

Artificial-Noise-Aided Message Authentication Codes with Information-Theoretic Security

Xiaofu Wu, Zhen Yang, Cong Ling, and Xiang-Gen Xia

Abstract—In the past, two main approaches for the purpose of authentication, including information-theoretic authentication codes and complexity-theoretic message authentication codes (MACs), were almost independently developed. In this paper, we propose a new cryptographic primitive, namely, artificial-noise-aided MACs (ANA-MACs), which can be considered as both computationally secure and information-theoretically secure. For ANA-MACs, we introduce artificial noise to interfere with the complexity-theoretic MACs and quantization is further employed to facilitate packet-based transmission. With a channel coding formulation of key recovery in the MACs, the generation of standard authentication tags can be seen as an encoding process for the ensemble of codes, where the shared key between Alice and Bob is considered as the input and the message is used to specify a code from the ensemble of codes. Then, we show that the introduction of artificial noise in ANA-MACs can be well employed to resist the key recovery attack even if the opponent has an unlimited computing power. Finally, a pragmatic approach for the analysis of ANA-MACs is provided, and we show how to balance the three performance metrics, including the completeness error, the false acceptance probability, and the conditional equivocation about the key. The analysis can be well applied to a class of ANA-MACs, where MACs with Rijndael cipher are employed.

Index Terms—Information-theoretic authentication codes, message authentication codes, channel coding and decoding, information-theoretic security.

I. INTRODUCTION

MESSAGE authentication codes (MACs) are cryptographic primitives used extensively in the construction of security services, including authentication, nonrepudiation, and integrity. Basically, message authentication is to ensure that an accepted message truly comes from its acclaimed transmitter. When the transmitter intends to send a message, it also generates a MAC, which is a function of the message and a shared key, known only to both the transmitter and the receiver. The generated MAC is often appended to the message [1]. At the receiver, a MAC is computed from the received message and compared to the MAC that is transmitted. If the

two MACs are identical, then the transmitter is identified as a legal user and it is highly likely the received message is exactly equal to the one transmitted.

In the past, two main approaches, including information-theoretic authentication codes [2], [3] and complexity-theoretic MACs, were almost independently developed for the purpose of authentication. In general, they differ in the assumptions about the capabilities of an opponent. Information-theoretic authentication codes, which are based on information theory, offer unconditional security, i.e., security independent of the computing power of an adversary. The complexity-theoretic approach starts from an abstract model for computation, and assumes that the opponent has limited computing power. Due to their high flexibility, the complexity-theoretic MACs find widespread applications in practice.

Complexity-theoretic MAC algorithms can be constructed from other cryptographic primitives, such as cryptographic hash functions, or block cipher algorithms. Currently, the security of MAC algorithms rely on the hardness of hash functions, i.e, given the message and its MAC, it is “hard” to forge a MAC on a new message. This means that they can be broken if the adversary has an unlimited power of computation.

In recent years, there has been various efforts [4]–[7] in authenticating the transmitter and receiver at the physical layer, based on prior coordination or secret sharing, where the sender is authenticated if the receiver can successfully demodulate and decode the transmission. In [4], a physical-layer authentication scheme was proposed, in which MACs, along with messages, are transmitted concurrently over the physical layer. Compared to the traditional transmission approach above the physical layer, the authors claim the possibility of information-theoretic security due to the presence of channel noise. However, its security often depends on the physical channel.

In this paper, we develop a new cryptographic primitive, artificial-noise-aided MACs (ANA-MACs) for ensuring information-theoretic security. The use of artificial noise in ANA-MACs makes it difficult for an opponent to derive the key. With the use of quantization, ANA-MACs can be encapsulated and transmitted in packets above the physical layer, just like the traditional MACs, which is in sharp contrast to existing physical layer authentication schemes.

It should be pointed out that the proposed ANA-MACs are also different with the binary approximate message authentication codes (AMACs) [8], [9] and the noise-tolerant message authentication codes (NT-MACs) [10]. Both AMACs and NT-MACs are designed to tolerate some channel errors during the transmission of messages. For ANA-MACs, a slight change

This work was supported in part by the National Natural Science Foundation of China under Grants 61372123, 61271335, by the Key University Science Research Project of Jiangsu Province under Grant 14KJA510003 and by the Scientific Research Foundation of Nanjing University of Posts and Telecommunications under Grant NY213002.

Xiaofu Wu and Zhen Yang are with the Key Lab of Ministry of Education in Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mails: xfuwu@ieee.org, yangz@njupt.edu.cn).

Cong Ling is with the Department of Electrical and Electronic Engineering, Imperial College London, London, UK (e-mail: cling@ieee.org).

Xiang-Gen Xia is with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 (e-mail: xxia@ee.udel.edu).

in messages may result in a rapid change for authentication tags, as often encountered in the traditional MACs. Yet, ANA-MACs can tolerate some channel errors occurred during the transmission of tags. Furthermore, both AMACs and NT-MACs are computationally secure, while ANA-MACs may ensure some degree of information-theoretic security.

Throughout this paper, we do not discriminate the notations between scalars and vectors, which will be made clear from the contexts. For a binary vector t , its bipolar form is simply denoted as \bar{t} , in which each component takes value from $\{+1, -1\}$. To be consistent with the standard convention in algorithms and complexity theory, where the running time of an algorithm is measured as a function of the length of its input n , we will thus provide the adversary and the honest parties with the security parameter in unary as 1^n (i.e., a string of n 1's) when necessary [11].

The rest of the paper is organized as follows. Some preliminaries on both information-theoretic authentication codes and MACs are made in Section-II. In Section-III, a new cryptographic primitive, ANA-MACs, is proposed and its verification mechanism is given. Then, its security analysis is formulated in Section-IV. In Section-V, we provide a pragmatic approach for analysis of ANA-MACs. Section-VI presents numerical results and the conclusion is made in Section-VII.

II. PRELIMINARY

A. Information-Theoretic (Systematic) Authentication Codes

A systematic authentication code is a triple of $(\mathcal{S}, \mathcal{T}, \mathcal{K})$ of finite sets and a mapping $E : \mathcal{K} \times \mathcal{S} \rightarrow \mathcal{T}$, where \mathcal{S} is the source state space, \mathcal{T} is the tag space, \mathcal{K} is the key space, and $E(k, \cdot) \triangleq E_k : \mathcal{S} \rightarrow \mathcal{T}$ is often called an encoding rule for a given $k \in \mathcal{K}$.

Two trusting parties, Alice (or a transmitter) and Bob (or a receiver), share a secret key $k \in \mathcal{K}$. To send a piece of information (called source state) $s \in \mathcal{S}$ to Bob, Alice computes $t = E_k(s) \in \mathcal{T}$ and puts the message $m = (s, t)$ into a public channel. After receiving $m' = (s', t')$, Bob will compute $E'_k(s)$ and check whether $t' = E'_k(s)$. If yes, Bob will accept it as authentic. Otherwise, Bob will reject it.

We assume that an opponent (or Eve) has a complete understanding of the system, including the mapping E . The only thing she does not know is the key k agreed upon by Alice and Bob, which is used to specify a particular encoding rule E_k . We also assume that Eve has the ability to introduce a message into the channel. After observation of the first r messages m_1, \dots, m_r , Eve places her own message m into the channel, attempting to make Bob accept it as authentic. This is called a spoofing attack of order r . In literature, there are often two different types of spoofing attack, i.e., impersonation attack and substitution attack. An impersonation attack at time $r + 1$ [12] is just the spoofing attack of order r . In a so-called substitution attack at time r , Eve observed r messages m_1, \dots, m_r and replaces the message m_r by a different message which she hopes to be accepted by Bob.

For systematic authentication codes, a source state s is assumed to be public (without security) whenever $m = (s, t)$ is transmitted, which can be freely accessed by both Bob and

Eve. For this reason, we simply use the authentication tag t instead of a full message m in what follows.

Let K, T_{r+1} and T^r denote the random variables describing the key, the $r + 1$ -th tag and a sequence of r tags from time 1 to r , and taking values k, t_{r+1} and $t^r = (t_1, \dots, t_r)$, respectively. Let p_r denote the expected probability of successful deception for a spoofing attack of order r and P_r the probability of successful deception if Eve can observe at most r messages. Walker [13] proved

$$p_r \geq 2^{H(K|T^{r+1}) - H(K|T^r)} = 2^{-I(K; T_{r+1}|T^r)} \quad (1)$$

and Rosenbaum [14] proved

$$P_r \geq 2^{-\frac{1}{r+1}H(K)}, \quad (2)$$

which hold even if Eve has an unlimited power of computation. If the equality in (2) holds, the corresponding authentication code is called r -perfect.

To prevent Eve from using $t = E_k(s)$ to learn the key k , it should have sufficient number of solutions of k for a given $t = E_k(s)$ [2]. Given s and t , let $\mathcal{K}(s, t) \triangleq \{k : E_k(s) = t, \forall k \in \mathcal{K}\}$ denotes the set of solutions for $t = E_k(s)$. It follows that the successful deception probability for a given pair (s, t) has a lower bound of

$$p_1(s, t) \geq \frac{1}{|\mathcal{K}(s, t)|}. \quad (3)$$

In [2], projective plane codes were proposed to achieve the best possible spoofing attack of order 1, namely, $P_1 = \frac{1}{\sqrt{|\mathcal{K}|}}$. For the best authentication codes achieving the lower bound of P_1 , it was proved that

- 1) $|\mathcal{K}(s_1, t_1) \cap \mathcal{K}(s_2, t_2)| = 1$ if $s_1 \neq s_2$;
- 2) $|\mathcal{K}(s, t)| = \sqrt{|\mathcal{K}|}$ for $\forall s \in \mathcal{S}, t \in \mathcal{T}$;
- 3) $|\{t : |\mathcal{K}(s, t)| > 0\}| = \sqrt{|\mathcal{K}|}$ for $\forall s \in \mathcal{S}$.

However, this class of authentication codes cannot resist the spoofing attack of order $r \geq 2$.

Theorem 1: For 1-perfect systematic authentication codes, they cannot resist the spoofing attack of order $r \geq 2$, namely, $p_r = 1, \forall r \geq 2$.

Proof: It is enough to consider $r = 2$. Suppose that Eve has accessed two different messages $m_1 = (s_1, t_1)$ and $m_2 = (s_2, t_2)$, where $s_1 \neq s_2$. To insert a new message $m = (s, t)$, where $s \neq s_1, s_2$, Eve wants to derive the key k , which can be surely learned from two available messages since $|\mathcal{K}(s_1, t_1) \cap \mathcal{K}(s_2, t_2)| = 1$. Indeed, there is a single common solution of k for $t_1 = E_k(s_1)$ and $t_2 = E_k(s_2)$ if $s_1 \neq s_2$. ■

Given $s^r = (s_1, \dots, s_r)$ and $t^r = (t_1, \dots, t_r)$, let $\mathcal{K}(s^r, t^r) \triangleq \{k : E_k(s_i) = t_i, i = 1, \dots, r, \forall k \in \mathcal{K}\}$ denote the set of solutions for $t_i = E_k(s_i), i = 1, \dots, r$. Clearly, $\mathcal{K}(s^r, t^r) = \bigcap_{i=1, \dots, r} \mathcal{K}(s_i, t_i)$.

For r -perfect authentication codes, it was shown in [14] that

$$|\mathcal{K}(s^i, t^i)| = |\mathcal{K}|^{\frac{r+1-i}{r+1}}, i \in \{1, \dots, r+1\}.$$

and $H(K|T^{r+1}) = 0$. Hence, we also have the same result as that of Theorem 1 for r -perfect authentication codes.

Theorem 2: For r -perfect authentication codes, they cannot resist the spoofing attack of order $l \geq r + 1$, namely, $p_l = 1, \forall l \geq r + 1$.

B. Complexity-Theoretic MACs

Definition 1: A message authentication code $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ is a triple of algorithms with associated key space \mathcal{K} , source message (state) space \mathcal{S}^1 , and tag space \mathcal{T} .

- Key Generation. Upon input 1^n , the algorithm Gen outputs a uniformly distributed key k of length n : $k \leftarrow \text{Gen}(1^n)$.
- Tagging. The probabilistic authentication algorithm $\text{Mac}_k(s)$ takes as input a secret key $k \in \mathcal{K}$ and a source message $s \in \mathcal{S}$ and outputs an authentication tag $t \in \mathcal{T}$.
- Verification. The deterministic verification algorithm $\text{Vrfy}_k(s, t)$ takes as input a secret key k , a source message $s \in \mathcal{S}$ and a tag $t \in \mathcal{T}$ and outputs an element of the set $\{0, 1\}$.

A complexity-theoretic MAC $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ can be formulated with a keyed hash function. Formally, the tag is a function of the source message s and the secret key k

$$t = \bar{h}(k, s), \quad (4)$$

where $\bar{h} : \mathcal{K} \times \mathcal{S} \rightarrow \mathcal{T}$ is a keyed hash function.

The verification algorithm takes k, s, t as inputs and outputs a binary decision

$$\nu = \vartheta(k, s, t), \quad (5)$$

where $\nu \in \{0, 1\}$, and $\vartheta(k, s, t) = 1$ if $t = \bar{h}(s, k)$, zero otherwise.

Note that a MAC implies a two-round authentication protocol: the verifier chooses a random message as challenge, and the prover returns the MAC on the message.

Definition 2 (Completeness [15]): We say that a MAC has completeness error α if for all $s \in \mathcal{S}$ ²

$$P[\vartheta(k, s, t) = 0 : k \leftarrow \text{Gen}(1^n), t \leftarrow \bar{h}_k(s)] \leq \alpha. \quad (6)$$

It is clear that the completeness error α means that the successful authentication probability is larger than $1 - \alpha$ for two trusted parties.

C. Remark

Information-theoretic (systematic) authentication codes provide message authenticity guarantees in an information theoretic sense within a symmetric key setting. However, information theoretic bounds on the spoofing attack of order r show that they are still vulnerable (Theorems 1 and 2) if the opponent can access much more authenticated messages. Complexity-theoretic MACs can be seen as a *counterpart* of information-theoretic authentication codes *in the field of computational security*, without considering the information-theoretic deception probability.

In the past, information-theoretic authentication codes and complexity-theoretic MACs are almost independently developed. It is interesting to ask if we can construct MACs, which are both computationally secure and information-theoretically secure.

¹In literature, the message space \mathcal{M} is often used.

²It requires to hold for all $n \in \mathbb{N}$ in [15] while the completeness error is defined for a given and fixed n in this paper.

III. ARTIFICIAL-NOISE-AIDED MACS

A. Basic Idea

We have shown that information-theoretic (systematic) authentication codes take the same function as message authentication codes. If $E(k, s) = \bar{h}(k, s), \forall k \in \mathcal{K}, s \in \mathcal{S}$, they are actually the same.

In general, the authentication tag is a deterministic function of a source message s and the key k shared between Alice and Bob. The only exception is the authentication codes with splitting, where the mapping $\bar{h} : \mathcal{K} \times \mathcal{S} \rightarrow \mathcal{T}$ is allowed to be stochastic in the sense that, for given k and s , $\bar{h}(k, s)$ is a stochastic variable.

Noting that the use of a stochastic encoding mapping in authentication may be helpful for preventing possible spoofing attacks, since the conditional equivocation about the key may increase compared to a deterministic mapping. In order to make this ideal more practical, we propose to introduce artificial noise to corrupt the standard authentication tags.

On one hand, the introduction of artificial noise may increase the conditional equivocation about the key, namely, $H(K|\tilde{T}) \geq H(K|T)$. Here T and \tilde{T} denote the random variables for the standard authentication tag and artificial-noise-corrupted authentication tag, respectively. On the other hand, the successful authentication probability may decrease as the introduction of noise. Nevertheless, this can be made acceptable in practice if the completeness error is negligible.

B. Formulation

Suppose that $|\mathcal{T}| = 2^l, |\mathcal{K}| = 2^n$. To prevent possible eavesdropping, we propose to introduce artificial noise to interfere with the clean tag, and then quantization is used to facilitate packet-based transmission.

An artificial-noise-aided message authentication code (ANA-MAC) is thus with a probabilistic algorithm \bar{h}_k^{qw} to produce the tag

$$\tilde{t} \leftarrow \bar{h}_k^{qw}(s) \quad (7)$$

when the inputs are k, s .

In this paper, we consider an explicit construction of $\bar{h}_k^{qw}(s)$ as follows

$$\begin{aligned} t &= \bar{h}(k, s), \\ \tilde{t} &= \mathcal{Q}(\bar{t} + w), \end{aligned} \quad (8)$$

where \bar{t} is the l -length bipolar vector form of t , w is an artificially-introduced Gaussian-distributed noise vector with zero mean and variance of $\sigma_w^2 I_l$ (I_l denotes the identity matrix of size $l \times l$), $\mathcal{Q}(x)$ is a q -bit quantization function, and $\bar{t} \in \bar{\mathcal{T}}$ is a l -length vector, where each component takes value from a finite quantization level set $V = \{v_1, v_2, \dots, v_{2^q}\}$ of size 2^q . Clearly, $\bar{\mathcal{T}} = V^l$, where V^l denotes the cartesian power of a set V .

With the introduction of artificial noise and quantization, the size of an original tag t is expanded by q times. In practice, $q = 8$ is often enough.

Given s and k , it is possible to partition $\bar{\mathcal{T}}$ into two disjoint sets, namely, $\bar{\mathcal{T}} = \bar{\mathcal{T}}_A(k, s) \cup \bar{\mathcal{T}}_F(k, s)$, where

$P(\tilde{t} \in \tilde{\mathcal{T}}_A(k, s)) \geq 1 - \alpha$. In essence, the verification algorithm for ANA-MAC is to find a deterministic partition of $\tilde{\mathcal{T}}$ for given s and k , which minimizes the false acceptance probability and at the same time keeps the successful authentication probability not smaller than a target value of $1 - \alpha$.

Whenever such a partition is determined, the verification algorithm can be well formulated. It takes k, s, \tilde{t} as inputs and outputs a binary decision

$$\nu = \vartheta(k, s, \tilde{t}), \quad (9)$$

where $\nu \in \{0, 1\}$, $\vartheta(k, s, \tilde{t}) = 1$ if $\tilde{t} \in \tilde{\mathcal{T}}_A(k, s)$ and zero otherwise.

An ANA-MAC has completeness error α if for all $s \in \mathcal{S}$,

$$P[\vartheta(k, s, \tilde{t}) = 0 : k \leftarrow \text{Gen}(1^n), \tilde{t} \leftarrow \tilde{h}_k^{qw}(s)] \leq \alpha. \quad (10)$$

C. Verification with Hypothesis Testing

1) *Hypothesis Testing*: Hypothesis testing is the task of deciding which of two hypotheses, H_0 or H_1 , is true, when one is given the value of a random variable U (e.g., the outcome of a measurement). The behavior of U is described by two probability distributions: If H_0 or H_1 is true, then U is distributed according to the distribution $p_{H_0}(u)$ or $p_{H_1}(u)$, respectively.

Let $P_D = 1 - \alpha$ be the detection probability, namely, the probability of successful declaration of H_0 when H_0 is actually true, and $P_f = \beta$ be the false alarm probability, namely, the probability of false declaration of H_0 when H_1 is actually true.

The optimal decision rule is given by the famous Neyman-Pearson theorem which states that, for a given maximal tolerable false alarm probability β , α can be minimized by assuming hypothesis if and only if

$$\log \frac{p_{H_0}(U = u)}{p_{H_1}(U = u)} \geq \varrho \quad (11)$$

for some threshold ϱ depending on α .

Let the function $\mathcal{D}(\alpha, \beta)$ be defined by

$$\mathcal{D}(\alpha, \beta) = \alpha \log \frac{\alpha}{1 - \beta} + (1 - \alpha) \log \frac{1 - \alpha}{\beta}. \quad (12)$$

With optimal hypothesis testing (11), its detection probability and false alarm probability are closely connected [12].

Lemma 1: The detection probability $1 - \alpha$ and the false alarm probability β satisfy

$$\mathcal{D}(\alpha, \beta) \leq D_{KL}(p_{H_0}(u) || p_{H_1}(u)) \quad (13)$$

where the Kullback-Leibler (KL) divergence can be written as

$$D_{KL}(f(x) || g(x)) = \sum_x f(x) \log \frac{f(x)}{g(x)} \quad (14)$$

for two probability distributions $f(x), g(x)$.

2) *Verification*: Now, we focus on the design of verification algorithm for ANA-MACs, which often deals with the impersonation attack. The problem of deciding whether a received tag is authentic or not can be viewed as a hypothesis testing problem [12].

Let H_0 correspond to the hypothesis that the tag is authentic, and H_1 correspond to the hypothesis that the tag has been generated by an adversary. With a standard packet-level transmission above the physical layer, it is assumed that both a legitimate user and an adversary can get a error-free copy of the tag, namely, \tilde{t} .

To facilitate the derivation, we simply assume that $\tilde{t} = \bar{t} + w$, where the quantization is simply omitted. This is a reasonable approximation if a fine quantization method with sufficient number of quantization levels is employed.

To be more concrete, we consider the ‘‘Alice-Bob-Eve’’ model, where Eve, as an impersonation attacker, wants to inject messages into the legitimate transmission from Alice to Bob. Suppose Alice and Bob shared a key k , which is employed to authenticate each other. With inputs k, s, \tilde{t} , Bob wants to decide if \tilde{t} is from Alice. Eve does not know the shared key k , and it is assumed that Eve generates a random key k_E for authentication as there is no any information about k available. Essentially, this is cast as a binary hypothesis testing problem:

$$\begin{aligned} H_0 &: K = k \\ H_1 &: K = k_E. \end{aligned}$$

In this case, $U = (\tilde{T}, K)$, $u = (\tilde{t}, k)$. Under hypothesis H_0 , the pair $u = (\tilde{t}, k)$ (seen by the receiver) is generated according to the distribution $p(\tilde{t}, K = k)$, whereas under hypothesis H_1 , $u = (\tilde{t}, k)$ is generated according to the distribution $p(\tilde{t}) \cdot P(K = k)$. This is because that in the case of H_1 , the generations of authentication tag and key are independent of each other as there is no means to efficiently guess the key.

The formulation of the optimum binary hypothesis testing can be written as

$$\begin{aligned} \eta &= \log \frac{p_{H_0}(U = u)}{p_{H_1}(U = u)} = \log \frac{p(\tilde{t}, K = k)}{p(\tilde{t})P(K = k)} \\ &= \log \frac{p(\tilde{t}|K = k)}{\sum_{k' \in \mathcal{K}} p(\tilde{t}|K = k')P(K = k')}. \end{aligned} \quad (15)$$

The optimal decision rule is given by $\eta > \varrho$ for some threshold ϱ depending on α .

Now, it is clear that a partition of $\tilde{\mathcal{T}}$ for the purpose of verification can be done as

$$\tilde{\mathcal{T}}_A(k, s) = \left\{ \tilde{t} \in \tilde{\mathcal{T}} : \eta > \varrho \right\}. \quad (16)$$

As the source message s is assumed to be available, it follows that

$$p(\tilde{t}|k) \propto \exp \left[-\frac{(\tilde{t} - \bar{t})^T (\tilde{t} - \bar{t})}{2\sigma_w^2} \right] \quad (17)$$

with $t = \tilde{h}(k, s)$ and \bar{t} is its bipolar (column) vector form.

In general, this binary hypothesis testing problem in its optimum form can not be easily tackled as it requires to enumerate 2^n keys with a priori uniform distribution.

As the optimum hypothesis testing is difficult to implement, we propose to use a simple test statistic

$$\eta = \bar{\mu}^T \tilde{t}, \quad (18)$$

and η is further compared to a threshold value ϱ for making a final decision, where $\mu = \tilde{h}(k, s)$ is the tag generated by Bob and $\bar{\mu}$ is its bipolar vector form.

This approach can be viewed as a code acquisition approach encountered in code-division multiple-access (CDMA) communication systems, where the tag signature μ can be considered as a unique pseudo-noise (PN) code, which is available at the sides of both Alice and Bob, but keeps unknown to any potential attacker.

In both hypotheses, η is the sum of l normally distributed random variables, which is still normally distributed. Therefore, it suffices to compute its mean and variance.

In the case of hypothesis H_0 , one can show that

$$\eta|H_0 = l + z_0, \quad (19)$$

where $z_0 = \sum_{i=1}^l \bar{\mu}_i w_i$. We denote its mean and variance as

$$\begin{aligned} \bar{\eta}_0 &\triangleq E\{\eta|H_0\} = l, \\ \sigma_{H_0}^2 &\triangleq \text{Var}\{\eta|H_0\} = l\sigma_w^2. \end{aligned} \quad (20)$$

By decomposing the hypothesis H_1 into a series of sub-hypotheses $\{H_1^{k'} : H_1, K = k'\}$, i.e., by further assuming that Eve impersonates Alice using the key k' , we have

$$\eta|H_1^{k'} = l - 2d_H(\tilde{h}(k, s), \tilde{h}(k', s)) + z_1, \quad (21)$$

where $z_1 = \sum_{i=1}^l \bar{\mu}_i w_i$ and $d_H(x, y)$ denotes the Hamming distance between two binary strings of x and y . Then,

$$\begin{aligned} \bar{\eta}_1^{k'} &\triangleq E\{\eta|H_1, k'\} = l - 2d_H(\tilde{h}(k, s), \tilde{h}(k', s)), \\ \sigma_{H_1^{k'}}^2 &\triangleq \text{Var}\{\eta|H_1, k'\} = l\sigma_w^2. \end{aligned} \quad (22)$$

It is clear that $\eta|H_0 \sim \mathcal{N}(\bar{\eta}_0, \sigma_{H_0}^2)$ and $\eta|H_1^{k'} \sim \mathcal{N}(\bar{\eta}_1^{k'}, \sigma_{H_1^{k'}}^2)$.

The authentication is typically claimed if $\eta \geq \varrho$. Hence, the successful authentication probability (or the detection probability) can be simply computed as

$$P_D = Q\left(\frac{\varrho - \bar{\eta}_0}{\sigma_{H_0}}\right), \quad (23)$$

where

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{t^2}{2}\right) dt. \quad (24)$$

With this setting of threshold ϱ , according to the distribution of $\eta|H_1$, a false alarm probability β can be calculated as

$$\beta = E_{k'} \left[Q\left(\frac{\varrho - \bar{\eta}_1^{k'}}{\sigma_{H_1^{k'}}}\right) \right]. \quad (25)$$

We comment here that the successful authentication probability (23) can be directly computed while the false alarm probability is difficult to compute in general, since it should enumerate all possible keys, which is of size 2^n . Furthermore, the above formulation in general depends on the source message s as show by (22). Indeed, one should enumerate

all keys to compute the false alarm probability for any given $s \in \mathcal{S}$. This seems to be an impossible task. Later in Section-V, we, however, show that it is possible to compute it in a closed-form expression thanks to the pseudorandomness of the complexity-theoretic MACs.

IV. SECURITY ANALYSIS

A. Information-Theoretic Bounds

Consider an impersonation attack on the $(r+1)$ th source message s_{r+1} . We adopt the powerful hypothesis-testing formulation originally proposed by Maurer [12]. The receiver knows K and r messages $m_1 = (s_1, \tilde{t}_1), \dots, m_r = (s_r, \tilde{t}_r)$, and sees a message $m_{r+1} = (s_{r+1}, \tilde{t}_{r+1})$ which could either be a correct message sent by Alice (hypothesis H_0) or a fraudulent message inserted by Eve (hypothesis H_1).

For this spoofing attacker of order r , the opponent's strategy for impersonation at time $r+1$ can be described by an arbitrary probability distribution [12] $Q_{M_{r+1}=m_{r+1}|M_1=m_1, \dots, M_r=m_r}$. If the opponent chooses to use $Q_{M_{r+1}=m_{r+1}|M_1=m_1, \dots, M_r=m_r} = P_{M_{r+1}=m_{r+1}|M_1=m_1, \dots, M_r=m_r}$, the cheating probability has the following lower bound.

Theorem 3: Consider the spoofing attack of order r for an ANA-MAC, where the opponent generates an ANA-MAC tag \tilde{T}_{r+1} when she/he observed r ANA-MAC tags (\tilde{T}^r) . We have

$$\mathcal{D}(\alpha, p_r) \leq I\left(K; \tilde{T}_{r+1} | \tilde{T}_1, \dots, \tilde{T}_r\right), \quad (26)$$

and for $\alpha = 0$,

$$p_r \geq 2^{-I(K; \tilde{T}_{r+1} | \tilde{T}_1, \dots, \tilde{T}_r)}. \quad (27)$$

Proof: Consider probability distributions conditioned on the event that $M_1 = m_1, \dots, M_r = m_r$. Under hypothesis H_0 , the pair $U = [M_{r+1}, K]$ (seen by the receiver) is generated according to the probability distribution

$$P_{M_{r+1}, K | M_1=m_1, \dots, M_r=m_r},$$

whereas under hypothesis H_1 , $U = [M_{r+1}, K]$ is generated according to the distribution

$$P_{M_{r+1}=m_{r+1} | M_1=m_1, \dots, M_r=m_r} \cdot P_{K | M_1=m_1, \dots, M_r=m_r}.$$

For ANA-MACs, each message m can be written as $m = (s, \tilde{t})$, where the source message s is carried without secrecy and hence is accessible even for any opponent. Hence, we can employ a more compact form for probability distributions, namely,

$$\begin{aligned} P_{M_{r+1}, K | M_1=m_1, \dots, M_r=m_r} &= P_{\tilde{T}_{r+1}, K | \tilde{T}_1=\tilde{t}_1, \dots, \tilde{T}_r=\tilde{t}_r}, \\ P_{M_{r+1}=m_{r+1} | M_1=m_1, \dots, M_r=m_r} &= P_{\tilde{T}_{r+1} | \tilde{T}_1=\tilde{t}_1, \dots, \tilde{T}_r=\tilde{t}_r}, \\ P_{K | M_1=m_1, \dots, M_r=m_r} &= P_{K | \tilde{T}_1=\tilde{t}_1, \dots, \tilde{T}_r=\tilde{t}_r}. \end{aligned}$$

Let $p_r(\tilde{t}_1, \dots, \tilde{t}_r)$ denote the successful deception probability for a particular observed sequence $\tilde{T}_1 = \tilde{t}_1, \dots, \tilde{T}_r = \tilde{t}_r$, which is the probability of accepting hypothesis H_1 when H_0 is actually true. According to Lemma 1, we have

$$\mathcal{D}(\alpha, p_r(\tilde{t}_1, \dots, \tilde{t}_r)) \leq I\left(K; \tilde{T}_{r+1} | \tilde{T}_1 = \tilde{t}_1, \dots, \tilde{T}_r = \tilde{t}_r\right).$$

Then, it is straightforward to show both (26) and (27) just did in [12]. ■

To gain further insights into the spoofing attack, we can also follow the derivation process employed in [14] [16].

Within the framework of ANA-MACs, we argue that the opponent should do her/his best to generate a clear authentication tag t , instead of a noise-corrupted version \tilde{t} , given that \tilde{t}^r has been observed for a spoofing attack of order r . Indeed, if an illegal tag is generated by the opponent, the introduction of the artificial noise may slightly increase the false acceptance probability. However, this increase is often minor as the false acceptance probability should be less than a small target value in the design of ANA-MACs.

Theorem 4: Consider the spoofing attack of order r for an ANA-MAC, where the opponent generates a clear tag T_{r+1} when she/he observed r ANA-MAC tags (\tilde{T}^r) . We have

$$p_r \geq 2^{-I(K; T_{r+1} | \tilde{T}_1, \dots, \tilde{T}_r)}. \quad (28)$$

Proof: Let $P_r(t | \tilde{t}^r)$ denote the probability that t would be a valid choice for \tilde{T}_{r+1} given that $\tilde{T}^r = \tilde{t}^r$ has been observed. Then,

$$\begin{aligned} P_r(t | \tilde{t}^r) &= \sum_{k \in \mathcal{K}} P(t, k | \tilde{t}^r) = \sum_{k \in \mathcal{K}} P(t | k, \tilde{t}^r) P(k | \tilde{t}^r) \\ &= \sum_{k \in \mathcal{K}(t)} P(k | \tilde{t}^r), \end{aligned} \quad (29)$$

where $\mathcal{K}(t)$ is the set of keys under which t is a valid tag.

Given that \tilde{t}^r has been observed, the opponent's optimum strategy is to substitute the tag t that maximizes $P_r(t | \tilde{t}^r)$. Thus, the success probability given that \tilde{t}^r has been observed in an optimum spoofing attack of order r is

$$\begin{aligned} P_r(\tilde{t}^r) &\triangleq \max_{t \in \mathcal{T}} P_r(t | \tilde{t}^r) \\ &\geq \sum_{t \in \mathcal{T}} P(T_{r+1} = t | \tilde{t}^r) P_r(t | \tilde{t}^r) \\ &= \sum_{t \in \mathcal{T}} \sum_{k \in \mathcal{K}(t)} P(T_{r+1} = t | \tilde{t}^r) P(k | \tilde{t}^r) \\ &= E \left\{ \frac{P(T_{r+1} = t | \tilde{t}^r) P(k | \tilde{t}^r)}{P(T_{r+1} = t, k | \tilde{t}^r)} \right\} \end{aligned} \quad (30)$$

where E is the conditional expectation given that $\tilde{T}^r = \tilde{t}^r$.

By use of Jensen's inequality, we have

$$\begin{aligned} P_r(\tilde{t}^r) &\geq 2^{H(K, T_{r+1} | \tilde{T}^r = \tilde{t}^r) - H(T_{r+1} | \tilde{T}^r = \tilde{t}^r) - H(K | \tilde{T}^r = \tilde{t}^r)} \\ &= 2^{-I(K, T_{r+1} | \tilde{T}^r = \tilde{t}^r)}. \end{aligned} \quad (31)$$

As shown in (29), the conditional cheating probability is determined by the opponent's capability to compute the a posteriori probabilities about the key when she/he observed r tags, namely, $P(k | \tilde{t}^r)$, $\forall k \in \mathcal{K}$. Therefore, it is interesting to develop a coding formulation for the problem of key recovery in ANA-MACs. ■

B. A Coding Formulation for Key Recovery in MACs

Consider the key recovery problem for the spoofing attack of order r , namely, the opponent has accessed r messages $m_1 = (s_1, t_1), \dots, m_r = (s_r, t_r)$ and he/she wants to recover the key. Now, we present a coding formulation for this problem.

In the opponent's view (for key recovery), the generation of possible tags for a given message s can be considered as a deterministic encoding process of

$$\tilde{h}(\cdot, s) : \mathcal{K} \rightarrow \mathcal{T}. \quad (32)$$

Given r source messages s^r , the generation of possible r -tags is with a determinist encoding process of

$$\tilde{h}(\cdot, s^r) \triangleq [\tilde{h}(\cdot, s_1), \dots, \tilde{h}(\cdot, s_r)] : \mathcal{K} \rightarrow \mathcal{T}^r. \quad (33)$$

That means, given r source messages $s^r = (s_1, \dots, s_r) \in \mathcal{S}^r$, it is possible to generate a code $\mathcal{C}(s^r)$, which is comprised of $|\mathcal{K}| = 2^n$ codewords, namely,

$$\mathcal{C}(s^r) = \{c_1(s^r), \dots, c_{2^n}(s^r)\}, \quad (34)$$

where each codeword $c_k(s^r) = (\tilde{h}(k, s_1), \dots, \tilde{h}(k, s_r))$ is indexed by a possible key $k \in \mathcal{K}$.

In what follows, we say $\mathcal{C}(s^r)$ as an r -order MAC, corresponding to the spoofing attack of order r .

Clearly, there are $|\mathcal{K}| = 2^n$ codewords. Suppose that the cardinality of tag space is $|\mathcal{T}| = 2^l$ and each tag is of the equal binary bit length l , the coding rate of $\mathcal{C}(s^r)$ can be defined as

$$R_c(r) = \frac{n}{rl}. \quad (35)$$

Since the source message s is generated according to a finite message set \mathcal{S} , the opponent has to consider an ensemble of codes $\Omega_r(\mathcal{C}) = \{\mathcal{C}(s^r) : s^r \in \mathcal{S}^r\}$, which is all of fixed coding rate $R_c(r)$.

This ensemble of codes $\Omega_r(\mathcal{C})$ is revealed to both Alice and Bob. From a standard cryptographic view, this code ensemble is also revealed to Eve.

In the literature, the size of tag space is often not larger than the size of key, which yields $R_c(1) \geq 1$. For information-theoretic authentication codes, it is always assumed that $R_c(r) > 1$ for some r 's. Otherwise, it is not secure. For the MACs encountered in practice, $R_c(1) \geq 1$. However, $R_c(r) \leq 1$ typically for $r \geq 2$. For example, the 3GPP employs a challenge-response authentication scheme, where the binary length of a tag is $l = 64$, while the binary length of a key is $n = 128$.

According to the value of coding rate $R_c(r)$, it can be formulated as either a source coding problem ($R_c(r) > 1$) or a channel coding problem ($R_c(r) \leq 1$) for key recovery in MACs.

In [17], the link between authentication theory and rate-distortion theory was exploited and the rate-distortion function appears in a powerful lower bound to the probability of an authentication fraud. In essence, Sgarro introduced a binary fraud matrix, which tells which authenticated tags cheat which keys under the given attack: $\chi(k, t) = 1$ iff the authenticated message $m = (s, t)$ cheats the key k . The distortion between k and t can be defined as a complement form of $\chi(k, t)$, namely, $d(k, t) = 1 - \chi(k, t)$. Positive distortion levels $\Delta > 0$ make

sense in a situation when the legal user is recognized as such whenever a “sufficiently high fraction” of the received tags are authenticated.

It should be pointed out that Sgarro in [17] considered only the spoofing attack of order 1 by a careful definition of the fraud matrix. For the spoofing attack of order r , the distortion between k and t^r should be defined as a complement form of $\chi(k, t^r)$, namely,

$$d(k, t^r) = 1 - \chi(k, t^r). \quad (36)$$

The rate-distortion function for the “key source” K with probability distribution π (often uniform) and distortion measure $d(k, t^r)$ is defined as

$$R(\Delta) = \min_{P_{K=\pi, E\{d(K, T^r)\} < \Delta}} I(K; T^r). \quad (37)$$

For any opponent who observed r messages $m_1 = (s_1, t_1), \dots, m_r = (s_r, t_r)$, his/her equivocation about the key is upper bounded by

$$H(K|T^r) \leq H(K) - R(\Delta = 0), \quad (38)$$

where the rate-distortion function $R(\Delta)$ can be numerically computed.

In what follows, we mainly focus on the channel coding formulation, as this will eventually be the case ($R_c(r) \leq 1$) for some r 's when the opponent can access r (different) authentication tags. We point out that even in the case of $r = 1$, it is also possible to construct authentication tags with $l \geq n$ [18]. The expanded size of tag space can be well employed to enhance the receiver operating characteristic (ROC) performance for authentication, which, however, is more vulnerable to potential attackers. This vulnerability can be remedied by the introduction of artificial noise in ANA-MACs.

C. A Decoding Approach for Key Recovery in ANA-MACs

For an ANA-MAC under the spoofing attack of order r , we can characterize it using a quintuple $\{\mathcal{S}, \mathcal{K}, \mathcal{T}, \Omega_r(\mathcal{C}), p(y|x)\}$, where $p(y|x)$ denotes the conditional probability distribution for the artificially-introduced channel between \hat{t} (x) and \tilde{t} (y). In this paper, we always assume a memoryless channel and hence, $p(y|x) = \prod_{i=1}^r p(y_i|x_i)$.

Firstly, we consider the transmission of MACs, in which Eve can directly access the r source messages s^r and their tags

$$y = \tilde{h}(k, s^r) \triangleq [\tilde{h}(k, s_1), \dots, \tilde{h}(k, s_r)].$$

Given s^r and if the encoding rule

$$\tilde{h}(\cdot, s^r) : \mathcal{K} \rightarrow \mathcal{T}^r$$

is an injection ($R_c(r) \leq 1$), Eve can recover the key k by generating a lookup table of size 2^n and searching over this table for finding the key k , which admits $y = \tilde{h}(k, s^r)$.

In the language of coding, it means that the recovery of key can be considered as decoding of the received signal Y to its most likely input $\hat{K}(Y)$. Given r messages m_1, \dots, m_r , if any decoder $\hat{K}(Y)$ is of computational complexity $\mathcal{O}(2^n)$, we

claim that the computational security can be achieved for this message authentication code.

For ensuring computational security, it requires that no any efficient decoding algorithm exists for any code $\mathcal{C}(s^r) \in \Omega_r(\mathcal{C})$. Since the publication of Shannon's original paper in 1948, the search of the codes for achieving the channel capacity has been pursued for several decades. Currently, linear codes and their efficient decoding algorithms have been extensively studied. Therefore, for construction of a good ANA-MAC code, linear code ensembles should be better avoided as their complexity can often be reduced due to the linearity of codes. As various hash functions are nonlinear, this is practically avoided for the construction of MACs based on the keyed hash functions.

To derive an explicit key for the spoofing attack of order r , it is best to use a maximum-likelihood decoder for ANA-MACs if the adversary has unlimited computing power.

Definition 3: Let the binary codeword $c \in \mathcal{C}$, which is further modulated with $x(c)$ and transmitted over the channel $p(y|x)$, the received vector $y \in \mathcal{R}^{rl}$. A maximum-likelihood (ML) decoding algorithm decodes the vector y into a codeword \hat{c} , such that

$$\hat{c} = \max_{c \in \mathcal{C}} p(y|x(c)). \quad (39)$$

Definition 4: (ML recoverable) Given $y \in \mathcal{R}^{rl}$ and s^r , where $y = x + w$ and $x = \bar{c}$, $c = \tilde{h}(k, s^r)$. For an ML decoder $\hat{k}(y)$, we mean that

$$\hat{k} = \max_{k \in \mathcal{K}} p(y|k, s^r). \quad (40)$$

If $P(\hat{k} \neq k) = 0$, we claim that the authentication key is ML recoverable.

We consider a binary-input continuous-output AWGN channel (Bi-AWGN) as encountered in ANA-MACs (8). Its capacity $C_2(\gamma_t)$ is a function of $\gamma_t = 1/2\sigma_w^2$, which can be explicitly expressed as

$$C_2(\gamma_t) = \left[1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-(y-\beta)^2/2} \log_2(1 + e^{-2\beta y}) dy \right],$$

where $\beta = \sqrt{2\gamma_t}$. As the value of γ_t is determined by the introduced artificial noise, one can adjust it in practice for the best possible performance.

The sphere-packing bound of Shannon [19] provides a lower bound on the decoding error probability of block codes transmitted over the Bi-AWGN channel. With a coding approach for MACs, the best possible recovery of key for a potential eavesdropper to attack ANA-MACs is to use an ML decoder, with which, the decoding probability can be lower bounded with the Shannon's 1959 sphere-packing bound.

Lemma 2: (The SP59 Lower Bound [19]) Consider an r -order ANA-MAC code $\{\mathcal{S}^r, \mathcal{T}^r, \mathcal{K}, \Omega_r(\mathcal{C}), p(y|x)\}$. Let a sequence of source messages $s^r \in \mathcal{S}^r$ be sent, and $p(y|x)$ represents a Bi-AWGN channel with the signal-to-noise ratio of γ_t . For any decoder \hat{K} , it is clear that $K \rightarrow \tilde{h}(K, s^r) \rightarrow$

$X \rightarrow Y \rightarrow \hat{K}$ form a Markov process. Let $P_e = P(K \neq \hat{K})$, we have that

$$P_e > P_{SPB}(l, \theta, \gamma_t),$$

where

$$P_{SPB}(l, \theta, \gamma_t) = Q(\sqrt{2l\gamma_t}) + \frac{l-1}{\sqrt{2\pi}} e^{-l\gamma_t} \cdot \int_{\theta}^{\pi/2} \sin(\phi)^{l-2} f_l(\sqrt{2l\gamma_t} \cos(\phi)) d\phi,$$

$$f_l(x) = \frac{1}{2^{\frac{l-1}{2}} \Gamma(\frac{l+1}{2})} \int_0^{\infty} z^{l-1} \exp\left(-\frac{z^2}{2} + zx\right) dz,$$

and $\theta \in [0, \pi]$ satisfies the inequality $2^{-lR} \leq \frac{\Omega_l(\theta)}{\Omega_l(\pi)}$ with

$$\Omega_l(\theta) = \frac{2\pi^{\frac{l-1}{2}}}{\Gamma(\frac{l-1}{2})} \int_0^{\theta} (\sin(\phi))^{l-2} d\phi.$$

The SP59 bound is exponentially increasing with the block length l and the exponent is strictly negative for all $R_c(r) \triangleq \frac{n}{rl} > C_2(\gamma_t)$, it becomes clear that above capacity the minimum probability of error goes to 1 exponentially fast with the block length. Hence, any opponent cannot recover the key explicitly for a properly-designed ANA-MAC, as summarized as follows.

Theorem 5: Given an r -order ANA-MAC $\{\mathcal{S}^r, \mathcal{T}^r, \mathcal{K}, \Omega_r(\mathcal{C}), p(y|x)\}$. With an artificially-introduced Bi-AWGN channel of noise variance $1/2\gamma_t$, we say that this ANA-MAC can resist any explicit key-recovery attack as the recovery of key is with error probability *exponentially* approaching 1 even for any adversary with an unlimited power of computation if $R_c(r) > C_2(\gamma_t)$ when $l \rightarrow \infty$.

In practice, the key is often of short length, typically of length 128. Hence, it seems that Theorem 5 makes no sense. Fortunately, it is well known in coding theory that the decoding error probability can go to 1 even with short block length (*exponentially*) if the signal-to-noise ratio γ_t is sufficiently low, which is implied by the SP59 lower bound. We'll show numerical results later.

As shown in (29), the conditional cheating probability is determined by the opponent's capability to compute the a posteriori probabilities, $P(k|\tilde{t}^r), \forall k \in \mathcal{K}$. Therefore, it is more fundamental to derive a lower bound on the conditional equivocation about the key $H(K|\tilde{T}^r)$ when the opponent has accessed r tags.

Theorem 6: (Lower Bound on the Conditional Equivocation about the Key) For any adversary who has observed r ANA-MAC pairs of $(s_i, \tilde{t}_i), i = 1, \dots, r$, her/his equivocation about the key is lower bounded by

$$H(K|\tilde{T}^r) \geq n \left(1 - R_c(r)^{-1} C_2(\gamma_t)\right), \quad (41)$$

where n is the key length and γ_t is the SNR due to the introduction of artificial noise in ANA-MACs.

Proof: As the mutual information per channel use between the observation at the side of Eve and the shared key $\frac{1}{n}I(K; \tilde{T}^r)$ is upper bounded by the channel capacity, his/her

equivocation about K when Eve observed various realizations of \tilde{T}^r can be lower bounded as

$$\begin{aligned} H(K|\tilde{T}^r) &= H(K) - I(K; \tilde{T}^r), \\ &\geq H(K) - nR_c(r)^{-1} C_2(\gamma_t) \\ &= n \left(1 - R_c(r)^{-1} C_2(\gamma_t)\right). \end{aligned} \quad (42)$$

Let

$$\delta = 1 - R_c(r)^{-1} C_2(\gamma_t), \quad (43)$$

it follows that $H(K|\tilde{T}^r) \geq \delta H(K)$. Hence, the successful probability for an eavesdropper to guess the key is about $2^{-\delta n}$.

Clearly, δ is a lower bound on the normalized equivocation (relative to the entropy of key).

V. A PRAGMATIC APPROACH FOR THE ANALYSIS OF ANA-MACs

For the design of ANA-MACs, one should carefully balance the three performance metrics, namely, the successful authentication probability, the false acceptance probability and the security against spoofing attacks. For simplicity, we focus on the spoofing attack of order-1 and $R_c(1) \leq 1$, in which a channel coding formulation makes sense.

As shown in (29), the conditional cheating probability is determined by the opponent's capability to compute $P(k|\tilde{T} = \tilde{t}), \forall k \in \mathcal{K}$. Hence, a tractable metric for the security against spoofing attacks can be chosen to be the conditional equivocation about the key $H(K|\tilde{T})$.

With a channel coding formulation for MACs, we now show that it is possible to provide a design guideline for balancing the three performance metrics of ANA-MACs. We start with a brief review of some basic concepts of channel coding.

A binary (l, M, d) code represents a binary code with length l , size $M = |\mathcal{C}|$, and minimum Hamming distance d . An equidistant code (of length l and distance d) is a set \mathcal{C} of vectors of length l (called codewords), such that $d(x, y) = d$ for all distinct $x, y \in \mathcal{C}$.

The distance distribution of a binary code \mathcal{C} of length l is defined to be the $(l+1)$ -tuple $(A_0(\mathcal{C}), A_1(\mathcal{C}), \dots, A_l(\mathcal{C}))$, where $A_i(\mathcal{C})$ denotes the mean number of codewords at Hamming distance i from a fixed codeword.

A code \mathcal{C} is said to be distance invariant if the number of codewords at distance i from a fixed codeword only depends on i and not on the particular word chosen.

Given $s \in \mathcal{S}$ and an ANA-MAC, let us first suppose that the underlying MAC $\mathcal{C} \triangleq \mathcal{C}(s)$ is an equidistant code.

A. Equidistant MACs

Lemma 3 (Semakov and Zinoviev [20]): An optimal binary equidistant (l, M, d) code exists if and only if there exists a resolvable balanced incomplete block design (BIBD) with parameters $v = M, k = M/2, \lambda = l - d, r = l$.

For binary equidistant (l, M, d) code, the distance takes the value of

$$d_{opt} = \frac{Ml}{2(M-1)} = \frac{l+1}{2} \quad (44)$$

if d_{opt} is an integer. If d_{opt} is not an integer, i.e. the equidistant code is not optimal, then the code with $d = \lfloor d_{opt} \rfloor$ is called a good equidistant code. Some constructions of good equidistant codes from balanced arrays and nested BIBDs were described in [21].

Suppose now that the underlying MACs employed in ANA-MACs are $(l, 2^n, d)$ equidistant codes. Then, it is possible to compute the three performance metrics.

Firstly, the use of equidistant MACs can facilitate the computation of the successful authentication probability $1 - \alpha$ and the false acceptance probability β . According to the decision metric of (18) and further setting

$$\varrho = \rho l,$$

it follows that

$$\begin{aligned} \alpha &= 1 - P_D = Q\left(\frac{\tilde{\eta}_0 - \varrho}{\sigma_{H_0}}\right) = Q\left(\sqrt{2\gamma_t l}(1 - \rho)\right) \\ &= Q\left(\sqrt{2\gamma_b n}(1 - \rho)\right) \\ &\triangleq Q\left(\sqrt{2\gamma_b G}\right) \end{aligned} \quad (45)$$

where $G \triangleq (1 - \rho)^2$, $\gamma_b \triangleq R_c^{-1}\gamma_t$ and

$$\begin{aligned} \beta &= \Pr(\eta = \tilde{\mu}^T \tilde{t} \geq \rho l) \\ &= Q\left(\sqrt{2\gamma_t l}(2\delta_d - (1 - \rho))\right) \\ &= Q\left(\sqrt{2\gamma_b n}(2\delta_d - (1 - \rho))\right). \end{aligned} \quad (46)$$

For example, Let us consider the special case of $\beta = \alpha$. According to (45) and (46), this means that

$$\delta_{d,l} \triangleq \frac{d}{l} = \sqrt{\frac{G}{n}}. \quad (47)$$

The conditional equivocation about the key $H(K|\tilde{T})$ can be well evaluated by the lower bound proposed in Theorem 6. For equidistant MACs, we can provide a heuristic approximation method to evaluate it, which shows an explicit connection between $H(K|\tilde{T})$ and d .

Theorem 7: For an ANA-MAC with the use of $(l, 2^n, d)$ equidistant codes for the underlying MACs, the conditional equivocation about the key when the opponent has accessed a single tag can be approximated as

$$H(K|\tilde{T}) \approx n - 4 \ln(2)^{-1} R_c \gamma_b d. \quad (48)$$

Proof: Consider that a secret key k shared between Alice and Bob is used to select a MAC codeword t , which is further corrupted by artificial noise to form an ANA-MAC codeword \tilde{t} . When Eve receives \tilde{t} , she can calculate 2^n posteriori probabilities $P(k'|\tilde{t}^n)$, $k' \in \mathcal{K}$, or 2^n log-likelihood ratios

$$l_k(k') = \log \frac{P(k|\tilde{t})}{P(k'|\tilde{t})} = \frac{1}{\sigma_w^2} \sum_{i=1}^n \tilde{t}_i [\bar{t}_i(k) - \bar{t}_i(k')], \quad k' \in \mathcal{K} \quad (49)$$

Clearly, $l_k(k) = 0$. For equidistant MACs with (Hamming) distance d , we have that

$$d_H(t(k), t(k')) = d, \quad \forall k' \neq k. \quad (50)$$

Therefore, it is straightforward to compute the mean and variance of $l_k(k')$ for $\forall k' \neq k$ as

$$\begin{aligned} E\{l_k(k')\} &= \frac{2}{\sigma_w^2} d = 4\gamma_t d, \\ \text{Var}\{l_k(k')\} &= \frac{4}{\sigma_w^4} d \sigma_w^2 = \frac{4}{\sigma_w^2} d = 8\gamma_t d. \end{aligned} \quad (51)$$

In what follows, we denote $l_k(k')$ by $l_{k'}$ for simplicity. The posteriori probabilities can now be written as

$$P(k'|\tilde{t}) = e^{-l_{k'}} P(k|\tilde{t}), \quad (52)$$

or

$$P(k'|\tilde{t}) = \frac{e^{-l_{k'}}}{1 + \sum_{k' \neq k} e^{-l_{k'}}}. \quad (53)$$

$$\begin{aligned} H(K|\tilde{T}) &= E\{H(K|\tilde{T} = t)\} \\ &= E\left\{-\sum_{k' \in \mathcal{K}} P(k'|\tilde{t}) \log_2 P(k'|\tilde{t})\right\} \\ &= E\left\{\log_2 \left(1 + \sum_{i=1}^{2^n-1} e^{-l_i}\right)\right\} \\ &\quad + \ln(2)^{-1} \cdot E\left\{\frac{\sum_{i=1}^{2^n-1} l_i e^{-l_i}}{1 + \sum_{i=1}^{2^n-1} e^{-l_i}}\right\}. \end{aligned}$$

Since 2^n is practically very large (2^{128} for $n = 128$), the sum of 2^n identically-distributed random variables converges to the sum of their mean values, namely,

$$\begin{aligned} \sum_{i=1}^{2^n-1} e^{-l_i} &\approx \sum_{i=1}^{2^n-1} E\{e^{-l_i}\} = 2^n - 1, \\ \sum_{i=1}^{2^n-1} l_i e^{-l_i} &\approx \sum_{i=1}^{2^n-1} E\{l_i e^{-l_i}\} = -4\gamma_t d(2^n - 1). \end{aligned}$$

Hence, one finally have that

$$\begin{aligned} H(K|\tilde{T}) &\approx n - \ln(2)^{-1} \frac{4\gamma_t d(2^n - 1)}{2^n} \\ &\approx n - 4 \ln(2)^{-1} R_c \gamma_b d. \end{aligned}$$

As expected, the conditional equivocation increases when the noise variance increases. For ANA-MACs, one has to consider both the successful authentication probability $1 - \alpha$ and the false acceptance probability β , which, however, is closely related to the noise variance. Therefore, it is of importance to balance these requirements. ■

B. General Case

From coding theory, it is well known that the number of codewords for equidistant codes is very limited, which often results into a very low coding rate.

For a binary code C of length l having s distances, a general result by Delsarte [22] implies that

$$|C| \leq \sum_{i=0}^s \binom{l}{i}. \quad (54)$$

It should be pointed out that the derivations of (46) and (48) require the property of distance invariant for the underlying codes, since we cannot assume the use of a particular key between Alice and Bob. Fortunately, Delsarte told us how to decide if a code is distance invariant.

Lemma 4 (Distance Invariant [22]): Let C be a code for which the number s of distances is at most equal to the dual distance d' . Then C is distance invariant.

Unfortunately, it still remains a challenge for design of such distant-invariant codes in practice.

For ANA-MACs, the complexity-theoretic MACs are employed, which can be seen as random codes, due to their pseudorandomness property. Empirically, we claim that the complexity-theoretic MACs are distance-invariant thanks to their inherent pseudorandomness, as verified by extensive numerical results shown in Section-VI.

For the set of random codes of rate R_c , it is well known that

$$A_d = \binom{l}{d} 2^{-l(1-R_c)}, \quad (55)$$

where A_d denotes the mean number of codewords at Hamming distance d from a fixed codeword.

Then, according to (46) and (56), it is straightforward to show that

$$\beta = \sum_{d>0} \frac{A_d}{2^n} Q\left(\sqrt{2\gamma_b n} (2\delta_d - (1-\rho))\right), \quad (56)$$

while the successful authentication probability (45) remains unchanged.

Theorem 8: For an ANA-MAC with the use of $(l, 2^n)$ MACs, the conditional equivocation about the key when the opponent has accessed a single tag can be approximated as

$$H(K|\tilde{T}) \approx n - 4 \ln(2)^{-1} R_c \gamma_b \cdot \bar{d}. \quad (57)$$

where $\bar{d} = (2^{-n} \sum_d d A_d)$.

Proof: Let $\mathcal{K}(d)$ denote the set of keys with which the generated tags are at Hamming distance d from the tag with k . Clearly, $\bigcup_{d \geq 0} \mathcal{K}(d) = \mathcal{K}$. Hence,

$$\begin{aligned} H(K|\tilde{T}) &= E\{H(K|\tilde{T} = t)\} \\ &= E\left\{\log_2 \left(1 + \sum_{k' \in \mathcal{K}/k} e^{-l'_k}\right)\right\} \\ &\quad + \ln(2)^{-1} E\left\{\frac{\sum_{k' \in \mathcal{K}/k} l'_k e^{-l'_k}}{1 + \sum_{k' \in \mathcal{K}/k} e^{-l'_k}}\right\}, \end{aligned}$$

where

$$E\left\{1 + \sum_{k' \in \mathcal{K}/k} e^{-l'_k}\right\} = 1 + \sum_{d \geq 1} E\left\{\sum_{k' \in \mathcal{K}(d)} e^{-l'_k}\right\} \approx 2^n,$$

and

$$\begin{aligned} E\left\{\sum_{k' \in \mathcal{K}/k} l'_k e^{-l'_k}\right\} &= \sum_{d \geq 1} E\left\{\sum_{k' \in \mathcal{K}(d)} l'_k e^{-l'_k}\right\} \\ &\approx \sum_{d \geq 1} A_d (-4\gamma_b d). \end{aligned}$$

VI. NUMERICAL RESULTS

We consider ANA-MACs, where the underlying MACs are constructed by the Rijndael block cipher [18]. Hence, the underlying MACs in ANA-MACs allow the specification of variants with the block length (l) and key length (n) both ranging from 128 to 256 bits in steps of 32 bits.

A. Empirical Distance Distribution of Complexity-Theoretic MACs

To make sense a channel coding formulation for the Rijndael-cipher based MACs, we use $n = 128$ and $l = 256$. Hence, the coding rate is $R_c = 1/2$.

Given a $s \in \mathcal{S}$ and further fix a $k \in \mathcal{K}$, it is straightforward to generate authentication tags with $\forall k' \in \mathcal{K}/k$, and the Hamming distance between $h(s, k')$ and $h(s, k)$ can be numerically computed.

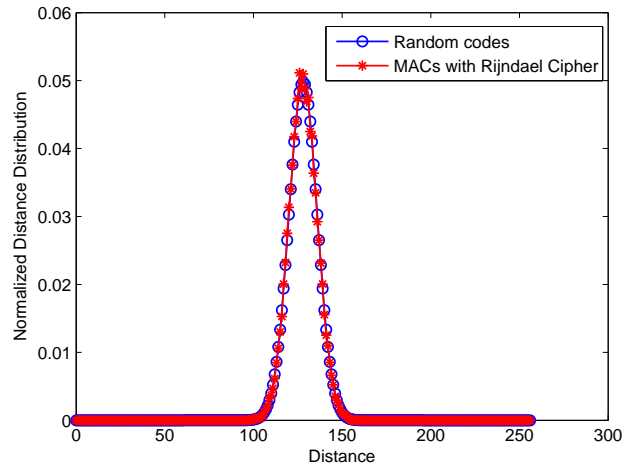


Fig. 1. Distance distribution for random codes and MACs with Rijndael cipher.

This empirical distance distribution is shown in Fig. 1, which coincides well with the random codes of the same coding rate. Extensive numerical results show that this empirical distance distribution keeps unchanged for the use of $\forall s \in \mathcal{S}$ and $\forall k \in \mathcal{K}$. Hence, the distant-invariant property has been empirically confirmed, thanks to the pseudorandomness of the complexity-theoretic MACs.

B. Fundamental Limits on the Key Recovery Attacks

To attack ANA-MACs, an opponent tries to do her/his best to decode the key.

A fundamental limit on the opponent's capability on guessing the key is the conditional equivocation, $H(K|\tilde{T})$, which can be estimated by (57). With a random-code-like distance distribution, it is immediately to see that $\bar{d} = n$. Hence,

$$H(K|\tilde{T}) = n(1 - 4(\ln 2)^{-1} R_c \gamma_b).$$

Numerically, we, however, found that it is often looser than the lower bound of (43). This is because that the law of

large number holds only approximately when random variables being summed are dependent.

Fig. 2 shows the lower bound on the normalized conditional equivocation, as determined by (43). At $E_b/N_0 = -3$ dB, $H(K|\tilde{T}) > 53$. Hence, the successful probability for an opponent with an unlimited power of computation to guess the key is about 2^{-53} .

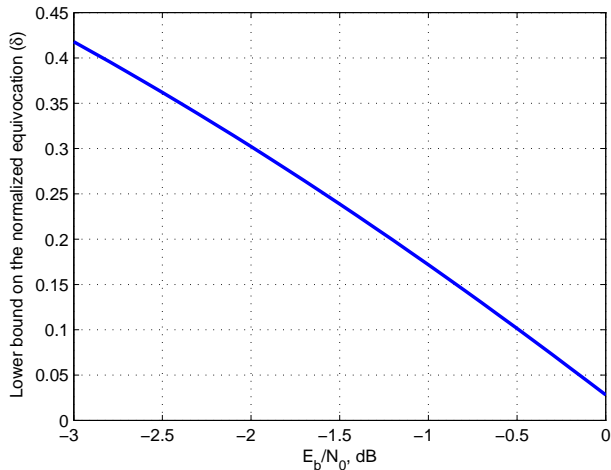


Fig. 2. Lower bound on the normalized equivocation.

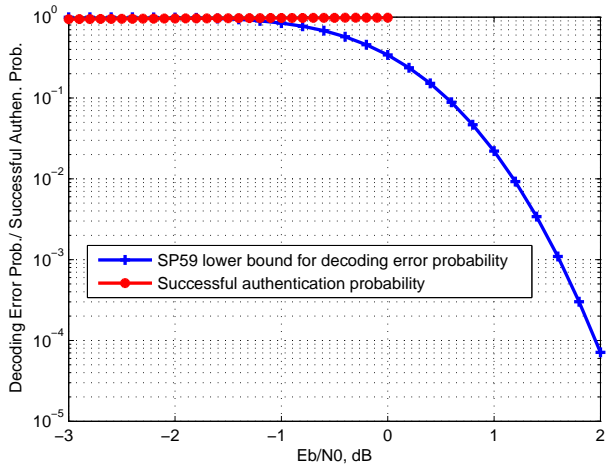


Fig. 3. The SP59 low bound on the decoding error probability and successful authentication probability.

If the opponent choose to decode the key based on her/his observation of a single authentication tag, we can employ the SP59 lower bound for estimating her/his possibility to successfully decode the key. Fig. 3 shows the SP59 bound on the decoding error probability and successful authentication probability for different E_b/N_0 's. As the opponent cannot do better than an ML decoder, the SP59 bound provides an over-estimate of its capability on guessing the key. As shown, the opponent becomes hopeless in guessing the key whenever E_b/N_0 is below about -1 dB, where the decoding error probability is around 1, while almost perfect successful

authentication probability can still be achieved in this low SNR regime.

C. Completeness Error vs. False Acceptance Probability

The completeness error α is defined as the complement of the successful authentication probability, which is closely connected to the normalized threshold value ρ . By the theory of hypothesis testing, the completeness error and the false acceptance probability β is fundamentally balanced with (13).

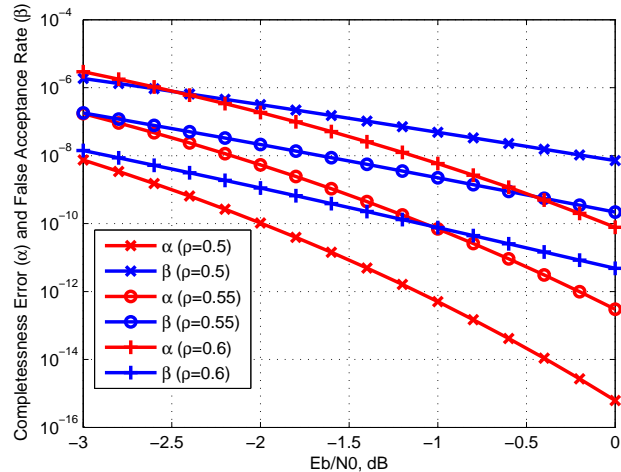


Fig. 4. Completeness error and false acceptance probability versus E_b/N_0 for different thresholds ρ .

To see the fine tradeoff between α and β , we plot them in Fig. 4 for different ρ 's. As the conditional equivocation about the key increases when the SNR decreases, the variance of the artificial noise is essentially determined by the system requirement on the completeness error and false acceptant rate.

D. The Effect of Quantization

To facilitate packet transmission, quantization should be introduced for ANA-MACs. In most cases, 8-bit quantization is often enough for ANA-MACs and no obvious difference can be observed in simulations for both the successful authentication probability and false acceptance probability with or without quantization. For the conditional equivocation about the key, the introduction of quantization can in general increase it due to the data processing inequality and the opponent becomes more difficult for implementing any key-recovery attack.

VII. CONCLUSION

We propose a channel coding approach for the key recovery problem encountered in the spoofing attacks of MACs. With this new approach, the computational security for MACs can be viewed as the requirement of exponential complexity for all possible decoders to succeed.

A new cryptographic primitive, namely, ANA-MACs, is proposed by employing the artificial noise to corrupt the complexity-theoretic MACs. This idea is shown to has some

degree of information-theoretic security. The proposed ANA-MACs are similar to the recently-proposed physical layer authentication schemes, as both are interfered with noise. However, the proposed ANA-MACs come with the artificially-introduced noise, the amount of which can be well controlled to meet various performance metrics. This, however, is not the case for physical layer authentication schemes, where the noise is introduced by the channel.

With the introduction of quantization, the proposed ANA-MACs can be encapsulated in packets and transmitted above the physical layer just like that of the traditional MACs, which contrasts sharply with the existing physical layer authentication schemes. We hope that this research can bridge two closely-related but almost independently developed primitives, namely, information-theoretic authentication codes, and complexity-theoretic MACs.

REFERENCES

- [1] B. Schneier, *Applied Cryptography*. New York: Wiley, 1996.
- [2] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, "Codes which detect deception," *Bell Syst. Tech. J.*, vol. 53, pp. 405–424, 1974.
- [3] G. J. Simmons, "A survey of information authentication," *Proceedings of the IEEE*, vol. 76, pp. 603–620, 1988.
- [4] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, pp. 38–51, Mar. 2008.
- [5] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2571–2579, Jul. 2008.
- [6] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1817–1827, 2013.
- [7] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1791–1802, 2013.
- [8] R. Graveman and K. Fu, "Approximate message authentication codes," *Proc. 3rd Annu. Fedlab Symp. Advanced Telecommunications/Information Distribution*, vol. 1, Feb. 1999.
- [9] L. Xie and G. Arce, "Approximate image message authentication codes," *IEEE Trans. Image Process.*, vol. 2, pp. 242–252, Mar. 2002.
- [10] C. G. Boncelet, "The NTMAC for authentication of noisy messages," *IEEE Trans. Inf. Forensics Security*, vol. 1, pp. 35–42, Mar. 2006.
- [11] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman and Hall/CRC, 2007.
- [12] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, pp. 1350–1356, Jul. 2000.
- [13] M. Walker, "Information-theoretic bounds for authentication schemes," *J. Cryptology*, vol. 2, pp. 131–143, 1990.
- [14] U. Rosenbaum, "A lower bound on authentication after having observed a sequence of messages," *J. Cryptology*, vol. 6, pp. 135–156, 1993.
- [15] J. Alwen, M. Hirt, U. Maurer, A. Patra, and P. Raykov, "Key-indistinguishable message authentication codes," *Lecture Notes in Computer Science*, vol. 8642, pp. 476–493, 2014.
- [16] D. Pei, "Information-theoretic bounds for authentication codes and block designs," *J. Cryptology*, vol. 8, pp. 177–188, 1995.
- [17] A. Sgarro, "Blind coding: Authentication frauds from the point of view of rate-distortion theory," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 4, pp. 133–150, 2001.
- [18] J. Daemen and V. Rijmen, *The design of Rijndael: AES — the Advanced Encryption Standard*. Springer-Verlag, 2002.
- [19] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel," *Bell Syst. Tech. J.*, vol. 38, pp. 611–656, May 1959.
- [20] N. V. Semakov and V. A. Zinoviev, "Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs," *Problemi Peredatchi Informatzii*, vol. 4, pp. 3–10, 1968.
- [21] K. Sinha, Z. Wang, and D. Wu, "Good equidistant codes constructed from certain combinatorial designs," *Discrete Math.*, vol. 308, pp. 4205–4211, 2008.
- [22] P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance," *Inform. and Control*, vol. 23, pp. 407–438, 1973.