密码学

第十讲　公钥密码（2）

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室

内容简介

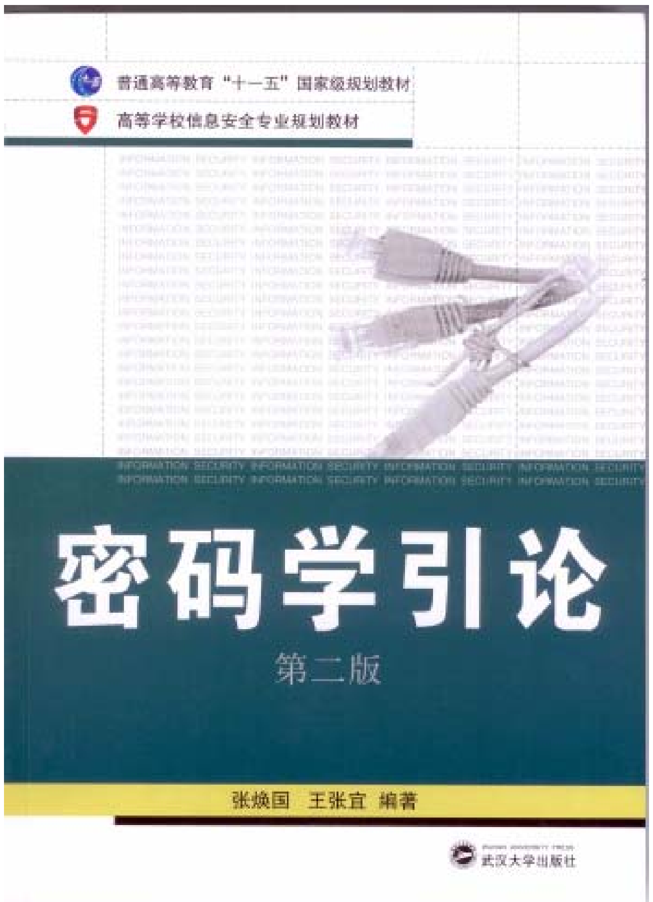
第一讲 信息安全概论
第二讲 密码学的基本概念
第三讲 数据加密标准（**DES**）
第四讲 高级数据加密标准（**AES**）
第五讲 中国商用密码（**SMS4**）
第六讲 分组密码的应用技术
第七讲 序列密码
第八讲 复习
第九讲 公钥密码（**1**）

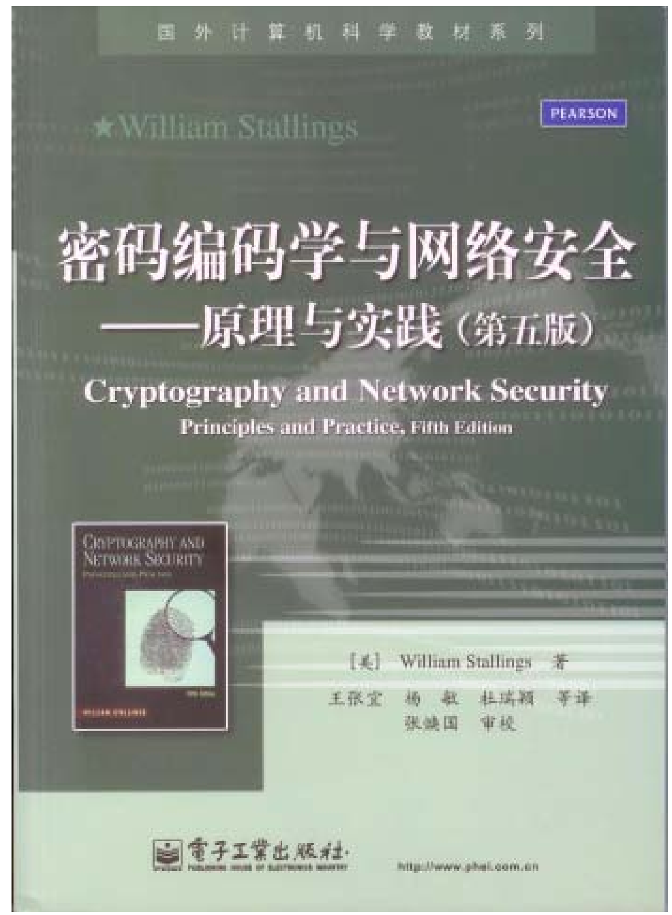
内容简介

第十讲 公钥密码（2）
第十一讲 数字签名（1）
第十二讲 数字签名（2）
第十三讲 HASH函数
第十四讲 认证
第十五讲 密码协议
第十六讲 密钥管理（1）
第十七讲 密钥管理（2）
第十八讲 复习

教材与主要参考书

教材 参考书





一、离散对数问题

1、基本情况:

- 公钥密码的理论模型是单向陷门函数

① 用正变换作加密，加密效率高；

② 用逆变换作解密，安全；

③ 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。

- 成功实例

① **RSA**密码建立在大合数分解的困难性之上。

② **ElGamal**密码建立在离散对数的困难性之上。

③ **ECC**密码建立在椭圆曲线离散对数的困难性之上。

一、离散对数问题

2、离散对数问题：

①设p为素数，则模p的剩余构成有限域：

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

F_p的非零元素构成乘法循环群F_p^*

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

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：

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

一、离散对数问题

2、离散对数问题

③求对数 x 的运算为

$$x=\log_{a} y,\ 1\leqslant x\leqslant p-1$$

由于上述运算是定义在有限域F_p 上的，所以称为离散对数运算。

- 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 公开作为密码的基础参数。

(1) 密钥生成

- 用户随机地选择一个整数d作为自己保密的解密钥，$2 \leqslant d \leqslant p-2$ 。
- 用户计算$y = \alpha^d \bmod p$，并取y为自己公开的加密钥。
- 显然，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、EIGamal公钥密码

(2) 加密

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

①随机地选取一个整数k，$2 \leqslant k \leqslant p-2$。

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。

武漢大學

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

$$M = C_2 V^{-1} \bmod p$$

获得明文。

二、ElGamal公钥密码

- 解密的可还原性证明如下：

$$
\begin{aligned}
C_2 V^{-1} \bmod p &= (UM)V^{-1} \bmod p \\
&= UM\left(C_1{}^{d}\right)^{-1} \bmod p \\
&= UM\left(\left(\alpha^{k}\right)^{d}\right)^{-1} \bmod p \\
&= UM\left(\left(\alpha^{d}\right)^{k}\right)^{-1} \bmod p \\
&= UM\left((y)^{k}\right)^{-1} \bmod p \\
&= UM(U)^{-1} \bmod p \\
&= M \bmod p
\end{aligned}
$$

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。
- *d*和*k*都不能太小。
- 为了安全加密和签名所使用的*k*必须是一次性的。

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。
  - 电子邮件标准S/MIME采用了ElGamal密码。
  - 俄罗斯的数字签名标准也是ElGamal密码的一种变形，而且数据规模选得更大。
- 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

⑸ 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、椭圆曲线离散对数问题

1、素域上的椭圆曲线

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

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

为GF（p）上的椭圆曲线。

- 由椭圆曲线可得到一个同余方程：

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

- 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，故称其为一个解点。

三、椭圆曲线离散对数问题

2、素域上的椭圆曲线

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O（∞，∞），简记为O，作为0元素。

$O(\infty, \infty) + O(\infty, \infty) = 0 + 0 = 0$。

并定义对于所有的解点P（x，y），

$P(x, y) + O = O + P(x, y) = P(x, y)$。

三、椭圆曲线离散对数问题

2、素域上的椭圆曲线

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）＝O 。

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（∞，∞）＝-O（∞，∞）

三、椭圆曲线离散对数问题

2、素域上的椭圆曲线

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

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

三、椭圆曲线离散对数问题

2、素域上的椭圆曲线

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

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

。

三、椭圆曲线离散对数问题

2、素域上的椭圆曲线

- 作集合E={全体解点，无穷点O}。
- 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G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、椭圆曲线离散对数问题

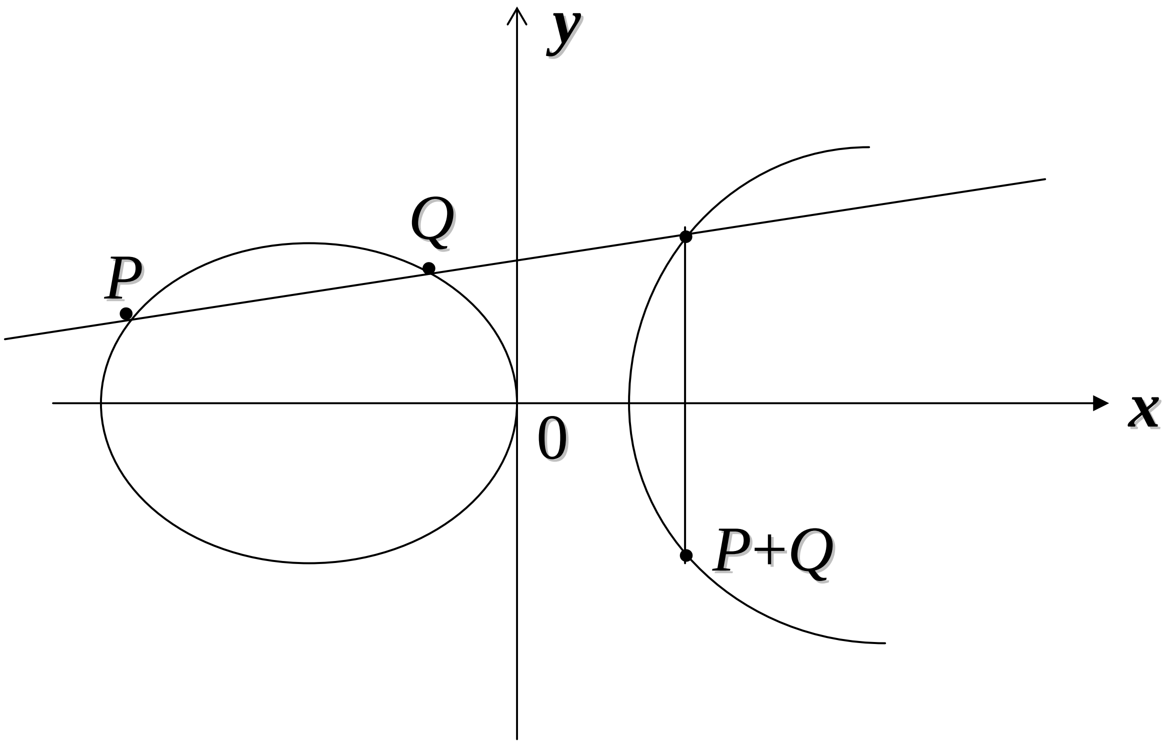
3、椭圆曲线解点加法运算的几何意义

设P（x_1 ，y_1）和Q（x_2 ，y_2）是椭圆曲线上的两个点，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、椭圆曲线离散对数问题

3、椭圆曲线解点加法运算的几何意义：



三、椭圆曲线离散对数问题

4、例10-1

- 求出椭圆曲线 $y^2=x^3+x+6 \bmod 11$ 的解点。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y，使得

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

则称 a是模p的平方剩余。

三、椭圆曲线离散对数问题

x	$x^3+x+6 \bmod 11$	是否是模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

武漢大學

三、椭圆曲线离散对数问题

- 根据上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O，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、椭圆曲线离散对数问题

- 由于是加法群，n个元素G相加表示为：

$$G+G+\ldots+G = nG ,$$

并称为倍点运算。

- 我们取G =（2，7）为生成元，2倍点计算如下：

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

- 因为 $\lambda = (3\times 2^2+1)(2\times 7)^{-1} \bmod 11 = 2\times 3^{-1} \bmod 11 = 2\times 4 \bmod 11 = 8$。于是，

$$x_3 = 8^2-2\times 2 \bmod 11 = 5 ,$$

$$y_3 = 8(2-5)-7 \bmod 11 = 2 。$$

武漢大學

三、椭圆曲线离散对数问题

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 ＝O（ ∞， ∞ ）	

- 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

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

武漢大學

三、椭圆曲线离散对数问题

5、 GF(2^m)上的椭圆曲线

- 除了GF(p)上的椭圆曲线，还有定义在GF(2^m)上的圆曲线。
- 基于这两种椭圆曲线都可以设计出安全的椭圆曲线密码。

三、椭圆曲线离散对数问题

6、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、椭圆曲线离散对数问题

6、椭圆曲线群上的离散对数问题

- 设P是椭圆曲线上的一个解点，t 为一正整数，且$1\leqslant t<n$。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)。
- 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。因子分解和DLP问题都有亚指数求解算法，而ECDLP尚没有发现亚指数求解算法。
- 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。

四、椭圆曲线公钥密码

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。
- 我国商用密码采用了椭圆曲线密码，并具体颁布了椭圆曲线密码标准算法SM2。

四、椭圆曲线公钥密码

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，软件实现规模小、硬件实现节省电路。
- 由于椭圆曲线离散对数问题尚没有发现亚指数算法，所以普遍认为，椭圆曲线密码比RSA和ElGamal密码更安全。
  - 160位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。

武漢大學

四、椭圆曲线公钥密码

1、椭圆曲线密码概况

- 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。
- 基于GF（p）和GF(2^m)上的椭圆曲线，都可以构成安全的椭圆曲线密码。

四、椭圆曲线公钥密码

2、GF(p)上椭圆曲线密码基础参数

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

- p为大于3素数，p 确定了有限域GF（p）；
- 元素$a, b \in GF(p)$, a和b确定了椭圆曲线：

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

- 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E_1联系起来。

四、椭圆曲线公钥密码

3、 GF(p)上椭圆曲线密码的密钥

- 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，

$$Q=dG 。$$

- 由公开钥Q求私钥d是求解椭圆曲线离散对数问题，当p足够大时，这是困难的。

四、椭圆曲线公钥密码

4、 GF(p)上椭圆曲线密码算法

- 设d为用户私钥，Q为用户公钥。
- 设明文数据为M，$0 \leqslant M \leqslant n-1$ 。
- 加密过程：

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

② 计算点X_1（x_1 ，y_1）$= kG$ 。

③ 计算点X_2（x_2 ，y_2）$=kQ$，如果分量$x_2=0$，则转①。

④ 计算密文 $C = Mx_2 \bmod n$ 。

⑤ 以（X_1，C）为最终的密文数据。

武汉大学

四、椭圆曲线公钥密码

4、 GF(p)上椭圆曲线密码算法

- 解密过程：

① 用私钥d求出点X_2：

$$
\begin{aligned}
dX_1 &= d\,(kG) \\
&= k(dG) \\
&= k\,Q \\
&= X_2\,(x_2,\ y_2)
\end{aligned}
$$

② 对C 解密：利用x_2计算得到明文

$$M = C\,x_2^{-1} \bmod n\text{。}$$

四、椭圆曲线公钥密码

5、 GF(p)上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，从而使得其工程实现也比较困难。
- 虽然目前椭圆曲线密码的实现技术已经成熟，但仍有些难度问题值得研究和改进。
- 难点：

①安全椭圆曲线的产生；

- 美国NIST公布了15条曲线
- 我们应对取进行验证
- 这之外还有好曲线吗？如何产生？

②倍点运算。

四、椭圆曲线公钥密码

5、 GF(*p*)上椭圆曲线密码的实现

- 我们在椭圆曲线产生方面的研究

①**Koblitz**椭圆曲线的产生；

- 提出一种**Koblitz**椭圆曲线的演化产生算法
- 在**PC**机上完成了**GF**(2^{2000})以下的曲线产生
- 得到一大批安全曲线，其基域范围和曲线规模，都超过美国**NIST**的公开报道

②素域上的椭圆曲线的产生；

- 在**PC**机上实际产生出一大批安全椭圆曲线
- 基域范围和曲线规模超过美国**NIST**的公开报道

武漢大學

五、中国商用椭圆曲线公钥密码SM2

1、 推荐使用256位素域GF(p)上的椭圆曲线：

$$y^2 = x^3 + ax + b$$

曲线参数：

p=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF
a=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC
b=28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93
n=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123
Gx=32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7
Gy=BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

2、密钥：

- 私钥随机数d，$d \in [1, n\text{-}1]$
- 公钥$P=dG$

五、中国商用椭圆曲线公钥密码SM2

3、加密算法：

① 产生随机数k，$1 \leqslant k \leqslant n-1$；

② 计算椭圆曲线点$C_1 = kG = (x_1, y_1)$；

③ 计算椭圆曲线点$kP=(x_2, y_2)$；

④ 计算$t = \mathrm{KDF}(x_2 \parallel y_2, klen)$，若$t$为全0比特串，则返回① ；

⑤ 计算$C_2 = M \oplus t$；

⑥ 计算$C_3 = \mathrm{Hash}(x_2 \parallel M \parallel y_2)$；

⑦ 输出密文$C = C_1 \parallel C_2 \parallel C_3$。

说明：KDF(Z , *klen*)是密钥派生函数，它利用Hash函数从数据Z产生出长度为*klen*的密钥数据。

五、中国商用椭圆曲线公钥密码SM2

4、解密算法：

① 计算$dC_1 = (x_2, y_2)$；

② 计算$t = \mathrm{KDF}(x_2 \parallel y_2, klen)$，若$t$为全0比特串，则报错并退出；

③ 计算$M' = C_2 \oplus t$；

④ 输出明文M'。

武漢大學

五、中国商用椭圆曲线公钥密码SM2

5、解密正确性：

- 证明：$dC_1 = d(kG) = k(dG) = kP = (x_2, y_2)$；

  如果(x_2, y_2)是正确的，则$t = \mathrm{KDF}(x_2 \parallel y_2, klen)$也将是正确的。

  又因为$C_2 = M \oplus t$，所以$M' = C_2 \oplus t$。

- 验证：根据解密得到的x_2、y_2和M'重新计算C_3，并于接收到的C_3比较，若相等则说明密文和解密正确，否则说明密文或解密不正确。

6、应用

- 我国二代居民身份证采用了SM2椭圆曲线密码。
- 我国的许多商用系统采用了SM2椭圆曲线密码。

武漢大學

五、中国商用椭圆曲线公钥密码SM2

6、比较：

- 传统ECC：
  - 计算点X_2（x_2，y_2）$=kQ$。
  - 计算密文 $C = Mx_2 \bmod n$ 。
  - 最终密文是$< X_1, C >$
- SM2：
  - 计算$t = \mathrm{KDF}(x_2 \parallel y_2, klen)$；
  - 计算$C_2 = M \oplus t$;
  - 最终密文是$< C_1, C_2, C_3 >$
- 比较
  - 传统ECC直接用x_2加密，加密是乘法；SM2对（x_2，y_2）处理后产生t ,用t加密，加密是摸2加。t与（x_2，y_2）相关，更安全。
  - SM2增加了利用C_3的验证，进一步确保密文和解密的正确性。
  - SM2的密文数据扩展较大。

作 业 题

1、p165第11题。

2、p165第15题：

以例5-6为例，分别以G=(2,7)为生成元点构造一个椭圆曲线密码，并设明文M=3，进行加密和解密计算。

谢　谢！