CSIDH方案描述（初步）

2024年10月13日 12:40

Parameters: $p \equiv 3\ (8)$, // $p = 4\ell_1\ell_2\cdots\ell_n - 1$, ℓ_i为小奇素数. // $p \equiv 3(4)$. $-1 \in QNR(p)$

$\mathcal{O} := \mathbb{Z}[\pi] \cong \mathbb{Z}[\sqrt{-p}]$, // $i = \sqrt{-1} \in \mathbb{F}_{p^2}$.

$G := Cl(\mathcal{O})$, $X := \{E/\mathbb{F}_p : E$超奇异$,\ End_{\mathbb{F}_p}(E) = \mathcal{O}\}/\cong_{\mathbb{F}_p}$

Facts: $E_0 \in X$, $|X| = |G| \approx \sqrt{p}$, G交换. $E_0: y^2 = x^3 + x$

(CM Torsor) $G \curvearrowright X$ 自由且可迁. //类比复环面的复乘.

CSIDH 协议

	Alice		Bob
skgen:	$a \xleftarrow{\$} G$.		$b \xleftarrow{\$} G$
pkgen:	$E_A = a * E_0$	$\xrightarrow{E_A}$ $\xleftarrow{E_B}$	$E_B = b * E_0$
derive:	$a * E_B = E_S$		$b * E_A = E_S$

$S \in \mathbb{F}_p$ 作为共享密钥.

正确性: $a*(b*E_0) = ab*E_0$ $b*(a*E_0) = ba*E_0 \overset{G交换}{=\!=} ab*E_0$.

同源在哪？

同源计算与密钥空间

2024年10月13日　17:12

1. 同源↔群作用

$g*E$ 对应一些同源 $\{\varphi : E \to g*E\}$. 算 $g*E$ 就是算同源的值域.

$g*E$: 实际上,定义 $I*E := E/E[I] =: E_I$　　　$J \lhd \mathbb{Z}[\pi] = \mathrm{End}_{\mathbb{F}_p}(E)$

$E[I] = \{P\in E : \alpha(P) = \infty,\ \forall \alpha \in I\} = \bigcap_{\alpha\in I} \ker(\alpha) \leq E$

若 $I_1 \sim I_2$, 则 $E_{I_1} \cong_{\mathbb{F}_p} E_{I_2}$. 可以定义 $[I]*E = E_I$ 所在 $\mathbb{F}_p$-同构类.

具体来说, 选定 $E\in X$, $[I]\in G \leftrightarrow \{E[J] \mid J\in[I]\} \leftrightarrow \{\varphi_J : E \to E/\underbrace{E[J]}_{\text{定义在 } \mathbb{F}_p \text{ 上}} := \overset{[I]*E}{E_J}\}$

有 $\forall I_1, I_2 \in [I]$, $E_{I_1} \cong_{\mathbb{F}_p} E_{I_2} \in g*E$.

2、 l_i-同源.

Q: 直接选一个 $J\in[I]$, 计算 φ_J

A: ① $\#E[I]$ 通常很大. Vélu算法: $O(\#E[I])$ or $\tilde{O}(\sqrt{\#E[J]})$

② 通常 $E[I] \not\subset E(\mathbb{F}_p)$, 扩域上开销大.

③ 选哪个 φ_J 来算?

(1) 先找好算的!

回顾 $p = 4l_1l_2\cdots l_n - 1$, E 超奇异 $\Rightarrow$ $E(\mathbb{F}_p)$ 是 $4l_1\cdots l_n$ 阶循环群.

设 $P_i \in E(\mathbb{F}_p)$, $\mathrm{ord}(P_i) = l_i$.

FACT: $\exists\, g_i \in G$, $g_i * E = E/\langle P_i\rangle$

$\prod g_i^{e_i} * E$ 好算! (l_i 小)　　　// 一连串 l_i-同源.

(2) 都能算、

启发式假设: 取 $K = \{(e_1,\ldots,e_n)\in\mathbb{Z}^n, |e_i|\leq m\}$, $|K| < |G|$, 则 $\#\{\prod g_i^{e_i} : (e_1,\ldots,e_n)\in K\} \approx |K|$ (很少重复)

来自 Gauss 启发式 + Cohen-Lenstra 启发式.

Cohen-Lenstra: $G = Cl(\mathcal{O})$ "几乎循环". i.e. 有大循环子群 H,

$g_1,\ldots,g_n$ 中有生成元, 不妨设为 g_1. 且 $g_i = g_1^{a_i}$. 给定 $h = g_1^{b} \in G$, 则

$g_1^{e_1}\cdots g_n^{e_n} = h$, e_i 小 $\Leftrightarrow x_1 + x_2a_2 + \cdots + x_na_n = b$ 有小解 $(e_1,\ldots,e_n)$

$(e_1,\dots,e_n) \in$ 格 L 的陪集， $L = \begin{bmatrix} |H| & 0 & 0 & \cdots & 0 \\ -a_2 & 1 & 0 & \cdots & 0 \\ -a_3 & 0 & 1 & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \\ -a_n & 0 & 0 & \cdots & 1 \end{bmatrix}$ （行向量张成）

解数 $\approx \dfrac{\mathrm{vol}([-m,m]^n)}{\det(L)} = \dfrac{|K|}{|H|} \gtrsim \dfrac{|K|}{|G|} < 1.$

$\Rightarrow \#\{\prod g_i^{e_i}\} \approx |K|.$

Q: $K \subset \{(e_1,\dots,e_n) \in \mathbb{Z}^n\}$

允许 $e_i < 0$?

A: $g_t^{-1} * E = E/\langle Q_t\rangle$, $Q_t = (x, iy)$, $\mathrm{ord}(Q_t) = \ell_i$, 能算.

RMK. 私钥空间 $|K| = (2m+1)^n$. CSIDH-512. p 512 bit, $|G| \approx \sqrt{p} \approx 2^{256}$. 选取 m s.t. $(2m+1)^n \approx 2^{256}$.

skgen: 即 $\vec{v} \xleftarrow{\$} K$

g_i, g_i^{-1}是什么

13:22

$End_{\mathbb{F}_p}(E) = \mathcal{O} = \mathbb{Z}[\pi] \cong \mathbb{Z}[\sqrt{-p}]$.

$$\pi : E \to E$$
$$(x,y) \mapsto (x^p, y^p)$$
$$\infty \mapsto \infty.$$

Let π the Frobenius endomorphism. Ideal in $\mathcal{O}$ above ℓ_i.

$$\mathfrak{l}_i = (\ell_i, \pi - 1).$$

Why $g_i = [L_i]$?

Moving $+$ in X with ℓ_i isogeny $\iff$ action of $\mathfrak{l}_i$ on X.

More precisely:
Subgroup corresponding to $\mathfrak{l}_i$ is $E[\mathfrak{l}_i] = E(\mathbb{F}_p)[\ell_i]$.
(Note that $\ker(\pi - 1)$ is just the $\mathbb{F}_p$-rational points!)

Subgroup corresponding to $\overline{\mathfrak{l}_i}$ is

$$E[\overline{\mathfrak{l}_i}] = \{P \in E[\ell_i] \mid \pi(P) = -P\}.$$

For supersingular Montgomery curves over $\mathbb{F}_p$, $p \equiv 3 \bmod 4$

$$E[\overline{\mathfrak{l}_i}] = \{(x,y) \in E[\ell_i] \mid x \in \mathbb{F}_p;\ y \notin \mathbb{F}_p\} \cup \{\infty\}.$$

$g_i = [L_i]$, $L_i = (\ell_i, \pi - 1)$ $\longleftrightarrow$

$$E[L_i] = \{P \in E : \alpha(P) = \infty, \forall \alpha \in L_i\} \leq E$$
$$= \bigcap_{\alpha \in L_i} \ker(\alpha) = \ker(\ell_i) \cap \ker(\pi - 1).$$

$$\ell_i : \begin{array}{l} E \to E \\ P \mapsto [\ell_i]P \end{array} \qquad \pi - 1 : P \mapsto \pi(P) - P$$

$\ker(\pi - 1) = \{P \in E \mid \pi(P) = P\} = \{(x,y) \in E \mid x^p = x, y^p = y\}$

$= E(\mathbb{F}_p)$ $\quad \ker(\ell_i) = E[\ell_i]$, $E(\mathbb{F}_p)$ 是 $4\ell_1 \cdots \ell_n$ 循环群

$E[L_i] = \langle P_i \rangle$, $P_i \in E(\mathbb{F}_p)$, $\mathrm{ord}(P_i) = \ell_i$

Ref: [Tanja Lange - Isogeny-basd cryptography IV - Math details]

在 $Cl(\mathcal{O})$ 中, 单位元 = {主理想}. $[\ell_i \mathcal{O}]$ = 单位元.

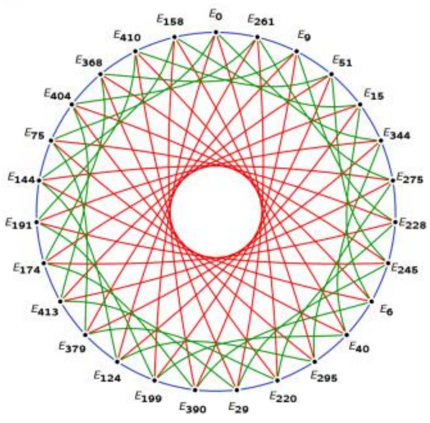
$\ell_i \mathcal{O} = L_i \overline{L_i}$, $L_i = (\ell_i, \pi - 1)$, $\overline{L_i} = (\ell_i, \pi + 1)$

$\ker(\pi + 1) = \{(x, iy) \in E \mid x, y \in \mathbb{F}_p\}$.

$E[L_i] = E[\ell_i] \cap E[\pi - 1] = E[\ell_i] \cap E(\mathbb{F}_p)$

$E[\overline{L_i}] = $ ------ $\pi + 1$ $= E[\ell_i] \cap \{(x, iy) \in E \mid x, y \in \mathbb{F}_p\}$

Graphs of elliptic curves



Nodes: Supersingular elliptic curves $E_A: y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.
Each E_A on the left has E_{-A} on the right.
Negative direction means: flip to twist, go positive direction, flip back.

Tanja Lange $\quad$ Isogeny-basd cryptography IV $\quad$ 7

群作用计算

2024年10月13日　18:51

例：　$p = 4\cdot l_1\cdot l_2\cdot l_3\cdots l_n - 1$.　$l_i = 3,5,7$　.　p有1024 bit.

任务：算 $g_3 * g_2 * g_1 * E$.　暂记　$g_i * \cdots * g_1 * E = E_i$，$\varphi_i : E_{i-1} \to E_i$

1、朴素法

1° 算 $\varphi_1 : E \longrightarrow E_1$

① $R \xleftarrow{\$} E(\mathbb{F}_p)$,

② $P_1 := [\frac{p+1}{l_1}] R$,　假定 $P_1 \neq \infty$.

③ Vélu算法算 $E \longrightarrow E_1 = E/\langle P_1 \rangle$ 的值域曲线系数.

2° 算 $\varphi_2 : E_1 \to E_2$

① $R \xleftarrow{\$} E_1(\mathbb{F}_p)$

② $P_2 = [\frac{p+1}{l_2}] R$.　$P_2 \neq \infty$　③ Vélu 值域

3° …… .

取点需算 Legendre 符号！ 开销大.　1次 ≈ 1500M + 3000S

能否少取点？

2. 改进：一次取点，做完全部.

1° 算 $\varphi_1 : E \longrightarrow E_1$

① $R \xleftarrow{\$} E(\mathbb{F}_p)$,　$R \leftarrow [4] R_1$　// 可改为 $[4 l_4 l_5 l_6 \cdots l_n] R$.

② $P_1 := [\frac{p+1}{4 l_1}] R$,　假定 $P_1 \neq \infty$.

③ Vélu算法算 $E \longrightarrow E_1 = E/\langle P_1 \rangle$ 的值域曲线系数，推点 $R' \leftarrow \varphi_1(R)$

2° 算 $\varphi_2 : E_1 \to E_2$：

① $P_2 \leftarrow [\frac{p+1}{4 l_1 l_2}] R'$.　// $\mathrm{ord}(R') = \frac{\mathrm{ord}(R)}{l_1}$

② 算 φ_2 值域，　$R'' \leftarrow \varphi_1(R)$

3° 算 $\varphi_3 : E_2 \to E_3$：

① $P_3 \leftarrow [\frac{p+1}{4 l_1 l_2 l_3}] R''$

② 算 φ_3 值域 .

实际 CSIDH 中算 $g_1^{e_1} \cdots g_n^{e_n} * E$. 每轮算下所有没算完的.

Q1: $P_i = \infty$ 咋办

A1: 跳过 g_i, 以后再算. 偶尔才会.

Q2: 算负的呢?

A2: Elligator 算法, 一次取到 $(x,y) \in E_A(\mathbb{F}_p)$ 和 $(x, iy) \in E_A^t(\mathbb{F}_p) \cong E_{-A}(\mathbb{F}_p)$.

$g_i \updownarrow$, $g_i^{-1} \updownarrow$

$E_A: \quad y^2 = x^3 + Ax^2 + x$.

开销: 1 个 Legendre 符号. $\quad x \xleftarrow{\$} \mathbb{F}_p$. $\quad x^3 + Ax^2 + x \overset{?}{\in} QR(p)$

3, 更换顺序.

$g_1 * g_2 * g_3 * E = g_3 * g_2 * g_1 * E$. Exercise: 开销?

同源前: 无区别, 取点: 无区别

假设 $p = 4 \cdot 3 \cdot 5 \cdot 7 - 1$, $\quad g_3 * g_2 * g_1 * E$: $\quad 1^\circ\ R \xleftarrow{\$} E(\mathbb{F}_p)$ $\quad 2^\circ\ R \leftarrow [4]R$. ($ord(R) = 3.5.7$) $\quad 3^\circ\ \underset{P_1}{[5 \cdot 7]R}$, $R' = \varphi_1(R)$ ($ord(R') = 5 \cdot 7$)

$4^\circ\ P_2 \leftarrow [7]R'$ $\quad R'' \leftarrow \varphi_2(R')$ ($ord(R'') = 7$) $\quad 5^\circ\ P_3 = [1]R$

效率: $\wedge$

$g_1 * g_2 * g_3 * E$: $\quad 1^\circ \cdots 2^\circ \cdots 3^\circ\ P_3 = [3 \cdot 5]R$, $R' = \varphi_1(R)$ ($ord(R') = 3.5$) $\quad 4^\circ\ P_2 = [3]R'$, $\cdots$

$5^\circ\ [1]$

4. 再调整

次数最大同源, 放在最后一个.

5. 长串作用计算

$g_1 * \cdots * g_n * E \qquad n = 100 \sim 200$

先作 $g_1 * \cdots * g_k$, 再作 $g_k * \cdots * g_n$, 减少标量乘开销, 增加1次取点 (Legendre 符号).

调优: 最优分批.

6. CSIDH 计算层次

- 密钥生成
- 群作用计算
- ℓ_i-同源计算，超奇异验证。 Vélu, √élu,
- 椭圆曲线点（加法，倍点，取随机点） XMUL-Ladder $A_1 A_2^{-1}$. A_1, A_2
- 有限域

安全性和开销

2024年10月13日 21:21

经典安全性：{ 中间相遇 / 小步大步　　复杂度 $\sqrt{|K|} \approx \sqrt{|G|} \approx p^{\frac{1}{4}}$　　NIST-I 经典安全性 128 bit ⇓ CSIDH-512

量子安全性：Hidden Shift Problem over Abelian group ⇒ $\overset{\text{subgroup}}{\text{HSP}}$ 隐藏子群是一个二面体群(非交换)
有亚指数攻击
Kuperberg sieve

$\underbrace{E_A}$ = $\underbrace{sk}$ * $\underbrace{E_0}$ ↑ Hidden Shift Problem

最初评估　CSIDH-512 ≈ AES-128 (Grover) ≈ 2^{84}　　最初一次 oracle：$O(2^{40+})$
反折后　CSIDH-512　$2^{57.\cdots}$　≈ 2^{60}　　一次 oracle：$O(2^{19\sim 20\cdots})$

现在　CSIDH-2048 达到 NIST-I

开销：CSIDH-512　：$\overset{\text{一次群作用}}{50\text{ms}}$，甚至 40ms
CSIDH-2048：一次群作用　1.2G CPU周期 $\overset{(2.4\text{GHz})}{}$ = 500ms

假如 512 复活，并行 + 优化 $\overset{\text{个人估计}}{\approx}$ 10ms (偏理论)　　$a_1 a_2 \cdots a_n$　4核、3X ~ 4X 加速
2048　$\overset{\text{估计}}{\approx}$ 100ms

一些误区

2024年10月13日 15:53

1. Q: 选定 $E \in X$, $\{g \in G\} \longleftrightarrow \{E[g] \leq E\} \longleftrightarrow \{\varphi_g : E \to E/E[g]\}$ 一一对应?

并非E的任意子群　　　　定义在 $\mathbb{F}_p$ 上.

A: 错. 真实情况: $[I] \longleftrightarrow \{E[I] \leq E\} \longleftrightarrow \{\varphi_I : E \to E/E[I] =: E_I\}$.

但是当 $I \sim J$ 时, 有 $E_I \simeq_{\mathbb{F}_p} E_J$.

The ideal class group $\mathcal{C}\ell(\mathcal{O})$ acts freely and transitively on $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ [15, Theorem 7] as follows: given $[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O})$, we define $[\mathfrak{a}] \star [E]$ — or $E/\mathfrak{a}$ or $\mathfrak{a} \star E$ for simplicity — to be the codomain of the unique (up to $\mathbb{F}_p$-isomorphism) isogeny $\varphi_{\mathfrak{a}} : E \to E/\mathfrak{a}$ with kernel $\cap_{\alpha \in \mathfrak{a}} \mathrm{Ker}(\alpha)$. One can check that this definition does not depend on the representative chosen for $[\mathfrak{a}]$. On the other hand, we remark that $\varphi_{\mathfrak{a}}$ *does* depend on such choice, and its degree equals the norm of $\mathfrak{a}$.

Ref: A review of mathematical and computational aspects of CSIDH algorithms