网络空间安全数学基础（5）

网络空间安全学院

高莹

2020年 10 月 28日

回顾：本原根定理

本原根定理

设p为素数，$\mathbb{F}_p^* = \mathbb{F}_p - \{0\}$,则存在一个元素$g \in \mathbb{F}_p^*$使得其他所有非零元素都可以表示成$g$的幂.即

$$\mathbb{F}_p^* = \{1, g, g^2, \cdots, g^{p-2}\}$$

具有这种性质的元素称为$\mathbb{F}_p$的本原元，或者称其为$\mathbb{F}_p^*$的生成元，或叫模p的原根.

回顾：离散对数（DLP）问题

DLP问题

设g为模p的原根，$0 < h < p$为整数，DLP问题即求解指数x满足

$$g^x \equiv h \, (mod \, p)$$

x称为以g为底的h的对数，记为$log_g(h)$.

回顾：离散对数（DLP）问题

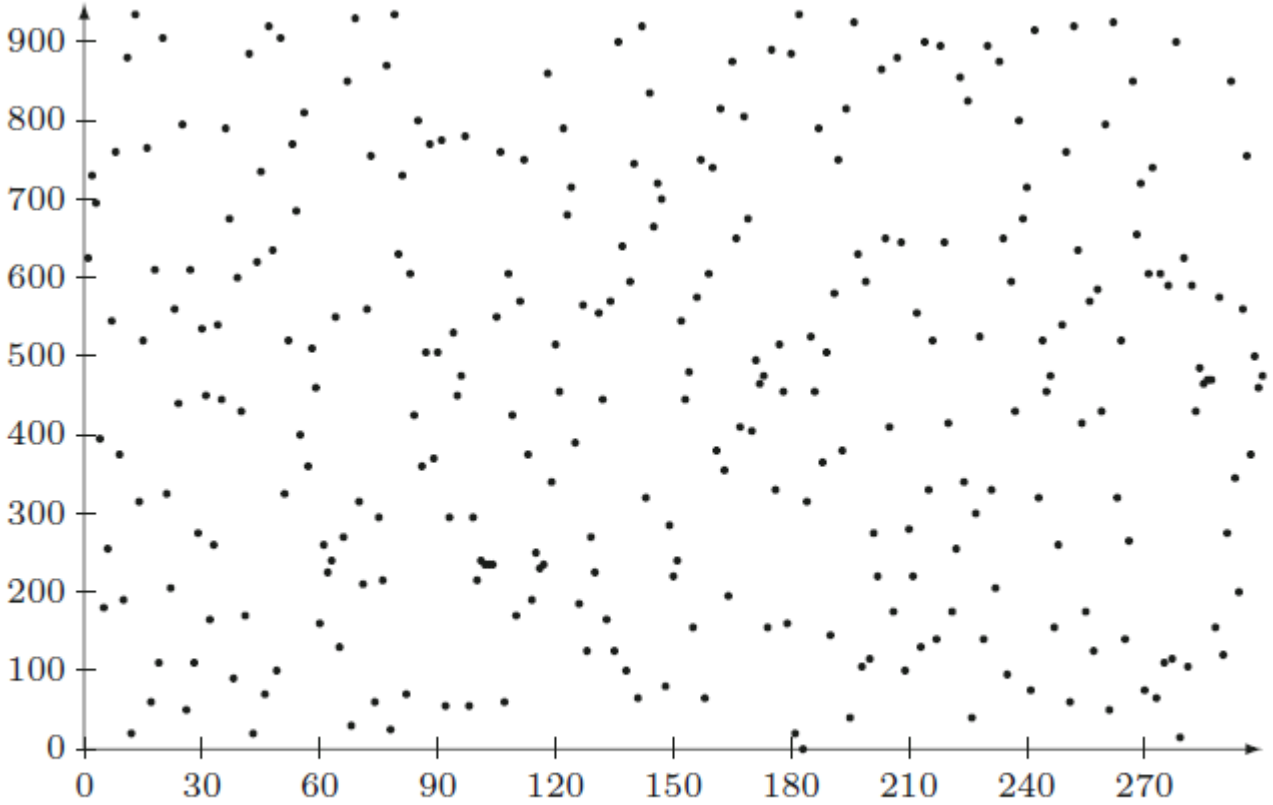


Figure 2.2: Powers 627^i mod 941 for $i = 1, 2, 3, \ldots$

回顾：ElGamal公钥密码算法

ElGamal公钥密码算法安全性依赖于有限域上离散对数的困难性

密钥生成

选择素数p，两个随机数g,x，使得g,x都小于p,计算

$$p \equiv g^x (mod\ p).$$

公钥是y,g,p

私钥是x

加解密

加密：可随机选择k（但ElGamal签名算法中k需要与p-1互素）

$$a(\text{密文}) \equiv g^k\ (mod\ p)$$

$$b(\text{密文}) \equiv y^k\, m\ (mod\ p)$$

解密：$m(\text{明文}) = b/a^x (mod\ p)$

ElGamal密码体制描述

Public parameter creation	
A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.	
Alice	**Bob**
Key creation	
Choose private key $1 \leq a \leq p-1$. Compute $A = g^a \pmod{p}$. Publish the public key A.	
Encryption	
	Choose plaintext m. Choose random element k. Use Alice's public key A to compute $c_1 = g^k \pmod{p}$ and $c_2 = mA^k \pmod{p}$. Send ciphertext (c_1, c_2) to Alice.
Decryption	
Compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$. This quantity is equal to m.	

椭圆曲线的发现

椭圆曲线是由Neil Koblitz和Victor Miller两位学者分别于1985年首先独立提出。椭圆曲线具有的性质：

- 有限域上椭圆曲线在点加运算下构成有限交换群，且其阶与基域规模相近；
- 类似于有限域乘法群中的乘幂运算，椭圆曲线多倍点运算构成一个单向函数。

密钥强度对比

RSA与ElGamal系统中需要使用长度为1024位的模数，才能达到足够的安全等级。而ECC只需使用长度为160位的模数即可，且传送密文或签章所需频宽较少，并已正式列入IEEE 1363标准，使ECC成为构造公开密钥密码体制一个有力的工具

RSA密钥强度（比特）	椭圆曲线密钥强度（比特）	攻破时间
768	132	2009. 12
829	140左右	2019. 12
1024	160	
2048	210	

椭圆曲线的定义

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。

椭圆曲线的方程：$y^2 + axy + by = x^3 + cx^2 + dx + e$，其中a,b,c,d,e是满足某些条件的实数。

椭圆曲线有一个特殊的点，记为O，它并不在椭圆曲线E上，此点称为无穷远点。

一条椭圆曲线E(x,y)是由全体解(x,y)再加上一个无穷远点构成的集合。

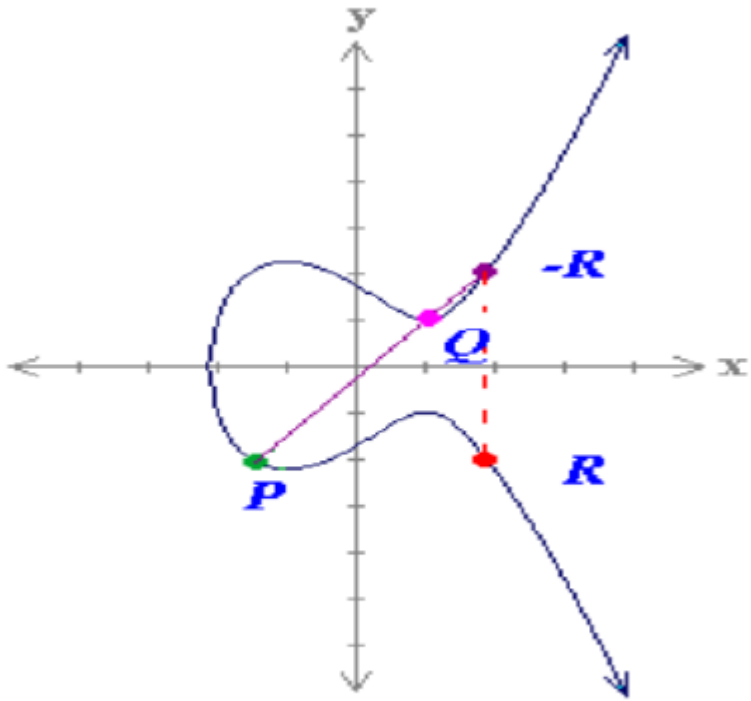
$$E = \{(x, y) | Y^2 + aXY + bY = X^3 + cX^2 + dX + e\} \cup \{O\}$$

实数域上椭圆曲线的定义

在实数域上，椭圆曲线可定义成 $E : y^2 = x^3 + ax + b$
若方程式没有重复的因式或$4a^3 + 27b^2 \neq 0$，E（a,b）是一条非奇异椭圆曲线。
否则，E（a,b）是一条奇异椭圆曲线（某些数的逆元素(inverse)将不存在）。

椭圆曲线上的加法

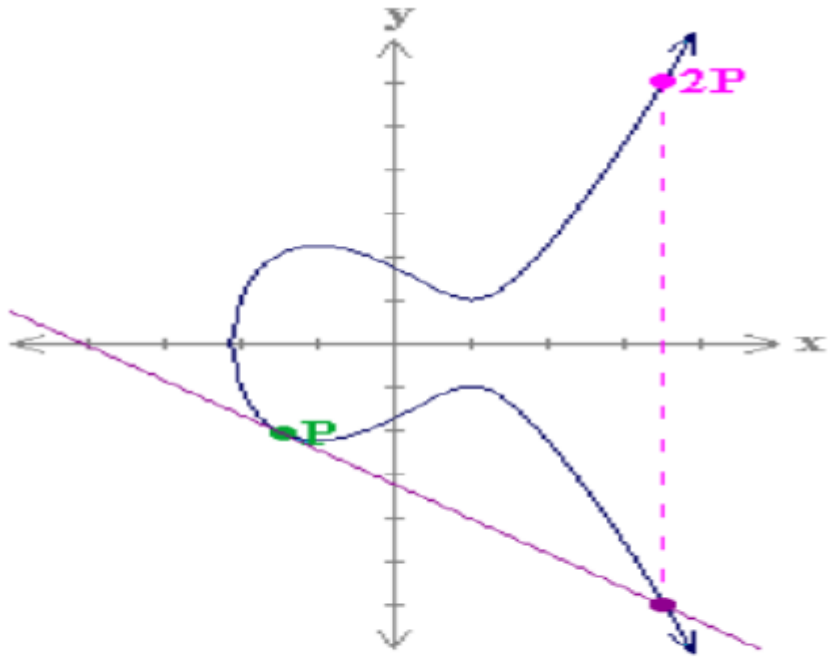
两异点相加：假设P和Q是椭圆曲线上两个相异的点，而且P不等于-Q 。若P+Q=R ，则点R是经过P、Q两点的直线与椭圆曲线相交之唯一交点的负点。



$y^2 = x^3 - 3x + 3$

椭圆曲线上的加法

双倍的点：令P +P=2P ，则点2P是经过P的切线与椭圆曲线相交之唯一交点的负点。



$y^2 = x^3 - 3x + 3$

椭圆曲线的定义

定义.

一条椭圆曲线E是一个Weierstrass方程

$$E : Y^2 = X^3 + AX^2 + B,$$

的一组解加上一个额外的点O，A,B两个常数满足：

$$4A^3 + 27B^2 \neq 0.$$

椭圆曲线的定义

定理.

E是一条椭圆曲线，则E上加法有如下性质(E上的点组成一个交换群)：

- P+O=O+P=P, for all $P \in E$ [Identity]
- P+(-P)=O, for all $P \in E$ [Inverse]
- (P+Q)+R=P+(Q+R), for all $P, Q, R \in E$ [Associate]
- P+Q=Q+P , for all $P, Q \in E$ [Commutative]

椭圆曲线的定义

定理(椭圆曲线加法定理).

$$E\text{æ}Y^2 = X^3 + AX + B$$

是一条椭圆曲线，P_1和P_2是E上的点。
(a)如果$P_1 = O$,则$P_1 + P_2 = P_2$.
(b)否则$P_2 = O$,则$P_1 + P_2 = P_1$.
(c)否则，记$P_1 = (x_1, y_1), P_2 = (x_2, y_2)$.
(d)若$x_1 = x_2, y_1 = -y_2$,则$P_1 + P_2 = O$
(e)否则定义λ:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, P_1 \neq P_2, \\ \dfrac{3x_1^2 + A}{2y_1}, P_1 = P_2 \end{cases} \tag{1}$$

然后让$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1$.
$P_1 + P_2 = (x_3, y_3)$

有限域上椭圆曲线的定义

定义.

$p \geq 3$为一个素数，一条在域$\mathbb{F}_p$上的椭圆曲线为如下形式的等式

$$E : Y^2 = X^3 + AX + B,\ A, B \in \mathbb{F}_p,\ 4A^3 + 27B^2 \neq 0$$

E上所有点的集合为：

$$E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p,\ y^2 = x^3 + Ax + B\} \cup O$$

有限域上的椭圆曲线可以定义在任意有限域上，因二元域上的情形比较复杂，放在后面讲

椭圆曲线在模p下的运算规则

加法规则：

- 对所有的点$P \in E(\mathbb{F}_p)$, $P + O = O + P, P + (-P) = O$
- 记$P_1 = (x_1, y_1), P_2 = (x_2, y_2), P \neq -Q$,则$P + Q = (x_3, y_3)$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, P_1 \neq P_2, \\ \dfrac{3x_1^2 + A}{2y_1}, P_1 = P_2 \end{cases} \tag{2}$$

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1.$$

如果$s, t \in \mathbb{F}_p$，则对所有$P \in E(\mathbb{F}_p)$,

$$(s + t)P = sP + tP$$

椭圆曲线在模p下的运算规则举例

例1.

有限域$\mathbb{F}_{23}$之下，点P=(0,1)是椭圆曲线

$$E : y^2 = x^3 + 12x + 1$$

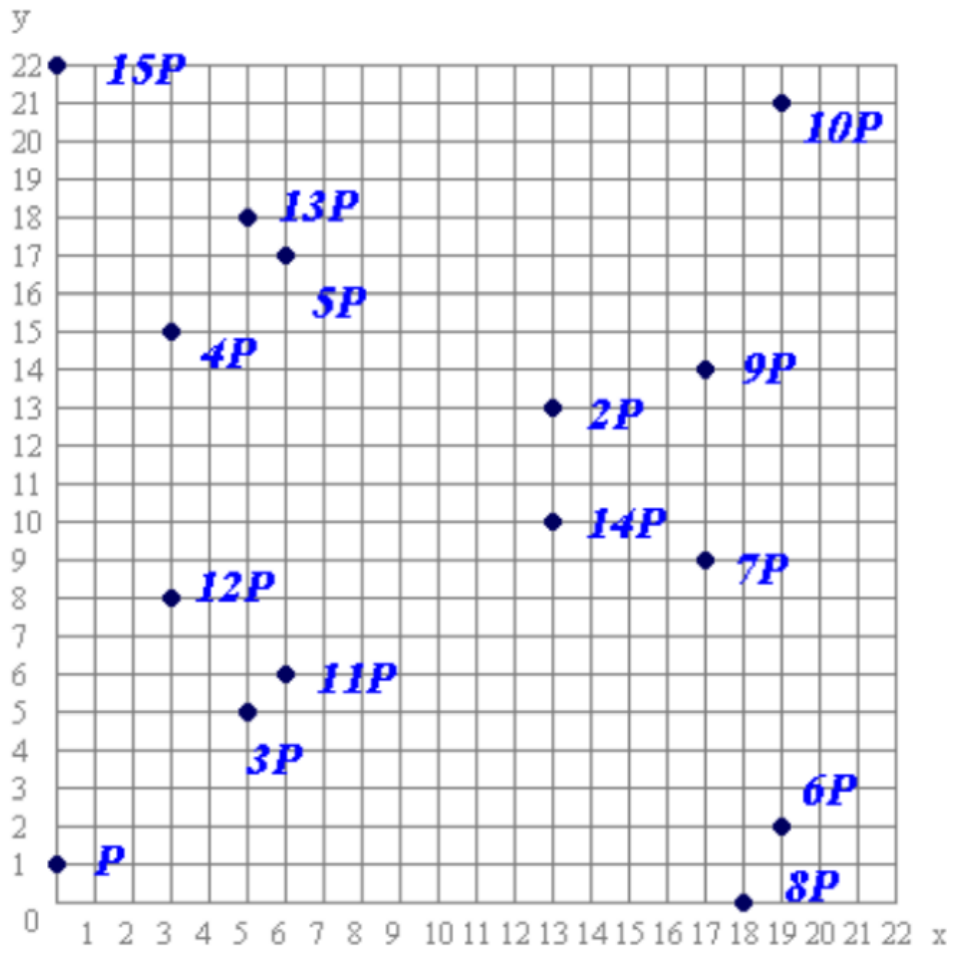
的生成数，求nP

$$
\begin{array}{l|l}
P = (0, 1) & 9P = (17, 14) \\
2P = (13, 13) & 10P = (19, 21) \\
3P = (5, 5) & 11P = (6, 6) \\
4P = (3, 15) & 12P = (3, 8) \\
5P = (6, 17) & 13P = (5, 18) \\
6P = (19, 2) & 14P = (13, 10) \\
7P = (17, 9) & 15P = (0, 22) \\
8P = (18, 0) &
\end{array}
$$

注：$|E(\mathbb{F}_{23})| = 15$，其实还要加上一个无穷远点，故E上共有16个点，点P的秩n=16。

椭圆曲线在模p下的运算规则

在坐标上画出，并观察图像特点



椭圆曲线在模p下的运算规则

例2.

有限域$\mathbb{F}_{23}$之下，取椭圆曲线

$$E : y^2 = x^3 + 16x + 10$$

上的两点P=(18,14), Q=(5,10), $R = P + Q = (x_3, y_3) = ?$

$$\lambda = \frac{3x^1 + A}{2y_1} mod\ p = 9$$

$$x_3 = \lambda^2 - x_1 - x_2 mod\ p = 22$$

$$y_3 = \lambda(x_1 - x_3) - y_1 mod\ p = 19$$

$$R = (22, 19)$$

椭圆曲线在模p下的运算规则

例3.

条件同例2，若$P+P=2P=R=(x_3,y_3)$，则R=?

$$x_3=\lambda^2-x_1-x_1 mod\ p=22$$

$$y_3=\lambda(x_1-x_3)-y_1 mod\ p=19$$

$$P+P=2P=R=(22,19)$$

椭圆曲线在模p下的点数

显然$E(\mathbb{F}_p)$是一个有限集，因为对X,Y分量来说都只有有限个可能。更确切地说，X取值一共有p中可能，对每一个X，等式

$$Y^2 = X^3 + AX + B$$

表明对应的Y最多只有两种可能，再加上一个点O，$E(\mathbb{F}_p)$最多只有2p+1个点。然而这一估计数值想当然的比实际大小要大。

椭圆曲线在模p下的点数

当我们为X赋一个值时，以下的三次多项式的值一共有三种可能

$$X^3 + AX + B$$

第一，它可能是一个模p的2次剩余，说明它有两个方根，因此我们得到$E(\mathbb{F}_p)$中的两个点。这件事50%会发生。第二，它可能是一个模p的非2次剩余，此时我们舍弃X，这件事50%发生。第三，它可能等于0，我们得到$E(\mathbb{F}_p)$中的一个点，但这概率非常非常低。因此我们期望$E(\mathbb{F}_p)$中点的个数约为

$$\#E(\mathbb{F}_p) \approx 50\% \cdot 2 \cdot p + 1 = p + 1$$

椭圆曲线在模p下的点数举例

求$\mathbb{F}_p$上的椭圆曲线

$$E: y^2 \equiv x^3 + 2x + 3 (\mathrm{mod}\, 5)$$

上的所有点，并在其中选择两个点计算它们的加法.

$x = 0$	$y^2 \equiv \mathbf{3}(\boldsymbol{mod}\ \mathbf{5})$	y无解
$x = 1$	$y^2 \equiv \mathbf{1}(\boldsymbol{mod}\ \mathbf{5})$	$y \equiv 1,4(mod\ 5)$
$x = 2$	$y^2 \equiv \mathbf{0}(\boldsymbol{mod}\ \mathbf{5})$	$y \equiv 0(mod\ 5)$
$x = 3$	$y^2 \equiv \mathbf{1}(\boldsymbol{mod}\ \mathbf{5})$	$y \equiv 1,4(mod\ 5)$
$x = 4$	$y^2 \equiv \mathbf{0}(\boldsymbol{mod}\ \mathbf{5})$	$y \equiv 0(mod\ 5)$

椭圆曲线在模p下的点数

Hasse提出了一个非常著名的定理，在之后被Weil和Deligne广义化，描述了在随机波动的情况下这是正确的

定理 (Hasse).

E是$\mathbb{F}_p$上的一条椭圆曲线，则

$$\#E(\mathbb{F}_p) = p + 1 - t_p \text{ with } |t_p| \leq 2\sqrt{p}$$

定义

$t_p = p + 1 - \#E(\mathbb{F}_p)$这个数称为$E/\mathbb{F}_p$的Frobenius迹(the trace of Frobenius)。这里不解释这个名字的由来，但要说的是t_p实际上是一个确定的2x2矩阵的迹，并且这个矩阵代表的是$E/\mathbb{F}_p$相关的2维向量空间一个线性变换。

椭圆曲线在模p下的点数

p	$\#E(\mathbb{F}_p)$	t_p	$2\sqrt{p}$
3	4	0	3.46
5	8	−2	4.47
7	11	−3	5.29
11	16	−4	6.63
13	14	0	7.21
17	15	3	8.25

Figure: number of points and trace of Frobenius for E: $Y^2 = X^3 + 4X + 6$

注：若$\#E(\mathbb{F}_p) = p + 1$，曲线$E(\mathbb{F}_p)$称为超奇异的，否则称为非超奇异的

本次课程内容目录

二次剩余的定义

定义（二次剩余和非剩余）

设m为大于1的正整数，$(n,m)=1$，如果方程

$$x^2 \equiv n(mod m)$$

有解，则n称为模m的 二次剩余，否则称为模m的 二次非剩余。

当m为奇素数p时，有Euler判别法

二次剩余的判别

定理（Euler判别法）

设p为奇素数，$p \nmid n$，则

当$n^{\frac{p-1}{2}} \equiv 1(modp)$时，$n$是二次剩余；

当$n^{\frac{p-1}{2}} \equiv -1(modp)$时，$n$是二次非剩余；

若n是模p的二次剩余，则

$$x^2 \equiv n(modp), (n,p) = 1$$

恰好有两个解。

当p很大时Euler判别法如何实施

平方根的计算

平方根的计算

若p为素数且满足$p \equiv 3 (\mathrm{mod}\, 4)$, 若$a$是模$p$的二次剩余,
即$x^2 \equiv a (\mathrm{mod}\, p)$有解, 则

$$b = a^{\frac{p+1}{4}} (\mathrm{mod}\, p)$$

是$x^2 \equiv a (\mathrm{mod}\, p)$的一个解.

平方根的计算

证明

设g为模p的原根，即为$\mathbb{F}_p^*$的生成元，a为模p的二次剩余，则存在整数k使得$a = g^{2k}$.

$$
\begin{aligned}
b^2 &\equiv a^{\frac{p+1}{2}} \\
&\equiv g^{k(p+1)} \\
&\equiv g^{2k+k(p-1)} \\
&\equiv g^{2k} \cdot g^{k(p-1)} \\
&\equiv a
\end{aligned}
$$

本次课程内容目录

倍点快速计算问题

对于$P, Q \in E(\mathbb{F}_p)$，满足Q=nP，似乎很难恢复出n即解决ECDLP问题。
我们将在接下来的章节说明ECDLP问题的困难。
在此之前首先需要在已知n和P的情况下，有效的计算nP。如果n足够大，我们当然不希望通过P,2P,3P....的方法来计算nP。
最有效的计算nP的方法类似于计算$a^n \pmod N$。然而在椭圆曲线中我们不是乘而是加，我们称之为“double-and-add”而非“square-and-multiply”

倍点快速计算

底层的想法和之前一样，我们首先将n写成二进制的形式

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 4 + n_3 \cdot 8 + ... + n_r \cdot 2^r, \ with \ n_0, n_1, ..., n^r \in \{0, 1\}$$

（不妨假设$n_r = 1$），则接下来我们可以计算如下几个数：

$$Q_0 = P, \ Q_1 = 2Q_0, \ Q_2 = 2Q_1, ..., Q_r = 2Q_{R-1}$$

注意到Q_i是Q_{i-1}的两倍，因此$Q_i = 2^i P$
这些点都是P的2的指数倍乘积，计算它们需要r次翻倍。最后我们计算nP最多只需要r次加操作

$$nP = n_0 Q_0 + n_1 Q_1 + n_2 Q_2 + ... + n_r Q_r$$

倍点快速计算

Input. Point $P \in E(\mathbb{F}_p)$ and integer $n \geq 1$.

1. Set $Q = P$ and $R = \mathcal{O}$.

2. Loop while $n > 0$.

  3. If $n \equiv 1 \pmod 2$, set $R = R + Q$.

  4. Set $Q = 2Q$ and $n = \lfloor n/2 \rfloor$.

  5. If $n > 0$, continue with loop at Step **2**.

6. Return the point R, which equals nP.

Figure: The Double-and-Add Algorithm

我们可以参照$E(\mathbb{F}_p)$中两个点的相加操作，因此计算nP的总时间最多为$E(\mathbb{F}_p)$中2r个点的相加。注意到$n \geq 2^r$，所以需要不超过于$2log_2(n)$次点相加操作。这意味着即使对很大的n也是一种计算nP的可行方法。

倍点快速计算举例

例子

我们使用Double-and-Add算法来计算$E(\mathbb{F}_p)$中的nP，其中

$$n = 947, \qquad E : Y^2 = X^3 + 14X + 19,\ p = 3623,\ P = (6, 730)$$

n的二元展开为

$$n = 947 = 1 + 2 + 2^4 + 2^5 + 2^7 + 2^8 + 2^9$$

一步步地计算过程如下一页的表格，需要9次翻倍与6次相加，最终结果947P=(3492,60)

倍点快速计算举例

Step i	n	$Q = 2^i P$	R
0	947	$(6, 730)$	$\mathcal{O}$
1	473	$(2521, 3601)$	$(6, 730)$
2	236	$(2277, 502)$	$(2149, 196)$
3	118	$(3375, 535)$	$(2149, 196)$
4	59	$(1610, 1851)$	$(2149, 196)$
5	29	$(1753, 2436)$	$(2838, 2175)$
6	14	$(2005, 1764)$	$(600, 2449)$
7	7	$(2425, 1791)$	$(600, 2449)$
8	3	$(3529, 2158)$	$(3247, 2849)$
9	1	$(2742, 3254)$	$(932, 1204)$
10	0	$(1814, 3480)$	$(3492, 60)$

在 $Y^2 = X^3 + 14X + 19 \ mod\ 3623$上计算$947 \cdot (6, 730)$

倍点快速计算进一步优化举例

下面的例子将帮助我们展示一个思想。
我们在例子中看到$947 = 1 + 2 + 2^4 + 2^5 + 2^7 + 2^8 + 2^9$，因此要15个点的操作来计算947P，但是如果我们写成

$$947 = 1 + 2 - 2^4 - 2^6 + 2^{10}$$

那么我们计算947P只需要10次翻倍和4次相加，总共14次操作。
将一个数n写为2的指数的正负和称为n的一个带符号的二进制展开.

BSD表示

对正整数k，$k = k_{n-1}2^{n-1} + ... + k_1 2^1 + k_0 2^0$，其中$k_i \in -1, 0, 1, 0 \leq i < n$为k的长度为n的带符号二进制表示（BSD:Binary Signed Digit）.

整数的BSD表示在计算机算术、密码学、数字信号处理等领域有广泛应用.

NAF表示

对正整数k，$(k_{n-1}, ..., k_0)$为一种BSD表示，若其中没有两个连续的k_i是非零的，则称它是非相邻形式的表示，记作NAF表示.

$(1, 0, ..., 0, -1) \Longleftrightarrow (0, 1, ..., 1, 1)$ $\quad 2^k - 1 = 1 + 2 + 2^2 + \cdots + 2^{k-1}$

倍点快速计算进一步优化

知道平均会发生什么很重要。对一个随机的数进行二元展开大约会有相同的1和0的个数，因此对于大多数n，用二元展开计算nP需要大约$\frac{3}{2}k$步（k次翻倍，1/2k次相加）。

如果我们允许带符号的二进制展开，则可以证明平均情况下，n的带符号的二进制展开中2/3的项都为0（作为练习）。
所以对于大多数n来说，我们计算nP需要大约$\frac{4}{3}k+1$步（k+1次翻倍，1/3k次相加）

本次课程内容目录

ECDLP问题

定义.

E是一条有限域$\mathbb{F}_p$上的椭圆曲线，让P和Q是$E(\mathbb{F}_p)$上的两个点，椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, 简称ECDLP)是指找到一个整数n使得Q=nP。通过类比$\mathbb{F}_p^*$上的离散对数问题，我们把这个整数n记为：

$$n = log_P(Q)$$

并且我们称n是关于P的Q的离散对数。

ECDLP问题

注记

- 第一个问题是可能存在$P, Q \in E(\mathbb{F}_p)$使得，Q不是P的乘积。这一情况下，$log_P(Q)$没有定义。
  但是从密码学的角度出发，Alice首先有一个公开的点P，秘密的整数值n并且可以计算并公开$Q = nP$。因此在实际应用中$log_P(Q)$存在并且是Alice的秘密值。

- 第二个问题是如果存在一个n满足$Q = nP$，那么就有很多个满足的值:
  - 为了说明这点，我们首先知道存在一个正整数s使得$sP=O$
  - 因此若s为P的阶，n_0满足$Q = n_0P$，那么Q=nP的解就为$n = n_0 + is, i \in \mathbb{Z}$
  - 这说明$log_P(Q)$的值是$\mathbb{Z}/s\mathbb{Z}$的一个元素，其中s为P的阶。这样具体来说，可以把$log_P(Q)$设置为n_0。

ECDLP问题举例

示例

考虑椭圆曲线

$$E : Y^2 = X^3 + 8X + 7 \bmod 73$$

点P(32,53)，点Q(39,17)都在E上，很容易验证

$$Q = 11P, log_P(Q) = 11$$

类似的，R=(35,47), S=(58,4)，在一定计算后有R=37P, S=28P,因此

$$log_P(R) = 37,\ log_P(S) = 28$$

ECDLP问题到底有多难

目前已知的最快的解决ECDLP的算法，在$E(\mathbb{F}_p)$的情况下大约需要花费$O(\sqrt{p})$步

本次课程内容目录

ECDHP问题

定义（ECDHP问题）.

$E(\mathbb{F}_p$是一条有限域上的椭圆曲线，P是E上的一个点，那么ECDHP问题(Elliptic Curve Diffie-Hellman Problem)是指在已知n_1P和n_2P两个值的情况下计算n_1n_2P

椭圆曲线Diffie-Hellman密钥交换

Public parameter creation	
A trusted party chooses and publishes a (large) prime p, an elliptic curve E over $\mathbb{F}_p$, and a point P in $E(\mathbb{F}_p)$.	
Private computations	
Alice	**Bob**
Chooses a secret integer n_A. Computes the point $Q_A = n_A P$.	Chooses a secret integer n_B. Computes the point $Q_B = n_B P$.
Public exchange of values	
Alice sends Q_A to Bob $\longrightarrow$	Q_A
Q_B $\longleftarrow$	Bob sends Q_B to Alice
Further private computations	
Alice	**Bob**
Computes the point $n_A Q_B$.	Computes the point $n_B Q_A$.
The shared secret value is $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A$.	

Table 6.5: Diffie–Hellman key exchange using elliptic curves

椭圆曲线Diffie-Hellman密钥交换举例

示例

Alice和Bob决定使用椭圆曲线版本的Diffie–Hellman密钥交换，其中参数用以下素数，曲线和点：

$$p = 3851, \qquad E : Y^2 = X^3 + 324X + 1287, \qquad P = (920, 303) \in E(\mathbb{F}_{3851})$$

Alice和Bob分别选择相应秘密值$n_A = 1194, n_B = 1759$。然后分别计算$Q_A = 1194P = (2067, 2178)$，$Q_B = 1759P = (3684, 3125)$ 他们分别将结果发送给对方并继续计算 $n_A Q_B = 1194(3684, 3125) = (3347, 1242)$，$n_B Q_A = 1759(2067, 2178) = (3347, 1242)$。最终他们交换了秘密点(3347,1242)。他们应该丢弃y值并只保留x值3347作为秘密分享值。Eve如果想要了解Alice和Bob分享的秘密值，那么她就需要解决一个ECDLP问题：$nP = Q_A$

椭圆曲线Diffie-Hellman密钥交换注记

注释

椭圆曲线版本的Diffie-Hellman密钥交换需要Alice和Bob交换在椭圆曲线上面的一个点。一个点$Q \in E(\mathbb{F}_p$包含了两个分量，$Q = (x_Q, y_Q)$。看上去Alice必须要向Bob发送两个数。然而，这样的两个数并不包含有任意两个数所包含的信息，因为它们一个形式相关联：

$$y_Q^2 = x_Q^3 + Ax_Q + B \quad in\ \mathbb{F}_p$$

注意如果Eve知道A和B，那么她只需要猜正确的x_Q，然后计算出y_Q即可

椭圆曲线Diffie-Hellman密钥交换注记

Alice几乎没有理由需要把Q_A的两个分量都发送给Bob，因为y分量本身所包含的信息量太少了。因此她只需要将x分量发送给Bob即可。Bob然后计算，可能会有两个y分量，Bob使用其中一个即可。如果他正好使用的是“正确”的y，那么Bob用的是Q_A，如果使用的是“不正确”的y（正好是正确的y的负值），则他使用的是$-Q_A$。在任何情况下，Bob都会计算

$$\pm n_B Q_A = \pm(n_A n_B)P$$

类似地，Alice最后也会计算得到$\pm(n_A n_B)P$的其中一个。然后Alice和Bob使用其中的x分量作为秘密分享值，因为此时x分量是相同的无论他们使用的y是什么。

举例

例子

Alice和Bob决定使用和示例6.19中相同的公共参数来交换另一个秘密值

$$p = 3851, \qquad E : Y^2 = X^3 + 324X + 1287, \qquad P = (920, 303) \in E(\mathbb{F}_{3851})$$

但是这次他们想发送一些比特给另一方。Alice和Bob分别选择相应秘密值$n_A = 2489, n_B = 2286$。然后分别计算

$$Q_A = 2489P = (593, 719)$$

$$Q_B = 2286P = (3681\text{fi}612)$$

这次，不发送两个分量而只互相发送$x_A = 593$和$x_B = 3681$ Alice带入$x_B = 3681$到E的等式中进行计算得到

$$y_B^2 = x_B^3 + 324x_B + 1287 = 997$$

举例

Alice需要计算997 mod 3851的平方根。这在素数满足$p \equiv 3 \pmod 4$下是不难的，因为已经证明$b^{(p+1)/4}$即为一个b的平方根。Alice代入即可

$$y_B = 997^{(3851+1)/4} = 997^9 63 \equiv 612 \ (mod\ 3851)$$

正好他所得到的$Q_B = (3681\text{fi}612)$是Bob所使用的，然后她计算$n_A Q_B = 2489(3681\text{fi}612) = (509, 1108)$

类似地，Bob将$x_A = 593$代入到E的等式中进行计算得到

$$y_A^2 = x_A^3 + 324x_A + 1287 = 927$$

$$y_A = 927^{(3851+1)/4} = 927^9 63 \equiv 3132 \ (mod\ 3851)$$

Bob使用点$Q'_A = (593, 3132)$，实际上这不是Alice的点Q_A。但Bob计算$n_B Q'_A = 2286(593\text{fi}3132) = (509, 2743)$ Bob和Alice最终分享的秘密值是x分量即509。

本次课程内容目录

椭圆曲线公钥密码体制

Public parameter creation	
A trusted party chooses and publishes a (large) prime p, an elliptic curve E over $\mathbb{F}_p$, and a point P in $E(\mathbb{F}_p)$.	
Alice	**Bob**
Key creation	
Choose a private key n_A. Compute $Q_A = n_A P$ in $E(\mathbb{F}_p)$. Publish the public key Q_A.	
Encryption	
	Choose plaintext $M \in E(\mathbb{F}_p)$. Choose a random element k. Use Alice's public key Q_A to compute $C_1 = kP \in E(\mathbb{F}_p)$. and $C_2 = M + kQ_A \in E(\mathbb{F}_p)$. Send ciphertext (C_1, C_2) to Alice.
Decryption	
Compute $C_2 - n_A C_1 \in E(\mathbb{F}_p)$. This quantity is equal to M.	

Table 6.6: Elliptic Elgamal key creation, encryption, and decryption

椭圆曲线公钥密码体制

假设我们在椭圆曲线上模仿ElGamal密码系统中的操作，我们可以拥有两个公开的椭圆曲线上的点P,Q。Q是P的一个倍数比如说$Q = mP$。其中m是私钥。加密过程将会涉及选择一个随机的数k来计算kP和kQ。然后kQ将用来加密明文。

椭圆曲线公钥密码体制

实现上的困难

- 目前没有便捷的确定算法来将明文和E上的点对应。
  解决的办法是选择明文为$\mathbb{Z}_p$中的任意元素。然后将其作为一个mask作用在点上。
- 消息扩张。椭圆曲线密码体制有4倍的消息扩张。

点压缩

解决第二个实现上困难的技巧叫做点压缩(point compression)。这将减少椭圆曲线上对点的存储需求。一个（非无限远）在椭圆曲线E上的点是一对(x,y)。给定一个x，对y来说存在两种可能的值，并且这两个值在模p下为相反数。由于p为奇数，因此y的两个可能的值中，一个为奇数，另一个为偶数。因此我们可以确定E上的唯一一个点P通过给定x的值以及一个0,1比特。这将带来约50%的存储节省，代价是需要额外计算P的y分量。

点压缩

Algorithm 7.5: POINT-DECOMPRESS(x, i)

$z \leftarrow x^3 + ax + b \bmod p$
if z is a quadratic non-residue modulo p
  then return ("failure")
  else
$$\begin{cases} y \leftarrow \sqrt{z} \bmod p \\ \textbf{if } y \equiv i \pmod 2 \\ \quad \textbf{then return } (x, y) \\ \quad \textbf{else return } (x, p - y) \end{cases}$$

Cryptosystem 7.2: *Elliptic Curve ElGamal*

Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Z}_p$ (where $p > 3$ is prime) such that $\mathcal{E}$ contains a cyclic subgroup $H = \langle P \rangle$ of prime order n in which the **Discrete Logarithm** problem is infeasible. Let $h : \mathcal{E} \to \mathbb{Z}_p$ be a secure hash function. Let $\mathcal{P} = \mathbb{Z}_p$ and $\mathcal{C} = (\mathbb{Z}_p \times \mathbb{Z}_2) \times \mathbb{Z}_p$. Define

$$\mathcal{K} = \{(\mathcal{E}, P, m, Q, n, h) : Q = mP\},$$

where P and Q are points on $\mathcal{E}$ and $m \in {\mathbb{Z}_n}^*$. The values $\mathcal{E}, P, Q, n$, and h are the public key and m is the private key.

For $K = (\mathcal{E}, P, m, Q, n, h)$, for a (secret) random number $k \in {\mathbb{Z}_n}^*$, and for a plaintext $x \in \mathbb{Z}_p$, define

$$e_K(x, k) = (\text{POINT-COMPRESS}(kP), x + h(kQ) \bmod p).$$

For a ciphertext $y = (y_1, y_2)$, where $y_1 \in \mathbb{Z}_p \times \mathbb{Z}_2$ and $y_2 \in \mathbb{Z}_p$, define

$$d_K(y) = y_2 - h(R) \bmod p,$$

where

$$R = m\,\text{POINT-DECOMPRESS}(y_1).$$

Example 7.12 Suppose that $P = (2,7)$ and Bob's private key is $m = 7$, so

$$Q = 7P = (7,2).$$

Suppose Alice wants to encrypt the plaintext $x = 9$, and she chooses the random value $k = 6$. First, she computes

$$kP = 6\,(2,7) = (7,9)$$

and

$$kQ = 6\,(7,2) = (8,3).$$

Then, suppose that $h(8,3) = 4$ for purposes of illustration. Next, she calculates

$$y_1 = \text{POINT-COMPRESS}(7,9) = (7,1)$$

and

$$y_2 = 9 + 4 \bmod 11 = 2.$$

The ciphertext she sends to Bob is

$$y = (y_1, y_2) = ((7,1),2).$$

When Bob receives the ciphertext y, he computes

$$\begin{aligned} \text{POINT-DECOMPRESS}(7,1) &= (7,9), \\ 7\,(7,9) &= (8,3), \\ h(8,3) &= 4 \quad \text{and} \\ 2 - 4 \bmod 11 &= 9. \end{aligned}$$

课后作业

1. 椭圆曲线E：$y^2 = x^3 + 2x + 7$定义在$\mathbb{Z}_{31}$上。

（1）计算椭圆曲线的点数

（2）$P = (2,9)$是E中阶为39的点

（3）计算$Q = 8P$

（4）确定17的NAF表示并利用快速算法计算$17P$

2. 令L_i代表NAF表示中恰好有i个系数，并且首系数为1的所有正整数的集合。记$k_i = |Li|$

（1）通过对Li进行适当的分解，证明k_i满足下列递推关系

$$k_1 = 1$$

$$k_2 = 1$$

$$k_{i+1} = 2(k_1 + k_2 + \cdots + k_{i-1}) + 1 \text{ (对} i \geq 2\text{)}$$

（2）导出k_i的一个二阶递归关系，算出递归关系的一个显式解。