# 第七届（2022）全国高校密码数学挑战赛
# 赛题三

## 一. 赛题名称：椭圆曲线加密体制破译

## 二. 赛题描述

### 2.1 椭圆曲线基础知识

设 $\mathbb{F}_p$ 表示具有 $p$ 个元素的有限域，其中 $p > 3$ 是一个素数. 椭圆曲线上的有理点集合 $E(\mathbb{F}_p)$ 定义为

$$E(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + ax + b,\ a, b \in \mathbb{F}_p\right\} \cup \{\infty\}, \tag{1}$$

其中 $\infty$ 表示无穷远点，且 $4a^3 + 27b^2 \neq 0 \pmod p$. $E(\mathbb{F}_p)$ 按照下面描述的群律规则形成群.

设 $P = (x_1, y_1)$，$Q = (x_2, y_2) \in E(\mathbb{F}_p)$, 在 $E$ 上定义 “+” 运算 $P + Q = R \in E(\mathbb{F}_p)$ 是过 $P, Q$ 的直线与曲线的另一交点关于 $x$ 轴的对称点 (当 $P = Q$ 时，$R$ 是 $P$ 点的切线与曲线的另一交点关于 $x$ 轴的对称点). 为了方便理解, 我们在图 1中给出了实数域上椭圆曲线有理点的加法情形.

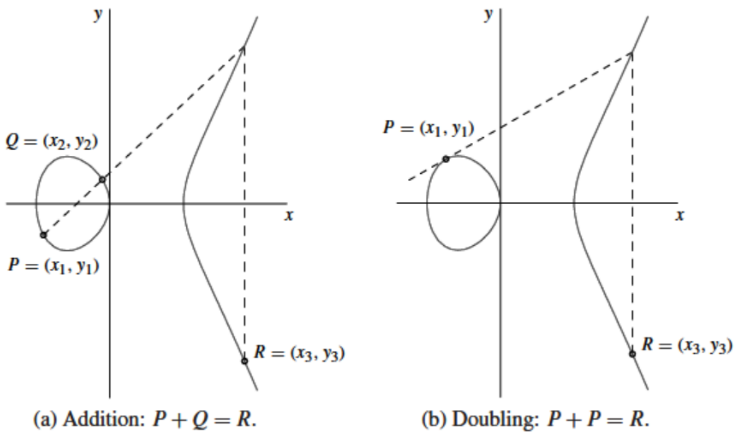


图 1: 椭圆曲线有理点的加法规则

上述计算可用公式表示如下:

- 当 $P \neq Q$ 时 (Addition)，
$$R = (x_3, y_3) = \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1\right);$$
- 当 $P = Q$ 时 (Doubling)，

$$R=(x_3,y_3)=\left(\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1,\left(\frac{3x_1^2+a}{2y_1}\right)(x_1-x_3)-y_1\right);$$

- $P+\infty=\infty+P=P$ ;
- $(x_1,y_1)+(x_1,-y_1)=\infty$ , 这里 $(x_1,-y_1)\in E(\mathbb{F}_p)$ 定义为 $P$ 的逆元 $-P$. 特别的，$-\infty=\infty$.

可验证 $E(\mathbb{F}_p)$ 关于上述定义的“+”运算构成一个交换群，记为 $E(\mathbb{F}_p)$.

设 $P\in E\ (F_p)$ , 记

$$[k]\,P=P+P+\ldots+P\ (k\ times),$$

则 $[k]P\in E(\mathbb{F}_p)$，该运算称为椭圆曲线标量乘法运算. 设 $r$ 为最小的正整数使得 $[r]\,P=\infty$, 则 $r$ 称为是 $P$ 的阶（order）. 令

$$\langle P\rangle=\{\infty\ ,\ P\ ,\ [2]P\ ,\cdots,\ [r-1]P\},$$

可验证 $\langle P\rangle$ 关于“+”运算构成 $E(\mathbb{F}_p)$ 的一个 $r$ 阶子群.

### 2.2 椭圆曲线加密体制

赛题中所使用的椭圆曲线加密体制 (ECC) 描述如下：

**公共参数设定**

(1) 选择一个大素数 $p$(在具体赛题中, 我们选择 $p$ 为 160 比特左右);

(2) 选择一条定义在 $\mathbb{F}_p$ 上的椭圆曲线 $E:y^2=x^3+ax+b$, 以及在椭圆曲线 $E$ 上的有理点 $P$ 作为基点 .

**公钥生成**

(1) Alice 选择私钥 $n_A$，之后计算 $Q_A=[n_A]P$;

(2) Alice 公布自己的公钥 $Q_A$.

**加密过程**

(1) Bob 将明文信息 $m$ 通过某种方式 (**嵌入方式下面会详细说明**) 嵌入到椭圆曲线上的一个点 $M\in E(\mathbb{F}_p)$;

(2) 每次加密时, 加密者 Bob 固定选择一个 160 比特的随机数 $k$(**部分随机数 $k$ 由某一特定的随机数发生器生成**), 计算

$$\begin{aligned}C_1=&[k]P\in E(\mathbb{F}_p),\\C_2=&M+[k]Q_A\in E(\mathbb{F}_p);\end{aligned}$$

(3) Bob 发送 $C_1$ 和 $C_2$ 给 Alice.

**解密过程**

(1) Alice 收到 $C_1$ 和 $C_2$ 后, 使用自己的私钥计算 $M=C_2-[n_A]C_1\in E(\mathbb{F}_p)$;

(2) Alice 根据 $M$ 恢复明文消息 $m$.

**明文嵌入**

本赛题中，加密这 Bob 每一次需要加密的明文消息包含 16 个明文字符以及分配给该消息的对应编号. 解密者 Alice 通过自己的私钥解密得到所有明文信息和相应编号后，按照正确编号排序所有明文消息, 可以恢复出 Bob 传输的完整有意义的消息. Bob 每次加密时的消息嵌入规则如下：

(1) 将该次明文消息的 16 个明文字符转为 ASCII 码 $M_1$，共计 128 比特;

(2) 将编号信息转为 ASCII 码 ((需要使用 8 比特)) 并添加在 $M_1$ 尾部，得到 $M_2$，此时 $M_2$ 为 136 比特；

(3) 在 $M_2$ 后再填充 0 变为 $M_3$, 使得 $M_3$ 的比特长度达到 160 比特；

(4) 把 $M_3$ 看做 $\mathbb{F}_p$ 中的元素, 考虑 $M_3$, $M_3+1$, $M_3+2$, $\cdots$, 直到某一个最小非负整数 $i$ 使得 $x_M = M_3 + i$ 满足：$x_M^3 + ax_M + b$ 在有限域 $\mathbb{F}_p$ 中等于某个元素的平方;

(5) 令 $M = (x_M, y_M) \in E(\mathbb{F}_p)$，其中 $y_M$ 满足

$$y_M^2 = x_M^3 + ax_M + b \mod p,$$

且 $y_M < \dfrac{p}{2}$ .

## 2.3 加密解密过程示范

如下我们提供一个实例供参赛选手理解.

**注:** 我们对有理点的表示采用点压缩技术：即对一个点 $R = (x_R, y_R) \in E(\mathbb{F}_p)$, 当 $y_R \equiv 1 \pmod 2$ 时我们将 $R$ 记为 $[x_R, 1]$, 否则记为 $[x_R, 0]$.

**参数设定:**

(1) 选择大素数 $p = $ 0xb77902abd8db9627f5d7ceca5c17ef6c5e3b0969;

(2) 选择定义在 $\mathbb{F}_p$ 上的一条椭圆曲线 $E: y^2 = x^3 + ax + b$, 其中

$$a = \text{0x9021748e5db7962e1b208e3949d42ad0388a18c},$$

$$b = \text{0x744f47974caabdd8b8192e99da51c87f91cc453e}.$$

之后选择椭圆曲线上的一点

$$P = [\text{0x4f1ecacc3b1e56066b02f6a6033f940fc5c9805}, 0]$$

该点 $P$ 已经使用点压缩技术表示, 以下所有的点都会使用点压缩技术表示.

**公钥生成:**

(1)Alice 选择私钥 $n_A = $ 0x9022802bb688656ee1914e6dd7f74e1ecd1d6780(在真正安全实现时该信息不会给出, 这里仅仅作为示范故给出该信息), 之后计算

$$Q_A = [n_A]P = [\text{0xb50e2eb55cd84112077a5acca94b4623a8b020d7}, 0],$$

(2)Alice 公布自己的公钥 $Q_A$.

**加密过程**

(1) Bob 将明文信息"I would like to share a secret. " 切段为"I would like to " 和"share a secret. " 后，对两个明文段编号为 1 和 2，并打乱顺序加密. 假设现在 Bob 要为 “share a secret. ” 加密, 则先将"share a secret. " 转为 ASCII 码

$$M_1 = \text{0x7368617265206120736563726574 2e20},$$

之后将编号 2 转为 ASCII 码"0x32", 得到

$$M_2 = \text{0x73686172652061207365637265742e2032},$$

最后补足 0 使其达到 160 比特:

$$M_3 = \text{0x73686172652061207365637265742e2032000000},$$

此时，取 $x_M = M_3$, 恰好使得 $x_M^3 + ax_M + b$ 是有限域 $\mathbb{F}_p$ 中某个元素的平方, 通过计算，可得 $E(\mathbb{F}_p)$ 上一点

$$M = [\text{0x73686172652061207365637265742e2032000000}, 1].$$

(2) Bob 选择一个随机数 $k = \text{0xe6ea1793a37dedf12ed676aef41ed68f4da4ae8f}$, 计算

$C_1 = [k]P = [\text{0x2592c6e5b7176ef74a7c7adc9a19906445759d5}, 0]$,

$C_2 = M + [k]Q_A = [\text{0x47190e98e7d440679b896e2a672c9ad58e13d212}, 1]$;

(3) Bob 发送 $(C_1, C_2)$ 给 Alice.

**解密过程**

(1) Alice 计算 $M = C_2 - [n_A]C_1 \in E(\mathbb{F}_p)$;

(2) Alice 根据 $M$ 恢复明文消息"share a secret"，编号为 2 .

### 2.4 问题描述

- 已知条件

  给定椭圆曲线加密体制中每次加密所使用的椭圆曲线 $E(\mathbb{F}_p)$ 的基本参数. 有理点 $P \in E(\mathbb{F}_p)$ 作为基点和公钥 $Q_A = [n_A]P$ 的坐标也被给定, 每次加密后的密文 $C_1$ 和 $C_2$ 也被给定.

- 求解目标

  1. 已知点 $P \in E(\mathbb{F}_p)$ 和 $Q_A = [n_A]P$ 的坐标信息, **求解出私钥** $n_A$.
  2. **恢复出**与密文 $C_1$ 和 $C_2$ 所对应的**明文** $m$.

### 2.5 成绩评判标准

- 共八道小题，随着序数递进每道小题的分值分别为 10、10、15、20、20、25、50、50，共计 200 分. 每道题目需要选手恢复出密文所对应的**有意义的**明文消息 $m$ 和 Alice 解密时所使用的私钥 $n_A$, 并说明获得正确结果的理由. 若只获得密文所对应的**有意义的**明文消息 $m$, 但有正确的理由论证获得结果的正确性, 则可获得该题分数的 40%. 获得其他部分结果将根据求解原理酌情给分.

- 分数相同的选手依照难度最高的挑战求解时间来排序，求解用时越少者排名越靠前；

- 针对每个小题，给出计算平台和计算结果，并简述求解原理、步骤和实现效率（包括计算需要的时间和空间等），引用前人方法的必须在报告中给出明确引用，否则报告内容作废；
- 利用特殊算法求解或求解算法中有创新内容的，酌情加分.

## 三. 国内外研究进展与现状

上世纪八十年代，Koblitz 和 Miller 分别独立提出了椭圆曲线密码体制 (ECC) . 该密码体制的安全性依赖于椭圆曲线离散对数问题 (ECDLP) 的难解性. 因为有限域中的离散对数问题还可用亚指数时间的指标演算法求解，而一般的 ECDLP 目前没有亚指数时间的求解算法，故而它被认为比有限域乘法群中的离散对数问题更加难以求解. 目前，大家认为 160 比特的椭圆曲线加密体制的安全强度与 1024 比特的 RSA 加密体制相当. 且随着模数的增大，它们之间安全性的差距也会增大. 因此，ECC 可以提供一个具有更小密钥长度的公开加密系统.

本质上，ECC 是 ElGamal 密码体制的一个变种，而 ElGamal 密码体制是 1985 年由 Taher ElGamal 提出的，现今在工业界应用广泛. ElGamal 密码体制可以定义在任何循环群 $G$ 上，其安全性取决于 $G$ 上离散对数问题的困难性. 而椭圆曲线加密体制的安全性主要由基于 ECDLP 的困难性保证. 对于 ECDLP 常见的求解算法有大步-小步法、Pollard’s rho 算法等. 一般来说,当参数 $p$ 较大时,这些算法并不容易求解. 而在参数设定不当时, ECDLP 的困难性会下降. 如 MOV 攻击可以利用双线性对将 ECDLP 求解转为有限域中乘法群的 DLP 求解，而有限域的乘法群中 DLP 存在亚指数时间的算法, 解题者可以考虑利用 CADO-NFS 软件 (`https://gitlab.inria.fr/cado-nfs/cado-nfs`) 或者数论库 NTL(`https://libntl.org/`) 来求解; 而 SSSA 攻击可以将迹为 1 的异常椭圆曲线转为有限域加法群的 DLP. 如果选择的椭圆曲线有理点的阶等于一些小素数因子的乘积, 那可以用 Pholig-Hellman 算法来求解相应的 ECDLP. 如果已知离散对数问题的解在某个固定区间时，其困难性可能也会降低. 除此以外，ElGamal 类型密码体制还依赖于加密时所使用随机数生成器的安全性.

## 四. 参考文献

[1] 李殿伟，王正义，赵俊阁，椭圆曲线密码体制安全性分析，计算机技术与发展，第 22 卷第 4 期, 227-234, 2012.

[2] Menezes A. J., Okamoto T., Vanstone S. A., Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory. 39(5), pp. 1639 -1646, 1993.

[3] Galbraith S. D., Gaudry P., Recent progress on the elliptic curve discrete logarithm problem, Des. Codes Cryptography. 78(1), pp. 51–72, 2016.