

椭圆曲线公钥密码体制 (ECC)

清华大学计算机系

于红波

2023年5月17日



关于椭圆曲线

- 椭圆曲线问题的研究有150多年的历史
- 1985年
 - Washington 大学的Neal Koblitz
 - IBM 的Victor Miller
 - 把椭圆曲线应用于密码领域
- 目前，椭圆曲线和RSA算法是使用最广泛的公钥加密算法



实数域上的椭圆曲线

□ 椭圆曲线并非椭圆，之所以称为椭圆曲线是因为它的曲线方程与计算椭圆周长的方程类似。一般来讲，椭圆曲线的曲线方程是以下形式的三次方程：

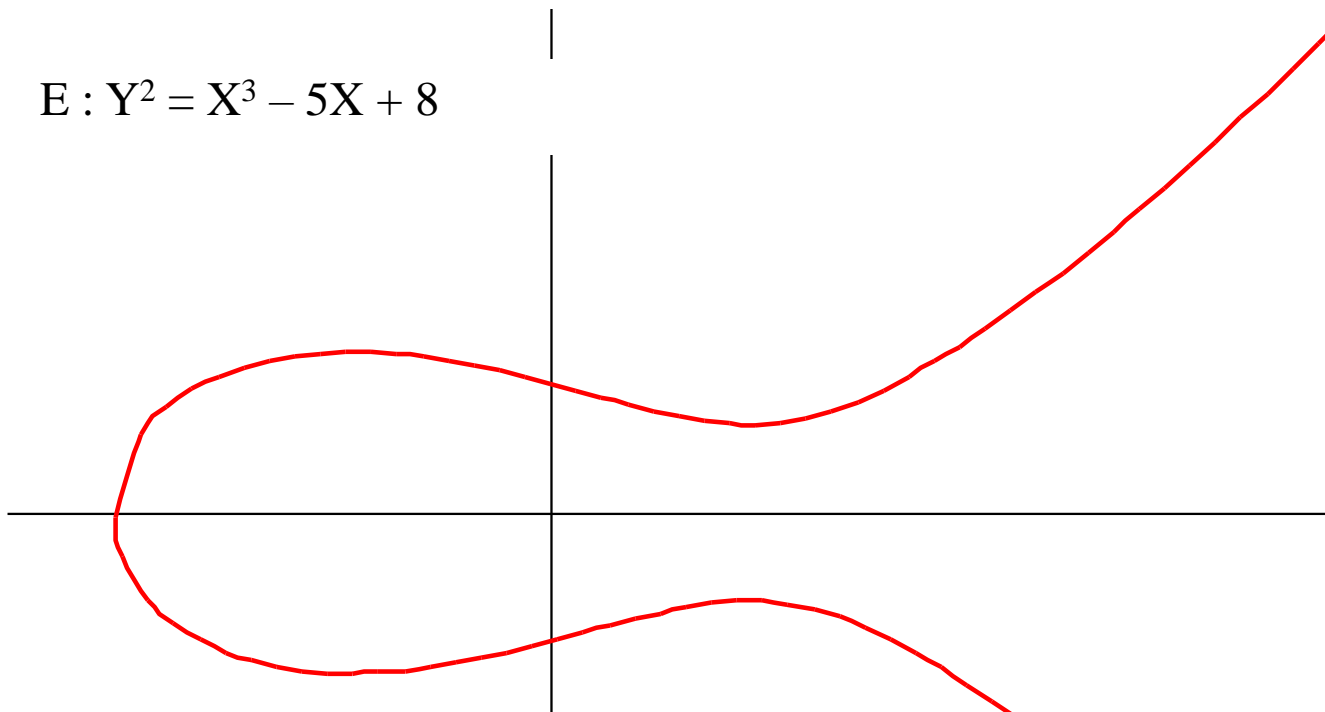
$$\square y^2 + axy + by = x^3 + cx^2 + dx + e$$

□ 其中 a, b, c, d, e 是满足某些简单条件的实数。



典型椭圆曲线

$$E : Y^2 = X^3 - 5X + 8$$



特点: 可以应用几何学使椭圆曲线上的点形成一个群.



椭圆曲线的加法

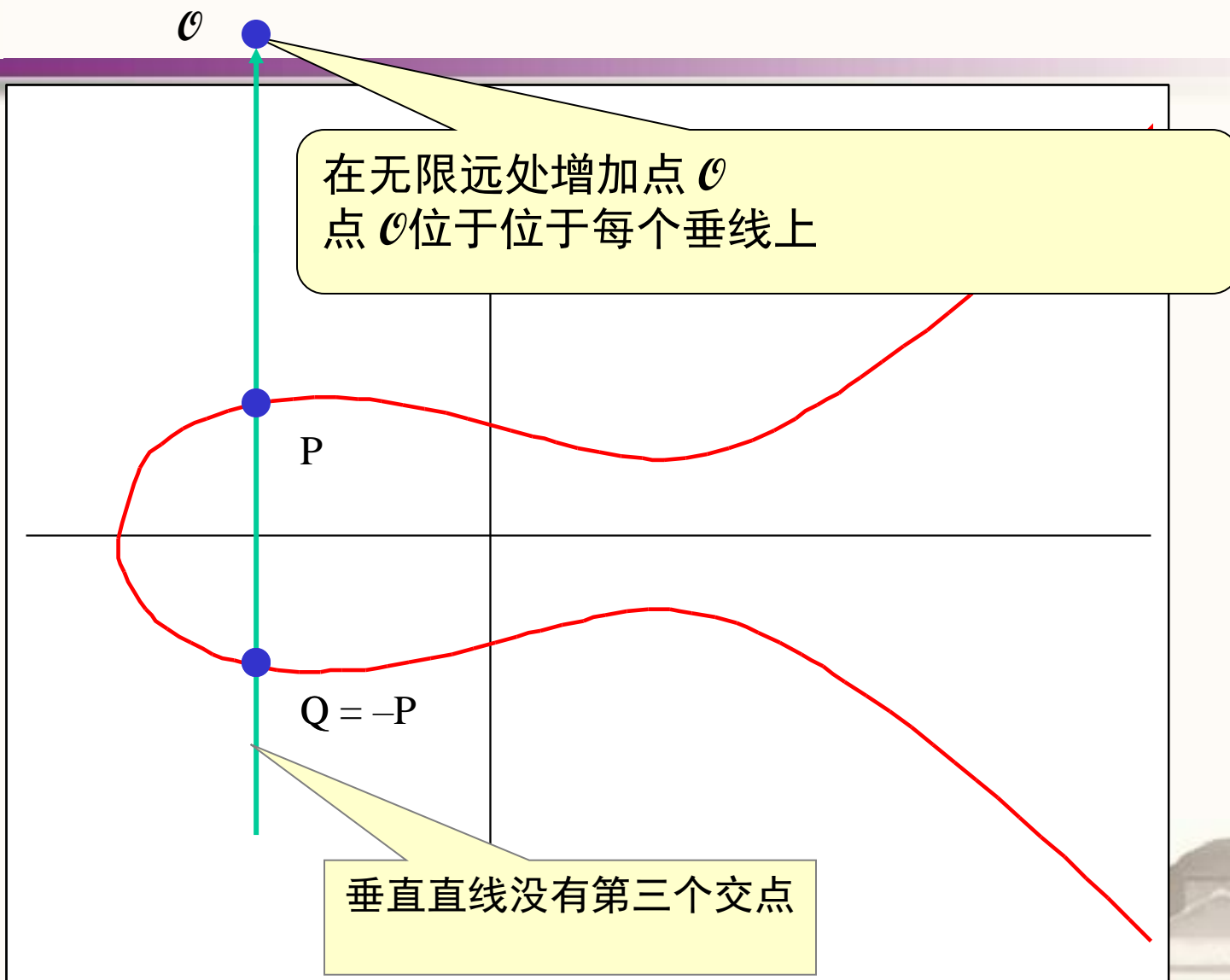
➤ 依据：

如果在椭圆曲线上有三个点存在于一条直线上，则它们的和为无穷远点。

➤ 其中无穷远点记为 \mathcal{O}



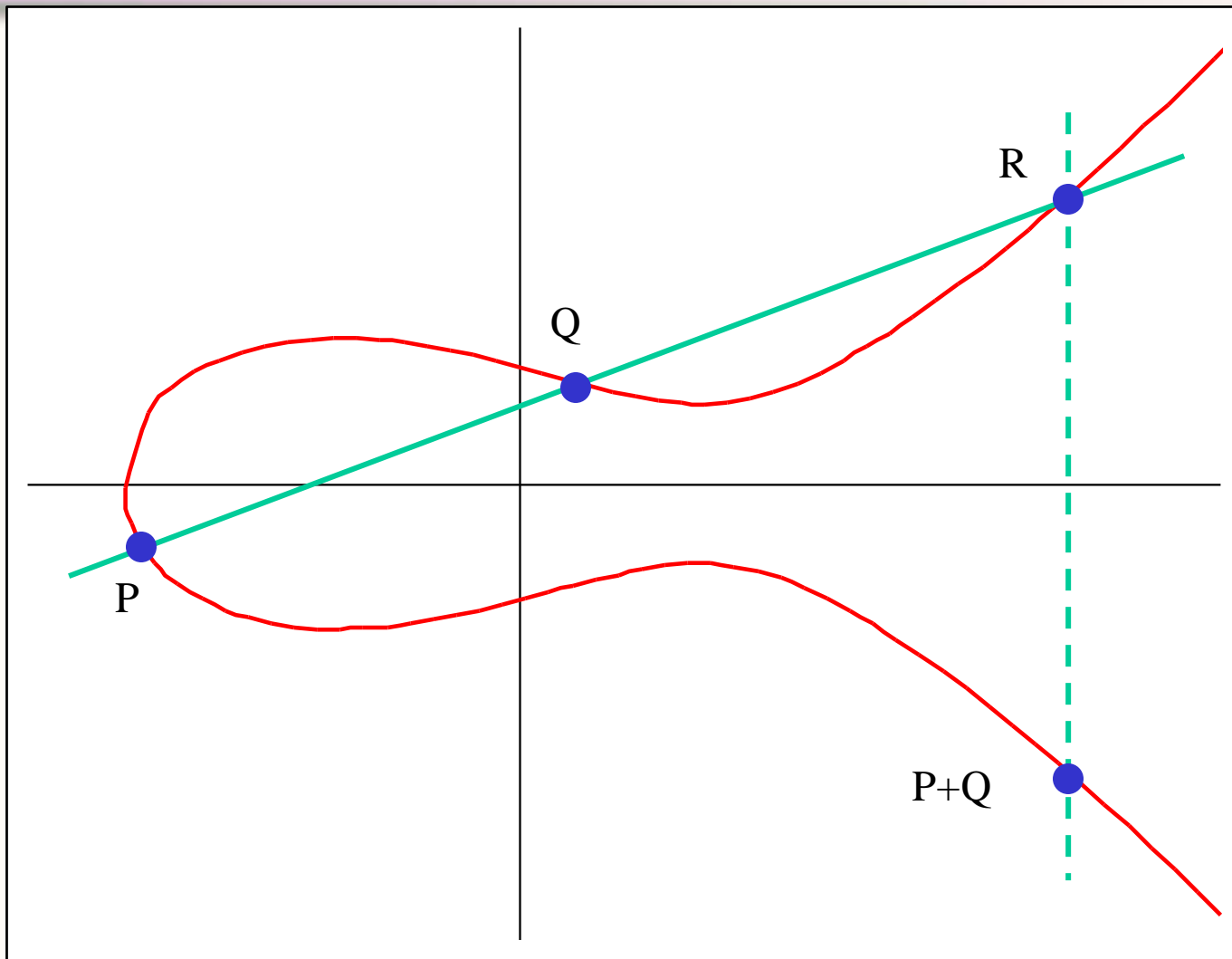
点P和点-P相加



点P和点-P相加的和为无穷远点



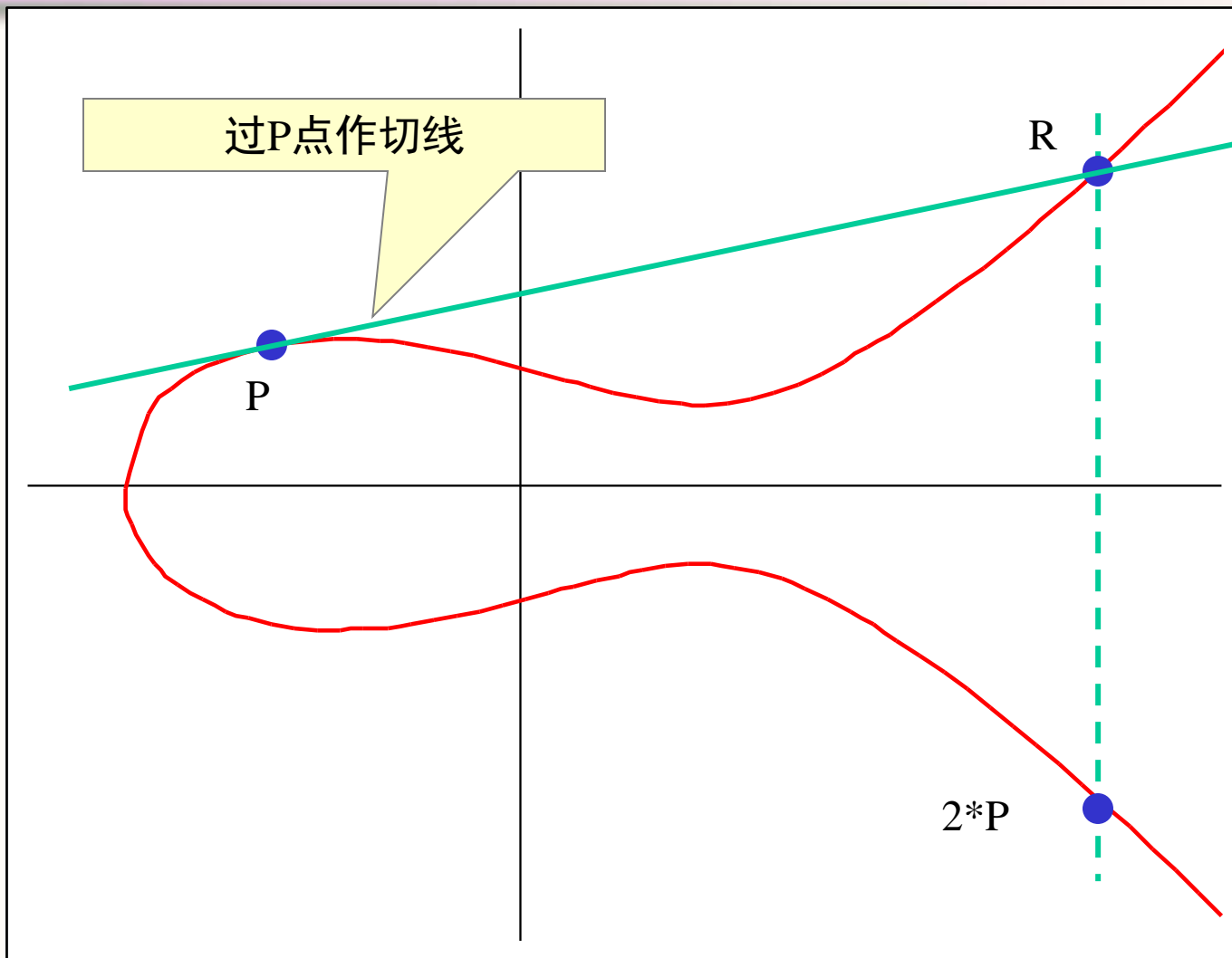
点P和点Q相加



设连接点P和Q的直线，交椭圆曲线于点R, 则点P和Q的和为点-R



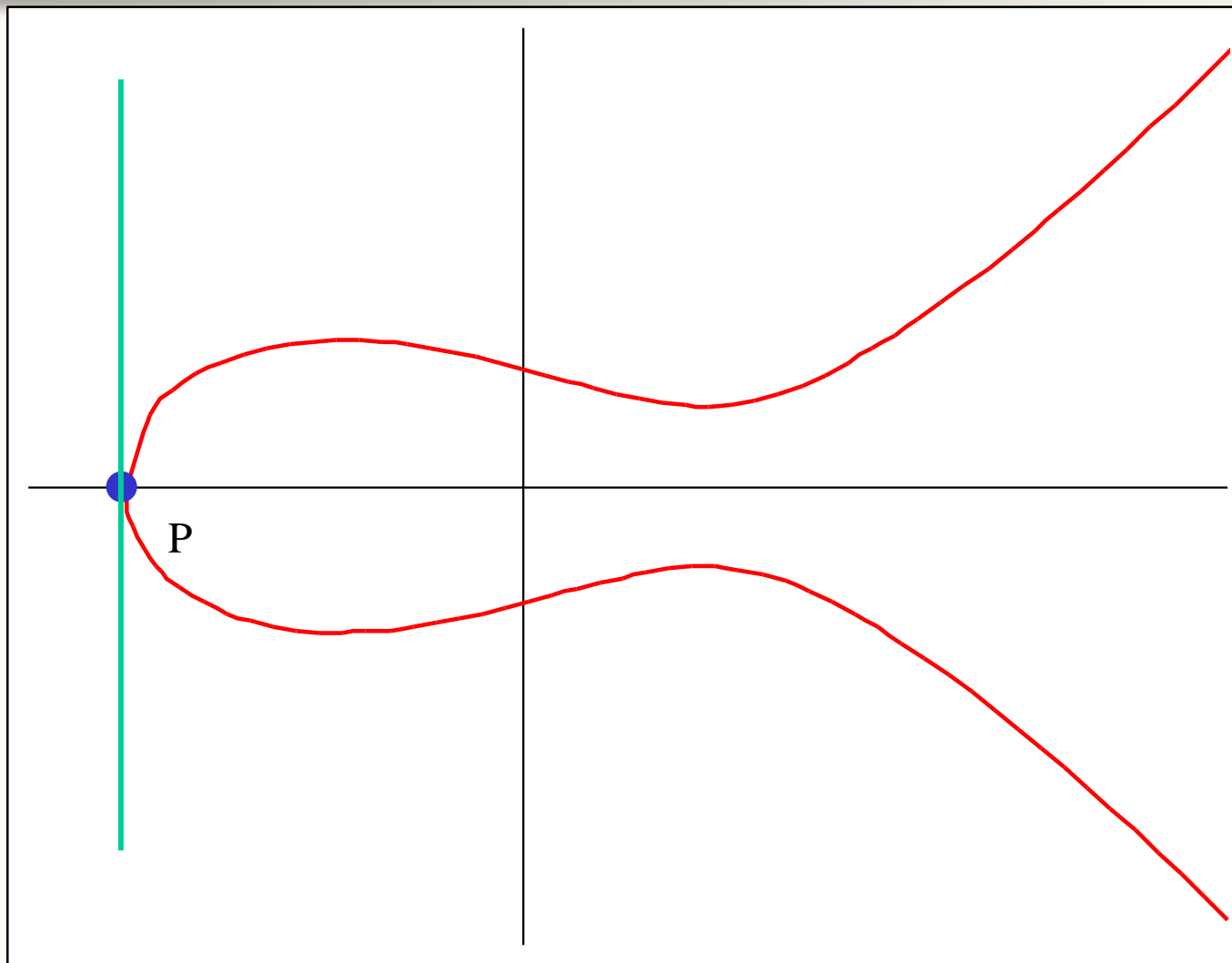
求点P的二倍



通过点P作曲线的切线，交曲线于另一点R，则 $2P = -R$



求点P的二倍的特例



若点P的切线的斜率是0，则 $2P=O$, $3P=P$, $4P=O$, $5P=P$



有限域上的椭圆曲线

定义：

对于曲线

$y^2 = x^3 + ax + b(\text{mod } p)$, a, b 为小于 p 的整数, 当 $4a^3 + 27b^2(\text{mod } p)$ 不为零时构成有限域 F_p 上的椭圆曲线群。记为 $E_p(a, b)$



有限域中椭圆曲线的运算

假设 E 是一个非奇异椭圆曲线。我们在 E 上定义一个二元运算，使其成为一个阿贝尔群。这个二元运算通常用加法表示。无穷远点 O 是单位元。

因此有 $P+O = O+P = P$ ，对于所有 $P \in E$ 。

假设 $P, Q \in E$ ，其中 $P = (x_P, y_P), Q = (x_Q, y_Q)$ 。

分三种情形讨论：

1) $x_P \neq x_Q$

2) $x_P = x_Q$ ，且 $y_P = y_Q$

3) $x_P = x_Q$ ，且 $y_P = -y_Q$



有限域上的两个点的加法

1) 若 $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$.

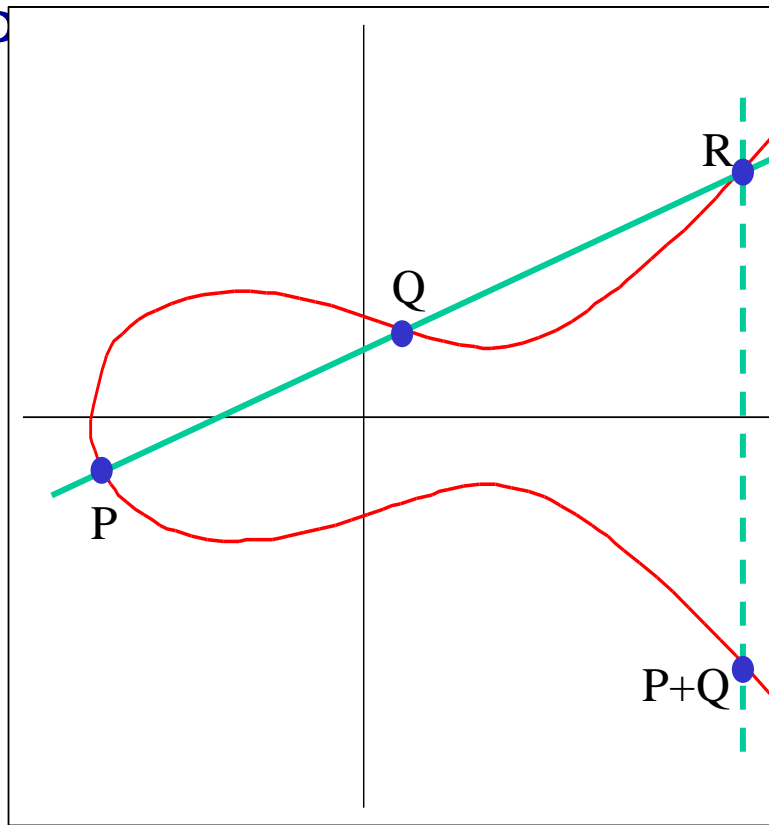
若 P 和 Q 是不同的点且 Q 不是 $-P$

$P + Q = -R$ 按如下方法计算:

$$\lambda = (y_P - y_Q) / (x_P - x_Q) \bmod p$$

$$x_R = \lambda^2 - x_P - x_Q \bmod p$$

$$y_R = -y_P + \lambda(x_P - x_R) \bmod p$$





例题

仍以 $E_{23}(1, 1)$ 为例，设 $P=(3, 10)$ ， $Q=(9, 7)$ ，求 $P+Q$

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

$$x_3 = 11^2 - 3 - 9 = 109 \equiv 17 \pmod{23}$$

$$y_3 = 11(3-17) - 10 = -164 \equiv 20 \pmod{23}$$

所以 $P+Q=(17, 20)$ ，仍为 $E_{23}(1, 1)$ 中的点。



求点P的2倍

2) 若 $P = (x_P, y_P)$

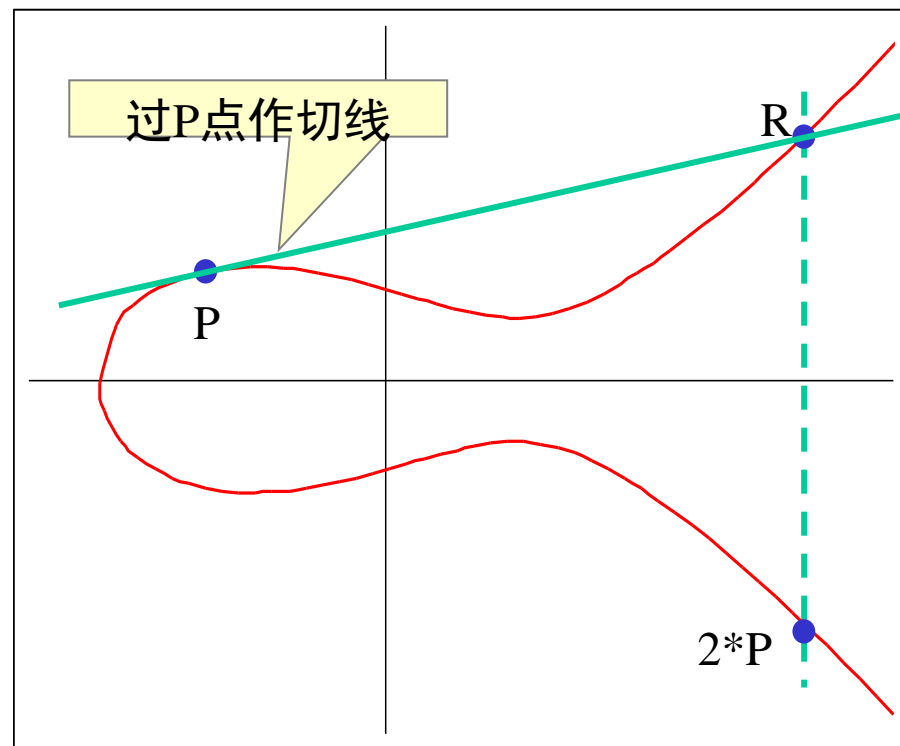
若 y_P 不为 0

$2P = -R$ 按如下方法计算:

$$\lambda = (3x_P^2 + a) / (2y_P) \mod p$$

$$x_R = \lambda^2 - 2x_P \mod p$$

$$y_R = -y_P + \lambda(x_P - x_R) \mod p$$





例题

仍以 $E_{23}(1, 1)$ 为例，设 $P=(3, 10)$ ，求 $2P$

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

$$x_3 = 6^2 - 3 - 3 = 30 \equiv 7 \pmod{23}$$

$$y_3 = 6(3 - 7) - 10 = -34 \equiv 12 \pmod{23}$$

所以 $2P=(7, 12)$ 。



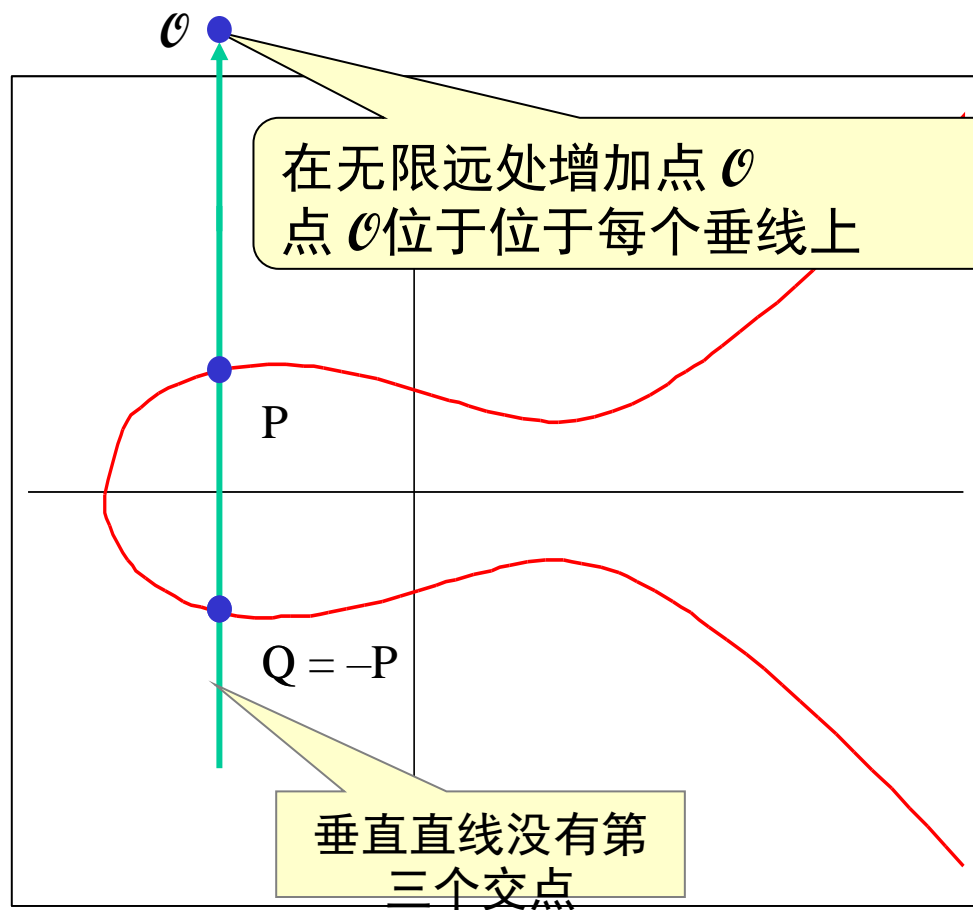
3) $x_P = x_Q$, 且 $y_P = -y_Q$

当 $x_P = x_Q, y_P = -y_Q$ 时
定义

$$(x, y) + (x, -y) = O,$$

$$(x, y) \in E$$

因此 (x, y) 与 $(x, -y)$ 是
关于椭圆曲线加法运
算互逆的。





有限域 F_p 上的椭圆曲线群

加法运算的下列性质应该是明确的:

1. 加法在集合 E 上是封闭的。
2. 加法是可交换的。
3. O 是加法的单位元。
4. E 上每一点有关于加法的逆元。
5. 要证明 $(E, +)$ 是阿贝尔群, 还须证明加法满足结合律。(此部分略)



有限域上的椭圆曲线的点的构造

1. 对于每一个 x ($0 \leq x < p$),
计算 $z = x^3 + ax + b \pmod{p}$;
2. 若 z 不是模 p 的平方根,
则没有具有 x 值的 $E_p(a, b)$ 点;
若 z 是模 p 的平方根,
则存在满足条件的两个点。



模素数的椭圆曲线

Example

设 E 是 \mathbb{Z}_{11} 上的椭圆曲线 $y^2 = x^3 + x + 6$ 。我们首先确定 E 的点。这可以通过对每个 $x \in \mathbb{Z}_{11}$, 计算 $x^3 + x + 6 \pmod{11}$, 试着解方程 (5) 求 y 。

对于给定的 x , 可以利用 Euler 判别法来测试是否 $z = x^3 + x + 6 \pmod{11}$ 是一个二次剩余。我们知道, 对素数 $p \equiv 3 \pmod{4}$, 有个现成的公式计算模 p 的剩余。利用这个公式, 二次剩余 z 的平方根是:

$$\pm z^{\frac{11+1}{4}} \pmod{11} = \pm z^3 \pmod{11}$$



椭圆曲线 $E_{11}(1,6)$ 的点的构造

即 $y^2 = x^3 + x + 6$ 在有限域 F_{11} 上的点的构造

x	$x^3 + x + 6 \pmod{11}$	是否为二次剩余	y
0	6	否	
1	8	否	
2	5	是	4, 7
3	3	是	5, 6
4	8	否	
5	4	是	2, 9
6	8	否	
7	4	是	2, 9
8	9	是	3, 8
9	7	否	
10	4	是	2, 9



椭圆曲线 $E_{23}(1,0)$ 的点的构造

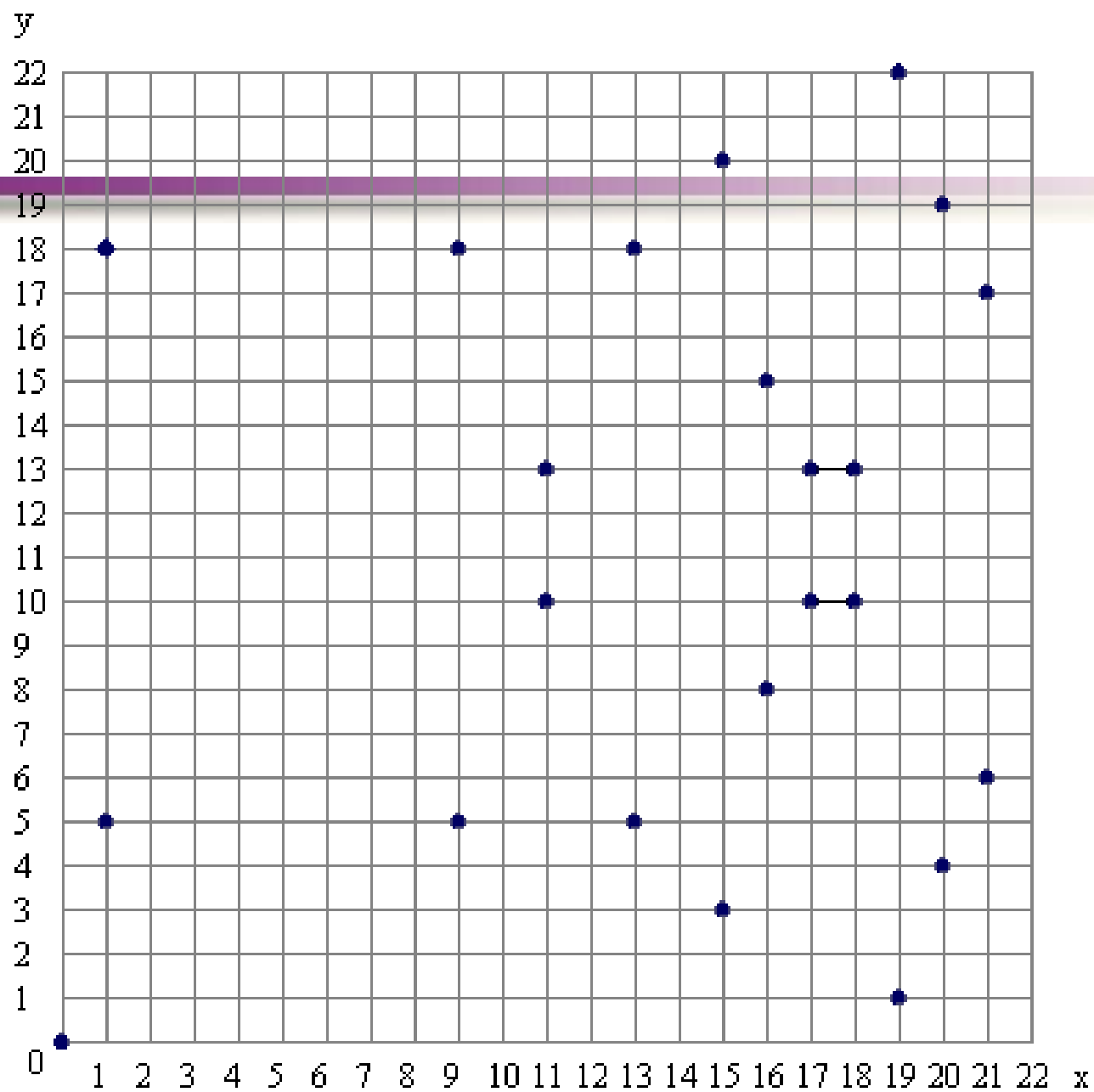
即 $y^2 = x^3 + x$ 在有限域 F_{23} 上的点的构造



椭圆曲线 $E_{23}(1,0)$ 的点的构造

满足条件的23个点是：

(0,0)	(1,5)	(1,18)	(9,5)	(9,18)
(11,10)	(11,13)	(13,5)	(13,18)	(15,3)
(15,20)	(16,8)	(16,15)	(17,10)	(17,13)
(18,10)	(18,13)	(19,1)	(19,22)	(20,4)
(20,19)	(21,6)	(21,17)		



Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}



椭圆曲线的离散对数问题

- 给定椭圆曲线上的点 P 和点 Q ，
寻找数 k 使得 $kP = Q$ ，
其中 k 称为 Q 基于 P 的离散对数。

- 例如：

对于椭圆曲线：

$$y^2 = x^3 + 9x + 17 \text{ over } F_{23},$$

求点 $Q = (4,5)$ 基于点 $P = (16,5)$ 的离散对数 k



椭圆曲线的离散对数问题的遍历求法

计算 kP , 直到的到 Q 为止

$$P = (16, 5) \quad 2P = (20, 20)$$

$$3P = (14, 14) \quad 4P = (19, 20)$$

$$5P = (13, 10) \quad 6P = (7, 3)$$

$$7P = (8, 7) \quad 8P = (12, 17)$$

$$9P = (4, 5)$$

离散对数为 $k = 9$.



群 Z_p^* 和 $E(F_p)$ 的比较

群	Z_p^*	$E(F_p)$
群元素	整数 $\{1, 2, \dots, p-1\}$	坐标属于 F_p 的椭圆曲线上的点的集合加上 O
群上的运算	模 p 乘法	点的加法
表示	元素: g, h 乘法: $g \cdot h$ 逆: g^{-1} 除法: g / h 幂: g^a	元素: P, Q 加法: $P+Q$ 逆: $-P$ 减法: $P-Q$ 乘: aP
离散对数问题	已知 $g \in Z_p^*$ 和 $h = g^a \bmod p$, 求 a	已知 $P \in E(Z_p)$ 和 $Q = aP$, 求 a



椭圆曲线上的Diffie-Hellman密钥交换

步骤：

1. Alice和Bob共享一个椭圆曲线 $E_q(a,b)$, 以及一个基点 G , $E_q(a,b)$ 的阶是 n .
2. Alice秘密随机选取正整数 $n_A < n$, 计算 $P_A = n_A \square G$
同时Bob选择随机数 $n_B < n$, 计算 $P_B = n_B \square G$
3. Alice发送 P_A 给Bob, 且Bob发送 P_B 给Alice
(Eve也知道 P_A 和 P_B)。
4. Alice计算 $K_A = n_A \square P_B$, Bob计算 $K_b = n_B \square P_A$; 则

$$K_A = n_A \square P_B = n_A \square (n_B \square G) = n_B \square (n_A \square G) = n_B \square P_A = K_B$$



ECElGamal加密体制

主要参数：

1. 选取有限域 F_p 、椭圆曲线 E_p 及基点 $P \in E(p)$
(这些参数可由一组用户公用).
2. 选取随机数 a , 计算 $Q=aP$.
3. Q 作为公钥, a 作为私钥



ECEIGamal加密体制的加/解密过程

➤ 加密:

Bob发送秘密消息 m 给Alice:

1. 将消息 m 转化为椭圆曲线上的点 M ;
2. 随机选取正整数 k .
3. 计算 kP , $kQ=(x, y)$, 若 $x=0$ 或 $y=0$ 返回第2步, 直到 $x \neq 0, y \neq 0$.

发送 $C=(kP, M+kQ)$ 给Alice.

➤ 解密:

收到密文 C 后,

Alice计算 $a(kP)=kQ$, 得到 M , 进而得到明文 m



举例

取 $p=751$, $E_p(-1,188)$,

即椭圆曲线为 $y^2 \equiv x^3 - x + 188$,

$E_p(-1,188)$ 的一个生成元是 $G=(0,376)$,

A的公开钥为 $P_A=(201,5)$ 。

假定B已将欲发往A的消息嵌入到椭圆曲线上的点 $P_m=(562,201)$,

B选取随机数 $k=386$, 由

$$kG=386(0,376)=(676,558), \quad P_m+kP_A=(562,201)+386(201,5)=(385,328),$$

得密文为 $\{(676,558),(385,328)\}$ 。



练习

已知ECElGamal加密算法中的椭圆曲线为 $T : (q=11, a=1, b=6, G=(2, 7))$

B的私钥为 $n_B=7$

1. 确定B的公钥

2. A要加密消息 $P_m=(10,9)$, 并且选择了随机数 $K=3$,

确定A发送给B的密文



SM2加密算法

- SM2 椭圆曲线公钥密码算法（简称 SM2）于 2010 年由国家密码管理局发布，2012 年成为密码行业标准，2016 年转化为国家标准
- SM2 算法的国家标准包括总则、数字签名算法、密钥交换协议、公钥加密算法、参数定义共 5 个部分
- 其中 SM2 数字签名算法于 2017 年被 ISO 采纳成为国际标准



SM2加密算法

- 系统参数: (p, a, b, G, n) 定义了椭圆曲线

$$E(\mathbb{F}_p) \triangleq \{(x, y) \in \mathbb{F}_p : y^2 = x^3 + ax + b\}$$

及一个 n 阶元 $G \in E(\mathbb{F}_p)$ 。其中, p, n 均为大素数, KDF 和 H 为公开的密钥派生算法和哈希算法 (均可由 SM3 加适当填充和编码规则来实例化), 细节略 (可参考标准文档)。

- 公钥: 私钥 $d \xleftarrow{\$} [1, n-2]$, 公钥 $P \leftarrow dG$
- 加密算法: 对消息 m 的加密为密文 $C = (C_1, C_2, C_3)$, 计算如下:
 - $k \xleftarrow{\$} [1, n-1]$, $C_1 \leftarrow kG \triangleq (x_1, y_1)$, $T \leftarrow kP \triangleq (x_2, y_2)$
 - $e = \text{KDF}(x_2 \| y_2, |m|)$, $C_2 \leftarrow m \oplus e$, $C_3 \leftarrow H(x_2 \| m \| y_2)$
- 解密算法: 请同学们思考



公钥密码系统中ECC与RSA的对比

- *RSA*算法的特点之一是数学原理简单、在工程应用中比较易于实现，但它的单位安全强度相对较低。
- 一般数域筛 (*NFS*) 方法去破译和攻击*RSA*算法，它的破译或求解难度是亚指数级的。
- *ECC*算法的数学理论非常深奥和复杂，在工程应用中比较难于实现，但它的单位安全强度相对较高。
- *Pollard rho*方法去破译和攻击*ECC*算法，它的破译或求解难度基本上是指数级的。



- **Elliptic curve logarithm** using Pollard's rho algorithm

Key size: p	MIPS-year
150	3.8×10^{10}
205	7.1×10^{18}
234	1.6×10^{28}

- **Integer factorization** using generalized number field sieve

Key size: n	MIPS-year
512	3×10^4
768	2×10^8
1024	3×10^{11}
1280	1×10^{14}
1536	3×10^{16}
2048	3×10^{20}

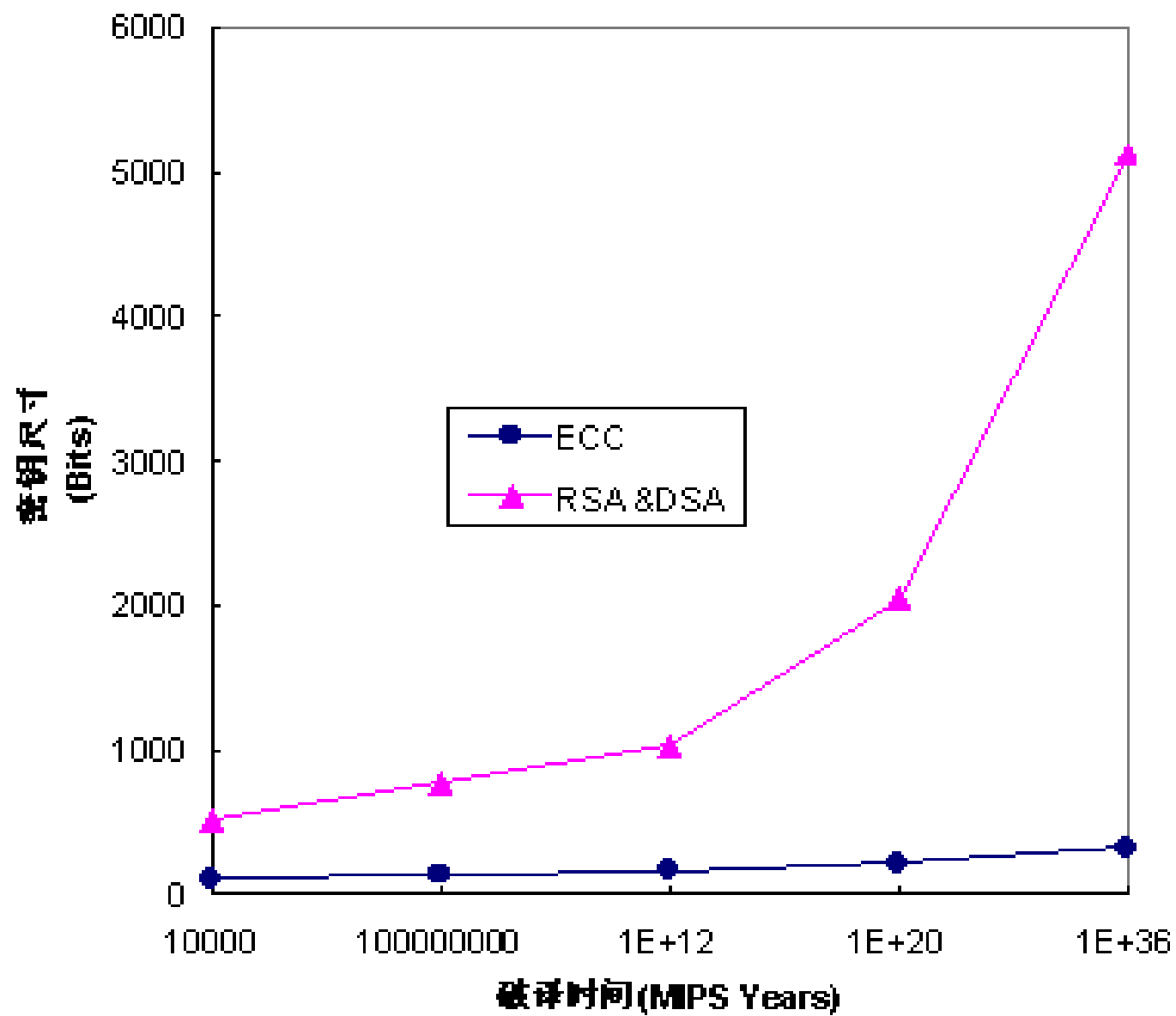




表1. RSA和ECC安全模长的比较

攻破时间	RSA/DSA	ECC密钥长度	RSA/ECC
MIPS年	密钥长度		密钥长度比
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1



表2. RSA和ECC速度比较

功能	Security Builder 1.2	BSAFE 3.0
	163位ECC (ms)	1,024位RSA (ms)
密钥对生成	3.8	4,708.3
签名	2.1 (ECNRA)	228.4
	3.0 (ECDSA)	
认证	9.9 (ECNRA)	12.7
	10.7 (ECDSA)	
Diffie--Hellman 密钥交换	7.3	1,654.0



谢谢！