Acordo de Chaves Hierárquico e Resistente ao Comprometimento de Nós

Vilc Q. Rufino

Instituto de Matemática e Estatística - Universidade de São Paulo

Fundamentos Metodológicos
MAC-5700 – Prof. Routo Terada
Novembro/2008

Sumário

Objetivo

- Objeter um algoritmo(procedimento), não interativo, para combinação de chaves criptográficas;
- Dentro de uma estrutura hierárquica para distribuição de chaves;
- Resistente ao comprometimento de qualquer número de nós *folhas* [1];
- Resistente ao comprometimento dos demais nós na hierarquia dentro de um *fator aceitável* [2].

[1] elementos no nível mais inferior dentro da hierarquia

[2] por exemplo o número máximo de nós comprometidos

Objetivo

- Objeter um algoritmo(procedimento), não interativo, para combinação de chaves criptográficas;
- Dentro de uma estrutura hierárquica para distribuição de chaves;
- Resistente ao comprometimento de qualquer número de nós *folhas* [1];
- Resistente ao comprometimento dos demais nós na hierarquia dentro de um *fator aceitável* [2].
- Eficiente e baseado em tecnologias modernas (diferente da estudada até o momento).

[1] elementos no nível mais inferior dentro da hierarquia

[2] por exemplo o número máximo de nós comprometidos

Motivação


MENSAGEM
NÃO CIFRADA
MENSAGEM
CIFRADA
MENSAGEM
DECIFRADA

Motivação

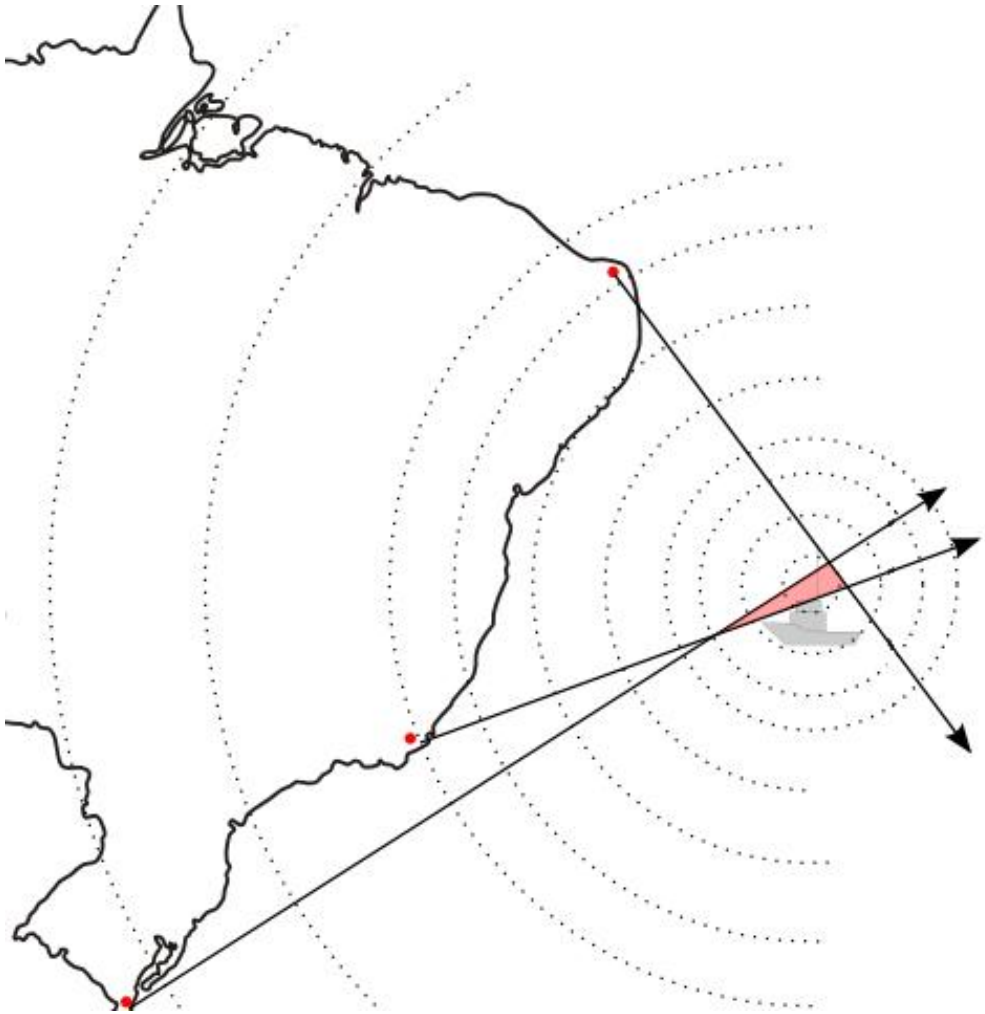

MENSAGEM
NÃO CIFRADA
MENSAGEM
CIFRADA
MENSAGEM
DECIFRADA

Motivação

- A distribuição de chaves criptográficas é o principal problema em sistemas criptográficos [Blundo et al.98];
- Os métodos mais utilizados usam da interação para a combinação de chaves;
- Porém quando a largura de banda é escassa e existem poucos recursos há necessidade de soluções não interativas;
- Em áreas de conflito militares a comunicação irradiada aumenta o risco de *exposição*[3], neste caso é fundamental a não interação para a combinação de chaves;
- Tipicamente em grandes organizações é desejável que a concessão de chaves possa ser realizada por entidades em níveis hierárquicos.

[3] a tecnologia atual permite triangularizar a origem de emissões eletromagnéticas e localizá-las

Motivação



Contribuição

- Combinação das melhores propriedades dos esquemas de acordo de chaves e distribuição de chaves hierárquica;
- Descrição de alto nível de um esquema resistente ao comprometimento de nós dentro de uma hierarquia;
- Novos nós podem ser adicionados a hierarquia sem que haja nova coordenação central;
- Flexibilidade do esquema baseado na identidade.

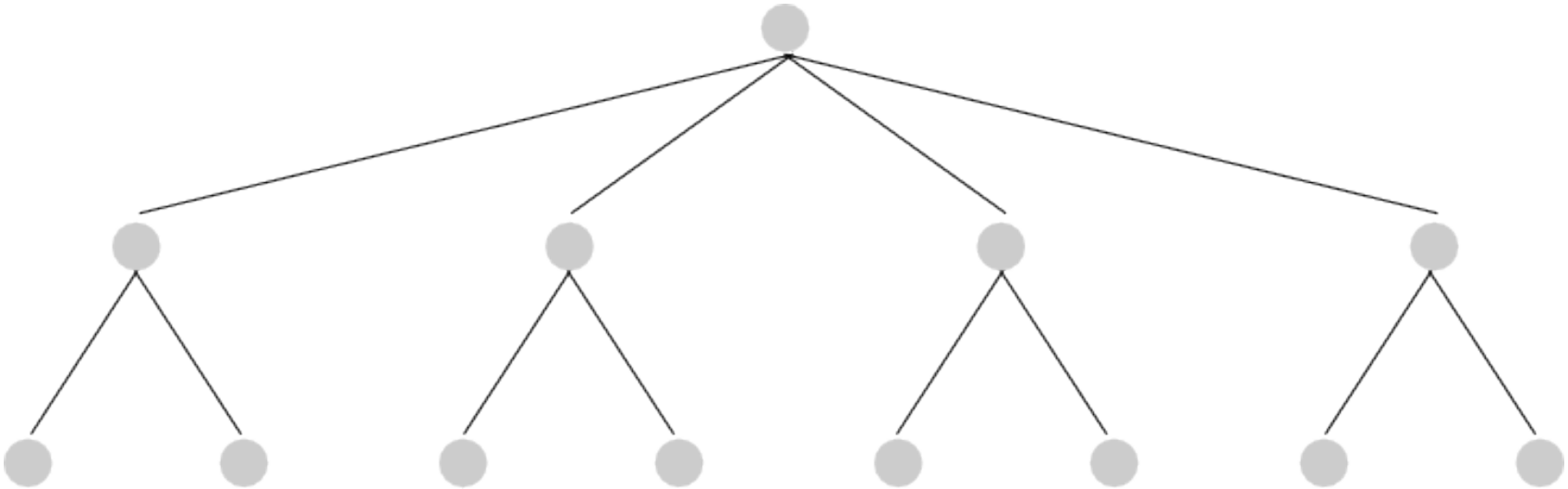
Trabalhos Relacionados

- Acordo de chaves não interativos há trabalhos como [Sakai 00], [Blundo et al.98], [Eschenauer e Gligor 02] com extensões de [Ramkumar et al 05].
- em [Blundo et al.98] e [Hanaoka et al 02] há um estudo de resistência dos modelos mais gerais, que se aplicam ao modelo estudado. Também apresenta a interferência de fatores como a existência de nós que nunca se comunicam.
- Estudos de sistemas baseados em identidade destacam-se [Boneh, Franklin 01], o trabalho de [Misaghi 08] desenvolvido na Poli-USP.

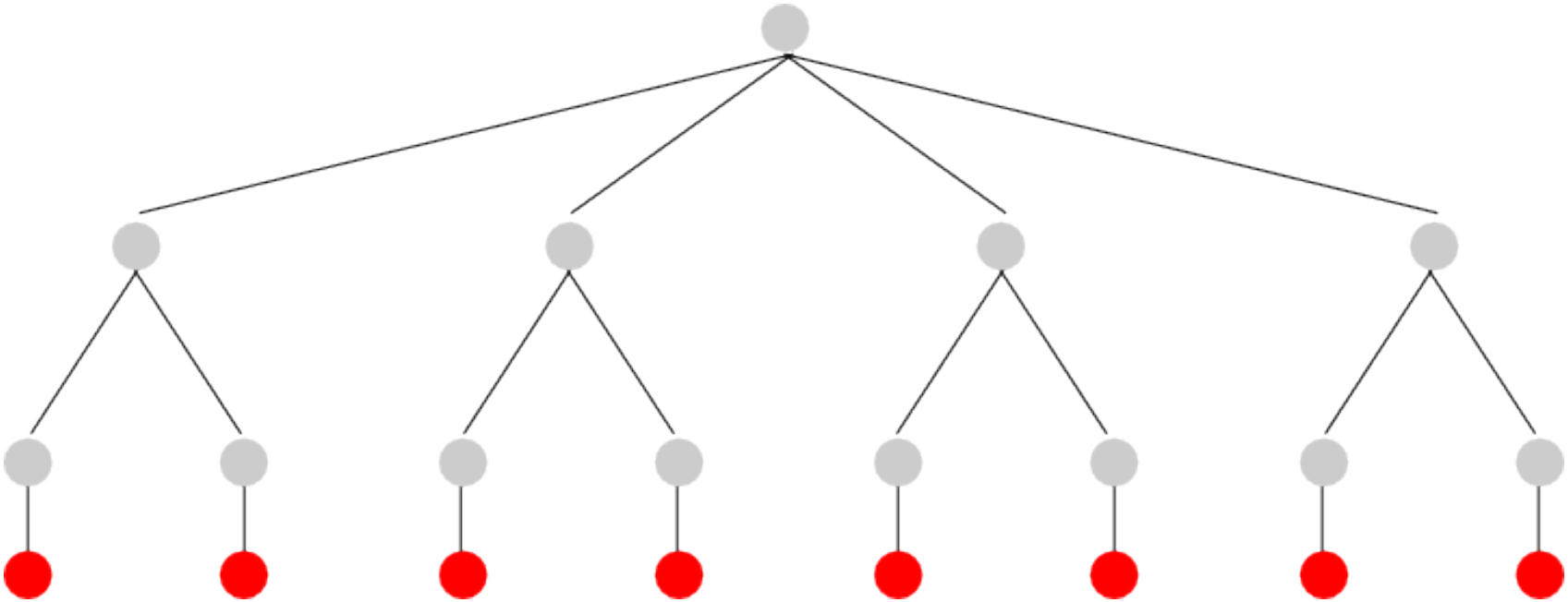
Acordo de Chaves

- Clássico [Diffie, Hellman 76]:
  - Requer formas de legitimação;
  - Necessidade de divulgação da chave pública; e
  - Comum a validação no momento da comunicação;
  - Ação evitada em ambientes de conflito, para minimizar emissões.
- Sistema baseado na identidade [Shamir 84]:
  - A chave pública é a própria identidade dos elementos participantes;
  - Requer uma única autoridade que emita as chaves secretas;
- Hierárquico:
  - Permitem que autoridades em níveis inferiores emitam as chaves de seus subordinados, independente de autoridade superior;
  - Maior flexibilidade para manuteção das chaves;
  - Ideal para ambientes militares e redes móveis ad-hoc;

Visão Macro



Visão Macro



Meta Esperada

- Reformular a proposta de [Gennaro et al 08] e incluir:
  - Otimização no cálculo da chave compartilhada;
  - Criar modelo independente de Criptografia assimétrica sem Infra-estrutura de Chaves Públicas (ICP);
  - Implementar um esquema usando “Certificateless”.

Meta Mínima

- Reformular a proposta de [Gennaro et al 08] e incluir:
  - Otimização no cálculo da chave compartilhada;

Meta Desejável

- Criar uma nova proposta para:
  - Implementar um esquema baseado em "Emparelhamento Bilinear" que satisfaça todos os níveis da hierarquia.

Mapeamento Bilinear

- Seja:
  - $\mathbb{G}_1$ e $\mathbb{G}_2$ grupos de ordem q (primo grande);
  - para todos a e $b \in \mathbb{Z}_q$; e
  - para todos P e $Q \in \mathbb{G}_1$.
- $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ é um mapeamento:
  1. Bilinear se $e(P^a, Q^b) = e(P, Q)^{ab}$;
  2. Não degenerativo se $e(P, Q)$ não leva à identidade em $\mathbb{G}_2$; e
  3. Computável se há algorítmo eficiente que calcule $e(P, Q)$.

Problema de Decisão Bilinear de Diffie-Hellman (BDDH)

- Apresentado por [Boneh, Franklin 01]
- Seja:
  - $\mathbb{G}_1$ e $\mathbb{G}_2$ grupos de ordem prima q;
  - $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ um mapeamento bilinear;
  - P um gerador de $\mathbb{G}_1$;
  - $a, b, c \in \mathbb{Z}_q^*$.
- O problema BDDH (original) em $\langle \mathbb{G}_1, \mathbb{G}_2, e \rangle$ é:

  Dado $\langle P, aP, bP, cP \rangle$
  Calcular um valor $W = e(P, P)^{abc}$

Problema de Decisão Bilinear de Diffie-Hellman (BDDH)

- Apresentado por [Boneh, Franklin 01]
- Seja:
  - $\mathbb{G}_1$ e $\mathbb{G}_2$ grupos de ordem prima q;
  - $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ um mapeamento bilinear;
  - P um gerador de $\mathbb{G}_1$;
  - $a, b, c \in \mathbb{Z}_q^*$.
- O problema BDDH em $\langle \mathbb{G}_1, \mathbb{G}_2, e \rangle$ é:

  Dado $\langle P, P^a, P^b, P^c \rangle$
  Distinguir se um valor $W = e(P, P)^{abc}$ de um outro $W = e(P, P)^r$, para valor aleatório $r \in \mathbb{Z}_q$

Acordo de Chaves Baseado em Identidades

- proposto por [Sakai 00]
- Autoridade do sistema define:
  - Dois grupos cíclicos $\mathbb{G}_1$ e $\mathbb{G}_2$;
  - O mapeamento bilinear $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$;
  - Uma função hash $H : \{0,1\}^* \rightarrow \mathbb{G}_1$;
  - Uma chave secreta $s \in \mathbb{Z}_q^*$; e
  - Calcula para cada identidade ID a chave secreta $S_{ID} = H(ID)^s \in \mathbb{G}_1$
- A chave compartilhada de ID_1 e ID_2 é $K = e(H(ID_1), H(ID_2))^s \in \mathbb{G}_2$;
- ID_1 calcula $K = e(S_{ID_1}, H(ID_2))$; e
- ID_2 calcula $K = e(H(ID_1), S_{ID_2})$.

Acordo de Chaves Hierárquicos Baseados em Polinômios

- Modelo baseado em polinômio multivariável seguindo [Blundo et al.98];
- Seja:
  - L a profundidade da hierarquia (raíz 0 e último nível L);
  - A ID corresponde o caminho da raíz até o nó, para um nó de nível i a ID é uma seqüência com i elementos $\langle ID_1, \ldots, ID_i \rangle$;
  - O nível de segurança em cada nível será definido pelo "threshold" $\{t_i : 1 \leq i \leq L\}$;
  - A raíz escolhe a chave secreta, um polinômio $F(x_1, y_1, \ldots, x_L, y_L)$ sobre $\mathbb{Z}_q$ (q primo), tal que: $F(x_1, y_1, \ldots, x_L, y_L) \equiv F(y_1, x_1, \ldots, y_L, x_L)$
  - o grau de x_i e y_i é t_i

Acordo de Chaves Hierárquicos Baseados em Polinômios

- Uma maneira simples de construir F:

Acordo de Chaves Hierárquicos Baseados em Polinômios

- Uma maneira simples de construir F:

$$F(x_1, y_1, \ldots, x_L, y_L) = f(x_1, y_1, \ldots, x_L, y_L) + f(y_1, x_1, \ldots, y_L, x_L)$$

Acordo de Chaves Hierárquicos Baseados em Polinômios

- Tamanho da descrição de F (número de coeficientes):

Acordo de Chaves Hierárquicos Baseados em Polinômios

- Tamanho da descrição de F (número de coeficientes):

$$\prod_{i=1}^{L} \frac{(t_i + 1)(t_i + 2)}{2}$$

- onde:

L é a pronfundidade da hierarquia; e
t_i é o grau de x_i e y_i.

Acordo de Chaves Hierárquicos Baseados em Polinômios

- Tamanho da descrição de F (número de coeficientes):

$$\prod_{i=1}^{L} \frac{(t_i + 1)(t_i + 2)}{2}$$

- onde:

  L é a pronfundidade da hierarquia; e
  t_i é o grau de x_i e y_i.

- Este esquema só poderá ser usado com moderados valores de t_i e pequenos valore de L.

Acordo de Chaves Hierárquicos Baseados em Polinômios

- A chave secreta é o próprio polinômio F;
- A chave secreta de um nó no primeiro nível é $F_{ID} = F(ID_1, y_1, x_2, y_2, \ldots, x_L, y_L)$, um polinômio de $2L - 1$ variáveis;

Acordo de Chaves Hierárquicos Baseados em Polinômios

- A chave secreta mestra é o próprio polinômio F;
- A chave secreta de um nó no primeiro nível é $F_{ID} = F(ID_1, y_1, x_2, y_2, \ldots, x_L, y_L)$, um polinômio de $2L - 1$ variáveis;
- A chave secreta de um nó no nível i é $F_{ID} = (ID_1, y_1, \ldots, ID_i, y_i, x_{i+1}, y_{i+1}, \ldots, x_L, y_L)$ um polinômio de $2L - i$ variáveis;

Acordo de Chaves Hierárquicos Baseados em Polinômios

- A chave secreta mestra é o próprio polinômio F;
- A chave secreta de um nó no primeiro nível é $F_{ID} = F(ID_1, y_1, x_2, y_2, \ldots, x_L, y_L)$, um polinômio de $2L - 1$ variáveis;
- A chave secreta de um nó no nível i é $F_{ID} = (ID_1, y_1, \ldots, ID_i, y_i, x_{i+1}, y_{i+1}, \ldots, x_L, y_L)$ um polinômio de $2L - i$ variáveis;
- A chave secreta de um nó folha é $F_{ID} = (ID_1, y_1, \ldots, ID_L, y_L)$ um polinômio de $2L - L = L$ variáveis.

Acordo de Chaves Hierárquicos Baseados em Polinômios

- A chave compartilhada entre dois nós folhas de identidades $ID^A = \langle ID_1^A, \ldots, ID_L^A \rangle$ e $ID^B = \langle ID_1^B, \ldots, ID_L^B \rangle$ é:

Acordo de Chaves Hierárquicos Baseados em Polinômios

- A chave compartilhada entre dois nós folhas de identidades $ID^A = \langle ID_1^A, \ldots, ID_L^A \rangle$ e $ID^B = \langle ID_1^B, \ldots, ID_L^B \rangle$ é:

$$F(ID_1^A, ID_1^B, \ldots, ID_L^A, ID_L^B) \equiv F(ID_1^B, ID_1^A, \ldots, ID_L^B, ID_L^A)$$

Acordo de Chaves Hierárquicos Baseados em Subconjuntos

- Modelo de acordo de chaves baseado em subconjuntos de chaves;
- Estudado inicialmente por [Eschenauer e Gligor 02];
- Neste protocolo a Autoridade seleciona um grande número de chaves secretas;
- E para cada participante cede-lhe um subconjunto aleatório de chaves;
- O acordo de chave é feito escolhendo-se as chaves em comum.

Acordo de Chaves Hierárquicos Baseados em Subconjuntos

- Modelo de acordo de chaves baseado em subconjuntos de chaves;
- Estudado inicialmente por [Eschenauer e Gligor 02];
- Neste protocolo a Autoridade seleciona um grande número de chaves secretas;
- E para cada participante cede-lhe um subconjunto aleatório de chaves;
- O acordo de chave é feito escolhendo-se as chaves em comum.
- Contudo este esquema não é hierárquico.

Acordo de Chaves Hierárquicos Baseados em Subconjuntos

- Para fazer deste um esquema hierárquico como [Ramkumar et al 05]:
- Cada nó pai cede aos seus filhos um subconjunto de suas chaves;
- O subconjunto de chaves é calculado deterministicamente pela *ID* do nó, usando-se uma função hash $H(\cdot)$;
- A raíz escolhe aleatóriamente N chaves secretas: $R = \langle K_1, \cdots, K_N \rangle$, onde $K_1, \cdots, K_N \in \mathbb{Z}_q$ (primo q);
- Para cada nível i a probabilidade $p_i \in (0, 1)$ diz que fração do subconjunto de chaves do nó pai é passada para o nó filho;

Acordo de Chaves Hierárquicos Baseados em Subconjuntos

- Seja um nó $ID^A = \langle ID_1, \ldots, ID_i \rangle$ um nó de nível i e subconjunto de chaves $R^A = \langle K_1, \Phi, K_3, \ldots \rangle$;
- Seja um nó $ID^B = \langle ID_1, \ldots, ID_i, ID_{i+1} \rangle$ um nó filho de ID^A;
- O nó ID^A calcula valores de $r_j \leftarrow H(ID^B, j)$, onde $0 < r_j < 1$ e $j = 1, \ldots, N$ e $H()$ é uma função hash;

Acordo de Chaves Hierárquicos Baseados em Subconjuntos

- ID^B irá receber as chaves $K_j \in R^A$ para o qual $r_j < P_i$,
- O subconjunto de chaves secretas de ID^B é $R^B = \{K_j \in R^A : r_j < p_i\}$
- O acordo de chaves entre nós raízes $ID^C = \langle ID_1^C, \ldots, ID_L^C \rangle$ e $ID^D = \langle ID_1^D, \ldots, ID_L^D \rangle$
  Repete-se o cálculo do Hash e determina-se a interseção;
- a chave compartilhada pode ser a soma módulo q.

Acordo de Chaves Hierárquicos Baseados em Subconjuntos

- Um ótimo ajutes para p_i é $p_i = \frac{1}{(t+1)}$;
- Dado todos os t_i e p_i, o parâmetro N deve ser grande suficiente para garantir segurança;
- acordo [Gennaro et al 08] o tamanho de N para garantir que um atacante não tenha uma probabilidade maior que e^{-m} de conseguir descobrir os valores secretos é:
  $N = \left\lceil \frac{m}{\prod_i p_i^2 (1-p_i)^t i} \right\rceil \approx me^L \cdot \prod_i t_i(t_i + 1)$;

Acordo de Chaves Hierárquicos Baseados em Subconjuntos

- Um ótimo ajutes para p_i é $p_i = \frac{1}{(t+1)}$;
- Dado todos os t_i e p_i, o parâmetro N deve ser grande suficiente para garantir segurança;
- acordo [Gennaro et al 08] o tamanho de N para garantir que um atacante não tenha uma probabilidade maior que e^{-m} de conseguir descobrir os valores secretos é:
  $N = \left\lceil \frac{m}{\prod_i p_i^2 (1-p_i)^t i} \right\rceil \approx me^L \cdot \prod_i t_i(t_i + 1)$;
- A complexidade também depende de um produtório $\prod_i t_i$

Acordos de Chaves Hierárquicos Lineares

Satisfaz as seguintes propriedades para um espaço linear V e um inteiro N [Gennaro et al 08]:

1. A autoridade raíz seleciona N valores aleatórios de V para ser usado como chave secreta mestre;
2. A chave secreta dos nós na hierarquia são valores $v_1, v_2, \ldots \in V$, obtidos por uma combinação linear em V da chave secreta mestre;
3. A chave compartilhada também é uma combinação linear em V da chave secreta mestre;
4. O número de valore v_i e os coeficientes da combinação linear são calculados deterministicamente a partir de valores públicos, tal como a posição do nó na hierarquia e sua identidade.

Modelo Híbrido

- Realizar a combinação dos esquemas:
  - Acordo de chaves hierárquico linear $\mathcal{H}$ e
  - Acordo de chaves bilinear baseado em identidade
- Resultando no modelo híbrido $\mathcal{H}'$

Modelo Híbrido

- A autoridade raíz publica os parâmetros para o sistema de chaves públicas baseado na identidade:
  - determina dois grupos cíclicos $\mathbb{G}_1$ e $\mathbb{G}_2$ de ordem prima q;
  - o mapeamento bilinear $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$; e
  - a função de hash $H : \{0,1\}^* \rightarrow \mathbb{G}_1$
- realiza também todas as ações do esquema hierárquico $\mathcal{H}$
- para os nós internos da hierarquia, que não sejam os nós folhas e seus pais, o procedimento é igual ao esquema $\mathcal{H}$;

Modelo Híbrido

- Um nó ID^A pai de um nó folha possui os seguintes valores secretos $v_1, \ldots, v_n \in \mathbb{Z}_q$ como em $\mathcal{H}$.
- Então ID^A provê para seus filhos com identidade ID_l no nível l os elementos $H(ID_l)^{v_i} \in \mathbb{G}_1$, $i = 1, \ldots, n$;

Modelo Híbrido

- A chave comum entre dois nós folhas ID^C e ID^D com nós pais ID^A e ID^B respectivamente, é calculado da seguinte forma:
  - $v_1, \ldots, v_n$ segredo de ID^A;
  - $\alpha_1, \ldots, \alpha_n$ coeficientes da combinação linear que ID^A usaria para calcular a chave compartilhada com ID^B (segredo $s = \sum_i \alpha_i v_i$)
  - a chave secreta para nós folhas são os valores $V_1 = H(ID)^{v_1}, \ldots, V_n = H(ID)^{v_n} \in \mathbb{G}_1$
  - os coeficientes $\alpha_1, \ldots, \alpha_n$ podem ser obtidos por informações públicas.
  - o nó folha ID^C então calcula:

$$U_1 \leftarrow \prod_i (V_{ID^C i})^{\alpha_i} \left(= H(ID^C)^{\sum_i \alpha_i v_i} = H(ID^C)^s \right)$$

Modelo Híbrido

- continuação
  - $U_2 \leftarrow H(ID^D)$
  - ID^C obtém a chave $K \leftarrow e(U_1, U_2) = e(H(ID^C), H(ID^D))^s$.
- Semelhantemente ID^D calcula:
  - $U_1' \leftarrow H(ID^C)$
  - determina os coeficientes β_i
  - $U_2' \leftarrow \prod_i (V_{ID^D i})^{\beta_i}$
  - ID^D obtém a chave $K \leftarrow e(U_1', U_2') = e(H(ID^C), H(ID^D))^s$.

Segurança do Modelo Hierárquico

- O modelo de segurança prevê que os níveis mais inferiores na hierarquia estão mais expostos, por isso necessitam maior segurança;
- As referências dos modelos hierárquicos apresentam uma análise da segurança destes sistemas mais gerais;

Segurança do Modelo Híbrido

- O estudo da segurança do modelo híbrido apresenta-o como tão seguro quanto o modelo hierárquico para os nós internos da hierarquia (exceto os nós folhas), inclusive a hierarquia permanece inalterada exceto pelo nível acrescentado no modelo;
- Para as folhas a segurança é equivalente ao modelo baseado em identidades, a demonstração é fazer uma redução do modelo híbrido ao Problema BDDH.

Público Alvo Científico

- Internacionais:
  - CRYPTO - Congresso nos EUA - Agosto (para 2009 submissão até 13FEV09);
  - EUROCRYPT - Congresso europeu - Maio;
  - Journal of Cryptology - Revista internacional.
- Nacional:
  - SBSEG [3] - Agosto.

[3] Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais

Público Alvo Profissional

- Forças militares (MB, EB e FAB);
- Forças auxiliares (Polícia Militar, Polícia Federal);
- Agências de Inteligência;

Conclusão

- Até NOV2008:
  - Estudar os trabalho de [Gennaro et al 08];
  - Preparar seminário (concluído);
- DEZ2008 à JAN2009, Utilizando a ferramenta MAGMA:
  - Estudo da ferramenta MAGMA;
  - Implementar os modelos existentes, utilizando novos algoritmos e tecnologias (utilizar a mesma idéia);
  - Comparar a complexidade com o modelo original proposto;
  - Testar modelos alternativos;
- FEV2009:
  - Exame de qualificação;
  - Se já obtiver sucesso nos modelos alternativos, preparar um artigo.
- FEV2009 à AGO2009:
  - Implementar um modelo alternativo;
  - Provar a segurança do modelo proposto;

Conclusão

- Ao final o trabalho deve responder:
  - Quais são os aspectos que podem melhorar?
  - É possível derivar um outro modelo com mesma segurança e melhor eficiência?
  - É possível criar um outro modelo seguro e eficiente em todos os níveis hierárquicos?

Exemplo de hierarquia

Exemplo de hierarquia

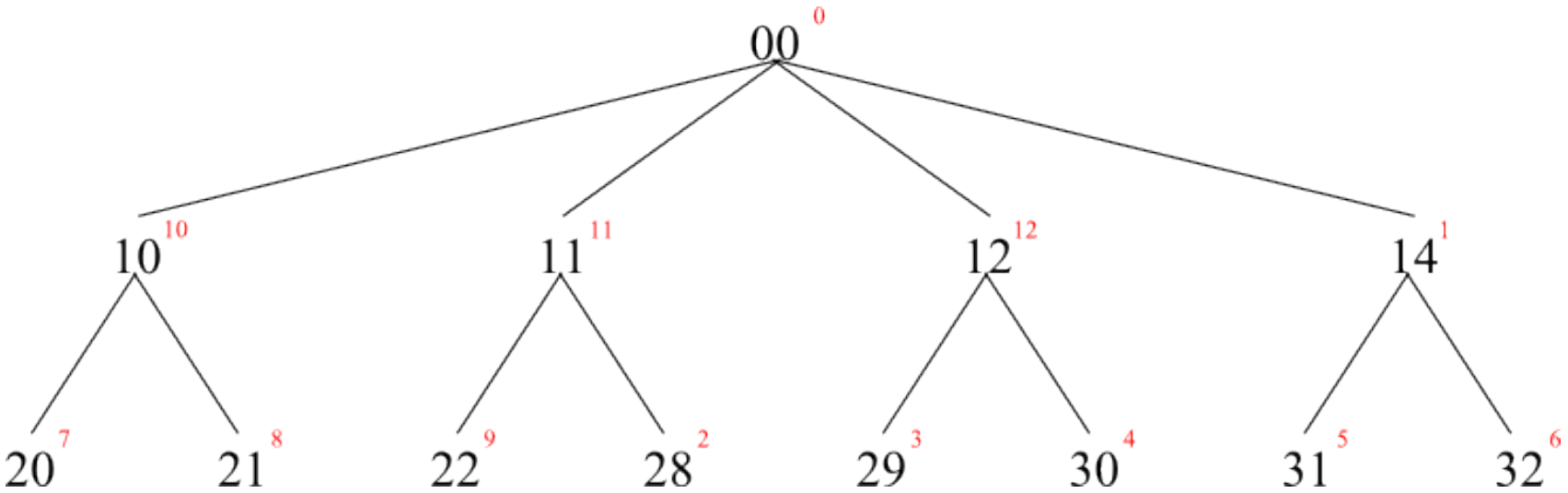


Figura: Modelo de Hierarquia

$t_1 = 2; \quad q = 13;$

$t_2 = 3; \quad Z_q = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

Exemplo de polinômio

$$F(x_1, y_1, x_2, y_2) = f(x_1, y_1, x_2, y_2) + f(y_1, x_1, y_2, x_2)$$

$$f(x_1, y_1, x_2, y_2) = x_1^2 + x_1 + y_1^2 + y_1 + x_2^3 + x_2^2 + x_2 + y_2^3 + x_2^3 y_2^3 + x_1 y_2$$
$$f(y_1, x_1, y_2, x_2) = y_1^2 + y_1 + x_1^2 + x_1 + y_2^3 + y_2^2 + y_2 + x_2^3 + x_2^3 y_2^3 + y_1 x_2$$

$$\begin{aligned} F(x_1, y_1, x_2, y_2) \quad = \quad & 2x_1^2 + 2x_1 + 2y_1^2 + 2y_1 + 2x_2^3 + 2y_2^3 + 2x_2^3 y_2^3 \\ & + x_2^2 + x_2 + x_1 y_2 + y_2^2 + y_2 + y_1 x_2 \end{aligned}$$

Exemplo de polinômio

$$F(x_1, y_1, x_2, y_2) = 2x_1^2+2x_1+2y_1^2+2y_1+2x_2^3+2y_2^3+2x_2^3y_2^3 + x_2^2 + x_2 + x_1y_2 + y_2^2 + y_2 + y_1x_2$$

$$F(10, y_1, x_2, y_2) = 2\cdot 10^2+2\cdot 10+2y_1^2+2y_1+2x_2^3+2y_2^3+2x_2^3y_2^3 + x_2^2 + x_2 + 10y_2 + y_2^2 + y_2 + y_1x_2$$

$$F(10, y_1, x_2, y_2) = 5+7+2y_1^2+2y_1+2x_2^3+2y_2^3+2x_2^3y_2^3 + x_2^2 + x_2 + 10y_2 + y_2^2 + y_2 + y_1x_2$$

$$F(10, y_1, x_2, y_2) = 12+2y_1^2+2y_1+2x_2^3+2y_2^3+2x_2^3y_2^3 + x_2^2 + x_2 + y_2^2 + 11y_2 + y_1x_2$$

Exemplo de polinômio

$$F(10, y_1, x_2, y_2) = 12+2y_1^2+2y_1+2x_2^3+2y_2^3+2x_2^3y_2^3 + x_2^2 + x_2 + y_2^2 +11y_2+ y_1x_2$$

$$F(11, y_1, x_2, y_2) = 4+2y_1^2+2y_1+2x_2^3+2y_2^3+2x_2^3y_2^3 + x_2^2 + x_2 + y_2^2 +12y_2+ y_1x_2$$

$$F(12, y_1, x_2, y_2) = 0+2y_1^2+2y_1+2x_2^3+2y_2^3+2x_2^3y_2^3 + x_2^2 + x_2 + y_2^2 +0y_2+ y_1x_2$$

$$F(14, y_1, x_2, y_2) = 4+2y_1^2+2y_1+2x_2^3+2y_2^3+2x_2^3y_2^3 + x_2^2 + x_2 + y_2^2 +2y_2+ y_1x_2$$

Exemplo de polinômio

$$F(10, y_1, 20, y_2) = 2y_1^2 + 9y_1 + 12y_2^3 + y_2^2 + 11y_2 + 0$$

$$F(10, y_1, 21, y_2) = 2y_1^2 + 10y_1 + 12y_2^3 + y_2^2 + 11y_2 + 3$$

$$F(11, y_1, 22, y_2) = 2y_1^2 + 11y_1 + 4y_2^3 + y_2^2 + 11y_2 + 5$$

$$F(11, y_1, 28, y_2) = 2y_1^2 + 4y_1 + 5y_2^3 + y_2^2 + 11y_2 + 0$$

Exemplo de polinômio

$$F(12, y_1, 29, y_2) = 2y_1^2 + 5y_1 + 4y_2^3 + y_2^2 + 0y_2 + 1$$

$$F(12, y_1, 30, y_2) = 2y_1^2 + 6y_1 + 0y_2^3 + y_2^2 + 0y_2 + 5$$

$$F(14, y_1, 31, y_2) = 2y_1^2 + 7y_1 + 5y_2^3 + y_2^2 + 2y_2 + 11$$

$$F(14, y_1, 32, y_2) = 2y_1^2 + 8y_1 + 5y_2^3 + y_2^2 + 2y_2 + 10$$

Acordo de Chaves Usando Polinômios

- Chave compartilhada entre os $ID(20)$ e $ID(32)$:
- $ID(20) = \langle 10, 20 \rangle = \langle 10, 7 \rangle$
- $ID(32) = \langle 14, 32 \rangle = \langle 1, 6 \rangle$

$$F(10, y_1, 20, y_2) = 2y_1^2 + 9y_1 + 12y_2^3 + y_2^2 + 11y_2 + 0$$

$$F(14, y_1, 32, y_2) = 2y_1^2 + 8y_1 + 5y_2^3 + y_2^2 + 2y_2 + 10$$

Acordo de Chaves Usando Polinômios

- Cáculo feito por $ID(20)$
- $F_{ID(20)}(10, 1, 7, 6)$

$$
\begin{aligned}
F(10,1,7,6) &= 2y_1^2 + 9y_1 + 12y_2^3 + y_2^2 + 11y_2 + 0 \\
&= 2(1)^2 + 9(1) + 12(6)^3 + (6)^2 + 11(6) + 0 \\
&= 2(1) + 9(1) + 12(216) + (36) + 11(6) + 0 \\
&= 2 + 9 + 2592 + 36 + 66 + 0
\end{aligned}
$$

$$= 2705 = 208 \cdot 13 + 1 = 1 \, mod \, 13$$

Acordo de Chaves Usando Polinômios

- Cáculo feito por $ID(32)$
- $F_{ID(20)}(1, 10, 6, 7)$

$$
\begin{aligned}
F(1,10,6,7) &= 2y_1^2 + 8y_1 + 5y_2^3 + y_2^2 + 2y_2 + 10 \\
&= 2(10)^2 + 8(10) + 5(7)^3 + (7)^2 + 2(7) + 10 \\
&= 2(100) + 8(10) + 5(343) + 49 + 2(7) + 10 \\
&= 200 + 80 + 1715 + 49 + 14 + 10
\end{aligned}
$$

$$= 2068 = 159 \cdot 13 + 1 = 1 \, mod \, 13$$

Exemplo de Subconjunto

- $t_1 = 2$ e $t_2 = 1$
- um bom ajuste de $p_i = \frac{1}{t_i+1}$; $p_1 = \frac{1}{3}$ e $p_2 = \frac{1}{2}$
- $R^{00} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
- Valores de $H(ID^{10}, j) = \{\frac{1}{4}, \frac{2}{3}, \frac{1}{2}, \frac{5}{6}, \frac{1}{5}, \frac{7}{9}, \frac{1}{6}, \frac{5}{9}, \frac{1}{7}, \frac{4}{9}, \frac{8}{9}, \frac{7}{12}\}$

Exemplo de Subconjunto

- $t_1 = 2$ e $t_2 = 1$
- um bom ajuste de $p_i = \frac{1}{t_i+1}$; $p_1 = \frac{1}{3}$ e $p_2 = \frac{1}{2}$
- $R^{00} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
- Valores de $H(ID^{10}, j) = \{ \frac{1}{4}, \frac{2}{3}, \frac{1}{2}, \frac{5}{6}, \frac{1}{5}, \frac{7}{9}, \frac{1}{6}, \frac{5}{9}, \frac{1}{7}, \frac{4}{9}, \frac{8}{9}, \frac{7}{12} \}$

Exemplo de Subconjunto

- $t_1 = 2$ e $t_2 = 1$
- um bom ajuste de $p_i = \frac{1}{t_i+1}$; $p_1 = \frac{1}{3}$ e $p_2 = \frac{1}{2}$
- $R^{00} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
- Valores de $H(ID^{10}, j) = \{ \frac{1}{4}, \frac{2}{3}, \frac{1}{2}, \frac{5}{6}, \frac{1}{5}, \frac{7}{9}, \frac{1}{6}, \frac{5}{9}, \frac{1}{7}, \frac{4}{9}, \frac{8}{9}, \frac{7}{12} \}$
- $R^{10} = \{1, 5, 7, 9\}$

Exemplo de Subconjunto

- $R^{10} = \langle 1, \phi, \phi, \phi, 5, \phi, 7, \phi, 9, \phi, \phi, \phi \rangle$
- $R^{11} = \langle 1, \phi, 3, \phi, 5, \phi, 7, \phi, \phi, \phi, \phi, \phi \rangle$
- $R^{12} = \langle 1, \phi, \phi, \phi, \phi, \phi, 7, \phi, 9, \phi, 11, \phi \rangle$
- $R^{14} = \langle 1, \phi, 3, \phi, 5, \phi, \phi, \phi, 9, \phi, \phi, \phi \rangle$

Exemplo de Subconjunto

- $R^{20} = \langle 1, \phi, \phi, \phi, 5, \phi, \phi, \phi, \phi, \phi, \phi, \phi \rangle$
- $R^{21} = \langle 1, \phi, \phi, \phi, \phi, \phi, 7, \phi, \phi, \phi, \phi, \phi \rangle$
- $R^{22} = \langle 1, \phi, 3, \phi, \phi, \phi, \phi, \phi, \phi, \phi, \phi, \phi \rangle$
- $R^{28} = \langle \phi, \phi, \phi, \phi, 5, \phi, 7, \phi, \phi, \phi, \phi, \phi \rangle$
- $R^{29} = \langle \phi, \phi, \phi, \phi, \phi, \phi, 7, \phi, 9, \phi, \phi, \phi \rangle$
- $R^{30} = \langle 1, \phi, \phi, \phi, \phi, \phi, \phi, \phi, \phi, \phi, 11, \phi \rangle$
- $R^{31} = \langle \phi, \phi, 3, \phi, \phi, \phi, \phi, \phi, 9, \phi, \phi, \phi \rangle$
- $R^{32} = \langle 1, \phi, \phi, \phi, \phi, \phi, \phi, \phi, 9, \phi, \phi, \phi \rangle$

Acordo de Chaves Usando Subconjuntos

- R^{20} calcula:
  - $H(ID^{32}, 1) = \frac{1}{3} < p_2 = \frac{1}{2}$
  - $H(ID^{32}, 5) = \frac{2}{3} > p_2$
- R^{32} calcula:
  - $H(ID^{20}, 1) = \frac{1}{4} < p_2 = \frac{1}{2}$
  - $H(ID^{20}, 9) = \frac{5}{6} > p_2$
- Chave compartilhada $K = \langle 1 \rangle$

Exemplo de Acordo de Chaves para o Modelo Híbrido e com Polinômios

$$F(10, y_1, 20, y_2) = 2y_1^2+9y_1+12y_2^3+y_2^2+11y_2+0$$

v_1	$=$	2	α_1	$=$	y_1^2	V_1	$=$	$H(ID^{20})^2$
v_2	$=$	9	α_2	$=$	y_1	V_2	$=$	$H(ID^{20})^9$
v_3	$=$	12	α_3	$=$	y_2^3	V_3	$=$	$H(ID^{20})^{12}$
v_4	$=$	1	α_4	$=$	y_2^2	V_4	$=$	$H(ID^{20})^1$
v_5	$=$	11	α_5	$=$	y_2	V_5	$=$	$H(ID^{20})^{11}$
v_6	$=$	0	α_6	$=$	1	V_6	$=$	$H(ID^{20})^0$

Exemplo de Acordo de Chaves para o Modelo Híbrido e com Polinômios

v_1	$=$	2	α_1	$=$	y_1^2	V_1	$=$	$H(ID^{20})^2$
v_2	$=$	9	α_2	$=$	y_1	V_2	$=$	$H(ID^{20})^9$
v_3	$=$	12	α_3	$=$	y_2^3	V_3	$=$	$H(ID^{20})^{12}$
v_4	$=$	1	α_4	$=$	y_2^2	V_4	$=$	$H(ID^{20})^1$
v_5	$=$	11	α_5	$=$	y_2	V_5	$=$	$H(ID^{20})^{11}$
v_6	$=$	0	α_6	$=$	1	V_6	$=$	$H(ID^{20})^0$

$$
\begin{aligned}
U_1 &= V_1^{\alpha_1} \quad V_2^{\alpha_2} \quad V_3^{\alpha_3} \quad V_4^{\alpha_4} \quad V_5^{\alpha_5} \quad V_6^{\alpha_6} \\
&= V_1^{y_1^2} \quad V_2^{y_1} \quad V_3^{y_2^3} \quad V_4^{y_2^2} \quad V_5^{y_2} \quad V_6^{1} \\
&= H(ID^{20})^{2y_1^2} \quad H(ID^{20})^{9y_1} \quad H(ID^{20})^{12y_2^3} \quad H(ID^{20})^{1y_2^2} \quad H(ID^{20})^{11y_2} \quad H(ID^{20})^{0\times 1}
\end{aligned}
$$

Exemplo de Acordo de Chaves para o Modelo Híbrido e com Polinômios

- $U_1 = H(ID^{20})^{F(10,y_1,20,y_2)}$
- $U_2 = H(ID^{32})$
- $K = e(U_1, U_2) = e(H(ID^{20}), H(ID^{32}))^{F(10,y_1,20,y_2)}$

Referências (1/4)

C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung.
Perfectly Secure Key Distribution for Dynamic Conferences.
Information and Computation 146(1):1-23, 1998.

D. Boneh, M. Franklin
Identity Based Encryption from Weil Pairing.
Crypto'2001, LNCS, Springer-Verlag, 2001, v.2139, p.213-229.

W. Diffie and M. E. Hellman.
New Directions in Cryptography.
IEEE Transactions on Information Theory, 22(6):644-654, 1976.

L. Eschenauer e V.D. Gligor
A key-management scheme for distributed sensor networks.

Referências (2/4)

C. Cocks

An identity based encryption scheme based on quadratic residues.

In Proceedings of the 8th IMA International Conference on Cryptography and Coding, 2001.

J. Crampton, H. Lim, K. Paterson

What Can Identity-Based Cryptography Offer to Web Services?.

In Proceedings of SWS'07, ACM, 2007.

C. Gentry

Certificate-Based Encryption and the Certificate Revocation Problem.

Cryptology ePrint Archive, 2003. Disponível em

Referências (3/4)


M.Girault
Self-Certified Public Keys.
EuroCrypt91, LCNS v.547, 490-497, Springer, 1991.


B. Lee, K. Kim
Self-Certified Signatures.
Indocrypt'02, LNCS v.2551, 199-214, Springer, 2002.

Referências (4/4)

S. Saeednia

A note on Girault's Self-certified Model.

Information Processing Letters, v.86, n.6, 323–327, Elsevier, 2003.

Tzong-Sun Wu, Han-Yu Lin

ECC Based Convertible Authenticated Encryption Scheme Using Self-Certified Public Key Systems.

International Journal of Algebra, v. 2, n. 3, 109-117, 2008.