The LIT problem and IS-CUBE

Tomoki Moriya

University of Birmingham

Isogeny club, 17th October 2023

Summary

1. I propose a new computational problem named the LIT problem.
   - Problem of computing a hidden isogeny from two elliptic curves and images of torsion points of order "relatively" small.

$$(E, E', P, Q, \phi(P), \phi(Q)) \text{ with } \mathrm{ord}(P) \ll \deg\phi \quad \rightsquigarrow \quad \phi\colon E \to E'$$

Summary

1. I propose a new computational problem named the LIT problem.
   - Problem of computing a hidden isogeny from two elliptic curves and images of torsion points of order "relatively" small.

$$(E, E', P, Q, \phi(P), \phi(Q)) \text{ with } \mathrm{ord}(P) \ll \deg \phi \quad \rightsquigarrow \quad \phi \colon E \to E'$$

2. I propose a new KEM named IS-CUBE based on the LIT problem.
   - We can use a prime about $2^{8\lambda}$ for the security parameter λ.
   - We can use a random supersingular elliptic curve as the starting curve.

Contents

SIDH (1/2)

Set a prime p as $p = \ell_A^a \ell_B^b f - 1$ for small integers ℓ_A and ℓ_B such that $\gcd(\ell_A, \ell_B) = 1$.

$$
\begin{tikzcd}
(E, P_A, Q_A, P_B, Q_B) \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & (E/\langle P_A + \alpha Q_A\rangle, \phi_A(P_B), \phi_A(Q_B)) \arrow[d] \\
(E/\langle P_B + \beta Q_B\rangle, \phi_B(P_A), \phi_B(Q_A)) \arrow[r] & E/\langle P_A + \alpha Q_A, P_B + \beta Q_B\rangle
\end{tikzcd}
$$

SIDH (1/2)

Set a prime p as $p = \ell_A^a \ell_B^b f - 1$ for small integers ℓ_A and ℓ_B such that $\gcd(\ell_A, \ell_B) = 1$.

$$\begin{tikzcd}
(E, P_A, Q_A, P_B, Q_B) \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & (E/\langle P_A + \alpha Q_A \rangle, \phi_A(P_B), \phi_A(Q_B)) \arrow[d] \\
(E/\langle P_B + \beta Q_B \rangle, \phi_B(P_A), \phi_B(Q_A)) \arrow[r] & E/\langle P_A + \alpha Q_A, P_B + \beta Q_B \rangle
\end{tikzcd}$$

We could take p such that $p \approx 2^{4\lambda}$.

SIDH (1/2)

Set a prime p as $p = \ell_A^a \ell_B^b f - 1$ for small integers ℓ_A and ℓ_B such that $\gcd(\ell_A, \ell_B) = 1$.

$$\begin{tikzcd}
(E, P_A, Q_A, P_B, Q_B) \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & (E/\langle P_A + \alpha Q_A \rangle, \phi_A(P_B), \phi_A(Q_B)) \arrow[d] \\
(E/\langle P_B + \beta Q_B \rangle, \phi_B(P_A), \phi_B(Q_A)) \arrow[r] & E/\langle P_A + \alpha Q_A, P_B + \beta Q_B \rangle
\end{tikzcd}$$

We could take p such that $p \approx 2^{4\lambda}$.

$\rightarrow$ One reason that SIDH was compact.

SIDH (2/2)

SIDH was broken in 2022.

- the Castryck-Decru attack ”An efficient key recovery attack on SIDH”
- the Maino-Martindale attack ”An attack on SIDH with arbitrary starting curve”
- the Robert attack ”Breaking SIDH in polynomial time”

SIDH (2/2)

SIDH was broken in 2022.

- the Castryck-Decru attack ”An efficient key recovery attack on SIDH”
- the Maino-Martindale attack ”An attack on SIDH with arbitrary starting curve”
- the Robert attack ”Breaking SIDH in polynomial time”

CSIDH and some isogeny-based KE/PKE schemes proposed after breaking SIDH (*e.g.*, M-SIDH, FESTA, terSIDH, etc...) are alive.

Primes of other KE/PKE schemes (1/2)

The sizes of p of *most* schemes are **NOT** guaranteed to be related linearly to λ.

Primes of other KE/PKE schemes (1/2)

The sizes of *p* of *most* schemes are **NOT** guaranteed to be related linearly to λ.

For example,

Schemes	CSIDH [1,2]		M-SIDH [3]		FESTA [4]	
	bit(p)	bit(p)/λ	bit(p)	bit(p)/λ	bit(p)	bit(p)/λ
$\lambda = 128$	3,072	24.00	5,911	46.18	1,292	10.09
$\lambda = 192$	8,192	42.67	9,382	48.86	1,966	10.24
$\lambda = 256$	-	-	13,000	50.78	2,772	10.83

[1] Castryck, Lange, Martindale, Panny and Renes ”CSIDH: an efficient post-quantum commutative group action”
[2] Jesús-Javier Chi-Domínguez, Jaques and Rodríguez-Henríquez ”The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents”
[3] Fouotsa, Moriya and Petit ”M-SIDH and MD-SIDH: Countering SIDH attacks by masking information”

[4] Basso, Maino and Pope ”FESTA: Fast encryption from supersingular torsion attacks”

Primes of other KE/PKE schemes (2/2)

The exceptions:

FESTA-HD (FESTA using isogenies of dimension 4 or 8) and QFESTA [5]

[5] Nakagawa and Onuki ”QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras”

Primes of other KE/PKE schemes (2/2)

The exceptions:
FESTA-HD (FESTA using isogenies of dimension 4 or 8) and QFESTA [5]

[5] Nakagawa and Onuki ”QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras”

FESTA-HD:

Primes of other KE/PKE schemes (2/2)

The exceptions:
FESTA-HD (FESTA using isogenies of dimension 4 or 8) and QFESTA [5]

[5] Nakagawa and Onuki ”QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras”

FESTA-HD:

- The size of the prime is about 7λ bits.

Primes of other KE/PKE schemes (2/2)

The exceptions:
FESTA-HD (FESTA using isogenies of dimension 4 or 8) and QFESTA [5]

[5] Nakagawa and Onuki ”QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras”

FESTA-HD:

- The size of the prime is about 7λ bits.
- There is no implementation (so far) due to the computation of high-dimensional isogenies.

Primes of other KE/PKE schemes (2/2)

The exceptions:
FESTA-HD (FESTA using isogenies of dimension 4 or 8) and QFESTA [5]

[5] Nakagawa and Onuki "QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras"

FESTA-HD:

- The size of the prime is about 7λ bits.
- There is no implementation (so far) due to the computation of high-dimensional isogenies.

QFESTA:

Primes of other KE/PKE schemes (2/2)

The exceptions:
FESTA-HD (FESTA using isogenies of dimension 4 or 8) and QFESTA [5]

[5] Nakagawa and Onuki ”QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras”

FESTA-HD:

- The size of the prime is about 7λ bits.
- There is no implementation (so far) due to the computation of high-dimensional isogenies.

QFESTA:

- The size of the prime is about 2λ bits.

Primes of other KE/PKE schemes (2/2)

The exceptions:
FESTA-HD (FESTA using isogenies of dimension 4 or 8) and QFESTA [5]

[5] Nakagawa and Onuki "QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras"

FESTA-HD:

- The size of the prime is about 7λ bits.
- There is no implementation (so far) due to the computation of high-dimensional isogenies.

QFESTA:

- The size of the prime is about 2λ bits.
- Use the curve of j-invariant 1728 as the starting curve. (This is a potential risk for the security.)

Required scheme

We ~~only me?~~ want to a scheme with

- the prime p whose size is linearly related to λ
- a random starting curve
- computation of isogenies 2 or less

Required scheme

We ~~only me?~~ want to a scheme with

- the prime p whose size is linearly related to λ
- a random starting curve
- computation of isogenies 2 or less

$\rightarrow$ The LIT problem, IS-CUBE

The Robert attack [Robert (EUROCRYPT 2023)] (1/5)

Problem (The CSSI problem)

Let p be a prime such that $p = A \cdot B \cdot f - 1$, where A and B are smooth large integers such that $\gcd(A, B) = 1$, and f is a small integer. Let E, E' be supersingular elliptic curves over $\mathbb{F}_{p^2}$, let $\phi\colon E \to E'$ is an A-isogeny, and let $\{P, Q\}$ be a basis of $E[B]$.

$$(E, E', P, Q, \phi(P), \phi(Q)) \quad \rightsquigarrow \quad \phi$$

The Robert attack [Robert (EUROCRYPT 2023)] (1/5)

Problem (The CSSI problem)

Let p be a prime such that $p = A \cdot B \cdot f - 1$, where A and B are smooth large integers such that $\gcd(A, B) = 1$, and f is a small integer. Let E, E' be supersingular elliptic curves over $\mathbb{F}_{p^2}$, let $\phi \colon E \to E'$ is an A-isogeny, and let $\{P, Q\}$ be a basis of $E[B]$.

$$(E, E', P, Q, \phi(P), \phi(Q)) \quad \rightsquigarrow \quad \phi$$

Robert's attack solves the CSSI problem if $A \leq B^2$.

The Robert attack [Robert (EUROCRYPT 2023)] (2/5)

Definition (Isogeny diamond (SIDH diagram))

Let A, B be integers such that $\gcd(A, B) = 1$, let E be an elliptic curve, and let R_A and R_B be cyclic subgroups of E of order A and B respectively. We call the following diagram *an isogeny diamond* or *a SIDH diagram*.

$$
\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E/\langle R_A \rangle \arrow[d, "\phi'_B"] \\
E/\langle R_B \rangle \arrow[r, "\phi'_A"'] & E/\langle R_A, R_B \rangle
\end{tikzcd}
$$

Here, $\ker \phi_A = \langle R_A \rangle$, $\ker \phi_B = \langle R_B \rangle$, $\ker \phi'_A = \langle \phi_B(R_A) \rangle$, and $\ker \phi'_B = \langle \phi_A(R_B) \rangle$.

The Robert attack [Robert (EUROCRYPT 2023)] (3/5)

Theorem (Kani's theorem [Kani (1997)])

$$\begin{tikzcd} E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_1 = E/\langle R_A \rangle \arrow[d, "\phi'_B"] \\ E_2 = E/\langle R_B \rangle \arrow[r, "\phi'_A"'] & E_3 = E/\langle R_A, R_B \rangle \end{tikzcd}$$

Let the above be an isogeny diamond, and let $\{P, Q\}$ *be a basis of* $E[A+B]$.

The Robert attack [Robert (EUROCRYPT 2023)] (3/5)

Theorem (Kani's theorem [Kani (1997)])

$$\begin{tikzcd} E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_1 = E/\langle R_A \rangle \arrow[d, "\phi'_B"] \\ E_2 = E/\langle R_B \rangle \arrow[r, "\phi'_A"'] & E_3 = E/\langle R_A, R_B \rangle \end{tikzcd}$$

Let the above be an isogeny diamond, and let $\{P, Q\}$ *be a basis of* $E[A + B]$.
Then, the kernel of an isogeny $\Psi\colon E_1 \times E_2 \to E \times E_3$ *of dimension 2 defined by*

$$\Psi = \begin{pmatrix} \hat{\phi_A} & \hat{\phi_B} \\ -\phi'_B & \phi'_A \end{pmatrix}$$

is $\langle (\phi_A(P), \phi_B(P)), (\phi_A(Q), \phi_B(Q)) \rangle$.

The Robert attack [Robert (EUROCRYPT 2023)] (4/5)

The strategy of Robert's attack:

The Robert attack [Robert (EUROCRYPT 2023)] (4/5)

The strategy of Robert's attack:

1. Compute $c = B^2 - A$.

The Robert attack [Robert (EUROCRYPT 2023)] (4/5)

The strategy of Robert's attack:

1. Compute $c = B^2 - A$.
2. Find c_1, c_2, c_3, c_4 such that $c^2 = c_1^2 + c_2^2 + c_3^2 + c_4^2$ from the four-square theorem.

The Robert attack [Robert (EUROCRYPT 2023)] (4/5)

The strategy of Robert's attack:

1. Compute $c = B^2 - A$.
2. Find c_1, c_2, c_3, c_4 such that $c^2 = c_1^2 + c_2^2 + c_3^2 + c_4^2$ from the four-square theorem.
3. Construct a 4×4-matrix $\mathbf{C}$ over $\mathbb{Z}$ such that ${}^t\mathbf{C}\mathbf{C} = c \cdot I_4$ using $c_1, \ldots, c_4$.

The Robert attack [Robert (EUROCRYPT 2023)] (4/5)

The strategy of Robert's attack:

1. Compute $c = B^2 - A$.
2. Find c_1, c_2, c_3, c_4 such that $c^2 = c_1^2 + c_2^2 + c_3^2 + c_4^2$ from the four-square theorem.
3. Construct a 4×4-matrix $\mathbf{C}$ over $\mathbb{Z}$ such that ${}^t\mathbf{C}\mathbf{C} = c \cdot I_4$ using $c_1, \ldots, c_4$.
4. Consider the SIDH diagram (of high-dimensional)

$$\begin{array}{ccc} E^4 & \xrightarrow{\phi_A I_4} & E'^4 \\ \mathbf{C}\downarrow & & \downarrow\mathbf{C} \\ E^4 & \xrightarrow[\phi_A I_4]{} & E'^4 \end{array}$$

The Robert attack [Robert (EUROCRYPT 2023)] (5/5)

5. From Kani's theorem, the kernel of $\Psi = \begin{pmatrix} \hat{\phi}_A I_4 & \mathbf{C} \\ -\mathbf{C} & \phi_A I_4 \end{pmatrix}$ is constructed by $\phi_A(E[B^2])$ and $E[B^2]$.

The Robert attack [Robert (EUROCRYPT 2023)] (5/5)

5. From Kani's theorem, the kernel of $\Psi = \begin{pmatrix} \hat{\phi}_A I_4 & \mathbf{C} \\ -\mathbf{C} & \phi_A I_4 \end{pmatrix}$ is constructed by $\phi_A(E[B^2])$ and $E[B^2]$.
6. The kernel of $\hat{\Psi}$ is also constructed by $\phi_A(E[B^2])$ and $E[B^2]$.

The Robert attack [Robert (EUROCRYPT 2023)] (5/5)

5. From Kani's theorem, the kernel of $\Psi = \begin{pmatrix} \hat{\phi}_A I_4 & \mathbf{C} \\ -\mathbf{C} & \phi_A I_4 \end{pmatrix}$ is constructed by $\phi_A(E[B^2])$ and $E[B^2]$.
6. The kernel of $\hat{\Psi}$ is also constructed by $\phi_A(E[B^2])$ and $E[B^2]$.
7. Compute Ψ by using $P_B, Q_B, \phi_A(P_B), \phi_A(Q_B)$ as

$$E^4 \times E'^4 \to (\text{An abelian variety}) \leftarrow E^4 \times E'^4.$$

The Robert attack [Robert (EUROCRYPT 2023)] (5/5)

5. From Kani's theorem, the kernel of $\Psi = \begin{pmatrix} \hat{\phi}_A I_4 & \mathbf{C} \\ -\mathbf{C} & \phi_A I_4 \end{pmatrix}$ is constructed by $\phi_A(E[B^2])$ and $E[B^2]$.
6. The kernel of $\hat{\Psi}$ is also constructed by $\phi_A(E[B^2])$ and $E[B^2]$.
7. Compute Ψ by using $P_B, Q_B, \phi_A(P_B), \phi_A(Q_B)$ as

$$E^4 \times E'^4 \to (\text{An abelian variety}) \leftarrow E^4 \times E'^4.$$

8. Recover ϕ_A from Ψ.

The Robert attack [Robert (EUROCRYPT 2023)] (5/5)

5. From Kani's theorem, the kernel of $\Psi = \begin{pmatrix} \hat{\phi}_A I_4 & \mathbf{C} \\ -\mathbf{C} & \phi_A I_4 \end{pmatrix}$ is constructed by $\phi_A(E[B^2])$ and $E[B^2]$.
6. The kernel of $\hat{\Psi}$ is also constructed by $\phi_A(E[B^2])$ and $E[B^2]$.
7. Compute Ψ by using $P_B, Q_B, \phi_A(P_B), \phi_A(Q_B)$ as

$$E^4 \times E'^4 \to (\text{An abelian variety}) \leftarrow E^4 \times E'^4.$$

8. Recover ϕ_A from Ψ.

Robert's attack solves the CSSI problem if $A \leq B^2$.

Countermeasures for SIDH attacks (1/2)

Countermeasures for SIDH attacks (1/2)

- Mask A (the degree of ϕ_A)

Countermeasures for SIDH attacks (1/2)

- Mask A (the degree of ϕ_A)
  $\leftarrow$ MD-SIDH [Fouotsa, M. and Petit (EUROCRYPT 2023)]

Countermeasures for SIDH attacks (1/2)

- Mask A (the degree of ϕ_A)
  $\leftarrow$ MD-SIDH [Fouotsa, M. and Petit (EUROCRYPT 2023)]
- Mask $\phi_A(P_B)$ and $\phi_A(Q_B)$ by scalars

Countermeasures for SIDH attacks (1/2)

- Mask A (the degree of ϕ_A)
  $\leftarrow$ MD-SIDH [Fouotsa, M. and Petit (EUROCRYPT 2023)]
- Mask $\phi_A(P_B)$ and $\phi_A(Q_B)$ by scalars
  $\leftarrow$ M-SIDH [F. M. P.] and FESTA [Basso, Maino and Pope (ASIACRYPT 2023)]

Countermeasures for SIDH attacks (1/2)

- Mask A (the degree of ϕ_A)
  $\leftarrow$ MD-SIDH [Fouotsa, M. and Petit (EUROCRYPT 2023)]
- Mask $\phi_A(P_B)$ and $\phi_A(Q_B)$ by scalars
  $\leftarrow$ M-SIDH [F. M. P.] and FESTA [Basso, Maino and Pope (ASIACRYPT 2023)]
- Set $A \gg B^2$

Countermeasures for SIDH attacks (1/2)

- Mask A (the degree of ϕ_A)
  $\leftarrow$ MD-SIDH [Fouotsa, M. and Petit (EUROCRYPT 2023)]
- Mask $\phi_A(P_B)$ and $\phi_A(Q_B)$ by scalars
  $\leftarrow$ M-SIDH [F. M. P.] and FESTA [Basso, Maino and Pope (ASIACRYPT 2023)]
- Set $A \gg B^2$
  $\leftarrow$ The LIT problem and IS-CUBE

Countermeasures for SIDH attacks (2/2)

Problem (The CIST problem [Basso, Maino and Pope (ASIACRYPT 2023)])

Let p be a prime such that $p = A \cdot B \cdot f - 1$, where A and B are smooth large integers such that $\gcd(A, B) = 1$, and f is a small integer. Let E, E' be supersingular elliptic curves over $\mathbb{F}_{p^2}$, let $\phi\colon E \to E'$ is an A-isogeny, and let $\{P, Q\}$ be a basis of $E[B]$. Let α be a random element in $(\mathbb{Z}/B\mathbb{Z})^\times$.

$$(E, E', P, Q, \alpha\phi(P), \alpha^{-1}\phi(Q)) \quad \rightsquigarrow \quad \phi$$

The LIT problem (1/4)

Problem (The LIT problem (The Long Isogeny with Torsion problem))

Let p be a prime such that $p = A \cdot B \cdot f - 1$*, where* A *and* B *are smooth large integers such that* $\gcd(A, B) = 1$*, and* f *is a small integer. Let* E, E' *be supersingular elliptic curves over* $\mathbb{F}_{p^2}$*, let* $\phi\colon E \to E'$ *is an* A*-isogeny, and let* $\{P, Q\}$ *be a basis of* $E[B]$*. Assume that* $\deg\phi \gg B$*.*

$$(E, E', P, Q, \phi(P), \phi(Q)) \quad \rightsquigarrow \quad \phi$$

The LIT problem (1/4)

Problem (The LIT problem (The Long Isogeny with Torsion problem))

Let p be a prime such that $p = A \cdot B \cdot f - 1$, where A and B are smooth large integers such that $\gcd(A, B) = 1$, and f is a small integer. Let E, E' be supersingular elliptic curves over $\mathbb{F}_{p^2}$, let $\phi\colon E \to E'$ is an A-isogeny, and let $\{P, Q\}$ be a basis of $E[B]$. Assume that $\deg \phi \gg B$.

$$(E, E', P, Q, \phi(P), \phi(Q)) \quad \rightsquigarrow \quad \phi$$

$\deg \phi \approx B^3$?

The LIT problem (1/4)

Problem (The LIT problem (The Long Isogeny with Torsion problem))

Let p be a prime such that $p = A \cdot B \cdot f - 1$, where A and B are smooth large integers such that $\gcd(A, B) = 1$, and f is a small integer. Let E, E' be supersingular elliptic curves over $\mathbb{F}_{p^2}$, let $\phi\colon E \to E'$ is an A-isogeny, and let $\{P, Q\}$ be a basis of $E[B]$. Assume that $\deg \phi \gg B$.

$$(E, E', P, Q, \phi(P), \phi(Q)) \quad \rightsquigarrow \quad \phi$$

$\deg \phi \approx B^3$? $\deg \phi \approx B^2 \cdot 2^{2\lambda}$?

The LIT problem (1/4)

Problem (The LIT problem (The Long Isogeny with Torsion problem))

Let p be a prime such that $p = A \cdot B \cdot f - 1$, where A and B are smooth large integers such that $\gcd(A, B) = 1$, and f is a small integer. Let E, E' be supersingular elliptic curves over $\mathbb{F}_{p^2}$, let $\phi\colon E \to E'$ is an A-isogeny, and let $\{P, Q\}$ be a basis of $E[B]$. Assume that $\deg \phi \gg B$.

$$(E, E', P, Q, \phi(P), \phi(Q)) \quad \rightsquigarrow \quad \phi$$

$\deg \phi \approx B^3$? $\deg \phi \approx B^2 \cdot 2^{2\lambda}$? $\deg \phi \approx B^{10000}$?

The LIT problem (1/4)

Problem (The LIT problem (The Long Isogeny with Torsion problem))

Let p be a prime such that $p = A \cdot B \cdot f - 1$, where A and B are smooth large integers such that $\gcd(A, B) = 1$, and f is a small integer. Let E, E' be supersingular elliptic curves over $\mathbb{F}_{p^2}$, let $\phi \colon E \to E'$ is an A-isogeny, and let $\{P, Q\}$ be a basis of $E[B]$. Assume that $\deg \phi \gg B$.

$$(E, E', P, Q, \phi(P), \phi(Q)) \quad \rightsquigarrow \quad \phi$$

$\deg \phi \approx B^3$? $\deg \phi \approx B^2 \cdot 2^{2\lambda}$? $\deg \phi \approx B^{10000}$? $\deg \phi \approx B^2 \cdot 2^{100\lambda}$?

The LIT problem (1/4)

Problem (The LIT problem (The Long Isogeny with Torsion problem))

Let p be a prime such that $p = A \cdot B \cdot f - 1$, where A and B are smooth large integers such that $\gcd(A, B) = 1$, and f is a small integer. Let E, E' be supersingular elliptic curves over $\mathbb{F}_{p^2}$, let $\phi \colon E \to E'$ is an A-isogeny, and let $\{P, Q\}$ be a basis of $E[B]$. Assume that $\deg \phi \gg B$.

$$(E, E', P, Q, \phi(P), \phi(Q)) \quad \rightsquigarrow \quad \phi$$

$\deg \phi \approx B^3$? $\deg \phi \approx B^2 \cdot 2^{2\lambda}$? $\deg \phi \approx B^{10000}$? $\deg \phi \approx B^2 \cdot 2^{100\lambda}$?
$\deg \phi \approx$
$B^{10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000}$

The LIT problem (1/4)

Problem (The LIT problem (The Long Isogeny with Torsion problem))

Let p be a prime such that $p = A \cdot B \cdot f - 1$, where A and B are smooth large integers such that $\gcd(A, B) = 1$, and f is a small integer. Let E, E' be supersingular elliptic curves over $\mathbb{F}_{p^2}$, let $\phi \colon E \to E'$ is an A-isogeny, and let $\{P, Q\}$ be a basis of $E[B]$. Assume that $\deg \phi \gg B$.

$$(E, E', P, Q, \phi(P), \phi(Q)) \quad \rightsquigarrow \quad \phi$$

$\deg \phi \approx B^3$? $\deg \phi \approx B^2 \cdot 2^{2\lambda}$? $\deg \phi \approx B^{10000}$? $\deg \phi \approx B^2 \cdot 2^{100\lambda}$?
$\deg \phi \approx B^{100000000000000000000000000000000000000000000000000000000000000000000000000000000}$

When does the LIT problem seem hard to solve?

The LIT problem (2/4)

Strategies to solve the LIT problem:

The LIT problem (2/4)

Strategies to solve the LIT problem:

1. Find points P', Q' and $\phi(P'), \phi(Q')$ of order BN such that $\deg \phi \approx (BN)^2$, $NP' = P$ and $NQ' = Q$.

The LIT problem (2/4)

Strategies to solve the LIT problem:

1. Find points P', Q' and $\phi(P'), \phi(Q')$ of order BN such that $\deg \phi \approx (BN)^2$, $NP' = P$ and $NQ' = Q$.
2. Combine Robert's attack and the meet-in-the-middle attack.

$$E^4 \times E'^4 \to V \rightsquigarrow (\text{MitM}) \leftsquigarrow V' \leftarrow E^4 \times E'^4$$

The LIT problem (3/4)

1. Find points P', Q' and $\phi(P'), \phi(Q')$ of order BN such that $\deg \phi \approx (BN)^2$, $NP' = P$ and $NQ' = Q$.

The LIT problem (3/4)

1. Find points P', Q' and $\phi(P'), \phi(Q')$ of order BN such that $\deg \phi \approx (BN)^2$, $NP' = P$ and $NQ' = Q$.

If we fix P', Q', then the number of the candidates for $\phi(P'), \phi(Q')$ is $\#\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$.

$$\#\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{q|N \text{ prime}} \frac{1}{q^2}(q^2 - 1) > N.$$

The LIT problem (3/4)

1. Find points P', Q' and $\phi(P'), \phi(Q')$ of order BN such that $\deg\phi \approx (BN)^2$, $NP' = P$ and $NQ' = Q$.

If we fix P', Q', then the number of the candidates for $\phi(P'), \phi(Q')$ is $\#\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$.

$$\#\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{q|N \text{ prime}} \frac{1}{q^2}(q^2-1) > N.$$

We prefer to set $N \geq 2^\lambda$. $\rightsquigarrow$ We prefer to set $\deg\phi \approx B^2 \cdot 2^{2\lambda}$.

The LIT problem (4/4)

2. Combine Robert's attack and the meet-in-the-middle attack.

The LIT problem (4/4)

2. Combine Robert's attack and the meet-in-the-middle attack.

$$\underbrace{\overbrace{E^4 \times E'^4 \longrightarrow V}^{(B,\ldots,B)\text{-isogeny}} \rightsquigarrow (\mathrm{MitM}) \leftsquigarrow \overbrace{V' \longleftarrow E^4 \times E'^4}^{(B,\ldots,B)\text{-isogeny}}}_{(\deg\phi,\ldots,\deg\phi)\text{-isogeny}}$$

The LIT problem (4/4)

2. Combine Robert's attack and the meet-in-the-middle attack.

$$\underbrace{\overbrace{E^4 \times E'^4 \longrightarrow V}^{(B,\dots,B)\text{-isogeny}} \rightsquigarrow (\text{MitM}) \leftsquigarrow \overbrace{V' \longleftarrow E^4 \times E'^4}^{(B,\dots,B)\text{-isogeny}}}_{(\deg\phi,\dots,\deg\phi)\text{-isogeny}}$$

We prefer to set $\deg \phi / B^2 \geq 2^{2\lambda}$.

The LIT problem (4/4)

2. Combine Robert's attack and the meet-in-the-middle attack.

$$\underbrace{\overbrace{E^4 \times E'^4 \longrightarrow V}^{(B,\ldots,B)\text{-isogeny}} \rightsquigarrow (\text{MitM}) \leftsquigarrow \overbrace{V' \longleftarrow E^4 \times E'^4}^{(B,\ldots,B)\text{-isogeny}}}_{(\deg\phi,\ldots,\deg\phi)\text{-isogeny}}$$

We prefer to set $\deg\phi / B^2 \geq 2^{2\lambda}$.
$\rightsquigarrow$ We prefer to set $\deg\phi \approx B^2 \cdot 2^{2\lambda}$.

Why do we want the LIT problem?

We can construct parallel isogenies with a small overhead.

$$
\begin{tikzcd}
(E, P, Q) \arrow[r, "2b+2\lambda"] \arrow[d, "b"'] & (E', \phi(P), \phi(Q)) \arrow[d, "b"] \\
E_1 \arrow[r, "2b+2\lambda"'] & E_1'
\end{tikzcd}
$$

Core idea

$p = \ell_C^c \cdot \ell_A \cdot \ell_B^b \cdot f - 1$, where ℓ_A, ℓ_B, ℓ_C are small distinct primes and f is a small integer.
$\ell_C^c \approx 2^{6\lambda}$, $\ell_A^a \approx 2^{6\lambda}$, $\ell_B^b \approx 2^{2\lambda}$, $p \approx 2^{8\lambda}$.

$$
\begin{tikzcd}
 & E_s \arrow[rr, "\deg = \ell_A^a"] \arrow[dl, "\deg = (\ell_C^c - \ell_A^a)"'] \arrow[dd, dashed] & & E_1 \arrow[dl, dotted] \arrow[dd, dashed] \\
\tilde{E}_s \arrow[rr, dotted] \arrow[dd, dashed, "\deg = \ell_B^b"'] & & E_2 \arrow[dd, dotted] & \\
 & E & & E_1' \arrow[ll, rightsquigarrow] \arrow[dl, rightsquigarrow] \\
E_s' \arrow[ur, rightsquigarrow] \arrow[rr, rightsquigarrow] & & E_2' &
\end{tikzcd}
$$

Public pamameter: $(E_s, \tilde{E}_s)$
Public key: E_1
Ciphertext: (E_s', E_1')
Shared key: E

IS-CUBE (1/3)

Public key generation:

$\{P_C, Q_C\}$: a basis of $E_s[\ell_C^c]$, $\{P_B, Q_B\}$: a basis of $E_s[\ell_B^b]$

$\deg \phi_1 = \ell_A^a \approx 2^{6\lambda}$, $\deg \tau = \ell_C^c - \ell_A^a$

$$\begin{tikzcd}
(E_s, P_B, Q_B, P_C, Q_C) \arrow[r, "\phi_1"] \arrow[d, "\tau"'] & (E_1, \phi_1(P_B), \phi_1(Q_B), \alpha\phi_1(P_C), \alpha^{-1}\phi_1(Q_C)) \arrow[d, dotted] \\
(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C)) \arrow[r, dotted] & E_2
\end{tikzcd}$$

IS-CUBE (1/3)

Public key generation:

$\{P_C, Q_C\}$: a basis of $E_s[\ell_C^c]$, $\{P_B, Q_B\}$: a basis of $E_s[\ell_B^b]$
$\deg \phi_1 = \ell_A^a \approx 2^{6\lambda}$, $\deg \tau = \ell_C^c - \ell_A^a$

$$\begin{tikzcd}
(E_s, P_B, Q_B, P_C, Q_C) \arrow[r, "\phi_1"] \arrow[d, "\tau"'] & (E_1, \phi_1(P_B), \phi_1(Q_B), \alpha\phi_1(P_C), \alpha^{-1}\phi_1(Q_C)) \arrow[d, dotted] \\
(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C)) \arrow[r, dotted] & E_2
\end{tikzcd}$$

Public parameters: $(E_s, P_B, Q_B, P_C, Q_C)$ and $(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C))$

IS-CUBE (1/3)

Public key generation:

$\{P_C, Q_C\}$: a basis of $E_s[\ell_C^c]$, $\{P_B, Q_B\}$: a basis of $E_s[\ell_B^b]$

$\deg \phi_1 = \ell_A^a \approx 2^{6\lambda}$, $\deg \tau = \ell_C^c - \ell_A^a$

$$\begin{tikzcd}
(E_s, P_B, Q_B, P_C, Q_C) \arrow[r, "\phi_1"] \arrow[d, "\tau"'] & (E_1, \phi_1(P_B), \phi_1(Q_B), \alpha\phi_1(P_C), \alpha^{-1}\phi_1(Q_C)) \arrow[d, dotted] \\
(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C)) \arrow[r, dotted] & E_2
\end{tikzcd}$$

Public parameters: $(E_s, P_B, Q_B, P_C, Q_C)$ and $(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C))$

Public key: $(E_1, \phi_1(P_B), \phi_1(Q_B), \alpha\phi_1(P_C), \alpha^{-1}\phi_1(Q_C))$

IS-CUBE (1/3)

Public key generation:

$\{P_C, Q_C\}$: a basis of $E_s[\ell_C^c]$, $\{P_B, Q_B\}$: a basis of $E_s[\ell_B^b]$

$\deg \phi_1 = \ell_A^a \approx 2^{6\lambda}$, $\deg \tau = \ell_C^c - \ell_A^a$

$$\begin{tikzcd}
(E_s, P_B, Q_B, P_C, Q_C) \arrow[r, "\phi_1"] \arrow[d, "\tau"'] & (E_1, \phi_1(P_B), \phi_1(Q_B), \alpha\phi_1(P_C), \alpha^{-1}\phi_1(Q_C)) \arrow[d, dotted] \\
(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C)) \arrow[r, dotted] & E_2
\end{tikzcd}$$

Public parameters: $(E_s, P_B, Q_B, P_C, Q_C)$ and $(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C))$
Public key: $(E_1, \phi_1(P_B), \phi_1(Q_B), \alpha\phi_1(P_C), \alpha^{-1}\phi_1(Q_C))$
Secret key: (ϕ_1, α)

IS-CUBE (2/3)

Encapsulation:

$$\begin{array}{ccccc}
(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C)) & \xleftarrow{\tau} & (E_s, P_B, Q_B) & \xrightarrow{\phi_1} & (E_1, \phi_1(P_B), \phi_1(Q_B), P_1, Q_1) \\
\Big\downarrow \phi_{0,B} & & \Big\downarrow \phi_B & & \Big\downarrow \phi_{1,B} \\
(E_s', \beta\phi_{0,B}(\tau(P_C)), \beta^{-1}\phi_{0,B}(\tau(Q_C))) & & E & & (E_1', \beta\phi_{1,B}(P_1), \beta^{-1}\phi_{1,B}(Q_1))
\end{array}$$

$$\ker \phi_B = \langle P_B + rQ_B \rangle, \quad \ker \phi_{0,B} = \langle \tau(P_B) + r\tau(Q_B) \rangle, \quad \ker \phi_{1,B} = \langle \phi_1(P_B) + r\phi_1(Q_B) \rangle$$

IS-CUBE (2/3)

Encapsulation:

$$
\begin{tikzcd}
(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C)) \arrow[d, dashed, "\phi_{0,B}"] & (E_s, P_B, Q_B) \arrow[l, "\tau"'] \arrow[r, "\phi_1"] \arrow[d, dashed, "\phi_B"] & (E_1, \phi_1(P_B), \phi_1(Q_B), P_1, Q_1) \arrow[d, dashed, "\phi_{1,B}"] \\
(E_s', \beta\phi_{0,B}(\tau(P_C)), \beta^{-1}\phi_{0,B}(\tau(Q_C))) & E & (E_1', \beta\phi_{1,B}(P_1), \beta^{-1}\phi_{1,B}(Q_1))
\end{tikzcd}
$$

$\ker\phi_B = \langle P_B + rQ_B \rangle$, $\ker\phi_{0,B} = \langle \tau(P_B) + r\tau(Q_B) \rangle$, $\ker\phi_{1,B} = \langle \phi_1(P_B) + r\phi_1(Q_B) \rangle$

Ciphertext: $(E_s', \beta\phi_{0,B}(\tau(P_C)), \beta^{-1}\phi_{0,B}(\tau(Q_C)))$ and $(E_1', \beta\phi_{1,B}(P_1), \beta^{-1}\phi_{1,B}(Q_1))$

IS-CUBE (2/3)

Encapsulation:

$$
\begin{tikzcd}
(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C)) \arrow[d, dashed, "\phi_{0,B}"] & (E_s, P_B, Q_B) \arrow[l, "\tau"'] \arrow[r, "\phi_1"] \arrow[d, dashed, "\phi_B"] & (E_1, \phi_1(P_B), \phi_1(Q_B), P_1, Q_1) \arrow[d, dashed, "\phi_{1,B}"] \\
(E_s', \beta\phi_{0,B}(\tau(P_C)), \beta^{-1}\phi_{0,B}(\tau(Q_C))) & E & (E_1', \beta\phi_{1,B}(P_1), \beta^{-1}\phi_{1,B}(Q_1))
\end{tikzcd}
$$

$\ker\phi_B = \langle P_B + rQ_B\rangle$, $\ker\phi_{0,B} = \langle\tau(P_B) + r\tau(Q_B)\rangle$, $\ker\phi_{1,B} = \langle\phi_1(P_B) + r\phi_1(Q_B)\rangle$

Ciphertext: $(E_s', \beta\phi_{0,B}(\tau(P_C)), \beta^{-1}\phi_{0,B}(\tau(Q_C)))$ and $(E_1', \beta\phi_{1,B}(P_1), \beta^{-1}\phi_{1,B}(Q_1))$
Shared key: E

IS-CUBE (2/3)

Encapsulation:

$$\begin{tikzcd}
(\tilde{E}_s, \tau(P_B), \tau(Q_B), \tau(P_C), \tau(Q_C)) \arrow[d, dashed, "\phi_{0,B}"] & (E_s, P_B, Q_B) \arrow[l, "\tau"'] \arrow[r, "\phi_1"] \arrow[d, dashed, "\phi_B"] & (E_1, \phi_1(P_B), \phi_1(Q_B), P_1, Q_1) \arrow[d, dashed, "\phi_{1,B}"] \\
(E_s', \beta\phi_{0,B}(\tau(P_C)), \beta^{-1}\phi_{0,B}(\tau(Q_C))) & E & (E_1', \beta\phi_{1,B}(P_1), \beta^{-1}\phi_{1,B}(Q_1))
\end{tikzcd}$$

$$\ker \phi_B = \langle P_B + rQ_B \rangle, \quad \ker \phi_{0,B} = \langle \tau(P_B) + r\tau(Q_B) \rangle, \quad \ker \phi_{1,B} = \langle \phi_1(P_B) + r\phi_1(Q_B) \rangle$$

Ciphertext: $(E_s', \beta\phi_{0,B}(\tau(P_C)), \beta^{-1}\phi_{0,B}(\tau(Q_C)))$ and $(E_1', \beta\phi_{1,B}(P_1), \beta^{-1}\phi_{1,B}(Q_1))$
Shared key: E
Secret key: (r, β)

IS-CUBE (3/3)

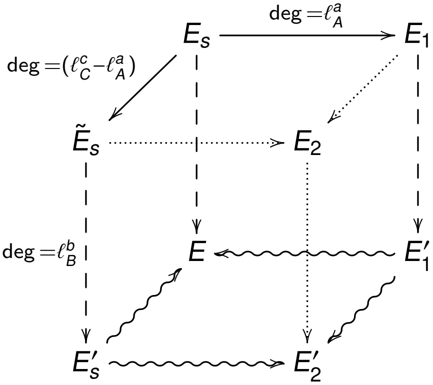
Decapsulation:

$$\begin{tikzcd}
 & E & \\
(E'_s, \alpha P'_0, \alpha^{-1} Q'_0) \arrow[ur, squiggly] \arrow[dr, squiggly] & & (E'_1, P'_1, Q'_1) \arrow[ul, squiggly] \arrow[dl, squiggly] \\
 & E' &
\end{tikzcd}$$

From Kani's theorem, the kernel of the isogeny $E'_s \times E'_1 \to E \times E'$ is $\langle(\alpha P'_0, P'_1), (\alpha^{-1} Q'_0, Q'_1)\rangle$.

Core idea (recall)

$p = \ell_C^c \cdot \ell_A \cdot \ell_B^b \cdot f - 1$, where ℓ_A, ℓ_B, ℓ_C are small distinct primes and f is a small integer.
$\ell_C^c \approx 2^{6\lambda}$, $\ell_A^a \approx 2^{6\lambda}$, $\ell_B^b \approx 2^{2\lambda}$, $p \approx 2^{8\lambda}$.



Public pamameter: $(E_s, \tilde{E}_s)$
Public key: E_1
Ciphertext: (E_s', E_1')
Shared key: E

How to construct τ (1/6)

$\deg \tau = \ell^c_C - \ell^a_A$ is not smooth in general.
$\rightarrow$ How do we construct τ?

How to construct τ (1/6)

$\deg \tau = \ell_C^c - \ell_A^a$ is not smooth in general.
$\rightarrow$ How do we construct τ?

Use the structure of the endomorphism ring of the curve of j-invariant 1728.

How to construct τ (1/6)

$\deg \tau = \ell_C^c - \ell_A^a$ is not smooth in general.
$\rightarrow$ How do we construct τ?

Use the structure of the endomorphism ring of the curve of j-invariant 1728.

Let E_0 be the curve of j-invariant 1728.
Then, $\mathrm{End}(E_0) \cong \mathbb{Z}\langle \sqrt{-1}, \frac{1+\sqrt{-p}}{2} \rangle$ (an order in a quaternion algebra over $\mathbb{Q}$).

How to construct τ (2/6)

Let $N = (\ell_C^c - \ell_A^a) \cdot (\ell_B^b)^2$.

From the Cornacchia algorithm, we can find integers z_1, z_2, z_3, z_4 such that

$$z_1^2 + z_2^2 + p(z_3^2 + z_4^2) = N.$$

How to construct τ (2/6)

Let $N = (\ell_C^c - \ell_A^a) \cdot (\ell_B^b)^2$.

From the Cornacchia algorithm, we can find integers z_1, z_2, z_3, z_4 such that

$$z_1^2 + z_2^2 + p(z_3^2 + z_4^2) = N.$$

Set $\gamma := [z_1] + [z_2]\sqrt{-1} + \sqrt{-p}([z_3] + [z_4]\sqrt{-1}) \in \mathrm{End}(E_0)$. Then $\deg \gamma = N$.

How to construct τ (2/6)

Let $N = (\ell_C^c - \ell_A^a) \cdot (\ell_B^b)^2$.

From the Cornacchia algorithm, we can find integers z_1, z_2, z_3, z_4 such that

$$z_1^2 + z_2^2 + p(z_3^2 + z_4^2) = N.$$

Set $\gamma := [z_1] + [z_2]\sqrt{-1} + \sqrt{-p}([z_3] + [z_4]\sqrt{-1}) \in \mathrm{End}(E_0)$. Then $\deg\gamma = N$.

$\rightarrow$ We have $\gamma = \hat{\psi}' \circ \tau_0 \circ \psi$, where $\deg\psi' = \ell_B^b$, $\deg\psi = \ell_B^b$, and $\deg\tau_0 = \ell_C^c - \ell_A^a$.

How to construct τ (3/6)

$$\begin{tikzcd} & E_0 \arrow[dl, "\psi"'] \arrow[dr, "\psi'"] & \\ E_{s,0} \arrow[rr, "\tau_0"'] & & \tilde{E}_{s,0} \end{tikzcd}$$

$\ker \psi = \ker \gamma \cap E[\ell_B^b]$ and $\ker \psi' = \ker \hat{\gamma} \cap E[\ell_B^b]$.

How to construct τ (3/6)

$$\begin{tikzcd} & E_0 \arrow[dl, "\psi"'] \arrow[dr, "\psi'"] & \\ E_{s,0} \arrow[rr, "\tau_0"'] & & \tilde{E}_{s,0} \end{tikzcd}$$

$\ker\psi = \ker\gamma \cap E[\ell_B^b]$ and $\ker\psi' = \ker\hat{\gamma} \cap E[\ell_B^b]$.

Image points $\rightarrow$ $\tau_0(P) = \frac{1}{\ell_B^{2b}}\psi'(\gamma(\hat{\psi}(P)))$ if $\gcd(\mathrm{ord}(P), \ell_B) = 1$.

How to construct τ (3/6)

$$\begin{tikzcd} & E_0 \arrow[dl, "\psi"'] \arrow[dr, "\psi'"] & \\ E_{s,0} \arrow[rr, "\tau_0"'] & & \tilde{E}_{s,0} \end{tikzcd}$$

$\ker \psi = \ker \gamma \cap E[\ell_B^b]$ and $\ker \psi' = \ker \hat{\gamma} \cap E[\ell_B^b]$.

Image points $\rightarrow$ $\tau_0(P) = \frac{1}{\ell_B^{2b}} \psi'(\gamma(\hat{\psi}(P)))$ if $\gcd(\mathrm{ord}(P), \ell_B) = 1$.

How do we compute image points of $E_{s,0}[\ell_B^b]$?

How to construct τ (4/6)

$\{P_{C,0}, Q_{C,0}\}$: a basis of $E_{s,0}[\ell_C^c]$
Assume that a is even (for simplicity).

$$\begin{tikzcd}
(E_{s,0}, P_{C,0}, Q_{C,0}) \arrow[r, "\tau_0"] \arrow[d, "{[\ell_A^{a/2}]}"'] & (\tilde{E}_{s,0}, \tau_0(P_{C,0}), \tau_0(Q_{C,0})) \arrow[d, "{[\ell_A^{a/2}]}"] \\
(E_{s,0}, \ell_A^{a/2} P_{C,0}, \ell_A^{a/2} Q_{C,0}) \arrow[r, "\tau_0"'] & (\tilde{E}_{s,0}, \ell_A^{a/2}\tau_0(P_{C,0}), \ell_A^{a/2}\tau_0(Q_{C,0}))
\end{tikzcd}$$

How to construct τ (4/6)

$\{P_{C,0}, Q_{C,0}\}$: a basis of $E_{s,0}[\ell_C^c]$
Assume that a is even (for simplicity).

$$\begin{tikzcd}
(E_{s,0}, P_{C,0}, Q_{C,0}) \arrow[rr, "\tau_0"] \arrow[d, "{[\ell_A^{a/2}]}"'] & & (\tilde{E}_{s,0}, \tau_0(P_{C,0}), \tau_0(Q_{C,0})) \arrow[d, "{[\ell_A^{a/2}]}"] \\
(E_{s,0}, \ell_A^{a/2} P_{C,0}, \ell_A^{a/2} Q_{C,0}) \arrow[rr, "\tau_0"'] & & (\tilde{E}_{s,0}, \ell_A^{a/2}\tau_0(P_{C,0}), \ell_A^{a/2}\tau_0(Q_{C,0}))
\end{tikzcd}$$

From Kani's theorem, $\langle (\ell_A^{a/2} P_{C,0}, \tau_0(P_{C,0})), \ell_A^{a/2} Q_{C,0}, \tau_0(Q_{C,0}) \rangle$ is the kernel of

$$\Psi_0 = \begin{pmatrix} [\ell_A^{a/2}] & \hat{\tau}_0 \\ {\color{blue}-\tau_0} & [\ell_A^{a/2}] \end{pmatrix}.$$

How to construct τ (4/6)

$\{P_{C,0}, Q_{C,0}\}$: a basis of $E_{s,0}[\ell_C^c]$
Assume that a is even (for simplicity).

$$\begin{tikzcd}
(E_{s,0}, P_{C,0}, Q_{C,0}) \arrow[r, "\tau_0"] \arrow[d, "{[\ell_A^{a/2}]}"'] & (\tilde{E}_{s,0}, \tau_0(P_{C,0}), \tau_0(Q_{C,0})) \arrow[d, "{[\ell_A^{a/2}]}"] \\
(E_{s,0}, \ell_A^{a/2} P_{C,0}, \ell_A^{a/2} Q_{C,0}) \arrow[r, "\tau_0"'] & (\tilde{E}_{s,0}, \ell_A^{a/2}\tau_0(P_{C,0}), \ell_A^{a/2}\tau_0(Q_{C,0}))
\end{tikzcd}$$

From Kani's theorem, $\langle(\ell_A^{a/2} P_{C,0}, \tau_0(P_{C,0})), \ell_A^{a/2} Q_{C,0}, \tau_0(Q_{C,0})\rangle$ is the kernel of

$$\Psi_0 = \begin{pmatrix} [\ell_A^{a/2}] & \hat{\tau}_0 \\ -\tau_0 & [\ell_A^{a/2}] \end{pmatrix}.$$

$\rightarrow$ We can compute $\tau_0(P_{B,0})$ and $\tau_0(Q_{B,0})$, where $\{P_{B,0}, Q_{B,0}\}$ is a basis of $E_{s,0}[\ell_B^b]$.

How to construct τ (5/6)

Remaining problem: $E_{s,0}$ and $\tilde{E}_{s,0}$ are not random curves!

How to construct τ (5/6)

Remaining problem: $E_{s,0}$ and $\tilde{E}_{s,0}$ are not random curves!

Randomize the starting curve:
We have $(E_{s,0}, P_{C,0}, Q_{C,0}, P_{B,0}, Q_{B,0})$ and $(\tilde{E}_{s,0}, \tau_0(P_{C,0}), \tau_0(Q_{C,0}), \tau_0(P_{B,0}), \tau_0(Q_{B,0}))$.

How to construct τ (5/6)

Remaining problem: $E_{s,0}$ and $\tilde{E}_{s,0}$ are not random curves!

Randomize the starting curve:
We have $(E_{s,0}, P_{C,0}, Q_{C,0}, P_{B,0}, Q_{B,0})$ and $(\tilde{E}_{s,0}, \tau_0(P_{C,0}), \tau_0(Q_{C,0}), \tau_0(P_{B,0}), \tau_0(Q_{B,0}))$.

1. Compute two parallel ℓ_B^b-isogenies using $P_{B,0}, Q_{B,0}$ and $\tau_0(P_{B,0}), \tau_0(Q_{B,0})$. Obtain $(E_{s,1}, P'_{C,1}, Q'_{C,1})$ and $(\tilde{E}_{s,1}, \tau_1(P'_{C,1}), \tau_1(Q'_{C,1}))$.

How to construct τ (5/6)

Remaining problem: $E_{s,0}$ and $\tilde{E}_{s,0}$ are not random curves!

Randomize the starting curve:
We have $(E_{s,0}, P_{C,0}, Q_{C,0}, P_{B,0}, Q_{B,0})$ and $(\tilde{E}_{s,0}, \tau_0(P_{C,0}), \tau_0(Q_{C,0}), \tau_0(P_{B,0}), \tau_0(Q_{B,0}))$.

1. Compute two parallel ℓ_B^b-isogenies using $P_{B,0}, Q_{B,0}$ and $\tau_0(P_{B,0}), \tau_0(Q_{B,0})$. Obtain $(E_{s,1}, P'_{C,1}, Q'_{C,1})$ and $(\tilde{E}_{s,1}, \tau_1(P'_{C,1}), \tau_1(Q'_{C,1}))$.
2. Set ${}^t(P_{C,1}, Q_{C,1}) = \mathbf{A}\,{}^t(P'_{C,1}, Q'_{C,1})$ for a random regular matrix $\mathbf{A}$ over $\mathbb{Z}/\ell_C^c\mathbb{Z}$.

How to construct τ (5/6)

Remaining problem: $E_{s,0}$ and $\tilde{E}_{s,0}$ are not random curves!

Randomize the starting curve:
We have $(E_{s,0}, P_{C,0}, Q_{C,0}, P_{B,0}, Q_{B,0})$ and $(\tilde{E}_{s,0}, \tau_0(P_{C,0}), \tau_0(Q_{C,0}), \tau_0(P_{B,0}), \tau_0(Q_{B,0}))$.

1. Compute two parallel ℓ_B^b-isogenies using $P_{B,0}, Q_{B,0}$ and $\tau_0(P_{B,0}), \tau_0(Q_{B,0})$. Obtain $(E_{s,1}, P'_{C,1}, Q'_{C,1})$ and $(\tilde{E}_{s,1}, \tau_1(P'_{C,1}), \tau_1(Q'_{C,1}))$.
2. Set ${}^t(P_{C,1}, Q_{C,1}) = \mathbf{A}\,{}^t(P'_{C,1}, Q'_{C,1})$ for a random regular matrix $\mathbf{A}$ over $\mathbb{Z}/\ell_C^c\mathbb{Z}$.
3. Compute $\tau_1(P_{B,1}), \tau_1(Q_{B,1})$ for a random basis $\{P_{B,1}, Q_{B,1}\}$ of $E_{s,1}[\ell_B^b]$ from $P_{C,1}, Q_{C,1}, \tau_1(P_{C,1}), \tau_1(Q_{C,1})$ and Kani's theorem.

How to construct τ (5/6)

Remaining problem: $E_{s,0}$ and $\tilde{E}_{s,0}$ are not random curves!

Randomize the starting curve:
We have $(E_{s,0}, P_{C,0}, Q_{C,0}, P_{B,0}, Q_{B,0})$ and $(\tilde{E}_{s,0}, \tau_0(P_{C,0}), \tau_0(Q_{C,0}), \tau_0(P_{B,0}), \tau_0(Q_{B,0}))$.

1. Compute two parallel ℓ_B^b-isogenies using $P_{B,0}, Q_{B,0}$ and $\tau_0(P_{B,0}), \tau_0(Q_{B,0})$. Obtain $(E_{s,1}, P'_{C,1}, Q'_{C,1})$ and $(\tilde{E}_{s,1}, \tau_1(P'_{C,1}), \tau_1(Q'_{C,1}))$.
2. Set ${}^t(P_{C,1}, Q_{C,1}) = \mathbf{A}\,{}^t(P'_{C,1}, Q'_{C,1})$ for a random regular matrix $\mathbf{A}$ over $\mathbb{Z}/\ell_C^c\mathbb{Z}$.
3. Compute $\tau_1(P_{B,1}), \tau_1(Q_{B,1})$ for a random basis $\{P_{B,1}, Q_{B,1}\}$ of $E_{s,1}[\ell_B^b]$ from $P_{C,1}, Q_{C,1}, \tau_1(P_{C,1}), \tau_1(Q_{C,1})$ and Kani's theorem.
4. Output $(E_{s,1}, P_{C,1}, Q_{C,1}, P_{B,1}, Q_{B,1})$ and $(\tilde{E}_{s,1}, \tau_1(P_{C,1}), \tau_1(Q_{C,1}), \tau_1(P_{B,1}), \tau_1(Q_{B,1}))$.

How to construct τ (5/6)

Remaining problem: $E_{s,0}$ and $\tilde{E}_{s,0}$ are not random curves!

Randomize the starting curve:
We have $(E_{s,0}, P_{C,0}, Q_{C,0}, P_{B,0}, Q_{B,0})$ and $(\tilde{E}_{s,0}, \tau_0(P_{C,0}), \tau_0(Q_{C,0}), \tau_0(P_{B,0}), \tau_0(Q_{B,0}))$.

1. Compute two parallel ℓ_B^b-isogenies using $P_{B,0}, Q_{B,0}$ and $\tau_0(P_{B,0}), \tau_0(Q_{B,0})$. Obtain $(E_{s,1}, P'_{C,1}, Q'_{C,1})$ and $(\tilde{E}_{s,1}, \tau_1(P'_{C,1}), \tau_1(Q'_{C,1}))$.
2. Set ${}^t(P_{C,1}, Q_{C,1}) = \mathbf{A}\,{}^t(P'_{C,1}, Q'_{C,1})$ for a random regular matrix $\mathbf{A}$ over $\mathbb{Z}/\ell_C^c\mathbb{Z}$.
3. Compute $\tau_1(P_{B,1}), \tau_1(Q_{B,1})$ for a random basis $\{P_{B,1}, Q_{B,1}\}$ of $E_{s,1}[\ell_B^b]$ from $P_{C,1}, Q_{C,1}, \tau_1(P_{C,1}), \tau_1(Q_{C,1})$ and Kani's theorem.
4. Output $(E_{s,1}, P_{C,1}, Q_{C,1}, P_{B,1}, Q_{B,1})$ and $(\tilde{E}_{s,1}, \tau_1(P_{C,1}), \tau_1(Q_{C,1}), \tau_1(P_{B,1}), \tau_1(Q_{B,1}))$.

Repeat the above procedure.

How to construct τ (6/6)

$$\begin{tikzcd}
(E_{s,0}, P_{C,0}, Q_{C,0}, P_{B,0}, Q_{B,0}) \arrow[r, "\tau_0"] \arrow[d, "\deg = \ell_B^b"'] & (\tilde{E}_{s,0}, \tau_0(P_{C,0}), \tau_0(Q_{C,0}), \tau_0(P_{B,0}), \tau_0(Q_{B,0})) \arrow[d, "\deg = \ell_B^b"] \\
(E_{s,1}, P_{C,1}, Q_{C,1}, P_{B,1}, Q_{B,1}) \arrow[r, "\tau_1"] \arrow[d] & (\tilde{E}_{s,1}, \tau_1(P_{C,1}), \tau_1(Q_{C,1}), \tau_1(P_{B,1}), \tau_1(Q_{B,1})) \arrow[d] \\
\vdots \arrow[d] & \vdots \arrow[d] \\
(E_s, P_C, Q_C, P_B, Q_B) \arrow[r, "\tau"] & (\tilde{E}_s, \tau(P_C), \tau(Q_C), \tau(P_B), \tau(Q_B))
\end{tikzcd}$$

Parameters for IS-CUBE

Table: Parameters for IS-CUBE

λ	p (in bits)	Public key	Ciphertext	Compressed (P)	Compressed (C)
128	$1,044$	$1,305$ bytes	$1,566$ bytes	649 bytes	$1,104$ bytes
192	$1,558$	$1,948$ bytes	$2,337$ bytes	969 bytes	$1,649$ bytes
256	$2,068$	$2,585$ bytes	$3,102$ bytes	$1,289$ bytes	$2,192$ bytes

In any cases, $\text{bit}(p) \approx 8\lambda$.

SIKE vs IS-CUBE

Assume that the prime for SIKE has the size of 4λ bits.

Table: Comparison of IS-CUBE with SIKE

	SIKE		IS-CUBE	
	original	compressed	original	compressed
Public key	24λ	14λ	80λ	40λ
Ciphertext	25λ	17λ	96λ	68λ

The public key of IS-CUBE is about 3 times larger than that of SIKE, and the ciphertext of IS-CUBE is about 4 times larger than that of SIKE.

PoC implementation

I implemented IS-CUBE via sagemath.

Table: Computational time of IS-CUBE

Computation \ Security parameter	128	192	256
Public parameters generation*	38.36 sec	112.18 sec	165.75 sec
Public key generation	4.34 sec	13.99 sec	34.43 sec
Key encapsulation	0.61 sec	1.22 sec	2.10 sec
Key decapsulation	17.13 sec	39.06 sec	74.61 sec

We measured the averages of 100 run times of each algorithm of IS-CUBE except for the computational time of the public parameters generation. We used a MacBook Air with an Apple M1 CPU (3.2 GHz) to measure the computational time.