同種写像暗号 3
デジタル署名方式 SQISign

九州大学 IMI 共同利用・短期共同研究 プログラム
セキュアな量子情報活用に向けた次世代暗号の数理

小貫 啓史

東京大学

2022/8/2

目次

目次

概要

SQISign

- 同種写像ベース署名方式 [DKL+20a, Asiacrypt 2020]
- 同種写像暗号の中では最も有望な署名方式の候補
- 2 つの重要なアルゴリズムを構築:
  - generalized KLPT
  - IdealToIsogeny

その後の研究

- SQISign 著者の一部による高速化・ゼロ知識性の解析 (2022) [DLW22]
- 公開鍵の安全性解析 (2022) [Onu22]

※ SIDH への攻撃 [CD22] は (少なくともそのままでは) 適用できない.

同種写像ベース署名方式

- Stolbunov のアイデア [Sto12]: 通常曲線の HHS ベース
- GPS schemes [GPS17]: KLPT ベース, SIDH ベース
- SeaSign [DG19]: CSIDH ベース
- CSI-FiSh [BKV19]: CSIDH ベース (SeaSign の改善版)
- **SQISign** [DKL+20a]: generalized KLPT ベース, 今回のテーマ

SQISign の性能

	公開鍵長+署名長 (Byte)	鍵生成 (ms)	署名 (ms)	検証 (ms)
Falcon*1	$897 + 666 = 1563$	8.64	$1/5.948$	$1/27.933$
CSI-FiSh	$512 + 956 = 1468$	400	1480	1480
SQISign*2	**64 + 204 = 268**	**218**	**1081**	**19**

*1 格子ベース署名, NIST PQC 標準方式で公開鍵長＋署名長が最も短い
*2 [DLW22] による高速化を適用. パラメータの選び方は若干要修正 (後述).

- 公開鍵長＋署名長は、Falcon, CSI-FiSh の 1/5 以下
- CSI-FiSh より速いが、Falcon よりは遅い

目次

Deuring 対応

p：(大きな) 素数.
$B_{p,\infty}$：p と ∞ で分岐する $\mathbb{Q}$ 上の四元数代数.

$$B_{p,\infty} \cong \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij \quad (i^2 = -q, j^2 = -p, ij = -ji)$$

となる正整数 q が存在する. ($p \equiv 3 \pmod 4$ のとき, $q = 1$ と取れる.)

Deuring 対応

$$\{ \text{超特異楕円曲線 } /\mathbb{F}_{p^2} \}/\cong \; / \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) \quad \overset{1:1}{\longleftrightarrow} \quad \{ \text{極大整環 } \subset B_{p,\infty} \}/\cong$$

$$E \quad \longleftrightarrow \quad \mathcal{O} \text{ s.t. } \mathcal{O} \cong \mathrm{End}(E)$$

$$\text{同種写像 } \varphi : E_1 \to E_2 \quad \longleftrightarrow \quad I : \text{左 } \mathcal{O}_1\text{-ideal, 右 } \mathcal{O}_2\text{-ideal}$$

上の I を $\mathcal{O}_1$ と $\mathcal{O}_2$ の **connecting ideal** という.

$p = 3 \pmod 4$ のとき, $j(E) = 1728$ となる楕円曲線 E は超特異で,

$$\mathrm{End}(E) \cong \left\langle 1, i, \frac{1+j}{2}, \frac{i+ij}{2} \right\rangle.$$

用語の定義

定義 1

$x = a + bi + cj + dij \in B_{p,\infty}$ の**ノルム** $n(x) := a^2 + b^2q + c^2p + d^2pq$.
Ideal I の**ノルム** $n(I) := \gcd\{n(x) \mid x \in I\}$.

$\deg(\varphi_I) = n(I)$.

定義 2

左 $\mathcal{O}$-ideal I, J が **equivalent** $\overset{\text{Def.}}{\iff} \exists \beta \in (B_{p,\infty})^\times$ s.t. $I = J\beta$.

このとき, $I \sim J$ とかく, さらに対応する同種写像 φ_I, φ_J の行き先は同型.

定義 3

$B_{p,\infty}$ の極大整環 $\mathcal{O}$ が **special extremal** とは,
R を $Q(i)$ の整数環としたとき, $R + jR \subseteq \mathcal{O}$ が成り立つこと.

$p = 3 \pmod 4$ のとき, $\left\langle 1, i, \frac{1+j}{2}, \frac{i+ij}{2} \right\rangle$ は special extremal.

数論アルゴリズム的 Deuring 対応 (1/4)

問題 1 (Deuring 対応 $\to$)

超特異楕円曲線 E に対して, 極大整環 $\mathcal{O}$ s.t. $\mathcal{O} \cong \mathrm{End}(E)$ を計算せよ.

問題 2 (Deuring 対応 $\leftarrow$)

極大整環 $\mathcal{O}$ に対して, 超特異楕円曲線 E s.t. $\mathcal{O} \cong \mathrm{End}(E)$ を計算せよ.

定理 1

- 超特異同種写像問題と問題 1 は, $\log p$ の確率的多項式時間アルゴリズムで互いに帰着可能.
- 問題 2 は $\log p$ の確率的多項式時間アルゴリズムで計算可能.

under some heuristics [EHL+18] or GRH [Wes22].

数論アルゴリズム的 Deuring 対応 (2/4)

定理 2 ([Piz80])

以下の $\mathcal{O}_0$ は $B_{p,\infty}$ の極大整環.

p	(i^2, j^2)	$\mathcal{O}_0$
$3 \bmod 4$	$(-1, -p)$	$\left\langle 1, i, \frac{1+j}{2}, \frac{i+ij}{2} \right\rangle$
$5 \bmod 8$	$(-2, -p)$	$\left\langle 1, i, \frac{2-j+ij}{2}, \frac{-1+i+j}{2} \right\rangle$
$1 \bmod 8$	$(-q, -p)$	$\left\langle \frac{1+i}{2}, \frac{j+ij}{2}, \frac{i+cij}{q}, ij \right\rangle$

q は素数で $q \equiv 3 \pmod 4$, $\left(\frac{p}{q}\right) = -1$, $c \equiv -1/p \pmod q$.
(GRH の下で $q = O(\log^2 p)$.)

定理 3 ([PL17])

$\mathcal{O}_0$ に対応する超特異楕円曲線 E_0 と同型写像 $\mathcal{O}_0 \xrightarrow{\sim} \mathrm{End}(E_0)$ は $\log p$ の確率的多項式時間で計算可能.

$\mathcal{O}_0$ は special extremal. $\because R = \mathbb{Z}[i]$ or $\mathbb{Z}[\frac{1+i}{2}]$.

数論アルゴリズム的 Deuring 対応 (3/4)

問題 2 の解法

入力: 極大整環 $\mathcal{O}$
出力: 超特異楕円曲線 E s.t. $\mathcal{O} \cong \mathrm{End}(E)$.

1. 1 つ Deuring 対応 $(E_0, \mathcal{O}_0, \iota)$ s.t. $\iota : \mathcal{O}_0 \xrightarrow{\sim} \mathrm{End}(E_0)$ をとる.
2. $\mathcal{O}_0$ と $\mathcal{O}$ の connecting ideal I を計算する.
   ($I = N\mathcal{O}_0\mathcal{O}$ where $N = [\mathcal{O}_0 : \mathcal{O}_0 \cap \mathcal{O}]$)
3. I に対応する同種写像 φ_I を計算し, その行き先 E を出力.
   ($\ker \varphi_I = E_0[I] := \{P \in E \mid \iota(\alpha)P = \infty \text{ for all } \alpha \in I\}$)

問題点:

1. $\deg \varphi_I = n(I)$ が smooth とは限らない. (高い確率で $n(I) > p^{1/2}$.)
2. $E_0[I]$ の定義体が ($\log p$ に関して指数的な) 高次元かもしれない.

I を同種写像が計算し易い equivalent な ideal に変換したい
$\Rightarrow$ KLPT アルゴリズム [KLPT14]

数論アルゴリズム的 Deuring 対応 (4/4)

同種写像問題 $\Rightarrow$ 問題 1 の帰着

入力: 超特異楕円曲線 E_1, E_2, 問題 1 のオラクル $\mathcal{A}$.
出力: 同種写像 $\varphi : E_1 \to E_2$.

1. $\mathcal{O}_1 = \mathcal{A}(E_1)$, $\mathcal{O}_2 = \mathcal{A}(E_2)$ を計算.
2. 問題 2 のアルゴリズムで $\varphi_1 : E_0 \to E_1$, $\varphi_2 : E_0 \to E_2$ を計算.
3. $\varphi_2 \circ \widehat{\varphi_1}$ を出力.

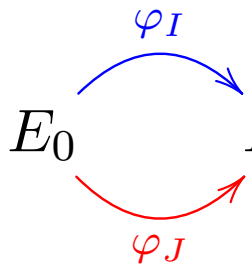
KLPT アルゴリズム [KLPT14]

Kohel-Lauter-Petit-Tignol アルゴリズム

入力：special extremal 極大整環 $\mathcal{O}_0$, 左 $\mathcal{O}_0$-ideal I,
$\mathbb{Z}_{>0}$ の部分集合 $\mathcal{C}$ (出力ノルムの条件).

出力：左 $\mathcal{O}_0$-ideal J s.t. $J \sim I$, $n(J) \in \mathcal{C}$.

楕円曲線の世界での対応



Given φ_I, find φ_J s.t. $\deg(\varphi_J) \in \mathcal{C}$.

$\widehat{\varphi_J} \circ \varphi_I \in \mathrm{End}(E_0) \leftrightarrow \beta \in I$ s.t. $n(\beta)/n(I) \in \mathcal{C}$.
$\Rightarrow$ rank 4 の $\mathbb{Z}$ 格子 I 上でノルム条件を満たす元を探す問題

ノルム条件 $\mathcal{C}$ の例

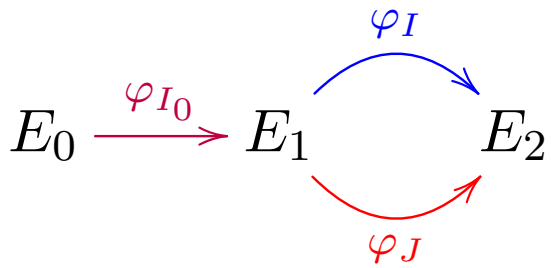
{ 小さな素数のべき }, {power smooth numbers}, {(Given)T の約数 }

generalized KLPT アルゴリズム [DKL+20a]

入力：special extremal 極大整環 $\mathcal{O}_0$, 極大整環 $\mathcal{O}$,
$\mathcal{O}_0$ と $\mathcal{O}$ の connecting ideal I_0, 左 $\mathcal{O}$-ideal I.
$\mathbb{Z}_{>0}$ の部分集合 $\mathcal{C}$ (出力ノルムの条件).

出力：左 $\mathcal{O}$-ideal J s.t. $J \sim I$, $n(J) \in \mathcal{C}$.

楕円曲線の世界での対応



一般の超特異楕円曲線 E_1 に対して, $\widehat{\varphi_J} \circ \varphi_I \in \mathrm{End}(E_1) \backslash \mathbb{Z}$ を見つけるのは**同種写像問題を解くのと同じくらい難しい**.

$\Rightarrow$ generalized KLPT を実行するには I_0 が必要.

SQISign では, I_0 が秘密鍵, generalized KLPT の実行が署名となる.

出力ノルムの制約

(generalized) KLPT アルゴリズムでは以下の Diophantus 方程式 (の変種) が (何度か) 現れる.

Given N, find $a, b, c, d \in \mathbb{Z}$ s.t. $n(a+bi+cj+bij) = N,\ (c,d) \neq (0,0)$.

$(a^2 + b^2 + p(c^2 + d^2) = N$ if $p \equiv 3 \pmod 4$.)

解法: ランダムに c, d を取り, $a^2 + b^2 = N - p(c^2 + d^2)$ を解く.

- 少なくとも $N > p$.
- p くらいのサイズの素因数分解が必要.
- 成功するかどうかはランダム.

出力ノルムのサイズ

- KLPT では $> p^3$.
- generalized KLPT では $> p^3 n(I_0)^3$ ($n(I_0)$ は素数).
- このサイズ以上であればどのような数でも良い.

IdealToIsogeny (1/3)

KLPT の出力 I に対して, φ_I をどのように計算するか？

Power-smooth 法

ある閾値 B と相異なる素数 $\ell_1, \ldots, \ell_n$ を取って,

$$n(I) = \prod_i \ell_i^{e_i} \text{ for } \ell^{e_i} < B$$

とし, $I = I_1 \cdots I_n$ s.t. $n(I_i) = \ell_i^{e_i}$ と分解して, $I_1, \ldots, I_n$ に対応する同種写像を順に計算する:

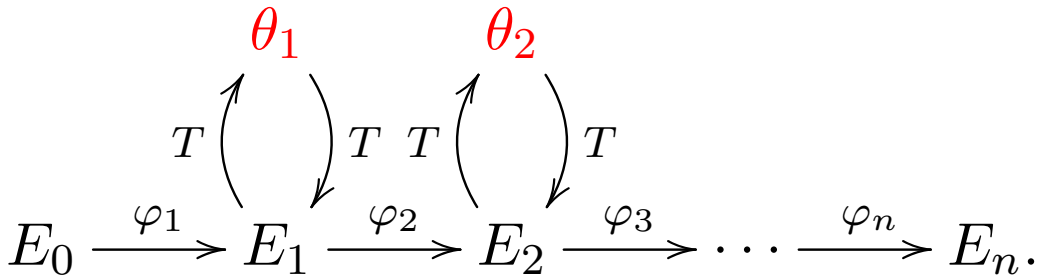
$$E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} E_n.$$

- φ_i によって $I_{i+1} \cdots I_n$ の情報を E_i に送る必要がある.
  $\Rightarrow \deg \varphi_i$ と $n(I_{i+1} \cdots I_n)$ が**互いに素**でなくてはならない.
- p^3 以上の数の約数の torsion subgroup が必要.

IdealToIsogeny (2/3)

IdealToIsogenyEichler [DLW22]

$E_0[\ell^e] \subset E_0(\mathbb{F}_{p^2})$ なる素数 ℓ と正整数 e をとり,
$n(I) = \ell^{en}$ とし, $I = I_1 \cdots I_n$ s.t. $n(I_i) = \ell^e$ と分解する.
ℓ と素な T に対して, $\ker \widehat{\varphi_i}$ の distortion map θ_i s.t. $\deg \theta_i \mid T^2$.
(I.e., $\langle P_i \rangle = \ker \widehat{\varphi_i}$ なる P_i に対して $\theta_i(P_i) \notin \langle P_i \rangle$.)



$\langle [A]P_i + [B]\theta_i(P_i) \rangle = \ker \varphi_{i+1}$ となる $A, B \in \mathbb{Z}$ が計算可能.

- θ_i により四元数代数の情報を楕円曲線に移している.
- $T > p^{1.25}$ なら θ_i が見つかる.
- $p^{1.25}$ 以上の数の約数の torsion subgroup が必要.

IdealToIsogeny (3/3)

どれぐらいの体拡大が必要？

⇒ 2 次 twist により, $p^2 - 1$ の約数次の同種写像は $\mathbb{F}_{p^2}$ 上で計算可能.
SQISign は $p^2 - 1$ を smooth にとり, $\mathbb{F}_{p^2}$ 上の計算で完結.

どれぐらい smooth なら同種写像が “**現実的に計算可能**” か？

⇒ $\sqrt{\text{élu}}$ の公式 [BDLS20] により高次の同種写像の計算が高速化.
改善版 SQISign [DLW22] では最大 3923 次,
鍵交換方式 B-SIDH [Cos20] では最大 76667 次の同種写像が現れる [1].

[1] B-SIDH の KEM 版の計算時間は 119 Mcycles と見積もられている [ACDRH22].

目次

ゼロ知識証明

ゼロ知識証明とは, 証明者が「秘密の情報 s を知っている」ことを情報を一切漏らすことなく (ゼロ知識), 検証者に納得されるプロセスのこと.

Σ プロトコル

1. 証明者は検証者に**コミットメント** M を送る.
2. 検証者は証明者に**チャレンジ** $C = C(M)$ を送る.
3. 証明者は検証者に**レスポンス** $R = R(s, M, C)$ を送る.
4. 検証者は M, C, R により受け入れか, 拒否かを決める.

- **(correctness)**
  プロトコルが正しく行われれば, 必ず証明が受け入れられる.
- **(soundness)**
  $R(s, M, C)$ と $R(s, M, C')$ $(C \neq C')$ から s が計算できる.
- **(honest-verifier zero-knowledge)**
  受け入れられる組 (M, C, R) は s なしで計算できる.

SQISign のプロトコル

秘密の同種写像 $\tau : E_0 \to E_A$ を知っていることのゼロ知識証明

E_0 : 超特異楕円曲線 s.t. $\mathrm{End}(E_0) \cong \mathcal{O}_0$, 固定の公開パラメータ

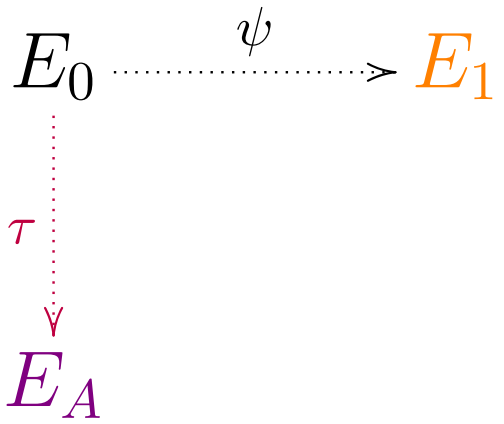
E_A : $\mathbb{F}_{p^2}$ 上の超特異楕円曲線, 公開鍵

SQISign のプロトコル

秘密の同種写像 $\tau : E_0 \to E_A$ を知っていることのゼロ知識証明

E_0 : 超特異楕円曲線 s.t. $\mathrm{End}(E_0) \cong \mathcal{O}_0$, 固定の公開パラメータ

E_A : $\mathbb{F}_{p^2}$ 上の超特異楕円曲線, 公開鍵



E_1 : コミットメント

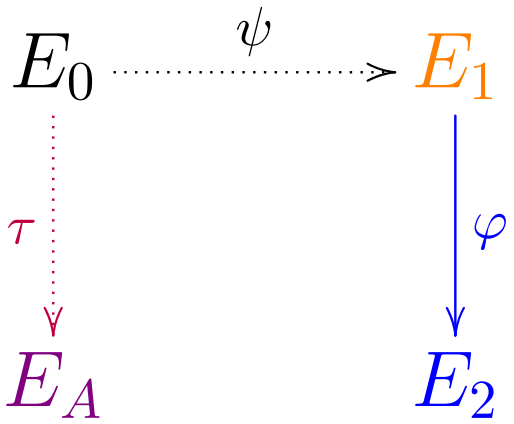
証明者は $\psi : E_0 \to E_1$ を計算し、コミットメント E_1 を検証者に送る

SQISign のプロトコル

秘密の同種写像 $\tau : E_0 \to E_A$ を知っていることのゼロ知識証明

E_0 : 超特異楕円曲線 s.t. $\mathrm{End}(E_0) \cong \mathcal{O}_0$, 固定の公開パラメータ

E_A : $\mathbb{F}_{p^2}$ 上の超特異楕円曲線, 公開鍵



E_1 : コミットメント

φ, E_2 : チャレンジ

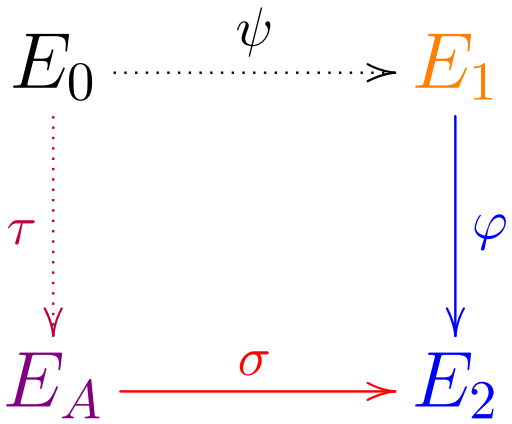
検証者は $\varphi : E_1 \to E_2$ を計算し、チャレンジ φ, E_2 を証明者に送る

SQISign のプロトコル

秘密の同種写像 $\tau : E_0 \to E_A$ を知っていることのゼロ知識証明

E_0 : 超特異楕円曲線 s.t. $\mathrm{End}(E_0) \cong \mathcal{O}_0$, 固定の公開パラメータ

E_A : $\mathbb{F}_{p^2}$ 上の超特異楕円曲線, 公開鍵



E_1	:	コミットメント
φ, E_2	:	チャレンジ
σ	:	レスポンス

証明者は τ と $\varphi \circ \psi \circ \hat{\tau}$ から generalized KLPT アルゴリズムにより

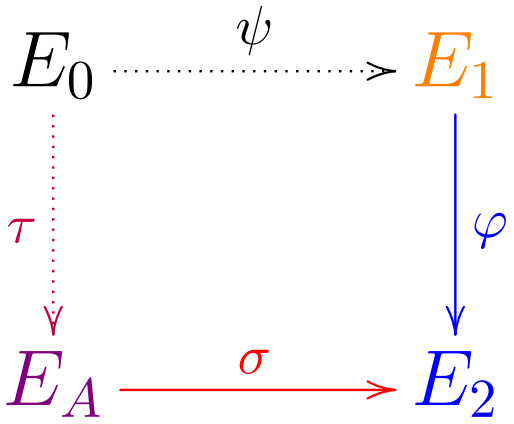
$\sigma : E_A \to E_2$ を計算し、レスポンス σ を検証者に送る

SQISign のプロトコル

秘密の同種写像 $\tau : E_0 \to E_A$ を知っていることのゼロ知識証明

E_0 : 超特異楕円曲線 s.t. $\mathrm{End}(E_0) \cong \mathcal{O}_0$, 固定の公開パラメータ

E_A : $\mathbb{F}_{p^2}$ 上の超特異楕円曲線, 公開鍵



E_1 : コミットメント

φ, E_2 : チャレンジ

σ : レスポンス

検証者は σ が E_A から E_2 への同種写像であることを確認する

目次

想定される攻撃

$\mathbb{F}_{p^2}$ 上の超特異楕円曲線上の同種写像問題を解くアルゴリズム

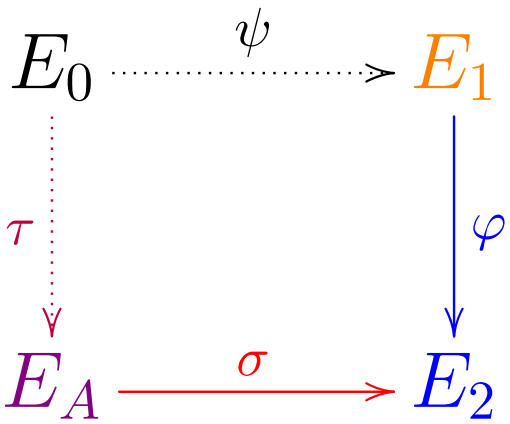
1. Meet in the middle [Gal99]
   - smooth な次数 d の同種写像があることが既知の場合
   - 対象となる 2 つの超特異楕円曲線の両方から探索を行う
2. Delfs-Galbraith アルゴリズム [DG16]
   - $\mathbb{F}_p$ 上定義される曲線への同種写像を探し, 簡単な問題に帰着
3. Eisenträger-Hallgren-Leonardi-Morrison-Park アルゴリズム [EHL+18]
   - 自己準同型環を計算する

①の計算量, 記憶領域はいずれも $\tilde{O}(d^{1/2})$,

②, ③の計算量は $\tilde{O}(p^{1/2})$, 記憶領域は $O(\log p)$.

安全なパラメータ (1/2)

λ ビット安全なパラメータを考える.



E_1 : コミットメント

φ, E_2 : チャレンジ

σ : レスポンス

- 前述②, ③ を防ぐため $p \approx 2^{2\lambda}$.
- $\deg \psi$ は smooth かつ公開. $\Rightarrow$ 前述①を防ぐため $\deg \psi \approx 2^{2\lambda}$.
- チャレンジの可能性を 2^λ としたい. $\Rightarrow$ $\deg \varphi \approx 2^\lambda$.
- $\deg \tau$ は非公開 $\in (1, B]$. $\Rightarrow$ 全数探索を防ぐため $B \approx 2^{\lambda/2}$.
- $\deg \sigma$ は generalized KLPT で決まる. $\Rightarrow$ $\deg \sigma \approx (pB)^3 \approx 2^{7.5\lambda}$.

安全なパラメータ (1/2)

128 ビット安全の p (254 ビット) [2]. [DLW22].

$$p+1 = 2^{65} \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 29^2 \cdot 37^2 \cdot 47 \cdot 197 \cdot 263 \cdot 281 \cdot 461 \cdot 521 \cdot 3923 \cdot 62731 \cdot 96362257 \cdot 3924006112952623,$$

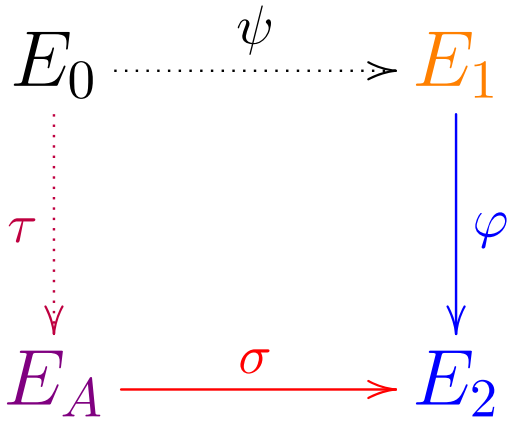
$$p-1 = 2 \cdot 3^{65} \cdot 13 \cdot 17 \cdot 43 \cdot 79 \cdot 157 \cdot 239 \cdot 271 \cdot 283 \cdot 307 \cdot 563 \cdot 599 \cdot 607 \cdot 619 \cdot 743 \cdot 827 \cdot 941 \cdot 2357 \cdot 10069.$$

レスポンスの次数 (署名長) $\deg \sigma = 2^{989} \approx p^{3.9}$,
IdealToIsogeny の θ の次数の平方根 $T = \prod$ 青の因子 $\approx p^{1.3}$,
コミットメントの次数 $\deg \psi = T/(3^{65} \cdot 3923) \approx 2^{219}$ $(< 2^{2\lambda})$,
チャレンジの次数 $\deg \varphi = 2^{65} \cdot 3^{65} \approx 2^{168}$ $(> 2^{\lambda})$.

($\deg \psi$ と $\deg \varphi$ は要調整.)

[2] $p^2 - 1$ が smooth な p の探索についての研究 [Cos20, DKL+20b, CMN21]

署名のゼロ知識性 (1/2)



E_1 : コミットメント

φ, E_2 : チャレンジ

σ : レスポンス

仮定 1

以下の分布は計算量的に判別不可能.

1. コミットメント ψ を一様ランダムとしたレスポンス σ
2. E_A を始点とする次数 $\deg\sigma$ の一様ランダムな巡回同種写像

定理 4

仮定 1 の下で SIQSign は honest-verifier zero-knowledge.

署名のゼロ知識性 (2/2)

オリジナル [DKL+20a] では, 仮定 1 は不成立.
$\because$ レスポンス σ の最初の 2-同種写像が常に同じ.

[DLW22] で修正された. さらに

- $2^k \approx p^{1/2}$ となる k に対して
  $\#(\sigma$ の最初の k 個の 2-同種写像の像$)/\ \#(2^k$-同種写像の像$) \geq c/(\log p)$
  under some heuristics.
- $k \leq 3$ のとき, 実験的に「σ の最初の k 個の 2-同種写像の像」は一様.

目次

論文紹介

[Onu22] の内容の一部を概説する.

- 秘密鍵の次数 $\deg \tau < B$ for $B \approx 2^{\lambda/2} \approx p^{1/4}$ であることの是非.
- 実装で使われている鍵生成の問題的を指摘, 修正方法を提案.

$\mathbb{F}_p$ 上定義される曲線の割合

ヒューリスティック 5

N を SQISign の公開鍵の次数の空間から一様サンプルしたときに
N が p を法として平方剰余になる確率は $1/2$ となる

定理 6

ヒューリスティック 5 の下で SQISign の公開鍵が $\mathbb{F}_p$ 上定義される確率は
$1/(p^{1/4}+1)$ よりも大きい

一様に選んだ $\mathbb{F}_{p^2}$ 上の超特異楕円曲線が $\mathbb{F}_p$ 上定義される確率は約 $p^{-1/2}$

$\Rightarrow$ SQISign の公開鍵は $\mathbb{F}_p$ 上定義される割合が高い

$\Rightarrow$ Delfs-Galbraith アルゴリズムへの**耐性が低い**

対策: $\mathbb{F}_p$ 上の超特異楕円曲線を公開鍵から除けば良い
それでも公開鍵の空間には十分な広さがある

鍵生成の代替的方法

大きな素数次数 N の同種写像 $\tau : E_0 \to E_A$ は直接計算できない

$\Rightarrow$ KLPT アルゴリズムで τ を 2 べき次数の同種写像 κ で E_A にして計算
このとき、$\deg \kappa \approx p^3$

SQISign の full paper [DKL+20b] では、$\deg \kappa \approx p$ とする**代替的方法**が提案されている.

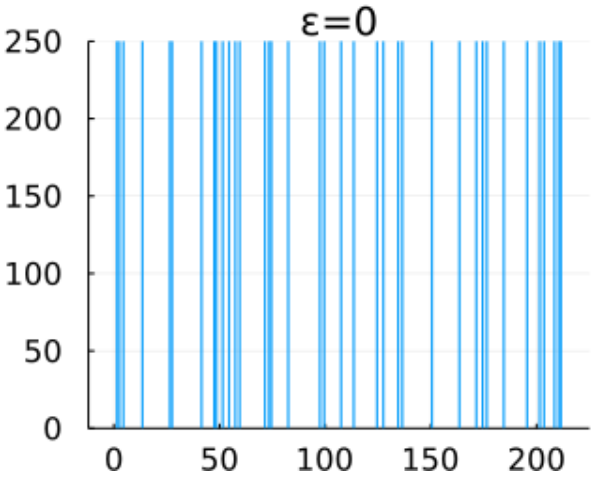
- これにより鍵生成時間が約 $1/3$.
- 鍵が一様ランダムに生成されるかは未解決.
- **実装では代替的方法が使われている**.

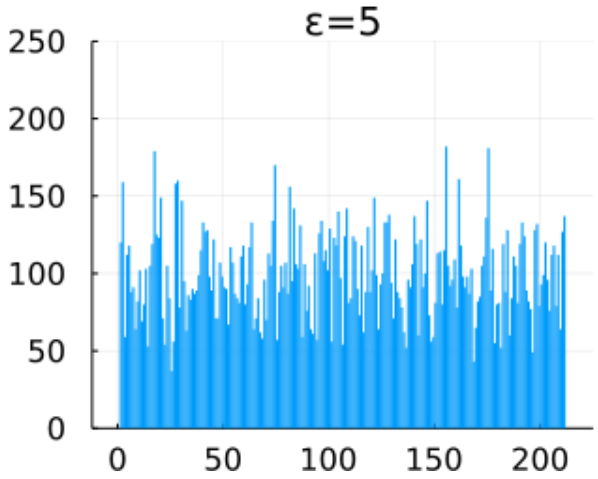
[Onu22] の結果

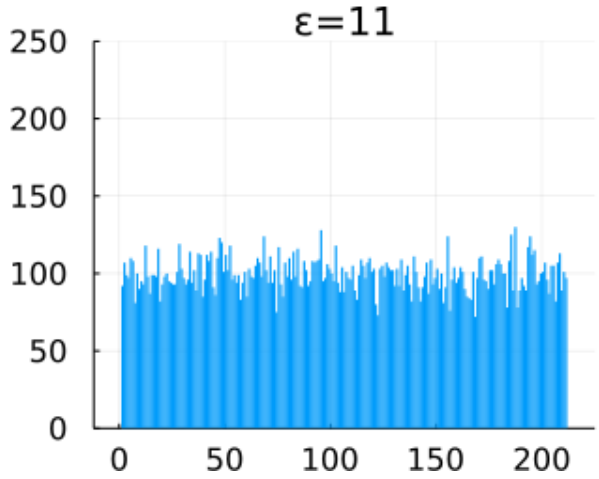
- 代替的方法では生成されない鍵がある可能性を指摘.
- 次数を増やす $(\deg \kappa = 2^e \to 2^{e+\epsilon})$ ことで修正できる,
- $p \approx 2^{256}$ のとき, $\epsilon = 11$ とすれば**鍵がほぼ一様に生成される** under heuristics (計算時間の overhead は 4.3%程度).
- 実験で確認.

実験結果

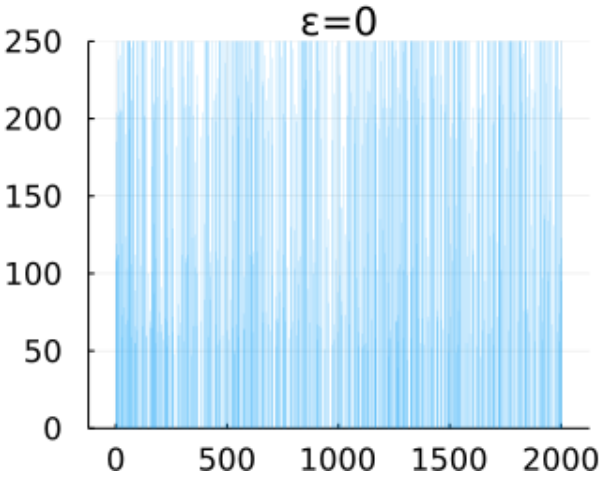
$\deg \tau = 211$

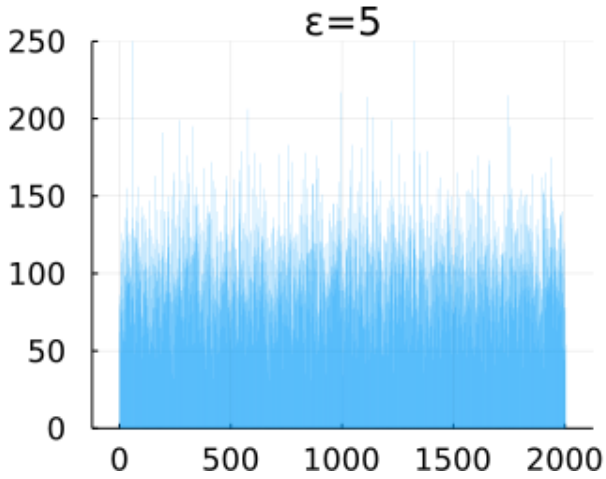


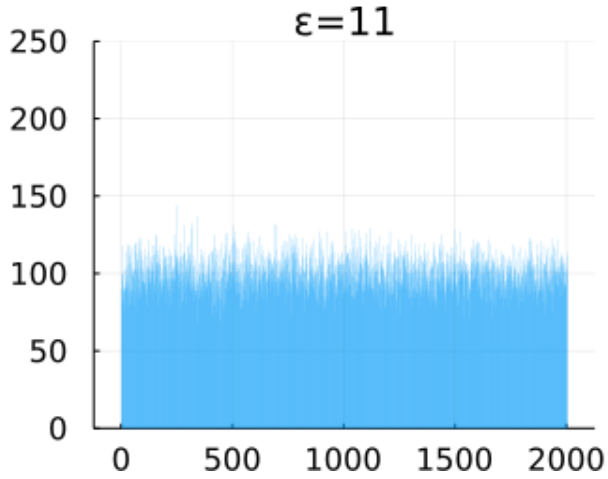




$\deg \tau = 2003$







今後の課題

効率化

- (generalized) KLPT の出力サイズを削減 $\Rightarrow$ 高速化 & 署名長削減
- IdealToIsogeny の更なる高速化
- $p^2 - 1$ が smooth な素数の探索 $\Rightarrow$ 高速化
- $\sqrt{}$élu の高速化

安全性解析

- 署名のゼロ知識性 ($\Leftrightarrow$ gen. KLPT の出力の一様性) の解析
- 秘密鍵 τ の次数が短いことの是非の解析
- 定時間実装 (特に (gen.) KLPT)

参考文献 I

[ACDRH22] Gora Adj, Jesús-Javier Chi-Domínguez, and Francisco Rodríguez-Henríquez.
Karatsuba-based square-root vélu's formulas applied to two isogeny-based protocols.
Journal of Cryptographic Engineering, Jul 2022.

[BDLS20] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith.
Faster computation of isogenies of large prime degree.
In Steven Galbraith, editor, *ANTS-XIV - 14th Algorithmic Number Theory Symposium*, volume 4 of *Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV)*, pages 39–55, Auckland, New Zealand, 2020. Mathematical Sciences Publishers.

[BKV19] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren.
CSI-FiSh: Efficient isogeny based signatures through class group computations.
In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 227–247, Cham, 2019. Springer International Publishing.

[CD22] Wouter Castryck and Thomas Decru.
An efficient key recovery attack on sidh (preliminary version).
Cryptology ePrint Archive, Paper 2022/975, 2022.
https://eprint.iacr.org/2022/975.

参考文献 II

[CMN21] Craig Costello, Michael Meyer, and Michael Naehrig.
Sieving for twin smooth integers with solutions to the Prouhet-Tarry-Escott problem.
In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 272–301, Cham, 2021. Springer International Publishing.

[Cos20] Craig Costello.
B-SIDH: Supersingular isogeny Diffie-Hellman using twisted torsion.
In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 440–463, Cham, 2020. Springer International Publishing.

[DG16] Christina Delfs and Steven D. Galbraith.
Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$.
Designs, Codes and Cryptography, 78(2):425–440, 2016.

[DG19] Luca De Feo and Steven D. Galbraith.
SeaSign: Compact isogeny signatures from class group actions.
In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 759–789, Cham, 2019. Springer International Publishing.

参考文献 III

[DKL+20a] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski.
SQISign: Compact post-quantum signatures from quaternions and isogenies.
In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham, 2020. Springer International Publishing.

[DKL+20b] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski.
SQISign: compact post-quantum signatures from quaternions and isogenies (extended version).
Cryptology ePrint Archive, Report 2020/1240, 2020.
https://ia.cr/2020/1240.

[DLW22] Luca De Feo, Antonin Leroux, and Benjamin Wesolowski.
New algorithms for the Deuring correspondence: SQISign twice as fast.
Cryptology ePrint Archive, Report 2022/234, 2022.
https://ia.cr/2022/234.

参考文献 IV

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit.
Supersingular isogeny graphs and endomorphism rings: Reductions and solutions.
In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 329–368, Cham, 2018. Springer International Publishing.

[Gal99] Steven D. Galbraith.
Constructing isogenies between elliptic curves over finite fields.
LMS Journal of Computation and Mathematics, 2:118–138, 1999.

[GPS17] Steven D. Galbraith, Christophe Petit, and Javier Silva.
Identification protocols and signature schemes based on supersingular isogeny problems.
In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 3–33, Cham, 2017. Springer International Publishing.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol.
On the quaternion ℓ-isogeny path problem.
LMS Journal of Computation and Mathematics, 17(A):418–432, 2014.

参考文献 V

[Onu22] Hiroshi Onuki.
On the key generation in SQISign.
Cryptology ePrint Archive, Paper 2022/900, 2022.
https://eprint.iacr.org/2022/900.

[Piz80] Arnold Pizer.
An algorithm for computing modular forms on $\gamma 0(n)$.
Journal of Algebra, 64:340–390, 1980.

[PL17] Christophe Petit and Kristin Lauter.
Hard and easy problems for supersingular isogeny graphs.
Cryptology ePrint Archive, Paper 2017/962, 2017.
https://eprint.iacr.org/2017/962.

[Sto12] Anton Stolbunov.
Cryptographic schemes based on isogenies.
Doctoral thesis, NTNU, 2012.

[Wes22] Benjamin Wesolowski.
The supersingular isogeny path and endomorphism ring problems are equivalent.
In *FOCS 2021–62nd Annual IEEE Symposium on Foundations of Computer Science*, 2022.