椭圆曲线密码体制(Elliptic Curve Cryptography，ECC)

1976 年,美国斯坦福大学的迪菲（Diffie）和赫尔曼(Hellman)在论文《New Direction in Cryptography》首次提出公开密钥算法思想。即一个具体用户可以将自己设计的加密密钥(公钥)和算法公诸于众，而只保密解密密钥(私钥)。任何人利用公钥和算法向该用户发送的加密信息，该用户均可以利用私钥解密即可获得原始信息。

1978 年，MIT 教授 Ronald Rivest，A .Shamir 和 Leonard M.Adleman 提出 RSA 公钥密码体制，后续很多公钥密码体制相继被提出。

目前应用较为广泛的公钥密码体制主要有 3 个：

(1)基于大整数因子分解问题的 RSA 公钥密码体制；

(2)基于有限域乘法群上的离散对数问题的 ElGamal 公钥密码体制；

(3)基于椭圆曲线上离散对数问题的 ECC。

基于 RSA，ElGamal 算法广泛应用，计算机处理能力的不断提高,引出新的挑战：

(1)安全性的需求：对 RSA 密钥长度的要求越来越长，512bit~1024bit；

(2)计算效率：密钥长度增加导致，RSA 算法计算速度缓慢的。

椭圆曲线密码体制（ECC，Elliptic Curve Cryptosystem）实现了密钥效率的重大突破，大有取代 RSA 之势。它也成为迄今被实践证明安全、有效、应用较广的 3 个公钥密码体制之一，以高效著称。

一、椭圆曲线

1.椭圆曲线的定义

椭圆曲线是指由魏尔斯特拉斯(Weierstrass)方程：

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

所确定的平面曲线，其中 a,b,c,d,e 属于一个域，可以是有理数域，复数域也可以有限域 GF(p)，椭圆曲线是 E 上所有点 (x,y) 的集合，外加一个无限远点 O (椭圆曲线 E 有一个特殊的点，记为 O，它并不在 E 上，此点称为无限远点)

椭圆曲线 E 满足 $\Delta \neq 0$，Δ 是判别式

$$\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^3 + 9d_2 d_4 d_6$$

$$d_2 = a^2 + 4c \quad d_4 = 2d + ab$$

$$d_6 = b^2 + 4e \quad d_8 = a^2 e + 4ce - abd + cb^2 - d^2$$

条件 $\Delta \neq 0$ 是确保椭圆曲线是“光滑的”，即曲线上的每个点都必须是非奇异的（光滑的），即偏导数 $f_x(,x,y)$，$f_y(,x,y)$ 不为 0。

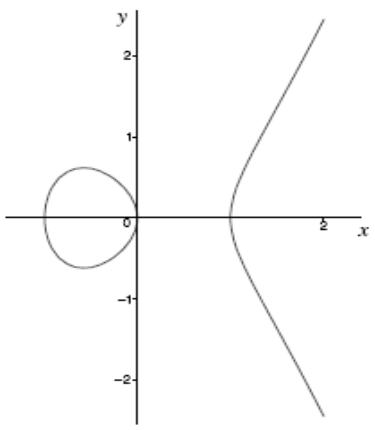
2.有限域 GF(p)上的椭圆曲线

在密码学中，普遍采用有限域 GF(p)上，下列形式的椭圆曲线：

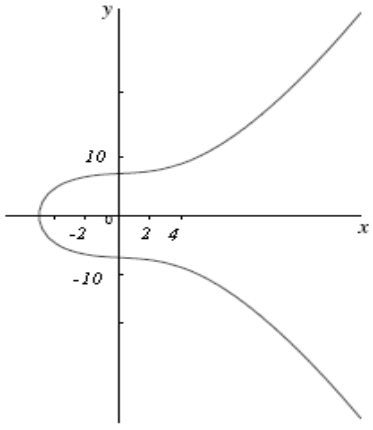
$E: y^2 \equiv x^3 + ax + b \bmod p$，通常表示为 $E_p(a,b)$

系数 $a,b \in \mathrm{GF}(p)$，$\Delta = -16(4a^3 + 27b^2) \neq 0$，$\Delta \neq 0$ 是 $y^2 = x^3 + ax + b$ 有三个解的充要条件且 $\Delta \neq 0$ 保证曲线非奇异。

$y^2 = x^3 - 4x$ 的图像　　(关于 X 轴对称)　　$y^2 = x^3 + 73$ 的图像



(a)



(b)

$E: y^2 \equiv x^3 + ax + b \bmod p$ 中， p 为一个大素数，$a,b,x,y \in \mathrm{GF}(p)$，即从 $\{0,1,\cdots,p-1\}$ 上取值，$E_p(a,b)$ 只有有限个点 N (称为椭圆曲线的阶，包括无限远点 O)， N 越大安全性越高。

有限域 GF(p)上椭圆曲线 E 上点的个数 N，一般满足 $|N-(p+1)| \leq 2\sqrt{p}$ 。

3.椭圆群的构造

$E_p(a,b)$ 的生成过程如下：

(1) 对 $x = 0,1,\cdots,p-1$，计算 $x^3 + ax + b \bmod p$；

(2) 根据 $x^3 + ax + b \bmod p$ 的结果确定是否有一个模 p 的平方根：

如果有，则有两个平方根 y 和 $-y$ (GF(p)中 $-y = p - y$)，从而点 (x,y) 和 $(x,p-y)$ 都是 $E_p(a,b)$ 的点。如果 $y = 0$，则只有 $(x,0)$ 一个点)

如果没有，则 $E_p(a,b)$ 中没有以该结果相应的 x 为横坐标的点。

例如： $GF(23)$ 上的一个椭圆曲线为：$y^2 \equiv x^3 + x + 1 \bmod 23$ (即 p=23，a=1，b=1)，求该椭圆曲线在 $GF(23)$ 上的整数点集。

解：取 $x = 0,1,\cdots,22$ 分别计算 $x^3 + x + 1 \bmod 23$：

$x = 0$ 时， $y^2 \equiv 0^3 + 0 + 1 \bmod 23 \equiv 1 \bmod 23 \Rightarrow y = 1$，所以 $y = p - 1 = 23 - 1 = 22$ 也满足，故 $(0,1)$， $(0,22)$ 为椭圆曲线上的点。

$x = 1$ 时， $y^2 \equiv 3 \bmod 23 \equiv 49 \bmod 23 \Rightarrow y = 7$，所以 $y = p - 1 = 23 - 7 = 16$ 也满足，故 $(1,7)$，$(1,16)$ 为椭圆曲线上的点。

$x = 2$ 时， $y^2 \equiv 119 \bmod 23$，没有满足条件的 y。

$x = 3$ 时， $y^2 \equiv 8 \bmod 23 \equiv 100 \bmod 23 \Rightarrow y = 10$，所以 $y = p - 1 = 23 - 10 = 13$ 也满足，故 $(3,10)$， $(3,13)$ 为椭圆曲线上的点。

$x = 4$ 时， $y^2 \equiv 0 \bmod 23$，只有 $(4,0)$ 为椭圆曲线上的点。

同理，可求出椭圆曲线上其他的点，$GF(23)$ 上共有 28 个解(包括无穷远点 O)。

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

4.椭圆曲线在模 p 下的 Abel 群

椭圆曲线上的点集合 $E_p(a,b)$ 对于如下定义的加法规则构成一个 Abel 群。

加法规则：

(1) $O+O=O$；

(2)对于所有的点 $P(x,y)\in E_p(a,b)$，有 $P+O=O+P=P$；

(3)对于所有的点 $P(x,y)\in E_p(a,b)$，有 $P+(-P)=O$，即点 P 的逆为 $-P=(x,-y)$；

(4)点 $P(x_1,y_1)\in E_p(a,b)$，$Q(x_2,y_2)\in E_p(a,b)$，且 $P\neq -Q$，则 $P+Q=R=(x_3,y_3)\in E_p(a,b)$

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

(5) 倍点规则：$P(x_1,y_1)\in E_p(a,b)$，$P=Q$，$P+Q=P+P=2P=R=(x_3,y_3)\in E_p(a,b)$

其中：$\begin{cases}x_3=l^2-x_1-x_2\\ y_3=l(x_1-x_3)-y_1\end{cases}$，$l=\dfrac{3x_1^2+a}{2y_1}$

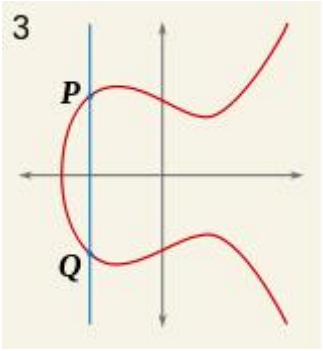
(6))对于所有的点 P,Q，满足加法交换律，即 $P+Q=Q+P$；

(7) 对于所有的点 P,Q,R，满足加法结合律，即 $P+(Q+R)=(P+Q)+R$；

以上加法规则体现在椭圆曲线图形上的含义：

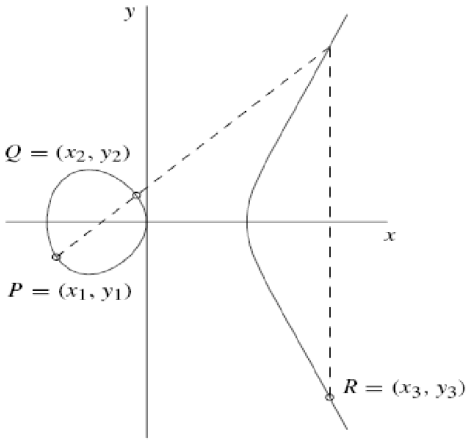
(1) O 加法单位元；

(2) $P=(x,y)$，$Q=(x,-y)$，P,Q 两点确定的直线垂直于 X 轴，它与曲线相交于无穷远点 O，因此 $Q=-P$



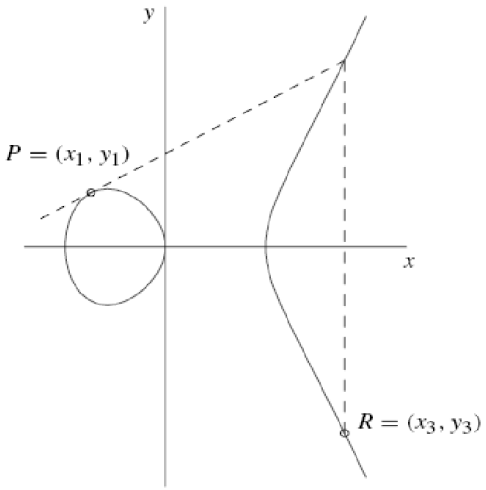
$P+(-P)=O$

(3) $P(x_1,y_1)\in E_p(a,b)$，$Q(x_2,y_2)\in E_p(a,b)$，且 $P\neq -Q$，$l=\dfrac{y_2-y_1}{x_2-x_1}$ 为直线 PQ 的斜率，直线与椭圆曲线相交于第三点为 $-R$，则 $P+Q=R=(x_3,y_3)\in E_p(a,b)$



(a) 相加： $P+Q=R$.

(4) $P(x_1,y_1)\in E_p(a,b)$，在 P 作椭圆曲线的切点，切线与曲线相交于第二点为 R 关于 X 轴的对称点 $-R$， $P+P=2P=R=(x_3,y_3)\in E_p(a,b)$



(b) 倍点： $P+P=R.$

乘法规则：

(1)如果 k 为整数，对于所有的点 $P(x,y)\in E_p(a,b)$，有

$$kP=P+P+\cdots+P\ (\ k\text{ 个 }P\text{ 相加}),\ kP=(k-1)P+P$$

(1)如果 k 和 s 为整数，对于所有的点 $P(x,y)\in E_p(a,b)$，有

$$(s+k)P=sP+kP, s\left(kP\right)=(sk)P$$

例如： $GF(23)$ 上的一个椭圆曲线为： $y^2\equiv x^3-4x+1 \bmod 23$，令 $P=(4,7),Q=(10,31)$，求(1) $R=(x_3,y_3)=P+Q$

(2) $2P$

(3) $3P$

解：(1)计算斜率 $l=\dfrac{y_2-y_1}{x_2-x_1}=\dfrac{31-7}{10-6}=\dfrac{24}{6}\equiv 24\times 4 \bmod 23=4$；

$$\begin{cases}x_3=l^{\,2}-x_1-x_2=4^2-4-10=2\equiv 2 \bmod 23=2\\ y_3=l\,(x_1-x_3)-y_1=4\times(4-2)-7=1\equiv 1 \bmod 23=1\end{cases}$$ 所以 $R=(2,1)$

(2) $l=\dfrac{3x_1^2+a}{2y_1}=\dfrac{3\times 4^2-4}{2\times 7}=\dfrac{44}{14}\equiv\dfrac{21}{14} \bmod 23\equiv\dfrac{3}{2} \bmod 23\equiv 36 \bmod 23=13$

$$\begin{cases}x_3=l^{\,2}-2x_1=13^2-8=161 \bmod 23=0\\ y_3=l\,(x_1-x_3)-y_1=13\times 4-7=45\equiv 45 \bmod 23=22\end{cases}$$ 所以 $R=(0,22)$

(3) $R=(0,22)$,

二、椭圆曲线密码体制

在椭圆曲线构成 Abel 群上考虑方程 $Q=kP$，其中 $P\in E_p(a,b)$ 且为生成元，Q 为 P 的倍点，即存在正整数 k（小于 P），则由 k 和 P 易求出 Q，

但由 P、Q 求 k 是困难的，这就是椭圆曲线上的离散对数问题，可设计公钥密码体制。

例如，对基于 $GF(23)$的椭圆群 $y^2=x^3+ax+b$，求 $Q=(x_1,y_1)$ 对于 $P=(x_1,y_1)$ 的离散对数，最直接的方法就是计算 P 的倍数，直到找到 k。若 $P=(x,y),2P=(x_2,y_2),3P=(x_3,y_3),\cdots,9P=(x_1,y_1)=Q$，因此，$Q$ 关于 P 的离散对数是 9，对于大素数构成的群 E，这样计算离散对数是不现实的。

1.密钥生成：

椭圆曲线公私钥对，其步骤如下：

（1）选择一个椭圆曲线 E：$y^2 \equiv x^3 + ax + b(\mathrm{mod}\ p)$，构造一个椭圆群 $E_p(a,b)$；

（2）在 $E_p(a,b)$ 中挑选生成元点 $G=(x_0,y_0)$，G 应使得满足 $nG=O$ 的最小的 n 是一个非常大的素数（N 表示椭圆群 $E_p(a,b)$ 的元素个数，n 是 N 的素因子）；

（3）选择一个小于整数 $n_B < n$ 作为其私钥，公钥 $P_B = n_B G$，则公钥为 (E,n,G,P_B)，私钥为 n_B。

2.加密过程

（1）选择明文消息 $m < p$，并在椭圆群 $E_p(a,b)$ 中选择一点 $P_t=(x_t,y_t)$；

（2）选取一个随机数 k 满足 $1 \le k \le n-1$，计算点 $P_1 : P_1=(x_1,y_1)=kG$，$P_2=(x_2,y_2)=kP_B$；

（3）计算密文 $C = mx_t + y_t$；

（4）最终的加密数据 $C_m=\{\mathrm{P_1},\mathrm{P_t}+\mathrm{P_2},\mathrm{C}\}$。

3.解密过程

（1）用自己的私钥 n_B 解密 $C_m=\{\mathrm{P_1},\mathrm{P_t}+\mathrm{P_2},\mathrm{C}\}$：

$$P_t + P_2 - n_B P_1 = P_t + k(n_B G) - n_B(kG) = P_t$$

（2）计算 $m=(C-y_t)/x_t \bmod p$，得明文 m。

攻击者若想由密文 C 得到明文 m，就必须知道 k 或 n_B。但一直 kG 和 P_B 求得 k 或 n_B，都必须去解决椭圆曲线上的离散对数问题，因此，其加解密过程是安全的。

椭圆曲线公钥密码体制总结

公钥	E：椭圆曲线　　n:非常大的素数（N 的素因子） G：椭圆曲线 $E_p(a,b)$ 的生成元，$nG=O$　　$P_B : P_B = n_B G$
私钥	$n_B : P_B = n_B G$
加密算法	k、$P_t(x_t,y_t)$：随机选择　　m：明文消息 $P_1 : P_1=(x_1,y_1)=kG$　　$P_2 : P_2=(x_2,y_2)=kP_B$ $C : C = mx_t + y_t$ 加密数据：$C_m=(kG, P_t+kP_B, C)$
解密算法	$P_t + kP_B - n_B(kG) = P_t + k(n_B G) - n_B(kG) = P_t = (x_t,y_t)$ 明文：$m=(C-y_t)/x_t$

例：取 p=23，$E_p=(13,22)$，即椭圆密码曲线为 $y^2 \equiv x^3 + 13x + 22(\mathrm{mod}\,23)$，$E_p=(13,22)$ 的一个生成元是 $G=(10,5)$，B 的私钥 $n_B=7$。假设 A 欲将发往 B 的消息 m=15 进行加密，椭圆曲线上的点 $P_t=(11,1)$，求其加解密过程。

密钥生成：由 $P_B=7G=(17,21)$，得 B 的公钥为 $\{\mathrm{E}:\mathrm{y}^2 \equiv \mathrm{x}^3+13\mathrm{x}+22(\mathrm{mod}23),\mathrm{G}=(10,5),\mathrm{P_B}=(17,21)\}$，私钥为 $n_B=7$。

加密：A 选取随机数 k=13，则得

$$P_1 = kG = 13(10,5) = (16,5)$$
$$P_2 = kP_B = 13(17,21) = (20,18)$$
$$P_t + kP_B = (11,1) + (20,18) = (18,19)$$
$$C = mx_t + y_t = 15 \times 11 + 1 = 5$$

得加密数据为 $C_m=\{(16,5),(18,19),5\}$。

解密：B 接收到密文 C_m，使用自己的私钥 $n_B = 7$ 解密消息，故

$P_t = P_t + k(n_B G) - n_B(kG) = P_t + kP_B - n_B(kG) = (18,19) - 7(16,5) = (11,1)$

$m = (C - y_t)/x_t = (5-1)/11 = 15$（上面的运算都是在 *mod* 23 下进行的）。

ECC 安全性分析(略讲)

1985 年，Koblitz 和 Miller 将椭圆曲线引入密码学，提出了基于有限域 GF(p)的椭圆曲线上的点集构成群，在这个群上定义离散对数系统并构造出基于离散对数的一类公钥密码体制，即基于椭圆曲线的离散密码体制，其安全性基于椭圆曲线上离散对数问题的安全性。基于椭圆曲线上离散对数问题被公认要比整数分解问题（RSA 密码体制的基础）和模 p 离散对数问题（ElGamal 密码体制的基础）难解得多，因此，ECC 仅需要较小的密钥长度就可以提供与 RSA 和 ElGamal 相当的安全性。

要保证 ECC 的安全性，就要使所选取的曲线能够抵抗各种已知的攻击，这就涉及选取安全椭圆曲线的问题。用于建立密码体制的椭圆曲线的主要参数有 p, a, b, P, n 和 h，其中 p 是域的大小，取值为素数（模数）或 2 的幂；a, b 是方程中的系数，取值于 GF(p)；P 为基数（生成元）；n 为点 P 的阶；h 是椭圆曲线上所有点的个数 N 除以 n 的结果。为了使所建立的密码体制有较好的安全性，这些参数的选取应满足如下条件：

（1） p 越大越安全，但越大，计算速度会变慢，160 位可以满足目前的安全要求；

（2）为了防止 Pohlig-Hellman 方法攻击，n 为大素数（$n > 2^{160}$），对于固定的有限域 GF(p)，n 应当尽可能大；

（3）因为 $x^3 + ax + b$ 无重复因子才可基于椭圆曲线 $E_p(a,b)$ 定义群，所以要求

$4a^3 + 27b^2 \neq 0 (\mathrm{mod}\ p)$；

（4）为了防止小步——大步攻击，要保证 P 的阶 n 足够大，要求 $h \leq 4$；

（5）为了防止 MOV 规约法和 Smart 法，不能选取超奇异椭圆曲线和异常椭圆曲线等两类特殊曲线。

椭圆曲线的离散对数问题被公认为要比整数因子分解问题和基于有限域的离散对数问题难解得多，所以，它的密钥长度大大地减小，160 位的 ECC 密钥就可以达到 RSA 密钥 1024 位的安全水平，这使得 ECC 成为目前已知的公钥密码体制中安全强度最高的体制之一。

ECC 优势

	RSA	ElGamal	ECC
数论基础	欧拉定理	离散对数	离散对数
安全性基础	大素数的因数分解的困难性	有限域上离散对数问题的困难性	椭圆曲线离散对数问题的困难性
当前安全密钥长度	1024 位	1024 位	160 位
用途	加密、数字签名	加密、数字签名	加密、数字签名
是否申请专利	是	否	否