Hidden Stabilizers, the Isogeny To Endomorphism Ring Problem and the Cryptanalysis of pSIDH

Asiacrypt 2023, Guangzhou

Mingjie Chen, Muhammad Imran, Gábor Ivanyos, Péter Kutas, Antonin Leroux, Christophe Petit

University of Birmingham

December 6, 2023

Outline

Introducing the IsERP

Theoretical background

Roadmap

Reductions and the resolution of the IsERP

Hard problems in isogeny-based cryptography

Let E, E' denote supersingular elliptic curves over $\mathbb{F}_{p^2}$.

Hard problems in isogeny-based cryptography

Let E, E' denote supersingular elliptic curves over $\mathbb{F}_{p^2}$.

A. Endomorphism ring problem:

Hard problems in isogeny-based cryptography

Let E, E' denote supersingular elliptic curves over $\mathbb{F}_{p^2}$.

A. Endomorphism ring problem:

$$\text{Given } E\text{, compute } \mathrm{End}(E).$$

Hard problems in isogeny-based cryptography

Let E, E' denote supersingular elliptic curves over $\mathbb{F}_{p^2}$.

A. Endomorphism ring problem:

$$\text{Given } E\text{, compute } \mathrm{End}(E).$$

B. Path-finding problem:

Hard problems in isogeny-based cryptography

Let E, E' denote supersingular elliptic curves over $\mathbb{F}_{p^2}$.

A. Endomorphism ring problem:

$$\text{Given } E, \text{ compute } \mathrm{End}(E).$$

B. Path-finding problem:

Given a small prime ℓ and E, E', find a path from E to E' on the supersingular ℓ-isogeny graph.

Hard problems in isogeny-based cryptography

Let E, E' denote supersingular elliptic curves over $\mathbb{F}_{p^2}$.

A. Endomorphism ring problem:

Given E, compute $\mathrm{End}(E)$.

B. Path-finding problem:

Given a small prime ℓ and E, E', find a path from E to E' on the supersingular ℓ-isogeny graph.

Problems A, B are equivalent.

Hard problems in isogeny-based cryptography

Let E, E' denote supersingular elliptic curves over $\mathbb{F}_{p^2}$.

A. Endomorphism ring problem:

Given E, compute $\mathrm{End}(E)$.

B. Path-finding problem:

Given a small prime ℓ and E, E', find a path from E to E' on the supersingular ℓ-isogeny graph.

Problems A, B are equivalent.

Question: what if we consider a more general version of Problem B where we know (*the isogeny representation of*) an isogeny between E and E'?

Isogeny representation

An **isogeny representation** is a way to effectively represent the isogeny so that there is an efficient algorithm for evaluating the isogeny on given points.

Isogeny representation

An **isogeny representation** is a way to effectively represent the isogeny so that there is an efficient algorithm for evaluating the isogeny on given points.

Examples:

- Rational maps — can only be used for **small** degree isogenies.

Isogeny representation

An **isogeny representation** is a way to effectively represent the isogeny so that there is an efficient algorithm for evaluating the isogeny on given points.

Examples:

- Rational maps — can only be used for **small** degree isogenies.
- Isogeny chain

$$\phi = \phi_n \circ \phi_{n-1} \circ \cdots \circ \phi_2 \circ \phi_1$$

— can only be used for **smooth** degree isogenies.

Isogeny representation

An **isogeny representation** is a way to effectively represent the isogeny so that there is an efficient algorithm for evaluating the isogeny on given points.

Examples:

- Rational maps — can only be used for **small** degree isogenies.
- Isogeny chain

$$\phi = \phi_n \circ \phi_{n-1} \circ \cdots \circ \phi_2 \circ \phi_1$$

  — can only be used for **smooth** degree isogenies.
- Suborder representation — introduced in pSIDH key exchange [Leroux 2022], can be used to represent isogenies of **large prime degrees**.

Isogeny representation

An **isogeny representation** is a way to effectively represent the isogeny so that there is an efficient algorithm for evaluating the isogeny on given points.

Examples:

- Rational maps — can only be used for **small** degree isogenies.
- Isogeny chain

$$\phi = \phi_n \circ \phi_{n-1} \circ \cdots \circ \phi_2 \circ \phi_1$$

  — can only be used for **smooth** degree isogenies.
- Suborder representation — introduced in pSIDH key exchange [Leroux 2022], can be used to represent isogenies of **large prime degrees**.
- High dimension representation — introduced after the SIDH attacks [Robert 2022], can be used for **arbitrary degree** isogeny.

The IsERP

Problem (IsERP)

Let E_0, E be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and $\varphi : E_0 \to E$ be an isogeny of degree N. Given the endomorphism ring $\mathrm{End}(E_0)$ and an isogeny representation of φ, compute $\mathrm{End}(E)$.

The IsERP

Problem (IsERP)

Let E_0, E be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and $\varphi : E_0 \to E$ be an isogeny of degree N. Given the endomorphism ring $\mathrm{End}(E_0)$ and an isogeny representation of φ, compute $\mathrm{End}(E)$.

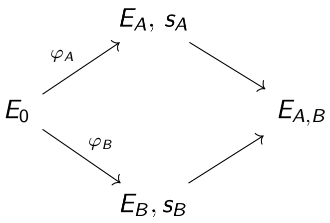
In the context of pSIDH key exchange:

The IsERP

Problem (IsERP)

Let E_0, E be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and $\varphi : E_0 \to E$ be an isogeny of degree N. Given the endomorphism ring $\mathrm{End}(E_0)$ and an isogeny representation of φ, compute $\mathrm{End}(E)$.

In the context of pSIDH key exchange:

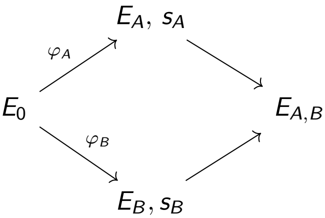


The IsERP

Problem (IsERP)

Let E_0, E be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and $\varphi : E_0 \to E$ be an isogeny of degree N. Given the endomorphism ring $\mathrm{End}(E_0)$ and an isogeny representation of φ, compute $\mathrm{End}(E)$.

In the context of pSIDH key exchange:



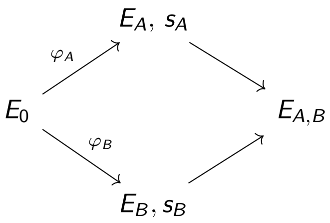
- E_0 is the public curve whose endomorphism ring is known

The IsERP

Problem (IsERP)

Let E_0, E be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and $\varphi : E_0 \to E$ be an isogeny of degree N. Given the endomorphism ring $\mathrm{End}(E_0)$ and an isogeny representation of φ, compute $\mathrm{End}(E)$.

<u>In the context of pSIDH key exchange:</u>



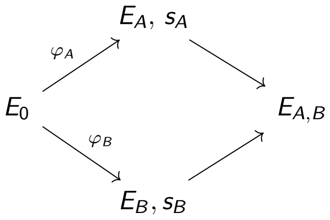
- E_0 is the public curve whose endomorphism ring is known
- $\varphi : E_0 \to E$ is the secret isogeny of large prime degree N that Alice (or Bob) computes

The IsERP

Problem (IsERP)

Let E_0, E be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and $\varphi : E_0 \to E$ be an isogeny of degree N. Given the endomorphism ring $\mathrm{End}(E_0)$ and an isogeny representation of φ, compute $\mathrm{End}(E)$.

In the context of pSIDH key exchange:



- E_0 is the public curve whose endomorphism ring is known
- $\varphi : E_0 \to E$ is the secret isogeny of large prime degree N that Alice (or Bob) computes
- s is the suborder representation of φ which is the embedding of $\mathbb{Z} + N\,\mathrm{End}(E_0)$ into $\mathrm{End}(E)$ induced by φ that allows Bob (or Alice) to compute $E_{A,B}$.

Deuring Correspondence

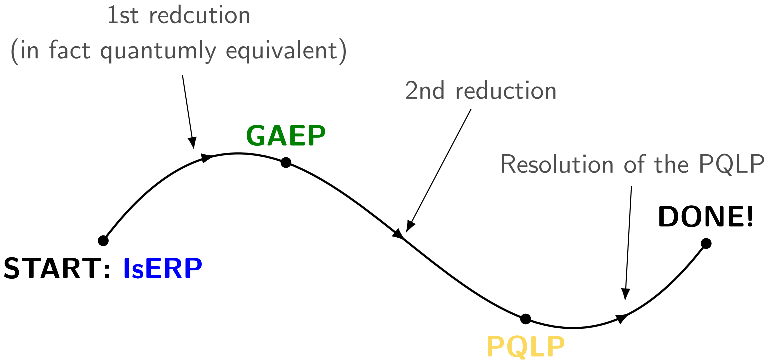
Supersingular elliptic curve **VS** Quaternion algebra

Deuring Correspondence

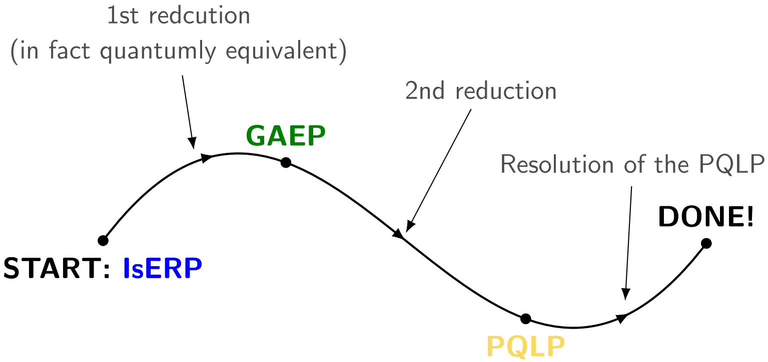
Supersingular elliptic curve **VS** Quaternion algebra

Supersingular j-invariants over $\mathbb{F}_{p^2}$ $j(E)$ (up to Galois conjugacy)	Maximal orders in $\mathcal{B}_{p,\infty}$ $\mathcal{O} \cong \mathrm{End}(E)$ (up to isomorphism)
(E_1, φ) with $\varphi : E_0 \to E_1$	I_φ integral left $\mathcal{O}_0$-ideal and right $\mathcal{O}_1$-ideal
$\theta \in \mathrm{End}(E_0)$	Principal ideal $\mathcal{O}_0\theta$
$\deg(\varphi)$	$n(I_\varphi)$

Roadmap

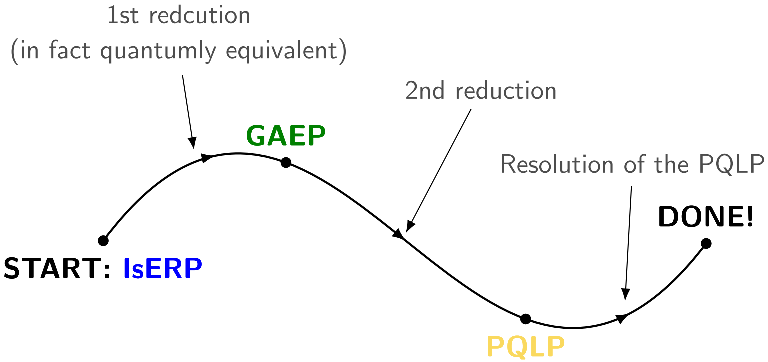

1st redcution
(in fact quantumly equivalent)
2nd reduction
Resolution of the PQLP
GAEP
DONE!
START: IsERP
PQLP

Roadmap



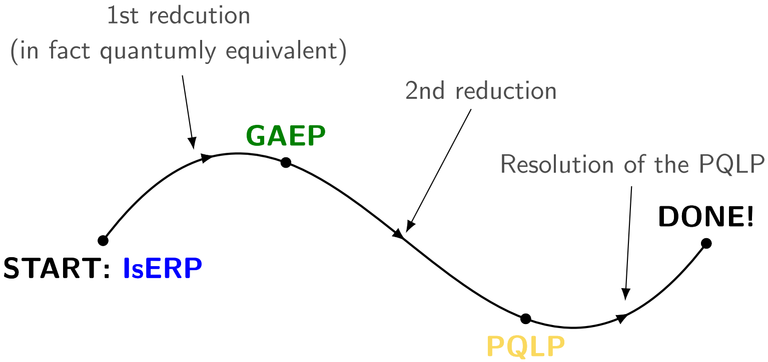
- Isogeny to Endomorphism Ring Problem (**IsERP**)

Roadmap



- Isogeny to Endomorphism Ring Problem (**IsERP**)
- Group Action Evaluation Problem (**GAEP**)

Roadmap



- Isogeny to Endomorphism Ring Problem (**IsERP**)
- Group Action Evaluation Problem (**GAEP**)
- Powersmooth Quaternion Lifting Problem (**PQLP**)

1st reduction

— the group action evaluation problem (GAEP)

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \curvearrowright \{\text{cyclic order } N \text{ subgroups of } \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}\}$$

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \star \langle (m, n) \rangle = \langle (am + bn, cm + dn) \rangle$$

$$\curvearrowright \{\text{cyclic subgroups of order } N \text{ of } E_0[N]\}$$

$$\curvearrowright \{\text{cyclic isogenies } \varphi : E_0 \to \cdot \text{ of degree } N\}$$

1st reduction

— the group action evaluation problem (GAEP)

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \curvearrowright \{\text{cyclic order } N \text{ subgroups of } \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}\}$$

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \star \langle (m,n) \rangle = \langle (am+bn, cm+dn) \rangle$$

$$\curvearrowright \{\text{cyclic subgroups of order } N \text{ of } E_0[N]\}$$

$$\curvearrowright \{\text{cyclic isogenies } \varphi : E_0 \to \cdot \text{ of degree } N\ \}$$

Problem (GAEP)

Let E_0, E be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and let $\varphi : E_0 \to E$ be an isogeny of degree N. Given $\mathrm{End}(E_0)$ and its corresponding quaternion order $\mathcal{O}_0$, a representation of φ and $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, find an isogeny representation of $g \star \varphi$.

1st reduction

— the group action evaluation problem (GAEP)

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \curvearrowright \{\text{cyclic order } N \text{ subgroups of } \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}\}$$

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \star \langle (m,n) \rangle = \langle (am+bn, cm+dn) \rangle$$

$$\curvearrowright \{\text{cyclic subgroups of order } N \text{ of } E_0[N]\}$$

$$\curvearrowright \{\text{cyclic isogenies } \varphi : E_0 \to \cdot \text{ of degree } N\ \}$$

Problem (GAEP)

Let E_0, E be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and let $\varphi : E_0 \to E$ be an isogeny of degree N. Given $\mathrm{End}(E_0)$ and its corresponding quaternion order $\mathcal{O}_0$, a representation of φ and $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, find an isogeny representation of $g \star \varphi$.

In the context of pSIDH key exchange:

1st reduction

— the group action evaluation problem (GAEP)

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \curvearrowright \{\text{cyclic order } N \text{ subgroups of } \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}\}$$
$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \star \langle (m,n) \rangle = \langle (am+bn, cm+dn) \rangle$$
$$\curvearrowright \{\text{cyclic subgroups of order } N \text{ of } E_0[N]\}$$
$$\curvearrowright \{\text{cyclic isogenies } \varphi : E_0 \to \cdot \text{ of degree } N\}$$

Problem (GAEP)

Let E_0, E be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and let $\varphi : E_0 \to E$ be an isogeny of degree N. Given $\mathrm{End}(E_0)$ and its corresponding quaternion order $\mathcal{O}_0$, a representation of φ and $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, find an isogeny representation of $g \star \varphi$.

In the context of pSIDH key exchange:

Given the embedding of $\mathbb{Z} + N\,\mathrm{End}(E_0)$ into $\mathrm{End}(E)$, compute the embedding of $\mathbb{Z} + N\,\mathrm{End}(E_0)$ into the endomorphism ring of the codomain curve of $g \star \varphi$.

1st reduction

— introducing the Stabilizer Subgroup

Consider the action

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \curvearrowright \{\text{cyclic isogenies } \varphi : E_0 \to \cdot \text{ of degree } N\}.$$

1st reduction

— introducing the Stabilizer Subgroup

Consider the action

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \curvearrowright \{\text{cyclic isogenies } \varphi : E_0 \to \cdot \text{ of degree } N\}.$$

Define

$$\mathrm{Stab}_\varphi = \{g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \mid g \star \varphi = \varphi\}.$$

1st reduction

— introducing the Stabilizer Subgroup

Consider the action

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \curvearrowright \{\text{cyclic isogenies } \varphi : E_0 \to \cdot \text{ of degree } N\ \}.$$

Define

$$\mathrm{Stab}_\varphi = \{g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \mid g \star \varphi = \varphi\}.$$

Proposition

Let $\varphi : E_0 \to E$ be an isogeny of degree N. The stabilizer subgroup $Stab_\varphi$ is conjugate of the subgroup of upper triangular matrices (i.e., a Borel subgroup).

1st reduction

— another look at the Stabilizer Subgroup

Question: how is Stab_φ related to φ?

1st reduction

— another look at the Stabilizer Subgroup

Question: how is Stab_φ related to φ?

Upon fixing a basis of $E_0[N]$, we have an isomorphism

$$(\mathrm{End}(E_0)/N\,\mathrm{End}(E_0))^\times \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$
$$\theta \mapsto g_\theta$$

1st reduction

— another look at the Stabilizer Subgroup

Question: how is Stab_φ related to φ?

Upon fixing a basis of $E_0[N]$, we have an isomorphism

$$(\mathrm{End}(E_0)/N\,\mathrm{End}(E_0))^\times \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$
$$\theta \mapsto g_\theta$$

Proposition

Let $\varphi : E_0 \to E$ be an isogeny of degree N. Stab_φ is made of the matrices g_θ such that θ is in the Eichler order $\mathbb{Z} + I_\varphi$ where I_φ is the ideal associated to φ under the Deuring correspondence.

1st reduction

— another look at the Stabilizer Subgroup

Question: how is Stab_φ related to φ?

Upon fixing a basis of $E_0[N]$, we have an isomorphism

$$(\mathrm{End}(E_0)/N\,\mathrm{End}(E_0))^\times \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$
$$\theta \mapsto g_\theta$$

Proposition

Let $\varphi : E_0 \to E$ be an isogeny of degree N. Stab_φ is made of the matrices g_θ such that θ is in the Eichler order $\mathbb{Z} + I_\varphi$ where I_φ is the ideal associated to φ under the Deuring correspondence.

Note that here we are abusing notations by viewing $\theta \in \mathcal{O}_0$ under the isomorphism $\mathcal{O}_0 \cong \mathrm{End}(E_0)$.

1st reduction

— reducing IsEPR to GAEP

Theorem

The **IsERP** *reduces to the* **GAEP** *in quantum polynomial time.*

1st reduction

— reducing IsEPR to GAEP

Theorem

The **IsERP** *reduces to the* **GAEP** *in quantum polynomial time.*

Proof Sketch

Knowing how to evaluate the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *on* $\varphi : E_0 \to E$ *of degree* N*, the goal is to compute the endomorphism ring of* E*.*

1st reduction
— reducing IsEPR to GAEP

Theorem

The **IsERP** *reduces to the* **GAEP** *in quantum polynomial time.*

Proof Sketch

Knowing how to evaluate the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *on* $\varphi : E_0 \to E$ *of degree* N*, the goal is to compute the endomorphism ring of* E*.*

- I: *Use a quantum algorithm to compute* $Stab_\varphi$ *in polynomial time.*

1st reduction

— reducing IsEPR to GAEP

Theorem

The **IsERP** *reduces to the* **GAEP** *in quantum polynomial time.*

Proof Sketch

Knowing how to evaluate the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *on* $\varphi : E_0 \to E$ *of degree* N*, the goal is to compute the endomorphism ring of* E.

I: *Use a quantum algorithm to compute* $Stab_\varphi$ *in polynomial time.— Borel HSP in general linear group:*

1st reduction

— reducing IsEPR to GAEP

Theorem

The **IsERP** *reduces to the* **GAEP** *in quantum polynomial time.*

Proof Sketch

Knowing how to evaluate the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *on* $\varphi : E_0 \to E$ *of degree* N*, the goal is to compute the endomorphism ring of* E*.*

- I: *Use a quantum algorithm to compute* $Stab_\varphi$ *in polynomial time.— Borel HSP in general linear group:*
  - $\mathrm{GL}_2(\mathbb{F}_p)$ *[Denney-Moore-Russell 2010]*

1st reduction
— reducing IsEPR to GAEP

Theorem

The **IsERP** *reduces to the* **GAEP** *in quantum polynomial time.*

Proof Sketch

Knowing how to evaluate the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *on* $\varphi : E_0 \to E$ *of degree* N*, the goal is to compute the endomorphism ring of* E*.*

I: *Use a quantum algorithm to compute* $Stab_\varphi$ *in polynomial time.— Borel HSP in general linear group:*

- $\mathrm{GL}_2(\mathbb{F}_p)$ *[Denney-Moore-Russell 2010]*
- $\mathrm{GL}_n(\mathbb{F}_{p^k})$ *[Ivanyos 2012]*

1st reduction
— reducing IsEPR to GAEP

Theorem

*The **IsERP** reduces to the **GAEP** in quantum polynomial time.*

Proof Sketch

Knowing how to evaluate the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *on* $\varphi : E_0 \to E$ *of degree* N*, the goal is to compute the endomorphism ring of* E.

I: *Use a quantum algorithm to compute* $Stab_\varphi$ *in polynomial time.— Borel HSP in general linear group:*

- $\mathrm{GL}_2(\mathbb{F}_p)$ *[Denney-Moore-Russell 2010]*
- $\mathrm{GL}_n(\mathbb{F}_{p^k})$ *[Ivanyos 2012]*
- *we generalize the result to* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *for any* $N > 1$

1st reduction

— reducing IsEPR to GAEP

Theorem

The **IsERP** *reduces to the* **GAEP** *in quantum polynomial time.*

Proof Sketch

Knowing how to evaluate the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *on* $\varphi : E_0 \to E$ *of degree* N*, the goal is to compute the endomorphism ring of* E*.*

I: *Use a quantum algorithm to compute* $Stab_\varphi$ *in polynomial time.— Borel HSP in general linear group:*

- $\mathrm{GL}_2(\mathbb{F}_p)$ *[Denney-Moore-Russell 2010]*
- $\mathrm{GL}_n(\mathbb{F}_{p^k})$ *[Ivanyos 2012]*
- *we generalize the result to* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *for any* $N > 1$

II: *Recover* I_φ *from* $Stab_\varphi = \mathbb{Z} + I_\varphi$*.*

1st reduction

— reducing IsEPR to GAEP

Theorem

The **IsERP** *reduces to the* **GAEP** *in quantum polynomial time.*

Proof Sketch

Knowing how to evaluate the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *on* $\varphi : E_0 \to E$ *of degree* N*, the goal is to compute the endomorphism ring of* E*.*

I: *Use a quantum algorithm to compute* $Stab_\varphi$ *in polynomial time.— Borel HSP in general linear group:*

- $\mathrm{GL}_2(\mathbb{F}_p)$ *[Denney-Moore-Russell 2010]*
- $\mathrm{GL}_n(\mathbb{F}_{p^k})$ *[Ivanyos 2012]*
- *we generalize the result to* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *for any* $N > 1$

II: *Recover* I_φ *from* $Stab_\varphi = \mathbb{Z} + I_\varphi$*.*

III: *Compute the right order of* I_φ*.*

1st reduction

— reducing GAEP to IsERP

Theorem

The **GAEP** *reduces to the* **IsERP** *in classical polynomial-time.*

Proof Sketch

Knowing $\mathrm{End}(E_0), \mathrm{End}(E), N, \varphi$ *and* $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, *we need to compute a representation of* $g \star \varphi$.

1st reduction

— reducing GAEP to IsERP

Theorem

The **GAEP** *reduces to the* **IsERP** *in classical polynomial-time.*

Proof Sketch

Knowing $\mathrm{End}(E_0), \mathrm{End}(E), N, \varphi$ *and* $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, *we need to compute a representation of* $g \star \varphi$.

I: *Compute the ideal* I_φ *corresponding to* φ.

1st reduction

— reducing GAEP to IsERP

Theorem

The **GAEP** *reduces to the* **IsERP** *in classical polynomial-time.*

Proof Sketch

Knowing $\mathrm{End}(E_0), \mathrm{End}(E), N, \varphi$ *and* $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, *we need to compute a representation of* $g \star \varphi$.

I: *Compute the ideal* I_φ *corresponding to* φ.

II: *Find* $\theta \in \mathrm{End}(E)$ *such that* $g_\theta = g$.

1st reduction

— reducing GAEP to IsERP

Theorem

*The **GAEP** reduces to the **IsERP** in classical polynomial-time.*

Proof Sketch

Knowing $\mathrm{End}(E_0), \mathrm{End}(E), N, \varphi$ *and* $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, *we need to compute a representation of* $g \star \varphi$.

- I: *Compute the ideal* I_φ *corresponding to* φ.
- II: *Find* $\theta \in \mathrm{End}(E)$ *such that* $g_\theta = g$.
- III: $I_{g\star\varphi} = \sigma(I_\phi \cap \mathcal{O}\sigma)\sigma^{-1} + N\mathcal{O}$ *(where we take* $\mathcal{O} \cong \mathrm{End}(E)$ *and* $\sigma \in \mathcal{O}$ *corresponds to* θ*).*

2nd reduction

— the powersmooth quaternion lifting problem (PQLP)

Problem (PQLP)

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer N and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ of powersmooth norm with some λ coprime to N.

2nd reduction

— the powersmooth quaternion lifting problem (PQLP)

Problem (PQLP)

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer N and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ of powersmooth norm with some λ coprime to N.

Fix a curve E_0 and let $\mathcal{O}_0 \cong \mathrm{End}(E_0)$:

2nd reduction

— the powersmooth quaternion lifting problem (PQLP)

Problem (PQLP)

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer N and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ of powersmooth norm with some λ coprime to N.

Fix a curve E_0 and let $\mathcal{O}_0 \cong \mathrm{End}(E_0)$:

$$\sigma \in (\mathcal{O}_0/N\mathcal{O}_0)^\times \longleftrightarrow \theta \in (\mathrm{End}(E_0)/N\,\mathrm{End}(E_0))^\times$$

$$(\mathcal{O}_0/N\mathcal{O}_0)^\times \longleftrightarrow g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \longleftrightarrow (\mathrm{End}(E_0)/N\,\mathrm{End}(E_0))^\times$$

2nd reduction

— reducing GAEP to PQLP

Note that $\ker(g \star \varphi) = \theta(\ker \varphi)$.

2nd reduction

— reducing GAEP to PQLP

Note that $\ker(g \star \varphi) = \theta(\ker \varphi)$.
Consider the commutative diagram

$$\begin{array}{ccc} E_0 & \xrightarrow{\theta} & E_0 \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle [\theta]^*\varphi} \\ E & \xrightarrow{[\varphi]^*\theta} & E' \end{array}$$

2nd reduction

— reducing GAEP to PQLP

Note that $\ker(g \star \varphi) = \theta(\ker \varphi)$.
Consider the commutative diagram

$$\begin{array}{ccc} E_0 & \xrightarrow{\theta} & E_0 \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle [\theta]^*\varphi} \\ E & \xrightarrow{[\varphi]^*\theta} & E' \end{array}$$

where $\ker([\theta]^*\varphi) = \theta(\ker \varphi)$ and $\ker([\varphi]^*\theta) = \varphi(\ker \theta)$.

2nd reduction

— reducing GAEP to PQLP

Note that $\ker(g \star \varphi) = \theta(\ker \varphi)$.
Consider the commutative diagram

$$
\begin{array}{ccc}
E_0 & \xrightarrow{\theta} & E_0 \\
\downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle [\theta]^*\varphi} \\
E & \xrightarrow{[\varphi]^*\theta} & E'
\end{array}
$$

where $\ker([\theta]^*\varphi) = \theta(\ker \varphi)$ and $\ker([\varphi]^*\theta) = \varphi(\ker \theta)$.

To compute the curve E' and evaluate $g \star \varphi$, it suffices to know the isogeny $[\varphi]^*\theta$. And this is possible when $\deg(\theta)$ is powersmooth.

2nd reduction

— reducing GAEP to PQLP

Note that $\ker(g \star \varphi) = \theta(\ker \varphi)$.
Consider the commutative diagram

$$\begin{array}{ccc} E_0 & \xrightarrow{\theta} & E_0 \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle [\theta]^*\varphi} \\ E & \xrightarrow{[\varphi]^*\theta} & E' \end{array}$$

where $\ker([\theta]^*\varphi) = \theta(\ker \varphi)$ and $\ker([\varphi]^*\theta) = \varphi(\ker \theta)$.

To compute the curve E' and evaluate $g \star \varphi$, it suffices to know the isogeny $[\varphi]^*\theta$. And this is possible when $\deg(\theta)$ is powersmooth.

Theorem

The **GAEP** *reduces to the* **PQLP** *in classical polynomial time.*

Resolution of the PQLP

Problem (PQLP)

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer N and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ of powersmooth norm with some λ coprime to N.

Resolution of the PQLP

Problem (PQLP)

Let $\mathcal{O}$ *be a maximal order in* $\mathcal{B}_{p,\infty}$*. Given an integer* N *and an element* $\sigma_0 \in \mathcal{O}$ *such that* $(n(\sigma_0), N) = 1$*, find* $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ *of powersmooth norm with some* λ *coprime to* N*.*

Observation: it suffices to solve this problem for one maximal order $\mathcal{O}$ for each given prime p.

Resolution of the PQLP

Problem (PQLP)

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer N and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ of powersmooth norm with some λ coprime to N.

Observation: it suffices to solve this problem for one maximal order $\mathcal{O}$ for each given prime p.

- When $p \equiv 3 \bmod 4$, we take $\mathcal{O} = \mathbb{Z}\langle i, \frac{j+1}{2}\rangle$ where $i^2 = -1, j^2 = -p$ as an example. Let $R = \mathbb{Z}[i]$, WLOG, we can work with the suborder $R + Rj \subseteq \mathcal{O}$.

Resolution of the PQLP

Problem (PQLP)

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer N and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ of powersmooth norm with some λ coprime to N.

Observation: it suffices to solve this problem for one maximal order $\mathcal{O}$ for each given prime p.

- When $p \equiv 3 \bmod 4$, we take $\mathcal{O} = \mathbb{Z}\langle i, \frac{j+1}{2}\rangle$ where $i^2 = -1, j^2 = -p$ as an example. Let $R = \mathbb{Z}[i]$, WLOG, we can work with the suborder $R + Rj \subseteq \mathcal{O}$.
- Elements in Rj have powersmooth lifts as desired by a result in [Kohel-Lauter-Petit-Tignol 2014].

Resolution of the PQLP

Problem (PQLP)

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer N and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ of powersmooth norm with some λ coprime to N.

Observation: it suffices to solve this problem for one maximal order $\mathcal{O}$ for each given prime p.

- When $p \equiv 3 \bmod 4$, we take $\mathcal{O} = \mathbb{Z}\langle i, \frac{j+1}{2}\rangle$ where $i^2 = -1, j^2 = -p$ as an example. Let $R = \mathbb{Z}[i]$, WLOG, we can work with the suborder $R + Rj \subseteq \mathcal{O}$.
- Elements in Rj have powersmooth lifts as desired by a result in [Kohel-Lauter-Petit-Tignol 2014].
- How to lift a general element $\sigma_0 \in R + Rj$?

Resolution of the PQLP

Problem (PQLP)

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer N and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ of powersmooth norm with some λ coprime to N.

Observation: it suffices to solve this problem for one maximal order $\mathcal{O}$ for each given prime p.

- When $p \equiv 3 \bmod 4$, we take $\mathcal{O} = \mathbb{Z}\langle i, \frac{j+1}{2}\rangle$ where $i^2 = -1, j^2 = -p$ as an example. Let $R = \mathbb{Z}[i]$, WLOG, we can work with the suborder $R + Rj \subseteq \mathcal{O}$.
- Elements in Rj have powersmooth lifts as desired by a result in [Kohel-Lauter-Petit-Tignol 2014].
- How to lift a general element $\sigma_0 \in R + Rj$?
  - Find $\gamma \in R + Rj$ such that $n(\gamma)$ is powersmooth.

Resolution of the PQLP

Problem (PQLP)

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer N and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ of powersmooth norm with some λ coprime to N.

Observation: it suffices to solve this problem for one maximal order $\mathcal{O}$ for each given prime p.

- When $p \equiv 3 \bmod 4$, we take $\mathcal{O} = \mathbb{Z}\langle i, \frac{j+1}{2}\rangle$ where $i^2 = -1, j^2 = -p$ as an example. Let $R = \mathbb{Z}[i]$, WLOG, we can work with the suborder $R + Rj \subseteq \mathcal{O}$.
- Elements in Rj have powersmooth lifts as desired by a result in [Kohel-Lauter-Petit-Tignol 2014].
- How to lift a general element $\sigma_0 \in R + Rj$?
    - Find $\gamma \in R + Rj$ such that $n(\gamma)$ is powersmooth.
    - Find $\alpha_1, \alpha_2, \alpha_3 \in Rj$ such that $\sigma_0 = \alpha_1\gamma\alpha_2\gamma\alpha_3 \bmod N\mathcal{O}$.

Conclusion:

1. We resolve the PQLP and thus quantumly resolve the IsERP through the reductions established earlier.

Conclusion:

1. We resolve the PQLP and thus quantumly resolve the IsERP through the reductions established earlier.
2. We need that N to be an odd integer with at most $O(\log\log p)$ many factors.

Conclusion:

1. We resolve the PQLP and thus quantumly resolve the IsERP through the reductions established earlier.
2. We need that N to be an odd integer with at most $O(\log\log p)$ many factors.
3. As an application, we break pSIDH key exchange quantumly.

Conclusion:

1. We resolve the PQLP and thus quantumly resolve the IsERP through the reductions established earlier.
2. We need that N to be an odd integer with at most $O(\log\log p)$ many factors.
3. As an application, we break pSIDH key exchange quantumly.

Thank you!