Relações Entre Protocolos de Criptografia de Chave Pública

Denise Goya (dhgoya@ime.usp.br)

DCC – IME – USP

2011, Abril

Fapesp no. 2008/06189-0

Objetivos

- Apresentar relações entre protocolos de chave pública.

Objetivos

- Apresentar relações entre protocolos de chave pública.
- Propriedades de interesse:
  - confidencialidade de mensagem e
  - autenticidade dos participantes;

Objetivos

- Apresentar relações entre protocolos de chave pública.
- Propriedades de interesse:
  - confidencialidade de mensagem e
  - autenticidade dos participantes;
- Classes de protocolos:
  - acordo de chave (não-interativos ou com autenticação);
  - cifração com chave pública (encryption);
  - encapsulamento de chave; e
  - cifrassinatura.

Roteiro

Roteiro

Motivação

- Protocolos criptográficos cada vez mais complexos;
- Como compreendê-los? Como construí-los?

Conceitos Preliminares

Criptografia de chave pública

- Grupos algébricos
- Problemas computacionais associados

Grupo Cíclico

- G: grupo cíclico finito (por ex. $\mathbb{Z}_p^*$)
- g: gerador de G

Grupo Cíclico

- G: grupo cíclico finito (por ex. $\mathbb{Z}_p^*$)
- g: gerador de G
- Problema do Logaritmo Discreto (DLP)
  - dados g e g^a, encontrar a

Grupo Cíclico

- G: grupo cíclico finito (por ex. $\mathbb{Z}_p^*$)
- g: gerador de G
- Problema do Logaritmo Discreto (DLP)
  - dados g e g^a, encontrar a
- Problema Diffie-Hellman Computacional (CDH)
  - dados g, g^a e g^b, encontrar g^{ab}
- Deseja-se G no qual DLP e CDH são supostamente difíceis

Emparelhamento Bilinear (tipo simétrico)

- Grupos G, G_T, onde DLP e CDH são difíceis
- P: gerador de G
- G em notação aditiva (soma de pontos; $aP = P + P + \cdots$)
- G_T em notação multiplicativa ($g^a = g \cdot g \cdot g \cdots$)
- mapeamento $e : GxG \rightarrow G_T$ é bilinear

$$e(aP, bP) = e(bP, aP) = e(P, P)^{ab}$$

Emparelhamento Bilinear (tipo simétrico)

- Grupos G, G_T, onde DLP e CDH são difíceis
- P: gerador de G
- G em notação aditiva (soma de pontos; $aP = P + P + \cdots$)
- G_T em notação multiplicativa ($g^a = g \cdot g \cdot g \cdots$)
- mapeamento $e : GxG \rightarrow G_T$ é bilinear

$$e(aP, bP) = e(bP, aP) = e(P, P)^{ab}$$

- Problema Diffie-Hellman Bilinear(BDH)
  - dados aP, bP e cP, encontrar $e(P, P)^{abc}$

Segurança dos Protocolos

Modelo de segurança:

- Definição de um conjunto de ações que um adversário pode ou não fazer
- Definição de segurança perante um adversário

Segurança dos Protocolos

Modelo de segurança:

- Definição de um conjunto de ações que um adversário pode ou não fazer
- Definição de segurança perante um adversário

Demonstração de segurança (por técnica de reduções):

- Demonstração por contradição;
- Suponha a existência de um adversário A
- Suponha que um determinado problema P é difícil
- Construa um algoritmo B, de tempo polinomial, que resolve P, usando passos de A

Roteiro

Non-Interactive Key Agreement - NIKA

- Acordo de chaves não interativo

Objetivo:

- Cálculo de um segredo compartilhado

Non-Interactive Key Agreement - NIKA

- Acordo de chaves não interativo

Objetivo:

- Cálculo de um segredo compartilhado

Motivação:

- Como combinar um segredo de forma segura?

Non-Interactive Key Agreement - NIKA

Exemplos:

- Diffie e Hellman, 1976 (DH76)
- Sakai, Ohgishi e Kasahara, 2000 (SOK00)

Diffie e Hellman, 1976

DH76	Alice	Beto
valor secreto valor público	a $A = g^a$	b $B = g^b$
cálculo do segredo	B^a	A^b
segredo compartilhado	$SK = g^{ab}$	

Sakai, Ohgishi e Kasahara, 2000

- Non-Interactive Key Agreement
- Baseado em identidades
- Chave pública é a própria identidade
- Requer autoridade de confiança: $< s, sP >$

Sakai, Ohgishi e Kasahara, 2000

SOK00	Alice	Beto
chave pública chave secreta	$Q_A = H(ID_A)$ sQ_A	$Q_B = H(ID_B)$ sQ_B
cálculo do segredo	$e(sQ_A, Q_B)$	$e(sQ_B, Q_A)$
segredo compartilhado	$SK = e(Q_A, Q_B)^s$	

Encryption

- Cifração no modelo de chave pública
- Objetivo:
  Cifrar uma mensagem m para o dono de uma chave pública

Encryption

- Cifração no modelo de chave pública
- Objetivo:
  Cifrar uma mensagem m para o dono de uma chave pública
- Cifra-se com a chave pública do destinatário
- Decifra-se com a chave secreta do destinatário

Encryption – Intuição de Como Obter

Cifrar:

1. Calcular um segredo compartilhado SK
2. Usar esse segredo SK para cifrar a mensagem m

Encryption – Intuição de Como Obter

Cifrar:

1. Calcular um segredo compartilhado SK
2. Usar esse segredo SK para cifrar a mensagem m

Decifrar:

1. Recuperar o segredo compartilhado SK
2. Recuperar a mensagem m, a partir da cifra e de SK

Encryption

Exemplos:

- ElGamal, 1985
- Boneh e Franklin, 2001

ElGamal, 1985

ElGamal85	Alice	Beto
valor secreto valor público	a $A = g^a$	b $B = g^b$
cifração de m p/ Beto	1) aleatório r 2) $SK = B^r$ 3) $U = g^r$ 4) $V = m \cdot SK$ 5) cifra $= (U, V)$	
decifração de (U, V) por Beto		1) $SK = U^b$ 2) $m = V \cdot SK^{-1}$

Encryption – Intuição de Como Obter

Cifrar:

1. Calcular um segredo compartilhado SK
2. Usar esse segredo SK para cifrar a mensagem m

Decifrar:

1. Recuperar o segredo compartilhado SK
2. Recuperar a mensagem m, a partir da cifra e de SK

Boneh e Franklin, 2001

BF01	Alice	Beto
chave pública chave secreta	$Q_A = H(ID_A)$ sQ_A	$Q_B = H(ID_B)$ sQ_B
cifração de m p/ Beto	1) aleatório r 2) $SK = H_2(e(sP, Q_B)^r)$ 3) $U = rP$ 4) $V = m \oplus SK$ 5) cifra $= (U, V)$	
decifração de (U, V) por Beto		1) $SK = H_2(e(U, sQ_B))$ 2) $m = V \oplus SK$

Non-Interactive Key Agreement ⟶ Encryption

- É possível descrever condições gerais em que vale a transformação
  Non-Interactive Key Agreement ⟶ Encryption
- Ex: Paterson e Srinivasan, 2009
  On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups

Non-Interactive Key Agreement $\longrightarrow$ Encryption

- É possível descrever condições gerais em que vale a transformação
  Non-Interactive Key Agreement $\longrightarrow$ Encryption
- Ex: Paterson e Srinivasan, 2009
  On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups
- Resultado: encryption fraco; não resistente a ataques de texto cifrado escolhido (ié, não é IND-CCA)
- Existem outras transformações que fortalecem a cifra FujisakiOkamotoO99, LibertQuisquater05, KiltzGalindo09, etc

Roteiro

Key Encapsulation Mechanism - KEM

- Mecanismo de encapsulamento de chave

Objetivo:

- Cifrar uma chave (para uso posterior em outro protocolo criptográfico)

Key Encapsulation Mechanism - KEM

- Mecanismo de encapsulamento de chave

Objetivo:

- Cifrar uma chave (para uso posterior em outro protocolo criptográfico)

Motivação:

- Encryption (chave pública) é mais lento/ineficiente que cifra simétrica

Key Encapsulation Mechanism - KEM

- Mecanismo de encapsulamento de chave

Objetivo:

- Cifrar uma chave (para uso posterior em outro protocolo criptográfico)

Motivação:

- Encryption (chave pública) é mais lento/ineficiente que cifra simétrica

Estratégia:

1. Usar cifra assimétrica para cifrar uma chave (KEM)
2. Usar cifra simétrica para cifrar os dados (DEM)

KEM – Intuição de Como Obter

Encapsular:

1. Calcular um segredo compartilhado SK
2. Enviar a parte pública do segredo compartilhado
3. Usar esse segredo SK como chave simétrica

KEM – Intuição de Como Obter

Encapsular:

1. Calcular um segredo compartilhado SK
2. Enviar a parte pública do segredo compartilhado
3. Usar esse segredo SK como chave simétrica

Desencapsular:

1. Recuperar o segredo compartilhado SK
2. Usar esse segredo SK como chave simétrica

KEM/DEM – Intuição de Como Obter

Encapsular Chave e Dado:

1. Calcular um segredo compartilhado SK
2. Usar esse segredo SK para cifrar a mensagem m, com cifra simétrica
3. Enviar a cifra e a parte pública do segredo compartilhado

KEM/DEM – Intuição de Como Obter

Encapsular Chave e Dado:

1. Calcular um segredo compartilhado SK
2. Usar esse segredo SK para cifrar a mensagem m, com cifra simétrica
3. Enviar a cifra e a parte pública do segredo compartilhado

Desencapsular Chave e Dado:

1. Recuperar o segredo compartilhado SK
2. Recuperar a mensagem m, a partir da cifra e de SK

Key Encapsulation Mechanism - KEM

Exemplos:

- Shoup, 2000
- DHIES: Abdalla, Bellare e Rogaway, 2000 – KEM/DEM
- Libert e Quisquater, 2005 (LQ05) – KEM/DEM

Libert e Quisquater, 2005 – parte KEM

LQ05	Alice	Beto
chave pública chave secreta	$Q_A = H(ID_A)$ sQ_A	$Q_B = H(ID_B)$ sQ_B
encapsular chave p/ Beto	1) aleatório r 2) $R = rP$ 3) $SK = H_2(e(sP, Q_B)^r, Q_B, R)$ 4) envia R para Beto	
desencapsular		$SK = H_2(e(R, sQ_B), Q_B, R)$

Libert e Quisquater, 2005 – partes KEM/DEM

LQ05	Alice	Beto
chaves	$< sQ_A, Q_A >$	$< sQ_B, Q_B >$
encapsular chave e dado	1) aleatório r 2) $R = rP$ 3) $SK = H_2(e(sP, Q_B)^r, Q_B, R)$ 4) $C = E_{SK}(M)$ 5) envia $< R, C >$ p/ Beto	
desencap. chave e dado		1) $SK = H_2(e(R, sQ_B), Q_B, R)$ 2) $M = D_{SK}(C)$

Encryption ⟶ KEM

- É possível descrever condições gerais em que vale a transformação
  Encryption ⟶ KEM

Encryption ⟶ KEM

- É possível descrever condições gerais em que vale a transformação
  Encryption ⟶ KEM
- Ex: Bentahar, Farshim, Malone-Lee e Smart, 2007
  Generic Constructions of Identity-Based and Certificateless KEMs
- Construções recentes admitem entrada fraca e saída forte

Como Obter KEM Forte, a Partir de Encryption Fraco

Encapsular:

1. Sorteia uma chave temporária m
2. $H_1(m)$ é aleatório temporário para calcular um segredo compartilhado
3. C é a cifra de m para dono de PK, usando aleatório $H_1(m)$
4. Chave encapsulada é $K = H_2(m)$
5. Envia C para dono de PK
6. Usa K como chave simétrica

Como Obter KEM Forte, a Partir de Encryption Fraco

Encapsular:

1. Sorteia uma chave temporária m
2. $H_1(m)$ é aleatório temporário para calcular um segredo compartilhado
3. C é a cifra de m para dono de PK, usando aleatório $H_1(m)$
4. Chave encapsulada é $K = H_2(m)$
5. Envia C para dono de PK
6. Usa K como chave simétrica

Desencapsular:

1. Recupera m a partir da chave secreta e de C
2. Verifica consistência de C perante m
3. Usa $K = H_2(m)$ como chave simétrica

Roteiro

Authenticated Key Agreement - AKA

- Acordo de Chave com Autenticação

Objetivo:

- Cálculo de um segredo compartilhado, com autenticação dos participantes

Authenticated Key Agreement - AKA

- Acordo de Chave com Autenticação

Objetivo:

- Cálculo de um segredo compartilhado, com autenticação dos participantes

Motivação:

- Como garantir que compartilho um segredo com a pessoa certa?

Authenticated Key Agreement - AKA

- Muitos modelos, muitos protocolos
- Bellare e Rogaway, 1993
- Blake-Wilson, Johnson e Menezes, 1997
- Canetti e Krawczyk, 2001
- LaMacchia, Lauter e Mityagin, 2007
- Protocolo padronizado não atende os modelos

AKA – Primeira Estratégia para Obter

Calcular um segredo compartilhado SK, dependente de:

1. Chaves púbica/secreta de ambos participantes
2. Chaves temporárias púbica/secreta de ambos participantes
3. Interação (troca de mensagens públicas)
4. Combinar convenientemente todos esses valores

Como Obter AKA a Partir de um KEM – Intuição

Cada participante:

1. Encapsula um segredo temporário e o envia para o parceiro
2. Desencapsula o segredo temporário recebido do parceiro (usando sua chave secreta)
3. Combina esses temporários para gerar o segredo compartilhado

Como Obter AKA a Partir de um KEM – Intuição

Cada participante:

1. Encapsula um segredo temporário e o envia para o parceiro
2. Desencapsula o segredo temporário recebido do parceiro (usando sua chave secreta)
3. Combina esses temporários para gerar o segredo compartilhado

Por que funciona?

KEM ⟶ AKA

- É possível descrever condições gerais em que vale a transformação
  KEM ⟶ AKA

KEM $\longrightarrow$ AKA

- É possível descrever condições gerais em que vale a transformação
  KEM $\longrightarrow$ AKA
- Ex: Boyd, Cliff, Gonzalez Nieto e Paterson, 2008
  Efficient One-Round Key Exchange in the Standard Model

Roteiro

Outras Relações

One-Way-ID-KA $\longrightarrow$ Certificateles-KEM

- Ex: Fiore, Gennaro e Smart, 2010
  Constructing Certificateless Encryption and ID-Based Encryption from ID-Based Key Agreement

Outras Relações

One-Way-ID-KA $\longrightarrow$ Certificateles-KEM

- Ex: Fiore, Gennaro e Smart, 2010
  Constructing Certificateless Encryption and ID-Based Encryption from ID-Based Key Agreement

One-Pass-KA $\longleftrightarrow$ Signcryption-KEM

- Ex: Gorantla, Boyd e Gonzalez Nieto, 2007
  On the Connection Between Signcryption and One-Pass Key Establishment

Conclusão

- Mostramos algumas construções intuitivas que transformam um tipo de protocolo em outro;
- Apontamos alguns trabalhos que formalizam tais construções.

Perguntas?

Obrigada!