北京邮电大学
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

《现代密码学》第七章

公钥加密体制

信息安全中心

本章主要内容

- 对称密码体制面临的问题
- 公钥密码体制的发展
- RSA单向陷门函数及其应用
- ElGmal单向陷门函数
- 椭圆曲线单向陷门函数简介
- DL/ECIES(IEEE 1363a-2004)

本章主要内容

- 对称密码体制面临的问题
- 公钥密码体制的发展
- RSA单向陷门函数及其应用
- ElGmal单向陷门函数
- 椭圆曲线单向陷门函数简介

ElGamal单向陷门函数

- Diffie-Hellman 密钥交换协议的变形；
- *T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Information Theory, vol IT-31(4), pp469-472, July 1985.*

ElGamal单向陷门函数

1）密钥生成

① 选择一大素数p, 选取Z_p^*的生成元g；

② 任选小于p的随机数x，计算$y \equiv g^x \bmod p$；

③ (y, g, p)为公开密钥，(x, g, p)为秘密密钥.

2）加密：设待加密明文为M.

① 随机选一整数k，$0<k<=p-1$；

② 计算密文对：$C=\{C_1,C_2\}$, 发送给接收者.

$$C_1 \equiv g^k \bmod p, \quad C_2 \equiv y^k M \bmod p.$$

ElGamal单向陷门函数

3）解密过程：设收到的密文对为(C_1,C_2).

计算明文：

$$M=\frac{C_2}{C_1^{\,x}}\bmod p$$

4）正确性

$$\frac{C_2}{C_1^{\,x}}\bmod p=\frac{y^kM}{g^{kx}}\bmod p=\frac{y^kM}{y^k}\bmod p=M\bmod p$$

ElGamal单向陷门函数

5）实例

- 密钥生成.

  Alice 选择公开参数p=97 及生成元g=5；

  选择秘密密钥x=58，计算并发布公钥$y=5^{58}$= 44 mod 97.

- 加密. Bob 待加密明文为M=3.

  首先得到 Alice 的公开密钥 y=44;

  选择随机 k=36 并计算:$K=44^{36}$=75 mod 97;

  计算密文对: $C_1 = 5^{36} = 50 \bmod 97$;

  $C_2 = 75*3 \bmod 97 = 31 \bmod 97$.

  发送 {50,31} 给Alice.

- 解密: Alice解密密文{50,31}.

  首先恢复分母 $K= C_1^{\,x} = 50^{58}$=75 mod 97.

  计算 $K^{-1} = 22 \bmod 97$.

  恢复明文 $M = 31*22 = 3 \bmod 97$.

ElGamal单向陷门函数

有限域上离散对数问题：

已知（Z_p，+，*）是一个有限域，g为Z_p^*的生成元，$y\in Z_p$，求x使得

$$y=g^x \bmod p.$$

如果求有限域离散对数问题是容易的，则获得公钥攻击者能够解出x，ElGamal加密算法完全破译.

加密过程：随机数k不能泄露；

随机数k不能重用。

本章主要内容

- 对称密码体制面临的问题
- 公钥密码体制的发展
- RSA单向陷门函数及其应用
- ElGmal单向陷门函数
- 椭圆曲线单向陷门函数简介

椭圆曲线单向陷门函数简介

椭圆曲线密码体制（elliptic curve cryptography, ECC）被IEEE公钥密码标准P1363采用.

GM/T 0003-2012 《SM2椭圆曲线公钥密码算法》

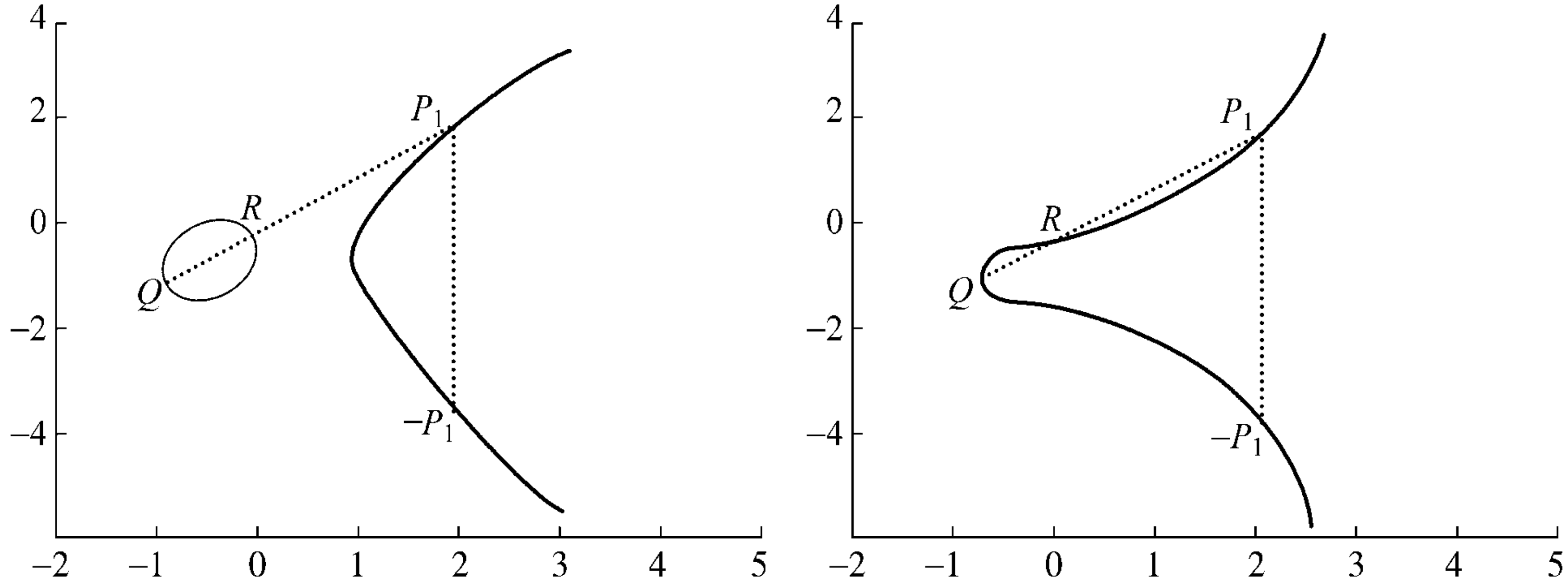
椭圆曲线是以下形式的三次方程定义的曲线：

$$y^2+axy+by=x^3+cx^2+dx+e$$

其中a,b,c,d,e是满足某些简单条件的实数.

定义中包括一个称为无穷点的元素，记为O.

椭圆曲线单向陷门函数简介



(a) $y^2=x^3-x$　　　(b) $y^2=x^3+x+1$

椭圆曲线的两个例子

椭圆曲线单向陷门函数简介

有限域上的椭圆曲线指曲线方程定义式中，所有系数都是有限域GF(p)中的元素(其中p为大素数).

最为常用的曲线是

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

$$(a,b \in GF(p),\ 4a^3 + 27b^2 \pmod{p} \neq 0).$$

例： $p=23$，$a=b=1$，$4a^3+27b^2 \pmod{23} \equiv 8 \neq 0$ I

则方程为$y^2 \equiv x^3 + x + 1$. II

椭圆曲线单向陷门函数简介

设$E_p(a,b)$表示上面方程所定义的椭圆曲线上的点集$\{(x,y)|0\le x<p, 0\le y<p, x,y\in Z\}\cup O$.

例：$E_{23}(1,1)$由下表给出（表中不包含O）.

(0, 1)	(0, 22)	(1, 7)	(1, 16)	(3, 10)	(3, 13)	(4, 0)	(5, 4)	(5, 19)
(6, 4)	(6, 19)	(7, 11)	(7, 12)	(9, 7)	(9, 16)	(11, 3)	(11, 20)	(12, 4)
(12, 19)	(13, 7)	(13, 16)	(17, 3)	(17, 20)	(18, 3)	(18, 20)	(19, 5)	(19, 18)

椭圆曲线单向陷门函数简介

设$P=(x_1,y_1)$, $Q=(x_2,y_2)$, $P\neq -Q$, 则$P+Q=(x_3,y_3)$

由以下规则确定：

$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod p$$

$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod p$$

其中

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\[2ex] \dfrac{3x_1^{\ 2} + a}{2y_1} & P = Q \end{cases}$$

椭圆曲线单向陷门函数简介

例： 以$E_{23}(1,1)$为例, 设$P=(3,10)$,$Q=(9,7)$,则

$$\lambda=\frac{7-10}{9-3}=\frac{-3}{6}=\frac{-1}{2}\equiv 11 \bmod 23$$

$$x_3=11^2-3-9=109\equiv 17 \bmod 23$$

$$y_3=11(3-17)-10=-164\equiv 20 \bmod 23$$

所以$P+Q=(17,20)$,仍为$E_{23}(1,1)$中的点.

椭圆曲线单向陷门函数简介

若求$2P$则

$$\lambda = \frac{3\cdot 3^2+1}{2\times 10} = \frac{5}{20} = \frac{1}{4} \equiv 6 \bmod 23$$

$$x_3 = 6^2 - 3 - 3 = 30 \equiv 7 \bmod 23$$

$$y_3 = 6(3-7) - 10 = -34 \equiv 12 \bmod 23$$

所以$2P$=(7,12)，仍为$E_{23}(1,1)$中的点.

椭圆曲线单向陷门函数简介

椭圆曲线上的离散对数问题:在椭圆曲线构成的Abel群$E_p(a,b)$上考虑方程$Q=kP$, 其中$P,Q\in E_p(a,b)$, $k<p$. 已知P, Q，求k?

1）椭圆曲线上ElGamal算法

- 密钥生成

  - 选取一条椭圆曲线$E_p(a,b)$，取$E_p(a,b)$的一个生成元G，$E_p(a,b)$和G作为公开参数.
  - 用户A选x_A作为秘密钥，并以$P_A=x_AG$作为公开钥.

椭圆曲线单向陷门函数简介

- 加密运算

用户Bob若想向Alice发送消息P_m，可选取一随机正整数k，产生以下点对作为密文：

$$C_m=\{kG, P_m+kP_A\}=\{c_1,c_2\}$$

- 解密运算

Alice解密时，以密文对中的第二个点减去用自己的秘钥与第一个点的倍乘，即

$$c_2 - x_A c_1 = P_m+kP_A-x_AkG=P_m+k(x_AG)-x_AkG = P_m$$

信息安全中心

椭圆曲线单向陷门函数简介

2）实例：

取p=23，$E_p(1,1)$，即椭圆曲线为$y^2 \equiv x^3+x+1$. $E_p(1,1)$的一个生成元是G=(1,7)，共有28个元素.

$2G=(7,11)$, $3G=(18,20)$,$4G=(17,20)$,$5G=(0,1)$,

$6G=(12,19)$,$7G=(11,3)$,$8G=(13,7)$, $9G=(9,16)$,

$10G=(6,19)$,$11G=(19,5)$,$12G=(5,19)$,$13G=(3,10)$,

$14G=(4,0)$,$15G=(3,13)$,$16G=(5,4)$,$17G=(19,18)$,

$18G=(6,4)$,$19G=(9,7)$,$20G=(13,16)$, $21G=(11,20)$,

$22G=(12,4)$,$23G=(0,22)$,$24G=(17,3)$,$25G=(18,3)$,

$26G=(7,12)$,$27G=(1,16)$,$28G=O$.

设Alice的秘密密钥为x_A=5，公开密钥为P_A=(0,1).

椭圆曲线单向陷门函数简介

- 假定Bob待加密的明文嵌入到椭圆曲线上的点 P_m=(0,22). 首先获取Alice的公钥，对该点进行加密：

① Bob 选取随机数k=3, 计算kG = 3(1,7)=(18,20).

② kP_A= 3(0,1)=(3,13), P_m+kP_A= (3,13)+ (0,22) = (6,19).

③ 密文为{(18,20), (6,19)}.

- Alice接收到密文{(18,20), (6,19)}, 用自己的私钥解密

① 计算 $x_A\cdot$(18,20) = 5(18,20) = (3,13),

② 然后用第二个点减去上面点的差：

P_m =(6,19)-(3,13)= (6,19)+[- (3,13)]

= (6,19)+(3, -13)= (6,19)+(3,10)= (0,22).

③ 恢复明文为(0, 22）.

椭圆曲线单向陷门函数简介

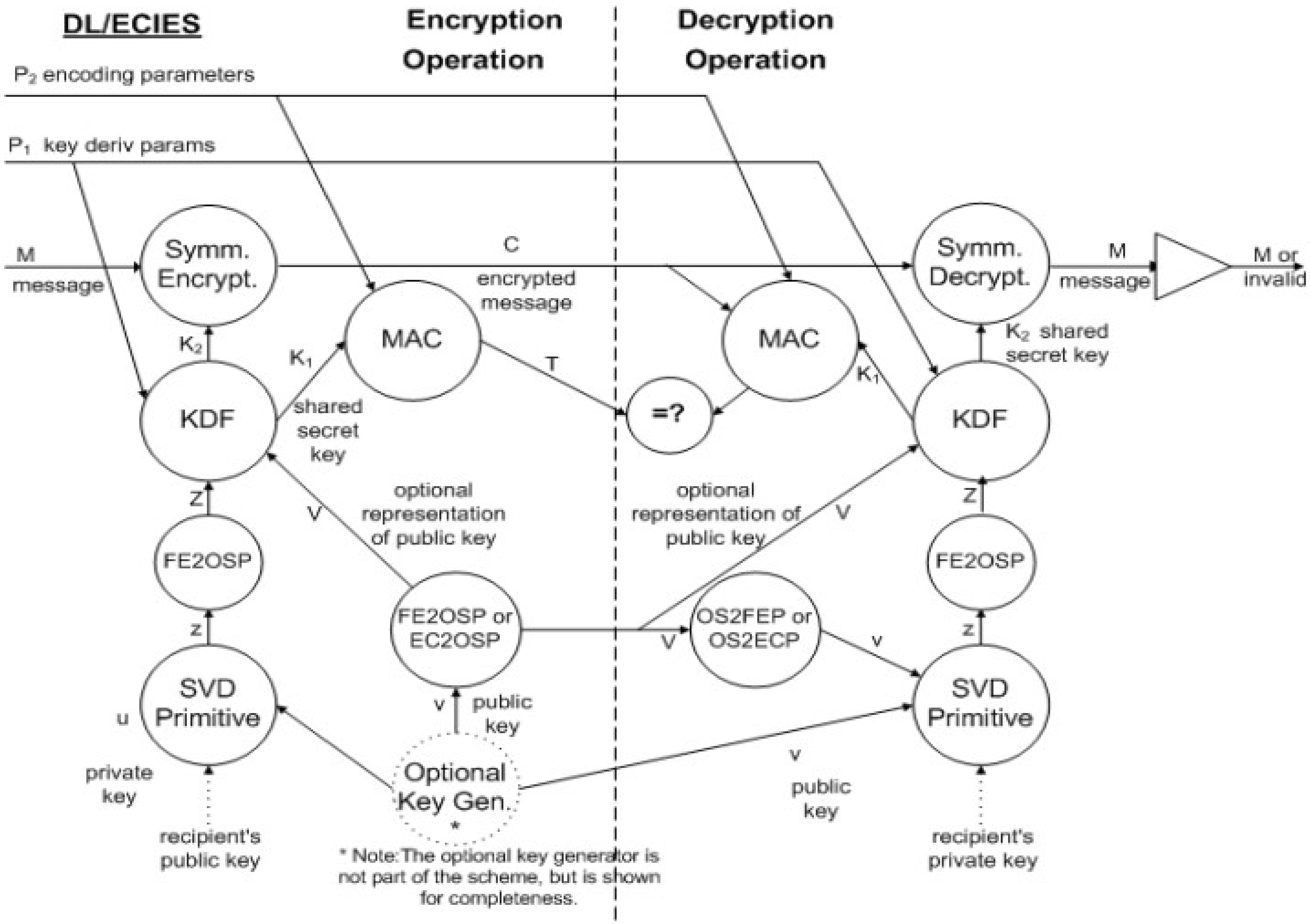
目前攻击椭圆曲线上的离散对数问题的方法只有适合攻击任何循环群上离散对数问题的大步小步法，其运算复杂度为$O(\exp(\log\sqrt{p_{\max}}))$，其中$p_{\max}$是椭圆曲线所形成的Abel群的阶的最大素因子.

保持和RSA体制同样安全强度的前提下可缩短密钥长度

RSA	512	768	1024	2048	2^{1000}
ECC	106	132	160	211	600

DL/ECIES(IEEE 1363a-2004)

DL/ECIES is
Scheme. It



DL/ECIES(IEEE 1363a-2004)

- 示例：

1） 密钥生成Gen:

- 选择循环群G中的随机生成元g和Z_n中的随机数a
- 输出sk = a ， pk = (g, h=g^a)

E(pk=(g,h), m) :

$^{R}b \leftarrow Z_n$, $u \leftarrow g^b$, $v \leftarrow h^b$

$k \leftarrow H(u,v)$, $c \leftarrow E_s(k, m)$

output (u, c)

D(sk=a, (u,c)) :

$v \leftarrow u^a$

$k \leftarrow H(u,v)$, $m \leftarrow D_s(k, c)$

output m

本章主要内容

- 对称密码体制面临的问题
- 公钥密码体制的发展
- RSA单向陷门函数及其应用
- ElGmal单向陷门函数
- 椭圆曲线单向陷门函数简介
- DL/ECIES(IEEE 1363a-2004)

THE END！