Mecanismos de conhecimento zero empregados por esquemas de chave pública

Vinicius G. Ribeiro
Coordenação de Pesquisa – Centro Universitário La Salle UNILASALLE(UFRGS)
Av. Victor Barreto, 2288 – 91.501-970 – Canoas – RS – Brasil
Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 92.010-000 – Porto Alegre – RS – Brasil
vribeiro@inf.ufrgs.br

Rafael Campello
Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 92.010-000 – Porto Alegre – RS – Brasil
campello@inf.ufrgs.br

e

Raul F. Weber
Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 92.010-000 – Porto Alegre – RS – Brasil
weber@inf.ufrgs.br

Abstract

This paper presents a comparative study among zero-knowledge mechanisms of public-key cryptography schemes. Special emphasis is given to a new proposed scheme, which computational problem is not based in Number Theory, but in problems of Differential Equations – that allows a simple authentication mechanism.

Keywords: Computer Security, Public-key Cryptography, Zero-knowledge.

Resumo

Este artigo apresenta um estudo comparativo dos esquemas de conhecimento zero empregados em alguns esquemas de criptografia de chave pública. Especial foco é dado a um novo esquema proposto, cujo problema computacional não é baseado na Teoria dos Números, mas em problemas das Equações Diferenciais – o que permite grande simplificação em seu mecanismo de autenticação.

Palavras-chave: Segurança Computacional, Criptografia de Chave Pública, Conhecimento Zero.

1. INTRODUÇÃO

Esquemas de chave pública têm chamado a atenção da comunidade acadêmica desde a sua criação – sendo o primeiro esquema Diffie-Hellman, em 1976. Tais esquemas têm, como base matemática, problemas de difícil resolução [8].

O objetivo de um desenvolvedor de sistemas é dotar, no sistema de informações em desenvolvimento, serviços de segurança. E dentre os diversos serviços de segurança, a autenticação ocupa um espaço relevante. Em se pensando na virtualização dos sistemas, nem sempre se pode contar com uma garantia de que, na outra extremidade, a outra parte seja quem afirma ser – e, por conseqüência, ter acesso a diversos serviços do sistema. Na verdade, isso se constitui em um dos grandes problemas existentes na criptografia: em uma comunicação, como garantir autenticação de uma das partes? Por autenticação de entidade, entende-se o serviço que permite que cada parte envolvida em uma comunicação possa assegurar-se que é quem afirma ser[10].

Considerando-se que, no campo dos esquemas de chave pública, há diversas formas de uma das partes se identificar, o presente artigo compara o mecanismos de autenticação de um tipo específico empregados por esquemas de chave pública. O tipo de mecanismo específico de interesse é a prova de conhecimento zero.

O presente trabalho está organizado da seguinte forma: na seção dois, é apresentado o foco do trabalho; na seção 3, são descritos os principais esquemas de conhecimento zero, sendo apresentado de forma mais detalhada o esquema Rafaella, proposto recentemente. A quarta seção apresenta o estudo comparativo e na última seção são apresentadas as considerações finais e trabalhos futuros.

2. CONSIDERAÇÕES SOBRE AUTENTICAÇÃO

A literatura emprega extensa terminologia no que se refere a mecanismos de autenticação - ou seja, o mecanismo de segurança que garante que cada parte é quem afirma ser [10, 11]. Na maior parte dos casos, considera método de autenticação como método para identificação de uma ou mais partes envolvidas; em outras, refere-se a provas de conhecimento zero. Tipicamente, os mecanismos empregados envolvem operação de verificação, nas qual se constata – dependendo do resultado obtido por essa operação – se a entidade é ou não quem alega ser. Algumas das características dos métodos empregados referem-se a situações onde a informação pode tornar-se ilegível, caso a parte não seja quem afirma ser.

O quadro a seguir apresenta os esquemas de Chave Pública, o problema que gera a dificuldade de descobrir a Chave Privada - aqui identificado como "Elemento de Dificuldade", bem como as funcionalidades que o esquema fornece.

Esquema de Chave Pública	Elemento de dificuldade					Funcionalidade				
	A	B	C	D	E	1	2	3	4	5
DSS		*						*	*	
ESIGN				*				*	*	
Feige-Fiat-Shamir	*				*			*		*
Guillou-Quisquater	*									*
Schnorr		*						*		*
Rafaella			*			*	*			*

Quadro 1 - Quadro comparativo dos principais esquemas de chave pública com alguma forma de identificação
Fonte: Elaborado pelos autores, com base no trabalho efetuado.

onde:

A - Fatoração de Números Inteiros
B - Logaritmo Discreto
C - Polinômio Quadrático/Cúbico
D - Resíduo Quadrático Módulo n
E - Determinação da função original

1 - Cifragem de Mensagens
2 - Decifragem de Mensagens
3 - Assinatura Digital
4 - Verificação de Mensagens
5 - Identificação/Autenticação

De modo geral, os algoritmos de esquemas de Chave Pública são baseados em problemas de grande dificuldade de fatoração de números, ou ainda para a determinação de expoentes de operações modulares, ou ainda a determinação de escalares que multiplicaram determinado ponto. Assim, assume-se que a fatoração, a determinação de escalares em curvas elípticas e o cálculo do logaritmo discreto são computacionalmente inviáveis, visto a não existência - ou conhecimento - de algoritmo que o resolva em tempo polinomial.

Por exemplo, acrônimo para *Digital Signature Standard*, o DSS é empregado apenas para fins de assinatura digital, foi proposto pelo Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards*

and Technology - NIST), em dezembro de 1994. Baseia-se na dificuldade de calcular o Logaritmo Discreto de determinado número módulo um primo. A demonstração encontra-se completa em Terada [12].

O ESIGN é um esquema de assinatura digital, criado pela equipe da NTT, liderado por T. Okamoto. Segundo os autores, é tão seguro quanto o RSA, mas seria mais rápido do que esse - dadas as condições similares de tamanhos das chaves e assinaturas. Já foram propostas variações para esse esquema, com o intuito de torná-lo de mais difícil quebra. Segundo os autores, esse algoritmo pode ser estendido para trabalhar com curvas elípticas. Mais informações podem ser obtidas em Schneier [11].

Schnorr é um esquema de assinatura digital e autenticação, o qual emprega idéias baseadas em ElGamal, Fiat-Shamir, e o protocolo interativo de David Shaum, Jan-Hendrick Evertse e Jeroen van de Graaf. Tem sua segurança baseada na dificuldade de calcular logaritmos discretos. Encontra-se a demonstração desse esquema em Terada [12].

Já o esquema Rafaella trabalha com funções. Assim, os procedimentos para determinação de mensagem original constituem-se nos problemas da área das Equações Diferenciais. Dada uma função original, e aplicando-se determinadas transformações, é um trabalho muito difícil efetuar a transformação inversa, ou mesmo determinar qual a função original, mesmo empregando-se técnicas avançadas - como o emprego de operadores infinitesimais de 1ª ordem de Lie, por exemplo.

Para o presente trabalho, são considerados os mecanismos de conhecimento zero, empregados pelos esquemas de chave pública. Por "conhecimento zero", entende-se a forma pela qual um participante legítimo de um protocolo pode ser convencido da identidade do outro participante - normalmente, por intermédio da solução de algum problema da Teoria dos Números, ou da Análise Combinatória [4].

A seção seguinte apresenta os principais esquemas de conhecimento zero.

3. AUTENTICAÇÃO POR PROVA DE CONHECIMENTO ZERO

Há diversas formas de classificar os esquemas de chave pública que empregam algum tipo de autenticação. No presente trabalho, interessa o estudo e a classificação dos métodos empregados em esquemas que ofereçam a funcionalidade de identificação, buscando identificar a forma pela qual é possível efetuar a identificação é realizada – mesmo sem alguma informação do outro usuário -, e o que ocorre caso um usuário não autorizado resolva passar-se por um participante do esquema. Trata-se, assim, de identificar os problemas matemáticos envolvidos nesses serviços, e como eles são empregados.

Um dos mais comuns problemas em criptografia diz respeito a um participante autorizado obter provas que o outro participante realmente é quem afirma [6, 11]. Implicitamente, essa colocação envolve a noção de comunicação entre partes, bem como as regras para essa comunicação – ou seja, um protocolo. Tipicamente, os esquemas de chave pública que empregam serviços de autenticação e semelhantes têm regras bem definidas para, em algum passo do protocolo, possibilitar a verificação da prova que identifica a outra parte. Pelo menos, duas partes se envolvem: o proponente da prova e o verificador.

Há diversas formas de realizar comprovações da identidade de um participante. Há protocolos criptográficos que identificam pessoas, através de testemunhos; há esquemas onde são geradas e verificadas assinaturas digitais; há também os esquemas onde não se conhecem detalhes do outro participante, mas há formas de mostrar que esse participante é quem afirma ser, por apresentar alguma prova: são os chamados esquemas de conhecimento zero [1].

O primeiro esquema baseado nesse últimos foi formalmente proposto por Goldwasser, Micali e Rackoff, em 1985 [2], considerando interação entre as partes. Esquemas de conhecimento zero podem classificados em quatro grandes grupos, segundo o modelo formal de computação proposto pelos autores citados anteriormente [5]:

- conhecimento zero perfeito;
- conhecimento zero com verificador honesto;
- conhecimento zero computacional; e
- conhecimento zero estatístico.

Diferente de empregar apenas uma função unidirecional para revelar determinada informação, tais esquemas provêem a funcionalidade de permitir que o verificador venha a conhecer algo que não poderia de ninguém, exceto pelo proponente da prova. O emprego de uma função unidirecional apenas possibilita informar que o proponente tem uma parte da informação, sem fornecer modo algum de determinar qual é a informação [11].

O esquema de prova de conhecimento zero perfeito tem, como exemplo mais fiel, o esquema proposto por Schnorr; já o exemplo que se baseia na prova de conhecimento zero com verificador honesto tem como exemplo o esquema heurístico Fiat-Shamir [11].

A seguir, são apontadas as descrições do funcionamento dos esquemas – ou seja, por que razão uma das partes pode vir a identificar a outra, mesmo sem estar em sua presença física.

3.1 Esquemas baseados em problemas da Teoria dos Números

Os esquemas de criptografia de chave pública pertencentes a essa família são baseados, em geral, nos problemas de fatoração de grandes números e logaritmo discreto. Com relação aos esquemas que empregam para fins de autenticação, tem-se como exemplos representativos os esquemas Guillou-Quisquater e Feige-Fiat-Shamir. No caso dos esquemas de criptografia de chave pública baseados em resolução de equações diferenciais, tem-se como exemplo representativo o esquema Rafaella, descrito em seção posterior.

O esquema proposto inicialmente por Amos Fiat e Adi Shamir é basicamente um esquema de autenticação e de assinaturas digitais. Posteriormente, com a participação de Uriel Feige, esse esquema foi alterado para constituir uma chamada prova de identidade com conhecimento zero. Atualmente, é considerado o melhor esquema para prova de identidade com conhecimento zero [11, 13]. Para esse esquema, é necessário empregar um árbitro - cuja principal função é realizar a escolha de um número randômico módulo n (produto de dois números primos grandes). O número n pode ser compartilhado com todos os envolvidos - interessados em se autenticar [11].

Para gerar as Chaves Pública e Privada de Alice, o árbitro de confiança escolhe um número v - v é um resíduo quadrático módulo n. Em outras palavras, escolhe v, tal que

$$x^2 = v \bmod n$$

tenha uma solução, e v^{-1} mod n exista. Essa última expressão é a chave pública. Calcula-se, então, s - o menor valor encontrado nas raízes da expressão

$$s = (\sqrt{(1/v)}) \bmod n,$$

que é a chave privada.

Para fins de identificação, tem-se o seguinte protocolo:

1 - Alice escolhe um número randômico r, sendo r menor do que n. Ela calcula $x = r^2$ mod n, e manda x para Bob.

2 - Bob manda um bit randômico b para Alice.

3 - Dependendo do valor do bit, Alice manda um valor diferente a Bob. Se o valor do bit for 0, Alice manda r para Bob. Se o valor do bit for 1, Alice manda y - sendo y = r * s mod n.

4 - Se o valor de b for igual a 0, então Bob verifica que $x = r^2$ mod n - o que prova que Alice conhece o valor de √x. Se o valor do bit for igual a 1, então Bob verifica que $x = y^2 * v$ mod n, o que prova que Alice conhece o valor de √ (x/v).

Destaca-se que esse protocolo deve ser realizado diversas vezes, para que Bob fique convencido que Alice conhece o valor de s - o qual depende do valor de v, escolhido pelo árbitro de confiança, que conhece a ambos. Em outras palavras, se ela desejar enganar Bob, terá apenas 50 % de chances de fazê-lo, em 1 tentativa. Em t tentativas, as chances dela são de 1 em 2^t. Ou seja, esse protocolo busca identificar a primeira pessoa(Alice) perante uma segunda (Bob).

Posteriormente, esse esquema foi alterado para um esquema de realmente executar a identificação: basicamente, Bob não envia apenas um bit, mas uma string de bits ($b_1b_2b_3..b_k$), e Alice realiza o cálculo $y = r * (s_1b_1 * s_2b_2 *... * s_nb_k)$ mod n - ou seja, s só é multiplicado, se o bit correspondente tiver calor 1; se tiver valor 0, não o será. De modo análogo, Bob verifica que $x = y * (v_1b_1 * v_2b_2 *... * v_nb_k)$. Da mesma forma, deve ser repetido t vezes, sendo a chance de que Alice engane Bob é de uma em 2^{kt}.

Modificações posteriores permitiram que esse esquema se tornasse um esquema de assinatura digital, e ainda, esquemas envolvendo mais de duas pessoas. Há autores que colocam a possibilidade de se embutir informação no protocolo, o que possibilitaria a operação de cifragem [11].

O esquema Guillou-Quisquater

O esquema Guillou-Quisqueter é uma outra forma de realizar um método de identificação, como conhecimento zero, mas com um menor número de iterações entre os participantes do esquema[13]. Contudo pode, com algumas alterações, ser convertido em um esquema de assinatura verificável publicamente. Esse esquema é uma extensão do Esquema Fiat-Shamir, mas com menor troca de mensagens, e se baseia na dificuldade da Fatoração de Números Primos.

Alice remete suas credenciais - J - para Bob. Essas credenciais podem ser uma grande *string* contendo dados diversos, como se fora um cartão de crédito , ou *smart card* - tais como nome, data de nascimento, nome do cartão, data de validade, número da conta bancária, entre outros. Qualquer outra informação que possa se tornar pública, é um expoente v e um módulo n - produto de dois grandes números primos. Já a chave privada é B, calculada tal que

$$JC_P^v \equiv 1 \pmod n.$$

Tendo remetido as suas credenciais para Bob, agora Alice deseja provar que essas credenciais lhe pertencem. Para tanto, deve provar que conhece "C_P", a Chave Privada, sem expô-la.

O esquema empregado para identificação é executado em três fases, e pode ser resumido da seguinte forma:

A - Fase de determinação dos parâmetros gerais

1 - Um terceiro confiável escolhe dois números primos grandes, e calcula n = p*q.

2 - A entidade confiável escolhe v - público - , tal que $v \leq 3$, e que seja relativamente primo a (p-1)*(q-1).

3 - A entidade confiável calcula s - secreto -, tal que $s = v\text{-}1 \bmod (p-1)*(q-1)$, e disponibiliza publicamente os parâmetros "v" e "n".

B - Fase de escolha dos parâmetros individuais

1 - Cada usuário recebe uma identificação única de usuário, I_u. Calcula-se uma identificação redundante J_u, a partir de uma função pública e conveniente, tal que $J_u = F(I_u)$, que J_u seja relativamente primo a "n", e que $1 \leq J_u \leq n$. "J_u" é a credencial de cada usuário.

2 - A entidade confiável calcula o segredo "s" para cada usuário. O objetivo será a posterior comprovação da identidade pelo conhecimento do segredo, associado à Chave Pública.

C - Fase de Identificação

1 - Alice escolhe um número randômico "r", tal que $1 < r < n-1$, e calcula o chamado testemunho $T \equiv r^v \pmod n$. Remete, então, T a Bob, juntamente com sua identificação única - fornecida por um terceiro confiável.

2 - Bob remete a Alice um desafio "e", tal que $1 \leq e \leq v$.

3 - Alice realiza a verificação para constatar se "e" se encontra nos limites. Caso se encontre no limite, ela envia a Bob a resposta

$$y = r\,(s_A)^e \bmod n.$$

4 - De posse da função f - que é pública -, Bob calcula $J_A = f(I_A)$, e $z = J^e_A\, y^v \bmod n$. Caso z seja diferente de zero, e for igual a x, Bob aceita a identidade de Alice.

Cabe questionar por que Bob aceita a identidade de Alice, caso z = x. Observa-se que

$$\begin{aligned} z &= J^e_A\, y^v \bmod n \\ &= J^e_A\, (r(s_A)^e)^v \bmod n \\ &= r^v(J_A\, (s_A)^v)^e \bmod n \\ &= r^v((s_A\,)^s(s_A)^v)^e \bmod n \\ &= r^v(1)^e \bmod n \\ &= r^v \bmod n = x. \end{aligned}$$

Destaca-se a dificuldade de determinar x^{-v}, sem fatorar n - pois é computacionalmente inviável, sendo equivalente ao problema de se decifrar RSA sem conhecer a chave secreta. A condição de z ser diferente de zero decorre da possibilidade que um adversário, passando-se por Alice, escolha r = 0 - o que incorreria em z = 0 (Terada, 2000). Esse esquema também pode ser alterado para possibilitar assinatura digital [11].

Na próxima seção, é apresentado um esquema baseado em paradigma não da Teoria dos Números, mas da área das Equações Diferenciais.

3.2 Esquemas baseados em grupos de Lie

Diferente dos esquemas tradicionais, baseados fortemente em grupos de Galois, essa família é baseada nos chamadas simetrias de Lie. O primeiro esquema dessa família foi proposto por Ribeiro e Weber, em 2004 [9], e é baseado na dificuldade de se identificar translações de variáveis sobre funções, considerando as propriedade das simetrias de Lie. A chave pública, nesse esquema, é uma função construída a partir da chave privada do usuário; a chave privada é um número complexo com as partes real e imaginária diferentes de zero. O problema inverso é a dificuldade é a determinação qual seria a possível equação diferencial que originaria as funções que transitam em aberto. Ao atacante, cabe apenas duas alternativas: determinar essa equação diferencial ou a varredura de todo o plano complexo. Empregado para realizar a cifragem de mensagens, inclui a funcionalidade de prova interativa de conhecimento zero. Contudo, todas as operações constituem procedimentos sobre funções, e não sobre números - razão pela qual o esquema Rafaella emprega programas de processamento simbólico (*Derive*, *SimbMath*, *Mathematica* ou *Maple V*®).

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 – podendo até ser empregado um operador infinitesimal dos grupos de Lie. 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 proponente da prova deve aplicar sua chave privada, a fim de produzir alterações sobre uma nova função. A nova função obtida é, então, utilizada por parte do verificador , para verificar a autenticidade do proponente da prova, através de um teste de autenticidade. A construção e a verificação são apresentadas a seguir:

Basicamente, é construída uma função em duas variáveis, empregando-se as chaves pública de cada participante, e a chave privada de participante verificador. O cálculo do chamado *argumento de autenticação* consiste em uma função contínua, formado pelo produto das chaves públicas de ambos os participantes, somados com uma função cuja raiz é a sua própria chave privada. Por exemplo,

$$aa = C_{pub}A * C_{pub}B + (y - C_{priv}A)^n.$$

Sobre essa função, o receptor deve aplicar sua chave privada, a fim de reduzir a uma expressão cuja validação final será efetuada pelo verificador. Assim, o receptor - Bob - retira o fator das chaves públicas, ao aplicar a sua chave privada

$$ta = aa(C_{priv}B) = C_{pub}A * 0 + (y - C_{priv}A)^n = (y - C_{priv}A)^n$$

, resultará a expressão ta - que nada mais é senão uma função cuja raiz é a chave privada de Alice.

A nova função obtida é, então, utilizada por parte do emissor, para verificar a autenticidade do receptor, através de um simples teste de autenticidade: ao aplicar na função restante a chave privada, deverá resultar no valor zero. Essa prova reconhece que o receptor realmente é quem afirma ser, por ter aplicado no argumento de autenticação a correta chave privada. Ou seja,

$$ta = 0.$$

Caso o número resulte nulo, a autenticidade do receptor é constatada; caso contrário, o verificador interrompe o processo, não permitindo que a mensagem final seja conhecida. Dessa forma, apenas o receptor autorizado poderá, ao final do processo, recuperar a mensagem original.

Esse processo é ilustrado no quadro a seguir, onde os passos referentes à autenticação da mensagem são destacados com um "S".

Procedimento do passo	Processo de Autenticação (S/N)
1. conversão da mensagem	N
2. escolha da forma da função e produção de argumentos de autenticação	S
3. aplicação do 1º deslocamento no plano complexo	N
4. envio da mensagem cifrada	N
5. aplicação do 2º deslocamento	S
6. envio da mensagem obtida	N
7. aplicação do 1º deslocamento inverso e verificação da autenticidade do proponente da prova	S
8. envio da mensagem obtida	N
9. aplicação da 2ª mudança inversa e verificação da autenticidade do verificador	S
10. recuperação dos caracteres originais	N

Quadro 2: Passos do esquema Rafaella onde se empregam procedimentos de autenticação

Na próxima seção, são levantadas considerações gerias sobre os esquemas.

4. CONSIDERAÇÕES FINAIS SOBRE OS ESQUEMAS DE CONHECIMENTO ZERO

Dentre diversos esquemas de chave pública que empregam prova de conhecimento zero, com o intuito de autenticar a outra parte, foi construído o quadro a seguir.

Esquema de Chave Pública	**Operações**	**Elementos sobre o qual são realizadas transformações**	**Condição de Aceitação**	**Área matemática do(a)**	
				problema inverso	**condição de aceitação**
Guillou-Quisquater	Algorítmicas	Números	Bob aceita a identidade de Alice, se z<> 0, e z = x	Teoria dos Números	Teoria dos Números
Feige-Fiat-Shamir	Algorítmicas	Números	Dependendo do valor do bit, Alice manda um valor diferente a Bob. Se 0, Alice manda r. Se 1, Alice manda y. Se b = 0 então Bob verifica que $x = r^2$ mod n (Alice conhece $\sqrt{x}$). Se b = 1 então Bob verifica que $x = y^2 * v$ mod n (Alice conhece $\sqrt{(x/v)}$).	Teoria dos Números	Teoria dos Números

Rafaella	Algébricas	Funções	Bob retorna a Alice uma função recebida de Alice, e devidamente operada por Bob. Se Alice obtiver o valor nulo ao inserir sua chave privada, aceita a identidade de Bob	Equações Diferenciais	Teoria dos Números

Quadro 3: Comparação entre esquemas de conhecimento zero dos esquemas de chave pública
Fonte: elaborado pelos autores, com base no estudo realizado.

Como é possível observar do quadro acima, os esquemas Feige-Fiat-Shamir, Guillou-Quisquater e Rafaella empregam problemas de determinação ou comparação com valores numéricos - sendo que o esquema Rafaella difere dos demais por seu mecanismo operar sobre funções, e seu problema inverso pertencer à área das equações diferenciais. Aparentemente, mecanismos de prova de conhecimento zero dificilmente diferirão de realizar operações - sejam numéricas, sejam algébricas - e posterior comparação com valores. Uma diferença do esquema Rafaella é o emprego de programas de processamento algébrico ou simbólico.

Considerando as informações de Ribeiro [8], o seu problema inverso é de difícil solução [2, 7]. Em Ribeiro, são levantadas considerações sobre o desempenho desse novo esquema - graças à dependência de empregar os programas supracitados. Outra diferença desse esquema sobre os outros é funcionalidade: sua principal funcionalidade é a cifragem e decifragem de mensagens, e não especificamente a autenticação dos participantes - embora, para essa funcionalidade, seja empregado de modo simétrico: tanto Alice identifica Bob, quanto Bob identifica Alice.

5. REFERÊNCIAS BIBLIOGRÁFICAS

[1] Blum, Manuel; De Sanctis, Alfredo; Micali, Silvio & Persiano, Giuseppe, *Non-interactive zero knowledge*, march 1995.

[2] Blumen, G. W. and Kumei, S. *Symmetries and differential equations*. New York: Springer-Verlag. 1989.

[3] Goldreich, Oded & Kahan, Ariel. "How to construct zero knowledge proofs systems for NP", Journal of Cryptology, march 1999.

[4] Koblitz, Neal. *Algebraic Aspects of Cryptography*. Berlin, Springer-Verlag. 1999.

[5] Mao, W. *Modern Cryptography – Theory and Practice*. Upper Saddle River: Prentice Hall. 2004.

[6] Menezes, A.; van Oorschot, P. & Vanstone, S. *Handbook of Applied Cryptography*. Boca Raton: CRC Press. 1996.

[7] Olver, P. *Applications of Lie Groups to Differential Equations*. New York: Springer. 2000.

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

[9] Ribeiro, Vinicius Gadis & Weber, Raul Fernando. Problemas matemáticos para esquemas de criptografia de chave pública. *Anais do SBRC/Wseg 2004*. Porto Alegre: Instituto de Informática/UFRGS. 2004. p. 101-112.

[10] Stallings, W. *Cryptography and Network Security: Principles and Practice*. Upper Saddle River: Prentice Hall. 1999.

[11] Schneier, Bruce. *Applied Cryptography - Protocols, Algorithms and Source Code in C*. New York: John Wiley & Sons. 1994.

[12] Terada, Routo. *Segurança de Dados - Criptografia em redes de computador*. São Paulo: Ed. Blücher. 2000.

[13] Weber, Raul F. Criptografia Contemporânea. In: Simpósio de Computadores Tolerantes a Falhas, 6, 1995, Canela. *Anais*... Porto Alegre: Instituto de Informática da UFRGS, 1995. pp. 7-32.