# 现代密码学
# Modern Cryptography

张方国

中山大学计算机学院

Office: Room A305, IM School Building
E-mail: isszhfg@mail.sysu.edu.cn
HomePage: http://cse.sysu.edu.cn/content/2460

# 第十七讲 RSA(四)

- RSA的语义安全性

1）密文可识别

2）语义安全的公钥密码体制

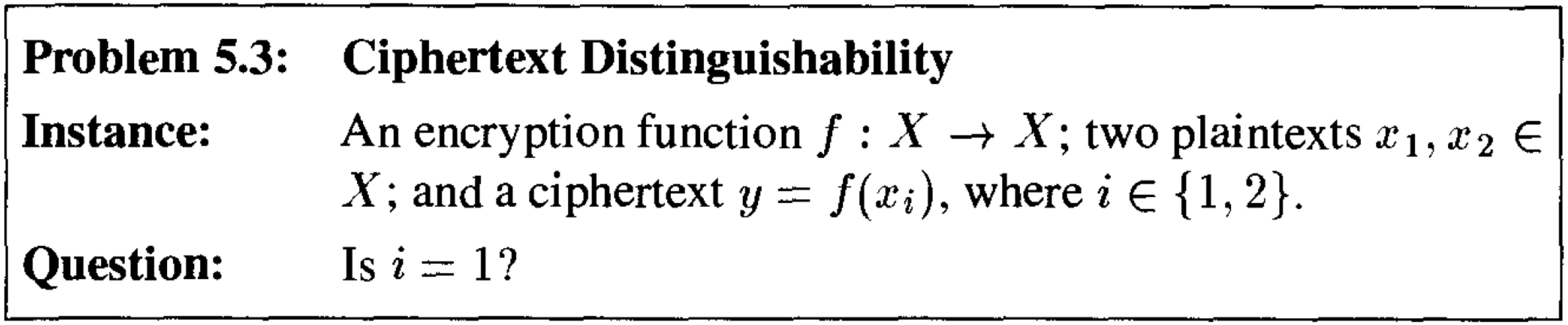
3）最优非对称加密填充（OAEP）

# 密文识别

- 敌手能够以1/2的概率识别两个给定明文对应的密文，或者识别出给定明文的密文和随机串。

# 5.9.2 最优非对称加密填充

- 设计目标：找到一个设计密码体制的方法，这个密码体制允许我们证明不可能在多项式时间内通过检查密文的手段找到任何有关明文的信息。
- 可以证明这个命题等价于攻击者不能区别密文。
- 问题5.3 密文识别



**Problem 5.3:** **Ciphertext Distinguishability**

**Instance:** An encryption function $f : X \to X$; two plaintexts $x_1, x_2 \in X$; and a ciphertext $y = f(x_i)$, where $i \in \{1, 2\}$.

**Question:** Is $i = 1$?

# 公钥加密的安全性定义

- IND-CPA
- IND-CCP
- IND-CCP2

# 语义安全的公钥密码体制

（1）设$m, k$为正整数；设$F$为一族陷门单向置换，且对任意的$f \in F$，有$f : \{0,1\}^k \to \{0,1\}^k$;且设$G : \{0,1\}^k \to \{0,1\}^m$为一个随机谕示器。令$P = \{0,1\}^m$,且$C = \{0,1\}^k \times \{0,1\}^m$,定义$K = \{(f, f^{-1}, G) : f \in F\}$。

（2）加密：对$K = (f, f^{-1}, G)$,随机选取$r \in \{0,1\}^k$,且定义$e_K(x) = (y_1, y_2) = (f(r), G(r) \oplus x)$,

其中$y_1 \in \{0,1\}^k, x, y_2 \in \{0,1\}^m$。

（3）解密：$d_K(y_1, y_2) = G(f^{-1}(y_1)) \oplus y_2$。

函数$f$和$G$为公钥，函数$f^{-1}$为私钥。

We are going to describe a reduction that is more general than the Turing reductions considered previously. We will assume the existence of an algorithm DISTINGUISH that solves the problem of **Ciphertext Distinguishability** for two plaintexts $x_1$ and $x_2$, and then we will modify this algorithm in such a way that we obtain an algorithm to invert $f$. The algorithm DISTINGUISH need not be a "perfect" algorithm; we will only require that it gives the right answer with some probability $1/2 + \epsilon$, where $\epsilon > 0$ (i.e., it is more accurate than a random guess of "1" or "2"). DISTINGUISH is allowed to query the random oracle, and therefore it can compute encryptions of plaintexts. In other words, we are assuming it is a chosen plaintext attack.

1. $G$ is assumed to be a random oracle, so the only way to determine any information about a value $G(r)$ is to call the function $G$ with input $r$.
2. We construct a new algorithm INVERT, by modifying the algorithm DISTINGUISH, which will invert randomly chosen elements $y$ with probability bounded away from 0 (i.e., given a value $y = f(x)$ where $x$ is chosen randomly, the algorithm INVERT will find $x$ with some specified probability).
3. The algorithm INVERT will replace the random oracle by a specific function that we will describe, SIMG, all of whose outputs are random numbers. SIMG is a perfect simulation of a random oracle.

**Algorithm 5.14:** INVERT($y$)

```
external $f$
global $RList, GList, \ell$
procedure SIMG($r$)
  $i \leftarrow 1$
  $found \leftarrow$ false
  while $i \leq \ell$ and not $found$
    do { if $RList[i] = r$
           then $found \leftarrow$ true
           else $i \leftarrow i + 1$
  if $found$
    then return ($GList[i]$)
  if $f(r) = y$
    then { let $j \in \{1, 2\}$ be chosen at random
           $g \leftarrow y_2 \oplus x_j$
    else let $g$ be chosen at random
  $\ell \leftarrow \ell + 1$
  $RList[\ell] \leftarrow r$
  $GList[\ell] \leftarrow g$
  return ($g$)

main
  $y_1 \leftarrow y$
  choose $y_2$ at random
  $\ell \leftarrow 0$
  insert the code for DISTINGUISH($x_1, x_2, (y_1, y_2)$) here
  for $i \leftarrow 1$ to $\ell$
    do { if $f(RList[i]) = y$
           then return ($RList[i]$)
  return ("failure")
```

We now proceed to compute a lower bound on the success probability of the algorithm INVERT. We do this by examining the success probability of DISTINGUISH. We are assuming that the success probability of DISTINGUISH is at least $1/2 + \epsilon$ when it interacts with a random oracle. In the algorithm INVERT, DISTINGUISH interacts with the simulated random oracle, SIMG. Clearly SIMG is completely indistinguishable from a true random oracle for all inputs, except possibly for the input $r = f^{-1}(y)$. However, if $f(r) = y$ and $(y, y_2)$ is a valid encryption of $x_1$ or $x_2$, then it must be the case that $\text{SIMG}(r) = y_2 \oplus x_1$ or $\text{SIMG}(r) = y_2 \oplus x_2$. SIMG is choosing randomly from these two possible alternatives. Therefore, the output it produces is indistinguishable from a true random oracle for the input $r = f^{-1}(y)$, as well. Consequently, the success probability of DISTINGUISH is at least $1/2 + \epsilon$ when it interacts with the simulated random oracle, SIMG.

We now calculate the success probability of DISTINGUISH, conditioned on whether (or not) $f^{-1}(y) \in RList$:

$$\begin{aligned}&\mathbf{Pr}[\textsc{Distinguish}\text{ succeeds}] = \\ &\qquad \mathbf{Pr}[\textsc{Distinguish}\text{ succeeds} \mid f^{-1}(y) \in RList]\,\mathbf{Pr}[f^{-1}(y) \in RList] + \\ &\qquad \mathbf{Pr}[\textsc{Distinguish}\text{ succeeds} \mid f^{-1}(y) \notin RList]\,\mathbf{Pr}[f^{-1}(y) \notin RList].\end{aligned}$$

It is clear that

$$\mathbf{Pr}[\textsc{Distinguish}\text{ succeeds} \mid f^{-1}(y) \notin RList] = 1/2,$$

because there is no way to distinguish an encryption of $x_1$ from an encryption of $x_2$ if the value of $\textsc{SimG}(f^{-1}(y))$ is not determined. Now, using the fact that

$$\mathbf{Pr}[\textsc{Distinguish}\text{ succeeds} \mid f^{-1}(y) \in RList] \leq 1,$$

we obtain the following:

$$\begin{aligned}\frac{1}{2}+\epsilon &\leq \mathbf{Pr}[\textsc{Distinguish}\text{ succeeds}]\\ &\leq \mathbf{Pr}[f^{-1}(y)\in RList]+\frac{1}{2}\mathbf{Pr}[f^{-1}(y)\notin RList]\\ &\leq \mathbf{Pr}[f^{-1}(y)\in RList]+\frac{1}{2}.\end{aligned}$$

Therefore, it follows that

$$\mathbf{Pr}[f^{-1}(y)\in RList]\geq\epsilon.$$

Since

$$\mathbf{Pr}[\textsc{Inverse}\text{ succeeds}]=\mathbf{Pr}[f^{-1}(y)\in RList],$$

it follows that

$$\mathbf{Pr}[\textsc{Inverse}\text{ succeeds}]\geq\epsilon.$$

# 最优的可证明安全的密码体制

（1）参数：设$m,k$为正整数，且$m<k$。令$k_0=k-m$。设$F$为一族陷门单向置换，使得对于所有的$f\in F$，有$f:\{0,1\}^k\to\{0,1\}^k$。设$G:\{0,1\}^{k_0}\to\{0,1\}^m$，且设$H:\{0,1\}^m\to\{0,1\}^{k_0}$为“随机”函数。定义$P=\{0,1\}^m,C=\{0,1\}^m$,且定义$K=\{(f,f^{-1},G,H):f\in F\}$。

（2）加密：对于$K=(f,f^{-1},G,H)$,设$r\in\{0,1\}^{k_0}$随机选择，定义$e_K(x)=f(x\oplus G(r)\|r\oplus H(x\oplus G(r)))$,$x,y_1\in\{0,1\}^m$，$y_2\in\{0,1\}^{k_0}$。

（3）解密：定义$f^{-1}(y)=x_1\|x_2$,然后定义$r=x_2\oplus H(x_1)$且$d_K(y)=G(r)\oplus x_1$。

其中$f,G,H$为公钥，$f^{-1}$为私钥。

# 期中大作业