Post-Quantum Public-Key Cryptography with Isogenies

James Clements

(PhD student 2020 – 2025)

Crypto & PL & Algorithms Away Day 2024

- All practical cryptographic constructions rely on hardness assumptions.

- All practical cryptographic constructions rely on hardness assumptions.
- Public-key cryptography (PKC) - each party has distinct public keys and secret keys.

- All practical cryptographic constructions rely on hardness assumptions.
- Public-key cryptography (PKC) - each party has distinct public keys and secret keys.
- PKC uses functions which are easy to evaluate with the public key (e.g. encrypt), but hard to invert (e.g. decrypt), unless you have the secret key.

- All practical cryptographic constructions rely on hardness assumptions.
- Public-key cryptography (PKC) - each party has distinct public keys and secret keys.
- PKC uses functions which are easy to evaluate with the public key (e.g. encrypt), but hard to invert (e.g. decrypt), unless you have the secret key.
- Current PKC schemes - hardness comes from Integer Factorization or Discrete Logarithm Problems.

Integer Factorization

Given an integer N which is the product of two primes $N = p \times q$, find p and q.

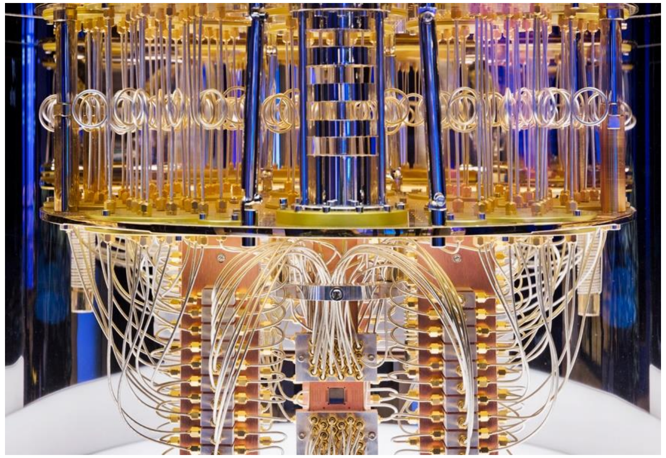
Discrete Logarithm Problem

Given a number N which is a number g to a power a, ($N = g^a$), find a.

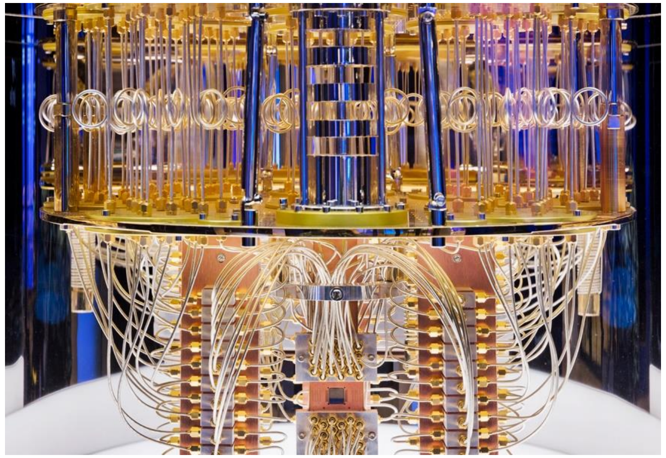
- It turns out these problems are not hard (Shor, 1994).

- It turns out these problems are not hard (Shor, 1994).
- Meaning all cryptography using them is broken.

- It turns out these problems are not hard (Shor, 1994).
- Meaning all cryptography using them is broken.
- Luckily, they can only be broken with use of a large-scale universal quantum computer.

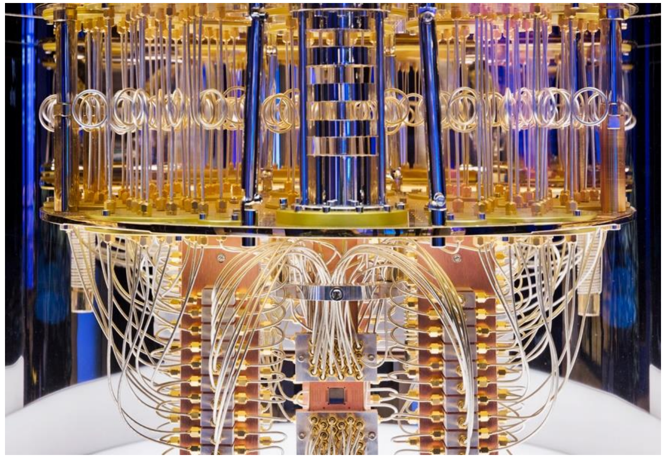


- It turns out these problems are not hard (Shor, 1994).
- Meaning all cryptography using them is broken.



- Luckily, they can only be broken with use of a large-scale universal quantum computer.
- Such devices do not exist yet, but are 10-30 years away.

- It turns out these problems are not hard (Shor, 1994).
- Meaning all cryptography using them is broken.
- Luckily, they can only be broken with use of a large-scale universal quantum computer.



- Such devices do not exist yet, but are 10-30 years away.
- Post-quantum cryptography refers to new public-key schemes which rely on newer quantum resistant hard problems.

- Elliptic curves are certain kinds of algebraic groups.

- Elliptic curves are certain kinds of algebraic groups.
- Structure-preserving maps between elliptic curves are called isogenies.

- Elliptic curves are certain kinds of algebraic groups.
- Structure-preserving maps between elliptic curves are called isogenies.
- Isogeny-based cryptography is a branch of PKC where underlying hard problems relate to isogenies.

- Elliptic curves are certain kinds of algebraic groups.
- Structure-preserving maps between elliptic curves are called isogenies.
- Isogeny-based cryptography is a branch of PKC where underlying hard problems relate to isogenies.
- For example, given two elliptic curves, it can be hard to find an isogeny (of a given degree) between them.

- Elliptic curves are certain kinds of algebraic groups.
- Structure-preserving maps between elliptic curves are called isogenies.
- Isogeny-based cryptography is a branch of PKC where underlying hard problems relate to isogenies.
- For example, given two elliptic curves, it can be hard to find an isogeny (of a given degree) between them.

Pros	Cons
Small keys	Slow
Malleable	Algebraic complexity (less confidence in security)

- Elliptic curves are certain kinds of algebraic groups.
- Structure-preserving maps between elliptic curves are called isogenies.
- Isogeny-based cryptography is a branch of PKC where underlying hard problems relate to isogenies.
- For example, given two elliptic curves, it can be hard to find an isogeny (of a given degree) between them.

Pros	Cons
Small keys	Slow
Malleable	Algebraic complexity (less confidence in security)

Isogeny-based digital signature scheme **SQISign** was entered into the NIST post-quantum “competition” with the potential of being chosen to be standardized.

Aims of my research:

- Study the hardness of the underlying problems to improve confidence in isogenies, via algorithmic reductions.
- Explore new ways of applying mathematical results of quaternion algebras to isogeny-based cryptography.

An introduction to isogeny-based cryptography

Disclaimer: Using simplified, very imprecise, definitions.

Elliptic Curves

Elliptic Curves

Fix large prime p.

$\mathbb{F}_{p^2}$ - **Finite field** containing p^2 elements.

Elliptic Curves

Fix large prime p.

$\mathbb{F}_{p^2}$ - **Finite field** containing p^2 elements.

Elliptic curves over $\mathbb{F}_{p^2}$ are sets of points solving an equation.

$$E_{A,B} = \{(x, y) \in \mathbb{F}_{p^2} : y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

"Point at infinity"

Elliptic Curves

Fix large prime p.

$\mathbb{F}_{p^2}$ - **Finite field** containing p^2 elements.

Elliptic curves over $\mathbb{F}_{p^2}$ are sets of points solving an equation.

$$E_{A,B} = \{(x, y) \in \mathbb{F}_{p^2} : y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

"Point at infinity"

Points form a group.

$$P + Q + R = \infty \iff P, Q, R \text{ lie on line.}$$

Elliptic Curves

Fix large prime p.

$\mathbb{F}_{p^2}$ - **Finite field** containing p^2 elements.

Elliptic curves over $\mathbb{F}_{p^2}$ are sets of points solving an equation.

$$E_{A,B} = \{(x,y) \in \mathbb{F}_{p^2} : y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

"Point at infinity"

Points form a group.

$$P + Q + R = \infty \quad \iff \quad P, Q, R \text{ lie on line.}$$

Elliptic curves are **isomorphic** $E \sim E'$ if there exists a group isomorphism.

Elliptic Curves

Fix large prime p.

$\mathbb{F}_{p^2}$ - **Finite field** containing p^2 elements.

Elliptic curves over $\mathbb{F}_{p^2}$ are sets of points solving an equation.

$$E_{A,B} = \{(x,y) \in \mathbb{F}_{p^2} : y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

"Point at infinity"

Points form a group.

$$P + Q + R = \infty \quad \iff \quad P, Q, R \text{ lie on line.}$$

Elliptic curves are **isomorphic** $E \sim E'$ if there exists a group isomorphism.

The j-**invariant** is an isomorphism invariant. $j(E_{A,B}) = 1728 \cdot \frac{4A^2}{4A^3+27B^2} \in \mathbb{F}_{p^2}$

Elliptic Curves

Fix large prime p.

$\mathbb{F}_{p^2}$ - **Finite field** containing p^2 elements.

Elliptic curves over $\mathbb{F}_{p^2}$ are sets of points solving an equation.

$$E_{A,B} = \{(x,y) \in \mathbb{F}_{p^2} : y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

"Point at infinity"

Points form a group.

$$P + Q + R = \infty \qquad \Longleftrightarrow \qquad P, Q, R \text{ lie on line.}$$

Elliptic curves are **isomorphic** $E \sim E'$ if there exists a group isomorphism.

The j-**invariant** is an isomorphism invariant. $j(E_{A,B}) = 1728 \cdot \frac{4A^2}{4A^3+27B^2} \in \mathbb{F}_{p^2}$

We only care about **supersingular** elliptic curves (which I won't define).

Isogenies

Isogenies

Isogenies are maps between elliptic curves which preserve the group structure and have finite kernel.

$$\varphi : E \to E' \qquad \varphi(P + Q) = \varphi(P) + \varphi(Q)$$

Isogenies

Isogenies are maps between elliptic curves which preserve the group structure and have finite kernel.

$$\varphi : E \to E' \qquad \varphi(P+Q) = \varphi(P) + \varphi(Q)$$

The **degree** of an isogeny is the size of its kernel.

$$\deg(\varphi) = \#\ker(\varphi)$$

Isogenies

Isogenies are maps between elliptic curves which preserve the group structure and have finite kernel.

$$\varphi : E \to E' \qquad \varphi(P+Q) = \varphi(P) + \varphi(Q)$$

The **degree** of an isogeny is the size of its kernel.

$$\deg(\varphi) = \#\ker(\varphi)$$

Isogenies can be **composed/decomposed**, and degrees are multiplicative.

$$\varphi = \varphi_n \circ \ldots \circ \varphi_2 \circ \varphi_1, \qquad \begin{tikzcd} E_1 \arrow[r] \arrow[rrr, bend right] & E_2 \arrow[r] & \cdots \arrow[r] & E_n \end{tikzcd}, \qquad \deg(\varphi) = \prod_i \deg(\varphi_i)$$

Isogenies

Isogenies are maps between elliptic curves which preserve the group structure and have finite kernel.

$$\varphi : E \to E' \qquad \varphi(P+Q) = \varphi(P) + \varphi(Q)$$

The **degree** of an isogeny is the size of its kernel.

$$\deg(\varphi) = \#\ker(\varphi)$$

Isogenies can be **composed/decomposed**, and degrees are multiplicative.

$$\varphi = \varphi_n \circ \ldots \circ \varphi_2 \circ \varphi_1, \qquad \begin{tikzcd} E_1 \arrow[r] \arrow[rrr, bend right] & E_2 \arrow[r] & \cdots \arrow[r] & E_n, \end{tikzcd} \qquad \deg(\varphi) = \prod_i \deg(\varphi_i)$$

Every isogeny has a **dual isogeny** of the same degree.

Isogenies

Isogenies are maps between elliptic curves which preserve the group structure and have finite kernel.

$$\varphi : E \to E' \qquad \varphi(P+Q) = \varphi(P) + \varphi(Q)$$

The **degree** of an isogeny is the size of its kernel.

$$\deg(\varphi) = \#\ker(\varphi)$$

Isogenies can be **composed/decomposed**, and degrees are multiplicative.

$$\varphi = \varphi_n \circ \ldots \circ \varphi_2 \circ \varphi_1, \qquad \begin{tikzcd} E_1 \arrow[r] \arrow[rrr, bend right] & E_2 \arrow[r] & \cdots \arrow[r] & E_n \end{tikzcd}, \qquad \deg(\varphi) = \prod_i \deg(\varphi_i)$$

Every isogeny has a **dual isogeny** of the same degree.

For a prime q, there are always $q+1$ isogenies of degree q.

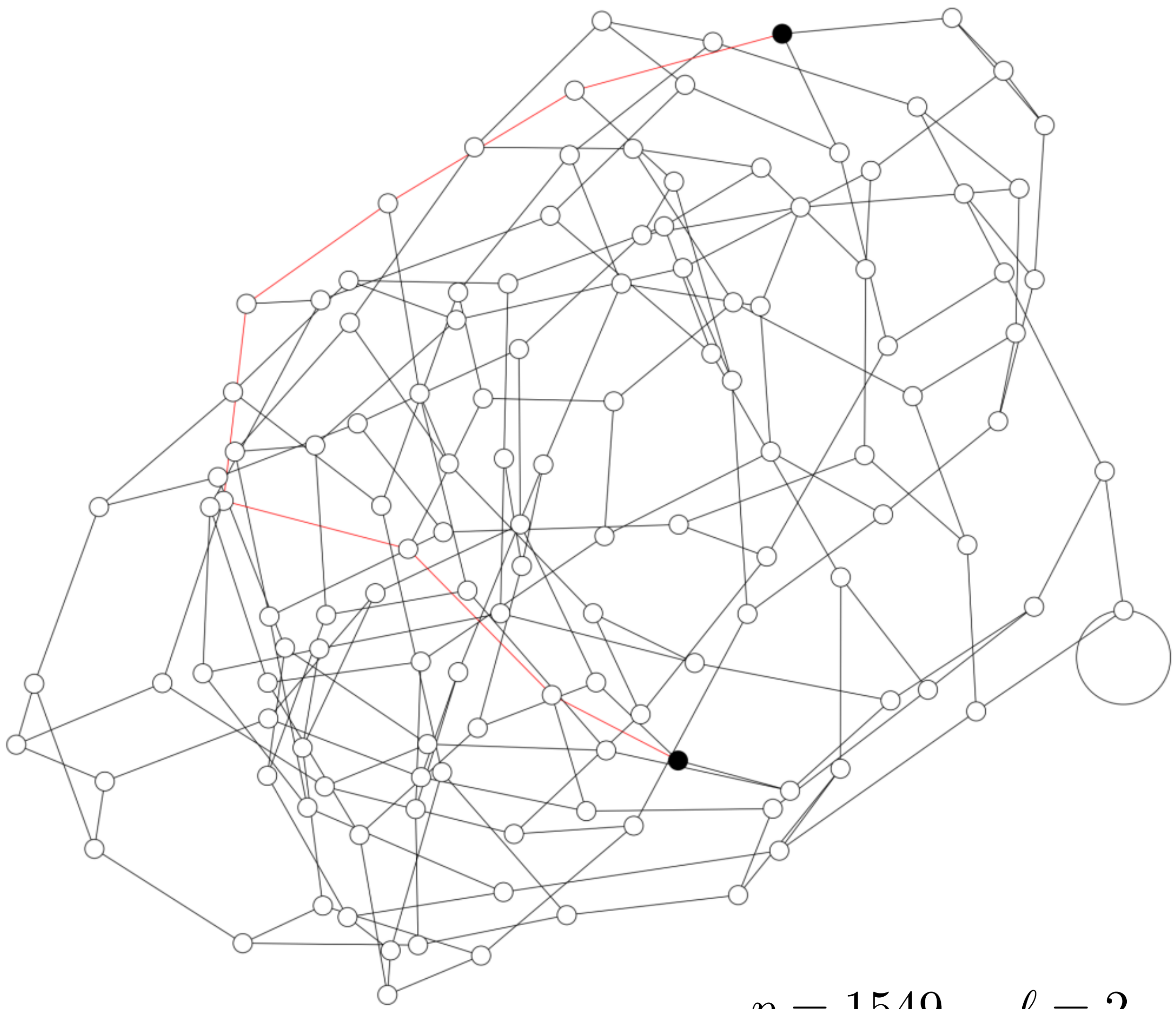
Isogeny Graphs

Isogeny Graphs

An ℓ - **isogeny graph** is a graph where,

Vertices = Supersingular elliptic curves up to isomorphism,

Edges = Isogenies of degree ℓ together with it's dual, up to composition with isomorphisms.



$$p = 1549, \quad \ell = 2$$

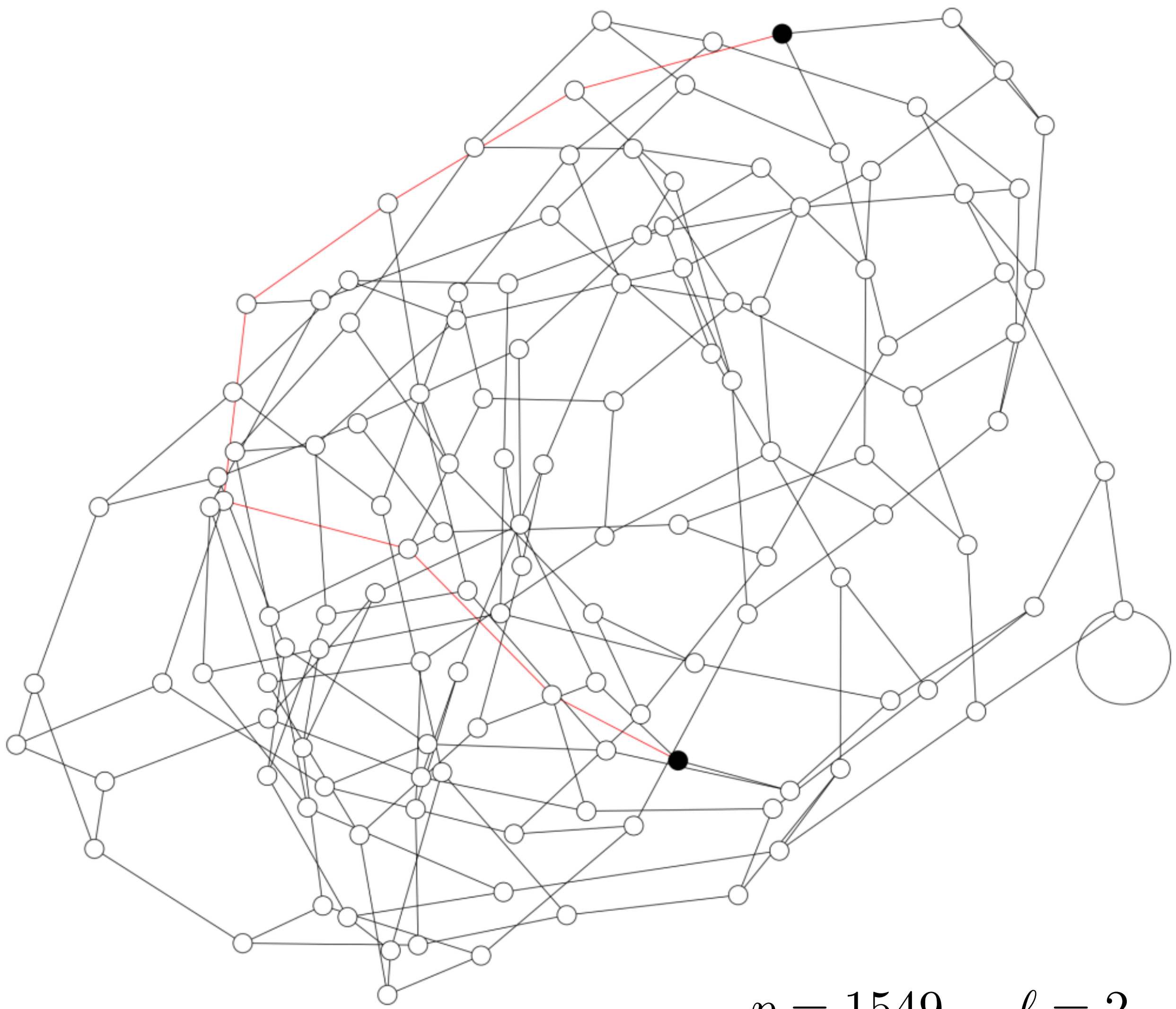
Isogeny Graphs

An ℓ - **isogeny graph** is a graph where,

Vertices = Supersingular elliptic curves up to isomorphism,

Edges = Isogenies of degree ℓ together with it's dual, up to composition with isomorphisms.

All isogeny-based cryptographic schemes walk around in these graphs.



$p = 1549, \quad \ell = 2$

Example – Key Exchange

i.e. Alice and Bob who have never interacted before,
want to talk without anyone listening in.

Example – Key Exchange

i.e. Alice and Bob who have never interacted before, want to talk without anyone listening in.

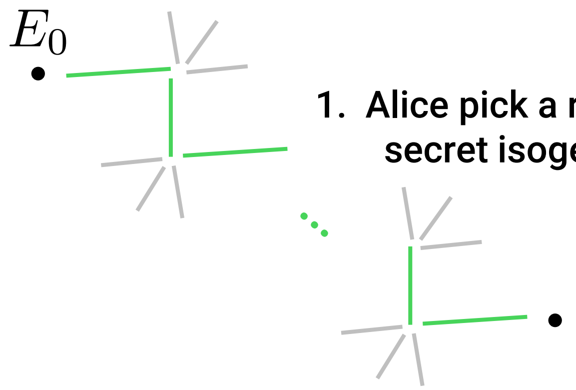
Public starting curve

E_0

Example – Key Exchange

i.e. Alice and Bob who have never interacted before, want to talk without anyone listening in.

Public starting curve

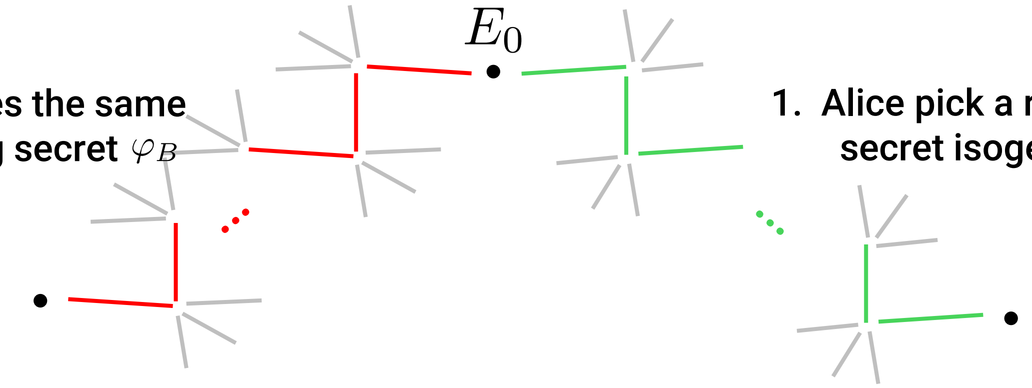


1. Alice pick a random secret isogeny φ_A

Example – Key Exchange

i.e. Alice and Bob who have never interacted before, want to talk without anyone listening in.

Public starting curve

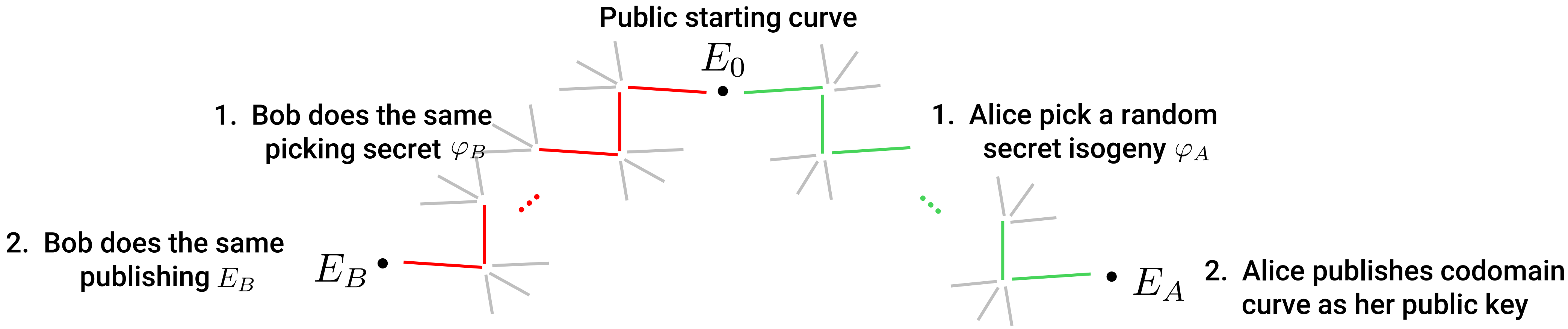


1. Bob does the same picking secret φ_B

1. Alice pick a random secret isogeny φ_A

Example – Key Exchange

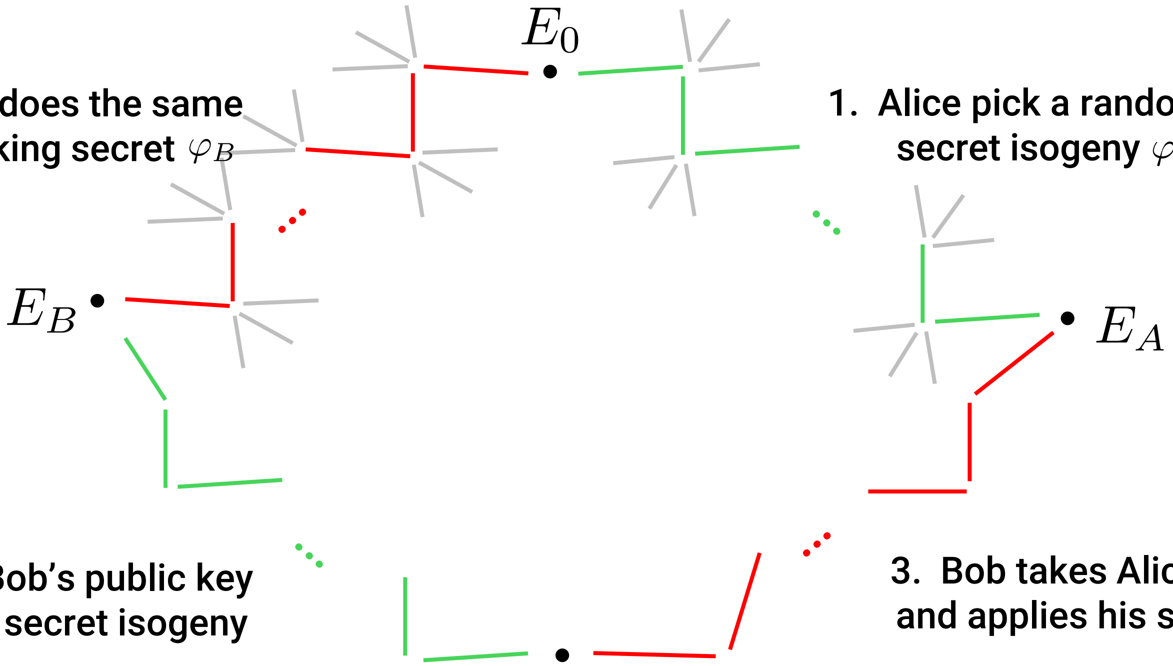
i.e. Alice and Bob who have never interacted before, want to talk without anyone listening in.



Example – Key Exchange

i.e. Alice and Bob who have never interacted before, want to talk without anyone listening in.

Public starting curve

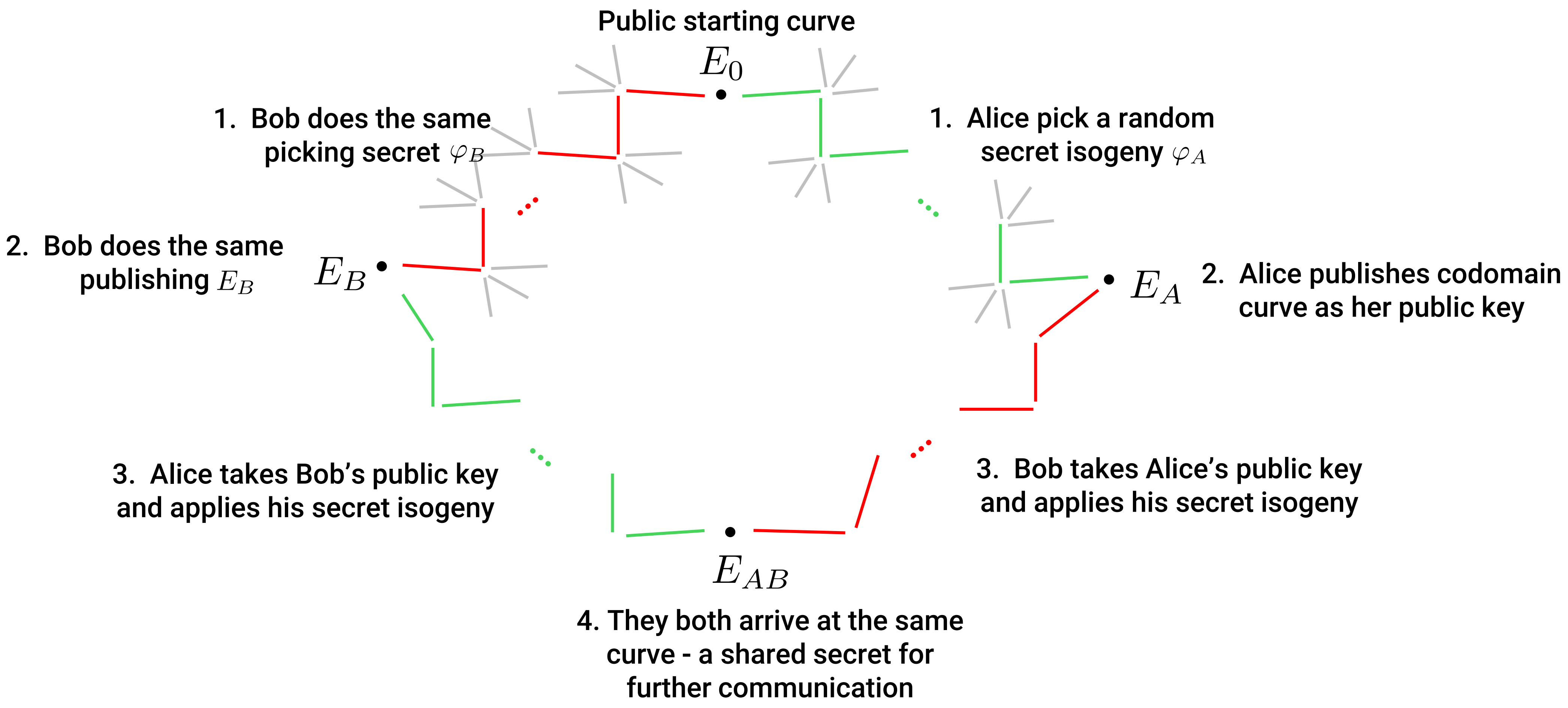


1. Bob does the same picking secret φ_B
2. Bob does the same publishing E_B
3. Alice takes Bob's public key and applies his secret isogeny

1. Alice pick a random secret isogeny φ_A
2. Alice publishes codomain curve as her public key
3. Bob takes Alice's public key and applies his secret isogeny

Example – Key Exchange

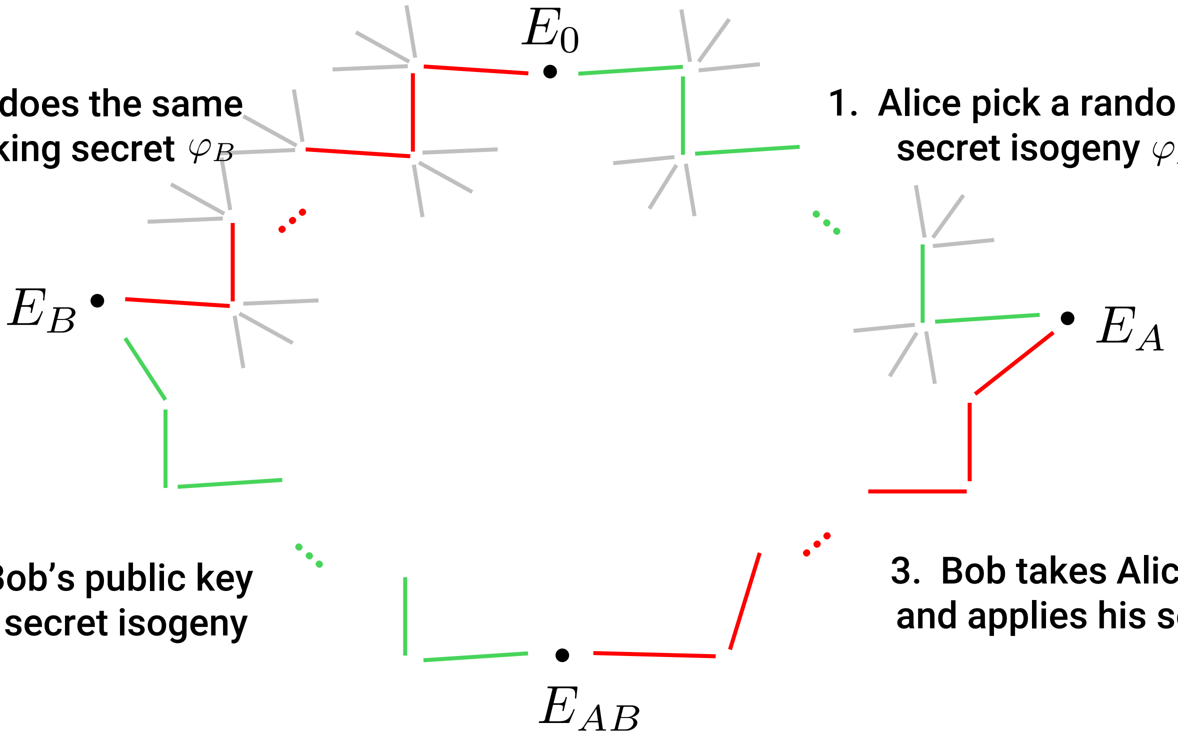
i.e. Alice and Bob who have never interacted before, want to talk without anyone listening in.



Example – Key Exchange

i.e. Alice and Bob who have never interacted before, want to talk without anyone listening in.

Public starting curve



1. Bob does the same picking secret φ_B
2. Bob does the same publishing E_B
3. Alice takes Bob's public key and applies his secret isogeny

1. Alice pick a random secret isogeny φ_A
2. Alice publishes codomain curve as her public key
3. Bob takes Alice's public key and applies his secret isogeny

4. They both arrive at the same curve - a shared secret for further communication

(Detail Omitted - In step 3, how does Alice "evaluate" their isogeny $\varphi_A : E_0 \to E_A$ from a different curve E_B in a commutative way?)

Quaternion Algebras

Quaternion Algebras

Fix the same large prime p as before.

Quaternion Algebras

Fix the same large prime p as before.

Consider the rational numbers $\mathbb{Q}$ extended by elements i and j.

$$B = \{w + xi + yj + zij : w, x, y, z \in \mathbb{Q}\}$$

Quaternion Algebras

Fix the same large prime p as before.

Consider the rational numbers $\mathbb{Q}$ extended by elements i and j.

$$B = \{w + xi + yj + zij : w, x, y, z \in \mathbb{Q}\}$$

We define multiplication using the following laws:

$$i^2 = -1, \quad j^2 = -p, \quad ji = -ij.$$

This is a **quaternion algebra**.

Quaternion Algebras

Fix the same large prime p as before.

Consider the rational numbers $\mathbb{Q}$ extended by elements i and j.

$$B = \{w + xi + yj + zij : w, x, y, z \in \mathbb{Q}\}$$

We define multiplication using the following laws:

$$i^2 = -1, \quad j^2 = -p, \quad ji = -ij.$$

This is a **quaternion algebra**.

Quaternions have (reduced) **norm** and **trace** given by,

$$\mathrm{nrd}(w + xi + yj + zij) = w^2 + x^2 + p(y^2 + z^2),$$

$$\mathrm{Tr}(w + xi + yj + zij) = 2w.$$

Quaternion Algebras

Fix the same large prime p as before.

Consider the rational numbers $\mathbb{Q}$ extended by elements i and j.

$$B = \{w + xi + yj + zij : w, x, y, z \in \mathbb{Q}\}$$

We define multiplication using the following laws:

$$i^2 = -1, \quad j^2 = -p, \quad ji = -ij.$$

This is a **quaternion algebra**.

Quaternions have (reduced) **norm** and **trace** given by,

$$\mathrm{nrd}(w + xi + yj + zij) = w^2 + x^2 + p(y^2 + z^2),$$

$$\mathrm{Tr}(w + xi + yj + zij) = 2w.$$

Any quaternion $\alpha \in B$ with integral norm and trace $\mathrm{nrd}(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Z}$ is a **quaternion integer**.

Orders and Ideals

Orders and Ideals

An **integral lattice** is the linear span of 4 quaternion integers over $\mathbb{Z}$.

$L = \mathbb{Z}e_0 + \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3$ for generators $e_0, e_1, e_2, e_3 \in B$ with $\mathrm{nrd}(e_i), \mathrm{Tr}(e_i) \in \mathbb{Z}$

Orders and Ideals

An **integral lattice** is the linear span of 4 quaternion integers over $\mathbb{Z}$.

$$L = \mathbb{Z}e_0 + \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \text{ for generators } e_0, e_1, e_2, e_3 \in B \text{ with } \mathrm{nrd}(e_i), \mathrm{Tr}(e_i) \in \mathbb{Z}$$

It is an **order** if it contains 1 and is closed under multiplication.

Orders and Ideals

An **integral lattice** is the linear span of 4 quaternion integers over $\mathbb{Z}$.

$L = \mathbb{Z}e_0 + \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3$ for generators $e_0, e_1, e_2, e_3 \in B$ with $\mathrm{nrd}(e_i), \mathrm{Tr}(e_i) \in \mathbb{Z}$

It is an **order** if it contains 1 and is closed under multiplication.

A **maximal order** is an order, not contained within any larger order.

Orders and Ideals

An **integral lattice** is the linear span of 4 quaternion integers over $\mathbb{Z}$.

$L = \mathbb{Z}e_0 + \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3$ for generators $e_0, e_1, e_2, e_3 \in B$ with $\mathrm{nrd}(e_i), \mathrm{Tr}(e_i) \in \mathbb{Z}$

It is an **order** if it contains 1 and is closed under multiplication.

A **maximal order** is an order, not contained within any larger order.

An ideal of an **order** $\mathcal{O}$ is an integral lattice which is fully contained within the order $I \subseteq \mathcal{O}$.

Orders and Ideals

An **integral lattice** is the linear span of 4 quaternion integers over $\mathbb{Z}$.

$L = \mathbb{Z}e_0 + \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3$ for generators $e_0, e_1, e_2, e_3 \in B$ with $\mathrm{nrd}(e_i), \mathrm{Tr}(e_i) \in \mathbb{Z}$

It is an **order** if it contains 1 and is closed under multiplication.

A **maximal order** is an order, not contained within any larger order.

An ideal of an **order** $\mathcal{O}$ is an integral lattice which is fully contained within the order $I \subseteq \mathcal{O}$.

Ideals have a notion of **norm**, an integer representing their size, $N(I) = \left|\frac{\mathcal{O}}{I}\right|$.

Orders and Ideals

An **integral lattice** is the linear span of 4 quaternion integers over $\mathbb{Z}$.

$L = \mathbb{Z}e_0 + \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3$ for generators $e_0, e_1, e_2, e_3 \in B$ with $\mathrm{nrd}(e_i), \mathrm{Tr}(e_i) \in \mathbb{Z}$

It is an **order** if it contains 1 and is closed under multiplication.

A **maximal order** is an order, not contained within any larger order.

An ideal of an **order** $\mathcal{O}$ is an integral lattice which is fully contained within the order $I \subseteq \mathcal{O}$.

Ideals have a notion of **norm**, an integer representing their size, $N(I) = \left|\frac{\mathcal{O}}{I}\right|$.

For a prime q, there are always $q+1$ norm q ideals within a maximal order $\mathcal{O}$.

Orders and Ideals

An **integral lattice** is the linear span of 4 quaternion integers over $\mathbb{Z}$.

$$L = \mathbb{Z}e_0 + \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \text{ for generators } e_0, e_1, e_2, e_3 \in B \text{ with } \mathrm{nrd}(e_i), \mathrm{Tr}(e_i) \in \mathbb{Z}$$

It is an **order** if it contains 1 and is closed under multiplication.

A **maximal order** is an order, not contained within any larger order.

An ideal of an **order** $\mathcal{O}$ is an integral lattice which is fully contained within the order $I \subseteq \mathcal{O}$.

Ideals have a notion of **norm**, an integer representing their size, $N(I) = \left|\frac{\mathcal{O}}{I}\right|$.

For a prime q, there are always $q+1$ norm q ideals within a maximal order $\mathcal{O}$.

And each ideal “connects” two maximal orders $I = N \cdot \mathcal{O}_1\mathcal{O}_2$.

More Graphs?

More Graphs?

A **quaternion ℓ-ideal graph** has:

Vertices = Maximal orders up to isomorphism,

Edges = Ideals between orders, of norm ℓ.

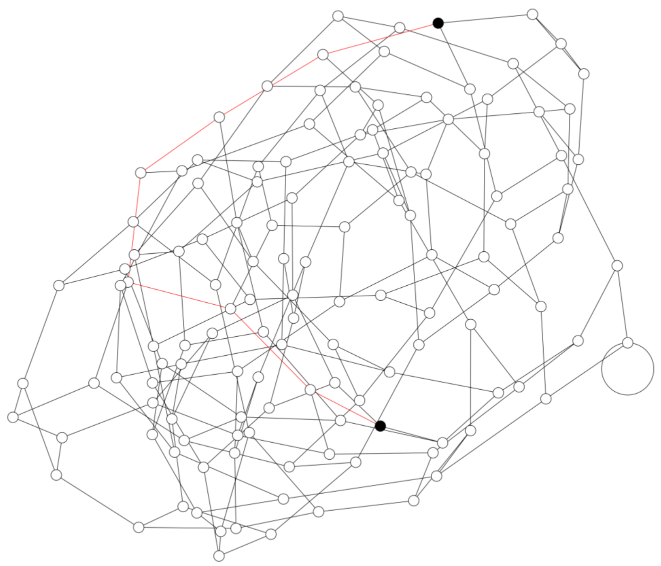
More Graphs?

A **quaternion ℓ-ideal graph** has:

Vertices = Maximal orders up to isomorphism,

Edges = Ideals between orders, of norm ℓ.

For $p = 1549$, $\ell = 2$ it looks like …



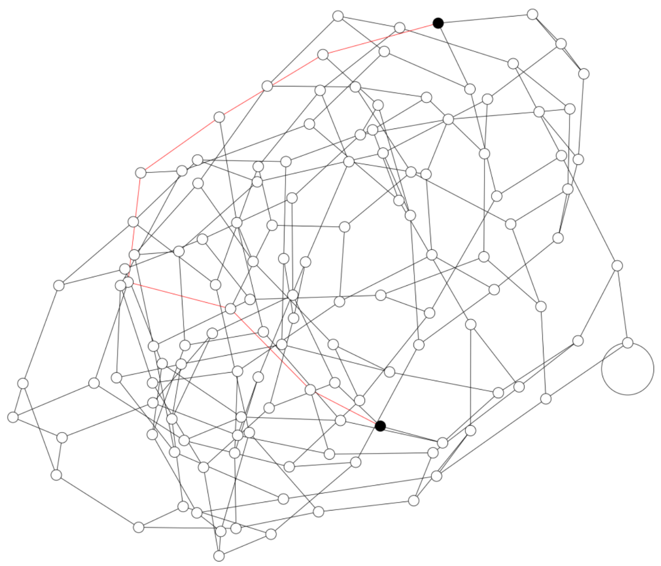
More Graphs?

A **quaternion ℓ-ideal graph** has:

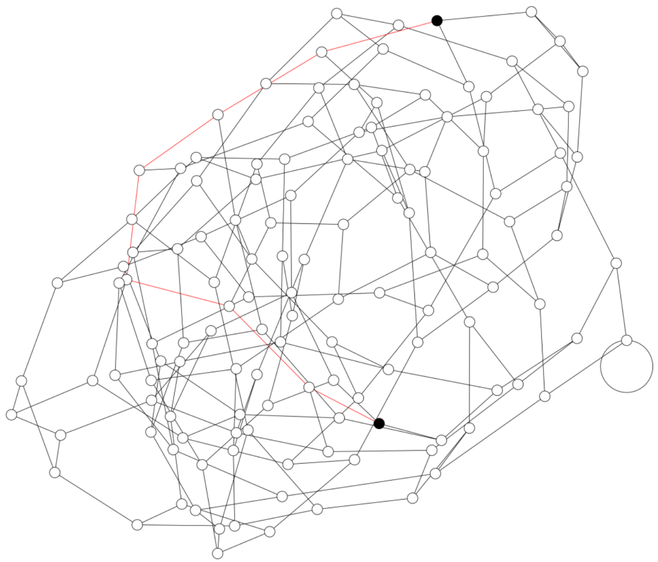
Vertices = Maximal orders up to isomorphism,

Edges = Ideals between orders, of norm ℓ.

For $p = 1549$, $\ell = 2$ it looks like …



This looks familiar! The ℓ-isogeny graph was …



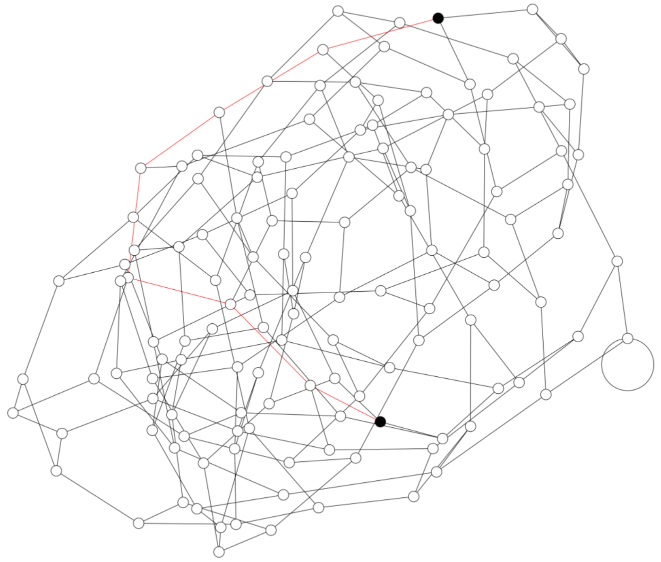
More Graphs?

A **quaternion ℓ-ideal graph** has:

Vertices = Maximal orders up to isomorphism,

Edges = Ideals between orders, of norm ℓ.

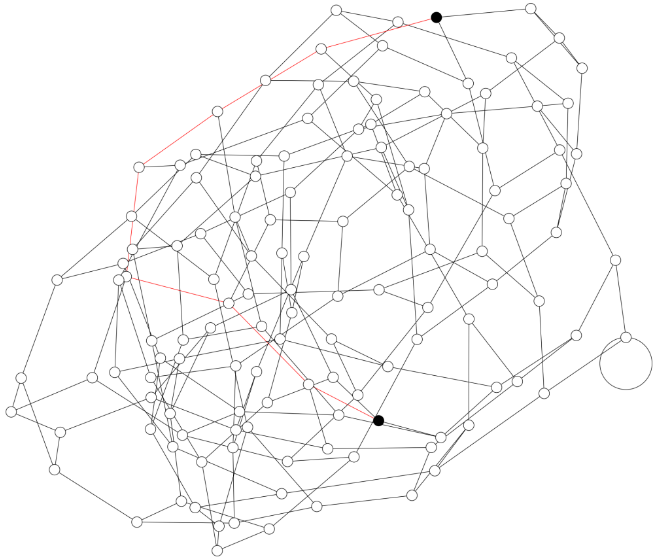
For $p = 1549$, $\ell = 2$ it looks like ...



graph isomorphism

(almost)

This looks familiar! The ℓ-isogeny graph was ...



More Graphs?

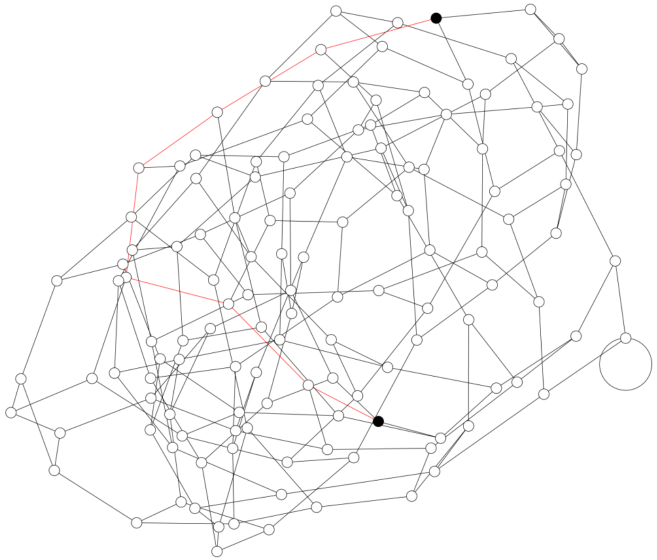
A **quaternion ℓ-ideal graph** has:

Vertices = Maximal orders up to isomorphism,

Edges = Ideals between orders, of norm ℓ.

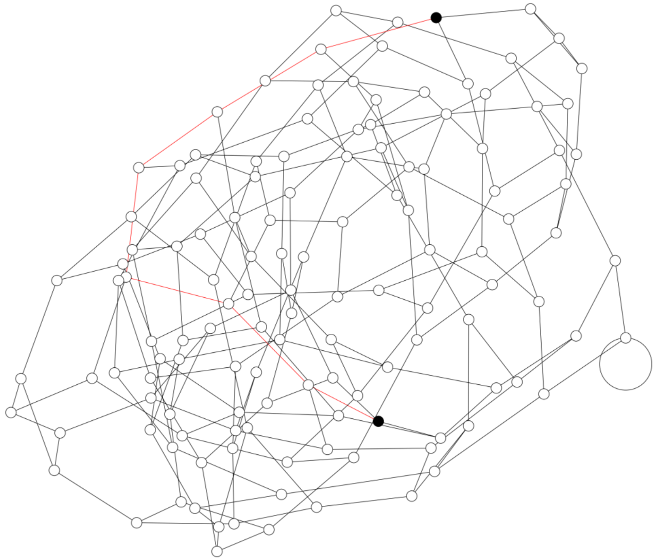
For $p = 1549$, $\ell = 2$ it looks like …

This looks familiar! The ℓ-isogeny graph was …



graph isomorphism

(almost)



This is the **Deuring Correspondence** relating the two worlds of isogenies and quaternions.

What I'm trying to achieve…

Finding best algorithms to solve the Quaternion Embedding Problem.

Given a maximal order $\mathcal{O}$ find an element $\alpha \in \mathcal{O}$ of prescribed trace t and norm d .

Hardness of this problem gives arguments for the hardness of isogeny problems in general.

Finding shortest norm q^n ideal paths connecting two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$.

This would result in major speedups to digital signature scheme SQISign and give better estimates to aid security analysis.

Fast constant-time sampling of random ideals of a given norm.

Giving further improvements to SQISign.

Thanks!