Aprimoramento de Protocolo de Identificação Baseado no Problema $\mathcal{MQ}$

Fábio S. Monteiro[1] [2], **Denise Goya e Routo Terada**[1]

[1]Departamento de Ciência da Computação – IME – USP

[2]Centro de Coordenação de Estudos da Marinha em São Paulo – Marinha do Brasil

{fsm, dhgoya, rt}@ime.usp.br

Abstract. *The $\mathcal{MQ}$ problem, which consists in solving a system of multivariate quadratic polynomials over finite field, has attracted the attention of researchers for the development of public-key cryptosystems because (1) it's NP-complete, (2) there is no known polynomial-time algorithm for it's solution, even in the quantum computational model, and (3) enable cryptographic primitives of practical interest. In 2011, Sakumoto, Shirai and Hiwatari presented two new zero-knowledge identification protocols based exclusively on the $\mathcal{MQ}$ problem. The 3-pass identification protocol of Sakumoto et al. has knowledge error 2/3. In this paper, we propose an improvement that reduces the knowledge error to 1/2. The result is a protocol that reduces the total communication needed and requires a smaller number of rounds for the same security level.*

Resumo. *O problema $\mathcal{MQ}$, que consiste em resolver um sistema de equações polinomiais multivariáveis quadráticas sobre um corpo finito, tem atraído a atenção de pesquisadores para o desenvolvimento de sistemas criptográficos de chave pública por ser (1) NP-completo, (2) não ter algoritmo conhecido de tempo polinomial para sua solução nem mesmo no modelo computacional quântico e (3) viabilizar primitivas criptográficas de interesse prático. Em 2011, Sakumoto, Shirai e Hiwatari apresentaram dois novos protocolos de identificação de conhecimento-zero baseados exclusivamente no problema $\mathcal{MQ}$. O protocolo em 3 passos de Sakumoto et al. apresenta probabilidade de personificação de 2/3 em uma rodada. No presente artigo é proposto um protocolo aprimorado que reduz essa probabilidade para 1/2. O resultado é um protocolo que diminui a comunicação total necessária e requer um número menor de iterações para o mesmo nível de segurança.*

1. Introdução

Protocolos de identificação são peças fundamentais para a construção de mecanismos de autenticação e assinaturas digitais. Quando baseados no modelo de chave pública, sua segurança depende da hipótese de intratabilidade de um determinado problema computacional. O problema de encontrar solução para um sistema de equações polinomiais multivariáveis quadráticas sobre um corpo finito, conhecido por Problema $\mathcal{MQ}$, reúne propriedades de interesse para o desenvolvimento de primitivas criptográficas, visto que é um problema NP-completo [Garey e Johnson 1979], não se conhecendo, até hoje, solução de tempo polinomial, nem mesmo no modelo computacional quântico [Bernstein et al. 2009] e tem possibilitado o desenvolvimento de protocolos com desempenho prático, como em [Petzoldt et al. 2011].

Durante a conferência CRYPTO 2011, Sakumoto, Shirai e Hiwatari apresentaram uma nova forma de construir parâmetros públicos e secretos com base no problema $\mathcal{MQ}$, de modo a eliminar a hipótese de dificuldade do problema de isomorfismo de polinômios (IP), presente em vários outros trabalhos [Sakumoto et al. 2011]. Os autores apresentaram dois protocolos de identificação de conhecimento-zero baseados exclusivamente no problema $\mathcal{MQ}$, aplicando uma técnica de divisão do segredo e a forma polar (com propriedade de bilinearidade) de uma função $\mathcal{MQ}$. Para reduzir ao mínimo possível a comunicação, eles utilizaram ainda uma técnica criada originalmente por Jacques Stern [Stern 2006], que consiste em enviar apenas um hash de todos os compromissos no primeiro passo e depois incluir em Rsp aqueles compromissos que não podem ser verificados, para que juntamente com os compromissos reconstituídos pelo verificador seja possível efetuar um novo hash para validar o recebido inicialmente. No artigo de Sakumoto, Shirai e Hiwatari todos os dados atinentes ao tamanho da comunicação do protocolo consideram a utilização desta técnica e por isso iremos assumir que ela será obrigatoriamente utilizada, visto que nosso objetivo principal é, de fato, a diminuição do tamanho da comunicação do protocolo, objetivando atender aplicações onde o consumo de energia é crítico e a complexidade de comunicação requer mais energia do que a complexidade de processamento local, como em redes de sensores sem fio. Chamaremos o protocolo em 3 passos de Sakumoto, Shirai e Hiwatari de $\mathcal{MQID}$-3 e, consequentemente, de $\mathcal{MQID}$-5 o protocolo original em 5 passos.

$\mathcal{MQID}$-3, como o nome sugere, funciona com três trocas de mensagens entre provador e verificador e apresenta probabilidade de personificação de 2/3 em uma rodada. Para alcançar um nível de segurança de 2^{-30}, comparável a propostas anteriores, esse protocolo precisa ser iterado 52 vezes.

Contribuições e Organização deste Trabalho

No presente artigo, propomos a construção de uma versão aprimorada do protocolo de identificação $\mathcal{MQID}$-3, apresentado durante a CRYPTO'2011 por Sakumoto, Shirai e Hiwatari [Sakumoto et al. 2011], utilizando uma construção que diminui a probabilidade de personificação em uma rodada de 2/3 para 1/2, elevando o nível de segurança do protocolo e diminuindo o tamanho da comunicação necessária em uma execução. Nossa proposta apresenta uma diminuição de 9,5% no tamanho da comunicação, sempre considerando a utilização da técnica sugerida por Jacques Stern [Stern 2006] para reduzir o número de compromissos trafegados, enviando apenas um hash de todos os compromissos no primeiro passo do protocolo e depois incluindo na resposta do provador apenas aqueles que não podem ser reconstituídos, para que juntamente com os compromissos validados pelo verificador seja possível efetuar um novo hash para comparar com o recebido inicialmente. Nosso protocolo preserva o tamanho dos parâmetros do sistema e também independe da hipótese de dificuldade do problema de isomorfismo de polinômios.

O restante deste documento está organizado da seguinte forma: na Seção 2, estabelecemos algumas notações e terminologia necessárias, bem como revemos algumas definições que nos servirão como base para o desenvolvimento do artigo. Na Seção 3, explicamos o problema $\mathcal{MQ}$, seu uso em criptografia de chave pública e a formulação de Sakumoto *et al.* para os parâmetros do criptossistema. Na Seção 4, revisamos brevemente o protocolo $\mathcal{MQID}$-3 apresentado em [Sakumoto et al. 2011] para, então, propormos

modificações na Seção 5, onde o protocolo aprimorado de 3 passos é descrito e analisado. Por fim, na Seção 6, listamos algumas considerações e propomos trabalhos que podem ser derivados deste.

2. Fundamentos

Iniciaremos estabelecendo algumas notações e terminologia, bem como revendo definições que nos servirão como base. Durante este texto utilizaremos $\mathbb{F}$ ou $\mathbb{F}_q$ para designar um corpo finito de Galois de ordem q. Quando utilizamos $\mathbb{F}^n$ estamos falando do espaço vetorial de dimensão n sobre $\mathbb{F}$. Em nossa notação, $a \in_R \mathcal{D}$ determina que um valor a pertencente ao domínio $\mathcal{D}$ é escolhido aleatoriamente, com igual probabilidade, entre todos os elementos pertencentes a $\mathcal{D}$.

2.1. Esquemas de Identificação

Esquemas de identificação são peças fundamentais para a construção de mecanismos de autenticação e assinaturas digitais. Seu objetivo é possibilitar que uma entidade $\mathcal{B}eto$, também chamado de verificador, possa validar com segurança a identidade de uma outra entidade $\mathcal{A}lice$, também chamada de provadora. Obviamente, existem diversas maneiras de se alcançar o objetivo proposto. Podemos, por exemplo, considerar o *login* de um usuário em um sistema operacional como sendo um esquema de identificação baseado em chave secreta, onde o usuário é o provador e o SO é o verificador. Neste exemplo, o verificador simplesmente conhece a chave secreta do provador e faz a checagem validando-o. Em nosso trabalho no entanto, vamos focar apenas em esquemas de identificação baseados no modelo de chave pública, mais especificamente vamos utilizar apenas esquemas de identificação de conhecimento-zero, por isso, a partir de agora, quando nos referirmos a esquema de identificação, estamos falando de um esquema de conhecimento-zero.

Para formalizarmos nossa definição dizemos que, um esquema de identificação $\mathcal{ID}$ é uma tupla de algoritmos composta por Setup, Gen, P e V. Onde Setup recebe um parâmetro de segurança 1^κ e devolve um parâmetro de sistema *param*. Gen é o algoritmo de geração de chaves que utiliza *param* e retorna um par de chaves sk e pk, onde sk é a chave privada e pk a chave pública. P e V constituem um protocolo interativo de identificação, onde P é executado por $\mathcal{A}lice$ (provadora), utilizando sua chave privada, e V é utilizado por $\mathcal{B}eto$ (verificador), com acesso a chave pública de $\mathcal{A}lice$. A seguir estabelecemos as propriedades requeridas para o nosso esquema de identificação:

Correção (*completeness*) $-$ Seja $\mathcal{ID}$ um esquema de identificação, dizemos que ele satisfaz a noção de correção se, dados uma provadora honesta $\mathcal{A}lice$ e um verificador honesto $\mathcal{B}eto$, a execução do protocolo resulta no aceite da identidade de $\mathcal{A}lice$ por $\mathcal{B}eto$, ou seja:

$$\Pr[\mathrm{V}(pk_{\mathcal{A}lice}, Cmt \| Ch \| \mathrm{P}(sk_{\mathcal{A}lice}, Cmt \| Ch)) = 1] = 1$$

Solidez (*soundness*) $-$ Seja $\mathcal{ID}$ um esquema de identificação, dizemos que ele possui solidez se, nenhum falso provador puder convencer um verificador honesto a aceitar sua interação como sendo de uma outra entidade, exceto com uma probabilidade negligenciável. Isto é, se um adversário $\mathcal{C}arlos$ tentar personificar $\mathcal{A}lice$ perante $\mathcal{B}eto$, sua chance de sucesso será desprezível ou, formalmente, menor que ϵ.

$$\Pr[\mathrm{V}(pk_{Alice}, Cmt \| Ch \| \mathrm{P}(sk_{falsa}, Cmt \| Ch)) = 1] < \epsilon$$

Conhecimento-Zero (*zero-knowledge*) − Seja $\mathcal{ID}$ um esquema de identificação, dizemos que ele é de conhecimento-zero se, caso a afirmação seja verdadeira, nenhum verificador aprende outra coisa senão este fato.

Quando o esquema de identificação é composto de 3 passos, normalmente nomeados como: comprometimento, desafio e resposta, ele é chamado de canônico por Abdalla *et al* [Abdalla et al. 2002] que especifica esta condição como um dos requisitos para possibilitar a geração de um esquema de assinatura digital, seguro no modelo do oráculo aleatório [Bellare e Rogaway 1993], utilizando-se o paradigma da transformação Fiat-Shamir [Fiat e Shamir 1987].

2.2. Esquemas de Comprometimento

Para construção do esquema de identificação de conhecimento-zero utilizaremos um esquema de comprometimento (*Commitment Scheme*), que tem por objetivo esconder temporariamente um valor que não pode ser alterado.

Podemos ilustrar o funcionamento de um esquema de comprometimento com um remetente que tranca uma mensagem em uma caixa e a entrega para um destinatário. Podemos ver que a mensagem está escondida, visto que se encontra trancada no interior da caixa, como queríamos desde o princípio. Também percebemos que não é mais possível ao remetente alterar essa mensagem, pois já entregou a caixa ao destinatário. Posteriormente, quando convier ao remetente, ele entrega a chave para o destinatário possibilitando que ele confira a mensagem. Vemos assim que um esquema de comprometimento funciona em duas fases distintas. Na primeira, que chamamos de fase de comprometimento, um remetente irá se "comprometer" com uma mensagem específica, entregando ao destinatário a "caixa trancada". Uma segunda fase, que chamamos de verificação, ocorrerá quando o remetente entregar ao destinatário a "chave" que possibilitará verificar a mensagem original.

Para formalizarmos este conceito, dizemos que um esquema de comprometimento $\mathcal{C}om$ é uma tupla com dois algoritmos chamados Empenha e Abre, onde Empenha recebe uma mensagem $msg \in \mathcal{M}$, sendo $\mathcal{M}$ o espaço de mensagens, e retorna um par c e d, onde c é um valor de compromisso e d é a chave para recuperar msg com a utilização do algoritmo Abre e o próprio c. Abre retorna msg ou então $\perp$, caso c seja inválido. Em um esquema de comprometimento correto deveremos ter que Abre(Empenha$(msg)) = msg$. Precisamos ainda que este esquema de comprometimento possua as seguintes propriedades:

Ocultação (*hiding*) − Seja $\mathcal{C}om$ um esquema de comprometimento, dizemos que ele possui ocultação se é computacionalmente difícil descobrir qualquer informação sobre msg a partir de c.

Vinculação (*binding*) − Seja $\mathcal{C}om$ um esquema de comprometimento, dizemos que ele possui vinculação se, efetuado Empenha(msg_1) $\rightarrow$ c, d, é computacionalmente difícil formular um valor d' tal que Abre(c,d') = msg_1 ou Abre(c, d') $\neq \perp$.

Em [Halevi e Micali 1996] pode ser visto um modelo de esquema de comprometimento prático que é mostrado seguro e é construído a partir da utilização de funções de hash.

3. Problema $\mathcal{MQ}$ e os Criptossistemas de Chave Pública Multivariável

Os sistemas criptográficos de chave pública amplamente utilizados hoje em dia têm sua segurança baseada na suposição da intratabilidade dos problemas de fatoração de inteiros, no caso de sistemas RSA, e do logaritmo discreto, em sistemas ElGamal ou de Curvas Elípticas. O fato de que tais problemas podem ser resolvidos em tempo polinomial com algoritmos quânticos [Shor 1997], tornaria inseguros os sistemas criptográficos atuais na presença de computadores quânticos com a capacidade adequada. Uma proposta para enfrentar este desafio é a utilização do Problema $\mathcal{MQ}$ como base para o desenvolvimento de sistemas criptográficos de chave pública seguros.

Inicialmente iremos apresentar o problema do Sistema de Equações Polinomiais Multivariáveis Simultâneas, seja $\mathcal{P} = (p_1, \ldots, p_m)$ um sistema de m polinômios de grau d em n variáveis sobre um corpo finito $\mathbb{F}$ de ordem q, o problema do Sistema de Equações Polinomiais Multivariáveis Simultâneas consiste em encontrar $\mathrm{x} = (x_1, \ldots, x_n) \in \mathbb{F}^n$ tal que $\mathcal{P}(\mathrm{x}) = \mathrm{y}$, sendo $\mathrm{y} = (y_1, \ldots, y_m) \in \mathbb{F}^m$:

$$\mathcal{P} = \begin{cases} p_1(x_1, ..., x_n) = y_1 \\ p_2(x_1, ..., x_n) = y_2 \\ \vdots \\ p_m(x_1, ..., x_n) = y_m \end{cases}$$

Quando o grau do sistema de equações $\mathcal{P}$ é igual a 2 $(d = 2)$, chamamos então de Problema $\mathcal{MQ}$. Patarin e Goubin demonstraram em [Patarin e Goubin 1997] que o problema $\mathcal{MQ}$ é NP-Completo, não se conhecendo até hoje nenhum algoritmo, nem mesmo quântico, de tempo polinomial que possa resolver este problema [Bernstein et al. 2009], contribuindo assim para a segurança de sistemas criptográficos baseados nesta primitiva. Estes criptossistemas foram de alguma forma originados do trabalho de Matsumoto e Imai [Matsumoto e Imai 1988] e são conhecidos como MPKC [Ding et al. 2006, Wolf e Preneel 2005, Wolf 2005] (acrônimo da nomenclatura em inglês que significa Criptossistema de Chave Pública Multivariável).

Chamamos o Sistema de Equações Polinomiais Multivariáveis Quadráticas $\mathcal{P}$ de Função $\mathcal{MQ}$ e a denotamos por $\mathcal{MQ}(n, m, \mathbb{F})$ para estabelecer suas propriedades. Uma função $\mathcal{MQ}$ é uma função de via-única (*one-way function*) [Patarin e Goubin 1997].

Uma característica dos MPKC conhecidos atualmente é que nenhum tem sua segurança baseada exclusivamente no problema $\mathcal{MQ}$, sendo a grande maioria dependente também do problema de Isomorfismo de Polinômios (IP), o qual podemos dizer de forma simplificada que, consiste em, dados $\mathcal{P}$ e F, encontrar duas transformações afins S e T tais que $S \circ F \circ T = S(F(T(x)))) = \mathcal{P}(x)$, sendo $\mathcal{P}$, uma função $\mathcal{MQ}$ utilizada como chave pública de um MPKC e F um mapeamento inversível utilizado juntamente com S e T como chave secreta do mesmo criptossistema. Acredita-se que uma instância aleatória do problema IP seja difícil, porém, quando aplicado às atuais $\mathcal{MQ}$-Trapdoor ainda suscita controvérsia quanto à sua intratabilidade, já tendo inclusive possibilitado a quebra de vários esquemas e protocolos criptográficos anteriormente apresentados, como o esquema de assinatura SFlash [Patarin et al. 2001, Courtois et al. 2003, Dubois et al. 2007, Bouillaguet et al. 2011], que chegou a ser recomendado pelo NESSIE. Esta vulnerabilidade existe pois as atuais $\mathcal{MQ}$-Trapdoor possuem esta estrutura específica de construção que consiste na composição de um mapeamento central F de formato determinado, com

duas transformações afins (S e T), resultando em uma forma limitada de função $\mathcal{MQ}$, e que, em consequência, possibilita em alguns casos soluções fáceis desta versão do problema IP.

3.1. Novo Modelo MPKC de Sakumoto-Shirai-Hiwatari

Recentemente, Sakumoto, Shirai e Hiwatari apresentaram em [Sakumoto et al. 2011] dois novos protocolos de identificação de conhecimento-zero (*zero-knowledge*) os quais chamamos de $\mathcal{MQID}-3$ e $\mathcal{MQID}-5$. Estes protocolos se baseiam em um novo modelo de MPKC, o qual tem sua segurança reduzida ao problema $\mathcal{MQ}$, visto que utiliza uma instância aleatória de função $\mathcal{MQ}$, em vez da forma limitada descrita anteriormente. Neste novo modelo uma chave privada s passa a ser os valores das n variáveis nas m equações que compõe a função $\mathcal{MQ}$, isto é, s $= (x_1, ..., x_n) \in \mathbb{F}^n$, sendo a chave pública então o resultado v $= (y_1, ..., y_m) \in \mathbb{F}^m$ e a função $\mathcal{MQ}$ em si passa a ser uma instância aleatória disponível como parâmetro do sistema para todos os usuários. Por se tratar de uma instância aleatória de função $\mathcal{MQ}$, não se consegue construir uma trapdoor a partir dela.

4. Revisão do Esquema de Identificação de Sakumoto-Shirai-Hiwatari

No esquema de identificação de Sakumoto-Shirai-Hiwatari o algoritmo Setup recebe um parâmetro de segurança 1^κ que determina n, m e $\mathbb{F}$ e retorna um parâmetro de sistema $\mathcal{P} \in_R \mathcal{MQ}(n, m, \mathbb{F})$, o qual é uma instância aleatória de função $\mathcal{MQ}$. O algoritmo Gen sorteia uma chave privada aleatória s $\in \mathbb{F}^n$, e executa $\mathcal{P}$(s) =v, onde v será então a chave pública.

O protocolo $\mathcal{MQID}$-3 utiliza uma função bilinear $\mathcal{G}$, que chamamos de forma polar de $\mathcal{P}$, sendo $\mathcal{G}(a, b) = \mathcal{P}(a + b) - \mathcal{P}(a) - \mathcal{P}(b)$, com $a, b \in \mathbb{F}^n$.

Os autores utilizaram uma abordagem de divisão-escolha, onde o segredo é dividido em vários pedaços e o verificador escolhe algum para validar. A ideia básica é que o provador demonstre que possui uma tupla $(r_0, r_1, t_0, t_1, e_0, e_1)$ que satisfaça:

$$\mathcal{G}(t_0, r_1) + e_0 = \mathcal{P}(\mathrm{s}) - \mathcal{P}(r_1) - \mathcal{G}(t_1, r_1) - e_1 \quad (1)$$

$$\text{e} \qquad (t_0, e_0) = (r_0 - t_1, \mathcal{P}(r_0) - e_1) \quad (2)$$

A equação (1) acima vem da seguinte maneira, utilizando-se a bilinearidade de $\mathcal{G}$:

$$\begin{aligned}
\mathcal{G}(r_0, r_1) &= \mathcal{P}(s) - \mathcal{P}(r_0) - \mathcal{P}(r_1) \\
\mathcal{G}(t_0, r_1) + \mathcal{G}(t_1, r_1) &= \mathcal{P}(s) - \mathcal{P}(r_0) - \mathcal{P}(r_1) \\
\mathcal{G}(t_0, r_1) &= \mathcal{P}(s) - \mathcal{P}(r_0) - \mathcal{P}(r_1) - \mathcal{G}(t_1, r_1) \\
\mathcal{G}(t_0, r_1) &= \mathcal{P}(s) - (e_0 + e_1) - \mathcal{P}(r_1) - \mathcal{G}(t_1, r_1) \\
\mathcal{G}(t_0, r_1) + e_0 &= \mathcal{P}(s) - \mathcal{P}(r_1) - \mathcal{G}(t_1, r_1) - e_1
\end{aligned}$$

Para isso a chave secreta s é dividida da forma descrita a seguir. Inicialmente são escolhidos $r_0, t_0 \in_R \mathbb{F}^n$ e $e_0 \in_R \mathbb{F}^m$, e então calculados $r_1 \leftarrow \mathrm{s} - r_0$, $t_1 \leftarrow r_0 - t_0$ e $e_1 \leftarrow \mathcal{P}(r_0) - e_0$, ou seja, s$= r_0 + r_1 = r_1 + t_0 + t_1$ e $\mathcal{P}(r_0) = e_0 + e_1$.

A Figura 1 apresenta o protocolo $\mathcal{MQID}$-3 original.

Entrada do Provador: $((\mathcal{P}, \text{v}), \text{s})$		Entrada do Verificador: $(\mathcal{P}, \text{v})$
Escolhe $r_0, t_0 \in_R \mathbb{F}^n$, $e_0 \in_R \mathbb{F}^m$		
$r_1 \leftarrow \text{s} - r_0$, $t_1 \leftarrow r_0 - t_0$		
$e_1 \leftarrow \mathcal{P}(r_0) - e_0$		
$c_0 \leftarrow Com(r_1, \mathcal{G}(t_0, r_1) + e_0)$		
$c_1 \leftarrow Com(t_0, e_0)$		
$c_2 \leftarrow Com(t_1, e_1)$		
$hc \leftarrow H(c_0, c_1, c_2)$		
	$\xrightarrow{hc}$	
		Escolhe $Ch \in_R \{0, 1, 2\}$
	$\xleftarrow{Ch}$	
Se $Ch = 0, Rsp \leftarrow (r_0, t_1, e_1, c_0)$		
Se $Ch = 1, Rsp \leftarrow (r_1, t_1, e_1, c_1)$		
Se $Ch = 2, Rsp \leftarrow (r_1, t_0, e_0, c_2)$		
	$\xrightarrow{Rsp}$	
		Se $Ch = 0$, utiliza $Rsp = (r_0, t_1, e_1, c_0)$ para verificar:
		$c'_1 \leftarrow Com(r_0 - t_1, \mathcal{P}(r_0) - e_1)$
		$c'_2 \leftarrow Com(t_1, e_1)$
		$hc \stackrel{?}{=} H(c_0, c'_1, c'_2)$
		Se $Ch = 1$, utiliza $Rsp = (r_1, t_1, e_1, c_1)$ para verificar:
		$c'_0 \leftarrow Com(r_1, \text{v} - \mathcal{P}(r_1) - \mathcal{G}(t_1, r_1) - e_1)$
		$c'_2 \leftarrow Com(t_1, e_1)$
		$hc \stackrel{?}{=} H(c'_0, c_1, c'_2)$
		Se $Ch = 2$, utiliza $Rsp = (r_1, t_0, e_0, c_2)$ para verificar:
		$c'_0 \leftarrow Com(r_0, \mathcal{G}(t_0, r_1) + e_0)$
		$c'_1 \leftarrow Com(t_0, e_0)$
		$hc \stackrel{?}{=} H(c'_0, c'_1, c_2)$

Figura 1. Resumo do protocolo de identificação $\mathcal{MQID}$-3 de Sakumoto, Shirai e Hiwatari

O protocolo $\mathcal{MQID}$-3 possui probabilidade de personificação de 2/3 em uma rodada. Por isso, para termos uma probabilidade total de personificação menor ou igual a $2^{-\lambda}$, é preciso repetir o protocolo um total de pelo menos $\lceil \frac{\lambda}{log_2 3 - 1} \rceil$ vezes, como podemos ver abaixo, onde r é o número total de rodadas necessárias:

$$\left(\frac{2}{3}\right)^r \leq 2^{-\lambda}$$
$$r(log_2 2 - log_2 3) \leq -\lambda \cdot log_2 2$$
$$r(1 - log_2 3) \leq -\lambda$$
$$r(log_2 3 - 1) \geq \lambda$$
$$r \geq \frac{\lambda}{log_2 3 - 1}$$

A comunicação em uma rodada é igual a $2n + 5m + 2$ bits, visto que o provador gera um hash hc dos 3 compromissos criados, o qual possui $2m$ bits, e o envia para o verificador, que responde com um desafio Ch de tamanho 2 bits, do qual decorre o envio

de Rsp pelo provador, o qual possui $2n + 3m$ bits. Vemos então que a comunicação total seria de $r \cdot (2n+5m+2)$ bits, ou $52 \cdot (2 \cdot 84+5 \cdot 80+2) = 29640$ bits, com os parâmetros originalmente propostos.

5. $\mathcal{MQID}$-3 Aprimorado

Primeiramente vale destacar que também em [Sakumoto et al. 2011] foi introduzido o protocolo $\mathcal{MQID}$-5, o qual já possui probabilidade de personificação 1/2 em uma rodada. Porém, ele não é canônico [Abdalla et al. 2002], o que impossibilitaria a geração a partir dele de um esquema de assinaturas pelo paradigma da transformação Fiat-Shamir [Fiat e Shamir 1987]. Muito recentemente, Alaoui et al [Alaoui et al. 2012] propuseram uma extensão do Forking Lemma de Pointcheval e Stern [Pointcheval e Stern 1996, Pointcheval e Stern 2000] e da transformação Fiat-Shamir para possibilitar a utilização de protocolos com $2n+1$ passos, utilizando exatamente o protocolo $\mathcal{MQID}$-5 de Sakumoto, Shirai e Hiwatari como exemplo, porém essa assinatura seria teoricamente mais lenta que uma baseada na nossa proposta, visto que a solução derivada do protocolo em 5 passos necessita de $2r$ hashes para simular o verificador, enquanto a nossa utilizaria apenas um hash.

Para conseguirmos aprimorar o protocolo de identificação $\mathcal{MQID}$-3, incrementamos a divisão do segredo de forma a possibilitar duas alternativas exclusivas de verificação. Vimos que no protocolo original a chave privada s é dividida em r_0 e r_1, sendo s$= r_0 + r_1$. E que depois é efetuada a divisão de r_0 em t_0 e t_1 e de $\mathcal{P}(r_0)$ em e_0 e e_1, da mesma forma. Nós mantemos as mesmas divisões originais e acrescentamos a divisão de r_1 em d_0 e d_1 e de $\mathcal{P}(r_1)$ em u_0 e u_1, efetuando o seguinte: escolhemos $d_0 \in_R \mathbb{F}^n$ e $u_0 \in_R \mathbb{F}^m$, e calculamos $d_1 \leftarrow r_1 - d_0$ e $u_1 \leftarrow \mathcal{P}(r_1) - u_0$. Podemos ver então que a Equação (1) em função de r_1 pode ser reescrita em função de r_0: $\mathcal{G}(r_0, d_1) + u_1 = \mathcal{P}(s) - \mathcal{P}(r_0) - \mathcal{G}(r_0, d_0) - u_0$. Assim, propomos que o provador demonstre que possui uma tupla $(r_0, r_1, t_0, t_1, e_0, e_1, d_0, d_1, u_0, u_1)$ que satisfaça (1 e 4) OU (3 e 4):

$$\mathcal{G}(t_0, r_1) + e_0 = \mathcal{P}(s) - \mathcal{P}(r_1) - \mathcal{G}(t_1, r_1) - e_1 \quad (1)$$

$$\mathcal{G}(r_0, d_1) + u_1 = \mathcal{P}(s) - \mathcal{P}(r_0) - \mathcal{G}(r_0, d_0) - u_0 \quad (3)$$

$$(t_0, e_0) = (r_0 - t_1, \mathcal{P}(r_0) - e_1) \text{ E } (d_0, u_0) = (r_1 - d_1, \mathcal{P}(r_1) - u_1) \quad (4)$$

Na Figura 2 detalhamos o protocolo $\mathcal{MQID}$-3 aprimorado com probabilidade de personificação em uma rodada de 1/2.

5.1. Análise da Proposta

Vemos que nosso protocolo aprimorado satisfaz a definição de Correção, pois uma provadora honesta $\mathcal{A}lice$, utilizando sua chave secreta s, sempre será aceita por um verificador honesto $\mathcal{B}eto$.

Percebe-se que se um adversário $\mathcal{C}arlos$ executar o protocolo tentando personificar $\mathcal{A}lice$ sem a chave secreta dela, e utilizando um valor s' $\in_R \mathbb{F}^n$ em substituição, ele irá obter sucesso em 1/2 das vezes. Mais precisamente, sempre que $Ch \in \{1, 2\}$, quando o verificador não utiliza a chave pública na checagem e sim os valores enviados pelo próprio provador. É fato que no caso de $\mathcal{C}arlos$ trapacear para conseguir obter sucesso em um dos desafios onde é utilizada a chave pública de $\mathcal{A}lice$, ele inevitavelmente

Entrada do Provador: $((\mathcal{P}, \text{v}), \text{s})$ Entrada do Verificador: $(\mathcal{P}, \text{v})$

$c_0 \leftarrow Com(r_0, \mathcal{G}(r_0, d_1) + u_1)$
$c_1 \leftarrow Com(r_1, \mathcal{G}(t_0, r_1) + e_0)$
$c_2 \leftarrow Com(t_0, e_0)$
$c_3 \leftarrow Com(t_1, e_1)$
$c_4 \leftarrow Com(d_0, u_0)$
$c_5 \leftarrow Com(d_1, u_1)$
$hc \leftarrow H(c_0, c_1, c_2, c_3, c_4, c_5)$

$\xrightarrow{hc}$

Escolhe $Ch \in_R \{0, 1, 2, 3\}$

$\xleftarrow{Ch}$

Se $Ch = 0, Rsp \leftarrow (r_1, t_1, e_1, d_0, u_0, c_0, c_2)$
Se $Ch = 1, Rsp \leftarrow (r_1, t_0, e_0, d_1, u_1, c_0, c_3)$
Se $Ch = 2, Rsp \leftarrow (r_0, t_0, e_0, d_1, u_1, c_1, c_4)$
Se $Ch = 3, Rsp \leftarrow (r_0, t_1, e_1, d_0, u_0, c_1, c_5)$

$\xrightarrow{Rsp}$

Se $Ch = 0$, utiliza $Rsp = (r_1, t_1, e_1, d_0, u_0, c_0, c_2)$ para verificar:
$c'_1 \leftarrow Com(r_1, \text{v} - \mathcal{P}(r_1) - \mathcal{G}(t_1, r_1) - e_1)$
$c'_3 \leftarrow Com(t_1, e_1)$
$c'_4 \leftarrow Com(d_0, u_0)$
$c'_5 \leftarrow Com(r_1 - d_0, \mathcal{P}(r_1) - u_0)$
$hc \stackrel{?}{=} H(c_0, c'_1, c_2, c'_3, c'_4, c'_5)$

Se $Ch = 1$, utiliza $Rsp = (r_1, t_0, e_0, d_1, u_1, c_0, c_3)$ para verificar:
$c'_1 \leftarrow Com(r_1, \mathcal{G}(t_0, r_1) + e_0)$
$c'_2 \leftarrow Com(t_0, e_0)$
$c'_4 \leftarrow Com(r_1 - d_1, \mathcal{P}(r_1) - u_1)$
$c'_5 \leftarrow Com(d_1, u_1)$
$hc \stackrel{?}{=} H(c_0, c'_1, c'_2, c_3, c'_4, c'_5)$

Se $Ch = 2$, utiliza $Rsp = (r_0, t_0, e_0, d_1, u_1, c_1, c_4)$ para verificar:
$c'_0 \leftarrow Com(r_0, \mathcal{G}(r_0, d_1) + u_1)$
$c'_2 \leftarrow Com(t_0, e_0)$
$c'_3 \leftarrow Com(r_0 - t_0, \mathcal{P}(r_0) - e_0)$
$c'_5 \leftarrow Com(d_1, u_1)$
$hc \stackrel{?}{=} H(c'_0, c_1, c'_2, c'_3, c_4, c'_5)$

Se $Ch = 3$, utiliza $Rsp = (r_0, t_1, e_1, d_0, u_0, c_1, c_5)$ para verificar:
$c'_0 \leftarrow Com(r_0, \text{v} - \mathcal{P}(r_0) - \mathcal{G}(r_0, d_0) - u_0)$
$c'_2 \leftarrow Com(r_0 - t_1, \mathcal{P}(r_0) - e_1)$
$c'_3 \leftarrow Com(t_1, e_1)$
$c'_4 \leftarrow Com(d_0, u_0)$
$hc \stackrel{?}{=} H(c'_0, c_1, c'_2, c'_3, c'_4, c_5)$

Figura 2. Protocolo de Identificação $\mathcal{MQID}$-3 Aprimorado

causará a falha em um dos desafios que ele normalmente passaria, ou seja, ele sempre permanecerá com uma chance de personificação igual a 1/2 por rodada. Para ilustrarmos essa

situação vamos considerar que $\mathcal{C}arlos$ gere $c_0 \leftarrow Com(r'_0, \text{v} - \mathcal{P}(r'_0) - \mathcal{G}(r'_0, d'_0) - u'_0)$ e $c_1 \leftarrow Com(r'_1, \text{v} - \mathcal{P}(r'_1) - \mathcal{G}(t'_1, r'_1) - e'_1)$ utilizando a chave pública da entidade que ele quer personificar. Neste caso, se $Ch \in \{0, 3\}$ $\mathcal{C}arlos$ terá sucesso na validação, pois o verificador $\mathcal{B}eto$ irá efetuar rigorosamente a mesma conta, obtendo o mesmo resultado. Porém, a chance continua sendo 1/2 visto que não será possível satisfazer, neste caso, as checagens de c_0 e c_1 quando $Ch \in \{1, 2\}$, ocorrendo o mesmo de forma análoga para outras alternativas de trapaça. Por uma questão de espaço não podemos detalhar neste artigo todos os casos onde um adversário tentando forjar a validade dos dados para um determinado desafio acaba, inevitavelmente, por impossibilitar a verificação de um outro, permanecendo sempre com uma probabilidade 1/2 de personificação em uma rodada. Estas demonstrações constarão de um futuro trabalho completo.

Vamos demonstrar que nosso protocolo é de conhecimento-zero, visto que um verificador trapaceiro utilizando um simulador $\mathcal{S}$, sem conhecimento da chave secreta, gera uma transcrição do protocolo estatisticamente indistinguível de uma transcrição gerada pela interação de uma provadora honesta $\mathcal{A}lice$ e um verificador honesto $\mathcal{B}eto$. E ainda, que nosso protocolo possui solidez, uma vez que dadas duas execuções do protocolo com o mesmo início (ou seja, os mesmos valores de compromisso) e continuações diferentes (ou seja, Ch e Rsp diferentes) é possível descobrir o segredo s ou então o esquema de comprometimento está quebrado, não possuindo vinculação, visto que teria gerado valores iguais de compromisso a partir de valores diferentes de msg.

Teorema 1 *O Protocolo $\mathcal{MQID}$-3 aprimorado é de conhecimento-zero estatístico quando o esquema de comprometimento $\mathcal{C}om$possui ocultação estatística.*

Demonstração: Seja $\mathcal{S}$ um simulador que irá personificar uma entidade qualquer utilizando apenas a chave pública v dessa entidade e possuindo acesso a um oráculo $\mathcal{O}$ que indica por meio de um bit se a próxima verificação será em função de r_1 ou de r_0, ou seja, se o próximo desafio a ser recebido será $Ch \in \{0, 1\}$ ou $Ch \in \{2, 3\}$, respectivamente. A cada rodada do protocolo, $\mathcal{S}$ consulta $\mathcal{O}$ e recebe dele um bit Ch^* indicando que $Ch^* = 1 \rightarrow Ch \in \{0, 1\}$, $Ch^* = 0 \rightarrow Ch \in \{2, 3\}$. $\mathcal{S}$ então escolhe $\text{s}', r'_0, t'_0, d'_0 \in_R \mathbb{F}^n$, $e'_0, u'_0 \in_R \mathbb{F}^m$ e prepara $r'_1 \leftarrow s' - r'_0$, $t'_1 \leftarrow r'_0 - t'_0$ e $d'_1 \leftarrow r'_1 - d'_0$. Se $Ch^* = 0$ então calcula $e'_1 \leftarrow v - \mathcal{P}(s') + \mathcal{P}(r'_1) - e'_0$ e $u'_1 \leftarrow \mathcal{P}(r'_1) - u'_0$, senão $\mathcal{S}$ faz $e'_1 \leftarrow \mathcal{P}(r'_0) - e'_0$ e $u'_1 \leftarrow v - \mathcal{P}(s') + \mathcal{P}(r'_0) - u'_0$. Finalmente, $\mathcal{S}$ gera os valores de compromisso e os envia para o verificador: $c_0 \leftarrow Com(r'_0, \mathcal{G}(r'_0, d'_1) + u'_1)$, $c_1 \leftarrow Com(r'_1, \mathcal{G}(t'_0, r'_1) + e'_0)$, $c_2 \leftarrow Com(t'_0, e'_0)$, $c_3 \leftarrow Com(t'_1, e'_1)$, $c_4 \leftarrow Com(d'_0, u'_0)$ e $c_5 \leftarrow Com(d'_1, u'_1)$.

Após receber Ch, $\mathcal{S}$ responde normalmente com seus valores já calculados, ou seja, se $Ch = 0, Rsp \leftarrow (r'_1, t'_1, e'_1, d'_0, u'_0, c_0, c_2)$, ou se $Ch = 1, Rsp \leftarrow (r'_1, t'_0, e'_0, d'_1, u'_1, c_0, c_3)$, ou se $Ch = 2, Rsp \leftarrow (r'_0, t'_0, e'_0, d'_1, u'_1, c_1, c_4)$, ou se $Ch = 3, Rsp \leftarrow (r'_0, t'_1, e'_1, d'_0, u'_0, c_1, c_5)$.

Verificamos que nos casos em que $\mathcal{O}$ prediz corretamente o desafio, ou seja, em que $Ch^* = 1$ e $Ch \in \{0, 1\}$, ou então, $Ch^* = 0$ e $Ch \in \{2, 3\}$, os valores enviados por $\mathcal{S}$ serão aceitos por qualquer verificador executando normalmente o protocolo. Podemos confirmar o caso concreto quando $Ch^* = 1$ e $Ch = 0$, temos $e'_1 = \text{v} - \mathcal{P}(\text{s}') + \mathcal{P}(r'_1) - e'_0$, logo c_1 ao ser verificado será válido pois teremos então $\text{v} - \mathcal{P}(r'_1) - \mathcal{G}(t'_1, r'_1) - e'_1 = \mathcal{G}(t'_0, r'_1) + e_0$. O caso de $Ch^* = 1$ e $Ch = 1$ é mais simples, pois o verificador não utiliza a chave pública v, fazendo a reconstrução dos compromissos com os mesmos valores preparados pelo simulador, o que obviamente redunda no aceite da verificação. Para os

casos em que $Ch^* = 0$, e consequentemente $Ch \in \{2, 3\}$, teremos a rigor a mesma situação que acabamos de enumerar, porém com as verificações em função r_0.

Vemos assim que um verificador desonesto utilizando $\mathcal{S}$ pode gerar uma transcrição do protocolo que é indistinguível de uma gerada pela interação de uma provadora honesta $\mathcal{A}lice$ e um verificador honesto $\mathcal{B}eto$, comprovando assim que um adversário não adquire conhecimento útil a partir de transcrições do protocolo, desde que o esquema de comprometimento $\mathcal{C}om$ possua ocultação estatística.

Teorema 2 *O Protocolo $\mathcal{MQID}$-3 aprimorado é argumento de conhecimento com probabilidade de erro 1/2 em uma rodada quando o esquema de comprometimento $\mathcal{C}om$ possui vinculação computacional.*

Demonstração: Sejam (hc_0, Ch_0, Rsp_0), (hc_1, Ch_1, Rsp_1), (hc_2, Ch_2, Rsp_2) e (hc_3, Ch_3, Rsp_3) quatro transcrições da execução de $\mathcal{MQID}$-3 Aprimorado, tais que $Ch_i = i$ e $Dec(\mathcal{P}, \mathrm{v}, hc_i, Ch_i, Rsp_i) = 1$. Sejam $c_0, c_1, c_2, c_3, c_4, c_5$ valores de compromisso gerados de acordo com o estabelecido na definição do protocolo $\mathcal{MQID}$-3 Aprimorado, e ainda, sejam $hc_0 = hc_1 = hc_2 = hc_3 = H(c_0, c_1, c_2, c_3, c_4, c_5)$ e $Rsp_0 = (r_1^{(0)}, t_1^{(0)}, e_1^{(0)}, d_0^{(0)}, u_0^{(0)}, c_0, c_2)$, $Rsp_1 = (r_1^{(1)}, t_0^{(1)}, e_0^{(1)}, d_1^{(1)}, u_1^{(1)}, c_0, c_3)$, $Rsp_2 = (r_0^{(2)}, t_1^{(2)}, e_1^{(2)}, d_0^{(2)}, u_0^{(2)}, c_1, c_4)$ e $Rsp_3 = (r_0^{(3)}, t_0^{(3)}, e_0^{(3)}, d_1^{(3)}, u_1^{(3)}, c_1, c_5)$, temos então que:

$$c_0 = \mathcal{C}om(r_0^{(2)}, \mathcal{G}(r_0^{(2)}, d_1^{(2)}) + u_1^{(2)}) = \mathcal{C}om(r_0^{(3)}, \mathrm{v} - \mathcal{P}(r_0^{(3)}) - \mathcal{G}(r_0^{(3)}, d_0^{(3)}) - u_0^{(3)}) \quad \text{(a)}$$

$$c_1 = \mathcal{C}om(r_1^{(0)}, \mathrm{v} - \mathcal{P}(r_1^{(0)}) - \mathcal{G}(t_1^{(0)}, r_1^{(0)}) - e_1^{(0)}) = \mathcal{C}om(r_1^{(1)}, \mathcal{G}(t_0^{(1)}, r_1^{(1)}) + e_0^{(1)}) \quad \text{(b)}$$

$$c_2 = \mathcal{C}om(t_0^{(1)}, e_0^{(1)}) = \mathcal{C}om(t_0^{(2)}, e_0^{(2)}) = \mathcal{C}om(r_0^{(3)} - t_1^{(3)}, \mathcal{P}(r_0^{(3)}) - e_1^{(3)}) \quad \text{(c)}$$

$$c_3 = \mathcal{C}om(t_1^{(0)}, e_1^{(0)}) = \mathcal{C}om(r_0^{(2)} - t_0^{(2)}, \mathcal{P}(r_0^{(2)}) - e_0^{(2)}) = \mathcal{C}om(t_1^{(3)}, e_1^{(3)}) \quad \text{(d)}$$

$$c_4 = \mathcal{C}om(d_0^{(0)}, u_0^{(0)}) = \mathcal{C}om(r_1^{(1)} - d_1^{(1)}, \mathcal{P}(r_1^{(1)}) - u_1^{(1)}) = \mathcal{C}om(d_0^{(3)}, u_0^{(3)}) \quad \text{(e)}$$

$$c_5 = \mathcal{C}om(r_1^{(0)} - d_0^{(0)}, \mathcal{P}(r_1^{(0)}) - u_0^{(0)}) = \mathcal{C}om(d_1^{(1)}, u_1^{(1)}) = \mathcal{C}om(d_1^{(2)}, u_1^{(2)}) \quad \text{(f)}$$

Das equações (a), (b), (c), (d), (e) e (f) resultam as igualdades a seguir ou então $\mathcal{C}om$ não possui vinculação, visto que teria gerado valores iguais de compromisso a partir de valores diferentes de msg. Desta forma temos: $r_1^{(0)} = r_1^{(1)}$, $r_0^{(2)} = r_0^{(3)}$, $t_0^{(1)} = t_0^{(2)} = r_0^{(3)} - t_1^{(3)}$, $t_1^{(0)} = r_0^{(2)} - t_0^{(2)} = t_1^{(3)}$, $e_0^{(1)} = e_0^{(2)} = \mathcal{P}(r_0^{(3)}) - e_1^{(3)}$, $e_1^{(0)} = \mathcal{P}(r_0^{(2)}) - e_0^{(2)} = e_1^{(3)}$, $d_0^{(0)} = r_1^{(1)} - d_1^{(1)} = d_0^{(3)}$, $r_0^{(0)} - d_0^{(0)} = d_1^{(1)} = d_1^{(2)}$, $u_0^{(0)} = \mathcal{P}(r_1^{(1)}) - u_1^{(1)} = u_0^{(3)}$, $\mathcal{P}(r_1^{(0)}) - u_0^{(0)} = u_1^{(1)} = u_1^{(2)}$.

A partir de (a) e (b) nós temos que $\mathrm{v} = \mathcal{G}(r_0^{(2)}, d_1^{(2)}) + u_1^{(2)} + \mathcal{P}(r_0^{(3)}) + \mathcal{G}(r_0^{(3)}, d_0^{(3)}) + u_0^{(3)} = \mathcal{G}(t_0^{(1)}, r_1^{(1)}) + e_0^{(1)} + \mathcal{P}(r_1^{(0)}) + \mathcal{G}(t_1^{(0)}, r_1^{(0)}) + e_1^{(0)})$.

Das equações e igualdades citadas acima podemos verificar que:

$$t_0^{(1)} + t_1^{(0)} = r_0^{(3)} - t_1^{(3)} + t_1^{(0)} = r_0^{(3)}$$
$$e_0^{(1)} + e_1^{(0)} = \mathcal{P}(r_0^{(3)}) - e_1^{(3)} + e_1^{(0)} = \mathcal{P}(r_0^{(3)})$$
$$d_0^{(3)} + d_1^{(2)} = r_1^{(1)} - d_1^{(1)} + d_1^{(2)} = r_1^{(1)}$$
$$u_0^{(3)} + u_1^{(2)} = \mathcal{P}(r_1^{(1)}) - u_1^{(1)} + u_1^{(2)} = \mathcal{P}(r_1^{(1)})$$
$$\mathcal{G}(r_0^{(2)}, d_1^{(2)}) + \mathcal{G}(r_0^{(3)}, d_0^{(3)}) = \mathcal{G}(r_0^{(3)}, r_1^{(1)})$$
$$\mathcal{G}(t_0^{(1)}, r_1^{(1)}) + \mathcal{G}(t_1^{(0)}, r_1^{(0)}) = \mathcal{G}(r_0^{(3)}, r_1^{(0)})$$

Chegamos então a v $= \mathcal{G}(r_0^{(3)}, r_1^{(0)}) + \mathcal{P}(r_0^{(3)}) + \mathcal{P}(r_1^{(0)}) = \mathcal{P}(r_0^{(3)} + r_1^{(0)})$, confirmando assim que poderíamos recuperar a chave secreta s com $r_0^{(3)} + r_1^{(0)}$.

5.2. Comparação com o original

Em [Sakumoto et al. 2011], Sakumoto, Shirai e Hiwatari incluíram uma comparação da eficiência de $\mathcal{MQID}$-3 com outros protocolos de identificação em 3 passos baseados nos problemas SD binário, CLE e PP. Não vimos razão para repetir essa comparação aqui, uma vez que nosso foco, como já dito, é a diminuição da comunicação total do protocolo de Sakumoto *et al*. Por isso, vamos restringir esta análise comparativa ao tamanho da comunicação do nosso protocolo aprimorado ante ao originalmente apresentado.

Em comparação ao protocolo $\mathcal{MQID}$-3 original, vamos demonstrar que nossa versão aprimorada alcança uma comunicação 9,5% menor para os parâmetros sugeridos por Sakumoto *et al*, apesar de aumentar o tráfego em uma rodada. Este ganho é resultado da diminuição do número de rodadas para o mesmo nível de segurança, visto que conseguimos uma probabilidade de personificação em uma rodada de 1/2, contra 2/3 do protocolo $\mathcal{MQID}$-3.

Como já vimos na revisão do protocolo original, o $\mathcal{MQID}$-3 precisa de $\lceil \frac{\lambda}{log_2 3-1} \rceil$ repetições para alcançar uma probabilidade total de personificação menor que $2^{-\lambda}$, porém nosso protocolo aprimorado, por ter uma probabilidade 1/2 em uma rodada, precisa de apenas λ rodadas. Vemos assim que o protocolo original necessita aproximadamente 71% mais rodadas para o mesmo nível de segurança.

No protocolo original, lembrando que obrigatoriamente estamos sempre considerando a utilização da extensão de [Stern 2006], conforme já descrito anteriormente neste texto e também explicitado no último paragrafo do item 3 de [Sakumoto et al. 2011], temos que o provador gera 3 compromissos e envia um hash hc da concatenação dos mesmos para o verificador, que responde com um desafio Ch do qual decorre o envio de Rsp pelo provador. O hash dos compromissos (hc) possui o tamanho de $2m$ bits, Ch ocupa 2 bits e Rsp é igual a $2n + 3m$ bits, totalizando assim $2n + 5m + 2$ bits trafegados em uma rodada. Nosso protocolo gera 6 compromissos inicialmente, efetuando o envio de um hash hc da mesma forma já citada, um desafio de mesmo tamanho e nosso Rsp possui $3n + 6m$ bits, perfazendo um total de $3n + 8m + 2$ bits. Considerando agora a comunicação total para uma execução com probabilidade total de personificação menor que $2^{-\lambda}$, chegamos ao total de $\lambda \cdot (3n + 8m + 2)$ para o nosso protocolo aprimorado, enquanto o original totaliza $1,71\lambda \cdot (2n + 5m + 2) = \lambda \cdot (3,42n + 8,55m + 3,42)$. Considerando n=m temos nossa proposta alcançando um tráfego de dados aproximadamente 8% menor. Utilizando os parâmetros propostos pelos autores originais, $n = 84$ e $m = 80$, $\mathcal{MQID}$-3 dispende 570 bits por rodada, enquanto nosso protocolo utiliza 894, porém, para uma segurança igual a 2^{-30} o protocolo original utiliza 52 rodadas, enquanto o nosso necessita apenas de 30. Assim, teríamos uma comunicação total de 26820 bits com nosso protocolo aprimorado contra 29640 bits de $\mathcal{MQID}$-3, ou seja, uma redução de 9,5%.

6. Considerações Finais

Neste artigo, apresentamos um novo protocolo de identificação no modelo de chave pública baseado no problema $\mathcal{MQ}$, que é um aprimoramento do protocolo $\mathcal{MQID}$-3 descrito em [Sakumoto et al. 2011]. A proposta é fundamentada no emprego da forma polar da

função $\mathcal{MQ}$ sugerida por esses autores, porém adota uma divisão diferente da chave secreta. Como resultado, obtivemos um protocolo que apresenta probabilidade 1/2 para personificação em uma rodada, contra 2/3 do original, diminuindo o número total de rodadas necessárias para o mesmo nível de segurança e alcançando uma redução de 9,5% da comunicação necessária em uma execução, considerando os parâmetros de segurança propostos originalmente.

Agradecimento

Gostaríamos de registrar um agradecimento especial ao professor Paulo S. L. M. Barreto, da Escola Politécnica (USP), pelas valiosas sugestões que muito contribuíram para o aprimoramento deste trabalho.

Referências

[Abdalla et al. 2002] Abdalla, M., An, J. H., Bellare, M. e Namprempre, C. (2002). From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, EUROCRYPT '02, pages 418–433, London, UK. Springer-Verlag.

[Alaoui et al. 2012] Alaoui, S. M. E. Y., Dagdelen, O., Véron, P., Galindo, D. e Cayrel, P.-L. (2012). Extended security arguments for signature schemes. In *Proceedings of the 5th international conference on Cryptology in Africa*, AFRICACRYPT'12, pages 19–34, Berlin, Heidelberg. Springer-Verlag.

[Bellare e Rogaway 1993] Bellare, M. e Rogaway, P. (1993). Random oracles are practical: a paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and communications security*, CCS '93, pages 62–73, New York, NY, USA. ACM.

[Bernstein et al. 2009] Bernstein, D. J., Buchmann, J. e Dahmen, E., editors (2009). *Post-Quantum Cryptography*. Springer.

[Bouillaguet et al. 2011] Bouillaguet, C., Faugère, J.-C., Fouque, P.-A. e Perret, L. (2011). Practical cryptanalysis of the identification scheme based on the isomorphism of polynomial with one secret problem. In *Proceedings of the 14th international conference on Practice and theory in public key cryptography conference on Public key cryptography*, PKC'11, pages 473–493, Berlin, Heidelberg. Springer-Verlag.

[Courtois et al. 2003] Courtois, N. T., Goubin, L. e Patarin, J. (2003). SFLASHv3, a fast asymmetric signature scheme. *IACR Cryptology ePrint Archive*, 2003:211.

[Ding et al. 2006] Ding, J., Gower, J. E. e Schmidt, D. (2006). *Multivariate Public Key Cryptosystems*, volume 25 of *Advances in Information Security*. Springer.

[Dubois et al. 2007] Dubois, V., Fouque, P.-A., Shamir, A. e Stern, J. (2007). Practical cryptanalysis of SFLASH. In *Proceedings of Advances in Cryptology–CRYPTO '07*. Springer-Verlag.

[Fiat e Shamir 1987] Fiat, A. e Shamir, A. (1987). How to prove yourself: Practical solutions to identification and signature problems. In *Proceedings of Advances in Cryptology–CRYPTO '86*, pages 186–194, London, UK, UK. Springer-Verlag.

[Garey e Johnson 1979] Garey, M. R. e Johnson, D. S. (1979). *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman.

[Halevi e Micali 1996] Halevi, S. e Micali, S. (1996). Practical and provably-secure commitment schemes from collision-free hashing. In *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '96, pages 201–215, London, UK, UK. Springer-Verlag.

[Matsumoto e Imai 1988] Matsumoto, T. e Imai, H. (1988). Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Proceedings of Advances in Cryptology-EUROCRYPT '88*, pages 419–453. Springer-Verlag New York, Inc.

[Patarin et al. 2001] Patarin, J., Courtois, N. e Goubin, L. (2001). Flash, a fast multivariate signature algorithm. In *Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA*, CT-RSA 2001, pages 298–307, London, UK, UK. Springer-Verlag.

[Patarin e Goubin 1997] Patarin, J. e Goubin, L. (1997). Trapdoor one-way permutations and multivariate polynomials. In Han, Y., Okamoto, T. e Qing, S., editors, *Information and Communications Security*, volume 1334 of *Lecture Notes in Computer Science*, pages 356–368. Springer Berlin / Heidelberg.

[Petzoldt et al. 2011] Petzoldt, A., Thomae, E., Bulygin, S. e Wolf, C. (2011). Small public keys and fast verification for multivariate quadratic public key systems. In *Proceedings of the 13th international conference on Cryptographic hardware and embedded systems*, CHES'11, pages 475–490, Berlin, Heidelberg. Springer-Verlag.

[Pointcheval e Stern 1996] Pointcheval, D. e Stern, J. (1996). Security proofs for signature schemes. In *Proceedings of the 15th annual international conference on Theory and application of cryptographic techniques*, EUROCRYPT'96, pages 387–398, Berlin, Heidelberg. Springer-Verlag.

[Pointcheval e Stern 2000] Pointcheval, D. e Stern, J. (2000). Security arguments for digital signatures and blind signatures. *J. Cryptology*, 13(3):361–396.

[Sakumoto et al. 2011] Sakumoto, K., Shirai, T. e Hiwatari, H. (2011). Public-key identification schemes based on multivariate quadratic polynomials. In Rogaway, P., editor, *Advances in Cryptology CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 706–723. Springer Berlin / Heidelberg.

[Shor 1997] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509.

[Stern 2006] Stern, J. (2006). A new paradigm for public key identification. *IEEE Transactions on Information Theory*, 42(6):1757–1768.

[Wolf 2005] Wolf, C. (2005). *Multivariate Quadratic Polynomials in Public Key Cryptography*. PhD thesis, Katholieke Universiteit Leuven.

[Wolf e Preneel 2005] Wolf, C. e Preneel, B. (2005). Taxonomy of public key schemes based on the problem of multivariate quadratic equations. *IACR Cryptology ePrint Archive*, 2005:77.

