第六章　公钥密码学和离散对数

张磊

华东师范大学 • 软件学院

本章内容

1. ElGamal 密码体制
2. ElGamal 密码体制安全性
3. 椭圆曲线

§ 6.1　ElGamal 密码体制

离散对数问题

当 α 是一个模素数 p (或 $\mathbb{Z}_p$) 的本原元素时, 有

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

离散对数问题

当 α 是一个模素数 p (或 $\mathbb{Z}_p$) 的本原元素时, 有

$$\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\} = \{\alpha^1, \alpha^2, \cdots, \alpha^{p-2}, \alpha^{p-1}\} \bmod p.$$

离散对数问题

当 α 是一个模素数 p (或 $\mathbb{Z}_p$) 的本原元素时, 有

$$\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\} = \{\alpha^1, \alpha^2, \cdots, \alpha^{p-2}, \alpha^{p-1}\} \bmod p.$$

这样对任意的 $\beta \in \mathbb{Z}_p^*$, 肯定存在 i $(1 \le i \le p-1)$, 使得

$$\beta = \alpha^i \bmod p.$$

离散对数问题

当 α 是一个模素数 p (或 $\mathbb{Z}_p$) 的本原元素时, 有

$$\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\} = \{\alpha^1, \alpha^2, \cdots, \alpha^{p-2}, \alpha^{p-1}\} \bmod p.$$

这样对任意的 $\beta \in \mathbb{Z}_p^*$, 肯定存在 i $(1 \le i \le p-1)$, 使得

$$\beta = \alpha^i \bmod p.$$

离散对数 (DL) 问题

实例: 一个模素数 p 的本原元素 α 和元素 $\beta \in \mathbb{Z}_p^*$

问题: 找出唯一的整数 i, $1 \le i \le p-1$, 满足

$$\beta = \alpha^i \bmod p.$$

我们将这个整数 i 记为 $\log_\alpha \beta$, 称为 β 的离散对数.

离散对数问题

当 α 是一个模素数 p (或 $\mathbb{Z}_p$) 的本原元素时, 有

$$\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\} = \{\alpha^1, \alpha^2, \cdots, \alpha^{p-2}, \alpha^{p-1}\} \bmod p.$$

这样对任意的 $\beta \in \mathbb{Z}_p^*$, 肯定存在 i $(1 \le i \le p-1)$, 使得

$$\beta = \alpha^i \bmod p.$$

离散对数 (DL) 问题

实例: 一个模素数 p 的本原元素 α 和元素 $\beta \in \mathbb{Z}_p^*$

问题: 找出唯一的整数 i, $1 \le i \le p-1$, 满足

$$\beta = \alpha^i \bmod p.$$

我们将这个整数 i 记为 $\log_\alpha \beta$, 称为 β 的离散对数.

主要性质: 求解离散对数问题是困难的, 而其逆运算 (模指数运算) 则可以应有效计算.

$\mathbb{Z}_p^*$ 上的 ElGamal 密码体制

令 $\mathcal{P} = \mathbb{Z}_p^*, \mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*, \alpha$ 是一个模素数 p 本原元素. 定义

$$\mathcal{K} = \{(p, \alpha, a, \beta) \mid \beta = \alpha^a \bmod p\},$$

其中 (p, α, β) 是公钥, a 是私钥.

对 $K = (p, \alpha, a, \beta)$, 以及一个 (秘密) 随机数 $k \in \mathbb{Z}_{p-1}$, 定义:

$$E_K(x, k) = (y_1, y_2), \quad x \in \mathbb{Z}_p^*$$

其中

$$y_1 = \alpha^k \bmod p, \quad y_2 = x\beta^k \bmod p.$$

对 $y_1, y_2 \in \mathbb{Z}_p^*$, 定义:

$$D_K(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p.$$

说明

1. 解密运算是正确的:

$$D_K(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p = x\beta^k(\beta)^{-k} \bmod p = x.$$

说明

1. 解密运算是正确的:

$$D_K(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p = x\beta^k(\beta)^{-k} \bmod p = x.$$

2. 加密算法随机: 密文即依赖于明文 x, 也依赖于选择的随机数 k.

说明

1. 解密运算是正确的:

$$D_K(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p = x\beta^k(\beta)^{-k} \bmod p = x.$$

2. 加密算法随机: 密文即依赖于明文 x, 也依赖于选择的随机数 k.
3. 安全性依赖于 $\mathbb{Z}_p^*$ 上的离散对数问题是难处理的—此时 p 至少应该取 300 个十进制位, $p-1$ 应该具有至少一个较大的素数因子.

Examp-6-1-1: ElGamal 密码体制

设 $p = 2579$, $\alpha = 2$ 为 $\mathbb{Z}_p$ 的一个本原元, $a = 765$, 那么

$$\beta = \alpha^a \bmod p = 2^{765} \bmod 2579 = 949.$$

如果 Alice 想给 Bob 发送消息 $x = 1299$, 她进行如下加密运算：

1. 选取随机数 k, 假设 $k = 853$;
2. 计算：

$$\begin{aligned} y_1 &= 2^{853} \bmod 2579 \\ &= 435 \\ y_2 &= 1299 \cdot 949^{853} \bmod 2579 \\ &= 2396 \end{aligned}$$

当 Bob 收到 Alice 发来的密文 $y = (435, 2396)$ 后, 恢复明文如下:

$$x = 2396 \cdot (435^{765})^{-1} \bmod 2579 = 1299.$$

§ 6.2　ElGamal 密码体制安全性

二次剩余集合 QR(p) 大小

1. 定义映射 $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ (p 为奇素数) 为

$$f(x) = x^2 \bmod p$$

二次剩余集合 QR(p) 大小

1. 定义映射 $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ (p 为奇素数) 为

$$f(x) = x^2 \bmod p$$

2. 定义 QR(p) 为所有模 p 的二次剩余的集合, 即

$$\mathrm{QR}(p) = \{x^2 \bmod p \mid x \in \mathbb{Z}_p^*\}.$$

二次剩余集合 QR(p) 大小

1. 定义映射 $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ (p 为奇素数) 为
$$f(x) = x^2 \bmod p$$
2. 定义 QR(p) 为所有模 p 的二次剩余的集合, 即
$$\mathrm{QR}(p) = \{x^2 \bmod p \mid x \in \mathbb{Z}_p^*\}.$$
3. $|\mathrm{QR}(p)| = \frac{p-1}{2}$: 因为
$$w^2 \equiv x^2 \pmod p \Leftrightarrow p|(w-x)(w+x) \Leftrightarrow w \equiv \pm x \pmod p,$$
所以 $\forall\, y \in \mathrm{QR}(p)$, 有 $|f^{-1}(y)| = 2$. 故
$$|\mathrm{QR}(p)| = \frac{p-1}{2}.$$
即: $\mathbb{Z}_p^*$ 中恰有一半元素是二次剩余, 一半不是.

QR(p) 元素形式

假设 α 是一个 $\mathbb{Z}_p^*$ (p 为奇素数) 的本原元

1. 如果 a 是偶数, 则

$$\alpha^a = (\alpha^{a/2})^2 \in \mathrm{QR}(p);$$

QR(p) 元素形式

假设 α 是一个 $\mathbb{Z}_p^*$ (p 为奇素数) 的本原元

1. 如果 a 是偶数, 则
$$\alpha^a = (\alpha^{a/2})^2 \in \mathrm{QR}(p);$$
2. $(p-1)/2$ 个元素
$$\alpha^0, \alpha^2, \alpha^4, \cdots, \alpha^{p-3}$$
互不相同;

QR(p) 元素形式

假设 α 是一个 $\mathbb{Z}_p^*$ (p 为奇素数) 的本原元

1. 如果 a 是偶数, 则
$$\alpha^a = (\alpha^{a/2})^2 \in \mathrm{QR}(p);$$
2. $(p-1)/2$ 个元素
$$\alpha^0, \alpha^2, \alpha^4, \cdots, \alpha^{p-3}$$
互不相同;
3. $\mathrm{QR}(p) = \{\alpha^{2i} \bmod p \mid 0 \le i \le (p-3)/2\}$.

QR(p) 元素形式

假设 α 是一个 $\mathbb{Z}_p^*$ (p 为奇素数) 的本原元

1. 如果 a 是偶数, 则
$$\alpha^a = (\alpha^{a/2})^2 \in \mathrm{QR}(p);$$
2. $(p-1)/2$ 个元素
$$\alpha^0, \alpha^2, \alpha^4, \cdots, \alpha^{p-3}$$
互不相同;
3. $\mathrm{QR}(p) = \{\alpha^{2i} \bmod p \mid 0 \le i \le (p-3)/2\}$.

Corollary

假设 α 是一个 $\mathbb{Z}_p^*$ (p 为奇素数) 的本原元, 则 β 是一个模 p 的二次剩余 $\Leftrightarrow \log_\alpha \beta$ 是偶数.

Examp-6-2-1: QR(7)

考虑例子 QR(7): $p = 7$, $p - 1 = 6$,

Examp-6-2-1: QR(7)

考虑例子 QR(7): $p = 7$, $p - 1 = 6$,

1. 首先, 根据定义有

$$\begin{aligned} \mathrm{QR}(7) &= \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} \\ &= \{1^2 = 6^2 = 1, 2^2 = 5^2 = 4, 3^2 = 4^2 = 2\} \\ &= \{1, 2, 4\} \end{aligned}$$

Examp-6-2-1: QR(7)

考虑例子 QR(7): $p = 7$, $p - 1 = 6$,

1. 首先, 根据定义有

$$\begin{aligned} \mathrm{QR}(7) &= \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} \\ &= \{1^2 = 6^2 = 1, 2^2 = 5^2 = 4, 3^2 = 4^2 = 2\} \\ &= \{1, 2, 4\} \end{aligned}$$

故: $|\mathrm{QR}(p)| = 3 = \frac{p-1}{2}$.

Examp-6-2-1: QR(7)

考虑例子 QR(7): $p = 7$, $p - 1 = 6$,

1. 首先, 根据定义有

$$\begin{aligned} QR(7) &= \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} \\ &= \{1^2 = 6^2 = 1, 2^2 = 5^2 = 4, 3^2 = 4^2 = 2\} \\ &= \{1, 2, 4\} \end{aligned}$$

   故: $|QR(p)| = 3 = \frac{p-1}{2}$.

2. 另一方面, 由前面例题知, 5 是模 7 的一个本原元, 故:

$$QR(7) = \{5^0, 5^2, 5^4\}$$

Examp-6-2-1: QR(7)

考虑例子 QR(7): $p = 7$, $p - 1 = 6$,

1. 首先, 根据定义有

$$\begin{aligned} QR(7) &= \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} \\ &= \{1^2 = 6^2 = 1, 2^2 = 5^2 = 4, 3^2 = 4^2 = 2\} \\ &= \{1, 2, 4\} \end{aligned}$$

   故: $|QR(p)| = 3 = \frac{p-1}{2}$.

2. 另一方面, 由前面例题知, 5 是模 7 的一个本原元, 故:

$$\begin{aligned} QR(7) &= \{5^0, 5^2, 5^4\} \\ &= \{1,\ 4,\ 2\} \end{aligned}$$

ElGamal 密码体制的语义安全性

加密算法: $E_K(x,k) = (y_1, y_2) = (\alpha^k \bmod p, x\beta^k \bmod p)$.

ElGamal 密码体制的语义安全性

加密算法: $E_K(x, k) = (y_1, y_2) = (\alpha^k \bmod p, x\beta^k \bmod p)$.

相关知识

(1) $x \in \mathrm{QR}(p) \Leftrightarrow x^{(p-1)/2} \equiv 1 \pmod p$;

(2) $\beta \in \mathrm{QR}(p) \Leftrightarrow \log_\alpha \beta$ 是偶数.

ElGamal 密码体制的语义安全性

加密算法: $E_K(x,k)=(y_1,y_2)=(\alpha^k \bmod p, x\beta^k \bmod p)$.

相关知识

(1) $x\in QR(p)\Leftrightarrow x^{(p-1)/2}\equiv 1 \pmod p$;

(2) $\beta\in QR(p)\Leftrightarrow \log_\alpha\beta$ 是偶数.

1. 由 (1) 攻击者可确定是否 $y_1,\beta\in QR(p)$, 从而可确定 $k=\log_\alpha y_1$, $a=\log_\alpha\beta$, 进而确定 ak 的奇偶性, 最后可确定是否 $\beta^k=\alpha^{ak}\in QR(p)$.

ElGamal 密码体制的语义安全性

加密算法: $E_K(x,k)=(y_1,y_2)=(\alpha^k \bmod p, x\beta^k \bmod p)$.

相关知识

(1) $x\in QR(p) \Leftrightarrow x^{(p-1)/2}\equiv 1 \pmod p$;

(2) $\beta\in QR(p) \Leftrightarrow \log_\alpha \beta$ 是偶数.

1. 由 (1) 攻击者可确定是否 $y_1,\beta\in QR(p)$, 从而可确定 $k=\log_\alpha y_1$, $a=\log_\alpha \beta$, 进而确定 ak 的奇偶性, 最后可确定是否 $\beta^k=\alpha^{ak}\in QR(p)$.
2. 给攻击者两个明文 $x_1\in QR(p)$, $x_2\notin QR(p)$ 和一个密文

$$E_K(x_i,k)=(y_1,y_2),\ i\in\{1,2\}.$$

则 (y_1,y_2) 是 x_1 的加密, 当且仅当 β^k 与 y_2 二者同为二次剩余或同为非二次剩余.

ElGamal 密码体制的语义安全性

加密算法: $E_K(x,k) = (y_1, y_2) = (\alpha^k \bmod p, x\beta^k \bmod p)$.

相关知识

(1) $x \in \mathrm{QR}(p) \Leftrightarrow x^{(p-1)/2} \equiv 1 \pmod p$;

(2) $\beta \in \mathrm{QR}(p) \Leftrightarrow \log_\alpha \beta$ 是偶数.

1. 由 (1) 攻击者可确定是否 $y_1, \beta \in \mathrm{QR}(p)$, 从而可确定 $k = \log_\alpha y_1$, $a = \log_\alpha \beta$, 进而确定 ak 的奇偶性, 最后可确定是否 $\beta^k = \alpha^{ak} \in \mathrm{QR}(p)$.
2. 给攻击者两个明文 $x_1 \in \mathrm{QR}(p)$, $x_2 \notin \mathrm{QR}(p)$ 和一个密文

$$E_K(x_i, k) = (y_1, y_2),\ i \in \{1, 2\}.$$

则 (y_1, y_2) 是 x_1 的加密, 当且仅当 β^k 与 y_2 二者同为二次剩余或同为非二次剩余.

3. 综上, ElGamal 密码体制不具有语义安全性.

ElGamal 密码体制的语义安全性

加密算法: $E_K(x,k)=(y_1,y_2)=(\alpha^k \bmod p, x\beta^k \bmod p)$.

相关知识

(1) $x\in QR(p)\Leftrightarrow x^{(p-1)/2}\equiv 1 \pmod p$;

(2) $\beta\in QR(p)\Leftrightarrow \log_\alpha\beta$ 是偶数.

1. 由 (1) 攻击者可确定是否 $y_1,\beta\in QR(p)$, 从而可确定 $k=\log_\alpha y_1$, $a=\log_\alpha\beta$, 进而确定 ak 的奇偶性, 最后可确定是否 $\beta^k=\alpha^{ak}\in QR(p)$.
2. 给攻击者两个明文 $x_1\in QR(p)$, $x_2\notin QR(p)$ 和一个密文

$$E_K(x_i,k)=(y_1,y_2),\ i\in\{1,2\}.$$

   则 (y_1,y_2) 是 x_1 的加密, 当且仅当 β^k 与 y_2 二者同为二次剩余或同为非二次剩余.
3. 综上, ElGamal 密码体制不具有语义安全性.
4. 但如果我们选择 $p=2q+1$, 并限制在 $\mathbb{Z}_p^*$ 的 q 阶子群上实现 ElGamal 密码体制, 则这种版本被猜想是语义安全的.

ElGamal 密码体制的安全性依赖于以下两个 Diffie-Hellman 问题的难解性:

(1) Computational Diffie-Hellman (CDH) 问题:

实例: 给定 $(\alpha, \alpha^a, \alpha^b)$, 这里 α 为一个模素数 p 的本原元

问题: 计算 α^{ab}

ElGamal 密码体制的安全性依赖于以下两个 Diffie-Hellman 问题的难解性:

(1) Computational Diffie-Hellman (CDH) 问题:

实例: 给定 $(\alpha, \alpha^a, \alpha^b)$, 这里 α 为一个模素数 p 的本原元

问题: 计算 α^{ab}

(2) Decision Diffie-Hellman (DDH) 问题

实例: 给定 $(\alpha, \alpha^a, \alpha^b, \alpha^c)$, 这里 α 为一个模素数 p 的本原元

问题: 判断是否有 $\alpha^{ab} = \alpha^c$ (即是否有 $c = ab \bmod (p-1)$ 成立)

计算难度比较: DDH≤ CDH≤ DL

1. CDH≤DL: 假设 OracleDL 是一个解 DL 问题的算法, 即输入 α,β, 返回

$$i = \text{OracleDL}(\alpha,\beta) = \log_\alpha \beta.$$

对给定的 $(\alpha,\alpha^a,\alpha^b)$, 可如下得到 α^{ab} (即解决 CDH 问题):

   1. $a = \text{OracleDL}(\alpha,\alpha^a), \quad b = \text{OracleDL}(\alpha,\alpha^b)$;
   2. 计算: α^{ab}.

计算难度比较: DDH≤ CDH≤ DL

1. CDH≤DL: 假设 OracleDL 是一个解 DL 问题的算法, 即输入 α,β, 返回

$$i = \text{OracleDL}(\alpha,\beta) = \log_\alpha \beta.$$

   对给定的 $(\alpha,\alpha^a,\alpha^b)$, 可如下得到 α^{ab} (即解决 CDH 问题):

   1. $a = \text{OracleDL}(\alpha,\alpha^a), \quad b = \text{OracleDL}(\alpha,\alpha^b)$;
   2. 计算: α^{ab}.

2. DDH≤ CDH: 假设 OracleCDH 是一个解 CDH 问题的算法, 即输入 α,α^a,α^b, 返回

$$\alpha^{ab} = \text{OracleCDH}(\alpha,\alpha^a,\alpha^b).$$

   对给定的 $(\alpha,\alpha^a,\alpha^b,\alpha^c)$, 可如下判断是否 $\alpha^{ab} = \alpha^c$ (即解决 DDH 问题):

   1. $\alpha^{ab} = \text{OracleCDH}(\alpha,\alpha^a,\alpha^b)$;
   2. 检查是否 $\alpha^{ab} = \alpha^c$.

解密 ElGamal 密文与求解 CDH 问题的关系

关系定理

任何求解 CDH 问题的算法, 都可以用于解密 ElGamal 密文, 反之亦然.

解密 ElGamal 密文与求解 CDH 问题的关系

关系定理

任何求解 CDH 问题的算法, 都可以用于解密 ElGamal 密文, 反之亦然.

"⇒": 假设 OracleCDH 是解 CDH 问题的一个算法, (y_1, y_2) 是 ElGamal 密码体制的密文, 具有公钥 (p, α, β).

1. $\delta = \text{OracleCDH}(\alpha, \beta, y_1) = \alpha^{ak} \bmod p$;
2. $x = y_2\delta^{-1} \bmod p = x\alpha^{ak}(\alpha^{ak})^{-1} \bmod p$.

解密 ElGamal 密文与求解 CDH 问题的关系

关系定理

任何求解 CDH 问题的算法, 都可以用于解密 ElGamal 密文, 反之亦然.

"⇒": 假设 OracleCDH 是解 CDH 问题的一个算法, (y_1, y_2) 是 ElGamal 密码体制的密文, 具有公钥 (p, α, β).

1. $\delta = \text{OracleCDH}(\alpha, \beta, y_1) = \alpha^{ak} \bmod p$;
2. $x = y_2\delta^{-1} \bmod p = x\alpha^{ak}(\alpha^{ak})^{-1} \bmod p$.

"⇐": 假设 OracleElGamal 是解密 ElGamal 密文的一个算法, CDH 问题的输入为 $(\alpha, \alpha^a, \alpha^b)$.

1. 将 $(p, \alpha, \beta = \alpha^a)$ 看作 ElGamal 密码体制的公钥, $(y_1 = \alpha^b, y_2 = k)$ 看作密文, 其中 k 是随机数;
2. 计算 $x = \text{OracleElGamal}(\alpha, \beta, y_1, y_2) = y_2(y_1)^{-a} = y_2\alpha^{-ab}$;
3. 计算 $\delta = y_2x^{-1} = y_2(y_2\alpha^{-ab})^{-1} = \alpha^{ab}$, 这就是 CDH 给定实例的解.

§6.3　椭圆曲线

Definition

设 $a, b \in \mathbb{R}$ 是满足 $4a^3 + 27b^2 \neq 0$ 的实数. 方程

$$y^2 = x^3 + ax + b$$

的所有解 $(x, y) \in \mathbb{R} \times \mathbb{R}$ 连同一个无穷远点 O 组成的集合 E 称为一个非奇异椭圆曲线.

Definition

设 $a, b \in \mathbb{R}$ 是满足 $4a^3 + 27b^2 \neq 0$ 的实数. 方程

$$y^2 = x^3 + ax + b$$

的所有解 $(x, y) \in \mathbb{R} \times \mathbb{R}$ 连同一个无穷远点 O 组成的集合 E 称为一个非奇异椭圆曲线.

1. 条件 $4a^3 + 27b^2 \neq 0$ 是保证方程 $x^3 + ax + b = 0$ 有三个解的充要条件.

Definition

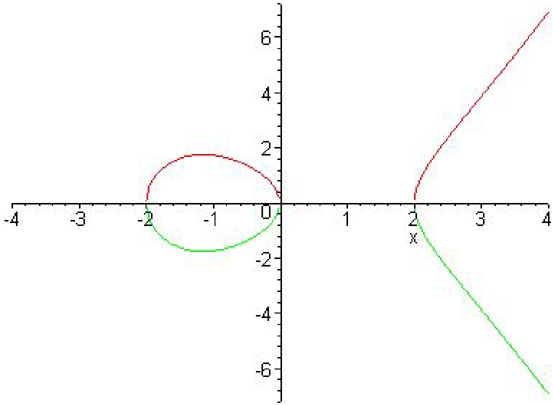
设 $a, b \in \mathbb{R}$ 是满足 $4a^3 + 27b^2 \neq 0$ 的实数. 方程

$$y^2 = x^3 + ax + b$$

的所有解 $(x, y) \in \mathbb{R} \times \mathbb{R}$ 连同一个无穷远点 O 组成的集合 E 称为一个非奇异椭圆曲线.

1. 条件 $4a^3 + 27b^2 \neq 0$ 是保证方程 $x^3 + ax + b = 0$ 有三个解的充要条件.
2. 如果 $4a^3 + 27b^2 = 0$, 对应的椭圆曲线称为奇异椭圆曲线.

Examp-6-3-1: 椭圆曲线 $y^2 = x^3 - 4x$



假设 E 是一个非奇异椭圆曲线, 点 $P=(x_1,y_1), Q=(x_2,y_2)\in E$, 定义点之间加法 “+” 为:

$$P+Q=R=(x_3,y_3),$$

其中

1. $x_1\neq x_2$ 时:

$$x_3=\lambda^2-x_1-x_2,\ \ y_3=\lambda(x_1-x_3)-y_1,\ \ \lambda=\tfrac{y_2-y_1}{x_2-x_1};$$

椭圆曲线上点的运算

假设 E 是一个非奇异椭圆曲线, 点 $P = (x_1, y_1), Q = (x_2, y_2) \in E$, 定义点之间加法“$+$”为:

$$P + Q = R = (x_3, y_3),$$

其中

1. $x_1 \neq x_2$ 时:

$$x_3 = \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1,\ \lambda = \frac{y_2 - y_1}{x_2 - x_1};$$

2. $x_1 = x_2$, 且 $y_1 = -y_2$ 时:

$$P + Q = \mathcal{O};$$

假设 E 是一个非奇异椭圆曲线, 点 $P=(x_1,y_1), Q=(x_2,y_2)\in E$, 定义点之间加法“+”为:

$$P+Q=R=(x_3,y_3),$$

其中

1. $x_1\neq x_2$ 时:

$$x_3=\lambda^2-x_1-x_2,\ y_3=\lambda(x_1-x_3)-y_1,\ \lambda=\frac{y_2-y_1}{x_2-x_1};$$

2. $x_1=x_2$, 且 $y_1=-y_2$ 时:

$$P+Q=\mathcal{O};$$

3. $x_1=x_2$, 且 $y_1=y_2$ 时:

$$x_3=\lambda^2-x_1-x_2,\ y_3=\lambda(x_1-x_3)-y_1,\ \lambda=\frac{3x_1^2+a}{2y_1}.$$

Definition

设 $p > 3$ 是素数, $4a^3 + 27b^2 \not\equiv 0 \pmod p$. $\mathbb{Z}_p$ 上同余方程

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

的所有解 $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ 连同一个无穷远点 O 组成的集合 E 称为一个 $\mathbb{Z}_p$ 上的非奇异椭圆曲线.

Definition

设 $p > 3$ 是素数, $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$. $\mathbb{Z}_p$ 上同余方程

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

的所有解 $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ 连同一个无穷远点 O 组成的集合 E 称为一个 $\mathbb{Z}_p$ 上的非奇异椭圆曲线.

1. $\mathbb{Z}_p$ 上的椭圆曲线没有象实数域上的椭圆曲线那样直观的几何解释.

Definition

设 $p > 3$ 是素数, $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$. $\mathbb{Z}_p$ 上同余方程

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

的所有解 $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ 连同一个无穷远点 O 组成的集合 E 称为一个 $\mathbb{Z}_p$ 上的非奇异椭圆曲线.

1. $\mathbb{Z}_p$ 上的椭圆曲线没有象实数域上的椭圆曲线那样直观的几何解释.
2. 但其仍然可以象 $\mathbb{Z}_p$ 上的椭圆曲线一样定义加法运算.

模素数椭圆曲线上点的运算

假设 E 是一个模素数椭圆曲线 $y^2 = x^3 + ax + b$, 点 $P = (x_1, y_1)$, $Q = (x_2, y_2)$ 之间的加法定义为:

1. 如果 $x_1 = x_2$, 且 $y_1 = -y_2$, 则
$$P + Q = \mathcal{O};$$
2. 否则 $P + Q = (x_3, y_3)$, 其中:
$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2; \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$
且
$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & P \neq Q; \\ (3x_1^2 + a)(2y_1)^{-1}, & P = Q. \end{cases}$$

Examp-6-3-2: 模素数椭圆曲线的运算

设 E 是 $\mathbb{Z}_{11}$ 上的椭圆曲线

$$y^2 = x^3 + x + 6. \tag{1}$$

我们首先确定 E 的点. 这可以通过对每个 $x \in \mathbb{Z}_{11}$, 试着解 $\mathbb{Z}_{11}$ 上方程 (1) 求 y. 具体步骤如下:

1. 对每个给定的 x, 首先利用欧拉准则来测试是否

$$z = x^3 + x + 6 \in \mathrm{QR}(11)?$$

2. 如果 $z \in \mathrm{QR}(11)$, 因 $11 \equiv 3 \pmod 4$ 时, 故 z 两个平方根是

$$\pm z^{(11+1)/4} \bmod 11 = \pm z^3 \bmod 11.$$

Examp-6-3-2 续: $\mathbb{Z}_{11}$ 上的椭圆曲线 $y^2 = x^3 + x + 6$ 的点

x	$x^3 + x + 6 \bmod 11$	$? \in QR(11)$	y
0	6	否	

Examp-6-3-2 续: $\mathbb{Z}_{11}$ 上的椭圆曲线 $y^2 = x^3 + x + 6$ 的点

x	$x^3 + x + 6 \bmod 11$	$? \in QR(11)$	y
0	6	否	
1	8	否	

Examp-6-3-2 续: $\mathbb{Z}_{11}$ 上的椭圆曲线 $y^2 = x^3 + x + 6$ 的点

x	$x^3 + x + 6 \bmod 11$	$? \in QR(11)$	y
0	6	否	
1	8	否	
2	5	是	4, 7

Examp-6-3-2 续: $\mathbb{Z}_{11}$ 上的椭圆曲线 $y^2 = x^3 + x + 6$ 的点

x	$x^3 + x + 6 \bmod 11$	$? \in \mathrm{QR}(11)$	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

Examp-6-3-2 续: $\mathbb{Z}_{11}$ 上的椭圆曲线 $y^2 = x^3 + x + 6$ 的点

x	$x^3 + x + 6 \bmod 11$	$? \in QR(11)$	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

$E = \{\mathcal{O}, (2,4), (2,7), (3,5), (3,6), (5,2), (5,9), (7,2), (7,9), (8,3), (8,8), (10,2), (10,9)\}$

Examp-6-3-2 续: 点的加法

计算: $(3,5)+(5,9)$

Examp-6-3-2 续: 点的加法

计算: $(3,5)+(5,9)$

解:

$$\begin{aligned}\lambda &= (y_2-y_1)(x_2-x_1)^{-1} \bmod p \\ &= 4\cdot 2^{-1} \bmod 11 = 2. \\ x_3 &= \lambda^2 - x_1 - x_2 = 2^2 - 8 = 7. \\ y_3 &= \lambda(x_1-x_3) - y_1 = 2\cdot 7 - 5 = 9.\end{aligned}$$

故: $(3,5)+(5,9)=(7,9)$.

倍数-和算法

对椭圆曲线上某点 P, 如何快速实现倍数运算 cP $(c \in \mathbb{Z}_{\geq 0})$?

对椭圆曲线上某点 P, 如何快速实现倍数运算 cP $(c \in \mathbb{Z}_{\geq 0})$?

DoubleAdd (c, P)

假定: c 的二进制表示为 $c = \sum_{i=0}^{l-1} c_i 2^i$, $c_i \in \{0, 1\}$

$Q \leftarrow \mathcal{O}$

for $i \leftarrow l - 1$ **downto** 0

$$\textbf{do} \begin{cases} Q \leftarrow 2Q \\ \textbf{if } c_i = 1 \\ \quad \textbf{then } Q \leftarrow Q + P \end{cases}$$

return (Q)

comment: $Q = cP$

椭圆曲线 ElGamal 密码体制

设 p 是一个大素数, E 是定义在 $\mathbb{Z}_p$ 上的椭圆曲线, 点 $\alpha \in E$. 令

$$\langle\alpha\rangle = \{n\alpha \mid n \in \mathbb{Z}_{\geq 0}\}$$

且 $\beta = a\alpha \in \langle\alpha\rangle$ (假设由 α, β 求 $a = \log_\alpha \beta$ 是困难的).
$\mathcal{P} = E, \mathcal{C} = E \times E$, 定义

$$\mathcal{K} = \{(p, \alpha, a, \beta) \mid \beta = a\alpha\},$$

其中 (p, α, β) 是公钥, a 是私钥.
对 $K = (p, \alpha, a, \beta)$, 以及一个 (秘密) 随机数 $0 < k < |\langle\alpha\rangle|$, 定义:

$$E_K(x, k) = (y_1, y_2), \quad x \in E$$

其中

$$y_1 = k\alpha, \quad y_2 = x + k\beta.$$

对 $y_1, y_2 \in E$, 定义:

$$D_K(y_1, y_2) = y_2 - ay_1.$$

9.1. 已知 ElGamal 密码体制的公钥为 $p = 31847$, $\alpha = 7$, $\beta = 18074$, 求

1. 私钥 a;
2. 加密明文 $x = 389$ (假设选择的随机数 $k = 511$), 并对得到的密文进行解密.