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

第十六讲 RSA(三)

- 模n的平方根
- Rabin体制
- RSA的语义安全性

  密文可识别

  比特安全性

模n的平方根

假定n是一个奇数，并且$gcd(n,a)=1$。第一个问题是考虑同余方程$y^2 \equiv a \pmod n$具有$y \in \mathbb{Z}_n$的根的个数。

由平方剩余的定义可知，如果n是素数，则同余方程要么有零个解，要么有两个解。

定理5.12 假定p为一个奇素数，e为一个正整数，且$gcd(a,p)=1$。那么同余方程$y^2 \equiv a \pmod{p^e}$当$(\frac{a}{p})=-1$时没有解，当$(\frac{a}{p})=1$时有两个解（模p^e）。

模n平方根

假定n是任意的奇整数，则如下结果是中国剩余定理的基本应用。

定理5.13 假定$n>1$为一个奇数，且有如下分解

$$n=\prod_{i=1}^{l} p_i^{e_i}$$

其中p_i为不同的素数，且e_i为正整数。进一步假定$gcd(a,p)=1$。那么同余方程$y^2\equiv a \pmod n$当$\left(\frac{a}{p_i}\right)=1$对所有的$i\in\{1,\ldots,l\}$成立时有$2^l$个模$n$的解，其他情况下没有解。

假定$x^2\equiv y^2\equiv a \pmod n$，其中$gcd(a,n)=1$。设$z=xy^{-1} \mod n$。于是可得出$z^2\equiv 1 \pmod n$。反过来，如果$z^2\equiv 1 \pmod n$，那么$(xz)^2\equiv x^2 \pmod n$对于任意的$x$成立。

因此，把$a\in\mathbb{Z}_n^*$的某个给定平方根与1的2^l个平方根做出2^l个乘积，就得到a的2^l个平方跟。

5.8 Rabin密码体制

假定模数$n = pq$不能被分解，则*Rabin*密码体制对于选择明文攻击是计算安全的。

*Rabin*密码体制提供了一个可证明安全的密码体制的例子:假设分解整数问题是计算上不可行的，*Rabin* 密码体制是安全的。

密码体制5.2 $Rabin$密码体制

设$n = pq$,其中p和q为素数,且$p \equiv q \equiv 3(\bmod 4)$.

设$P = C = Z_n^*$,且定义$K = \{(n, p, q)\}$.

对$K = (n, p, q)$,定义

$$e_K(x) = x^2 (\bmod n)$$

和

$$d_K(y) = \sqrt{y} (\bmod n)$$

n为公钥,p和q为私钥

*Rabin*密码体制

*Rabin*密码体制的一个缺陷是加密函数 e_K不是一个单射，所以解密不能以一种明显的方式完成。

通常对应某个密文有四个可能的解，一般不能区分四个可能的明文中哪一个是正确的，除非明文中包含足够的冗余信息来排除四个可能值中的三个。

解密*Rabin*密码体制相当于求解余下的同余方程:

$$\begin{cases} z^2 \equiv y \pmod p \\ z^2 \equiv y \pmod q \end{cases}$$

我们可以使用*Euler*准则来判断y是否为一个模p或q的二次剩余。事实上，如果正确地执行，y 是模p和q的二次剩余。

当$p \equiv 3 \pmod 4$时，有一个简单公式来计算模p二次剩余平方根。

如果y是模p的二次剩余，那么y模p的两个平方根为$\pm y^{(p+1)/4} \bmod p$。

同样，y 模q的两个平方根为$\pm y^{(q+1)/4} \bmod q$。然后可以用中国剩余定理来得到模n的个平方根。

为什么*Rabin*密码体制中，限定

$$p \equiv q \equiv 3 \pmod 4 ?$$

对$p \equiv 1 \pmod 4$,还不知道是否存在多项式时间的确定性算法来计算模p二次剩余的平方根(然而已有一个多项式时间的*Las Vegas*算法)。

例5.18 $Rabin$密码体制的加密和解密过程

设$n = 77 = 7 \times 11$,那么加密函数为

$$e_K(x) = x^2 \pmod{77}$$

解密函数为

$$d_K(y) = \sqrt{y} \pmod{77}$$

按照我们的方法，可以得到密文23的可能明文分别为10,32,45,67

*Rabin*密码体制的安全性

讨论*Rabin*密码体制的可证明安全性，其证明使用了一个图灵归约，定义如下*:*

定义5.5　假定G和H为问题。一个从G到H的图灵归约是一个具有如下性质的算法$SloveG$:

1: $SloveG$假定了存在某一算法$SolveH$求解问题H;

定义5.5续

$2: SolveG$可以调用$SolveH$并使用它的任一输出值，但$SolveG$不能对$SolveH$执行的实际运算做任何限定(即$SolveH$是一个黑盒子或预示器);

$3: SolveG$是一个多项式时间算法;

$4: SolveG$正确地求解问题G;

如果存在一个从G到H的图灵归约，我们记为$G \propto_T H$

$Rabin$密码体制的安全性

一个图灵归约$G \propto_T H$并不一定得到一个求解问题G的多项式时间算法。它实际上证明如下的事实：

如果存在一个多项式时间算法求解问题H，那么存在一个多项式时间算法求解问题G。

我们将提供一个图灵归约的例子。

*Rabin*密码体制的安全性

我们将证明，一个解密喻示器*Rabin Decrypt*可以并入到一个分解模数n的*Las Vegas*算法中，至少具有$1/2$的概率

也就是说，可以得到一个归约

$$Factoring \ \propto_T \ Rabin \ Decryption,$$

其中图灵归约本身是一个随机算法。

算法5.12 $Rabin\quad Oracle$

$external\quad Rabin\quad Decrypt$

随机选择一个整数$r \in Z_n^*$

$y \leftarrow r^2 \bmod n$

$x \leftarrow Rabin\quad Decrypt(y)$

$if\quad x \equiv \pm r \pmod n$

$\quad then\quad return("failure")$

$$else\begin{cases} p \leftarrow \gcd(x+r, n) \\ q \leftarrow n/p \\ return("n = p \times q") \end{cases}$$

说明：

1：y是一个有效的密文，且$Rabin\ \ Decrypt(y)$将返回四个可能明文中的一个作为x的值。

2：算法成功的概率为$1/2$；

3：在选择密文攻击下是不安全的。事实上，算法5.12可以用来在选择密文攻击中攻破$Rabin$密码体制。

在选择密文攻击中，喻示器用实际解密算法来代替

- 在前面，我们都假定敌手试图攻破密码体制实际上是试图找出秘密密钥或私钥。
- 如果敌手能做到这点，那么密码体制被完全攻破。
- 敌手可能没有这么大的野心，即使敌手不能找到密钥或私钥，它仍然可以获得比我们所希望的更多信息。
- 如果要确保一个密码体制是“安全的”，我们应该考虑这些敌手所具有的适度的目标。

完全攻破

- 敌手能够找出Bob的秘密密钥或者私钥。因此，它能解密利用给定密钥加密的任意密文

部分攻破

- 敌手能以某一不可忽略的概率解密以前没有见过的密文。或者，敌手能够对于给定的密文，得出明文的一些特定信息。

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。

语义安全的

- 针对RSA型密码体制，我们考虑达到上面某种类型的目的的可能攻击。
- 我们也描述在一定的计算假设成立的情形下，如何构造一个公钥密码体制使得敌手不能（在多项式时间内）识别密文，这样的密码体制称为语义安全的。
- 达到语义安全性是非常困难的，因为我们是针对敌手的非常弱的目的提供保护。

5.9.1 与明文比特相关的部分信息

1：一些密码体制的弱点就是关于明文的部分信息可以通过密文泄露出去。

2：比如RSA密码体制，因为

$\left(\frac{y}{n}\right)=\left(\frac{x}{n}\right)^{b}=\left(\frac{x}{n}\right)$。所以给定密文$y$，无需计算$x$，就可以知道$\left(\frac{x}{n}\right)$。

也就是说，一个RSA加密"泄露"了一些明文的信息。

5.9.1 与明文比特相关的部分信息

我们考虑如下两种情形：

1：给定$y=e_K(x)$,计算$parity(y)$,其中$parity(y)$表示x的二进制表示的最低位数。

2：给定$y=e_K(x)$,计算$half(y)$，其中当$0\le x<n/2$时$half(y)=0$;当$n/2<x\le n-1$时$half(y)=1$

5.9.1 与明文比特相关的部分信息

我们将证明假定RSA加密是安全的，RSA密码体制不会泄露这种类型的信息。

我们将证明RSA解密问题可以图灵归约为计算$half(y)$的问题。

5.9.1 与明文比特相关的部分信息

这意味着如果存在一个多项式时间算法计算$half(y)$，那么存在RSA解密的多项式时间算法。

计算关于明文的特定部分信息，即$half(y)$，不会比解密密文得到整个明文来的容易。

5.9.1 与明文比特相关的部分信息

算法5.13 $Orcle\quad RSA\quad Decryption(n,b,y)$

$external\quad HALF$

$k \leftarrow \lfloor lbn \rfloor$

$for\quad i \leftarrow 0\quad to\quad k$

$$do\quad \begin{cases} h_i \leftarrow Half(n,b,y) \\ y \leftarrow (y \times 2^b) \bmod n \end{cases}$$

$lo \leftarrow 0$

$hi \leftarrow n$

$for\quad i \leftarrow 0\quad to\quad k$

$$do\quad \begin{cases} mid \leftarrow (hi + lo)/2 \\ \quad if\quad h_i = 1 \\ \quad then\quad lo \leftarrow mid \\ \quad else\quad hi \leftarrow mid \end{cases}$$

$return(\lfloor hi \rfloor)$

$$half(y) = parity((y \times e_K(2)) \bmod n) \tag{5.3}$$

$$parity(y) = half((y \times e_K(2^{-1})) \bmod n) \tag{5.4}$$

即计算$parity(y)$和$half(y)$是困难的。