Reduções da segurança de esquemas criptográficos: “Sequências de Jogos”

M. B. Barbosa @ di.uminho.pt

mbb@di.uminho.pt
Departamento de Informática
Escola de Engenharia
Universidade do Minho

Abril de 2006

Contexto

- As “provas” de segurança de **esquemas criptográficos** são muitas vezes estruturadas como sequências de jogos.
- O objectivo é tornar as provas mais claras e melhorar a sua verificabilidade. A aproximação alternativa é baseada puramente em teoria das probabilidades e em argumentos da teoria da informação.
- Há diversos estilos de apresentação deste tipo de prova. Aqui vamos seguir a aproximação de Shoup [`www.shoup.net`].
- Esta aproximação permite um rigor matemático razoável, sem entrar num formalismo exagerado.

Porquê jogos?

- A segurança de uma **primitiva criptográfica** é definida através de um jogo entre um **adversário** e uma entidade benigna chamada **desafiador** (*challenger*).
- Ambas as entidades são processos probabilísticos que comunicam entre sí. O jogo é visto como um espaço de probabilidades.
- O sucesso do adversário está associado a um evento S.
- Um esquema é seguro se a probabilidade de S ocorrer, para qualquer adversário *eficiente*, se afaste uma quantidade desprezável de um determinado alvo.
- Este alvo pode ser 0, $1/2$ ou a probabilidade de que um outro evento T ocorra num outro jogo em que o adversário esteja envolvido.

Sequências de Jogos

- As provas são apresentadas como sequências de n jogos $\textbf{Jogo}_1 \ldots \textbf{Jogo}_n$. Designa-se por $\textbf{Pr}[S_i]$ a probabilidade de sucesso de um adversário no $\textbf{Jogo}_i$.
- O $\textbf{Jogo}_1$ é o jogo associado à definição de segurança da primitiva criptográfica.
- O $\textbf{Jogo}_n$ é construído de forma a que $\textbf{Pr}[S_n]$ seja igual à probabilidade alvo (ou dela se afaste uma quantidade desprezável).
- As transições entre jogos são elas próprias analisadas por forma a garantir que

$$|\textbf{Pr}[S_i] - \textbf{Pr}[S_{i+1}]| \leq \epsilon_i$$

  sendo ϵ_i desprezável.
- A combinação destes resultados garante que a vantagem de qualquer adversário é sempre desprezável.

Transições entre jogos

- **Transições baseadas na indistinção**
  A transformação é efectuada tal que a existência de um adversário para o qual $|\mathbf{Pr}[S_i] - \mathbf{Pr}[S_{i+1}]|$ seja não desprezável implica a distinção entre duas distribuições computacionalmente indistinguíveis.
- **Transições baseadas em eventos de falha**
  O funcionamento dos jogos é idêntico, a não ser que ocorra um evento de falha F:
  $\mathbf{Pr}[S_i|\neg F] = \mathbf{Pr}[S_{i+1}|\neg F] \implies |\mathbf{Pr}[S_i] - \mathbf{Pr}[S_{i+1}]| \leq \mathbf{Pr}[F]$
  Interessa que $\mathbf{Pr}[F]$ seja desprezável.
- **Transições conservativas**
  Alterações apenas de forma, para tornar mais fácil a análise de transições posteriores: $\mathbf{Pr}[S_i] = \mathbf{Pr}[S_{i+1}]$.

Caso de Estudo: Cifras Assimétricas

A primitiva **cifra assimétrica** é definida através de um triplo de três algoritmos:

- O algoritmo PPT de geração dos parâmetros $\mathbb{G}(1^t)$ que recebe um parâmetro de segurança t e retorna um par de chaves $(\mathbf{Pk}, \mathbf{Sk})$.
- O algoritmo PPT de cifragem $\mathbb{E}(\mathrm{m}, \mathbf{Pk})$ que recebe uma mensagem e a chave pública e retorna um criptograma c.
- O algoritmo determinístico de decifragem $\mathbb{D}(c, \mathbf{Sk})$ que recebe um criptograma e a chave privada e retorna um texto limpo, ou um sinal de erro $\perp$.

Em geral pretende-se que, para qualquer par de chaves,

$$\mathbb{D}(\mathbb{E}(\mathrm{m}, \mathbf{Pk}), \mathbf{Sk}) = \mathrm{m}.$$

Segurança de Cifras Assimétricas

A **segurança semântica** para um ataque de **texto limpo escolhido** (IND-CPA) define-se através do seguinte jogo:

1. O desafiador executa o algoritmo de geração e obtém $(\mathbf{Pk}, \mathbf{Sk})$. Entrega **Pk** ao adversário.
2. O adversário eventualmente entrega ao desafiador um par de mensagens $(\mathtt{m}_0, \mathtt{m}_1)$ do mesmo comprimento.
3. O desafiador escolhe um bit b de forma aleatória, e entrega $c = \mathbb{E}(\mathtt{m}_b, \mathbf{Pk})$ ao adversário.
4. O adversário eventualmente devolve um bit b'.

Um esquema é seguro neste modelo de segurança se a vantagem máxima de qualquer adversário A

$$\mathbf{Adv}^{\mathtt{IND-CPA}}(A) = |\mathbf{Pr}(b' = b) - 1/2|$$

for desprezável.

Cifra El-Gamal simples

A cifra El-Gamal simples transforma mensagens codificadas como elementos de um grupo G:

- Seja G um grupo de ordem q, primo, e γ um gerador desse grupo.
- O algoritmo $\mathbb{G}$ gera $x \leftarrow \mathbb{Z}_q$ aleatóriamente, e faz $\alpha \leftarrow \gamma^x$. Retorna $(\mathbf{Pk}, \mathbf{Sk}) = (\alpha, x)$.
- O algoritmo $\mathbb{E}$ gera $y \leftarrow \mathbb{Z}_q$ aleatóriamente, e faz $\beta \leftarrow \gamma^y$, $\delta \leftarrow \alpha^y$ e $\psi \leftarrow \delta \cdot \mathrm{m}$. Retorna $c = (\beta, \psi)$.
- O algoritmo $\mathbb{D}$ simplesmente retorna $\mathrm{m} \leftarrow \psi \cdot (\beta^x)^{-1}$.

Claramente

$$\mathbb{D}(\mathbb{E}(\mathrm{m}, \mathbf{Pk}), \mathbf{Sk}) = (\mathrm{m} \cdot \delta) \cdot \beta^{-x} = \mathrm{m} \cdot \gamma^{xy-yx} = \mathrm{m}$$

Segurança da Cifra El-Gamal simples

A segurança da cifra El Gamal baseia-se no pressuposto de que é computacionalmente intratável distinguir tuplos da forma $(\gamma^x, \gamma^y, \gamma^{xy})$ de tuplos genéricos $(\gamma^x, \gamma^y, \gamma^z)$.

Definition (Pressuposto da Decisão Diffie-Hellman (DDH))

Seja A um algoritmo que recebe um triplo da forma $(\gamma^x, \gamma^y, \gamma^z)$ e retorna 0 ou 1. Então, para qualquer A temos que

$$\mathbf{Adv}^{\mathrm{DDH}}(A) = |\mathbf{Pr}[A(\gamma^x, \gamma^y, \gamma^{xy}) = 1] - \mathbf{Pr}[A((\gamma^x, \gamma^y, \gamma^z) = 1]|$$

é desprezável.

Segurança da Cifra El-Gamal simples

Theorem

Seja A um adversário da cifra El-Gamal simples no jogo IND-CPA. Se A tem vantagem não desprezável, então existe um algoritmo B, que utiliza A como sub-rotina, e que tem vantagem não desprezável na resolução do problema DDH

$$\mathbf{Adv}^{\mathrm{DDH}}(B) = \mathbf{Adv}^{\mathrm{IND-CPA}}(A)$$

Por outras palavras, o teorema diz:

Se é intratável resolver o problema DDH, também é intratável ganhar o jogo IND-CPA contra a cifra El-Gamal simples.

Chamemos ϵ_{DDH} à vantagem máxima de qualquer algoritmo na resolução do problema DDH.

Prova de segurança da Cifra El-Gamal simples

O ponto de partida é o jogo que define a segurança IND-CPA:

Definition (**Jogo**$_0$)

1. $x \leftarrow \mathbb{Z}_q$
2. $\alpha \leftarrow \gamma^x$
3. $(\mathrm{m}_0, \mathrm{m}_1) \leftarrow A(\alpha)$
4. $b \leftarrow \{0, 1\}$
5. $y \leftarrow \mathbb{Z}_q$
6. $\beta \leftarrow \gamma^y$
7. $\psi \leftarrow \mathrm{m}_b \cdot \alpha^y$
8. $b' \leftarrow A(\alpha, \beta, \psi)$

Definindo S_0 como o evento $b' = b$, temos

$$\mathbf{Adv}^{\mathtt{IND-CPA}}(A) = |\mathbf{Pr}[S_0] - 1/2|$$

Prova de segurança da Cifra El-Gamal simples

Utiliza-se uma transição baseada na distinção de jogos:

Definition (**Jogo**$_1$)

1. $x \leftarrow \mathbb{Z}_q$
2. $\alpha \leftarrow \gamma^x$
3. $(\mathrm{m}_0, \mathrm{m}_1) \leftarrow A(\alpha)$
4. $b \leftarrow \{0, 1\}$
5. $y \leftarrow \mathbb{Z}_q$
6. $\beta \leftarrow \gamma^y$
7. $z \leftarrow \mathbb{Z}_q$
8. $\psi \leftarrow \mathrm{m}_b \cdot \gamma^z$
9. $b' \leftarrow A(\alpha, \beta, \psi)$

Fazendo de S_1 o evento $b = b'$ neste jogo, temos

$$\mathbf{Pr}[S_1] = 1/2.$$

porque γ^z é efectivamente um *one-time-pad*.

Prova de segurança da Cifra El-Gamal simples

Para completar a prova, é necessário demonstrar que $|\mathbf{Pr}[S_0] - \mathbf{Pr}[S_1]|$ é desprezável. Para isso utilizamos um algoritmo de interpolação que resolve o problema DDH.

Definition (Algoritmo $B(\alpha, \beta, \delta)$)

1. $(\mathrm{m}_0, \mathrm{m}_1) \leftarrow A(\alpha)$
2. $b \leftarrow \{0, 1\}$
3. $\psi \leftarrow \delta \cdot \mathrm{m}_b$
4. $b' \leftarrow A(\alpha, \beta, \psi)$
5. `If` $b = b'$
   `return` 1
   `else return` 0

Prova de segurança da Cifra El-Gamal simples

- No caso do input do algoritmo B ser um tuplo Diffie Hellman $(\alpha, \beta, \delta) = (\gamma^x, \gamma^y, \gamma^{xy})$, o algoritmo A está a ser executado exactamente de acordo com o **Jogo**$_0$, donde

$$\mathbf{Pr}[B(\gamma^x, \gamma^y, \gamma^{xy}) = 1] = \mathbf{Pr}[S_0]$$

- No caso do input do algoritmo B não ser um tuplo Diffie Hellman $(\alpha, \beta, \delta) = (\gamma^x, \gamma^y, \gamma^z)$, o algoritmo A está a ser executado exactamente de acordo com o **Jogo**$_1$, donde

$$\mathbf{Pr}[B(\gamma^x, \gamma^y, \gamma^z) = 1] = \mathbf{Pr}[S_1]$$

- Mas nós sabemos que

$$|\mathbf{Pr}[B(\gamma^x, \gamma^y, \gamma^{xy}) = 1] - \mathbf{Pr}[B(\gamma^x, \gamma^y, \gamma^z) = 1]| \leq \epsilon_{\mathrm{DDH}}$$

donde

$$\mathbf{Adv}^{IND-CPA}(A) = |\mathbf{Pr}[S_0] - 1/2| = |\mathbf{Pr}[S_0] - \mathbf{Pr}[S_1]|| \leq \epsilon_{\mathrm{DDH}}$$

Cifra El-Gamal Hashed

Na cifra El-Gamal Hashed as mensagens são sequências arbitrárias de bits:

- Seja G um grupo de ordem q, primo, e γ um gerador desse grupo.
- O algoritmo $\mathbb{G}$ gera $x \leftarrow \mathbb{Z}_q$ aleatóriamente, e faz $\alpha \leftarrow \gamma^x$. Retorna $(\mathbf{Pk}, \mathbf{Sk}) = (\alpha, x)$.
- O algoritmo $\mathbb{E}$ gera $y \leftarrow \mathbb{Z}_q$ aleatóriamente, e faz $\beta \leftarrow \gamma^y$, $\delta \leftarrow \alpha^y$ e $\psi \leftarrow H(\delta) \oplus \mathrm{m}$. Retorna $c = (\beta, \psi)$.
- O algoritmo $\mathbb{D}$ simplesmente retorna $\mathrm{m} \leftarrow \psi \oplus H(\beta^x)$.

Claramente

$$\mathbb{D}(\mathbb{E}(\mathrm{m}, \mathbf{Pk}), \mathbf{Sk}) = (\mathrm{m} \oplus H(\delta)) \oplus H(\beta^x) = \mathrm{m} \oplus H(\gamma^{xy}) \oplus H(\gamma^{yx}) = \mathrm{m}$$

Segurança da Cifra El-Gamal Hashed

Assumimos que a função de hash é uma função aleatória perfeita: apenas fornecendo o input δ correcto podemos obter o resultado $H(\delta)$ (Modelo Random-Oracle).

Neste modelo, a segurança da cifra El Gamal Hashed baseia-se no pressuposto de que é impossível calcular γ^{xy} dados (γ^x, γ^y).

Definition (Pressuposto Computacional Diffie-Hellman (CDH))

Seja A um algoritmo que recebe um par da forma (γ^x, γ^y) e retorna um valor da mesma forma. Então, para qualquer A temos que

$$\mathbf{Adv}^{\mathrm{CDH}}(A) = \mathbf{Pr}[A(\gamma^x, \gamma^y) = \gamma^{xy}]$$

é desprezável.

Segurança da Cifra El-Gamal Hashed

Theorem

Seja A um adversário da cifra El-Gamal Hashed no jogo IND-CPA e no modelo RO. Se A tem vantagem não desprezável, então existe um algoritmo B, que utiliza A como sub-rotina, e que tem vantagem não desprezável na resolução do problema CDH

$$\mathbf{Adv}^{\mathtt{CDH}}(B) \geq \frac{1}{q_H}\mathbf{Adv}^{\mathtt{IND-CPA}}(A)$$

em que q_H é o número máximo de chamadas de A a H.

Por outras palavras, o teorema diz:

Se a função de hash é perfeita, e se é intratável resolver o problema CDH, também é intratável ganhar o jogo IND-CPA contra a cifra El-Gamal Hashed.

Prova de segurança da Cifra El-Gamal Hashed

O ponto de partida é o jogo que define a segurança IND-CPA:

Definition (**Jogo**$_0$)

1. $x \leftarrow \mathbb{Z}_q$
2. $\alpha \leftarrow \gamma^x$
3. $(\mathrm{m}_0, \mathrm{m}_1) \leftarrow A(\alpha)$
4. $b \leftarrow \{0, 1\}$
5. $y \leftarrow \mathbb{Z}_q$
6. $\beta \leftarrow \gamma^y$
7. $\psi \leftarrow \mathrm{m}_b \oplus H(\alpha^y)$
8. $b' \leftarrow A(\alpha, \beta, \psi)$

Cada chamada de A à função H, para um valor δ, é efectuada através do desafiador, que simplesmente retorna $H(\delta)$.

Definindo S_0 como o evento $b' = b$, temos

$$\mathbf{Adv}^{\mathtt{IND-CPA}}(A) = |\mathbf{Pr}[S_0] - 1/2|$$

Prova de segurança da Cifra El-Gamal Hashed

Utiliza-se uma transição baseada num evento de falha:

Definition (**Jogo**$_1$)

1. $x \leftarrow \mathbb{Z}_q$
2. $\alpha \leftarrow \gamma^x$
3. $(\mathrm{m}_0, \mathrm{m}_1) \leftarrow A(\alpha)$
4. $b \leftarrow \{0,1\}$
5. $y \leftarrow \mathbb{Z}_q$
6. $\beta \leftarrow \gamma^y$
7. $h \leftarrow \{0,1\}^{|\mathrm{m}|}$
8. $\psi \leftarrow \mathrm{m}_b \oplus h$
9. $b' \leftarrow A(\alpha, \beta, \psi)$

Cada chamada de A à função H, para um valor δ, é efectuada através do desafiador, que simplesmente retorna $H(\delta)$.

Fazendo de S_1 o evento $b = b'$ neste jogo, temos $\mathbf{Pr}[S_1] = 1/2$ porque h é efectivamente um *one-time-pad*.

Prova de segurança da Cifra El-Gamal Hashed

Para completar a prova, é necessário demonstrar que $|\mathbf{Pr}[S_0] - \mathbf{Pr}[S_1]|$ é desprezável.

Para isso recorremos ao facto de os jogos serem idênticos a não ser que o adversário efectue a chamada $H(\delta = \gamma^{xy})$.

Chamemos F a este evento:

$$|\mathbf{Pr}[S_0] - \mathbf{Pr}[S_1]| \leq \mathbf{Pr}[F]$$

É necessário demonstrar que a probabilidade de F ocorrer é desprezável.

Para isso construimos um algoritmo B que utiliza A como sub-rotina num ambiente idêntico ao do $\mathbf{Jogo}_1$ e que resolve o problema CDH com vantagem não desprezável, se F ocorrer com vantagem não desprezável.

Prova de segurança da Cifra El-Gamal Hashed

O algoritmo B funciona da seguinte maneira.

Definition (Algoritmo $B(\alpha, \beta)$)

1. $(\mathrm{m}_0, \mathrm{m}_1) \leftarrow A(\alpha)$
2. $b \leftarrow \{0,1\}$
3. $h \leftarrow \{0,1\}^{|\mathrm{m}|}$
4. $\psi \leftarrow h \oplus \mathrm{m}_b$
5. $b' \leftarrow A(\alpha, \beta, \psi)$
6. Retorna um elemento de L à sorte.

Cada chamada de A à função H, para um valor δ, é efectuada através de B, que retorna $H(\delta)$. B mantém uma lista L onde insere todos os valores δ.

O algoritmo B terá a resposta ao problema CDH na lista L caso o evento F ocorra. Nesse caso, resolve o problema com probabilidade $1/|L| = 1/q_H$.

Prova de segurança da Cifra El-Gamal Hashed

- Juntando tudo, temos:

$$\mathbf{Adv}^{\mathrm{CDH}}(B) = \frac{1}{q_H}\mathbf{Pr}[F] \leq \epsilon_{\mathrm{CDH}}$$

$$\mathbf{Adv}^{\mathrm{IND-CPA}}(A) = |\mathbf{Pr}[S_0] - 1/2| = |\mathbf{Pr}[S_0] - \mathbf{Pr}[S_1]| \leq q_H \cdot \epsilon_{\mathrm{CDH}}$$

- A vantagem de qualquer adversário que execute em tempo polinomial é desprezável porque qualquer factor polinomial multiplicado por um valor desprezável (exponencialmente pequeno no factor de segurança) é ainda desprezável.