Esquemas de criptografia de chave pública: elementos comuns e diferenciais

Vinicius Gadis Ribeiro[1, 2] •

Raul Fernando Weber[1]

[1] Programa de Pós-Graduação em Ciência da Computação, Universidade Federal do Rio Grande do Sul

Av. Bento Gonçalves, 9500 Agronomia CEP 91501-970 Porto Alegre/RS

[2] Coordenação de Pesquisa, Curso de Ciência da Computação, UNILASALLE

Av. Victor Barreto, 2288 Cep 92010-000 Centro - Canoas/RS - Brazil

{vribeiro, weber}@inf.ufrgs.br

Abstract*: Public key cryptography has been contributed some important functionality to computer systems security. Each pubic key scheme is based in some mathematics or computational problem, easy to solve in one way (an intended recipient) but hard to solve the inverse problem (an adversary). This paper presents a comparative study about computational problems, which is employed by public key cryptography schemes. It is reported a brief description of these problems, and a new public key scheme, called Rafaella, is presented. A comparative table containing the main features of the most commonly used public key methods is also presented.*

Keywords*: Computer security, Cryptography, Public key cryptography, Comparative study.*

Resumo: A Criptografia de chave pública tem proporcionado consideráveis facilidades à segurança de sistemas computacionais. Cada um dos diversos esquemas de chave pública é baseado em algum problema matemático - ou computacional - de considerável facilidade para uso direto (para usuários autorizados) e de elevada dificuldade de problema inverso (usuários não autorizados). O presente trabalho apresenta um estudo comparativo dos problemas na qual esquemas de criptografia de chave pública são baseados. Uma breve descrição dos problemas matemáticos – ou computacionais - nos quais se baseiam os esquemas de chave pública é relacionada, incluindo os problemas empregados por um novo esquema, chamado Rafaella. É apresentado, ao final, um quadro comparativo.

Palavras-chave: Segurança computacional, Criptografia, Criptografia de Chave Pública, Estudo comparativo.

Observação: submissão ao CACIC - não a algum Workshop.

• O primeiro autor agradece o apoio do UNILASALLE, FACENSA e ULBRA.

Esquemas de criptografia de chave pública: elementos comuns e diferenciais

1 . INTRODUÇÃO

As operações para realizar criptografia de chave pública podem ser relacionadas com um problema de difícil solução – podendo o mesmo ser computacional ou matemático. Esse problema, via de regra, deve ter duas características básicas: ser de rápida execução, para usuários autorizados, e o problema inverso deve ser de difícil resolução – o que inviabilizaria a exposição da informação sensível a adversários.

Entende-se como problema inverso ao trabalho ao qual um adversário é exposto, para tentar obter a informação sensível ou texto pleno. Normalmente, envolve a descoberta da chave privada. Os esquemas de chave pública tipicamente implementam operações que são rápidas para um usuário autorizado efetuar, mas descobrir o problema inverso é extremamente moroso.

O presente artigo compara os esquemas de chave pública, pela ótica de seus problemas computacionais – considerados por alguns autores como problemas matemáticos. Para tanto, apresenta brevemente os esquemas atualmente empregados na seção 2, em termos de seus problemas inversos. Já na seção 3 é descrito um novo esquema proposto: o esquema Rafaella, enquanto que na seção posterior é explanado o problema inverso do mesmo. Considerando-se essa proposta recente, é demandada maior discussão sobre esse método, no intuito de minimizar dúvidas. Um quadro comparativo ente os esquemas e possíveis melhoramentos sobre o esquema aqui proposto são colocados na seção V, onde também são descritos alguns trabalhos futuros.

2. CRIPTOGRAFIA DE CHAVE PÚBLICA: PROBLEMA INVERSO

Basicamente, os esquemas de criptografia de chave pública baseiam-se em problemas matemáticos de difícil solução. Dentre aqueles que são atualmente implementados, observa-se que a maioria dos esquemas determinísticos baseados em problemas matemáticos são calcados nos problemas de fatorização de números compostos, mochilas ou logaritmos discretos.

Os esquemas baseados em problemas de fatorização de números inteiros podem ser resumidas na seguinte situação: tendo-se dois números primos, é fácil calcular o produto desses. Contudo, dado o produto resultante, não é um problema fácil determinar os seus números primos compostos. Assim, diz-se que o problema inverso é a fatoração de dado número público. A mais conhecida implementação de esquemas baseados nesse problema é o RSA, proposto por Rivest, Shamir e Adleman, em 1978 – embora destaquem-se ainda os esquemas Rabin, e Williams, entre outros (Schneier,1994). Stallings (1999) lista os principais ataques efetuados contra esse esquema, destacando ataques matemáticos e relacionados com tempo.

Já esquemas baseados em problemas de mochilas podem ser descritos da seguinte forma: determinar os valores que, somados, resultaram em um determinado valor. A soma desses pesos é de fácil realização; contudo, o problema inverso não é de fácil resolução. Destacam-se aqui os esquemas Merkle-Hellman e Chor-Rivest (Schneier,1994; Nichols, 1999).

Os esquema baseados em problemas de logaritmos discretos podem ser classificados em dois grupos: os problemas de logaritmos discretos em campos finitos, e os problemas de logaritmos discretos em curvas elípticas. Os primeiros podem ser apresentados do seguinte modo: dados um número primo p, um número g e o número y, resultante do cálculo

$$y = g^a \bmod p ,$$

não é um problema fácil determinar o expoente a. O esquema mais conhecido é o ElGamal – embora tenha sido projetado para assinaturas digitais, pode ser também empregado para criptografia de dados

(Menezes, 1996; Schneier, 1994). O esquema Diffie-Hellman também pode ser aqui enquadrado, com algumas reservas – visto constituir problema próprio.

Ainda nesse âmbito, há um esquema proposto pelo neozelandês William Raike, que não é baseado explicitamente em um problema matemático, mas é baseado em características específicas de uma máquina de estados que são equivalentes ao problema do logaritmo discreto (Nichols, 1999).

Já os esquemas de chave pública baseados em problemas de logaritmos discretos em curvas elípticas podem ser expressos da seguinte forma: dados um ponto P, com suas respectivas coordenadas (x_1,y_1), a determinação do número de vezes que esse ponto foi somado com ele mesmo, resultando um terceiro ponto – ou até o mesmo, em determinadas condições - é um problema de grande dificuldade matemática – visto não haver ainda algoritmo eficaz que determine quais foram os pontos que, somados, originaram o terceiro ponto.

Assim, pode-se observar que a maioria dos problemas inversos na qual são baseados os esquemas supra mencionados têm ao menos um aspecto em comum: baseiam-se em problemas da Teoria dos Números – habitualmente, esforços computacionais com o intuito de efetuar a determinação de um número, que pode ser a chave privada, por exemplo. Contudo, esquemas baseados na Teoria dos Números não constituem exclusividade, conforme relatado a seguir.

Jacques Patarin sugeriu, em 1993, um esquema cujo problema matemático de dificuldade é a resolução de um sistema de equações polinomiais multivariadas. Sabe-se que sistemas de equações podem gerar zero, uma ou um indeterminado número de soluções. Baseado nisso, esquema similar já havia sido proposto anteriormente, por Matsumoto e Imai, em 1983.

Há esquemas que empregam características da Álgebra Linear. Um exemplo é o esquema McEliece emprega um caso especial de problema NP, para fins de decriptografia da mensagem cifrada. O problema em questão é a decodificação de um código de detecção de erros linear. A chave pública é um código linear; a chave privada é um código Goppa. O objeto que se trabalha, tipicamente, são matrizes unidimensionais – vetores -, para os quais a mensagem deve ser codificada. O algoritmo que realiza essas operações é citado na literatura como sendo de duas a três vezes mais rápido do que o RSA. Para Alice codificar um bloco de texto para Bob, ela multiplica pela matriz de codificação de Bob, e adiciona um bloco de ruído. Alguns do problemas tipicamente relatados nesse esquema são o tamanho da chave privada – normalmente, excede 1 MB -, bem como considerável expansão de dados na transformação para o texto codificado.

Na próxima seção, é apresentado o esquema Rafaella – o qual é baseado em problemas de área diversa, pois trata de problemas da área das Equações Diferenciais.

3. EQUAÇÕES DIFERENCIAIS E O ESQUEMA RAFAELLA

O esquema Rafaella foi proposto em 2004 por Ribeiro e Weber (Ribeiro, 2004), constituindo-se na alternativa mais simples para realizar mapeamentos sobre equações diferenciais. É baseado na teoria dos grupos de Lie – os quais empregam os operadores diferenciais propostos pelo matemático norueguês Marius Sophus Lie, para resolução de equações diferenciais.

Esquemas propostos por Lie para trabalhar equações diferenciais baseiam-se fortemente em simetrias. Simetrias, no contexto de equações diferenciais, são transformações que preservam as formas da equação diferencial, modificando apenas as variáveis - o que permite transformar uma solução de uma equação diferencial em outra solução de equação diferencial. Dada uma função transladada, identificar a equação diferencial por ela satisfeita é um problema cuja solução tem elevada dificuldade (Olver, 2000).

Basicamente, o esquema Rafaella trata de efetuar operações sobre funções – ou seja, translações gerando as simetrias supra citadas -, gerando outras funções. Contudo, foi observado que trabalhar

diretamente com os operadores diferenciais de Lie não é tarefa amigável (Zwillinger, 1992). Assim, ao se propor o esquema Rafaella, objetivou-se torná-lo o mais simples possível. E, como a aplicação de um operador diferencial tem a mesma conseqüência de efetuar mudanças de variável nos argumentos da função, foi escolhida uma transformação específica que realiza uma translação no plano complexo. Essa transformação é conseqüência da aplicação do exponencial de um operador de 1ª ordem com coeficientes constantes e complexos.

Dentre as funcionalidades projetadas para o esquema proposto, encontram-se a cifragem/decifragem de mensagem, e uma forma simples de autenticação, por prova de identidade com conhecimento zero.

3.1 Rafaella: o processo de cifragem

A partir de uma mensagem dada, o processo de cifragem consiste na aplicação de dez passos básicos:

1. Converter a mensagem original para valores numéricos usando, para isso, o código ASCII, compondo os coeficientes da função correspondente à mensagem - m_0;
2. Escolha de uma função real, contínua e "n" vezes derivável, contendo um número de parcelas igual ao número de coeficientes numéricos resultantes – sendo que todas as parcelas deve ser distintas entre si – seguida da adição da Chave Pública do participante receptor da mensagem. Produção de argumentos de autenticação, que contém o produto entre potências inteiras da Chaves Pública, por cada participante.
3. Aplicação, por parte do emissor, de deslocamento no plano complexo, com componentes real e imaginário – essa operação corresponde à cifragem da função original, vindo a compor a mensagem a ser remetida;
4. Envio da mensagem cifrada para o receptor autorizado;
5. Aplicação, por parte do receptor, de um novo deslocamento – tal como no passo 3 -, com componentes real e imaginário e geração de um argumento auxiliar, que consiste em uma função contínua;
6. Envio da mensagem mapeada, e do argumento auxiliar, ao emissor;
7. Aplicação, por parte do emissor, da mudança inversa e verificação da autenticidade do argumento auxiliar do receptor através da geração de um novo argumento – denominado de argumento de verificação (o novo argumento é utilizado para deturpar a mensagem cifrada, caso não se constate a autenticidade do receptor);
8. Envio, ao receptor, da mensagem mapeada e do argumento auxiliar gerado pelo emissor;
9. Aplicação da mudança inversa por parte do receptor, verificação da autenticidade do argumento auxiliar do emissor, e extração da chave pública do receptor – essa operação corresponde à decifragem da mensagem, através da qual a função original é recuperada;
10. Recuperação dos caracteres originais - os quais são os coeficientes da função original.

A codificação prévia da mensagem consiste na determinação dos códigos ASCII de cada caracter envolvido, os quais constituirão os coeficientes da função f_0.

A escolha da função contínua consiste na determinação de uma função de uma variável f(x), a partir da composição das funções básicas disponíveis em linguagens convencionais de programação: sen(x); cos(x); ln(x); exp(x); e polinomiais.

A função f(x) pode ser obtida a través da combinação linear de duas ou mais funções da lista, de composições ente funções, ou da aplicação de ambos os recursos.

A aplicação da simetria de deslocamento contendo as partes real e imaginária consiste na seguinte mudança de variável

$$x \leftarrow x + a + ib.$$

Essa mudança mapeia a função f(x) na função f(x + a + ib).

A aplicação da simetria inversa consiste na mudança de variável que atua em sentido contrário, ou seja,

$$x \leftarrow x - a - ib,$$

que mapeia f(x) em f(x - a - ib).

Salienta-se que as chaves privadas de cada participante do esquema são as componentes real e imaginária do deslocamento aplicado sobre a função f. Dessa forma, cada participante arbitra um número complexo, que é empregado unicamente para efetuar a **cifragem** e a **decifragem da função**1. A Chave Pública **do esquema proposto consiste**, por sua vez, em uma **função –** podendo eventualmente, ser empregado um **operador diferencial**, construído a partir da chave privada do participante. Como exemplo, a chave privada a = 190 + 65i, e b = 135 – 102i geram o operador diferencial A, definido como

$$25650(\partial^2/\partial x^2) - 10605(\partial/(\partial y\, \partial x)) - 6630(\partial^2/\partial y^2).$$

De posse dessa Chave Pública, o processo de reconstituição da Chave Privada é extremamente oneroso. Cabe salientar que o operador A, do exemplo dado, foi obtido a partir de uma forma fatorada bastante simples. Exemplos completos onde se aplica esse processo podem ser encontrados em Ribeiro(2004).

3.2 Rafaella: O processo de autenticação

No esquema proposto, o processo de autenticação é realizado através do cálculo de dois argumentos auxiliares; o primeiro é uma função contínua, e o segundo, um número complexo. O primeiro argumento, denominado de *argumento de autenticação*, consiste em uma função contínua, formado por combinações lineares entre potências das chaves públicas de ambos os participantes. Sobre essa função, o receptor deve aplicar sua chave privada, a fim de produzir uma nova função. A nova função obtida é, então, utilizada por parte do emissor, para verificar a autenticidade do receptor, através do seguinte teste de autenticidade:

O emissor substitui sua chave privada na função obtida, verificando o número complexo resultante. Caso o número resulte nulo, a autenticidade do emissor é constatada; caso contrário, o número complexo é multiplicado pela derivada da mensagem cifrada em seu estado atual, a fim de alterar o seu conteúdo. Dessa forma, apenas o receptor autorizado poderá, ao final do processo, recuperar a mensagem original.

Assim, emprega-se uma prova de conhecimento zero para autenticar cada uma das partes. Maiores detalhes desse processo podem ser encontradas em Ribeiro(2004).

3.3 Considerações sobre os processos de cifragem e decifragem

É importante salientar que o emprego de simetrias de Lie corresponde a aplicação de operadores diferenciais com coeficientes constantes sobre funções, o qual constitui o processo de cifragem a ser proposto no presente trabalho. O processo inverso, ou seja, a inversão do operador diferencial, e sua posterior aplicação sobre a função operada constitui o processo de quebra da mensagem cifrada, por parte do adversário.

---

1 Por cifragem de função, entende-se o mapeamento de uma função de variável real f(x) em outra função de variável complexa, o que corresponde a um caso particular de simetria de Lie translacional.

Do ponto de vista do participante, a mensagem original M deve ser codificada de tal forma que se possa representá-la por uma função f. A operação de criptografar a mensagem eqüivale a aplicar o operador que transforme a função f, tal que

$$Cf = g ,$$

sendo g, uma função correspondente a mensagem criptografada - ao passo que a operação de decifrá-la será denotada pela determinação de f, tal que

$$f = C^{-1}g .$$

O modo tradicional de se descobrir a função f consiste, portanto, em se obter a solução da equação Cf = g, através da inversão do operador C. Ocorre que o processo de inversão do operador C requer um número elevado de operações simbólicas (Ayres, 1974), o que demanda alto tempo de processamento, de modo que o procedimento clássico deve ser evitado.

O procedimento alternativo consiste em empregar operadores diferenciais particulares, para proceder à codificação e à decodificação da mensagem. Considere-se A, o operador diferencial que efetua a translação sobre o plano complexo, correspondente à partir da chave privada de Alice, e B, o operador diferencial que efetua a translação sobre o plano complexo, correspondente à partir da chave privada de Bob, do mesmo modo que Alice. A mensagem a codificar deve ser expressa na forma de uma função, f. Alice procede do modo se segue:

$$g = Af \rightarrow g_1 = Bg \rightarrow g_2 = A^{-1}g_1 \rightarrow g_3 = B^{-1}g_2 = f .$$

Pode-se demonstrar da seguinte maneira:

$$g = Af \rightarrow g_1 = Bg = Baf \rightarrow g_2 = A^{-1}g_1 = A^{-1}Baf$$
$$g_3 = B^{-1}g_2 = B^{-1}A^{-1}BAf$$

Assumindo-se que A e B comutam, tem-se que

$$g_3 = B^{-1}B\,A^{-1}A\,f \text{ , e } A^{-1}A = B^{-1}B = I ,$$

Portanto,

$$g_3 = I\,If = If = f .$$

É necessário, portanto, que os operadores A e B comutem entre si – ou seja, AB=BA.

3.4 Características do esquema Rafaella

As principais dificuldades encontradas nos diversos processos de resolução de equações diferenciais estão relacionadas a elevada quantidade de memória requerida, e o elevado tempo de processamento necessárias para a obtenção de soluções numéricas (Greenspan & Casulli, 1988; Ortega & Poole Jr, 1981; Reddy, 1986; Tikhonov 1990). Quanto aos métodos analíticos, a manipulação algébrica de expressões envolve duas dificuldades básicas:

1 – o crescimento exponencial do string função(ou tamanho da expressão); e

2 – a aplicação de determinados operadores sobre expressões analíticas (como exemplo, integrais iteradas).

A primeira dificuldade se refere a ineficácia dos algoritmos de simplificação de expressões. Em qualquer dos programas aplicativos de computação simbólica (por exemplo, *MAPLE, Mathematica, SimbMath, Derive* e outros), os comandos de simplificação limitam-se a expandir expressões, freqüentemente gerando funções com maior número de caracteres do que a expressão original a ser simplificada. Não existem atualmente, no mercado, sistemas eficientes de reconhecimento de padrões e reagrupamento de expressões algébricas, bem como publicações científicas referentes a elaboração de tais sistemas.

Já a segunda dificuldade se deve ao fato de que a aplicação de determinados operadores exige a resolução de problemas inversos.

Do ponto de vista matemático, a grande dificuldade encontrada na resolução de equações diferenciais consiste na aplicação de operadores inversos. Como exemplo, suponha-se que sobre a função

$$f(x,y) = x.cos(y) + e^{(-x2 - 3.x.y - 2.x - y)}$$

seja aplicado o operador diferencial

$$\frac{\partial^3}{\partial x^3} + 2\frac{\partial^2}{\partial x^2} + \frac{\partial}{\partial x}.$$

Tem-se, assim, como resultado a expressão

$$-5(-2x-3y+2)exp(-x^2-3xy+2x-y)+(-2x-3y+2)^3exp(-x^2-3xy+2x-y) -2x\ cos(y)+2(-3x-1)^2exp(-x^2-3xy+2x-y)+cos(y).$$

Percebe-se claramente que uma única aplicação do operador produz apreciável aumento no tamanho da expressão resultante. Ocorre que, na grande maioria dos métodos analíticos convencionais, operações dessa natureza são efetuadas recursivamente, produzindo expressões excessivamente extensas. A fim de ilustrar o argumento, os métodos espectrais baseados em operações simbólicas requerem, em média, cerca de 1.000 aplicações de operadores diferenciais análogos ao acima apresentado, produzindo expressões finais contendo entre 5.000 e 150.000 vezes mais caracteres do que havia na expressão original.

Por outro lado, as regras de manipulação de operadores diferenciais obtidos através dos grupos de Lie para a resolução de equações diferenciais parciais reduzem significativamente o número de operações simbólicas necessárias para a obtenção da expressão final, uma vez que dispensa a aplicação **direta** desses operadores diferenciais. O recurso que evita a aplicação recursiva de operadores diferenciais sobre expressões analíticas é baseado no emprego das chamadas **simetrias de Lie** das soluções particulares das equações diferenciais.

A próxima seção apresenta as dificuldades para se resolver o problema inverso.

4 DIFICULDADES PARA O PROBLEMA INVERSO: RAFAELLA

Existem, basicamente, dois argumentos que justificam a viabilidade do método como base para um esquema de chave pública: o primeiro reside no elevado número de operações simbólicas necessárias para que um adversário possa restaurar a mensagem original a partir da mensagem cifrada. O segundo argumento se refere às dificuldades encontradas na execução desse processo. Na ausência das chaves privadas, o adversário deve proceder da seguinte maneira, para decodificar a mensagem:

I) inferir a forma do operador diferencial presente na equação diferencial satisfeita por $f_0(x)$.

II) encontrar o sistema de equações determinantes, empregadas na obtenção dos coeficientes variáveis presentes nos geradores infinitesimais dos grupos de simetria;

III) resolver o sistema obtido, empregando bibliotecas de mapeamento e resolução de equações diferenciais parciais;

IV) encontrar uma solução particular da equação diferencial, para dar início ao processo de mapeamento;

V) mapear a solução particular, utilizando a exponencial de uma combinação linear dos geradores infinitesimais obtidos;

VI) inferir e aplicar as condições iniciais de contorno – ou de passagem por pontos -, que estabelecem a unicidade da solução;

VII) recuperação da mensagem original, aplicando o comando ASC sobre os códigos ASCII da função obtida.

Cada passo supra mencionado é detalhado a seguir.

A construção das equações determinantes requer, em média, cerca de 250 operações simbólicas, para equações bidimensionais parciais de segunda ordem com coeficientes variáveis. Isso ocorre porque se faz necessário calcular os prolongamentos (domínio estendido composto pelas variáveis independentes, pelas funções incógnitas e por suas derivadas) de segunda ordem dos geradores infinitesimais do grupo de simetria e, em seguida, aplicar o critério de variância infinitesimal (Olver, 2000). É importante salientar que o número de operações simbólicas requeridas para a obtenção das equações determinantes **cresce exponencialmente** com o aumento da ordem do prolongamento utilizado – que é a mesma ordem da equação diferencial a solucionar.

O número de operações simbólicas exigidas para a resolução do sistema de equações determinantes varia, essencialmente, com o grau de acoplamento do sistema obtido. Em geral, o número de operações simbólicas necessárias para resolver um sistema de equações determinantes produzidas por equações bidimensionais parciais de segunda ordem com coeficientes variáveis é da ordem de 500 – considerando que o número médio de equações determinantes situe-se em torno de 10. Ocorre que o número de operações simbólicas cresce com o quadrado do número de equações que, por sua vez, cresce linearmente com a ordem da equação diferencial a solucionar.

A obtenção de uma solução particular para a equação diferencial pode ser obtida de duas maneiras: utilizando comandos que efetuam a resolução direta da equação em formas especiais, ou encontrando as equações determinantes para a forma especial estabelecida. No primeiro caso, a solução pode ser obtida imediatamente, em uma única linha de comando. Caso a resolução direta não seja possível, deve-se retornar ao passo I), e efetuar todas as etapas do roteiro estabelecido para a forma especial da equação diferencial.

O mapeamento da solução também pode ser obtido de três formas: através do emprego de regras de manipulação para exponenciais de operadores, através do uso de expansões desses operadores em séries de Taylor, ou da resolução de equações diferenciais auxiliares. Caso existam regras disponíveis para a manipulação das exponenciais dos geradores infinitesimais obtidos, o número de operações resultantes é bastante reduzido – sendo freqüentemente da ordem do número de geradores infinitesimais (ou seja, da dimensão do grupo de Lie correspondente). O número de operações exigidas para obtenção das expansões da série de Taylor depende unicamente do raio de convergência da série, sendo proporcional ao número de termos utilizados. Já a resolução de equações auxiliares – a exemplo do cálculo de encontrar as equações determinantes para a forma especial estabelecida -, também requer a execução do algoritmo por completo.

A aplicação das condições iniciais de contorno – ou de passagem por pontos -, consistem basicamente na determinação de funções arbitrárias contidas na solução mapeada, através da resolução de equações algébricas ou diferenciais de 1ª ordem – recaindo, portanto, no mesmo problema do passo anterior.

Os demais passos são essencialmente numéricos e não exigem o emprego de operações simbólicas – mas apenas um pequeno número de operações com ponto flutuante.

Embora o crescimento exponencial do número de operações simbólicas requeridas com o aumento da ordem da equação diferencial seja suficiente para justificar a viabilidade do método, existem dificuldades adicionais na execução do próprio processo supra apresentado – de tentativa de quebra da cifragem por um adversário. Em primeiro lugar, a própria equação diferencial a solucionar não é fornecida como chave pública – de modo que se torna necessário inferir sua estrutura a partir de um processo de tentativa e erro. Além disso, as condições iniciais de contorno e passagem por pontos

também não são fornecidas. Na hipótese extremamente improvável do adversário encontrar a solução geral da equação, torna-se necessário, ainda, escolher dentre as diversas famílias de superfícies que a representam, uma superfície que obedeça às **condições de contorno implicitamente aplicadas**. Isso implica a execução de um novo processo de tentativa e erro semelhante ao aplicado na determinação da forma da equação diferencial – portanto, extremamente oneroso. Ademais, não existe nenhum procedimento sistemático para orientar o processo de tentativa e erro em ambos os casos apresentados (Czichowski, 1991). Outrossim, a solução de problemas auxiliares que surgem durante a execução dos passos do algoritmo exigem, com freqüência, a reaplicação recursiva dos cinco primeiros passos do algoritmo proposto. Esse procedimento efetuado em laço aumenta significativamente o número de operações simbólicas requeridas, uma vez que a cada aplicação recursiva desdobra exponencialmente esse número de operações.

Na próxima seção, é apresentado um quadro resumido com as características dos principais problemas inversos citados no presente trabalho, assim como considerações e trabalhos futuros no que tange ao esquema aqui apresentado.

5 . CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Com base nas informações das sessões II e IV, onde se encontram as descrições dos métodos aqui tratados, pode-se montar o seguinte quadro comparativo.

	Área do Problema	Objeto a operar	Chave Pública	Chave Privada	Problema inverso	Implementação	Esquema exemplo
Fatoração de números grandes	Teoria dos Números	Número	Nº d, relacionado com e tal que a relação $E*D \equiv 1 \text{MOD } N$ seja verdadeira	Primo relativo a z (produto dos valores anteriores aos primos escolhidos)	Fatoração de dado N grande (público)	Algorítmica	RSA(1978), Pohlig-Hellman(1978), Rabin(1979), Williams(1980)
Logaritmo discreto	Teoria dos Números	Número	Primo escolhido, número escolhido como base, e resultado da exponenciação	Valor a qualquer, o qual será expoente	Determinação do expoente ao qual foi elevado valor específico, em determinada base	Algorítmica	ElGamal(1985), Diffie-Hellman(1976)
Código Linear	Álgebra Linear	Matriz	Código linear	Código Goppa	Decodificação de código linear	Algorítmica	McEliece(1978)
Máquina de estados (logaritmo discreto)	Teoria dos Números	Número (Estados)	Estado inicial	Número de passos entre estados	Dado um estado inicial e um final, determinar o número de estados entre eles	Algorítmica	Raike (1998)
Curvas Elípticas (logaritmo discreto)	Teoria dos Números	Pontos	Pontos G (gerador, comum a todos), e P (resultado do produto da chave privada por G)	n inteiro (escolhido)	Dados dois pontos, determinar o número x pelo qual um dos pontos fora multiplicado, resultando o segundo ponto	Algorítmica	Curvas Elípticas (1985)
Soma de subconjuntos (problema da mochila)	Análise Combinatória	Número	Seqüência normal de valores (calculados perante um primo relativo)	Seqüência supercrescente de valores (cada valor é maior do que a soma de seus 2 anteriores)	Dada uma série de itens de diferentes valores, é possível agrupá-los para obter determinada soma?	Algorítmica	Merkle-Hellman(1978) ,Chor-Rivest (1985)

Sistemas de equações	Álgebra	Sistema de equações	conjunto de equações polinomiais bivariadas (quadráticas), o campo F; e conjunto de símbolos desse campo (um alfabeto)	polinômio; campo K; conjunto de identidades geradas quando da seleção da chave pública; e coeficientes das equações de um sistema	Resolução de sistema polinomial multivariado	Algorítmica	HFE(1993) , Matsumoto-Imai(1983)
Translações (Lie)	Equações Diferenciais	Função	Função ou operador diferencial	Complexo, com partes real e imaginária <> 0, ou operador diferencial	Ou varredura do plano complexo, ou processo descrito na seção IV	Necessita processador simbólico	Rafaella(2004)

Quadro 1. Quadro comparativo dos esquemas de chave pública

Consideraram-se como características a área matemática do problema, o objeto em que são aplicadas as transformações da informação para efetuar a criptografia, o que são as chaves pública e privada, o que o adversário deve fazer para tentar quebrar o esquema – descobrindo a chave privada -, o que é necessário para implementação e um ou mais esquemas representativos dessa problema inverso.

Conforme o quadro acima, é possível observar que todos os esquemas possuem abordagem algorítmica – excetuando-se o esquema baseado nas translações de Lie. As duas primeiras linhas apresentam resumidamente os esquemas que, na realidade, contém a maioria dos esquema de chave pública publicados até o presente. Os problemas da fatoração de números primos e do logaritmo discreto são conhecidos há muito tempo, e têm sido bastante explorados como funções unidirecionais – de fácil abordagem direta, mas de onerosa inversão. Alguns problemas da Teoria dos Números são conhecidos desde os gregos antigos, como os das curvas elípticas, mas seu emprego em criptografia é relativamente recente, havendo diversas idéias sendo propostas. Observa-se, contudo, problemas de outras áreas têm sido recentemente explorados – como resolução de sistemas de equações multivariadas, ou decodificação de código linear.

No que tange ao problema inverso do esquema aqui proposto, uma alternativa para o adversário quebrar o esquema seria determinar a chave privada escolhida por uma das partes. Para tanto, o oponente deveria empregar a varredura de todo o plano complexo – o que constitui um processo de tentativa e erro, também chamado de método de força bruta. A opção aqui empregada – ou seja, a partir de números complexos – é a de maior facilidade de entendimento e de implementação dente as outras possíveis mudanças de variável, sendo equivalentes ao emprego de operadores diferenciais – o que pode ser demonstrado utilizando séries de Taylor. Contudo, outras formas podem ser empregadas, como a aplicação direta dos grupos de Lie – sendo os operadores conhecidos como *operadores infinitesimais dos grupos de simetrias*.

O fato de o esquema Rafaella necessitar de um processador simbólico, ao invés de um simples algoritmo, constitui certa limitação no que tange ao imediato emprego comercial. Outra limitação é a expansão de dados que ocorre nas transformações. É necessário tratamento especial, ao se considerar problemas de ponto flutuante, entre outros. Para tanto, o Grupo de Segurança da UFRGS e outras instituições (UNILASALLE e UNIRITTER) está construindo bibliotecas para que desenvolvedores de programas possam implementar o esquema citado de modo mais amigável – empregando-se apenas os

recursos necessários para realizar os deslocamentos, ao invés de um sistema completo de processamento simbólico, bem como o tratamento necessário aos problemas de ponto flutuante.

Existem diversas formas de construir chaves públicas, empregando equações diferenciais. Todas elas, contudo, resultam na obtenção de funções ou de operadores diferenciais. Entretanto, a escolha de uma chave na forma de um operador diferencial fornece uma contra-informação ao adversário, induzindo-o a concluir que se trata de um operador presente na própria equação diferencial satisfeita por f_0 – o que, não necessariamente, é verdade.

Versões anteriores do método proposto vinham utilizando, como chaves públicas, as próprias equações diferenciais satisfeitas pela função f_0. Nesse caso, a implementação de simetrias de Lie-Bäcklund(são aquelas cujos coeficientes dos geradores infinitesimais dependem não apenas das variáveis independentes, mas também da função incógnita e de suas derivadas) (Blumen & Kumei, 1989) constituiria um fator de segurança extra a ser empregado, uma vez que tornariam inviáveis as tentativas de determinação dos geradores infinitesimais do grupo de simetria associado àquela equação diferencial. Essa versão foi abandonada em favor do esquema proposto, pelo fato de não haver necessidade de relacionar o operador diferencial utilizado (como chave pública) e a equação diferencial satisfeita pela equação f_0. Em outras palavras, a omissão da equação diferencial como medida extra de segurança foi considerado mais eficaz do que sua utilização em conjunto com as simetrias de Lie-Bäcklund.

Assim, o esquema proposto por Ribeiro e Weber constitui-se em um paradigma diferente daqueles encontrados em outros esquemas de chave pública, principalmente no que tange aos procedimentos e dificuldades que o adversário deveria fazer para quebrar o esquema. Maiores detalhes sobre a dificuldade de resolução do problema inverso pode ser encontrado em Olver (Olver, 2000). Exemplos do emprego desse esquema podem ser encontrados na área de download em http://www.sinpro-rs.org.br/vinicius.gadis.ribeiro.

REFERÊNCIAS BIBLIOGRÁFICAS

F. Ayres Jr., “Equações Diferenciais”. 2. ed. São Paulo: Makron Books, 1994.

G. W. Blumen & S. Kumei, “Symmetries and differential equations”. New York: Springer-Verlag, 1989.

G. Czichowski. “Lie Theory of Differential Equations and Computer Algebra”. Seminar Sophus Lie (Heldermann Verlag Berlin), 2 (1991), 83--91. Disponível na Internet por http, em *http://citeseer.nj.nec.com/ czichowski91lie.html*

D. Greenspan & V. Casulli,. “Numerical Analysis for Applied Mathematics, Science and Engineering”. Redwood City, CA: Addison Wesley, 1988.

A. Menezes, P. van Oorschot, & S. Vanstone. “Handbook of Applied Cryptography”. Boca Raton, CRC Press, 1996.

P. Olver. Applications of Lie Groups to Differential Equations. 2 nd ed. New York: Springer, 2000.

R. K. Nichols. “ICSA Guide to Cryptography”. New York, McGraw Hill, 1999.

J. Ortega; W. G. Poole Junior “Numerical Methods for Differential Equations”. Massachusetts: Pitman, 1981.

J. N. Reddy. “Applied Functional Analysis and Variational Methods in Engineering”. New York: McGraw-Hill, 1986.

V.G. Ribeiro, “Rafaella: um esquema de criptografia de chave pública baseado em um novo paradigma matemático”, Tese de doutorado, Programa de Pós-Graduação em Computação, Universidade Federal do Rio Grande do Sul, 2004.

W. Stallings. “Cryptography and Network Security: Principles and Practice”. Upper Saddle River, N. Jersey: Prentice Hall, 1999.
B. Schneier. “Applied Cryptography”, 2nd edition. John Wiley & Sons, 1996.
A. Tikhonov, A. et al. “Numerical methods for ill-posed problems”. Moscou: Nauka, 1990.
D. Zwillinger. “Handbook of Differential Equations”. San Diego: Academic Press, 1992.