Como vazar uma mensagem de forma anônima e depois resgatar a autoria

José Arteiro Frota Filho e José Cláudio do Nascimento

***Resumo*— Esquemas de assinaturas em anel são usados para produzir uma assinatura que representa um conjunto de indivíduos mantendo o anonimato daquele que gera a assinatura. Em outras palavras, dentre um conjunto de pessoas, qualquer uma delas pode gerar tal assinatura, ou seja, somente indivíduos do conjunto podem gerá-la. Neste trabalho, uma assinatura em anel é gerada usando a propriedade de não localidade da mecânica quântica. Assim, um delator pode escolher se pode ou não revelar a sua autoria na assinatura após a solução de um conflito.**

***Palavras-Chave*— Dispositivo quântico à prova de falsificação, prova de conhecimento nulo, isomorfismo de grafos, informação quântica.**

***Abstract*— Ring signature schemes are used to produce a signature that represents a set of individuals while maintaining the anonymity of the one who generates the signature. In other words, among a group of people, any of them may generate such signature, that is, only individuals inside group can generate it. In this paper, a ring signature is generated using the property of non-locality of quantum mechanics. So, a taleteller can choose whether or not to reveal his authorship after the soluction in a conflict.**

***Keywords*— quantum tamper-proof device, zero knowledge proof, graph isomorfism, quantum information.**

I. INTRODUÇÃO

O problema tratado neste trabalho começa em um cenário de criptografia assimétrica, usando o conceito de funções *trapdoor*, em que cada usuário publica uma chave pública e guarda em sigilo uma chave privada. Agora, imaginemos o seguinte cenário: Os membros de uma instituição $\mathcal{A}$ usam criptografia assimétrica para uma comunicação secreta entre eles na rede. Portanto, cada membro da instituição possui uma chave pública P_i que lhe permite cifrar em tempo polinomial qualquer string x_i, $g_{P_i}(x_i) = y_i$. O i-ésimo membro guarda em segredo uma chave secreta S_i, da qual, ele consegue calcular em tempo hábil o resultado inverso, $g_{S_i}(y_i) = x_i$.

Dentro desse cenário, vamos imaginar a seguinte situação: a Instituição $\mathcal{A}$ está em negociação com uma outra Instituição $\mathcal{B}$ para a assinatura de um acordo entre elas. Na negociação, as duas partes tomam a decisão de assinar um acordo dentro das próximas horas. Um conjunto de membros dentro da Instituição $\mathcal{A}$ tem acesso a dados internos que, vindo a público, impedem a assinatura do acordo e geram um conflito entre as duas partes no tribunal. Dentro da Instituição $\mathcal{A}$ existe um membro que deseja revelar uma informação secreta valiosa ao público (na internet) a respeito das transações da instituição. Ao revelar esta informação, o delator provoca um conflito entre as instituições $\mathcal{A}$ e $\mathcal{B}$, em que ele pode ser beneficiado ou penalizado. Dependendo de qual das partes vai vencer o conflito nos tribunais, o delator busca realizar uma assinatura que satisfaça os seguintes casos:

1) Se ele for descoberto como delator e a Instituição $\mathcal{A}$ ganhar o conflito no tribunal, ele será penalizado. Nesse caso, o interesse do membro da Instituição $\mathcal{A}$ é preservar o seu anonimato para não ser penalizado. Portanto, ninguém deve saber qual dos membros foi o delator, mas todo o público deve ter certeza de que a informação saiu de dentro da Instituição $\mathcal{A}$ para dar credibilidade à informação.
2) Se a instituição $\mathcal{B}$ ganhar o conflito, ele será beneficiado. Nesse caso, é interesse do delator que ele revele a sua identidade.

Para proteger-se da Instituição $\mathcal{A}$, o delator aplica o esquema de assinaturas em anel apresentado em [1]. O jornal de publicação dessa notícia precisa ter certeza de que essa informação veio de um membro da Instituição. Caso a Instituição $\mathcal{A}$ vença o conflito, o delator precisa ter certeza de que o seu anonimato será preservado, mesmo que o jornalista seja obrigado a revelar a fonte em um tribunal. Na abordagem proposta em [1], o informante envia a história ao jornalista assinada com um esquema de assinaturas em anel, em que o delator usa a assinatura de todos os membros da Instituição $\mathcal{A}$, de forma a ser computacionalmente indistinguível qual dos membros tenha produzido a assinatura. Embora a assinatura seja construída pelas funções públicas dos membros da Instituição $\mathcal{A}$, somente quem pode calcular a inversa é capaz de produzir a assinatura em anel. O jornalista pode verificar o anel de assinaturas na mensagem e saber que ela, definitivamente, veio de um membro da Instituição $\mathcal{A}$. Ele pode até mesmo postar a assinatura em anel em seu trabalho ou página da web, para provar aos seus leitores que a história veio de uma fonte confiável. No entanto, nem ele, nem seus leitores podem determinar a verdadeira origem do vazamento, já que, o delator tem proteção perfeita, mesmo que o jornalista seja forçado mais tarde a revelar a sua "fonte" a um juiz.

No cenário desse protocolo também há uma entidade confiável que fornece partículas de pares de Bell. Para cada par, a entidade fornece uma partícula e guarda a outra em seu laboratório. Também ela não permite que qualquer usuário insira uma partícula em seu laboratório, ou seja, nenhum usuário pode ter acesso aos estados quânticos internos da entidade. Além disso, um estado quântico só é publicado quando existe uma solicitação do usuário para tal atitude. Assim, vamos considerar que a entidade compartilha $(r-1)b$

José Arteiro Frota Filho e José Cláudio do Nascimento, Departamento de Engenharia Elétirca, Campus Sobral, Universidade Federal do Ceará, Sobral, Brasil, E-mails: claudio.nasce@gmail.com. Este trabalho foi parcialmente financiado pela CAPES, FUNCAP e CNPq.

pares de Bell com o membro delator,

$$\left(\frac{|00\rangle_{E,T_s}+|11\rangle_{E,T_s}}{\sqrt{2}}\right)^{(r-1)b}. \quad (1)$$

Consideramos que o membro delator $T_s \in \{T_1, T_2, \dots T_r\}$ é um dentre os r membros da Instituição $\mathcal{A}$. Assim, dada uma mensagem m, uma seqüência de chaves públicas P_1, P_2, ..., P_r (cada chave púbica P_i específica uma função de sentido único g_i), uma seqüência de chaves secretas S_1, S_2, ..., S_r (cada chave privada S_i específica a função inversa g_i^{-1}), então o delator, para causar a crise, gera uma assinatura que é calculada da seguinte forma:

Protocolo 1: Cálculo da assinatura com anonimato controlado pelo assinante.

1) O assinante calcula um valor k que é o hash da mensagem m, $h(m) = k$ (h é uma função hash predeterminada). O valor de k é para selecionar uma função de encriptação E_k como em [2];
2) O assinante escolhe aleatoriamente com distribuição de probabilidade uniforme um valor de inicialização $v \in \{0,1\}^b$;
3) O assinante tem v como uma sequência de bases de medição para as partículas que estão em seu laboratório. Portanto, as medições são realizadas da seguinte maneira:
   - Para $i = 1, 2, \dots, r-1$ faça:
   - Para $j = 1, 2, \dots, b$ faça:
     a) Se $v_j = 0$, então a medição é feita na base retangular, $\{|0\rangle, |1\rangle\}$. O resultado é atribuído em x_{ij};
     b) Se $v_j = 1$ a medição é feita na base diagonal, $\{|+\rangle, |-\rangle\}$. O resultado é atribuído em x_{ij}.

   Com distribuição de probabilidade uniforme, $r-1$ entradas x_i, $1 \le i \le r-1$ são obtidas nas medições, tal que $x_i \in \{0,1\}^b$. Assim o assinante delator computa $y_i = g_i(x_i)$;
4) O delator soluciona a equação do anel para y_s

$$C_{(k,v)}(y_1, y_2, y_3, ..., y_r) = v.$$

   O delator T_s é capaz de resolver a equação em tempo hábil se ele for capaz de calcular $g_s^{-1}(y_s) = x_s$. Ele só é capaz desse feito se possuir a chave secreta S_s.
5) A mensagem m é assinada com a tupla $(P_1, ..., P_r;\ v;\ x_1, ..., x_r)$.

A assinatura pode ser verificada para dois diferentes casos. No primeiro caso, a verificação é feita de forma pública em que o delator permanece como autor anônimo da mensagem. No segundo caso, ele pode sair do anonimato apresentando uma prova que está correlacionada com a assinatura, de forma que qualquer pessoa fique convencida de que a assinatura foi gerada por ele.

Protocolo 2: Verificação da validade da assinatura $(P_1, ..., P_r;\ v;\ x_1, ..., x_r)$.

1) Para $i = 1, 2, \dots, r$ o verificador calcula $g_i(x_i)$;
2) O verificador calcula o $h(m) = k$ para obter E_k;
3) O verificador checa se todo $g_i(x_i)$ satisfaz $C_{(k,v)}\left(g_1(x_1), \dots, g_r(x_r)\right) = v$
4) Finalmente, se o grupo $\mathcal{A}$ vencer o conflito, T_s não se manifesta. Caso contrário, quando o grupo $\mathcal{B}$ vence o conflito, então ele afirma ter $b(r-1)$ partículas de pares de Bell na entidade confiável e autoriza esta a realizar medições como descritas por ele (as medições seguem a mesma ordem que foi apresentada no protocolo da geração da assinatura em anel). Assim, todos notam que a assinatura $(P_1, ..., P_r; v;\ x_1, ..., x_r)$ foi calculada a partir destes resultados.

O delator pode proteger-se da punição do grupo pela segurança do anonimato apresentada em [1]. A assinatura é facilmente conferida calculando a função $C_{(k,v)}(g_1(x_1), ..., g_r(x_r)) = v$. Percebe-se que a legitimidade da assinatura está assegurada pela capacidade que qualquer um dos membros da instituição $\mathcal{A}$ tem de inverter a função de sentido único. Embora os valores $y_1, ..., y_r$ sejam facilmente calculados por qualquer usuário, a equação $C_{(k,v)}$ (y_1, y_2, y_3, ..., y_r)=v só é facilmente resolvida, se ao menos uma inversão puder ser facilmente computável, $g_s^{-1}(y_s) = x_s$. Em [1] é definida uma equação que possui como entrada uma chave k, um valor de inicialização v e valores arbitrários y_1, ...,y_r em $\{0,1\}^b$. Esse algoritmo usa como subrotina E_k e produz uma saída $z \in \{0,1\}^b$, tal que, dada qualquer entrada fixada k e v, as seguintes propriedades são satisfeitas:

1) **Permutação em cada entrada** - Para cada $s \in \{1, \dots, r\}$ e para quaisquer valores fixados de todas as entradas y_i, $i \neq s$, a função $C_{k,v}(y_1, \dots, y_r) = z$ é um mapeamento de y_s para z;
2) **A equação é eficientemente solúvel** - Para cada $i \in \{1, \dots, r\}$, dada uma entrada z de b bits para toda entrada y_i, é possível encontrar eficientemente uma entrada y_i de b bits tal que $C_{k,v}(y_1, \dots, y_r) = z$;
3) **Impraticável verificar a solução da equação por entradas de funções de sentido único** - Dado k, v e z é impraticável para um adversário solucionar a equação

$$C_{(k,v)}(g_1(x_1), g_2(x_2), ..., g_r(x_r)) = z$$

   para y_1, y_2, ...,y_r (dado acesso para cada g_i e E_k) se o adversário não pode inverter qualquer das funções de sentido único g_1, $g_2, \dots, g_r$.

Os autores resolveram aplicar uma permutação pseudo-aleatória após cada operação XOR. Na proposta [1], $C_{(k,v)}$ é calculada usando funções de encriptação simétrica, E_k (a função E_k é uma função de permutação pseudo-aleatória sobre $\{0,1\}^b$). Portanto $C_{(k,v)}$ é definida por

$$\begin{aligned} C_{(k,v)}(y_1, ..., y_r) &= E_k(y_r \oplus E_k(y_{(r-1)} \oplus E_k(y_{(r-2)} \\ &\oplus E_k(... \oplus E_k(y_1 \oplus v)...))). \end{aligned} \quad (2)$$

Essa função é aplicada para a sequência (y_1, y_2, ..., y_r), em que $y_i = g_i(x_i)$. Essa equação é claramente uma permutação sobre cada entrada após uma operação XOR. Além disso, ela é eficientemente resolvida para qualquer entrada dado o conhecimento de k, o que torna possível executar o cálculo à frente a partir de um valor inicial v e para trás a partir do final z, excepcionalmente, a fim de calcular qualquer valor em falta de y_i. Essa função pode ser usada para verificar assinaturas usando uma função hash do m para a escolha de uma chave

simétrica k, e forçar a saída z a ser igual à entrada v. A prova para a primeira condição do protocolo é a prova apresentada em [1].

Agora, vamos tratar do caso em que o grupo B sai vitorioso e o assessor quer provar a autoria da mensagem. Primeiro, devemos mencionar que, nesse momento, todos os assessores estão interessados em receber a recompensa do grupo B. Também, todos eles são capazes de afirmar que as suas chaves podem produzir essa assinatura. Mas, quando T_s afirma haver partículas quânticas na entidade confiável, medidas na base v fornecem os dados da assinatura. Assim, apenas com probabilidade $1/2^{b(r-1)}$, qualquer outro dos membros pode gerar a mesma assinatura, sendo essa probabilidade um valor negligenciável no tamanho da assinatura. O dispositivo à prova de falsificação proíbe a simulação dos outros assessores em gerar a mesma assinatura.

A. Anel de assinatura quântica anônima em que apenas um delator assina

O problema que será apresentado a seguir é modelo quântico de computação multiparte segura. Este problema foi apresentado a primeira vez por David Chaum em 1998 [3]. Nesse problema, deve-se considerar uma Instituição que contém um grupo de membros que mantém relações com uma autoridade dentro da instituição, a quem chamamos de $\mathcal{B}$ (o chefe). Todos eles se comunicam através de teleportação de um para o outro de qualquer lugar em que estejam. Considera-se que todo membro $A_i \in \{A_1, A_2, \ldots, A_r\}$ compartilha o estado quântico

$$\left(\frac{|00\rangle_{A_i\ A_{i+1}} + |11\rangle_{A_i\ A_{i+1}}}{\sqrt{2}}\right)^{\otimes n}$$

com o membro A_{i+1}. O mesmo compartilhamento de estados quânticos é feito entre a autoridade $\mathcal{B}$ e o membro A_1, e entre o membro A_r e a autoridade $\mathcal{B}$. Ressalta-se que a comunicação clássica requerida na teleportação é segura, ou seja, a comunicação é pública e devidamente autenticada entre os usuários da teleportação.

Agora é importante considerar a seguinte situação: o chefe está sempre interessado que os membros vigiem uns aos outros, portanto, ele sempre busca alguma informação de irregularidade a respeito dos membros. No entanto, ele sabe que os membros trabalham sempre cooperando uns com os outros e um delator que faça qualquer denúncia de irregularidade a respeito de um dos membros pode perder a cooperação dos demais. Então, $\mathcal{B}$ deve prover um método de denúncia que mantenha o anonimato do delator. Para construir tal sistema de denúncia, $\mathcal{B}$ sempre passa um estado quântico que dever ser repassado para todos os membros da instituição, $\{A_1, A_2, \ldots, A_r\}$. É importante considerar esse estado quântico como uma folha em branco em que qualquer membro pode assinar para fazer uma denúncia a respeito de um outro membro da mesma Instituição. Então, quando o membro A_s sabe um segredo a respeito de um outro membro A_y, ele aproveita esse momento para denunciá-lo. O membro A_y acredita que nenhum outro membro sabe da sua atitude irregular e ele não imagina que alguém possa fazer tal denúncia. Dentro desse cenário, o método de denúncia provido por $\mathcal{B}$ é executado da seguinte maneira:

Protocolo 3: Assinatura privada em anel usando estados quânticos

1) Inicialmente $\mathcal{B}$ prepara aleatoriamente um estado quântico $|\psi_b^a\rangle = \bigotimes_{k=1}^n |\psi_{b_k}^{a_k}\rangle$, lembrando que $|\psi_{b_k}^{a_k}\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$;
2) O estado quântico $|\psi_b^a\rangle$ é teleportado para o membro A_1, depois A_1 teleporta-o para A_2, e assim sucessivamente, até que A_r teleporta este estado para $\mathcal{B}$;
3) O membro A_s que conhece uma informação secreta a respeito de um outro membro, do qual ninguém sabe que ele sabe desta informação, resolve fazer uma denúncia para $\mathcal{B}$. Assim, ele aplica a transformação unitária $U_x = \bigotimes_{k=1}^n (ZX)^{x_k}$ no estado quântico recebido e teleporta para o membro A_{s+1} o estado $|\psi_b^{a\oplus x}\rangle = \bigotimes_{k=1}^n |\psi_{b_k}^{a_k \oplus x_k}\rangle$;
4) Quando o estado chegar no usuário $\mathcal{B}$, ele mede o estado que foi teleportado a ele, obtendo o resultado $a \oplus x$ na medição. Assim, ele aplica $a \oplus a \oplus x$ pra extrair a string x.
5) Mais tarde, ele recebe a denúncia publicamente assinada por $m, h_x(m)$. Em que m é a mensagem que faz a denúncia e $h_x(\cdot)$ é uma função hash universal escolhida de dentro de uma família de funções hash com 2^n funções.

Antes de explicarmos o protocolo, devemos justificar porque

$$\bigotimes_{k=1}^n (ZX)^{x_k} |\psi_b^a\rangle = |\psi_b^{a\oplus x}\rangle.$$

Sem perda de generalidade, considera-se o caso de $n = 1$. Por conseguinte, temos $x \in \{0, 1\}$. operação X inverte o valor lógico dos qubits $|0\rangle$ e $|1\rangle$, desta maneira $X|\psi_0^y\rangle$, em que $y \in \{0, 1\}$, resulta no estado $|\psi_0^{y\oplus 1}\rangle$. No entanto, a operação X nada de efetivo faz sobre os qubits da base diagonal, ou seja, $X|\psi_1^y\rangle$ resulta no estado quântico $(-1)^y|\psi_1^y\rangle$. Considerando que a fase global não afeta a medição, ela será desconsiderada a partir de agora. De forma análoga, a transformação Z só é relevante para a mudança do valor lógico dos qubits da base diagonal. Portanto, quando o produto XZ é aplicado no estado $|\psi_t^y\rangle$ temos $|\psi_t^{y\oplus 1}\rangle$ para todo $t \in \{0, 1\}$. Finalmente, consideramos que $(XZ)^0 = I$. Portanto, $(XZ)^x|\psi_t^y\rangle = |\psi_t^{y\oplus x}\rangle$.

A primeira questão sobre o Protocolo 3 que devemos investigar é: A denúncia é completamente anônima? O estado quântico é desconhecido de todos os membros da instituição, portanto, se um deles resolver medir o estado, não poderá reconstruí-lo para que a informação possa ser lida mais tarde. Assim, o usuário que resolver medir o estado quântico invalida totalmente o esquema de assinaturas, impossibilitando $\mathcal{B}$ de ler qualquer mensagem autenticada. Portanto, aquele que assina a mensagem tem a sua identidade preservada porque somente $\mathcal{B}$ pode ler o que foi escrito sem saber qual dos membros escreveram a assinatura.

Devemos destacar que o esquema está restrito apenas a um delator. Pois somente quem conhece a denúncia, como pressuposto inicialmente, gera a assinatura mantendo-se anônimo, de

forma que, todos os membros são suspeitos de terem assinado esta mensagem.

Para resgatar a autoria da assinatura, o delator simplesmente revela x a $\mathcal{B}$, pois este dado não é público e somente quem gerou a assinatura pode fornecer esta informação.

II. Conclusão

Neste trabalho é mostrado como dispositivos quânticos à prova de falsificação podem impedir a simulação de protocolos clássicos. Em primeira proposta, seguindo a linha de pensamento em [4], nós mostramos como uma simples memória quântica, sem entrelaçamento, é capaz de traçar a interação entre o provador e o verificador em sistemas de prova interativo de conhecimento nulo. Este resultado ainda não tinha sido proposto, pois as propostas anteriores usam estados entrelaçados. Ainda apresentamos, um ataque completamente quântico para o mesmo protocolo de prova de conhecimento nulo sem o uso de função hash. Adicionalmente, neste trabalho é mostrado como num esquema de assinatura em anel, que preserva o anonimato do delator, pode ter o anonimato da assinatura quebrado pelo próprio autor da assinatura quando este usa um dispositivo quântico à prova de falsificação para gerar os dados de entrada da assinatura.

Deve ser ressaltado, que o esquema de assinatura em anel que usa funções trapdoor do tipo RSA e Rabin perde a sua validade diante de computadores quânticos que executem o algoritmo de Shor, [5]. Pois, com estes computadores, qualquer um que conheça a chave pública é capaz de produzir a assinatura. Portanto, o argumento de que a informação veio de dentro da instituição $\mathcal{A}$ perde a sua validade. No entanto, a propriedade de resgate da autoria, continua válida, independente da existência do algoritmo de Shor. Mas para isso é necessário que uma função trapdoor exista independente da fatoração de números inteiros e da inversão do logaritmo discreto. Em sistemas de criptografia clássica, as únicas propostas válidas de funções trapdoor são os esquemas de encriptação RSA e o método de Rabin, pois as outras propostas falharam ao longo dos anos. No entanto, esquemas de funções trapdoor quânticas têm surgido [6], [7], [8]. Em [6], um esquema de função trapdoor quântica é construído a partir do problema de automorfismo de grafos. Encontrar um automorfismo de grafos não trivial para um conjunto de grafos é um problema $\mathcal{NP}$-completo. Esse trabalho mostra que, se um computador quântico é capaz de decifrar em tempo polinomial uma mensagem cifrada por este esquema de assinatura, sem possuir a chave secreta, então o problema de automorfismo de grafos poderá ser resovido em tempo polinomial por um computador quântico. Para este esquema de assinaturas, fica como proposta futura, a construção de anel de assinatura usando funções trapdoor quânticas.

III. Conclusões

Neste trabalho mostramos como uma simples memória quântica pode ser usada para atacar uma importante propriedade de sistemas de prova de conhecimento nulo. Neste ataque, o provador perde o anonimato após uma interação com o verificador em um algoritmo de prova de conhecimento nulo. O resultado aqui apresentado usa apenas processos de leitura e escrita em memória quântica para realizar tal ataque. A não-localidade, uma propriedade da mecânica quântica, não é usada no ataque aqui proposto. O objetivo é deixar claro que memórias quânticas são dispositivos a prova de falsificação e isto é suficiente para a transferência de prova do traço de interação entre o provador e o verificador.

Agradecimentos

A Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e a Fundação Cearense de Apoio ao Desenvolvimento Científico e Tecnológico (FUNCAP).

Referências

[1] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," *Communications of the ACM*, vol. 22, no. 22, pp. 612–613, 2001.

[2] M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions," *SIAM J. Comput.*, vol. 17, no. 2, pp. 373–386, 1988.

[3] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, pp. 65–75, 1988, 10.1007/BF00206326. [Online]. Available: http://dx.doi.org/10.1007/BF00206326

[4] J. Bouda, P. Mateus, N. Paunkovic, and J. Rasga., "On the power of quantum tamper-proof device," *International Journal of Quantum Information*, vol. 6, pp. 281 – 302, 2008.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[6] A. Kawachi, T. Koshiba, and T. Y. H. Nishimura, "A quantum trapdoor one-way function that relies on the hardness of the graph automorphism problem," in *Quantum Information Science Workshop*, 2003, pp. 115–116.

[7] G. M. Nikolopoulos, "Applications of single-qubit rotations in quantum public-key cryptography," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 77, no. 3, p. 032348, 2008. [Online]. Available: http://link.aps.org/abstract/PRA/v77/e032348

[8] T. Okamoto, K. Tanaka, and S. Uchiyama, "Quantum public-key cryptosystems," in *CRYPTO '00: Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 2000, pp. 147–165.