SETA: supersingular encryption from torsion attacks

Antonin Leroux, joint work with L. De Feo, C. Delpech de Saint Guilhem, T. B. Fouotsa, P. Kutas, C. Petit, J. Silva, B. Wesolowski

DGA, Ecole Polytechnique, Institut Polytechnique de Paris, Inria Saclay

The State of Post-Quantum Cryptography

Six families still in Round 3 NIST post-quantum competition (Finalists + Alternate Candidates):

Lattices	4 encryption	2 signature
Codes	3 encryption	
Multivariate		2 signature
Isogenies	1 encryption	
Hash-based		1 signature
MPC		1 signature

The State of Post-Quantum Cryptography

Six families still in Round 3 NIST post-quantum competition (Finalists + Alternate Candidates):

Lattices	4 encryption	2 signature	
Codes	3 encryption		
Multivariate		2 signature	
Isogenies	1 encryption		compact keys
Hash-based		1 signature	
MPC		1 signature	

The State of Post-Quantum Cryptography

Six families still in Round 3 NIST post-quantum competition (Finalists + Alternate Candidates):

Lattices	4 encryption	2 signature	
Codes	3 encryption		
Multivariate		2 signature	
Isogenies	1 encryption		compact keys poor efficiency
Hash-based		1 signature	
MPC		1 signature	

The State of Post-Quantum Cryptography

Six families still in Round 3 NIST post-quantum competition (Finalists + Alternate Candidates):

Lattices	4 encryption	2 signature	
Codes	3 encryption		
Multivariate		2 signature	
Isogenies	1 encryption		compact keys poor efficiency
Hash-based		1 signature	
MPC		1 signature	

Many more isogeny-based protocols since then....

The State of Post-Quantum Cryptography

Six families still in Round 3 NIST post-quantum competition (Finalists + Alternate Candidates):

Lattices	4 encryption	2 signature	
Codes	3 encryption		
Multivariate		2 signature	
Isogenies	1 encryption		compact keys poor efficiency
Hash-based		1 signature	
MPC		1 signature	

Many more isogeny-based protocols since then....

Other encryption schemes?

Contributions

SETA: a *public key encryption* based on a *trapdoor one way function* inspired by the **torsion points attacks** from Petit, 2017.

Petit, "Faster algorithms for isogeny problems using torsion point images," 2017

Contributions

SETA: a *public key encryption* based on a *trapdoor one way function* inspired by the **torsion points attacks** from Petit, 2017.

A concrete set of parameters for SETA and a first implementation.

Petit, "Faster algorithms for isogeny problems using torsion point images," 2017

Contributions

SETA: a *public key encryption* based on a *trapdoor one way function* inspired by the **torsion points attacks** from Petit, 2017.

A concrete set of parameters for SETA and a first implementation.

A new "uber"-isogeny assumption to encompass all isogeny-based assumption.

Petit, “Faster algorithms for isogeny problems using torsion point images,” 2017

Introduction to isogeny-based cryptograpy

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

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

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

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

$E(\mathbb{F}_q)$ is an *additive* group.

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

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

$E(\mathbb{F}_q)$ is an *additive* group. *Scalar multiplication* $[n]_E$ is the analog of exponentiation in this group. $E[n] \cong \mathbb{Z}/n\mathbb{Z}^2$: n-torsion subgroup.

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

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

$E(\mathbb{F}_q)$ is an *additive* group. *Scalar multiplication* $[n]_E$ is the analog of exponentiation in this group. $E[n] \cong \mathbb{Z}/n\mathbb{Z}^2$: n-torsion subgroup.

Separable isogeny :

$$\varphi : E \to F, \text{ uniquely defined by } \ker \varphi$$

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

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

$E(\mathbb{F}_q)$ is an *additive* group. *Scalar multiplication* $[n]_E$ is the analog of exponentiation in this group. $E[n] \cong \mathbb{Z}/n\mathbb{Z}^2$: n-torsion subgroup.

Separable isogeny :

$$\varphi : E \to F, \text{ uniquely defined by } \ker \varphi$$

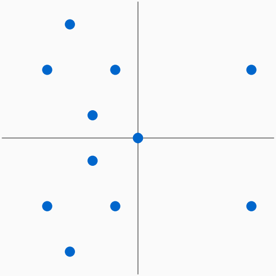
The **degree** is $\deg(\varphi) = \# \ker(\varphi)$.

The **dual** isogeny $\hat{\varphi} : F \to E$

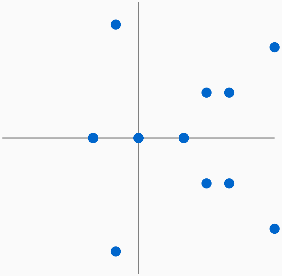
$$\hat{\varphi} \circ \varphi = [\deg(\varphi)]_E.$$

Isogenies: an example over $\mathbb{F}_{11}$

$E\ :\ y^2 = x^3 + x$

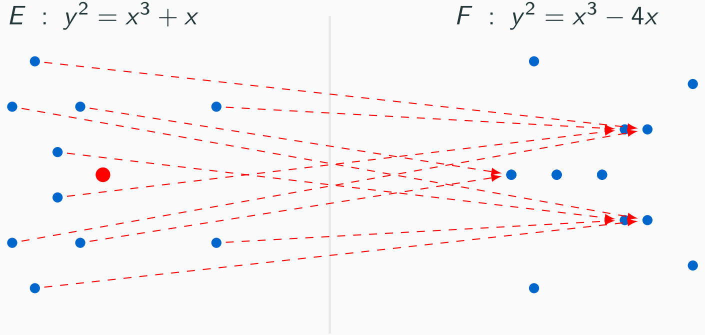


$F\ :\ y^2 = x^3 - 4x$



$$\varphi(x,y) = \left(\frac{x^2+1}{x},\quad y\frac{x^2-1}{x^2}\right)$$

Isogenies: an example over $\mathbb{F}_{11}$



$$\varphi(x, y) = \left(\frac{x^2+1}{x},\quad y\frac{x^2-1}{x^2}\right)$$

- Kernel generator in red.
- This is a degree 2 map.
- Analogous to $x \mapsto x^2$ in $\mathbb{F}_q^*$.

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Examples: $[n]_E$ for $n \in \mathbb{Z}$,

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Examples: $[n]_E$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Examples: $[n]_E$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

$E(\mathbb{F}_q)$:

- **Ordinary** when $\mathrm{End}(E)$ is an *order* of a quadratic imaginary field.

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Examples: $[n]_E$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

$E(\mathbb{F}_q)$:

- **Ordinary** when $\mathrm{End}(E)$ is an *order* of a quadratic imaginary field.
- **Supersingular** when $\mathrm{End}(E)$ is a maximal *order* of a quaternion algebra.

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Examples: $[n]_E$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

$E(\mathbb{F}_q)$:

- **Ordinary** when $\mathrm{End}(E)$ is an *order* of a quadratic imaginary field.
- **Supersingular** when $\mathrm{End}(E)$ is a maximal *order* of a quaternion algebra.

This talk $\to$ supersingular curves.

Supersingular Isogeny Diffie Hellman

Key exchange betw. Alice and Bob.

Jao and De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," 2011

Supersingular Isogeny Diffie Hellman

Key exchange betw. Alice and Bob. Deg. N_A, N_B with $N_A \wedge N_B = 1$.

Jao and De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," 2011

Key exchange betw. Alice and Bob. Deg. N_A, N_B with $N_A \wedge N_B = 1$.

$$\begin{tikzcd}
 & E_A \\
E_0 \arrow[ur, "\varphi_A"] \arrow[dr, "\varphi_B"'] & \\
 & E_B
\end{tikzcd}$$

Jao and De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," 2011

Supersingular Isogeny Diffie Hellman

Key exchange betw. Alice and Bob. Deg. N_A, N_B with $N_A \wedge N_B = 1$.

$$
\begin{tikzcd}
 & E_A \arrow[r, "{[\varphi_A]_*\varphi_B}"] & {} \\
E_0 \arrow[ur, "\varphi_A"] \arrow[dr, "\varphi_B"'] & & \\
 & E_B \arrow[r, "{[\varphi_B]_*\varphi_A}"'] & {}
\end{tikzcd}
$$

Push-forward isogeny: $\ker([\varphi]_*\psi) = \varphi(\ker \psi)$.

Jao and De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," 2011

Supersingular Isogeny Diffie Hellman

Key exchange betw. Alice and Bob. Deg. N_A, N_B with $N_A \wedge N_B = 1$.

$$\begin{tikzcd}
& E_A \arrow[dr, "{[\varphi_A]_*\varphi_B}"] & \\
E_0 \arrow[ur, "\varphi_A"] \arrow[dr, "\varphi_B"'] & & E_{AB} \arrow[d, phantom, "\simeq"] \\
& E_B \arrow[r, "{[\varphi_B]_*\varphi_A}"'] & E_{BA}
\end{tikzcd}$$

Push-forward isogeny: $\ker([\varphi]_*\psi) = \varphi(\ker\psi)$.

Jao and De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," 2011

Supersingular Isogeny Diffie Hellman

Key exchange betw. Alice and Bob. Deg. N_A, N_B with $N_A \wedge N_B = 1$.

$$\begin{tikzcd}
 & E_A \arrow[r, "{[\varphi_A]_*\varphi_B}"] & E_{AB} \arrow[d, phantom, "\simeq"] \\
E_0 \arrow[ur, "\varphi_A"] \arrow[dr, "\varphi_B"'] & & E_{BA} \\
 & E_B \arrow[ur, "{[\varphi_B]_*\varphi_A}"'] &
\end{tikzcd}$$

Push-forward isogeny: $\ker([\varphi]_*\psi) = \varphi(\ker\psi)$.

PK_A (resp. for PK_B) include $\varphi_A(P_B), \varphi_A(Q_B)$ (resp. $\varphi_B(P_A), \varphi_B(Q_A)$)
with $E_0[N_B] = \langle P_B, Q_B\rangle$ and $E_0[N_A] = \langle P_A, Q_A\rangle$.

Jao and De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," 2011

Key recovery Problem

The **Computational Supersingular Isogeny (CSSI)** problem:

CSSI: Find $\varphi_A : E_0 \to E_A$ of degree N_A given E_0, E_A.

Key recovery Problem

The **Computational Supersingular Isogeny (CSSI)** problem:

CSSI: Find $\varphi_A : E_0 \to E_A$ of degree N_A given E_0, E_A.

SIDH key recovery is the **CSSI with Torsion (CSSI-T)** problem:

CSSI-T : Find $\varphi_A : E_0 \to E_A$ from $E_A, \varphi_A(P_B), \varphi_A(Q_B)$ when $E_0[N_B] = \langle P_B, Q_B \rangle$.

Key recovery Problem

The **Computational Supersingular Isogeny (CSSI)** problem:

CSSI: Find $\varphi_A : E_0 \to E_A$ of degree N_A given E_0, E_A.

SIDH key recovery is the **CSSI with Torsion (CSSI-T)** problem:

CSSI-T : Find $\varphi_A : E_0 \to E_A$ from $E_A, \varphi_A(P_B), \varphi_A(Q_B)$ when $E_0[N_B] = \langle P_B, Q_B \rangle$.

In the case of SIDH, E_0 is *fixed* and has known endomorphism ring.

Key recovery Problem

The **Computational Supersingular Isogeny (CSSI)** problem:

CSSI: Find $\varphi_A : E_0 \to E_A$ of degree N_A given E_0, E_A.

SIDH key recovery is the **CSSI with Torsion (CSSI-T)** problem:

CSSI-T : Find $\varphi_A : E_0 \to E_A$ from $E_A, \varphi_A(P_B), \varphi_A(Q_B)$ when $E_0[N_B] = \langle P_B, Q_B \rangle$.

In the case of SIDH, E_0 is *fixed* and has known endomorphism ring.

Endomorphism Ring problem: Given a curve E, find $\mathrm{End}(E)$.

Torsion point attacks and applications

Starting curve with known endomorphism ring

Target **CSSI-T** when $\mathrm{End}(E_0)$ is known.

Starting curve with known endomorphism ring

Target **CSSI-T** when $\mathrm{End}(E_0)$ is known.

$\varphi_A : E_0 \to E_A$ imply

$$\mathbb{Z} + \varphi_A \circ \mathrm{End}(E_0) \circ \hat{\varphi}_A \hookrightarrow \mathrm{End}(E_A)$$

$$\begin{tikzcd} E_0 \arrow[loop left, "\theta"] \arrow[r, shift left, "\varphi_A"] & E_A \arrow[l, shift left, "\hat{\varphi}_A"] \end{tikzcd}$$

Starting curve with known endomorphism ring

Target **CSSI-T** when $\mathrm{End}(E_0)$ is known.

$\varphi_A : E_0 \to E_A$ imply

$$\mathbb{Z} + \varphi_A \circ \mathrm{End}(E_0) \circ \hat{\varphi}_A \hookrightarrow \mathrm{End}(E_A)$$

$$\begin{tikzcd} E_0 \arrow[loop left, "\theta"] \arrow[r, shift left, "\varphi_A"] & E_A \arrow[l, shift left, "\hat{\varphi}_A"] \end{tikzcd}$$

When $\psi = [d] + \varphi_A \circ \theta \circ \hat{\varphi}_A$ has **degree** N_B^2, $\ker \psi$ computed from $\varphi_A(P_B), \varphi_A(Q_B)$.

The torsion point attack

Once $\psi = [d] + \varphi_A \circ \theta \circ \hat{\varphi}_A$ is known:

$$\ker \hat{\varphi}_A =^1 \ker(\psi - [d]) \cap E_2[N_A]$$

[1]under a small condition on θ

The torsion point attack

Once $\psi = [d] + \varphi_A \circ \theta \circ \hat{\varphi}_A$ is known:

$$\ker \hat{\varphi}_A =^{1} \ker(\psi - [d]) \cap E_2[N_A]$$

Break CSSI-T $\Rightarrow$ find d, θ such that

$$\deg([d] + \varphi_A \circ \theta \circ \hat{\varphi}_A) = N_B^2.$$

[1] under a small condition on θ

The torsion point attack

Once $\psi = [d] + \varphi_A \circ \theta \circ \hat{\varphi}_A$ is known:

$$\ker \hat{\varphi}_A =^1 \ker(\psi - [d]) \cap E_2[N_A]$$

Break CSSI-T $\Rightarrow$ find d, θ such that

$$\deg([d] + \varphi_A \circ \theta \circ \hat{\varphi}_A) = N_B^2.$$

$j(E_0) = 1728 \Rightarrow$ **norm equation** $d^2 + N_A^2(c^2 + p(b^2 + a^2)) = N_B^2$.

[1] under a small condition on θ

The torsion point attack

Once $\psi = [d] + \varphi_A \circ \theta \circ \hat{\varphi}_A$ is known:

$$\ker \hat{\varphi}_A =^1 \ker(\psi - [d]) \cap E_2[N_A]$$

Break CSSI-T $\Rightarrow$ find d, θ such that

$$\deg([d] + \varphi_A \circ \theta \circ \hat{\varphi}_A) = N_B^2.$$

$j(E_0) = 1728 \Rightarrow$ **norm equation** $d^2 + N_A^2(c^2 + p(b^2 + a^2)) = N_B^2$.

Known solutions when $N_B > pN_A$.

[1] under a small condition on θ

The torsion point attack

Once $\psi = [d] + \varphi_A \circ \theta \circ \hat{\varphi}_A$ is known:

$$\ker \hat{\varphi}_A =^{1} \ker(\psi - [d]) \cap E_2[N_A]$$

Break CSSI-T $\Rightarrow$ find d, θ such that

$$\deg([d] + \varphi_A \circ \theta \circ \hat{\varphi}_A) = N_B^2.$$

$j(E_0) = 1728 \Rightarrow$ **norm equation** $d^2 + N_A^2(c^2 + p(b^2 + a^2)) = N_B^2$.

Known solutions when $N_B > pN_A$. SIDH : $N_A \approx N_B \approx \sqrt{p}$. Still Secure !

[1] under a small condition on θ

Backdoor curves

What if E_0 is a special choice?

Backdoor curves

What if E_0 is a special choice?

Most generic **norm equation:** $d^2 + {N_A}^2 n = N_B^2,$

Backdoor curves

What if E_0 is a special choice?

Most generic **norm equation:** $d^2 + {N_A}^2 n = N_B^2$, solution when $N_B > N_A^2$.

Backdoor curves

What if E_0 is a special choice?

Most generic **norm equation:** $d^2 + {N_A}^2 n = N_B^2$, solution when $N_B > N_A^2$.

If $\mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0)$, E_0 is a **backdoor curve**.

Backdoor curves

What if E_0 is a special choice?

Most generic **norm equation:** $d^2 + {N_A}^2 n = N_B^2$, solution when $N_B > N_A^2$.

If $\mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0)$, E_0 is a **backdoor curve**.

The knowledge of $\theta \in \mathrm{End}(E_0)$ with $\mathbb{Z}[\theta] \cong \mathbb{Z}[\sqrt{-n}]$ breaks CSSI-T.

Backdoor curves

What if E_0 is a special choice?

Most generic **norm equation:** $d^2 + {N_A}^2 n = N_B^2$, solution when $N_B > N_A^2$.

If $\mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0)$, E_0 is a **backdoor curve**.

The knowledge of $\theta \in \mathrm{End}(E_0)$ with $\mathbb{Z}[\theta] \cong \mathbb{Z}[\sqrt{-n}]$ breaks CSSI-T.

We have a *trapdoor mechanism*!

The SETA trapdoor one-way function

Let d, n, N_A, N_B be a solution of $d^2 + {N_A}^2 n = N_B^2$.

The SETA trapdoor one-way function

Let d, n, N_A, N_B be a solution of $d^2 + {N_A}^2 n = N_B^2$.

Public description:

$$E_0, P, Q \text{ with } \mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0) \text{ and } \langle P, Q \rangle = E_0[N_B]$$

The SETA trapdoor one-way function

Let d, n, N_A, N_B be a solution of $d^2 + {N_A}^2 n = N_B^2$.

Public description:

$$E_0, P, Q \text{ with } \mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0) \text{ and } \langle P, Q \rangle = E_0[N_B]$$

Function:

$$(\varphi_A : E_0 \to E_A) \quad \mapsto \quad E_A, \varphi_A(P), \varphi_A(Q)$$

The SETA trapdoor one-way function

Let d, n, N_A, N_B be a solution of $d^2 + {N_A}^2 n = N_B^2$.

Public description:

$$E_0, P, Q \text{ with } \mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0) \text{ and } \langle P, Q \rangle = E_0[N_B]$$

Function:

$$(\varphi_A : E_0 \to E_A) \;\; \mapsto \;\; E_A, \varphi_A(P), \varphi_A(Q)$$

Trapdoor:

$$\theta \in \mathrm{End}(E_0) \text{ and } \mathbb{Z}[\theta] \cong \mathbb{Z}[\sqrt{-n}]$$

The SETA trapdoor one-way function

Let d, n, N_A, N_B be a solution of $d^2 + {N_A}^2 n = N_B^2$.

Public description:

$$E_0, P, Q \text{ with } \mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0) \text{ and } \langle P, Q \rangle = E_0[N_B]$$

Function:

$$(\varphi_A : E_0 \to E_A) \;\; \mapsto \;\; E_A, \varphi_A(P), \varphi_A(Q)$$

Trapdoor:

$$\theta \in \mathrm{End}(E_0) \text{ and } \mathbb{Z}[\theta] \cong \mathbb{Z}[\sqrt{-n}]$$

Inversion: Torsion points attack against the CSSI-T.

The SETA trapdoor one-way function

Let d, n, N_A, N_B be a solution of $d^2 + {N_A}^2 n = N_B^2$.

Public description:

$$E_0, P, Q \text{ with } \mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0) \text{ and } \langle P, Q \rangle = E_0[N_B]$$

Function:

$$(\varphi_A : E_0 \to E_A) \quad \mapsto \quad E_A, \varphi_A(P), \varphi_A(Q)$$

Trapdoor:

$$\theta \in \mathrm{End}(E_0) \text{ and } \mathbb{Z}[\theta] \cong \mathbb{Z}[\sqrt{-n}]$$

Inversion: Torsion points attack against the CSSI-T.

Inversion pb is the **CSSI-T** + $\mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0)$.

Implementation and parameters

Key Generation

Goal: Compute E_0 with $\mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0)$.

Key Generation

Goal: Compute E_0 with $\mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0)$.

Idea: use the *Deuring Correspondence*.

Need: a curve F_0 with known $\mathrm{End}(F_0) \cong \mathcal{O}_0$.

Key Generation

Goal: Compute E_0 with $\mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0)$.

Idea: use the *Deuring Correspondence*.

Need: a curve F_0 with known $\mathrm{End}(F_0) \cong \mathcal{O}_0$.

KeyGen:

1. Find θ of norm n and trace 0 inside *quaternion algebra*.
2. Find $\mathcal{O}$ max order containing θ.
3. Compute $I = \mathrm{ConnectingIdeal}(\mathcal{O}_0, \mathcal{O})$.
4. Compute $\varphi : F_0 \to E_0$ from I.

Key Generation

Goal: Compute E_0 with $\mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E_0)$.

Idea: use the *Deuring Correspondence*.

Need: a curve F_0 with known $\mathrm{End}(F_0) \cong \mathcal{O}_0$.

KeyGen:

1. Find θ of norm n and trace 0 inside *quaternion algebra*.
2. Find $\mathcal{O}$ max order containing θ.
3. Compute $I = \mathrm{ConnectingIdeal}(\mathcal{O}_0, \mathcal{O})$.
4. Compute $\varphi : F_0 \to E_0$ from I.

Bottleneck is Step 4.

Choice of parameters

Need smooth deg and have kernel def. over $\mathbb{F}_{p^k}$ for small k (deg $|p^k - 1$).

2

Choice of parameters

Need smooth deg and have kernel def. over $\mathbb{F}_{p^k}$ for small k (deg $| p^k - 1$).

Torsion requirement:

- N_A, N_B with $N_B > N_A^2$ and $\gcd(N_A, N_B) = 1$ (for enc/dec).
- T, ℓ^e with $T > p^{3/2}$ and $\gcd(\ell, T) = 1$ (for key generation).

2

Choice of parameters

Need smooth deg and have kernel def. over $\mathbb{F}_{p^k}$ for small k (deg $| p^k - 1$).

Torsion requirement:

- N_A, N_B with $N_B > N_A^2$ and $\gcd(N_A, N_B) = 1$ (for enc/dec).
- T, ℓ^e with $T > p^{3/2}$ and $\gcd(\ell, T) = 1$ (for key generation).

Security constraint:

- $\log N_A > 2\lambda$ (meet-in-the-middle attack).
- $\log p > 2\lambda$ (generic endomorphism ring computation).

2

Choice of parameters

Need smooth deg and have kernel def. over $\mathbb{F}_{p^k}$ for small k (deg $| p^k - 1$).

Torsion requirement:

- N_A, N_B with $N_B > N_A^2$ and $\gcd(N_A, N_B) = 1$ (for enc/dec).
- T, ℓ^e with $T > p^{3/2}$ and $\gcd(\ell, T) = 1$ (for key generation).

Security constraint:

- $\log N_A > 2\lambda$ (meet-in-the-middle attack).
- $\log p > 2\lambda$ (generic endomorphism ring computation).

A **tradeoff** between enc/dec and key gen time :

- $p > N_A N_B = 2^a 3^b$ over $\mathbb{F}_{p^2}$, T over $\mathbb{F}_{p^k}$: fast enc/dec, slow key gen[2]

[2] VERY VERY SLOW!

Choice of parameters

Need smooth deg and have kernel def. over $\mathbb{F}_{p^k}$ for small k (deg $|p^k - 1$).

Torsion requirement:

- N_A, N_B with $N_B > N_A^2$ and $\gcd(N_A, N_B) = 1$ (for enc/dec).
- T, ℓ^e with $T > p^{3/2}$ and $\gcd(\ell, T) = 1$ (for key generation).

Security constraint:

- $\log N_A > 2\lambda$ (meet-in-the-middle attack).
- $\log p > 2\lambda$ (generic endomorphism ring computation).

A **tradeoff** between enc/dec and key gen time :

- $p > N_A N_B = 2^a 3^b$ over $\mathbb{F}_{p^2}$, T over $\mathbb{F}_{p^k}$: fast enc/dec, slow key gen[2]
- $T\ell^e \approx N_A N_B$ def. over $\mathbb{F}_{p^2}$: reasonnable key gen, slow enc/dec

[2] VERY VERY SLOW!

Implementation result

Found a 400-bit prime $p = 2 \cdot 8426067021^{12} - 1$.

Implementation result

Found a 400-bit prime $p = 2 \cdot 8426067021^{12} - 1$.

$$
\begin{aligned}
N_A &= 43^{12} \cdot 84719^{11}, \\
N_B &= 3^{21} \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 73 \cdot 257^{12} \cdot 313 \cdot 1009 \cdot 2857 \cdot 3733 \cdot 5519 \cdot 696 \\
&\quad \cdot 53113 \cdot 499957 \cdot 763369 \cdot 2101657 \cdot 2616791 \cdot 7045009 \cdot 11959093 \\
&\quad \cdot 17499277 \cdot 20157451 \cdot 33475999 \cdot 39617833 \cdot 45932333, \\
T &= N_A \cdot N_B, \\
\ell^e &= 2^5.
\end{aligned}
$$

Implementation result

Found a 400-bit prime $p = 2 \cdot 8426067021^{12} - 1$.

$$
\begin{aligned}
N_A &= 43^{12} \cdot 84719^{11}, \\
N_B &= 3^{21} \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 73 \cdot 257^{12} \cdot 313 \cdot 1009 \cdot 2857 \cdot 3733 \cdot 5519 \cdot 696 \\
&\quad \cdot 53113 \cdot 499957 \cdot 763369 \cdot 2101657 \cdot 2616791 \cdot 7045009 \cdot 11959093 \\
&\quad \cdot 17499277 \cdot 20157451 \cdot 33475999 \cdot 39617833 \cdot 45932333, \\
T &= N_A \cdot N_B, \\
\ell^e &= 2^5.
\end{aligned}
$$

Keygen	Encryption	Decryption
10h	4.6s	10.6m

Table 1: SETA performances

Uber-isogeny assumption

CSIDH and group actions

Quadratic order $\mathfrak{O}$,

$$\mathcal{F}_{\mathfrak{O}} = \{(E,\iota) \mid \iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)\}, \ \ \mathcal{E}_{\mathfrak{O}} = \{E \mid \exists \iota, (E,\iota) \in \mathcal{F}_{\mathfrak{O}}\}.$$

CSIDH and group actions

Quadratic order $\mathfrak{O}$,

$$\mathcal{F}_{\mathfrak{O}} = \{(E, \iota) \mid \iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)\}, \ \ \mathcal{E}_{\mathfrak{O}} = \{E \mid \exists \iota, (E, \iota) \in \mathcal{F}_{\mathfrak{O}}\}.$$

Abelian Group Action:

$$\begin{aligned} Cl(\mathfrak{O}) \times \mathcal{F}_{\mathfrak{O}} &\to \mathcal{F}_{\mathfrak{O}} \\ \mathfrak{a}, (E, \iota) &\mapsto \mathfrak{a} \star (E, \iota). \end{aligned}$$

CSIDH and group actions

Quadratic order $\mathfrak{O}$,

$$\mathcal{F}_{\mathfrak{O}} = \{(E,\iota) \mid \iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)\}, \;\; \mathcal{E}_{\mathfrak{O}} = \{E \mid \exists \iota, (E,\iota) \in \mathcal{F}_{\mathfrak{O}}\}.$$

Abelian Group Action:

$$\begin{aligned} Cl(\mathfrak{O}) \times \mathcal{F}_{\mathfrak{O}} &\to \mathcal{F}_{\mathfrak{O}} \\ \mathfrak{a}, (E,\iota) &\mapsto \mathfrak{a} \star (E,\iota). \end{aligned}$$

CSIDH: $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$, ι induced by Frobenius π.

$$\begin{tikzcd} & \mathfrak{a} \star E \\ E \arrow[ur, "\varphi_{\mathfrak{a}}"] \arrow[dr, "\varphi_{\mathfrak{b}}"'] & \\ & \mathfrak{b} \star E \end{tikzcd}$$

Castryck et al., "CSIDH: an efficient post-quantum commutative group action," 2018

CSIDH and group actions

Quadratic order $\mathfrak{O}$,

$$\mathcal{F}_{\mathfrak{O}} = \{(E, \iota) \mid \iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)\}, \ \ \mathcal{E}_{\mathfrak{O}} = \{E \mid \exists \iota, (E, \iota) \in \mathcal{F}_{\mathfrak{O}}\}.$$

Abelian Group Action:

$$\begin{aligned} Cl(\mathfrak{O}) \times \mathcal{F}_{\mathfrak{O}} &\to \mathcal{F}_{\mathfrak{O}} \\ \mathfrak{a}, (E, \iota) &\mapsto \mathfrak{a} \star (E, \iota). \end{aligned}$$

CSIDH: $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$, ι induced by Frobenius π.

$$\begin{tikzcd} & \mathfrak{a} \star E \arrow[dr, "\varphi_{\mathfrak{ab}}"] & \\ E \arrow[ur, "\varphi_{\mathfrak{a}}"] \arrow[dr, "\varphi_{\mathfrak{b}}"'] & & {} \\ & \mathfrak{b} \star E \arrow[ur, "\varphi_{\mathfrak{ba}}"'] & \end{tikzcd}$$

Castryck et al., "CSIDH: an efficient post-quantum commutative group action," 2018

CSIDH and group actions

Quadratic order $\mathfrak{O}$,

$$\mathcal{F}_{\mathfrak{O}} = \{(E,\iota) \mid \iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)\},\ \ \mathcal{E}_{\mathfrak{O}} = \{E \mid \exists\iota, (E,\iota) \in \mathcal{F}_{\mathfrak{O}}\}.$$

Abelian Group Action:

$$\begin{aligned} Cl(\mathfrak{O}) \times \mathcal{F}_{\mathfrak{O}} &\to \mathcal{F}_{\mathfrak{O}} \\ \mathfrak{a}, (E,\iota) &\mapsto \mathfrak{a} \star (E,\iota). \end{aligned}$$

CSIDH: $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$, ι induced by Frobenius π.

$$\begin{tikzcd}
 & \mathfrak{a} \star E \arrow[dr, "\varphi_{\mathfrak{a}\mathfrak{b}}"] & \\
E \arrow[ur, "\varphi_{\mathfrak{a}}"] \arrow[dr, "\varphi_{\mathfrak{b}}"'] & & \mathfrak{a}\mathfrak{b} \star E \\
 & \mathfrak{b} \star E \arrow[ur, "\varphi_{\mathfrak{b}\mathfrak{a}}"'] &
\end{tikzcd}$$

Castryck et al., "CSIDH: an efficient post-quantum commutative group action," 2018

Uber isogeny problem

The $\mathfrak{O}$-**Uber-isogeny problem ($\mathfrak{O}$-UIP)**

$\mathfrak{O}$-**UIP**: Given $(E_0, \iota_0) \in \mathcal{F}_{\mathfrak{O}}$ and $E \in \mathcal{E}_{\mathfrak{O}}$. Find $\mathfrak{a}$ such that
$$(E, \iota) = \mathfrak{a} \star (E_0, \iota_0).$$

Uber isogeny problem

The $\mathfrak{O}$-**Uber-isogeny problem ($\mathfrak{O}$-UIP)**

$\mathfrak{O}$-**UIP**: Given $(E_0, \iota_0) \in \mathcal{F}_{\mathfrak{O}}$ and $E \in \mathcal{E}_{\mathfrak{O}}$. Find $\mathfrak{a}$ such that

$$(E, \iota) = \mathfrak{a} \star (E_0, \iota_0).$$

Best *generic* algorithm: $O(\#\mathcal{E}_{\mathfrak{O}})$ (we have $\#\mathcal{E}_{\mathfrak{O}} \leq \#\mathcal{F}_{\mathfrak{O}} \approx \sqrt{\operatorname{disc} \mathfrak{O}}$).

The $\mathfrak{O}$-**Uber-isogeny problem ($\mathfrak{O}$-UIP)**

$\mathfrak{O}$-**UIP**: Given $(E_0, \iota_0) \in \mathcal{F}_{\mathfrak{O}}$ and $E \in \mathcal{E}_{\mathfrak{O}}$. Find $\mathfrak{a}$ such that

$$(E, \iota) = \mathfrak{a} \star (E_0, \iota_0).$$

Best *generic* algorithm: $O(\#\mathcal{E}_{\mathfrak{O}})$ (we have $\#\mathcal{E}_{\mathfrak{O}} \leq \#\mathcal{F}_{\mathfrak{O}} \approx \sqrt{\operatorname{disc} \mathfrak{O}}$).

If ι is given, there is a subexponential algorithm in disc $\mathfrak{O}$. This is the case for **CSIDH** where ι is trivial from Frobenius.

Link with isogeny-based crypto

CSIDH: $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$.

$\mathbb{Z}[\sqrt{-p}]$-UIP $\Leftrightarrow$ **CSIDH** key recovery.

Link with isogeny-based crypto

CSIDH: $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$.

$$\mathbb{Z}[\sqrt{-p}]\text{-UIP} \Leftrightarrow \textbf{CSIDH} \text{ key recovery.}$$

SIDH: If $E_0 \in \mathcal{E}_{\mathfrak{O}_\mathbf{0}}$ and $\varphi_A : E_0 \to E_A$, then $E_A \in \mathcal{E}_{\mathbb{Z}+N_A\mathfrak{O}_\mathbf{0}}$.

$$\mathbb{Z} + N_A\mathfrak{O}_0\text{-UIP} \Rightarrow \textbf{SIDH} \text{ key recovery.}$$

Link with isogeny-based crypto

CSIDH: $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$.

$$\mathbb{Z}[\sqrt{-p}]\text{-UIP} \Leftrightarrow \textbf{CSIDH} \text{ key recovery.}$$

SIDH: If $E_0 \in \mathcal{E}_{\mathfrak{O}_0}$ and $\varphi_A : E_0 \to E_A$, then $E_A \in \mathcal{E}_{\mathbb{Z}+N_A\mathfrak{O}_0}$.

$$\mathbb{Z} + N_A\mathfrak{O}_0\text{-UIP} \Rightarrow \textbf{SIDH} \text{ key recovery.}$$

SETA: If $d^2 + nN_A^2 = N_B^2$, and $E_0 \in \mathcal{E}_{\mathbb{Z}[\sqrt{-n}]}$.

$$\mathbb{Z}[\sqrt{-n}]\text{-UIP} \Rightarrow \textbf{SETA} \text{ key recovery.}$$

Link with isogeny-based crypto

CSIDH: $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$.

$\mathbb{Z}[\sqrt{-p}]$-UIP $\Leftrightarrow$ **CSIDH** key recovery.

SIDH: If $E_0 \in \mathcal{E}_{\mathfrak{O}_\mathbf{0}}$ and $\varphi_A : E_0 \to E_A$, then $E_A \in \mathcal{E}_{\mathbb{Z}+N_A\mathfrak{O}_\mathbf{0}}$.

$\mathbb{Z} + N_A\mathfrak{O}_0$-UIP $\Rightarrow$ **SIDH** key recovery.

SETA: If $d^2 + nN_A^2 = N_B^2$, and $E_0 \in \mathcal{E}_{\mathbb{Z}[\sqrt{-n}]}$.

$\mathbb{Z}[\sqrt{-n}]$-UIP $\Rightarrow$ **SETA** key recovery.

CSSI: Exists $\mathfrak{O}$ such that every curve $E \in \mathcal{E}_{\mathfrak{O}}$.

$\mathfrak{O}$-UIP $\Rightarrow$ **CSSI**.

Conclusion and Open Problems

We presented a new post-quantum encryption scheme inspired by torsion attacks on SIDH. Efficiency is still order of magnitudes below SIDH but security relies on new problems. We have introduced the $\mathfrak{O}$-UIP, a new generic assumption for isogeny-based cryptography.

Future directions:

Conclusion and Open Problems

We presented a new post-quantum encryption scheme inspired by torsion attacks on SIDH. Efficiency is still order of magnitudes below SIDH but security relies on new problems. We have introduced the $\mathfrak{O}$-UIP, a new generic assumption for isogeny-based cryptography.

Future directions:

- Explore the tradeoffs for parameters.

Conclusion and Open Problems

We presented a new post-quantum encryption scheme inspired by torsion attacks on SIDH. Efficiency is still order of magnitudes below SIDH but security relies on new problems. We have introduced the $\mathfrak{O}$-UIP, a new generic assumption for isogeny-based cryptography.

Future directions:

- Explore the tradeoffs for parameters.
- Improve efficiency of key generation algorithms.

Conclusion and Open Problems

We presented a new post-quantum encryption scheme inspired by torsion attacks on SIDH. Efficiency is still order of magnitudes below SIDH but security relies on new problems. We have introduced the $\mathfrak{O}$-UIP, a new generic assumption for isogeny-based cryptography.

Future directions:

- Explore the tradeoffs for parameters.
- Improve efficiency of key generation algorithms.
- Understand the $\mathfrak{O}$-UIP and study $\mathcal{E}_{\mathfrak{O}}$.

Conclusion and Open Problems

We presented a new post-quantum encryption scheme inspired by torsion attacks on SIDH. Efficiency is still order of magnitudes below SIDH but security relies on new problems. We have introduced the $\mathfrak{O}$-UIP, a new generic assumption for isogeny-based cryptography.

Future directions:

- Explore the tradeoffs for parameters.
- Improve efficiency of key generation algorithms.
- Understand the $\mathfrak{O}$-UIP and study $\mathcal{E}_{\mathfrak{O}}$.
- SETA security.

Conclusion and Open Problems

We presented a new post-quantum encryption scheme inspired by torsion attacks on SIDH. Efficiency is still order of magnitudes below SIDH but security relies on new problems. We have introduced the $\mathfrak{O}$-UIP, a new generic assumption for isogeny-based cryptography.

Future directions:

- Explore the tradeoffs for parameters.
- Improve efficiency of key generation algorithms.
- Understand the $\mathfrak{O}$-UIP and study $\mathcal{E}_{\mathfrak{O}}$.
- SETA security.

https://eprint.iacr.org/2019/1291