

密码学

第十一讲 中国商用公钥密码 SM2加密算法

王后珍

武汉大学国家网络安全学院

空天信息安全与可信计算教育部重点实验室





目录

- 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与分组密码应用技术
- 第六讲 序列密码基础
- 第七讲 祖冲之密码
- 第八讲 中国商用密码HASH函数SM3
- 第九讲 复习





目录

第十讲 公钥密码基础

第十一讲 中国商用公钥密码SM2加密算法

第十二讲 数字签名基础

第十三讲 中国商用公钥密码SM2签名算法

第十四讲 密码协议

第十五讲 认证

第十六讲 密钥管理：对称密码密钥管理

第十七讲 密钥管理：公钥密码密钥管理

第十八讲 复习

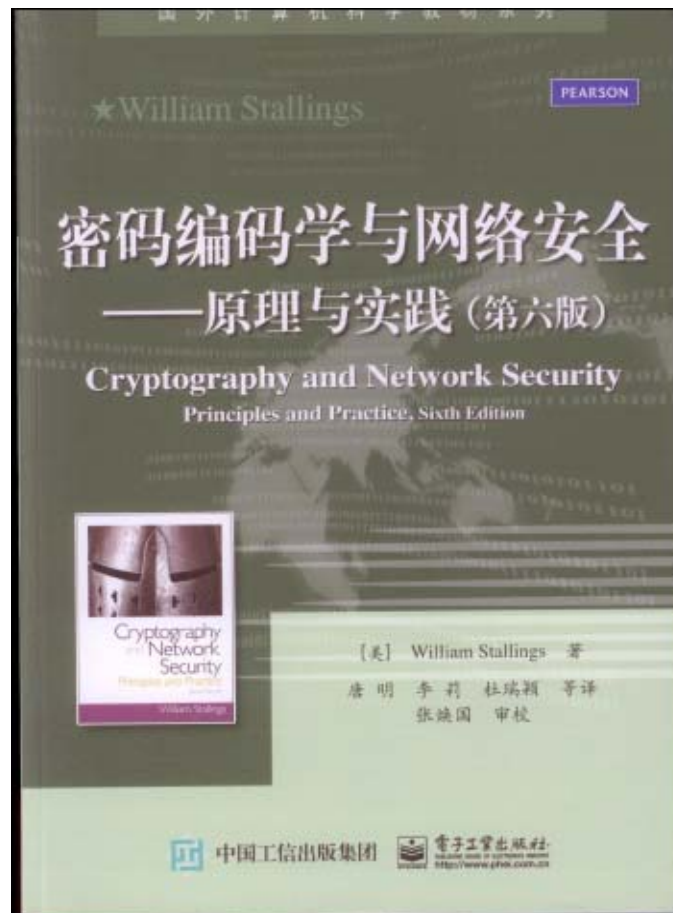


教材与主要参考书

教材



参考书



武汉大学



本讲内容

- 一、椭圆曲线
- 二、椭圆曲线离散对数问题
- 三、椭圆曲线公钥密码
- 四、中国商用椭圆曲线公钥密码SM2





回顾公钥密码的基本思想

1、传统密码的优缺点：

①优点

- 理论与实践都很成熟。
- 安全容易把握。
- 加解密速度快。

②缺点

- 收发双方持有相同密钥， $K_e = K_d$ ，密钥分配困难，网络环境更突出。
- 不能方便地实现数字签名，商业等应用不方便。





回顾公钥密码的基本思想

2、公开密钥密码的基本思想：

- ①将密钥 K 一分为二： K_e 和 K_d 。 K_e 专门加密， K_d 专门解密， $K_e \neq K_d$ 。
 - ②由 K_e 不能计算出 K_d ，于是可将 K_e 公开，使密钥 K_e 分配简单。
 - ③由于 $K_e \neq K_d$ 且由 K_e 不能计算出 K_d ，所以 K_d 便成为用户的指纹，于是可方便地实现数字签名。
- 称上述密码为公开密钥密码，简称为公钥密码。





回顾公钥密码的基本思想

3、公开密钥密码的基本条件：

① E 和 D 互逆； _____ 保密条件

$$D(E(M)) = M$$

② $K_e \neq K_d$ 且由 K_e 不能计算出 K_d ； _____ 安全条件

③ E 和 D 都高效； _____ 实用条件

④ $E(D(M)) = M$ _____ 保真条件

● 如果满足① ② ③可用于保密，如果满足② ③ ④可用于保真，如果4个条件都满足，可同时用于保密和保真。

● 注意：条件④是保真的一个充分条件，不是必要条件。





回顾公钥密码的基本思想

4、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：

- ① 如果对于给定的 x ，要计算出 $y=f(x)$ 很容易；
- ② 而对于给定的 y ，要计算出 $x=f^{-1}(y)$ 很难。

(2)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；
- 但是合法收信者也无法解密。





回顾公钥密码的基本思想

(3) 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：

- ① 如果对于给定的 x ，要计算出 $y=f(x)$ 很容易；
- ② 而对于给定的 y ，如果不掌握陷门要计算出 $x=f^{-1}(y)$ 很难，而如果掌握陷门要计算出 $x=f^{-1}(y)$ 就很容易。

(4) 利用单向陷门函数构造密码

- 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。





回顾公钥密码的基本思想

(5)单向函数的研究现状

- 理论上：尚不能证明单向函数一定存在；
- 实际上：密码学认为只要函数单向性足够应用就行了；
- 已找到一些单向性足够的函数：

①大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（ $\log_a c \Rightarrow b$ ）。

③椭圆曲线离散对数问题

设 d 是正整数， G 是解点群的基点，计算 $dG=Q$ 是容易的，而由 Q 求出 d 是困难的。





一、椭圆曲线

人们对椭圆曲线的研究已有100多年的历史

1、素域上的椭圆曲线

- 设 p 是大于3的素数，且 $4a^3+27b^2 \not\equiv 0 \pmod{p}$ ，称

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

为 $\text{GF}(p)$ 上的椭圆曲线。

- 由椭圆曲线可得到一个同余方程：

$$y^2 = x^3 + ax + b \pmod{p}$$

- 其解为一个二元组 $\langle x, y \rangle$ ， $x, y \in \text{GF}(p)$ ，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。





一、椭圆曲线

1、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 O

引进一个无穷点 $O(\infty, \infty)$ ，简记为 O ，作为0元素。

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

并定义对于所有的解点 $P(x, y)$ ，

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





一、椭圆曲线

1、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。

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





一、椭圆曲线

1、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

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





一、椭圆曲线

1、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

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





一、椭圆曲线

1、素域上的椭圆曲线

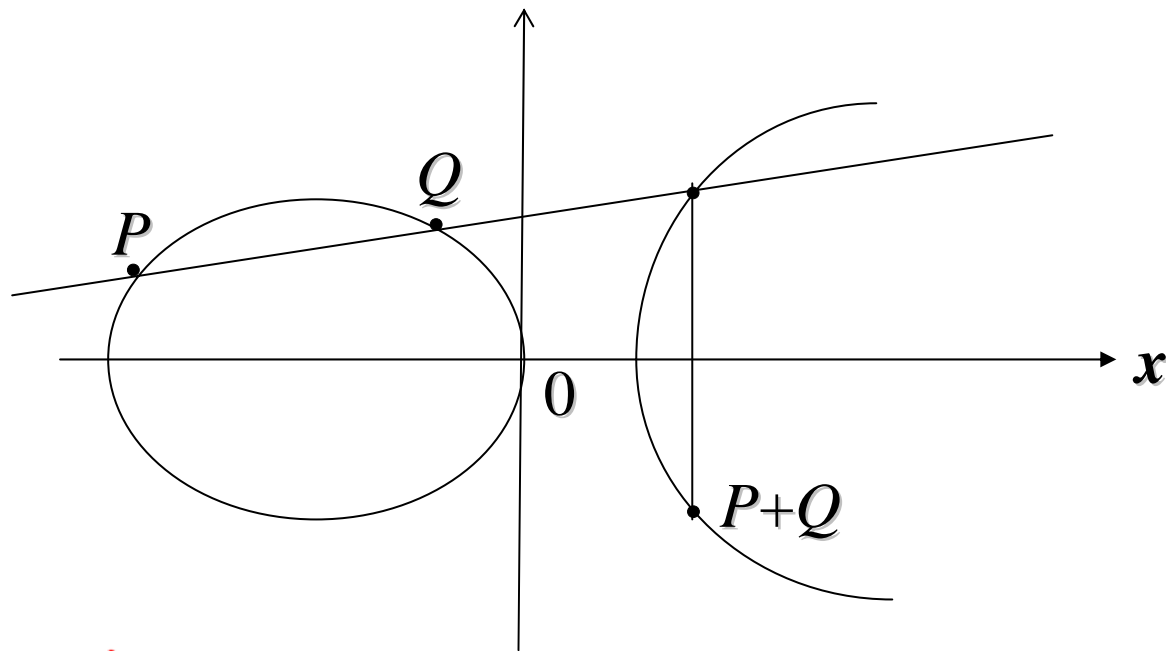
- 作集合 $E = \{\text{全体解点}, \text{无穷点 } O\}$ 。
- 可以验证，如上定义的集合 E 和加法运算构成加法交换群。
- 复习：群 G 的定义
 - G 是一个非空集，定义了一种运算，且运算是自封闭的；
 - 运算满足结合律；
 - G 中有单位元；
 - G 中的元素都有逆元；



一、椭圆曲线

2、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。





一、椭圆曲线

3、举例

- 求出椭圆曲线 $y^2 = x^3 + x + 6 \pmod{11}$ 的解点。由于 p 较小，使 $\text{GF}(p)$ 也较小，故可以利用穷举的方法根据

$$y^2 = x^3 + x + 6 \pmod{11}$$

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

$$y^2 = a \pmod{p},$$

则称 a 是模 p 的平方剩余。





一、椭圆曲线

3、举例

● 求出mod 11 的平方剩余。

■ $1^2=1 \bmod 11$

$2^2=4 \bmod 11$

■ $3^2=9 \bmod 11$

$4^2=16=5 \bmod 11$

■ $5^2=25=3 \bmod 11$

$6^2=36=3 \bmod 11$

■ $7^2=49=5 \bmod 11$

$8^2=64=9 \bmod 11$

■ $9^2=81=4 \bmod 11$

$10^2=100=1 \bmod 11$

所以，mod 11的平方剩余为：

$\{1,3,4,5,9\}$





一、椭圆曲线

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





一、椭圆曲线

- 根据上表可知椭圆曲线 $y^2=x^3+x+6 \bmod 11$ 的全部解点集为：

(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。

- $E=\{\text{全体解点} \cup \text{无穷远点} O\}$
- 由于群 E 的元素个数为13，而13为素数，所以群 E 是循环群，而且任何一个非0元素都是生成元。





一、椭圆曲线

- 由于是加法群， n 个元素 G 相加表示为：

$$G+G+\dots+G = nG ,$$

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，

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

$$y_3 = 8 (2 - 5) - 7 \bmod 11 = 2 .$$





一、椭圆曲线

$$G = (2, 7)$$

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

$$3G = (8, 3)$$

$$4G = (10, 2)$$

$$5G = (3, 6)$$

$$6G = (7, 9)$$

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

$$8G = (3, 5)$$

$$9G = (10, 9)$$

$$10G = (8, 8)$$

$$11G = (5, 9)$$

$$12G = (2, 4)$$

$$13G = \mathbf{O} \text{ (} \infty, \infty \text{)}$$

- 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

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





一、椭圆曲线

4、 $GF(2^m)$ 上的椭圆曲线

- 除了 $GF(p)$ 上的椭圆曲线，还有定义在 $GF(2^m)$ 上的椭圆曲线。
- 基于这两种椭圆曲线都可以设计出安全的椭圆曲线密码。
- 定义：设 m 是正整数，且 $b \neq 0$ ，称曲线
$$y^2 + xy = x^3 + ax^2 + b, \quad a, b \in GF(2^m)$$
为 $GF(2^m)$ 上的椭圆曲线。
- 注意： $GF(2^m)$ 上的椭圆曲线与 $GF(p)$ 上的椭圆曲线的加法定义不同。





一、椭圆曲线

- **举例：** $g(x)=x^4+x+1$ 是 $GF(2)$ 上的既约多项式，用 $g(x)$ 构造扩域 $GF(2^4)$ 。取 $a = \alpha^3$, $b = \alpha^{14}$, 考虑 $GF(2^4)$ 上的椭圆曲线多项式

$$y^2 + xy = x^3 + ax^2 + b = x^3 + \alpha^3 x^2 + \alpha^{14}$$

- 通过穷举，求出其全部解点如下：

$P_1 = (0000, 1011)$	$P_2 = (0001, 0000)$	$P_3 = (0001, 0001)$
$P_4 = (0010, 1101)$	$P_5 = (0010, 1111)$	$P_6 = (0011, 1100)$
$P_7 = (0011, 1111)$	$P_8 = (0101, 0000)$	$P_9 = (0101, 0101)$
$P_{10} = (0111, 1011)$	$P_{11} = (0111, 1100)$	$P_{12} = (1000, 0001)$
$P_{13} = (1000, 1001)$	$P_{14} = (1001, 0110)$	$P_{15} = (1001, 1111)$
$P_{16} = (1011, 0010)$	$P_{17} = (1011, 1001)$	$P_{18} = (1100, 0000)$
$P_{19} = (1100, 1100)$	$P_{20} = (1111, 0100)$	$P_{21} = (1111, 1011)$






一、椭圆曲线

- $E = \{21 \text{ 个解点} \cup \text{无穷远点 } O\}$ 构成一个加法交换群。
- 取 $P_5 = (0010, 1111)$ 进行一系列的运算，可得如下结果：

$1P_5 = P_5$	$2P_5 = P_{16}$	$3P_5 = P_8$	$4P_5 = P_{13}$	$5P_5 = P_{10}$
$6P_5 = P_{21}$	$7P_5 = P_7$	$8P_5 = P_{14}$	$9P_5 = P_2$	$10P_5 = P_{18}$
$11P_5 = P_1$	$12P_5 = P_{19}$	$13P_5 = P_3$	$14P_5 = P_{15}$	$15P_5 = P_6$
$16P_5 = P_{20}$	$17P_5 = P_{11}$	$18P_5 = P_{12}$	$19P_5 = P_9$	$20P_5 = P_{17}$
$21P_5 = P_4$	$22P_5 = O$			
- 结果说明，**这个群是循环群， P_5 是群的一个生成元。**
- 注意：**并不是所有非零元素都是群的生成元，如 $P_{12} = (1000, 0001)$ 的阶为11。**





二、椭圆曲线离散对数问题

1、对比素域上的离散对数问题

①设 p 为素数，则模 p 的剩余构成有限域：

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

F_p 的非零元素构成乘法循环群 F_p^* ：

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


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

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：

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





二、椭圆曲线离散对数问题


③求对数 x 的运算为

$$x = \log_a y, \quad 1 \leq x \leq p-1$$

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，对于认真选择的 p ，求解离散对数问题的计算复杂性为 $O(p^{1/2})$ 。
- 据此，对于认真选择的、足够大的 p ，求解离散对数问题是困难的。






二、椭圆曲线离散对数问题

2、椭圆曲线群上的离散对数问题

- 设 G 是椭圆曲线上的一个解点，它的阶为 n ， t 为一正整数，且 $1 \leq t < n$ 。对于给定的 G 和 t ，计算 $tG = Q$ 是容易的。但若已知 G 和 Q 点，要计算出 t 则是困难的。这便是椭圆曲线群上的离散对数问题，简记为ECDLP。
- 除了几类特殊的椭圆曲线外，对于一般ECDLP目前尚没有有效求解方法。因子分解和DLP问题都有亚指数求解算法，而ECDLP尚没有亚指数求解算法。
- 据此，对于认真选择的、足够大的解点群，椭圆曲线离散对数问题是困难的。





二、椭圆曲线离散对数问题

2、椭圆曲线群上的离散对数问题

- 一般情况下，椭圆曲线上的解点所构成的群 E 不一定是循环群。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，这个循环子群中的椭圆离散对数问题是困难的。
- 基于子群 E_1 的椭圆离散对数问题可以构造密码，并称为椭圆曲线密码。





三、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，并颁布了椭圆曲线密码标准算法**SM2**。





三、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。





三、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。





三、椭圆曲线公钥密码

2、 $GF(p)$ 上椭圆曲线密码基础参数

$$T = \langle p, a, b, G, n, h \rangle$$

- p 是一个大素数， 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:

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

- E 为全体解点和无穷远点组成的群， E_1 是其子群。
- G 为循环子群 E_1 的生成元， 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。





三、椭圆曲线公钥密码

3、 $GF(p)$ 上的椭圆曲线密码 (ElGamal型)

(1) 密钥生成

- 用户选择一个随机数 d 作为私钥,

$$d \in \{1, 2, \dots, n-1\}.$$

- 用户计算

$$Q = dG$$

以 Q 点为自己的公开钥。

● $GF(p)$ 上的ElGamal密码

(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密钥,

$$2 \leq d \leq p-2.$$

- 用户计算

$$y = \alpha^d \bmod p,$$

以 y 为自己的公开钥。



三、椭圆曲线公钥密码

(2)加密:

- 设明文数据为 M , $0 \leq M \leq n-1$ 。
- 加密过程:
 - ① 选择一个随机数 k , $k \in \{1, 2, \dots, n-1\}$ 。
 - 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) 为最终密文。

(2) 加密

- 设明文消息 M ($0 \leq M \leq p-1$)
- 加密过程:
 - ① 随机地选取一个整数 k , $2 \leq k \leq p-2$ 。
 - ② 计算: $C_1 = a^k \bmod p$;
 $U = y^k \bmod p$;
 $C_2 = UM \bmod p$;
 - ③ 取 $C = (C_1, C_2)$ 为最终密文。





三、椭圆曲线公钥密码

(3)解密:

① 用私钥 d 求出点 X_2 :

$$dX_1 = d (kG)$$

$$= k(dG)$$

$$= kQ$$

$$= X_2(x_2, y_2)$$

② 对 C 解密: 利用 x_2
计算得到明文

$$M = C x_2^{-1} \bmod n。$$

(3) 解密

$$\begin{aligned} \text{① 计算 } V &= C_1^d \bmod p \\ &= (\alpha^k)^d \bmod p \\ &= (\alpha^d)^k \bmod p \\ &= (y)^k \bmod p \\ &= U \end{aligned}$$

② 计算

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

获得明文。





三、椭圆曲线公钥密码

4、 $GF(p)$ 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
- 我们应对其进行验证
- 此外还有好曲线吗？如何产生？

②倍点运算比较麻烦。





三、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 $GF(2^{10000})$ 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





四、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:

$p = 8542D69E\ 4C044F18\ E8B92435\ BF6FF7DE\ 45728391\ 5C45517D\ 722EDB8B\ 08F1DFC3$

$a = 787968B4\ FA32C3FD\ 2417842E\ 73BBFEFF\ 2F3C848B\ 6831D7E0\ EC65228B\ 3937E498$

$b = 63E4C6D3\ B23B0C84\ 9CF84241\ 484BFE48\ F61D59A5\ B16BA06E\ 6E12D1DA\ 27C5249A$

$n = 8542D69E\ 4C044F18\ E8B92435\ BF6FF7DD\ 29772063\ 0485628D\ 5AE74EE7\ C32E79B7$

$h=1$

$G_x = 421DEBD6\ 1B62EAB6\ 746434EB\ C3CC315E\ 32220B3B\ ADD50BDC\ 4C4E6C14$
 $7FEDD43D$

$G_y = 0680512B\ CBB42C07\ D47349D2\ 153B70C4\ E5D7FDFC\ BFA36EA1\ A85841B9\ E46E09A2$

2、密钥:

● 私钥随机数 d , $d \in [1, n-1]$

A的私钥: d_A

● 公钥 $P = dG$

A的公钥: $P_A = d_A G$





四、中国商用椭圆曲线公钥密码SM2

3、加密算法：A发 M 给B

- ① 产生随机数 k , $1 \leq k \leq n-1$;
- ② 计算椭圆曲线点 $C_1 = kG = (x_1, y_1)$;
- ③ 计算椭圆曲线点 $S = hP_B$, 若 S 是无穷远点, 则报错并退出;
- ④ 计算椭圆曲线点 $kP_B = (x_2, y_2)$;
- ⑤ 计算 $t = \text{KDF}(x_2 \parallel y_2, \text{klen})$, 若 t 为全0比特串, 则返回①;
- ⑥ 计算 $C_2 = M \oplus t$;
- ⑦ 计算 $C_3 = \text{Hash}(x_2 \parallel M \parallel y_2)$;
- ⑧ 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**函数从输入数据 Z 产生出长度为 klen 的密钥数据。



四、中国商用椭圆曲线公钥密码SM2

● 密钥派生函数KDF(Z, K)

① For (CT=1; CT ≤ [klen/v]; CT++) / *产生[klen/v]个中间Hash值* /

$$HA[CT] = H_v(Z \parallel CT);$$

② If [klen/v] ≠ klen/v Then HA[[klen/v]] = HA[[klen/v]] 最左边的(klen - (v × [klen/v]))比特;

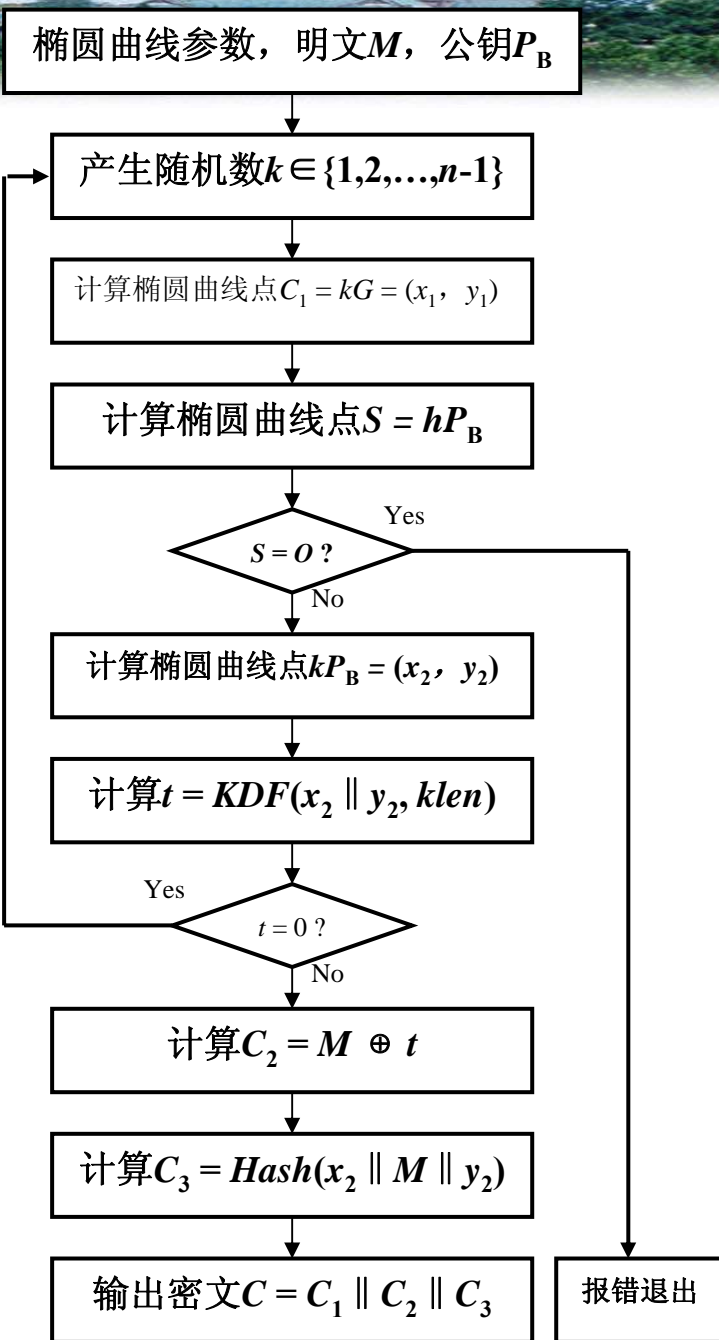
/*若[klen/v]是整数，则不作处理，否则截短HA[[klen/v]]，以确保整个的Hash值的长度等于klen * /

③ K = HA[1] ∥ HA[2] ∥ ... ∥ HA[[klen/v]-1] ∥ HA[[klen/v]]。

■ 注意，其中H_v()表示长度为v比特的Hash值。CT 是一个32位的计数器。HA[[klen/v]]是存储[klen/v]个中间值的数组。Z是输入比特串，K是输出密钥。klen表示密钥的比特长度，要求该值小于v (2³²-1)。Hash函数使用SM3。



加密框图





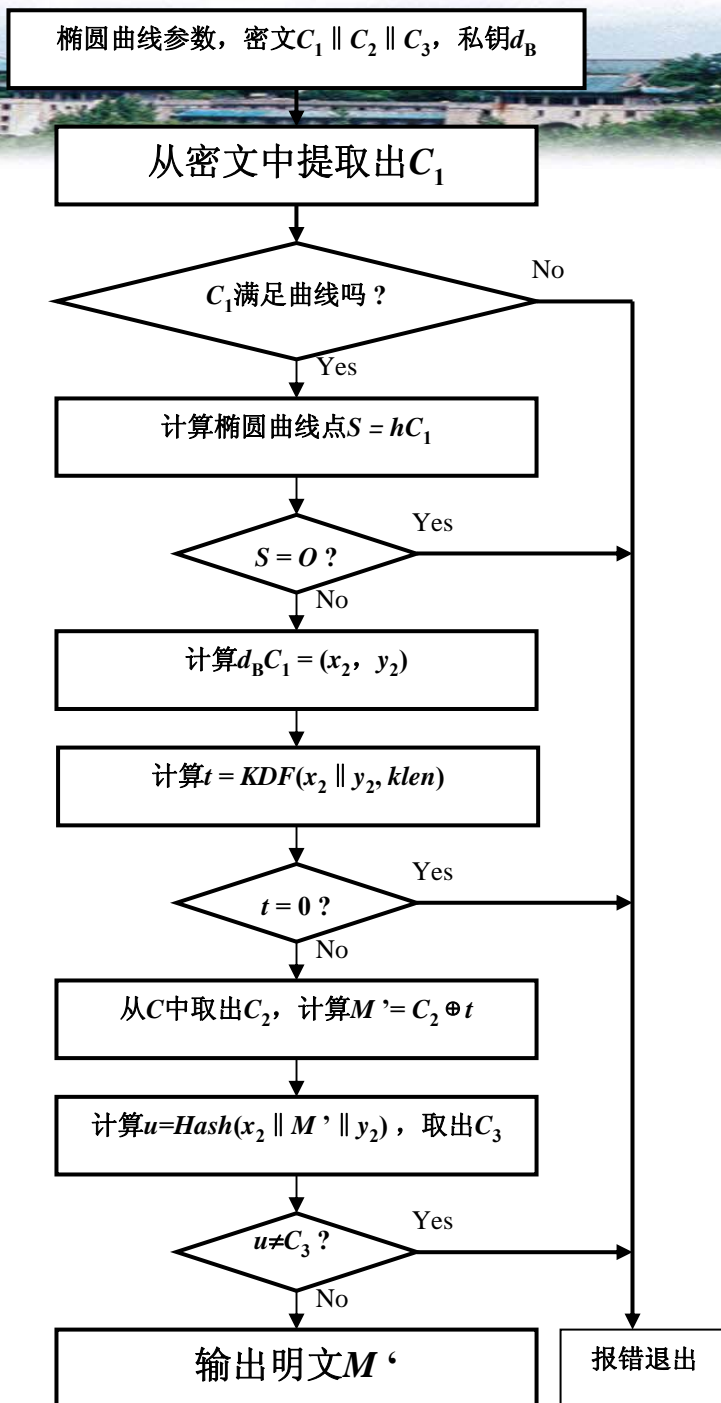
四、中国商用椭圆曲线公钥密码SM2

4、解密

- ①从 C 中取出比特串 C_1 ，将 C_1 的数据表示为椭圆曲线上的点，验证 C_1 是否满足椭圆曲线方程，若不满足则报错并退出。
- ② 计算椭圆曲线点 $S = hC_1$ ，若 S 是无穷远点，则报错并退出。
- ③ 计算 $dC_1 = (x_2, y_2)$ ；
- ④ 计算 $t = \text{KDF}(x_2 \parallel y_2, \text{klen})$ ，若 t 为全0比特串，则报错并退出；
- ⑤从 C 中取出比特串 C_2 ，计算 $M' = C_2 \oplus t$ ；
- ⑥ 计算 $u = \text{Hash}(x_2 \parallel M' \parallel y_2)$ ，从 C 中取出比特串 C_3 ，若 $u \neq C_3$ ，则报错并退出。
- ⑦ 输出明文 M' 。



解密框图





五、中国商用椭圆曲线公钥密码SM2

5、解密正确性：

- **证明：** $d_B C_1 = d_B(kG) = k(d_B G) = kP_B = (x_2, y_2)$;
如果 (x_2, y_2) 是正确的，则 $t = \text{KDF}(x_2 \parallel y_2, klen)$ 也将是正确的。
又因为加密时 $C_2 = M \oplus t$ ，所以解密时
$$M' = C_2 \oplus t。$$
- **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，若两者相等则说明密文和解密正确，否则说明密文或解密不正确。





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 $\langle X_1, C \rangle$

- SM2:

- 计算点 $kP_B = (x_2, y_2)$;
- 计算 $t = \text{KDF}(x_2 \parallel y_2, klen)$;
- 计算 $C_2 = M \oplus t$;
- 最终密文是 $\langle C_1, C_2, C_3 \rangle$





五、中国商用椭圆曲线公钥密码SM2

6、比较

● 传统椭圆曲线密码

- 利用分量 x_2 作密钥进行加密： $C = m x_2 \bmod n$ ，加密运算是乘法比较复杂。
- 分量 y_2 没有利用。
- (X_1, C) 为密文。

● SM2

- 利用分量 x_2 和 y_2 经过密钥派生函数产生中间密钥 t ，再用 t 进行加密： $C_2 = M \oplus t$ ，加密运算是模2加，因此效率更高，
- 密钥派生函数提高了安全性，却增加了时间消耗。
- $C = C_1 \parallel C_2 \parallel C_3$ 为密文，密文数据扩张较前者严重。
- SM2 采取了许多检错措施，从而提高了密码系统的数据完整性和系统可靠性，进而提高了密码系统的安全性。





五、中国商用椭圆曲线公钥密码SM2

6、比较

- 对于SM2所使用的椭圆曲线， $h=1$ 。因此，步骤③对于保密来说是非本质的。但是，如果 h 或 P_B 发生了错误或 P_B 选得不好，致使 $S=hP_B=O$ ，则它可以把错误检查出来。
- 在解密算法中加入了更多的检错功能，这是因为解密的密文是经过信道传输过来的，由于信道干扰的影响和对手的篡改，在密文中含有错误或被篡改的可能性是存在的。采取措施把错误和篡改检测出来，对提高密码系统的数据完整性、系统可靠性和安全性是有益的。





五、中国商用椭圆曲线公钥密码SM2

6、比较

●解密算法中的检错

- ①检查密文 C_1 是否是正确的。
- ②进一步检查 C_1 的正确性，其作用与加密算法中的③类似。
- ④检查 t 的正确性，其中包含着 C_2 的正确性。
- ⑥检查 C_3 的正确性。
- 这样，密文 $C = C_1 \parallel C_2 \parallel C_3$ 的正确性都得到检查。





五、中国商用椭圆曲线公钥密码SM2

7、SM2的应用

●SM2已得到广泛应用

- 二代居民身份证
- 可信计算、通信、金融、卫生、电力等系统

●我国政府正推动我国商用密码算法成为国际标准

- 3Gpp采纳ZUC为4G标准
- SM系列算法纳入TCG TPM2.0规范（ISO标准）
- SM系列算法已在ISO立项
- EMVC0研究采纳SM系列算法

●我国密码科学技术与应用取得巨大成果！



武汉大学



研究前沿介绍



武汉大学



量子计算对密码学的影响 及对策探讨

王后珍

空天信息安全与可信计算教育部重点实验室





一、量子计算机发展动向

1、加拿大量子计算机已开始商用

- 《Nature》2011年5月：加拿大D-Wave公司推出世界上首台128量子位（Qbit）商用量子计算机D-Wave One 系统。
- 1000万美元/台，卖给著名军火商洛克希德马丁公司，用于：F35战机分析、新武器开发和雷达、航天、航空器系统测试等。



一、量子计算机发展动向

1、加拿大量子计算机已开始商用

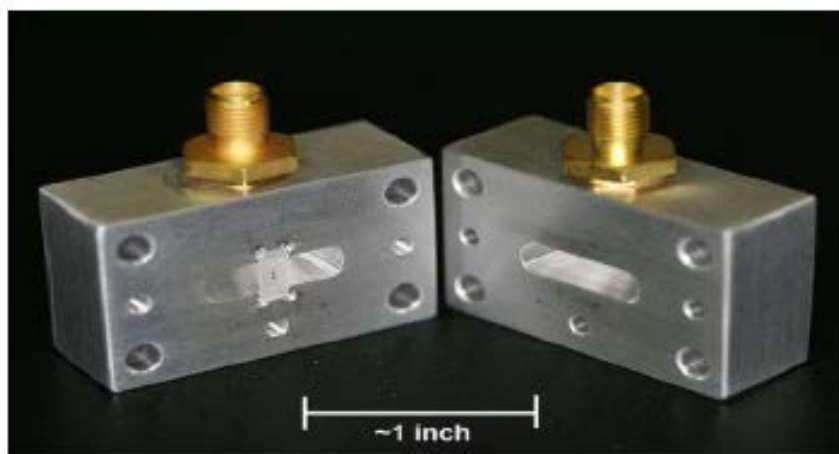
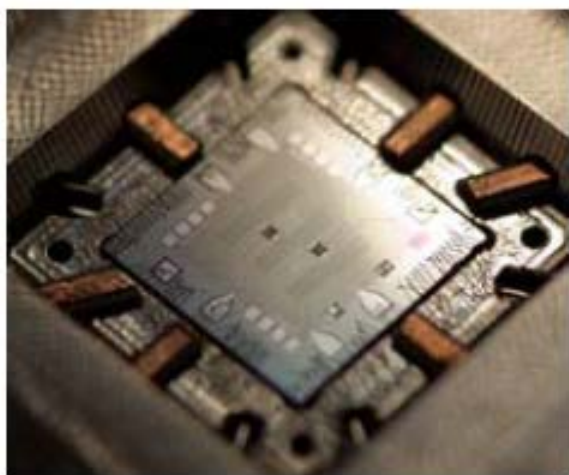
- 2013年初，加拿大D-Wave公司又推出512qbit的D-Wave Two。
- 1500万美元/台，卖给著名信息服务商谷歌公司，用于加速信息搜索的速度和人工智能。
- 根据常规，很可能已开始1024qbit的系统研发。



一、量子计算机发展动向

1、美国通用量子计算机已出现

- 《Nature》2011年9月报道：UCSB通过量子电路成功实现了冯诺依曼结构的量子计算机。
- IBM找到了可以大规模提升量子计算机规模的一种关键技术





一、量子计算机发展动向

3、斯诺登爆料NSA研制破译密码的量子计算机

- 对外严格保密
- 外界两种观点

NSA seeks to build quantum computer that could crack most types of encryption

By Steven Rich and Barton Gellman, Published: January 2 [E-mail the writers](#)

- ◆ 已取得实质进展
- ◆ 遇到技术困难



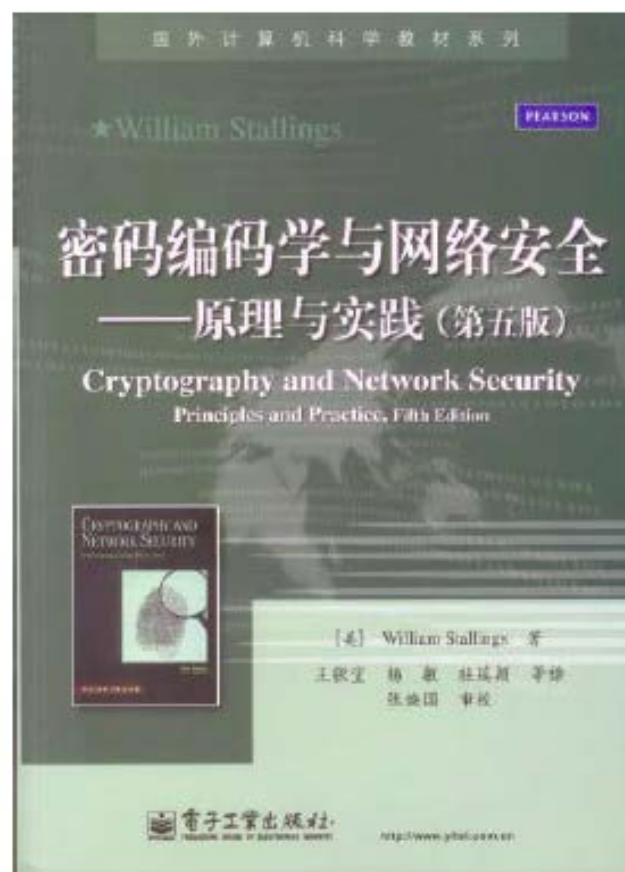
武汉大学

二、量子计算对密码学的影响

教材



参考书



武汉大学



二、量子计算对密码学的影响

◆ 密码学的主要研究内容：

- 序列密码
- 分组密码
- 公钥密码
- Hash函数
- 数字签名及认证
- 密钥管理





二、量子计算对密码学的影响

◆ 目前广泛应用的公钥密码算法：

➤ **RSA**：基于大整数因子分解难题

➤ **ElGamal**：基于离散对数难题

➤ **ECC**：基于椭圆曲线离散对数难题





二、量子计算对密码学的影响

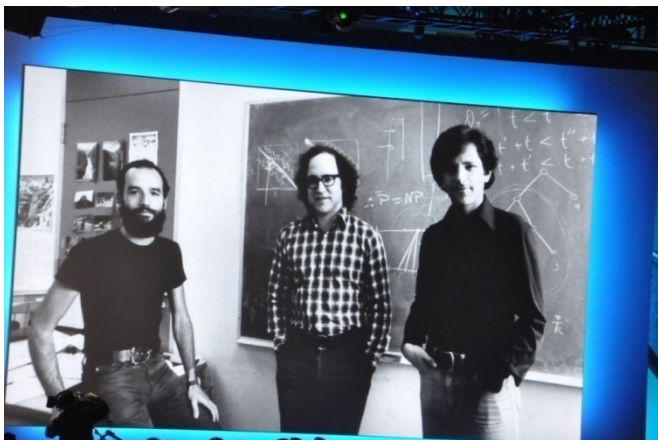
◆ RSA密码:

- 1978年美国麻省理工学院的三名密码学者R.L.Rivest,A.Shamir和L.Adleman提出了一种基于大合数因子分解困难性的公开密钥密码,简称为RSA密码。
- **RSA密码被誉为是一种风格幽雅的公开密钥密码。既可用于加密,又可用于数字签名,安全、易懂。**
- RSA密码已成为目前应用最广泛的公开密钥密码之一。



二、量子计算对密码学的影响

◆ RSA密码:



SECURITY™



The Security Division of EMC

RSA®
CONFERENCE
2014





二、量子计算对密码学的影响

◆ RSA密码:

- ①随机地选择两个大素数 p 和 q ，而且保密；
 - ②计算 $n=pq$ ，将 n 公开；
 - ③计算 $\phi(n)=(p-1)(q-1)$ ，对 $\phi(n)$ 保密；
 - ④随机地选取一个正整数 e ， $1 < e < \phi(n)$ 且 $(e, \phi(n)) = 1$ ，将 e 公开；
 - ⑤根据 $ed=1 \bmod \phi(n)$ ，求出 d ，并对 d 保密；
 - ⑥加密运算： $C=M^e \bmod n$
 - ⑦解密运算： $M=C^d \bmod n$
- 公开加密钥 $K_e = \langle e, n \rangle$ ，保密解密密钥 $K_d = \langle p, q, d, \phi(n) \rangle$





二、量子计算对密码学的影响

◆ RSA密码：基于大整数因子分解数学难题

- $15 = 3 \times 5$
- 1350664108659952233496032162788059699388
8147560566702752448514385152651060485953
3833940287150571909441798207282164471551
3736804197039641917430464965892742562393
4102086438320211037295872576235850964311
0564073501508187510676594629205563685529
4752135008528794163773285339061097505443
34999811150056977236890927563 = ? × ?





二、量子计算对密码学的影响

◆ RSA密码：基于大整数因子分解数学难题

保密级别	对称密钥长度 (bit)	RSA密钥长度 (bit)	ECC密钥长度 (bit)	保密年限
80	80	1024	160	2010
112	112	2048	224	2030
128	128	3072	256	2040
192	192	7680	384	2080
256	256	15360	512	2120





二、量子计算对密码学的影响

◆ 1994年贝尔实验室的Peter Shor提出了一种攻击RSA密码的量子多项式算法。

算法 1: 因子分解的量子算法 (Shor 算法)

Input: 大整数 N .

Output: N 的因子.

Step1: 如果 N 为偶数, 则输出因子 2;

Step2: 随机选取 $a(1 < a < N - 1)$, 若最大公因子 $\gcd(a, N) > 1$, 则输出 $\gcd(a, N)$;

Step3: 利用量子算法求出函数 $f(x) = a^x \bmod N$ 的周期, 记为 r ;

Step4: 若 r 为偶数且 $a^{r/2} \not\equiv -1 \bmod N$, 则计算 $\gcd(a^{r/2} - 1, N)$ 和 $\gcd(a^{r/2} + 1, N)$, 二者至少有一个必为 N 的因子.





二、量子计算对密码学的影响

◆ 1994年贝尔实验室的Peter Shor提出了一种攻击RSA密码的量子多项式算法。

算法 1: 因子分解的量子算法 (Shor 算法)

Input: 大整数 N .

Output: N 的因子.

Step1: 如果 N 为偶数, 则输出因子 2;

Step2: 随机选取 $a(1 < a < N - 1)$, 若最大公因子 $\gcd(a, N) > 1$, 则输出 $\gcd(a, N)$;

Step3: 利用量子算法求出函数 $f(x) = a^x \bmod N$ 的周期, 记为 r ;

Step4: 若 r 为偶数且 $a^{r/2} \not\equiv -1 \bmod N$, 则计算 $\gcd(a^{r/2} - 1, N)$ 和 $\gcd(a^{r/2} + 1, N)$, 二者至少有一个必为 N 的因子.





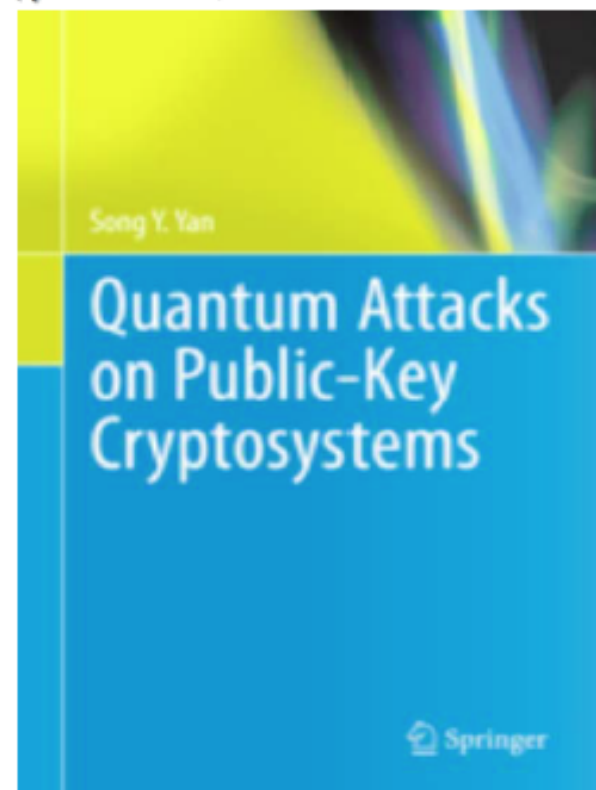
二、量子计算对密码学的影响

量子计算机严重威胁公钥密码的安全

● Shor算法:

- 离散傅里叶变换→整数分解、离散对数→有效攻击RSA、ECC、ElGamal、HD等密码
- 现已扩展到隐藏子群问题 (HSP)

● 量子计算时代我们使用什么密码，是摆在我国面前的一个十分紧迫的重大战略问题！



武汉大学



三、抗量子计算密码学的研究

● 计算复杂性理论是基础

- 电子计算复杂性: P类, NP类, NPC类

- 量子计算复杂性: QP类, QNP类

 - ◆ P类在量子计算环境下变成QP类

 - ◆ 一部分NP问题在量子计算环境下变成QP, 这是Shor算法有效攻击RSA、ECC、ElGamal、HD密码的依据

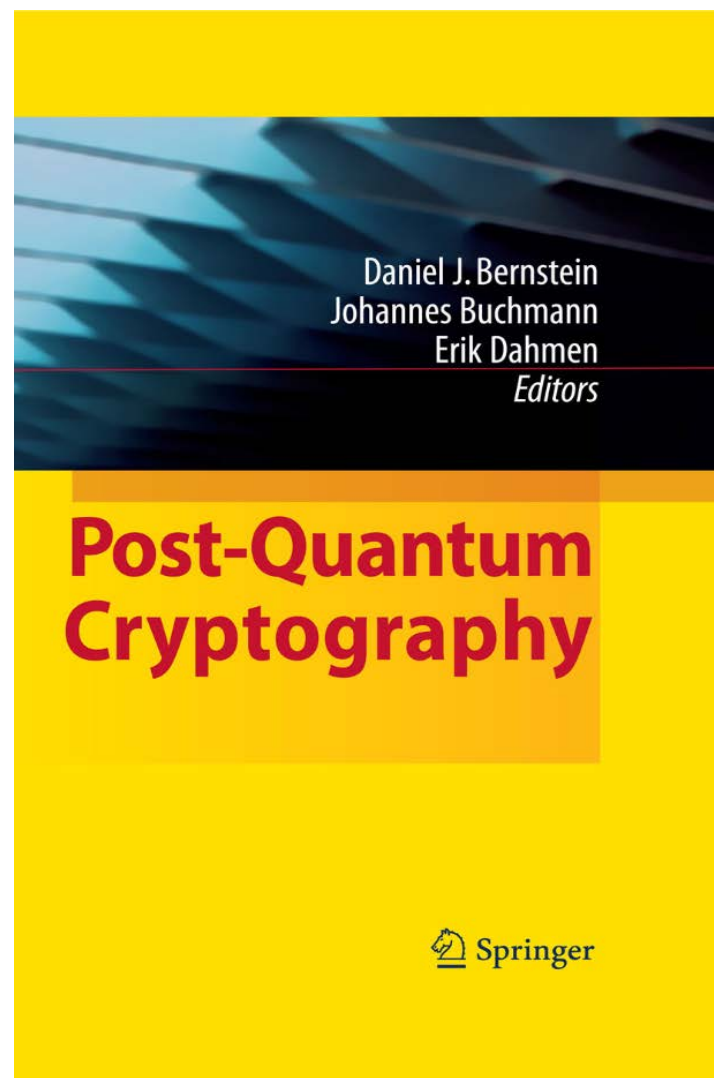
 - ◆ 一部分NP问题仍是QNP, 这是Shor算法不能有效攻击所有密码的依据





三、抗量子计算密码学的研究

- 量子计算时代我们用什么密码是摆在我们面前的一个十分紧迫的战略问题！
- 抗量子计算密码
 - 量子密码
 - DNA密码
 - 基于量子计算不擅长计算的数学问题的密码

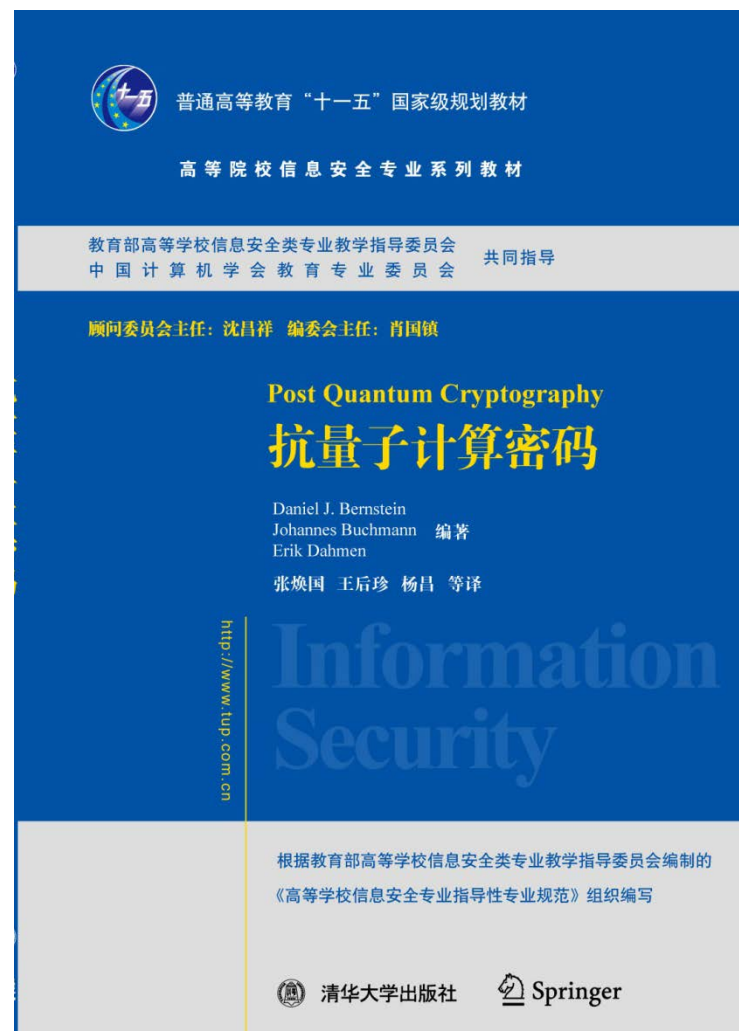


武汉大学

三、抗量子计算密码学的研究

■ 目前国际上公认的几种抗量子计算密码

- Merkle树签
- 格公钥密码
- 纠错公钥密码
- MQ公钥密码



武汉大学



四、重要的研究问题

1、量子计算复杂性

- 哪些NP类问题是QP的？
- 哪些NP类问题仍是QNP的？
- 量子计算复杂性有QNPC类吗？
- 有文献说NPC的问题是QNP的，即是抗量子计算的，这是正确的吗？





四、重要的研究问题

2、量子计算攻击

- 如何进行量子穷举攻击？它的实际攻击能力如何？如何抵抗量子穷举攻击？
- Shor 算法还能攻击什么密码？如何抵抗Shor算法的攻击？
- 其他量子计算算法？

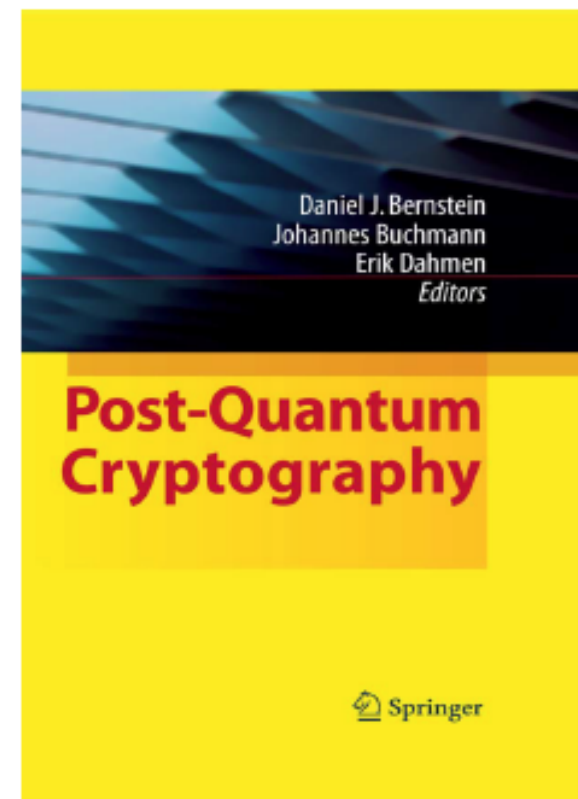




四、重要的研究问题

3、抗量子计算密码

- 目前普遍认为，纠错码密码、QM密码、格密码是抗量子计算的。尚没有证明。如何证明？
- 应当重视其他抗量子计算密码（MQ和格之外的密码）！





四、重要的研究问题

4、基于量子物理困难问题设计抗量子计算密码

■ 量子物理中有一些著名的困难问题:

◆ 量子态的测量困难问题

◆ 量子态的复制困难问题

◆ 其他

■ 这些问题是非计算的，基于这些问题设计密码是抗量子计算的。如何设计构建密码？





LSS

信息安全研究所

谢谢！

