A new isogeny representation and application to cryptography.

Antonin Leroux

ASIACRYPT, 2022

DGA, Ecole Polytechnique, INRIA Saclay

A little bit of isogeny-based cryptography recent history

1. (2011) SIDH
2. (2016) SIKE
3. (2018) CSIDH
4. (End of 2021) This work (pSIDH): new directions to explore.
5. (Summer of 2022) Attacks on SIDH.

Status report on recent attacks

Recent attacks by Castryck, Decru, Maino, Martindale and Robert break SIDH (isogeny problem with extra torsion information: images of some points through the secret isogeny).

Status report on recent attacks

Recent attacks by Castryck, Decru, Maino, Martindale and Robert break SIDH (isogeny problem with extra torsion information: images of some points through the secret isogeny).

The attack: Torsion information $\Rightarrow$ Can evaluate the secret isogeny $\Rightarrow$ Compute the kernel and recover the secret isogeny (under some conditions!)

Generic Isogeny problem is safe because no torsion information.

Status report on recent attacks

Recent attacks by Castryck, Decru, Maino, Martindale and Robert break SIDH (isogeny problem with extra torsion information: images of some points through the secret isogeny).

The attack: Torsion information $\Rightarrow$ Can evaluate the secret isogeny $\Rightarrow$ Compute the kernel and recover the secret isogeny (under some conditions!)

Generic Isogeny problem is safe because no torsion information.

- CSIDH and variants, SQISign are safe.
- SIDH, B-SIDH and Séta broken.
- pSIDH??

Mathematical Background

Elliptic curve and isogeny notations

Elliptic Curve over $\mathbb{F}_{p^k}$: $y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^k}$

Isogeny: rational map between elliptic curves.

Degree is $\approx$ degree of the defining polynomials $= \#\ker$.

Elliptic curve and isogeny notations

Elliptic Curve over $\mathbb{F}_{p^k}$: $y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^k}$

Isogeny: rational map between elliptic curves.

Degree is $\approx$ degree of the defining polynomials $= \#\ker$.

An **endomorphism** is an isogeny $\varphi : E \to E$.

Supersingular curves $\Leftrightarrow$ $\mathrm{End}(E)$ is a max. *order* in a quaternion algebra.

Elliptic curve and isogeny notations

Elliptic Curve over $\mathbb{F}_{p^k}$: $y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^k}$

Isogeny: rational map between elliptic curves.

Degree is $\approx$ degree of the defining polynomials $= \#\ker$.

An **endomorphism** is an isogeny $\varphi : E \to E$.

Supersingular curves $\Leftrightarrow$ $\mathrm{End}(E)$ is a max. *order* in a quaternion algebra.

The Isogeny Problem: Given two supersingular elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$.

Elliptic curve and isogeny notations

Elliptic Curve over $\mathbb{F}_{p^k}$: $y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^k}$

Isogeny: rational map between elliptic curves.

Degree is $\approx$ degree of the defining polynomials $= \#\ker$.

An **endomorphism** is an isogeny $\varphi : E \to E$.

Supersingular curves $\Leftrightarrow$ $\mathrm{End}(E)$ is a max. *order* in a quaternion algebra.

The Isogeny Problem: Given two supersingular elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$.

Best known attacks: requires random walk in the isogeny graph.
Complexity is polynomial in the size of the graph.

Quaternion algebra definitions

The quaternion algebra $\mathcal{B}(a, b)$ over $\mathbb{Q}$ with $a, b \in \mathbb{Z}$ is

$$\mathcal{B}(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = a$, $j^2 = b$ and $k = ij = -ji$.

Quaternion algebra definitions

The quaternion algebra $\mathcal{B}(a, b)$ over $\mathbb{Q}$ with $a, b \in \mathbb{Z}$ is

$$\mathcal{B}(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = a$, $j^2 = b$ and $k = ij = -ji$.

An **order** $\mathcal{O}$ is a $\mathbb{Z}$-lattice of rank 4 inside $\mathcal{B}(a, b)$ which is also a ring, it is **maximal** when not contained in another order.

Quaternion algebra definitions

The quaternion algebra $\mathcal{B}(a, b)$ over $\mathbb{Q}$ with $a, b \in \mathbb{Z}$ is

$$\mathcal{B}(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = a$, $j^2 = b$ and $k = ij = -ji$.

An **order** $\mathcal{O}$ is a $\mathbb{Z}$-lattice of rank 4 inside $\mathcal{B}(a, b)$ which is also a ring, it is **maximal** when not contained in another order.

Orders are rings: so we have ideals. In a non-commutative algebra, ideals have distinct left and right orders.

The Deuring Correspondence

p : prime characteristic, $\mathcal{B}(-q, -p)$ where $q > 0$ depends only on p.

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E (up to Galois conjugacy)	Maximal Orders in $\mathcal{B}(-q, -p)$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E \to E_1$	Ideal I_φ left $\mathcal{O}$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

The Deuring Correspondence

p : prime characteristic, $\mathcal{B}(-q,-p)$ where $q > 0$ depends only on p.

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E (up to Galois conjugacy)	Maximal Orders in $\mathcal{B}(-q,-p)$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E \to E_1$	Ideal I_φ left $\mathcal{O}$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

Example: $p \equiv 3 \mod 4$, $q = 1$.

The Deuring Correspondence

p : prime characteristic, $\mathcal{B}(-q, -p)$ where $q > 0$ depends only on p.

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E (up to Galois conjugacy)	Maximal Orders in $\mathcal{B}(-q, -p)$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E \to E_1$	Ideal I_φ left $\mathcal{O}$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

Example: $p \equiv 3 \mod 4$, $q = 1$.

$$E_0 : y^2 = x^3 + x$$

The Deuring Correspondence

p : prime characteristic, $\mathcal{B}(-q,-p)$ where $q > 0$ depends only on p.

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E (up to Galois conjugacy)	Maximal Orders in $\mathcal{B}(-q,-p)$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E \to E_1$	Ideal I_φ left $\mathcal{O}$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

Example: $p \equiv 3 \mod 4$, $q = 1$.

$$E_0 : y^2 = x^3 + x$$

$$\mathrm{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota\pi}{2} \rangle \cong \langle 1, i, \frac{i + j}{2}, \frac{1 + k}{2} \rangle$$

$\pi : (x, y) \mapsto (x^p, y^p)$ is the Frobenius morphism with $\pi \circ \pi = [-p]$.

$\iota : (x, y) \mapsto (-x, \sqrt{-1}y)$ is a twisting automorphism with $\iota \circ \iota = [-1]$.

Making the Deuring correspondence effective

Original motivation: cryptanalysis.

We end up with a bunch of nice algorithmic tools:

- Convert a maximal order in a supersingular curve.
- Translate an ideal into an isogeny.
- Find isogenies between curves of known endomorphism rings.

These algorithms are used in GPS and SQISign, and our goal is to explore the new possibilities they offer.

Isogeny representations.

Definition

Let us take $\varphi : E_1 \to E_2$ of degree D. By definition, we have:

$$\varphi : (x, y) \mapsto \left(\frac{f_1(x, y)}{f_2(x, y)}, \frac{g_1(x, y)}{g_2(x, y)} \right)$$

Isogeny representation: a string s_φ for which there exists algorithms

- $\texttt{Verify}(s_\varphi, E_1, E_2, D) \to b \in \{0, 1\}$ to tell if s_φ is valid.
- $\texttt{Evaluate}(s_\varphi, P)$ to compute $\varphi(P)$.

The standard and kernel representation

Standard rep: rational maps f_1, f_2, g_1, g_2 (ok when degree is small but that's all).

Kernel rep: from a generator of the kernel. Uses the Vélu Formulas!

1. Compact and efficient, when the degree is "nice" = smooth and torsion pts defined over small extension. Most often used in isogeny crypto.
2. Complexity polynomial in D: not adapted for isogenies of arbitrary degrees.

The ideal representation

Ideal rep: the ideal I_φ associated to φ.

Algorithmic study of Deuring correspondence $\Rightarrow$ the ideal rep is both compact and efficient for any degree D and prime p.

Complexity and sizes are polynomial in $\log(p)$ and $\log(D)$!

The ideal representation

Ideal rep: the ideal I_φ associated to φ.

Algorithmic study of Deuring correspondence $\Rightarrow$ the ideal rep is both compact and efficient for any degree D and prime p.

Complexity and sizes are polynomial in $\log(p)$ and $\log(D)$!

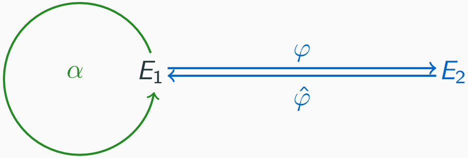
It is almost too good! It reveals every information about φ, E_1, E_2! The ideal representation cannot be anything else than a secret in cryptography.

Can we have a representation "in the middle"?

The suborder representation

Lollipop endomorphisms for proving isogeny existence.

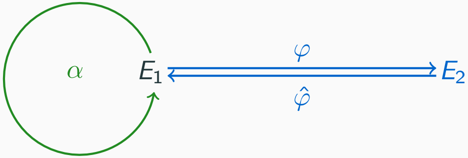
Lollipop endomorphisms for $\varphi : E_1 \to E_2$ of degree D:



The order of lollipop endomorphisms is $\mathbb{Z} + D\mathrm{End}(E_1) \hookrightarrow \mathrm{End}(E_2)$.

Lollipop endomorphisms for proving isogeny existence.

Lollipop endomorphisms for $\varphi : E_1 \to E_2$ of degree D:



The order of lollipop endomorphisms is $\mathbb{Z} + D\mathrm{End}(E_1) \hookrightarrow \mathrm{End}(E_2)$.

Conversely: the existence of $\mathbb{Z} + D\mathrm{End}(E_1) \hookrightarrow \mathrm{End}(E_2)$ proves the existence of $\varphi : E_1 \to E_2$ of degree D!

The suborder representation

Let us take $\varphi : E_1 \to E_2$ of degree D. The suborder representation π_φ of φ is made of:

1. D, E_1, E_2
2. $\mathrm{End}(E_1)$ (≈ 16 coefficients in $\mathbb{Z}$ for a basis).
3. s_1, s_2, s_3 where s_i is the kernel representation of an endomorphism $\theta_i : E_2 \to E_2$. Such that $\mathbb{Z} + D\mathrm{End}(E_1) \hookrightarrow \mathrm{End}(E_2)$ is generated by $\{[1], \theta_1, \theta_2, \theta_3\}$.

We can derive polynomial time algorithms `Verify`,`Evaluate` for this representation for any isogeny φ from several new algorithm tools.

Cryptography

A new hard problem?

Going back to our motivation: need a rep not equivalent to the ideal rep.

(ISOP) : Ideal rep $\Rightarrow$ Suborder Rep : Easy!

(SOIP) Suborder rep $\Rightarrow$ Ideal rep: SOIP??

A new hard problem?

Going back to our motivation: need a rep not equivalent to the ideal rep.

(ISOP) : Ideal rep $\Rightarrow$ Suborder Rep : Easy!

(SOIP) Suborder rep $\Rightarrow$ Ideal rep: SOIP??

(SOERP) Suborder rep. $\Rightarrow$ Endo ring of the codomain.

(T-SIP) Torsion information $\Rightarrow$ Ideal rep.

A new hard problem?

Going back to our motivation: need a rep not equivalent to the ideal rep.

(ISOP) : Ideal rep $\Rightarrow$ Suborder Rep : Easy!

(SOIP) Suborder rep $\Rightarrow$ Ideal rep: SOIP??

(SOERP) Suborder rep. $\Rightarrow$ Endo ring of the codomain.

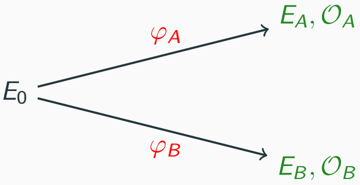
(T-SIP) Torsion information $\Rightarrow$ Ideal rep.

Thm: SOIP $\Leftrightarrow$ SOERP $\Leftrightarrow$ T-SIP.

Best attack: quantum subexponential in D: because we reveal some endomorphisms, but they are chosen as not to give the full endomorphism rings!

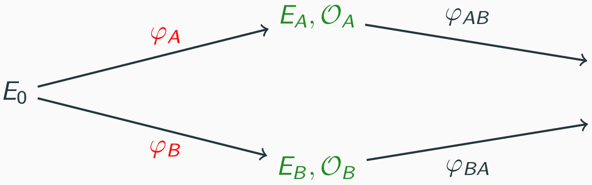
pSIDH: a new key exchange?

pSIDH: A new SIDH-like key exchange with public keys as suborders and secrets keys as ideals for big prime degree, $\mathrm{GCD}(\deg \varphi_A, \deg \varphi_B) = 1$.



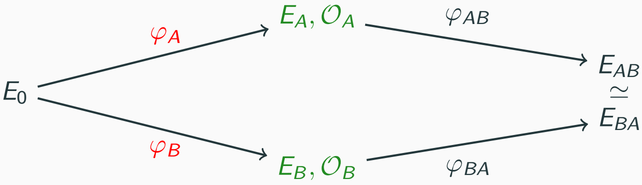
pSIDH: a new key exchange?

pSIDH: A new SIDH-like key exchange with public keys as suborders and secrets keys as ideals for big prime degree, GCD($\deg \varphi_A, \deg \varphi_B$) = 1.



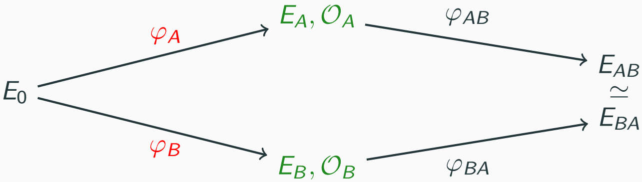
pSIDH: a new key exchange?

pSIDH: A new SIDH-like key exchange with public keys as suborders and secrets keys as ideals for big prime degree, GCD($\deg \varphi_A, \deg \varphi_B$) $= 1$.



pSIDH: a new key exchange?

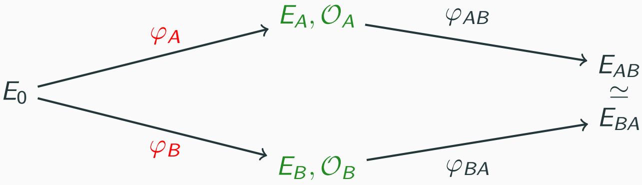
pSIDH: A new SIDH-like key exchange with public keys as suborders and secrets keys as ideals for big prime degree, GCD($\deg \varphi_A, \deg \varphi_B$) = 1.



Performance profile similar to CSIDH: quantum subexp attack and verifiable public keys.

pSIDH: a new key exchange?

pSIDH: A new SIDH-like key exchange with public keys as suborders and secrets keys as ideals for big prime degree, GCD($\deg \varphi_A, \deg \varphi_B) = 1$.



Performance profile similar to CSIDH: quantum subexp attack and verifiable public keys.

In practice not as good... But the structure and the hard problem are different!

Future work and open problems

Isogeny-based cryptography is not dead! It is an exciting time to work on isogenies and the Deuring correspondence. We have introduced some new ideas to build cryptography, time will tell where it will lead us.

Future work and open problems

Isogeny-based cryptography is not dead! It is an exciting time to work on isogenies and the Deuring correspondence. We have introduced some new ideas to build cryptography, time will tell where it will lead us.

The new attacks are a concern for pSIDH, the hardness of isogeny problem with torsion information in high degree needs more study!

The new attacks are also a new opportunity: can be used for isogeny representations [Robert 2022].

Future work and open problems

Isogeny-based cryptography is not dead! It is an exciting time to work on isogenies and the Deuring correspondence. We have introduced some new ideas to build cryptography, time will tell where it will lead us.

The new attacks are a concern for pSIDH, the hardness of isogeny problem with torsion information in high degree needs more study!

The new attacks are also a new opportunity: can be used for isogeny representations [Robert 2022].

`https://eprint.iacr.org/2021/1600`

Questions?