Geração de *Tags* para Autenticação em Camada Física Utilizando Sequências Caóticas Discretizadas

Davi Moreno, Daniel P. B. Chaves, and Cecilio Pimentel

***Resumo*— Neste trabalho, analisamos um método de autenticação na camada física que utiliza um código de autenticação de mensagem, chamado de *tag*, que é transmitido juntamente com uma mensagem para garantir uma autenticação robusta. Enquanto estudos anteriores utilizam prioritariamente funções de *hash* criptográficas para geração de *tag*, nosso sistema utiliza mapas caóticos unidimensionais discretos para gerá-los. Por meio de uma abordagem baseada em teoria da informação, quantificamos o nível mínimo de segurança proporcionado pelo sistema proposto, o qual é não nulo mesmo em ambientes sem ruído. Uma análise da segurança do sistema é feita para o caso em que um atacante intercepta vários pares de mensagem e *tags* legítimos.**

***Palavras-Chave*— autenticação em camada física, geração de *tags*, mapas caóticos, segurança.**

***Abstract*— In this work, we analyze a physical layer authentication method that employs a message authentication code, called tag, which is transmitted along with a message to ensure robust authentication. While previous studies primarily use cryptographic hash functions for tag generation, our system utilizes discrete one-dimensional chaotic maps to generate them. Through an information theory-based approach, we quantify the minimum level of security provided by the proposed system, which is non-zero even in noiseless environments. A security analysis of the system is conducted for the scenario where an attacker intercepts multiple legitimate message-tag pairs.**

***Keywords*— physical layer authentication, tag generation, chaotic maps, security.**

I. Introdução

A autenticação de mensagem, que confirma que uma mensagem recebida vem do seu remetente declarado, é relevante para sistemas de comunicação seguros. Essas operações são realizadas em várias camadas da rede. Especificamente, um esquema de autenticação de camada física (PLA, *physical layer authentication*) permite que os nós de uma rede rejeitem prontamente mensagens fraudulentas e reduz a complexidade dos protocolos de autenticação em camadas superiores.

Duas abordagens para esquemas PLA constituem mecanismos ativos e passivos. No PLA ativo, uma chave secreta compartilhada entre os usuários legítimos é utilizada para gerar um sinal, denominado *tag*, que é incorporado de alguma forma às mensagens [1]–[3]. O receptor utiliza técnicas de detecção da *tag* para verificar a autenticidade da mesma, e assim autenticar o remetente da mensagem. A métrica de segurança considerada neste caso é a incerteza em relação a chave secreta, dado observações ruidosas de *tags* interceptadas. A análise do PLA baseado em *tags* foi conduzida para cenários de Internet das Coisas [4], veículos aéreos não tripulados (UAV) [5], superfícies inteligentes reconfiguráveis [6]. Já no PLA passivo, a singularidade da resposta ao impulso em canais com desvanecimento multipercurso entre os usuários legítimos [7], [8] é explorada. Algumas limitações práticas de esquemas de PLA passivo são discutidas em [1].

No que diz respeito ao processo de geração de *tags* no PLA ativo, a maioria dos trabalhos da literatura utiliza uma função *hash*, na qual as entradas são a mensagem e uma chave secreta [1]–[4], [9], [10]. Este trabalho propõe um novo método para gerar as *tags* utilizando sequências caóticas discretizadas. Além disso, quantifica-se a segurança incondicional do sistema proposto por meio de uma abordagem de teoria da informação. Ao contrário dos esquemas de PLA baseados em funções de *hash*, o esquema proposto fornece segurança incondicional mesmo em um ambiente sem ruído. As contribuições deste trabalho são as seguintes:

- Utilizamos sequências discretizadas geradas por mapas caóticos unidimensionais como *tags* de autenticação para sistemas PLA.
- Demonstramos que o esquema proposto oferece segurança do ponto de vista da teoria da informação, mesmo em um canal sem ruído. Isso ocorre devido à estrutura imposta às órbitas caóticas por meio do ocultamento adequado de pontos da mesma. Portanto, o esquema proporciona uma segurança incondicional finita e positiva (dependendo do número de pontos ocultados) em canais sem ruído. Como consequência, há uma perda drástica de informação dos valores iniciais do mapa à medida que o mapa caótico itera, e isso é usado para ocultar a chave secreta das *tags* geradas.
- Analisamos o impacto sobre o sistema proposto quando um atacante intercepta vários pares de mensagem e *tags* legítimos, mostrando o quanto de informação o mesmo possui sobre a chave legítima dado os pares observados.

O restante trabalho está organizado da seguinte forma. Uma revisão de esquemas PLA usando *tags* é abordada na Seção II. O sistema proposto é descrito na Seção III. A segurança incondicional da proposta também é tratada nesta seção. A Seção IV trata do problemas das múltiplas observações e resultados sobre este tema são apresentados na Seção V. A Seção VI traz as conclusões do trabalho.

II. Autenticação em Camada Física

Considera-se o cenário clássico em que três usuários compartilham o mesmo canal inseguro. Alice e Bob são os usuários

Davi Moreno, Daniel Chaves e Cecilio Pimentel, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife-PE, e-mails: {davi.moreno, daniel.chaves, cecilio.pimentel}@ufpe.br; Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco (FACEPE), Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

legítimos, ou seja, eles utilizam um protocolo de PLA e compartilham uma chave secreta $\mathbf{k}$. Alice envia a Bob uma mensagem $\mathbf{s}$ juntamente com uma *tag* $\mathbf{t}$, que normalmente é gerada usando $\mathbf{s}$ e $\mathbf{k}$. Supõe-se que Bob decodifica $\mathbf{s}$ sem erros. Já que Bob também tem conhecimento da chave secreta $\mathbf{k}$, ele pode obter localmente, a partir de $\mathbf{s}$ e $\mathbf{k}$, a *tag* legítima. Bob então realiza um teste de detecção para verificar se a *tag* legítima está presente no sinal recebido. Se Bob conclui que a *tag* legítima está presente no sinal recebido, ele aceita a mensagem; caso contrário, a mensagem é rejeitada. Eva é uma usuária maliciosa que tem conhecimento de todos os detalhes do protocolo de autenticação, exceto a chave secreta. Considera-se que ela é um adversário ativo, sendo capaz de escutar as mensagens enviadas por Alice e enviar pacotes maliciosos para Bob. Esse sistema é ilustrado na Fig. 1.

A. Equivocação da Chave

Uma das métricas mais comuns para mensurar um sistema de geração de *tags* é a equivocação da chave. Para definir a equivocação da chave, utiliza-se a entropia $H(\cdot)$ definida como o valor esperado de $-\log_2 \Pr(X)$, em que X é uma variável aleatória. Ao definir a entropia utilizando o logaritmo em base 2, a medida da entropia é feita em bits.

Seja $(\mathbf{s}, \mathbf{t})$ um par observado pela atacante Eva. Suponha que a chave $\mathbf{k}$ é a chave legítima utilizada por Alice para transmitir os pares para Bob. A equivocação da chave $\mathbf{k}$ é a medida de incerteza que Eva tem sobre a chave $\mathbf{k}$, dado que ela intercepta o par $(\mathbf{s}, \mathbf{t})$. Essa medida é dada por $H(\mathbf{k} \mid \mathbf{s}, \mathbf{t})$.

B. Sistema Clássico de Geração de Tags

O sistema descrito nesta seção é o que será chamado de clássico, e está em diversos artigos da literatura [1]–[4], [9], [10]. No sistema clássico, a *tag* é gerada utilizando uma função $g(\cdot)$ unidirecional difícil de inverter:

$$g(\mathbf{s}, \mathbf{k}) = \mathbf{t}. \tag{1}$$

É comum escolher a função $g(\cdot)$ como uma função *hash*. Os conjuntos de chaves, mensagens e *tags* possíveis são denotados por $\mathcal{K}$, $\mathcal{S}$, e $\mathcal{T}$, respectivamente. Quando $|\mathcal{K}| \leq |\mathcal{T}|$, assume-se que, fixada a mensagem $\mathbf{s}$, a função $g(\cdot)$ mapeia cada chave em uma *tag* distinta. Desta maneira, como assume-se que a atacante Eva recupera $\mathbf{s}$ sem erros e também tem acesso ao conjunto $\mathcal{K}$, ela pode enumerar todas as *tags* possíveis:

$$\mathbf{t}_i = g(\mathbf{s}, \mathbf{k}_i), \quad \forall\, \mathbf{k}_i \in \mathcal{K}, \tag{2}$$

e, consequentemente, se Eva consegue obter a *tag* transmitida sem ruído, um ataque de força bruta sobre a chave tem garantia de sucesso, assumindo que a atacante tem um poder computacional ilimitado. Portanto, no caso sem ruído, tem-se $H(\mathbf{k} \mid \mathbf{s}, \mathbf{t}) = 0$. A segurança deste esquema está unicamente baseada no ruído sobre a *tag* que é inserida pelo canal durante a transmissão.

III. Sistema Proposto de Geração de *Tags*

A. Definição de mapa caótico unidimensional

Um mapa caótico unidimensional é caracterizado por um sistema dinâmico com comportamento caótico obtido pela iteração sobre uma função não invertível e não linear adequada $f : A \to A$, de forma que:

$$x[n] = f(x[n-1]), \quad n = 1, 2, \ldots \tag{3}$$

O valor $x[0]$ é a condição inicial do mapa. Chamamos de $\mathcal{O}$ a órbita de $x[0]$ sobre $f(\cdot)$, representada pela série temporal $x[n]_{n=0}^{\infty}$:

$$\mathcal{O} = [x[0], f(x[0]), f^2(x[0]) \cdots] = [x[0], x[1], x[2] \cdots] \tag{4}$$

em que $f^n(x) = f^{n-1}(f(x))$.

B. Mapas com pré-imagens binárias constantes

Uma classe de mapas caóticos de interesse neste trabalho são os mapas com pré-imagens binárias constantes. Seja $f(\cdot)$ a função que representa um mapa caótico unidimensional. Define-se a i-ésima pré-imagem do ponto y como o conjunto $\mathcal{S}_i(y) = \{x \mid f^i(x) = y\}$. Os mapas com pré-imagens binárias constantes são aqueles que obedecem a $|\mathcal{S}_i(y)| = 2^i, i \geq 0$, para todos os valores de y pertencentes à imagem de $f(\cdot)$, exceto por possivelmente um conjunto finito de pontos. Existem vários mapas que possuem essa propriedade, como o mapa da tangente hiperbólica [11], o mapa tenda [12].

C. Discretização das órbitas do mapa caótico

Considere um mapa caótico com pré-imagens binárias constantes representado pela função $f(\cdot)$, como o definido na Subseção III-B. Para um y pertencente ao domínio A do mapa, considere os conjuntos $\mathcal{S}_1(y), \mathcal{S}_2(y), \ldots, \mathcal{S}_K(y)$, em que $\mathcal{S}_i(y)$ contém as i-ésimas pré-imagens de y no mapa, com $|S_i(y)| = 2^i$. A forma como estes subconjuntos iteram sobre o mapa pode ser representada como uma árvore binária, pois vão existir sempre um par de elementos presentes no conjunto $\mathcal{S}_{i+1}(y)$ que mapeiam em um mesmo elemento do conjunto $\mathcal{S}_i(y)$.

Para algum valor de y, define-se o conjunto $\mathcal{X}_i$ como $\mathcal{X}_i = \mathcal{S}_{K-i}(y), 0 \leq i < K$, e, portanto, como $|\mathcal{X}_i| = 2^{K-i}$, pode-se reescrever $\mathcal{X}_i$ enumerando seus elementos:

$$\mathcal{X}_i = \{x_i^0, x_i^1, \ldots, x_i^{2^{K-i}-1}\}, \quad 0 \leq i < K. \tag{5}$$

O conjunto $\mathcal{X}_0$ é chamado de conjunto de condições iniciais do mapa. Uma condição inicial $x[0] \in \mathcal{X}_0$ possui uma órbita $\mathcal{O}$ sobre o mapa definida em (4). Existem $|\mathcal{X}_0| = 2^K$ condições iniciais, e como a iteração sobre as mesmas pode ser vista no formato de uma árvore binária, sabe-se que as órbitas associadas a estas condições iniciais distintas encontram-se em algum momento até a iteração K do mapa. A órbita discretizada $\mathcal{O}_d$ de $x[0]$ é obtida pela discretização dos elementos de $\mathcal{O}$ por uma função de discretização $d(\cdot)$, de forma que:

$$\mathcal{O}_d = \begin{bmatrix} d(x[0]) & d(x[1]) & \cdots & d(x[K-1]) \end{bmatrix}. \tag{6}$$

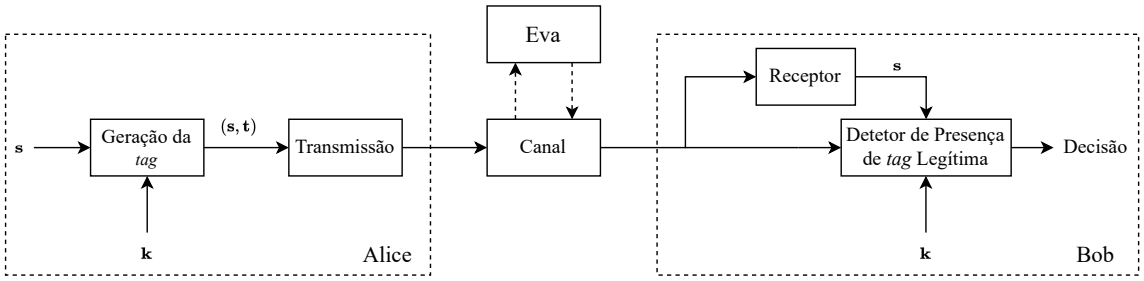

Fig. 1. Sistema genérico de PLA utilizando *tags*.

A função de discretização $d : A \to \{-1, +1\}$ mapeia pontos do domínio do mapa nos valores -1 ou $+1$. Assume-se também que $d(\cdot)$ é uma função com a propriedade:

$$d(x_i^m) \neq d(x_i^n) \text{ se } f(x_i^m) = f(x_i^n), \tag{7}$$

ou seja, se dois elementos x_i^m e x_i^n são mapeados no mesmo ponto pelo mapa, seus valores de discretização são distintos. A função de discretização garante que órbitas discretizadas com condições iniciais distintas são distintas, pois na iteração anterior ao encontro das órbitas elas possuem valores diferentes de discretização, como descrito em (7). Consequentemente, cada condição inicial gera uma órbita discretizada distinta $\mathcal{O}_d$ pertencente no conjunto $\{-1, +1\}^K$.

D. Geração da tag a partir das órbitas discretizadas

A geração da *tag* depende da mensagem $\mathbf{s}$ transmitida e da chave $\mathbf{k}$ compartilhada entre os usuários legítimos. Os valores $\mathbf{s}$ e $\mathbf{k}$ são mapeados nas condições iniciais $\mathcal{X}_0$ do mapa utilizando:

$$M(\mathbf{k} \oplus \mathbf{s}) = x[0], \quad x[0] \in \mathcal{X}_0, \tag{8}$$

em que $M(\cdot)$ é uma função bijetiva e $\oplus$ é a operação OU exclusivo entre os vetores binários $\mathbf{s}$ e $\mathbf{k}$. A *tag* $\mathbf{t}$ é obtida desconsiderando os σ primeiros valores da órbita discretizada $\mathcal{O}_d$ associada a $x[0]$, e considerando os L valores seguintes, sendo definida como:

$$\mathbf{t} = \begin{bmatrix} d(x[\sigma]) & d(x[\sigma+1]) & \cdots & d(x[\sigma+L-1]) \end{bmatrix}. \tag{9}$$

A *tag* é então uma fatia de comprimento L da órbita discretizada $\mathcal{O}_d$. Como cada uma das 2^K condições iniciais possui uma órbita discretizada distinta $\mathcal{O}_d \in \{-1, +1\}^K$, existem 2^{K-L} condições iniciais que geram a mesma *tag*. O conjunto de *tags* possíveis é $\mathcal{T} = \{-1, +1\}^L$. Como são feitas $\sigma+L-1$ iterações, e o número máximo de iterações antes de todas as órbitas convergirem é $K-1$, tem-se a restrição:

$$\sigma + L \leq K. \tag{10}$$

O procedimento de gerar uma *tag* a partir de uma condição inicial pode ser descrito em termos da função $T : \mathcal{X}_0 \to \mathcal{T}$, de forma que:

$$T(x[0]) = \begin{bmatrix} d(x[\sigma]) & d(x[\sigma+1]) & \cdots & d(x[\sigma+L-1]) \end{bmatrix}, \tag{11}$$

em que $x[0] \in \mathcal{X}_0$. A obtenção de uma *tag* a partir dos valores de $\mathbf{s}$ e $\mathbf{k}$ pode então ser representada em termos da composição $F = T \circ M$, e, portanto, o processo de geração da *tag* associada para um par $\mathbf{s}$ e $\mathbf{k}$ é descrita como:

$$F(\mathbf{k} \oplus \mathbf{s}) = T(M(\mathbf{k} \oplus \mathbf{s})) = \mathbf{t}. \tag{12}$$

E. Equivocação incondicional da chave

Como visto na Subseção II-A, a equivocação da chave $H(\mathbf{k} \mid \mathbf{s}, \mathbf{t})$ mede a quantidade de informação que a atacante Eva tem sobre a chave secreta $\mathbf{k}$, dado que ela interceptou um par legítimo $(\mathbf{s}, \mathbf{t})$ [13]. Para o cálculo deste valor, considere inicialmente $H(x[0], \mathbf{k} \mid \mathbf{s}, \mathbf{t})$ e a regra da cadeia para a entropia. Pode-se reescrever:

$$\begin{aligned} H(x[0], \mathbf{k} \mid \mathbf{s}, \mathbf{t}) &= H(x[0] \mid \mathbf{k}, \mathbf{s}, \mathbf{t}) + H(\mathbf{k} \mid \mathbf{s}, \mathbf{t}) \\ &= H(\mathbf{k} \mid x[0], \mathbf{s}, \mathbf{t}) + H(x[0] \mid \mathbf{s}, \mathbf{t}). \end{aligned} \tag{13}$$

Como $M(\cdot)$ em (8) é injetiva, então $H(x[0] \mid \mathbf{k}, \mathbf{s}, \mathbf{t}) = 0$ e $H(\mathbf{k} \mid x[0], \mathbf{s}, \mathbf{t}) = 0$, portanto:

$$H(\mathbf{k} \mid \mathbf{s}, \mathbf{t}) = H(x[0] \mid \mathbf{s}, \mathbf{t}). \tag{14}$$

Analogamente, considera-se agora $H(x[0], \mathbf{s} \mid \mathbf{t})$:

$$H(x[0], \mathbf{s} \mid \mathbf{t}) = H(x[0] \mid \mathbf{s}, \mathbf{t}) + H(\mathbf{s} \mid \mathbf{t}) \tag{15}$$

$$= H(\mathbf{s} \mid x[0], \mathbf{t}) + H(x[0] \mid \mathbf{t}). \tag{16}$$

Como $\mathbf{s}$ e $\mathbf{k}$ são sequências binárias de mesmo comprimento e a distribuição de probabilidade de $\mathbf{k}$ é uniforme, então $H(\mathbf{k}) \geq H(\mathbf{s})$. Tendo em vista (8), isto implica que para qualquer par $x[0]$ e $\mathbf{s}$ existe uma chave $\mathbf{k}'$, tal que, $x[0] = M(\mathbf{s} \oplus \mathbf{k}')$. Consequentemente, se $\mathbf{k}$ é desconhecida, o conhecimento de $x[0]$ não dá nenhuma informação sobre $\mathbf{s}$. Como $\mathbf{s}$ é independente do $x[0]$ e de $\mathbf{t}$, tem-se que $H(\mathbf{s}|\mathbf{t}) = H(\mathbf{s})$ e $H(\mathbf{s} \mid x[0], \mathbf{t}) = H(\mathbf{s})$. Então, $H(x[0] \mid \mathbf{s}, \mathbf{t}) = H(x[0] \mid \mathbf{t})$, que em conjunto com (14) permite obter a seguinte igualdade:

$$H(\mathbf{k} \mid \mathbf{s}, \mathbf{t}) = H(x[0] \mid \mathbf{t}). \tag{17}$$

Para calcular a equivocação de $x[0]$ em relação a $\mathbf{t}$, considere a partição do espaço de condições iniciais $\mathcal{X}_0$ em 2^L conjuntos $\mathcal{X}_0^i$, de forma que:

$$\mathcal{X}_0 = \mathcal{X}_0^0 \cup \mathcal{X}_0^1 \cup \cdots \cup \mathcal{X}_0^{2^L-1}, \quad \mathcal{X}_0^i \cap \mathcal{X}_0^j = \emptyset, \forall i \neq j \tag{18}$$

e

$$\mathcal{X}_0^i = \{x[0] \mid T(x[0]) = \mathbf{t}_i, x[0] \in \mathcal{X}_0\},\ \mathbf{t}_i \in \mathcal{T}, \quad 0 \leq i < 2^L \tag{19}$$

ou seja, $\mathcal{X}_0^i$ é formado por todas as condições iniciais que geram a *tag* $\mathbf{t}_i$, logo, $|\mathcal{X}_0^i| = 2^{K-L}$. Em virtude da distribuição

de $\mathbf{k}$ ser uniforme, a expressão (8) garante que a distribuição de $x[0]$ também é uniforme. Como o número de condições iniciais que gera cada *tag* também é constante, a distribuição de $\mathbf{t}$ também é uniforme. A probabilidade condicional de uma condição inicial $x[0]$ qualquer gerar uma *tag* $\mathbf{t}_i$ é dada por:

$$\Pr(x[0] \mid \mathbf{t}_i) = \begin{cases} \frac{1}{2^{K-L}} & , \quad \text{se } x[0] \in \mathcal{X}_0^i \\ 0 & , \quad \text{c.c.} \end{cases} \tag{20}$$

Pode-se então calcular a equivocação $H(x[0] \mid \mathbf{t})$:

$$\begin{aligned} H(x[0] \mid \mathbf{t}) &= \mathbb{E}[-\log_2 \Pr(x[0] \mid \mathbf{t})] \\ &= -\sum_{i=0}^{2^L-1} \Pr(\mathbf{t}_i) \sum_{j=0}^{2^K-1} \Pr(x_0^j|\mathbf{t}_i) \log_2 \Pr(x_0^j|\mathbf{t}_i) \\ &= K - L, \end{aligned} \tag{21}$$

em que $\mathbb{E}[\cdot]$ é o operador valor esperado. Conclui-se a partir de (17) que a equivocação da chave para o método de geração da *tag* utilizando sequências caóticas discretizadas é dada por:

$$H(\mathbf{k} \mid \mathbf{s}, \mathbf{t}) = K - L, \tag{22}$$

e assim, uma segurança incondicional positiva é garantida por este método de geração da *tag*. Já que L é positivo e obedece (10), pode-se escolher L no intervalo $1 \leq L \leq K - \sigma$.

IV. O Problema das Múltiplas Observações

A. Descrição do Problema

Suponha que uma chave $\mathbf{k}$ é utilizada para transmitir N mensagens $\mathbf{s}^1, \mathbf{s}^2, \ldots, \mathbf{s}^N$. Cada $\mathbf{s}^i$ pode assumir algum valor de $\mathcal{S}$ com igual probabilidade. A cada mensagem $\mathbf{s}^i$ transmitida, existe a *tag* $\mathbf{t}^i = F(\mathbf{k} \oplus \mathbf{s}^i)$ associada a essa mensagem. Já que existem 2^{K-L} valores distintos $\mathbf{k} \oplus \mathbf{s}^i$ que são mapeados pela função $F(\cdot)$ em $\mathbf{t}^i$, então vão existir 2^{K-L} chaves distintas que podem ter sido utilizadas para transmitir um par $(\mathbf{s}^i, \mathbf{t}^i)$. Define-se o conjunto de chaves que podem ter sido utilizadas para transmitir o par $(\mathbf{s}^i, \mathbf{t}^i)$ como:

$$\mathcal{K}^i = \{\mathbf{k}_j \mid F(\mathbf{k}_j \oplus \mathbf{s}^i) = \mathbf{t}^i, \mathbf{k}_j \in \mathcal{K}\}, \tag{23}$$

em que $|\mathcal{K}^i| = 2^{K-L}$. Para cada uma das N mensagens transmitidas com a chave $\mathbf{k}$, pode-se construir um subconjunto como este a partir do par $(\mathbf{s}^i, \mathbf{t}^i)$ transmitido. Têm-se então os subconjuntos $\mathcal{K}^1, \mathcal{K}^2, \ldots, \mathcal{K}^N$, cada um associado a um dos N pares enviados. Como a chave $\mathbf{k}$ foi a chave utilizada para transmitir todos os N pares, então obrigatoriamente tem-se que $\mathbf{k} \in \mathcal{K}^1 \cap \mathcal{K}^2 \cap \cdots \cap \mathcal{K}^N$. O problema das múltiplas observações consiste em calcular o conhecimento que a atacante Eva tem sobre a chave $\mathbf{k}$, supondo que ela tem acesso aos N pares transmitidos, todos utilizando a chave $\mathbf{k}$. Quando se considera apenas uma observação, a atacante pode construir $\mathcal{K}^1$, e a chave legítima $\mathbf{k}$ é uma dentre as $|\mathcal{K}^1| = 2^{K-L}$ chaves deste conjunto. Para N observações, a atacante pode construir os N subconjuntos $\mathcal{K}^1, \mathcal{K}^2, \ldots, \mathcal{K}^N$, e a chave legítima será uma dentre as $|\mathcal{K}^1 \cap \mathcal{K}^2 \cap \cdots \cap \mathcal{K}^N|$ chaves possíveis. Uma forma de estimar a informação que a atacante tem sobre a chave legítima $\mathbf{k}$ é então calculando:

$$\mathbb{E}[|\mathcal{K}^1 \cap \mathcal{K}^2 \cap \cdots \cap \mathcal{K}^N|]. \tag{24}$$

B. Mapeamento aleatório

Inicialmente considera-se o caso em que $F(\cdot)$ representa algum mapeamento aleatório. Assume-se que os pares $(\mathbf{s}^i, \mathbf{t}^i)$ são transmitidos utilizando a chave legítima $\mathbf{k}$. As mensagens $\mathbf{s}^i$ são escolhidas de maneira aleatória sobre o conjunto $\mathcal{S}$, e consequentemente as *tags* $\mathbf{t}^i$ também são aleatoriamente escolhidas sobre $\mathcal{T}$. A probabilidade de uma chave $\mathbf{k}_j$ utilizada na transmissão do par $(\mathbf{s}^1, \mathbf{t}^1)$ pertencer ao conjunto $\mathcal{K}^1$ é:

$$\begin{aligned} \Pr(\mathbf{k}_j \in \mathcal{K}^1) &= \Pr(F(\mathbf{k}_j \oplus \mathbf{s}^1) = F(\mathbf{k} \oplus \mathbf{s}^1)) \\ &= \Pr(F(\mathbf{k}_j \oplus \mathbf{s}^1) = \mathbf{t}^1). \end{aligned} \tag{25}$$

Quando $\mathbf{k}_j = \mathbf{k}$ (a chave legítima), a probabilidade é igual a 1. Como $F(\cdot)$ representa uma permutação aleatória, quando $\mathbf{k}_j \neq \mathbf{k}$ a probabilidade pode ser calculada como:

$$\begin{aligned} \Pr(\mathbf{k}_j \in \mathcal{K}^1) &= \frac{|\{\mathbf{k}_j \mid F(\mathbf{k}_j \oplus \mathbf{s}^1) = \mathbf{t}^1, \mathbf{k}_j \in \mathcal{K} - \{\mathbf{k}\}\}|}{|\mathcal{K} - \{\mathbf{k}\}|} \\ &= \frac{2^{K-L} - 1}{2^K - 1}, \quad \forall \mathbf{k}_j \neq \mathbf{k}. \end{aligned} \tag{26}$$

Tem-se então que:

$$\Pr(\mathbf{k}_j \in \mathcal{K}^1) = \begin{cases} 1, & \text{se } \mathbf{k}_j = \mathbf{k} \\ \frac{2^{K-L}-1}{2^K-1}, & \text{se } \mathbf{k}_j \neq \mathbf{k}. \end{cases} \tag{27}$$

Ao considerar a transmissão de um outro par $(\mathbf{s}^2, \mathbf{t}^2)$, tem-se a probabilidade de uma chave $\mathbf{k}_j$ pertencer a interseção $\mathcal{K}^1 \cap \mathcal{K}^2$. Como as mensagens $\mathbf{s}^1$ e $\mathbf{s}^2$ são variáveis independentes e uniformemente distribuídas sobre $\mathcal{S}$, é possível escrever que $\Pr(\mathbf{k}_j \in \mathcal{K}^1 \cap \mathcal{K}^2) = \Pr(\mathbf{k}_j \in \mathcal{K}^1) \Pr(\mathbf{k}_j \in \mathcal{K}^2)$. De forma semelhante, pode-se estender o raciocínio para a transmissão de N pares, de forma que $\Pr(\mathbf{k}_j \in \mathcal{K}^1 \cap \mathcal{K}^2 \cap \cdots \cap \mathcal{K}^N) = \Pr(\mathbf{k}_j \in \mathcal{K}^1) \Pr(\mathbf{k}_j \in \mathcal{K}^2) \cdots \Pr(\mathbf{k}_j \in \mathcal{K}^N)$, e assim:

$$\Pr(\mathbf{k}_j \in \mathcal{K}^1 \cap \mathcal{K}^2 \cap \cdots \cap \mathcal{K}^N) = \begin{cases} 1, & \text{se } \mathbf{k}_j = \mathbf{k} \\ \left(\frac{2^{K-L}-1}{2^K-1}\right)^N, & \text{se } \mathbf{k}_j \neq \mathbf{k}. \end{cases} \tag{28}$$

Pode-se agora definir o evento A_j como:

$$A_j = \begin{cases} 1, & \text{se } \mathbf{k}_j \in \mathcal{K}^1 \cap \mathcal{K}^2 \cap \cdots \cap \mathcal{K}^N \\ 0, & \text{caso contrário.} \end{cases} \tag{29}$$

O cálculo de (24) pode então ser feito através de:

$$\begin{aligned} \mathbb{E}[|\mathcal{K}^1 \cap \mathcal{K}^2 \cap \cdots \cap \mathcal{K}^N|] &= \mathbb{E}\left[\sum_j A_j\right] \\ &= 1 + (2^K - 1)\left(\frac{2^{K-L} - 1}{2^K - 1}\right)^N. \end{aligned} \tag{30}$$

Se forem escolhidos valores de K e L tal que $2^{K-L} >> 1$, pode-se aproximar a expressão acima por:

$$\mathbb{E}[|\mathcal{K}^1 \cap \mathcal{K}^2 \cap \cdots \cap \mathcal{K}^N|] \approx 1 + 2^{K-NL}. \tag{31}$$

Conclui-se então que para um mapeamento $F(\cdot)$ aleatório, a queda do número de chaves possíveis decai rapidamente por um fator de 2^L a cada nova transmissão.

V. Resultados

Para exemplificar como o resultado obtido em (31) se aplica a um mapeamento específico, considere a função $F = T \circ M$ como definida em (12). Considere o particionamento do conjunto de condições iniciais $\mathcal{X}_0$ em 2^L subconjuntos $\mathcal{X}^i$ de tamanho 2^{K-L} tal que:

$$\begin{aligned}\mathcal{X}_0^i &= \{x_0^{i2^{K-L}}, x_0^{i2^{K-L}+1}, \ldots, x_0^{i2^{K-L}+2^{K-L}-1}\} \\ &= \{x_0^{i2^{K-L}}, x_0^{i2^{K-L}+1}, \ldots, x_0^{(i+1)2^{K-L}-1}\}, \quad 0 \leq i < 2^L.\end{aligned} \tag{32}$$

Considera-se que o mapeamento $T(\cdot)$ é tal que:

$$T(x[0]) = \mathbf{t}_i, \quad \forall x[0] \in \mathcal{X}_0^i, \quad 0 \leq i < 2^L. \tag{33}$$

O mapeamento $M(\cdot)$ tem no seu domínio os 2^K valores possíveis de $\mathbf{k} \oplus \mathbf{s}$. Como $\mathbf{k} \oplus \mathbf{s}$ é um vetor binário, pode-se representar o valor associado a este vetor como um número inteiro em $\{0, 1, \ldots, 2^K - 1\}$. Já a imagem de $M(\cdot)$ são as 2^K condições iniciais pertencentes a $\mathcal{X}_0$, cada uma enumerada por um índice diferente pertencente a $\{0, 1, \ldots, 2^K - 1\}$. A função $M(\cdot)$ aqui considerada mapeia o valor decimal associado a $\mathbf{k} \oplus \mathbf{s}$ no índice associado a alguma condição inicial x_0^i, de forma que:

$$M(\mathbf{k} \oplus \mathbf{s}) = x_0^{P(\mathbf{k} \oplus \mathbf{s})}, \tag{34}$$

em que $P(\cdot)$ representa alguma permutação dos inteiros no intervalo $\{0, 1, \ldots, 2^K - 1\}$. Neste exemplo considera-se $K = 12$, $L = 4$ e a função $P(x) = (6x^2 + x + 1)(\text{mod } 2^K)$, que é um polinômio de permutação módulo 2^K, construído seguindo o resultado apresentado em [14]. Uma simulação de (24) para este mapeamento é realizada, considerando de uma até dez observações com 10000 pares $(\mathbf{s}^1, \mathbf{t}^1), \ldots, (\mathbf{s}^{10}, \mathbf{t}^{10})$ diferentes. A Fig. 2 mostra o resultado da simulação, juntamente com o valor teórico aproximado encontrado em (31). Observa-se que os valores teóricos e simulados são próximos.

Um outro mapeamento que será considerado utiliza o mesmos parâmetros $K = 12$ e $L = 4$, além de uma função $F = T \circ M$ com $T(\cdot)$ e $M(\cdot)$ definidos como em (33) e (34), respectivamente. A diferença aqui está na função de permutação $P(\cdot)$ escolhida, que neste caso é escolhida como:

$$P(x) = (6x^2 + x + 1)(\text{mod } 2^{K-L+1}) + \left\lfloor \frac{x}{2^{K-L+1}} \right\rfloor 2^{K-L+1}. \tag{35}$$

A particularidade desta função permutação $P(\cdot)$ se dá no fato de que ela divide o domínio $\{0, 1, \ldots, 2^K - 1\}$ em intervalos de tamanho 2^{K-L+1}, e permuta apenas os elementos dentro de cada intervalo. Esta peculiaridade faz com que os conjuntos $\mathcal{K}^i$ sejam montados utilizando uma quantidade mais restrita de chaves, o que faz com que exista uma maior chance de uma chave pertencente a um $\mathcal{K}^i$ pertencer a um $\mathcal{K}^j$. A simulação deste caso específico apresenta um decaimento mais suave de (24), decaindo aproximadamente por um fator de 2 (1 bit) a cada nova observação, como ilustra a Fig. 2.

VI. Conclusões

Neste estudo, apresentamos um novo método para gerar *tags* para PLA com base em mapas caóticos. Esse método estabelece um limite mínimo para as informações reveladas sobre a chave secreta, mesmo em um canal livre de ruído, e oferece um controle significativo dos níveis de segurança por meio da seleção dos parâmetros apropriados σ (parâmetro de salto do mapa), L (comprimento da *tag*) e K (comprimento da chave secreta). Também é realizada uma análise da informação que um atacante tem sobre a chave secreta para o caso em que o mesmo intercepta múltiplos pares de mensagem e *tags*.

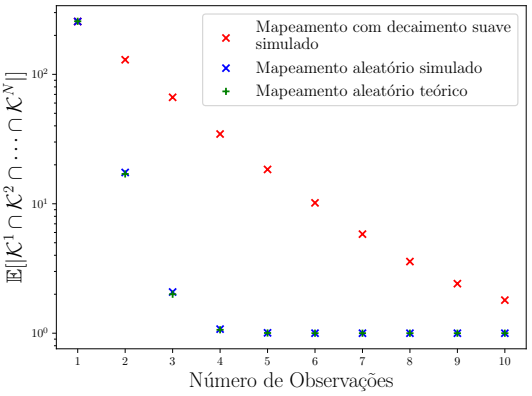

Fig. 2. Valores simulados e teóricos de $\mathbb{E}[|\mathcal{K}^1 \cap \mathcal{K}^2 \cap \cdots \cap \mathcal{K}^N|]$ para um mapeamento aleatório e um mapeamento com decaimento suave com $K = 12$ e $L = 4$.

Referências

[1] N. Xie, C. Chen, and Z. Ming, "Security model of authentication at the physical layer and performance analysis over fading channels," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 1, pp. 253-268, Feb. 2021.

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

[3] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, "Cryptographic side-channel signaling and authentication via fingerprint embedding,"*IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2216-2225, Sept. 2018.

[4] M. Qaisi, S. Althunibat and M. Qaraqe, "Phase-assisted dynamic tag-embedding message authentication for IoT networks," *IEEE Internet Things J.*, vol. 9, no. 20, pp. 20620-20629, Oct., 2022.

[5] S. J. Maeng, Y. Yapıcı, İ. Güvenç, A. Bhuyan, and H. Dai, "Precoder design for physical-layer security and authentication in massive MIMO UAV communications," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2949-2964, Mar. 2022.

[6] P. Zhang, Y. Teng, Y. Shen, X. Jiang and F. Xiao, "Tag-Based PHY-Layer Authentication for RIS-Assisted Communication Systems," *IEEE Trans. Depend. Secure Comput.*, 2023.

[7] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171-4182, June 2016.

[8] P. Zhang, Y. Shen, X. Jiang, and B. Wu, "Physical layer authentication jointly utilizing channel and phase noise in MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2446-2458, April 2020.

[9] P. L. Yu and B. M. Sadler, "MIMO authentication via deliberate fingerprinting at the physical layer," in *IEEE Trans. Inf. Forensics and Security*, vol. 6, no. 3, pp. 606-615, Sept. 2011.

[10] N. Xie, Q. Zhang, J. Chen, and H. Tan, "Privacy-preserving physical-layer authentication for non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 4, pp. 1371-1385, April 2022.

[11] D. P. B. Chaves, C. E. C. Souza, and C. Pimentel, "A smooth chaotic map with parameterized shape and symmetry," *EURASIP Journal on Advances in Signal Processing*, vol. 48, pp. 1537-1538, Nov. 2016.

[12] S. H. Strogatz, *Nonlinear dynamics and chaos with applications to physics, biology, chemistry, and engineering*. Cambridge, MA: Westview Press, second ed., 2014.

[13] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, Oct. 1949.

[14] Ronald L. Rivest, Permutation Polynomials Modulo 2^w, Finite Fields and Their Applications, Volume 7, Issue 2, 2001, Pages 287-292.