Provas de Segurança

Mestrado em Engenharia Física

J. Bacelar Almeida (`jba@di.uminho.pt`)

Departamento de Informática
Universidade do Minho

Formalização da Segurança

- Interessa caracterizar formalmente (de forma rigorosa) *o que se entende por segurança de uma primitiva criptográfica*.
- Em particular, pressupõe caracterizar:
    1. a primitiva criptográfica considerada e qual é o seu objectivo;
    2. critérios que estabelecem a segurança da primitiva.
- No primeiro ponto, define-se o *Sistema Criptográfico* em análise;
- No segundo, define-se
    - no que consiste um ataque à primitiva;
    - capacidades atribuídas ao adversário
        - interacção que lhe é permitida com o Sistema Criptográfica;
        - informação a que tem acesso (argumentos, oráculos);
        - limitações computacionais (e.g. *Probabilistic Polynomial-Time (PTT)*);

Parte I

Criptografia Simétrica

Sistema Criptográfico

- Uma primitiva criptográfica consiste num conjunto de operações cuja utilização deve ser orquestrada por forma a cumprir com os objectivos pretendidos.
- Exemplo: cifra simétrica
  - KGen: **procedimento probabilístico** de geração da chave;
  - Enc: **procedimento probabilístico** que produz o criptograma correspondente a uma mensagem (para determinada chave)
  - Dec: **procedimento determinístico** que recupera a mensagem do criptograma
- Critério de **correcção**: uma cifra $\Sigma = \langle \mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec} \rangle$ diz-se correcta quando

$$\boxed{\begin{array}{l} \mathsf{Correct}^{\Sigma}(m) \\ \hline 1: \quad k \leftarrow_{\$} \mathsf{KGen}() \\ 2: \quad c \leftarrow_{\$} \mathsf{Enc}_k(m) \\ 3: \quad \textbf{return } \mathsf{Dec}_k(c) = m \end{array}}$$

$$\forall m \in \mathcal{M}, \Pr\left[\mathsf{Correct}^{\Sigma}(m) = \mathsf{true}\right] = 1$$

Jogos de Segurança

- Interacção entre as diversas componentes da análise (operações do sistema criptográfico; adversário; etc.) são capturadas por **experiências probabilísticas**.
- Essas experiências são descritas por programas probabilísticos designados por **Jogos de Segurança**.
- Nesses jogos, considera-se que o adversário "ganha" quando um *ataque* é bem sucedido.
- A segurança será assim estabelecida argumentando que, para qualquer adversário (da classe considerada), a probabilidade de sucesso é "insignificante".

Funções negligenciáveis

- Interessa capturar o conceito de "probabilidade de sucesso insignificante" (e.g. resultante de uma escolha aleatória num universo muito grande);
- Note-se a natureza *assimptóptica* do conceito pretendido – é relativo a um parâmetro de segurança λ (e.g. tamanho da chave)[1];
- Uma função diz-se *negligenciável* quando tende para zero mais rápido do que a inversa de qualquer polinómio.

Definition (Função Negligenciável)

Uma função $f : \mathbb{N} \to \mathbb{R}$ diz-se *negligenciável* ($f \in \mathrm{negl}(\lambda)$) quando, para qualquer $c \in \mathbb{N}$ existe $N_c \in \mathbb{N}$, tal que, para qualquer $k > N$,

$$|f(k)| < k^{-c}$$

[1] No que se segue, iremos normalmente considerar o parâmetro de segurança λ implícito.

Exemplo: função *one-way*

- Defina-se o "jogo" OW que desafia o adversário a inverter a função f:

$$
\begin{array}{l}
\mathsf{OW}^{f}(\mathcal{A}) \\
\hline
1: \quad x \leftarrow_{\$} \{0,1\}^{k} \\
2: \quad y = f(x) \\
3: \quad x' \leftarrow_{\$} \mathcal{A}(y) \\
4: \quad \textbf{return } f(x') = y
\end{array}
$$

- A **vantagem** de um adversário $\mathcal{A}$ é definida como a probabilidade de sucesso da experiência:

$$\mathsf{Adv}^{\mathsf{ow}}_{\mathcal{A}} = \Pr\left[\mathsf{OW}^{f}(\mathcal{A}) = \mathsf{true}\right]$$

- f é *one-way* quando, para qualquer adversário $\mathcal{A} \in \mathsf{PPT}$:

$$\mathsf{Adv}^{\mathsf{ow}}_{\mathcal{A}} \in \mathsf{negl}(\lambda)$$

Propriedade de Confidencialidade

- Para estabelecer a segurança de uma cifra, devemos garantir a confidencialidade da informação cifrada.
- Já estudamos o critério de "segurança absoluta" [Shannon], que pode ser expressa como: para qualquer par de mensagens $m_0, m_1 \in \mathcal{M}$ e criptograma $c \in \mathcal{C}$,

$$\Pr[\mathsf{Enc}_k(m_0) = c] = \Pr[\mathsf{Enc}_k(m_1) = c] .$$

- Esse critério pode ser relaxado para considerar a capacidade de um adversário, com limitações computacionais, em distinguir os criptogramas resultantes da cifra de duas mensagens <u>com o mesmo tamanho</u>.

Indistinguibilidade de criptogramas

- Uma forma de capturar a proximidade das duas probabilidades apresentadas consiste em desafiar o adversário a reconhecer qual a mensagem cifrada de entre duas mensagens de igual tamanho por si escolhidas:

$$
\begin{array}{|l|}
\hline
\mathrm{IND}(\mathcal{A}) \\
\hline
\begin{array}{rl}
1: & k \leftarrow_{\$} \mathsf{KGen}(1^{\lambda}) \\
2: & (m_0, m_1, \mathsf{state}) \leftarrow_{\$} \mathcal{A}_1() \\
3: & b \leftarrow_{\$} \{0,1\} \\
4: & c \leftarrow_{\$} \mathsf{Enc}_k(m_b) \\
5: & b' \leftarrow_{\$} \mathcal{A}_2(\mathsf{state}, c) \\
6: & \textbf{return } b = b'
\end{array} \\
\hline
\end{array}
$$

- Note-se que o adversário intervém em “duas fases” distintas ($\mathcal{A}_1$ e $\mathcal{A}_2$), mas admite-se que preserve a memória entre essas duas fases (através da variável state).

IND-CPA

- O jogo IND apresentado atrás acaba por capturar uma noção de segurança **muito fraca** por não considerar informação que tipicamente está disponível ao adversário:
  - pares texto-limpo/criptograma (ataque de **texto-limpo conhecido**);
  - observar o efeito da cifra sobre mensagens por si escolhidas (ataque de **texto-limpo escolhido**).
- Com vista a "enriquecer" a noção de segurança considerada, acrescenta-se a possibilidade de o adversário recorrer a um **oráculo** que possibilite cifrar mensagens.

- O jogo IND-CPA (*indistinguishability under choosen plaintext attack*) é então definido como:

$$
\begin{array}{|ll|}
\hline
\multicolumn{2}{|l|}{\mathrm{IND\text{-}CPA}(\mathcal{A})} \\
\hline
1: & k \leftarrow_{\$} \mathsf{KGen}(1^{\lambda}) \\
2: & (m_0, m_1, \mathsf{state}) \leftarrow_{\$} \mathcal{A}_1^{\mathsf{Enc}_k}() \\
3: & b \leftarrow_{\$} \{0,1\} \\
4: & c \leftarrow_{\$} \mathsf{Enc}_k(m_b) \\
5: & b' \leftarrow_{\$} \mathcal{A}_2^{\mathsf{Enc}_k}(\mathsf{state}, c) \\
6: & \textbf{return } b = b' \\
\hline
\end{array}
$$

- A vantagem do adversário é definida como

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{ind\text{-}cpa}} = |2 * \Pr[\mathrm{IND\text{-}CPA}(A) = \mathsf{true}] - 1|$$

- Uma cifra exibe segurança IND-CPA se, para qualquer adversário $\mathcal{A} \in \mathsf{PPT}$,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{ind\text{-}cpa}} \in \mathsf{negl}(\lambda) .$$

IND-CCA

- Uma noção de segurança mais forte surge quando disponibilizamos ao adversário um oráculo para decifrar criptogramas à sua escolha (condicionado a que não o aplique no “desafio” do jogo).
- O jogo IND-CCA (*indistinguishability under choosen ciphertext attack*) é definido como:

IND-CCA($\mathcal{A}$)

1 : $k \leftarrow_\$ \mathsf{KGen}(1^\lambda)$
2 : $(m_0, m_1, \mathsf{state}) \leftarrow_\$ \mathcal{A}_1^{\mathsf{Enc}_k,\mathsf{Dec}_k}()$
3 : $b \leftarrow_\$ \{0, 1\}$
4 : $c \leftarrow_\$ \mathsf{Enc}_k(m_b)$
5 : $b' \leftarrow_\$ \mathcal{A}_2^{\mathsf{Enc}_k,\mathsf{Dec}_k}(\mathsf{state}, c)$
6 : **return** $b = b' \wedge \mathsf{Dec}_k(c)$ não foi invocado

Raciocinar sobre a segurança de cifras

- A forma mais directa de beneficiar das definições apresentadas é em resulta-
dos "pela negativa" (e.g. demonstrar a "insegurança" de uma cifra):

  > *Para demonstrar a insegurança de uma cifra, é suficiente exibir uma adversário concreto $\mathcal{A}$ que obtenha uma vantagem de sucesso não negligenciável.*

- Já a demonstração de segurança é tipicamente estabelecida por um *argumento de redução*

  > *Admitindo que existe uma adversário $\mathcal{A}$ que obtém uma vantagem não negligenciável a atacar o jogo de segurança, constrói-se um adversário $\mathcal{B}(\mathcal{A})$ que será capaz de atacar uma **assumpção** de segurança.*

Exemplos:

- Insegurança IND do modo ECB numa cifra de blocos (para mensagens com mais de que um bloco);
- Insegurança IND-CPA do modo ECB para cifrar um único bloco (obs: e, em geral, para qualquer cifra determinística...);
- Segurança IND-CPA do modo CTR$ numa cifra por blocos (por redução à segurança da PRF subjacente);
- Insegurança IND-CCA do modo CTR numa cifra por blocos.

Integridade do Criptograma

- Para capturar a propriedade de integridade numa cifra, considera-se que a operação Dec possa falhar

$$\mathsf{Dec} : \mathcal{K} \times \mathcal{C} \to \mathcal{M} \cup \perp$$

- Quando um criptograma não for rejeitado pela operação Dec (i.e. $\mathsf{Dec}_k(c) \neq \perp$), diz-se que o criptograma é **válido**.
- Assim, para comprometer a integridade, o adversário irá procurar "forjar" um criptograma válido.
- *Verification Oracle*:

$$\mathsf{Dec}^{\star}_k(c) \triangleq (\mathsf{Dec}_k(c) \neq \perp)$$

INT-PTXT

- A propriedade de "integridade de texto-limpo" (*plaintext integrity (INT-PTXT)*) estabelece a incapacidade de um adversário "forjar" um criptograma válido.
- Para "forjar" esse criptograma, possibilita-se que o adversário recorra a oráculos que:
  - permitem cifrar qualquer mensagem à sua escolha;
  - testar se criptogramas são válidos ou não.
- Mas, evidentemente, impõe-se restrições sobre o criptograma forjado: *o texto limpo correspondente não deverá ter sido submetido ao oráculo* Enc_k.

INT-PTXT($\mathcal{A}$)

---

1 : $k \leftarrow_{\$} \mathsf{KGen}(1^\lambda)$

2 : $c \leftarrow_{\$} \mathcal{A}^{\mathsf{Enc}_k, \mathsf{Dec}_k^\star}()$

3 : **return** $\mathsf{Dec}_k(c) = m \wedge \mathsf{Enc}_k(m)$ não foi invocado por $\mathcal{A}$

INT-CTXT

- Uma noção mais forte de integridade é obtida quando se relaxa a restrição sobre a utilização do oráculo para impedir somente que $\mathcal{A}$ não use directamente o resultado.
- Obtém-se assim o que se designa por "integridade do criptograma" (*ciphertext integrity (INT-CTXT)*)

INT-CTXT($\mathcal{A}$)	
1 :	$k \leftarrow_{\$} \mathsf{KGen}(1^\lambda)$
2 :	$c \leftarrow_{\$} \mathcal{A}^{\mathsf{Enc}_k, \mathsf{Dec}^\star_k}()$
3 :	**return** $\mathsf{Dec}_k(c) = m \wedge c$ não foi obtido como resposta ao oráculo Enc_k

- Note que INT-CTXT implica INT-PTXT (quando $\mathsf{Enc}_k(\mathsf{Dec}_k(c))$ não for invocado, então c não pode surgir como resposta).
- Por outro lado, INT-CTXT é estritamente mais forte que INT-PTXT (e.g. considerando um bit redundante no criptograma...)

Cifra Autenticada

- Numa cifra autenticada, pretende-se garantir simultaneamente *confidencialidade* e *integridade*.
- Pode ser conseguido combinando uma “cifra” com um “MAC”.
- Possíveis combinações genéricas:
  - *encrypt & MAC* – aplicar separadamente a cifra e MAC;
  - *MAC-then-encrypt* – cifra mensagem juntamente com *tag* de autenticação;
  - *encrypt-then-MAC* – aplica MAC sobre criptograma.
- Estas diferentes combinações resultam em garantias muito distintas.

- Considere-se:
  - Uma cifra que exiba segurança IND-CPA;
  - Um MAC que garanta INT-PTXT.
- Nesse caso, pode-se demonstrar que[2]:

	Confidencialidade	**Integridade**
encrypt & MAC	X	INT-PTXT
MAC-then-encrypt	IND-CPA	INT-PTXT
encrypt-then-MAC	IND-CCA	INT-CTXT

[2] Bellare & Namprempre, 2007 – Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm

Parte II

Criptografia Assimétrica

Confidencialidade em Criptografia Assimétrica

- Os modelos de segurança IND-CPA e IND-CCA podem ser facilmente adaptados para criptografia assimétrica.
- Para tal, deveremos:
  1. disponibilizar ao adversário a chave pública;
  2. resultando que o oráculo para cifra pode ser dispensado (redundante).
- Consequentemente, resultados como "insegurança de cifras determinísticas" transferem-se directamente para a criptografia assimétrica (e.g. aplicação directa da primitiva RSA).

IND-CPA

- Para um sistema de cifra de chave pública

$$\Sigma = \langle \mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec} \rangle$$

$$\begin{array}{|ll|}
\hline
\multicolumn{2}{|l|}{\text{IND-CPA}(\mathcal{A})} \\
\hline
1: & (sk, pk) \leftarrow_{\$} \mathsf{KGen}(1^{\lambda}) \\
2: & (m_0, m_1, \mathsf{state}) \leftarrow_{\$} \mathcal{A}_1(pk) \\
3: & b \leftarrow_{\$} \{0, 1\} \\
4: & c \leftarrow_{\$} \mathsf{Enc}(pk, m_b) \\
5: & b' \leftarrow_{\$} \mathcal{A}_2(\mathsf{state}, c) \\
6: & \textbf{return } b = b' \\
\hline
\end{array}$$

- Tal como anteriormente, a segurança é estabelecida quando a vantagem do adversário é negligenciável

$$\mathsf{Adv}_{\mathcal{A}}^{\text{ind-cpa}} = |2 * \Pr[\text{IND-CPA}(A) = \mathsf{true}] - 1|$$

- De forma análoga, para IND-CCA:

IND-CCA($\mathcal{A}$)

1 : $(sk, pk) \leftarrow_\$ \mathsf{KGen}(1^\lambda)$
2 : $(m_0, m_1, \mathsf{state}) \leftarrow_\$ \mathcal{A}_1^{\mathsf{Dec}_{sk}}(pk)$
3 : $b \leftarrow_\$ \{0, 1\}$
4 : $c \leftarrow_\$ \mathsf{Enc}_k(m_b)$
5 : $b' \leftarrow_\$ \mathcal{A}_2^{\mathsf{Dec}_{sk}}(\mathsf{state}, c)$
6 : **return** $b = b' \wedge \mathsf{Dec}_{sk}(c)$ não foi invocado

Segurança de esquemas de assinatura

- As noções de segurança para esquemas de assinaturas são semelhantes às apresentadas para *integridade*:
  - A ideia consiste em desafiar o adversário a apresentar uma assinatura forjada,
  - sendo que durante o processo pode “solicitar” assinaturas para mensagens à sua escolha.
- Mais uma vez, o facto de a chave de verificação ser pública irá dispensar o respectivo oráculo.

EUF-CMA

- A propriedade de "*Existential UnForgeability under Choosen Message Attacks* (EUF-CMA)" caracteriza-se pelo seguinte jogo:

EUF-CMA($\mathcal{A}$)
1 : $(sk, pk) \leftarrow_\$ \mathsf{KGen}(1^\lambda)$
2 : $(m, \sigma) \leftarrow_\$ \mathcal{A}^{\mathsf{Sign}_{sk}}(pk)$
3 : **return** $\mathsf{Verify}(pk, \sigma) = m \wedge \mathsf{Sign}_{sk}(m)$ não foi invocado por $\mathcal{A}$

SUF-CMA

- Tal como no caso da integridade, é possível considerar uma propriedade mais forte se se relaxar a restrição sobre a utilização do oráculo para impedir somente que $\mathcal{A}$ não use directamente o resultado.
- Obtém-se assim o que se designa por "*Strong existential UnForgeability under Choosen Message Attacks* (SUF-CMA)":

SUF-CMA($\mathcal{A}$)

1 : $(sk, pk) \leftarrow_\$ \mathsf{KGen}(1^\lambda)$
2 : $(m, \sigma) \leftarrow_\$ \mathcal{A}^{\mathsf{Sign}_{sk}}(pk)$
3 : **return** $\mathsf{Verify}(_{pk}(\sigma) = m \wedge \sigma$ não foi obtido como resposta do oráculo