Proposta de Esquemas de Criptografia e de Assinatura sob Modelo de Criptografia de Chave Pública sem Certificado

Aluna: Denise Hideko Goya

Orientador: Prof. Dr. Routo Terada

DCC – IME – USP

28 de Junho de 2006

Motivações

- Criptografia de chave pública (PKC) requer:
  - uma chave **pública** (de criptografia ou verificação de assinatura);
  - uma chave **secreta** (de decriptografia ou assinatura).
- Para se garantir que uma chave pública é verdadeira, faz-se necessário um **certificado digital**;
- PKC requer uma autoridade de confiança para certificar chaves públicas;
- Infra-estrutura para gerenciamento de certificados é cara.

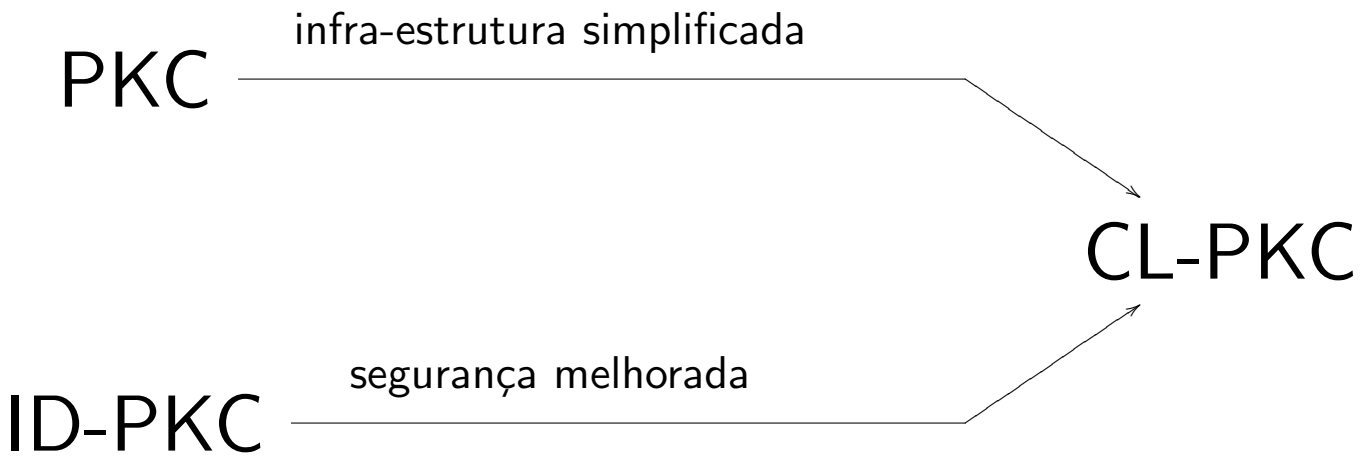
Motivações – PKC que dispensa certificado

- Criptografia de chave pública baseada em identidade (**ID-PKC**) [Shamir 1984], [Boneh e Franklin 2001]
  - chave pública $=$ identidade (CPF, $e\text{-}mail$, nº telefone);
  - desvantagem: autoridade de confiança conhece todas as chaves secretas (custódia de chaves).

- Criptografia de chave pública sem certificado (**CL-PKC**)
  - estende ID-PKC, eliminando custódia de chaves;
  - perda da chave-mestra não causa corrompimento total do sistema. [Al-Riyami e Paterson 2003]

Motivações – União de Pontos Positivos

CL-PKC apresenta características intermediárias:



Objetivos Gerais do Trabalho

- Descrição do modelo CL-PKC;
- Construção de esquemas CL-PKC que apresentem melhorias em relação a trabalhos existentes:
  - CL-PKE (esquema de criptografia e decriptografia);
  - CL-PKS (esquema de assinatura).

Modelo CL-PKC e Relação de Chaves

Tipo de Chave	Componentes	Descrição e Dependências
Pública	ID_A	identidade de A
	N_A	chave pública de A; depende de t_A
Secreta	$t_A(SecDir)$	segredo da entidade A
	$D_A(SecEsq)$	chave parcial; é compartilhada entre A e KGC; depende de ID_A e da chave-mestra de KGC (papel de um certificado "leve")

Adversários contra CL-PKC

- Adversário Tipo-I:
  - não conhece *chave-mestra*;
  - pode substituir valores de chaves pública;
- Adversário Tipo-II:
  - conhece *chave-mestra*;
  - não pode substituir valores de chaves pública;

Noções de Segurança para CL-PKC

- Ambos adversários realizam ataques adaptativos:
  - de texto ilegível escolhido (CCA2), contra CL-PKE e
  - de mensagem escolhida (CMA), contra CL-PKS.

- Dizemos que:
  - CL-PKE é **IND-CCA2**, quando todo adversário CCA2 é incapaz de distinguir entre duas mensagens cifradas;
  - CL-PKS é **EUF-CMA**, quando todo adversário CMA é incapaz de produzir assinaturas forjadas.

Nosso objetivo (mais específico)

- Construção de esquemas seguros:
  - CL-PKE, que seja **IND-CCA2** e
  - CL-PKS, que seja **EUF-CMA**.

- Ferramentas:
  - Emparelhamentos bilineares, sobre grupos gerados a partir de curvas elípticas;
  - Modelo de oráculos aleatórios, para demonstrações de segurança.

CL-PKE-Proposto – inicializações

inicializa. Dado um parâmetro de segurança k:

1. gerar dois grupos cíclicos $\mathbb{G}_1$ e $\mathbb{G}_2$ de ordem prima $q > 2^k$ e um emparelhamento bilinear $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$.
2. escolher aleatoriamente um gerador $P \in \mathbb{G}_1^*$.
3. escolher aleatoriamente $s \in \mathbb{Z}_q^*$ e calcular $P_{pub} = sP$.
4. escolher três funções de hash
   $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1^*$
   $H_2 : \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \{0,1\}^n$
   $H_3 : \{0,1\}^{n-k_0} \times \{0,1\}^{k_0} \longrightarrow \mathbb{Z}_q^*$
   para inteiros n e k_0, $0 < k_0 < n$,
   com k_0 polinomial em n.

CL-PKE-Proposto – inicializações

O espaço de mensagens é $\mathcal{M} = \{0,1\}^{n-k_0}$.

O espaço de textos cifrados é $\mathcal{C} = \mathbb{G}_1^* \times \{0,1\}^n$.

A chave-mestra do sistema é s.

Os parâmetros públicos do sistema são

$\texttt{params} = \langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, k_0, P, P_{pub}, H_1, H_2, H_3 \rangle$.

CL-PKE-Proposto – geração de chaves

extrai. Dados um identificador $ID_A \in \{0,1\}^*$, params e a chave-mestra s:

1. calcular $Q_A = H_1(ID_A)$.
2. devolver a chave secreta parcial $D_A = sQ_A$.

publica. Dado params, uma entidade A:

1. seleciona ao acaso uma informação secreta $t_A \in \mathbb{Z}_q^*$;
2. calcula sua chave pública $N_A = t_A P$;
3. A guarda t_A em sigilo e publica N_A.

CL-PKE-Proposto – criptografia

cript. Dados um texto $m \in \mathcal{M}$, uma identidade ID_A, params e a chave pública N_A:

1. escolher aleatoriamente $\sigma \in \{0,1\}^{k_0}$
2. calcular
   $r = H_3(m, \sigma)$
   $Q_A = H_1(ID_A)$
   $g^r = \hat{e}(P_{pub}, Q_A)^r$
   $f = rN_A$
3. devolver o texto cifrado
   $C = \langle rP, (m \parallel \sigma) \oplus H_2(rP, g^r, f) \rangle$.

CL-PKE-Proposto – decriptografia

decript. Dados $C = \langle U, V \rangle \in \mathcal{C}$
e os valores secretos D_A e t_A:

1. calcular
   $g' = \hat{e}(U, D_A)$
   $f' = t_A U$
   $V \oplus H_2(U, g', f') = (m \parallel \sigma)$
2. desmembrar $(m \parallel \sigma)$ e calcular $r = H_3(m, \sigma)$
3. se $U = rP$, devolver a mensagem m,
   senão devolver $\perp$.

Características de CL-PKE-Proposto

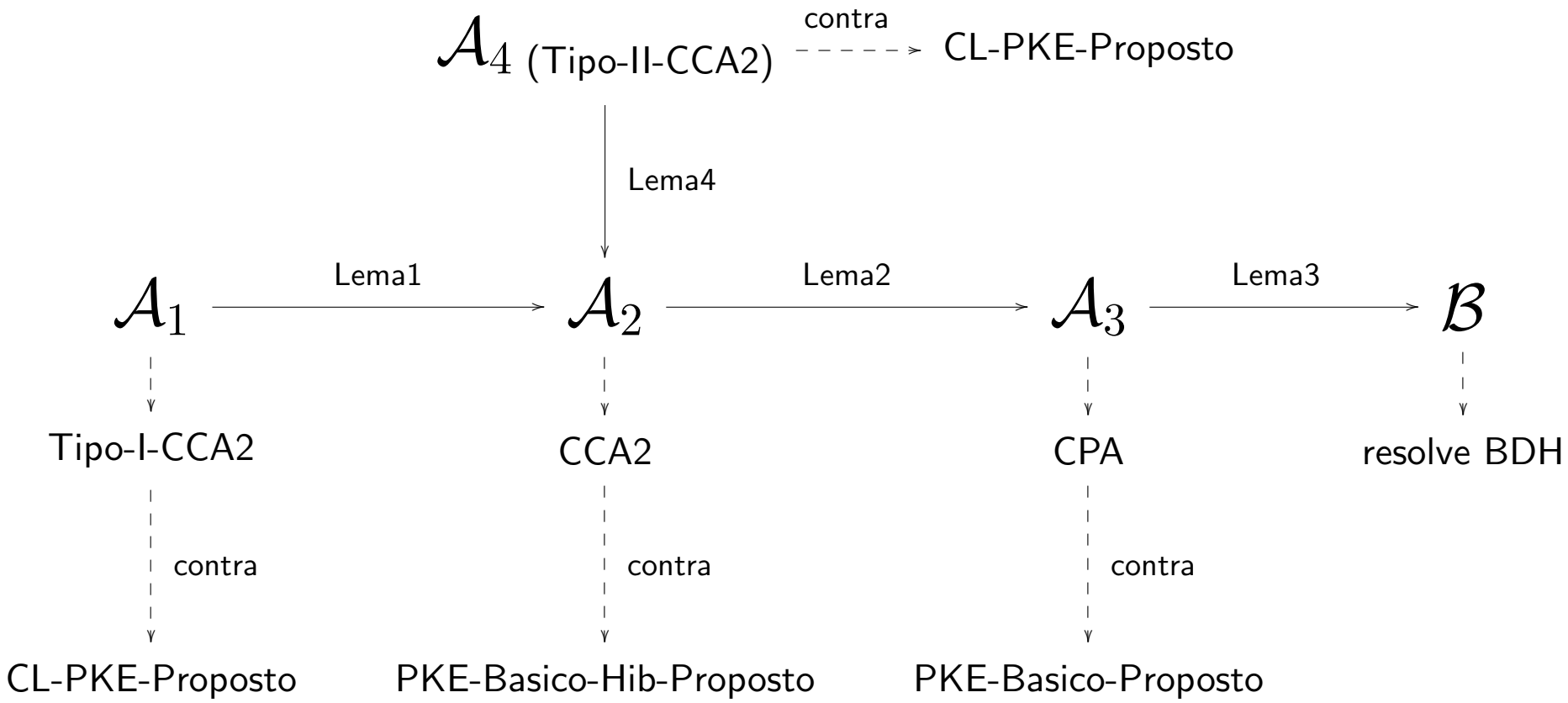
- CL-PKE-Proposto é válido, isto é, **decript** recupera corretamente a mensagem cifrada por **cript**;
- Pode ser implementado;
- É IND-CCA2, contra adversários Tipo-I e Tipo-II.
- Não é sucetível aos ataques já descobertos (sobre os esquemas relacionados).

Segurança de CL-PKE-Proposto

- Sob a hipótese de dificuldade do problema Diffie-Hellman Bilinear (BDH);

Teorema 1. *Se o problema BDH é difícil em* $\mathbb{G}_1$ *e as funções de* hash H_1, H_2 *e* H_3 *são oráculos aleatórios, então o esquema CL-PKE-Proposto é IND-CCA2, ou seja, é seguro contra adversários Tipo-I-CCA2 e Tipo-II-CCA2.*

Segurança IND-CCA2, sob BDH



CL-PKS-Proposto – inicializações

inicializa. Dado um parâmetro de segurança k:

1. gerar grupos G_1, G_2, de ordem prima $p > 2^k$, com geradores P e Q, tais que $P = \psi(Q)$, onde ψ é um homomorfismo.
2. gerar um emparelhamento bilinear $e : G_1 \times G_2 \rightarrow G_T$.
3. calcular $g = e(P, Q) \in G_T$.
4. escolher a chave-mestra $s \in Z_p^*$ e calcular $Q_{pub} = sQ$.
5. escolher funções de hash
   $H_1 : \{0,1\}^* \rightarrow Z_p^*$
   $H_2 : \{0,1\}^* \times \{0,1\}^* \times G_T \times G_T \rightarrow Z_p^*$

CL-PKS-Proposto – inicializações

O espaço de mensagens é $\mathcal{M} = \{0,1\}^*$.

O espaço de assinatura é $\mathcal{S} = G_1 \times Z_p^*$.

A chave-mestra do sistema é s.

Os parâmetros públicos do sistema são

$$\texttt{params} = \langle p, G_1, G_2, G_T, e(), \psi,\ P, Q, Q_{pub}, g, H_1, H_2 \rangle$$

CL-PKS-Proposto – geração de chaves

parcial. Dada uma identidade $ID_A \in \{0,1\}^*$, `params` e a `chave-mestra` s, o KGC:

1. calcula e entrega, via canal seguro, a chave parcial secreta $D_A = \frac{1}{H_1(ID_A)+s}P \in G_1^*$.

info-secreta, secreta e publica. Dado `params`, A:

1. escolhe aletoriamente uma informação secreta $t_A \in Z_p^*$.
2. define e mantém em sigilo sua chave secreta de assinatura, formada pelo par $(D_A, t_A) \in G_1^* \times Z_p^*$.
3. calcula e publica sua chave pública $N_A = g^{t_A} \in G_T$.

CL-PKS-Proposto – assinatura

assina. Dados `params`, uma mensagem M, uma identidade ID_A, a chave pública $N_A = g^{t_A}$ e a chave secreta de assinatura de A, formada pelo par (D_A, t_A), A:

1. escolhe aleatoriamente $x \in Z_p^*$.
2. calcula
   $r = g^x \in G_T$
   $h = H_2(M, ID_A, N_A, r) \in Z_p^*$
   $S = (x + ht_A)D_A \in G_1$
3. A assinatura sobre M é $\sigma = (S, h) \in G_1 \times Z_p^*$.

CL-PKS-Proposto – verificação

verifica. Dados `params`, uma mensagem M, a assinatura $\sigma = (S, h)$, a identidade ID_A e a chave pública N_A, o algoritmo:

1. aceita σ como autêntica, se:
   $h = H_2(M, ID_A, N_A, r')$
   onde:
   $r' = e[S, H_1(ID_A)Q + Q_{pub}](N_A)^{-h}$
2. rejeita, em caso contrário.

Características de CL-PKS-Proposto

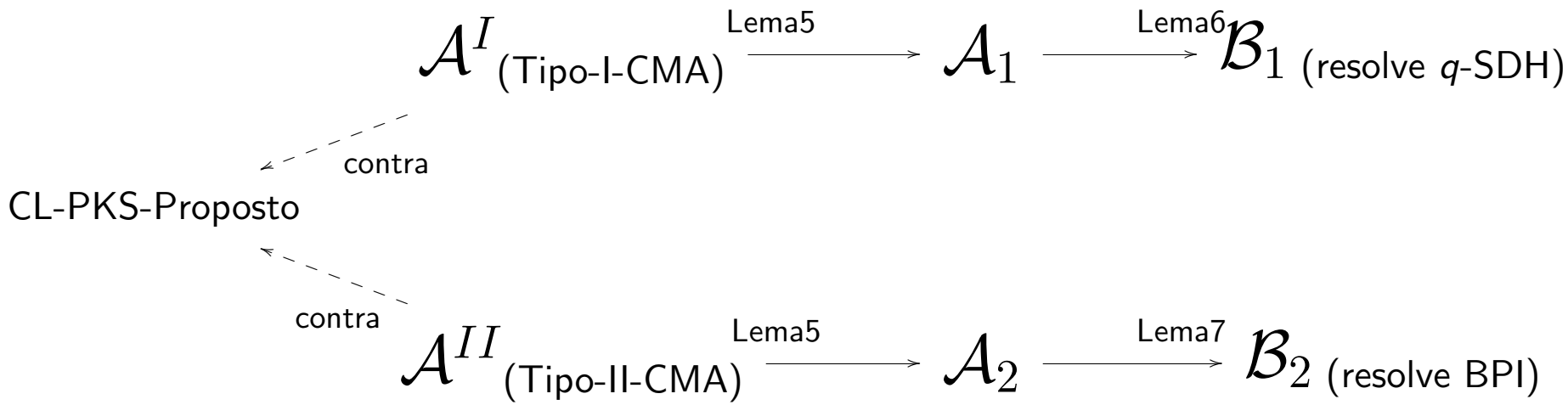
- CL-PKS-Proposto é válido, isto é, **verifica** aceita ou rejeita corretamente mensagens assinadas por **assina**;
- Pode ser implementado;
- É EUF-CMA, contra adversários Tipo-I e Tipo-II.
- Não é sucetível aos ataques já descobertos (sobre os esquemas relacionados).

Segurança de CL-PKS-Proposto

- Sob a hipótese de dificuldade dos problemas *q-Strong* Diffie-Hellman (*q*-SDH) e de Inversão do Emparelhamento Bilinear (BPI);

Teorema 2. *Se os problemas q-SDH e BPI são difíceis sobre o grupo bilinear $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ e as funções de* hash *H_1 e H_2 são oráculos aleatórios, então o esquema CL-PKS-Proposto é EUF-CMA, ou seja, é seguro contra adversários Tipo-I-CMA e Tipo-II-CMA.*

Segurança EUF-CMA, sob q-SDH e BPI



Comparação dos Esquemas CL-PKC

As operações mais caras envolvidas nos esquemas são, respectivamente:

E	Emparelhamento bilinear
P	Potenciação nos grupos multiplicativos
M	Multiplicação escalar nos grupos aditivos
m	multiexponenciação nos grupos multiplicativos
S	Soma de pontos nos grupos aditivos
H	cálculo de *Hash*

Comparação dos Esquemas CL-PKE

Esquema CL-PKE	Criptografia				Decriptografia			
	E	P	M	H	E	P	M	H
[Al-Riyami e Paterson 2003]	3	1	1	4	1	0	1	3
[Al-Riyami e Paterson 2005]	1	1	2	5	1	0	2	4
[Cheng e Comley 2005]	1	1	2	4	1	0	2	3
CL-PKE-Proposto	1	1	2	3	1	0	2	2

Comparação dos Esquemas CL-PKE

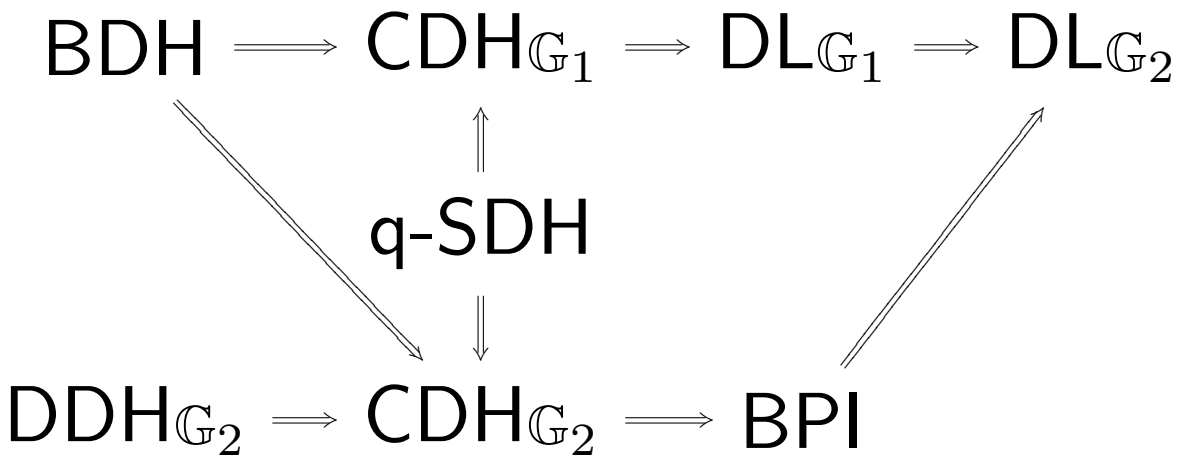
Esquema CL-PKE	Tamanhos (em bits)		
	chave pública	mensagem legível	mensagem cifrada
[Al-Riyami e Paterson 2003]	$2g$	n	$g + 2n$
[Al-Riyami e Paterson 2005]	g	n	$g + 2n$
[Cheng e Comley 2005]	g	n	$g + 2n$
CL-PKE-Proposto	g	$m - k_0$	$g + m$

Se $k_0 < n$, com $k_0(n) = O(n^{1/c})$, nosso esquema é mais econômico no uso de memória.

Comparação dos Esquemas CL-PKE

Esquema CL-PKE	Problemas Reduzidos	
	Advers. Tipo-I	Advers. Tipo-II
[Al-Riyami e Paterson 2003]	BDH	CDH
[Al-Riyami e Paterson 2005]	BDH	CDH
[Cheng e Comley 2005]	BDH	GDH
CL-PKE-Proposto	BDH	BDH

Mapa dos Problemas



Vantagens de CL-PKE-Proposto

- Maior velocidade na criptografia de textos;
- Menor tamanho de texto cifrado e de chave pública;
- Menor número de funções de *hash*.

Desvantagens de CL-PKE-Proposto

- Para adversários Tipo-II, foi usada hipótese mais forte (dificuldade de BDH contra a dificuldade de CDH ou GDH dos outros trabalhos);
- Segundo mais veloz para decriptografar.

Comparação dos Esquemas CL-PKS

Esquema CL-PKS	Assinatura					
	E	P	M	m	S	H
[Al-Riyami e Paterson 2003]	1	0	3	0	1	1
[Huang et al. 2005]	2	0	2	0	1	1
[Zhang et al. 2006]	0	0	3	0	2	2
CL-PKS-Proposto	0	1	1	0	0	1

Comparação dos Esquemas CL-PKS

Esquema CL-PKS	Verificação					
	E	P	M	m	S	H
[Al-Riyami e Paterson 2003]	4	1	0	1	0	1
[Huang et al. 2005]	4	1	0	1	0	2
[Zhang et al. 2006]	4	0	0	2	0	3
CL-PKS-Proposto	1	1	1	1	1	2

Comparação dos Esquemas CL-PKS

Esquema CL-PKS	Espaço de Assinatura	Espaço de Chave Pública
[Al-Riyami e Paterson 2003]	$\mathbb{G}_1 \times \{0,1\}^n$	$\mathbb{G}_1$
[Huang et al. 2005]	$\mathbb{G}_1 \times \{0,1\}^n$	$\mathbb{G}_1$
[Zhang et al. 2006]	$\mathbb{G}_1 \times \mathbb{G}_1$	$\mathbb{G}_1$
CL-PKS-Proposto	$\mathbb{G}_1 \times \mathbb{Z}_p^*$	$\mathbb{G}_T$

Comparação dos Esquemas CL-PKS

Esquema CL-PKS	Problemas Reduzidos aos Adversários	
	Adversário Tipo-I	Adversário Tipo-II
[Huang et al. 2005]	CDH	CDH
[Zhang et al. 2006]	CDH	CDH
CL-PKS-Proposto	q-SDH	BPI

Vantagens de CL-PKS-Proposto

- Maior velocidade, tanto para assinar mensagens, quanto para verificar assinaturas;
- Assinaturas de menor tamanho;
- Maior flexibilidade, devido ao uso de emparelhamento assimétrico;
- Hipótese menos forte, para adversários Tipo-II (dificuldade de BPI, contra a dificuldade de CDH dos outros trabalhos).

Desvantagens de CL-PKS-Proposto

- Chaves públicas maiores (definidas em $\mathbb{G}_T$, contra chaves em $\mathbb{G}_1$ nos demais esquemas).
- Para adversários Tipo-I, foi usada hipótese mais forte (dificuldade de q-SDH, contra a dificuldade de CDH dos outros trabalhos);

Resumo de Contribuições

1. Novo protocolo de criptografia, sob o modelo CL-PKC, que:
   - foi demonstrado seguro ao nível IND-CCA2;
   - apresenta melhorias em eficiência computacional e na utilização de memória ou banda, comparativamente a esquemas anteriores;
   - é uma opção para IBE, quando não é desejável a característica de custódia de chaves (*key escrow*);
   - dispensa certificados digitais e infra-estrutura de chaves públicas.

Resumo de Contribuições

2. Novo protocolo de assinatura, sob o modelo CL-PKC, que:
   - foi demonstrado seguro ao nível EUF-CMA;
   - apresenta maior eficiência computacional na assinatura e na verificação;
   - apresenta melhorias na utilização de memória ou banda;
   - mais flexível para escolha de grupos;
   - é uma opção para IBS (elimina custódia de chaves);
   - dispensa certificados digitais e ICP.

Resumo de Contribuições

Artigos gerados:

An Improved Certificateless Public Key Encryption, nos anais de *"The 2006 Symposium on Cryptography and Information Security"* (SCIS 2006), p.17-20, Hiroshima, Japão, Janeiro de 2006. Também submetido para *International Journal of Security on Networks*.

A Certificateless Signature Scheme Based on Bilinear Pairing Functions, submetido para *"1st International Workshop on Security"* (IWSEC2006), Kyoto, Japão, Outubro de 2006.

Trabalhos Futuros

- CL-PKE-Proposto2. É mais eficiente que CL-PKE-Proposto. Aprimorá-lo em relação a CL-PKE de [Libert e Quisquater 2006].
- Modelos Teóricos. Modelo padrão para demonstrações de segurança (sem oráculos aleatórios). Construções genéricas.
- Emparelhamentos assimétricos em CL-PKE-Proposto e de [Libert e Quisquater 2006].
- CL-PKE e CL-PKS sem emparelhamentos.

Trabalhos Futuros

- Criptografia autenticada: CL-Auth-PKE.
- Criptoassinatura sem custódia de chaves.
- Mecanismo de encapsulamento de chave: CL-KEM.
- Esquema CL-PKS com verificador designado.
- Esquema CL-PKE com segurança mediada.
- Modelos hierárquicos.
- Implementações e *benchmarking*.

Referências

[Al-Riyami e Paterson 2003]AL-RIYAMI, S. S.; PATERSON, K. G. Certificateless public key cryptography. In: *Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 - December 4, 2003, Proceedings*. [S.l.]: Springer, 2003. (Lecture Notes in Computer Science, v. 2894). ISBN 3-540-20592-6. Versão completa disponível em `http://eprint.iacr.org/2003/126`,.

[Al-Riyami e Paterson 2005]AL-RIYAMI, S. S.; PATERSON, K. G. Cbe from cl-pke: A generic construction and efficient schemes. In: *Public Key Cryptography - PKC 2005*. [S.l.: s.n.], 2005. p. 398–415.

[Boneh e Franklin 2001]BONEH, D.; FRANKLIN, M. K. Identity-based encryption from the weil pairing. In: *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 2001. p. 213–229. ISBN 3-540-42456-3. Versão completa disponível em `http://eprint.iacr.org/2001/090/`,.

[Cheng e Comley 2005]CHENG, Z.; COMLEY, R. *Efficient Certificateless Public Key Encryption*. 2005. Cryptology ePrint Archive, Report 2005/012. Disponível em: <http://eprint.iacr.org/>.

[Huang et al. 2005]HUANG, X. et al. On the security of certificateless signature schemes from asiacrypt 2003. In: DESMEDT, Y. et al. (Ed.). *CANS*. [S.l.]: Springer, 2005. (Lecture Notes in Computer Science, v. 3810), p. 13–25. ISBN 3-540-30849-0.

[Libert e Quisquater 2006]LIBERT, B.; QUISQUATER, J.-J. On Constructing Certificateless Cryptosystems from Identity Based Encryption. In: *Public Key Cryptography 2006 (PKC'06)*. [S.l.]: Springer-Verlag, 2006.

[Shamir 1984]SHAMIR, A. Identity-based cryptosystems and signature schemes. In: *Proceedings of CRYPTO 84 on Advances in cryptology*. New York, NY, USA: Springer-Verlag New York, Inc., 1984. p. 47–53. ISBN 0-387-15658-5.

[Zhang et al. 2006]ZHANG, Z. et al. Certificateless public key signature: Security model and efficient construction. In: *4th. International Conference on Applied Cryptography and Network Security*. [S.l.: s.n.], 2006.

CL-PKE e Adversário Tipo-I

- Adversário Tipo-I-CCA2:
  - não conhece *chave-mestra*;
  - pode substituir valores de chaves pública;
  - pode extrair chave secreta $SecDir$, desde que não tenha substituído a chave pública correspondente;
  - pode extrair chave secreta parcial $SecEsq$, desde que não seja a da entidade que se deseja atacar;
  - pode solicitar valores de chaves pública;
  - pode solicitar decriptografias, desde que não seja para o texto cifrado do desafio.

CL-PKE e Adversário Tipo-II

- Adversário Tipo-II-CCA2:
  - conhece *chave-mestra* (e, conseqüentemente, conhece todas as $SecEsq$ de interesse);
  - não pode substituir valores de chaves pública;
  - pode extrair $SecDir$ para identidades diferentes da desafiada;
  - pode solicitar valores de chaves pública;
  - pode solicitar decriptografias, desde que não seja para o texto cifrado do desafio.

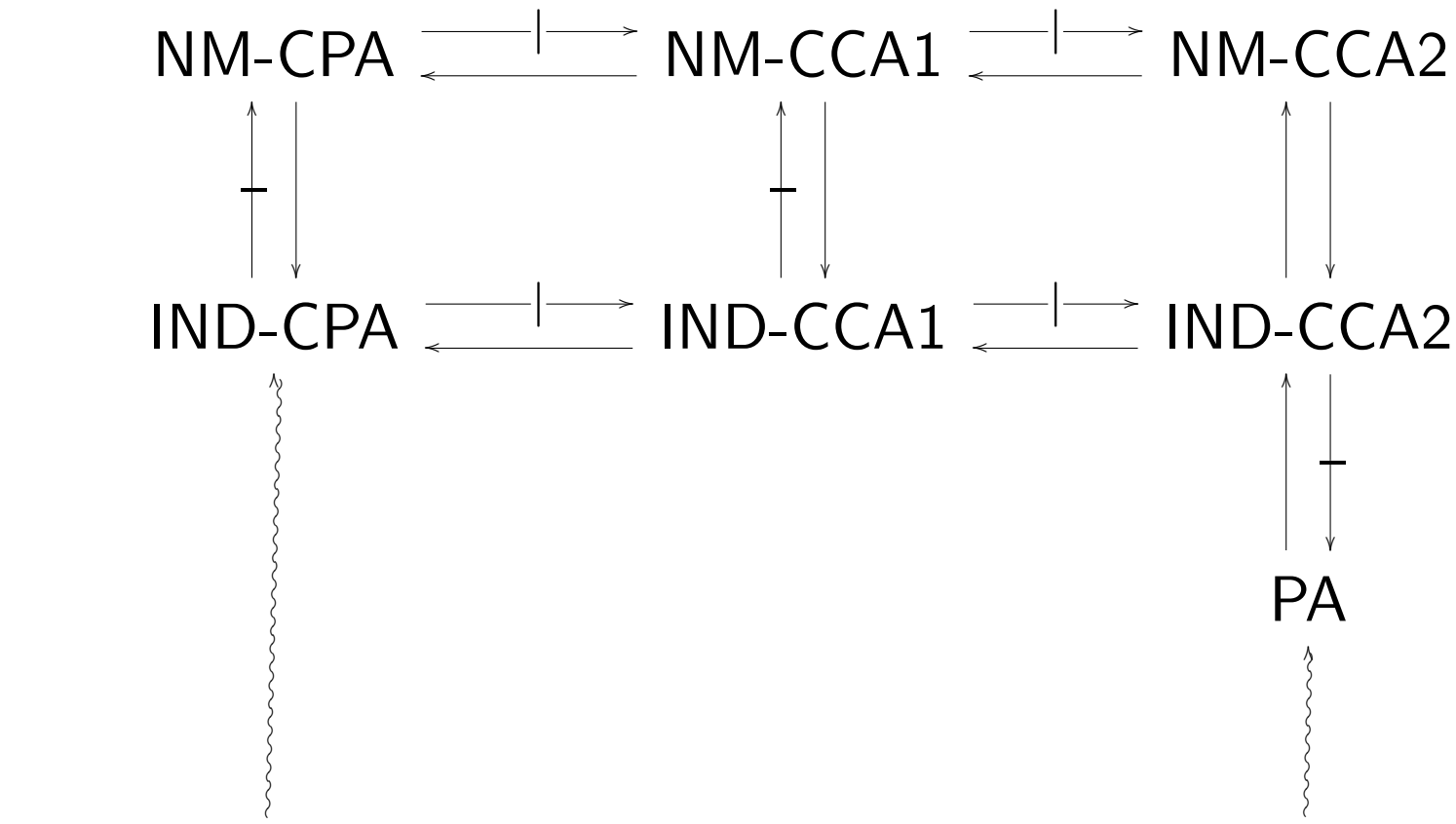
Noção de Segurança para CL-PKE

Vantagem de um adversário $\mathcal{A}$ Tipo-I (ou Tipo-II), contra o esquema $\mathcal{E}$:

$$Vant^{I}_{\mathcal{E},\mathcal{A}}(k) = \mid Pr[\text{conseguir diferenciar duas msgs}] - 1/2 \mid$$

Def: Um esquema $\mathcal{E}$ CL-PKE satisfaz a noção de segurança IND-CCA2 se para quaisquer adversários $\mathcal{A}$ Tipo-I e Tipo-II IND-CCA2, de tempo polinomial em k, são ínfimas as vantagens $Vant^{I}_{\mathcal{E},\mathcal{A}}(k)$ e $Vant^{II}_{\mathcal{E},\mathcal{A}}(k)$.

Noções de Segurança para PKE



Emparelhamento Bilinear

Sejam $\mathbb{G}_1$ e $\mathbb{G}_2$ grupos cíclicos de ordem prima q, então um *emparelhamento bilinear admissível* é uma função $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, que satisfaz:

1. Bilinearidade: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}, \forall P, Q \in \mathbb{G}_1$ e $a, b \in \mathbb{Z}_q$;
2. Não-degeneração: o mapeamento não envia todos os pares de $\mathbb{G}_1 \times \mathbb{G}_1$ para a identidade de $\mathbb{G}_2$;
3. Eficiência computacional: existe um algoritmo de complexidade de tempo polinomial que calcula $\hat{e}(P, Q)$, para todo $P, Q \in \mathbb{G}_1$.

Emparelhamentos de Weil e Tate, que adotam determinados grupos sobre pontos de curvas elípticas, satisfazem essas propriedades.

Emparelhamento Assimétrico

Sejam dois grupos cíclicos G_1, G_2, $G_1 \neq G_2$, e G_T, de ordem prima p, tais que:

1. $P \in G_1^*$ e $Q \in G_2^*$ são geradores;

2. $P = \psi(Q)$, onde $\psi()$ é um homomorfismo de G_2^* em G_1^*, eficientemente computável.

Um *emparelhamento assimétrico* é um emparelhamento bilinear admissível $e : G_1 \times G_2 \rightarrow G_T$.

Segurança de CL-PKE-Proposto

Assim como todos os esquemas precedentes, a segurança de CL-PKE-Proposto também recai na dificuldade do problema Diffie-Hellman Bilinear (BDH):

dados: $P, xP, yP, zP \in \mathbb{G}_1$

calcular: $\hat{e}(P, P)^{xyz}$