密 码 学

（第九讲）

公开密钥密码（2）

张焕国

武汉大学计算机学院

目　录

目　录

一、ELGamal公钥密码的基本情况

1、基本情况：

①*ELGamal密码是除了RSA密码之外最有代表性的公开密钥密码。*

②*RSA密码建立在大合数分解的困难性之上。*

③*ELGamal密码建立在离散对数的困难性之上。*

一、ELGamal公钥密码的基本情况

2、离散对数问题：

①*设p为素数，则模p的剩余构成有限域：*

$$F_p=\{0,1,2,\ldots,p-1\}$$

F_p 的非零元构成循环群F_p^*

$$F_p^*=\{1,2,\ldots,p-1\}$$

$$=\{\alpha,\ \alpha^2,\ \alpha^3,\ ,\ \alpha^{p-1}\},$$

则称α为F_p^*的生成元或模 p 的本原元。

②*求α的摸幂运算为:*

$$y=\alpha^x \bmod p,\ 1\le x\le p-1,$$

一、ELGamal公钥密码的基本情况

2、离散对数问题：

求对数 X 的运算为

$$x=\log_{\alpha}y，1\leq x\leq p-1$$

由于上述运算是定义在模p有限域上的，所以称为离散对数运算。

③*从x计算y是容易的。可是从y计算x就困难得多，利用目前最好的算法，对于小心选择的p将至少需用O($p^{½}$)次以上的运算，只要p足够大，求解离散对数问题是相当困难的。*

二、ELGamal公钥密码

- 准备：随机地选择一个大素数p，且要求p-1有大素数因子。再选择一个模p的本原元α。将p和α公开。

(1) 密钥生成

- 用户随机地选择一个整数d作为自己的秘密的解密钥，$2 \le d \le p-2$。
- 计算$y=\alpha^d \bmod p$，取y为自己的公开的加密钥。
- 由公开钥y 计算秘密钥d，必须求解离散对数，而这是极困难的。

二、ELGamal公钥密码

(2) *加密*

- *将明文消息M（$0 \le M \le p-1$）加密成密文的过程如下：*

①*随机地选取一个整数k，$2 \le k \le p-2$。*

②*计算：* $U = y^k \bmod p$；

$C_1 = \alpha^k \bmod p$；

$C_2 = UM \bmod p$；

③*取 $C =（C_1，C_2）$作为的密文。*

二、ELGamal公钥密码

(3) *解密*

- *将密文（C_1，C_2）解密的过程如下：*

①*计算*$V = C_1^{\,d} \bmod p$；

②*计算*$M = C_2 V^{-1} \bmod p$。

二、ELGamal公钥密码

- 解密的可还原性可证明如下：

$$C_2 V^{-1} \bmod p = (UM)V^{-1} \bmod p$$
$$= UM\ (C_1{}^{d})^{-1} \bmod p$$
$$= UM\ ((\alpha^{k})^{d})^{-1} \bmod p$$
$$= UM\ ((\alpha^{d})^{k})^{-1} \bmod p$$
$$= UM\ ((y)^{k})^{-1} \bmod p$$
$$= UM\ (U)^{-1} \bmod p$$
$$= M \bmod p$$

二、ELGamal公钥密码

(4) *安全性*

- *由于ELGamal密码的安全性建立在GF（p）离散对数的困难性之上，而目前尚无求解GF（p）离散对数的有效算法，所以在p足够大时ELGamal密码是安全的。*
- *为了安全p应为150位以上的十进制数，而且p-1应有大素因子。*
- *为了安全加密和签名所使用的k必须是一次性的。*
- *d和k都不能太小。*

二、ELGamal公钥密码

(4) *安全性*

- 如果 k不是一次性的，时间长了就可能被攻击着获得。又因y是公开密钥，攻击者自然知道。于是攻击者就可以根据$U=y^k \bmod p$计算出U，进而利用Euclid算法求出U^{-1}。又因为攻击者可以获得密文C_2，于是可根据式$C_2=UM \bmod p$通过计算$U^{-1}C_2$得到明文M。
- 设用同一个k加密两个不同的明文M和M'，相应的密文为（C_1，C_2）和（C_1'，C_2'）。因为$C_2/C_2'= M/M'$，如果攻击者知道M，则很容易求出M'。

二、ELGamal公钥密码

(5) *ELGamal密码的应用*

- *由于ELGamal密码的安全性得到世界公认，所以得到广泛的应用。著名的美国数字签名标准DSS，采用了ELGamal密码的一种变形。*
- *为了适应不同的应用，人们在应用中总结出18种不同的ELGamal密码的变形。*

二、ELGamal公钥密码

(5) *ELGamal密码的应用*

①加解密速度快

由于实际应用时ELGamal密码运算的素数p比RSA要小，所以ELGamal密码的加解密速度比RSA稍快。

②随机数源

由ELGamal密码的解密钥d和随机数k都应是高质量的随机数。因此，应用ELGamal密码需要一个好的随机数源，也就是说能够快速地产生高质量的随机数。

③大素数的选择

为了ELGamal密码的安全，p应为150位（十进制数）以上的大素数，而且p-1应有大素因子。

三、椭圆曲线密码

1、*椭圆曲线密码的一般情况*

- *受ELGamal密码启发，在其它离散对数问题难解的群中，同样可以构成ELGamal密码。于是人们开始寻找其它离散问题难解的群。*
- *研究发现，有限域GF（p）上的椭圆曲线的解点构成交换群，而且离散对数问题是难解的。于是可在此群上建立ELGamal密码，并称为椭圆曲线密码。*

三、椭圆曲线密码

1、*椭圆曲线密码的一般情况*

- *椭圆曲线密码已成为除RSA密码之外呼声最高的公钥密码之一。*
- *它密钥短、签名短，软件实现规模小、硬件实现电路省电。*
- *普遍认为，160位长的椭圆曲线密码的安全性相当于1024位的RSA密码，而且运算速度也较快。*

三、椭圆曲线密码

1、*椭圆曲线密码的一般情况*

- *一些国际标准化组织已把椭圆曲线密码作为新的信息安全标准。如，IEEE P1363/D4，ANSI F9.62，ANSI F9.63等标准，分别规范了椭圆曲线密码在Internet协议安全、电子商务、Web服务器、空间通信、移动通信、智能卡等方面的应用。*

三、椭圆曲线密码

2、*椭圆曲线*

设p是大于3的素数，且$4a^3+27b^2 \neq 0 \bmod p$，称

$$y^2 = x^3 + ax + b \text{，} a, b \in GF(p)$$

为GF（p）上的*椭圆曲线*。

由椭圆曲线可得到一个同余方程：

$$y^2 = x^3 + ax + b \quad \bmod p$$

其解为一个二元组$\langle x, y \rangle$，$x, y \in GF(p)$，将此二元组描画到椭圆曲线上便为一个点，于是又称其为*解点*。

三、椭圆曲线密码

2、*椭圆曲线*

为了利用解点构成交换群，需要引进一个0元素，并定义如下的加法运算：

①*定义单位元*

引进一个无穷点0（∞，∞），简记为0，作为0元素。

0（∞，∞）＋0（∞，∞）＝0＋0＝0 。

并定义对于所有的解点P（x ，y），

P（x ，y）+0＝0+ P（x ，y）＝P（x ，y）。

三、椭圆曲线密码

2、*椭圆曲线*

②*定义逆元素*

设P（x_1 ，y_1）和Q（x_2 ，y_2）是解点，如果 $x_1=x_2$ 且$y_1=-y_2$，则

$$P(x_1, y_1)+Q(x_2, y_2)=0 。$$

这说明*任何解点R（x，y）的逆就是*

R（x，-y）。

注意：规定无穷远点的逆就是其自己。

$$O(\infty, \infty)=-O(\infty, \infty)$$

三、椭圆曲线密码

2、*椭圆曲线*

③*定义加法*

- 设$P(x_1, y_1) \neq Q(x_2, y_2)$，且P和Q不互逆，则 $P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$。其中

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1, \\ \lambda = (y_2 - y_1)/(x_2 - x_1)。\end{cases}$$

三、椭圆曲线密码

2、*椭圆曲线*

③*定义加法*

- 当P $(x_1, y_1) = Q(x_2, y_2)$时

P $(x_1, y_1) + Q(x_2, y_2) = 2P(x_1, y_1) = R(x_3, y_3)$。

其中

$$\begin{cases} x_3 = \lambda^2 - 2x_1, \\ y_3 = \lambda(x_1 - x_3) - y_1, \\ \lambda = (3x_1^2 + a) / (2y_1)。 \end{cases}$$

三、椭圆曲线密码

2、*椭圆曲线*

- *作集合E={全体解点，无穷点0 }。*
- *可以验证，如上定义的集合E和加法运算构成加法交换群。*
- *复 习：群的定义*

♣ G是一个非空集，定义了一种运算，且运算是自封闭的；

♣ 运算满足结合律；

♣ G中有单位元；

♣ G中的元素都有逆元；

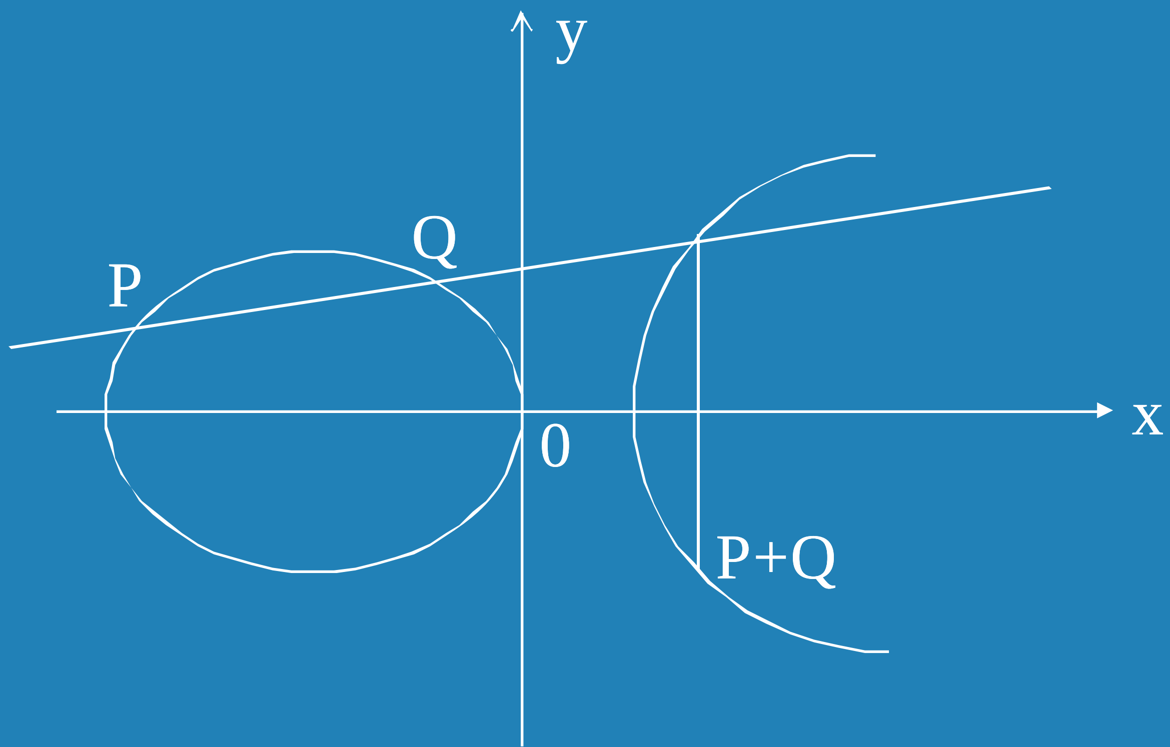
三、椭圆曲线密码

3、*椭圆曲线解点加法运算的几何意义：*

设P（x_1，y_1）和Q（x_2，y_2）是椭圆曲线的两个点，则连接P（x_1，y_1）和Q（x_2，y_2）的直线与椭圆曲线的另一交点关于横轴的对称点即为P（x_1，y_1）+Q（x_2，y_2）点。

三、椭圆曲线密码

3、*椭圆曲线解点加法运算的几何意义：*



三、椭圆曲线密码

4、*举例*：

- 取p=11，椭圆曲线$y^2=x^3+x+6$。由于p较小，使GF(p)也较小，故可以利用穷举的方法根据$y^2=x^3+x+6 \bmod 11$求出所有解点。
- *复习：平方剩余*

设p为素数，如果存在一个正整数x，使得

$$x^2=a \bmod p,$$

则称 a是模p的平方剩余。

三、椭圆曲线密码

x	$x^3+x+6 \bmod 11$	是否模11平方剩余	y
0	6	No	
1	8	No	
2	5	Yes	4,7
3	3	Yes	5,6
4	8	No	
5	4	Yes	2,9
6	8	No	
7	4	Yes	2,9
8	9	Yes	3,8
9	7	No	
10	4	Yes	2,9

三、椭圆曲线密码

- *根据表可知全部解点集为：*

(2，4),(2，7),(3，5),(3，6),(5，2),(5，9),(7，2),(7，9),(8，3),(8，8),(10，2),(10，9)。

再加上无穷远点0，共13的点构成一个加法交换群。

- *由于群的元素个数为13，而13为素数，所以此群是循环群，而且任何一个非0元素都是生成元。*

三、椭圆曲线密码

- 由于是加法群，n 个元素 G 相加，$G+G+...+G = nG$。我们取 $G=(2, 7)$ 为生成元，具体计算加法表如下：

  $2G=(2, 7)+(2, 7)=(5, 2)$

- 因为 $\lambda=(3\times2^2+1)(2\times7)^{-1} \bmod 11 =2\times3^{-1} \bmod 11=2\times4 \bmod 11=8$。于是，$x_3=8^2-2\times2 \bmod 11=5$，$y_3=8(2-5)-7 \bmod 11=2$。

三、椭圆曲线密码

G ＝ (2, 7) ， 2G ＝ (5, 2) ，
3G ＝ (8, 3) ， 4G ＝ (10, 2) ，
5G ＝ (3, 6) ， 6G ＝ (7, 9) ，
7G ＝ (7, 2) ， 8G ＝ (3, 5) ，
9G ＝ (10, 9) ，10G ＝ (8, 8) ，
11G ＝ (5, 9) ， 12G ＝ (2, 4) ，
13G ＝0 (∞, ∞) 。

三、椭圆曲线密码

- 除了GF(p)上的椭圆曲线，外还有定义在$GF(2^m)$上的椭圆曲线。这两种椭圆曲线都可以构成安全的椭圆曲线密码。
- 在上例中，由于p较小，使GF(p)也较小，故可以利用穷举的方法求出所有解点。但是，对于一般情况要确切计算椭圆曲线解点数N的准确值比较困难。
- N满足以下不等式

$$P+1-2P^{1/2} \leq N \leq P+1+2P^{1/2}$$ 。

三、椭圆曲线密码

5、*椭圆曲线密码*

ELGamal密码建立在有限域GF（p）的乘法群的离散对数问题的困难性之上。而椭圆曲线密码建立在椭圆曲线群的离散对数问题的困难性之上。两者的主要区别是其离散对数问题所依赖的群不同。因此两者有许多相似之处。

三、椭圆曲线密码

5、*椭圆曲线密码*

① *椭圆曲线群上的离散对数问题*

在上例中椭圆曲线上的解点所构成的交换群恰好是循环群，但是一般并不一定。于是我们希望从中找出一个循环子群E_1。可以证明当循环子群E_1的阶n是足够大的素数时，这个循环子群中的离散对数问题是困难的。

三、椭圆曲线密码

5、*椭圆曲线密码*

① *椭圆曲线群上的离散对数问题*

设P和Q是椭圆曲线上的两个解点，t为一正整数，且1≤t<n。对于给定的P和t，计算tP＝Q是容易的。但若已知P和Q点，要计算出t则是极困难的。这便是椭圆曲线群上的离散对数问题，简记为*ECDLP(Elliptic Curve Discrete Logarithm Problem)*。

三、椭圆曲线密码

5、椭圆曲线密码

① 椭圆曲线群上的离散对数问题

*除了几类特殊的椭圆曲线外，对于一般ECDLP目前尚没有找到有效的求解方法。于是可以在这个循环子群E_1中建立任何基于离散对数困难性的密码，并称这个密码为**椭圆曲线密码**。*

三、椭圆曲线密码

②椭圆曲线密码

$$T=<p,a,b,G,n,h>$$

- p为大于3素数，p确定了有限域GF（p）；
- 元素a,b∈GF(p),a和b确定了椭圆曲线；
- G为循环子群E_1的生成元点，n为素数且为生成元G的阶，G和n确定了循环子群E_1；
- h=|E|/n，并称为余因子，h将交换群E和循环子群联系起来。

三、椭圆曲线密码

②*椭圆曲线密码*

密钥：

- *用户的私钥定义为一个随机数d，*

  $d \in \{1,2,\cdots,n-1\}$。

- *用户的公开钥定义为Q点，*

  $Q=dG$ 。

三、椭圆曲线密码

②*椭圆曲线密码*

- *设d为用户私钥，Q为公钥，将Q存入PKDB。*
- *设要加密的明文数据为M，将M划分为一些较小的数据块，* $M=[m_1, m_2, \cdots, m_t]$，*其中* $0 \le m_i < n$ 。

三、椭圆曲线密码

②*椭圆曲线密码*

加密过程：*A把M加密发给B*

(1)A查**PKDB**，查到B的公开密钥Q_B。

(2)A选择一个随机数k，且$k\in\{1,2,\cdots,n-1\}$。

(3)A计算点X_1（x_1，y_1）$=kG$。

(4)A计算点X_2（x_2，y_2）$=kQ_B$，如果分量$x_2=0$，则转(2)。

(5)A计算密文 $C = m_i\ x_2 \mod n$。

(6)A发送加密数据（X_1，C）给B。

三、椭圆曲线密码

②*椭圆曲线密码*

- 解密过程：
- *用户B用自己的私钥d_B求出点X_2：*

$$d_B X_1 = d_B\ (kG)$$
$$= k(d_B\ G)$$
$$= k\ Q_B$$
$$= X_2\ (x_2\ ,\ y_2)$$

- 对C解密，得到明文$m_i = C\ x_2^{-1}\ \bmod n$。

三、椭圆曲线密码

②椭圆曲线密码

- 椭圆曲线密码的实现
- *由于椭圆曲线密码所依据的数学基础比较复杂，从而使得其具体实现也比较困难。*

难点：

- *安全椭圆曲线的产生；*
- *倍点运算。*

四、公钥密码的理论模型

1、单向函数

设函数 $y=f(x)$，如果满足以下两个条件，则称为单向函数：

- *如果对于给定的x，要计算出y很容易；*
- *而对于给定的y，要计算出x很难。*

2、单向函数的应用

- *安全HASH函数*
- *操作系统口令*

四、公钥密码的理论模型

3、利用单向函数构造密码

- *用正变换作加密，加密效率高；*
- *用逆变换作解密，安全，敌手不可破译；*
- *但是加密后不能还原。*

四、公钥密码的理论模型

4、单向陷门函数

设函数 $y=f(x)$，且 f 具有陷门，如果满足以下两个条件，则称为单向陷门函数：

- *如果对于给定的x，要计算出y很容易；*
- *而对于给定的 y，如果不掌握陷门要计算出 x很难，而如果掌握陷门要计算出x就很容易。*

四、公钥密码的理论模型

5、单向陷门函数的应用

- *用正变换作加密，加密效率高；*
- *用逆变换作解密，安全；*
- *把陷门信息作为密钥，且只分配给合法用户。确保合法用户能够方便地解密，而非法用户不能破译。*

四、公钥密码的理论模型

6、单向函数的研究现状

- 理论上：不能证明单向函数一定存在；
- 实际上：只要函数的单向性足够工程应用就行；
- 实际上已找到的单向性足够的函数有：

①合数的因子分解问题

大素数的乘积容易计算（$p \times q \Rightarrow n$），而大合数的因子分解困难($n \Rightarrow p \times q$)。

②有限域上的离散对数问题

有限域上大素数的幂乘容易计算（$a^b \Rightarrow c$），而对数计算困难($\log_a c \Rightarrow b$)。

习题

① 证明椭圆曲线密码的可逆性。

② 为令$p=5$,求出椭圆曲线$y^2=x^3+4x+2$的全部解点

③ 以教材例5-5为例，分别以$G=(2,7)$和$G=(5,2)$构造椭圆曲线密码，并设$m=3$，分别进行加密和解密。

谢 谢！