rigorous mathematical proof.
- Based on obtained theorem, an authentication protocol is devised to achieve information-theoretic security with high efficiency. The authentication rate $\rho_{auth} = \rho_{tag} \cdot (C_s - \delta)$ for any fixed tag rate ρ_{tag} and any small $\delta > 0$. The authentication rate can approach infinity with n, where n is the length of secure channel code X^n.
- We bridge the gap between PHY-layer secure transmission and PHY-layer message authentication. With the proposed framework and theorem, a strong secure channel coding with exponentially small (in code length n) average probability of error can induce a multi-message authentication with information-theoretic security.
- A feasible and efficient authentication protocol over B-SWC is proposed by leveraging the lightweight LFSR-based hashing functions and secure polar codes. Extensive experiments validate the feasibility and efficiency of the proposed protocol.

The remainder of the paper is organized as follows. The related work is reviewed in Section II. Section III introduces basic concepts and preliminaries used in the paper. Section IV presents the system model, including the authentication model, the adversary model, and security definitions. In Section V, a multiple-message authentication framework is proposed, and the theorem for authentication protocol to achieve information-theoretical security is provided. In Section VI, we propose a multi-message authentication protocol and analyze its efficiency. Section VII presents an efficient and feasible authentication protocol over BSWC. In Section VIII, we give the simulation studies for authentication over BSWC. The concluding remarks are provided in Section IX.

II. Related Work

A. PHY-Layer Secure Transmission:

The pioneering work on PHY-layer secure transmission in Wyner [12], demonstrated that information-theoretic security can be achieved, if the received signal at the attacker is a degraded version of that at the destination. This result was generalized by Csiszár and Köner [13], in which the attacker's channel is not necessary to be a degraded version of the receiver's channel. Afterwards, secure transmission over noisy channels were extensively investigated in both theory and implementations [7]–[11], [14], [15]. Particularly, in [7], a coset coding scheme with the low-density parity-check (LDPC) code was proposed to achieve weak secrecy on a binary erasure wiretap channel (BEWC). Extending this result, a coding scheme was presented by leveraging the dual of short-cycle-free LDPC code to achieve the strong secrecy on a BEWC in [8]. Subramanian *et al.* [9] proposed a strong secure channel coding scheme for binary erasure wiretap channel models (i.e., both the main cannel and the wiretapper's channel are binary erasure channels) by using large-girth LDPC codes. In [10], a channel coding scheme with polar code was proposed to achieve the strong secrecy capacity of general degraded and symmetric wiretap channels. Mahdavifar *et al.* [11] devised another channel coding algorithm based on polar codes for binary symmetric wiretap channel models (i.e., both the main channel and the wiretapper's channel are binary symmetric channels). Other related works such as [36] and [37] considered secure transmission from the perspective of signal processing instead of secure channel coding. Specifically, [36] studied secure transmission by using full-duplex jamming techniques against randomly located eavesdropper in decentralized wireless networks. [37] proposed a hybrid full-/half-duplex receiver deployment strategy to secure the transmission of legitimate nodes in wireless ad-hoc networks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

B. PHY-Layer Message Authentication:

PHY-layer message authentication can be traced back to Simmons' work in [16], where an authentication model over noiseless channels was proposed. Recently, authentication over noise channel models drawn increasing attentions [21]–[25]. The authentication over noise source model with a (noiseless) public discussion channel was studied by Korzhik *et al.* [21]. To achieve information-theoretic security for multiple messages authentication, Lai et al. [22] studied the message authentication over noisy channel, as shown in Fig. 2, where the channels from Alice to Bob and from Alice to Oscar can be regarded as a *wiretap channel model* (please refer to Section III-C). However, the authentication efficiency was bounded by the capacity of the channel from Alice to the adversary, denoted as $I(X;Z)$. After that, Jiang considered the keyless authentication problem in a noise channel model in [23], [24]. More recently, the security of physical layer message integrity protection scheme was studied by Pan *et al.* in [25], in which, a signal cancellation attack framework is established to model the attacker's behavior, and a physical layer message integrity protection approach with reconfigurable antenna is proposed based on the framework. The other related works also includes [33]–[35]. In [33], a physical layer authentication mechanism was proposed by using the multi-path effect between the sender and the receiver. In [35], a wireless physical-layer identification protocol was presented by utilizing the unique features of the physical waveforms of wireless signals.

Different from the existing works, this work focuses on multi-message authentication over wiretap channels with the same key. We integrate strong secure channel coding in the authentication framework to achieve information-theoretical security. The conditions for the authentication protocol to be secure are obtained. With the proposed framework, we bridge the gap between PHY-layer secure transmission and PHY-layer message authentication. In this way, any advances of the area of (computationally efficient) secure channel coding will result in the improvement of message authentication. Moreover, we propose an authentication protocol which can satisfy the security requirements, with the efficiency of $\rho_{tag} \cdot (I(X;Y) - I(X;Z) - \delta)$ which approaches infinity with n. Furthermore, an efficient authentication protocol over BSWC is proposed by leveraging secure polar codes and lightweight LFSR-based hashing functions.

III. Preliminaries

Notations: Random variables are denoted by $X, Y, Z, \cdots$, and their realizations are denoted by $x, y, z, \cdots$, with the domain of a random variable is denoted by $\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \cdots$. Probabilities $P(X = x)$ and $P(X = x|Y = y)$ are denoted by $P_X(x)$ and $P_{X|Y}(x|y)$, or $P(x)$ and $P(x|y)$, respectively. x^n denotes a sequence of $x_1, \cdots, x_n$. The following information theory terms can be found in [18].

- $I(X;Y) = \sum_{x,y} P(x,y) \log \frac{P(x,y)}{P(x)P(y)}$ is the *mutual information* between X and Y. $H(X) = -\sum_x P(x) \log P(x)$ and $H(X|Y) = -\sum_{x,y} P(x,y) \log P(x|y)$ is the *entropy* function and *conditional entropy* function, respectively.
- The *type* of a sequence $x^n \in \mathcal{X}^n$ is the distribution P_{x^n} on $\mathcal{X}$ defined by $P_{x^n}(a) = \frac{1}{n} N(a|x^n)$ for every $a \in \mathcal{X}$, where $N(a|x^n)$ is the number of occurrences of $a \in \mathcal{X}$ in x^n. For any type P of length n on $\mathcal{X}$, the set of sequences in $\mathcal{X}^n$ with type P is called a *type class* and is denoted by T_P^n.
- *Distance* between random variables X and X' over $\mathcal{X}$ is $SD(X;X') = \sum_{x \in \mathcal{X}} |P_X(x) - P_{X'}(x)|$. *Conditional distance between X and X given Y* is defined as

$$\mathtt{SD}(X|Y;X) = \sum_{y \in \mathcal{Y}} P(y) \sum_{x \in \mathcal{X}} |P(x|y) - P(x)|. \quad (1)$$

- Function $negl(n)$ is negligible in n if for any polynomial $poly(n)$, $lim_{n \to \infty} negl(n) poly(n) = 0$.

A. Universal Hash Functions

Any function $f : A \to B$ with $|A| > |B|$ is called a *hash function*. A universal hash function is a hash function such that the output frequency occurs almost uniformly [26]–[29]. We define the family of almost universal hash functions as follows.

Definition 1. *Let $\mathcal{M}$ and $\mathcal{S}$ be two finite sets. For $\varepsilon > 0$, a collection of functions Ψ from $\mathcal{M}$ to $\mathcal{S}$ is called ε-almost weak universal (ε-AWU$_2$) if*

$$\forall (m,s) \in \mathcal{M} \times \mathcal{S}, \quad \Pr[\psi : \psi(m) = s] \le \varepsilon; \quad (2)$$

$$\forall m_1, m_2 (\neq m_1) \in \mathcal{M}, \quad \Pr[\psi : \psi(m_1) = \psi(m_2)] \le \varepsilon. \quad (3)$$

The family of hash functions is ε-almost universal (ε-AU$_2$) if the first condition is replaced by

$$\forall (m,s) \in \mathcal{M} \times \mathcal{S}, \quad \Pr[\psi : \psi(m) = s] = 1/|\mathcal{S}|. \quad (4)$$

B. Discrete Memoryless Channel

A discrete channel $W : \mathcal{X} \to \mathcal{Y}$ with input alphabet $\mathcal{X}$ and output alphabet $\mathcal{Y}$ is defined as a stochastic matrix $W = \{W(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$. In this paper, we consider a *discrete memoryless channel* (DMC): suppose that the input sequence is $x^n = x_1, \cdots, x_n$ and the output sequence is $y^n = y_1, \cdots, y_n$, then $P_{Y^n|X^n}(y^n|x^n) = \prod_{i=1}^n P_{Y_i|X_i}(y_i|x_i) = \prod_{i=1}^n W(y_i|x_i)$. For simplicity, we denote $\prod_{i=1}^n W(y_i|x_i)$ by $W(y^n|x^n)$.

Consider Alice wants to send messages to Bob over DMC W. The message domain is $\mathcal{S}$. The communication is described through a pair of mappings (called a *coding scheme*) (f,g), where $f : \mathcal{S} \to \mathcal{X}^n$ and $g : \mathcal{Y}^n \to \mathcal{S} \cup \{\perp\}$. When Alice wants to send $s \in \mathcal{S}$, he sends $f(s)$ through channel W. When Bob receives vector y^n, he decodes the message as $s' = g(y^n)$, where $\perp$ denotes the detector of an error. Event $s \neq s'$ is called a *decoding error*. The set $\mathcal{C} = f(\mathcal{S})$ is called the *code book* of this coding scheme; and $c = f(s)$ is called a *codeword*.

C. Basics of Wiretap Channel

A *wiretap channel* is defined by two DMCs $W_1 : \mathcal{X} \to \mathcal{Y}$ and $W_2 : \mathcal{X} \to \mathcal{Z}$, where $\mathcal{X}$ is the input alphabet from the sender Alice, and $\mathcal{Y}$ and $\mathcal{Z}$ are the output alphabets at the legitimate receiver Bob and the wiretapper Oscar respectively. Alice aims to send private messages to Bob against Oscar. Denote the domain of message of Alice by $\mathcal{S}$. To send $s \in \mathcal{S}$, Alice sends

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

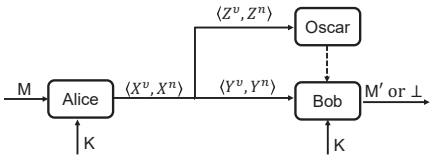


Fig. 3. The authentication model.

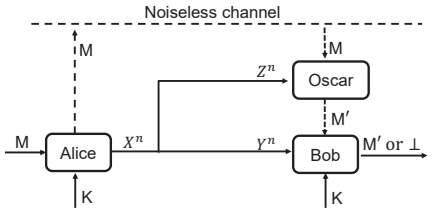


Fig. 4. The conceptual authentication model.

it through W_1 with a coding scheme (f,g). Specifically, she first sends $x^n = f(s)$ into DMCs W_1 and W_2, from which Bob receives $y^n \in \mathcal{Y}^n$ and Oscar receives $z^n \in \mathcal{Z}^n$. Bob decodes $s' = g(y^n) \in \mathcal{S} \cup \{\perp\}$. Let X^n, Y^n, Z^n, S, S' be random variables for x^n, y^n, z^n, s, s' respectively. $\frac{1}{n}\log|\mathcal{S}|$ is the *transmission rate*.

The goal of Alice and Bob is to maximize the transmission rate while keeping Oscar from knowing anything regarding S. The security is defined as follows.

Definition 2. *The sequence of coding schemes $\{(f_n, g_n)\}_n$ is called strong secure channel coding with exponentially small (in n) average probability of error for the wiretap channel (W_1, W_2) (denoted as* **strong secure channel coding** *for short), if the following conditions are satisfied:*

$$\textit{Reliability Condition:} \quad \Pr\{S' \neq S\} \to 0, \tag{5}$$

$$\textit{Strong Security Condition:} \quad I(S;Z^n) \to 0 \ \textit{exponencially}, \tag{6}$$

when $n \to \infty$. For $R > 0$, if $\frac{1}{n}\log|\mathcal{S}| \geq R$, we called rate R is securely achievable for (W_1, W_2). The supremum of securely achievable rates is called secret capacity of the wiretap channel and is denoted by C_s.

IV. System Model

In this section, the authentication model is first presented, and the adversary model and the definition of secure authentication protocol are then elaborated.

A. Authentication Model

We consider a wiretap channel $W_1 : \mathcal{X} \to \mathcal{Y}$, $W_2 : \mathcal{X} \to \mathcal{Z}$. Alice and Bob share a key K that is uniformly in a set $\mathcal{K}$. They are connected by channel W_1. When Alice sends $X \in \mathcal{X}$, Bob and Oscar will receive $Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$, respectively. Moreover, there is a noiseless channel from Oscar to Bob. Due to the fact that any noisy channel can be simulated with a noiseless channel by randomizing the transmitted signal, the noiseless channel actually gives Oscar an advantage. Note that, the noiseless channel and noisy channel are the same wireless medium, where the former employs an error-correcting code. Let $\mathcal{M}$ be a set of messages. As shown in Fig. 3, when Alice attempts to send $M \in \mathcal{M}$ to Bob, they perform the following procedure.

- Alice encodes M into X^{v} with an error-correcting code for channel W_1, and then transmits it to Bob over channel W_1, and then, encodes (M,K) into $X^n \in \mathcal{X}^n$ as an authentic with an encoder f and sends it over (W_1, W_2).
- Bob receives Y^{v} and Y^n from channel W_1. He then decodes M' from Y^{v} with the error-correcting code and decodes $D \in \{\top, \perp\}$ from M', Y^n and K using a decoder (or decider) g, where $D = \top$ means that Bob accept M' and $D = \perp$ means that Bob rejects M'.

Here, when $D = \top$, Alice indeed sends M and $M = M'$, i.e., the decoded message M' indeed is authenticated from Alice.

Without loss of generality, we regard the information transmission with an error-correcting code (e.g. LDPC code, Polar code, and convolution code) as the information transmission over a noiseless channel. For ease of presentation, we adopt a conceptual authentication framework (as shown in Fig. 4), in which, we assume that there exists a noiseless channel from Alice to Bob which is full controlled by Oscar. Then, the authentication is performed as follows:

- Alice sends M over a public but unauthenticated noiseless channel, and then, encodes (M,K) into X^n as an authentic with an encoder f and sends X^n over (W_1, W_2).
- Bob receives M' from the output of noiseless channel and Y^n from the output of channel W_1. He then decodes $D \in \{\top, \perp\}$ from M', Y^n and K using a decoder (or decider) g, where $D = \top$ means that Bob receives M' and $D = \perp$ means that Bob rejects M'.

The proposed authentication model can be applied for message authentication to enhance security in many scenarios, including device-to-device (D2D) communications, Near Field Communications, and so on, in which two mobile users can communicate directly, in the presence of adversaries, without traversing base stations or core networks.

B. Adversary Model

The communication link between Alice and Oscar is characterized by Channel W_2 and the link between Oscar and Bob is *noiseless*. Oscar's attack capability is formalized as follows.

1. He can adaptively request Alice to authenticate any message M of his choice. As a result, Alice normally authenticates M to Bob through channel (W_1, W_2), and Oscar receives Z^n from Channel W_2.
2. He can adaptively send any message $M' \in \mathcal{M}$ and vector $Y'^n \in \mathcal{Y}^n$ to Bob. Bob then decodes M', Y'^n and K into $D \in \{\top, \perp\}$. Oscar succeeds (denoted by *Succ*) if $D = \top$ occurs at least once.

C. Security Definition

The security requires completeness and authentication. Completeness essentially assures that Bob should receive M correctly with a high probability. Authentication assures that the authentication failure event *Succ* occurs negligibly. Formally, we define them as follows.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

Definition 3. *A cryptographic protocol* Π *for a wiretap channel* $W_1 : \mathcal{X} \to \mathcal{Y}, W_2 : \mathcal{X} \to \mathcal{Z}$ *is a secure authentication protocol if the following holds:*

1. **Completeness.** *When the wiretapper Oscar does not present, there exists* $\alpha > 0$ *such that* $\Pr(D = \perp) \leq \exp(-n\alpha)$, *where n is the number of use of the wiretap channel* (W_1, W_2) *in the protocol.*
2. **Authentication.** *For any wiretapper Oscar, the probability of success* $\Pr(Succ(Oscar))$ *is negligible in n.*

If we only require authentication to hold against Oscar that issues at most t authentication queries at item (1) of the adversary model, then Π *is t-secure authentication protocol.*

In [31], the efficiency metric for a secure authentication protocol is defined as follows.

3. **Efficiency.** The authentication rate is defined as the ratio of secure code length to message length, i.e., $\rho_{auth} = \frac{1}{n} log|\mathcal{M}|$, where $|\mathcal{M}|$ is the cardinality of message space $\mathcal{M}$, and $log|\mathcal{M}|$ is the bit length of the message. For instance, if $\mathcal{M} = \{1, 2, \cdots, 2^{10000}\}$ and n=1000, then the authentication rate is 10.

V. Authentication of Multiple Message

In this section, an authentication framework is first proposed. Based on this framework, the security analysis is then conducted to find the conditions/requirements for the authentication protocol to be secure (in Theorem 2).

A. Authentication Framework

Let $\{(f_n, g_n)\}_n$ be a secure channel coding for wiretap channel $W_1 : \mathcal{X} \to \mathcal{Y}, W_2 : \mathcal{X} \to \mathcal{Z}$; $\mathcal{S} = \{1, \cdots, 2^{nR_n}\}$ be the source messages for (f_n, g_n); and R_n be the code rate of (f_n, g_n). Let $k \in \mathcal{K}$ be the shared key between Alice and Bob, and $\Psi = \{\psi_k\}_{k \in \mathcal{K}}$ be a collection of hash functions from $\mathcal{M}$ to $\mathcal{S}$. If Alice intends to transmit message $m \in \mathcal{M}$ to Bob, they perform as follows.

1. Alice computes $s = \psi_k(m)$ (which is called the *message tag*), encodes $x^n = f_n(s)$, and then sends m and x^n over noiseless channel and channel (W_1, W_2), respectively. Suppose that Bob receives m' and y'^n and Oscar receives m and z^n, respectively.
2. Based on m', y'^n, Bob decodes $s' = g_n(y'^n)$. If $s' = \perp$ or $\psi_k(m') \neq s'$, Bob rejects the message m'; otherwise accepts m'.

Next, we employ the proposed framework to authenticate multiple messages $M_1, M_2, \cdots, M_J$ using the same key K. In such a scenario, the attacker can initiate either an impersonation attack or a substitution attack at any time slot j. For an impersonation attack at slot j, Oscar selects a message based on the information collected through the last $j-1$ rounds of authentication, and sends it to the receiver. For a substitution attack at slot j, Oscar intercepts the Alice's jth packet, modifies it, and sends the modified packet to Bob. Oscar can make the modification using the information gathered in the past transmissions. The probability of successful impersonation attack and substitution attack at the jth slot are denoted by $P_{I,j}$ and $P_{S,j}$, respectively.

B. Analysis on Attacks

For simplicity, we denote the random vectors $(x_1, \cdots, x_n)$ by $\vec{x}$. In slot j, if Alice transmits m_j over the noiseless channel. Then, Alice computes $\vec{x}_j = f_n(s_j)$ and transmits it over the wiretap channel, where k is the key and message tag $s_j = \psi_k(m_j)$. Through Oscar, Bob receives m'_j and $\vec{y}'_j$. Oscar receives m_j and $\vec{z}_j$.

Impersonation attack at slot j: Let $h_{j,im}$ be Oscar's strategy (or a function) which maps $m_1, \vec{z}_1, \cdots, m_{j-1}, \vec{z}_{j-1}$ to m_{oj}, $\vec{y}_{o,j}$. The decoded message tag is denoted by $s_{o,j} = g_n(\vec{y}_{o,j})$ and the message at the destination after Oscar's attack is denoted by m_{oj}. For each $m_1, \vec{z}_1, \cdots, m_{j-1}, \vec{z}_{j-1}$, Oscar adapts a strategy $h_{j,im}$ to maximize the the following probability:

$$\begin{aligned} &P(s_{oj} = \psi_K(m_{oj}) | m_1, \vec{z}_1, \cdots, m_{j-1}, \vec{z}_{j-1}) \\ &= \sum_{k \in \mathcal{K}} P(k | m_1, \vec{z}_1, \cdots, m_{j-1}, \vec{z}_{j-1})\ \theta(\psi_k(m_{oj}), s_{oj}), \end{aligned}$$

where

$$\theta(r_1, r_2) = \begin{cases} 1, & \text{if } r_1 = r_2; \\ 0, & \text{otherwise,} \end{cases} \qquad \text{for any } r_1, r_2 \in R.$$

Averaging over $m_1, \vec{z}_1, \cdots, m_{j-1}, \vec{z}_{j-1}$, the probability of successful impersonation attack is

$$\begin{aligned} P_{I,j} = &\sum_{m_1, \vec{z}_1, \cdots, m_{j-1}, \vec{z}_{j-1}} P(m_1, \vec{z}_1, \cdots, m_{j-1}, \vec{z}_{j-1}) \times \\ &\sup_{h_{j,im}} \left\{ P(s_{oj} = \psi_K(m_{oj}) | m_1, \vec{z}_1, \cdots, m_{j-1}, \vec{z}_{j-1}) \right\}. \end{aligned} \tag{7}$$

Substitution attack at slot j: For a substitution attack, if Alice sends $(m_j, \vec{x}_j)$ to Bob at slot j, Oscar can adaptively interleave two types of attacks as follows. In Type I attack, Oscar can revise m to $m_{oj} (\neq m_j)$, and send $m_{oj} (\neq m_j)$ to Bob; in Type II attack, Oscar can send any pair $m_{oj} (\neq m_j), \vec{y}_{oj}$ to Bob noiselessly. Oscar succeeds, if $s_{oj} = \psi_k(m_{oj})$ in Type I attacks (where $g_n(\vec{y}_j) = s_{oj}$), or $s_{oj} = \psi_k(m_{oj})$ in Type II attacks (where $g_n(\vec{y}_{oj}) = s_{oj}$).

Type I attack: Oscar knows $m_1, \vec{z}_1, \cdots, m_j, \vec{z}_j$. He can choose m_{oj} based on this information. Let $h_{1j,sb}$ be Oscar's strategy, which maps $m_1, \vec{z}_1, \cdots, m_j, \vec{z}_j$ to m_{oj}. Oscar transmits m_{oj} over the noiseless channel and does not modify the authentication information. Hence, m_{oj} and s_j are the message and message tag at Bob after the attack. Oscar is successful if $s_j = \psi_k(m_{oj})$, where $s_j = g(\vec{y}_j)$. Obviously, for each observation $m_1, \vec{z}_1, \cdots, m_j, \vec{z}_j$, Oscar should choose $h_{1j,sb}$ such that

$$\begin{aligned} &P(s_j = \psi_K(m_{oj}) | m_1, \vec{z}_1, \cdots, m_j, \vec{z}_j)\ (1 - \theta(m_{oj}, m_j)) \\ &= \sum_{k \in \mathcal{K}} P(k | m_1, \vec{z}_1, \cdots, m_j, \vec{z}_j) \times \\ &\qquad \left\{ \theta(\psi_k(m_{oj}), \psi_k(m_j))(1 - \theta(m_{oj}, m_j)) \right\} \end{aligned}$$

is maximized. Averaging over $m_1, \vec{z}_1, \cdots, m_j, \vec{z}_j$, the probability of successful type I substitution attack at slot j is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

$$P_{S_1,j} = \sum_{m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j} P(m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\times \sup_{h_{1j,sb}}\left\{P(s_j=\psi_K(m_{oj})|m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\ (1-\theta(m_{oj},m_j))\right\}. \quad (8)$$

Type II attack: Let $h_{2j,sb}$ be Oscar strategy which maps $m_1,\vec{z}_1,\cdots,m_{j-1},\vec{z}_{j-1}$ to m_{oj}, $\vec{y}_{o,j}$. After Type II attack, the decoded message tag is denoted as $s_{o,j}=g(\vec{y}_{o,j})$ and the message at Bob is denoted as m_{oj}. The attack is successful if $s_{oj}=\psi_k(m_{oj})$. For each $m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j$, the opponent adopts a strategy $h_{2j,sb}$ to maximize the following probability:

$$P(s_{oj}=\psi_K(m_{oj})|m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)(1-\theta(m_{oj},m_j)) = \sum_{k\in\mathcal{K}} P(k|m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\times\left\{\theta(\psi_k(m_{oj}),s_{oj})\ (1-\theta(m_{oj},m_j))\right\}.$$

Averaging over $m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j$, the probability for the jth type II substitution attack being successful is

$$P_{S_2,j} = \sum_{m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j} P(m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\times \sup_{h_{2j,sb}}\left\{P(s_{oj}=\psi_K(m_{oj})|m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\ (1-\theta(m_{oj},m_j))\right\}. \quad (9)$$

Then, the probability of successful substitution attack at slot j is

$$P_{S,j}=\max\{P_{S_1,j},P_{S_2,j}\}.$$

C. Security Theorem

When a strong secure channel coding is employed in the authenticate framework, the attacker obtains no significant amount of information about secret key K and the message tag S, in one time authentication, as depicted in Proposition 1.

Proposition 1. *Let M, S and Z^n be the random variables defined in the authentication framework (Sec.V.A). Then, with a strong secure channel coding, there exists a constant $\alpha>0$, such that*

$$I(S;Z^n|M)\le e^{-\alpha n}, \quad (10)$$

$$I(K;Z^n|M)\le e^{-\alpha n}. \quad (11)$$

Proof: The conditional mutual information can be rewritten as

$$\begin{aligned} I(S;Z^n|M) &= H(Z^n|M)-H(Z^n|S,M)\\ &=^{(a)} H(Z^n|M)-H(Z^n|S)=I(Z^n;S)-I(Z^n;M)\\ &\le I(Z^n;S)\le^{(c)} e^{-\alpha n},\\ I(K;Z^n|M) &= I(K,M;Z^n)-I(M;Z^n)\\ &\le^{(b)} I(S;Z^n)-I(M;Z^n)\\ &\le I(S;Z^n)\le^{(c)} e^{-\alpha n}, \end{aligned}$$

where (a) and (b) are based on the fact that $M\to MK\to S\to Z^n$ forms a Markov chain, while (c) comes from Definition 2. ■

Proposition 2. *When the same key K is used to authenticate a sequence j of messages $M_1,\cdots,M_j$, if a strong secure channel coding and a ε-AWU$_2$ hash function are employed, then there exists a constant $\alpha>0$, such that for any $b=1,\cdots,j$*

$$I(S_b;\vec{Z}_1,\cdots,\vec{Z}_j|M_1,\cdots,M_j) \le e^{-\alpha n} \quad (12)$$

$$I(K;\vec{Z}_1,\cdots,\vec{Z}_j|M_1,\cdots,M_j) \le j\cdot e^{-\alpha n} \quad (13)$$

where $S_j=\psi_K(M_j)$.

Proof: From inequality (10), there exists a constant $\alpha>0$ such that $I(S_j;\vec{Z}_j|M_j)\le e^{-\alpha n}$. Given $(M_1,\cdots,M_j)=(m_1,\cdots,m_j)$, for any $b\in\{1,\cdots,j\}$, we have

$$\vec{Z}_b\to S_b\to K\to(S_1\cdots,S_{b-1})\to(\vec{Z}_1,\cdots,\vec{Z}_{b-1}) \quad (14)$$

$$\vec{Z}_b\to S_b\to K\to(S_{b+1},\cdots,S_j)\to(\vec{Z}_{b+1},\cdots,\vec{Z}_j) \quad (15)$$

form two Markov chains. Hence, given $m_1,\cdots,m_j$, $\vec{Z}_b\to S_b\to\vec{Z}_1,\cdots,\vec{Z}_{b-1},\vec{Z}_{b+1},\cdots,\vec{Z}_j$ forms a Markov chain. Consequently, from data processing inequality, the following holds

$$I(S_b;\vec{Z}_1,\cdots,\vec{Z}_j|m_1,\cdots,m_j)\le I(S_b,\vec{Z}_b|m_1,\cdots,m_j). \quad (16)$$

Averaging over $m_1,\cdots,m_b$, we have

$$I(S_b;\vec{Z}_1,\cdots,\vec{Z}_j|M_1,\cdots,M_j) \quad (17)$$

$$\le I(S_b,\vec{Z}_b|M_1,\cdots,M_j)=I(S_b,\vec{Z}_b|M_b)\le e^{-\alpha n} \quad (18)$$

Given $(M_1,\cdots,M_j)=(m_1,\cdots,m_j)$, we have $\vec{Z}_b\to K\to(\vec{Z}_1,\cdots,\vec{Z}_{b-1})$ forms a Markov chain for any $b\le j$. Hence, by data processing inequality, we have $I(K;\vec{Z}_b|\vec{Z}_1,\cdots,\vec{Z}_{b-1},m_1,\cdots,m_j)\le I(K;\vec{Z}_b|m_1,\cdots,m_j)$. Averaging over $m_1,\cdots,m_b$, we have

$$I(K;\vec{Z}_b|\vec{Z}_1,\cdots,\vec{Z}_{b-1},M_1,\cdots,M_j)\le I(K;\vec{Z}_b|M_1,\cdots,M_j).$$

Thus,

$$\begin{aligned} &I(K;\vec{Z}_1,\cdots,\vec{Z}_j|M_1,\cdots,M_j)\\ &\le\sum_{b=1}^{j} I(K;\vec{Z}_b|\vec{Z}_1,\cdots,\vec{Z}_{b-1},M_1,\cdots,M_j)\\ &\le\sum_{b=1}^{j} I(K;\vec{Z}_b|M_1,\cdots,M_j)=\sum_{b=1}^{j} I(K;\vec{Z}_b|M_b)\le j\cdot e^{-\alpha n}. \end{aligned}$$

■

Based on the above results, we have the following theorem regarding to the requirements/conditions for a multi-message authentication protocol to be information-theoretical security.

Theorem 1. *Suppose that $\{(f_n,g_n)\}_n$ is a strong secure channel coding for wiretap channel (W_1,W_2), and $\Psi:\mathcal{M}\times\mathcal{K}\to\mathcal{S}$ is an ε- AWU$_2$ hash function with ε being negligible in n. Then, for any polynomial $t(\cdot)$ and sufficiently large n, the proposed protocol Π is $t(n)$-secure.*

Detailed proof is provided in Appendix. From this theorem, we only have to construct a family of hashing function and strong secure channel code satisfying the conditions above to achieve security of the proposed protocol. We will discuss how to design such kind of class of hash functions and channel code to meet these requirements in Sec. VII.

VI. Authentication Protocol and Efficiency

In this section, we first prove that there exist a family of hash functions and a secure channel coding scheme which can meet the security requirements. Then, we propose an authentication protocol and analyze the efficiency.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

A. Existence

The following result states that there exists an ε-AWU$_2$ class of hash functions with ε being negligible in n.

Theorem 2. *[28] Let q be a prime power and let $i \geq 1$ be an integer. Then, there exists hence $(i+1)/q$-AU$_2$ class of q^{i+2} hash functions from $\mathcal{M}$ to $\mathcal{S}$, where $|\mathcal{M}| = q^{2^i}$ and $|\mathcal{S}| = q$.*

A set with size v can be enumerated with $\log v$ bits. It is clear that a family of ε-AU$_2$ hash functions is ε-AWU$_2$. Therefore, the above theorem implies that there exists a family of $(i+1)/q$-AWU$_2$ hash function indexed by $(i+2)\log q$ bits which can compress a message with length $2^i \log q$ to a tag with length $\log q$. In practice, $\varepsilon = (i+2)/q$ and index length $(i+2)\log q$ should be small and the message length $2^i \log q$ should be large. If $i = 8$ and $q = 2^{50}$, then the index length is 62 bytes, $\varepsilon \approx 2^{-47}$, the message length is 1.5 Mb with the tag of 50 bits.

In [19], Csiszar showed the following lemma by using random coding.

Lemma 1. [19] *Let P be a type of length n over $\mathcal{X}$ with $P(x) > 0$ for all x and X is distributed according to P. Consider a wiretap channel $W_1 : \mathcal{X} \to \mathcal{Y}$, $W_2 : \mathcal{X} \to \mathcal{Z}$ with $I(X;Y) > I(X;Z) + 2\tau$ for some $\tau > 0$. Then, there exists a set $\mathcal{C}_n \subseteq T_P^n$ with size $2^{n(I(X;Y)-\tau)}$ and an equipartition $\phi : \mathcal{C}_n \to \{1, \cdots, \iota\}$ for $\mathcal{C}_n$ with $\iota \leq 2^{n(I(X;Y)-I(X;Z)-2\tau)}$ such that $\mathcal{C}_n$ is the code for channel W_1 with exponentially small (in n) average probability of error and $I(\phi(\tilde{X}^n); Z^n)$ is exponentially small (in n), where $\tilde{X}^n$ is uniformly random over $\mathcal{C}_n$.*

This lemma implies that a strong secure channel coding can achieve secrecy rate of $\frac{1}{n}\log \iota$, for any n. Specifically, suppose that (f_n, g_n) be the coding scheme for W_1, where f_n and g_n are the encoding and decoding methods, respectively. For $s \in \mathcal{S} = \{1, \cdots, \iota\}$, $f_n(s)$ for the wiretap channel is to take $\tilde{x}^n \leftarrow \phi^{-1}(s)$, and decoding $g_n(y^n) := \phi[\vec{x}^n]$, for $\vec{x}^n = g_n(y^n)$., where y^n is the receive message.

Let $\iota = 2^u \leq 2^{n(I(X;Y)-I(X;Z)-2\tau)}$. Taking $q = 2^u$ and $i = ploy(u)$ for some polynomial function $ploy(\cdot)$ (in Theorem 2), we can conclude that the family of hash functions in this theorem satisfies the conditions in Theorem 1. Based upon the discussion above, we have the theorem as follows.

Theorem 3. *Let $I(X;Y) > I(X;Z) + \tau$ for some constant $\tau > 0$, where Y, Z are the outputs of wiretap channel (W_1, W_2) with input X; and P_X is a type P with $P(x) > 0$. Then, for any polynomial $t(\cdot)$ and sufficiently large n, there exists a $t(n)$-secure authentication protocol Π.*

Proof: It can be directly obtained from Theorem 1, Theorem 2, and Lemma 1. ∎

In [12], the concepts of partial ordering of DMC with common input alphabet were introduced as follows. *Channel W_1 is more capable than channel W_2* if $I(X;Y) \geq I(X;Z)$ for every input X. *Channel W_1 is less noisy than channel W_2* if $I(U;Y) \geq I(U;Z)$ for any Markov chain $U \to X \to Y,Z$. *Channel W_2 is no less noisy than channel W_1* if there exists a Markov chain $U \to X \to Y,Z$ such that $I(U;Y) > I(U;Z)$. The following theorem show that the condition $I(X;Y) > I(X;Z) + \tau$ in Theorem 3 can be loosened to the condition that W_2 is no less noisy than W_1.

Corollary 1. *If W_2 is not less noisy than W_1. Then, for any polynomial $t(\cdot)$ and sufficiently large n, there exists a $t(n)$-secure authentication protocol Π for wiretap channel (W_1, W_2).*

Proof: It is directly obtained from Theorem 3 and the definition that W_2 is no less noisy than W_1. ∎

B. High-Efficiency Authentication Protocol

Note that, in Lemma 1, ι can be any number no more than $2^{n(I(X;Y)-I(X;Z)-2\tau)}$ and τ is any positive number. By [13, Theorem 3], if W_1 is more capable than W_2, then

$$C_s = \max_{P_X} I(X;Y) - I(X;Z).$$

Thus, from Lemma 1 and [13, Theorem 3], we have the following lemma.

Lemma 2. *There exists a sequence of types $\{P_n\}_n$ over $\mathcal{X}$ such that code rate R_n for coding scheme (f_n, g_n) satisfies $\lim_{n\to\infty} R_n = C_s$.*

In order to obtain an authentication protocol, which satisfy the security requirements and is efficient, we use the strong secure channel coding induced by Lemma 1. Next, we only need to specify τ, Ψ, $\mathcal{M}$, $\mathcal{K}$, $\mathcal{R}$ and ε. For our construction, the constraint for $\mathcal{S}$ is $\frac{\log \mathcal{S}}{n} < I(X;Y) - I(X;Z) + \tau$ (by Lemma 1), where τ only has the constraint $I(X;Y) > I(X;Z) + \tau$ (by Lemma 1). So for any $\delta \in (0, I(X;Y) - I(X;Z))$, we can define $\tau = I(X;Y) - I(X;Z) - \delta/2$ and then set $|\mathcal{S}| = 2^{n(I(X;Y)-I(X;Z)-\delta)}$. Then, we have

$$\rho_{chan} = \frac{\log |\mathcal{S}|}{n} = I(X;Y) - I(X;Z) - \delta \tag{19}$$

for any $\delta \in (0, I(X;Y) - I(X;Z))$.

Let $\tau = I(X;Y) - I(X;Z) - \delta/2$. Then, $\rho_{auth} = [I(X;Y) - I(X;Z) - \delta] \cdot \rho_{tag}$. Further, we realize ε-AWU$_2$ Ψ with $\frac{\lambda(n)+1}{q}$-AU$_2$ in Theorem 2, where $|\mathcal{S}| = q = 2^{n(I(X;Y)-I(X;Z)-\delta)}$, $|\mathcal{K}| = q^{\lambda(n)+2}$, $|\mathcal{M}| = q^{2^{\lambda(n)}}$, $\varepsilon = \frac{\lambda(n)+1}{q}$. Under this setup, the security conditions in Theorem 1 are satisfied if $\lambda(n) \leq 2^{\omega n}$ for some $\omega \in (0, \rho_{chan})$. As a result, $\rho_{tag} = 2^{\lambda(n)}$ and $\rho_{auth} = [I(X;Y) - I(X;Z) - \delta] 2^{\lambda(n)}$, where $\lambda(n) \leq 2^{\omega n}$ for some $\omega \in (0, \rho_{chan})$. The details of the message authentication protocol are shown in Protocol 1.

C. Efficiency

The authentication rate ρ_{auth} can be rewritten as $\rho_{auth} = \rho_{tag} \cdot \rho_{chan}$, where $\rho_{tag} = \frac{\log |\mathcal{M}|}{\log |\mathcal{S}|}$ and $\rho_{chan} = \frac{\log |\mathcal{S}|}{n}$. We name ρ_{tag} the *tag rate* and ρ_{chan} the *channel coding rate*, respectively. Combining with Lemma 2, we can have the following theorem.

Theorem 4. *If W_1 is more capable than W_2, for any $\delta \in (0, C_s)$, taking $\tau = C_s - \delta/2$, the proposed protocol is $t(n)$-secure (or polynomial secure) with*

$$\rho_{auth} = (C_s - \delta) \cdot 2^{\lambda(n)}, \tag{20}$$

where $\lambda(n) \leq 2^{\omega n}$ for some $\omega \in (0, \rho_{chan})$, and $C_s = \max_{P_X} I(X;Y) - I(X;Z)$. Furthermore, if $\lim_{n\to\infty} \lambda(n) = \infty$, then

$$\lim_{n\to\infty} \rho_{auth} = \infty. \tag{21}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

Scheme 1: High Efficiency Authentication Protocol

Preliminaries:

- Let $\triangle I = I(X;Y) - I(X;Z)$, $\delta \in (0, \triangle I)$, $\tau = \triangle I - \delta/2$, $\omega \in (0, \triangle I - \delta)$, and $q = 2^{n(\triangle I - \delta)}$.
- Let (f_n, g_n) be the secrecy capacity achievable strong secrecy coding (in Lemma 3), where n is the code length.
- Let $\Psi = \{\psi_k\}_{k \in \mathcal{K}}$ be a collection of ε-AWU$_2$ hash functions from $\mathcal{M}$ to $\mathcal{S}$, in which, $|\mathcal{M}| = q^{2^{\lambda(n)}}$, $|\mathcal{S}| = q$, $|\mathcal{K}| = q^{\lambda(n)+2}$, $\varepsilon = \frac{\lambda(n)+1}{q}$, and $\lambda(n) \leq 2^{\omega n}$.
- Let $k \in \mathcal{K}$ be the secret key shared by Alice and Bob.

Protocol:

If Alice intends to send and authenticate $m \in \mathcal{M}$ to Bob, then they perform the following protocol.

1. Alice first computes the message tag $s = \psi_k(m)$, and encodes $x^n = f_n(s)$ with the strong secure channel coding. And then, Alice transmits m and x^n over noiseless channel and wiretap channel (W_1, W_2), respectively.
2. Based on the received information m' and y'^n from noiseless channel and wiretap channel (W_1, W_2), respectively, Bob first decodes $s' = g_n(y'^n)$. Then Bob verifies if m' is sent from Alice as follows. If $s' = \perp$ or $\psi_k(m') \neq s'$, Bob rejects the message m'; otherwise accepts m'.

Note that, the security of the proposed protocol depends on the channel advantage (i.e., the main channel is more capable than the wiretapper's channel). Actually, there are several wireless scenarios which can provide such channel advantage, such as Near Field Communications (NFCs) and communications in military green zones. In these scenarios, the channel advantage holds because one of the legitimate user is physically closer to another legitimate user than the adversary. Moreover, there are some positive solutions to achieve such channel advantage, such as, secure beamforming [38] and self-interference [39].

From Theorem 4, we have the following corollary.

Corollary 2. *If W_2 is no less noisy than W_1, for any polynomial $t(\cdot)$ and a sufficiently large n, there exists a $t(n)$-secure authentication protocol Π with*

$$\rho_{auth} = (C_s - \delta) \cdot 2^{\lambda(n)}, \tag{22}$$

for wiretap channel (W_1, W_2), where C_s is the secrecy capacity of (W_1, W_2) denoted as $C_s = \max_{U \to X \to YZ} I(U;Y) - I(U;Z)$.

Proof: By Corollary 2 in [13], we have $C_s = \max_{U \to X \to YZ} I(U;Y) - I(U;Z)$. Thus, there exists a RV U such that $U \to X \to YZ$, and $I(U;Y) - I(U;Z) > C_s - \delta/4$ for any $\delta \in (0, C_s)$. By using U to replace X in Theorem 4 and taking $\tau = C_s - \delta/4$, it can be proved, based on Theorem 4. ■

Note that, in [22], a capacity achieving codebook is divided into $|\mathcal{K}|$ subsets, each of which is further partitioned into $|\mathcal{M}|$ bins, such that the information of the key K can be hidden from the attacker. Thus, the authentication rate of this protocol can be given as $\frac{1}{n}|\mathcal{M}| = I(X;Z) - \xi$ for a certain $\xi > 0$. The authentication rate of the proposed protocol can reach infinity when n goes to infinity by employing the security channel code and ε-AU$_2$ hash functions.

VII. Implementation: authentication over BSWC

In this section, we consider authentication problem over a binary symmetric wiretap channel (BSWC), where the main channel and the wiretapper's channel are the binary symmetric channel with crossover probability p and q, respectively, denoted by BSC(p) and BSC(q). From Theorem 1, we only need to design an ε-*AWU*$_2$ hash functions and a strong secure channel coding, which meet the requirements in this theorem, so as to achieve information-theoretic security. To this end, we study how to meet these requirements by leveraging LFSR-based hash functions and strong secure polar code.

A. ε-*AWU*$_2$ *Hash Functions*

Let the message space $\mathcal{M}$ and tag space $\mathcal{S}$ be the set of binary strings of length t and u, respectively. We consider a specific hash functions as follows. A family of hash functions $\Psi : \mathcal{M} \to \mathcal{S}$ is $\oplus$-linear iff

$$\psi_k(m \oplus m') = \psi_k(m) \oplus \psi_k(m') \tag{23}$$

for any $m, m' \in \mathcal{M}$.

For any $m, m' \in \mathcal{M}$, we have $\Pr[\psi : \psi(m) = \psi(m')] = \Pr[\psi : \psi(m) \oplus \psi(m') = \mathbf{0}] = \Pr[\psi : \psi(m \oplus m') = \mathbf{0}]$. It further equals to $\Pr[\psi : \psi(m) = \mathbf{0}]$ for any $m \in \mathcal{M}$, where $\mathbf{0}$ is the zero string. Thus, a family of $\oplus$-linear hash functions is ε-AWU$_2$ iff

$$\forall (m, s) \in \mathcal{M} \times \mathcal{S}, \quad \Pr[\psi : \psi(m) = s] \leq \varepsilon. \tag{24}$$

The family of $\oplus$-linear hash functions satisfying Equation (24) is called ε-balanced according to Krawczuk's work in [30].

Carter and Wegman [26] give a strong universal$_2$ family of hash functions

$$\left\{\psi_{A,b} : \psi_{A,b}(m) = m \cdot A + b\right\}_{A,b} \tag{25}$$

where A is a $t \times u$ Boolean matrix, $m (\neq \mathbf{0})$ is a message with length t, and b is a binary vector with length u. However, the key length is $u(t+1)$, which is too expensive for key distribution and storage.

To solve such a problem, Krawczuk in [30] constructs a family of ε-AWU$_2$ hash functions by slightly modifying Carter and Wegman's method. Specifically, Krawczuk provides an efficient construction of matrix A with an *Linear Feedback Shifting Register* (LFSR) to shorten the key length as follows. Let $p(x)$ be an irreducible polynomial over $GF(2)$, and $(a_0, a_1, \cdots, a_{u-1})$ be the initial state of a LFSR corresponding to the coefficients of $p(x)$. If $a_0, a_1, \cdots$ is the bit sequence generated by the LFSR, the matrix A can be expressed as

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{u-1} \\ a_1 & a_2 & \cdots & a_u \\ \vdots & \vdots & \ddots & \vdots \\ a_{t-1} & a_t & \cdots & a_{u+t-2} \end{pmatrix} \tag{26}$$

Krawczuk [30] shows that the LFSR-based construction defined above is ε-balanced (i.e., ε-AWU$_2$) for $\varepsilon \leq \frac{t}{2^{u-1}}$, and its key length is reduced from $t(u+1)$ to $3u$ (i.e., u bits for b, u bits for the generator polynomial $p(x)$, and u bits for the initial state of the LFSR).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

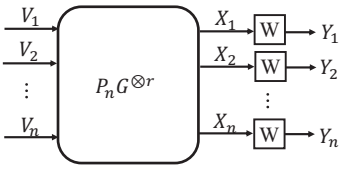


Fig. 5. The encoding process of polar codes.

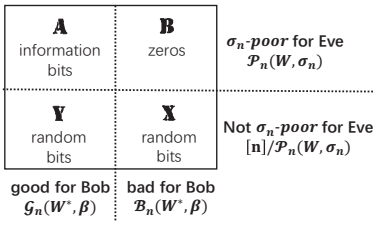


Fig. 6. Mahdavifar and Vardy's strong secure channel coding scheme.

B. Strong Secure Polar Codes

Polar code is introduced by Arikan in [32], which can achieve the capacity of any binary-input symmetric DMCs with low encoding and decoding complexity. Let $G = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, and $G^{\otimes r}$ be the m-th Kronecker power of G. For any $V^n \in \{0,1\}^n$, V^n is encoded as $X^n = V^n P_n G^{\otimes r}$, where $n = 2^r$ and P_n is the bit-reversal permutation matrix with size $n \times n$. As shown in Fig. 5, X^n is sent over a binary-input channel symmetric DMC W n times independently.

By defining

$$\widetilde{W}(y^n|v^n) = W^n(y^n|v^n P_n G^{\otimes r}), \tag{27}$$

for any $i \le n$, Arikan in [32] defines a channel $W_i : \{0,1\} \to \mathcal{Y}^n \times \{0,1\}^{i-1}$ as

$$W_i(y^n, v^{i-1}|v_i) = \frac{1}{2^{n-1}} \sum_{\mathbf{e}\in\{0,1\}^{n-i}} \widetilde{W}(y^n|v^i, \mathbf{e}). \tag{28}$$

Arikan shows that as r grows, it leads to channel polarization, i.e., for any i, W_i approaches either a noiseless channel (i.e., good channel) or a pure-noise channel (i.e., bad channel). Denoting Bhattacharyya parameter of channel W as

$$Z(W) = \sum_{y\in\mathcal{Y}} \sqrt{W(y|0)W(y|1)}, \tag{29}$$

the index sets of the good channels and bad channel can be defined as follows:

$$\mathcal{G}_n(W,\beta) = \left\{ i \in [n] : Z(W_i) < 2^{-n^\beta}/n \right\} \tag{30}$$

$$\mathcal{B}_n(W,\beta) = \left\{ i \in [n] : Z(W_i) \ge 2^{-n^\beta}/n \right\} \tag{31}$$

where $\beta < 1/2$ is a fixed constant, and $[n] = \{1,2,\cdots,n\}$.

Based on Arikan's work, a strong-security coding scheme with polar codes is proposed by Mahdavifar and Vardy in [11]. Let $C(W_i)$ be the capacity of channel W_i. Define the index set of σ_n-poor bit-channel as

$$\mathcal{P}_n(W,\sigma_n) = \{ i \in [n] : C(W_i) \le \sigma_n \} \tag{32}$$

for some positive constant σ_n.

Suppose that the main channel is $W^* = BSC(p)$, and the wiretapper's channel is $W = BSC(q)$. Define index sets $\mathbf{A}$, $\mathbf{B}$, $\mathbf{X}$, and $\mathbf{Y}$ as follows:

$$\mathbf{A} = \mathcal{P}_n(W,\sigma_n) \cap \mathcal{G}_n(W^*,\beta) \tag{33}$$

$$\mathbf{B} = \mathcal{P}_n(W,\sigma_n) \cap \mathcal{B}_n(W^*,\beta) \tag{34}$$

$$\mathbf{X} = \{[n] \setminus \mathcal{P}_n(W,\sigma_n)\} \cap \mathcal{B}_n(W^*,\beta) \tag{35}$$

$$\mathbf{Y} = \{[n] \setminus \mathcal{P}_n(W,\sigma_n)\} \cap \mathcal{G}_n(W^*,\beta) \tag{36}$$

The strong secure channel coding scheme proposed Mahdavifar and Vardy is shown in Fig. 6, in which the channels in $\mathbf{A}$ are used to transmit information bits; the channels in $\mathbf{B}$ are used to send zeros; and channels in $\mathbf{X}$ and $\mathbf{Y}$ are used to transmit random bits. Mahdavifar and Vardy show that their coding scheme is secrecy capacity achievable with strong security in [11]. The proposed encoding and decoding process is described as follows.

- Encoding f_n: Let $\mathbf{u}$ be the information bits in $\{0,1\}^{|\mathbf{A}|}$. Alice selects $\mathbf{e}$ for $\{0,1\}^{|\mathbf{Y}|}$ uniformly at random. Taking $v^n(\mathbf{A}) = \mathbf{u}$, $v^n(\mathbf{X}\cup\mathbf{Y}) = \mathbf{e}$ and $v^n(\mathbf{B}) = \mathbf{0}$, the codeword of v^n can be expressed as
$$x^n = v^n P_n G^{\otimes r}, \tag{37}$$
where $v^n(\mathbf{D}) = (v_{i_1}, v_{i_2} \cdots, v_{i_{|A|}})$ for any index set $\mathbf{D} = \{i_1, v_{i_2}, \cdots, i_{|\mathbf{D}|}\}$.
- Decoding g_n: After receiving y^n from the main channel W^*, Bob produces a vector $\hat{v}^n$ by invoking successive cancellation decoding in [32] for polar code $\mathcal{C}_n(\mathbf{A}\cup\mathbf{Y})$.

Without loss of generality, it is assumed that Eve knows the information sets and frozen sets. This can be done by calculating Bhattacharyya parameters if the crossover probability of the main channel is known by Eve. Clearly, this assumption is reasonable and even strengthens Eve's capability.

In our polar code construction, we take

$$\sigma_n = 2^{n^{-\gamma}} \tag{38}$$

to obtain σ_n-poor bit channels (i.e., Equation (32)) for wiretapper's channel. From [11, Theorem 17], the set of secure polar coding schemes $\{(f_n, g_n)\}_n$ is strong secure.

From [11], Mahdavifar's polar coding scheme cannot provide the reliability of the main channel when the coding scheme attempts to achieve the secrecy capacity. However, it is unnecessary to achieve the secrecy capacity when the coding scheme is used in the proposed authentication protocol, as the authentication rate is main determined by the rate of the hash functions. In fact, we will show that the reliability of the main channel is achievable if the secrecy rate is lower than the secrecy capacity in the following section.

VIII. Performance Evaluation

In this section, we evaluate the performance of the message authentication protocol over BSWC by conducting extensive simulations. In the simulations, LFSR-based ε-AWU$_2$ hash functions and strong secure polar codes are leveraged in the proposed authentication framework.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

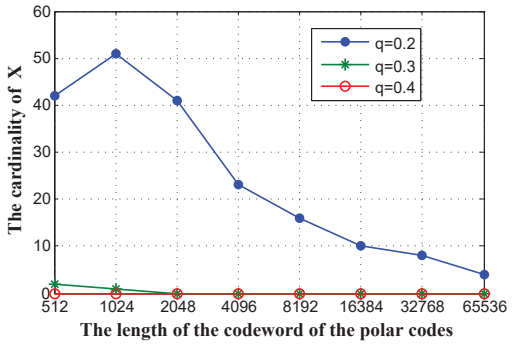


Fig. 7. The cardinality of index set X.

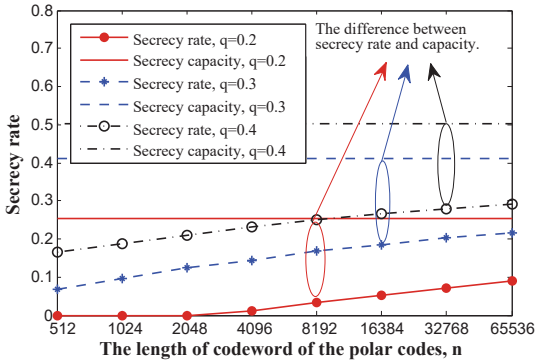


Fig. 8. Secrecy rate versus secrecy capacity.

A. Performance of Secure Polar Codes

Since secure polar codes play a key role in the proposed authentication protocol. It is necessary to evaluate the reliability and security of the channel coding scheme.

In order to measure the decoding error with respect to different code lengths, an experiment is designed by taking $\beta = 0.1$ (in Equ. (30) and (31)), $\gamma = 0.1$ (in Equ. (38)), the crossover probability of main channel $p = 0.1$, and the crossover probability of wiretapper's channel $q = 0.2, 0.3, 0.4$. In this experiment, Alice encodes a randomly chosen message with coding scheme in Section VII-B, and then, transmits the codeword over wiretap channel (BSC(p), BSC(q)). After receiving the output of their respective channels, Bob and Eve invoke successive cancellation decoding algorithm in [32]. We conduct the experiments for 100 times using each set of parameters to obtain the average performance.

From the simulations above, we find that all the decoding error rates at Bob is zero, i.e., the polar codes constructed by in Section VII-B with the parameters setting above can be correctly decoded by the main user. Note that, the reliability of the coding scheme mainly depends on the size of index set $\mathbf{X}$. Fig. 7 shows the cardinality of $\mathbf{X}$ with respect to the code length n. It can be seen that the number of $\mathbf{X}$ for each n under different wiretap channel scenarios are small. As a result, the reliability of the coding scheme is achievable.

Fig. 8 shows the secrecy capability of the corresponding wiretap channel and the secrecy rate of the polar codes under different code lengths. It can be seen that 1) a larger code length improves the secrecy rate; and 2) there is a substantial gap between secrecy rate and secrecy capacity. The results imply that, 1) a larger code length can lead to a higher authentication rate when polar codes are used in the proposed authentication protocol; and 2) there is substantial gap between the code rate and channel capacity, which leads to the reliability of the coding scheme, as a lower code rate results in a higher reliability.

Fig. 9 shows the decoding error rate of Eve versus the code length under different set of parameters and wiretap channel scenarios. It can be seen that the error rate is closer to 0.5 when the code length n increases. It is worth noting that, a smaller absolute value of the difference between the error rate and 0.5 means a higher entropy of the secure information at Eve, which further indicates a higher security of the secure

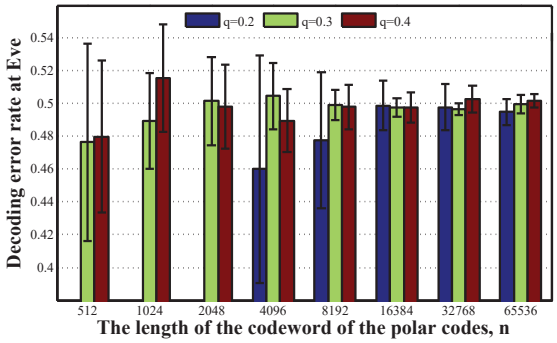


Fig. 9. Decoding error rate at Eve.

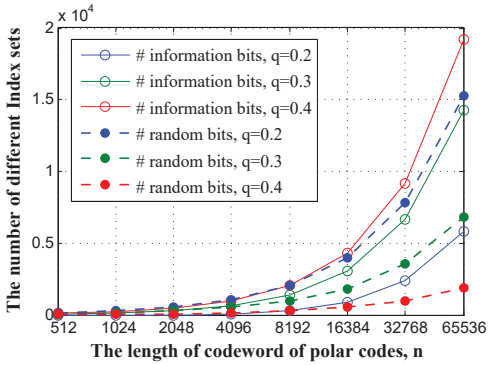


Fig. 10. The number of different index sets with varying code length.

information. As shown in this figure, the bar of decoding error rate does not exist for $q = 0.2$ and $n = 512$ (or $n = 1024$). The reason is that, $\mathbf{A} = \emptyset$ in these cases, which means Alice cannot transmit any secure information to Bob.

Fig. 10 shows the number of information bits and random bits versus the code length under different wiretap channel scenarios. We can find that both the number of information bits and random bits increase with the increasing of code length. Therefore, for any length $|S|$ of the message tag, there exists a code length n_0, such that $|S| \leq |\mathbf{A}(n)|$ for any $n > n_0$, where $\mathbf{A}(n)$ is the index set of information bits in terms of code length n.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

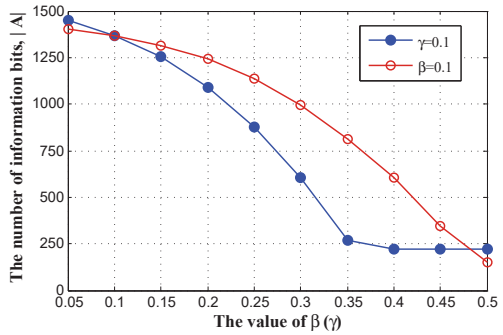


Fig. 11. The number of information bits against β and γ.

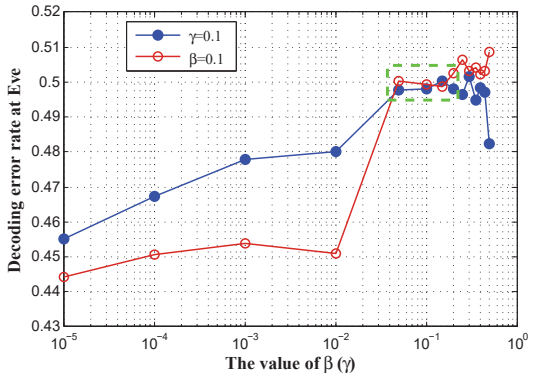


Fig. 12. The decoding error rate against β and γ.

B. Exploration of Protocol Parameters

We consider the effect of the channel partition parameters β and γ on the proposed protocol. Fig.11 and Fig. 12 show the change of the number of information bits and the decoding error rate at Eve, respectively, versus varying parameters β and γ, where $n = 8192$, $p = 0.1$, and $q = 0.3$.

As shown in Fig. 11, the blue line corresponds to the number of information bits by changing the value of β and fixing $\gamma = 0.1$, while the red line describes the number of information bits by fixing $\beta = 0.1$ and varying the value of γ. The result shows that the number of the information bit decreases with increasing the value of β and γ. The reason is that the cardinality of $\mathcal{P}_n(W,\sigma_n)$ and $\mathcal{G}_n(W^*,\beta)$ decrease with increasing β and γ, respectively. From this result, a smaller value of β and γ means a longer length of authentication tag, and further implies a higher authentication rate.

As shown in Fig. 12, the blue line corresponds to the decoding error rate at Eve by changing the value of β and fixing $\gamma = 0.1$, while the red line describes then decoding error rate of Eve by fixing $\beta = 0.1$ and varying the value of γ. It can be seen that, the error rate is less than 0.48 for $\beta,\gamma \in (0, 0.05)$; and the error rate is in $[0.495, 0.505]$ for $\beta,\gamma \in [0.05, 0.2]$. The reason is that, if β and γ are too small, the size of the set that is both good for Bob and poor for Eve becomes large. As a result, the probability of the event that, the indexes which are "not so bad" for Eve are in $\mathbf{A}$, increases.

Based on the discussion above, for both efficiency and security of the proposed protocol, we can choose β and γ in the interval $[0.05, 0.2]$.

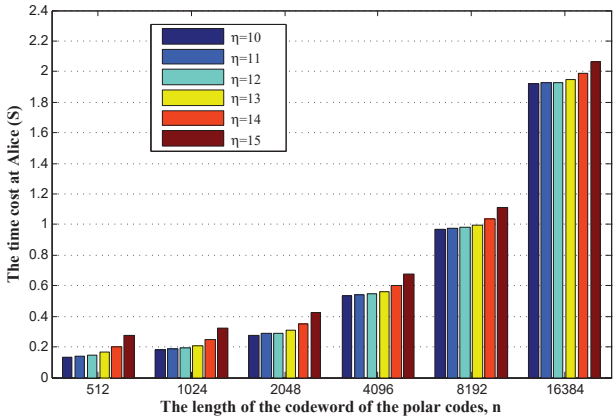


Fig. 13. Time cost at Alice.

C. Performance of the Proposed Protocol

We conduct simulations with a large variety of paraments under different crossover probabilities in both main channel and wiretap channel. The following metrics for performance evaluation are used: time cost, authentication error rate, and authentication rate.

Let the message length be 2^η bits, and the tag length be η' bits, The family of hash functions is

$$\left\{\Psi_k : \{0,1\}^{2^\eta} \to \{0,1\}^{\eta'}\right\}_k, \tag{39}$$

where $k = (p(x), e, b)$, and e is the initial state of the LFSR with primitive generator polynomial $p(x)$. So, the key length is $3\eta'$ bits and $\varepsilon \le 2^{\eta-\eta'+1}$.

In the authentication protocol, it is required that the index set number is larger than the tag length, i.e., $|\mathbf{A}| \ge \eta'$. If $|\mathbf{A}| > \eta'$, Alice transmits message tag s with the first η' channels in $\mathbf{A}$, and sends random bits with the remaining channels in $\mathbf{A}$.

We first consider the time cost of the proposed protocol. The time cost at Alice includes the tag generation time and the encoding time, while the time cost at Bob involves the tag generation time and the decoding time. In this simulation, the paraments are set as follows. $\beta = 0.1$, $\gamma = 0.1$, $q = 0.1$, $p = 0.3$, the message length is 2^η, and the primitive generator polynomial used to generate the LFSR is:

$$p(x) = x^{101} + x^{84} + x^{66} + x^{49} + x^{32} + x^{16} + 1. \tag{40}$$

Fig. 13 and Fig. 14 show the time cost at Alice and Bob, respectively, with respect to the code length under different message lengths. The results show that 1) a larger message length and code length improve the time cost; and 2) the impact of the code length on time cost is more sensitive than that of the message length on time cost. The latter result further reveals that the encoding/decoding time is far larger than the hashing time. The time cost of the proposed protocol will dramatically decrease if this protocol is implemented in hardware, as the encoding/decoding process of polar code and LFSR can be implemented in hardware with a low time cost.

Then, we evaluate the authentication error rate and authentication rate of the proposed protocol under different scenarios. In this simulation, we set $\beta = 0.1$, $\gamma = 0.1$ and $n = 8192$, and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

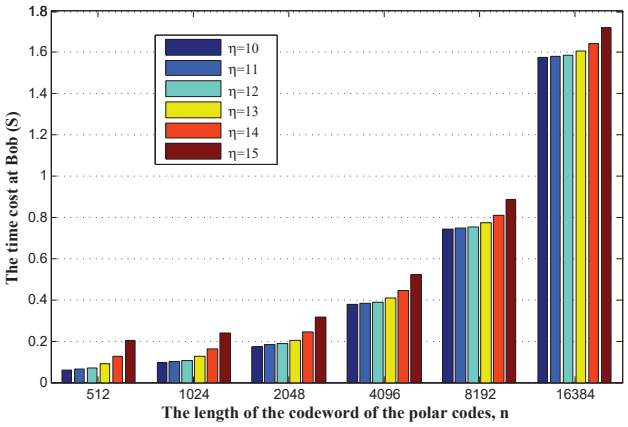


Fig. 14. Time cost at Bob.

TABLE I
SIMULATION SCENARIOS

Index	p	q	$L(M)$	$L(K)$	$L(S)$
A	0.1	0.2	2^{25} bits	303 bits	101 bits
B	0.1	0.3	2^{25} bits	303 bits	101 bits
C	0.1	0.4	2^{25} bits	303 bits	101 bits
D	0.2	0.3	2^{20} bits	192 bits	64 bits
E	0.2	0.4	2^{20} bits	192 bits	64 bits
F	0.3	0.4	2^{20} bits	192 bits	64 bits

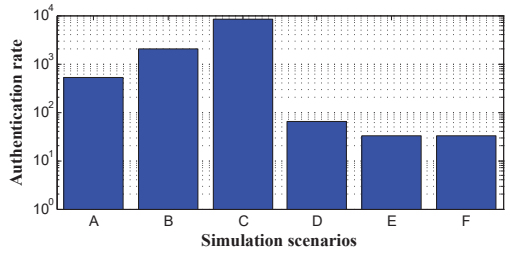


Fig. 15. Authentication rate under different scenarios.

take the primitive generator polynomial to generate the LFSR as Equ. (40) and

$$p(x) = x^{64} + x^9 + x^8 + x^7 + x^6 + x^3 + 1 \tag{41}$$

for tag length $L(S) = 101$ and $L(S) = 64$, respectively. The remaining parameters for each scenario are listed in Table I, where $L(M)$ is the message length, and $L(K)$ is the key length. For each scenario, we repeat the experiment 100 times. We find that all the messages authenticated by Alice is accepted by Bob in the simulations, i.e., the authentication error rate is zero in the simulations. Fig. 15 shows the authentication rate for each scenario. It can be seen that the proposed protocol can achieve a high authentication rate.

IX. Conclusion

In this paper, we have proposed a multi-message authentication framework over Wiretap Channel to achieve information theoretic security using the same key. Moreover, we have developed a theorem revealing the requirements/conditions for information-theoretic security, which can provide guidance and insights for authentication protocol design. We have further designed a multi-message authentication protocol to meet the security requirements, with high efficiency. The theoretical analysis demonstrated that the proposed protocol is information-theoretic secure for a polynomial number of messages and attacks. Finally, an efficient and feasible authentication protocol over binary symmetric wiretap channel has been proposed, using LFSR-based hash functions and strong secure polar code. For the future work, we will extend this study to develop a computationally efficient protocol for Gaussian wiretap channels.

References

[1] D. Chen, N. Cheng, N. Zhang, et al., "Multi-message Authentication over Noisy Channel with Polar Codes," *in Proc. IEEE MASS2017*, Orlando, Florida, pp. 46-54, Oct. 2017.
[2] Q. Wang, K. Xu, and K. Ren. "Cooperative Secret Key Generation from Phase Estimation in Narrowband Fading Channels," *IEEE Journal on Selected Areas in Commun.*, vol. 30, no. 9, pp. 1666-1674, Oct. 2012.
[3] J. Liu, Z. Liu, Y. Zeng, J. Ma, "Cooperative Jammer Placement for Physical Layer Security Enhancement," *IEEE Network*, vol. 30, no. 6, pp. 56-61, 2016.
[4] Z. Yang, P. Cheng, J. Chen, "Learning-Based Jamming Attack against Low-Duty-Cycle Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 6, pp. 650-663, Nov., 2017.
[5] D. Chen, Z. Qin, X. Mao, et al., "SmokeGrenade: An Efficient Key Generation Protocol with Artificial Interference,", *IEEE Trans. on Inform. Forens. and Security*, vol. 8, no. 11, pp. 1731-1745, Aug. 2013.
[6] D. Chen, N. Zhang, Z. Qin, et al., "S2M: A Lightweight Acoustic Fingerprints based Wireless device authentication protocol", *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88-100, Feb. 2017.
[7] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933-2945, Aug. 2007.
[8] A. T. Suresh, A. Subramanian, A. Thangaraj, M. Bloch, and S. W.McLaughlin, "Strong secrecy for erasure wiretap channels," *in Proc. IEEE Information Theory Workshop*, Dublin, pp. 1-5, Aug. 2010.
[9] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes," *IEEE Trans. on Inform. Forens. and Security*, vol. 6, no. 3, pp.585-594, Sep. 2011.
[10] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," *in Proc. of IEEE Information Theory Workshop*, Dublin, pp. 1-5, Aug. 2010.
[11] H. Mahdavifar, A. Vardy, " Achieving the secrecy capacity of wiretap channels using polar codes," IEEE *Trans. on Inf. Theory*, vol. 57, no. 10, pp. 6428-6443, Oct. 2011.
[12] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, pp. 1355-387, Oct. 1975.
[13] I. Csiszár and J. Köner, "Broadcast channels with confidential messages," *IEEE Trans. on Inf. Theory*, vol. IT-24, no. 3, pp. 339-48, May 1978.
[14] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography, Part II: CR capacity," *IEEE Trans. on Inf. Theory*, vol. 44, no. 1, pp. 225-240, Jan. 1998.
[15] R. Lu, X. Lin, X. Liang, and X. Shen, "An efficient and provably secure public key encryption scheme based on coding theory," *Security and Communication Networks*, vol. 4, no. 12, pp. 1440-1447, Dec. 2011.
[16] G. J. Simmons, "Authentication theory/coding theory," *in Proc. CRYPTO84 on Advances in Cryptology, NewYork*, Springer-Verlag, 1985, pp. 411-431.
[17] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. on Inf. Theory*, vol. 46, no. 4, pp. 1350-1356, July 2000.
[18] I. Csiszár and J. Körner, *Information Theory: Coding Theorem for Discrete Memoryless System,* Cambridge University Press, 2011.
[19] I. Csiszar, "Almost independence and secrecy capacity," *Probl. Inf. Transm.*, vol. 32, pp. 40-47, Jan. 1996.
[20] M. Walker, "Information theoretic bounds for authentication schemes," *Journal of Cryptology*, vol. 2, no. 3, pp. 131-143, Jan. 1990.
[21] V. Korzhik, V. Yakovlev, G. M. Luna, and R. Chesnokov, "Performance Evaluation of Keyless Authentication Based on Noisy Channel", MMM-ACNS 2007, CCIS 1, V. Gorodetsky, I. Kotenko and V. A. Skormin (Eds.), Springer-Verlag, Heidelberg, pp. 115-126, Jan. 2007.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

[22] L. Lai, H. E. Gamal, and H. V. Poor, "Authentication Over Noisy Channels," *IEEE Trans. on Inf. Theory*, vol. 55, no. 2, pp.906-916, Feb. 2009.

[23] S. Jiang. "Keyless Authentication in a Noisy Model," *IEEE Trans. on Inform. Forens. and Security*, vol. 9, no. 6, pp. 1024-1033, Apr. 2014.

[24] S. Jiang. "On the Optimality of Keyless Authentication in a Noisy Model," *IEEE Trans. on Inform. Forens. and Security*, vol. 10, no. 6, pp. 1250-1261, Feb. 2015.

[25] Y. Pan, Y. Hou, M. Li, R. M. Gerdes, K. Zeng, et al., "Message Integrity Protection over Wireless Channel: Countering Signal Cancellation via Channel Randomization," *IEEE Transactions on Dependable and Secure Computing*, DOI: 10.1109/TDSC.2017.2751600.

[26] J.L Carter and M.N.Wegman, "Universal classes of hash functions," *Journal of computer and system sciences*, vol.18, pp. 143-154, Apr. 1979.

[27] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *Journal of computer and system sciences*, vol.22, pp. 265-279, June 1981.

[28] D. R. Stinson, "Universal hashing and authentication codes," Advances in Cryptology-CRYPTO'91, *Lecture Notes in Computer Science*, vol. 576, pp. 74-85, Springer-Verlag, Jan. 1992.

[29] D.R. Stinson, "Combinatorial techniques for universal hashing," *Journal of Computer and System Sciences*, vol.48, pp. 337-346, Apr. 1994.

[30] H. Krawczyk, "LFSR-based hashing and authentication," Advances in Cryptology-CRYPTO'94, *Lecture Notes in Computer Science*, pp. 129-139, Springer Berlin/Heidelberg, Aug. 1994.

[31] D. Chen, S. Jiang, and Z. Qin, " Message Authentication Code over a wiretap channel," *in Proc. of ISIT2015*, HongKong, China, pp. 2301-2305 2015.

[32] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051-3073, July 2009.

[33] S. Fang, Y. Liu, and P. Ning, "Mimicry Attacks Against Wireless Link Signature and New Defense Using Time-Synched Link Signature," *IEEE Trans. on Inform. Forens. and Security*, vol. 11, no. 7, pp. 1515-1527, July 2016.

[34] N. Saxena, B. J. Choi, and R. Lu "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid," *IEEE Trans. on Inform. Forens. and Security*, vol. 11, no. 5, pp. 907-921, May 2016.

[35] W. Wang, Z. Sun, K. Ren, et al, "Wireless Physical-Layer Identification: Modeling and Validation," *IEEE Trans. on Inform. Forens. and Security*, vol. 11, no. 9, pp. 2091-2106, Oct. 2016.

[36] T. X. Zheng, H. M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278-292, Jan. 2017.

[37] T. X. Zheng, H. M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827-3839, Jun. 2017.

[38] A. Mukherjee amd A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351-361, Jan. 2011.

[39] F. Zhu, F. Gao, T. Zhang, K. sun, M. Yao, "Physical-Layer Security for Full Duplex Communications With Self-Interference Mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329-340, Jan. 2016.

APPENDIX

In what follows, we prove Theorem 1. The main idea is to prove that sender Alice can authenticate a polynomial number of messages using K, where the attacker Oscar can adaptively interleave polynomial number of the impersonation attacks or substitution attacks.

The following lemma is from [19, Lemma 1], where X has the form $f(X)$ for a function f in [19]. Since f is arbitrary except $|f(\mathcal{X})| \geq 4$, the two lemmas are equivalent.

Lemma 3. *Let X and Y be two random variables over $\mathcal{X}$ and $\mathcal{Y}$, respectively, where $|\mathcal{X}| \geq 4$. Then*

$$\frac{1}{2\ln 2}\mathtt{SD}(X|Y;X)^2 \leq I(X;Y) \leq \mathtt{SD}(X|Y;X)\log\frac{|\mathcal{X}|}{\mathtt{SD}(X|Y;X)}. \tag{42}$$

Lemma 4. *Suppose that Alice authenticates the message sequence $M_1, M_2, \cdots, M_j$ with the key K by using the proposed authentication framework j times. Let*

$$\Omega_j = \{m_1, \cdots, m_j : I(K;\vec{Z}_1, \cdots, \vec{Z}_j | m_1, \cdots, m_j) > (j \cdot e^{-\alpha n})^{1/2}\}.$$

Then, we have

$$P(\Omega_j) \leq (j \cdot e^{-\alpha n)^{1/2}}, \tag{43}$$

Moreover, for all $(m_1, \cdots, m_j) \in \Omega_j^c$,

$$I(K;\vec{Z}_1, \cdots, \vec{Z}_j | m_1, \cdots, m_j) \leq (j \cdot e^{-\alpha n})^{1/2}. \tag{44}$$

Proof: By the definition of the conditional mutual information, we have

$$\begin{aligned}
&(j\tau)^{1/2}\sum_{\Omega_j} P(m_1, \cdots, m_j) \\
\leq &\sum_{\Omega_j} P(m_1, \cdots, m_j) I(K;\vec{Z}_1, \cdots, \vec{Z}_j | m_1, \cdots, m_j) \\
\leq &I(K;\vec{Z}_1, \cdots, \vec{Z}_j | M_1, \cdots, M_j)) \leq j \cdot e^{-\alpha n}.
\end{aligned}$$

Therefore,

$$P(\Omega_j) = \sum_{\Omega_j} P(m_1, \cdots, m_j) = \leq (j \cdot e^{-\alpha n)^{1/2}}.$$

It holds that $I(K;\vec{Z}_1, \cdots, \vec{Z}_j | m_1, \cdots, m_j) \leq (j \cdot e^{-\alpha n)^{1/2}}$ for all $(m_1, \cdots, m_j) \in \Omega_j^c$. ∎

For all $(m_1, \cdots, m_j) \in \Omega_j^c$, we define probability $\widetilde{P}(k, \vec{z}_1, \cdots, \vec{z}_j)$ on $\mathcal{K} \times \vec{\mathcal{Z}}^j$ by

$$\widetilde{P}(k, \vec{z}_1, \cdots, \vec{z}_j) = \Pr(k, \vec{z}_1, \cdots, \vec{z}_j | m_1, \cdots, m_j). \tag{45}$$

Denote $\hat{P}(k)$ and $\hat{Q}(\vec{z}_1, \cdots, \vec{z}_j)$ as the marginal distribution of $\widetilde{P}$, respectively.

By Lemma 3, Proposition 2 and the definition of Ω_j^c, we can obtain that, for all $(m_1, \cdots, m_j) \in \Omega_j^c$,

$$\begin{aligned}
&SD(K|\vec{Z}_1, \cdots, \vec{Z}_j, m_1, \cdots, m_j; K | m_1, \cdots, m_j) \\
\leq &\sqrt{2\ln 2 I(K;\vec{Z}_1, \cdots, \vec{Z}_j | m_1, \cdots, m_j)} \leq \sqrt{2\ln 2}(j \cdot e^{-\alpha n})^{1/4},
\end{aligned} \tag{46}$$

where the conditional probability distance is denoted by

$$\begin{aligned}
&SD(K|\vec{Z}_1, \cdots, \vec{Z}_j, m_1, \cdots, m_j; K | m_1, \cdots, m_j) \\
= &\sum_{\vec{z}_1, \cdots, \vec{z}_j} \hat{Q}(\vec{z}_1, \cdots, \vec{z}_j) SD(K|\vec{z}_1, \cdots, \vec{z}_j, m_1, \cdots, m_j; K | m_1, \cdots, m_j).
\end{aligned} \tag{47}$$

Lemma 5. *For all $(m_1, \cdots, m_j) \in \Omega_j^c$, we define*

$$O_j = \{\vec{z}_1, \cdots, \vec{z}_j : d(\vec{z}_1, \cdots, \vec{z}_j) > (j \cdot e^{-\alpha n})^{1/8}\}, \tag{48}$$

where $d(\vec{z}_1, \cdots, \vec{z}_j) = SD(K|\vec{z}_1, \cdots, \vec{z}_j, m_1, \cdots, m_j; K | m_1, \cdots, m_j)$. Then,

$$\hat{Q}(O_j) \leq \sqrt{2\ln 2}(j \cdot e^{-\alpha n})^{1/8}. \tag{49}$$

Proof: From Equ. (46), (47) and (48), we have

$$\begin{aligned}
&(j \cdot e^{-\alpha n})^{1/4}\sum_{O_j} \hat{Q}(\vec{z}_1, \cdots, \vec{z}_j) \\
\leq &\sum_{O_j} \hat{Q}(\vec{z}_1, \cdots, \vec{z}_j) d(\vec{z}_1, \cdots, \vec{z}_j) \\
\leq &SD(K|\vec{Z}_1, \cdots, \vec{Z}_j, m_1, \cdots, m_j; K | m_1, \cdots, m_j) \\
\leq &\sqrt{2\ln 2}(j \cdot e^{-\alpha n})^{1/4}
\end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

and thus

$$\hat{Q}(O_j)=\sum_{O_j}\hat{Q}(\vec{z}_1,\cdots,\vec{z}_j)\le\sqrt{2\ln 2}(j\cdot e^{-\alpha n})^{1/8}.$$

■

Based on the discussion above, we present the details of proof of Theorem 1.

Proof: From Lemma 1, the completeness requirement can be satisfied. Next, we focus on the authentication property.

The Upper bound of $P_{I,j}$: For $j\ge 2$, $(m_1,\cdots,m_{j-1})\in\Omega^c_{j-1}$ and $(\vec{z}_1,\cdots,\vec{z}_{j-1})\in O^c_{j-1}$, we have

$$\begin{aligned}
&P(r_{oj}=\psi_K(m_{oj})|\vec{z}_1,m_1,\cdots,\vec{z}_{j-1},m_{j-1})\\
&=\sum_k P(k|\vec{z}_1,m_1,\cdots,\vec{z}_{j-1},m_{j-1})\ \theta(\psi_k(m_{oj}),r_{oj})\\
&\le\sum_k\Big\{|P(k|\vec{z}_1,m_1,\cdots,\vec{z}_{j-1},m_{j-1})-P(k|m_1,\cdots,m_{j-1})|\\
&\qquad+P(k|m_1,\cdots,m_{j-1})\Big\}\ \theta(\psi_k(m_{oj}),r_{oj})\\
&\le d(\vec{z}_1,\cdots,\vec{z}_{j-1})+\sum_k P(k|m_1,\cdots,m_{j-1})\ \theta(\psi_k(m_{oj}),r_{oj})\\
&\le d(\vec{z}_1,\cdots,\vec{z}_{j-1})+\sum_k P(k)\ \theta(\psi_k(m_{oj}),r_{oj})\\
&\qquad(K\text{ and }M_1,...,M_j\text{ are independent})\\
&=(j\cdot e^{-\alpha n})^{1/8}+\frac{1}{|\mathcal{K}|}(|\mathcal{K}|\varepsilon)\quad(\text{by the definition of }\varepsilon\text{-AWU}_2)\\
&=(j\cdot e^{-\alpha n})^{1/8}+\varepsilon
\end{aligned}$$

Then, by Equ. (7), the success probability of impersonation attack can be given as

$$\begin{aligned}
P_{I,j}&=\sum_{m_1,\vec{z}_1,\cdots,m_{j-1},\vec{z}_{j-1}}P(m_1,\vec{z}_1,\cdots,m_{j-1},\vec{z}_{j-1})\times\\
&\qquad\sup_{h_{j,im}}\Big\{P(s_{oj}=\psi_K(m_{oj})|m_1,\vec{z}_1,\cdots,m_{j-1},\vec{z}_{j-1})\Big\}\\
&=\Big\{\sum_{\{\Omega^c_{j-1}\times O^c_{j-1}\}^c}+\sum_{\Omega^c_{j-1}\times O^c_{j-1}}\Big\}P(m_1,\vec{z}_1,\cdots,m_{j-1},\vec{z}_{j-1})\times\\
&\qquad\sup_{h_{j,im}}\Big\{P(s_{oj}=\psi_K(m_{oj})|m_1,\vec{z}_1,\cdots,m_{j-1},\vec{z}_{j-1})\Big\}\\
&\le 3(j\cdot e^{-\alpha n})^{1/8}+\sum_{\Omega^c_{j-1}\times O^c_{j-1}}P(m_1,\vec{z}_1,\cdots,m_{j-1},\vec{z}_{j-1})\times\\
&\qquad\Big\{(j\cdot e^{-\alpha n})^{1/8}+\varepsilon\Big\}\\
&\le\varepsilon+4(j\cdot e^{-\alpha n})^{1/8}.
\end{aligned}$$

The Upper bound of $P_{S,j}$: We first bound the success probability $P_{S_1,j}$ of type I substitution attack in slot j.

For $j\ge 2$, $(m_1,\cdots,m_j)\in\Omega^c_j$ and $(\vec{z}_1,\cdots,\vec{z}_j)\in O^c_j$, we have

$$\begin{aligned}
&P(s_j=\psi_K(m_{oj})|m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\ (1-\theta(m_{oj},m_j))\\
&=\sum_{k\in\mathcal{K}}P(k|m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\times\\
&\qquad\Big\{\theta(\psi_k(m_{oj}),\psi_k(m_j))(1-\theta(m_{oj},m_j))\Big\}\\
&\le d(\vec{z}_1,\cdots,\vec{z}_j)+\sum_k P(k|m_1,\cdots,m_{j-1})\times\\
&\qquad\Big\{\theta(\psi_k(m_{oj}),\psi_k(m_j))(1-\theta(m_{oj},m_j))\Big\}\\
&\le d(\vec{z}_1,\cdots,\vec{z}_j)+\sum_k P(k)\theta(\psi_k(m_{oj}),r_j)(1-\theta(m_{oj},m_j))\\
&\qquad(K\text{ and }M_1,...,M_j\text{ are independent})\\
&=(j\cdot e^{-\alpha n})^{1/8}+\frac{1}{|\mathcal{K}|}\cdot\varepsilon|\mathcal{K}|\quad(\text{by the definition of }\varepsilon\text{-AWU}_2)\\
&=(j\cdot e^{-\alpha n})^{1/8}+\varepsilon
\end{aligned}$$

From Equ. (8), $P_{S_1,j}$ can be rewritten as

$$\begin{aligned}
P_{S_1,j}&=\sum_{m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j}P(m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\times\\
&\quad\sup_{h_{1j,sb}}\Big\{P(s_j=\psi_K(m_{oj})|m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\ (1-\theta(m_{oj},m_j))\Big\}\\
&=\Big\{\sum_{\{\Omega^c_j\times O^c_j\}^c}+\sum_{\Omega^c_j\times O^c_j}\Big\}P(m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\times\\
&\quad\sup_{h_{j,im}}\Big\{P(s_j=\psi_K(m_{oj})|m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\ (1-\theta(m_{oj},m_j))\Big\}\\
&\le 3(j\cdot e^{-\alpha n})^{1/8}+\sum_{\Omega^c_j\times O^c_j}P(m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)[(j\cdot e^{-\alpha n})^{1/8}+\varepsilon]\\
&\le\varepsilon+4(j\cdot e^{-\alpha n})^{1/8}.
\end{aligned}$$

Then, we bound the success probability $P_{S_2,j}$ of type II substitution attack in slot j. Similarly, we have

$$\begin{aligned}
&P(r_{oj}=\psi_k(m_{oj})|m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)(1-\theta(m_{oj},m_j))\\
&\le\varepsilon+(j\cdot e^{-\alpha n})^{1/8}
\end{aligned}$$

From Equ. (9) and following the same procedure in the proof of the upper bound of $P_{S_1,j}$, we have

$$\begin{aligned}
P_{S_2,j}&=\sum_{m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j}P(m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)\\
&\quad\sup_{h_{2j,sb}}\Big\{P(s_{oj}=\psi_k(m_{oj})|m_1,\vec{z}_1,\cdots,m_j,\vec{z}_j)(1-\theta(m_{oj},m_j))\Big\}\\
&\le\varepsilon+4(j\cdot e^{-\alpha n})^{1/8}.
\end{aligned}$$

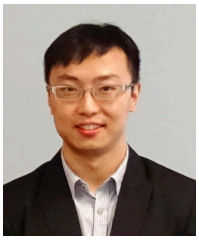
Thus, the success probability of Oscar after attacking $t(n)$ times from Oscar (and authenticating $t(n)$ messages with the same key) can be rewritten as

$$\begin{aligned}
P_D&\le\sum_{j=1}^{t(n)}\max\{P_{I,j},P_{S_1,j},P_{S_2,j}\}\\
&\le\sum_{j=1}^{t(n)}\varepsilon+4(j\cdot e^{-\alpha n})^{1/8}\qquad(\text{by }\varepsilon\ge\frac{1}{\mathcal{S}})\\
&\le t(n)\cdot\varepsilon+4\cdot t^2(n)\cdot e^{-\frac{1}{8}\alpha n}
\end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2846258, IEEE Transactions on Dependable and Secure Computing

This is negligible as $t(n)$ is a polynomial and ε is negligible. ■

Dajiang Chen (M'15)is currently an Assistant Professor in the School of information and software Engineering at University of Electronic Science and Technology of China (UESTC). He was a Post Doctoral Fellow at the University of Waterloo, Waterloo, ON, Canada, from 2015 to 2017. He was also a Post Doctoral Fellow in the School of information and software Engineering at UESTC, from 2014 to 2017. He received the B.Sc. degree in 2005 and the M.Sc. degree in 2009 from Neijiang Normal University and Sichuan University, respectively, and the Ph.D. degree in information and communication engineering from UESTC in 2014. His current research interest includes Information Theory, Secure Channel Coding, and their applications in Wireless Network Security, Wireless Communications and other related areas. Dr. Chen serves/served as a TPC Member for IEEE Globecom, IEEE VTC, IEEE WPMC, and IEEE WF-5G.



Ning Zhang (M'15) is currently an Assistant Professor at Texas A&M University at Corpus Christi, TX, USA. Before that, he was a Post Doctoral Fellow at the University of Waterloo and University of Toronto, respectively. He received the B.Sc. degree from Beijing Jiaotong University, Beijing in 2007, the M.Sc. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2010, and the Ph.D. degree from University of Waterloo, Waterloo, ON, Canada, in 2015. His current research interests include physical layer security, dynamic spectrum access, 5G, and vehicular networks.

Nan Cheng (S'13) is currently a Post Doctoral Fellow at the University of Waterloo, Waterloo, ON, Canada. He received his B.S. degree and M.S. degree from Tongji University, China, in 2009 and 2012, respectively. He obtained the Ph.D. degree from University of Waterloo, Waterloo, ON, Canada, in 2016. His research interests include vehicular communication networks, cognitive radio networks, resource allocation in smart grid, and cellular traffic offloading.

Kuan Zhang (S'13-M'17) has been an assistant professor at the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, USA, since September 2017. He received the B.Sc. degree in Communication Engineering and the M.Sc. degree in Computer Applied Technology from Northeastern University, China, in 2009 and 2011, respectively. He received the Ph.D. degree in Electrical and Computer Engineering from the University of Waterloo, Canada, in 2016. He was also a postdoctoral fellow with the Broadband Communications Research (BBCR) group, Department of Electrical and Computer Engineering, University of Waterloo, Canada, from 2016-2017. His research interests include security and privacy for mobile social networks, e-healthcare systems, cloud/edge computing and cyber physical systems.

Zhiguang Qin (S'95-A'96-M'14) is Dean of the School of Software of University of Electronic Science and Technology of China (UESTC), where he is also Director of the Key Laboratory of New Computer Application Technology and Director of UESTC-IBM Technology Center. His research interests include Computer Networking, Information Security, Cryptography, Information Management, Intelligent Traffic, Electronic Commerce, Distribution and middleware. He is a member of the IEEE.

Dr. Xuemin (Sherman) Shen (M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a University Professor and the Associate Chair for Graduate Studies, Department of Electrical and Computer Engineering, University of Waterloo, Canada. Dr. Shens research focuses on wireless resource management, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. He is the elected IEEE ComSoc VP Publication, was a member of IEEE ComSoc Board of Governor, and the Chair of Distinguished Lecturers Selection Committee. Dr. Shen served as the Technical Program Committee Chair/Co-Chair for IEEE Globecom16, Infocom14, IEEE VTC10 Fall, and Globecom07, the Symposia Chair for IEEE ICC10, the Tutorial Chair for IEEE VTC'11 Spring and IEEE ICC08, the General Co-Chair for ACM Mobihoc15, Chinacom07 and QShine06, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE Internet of Things Journal, IEEE Network, Peer-to-Peer Networking and Application, and IET Communications; a Founding Area Editor for IEEE Transactions on Wireless Communications; and an Associate Editor for IEEE Transactions on Vehicular Technology and IEEE Wireless Communications, etc. Dr. Shen received the IEEE ComSoc Education Award, the Joseph LoCicero Award for Exemplary Service to Publications, the Excellent Graduate Supervision Award in 2006, and the Premiers Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.