Esquema de Acordo de Chaves de Conferência Baseado em um Problema de Funções Quadráticas de Duas Variáveis

Luis Antonio B. Kowada[1], **Raphael C. S. Machado**[2,3]

[1]Instituto de Computação – Universidade Federal Fluminense
Niterói – RJ – Brazil

[2]Inmetro, Instituto Nacional de Metrologia, Qualidade e Tecnologia
Rio de Janeiro – RJ – Brazil.

[3]Programa de Pós-Graduação em Ciência da Computação – CEFET/RJ
Rio de Janeiro – RJ – Brazil.

luis@ic.uff.br, rcmachado@inmetro.gov.br

Abstract. *Conference key establishment is the process to determine a common shared key between three or more participants. If all participants influence key generated by this process, we have a* conference key agreement scheme. *In the present work, we propose a conference key agreement scheme with some significant advantages over the existing schemes, of which we highlight the following:*

1. *agreement of conference keys in a single round and with linear quantity of messages published;*
2. *combination of two conference keys in a single round and with constant number of published messages;*
3. *renewing conference keys in a single round and with only one published message.*

The proposed scheme is resilient against classical attack scenarios, but is vulnerable to attack by an attacker capable of calculating the discrete logarithm and is therefore vulnerable to attacks with a quantum computer.

Resumo. *Estabelecimento de chave de conferência é o processo de determinação de uma chave comum compartilhada entre três ou mais participantes. Se neste processo, todos os participantes influenciam a chave a ser gerada, temos um* esquema de acordo de chaves de conferência. No presente trabalho, propomos um esquema de acordo de chaves de conferência que apresenta vantagens significativas sobre os atuais esquemas existentes, como:

1. *acordo de chaves de conferência em uma única rodada e com quantidade linear de mensagens publicadas;*
2. *combinação de duas chaves de conferência em uma única rodada e com número constante de mensagens publicadas;*
3. *renovação de chaves de conferência em uma única rodada e com única mensagem publicada.*

O esquema proposto é resiliente face a cenários de ataques clássicos, mas é vulnerável a ataques executados por um atacante capaz de calcular o logaritmo discreto, sendo, portanto, vulnerável a ataques usando Computação Quântica.

1. Introdução

Esquemas de estabelecimento de chaves são uma primitiva fundamental em criptografia, pois permitem que um conjunto de participantes estabeleça uma chave criptográfica compartilhada [Barker et al. 2013] que poderá ser posteriormente utilizada, por exemplo, para fins de confidencialidade — com o uso de uma cifra — ou de autenticação — por exemplo, com o uso de um código de autenticação de mensagens. Esquemas de estabelecimento de chaves estão na origem dos modernos métodos de Criptografia: o primeiro método de criptografia assimétrica é exatamente um esquema de estabelecimento de chaves, a saber, o método de Diffie e Hellman [Diffie and Hellman 1976], desenvolvido em 1976, e que baseia-se na suposta dificuldade de se calcular o logaritmo discreto para permitir que dois (ou mais) participantes estabeleçam um segredo comum a partir de informações trocadas de maneira pública entre eles.

Desde que o método de Diffie e Hellman foi proposto, diversas variantes do método têm sido propostas, tais como o método ElGammal [ElGammal b], os protocolos MTI [Matsumoto et al.] e o protocolo STS [ElGammal a, Diffie et al. 1992]. O estabelecimento de uma chave compartilhada entre três ou mais participantes, denominado *conference keying* ou *chave de conferência* [Lee et al. 2004], tem ganhado cada vez mais atenção à medida em que comunicações em grupo ganham importância na Internet, seja devido aos protocolos multicast, seja devido à proliferação de aplicativos de mensagem instantânea envolvendo grupos de usuários. Observam-se diversos estudos a respeito de como estender o método de Diffie e Hellman para cenários multi-participantes (por exemplo, [Ateniese et al. 2000, Chunsheng 2015a, Chunsheng 2015b] ou a respeito de novas construções que suportem "nativamente" o estabelecimento de chaves de conferência em uma única rodada [Joux 2000, Boneh and Silverberg 2002].

No presente trabalho, propomos um esquema de acordo de chaves análogo ao método de Diffie e Hellman, porém, baseado na dificuldade de se encontrar as raízes inteiras de uma equação Diofantina com duas variáveis e com grau máximo 2. O esquema proposto apresenta vantagens estabelecimento de chaves de conferência, as quais enumeramos algumas a seguir:

1. Acordo de chaves de conferência em única rodada. Trata-se da principal característica do esquema proposto. Conforme discutimos na seção seguinte, desde o trabalho de Joux [Joux 2000], que construiu um esquema de acordo de chaves em rodada única para três participantes, a comunidade de criptografia busca por esquemas de acordo de chaves de conferência cujo número de rodada seja independente do número de participantes.
2. Combinação eficiente de chaves de conferência. O esquema proposto é eficiente no processo de criação de múltiplas chaves de conferência para múltiplos conjuntos de usuários, permitindo combinar a chave de dois grupos C_1 e C_2 de usuários para criar uma chave para $C_1 \cup C_2$, sem comprometer o sigilo das informações previamente encriptadas por meio das chaves originais.
3. Renovação automática de chaves de conferência. O esquema proposto permite a modificação dinâmica das chaves de conferência com base na publicação de uma única mensagem (em modo broadcast) — ou, mesmo, sem que haja necessidade de transmissão de mensagens, assumindo que os participantes estão sincronizados.

As vantagens acima enumeradas podem ser alcançadas porque, ao contrário do

método de Diffie e Hellman, o esquema proposto não necessita que "chaves temporárias" sejam trafegadas ao longo do processo de acordo de chave de conferência. Ao contrário, cada participante precisa divulgar apenas uma única informação, a qual é utilizada para construir chaves de conferência, mas que não constituem chaves, por si só. Essa propriedade permite a imediata definição de chaves de conferência para qualquer subconjunto de participantes, bastando que cada participante deste subconjunto realize uma única computação sobre as informações divulgadas pelos participantes do subconjunto. Esses cenários são melhor explicados ao longo do texto.

O presente documento está organizado da seguinte forma. Na Seção 2 apresentamos os conceitos e terminologia necessários para a compreensão do trabalho. A Seção 3 descreve a nossa proposta de esquema de acordo de chaves, enquanto a Seção 4 descreve os aspectos de segurança do esquema proposto. Na Seção 5, estudamos a questão de como estabelecer chaves de conferência e discutimos as vantagens do esquema proposto sobre os esquemas baseados no método de Diffie e Hellman. A Seção 6 contém nossas considerações finais e aponta para os próximos desenvolvimentos a serem realizados sobre o esquema de acordo de chaves proposto.

2. Referencial Teórico

2.1. Esquemas de Acordo de Chaves

Esquemas de estabelecimento de chaves são algoritmos que permitem que uma chave criptográfica seja estabelecida entre um grupo de participantes [Barker et al. 2013]. Esquemas de estabelecimento de chaves classificam-se em *esquemas de transporte de chaves*, em que ocorre o envio de uma chave criptográfica entre os participantes, e *esquemas de acordo de chaves*, em que a chave criptográfica não é enviada entre os participantes.

O presente trabalho propõe um esquema de estabelecimento de chaves que se classifica como um esquema de acordo de chaves. Em um esquema de acordo de chaves, os participantes trocam informações a partir das quais os participantes são capazes de computar uma chave criptográfica secreta comum. Um esquema de acordo de chaves é, portanto, um protocolo no qual dois ou mais participantes podem acordar uma chave de tal maneira que ambos possam influenciar na chave final construída. Ao contrário de outros protocolos nos quais uma das partes é responsável por gerar e transmitir a chave, esquemas de acordo de chaves eliminam os riscos de que estão associados à capacidade de uma das partes "forçar" uma chave [Diffie et al. 1992].

O clássico método de Diffie e Hellman [Diffie and Hellman 1976] é um esquema de acordo de chaves baseado na dificuldade de se calcular o logaritmo discreto.

2.2. Método de Diffie-Hellman

O método de Diffie e Hellman é uma referência básica para esquemas de acordo de chave, frente ao qual o esquema proposto será comparado. Por uma questão de completude, apresentaremos o funcionamento básico do método.

Como explicamos anteriormente, o método de Diffie e Hellman permite que dois participantes gerem uma chave secreta comum por meio da qual eles poderão trocar informações através de um canal inseguro. Sejam Alice e Bob tais participantes. Primeiro, eles acordam acerca de dois números primos g e p, onde p é grande e g é uma

raiz primitiva módulo p. Os números g e p não precisam ser mantidos em segredo de outros usuários. Agora Alice escolhe um grande número aleatório a e Bob também escolhe um grande número b. Alice então calcula $A = g^a \bmod p$, que ela envia para Bob, e Bob calcula $B = g^b \bmod p$, o qual Bob transmite para Alice. Finalmente, Alice e Bob calculam sua chave compartilhada $K = g^{(ab)} \bmod p$, que Alice calcula como $K = B^a \bmod p = (g^b)^a \bmod p$ e Bob calcula como $K = A^b \bmod p = (g^a)^b \bmod p$. Onde $x = y \bmod z$, significa que x é igual ao resto da divisão inteira de y por z.

Alice e Bob agora podem usar sua chave compartilhada K para trocar informações cifradas. Para que um potencial espião obtivesse a chave K, Eva precisaria obter $K = g^{(ab)} \bmod p$ conhecendo apenas g, p, $A = g^a \bmod p$ e $B = g^b \bmod p$, o que demandaria calcular a a partir de A, g e p (resp. b a partir de B, g e p), ou seja, calcular o logaritmo discreto, o que é computacionalmente inviável para grandes valores de p.

Veremos, a seguir, que, embora engenhoso, o método de Diffie e Hellman não estende-se de maneira simples ao cenário em que se deseja estabelecer chaves de conferência — ou seja, chaves compartilhadas entre membros de um conjunto com três ou mais participantes.

2.3. Chave de Conferência

Acordo de chaves de conferência refere-se à capacidade de se estabelecer uma chave criptográfica compartilhada entre três ou mais participantes de uma comunicação.

O clássico método de Diffie e Hellman permite que se estabeleça chaves de conferência. Porém, por uma característica construtiva, para se estabelecer uma chave compartilhada entre os membros de um grupo com n participantes, é necessário que se transmita entre tais n participantes informação que poderia ser utilizada como chave criptográfica de $n' < n$ participantes. Por este motivo, o método de Diffie e Hellman acaba não sendo eficiente quando de deseja estabelecer múltiplas chaves criptográficas em diversos subgrupos de um grupo de n pessoas.

Considere o caso em que se deseje utilizar o método de Diffie e Hellman para estabelecer uma chave de conferência compartilhada por três participantes, A, B e C. Basicamente, para que usuário C possa calcular chave de conferência G^{abc}, é necessário que A envie g^a a B, que calcula g^{ab} e envia a C — que só então será capaz de calcular g^{abc}. O processo deverá ser repetido para que A e B sejam capazes de calcular g^{abc}, cada um. O processo acima apresenta três problemas, os quais descrevemos a seguir. O primeiro problema é o fato de que as chaves "parciais" são transmitidas para que se possa calcular a chave final. Desta forma, a chave compartilhada apenas entre A e B — a saber, g^{ab}, não pode ser utilizada para transmitir informações confidenciais entre A e B, pois ela também é conhecida por C. O segundo problema é a necessidade de transmissão de uma grande quantidade de mensagens, já que cada participante somente é capaz de calcular a chave final se conhecer a chave parcial construída por todos os outros participantes. O terceiro participante é a impossibilidade de se realizar uma rápida modificação dinâmica da chave de conferência — o que somente pode ser realizada por meio de uma completa reexecução do protocolo.

No caso geral, considere uso do método de Diffie e Hellman para estabelecer uma chave de conferência compartilhada por participantes de um grupo de tamanho n. Neste caso, desejar-se-á que cada participante chegue à chave $k_{s_1,\ldots,s_n} := g^{s_1 \cdot \cdots \cdot s_n}$. Para que

o participante i seja capaz de construir $k_{s_1,...,s_n}$ tendo conhecendo apenas à sua própria informação privada s_n, é necessário que ele tenha acesso à chave "parcial" $k_{s_1,...,s_{n-1}} := g^{s_1 \cdot ... \cdot s_{n-1}}$. De maneira recursiva, a construção de $k_{s_1,...,s_{n-1}}$ demanda a "intervenção" de cada um dos participantes $s_1, ..., s_{n-1}$, o que leva a um número de rodadas igual a $O(n)$ até a definição da chave de conferência.

A busca por esquemas mais eficientes para o acordo de chaves de conferência tem despertado bastante atenção na comunidade de Criptografia. Em 2000, Joux [Joux 2000] demonstrou como utilizar emparelhamentos de Weil e Tate sobre curvas elípticas para construir um esquema com única rodada para acordo de chaves entre três participantes. O trabalho de Joux desencadeou uma série de novas pesquisas acerca de métodos para o acordo de chaves de conferência. Por um lado, uma série de trabalhos surgiram com o objetivo de aplicar o método de Joux à construção de protocolos mais eficientes para o acordo de chaves de conferência [Barua et al. 2003, Al-Riyami and Paterson 2003]. Por outro lado, uma série de estudos foi realizado com o objetivo de construir esquemas de acordo de chaves em um única rodada. Em 2002, Boneh e Silverberg [Boneh and Silverberg 2002] propõem diversas aplicações de formas multilineares à criptografia, incluindo a construção de esquemas de acordo de chaves de conferência em rodada única. Em 2013, Garg, Gentry e Halevi [Garg et al. 2013] descrevem construções baseadas em reticulados com propriedades que aproximam aquelas desejáveis para aplicações criptográficas, e apresentam diversos exemplos de aplicações, inclusive a esquemas de acordo de chaves de conferência. O método seria logo quebrado, em 2016, por Hu e Jia [Hu and Jia 2016], evidenciando a necessidade e o interesse pela definição de novos métodos para a construção de esquemas de acordo de chave em rodada única.

2.4. Equações Diofantinas

Muitos problemas de Teoria dos Números podem ser formulados como questões a respeito da solução de *equações Diofantinas*, ou seja, equações da forma $p(x_1, ..., x_n) = 0$ para um polinômio de várias variáveis e coeficientes inteiros. A importância das equações Diofantinas foi reconhecida por Hilbert ao formular suas famosa lista de problemas [Hilbert 1902] e relacionar o décimo problema como a busca por um algoritmo para determinar as raízes destas equações. Hoje, sabe-se que o problema não possui solução, ou seja, é indecidível no caso geral [Matijasevič 1970, Robinson 1972]. Mesmo para equações com duas variáveis, o problema é surpreendentemente difícil. Por exemplo, o teorema de Thue [Thue 1902], de 1909, enuncia que, para qualquer polinômio $f(x, y)$ irredutível sobre os racionais e homogêneo de grau 3, a equação $f(x, y) - m = 0$ possui no máximo um número finito de soluções inteiras. O argumento de Thue não permite construir um algoritmo que encontre tais soluções. Em 1967, Baker obteve um algoritmo não-determinístico de tempo exponencial para o problema — concluindo-se que, o problema, embora computável, é, aparentemente, intratável. Em 1978, Manders e Addleman [Manders and Adleman 1978] mostram que, para equações da forma $\alpha x_a^2 + \beta x_b = \gamma$, o problema de decidir se existe solução com x_a e x_b assumindo valores naturais é NP-completo.

3. Esquema de Acordo de Chaves Baseado em Funções Quadráticas

O esquema proposto no presente trabalho baseia-se na construção de uma chave comum a Alice e Bob a partir da troca de mensagens que contém o resultado de uma função

quadrática aplicada a valores aleatórios sorteados por Alice (e enviados a Bob) e por Bob (e enviados a Alice). Veremos que escolhendo valores apropriados para os parâmetros da função quadrática, é possível garantir que Alice e Bob chegarão à mesma chave.

Os parâmetros de domínio para o esquema proposto são os parâmetros α e β da função quadrática, um parâmetro de dimensão δ, e uma base y. Esses parâmetros de domínio podem ser gerados por um dos participantes ou por uma terceira parte confiável (Trent). Por questões de clareza, assumimos, no presente trabalho, que uma terceira parte confiável é responsável pela geração dos parâmetros de domínio.

O algoritmo a seguir descreve o funcionamento geral do esquema proposto. Usamos φ para representar a função Totiente de Euler, escrevemos $p|q$ significando que $q = 0 \bmod p$ e escrevemos $p \nmid q$ significando que $q \neq 0 \bmod p$.

Algoritmo 1: Procedimento para combinação de uma chave comum entre duas partes.

- Trent:
  1. Escolha um número natural δ
  2. Escolha um número natural β tal que $\varphi(\delta) \nmid \beta$
  3. Escolha α, tal que $\varphi(\delta)|\alpha$.
  4. Escolha $y < \delta$ tal que $\text{mdc}(y, \delta) = 1$.
  5. Publique y, α, β e δ.
- Alice:
  1. Escolha $x_a < \delta$
  2. Escolha $x_b < \varphi(\delta)$ tal que $\varphi(\delta) \nmid x_b\beta$
  3. Calcule $\gamma = \alpha x_a^2 + \beta x_b$.
  4. Envie para Bob (publique) γ e δ.
- Bob:
  1. Escolha $x'_a < \delta$
  2. Escolha x'_b tal que $\varphi(\delta) \nmid x'_b\gamma$
  3. Calcule $\gamma' = \alpha {x'_a}^2 + \beta x'_b$.
  4. Envie para Alice (publique) γ'.
- Alice:
  1. Calcule $k_{ab} = y^{\gamma' \cdot x_b} \bmod \delta$.
- Bob:
  1. Calcule $k_{ba} = y^{\gamma \cdot x'_b} \bmod \delta$.

3.1. Corretude do algoritmo

Mostramos, a seguir, que o Algoritmo 1 retorna uma chave comum entre Alice e Bob.
Teorema 1. *As chaves criptográficas k_{ab} e k_{ba} são idênticas. Adicionalmente, $k_{ab} \neq y$.*

Demonstração.

$$\begin{aligned} k_{ab} &= y^{\gamma' x_b} \bmod \delta \\ &= y^{(\alpha {x'_a}^2 + \beta x'_b) \cdot x_b} \bmod \delta \\ &= y^{\alpha {x'_a}^2 x_b + \beta x'_b x_b} \bmod \delta \\ &= y^{\alpha {x'_a}^2 x_b} \cdot y^{\beta x'_b x_b} \bmod \delta \\ &= (y^{{x'_a}^2 x_b})^{\alpha} \cdot y^{\beta x'_b x_b} \bmod \delta \end{aligned}$$

Considerando que mdc$(y, \delta) = 1$ e $\varphi(\delta)|\alpha$, o Teorema de Euler implica $(y^{{x'_a}^2 x_b})^\alpha \equiv 1 \bmod \delta$. Logo, $k_{ab} \equiv y^{\beta x'_b x_b} \bmod \delta$.

De forma análoga, podemos mostrar que $k_{ba} = y^{\gamma \cdot x'_b} \bmod \delta \equiv y^{\beta x_b x'_b} \bmod \delta$.

Portanto, $k_{ab} = k_{ba}$.

□

3.2. Escolha dos parâmetros de domínio

Como se sabe, a segurança de um esquema criptográficos assimétricos depende de forma decisiva dos critérios utilizados para a escolha dos parâmetros de domínio [Barker et al. 2013]. Isso porque as restrições impostas aos parâmetros de domínio é que irão definir se os "problemas computacionais" associado aos cenários de ataque são, de fato, intratáveis e, inviabilizarão a realização bem-sucedida de ataques tais como a recuperação da chave.

Sabe-se [Manders and Adleman 1978] que determinar se existem x_a e x_b naturais que satisfaçam a equação $\gamma = \alpha x_a^2 + \beta x_b$, dados α, β e γ naturais, é um problema NP-completo [Manders and Adleman 1978]. Em relação ao esquema proposto no presente trabalho, a segurança do procedimento depende do padrão utilizado para escolher β e δ. Em relação à α, podemos assumir que $\alpha = \varphi(\delta)$.

Apresentamos, a seguir, dois possíveis "padrões" a serem seguidos no que diz respeito à escolha de β e δ.

Padrão 1: β e δ como produtos de primos

- Escolha duas sequências de primos distintos $p_1, p_2, ..., p_m$ e $q_1, q_2, ..., q_n$, (os valores m e n irão impactar o tamanho de chave e o nível de segurança).
- Calcule $\delta = \Pi_i^n p_i$, $\alpha = \Pi_i^n (p_i - 1)$ e $\beta = \Pi_j^m q_j$.

Padrão 2: δ como produto de cubos de primos, $\alpha|\beta^2$, mas $\alpha \nmid \beta$

- Escolha duas sequências de primos distintos $p_1, p_2, ..., p_m$ e $q_1, q_2, ..., q_n$, (os valores m e n irão impactar o tamanho de chave e o nível de segurança).
- Calcule $\delta = \Pi_i^n p_i^3$, $\alpha = \Pi_i^n p_i^2 (p_i - 1)$ e $\beta = \Pi_i^n p_i (p_i - 1) \cdot \Pi_j^m q_j$.

3.3. Um pequeno exemplo

Para ilustrar o funcionamento do algoritmo, vamos mostrar um pequeno exemplo usando o Padrão 1.

- Seja $n = 2$ e $m = 3$.
- Alice escolhe $p_1 = 3$, $p_2 = 11$, $q_1 = 5$, $q_2 = 7$ e $q_3 = 13$.
- Isto significa que $\delta = 33$, $\alpha = 20$ e $\beta = 455$.
- Alice escolhe $y = 10$.
- Alice escolhe $x_a = 14$ e $x_b = 37$.
- Alice calcula $\gamma = 20755$.

- Alice envia para Bob a sequência $(10, 20, 455, 20755, 33)$
- Bob recebe a sequência de Alice.
- Bob escolhe $x'_a = 11$ e $x'_b = 23$.
- Bob calcula $\gamma' = 12885$.
- Bob envia para Alice $\gamma' = 12885$.
- Alice calcula $k_{ab} = 10$.
- Bob calcula $k_{ba} = 10$.

4. Análise da segurança do esquema proposto

O esquema proposto na Seção 3 será inseguro se for possível obter informações sobre x_a, x_b ou k_{ab} a partir de $\{\alpha, \beta, \delta, \gamma, \gamma', y\}$. Podemos ver que se um espião Eva conhecer x_a, então Eva pode calcular x_b, assim como, se conhecer x_b, Eva consegue calcular x_a. A dificuldade de calcular x'_a é a mesma de calcular x_a. O mesmo acontece com x'_b. Se ele tiver x_b e x'_b ele consegue calcular a chave k_{ab}.

Nas próximas subseções, estudamos a segurança do esquema proposto face a diversos cenários de ataque. Na Subseção 4.1, estudamos um modelo de ataque utilizando técnicas "clássicas", enquanto na Subseção 4.2, estudamos um modelo de ataque utilizando um computador capaz de resolver o Problema do Logaritmo Discreto (como é o caso do modelo de computação quântica). A Subseção 4.3 apresenta cenários de ataque sobre o exemplo apresentado ao final da Seção 3.

Os resultados do estudo levam a crer que o esquema proposto parece ser robusto para a Computação Convencional, mas é frágil para ataque com um Computador Quântico que consiga resolver o Problema do Logaritmo Discreto.

4.1. Modelo de ataque clássico

Uma possível estratégia para resolver o problema é fatorar β e calcular as possíveis soluções módulo potências dos fatores primos de β. Este problema continua sendo difícil, mesmo conhecendo os primos que compõem β.

Se α e β não forem coprimos (como é o caso do padrão 2), podemos dividir toda a equação por $\text{mdc}(\alpha, \beta)$.

Se α e β forem coprimos, mas β e γ não, temos que $\text{mdc}(\beta, \gamma)$ divide x_a^2. Se β for produto de primos distintos (como no padrão 1), então $\text{mdc}(\beta, \gamma)$ divide x_a.

Em qualquer caso, temos que $\text{mdc}(\alpha, \beta)$ divide γ. E então dividimos toda a equação por $\text{mdc}(\alpha, \beta)$, obtendo os mesmos ou novos α_1 e β_1 coprimos e γ_1. Pela equação $\alpha_1 x_a^2 + \beta_1 x_b = \gamma_1$, tem-se que $\alpha_1 x_a^2 \equiv \gamma_1 \bmod \beta_1$, e consequentemente $x_a^2 \equiv \gamma_1 \alpha_1^{-1} \bmod \beta_1$. Esta última equação pode ter até $2^{n'}$ soluções, considerando que β_1 seja o produto de n' primos distintos. Da mesma forma, ao procurar $x_b \bmod \alpha$, tem-se $\beta x_b \equiv \gamma \bmod \alpha$, ou seja, $x_b \equiv \gamma\beta^{-1} \bmod \alpha$. A mesma consideração sobre o $\text{mdc}(\alpha, \beta) = 1$ pode ser feita aqui. E após, obter novos valores de α_1, β_1 e γ_1, visto que $\text{mdc}(\alpha_1, \gamma_1)$ divide x_b. Isto significa que sabemos que $x_b = \gamma_\alpha \beta_\alpha + t\alpha$, onde β_α e γ_α são os restos da divisão de β e γ por α respectivamente, para algum t. Substituindo x_b na equação $\alpha x_a^2 + \beta x_b = \gamma$, tem-se $\alpha x_a^2 + \gamma_\alpha \beta \beta_\alpha + t\alpha\beta = \gamma$, que pode ser escrito como $\alpha x_a^2 + \overline{\beta} t = \overline{\gamma}$, onde $\overline{\beta} = \alpha\beta$ e $\overline{\gamma} = \gamma - \gamma_\alpha \beta \beta_\alpha$, que é uma equação do mesmo formato que a equação original e portanto com o mesmo grau de dificuldade de ser calculada.

Sobre o tamanho da chave

Considerando que a chave final é calculada módulo δ, obviamente o tamanho da chave depende do valor de δ, que por sua vez depende de m, quantidade de primos que o compõe. Se δ for muito pequeno, pode-se fazer um ataque de força bruta. Se δ for muito maior do que β, existirão poucos valores possíveis para t na expressão. $x_b = \gamma_\alpha \beta_\alpha + t\alpha$. Conforme comentado anteriormente, a quantidade de diferentes soluções possíveis para a expressão $x_a^2 \equiv \gamma\alpha^{-1} \bmod \beta$, depende do número de primos distintos, n, que compõe β. Isso significa que quanto maior valor de n, maior a quantidade de tentativas necessárias para encontrar a chave. O tamanho da chave depende do tamanho dos primos que compõe δ e β.

4.2. Modelo de ataque baseado no cálculo do Logaritmo Discreto

Considerando que $\alpha = \varphi(\delta)$.

- **Para encontrar x_b:** Um intruso pode encontrar $x_b \bmod \gamma$ da seguinte forma:
  1. Escolha $y < \delta$ tal que $\text{mdc}(y, \delta) = 1$ e preferencialmente que y seja um gerador de Z_δ.
  2. Calcule $c = y^\gamma \bmod \delta$.
  3. Calcule $y' = y^\beta$.
  4. Encontre x tal que $c = (y')^x \bmod \delta$.

  Podemos observar que $x = x_b \bmod \gamma$.
- **Para encontrar a chave k_{ab}:**
  1. Calcule $c = y^{\frac{\gamma\gamma'}{mdc(\alpha,\beta)}} \bmod \delta$.
  2. Calcule $y' = y^{\frac{\beta}{mdc(\alpha,\beta)}}$.
  3. Encontre x tal que $c = (y')^x \bmod \delta$.

  A chave $k_{ab} = y^x \bmod \delta$.

Justificativa

Considerando que $\gamma\gamma' = \alpha^2 x_a^2 {x'_a}^2 + \alpha\beta x_a^2 x'_b + \alpha\beta {x'_a}^2 x_b + \beta^2 x_b x'_b$, temos que $\frac{\gamma\gamma'}{\text{mdc}_{(\alpha,\beta)}} \equiv \frac{\beta}{\text{mdc}_{(\alpha,\beta)}} \beta x_b x'_b \bmod \alpha$.

Podemos observar que $c \equiv y^{\frac{\gamma\gamma'}{mdc(\alpha,\beta)}} \bmod \delta \equiv (y')^{\beta x_b x'_b} \bmod \delta$.

4.3. Exemplo de aplicação dos ataques

A seguir, mostraremos como os ataques descritos na presente seção seriam executados para determinar os valores de x_a, x_b e k_{ab} do exemplo da Seção 3. Lembramos que os valores públicos do exemplo são os seguintes: $y = 10$, $\alpha = 20$, $\beta = 455$, $\gamma = 20755$ e $\delta = 33$).

Determinando x_a com o ataque 4.1

Como $\text{mdc}(\alpha, \beta) = 5 \neq 1$, não seria possível calcular $\gamma\alpha^{-1} \bmod \beta$ diretamente, uma vez que seria necessário para deduzir x_a. Por esse motivo, é necessário dividir α, β e γ, por

5, obtendo os novos valores $\alpha_1 = 4, \beta_1 = 91, \gamma_1 = 4151$. O mdc$(\beta_1, \gamma_1) = 7$. Portanto, sabemos que x_a é multiplo de 7.

Neste caso, para os *novos* $\alpha_1 = 4$, $\beta_2 = 13$ e $\gamma_2 = 593$, temos que $x_a^2 \equiv$ mdc$(\beta_1, \gamma_1)\gamma_2\alpha_1^{-1} \equiv 7 \times 8 \times 10 \bmod \beta_2$, ou seja $x_a^2 \equiv 1 \bmod 13$. Para encontrar os possíveis valores de $x_a \bmod \beta_2$, usamos o Teorema Chinês do Resto sobre o sistema com as congruências módulo fatores primos de β_2; que neste caso, apenas uma congruência. Esta congruência possui soluções 1 e -1 módulo β_2. Ou seja, x_a é da forma $1 + 13q$ ou $12 + 13q$, para algum q natural. Sabemos também que $x_a < \delta$ e é múltiplo de 7. Como havia uma única congruência no sistema, há 2 possíveis soluções para a congruência módulo β_2. Se houvesse n' congruências (n' primos distintos compondo β_2), haveria $2^{n'}$ possíveis soluções.

Determinando x_b com o ataque 4.1

Como mdc$(\alpha, \beta) \neq 1$, não é possível, o atacante não consegue calcular $\gamma\alpha^{-1} \bmod \beta$ para os valores originais. Por esse motivo, usamos os novos valores $\alpha = 4, \beta = 91, \gamma = 4151$, como no cenário anterior.

Determinando x_b com o ataque em 4.2

1. Tomemos $y = 10$ (como escolhido pela Alice).
2. $c \equiv 1 \bmod 33$
3. $y' \equiv 10 \bmod 33$
4. x deve satisfazer a congruência $1 \equiv 10^x \bmod 33$. Ou seja, x_b é múltiplo de 2.

Rodando novamente para outro valor de y temos

1. Tomemos $y = 2$.
2. $c \equiv 32 \bmod 33$
3. $y' \equiv 32 \bmod 33$
4. x deve satisfazer a congruência $11 \equiv 11^x \bmod 33$. Ou seja, x_b pode ser qualquer valor.

Mais uma tentativa...

1. Tomemos $y = 17$.
2. $c \equiv 11 \bmod 33$
3. $y' \equiv 11 \bmod 33$
4. x deve satisfazer a congruência $11 \equiv 11^x \bmod 33$. Ou seja, x_b pode ser qualquer valor.

Determinando k_{ab} com o ataque em 4.2

1. $c = 10^{(20755 \times 12885)} \bmod 33 \equiv 10 \bmod 33$.
2. $y' = y^\beta \equiv 10 \bmod 33$.
3. $x = 1$.
4. $k_{ab} = 10$.

5. Esquema de Acordo de Chave de Conferência

A seguir, mostraremos como o esquema proposto no presente trabalho permite a instanciação eficiente de chaves de conferência. O segredo da eficiência do método é o fato de que o parâmetro γ_i enviado por um participante i a todos os outros pode ser utilizado diretamente para construir chaves de conferência para qualquer conjunto de participantes, mas γ_i, por si só, não configura uma chave criptográfica para nenhum grupo. Esta propriedade difere fundamentalmente do método de Diffie e Hellman, onde, para construir uma chave compartilhada $k_{s_1,...,s_n} := g^{s_1 \cdot ... \cdot s_n}$, um participante i precisa ter acesso a $k_{s_1,...,s_{i-1},s_{i+1},...,s_n} := g^{s_1 \cdot ... \cdot s_{i-1} \cdot s_{i+1} \cdot ... \cdot s_n}$.

Acordo de chave usando o Padrão 1

Considerando que foi utilizado o Padrão 1, é possível acordar uma chave comum com qualquer sub-cunjunto de um grupo da seguinte forma.

- Um representante do grupo:
  1. Escolhe δ e β conforme o padrão 1.
  2. Calcula $\alpha = \varphi(\delta)$.
  3. Escolhe y coprimo com δ.
  4. Publica y, α, β, γ e δ.
- Cada usuário i do grupo após receber a sequência:
  1. Escolhe um par (x_{a_i}, x_{b_i}), tal que $\text{mdc}(x_{b_i}, \alpha) = 1$.
  2. Calcula $\gamma_i = \alpha x_{a_i}^2 + \beta x_{b_i}$.
  3. Publica γ_i.

Seja $\{e_1, e_2, ..., e_r\} \in \{1, ..., s\}$ o sub-grupo de r partes (de um total de s) que se desejam comunicar. Para o e_1, por exemplo, saber a chave deste sub-grupo, basta calcular $k = y^z \bmod \delta$, onde $z \equiv x_{b_{e_1}} \Pi_{t=2}^{r} \gamma_{e_t} \bmod \alpha$. Neste caso, teremos

$$k = y^{\beta^{r-1} \Pi_{t=1}^{r} x_{b_{e_t}}} \bmod \delta.$$

O procedimento acima não pode ser usado sobre o Padrão 2, pois é necessário que $\varphi(\delta) \not| \beta^{r-1}$; no entanto, no Padrão 2, temos que $\varphi(\delta) \not| \beta^2$. A seguir, mostraremos outro protocolo para o acordo de chaves que não exige que os parâmetros sigam os requisitos do Padrão 1.

Atualização dinâmica de chaves

Outra vantagem do esquema proposto é a capacidade de se realizar a atualização dinâmica de chaves por meio da simples modificação do parâmetro y. O método é simples: uma vez realizadas as transmissões de todos os γ_i por cada participante i de um grupo, é possível redefinir a chave a partir dos novos γ_i. Cada novo valor de y pode ser transmitido via broadcast ou pode ser gerado por um gerador de números pseudo-aleatórios, conhecido por todos, usando y anterior como semente.

Acordo de chaves usando qualquer padrão

Apresentamos, a seguir, um método que permite o acordo de chaves de conferência mesmo que os parâmetros de domínio não atendam aos requisitos especificados no Padrão 1. Embora o procedimento possa ser considerado mais "geral" — na medida em que os parâmetros de domínio não precisam atender a restrições especiais — veremos que o método não permite o acordo de chaves de conferência em rodada única — ao contrário, é necessário um número de rodadas logarítmico no número de participantes.

Algoritmo 2: Procedimento para combinação de uma chave comum entre três partes

- Alice publica α, β e δ.
- Alice e Bob combinam uma chave k_{ab} conforme algoritmo 1 com o padrão escolhido.
- Alice escolhe $x''_a < \delta$.
- Alice calcula $\gamma'' = \alpha x''^2_a + \beta k_{ab}$.
- Alice escolhe y
- Alice envia γ'' e y para Bob e para Carlos.
- Carlos escolhe seu x_{c1} e x_{c2} e calcula $\gamma''' = \alpha x^2_{c1} + \beta x_{c2}$.
- Carlos envia para Alice e para Bob γ'''.
- Alice e Bob calculam $k_{abc} = y^{\gamma'''k_{ab}} \bmod \delta$.
- Carlos calcula $k_{abc} = y^{\gamma''x_{c2}} \bmod \delta$.

Podemos observar que $k_{abc} = y^{\beta k_{ab} x_{c2}}$.

Combinação de duas chaves de conferência

Embora o método acima possa parecer mais limitado, ele apresenta vantagens em relação ao primeiro método apresentado em um cenário específico, que é quando dois conjuntos C_1 e C_2 de usuários, cada um dos quais já tendo estabelecido uma chave comum k_{C_1} e k_{C_2}, desejam estabelecer uma chave comum a $C_1 \cup C_2$. Neste caso, não é necessária a transmissão de cada um dos γ_i de cada um dos participantes de cada conjunto C_1 e C_2. Basta que um "representante" do conjunto C_1 transmita a chave de conferência k_{C_1} aos participantes de C_2, e um "representante" do conjunto C_2 transmita a chave de conferência k_{C_2} aos participantes de C_1, que todos os participantes serão capazes de estabelecer uma chave de conferência para $C_1 \cup C_2$.

Depois, um representante do grupo 1 faz o papel de Alice e um representante do grupo 2 faz o papel de Bob. Se considerarmos que o procedimento recursivo divide o grupo em dois subgrupos de tamanhos aproximadamente iguais, então a chave comum é estabelecida em $O(\log n)$ rodadas.

6. Considerações Finais

No presente trabalho, apresentamos um esquema de acordo de chaves criptográficas baseado na dificuldade de se resolver equações Diofantinas de grau 2 com duas variáveis. O esquema proposto apresenta evidentes benefícios no cenário em que se deseja estabelecer "chaves de conferência".

Pelo fato de se basear em um problema NP-completo, o esquema seria um potencial candidato a esquema resistente a ataques originado de um computador quântico. Infelizmente, como mostramos no presente artigo, o esquema é vulnerável a uma atacante que seja capaz de realizar a computação eficiente do logaritmo discreto — e, portanto, vulnerável a um atacante de posse de um computador quântico. Ainda assim, mantemos em aberto a questão sobre se seria possível, por meio de uma escolha adequada de parâmetros de domínio, tornar o esquema proposto resistente a tais ataques.

Referências

Al-Riyami, S. S. and Paterson, K. G. (2003). *Tripartite Authenticated Key Agreement Protocols from Pairings*, pages 332–359. Springer Berlin Heidelberg, Berlin, Heidelberg.

Ateniese, G., Steiner, M., and Tsudik, G. (2000). New multiparty authentication services and key agreement protocols. *IEEE Journal on Selected Areas in Communications*, 18(4):628–639.

Barker, E., Chen, L., Roginsky, A., and Smid, M. (2013). *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (NIST Special Publication 800-56A, Revision 2)*. National Institute of Standards and Technology.

Barua, R., Dutta, R., and Sarkar, P. (2003). Extending joux's protocol to multi party key agreement. *IACR Cryptology ePrint Archive*, 2003:62.

Boneh, D. and Silverberg, A. (2002). Applications of multilinear forms to cryptography. *Contemporary Mathematics*, 324:71–90.

Chunsheng, G. (2015a). Multilinear maps using ideal lattices without encodings of zero. Cryptology ePrint Archive, Report 2015/023. `http://eprint.iacr.org/2015/023`.

Chunsheng, G. (2015b). Multilinear maps using ideal lattices without encodings of zero.

Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654.

Diffie, W., Van Oorschot, P. C., and Wiener, M. J. (1992). Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 2(2):107–125.

ElGammal, T. The first ten years of public-key cryptograph. *Proceedings of the IEEE*, 76.

ElGammal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31.

Garg, S., Gentry, C., and Halevi, S. (2013). *Candidate Multilinear Maps from Ideal Lattices*, pages 1–17. Springer Berlin Heidelberg, Berlin, Heidelberg.

Hilbert, D. (1902). Mathematical problems. *Bull. Amer. Math. Soc.*, 8(10):437–479.

Hu, Y. and Jia, H. (2016). Cryptanalysis of ggh map. In *Proceedings of the 35th Annual International Conference on Advances in Cryptology — EUROCRYPT 2016 - Volume 9665*, pages 537–565, New York, NY, USA. Springer-Verlag New York, Inc.

Joux, A. (2000). *A One Round Protocol for Tripartite Diffie–Hellman*, pages 385–393. Springer Berlin Heidelberg, Berlin, Heidelberg.

Lee, Y.-R., Lee, H.-S., and Lee, H.-K. (2004). Multi-party authenticated key agreement protocols from multi-linear forms. *Applied Mathematics and Computation*, 159(2):317 – 331.

Manders, K. L. and Adleman, L. (1978). Np-complete decision problems for binary quadratics. *Journal of Computer and System Sciences*, 16(2):168 – 184.

Matijasevič, J. V. (1970). The diophantineness of enumerable sets (russian). *Dokl. Akad. Nauk SSSR*, 191:279–282.

Matsumoto, T., Takashima, Y., and Ima, H. On seeking smart public-key distribution systems. *The Transactions of the IECE of Japan*, E69.

Robinson, J. (1972). Review: Ju. v. matijasevic, a. doohovskoy, enumerable sets are diophantine. *J. Symbolic Logic*, 37(3):605–606.

Thue, A. (1902). Uber annaherungswerte algebraischer. *J. Reine Angew Math*, 135:284–305.

