Assinaturas Digitais Baseadas em Polinômios de Chebyshev sobre Corpos Finitos Primos

J. B. Lima, R. M. Campello de Souza e D. Panario

***Resumo*— Neste artigo, uma nova definição de polinômios de Chebyshev sobre corpos finitos primos é considerada, a partir da qual um novo esquema de assinatura digital é proposto. Aspectos relacionados à segurança do método são discutidos e mostra-se que a realização de ataques contra o referido esquema envolve o problema do logaritmo discreto.**

***Palavras-Chave*— Polinômios de Chebyshev, corpos finitos, assinaturas digitais.**

***Abstract*— In this paper, a new definition of Chebyshev polynomials over prime finite fields is considered, from which a new digital signature scheme is proposed. Aspects concerning the security of the method are discussed and it is shown that attacks against the referred scheme involve the discrete logarithm problem.**

***Keywords*— Chebyshev polynomials, finite fields, digital signatures.**

I. Introdução

Recentemente, um esquema baseado em polinômios de Chebyshev, por meio do qual um usuário pode autenticar-se eficientemente a um servidor com o propósito de realizar um *log in*, foi proposto [1]. Tal esquema fundamenta-se no comportamento caótico apresentado pelos referidos polinômios, o que constitui um atrativo para aplicações no campo da Criptografia. Embora o esquema mencionado seja aparentemente seguro, em [2] são descritos ataques que empregam estratégias por meio das quais um adversário pode obter acesso ao sistema como se fosse um usuário autêntico do mesmo.

Neste artigo, uma nova definição para polinômios de Chebyshev sobre corpos finitos é considerada [3]. Tal definição é baseada numa trigonometria de corpos finitos, cuja teoria foi originalmente apresentada em [4]. Com base nessa ferramenta, formula-se, no contexto de corpos finitos, o esquema para autenticação de entidades proposto em [5]. Particularmente, demonstra-se que, no cenário considerado neste trabalho, a aplicação dos ataques descritos em [2] envolve o problema do logaritmo discreto. Isso significa que, diferentemente do que acontece quando a definição clássica dos polinômios de Chebyshev (sobre os números reais) é usada, o esquema implementado sobre corpos finitos, em função da intratabilidade do problema mencionado, provê certo grau de segurança.

J. B. Lima, Departamento de Engenharia Elétrica, Escola Politécnica de Pernambuco, Universidade de Pernambuco, Recife, Brasil, E-mail: juliano_bandeira@hotmail.com.

R. M. Campello de Souza, Departamento de Eletrônica e Sistemas, Centro de Tecnologia e Geociências, Universidade Federal de Pernambuco, Recife, Brasil, E-mail: ricardo@ufpe.br.

D. Panario, School of Mathematics and Statistics, Carleton University, Ottawa, Canada, E-mail: daniel@math.carleton.ca.

Este artigo é organizado da seguinte forma. A Seção II revisa a trigonometria sobre corpos finitos e introduz alguns conceitos novos. Na Seção III, os polinômios de Chebyshev sobre corpos finitos primos são definidos e algumas de suas propriedades são apresentadas. Na Seção IV apresenta-se um esquema de assinatura digital baseado nos polinômios de Chebyshev sobre corpos finitos e analisa-se a sua segurança. O artigo é finalizado com algumas conclusões na Seção V.

II. Trigonometria em Corpos Finitos

Nesta seção, os principais conceitos relacionados à trigonometria de corpos finitos são apresentados. Essa trigonometria foi introduzida como requisito para a definição da transformada de Hartley de corpo finito (FFHT) [4].

Definição 1: O conjunto de inteiros Gaussianos sobre GF(p) é o conjunto GI$(p) = \{a + bj, a, b \in \text{GF}(p)\}$, em que p é um número primo tal que $j^2 = -1$ é um resíduo não-quadrático sobre GF(p), isto é, $p \equiv 3 \pmod 4$.

O corpo de extensão GF(p^2) é isomórfico à estrutura "complexa" GI(p), cujos elementos $\zeta = a + bj$ possuem uma parte "real"$a = \Re\{\zeta\}$ e uma parte "imaginária" $b = \Im\{\zeta\}$. De modo análogo, poder-se-ia considerar um corpo finito GF(q), com $q = p^r$ (r sendo um inteiro positivo), e definir a estrutura GI(q) isomórfica a GF(q^2).

Definição 2 (Funções trigonométricas de corpo finito): Seja ζ um elemento não-nulo de GI(p) com ordem multiplicativa denotada por $\text{ord}(\zeta)$. As funções trigonométricas co-seno e seno de corpo finito relacionadas a ζ são calculadas módulo p, respectivamente, por

$$\cos_\zeta(x) := \frac{\zeta^x + \zeta^{-x}}{2} \tag{1}$$

e

$$\sin_\zeta(x) := \frac{\zeta^x - \zeta^{-x}}{2j},$$

$x = 0, 1, \ldots, \text{ord}(\zeta) - 1$.

Aqui, usa-se uma notação ligeiramente diferente daquela proposta em [4][1]. Todavia, independentemente desse fato, as funções trigonométricas acima possuem propriedades semelhantes àquelas das funções trigonométricas sobre os números

[1]Originalmente, as funções trigonométricas co-seno e seno de corpo finito estão relacionadas a $\angle\zeta^i$, o "arco" de ζ^i, e são chamadas funções k-trigonométricas. As mesmas são calculadas como $\cos_k(\angle\zeta^i) = (\zeta^{ki} + \zeta^{-ki})/2$ e $\sin_k(\angle\zeta^i) = (\zeta^{ki} - \zeta^{-ki})/2j$, para $i, k = 0, 1, \ldots, \text{ord}(\zeta) - 1$, e os parâmetros i e k são respectivamente associados ao domínio do "tempo" e ao da "frequência" da FFHT.

reais, como *círculo unitário* e *adição de arcos*, por exemplo [4]. A partir da Equação (1), observa-se que a função co-seno de corpo finito possui período $\mathrm{ord}(\zeta)$ e simetria par, ou seja,

$$\cos_\zeta(x) = \cos_\zeta(-x \,(\mathrm{mod}\ \mathrm{ord}(\zeta))). \tag{2}$$

Definição 3 (Conjunto unimodular): O conjunto unimodular de GI(p), denotado por G_1, é o conjunto de elementos $\zeta = (a + bj) \in \mathrm{GI}(p)$, tais que $a^2 + b^2 \equiv 1 (\mathrm{mod}\ p)$.

Também é possível definir GI(p) e funções trigonométricas de corpo finito para $p \equiv 1 \,(\mathrm{mod}\ 4)$. Nesse caso, que não é tratado neste artigo, usar-se-ia um resíduo não-quadrático $j^2 \neq -1$ sobre GF(p).

Proposição 1: A estrutura $\langle G_1, \bullet \rangle$ é um grupo cíclico de ordem $(p + 1)$ [6].

O Lema 1 a seguir desempenha um papel importante na definição da função co-seno inverso de corpo finito, que leva à nova definição dos polinômios de Chebyshev sobre corpos finitos.

Lema 1: Se $\zeta = (a + bj) \in \mathrm{GI}(p)$ é um elemento unimodular, então $\cos_\zeta(x) = \Re\{\zeta^x\}$, $x = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$ [7].

Demonstração: Usando a Definição 2 e $\zeta^x = c + dj$, $c, d \in \mathrm{GF}(p)$, tem-se

$$\cos_\zeta(x) = \frac{(c + dj) + (c + dj)^{-1}}{2}.$$

Devido à Proposição 1, $\zeta^x = c + dj$ também é unidomular e $(c + dj)^{-1} = (c + dj)^* = c - dj$, em que $(\cdot)^*$ denota o complexo conjugado. Portanto, a última expressão pode ser reescrita como

$$\cos_\zeta(x) = \frac{(c + dj) + (c - dj)}{2} = c = \Re\{\zeta^x\}.$$

■

No que se segue, alguns novos conceitos são introduzidos com o propósito de definir a função co-seno inverso de corpo finito. Escolhendo um elemento específico $\zeta_a \in \mathrm{GI}(p)$ com ordem multiplicativa $\mathrm{ord}(\zeta_a)$, sua função co-seno pode ser expressa como

$$\cos_{\zeta_a} : \mathbb{Z}_{\mathrm{ord}(\zeta_a)} \to \mathbb{I}_{\zeta_a}, \tag{3}$$

em que $\mathbb{Z}_{\mathrm{ord}(\zeta_a)}$ é o conjunto de inteiros módulo $\mathrm{ord}(\zeta_a)$ e $\mathbb{I}_{\zeta_a}$ é o conjunto imagem relacionado a $\cos_{\zeta_a}$. Devido à simetria do co-seno, a cardinalidade de $\mathbb{I}_{\zeta_a}$ é $\#\{\mathbb{I}_{\zeta_a}\} = \lfloor \mathrm{ord}(\zeta_a)/2 \rfloor + 1$. Portanto, a respectiva função co-seno inverso pode ser expressa como

$$\arccos_{\zeta_a} : \mathbb{I}_{\zeta_a} \to \mathbb{Z}_{\lfloor \frac{\mathrm{ord}(\zeta_a)}{2} \rfloor + 1}. \tag{4}$$

Seja ζ_1 um gerador do grupo G_1. A função co-seno relacionada a ζ_1 pode ser expressa como a Equação (3) e, analogamente, seu conjunto imagem é denotado por $\mathbb{I}_{\zeta_1}$. A partir da Proposição 1 e do Lema 1, uma vez que ζ_1 é unimodular e $\mathrm{ord}(\zeta_1) = p + 1$, $\mathbb{I}_{\zeta_1}$ é o conjunto de todos os elementos da forma $\Re\{\zeta\}$, tais que $\zeta \in \mathrm{GI}(p)$ é unimodular. Sua cardinalidade é $\#\{\mathbb{I}_{\zeta_1}\} = (p + 1)/2 + 1$, a qual, claramente, também representa a máxima cardinalidade do conjunto $\mathbb{I}_\zeta$ para ζ unimodular.

Exemplo 1: Seja $\zeta_1 = 2 + 2j$ um elemento unimodular de GI(7) tal que $\mathrm{ord}(\zeta_1) = 8$. Na Tabela I, todos os possíveis valores para $\cos_{\zeta_1}(x)$ são apresentados. Observa-se que $\mathbb{I}_{\zeta_1} = \{0, 1, 2, 5, 6\}$ e, consequentemente, a função $\arccos_{\zeta_1}(x)$ não está definida para $x \in \{3, 4\}$.

Conforme ilustrado no Exemplo 1, embora $\zeta_1 \in \mathrm{GI}(p)$ seja um elemento unimodular com ordem multiplicativa máxima $p + 1$, a função $\arccos_{\zeta_1}(x)$ não está definida para todo elemento $x \in \mathbb{Z}_p$. Assim, com o propósito de calcular a função co-seno inverso de elementos que estão em $\mathbb{Z}_p$ mas não estão em $\mathbb{I}_{\zeta_1}$, precisa-se selecionar um elemento ζ_2 $(\neq \zeta_1)$ tal que $\mathbb{I}_{\zeta_1} \cup \mathbb{I}_{\zeta_2} = \mathbb{Z}_p$. Tal elemento é especificado pelo seguinte teorema.

Teorema 1: Seja $\zeta_1 \in \mathrm{GI}(p)$ um gerador do grupo G_1 e $\zeta_2 \in \mathrm{GF}(p)$ tal que $\mathrm{ord}(\zeta_2) = p - 1$. Então, $\mathbb{I}_{\zeta_1} \cup \mathbb{I}_{\zeta_2} = \mathbb{Z}_p$.

Demonstração: A partir de observações anteriores, sabe-se que $\#\{\mathbb{I}_{\zeta_1}\} = (p+1)/2+1$ e $\#\{\mathbb{I}_{\zeta_2}\} = (p-1)/2+1$. De acordo com o Lema 1, o conjunto $\mathbb{I}_{\zeta_1} \cap \mathbb{I}_{\zeta_2}$ é composto por elementos $\cos_{\zeta_2}(x) = \Re\{\zeta\}$, $x = 0, 1, \ldots, p-2$, para algum ζ unimodular. Portanto, a partir da Definição 3, pode-se escrever

$$[\,\cos_{\zeta_2}(x)\,]^2 + b^2 \equiv 1 \,(\mathrm{mod}\ p),\ \ b \in \mathrm{GF}(p).$$

Usando a Definição 2, a equação acima pode ser reescrita como

$$\left(\frac{\zeta_2^x + \zeta_2^{-x}}{2}\right)^2 + b^2 \equiv 1 \,(\mathrm{mod}\ p).$$

Expandindo o termo no lado esquerdo da última equação, após algumas simplificações, tem-se

$$\left(\zeta_2^x - \zeta_2^{-x}\right)^2 \equiv -4b^2 \,(\mathrm{mod}\ p).$$

Tomando a raiz quadrada da ambos os lados da equação acima, obtem-se o seguinte:

$$\zeta_2^x - \zeta_2^{-x} \equiv \pm 2b\,j \,(\mathrm{mod}\ p).$$

Uma vez que $\zeta_2 \in \mathrm{GF}(p)$, a relação acima é atendida apenas se $b = 0$. Consequentemente, os possíveis valores para x são 0 e $(p - 1)/2$. Então, $\#\{\mathbb{I}_{\zeta_1} \cap \mathbb{I}_{\zeta_2}\} = 2$ e

$$\begin{aligned}\#\{\mathbb{I}_{\zeta_1} \cup \mathbb{I}_{\zeta_2}\} &= \#\{\mathbb{I}_{\zeta_1}\} + \#\{\mathbb{I}_{\zeta_1}\} - \#\{\mathbb{I}_{\zeta_1} \cap \mathbb{I}_{\zeta_2}\} \\ &= \frac{p+1}{2} + 1 + \frac{p-1}{2} + 1 - 2 = p.\end{aligned}$$

Todo elemento em $\mathbb{I}_{\zeta_1}$ ou $\mathbb{I}_{\zeta_2}$ está também em $\mathbb{Z}_p$, portanto, o teorema é válido. ■

Exemplo 2: Seja $\zeta_2 = 3$ um elemento de GF(7) tal que $\mathrm{ord}(\zeta_2) = 6$. Na Tabela II, todos os possíveis valores para $\cos_{\zeta_2}(x)$ são apresentados. Observa-se que $\mathbb{I}_{\zeta_2} = \{1, 3, 4, 6\}$. Como ζ_2 foi escolhido de acordo com o Teorema 1, considerando $\mathbb{I}_{\zeta_1} = \{0, 1, 2, 5, 6\}$ (ver Exemplo 1), tem-se $\mathbb{I}_{\zeta_1} \cup \mathbb{I}_{\zeta_2} = \mathbb{Z}_7$.

TABELA I

TODOS OS POSSÍVEIS VALORES PARA $\cos_{\zeta_1}(x)$, EM QUE $\zeta_1 = 2 + 2j$ É UM ELEMENTO UNIMODULAR, EM GI(7), DE ORDEM $\mathrm{ord}(\zeta_1) = 8$.

x	$\cos_{\zeta_1}(x)$	x	$\cos_{\zeta_1}(x)$
0	1	4	6
1	2	5	5
2	0	6	0
3	5	7	2

TABELA II

TODOS OS POSSÍVEIS VALORES PARA $\cos_{\zeta_2}(x)$, EM QUE $\zeta_2 = 3$ É UM ELEMENTO EM GF(7) DE ORDEM $\mathrm{ord}(\zeta_2) = 6$.

x	$\cos_{\zeta_2}(x)$	x	$\cos_{\zeta_2}(x)$
0	1	3	6
1	4	4	3
2	3	5	4

III. POLINÔMIOS DE CHEBYSHEV SOBRE CORPOS FINITOS

Nesta seção, apresenta-se uma definição para polinômios de Chebyshev sobre corpos finitos primos recentemente introduzida [3]. Diferentemente de propostas anteriores, tal definição é baseada na função co-seno de corpo finito, a qual está em perfeita analogia com a definição clássica de polinômios de Chebyshev sobre os números reais [8].

Definição 4: Os polinômios de Chebyshev do primeiro tipo sobre GF(p) são definidos como

$$T_n(x) := \cos_\zeta(n \arccos_\zeta(x)) (\mathrm{mod}\ p), \tag{5}$$

em que $n \in \mathbb{N}$, $\zeta \in$ GI(p) e $x \in \mathbb{I}_\zeta$.

A Equação (5) corresponde ao co-seno dos múltiplos de um arco. Portanto, analogamente ao caso real, a mesma pode ser expandida usando a *fórmula de De Moivre*. Esse procedimento forneceria polinômios de grau n em termos de co-senos do respectivo arco [8]. Entretanto, polinômios de Chebyshev para diferentes valores de n podem ser obtidos a partir de uma simples relação de recorrência. Para o caso de corpo finito, esta relação é derivada da Definição 4 e da fórmula de adição de arcos [4]. A mesma é dada por

$$T_{n+1}(x) = 2\,x\,T_n(x) - T_{n-1}(x) (\mathrm{mod}\ p), \tag{6}$$

em que $x \in$ GF(p), $n \in \mathbb{N}$, $T_0(x) = 1$ e $T_1(x) = x$. Polinômios de Chebyshev módulo p possuem a seguinte periodicidade.

Proposição 2: Seja ζ um elemento não-nulo de GI(p) tal que $\mathrm{ord}(\zeta) = N$. Se $x \in \mathbb{I}_\zeta$, então $T_{t\,N \pm n}(x) = T_n(x)$, $t \in \mathbb{Z}$.

Demonstração: A partir da Definição 4, tem-se

$$T_{t\,N \pm n}(x) = \cos_\zeta((t\,N \pm n) \arccos_\zeta(x)) (\mathrm{mod}\ p).$$

Aplicando a fórmula de adição de arcos, a equação acima é reescrita como

$$\begin{aligned} T_{t\,N \pm n}(x) = {} & \cos_\zeta(t\,N \arccos_\zeta(x)) \cos_\zeta(n \arccos_\zeta(x)) \\ & \mp \sin_\zeta(t\,N \arccos_\zeta(x)) \sin_\zeta(n \arccos_\zeta(x)). \end{aligned}$$

Uma vez que $\mathrm{ord}(\zeta) = N$, aplicando a Definição 2, sabe-se que $\cos_\zeta(t\,N \arccos_\zeta(x)) = 1$ e $\sin_\zeta(t\,N \arccos_\zeta(x)) = 0$. Consequentemente, a última equação é reduzida a $T_{t\,N \pm n}(x) = \cos_\zeta(n \arccos_\zeta(x)) = T_n(x)$. ■

Embora a Definição 4 requeira $x \in \mathbb{I}_\zeta$, essa restrição pode ser negligenciada caso se queira avaliar $T_n(x)$ para valores particulares de n, x e para um número primo p. Neste sentido, pode-se usar a Equação (6), a qual não depende de ζ. Assim, não é necessário lidar com a função co-seno e com sua inversa.

A propriedade de semi-grupo dos polinômios de Chebyshev sobre os números reais também é válida no caso de corpos finitos:

$$T_r(T_s(x)) = T_s(T_r(x)) = T_{rs}(x). \tag{7}$$

A consistência da equação acima é verificada pela Definição 4, cuja aplicação fornece

$$\begin{aligned} T_r(T_s(x)) &= \cos_\zeta(r \arccos_\zeta(\cos_\zeta(s \arccos_\zeta(x)))) \\ &= \cos_\zeta(rs \arccos_\zeta(x)) = T_{rs}(x). \end{aligned}$$

De modo análogo, demonstra-se que $T_s(T_r(x)) = T_{rs}(x)$. Essa propriedade desempenha um importante papel na corretude do esquema de assinatura digital que se discute na próxima seção.

IV. AUTENTICAÇÃO DE ENTIDADES BASEADA EM POLINÔMIOS DE CHEBYSHEV SOBRE CORPOS FINITOS

Em Criptografia, o conceito de assinatura digital está relacionado à garantia que determinada entidade oferece acerca de sua identidade. Nesse contexto, num protocolo de comunicação seguro, é permitida a uma segunda parte a verificação da autenticidade da referida entidade e, a partir disso, a liberação do seu acesso a determinado sistema, por exemplo [9].

Em [1], um esquema baseado em polinômios de Chebyshev por meio do qual um usuário pode autenticar-se eficientemente a um servidor, foi proposto. No cenário considerado, naturalmente, o usuário corresponde à entidade cuja identidade se deseja verificar; o servidor é a segunda parte, responsável pela verificação da assinatura do usuário. Nesta seção, o esquema mencionado é estendido para o contexto de corpos finitos. Mostra-se que, no cenário aqui considerado, diferentemente do que acontece quando se usam polinômios de Chebyshev sobre os reais, o esquema é seguro, uma vez que a aplicação dos ataques propostos em [2], originalmente desenvolvidos para o caso real, envolve o problema do logaritmo discreto.

A. Esquema proposto

Para a implementação do esquema proposto, é necessário escolher um número $m \in$ GF(p) e definir $T_s^i(\cdot)$, a i-ésima iteração do mapeamento $T_s(\cdot)$, ou seja, $T_s^i(\cdot) = T_s(T_s(T_s \ldots T_s(\cdot)) \ldots) = T_{s^i}(\cdot)$. Na fase de configuração, o servidor e o usuário executam, sequencialmente, as tarefas:

1. O servidor gera um número aleatório $r \in \mathbb{Z}_p$.
2. Calcula e envia $T_r(m)$ para o usuário.
3. O usuário escolhe um número aleatório $s \in \mathbb{Z}_p$.

Na i-ésima fase de autenticação, o usuário e o servidor fazem o seguinte:

---

1. O usuário calcula $T_s^i(m)$, e $aut = T_s^i(T_r(m))$, e envia ambos os resultados para o servidor.
2. O servidor calcula $aut' = T_r(T_s^i(m))$ e verifica se $aut = aut'$. Caso a última igualdade seja satisfeita, o acesso é permitido.

B. Análise da segurança do esquema proposto - cenário 1

Considerando um cenário em que um adversário tenha acesso a m e $T_r(m)$, parâmetros associados ao primeiro passo do processo de autenticação, o mesmo pode aplicar um ataque calculando um número s' tal que $T_{s'}(m) = T_s(m)$. Então, na i-ésima fase de autenticação, o adversário pode se passar pelo usuário real calculando $T_{s'}^i(m)$, e $aut = T_{s'}^i(T_r(m))$. Por indução, é possível mostrar que $T_{s'}^i(m) = T_s^i(m)$. Consequentemente, tem-se

$$\begin{aligned} aut &= T_{s'}^i(T_r(m)) \\ &= T_r(T_{s'}^i(m)) \\ &= T_r(T_s^i(m)) \\ &= T_s^i(T_r(m)). \end{aligned}$$

O cálculo de s' requer os conceitos introduzidos nas Seções II e III e é realizado de acordo com o seguinte lema.

Lema 2: Para cada par $(s, T_s(m))$, o inteiro s' satisfaz $T_{s'}(m) = T_s(m)$ se e somente se

$$s' = \pm \arccos_\zeta(T_s(m)) \, (\arccos_\zeta(m))^{-1} (\mathrm{mod}\ N), \qquad (8)$$

em que $N = \mathrm{ord}(\zeta)$.

Demonstração: Assume-se que

$$s' = \pm \arccos_\zeta(T_s(m)) \, (\arccos_\zeta(m))^{-1} (\mathrm{mod}\ N).$$

A partir da Definição 4,

$$\begin{aligned} T_{s'}(m) &= \cos_\zeta(s' \arccos_\zeta(m)) \\ &= \cos_\zeta(\pm \arccos_\zeta(T_s(m))) = T_s(m). \end{aligned}$$

Por outro lado, assume-se que $T_{s'}(m) = T_s(m)$ para certo s'. Então,

$$T_{s'}(m) = \cos_\zeta(s' \arccos_\zeta(m)) = T_s(m).$$

Aplicando a função $\arccos_\zeta$ a ambos os lados da última igualdade, obtém-se

$$\arccos_\zeta(\cos_\zeta(s' \arccos_\zeta(m))) = \arccos_\zeta(T_s(m)). \qquad (9)$$

Seja $y = \arccos_\zeta(w)$. De acordo com a Equação (2), para todo $\beta = 0, \ldots, N-1$, a relação de simetria $\cos_\zeta(\beta) = \cos_\zeta(-\beta(\mathrm{mod}\, N))$ é válida; devido à periodicidade da função $\cos_\zeta$, se $\cos_\zeta(\beta) = w$, tem-se $\beta = \pm y (\mathrm{mod}\ N)$. Portanto, a Equação (9) é satisfeita se e somente se

$$s' \arccos_\zeta(m) = \pm \arccos_\zeta(T_s(m)) (\mathrm{mod}\ N).$$

Multiplicando ambos os lados da última equação por $(\arccos_\zeta(m))^{-1} (\mathrm{mod}\ N)$, obtém-se

$$s' = \pm \arccos_\zeta(T_s(m)) \, (\arccos_\zeta(m))^{-1} (\mathrm{mod}\ N),$$

e o lema é satisfeito. ■

Diferentemente do ataque contra o esquema baseado em polinômios de Chebyshev clássicos, no cenário de corpos finitos, o Lema 2 fornece apenas dois valores para s'. Naturalmente, esses valores são necessariamente inteiros. Portanto, não é preciso considerar aspectos de precisão nem resolver qualquer sistema linear de equações modulares [2].

Entretanto, o cálculo de s' pela Equação (8) depende da restrição sobre a existência da função co-seno inverso. Conforme discutido previamente, $\arccos_\zeta(x)$ está definido se e somente se $x \in \mathbb{I}_\zeta$ (ver Seção II). De acordo com o esquema apresentado, o parâmetro m pode assumir qualquer valor em GF(p). Assim, o Teorema 1 é necessário para especificar elementos ζ_1 e ζ_2 tais que $\mathbb{I}_{\zeta_1} \cup \mathbb{I}_{\zeta_2} = \mathbb{Z}_p$. Isso garante que $\arccos_\zeta(x)$ está definido para $\zeta = \zeta_1$ ou $\zeta = \zeta_2$. Além disso, $\arccos_\zeta(T_s(m)) = s \arccos_\zeta(m)$. Assim, o cálculo de s' não requer uma avaliação explícita de $(\arccos_\zeta(m))^{-1} (\mathrm{mod}\ N)$.

Uma fórmula explícita para a função co-seno inverso pode ser derivada a partir da Definição 2. Após algumas manipulações de $\cos_\zeta(x) = (\zeta^x + \zeta^{-x})/2$, obtém-se

$$\arccos_\zeta(x) = \log_\zeta \left(x + \sqrt{x^2 - 1} \right),$$

a função $\arccos_\zeta$ na forma de um logaritmo discreto, calculado módulo p. Aplicando a fórmula acima à Equação (8) e usando algumas propriedades dos logaritmos, tem-se

$$s' = \pm \left[\log_{x+\sqrt{x^2-1}} \left(T_s(x) + \sqrt{T_s(x)^2 - 1} \right) \right] (\mathrm{mod}\ N).$$

Isso significa que a aplicação do ataque descrito envolve o problema do logaritmo discreto. Devido à presença de raízes quadradas na equação acima, possivelmente, tal problema requer considerar o corpo GI(p).

C. Análise da segurança do esquema proposto - cenário 2

Um outro cenário a ser considerado consiste em fazer m e $T_r(m)$ acessíveis apenas ao usuário e ao servidor. Nesse caso, na tentativa de autenticar-se como usuário real, um adversário poderia interceptar as informações que são trocadas em duas fases sucessivas de autenticação. Assim, assumindo que o adversário obtém $T_s^{i-1}(m)$, $T_s^{i-1}(T_r(m))$ e $T_s^i(m)$, $T_s^i(T_r(m))$, o mesmo aplicaria o ataque realizando os seguintes passos:

---

1. Calcula um número w tal que $T_w(T_s^{i-1}(m)) = T_s^i(m)$.
2. Para qualquer $l \geq 1$, para autenticar-se na $(i+l)$-ésima sessão,
   (a) Calcula $T_s^{i+l}(m) = T_w^l(T_s^i(m))$ e $aut = T_s^{i+l}(T_r(m)) = T_w^l(T_s^i(T_r(m)))$.
   (b) Envia o par $(T_s^{i+l}(m), aut)$.

Enfatiza-se que, no presente cenário, o adversário não precisa conhecer o índice i da sessão. Para a aplicação do procedimento descrito acima, apenas duas mensagens de

autenticação sucessivas são necessárias. Uma demonstração de que o ataque funciona devidamente para o caso dos polinômios de Chebyshev clássicos é encontrada em [2]. Sua extensão para o contexto de corpos finitos é imediata. O fato é que o cálculo do número inteiro w tal que $T_w(T_s^{i-1}(m)) = T_s^i(m)$, assim como no cenário considerado anteriormente, requer o Lema 2. Portanto, em função da necessidade de lidar com o problema do logaritmo discreto, o ataque descito acima é impraticável e, por conseguinte, o esquema proposto é seguro quando se utiliza polinômios de Chebyshev sobre corpos finitos.

V. CONCLUSÕES

Nesse artigo uma nova definição para polinômios de Chebyshev sobre corpos finitos primos foi considerada [3]. Essa definição é mais natural que aquela apresentada em [10], uma vez que se baseia nas funções co-seno e arco co-seno de corpo finito. Um esquema de asssinatura digital baseado em tais polinômios foi proposto. Devido à sua formulação em corpos finitos, o esquema, aparentemente, é imune a ataques que foram aplicados a versões do mesmo definidas sobre o corpo dos números reais, visto que agora esses ataques esbarram na dificuldade de resolver o problema do logaritmo discreto.

REFERÊNCIAS

[1] L. Kocarev and Z. Tasev, "Public-key encryption based on Chebyshev maps," in *Proc. IEEE Int. Symp. Circuits and Systems (ISCAS'03)*, 2003, vol. 3, pp. 28–31.

[2] P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Trans. Circuits and Systems–I: Regular Papers*, vol. 52, no. 7, pp. 1382–1393, July 2005.

[3] J. B. Lima, R. M. Campello de Souza, and D. Panario, "Security of public-key cryptosystems based on Chebyshev polynomials over prime finite fields," in *Proc. IEEE Int. Symp. Information Theory (ISIT'2008)*, 2008, pp. 1843–1847.

[4] R. M. Campello de Souza, H. M. de Oliveira, A.N. Kauffman, and A. J. A. Paschoal, "Trigonometry in finite fields and a new Hartley transform," in *Proc. IEEE Int. Symp. Information Theory (ISIT'98)*, 1998, p. 293.

[5] D. Xiao, X. Liao, G. Tang, and C. Li, "Using Chebyshev chaotic map to construct infinite length hash chains," in *Proc. Int. Conf. Communications, Circuits and Systems*, 2004, vol. 1, pp. 11–12.

[6] R. M. Campello de Souza, H. M. de Oliveira, and D. Silva, "Trigonometry in finite fields and a new Hartley transform," in *Proc. International Telecommunications Symposium (ITS'2002)*, 2002, vol. 1, pp. 384–389.

[7] R. M. Campello de Souza, H. M. de Oliveira, L. B. Espínola Palma, and M. M. Campello de Souza, "Hartley number theoretic transforms," in *Proc. IEEE Int. Symp. Information Theory (ISIT 2001)*, 2001, p. 210.

[8] J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*, Chapman & Hall/CRC, Boca Raton, FL, 2nd edition, 2002.

[9] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC, Boca Raton, FL, 1997.

[10] N. Hongzhou, L. Yun, and H. Dequan, "Public key encryption algorithm based on Chebyshev polynomials over finite fields," in *Proc. 8th Int. Conference on Signal Processing*, 2006.