New New Directions in Cryptography

Nick Egbert

Student Colloquium Talk

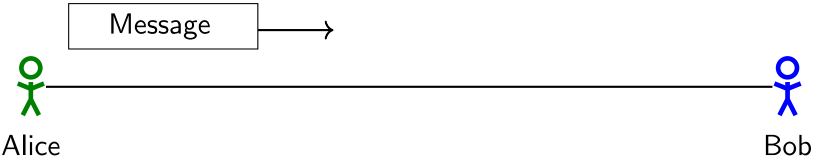
20 Februrary 2019

Overview

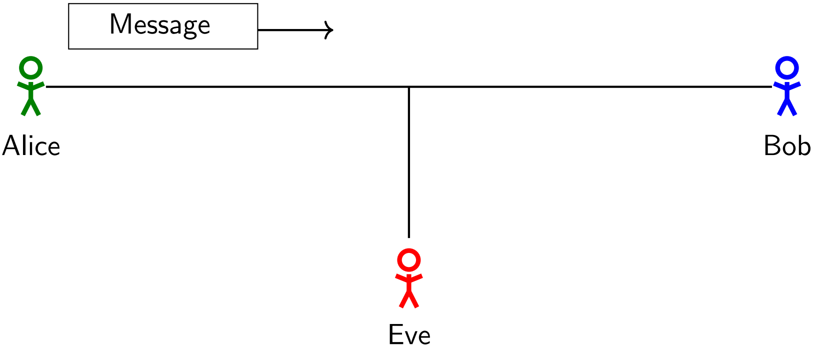
1. Cryptography overview
   - The general problem
   - Classical Diffie-Hellman
2. Elliptic curve basics
   - Definition
   - Group structure
3. Elliptic curves in cryptography
   - How they're used today
   - Advantages and potential doom
4. Post-quantum cryptography
   - Supersingular elliptic curves
   - Isogenies
   - Ideal class group

The problem

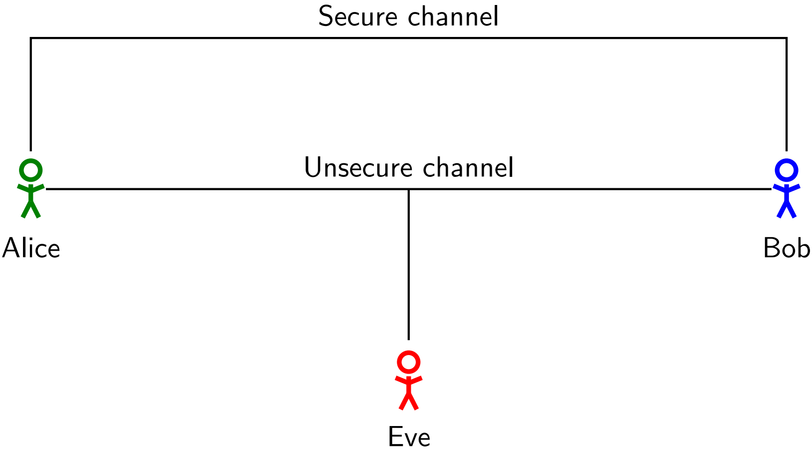
The problem



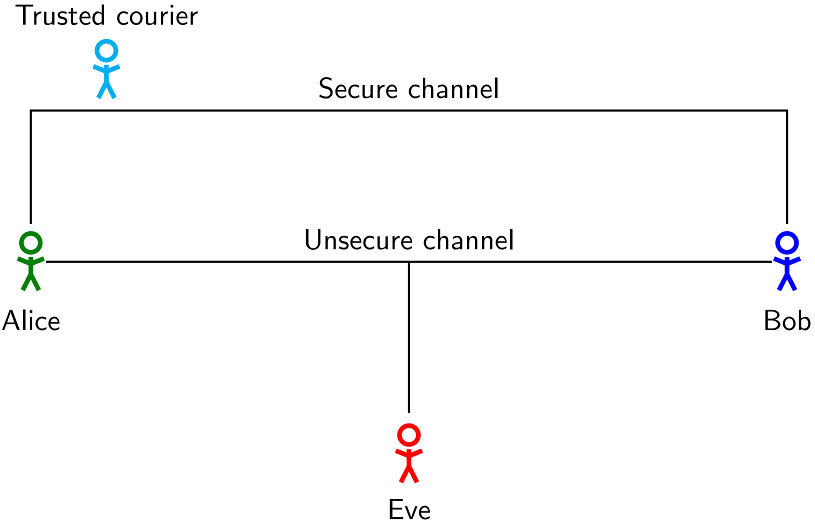
The problem



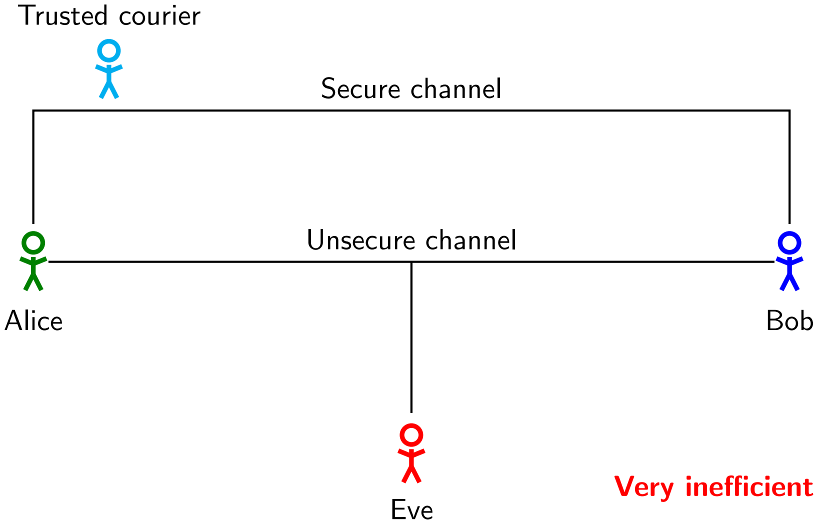
The problem



The problem


Trusted courier
Secure channel
Unsecure channel
Alice
Bob
Eve

The problem



Very inefficient

The solution

- There are two basic types of encryption: symmetric and asymmetric.

The solution

- There are two basic types of encryption: symmetric and asymmetric.
- In symmetric encryption, both parties have the same key for encrypting and decrypting.

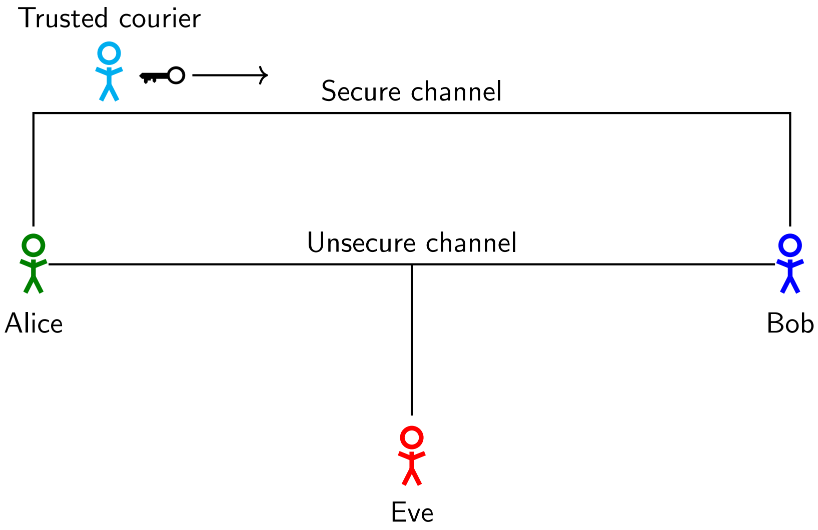
The solution

- There are two basic types of encryption: symmetric and asymmetric.
- In symmetric encryption, both parties have the same key for encrypting and decrypting.
- Asymmetric encryption is not symmetric.

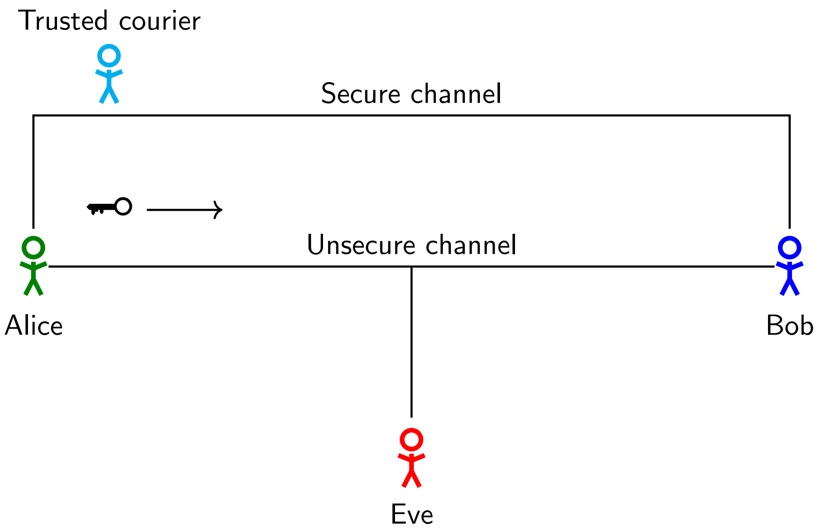
The solution

- There are two basic types of encryption: symmetric and asymmetric.
- In symmetric encryption, both parties have the same key for encrypting and decrypting.
- Asymmetric encryption is not symmetric.
- Asymmetric encryption is generally used to establish a shared key.

The solution



The solution



Discrete log problem (DLP)

Let p be a prime number, and let $a, b \in \mathbb{Z}$ such that $a, b \not\equiv 0 \bmod p$. Suppose we know there exists $k \in \mathbb{Z}$ such that

$$a^k \equiv b \pmod{p}.$$

The **(classical) discrete log problem** is to find k.

Discrete log problem (DLP)

Let p be a prime number, and let $a, b \in \mathbb{Z}$ such that $a, b \not\equiv 0 \bmod p$.
Suppose we know there exists $k \in \mathbb{Z}$ such that

$$a^k \equiv b \pmod{p}.$$

The **(classical) discrete log problem** is to find k.
More generally, if G is a group and $a, b \in G$, and given

$$a^k = b,$$

the discrete log problem is to find k.

Diffie-Hellman Key Exchange (1976)

- Alice and Bob publicly agree upon a prime p and a generator $g \in G = \mathbb{F}_p^\times$.
- Alice picks a random integer $a \in \{2, \ldots, p-2\}$ and computes $A = g^a \bmod p$.
- Bob picks a random integer $b \in \{2, \ldots, p-2\}$ and computes $B = g^b \bmod p$.
- The integers a, b are kept secret, and Alice and Bob transmit A and B publicly.
- They compute a shared secret $K = B^a = g^{ba} = g^{ab} = A^b$.
- Security relies upon the DLP.

Diffie-Hellman Key Exchange (1976)

- Alice and Bob publicly agree upon a prime p and a generator $g \in G = \mathbb{F}_p^\times$.
- Alice picks a random integer $a \in \{2, \ldots, p-2\}$ and computes $A = g^a \bmod p$.
- Bob picks a random integer $b \in \{2, \ldots, p-2\}$ and computes $B = g^b \bmod p$.
- The integers a, b are kept secret, and Alice and Bob transmit A and B publicly.
- They compute a shared secret $K = B^a = g^{ba} = g^{ab} = A^b$.
- Security relies upon the DLP.

Diffie-Hellman Key Exchange (1976)

- Alice and Bob publicly agree upon a prime p and a generator $g \in G = \mathbb{F}_p^\times$.
- Alice picks a random integer $a \in \{2, \dots, p-2\}$ and computes $A = g^a \bmod p$.
- Bob picks a random integer $b \in \{2, \dots, p-2\}$ and computes $B = g^b \bmod p$.
- The integers a, b are kept secret, and Alice and Bob transmit A and B publicly.
- They compute a shared secret $K = B^a = g^{ba} = g^{ab} = A^b$.
- Security relies upon the DLP.

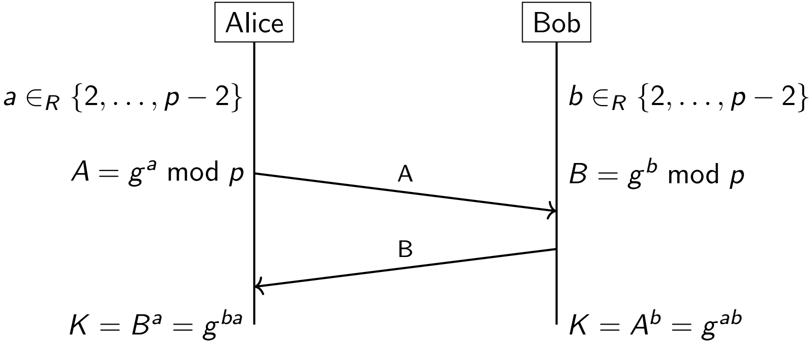
Diffie-Hellman Key Exchange (1976)

- Alice and Bob publicly agree upon a prime p and a generator $g \in G = \mathbb{F}_p^\times$.
- Alice picks a random integer $a \in \{2, \ldots, p-2\}$ and computes $A = g^a \bmod p$.
- Bob picks a random integer $b \in \{2, \ldots, p-2\}$ and computes $B = g^b \bmod p$.
- The integers a, b are kept secret, and Alice and Bob transmit A and B publicly.
- They compute a shared secret $K = B^a = g^{ba} = g^{ab} = A^b$.
- Security relies upon the DLP.

Diffie-Hellman Key Exchange (1976)

Public parameters:

g, p



Issues with DH

- When $G = \mathbb{F}_q^\times$, the DLP can be solved in subexponential time.
- This requires larger keys.
- In the 1980s, Victor Miller and Neal Koblitz independently suggested using elliptic curves for cryptography.

- An elliptic curve E is the graph of an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

  with coefficients in some field K.
- If $\text{char}K \neq 2, 3$, then via a change of variables, we may assume E has the form

$$y^2 = x^3 + Ax + B.$$

- To be considered an elliptic curve, we require that $4A^3 + 27B^2 \neq 0$, so that $x^3 + Ax + B$ does not have any repeated roots.

What is an elliptic curve?

- An elliptic curve E is the graph of an equation of the form
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
with coefficients in some field K.
- If $\mathrm{char} K \neq 2, 3$, then via a change of variables, we may assume E has the form
$$y^2 = x^3 + Ax + B.$$
- To be considered an elliptic curve, we require that $4A^3 + 27B^2 \neq 0$, so that $x^3 + Ax + B$ does not have any repeated roots.

What is an elliptic curve?

- An elliptic curve E is the graph of an equation of the form

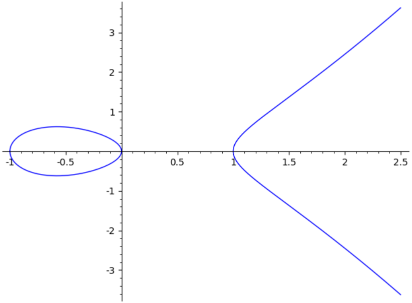
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

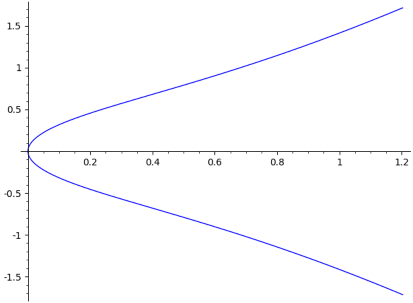
  with coefficients in some field K.
- If char$K \neq 2, 3$, then via a change of variables, we may assume E has the form

$$y^2 = x^3 + Ax + B.$$

- To be considered an elliptic curve, we require that $4A^3 + 27B^2 \neq 0$, so that $x^3 + Ax + B$ does not have any repeated roots.

Examples

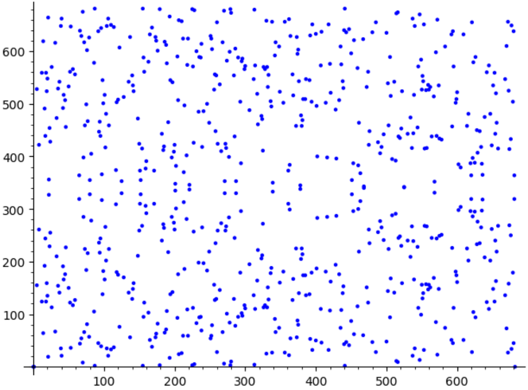




$$E1\colon y^2 = x^3 - x$$

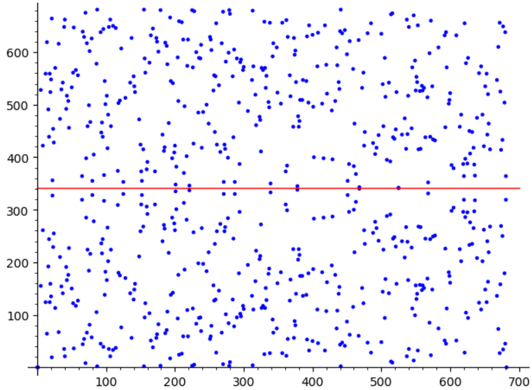
$$E_2\colon y^2 = x^3 + x$$

Examples



$$E_1 : y^2 = x^3 - x \pmod{683}$$

Examples

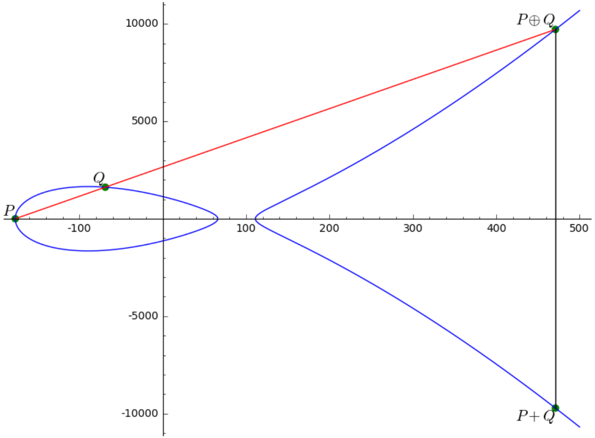


$$E_1 : y^2 = x^3 - x \pmod{683}$$

Group structure

- $E(K) = \{(x, y) \in K \times K \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}$
- Rational points plus the point at infinity form a group, where addition law is given by "chord-and-tangent" method

Adding points



$$E: y^2 = x^3 - 24003 * x + 1296702$$

Assumptions

- For $q = p^n$, where p is prime, we consider only $E(\mathbb{F}_q)$.
- We will assume that $\mathrm{char} K \neq 2, 3$ and that $E\colon y^2 = x^3 + Ax + B$.
- Later, we will want to write E in the form $y^2 = x^3 + Ax^2 + x$, referred to as a Montgomery curve.
- We define the j-invariant of E to be

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

- Fact: E_1, E_2 are isomorphic over $\overline{\mathbb{F}}_q$ if and only if $j(E_1) = j(E_2)$.

Assumptions

- For $q = p^n$, where p is prime, we consider only $E(\mathbb{F}_q)$.
- We will assume that $\mathrm{char} K \neq 2, 3$ and that $E\colon y^2 = x^3 + Ax + B$.
- Later, we will want to write E in the form $y^2 = x^3 + Ax^2 + x$, referred to as a Montgomery curve.
- We define the j-invariant of E to be

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

- Fact: E_1, E_2 are isomorphic over $\overline{\mathbb{F}}_q$ if and only if $j(E_1) = j(E_2)$.

Assumptions

- For $q = p^n$, where p is prime, we consider only $E(\mathbb{F}_q)$.
- We will assume that $\mathrm{char} K \neq 2, 3$ and that $E\colon y^2 = x^3 + Ax + B$.
- Later, we will want to write E in the form $y^2 = x^3 + Ax^2 + x$, referred to as a Montgomery curve.
- We define the j-invariant of E to be

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

- Fact: E_1, E_2 are isomorphic over $\overline{\mathbb{F}}_q$ if and only if $j(E_1) = j(E_2)$.

Assumptions

- For $q = p^n$, where p is prime, we consider only $E(\mathbb{F}_q)$.
- We will assume that $\mathrm{char} K \neq 2, 3$ and that $E\colon y^2 = x^3 + Ax + B$.
- Later, we will want to write E in the form $y^2 = x^3 + Ax^2 + x$, referred to as a Montgomery curve.
- We define the j-invariant of E to be

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

- Fact: E_1, E_2 are isomorphic over $\overline{\mathbb{F}}_q$ if and only if $j(E_1) = j(E_2)$.

Assumptions

- For $q = p^n$, where p is prime, we consider only $E(\mathbb{F}_q)$.
- We will assume that $\mathrm{char} K \neq 2, 3$ and that $E\colon y^2 = x^3 + Ax + B$.
- Later, we will want to write E in the form $y^2 = x^3 + Ax^2 + x$, referred to as a Montgomery curve.
- We define the j-invariant of E to be

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

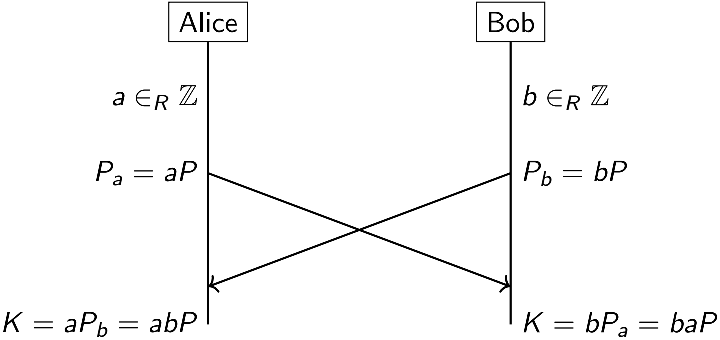
- Fact: E_1, E_2 are isomorphic over $\overline{\mathbb{F}}_q$ if and only if $j(E_1) = j(E_2)$.

ECDH

- ECDH = "Elliptic Curve Diffie-Hellman"
- Alice and Bob agree on an elliptic curve E and a field $\mathbb{F}_q$ such that the DLP is hard for $E(\mathbb{F}_q)$.
- They agree on a point $P \in E(\mathbb{F}_q)$ of large (usually prime) order.

ECDH

Public parameters:
$E(\mathbb{F}_q)$, P



Advantages of ECDH

- Using elliptic curves allows for *much* smaller key sizes: an RSA 4096-bit key provides the same level of security as a 313-bit EC key.
- The group law for elliptic curves can be performed efficiently.

Post-quantum cryptography

- In 1994, Peter Shor published an algorithm that solves the DLP (and factoring large numbers) in polynomial time.
- This effectively breaks any cryptosystem based on the hardness of these two problems.
- Is cryptography broken in a post-quantum world?

Post-quantum cryptography

- In 1994, Peter Shor published an algorithm that solves the DLP (and factoring large numbers) in polynomial time.
- This effectively breaks any cryptosystem based on the hardness of these two problems.
- Is cryptography broken in a post-quantum world?
    - Fear not.

Post-quantum cryptography

- In 1994, Peter Shor published an algorithm that solves the DLP (and factoring large numbers) in polynomial time.
- This effectively breaks any cryptosystem based on the hardness of these two problems.
- Is cryptography broken in a post-quantum world?
    - Fear not.
    - There have been several major developments in the past ten years.

Post-quantum cryptography

- In 1994, Peter Shor published an algorithm that solves the DLP (and factoring large numbers) in polynomial time.
- This effectively breaks any cryptosystem based on the hardness of these two problems.
- Is cryptography broken in a post-quantum world?
  - Fear not.
  - There have been several major developments in the past ten years.
  - Many of them use isogeny graphs of supersingular elliptic curves.

Supersingular elliptic curves

Definition

Let E be an elliptic curve over $\mathbb{F}_q$. We define the n-torsion subgroup to be

$$E[n] = \{P \in E(\overline{\mathbb{F}}_q) \mid nP = \infty\}.$$

Supersingular elliptic curves

Definition

Let E be an elliptic curve over $\mathbb{F}_q$. We define the n-torsion subgroup to be

$$E[n] = \{P \in E(\overline{\mathbb{F}}_q) \mid nP = \infty\}.$$

Remark

$E[n]$ is a subgroup of $E(\overline{\mathbb{F}}_q)$. In general, we can't expect that $E[n] \subset E(\mathbb{F}_q)$.

Supersingular elliptic curves

Definition

Let E be an elliptic curve over $\mathbb{F}_q$. We define the n-torsion subgroup to be

$$E[n] = \{P \in E(\overline{\mathbb{F}}_q) \mid nP = \infty\}.$$

Remark

$E[n]$ is a subgroup of $E(\overline{\mathbb{F}}_q)$. In general, we can't expect that $E[n] \subset E(\mathbb{F}_q)$.

Theorem

Let $p = \operatorname{char} \mathbb{F}_q$. If p does not divide n, then

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Supersingular elliptic curves

Definition

An elliptic curve $E/\mathbb{F}_q$ is called **supersingular** if $E[p] = \{\infty\}$, where p is the characteristic of $\mathbb{F}_q$.

Theorem

Let $E/\mathbb{F}_q$ be an elliptic curve, where $q = p^n$. Let $t = q + 1 - \#E(\mathbb{F}_q)$. Then E is supersingular if and only if

$$t \equiv 0 \pmod{p}.$$

Isogenies

Definition

Let E_1, E_2 be elliptic curves over $\mathbb{F}_q$. An **isogeny** from E_1 to E_2 is a nonconstant homomorphism

$$\alpha\colon E_1(\overline{\mathbb{F}}_q) \to E_2(\overline{\mathbb{F}}_q)$$

given by rational maps.

Definition

We may write $\alpha(x, y) = (r_1(x), yr_2(x))$, where r_1, r_2 are rational functions. Writing $r_1(x) = \frac{p(x)}{q(x)}$, the **degree** of α is

$$\deg \alpha = \max(\deg p, \deg q).$$

Endomorphisms of elliptic curves

Definition

An **endomorphism** of E is an isogeny from E to itself.

Endomorphisms of elliptic curves

Definition

An **endomorphism** of E is an isogeny from E to itself.

Example

The multiplication by n map:

$$\begin{aligned}[n]\colon E &\to E \\ (x, y) &\mapsto n(x, y)\end{aligned}$$

Endomorphisms of elliptic curves

Definition

An **endomorphism** of E is an isogeny from E to itself.

Example

The multiplication by n map:

$$\begin{aligned}[n]\colon E &\to E\\ (x, y) &\mapsto n(x, y)\end{aligned}$$

Example

The Frobenius endomorphism:

$$\begin{aligned}\pi\colon E &\to E\\ (x, y) &\mapsto (x^p, y^p)\end{aligned}$$

Quick aside on ANT

- Let $K = \mathbb{Q}(\sqrt{-p})$. Let $\mathcal{O}_K$ denote the **ring of integers** of K, i.e.,

$$\left\{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\right\}.$$

- An **order** $\mathcal{O} \in K$ is a ring such that $\mathbb{Z} \subsetneq \mathcal{O} \subseteq \mathcal{O}_K$.
- A **fractional ideal** of $\mathcal{O}$ is of the form $\alpha\mathfrak{a}$, where $\alpha \in K^\times$ and $\mathfrak{a}$ is an $\mathcal{O}$-ideal. A **principal fractional ideal** is of the form $\alpha\mathcal{O}$.
- We say a fractional ideal $\mathfrak{a}$ is **invertible** if $\exists \mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$.

Quick aside on ANT

- Let $K = \mathbb{Q}(\sqrt{-p})$. Let $\mathcal{O}_K$ denote the **ring of integers** of K, i.e.,

$$\left\{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\right\}.$$

- An **order** $\mathcal{O} \in K$ is a ring such that $\mathbb{Z} \subsetneq \mathcal{O} \subseteq \mathcal{O}_K$.
- A **fractional ideal** of $\mathcal{O}$ is of the form $\alpha\mathfrak{a}$, where $\alpha \in K^\times$ and $\mathfrak{a}$ is an $\mathcal{O}$-ideal. A **principal fractional ideal** is of the form $\alpha\mathcal{O}$.
- We say a fractional ideal $\mathfrak{a}$ is **invertible** if $\exists\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$.

Quick aside on ANT

- Let $K = \mathbb{Q}(\sqrt{-p})$. Let $\mathcal{O}_K$ denote the **ring of integers** of K, i.e.,

$$\left\{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\right\}.$$

- An **order** $\mathcal{O} \in K$ is a ring such that $\mathbb{Z} \subsetneq \mathcal{O} \subseteq \mathcal{O}_K$.
- A **fractional ideal** of $\mathcal{O}$ is of the form $\alpha\mathfrak{a}$, where $\alpha \in K^\times$ and $\mathfrak{a}$ is an $\mathcal{O}$-ideal. A **principal fractional ideal** is of the form $\alpha\mathcal{O}$.
- We say a fractional ideal $\mathfrak{a}$ is **invertible** if $\exists\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$.

Quick aside on ANT

- Let $K = \mathbb{Q}(\sqrt{-p})$. Let $\mathcal{O}_K$ denote the **ring of integers** of K, i.e.,

$$\{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\}.$$

- An **order** $\mathcal{O} \in K$ is a ring such that $\mathbb{Z} \subsetneq \mathcal{O} \subseteq \mathcal{O}_K$.
- A **fractional ideal** of $\mathcal{O}$ is of the form $\alpha\mathfrak{a}$, where $\alpha \in K^\times$ and $\mathfrak{a}$ is an $\mathcal{O}$-ideal. A **principal fractional ideal** is of the form $\alpha\mathcal{O}$.
- We say a fractional ideal $\mathfrak{a}$ is **invertible** if $\exists \mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$.

Ideal class group

- By construction, the set of invertible fractional ideals $I(\mathcal{O})$ forms an abelian group under multiplication of ideals.
- The set of principal ideals $P(\mathcal{O})$ is a (normal) subgroup, so we may consider the **ideal class group** of $\mathcal{O}$

$$\mathrm{cl}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}).$$

- Let $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic field.

Ideal class group

- By construction, the set of invertible fractional ideals $I(\mathcal{O})$ forms an abelian group under multiplication of ideals.
- The set of principal ideals $P(\mathcal{O})$ is a (normal) subgroup, so we may consider the **ideal class group** of $\mathcal{O}$

$$\mathrm{cl}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}).$$

- Let $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic field.

Ideal class group

- By construction, the set of invertible fractional ideals $I(\mathcal{O})$ forms an abelian group under multiplication of ideals.
- The set of principal ideals $P(\mathcal{O})$ is a (normal) subgroup, so we may consider the **ideal class group** of $\mathcal{O}$

$$\mathrm{cl}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}).$$

- Let $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic field.

Class group action

- Let $E/\mathbb{F}_p$ be an elliptic curve. Define

$$E[\mathfrak{a}] = \left\{ P \in E(\overline{\mathbb{F}}_p) \mid \alpha(P) = 0 \ \forall \alpha \in \mathfrak{a} \right\}.$$

- We can define the action of the $\mathcal{O}$-ideal $\mathfrak{a}$ on E as the image E' under the isogeny

$$\phi \colon E \to E'$$

whose kernel is $E[\mathfrak{a}]$. We denote $E' = \mathfrak{a} * E$.

- Fact: an isogeny is uniquely determined by its kernel (up to isomorphism).

Class group action

- Let $E/\mathbb{F}_p$ be an elliptic curve. Define

$$E[\mathfrak{a}] = \left\{ P \in E(\overline{\mathbb{F}}_p) \mid \alpha(P) = 0 \ \forall \alpha \in \mathfrak{a} \right\}.$$

- We can define the action of the $\mathcal{O}$-ideal $\mathfrak{a}$ on E as the image E' under the isogeny

$$\phi \colon E \to E'$$

whose kernel is $E[\mathfrak{a}]$. We denote $E' = \mathfrak{a} * E$.

- Fact: an isogeny is uniquely determined by its kernel (up to isomorphism).

Class group action

- Let $E/\mathbb{F}_p$ be an elliptic curve. Define

$$E[\mathfrak{a}] = \left\{ P \in E(\overline{\mathbb{F}}_p) \mid \alpha(P) = 0 \ \forall \alpha \in \mathfrak{a} \right\}.$$

- We can define the action of the $\mathcal{O}$-ideal $\mathfrak{a}$ on E as the image E' under the isogeny

$$\phi \colon E \to E'$$

whose kernel is $E[\mathfrak{a}]$. We denote $E' = \mathfrak{a} * E$.

- Fact: an isogeny is uniquely determined by its kernel (up to isomorphism).

Class group action

- Let S be the set of supersingular elliptic curves $E_A/\mathbb{F}_p \colon y^2 = x^3 + Ax^2 + x$, where $p \geq 5$ and $p \equiv 3 \pmod 8$.
- In this case, $\mathrm{End}_{\mathbb{F}_p}(E_A) \cong \mathbb{Z}[\sqrt{-p}]$.
- $\mathfrak{a} * E_A$ is an ℓ-isogeny if and only if $\mathfrak{a} = \langle [\ell], \pi \pm 1 \rangle$

Class group action

- Let S be the set of supersingular elliptic curves $E_A/\mathbb{F}_p\colon y^2 = x^3 + Ax^2 + x$, where $p \geq 5$ and $p \equiv 3 \pmod 8$.
- In this case, $\mathrm{End}_{\mathbb{F}_p}(E_A) \cong \mathbb{Z}[\sqrt{-p}]$.
- $\mathfrak{a} * E_A$ is an ℓ-isogeny if and only if $\mathfrak{a} = \langle [\ell], \pi \pm 1 \rangle$

Class group action

- Let S be the set of supersingular elliptic curves $E_A/\mathbb{F}_p\colon y^2 = x^3 + Ax^2 + x$, where $p \geq 5$ and $p \equiv 3 \pmod 8$.
- In this case, $\mathrm{End}_{\mathbb{F}_p}(E_A) \cong \mathbb{Z}[\sqrt{-p}]$.
- $\mathfrak{a} * E_A$ is an ℓ-isogeny if and only if $\mathfrak{a} = \langle [\ell], \pi \pm 1 \rangle$

CSIDH

- In November 2018, Castryck, Lange, Martindale, Panny and Renes published a paper on their algorithm CSIDH, which stands for Commutative Supersingular Isogeny Diffie-Hellman.
- CSIDH is thought to be a suitable post-quantum replacement for ECDH.
- Key sizes are extremely small.

CSIDH

- In November 2018, Castryck, Lange, Martindale, Panny and Renes published a paper on their algorithm CSIDH, which stands for Commutative Supersingular Isogeny Diffie-Hellman.
- CSIDH is thought to be a suitable post-quantum replacement for ECDH.
- Key sizes are extremely small.

CSIDH

- In November 2018, Castryck, Lange, Martindale, Panny and Renes published a paper on their algorithm CSIDH, which stands for Commutative Supersingular Isogeny Diffie-Hellman.
- CSIDH is thought to be a suitable post-quantum replacement for ECDH.
- Key sizes are extremely small.

Isogeny graphs

- Let p, ℓ be distinct primes. The isogeny graph G_ℓ over $\mathbb{F}_p$ has
  - Vertices: Elliptic curves $E_A \in S$ with $\mathrm{End}(E_A) \cong \mathbb{Z}[\sqrt{-p}]$
  - Edges: (E_A, E_B), where there is an ℓ-isogeny between E_A and E_B
- For illustration we will fix $p = 419$.
- In general, the CSIDH authors pick $p = 4\ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are distinct odd primes.

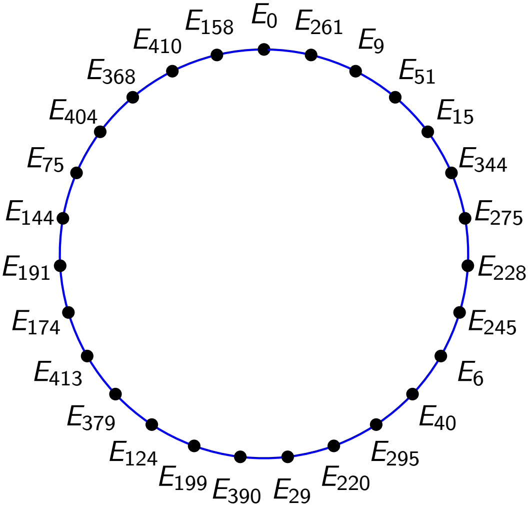
Isogeny graphs

- Let p, ℓ be distinct primes. The isogeny graph G_ℓ over $\mathbb{F}_p$ has
  - Vertices: Elliptic curves $E_A \in S$ with $\mathrm{End}(E_A) \cong \mathbb{Z}[\sqrt{-p}]$
  - Edges: (E_A, E_B), where there is an ℓ-isogeny between E_A and E_B
- For illustration we will fix $p = 419$.
- In general, the CSIDH authors pick $p = 4\ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are distinct odd primes.

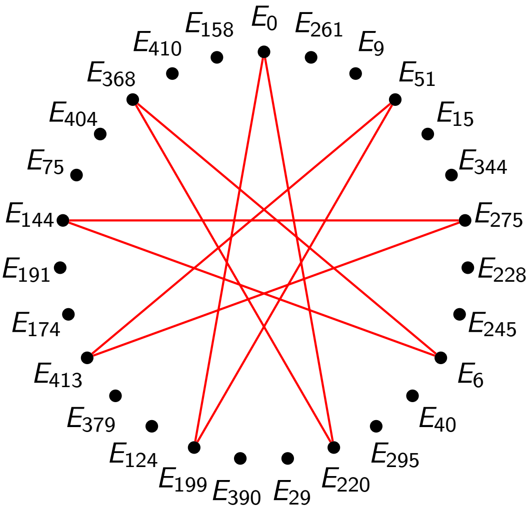
Isogeny graphs

- Let p, ℓ be distinct primes. The isogeny graph G_ℓ over $\mathbb{F}_p$ has
  - Vertices: Elliptic curves $E_A \in S$ with $\mathrm{End}(E_A) \cong \mathbb{Z}[\sqrt{-p}]$
  - Edges: (E_A, E_B), where there is an ℓ-isogeny between E_A and E_B
- For illustration we will fix $p = 419$.
- In general, the CSIDH authors pick $p = 4\ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are distinct odd primes.

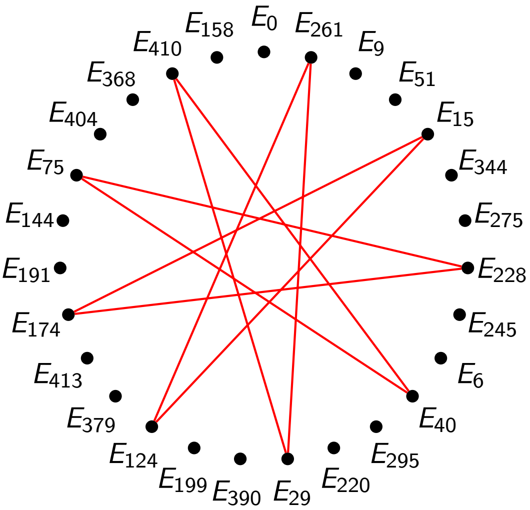
Isogeny graph G_3



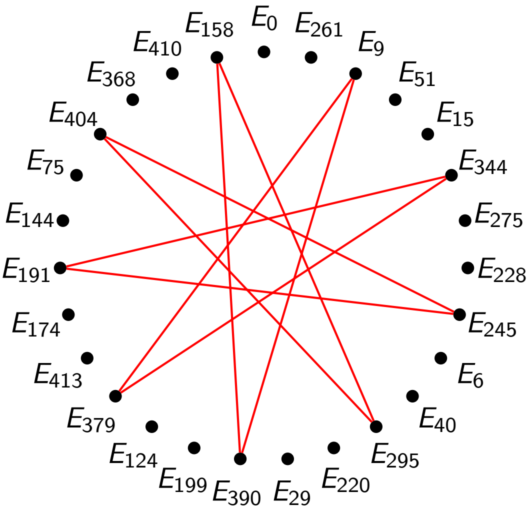
Isogeny graph G_5



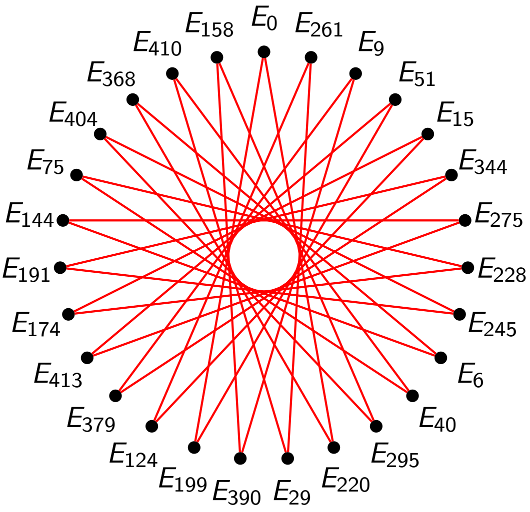
Isogeny graph G_5



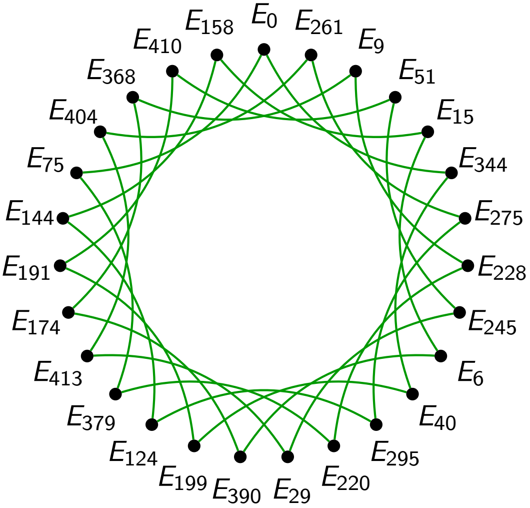
Isogeny graph G_5



Isogeny graph G_5



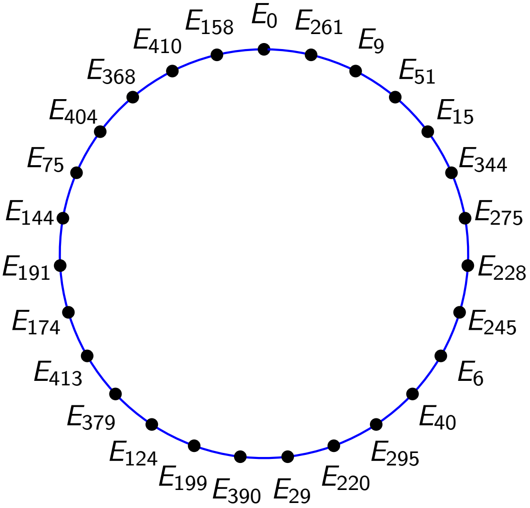
Isogeny graph G_7



CSIDH

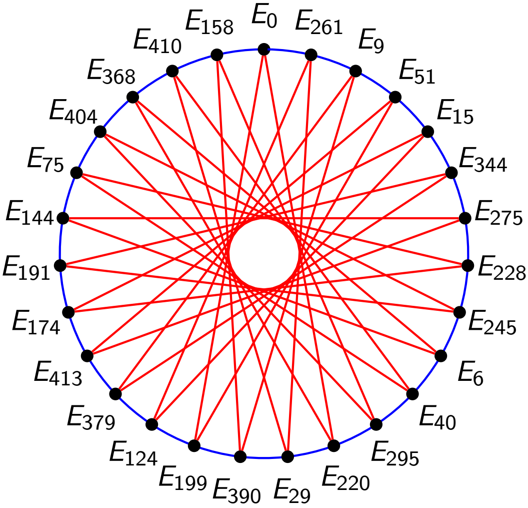
- CSIDH stands for Commutative Supersingular Isogeny Diffie-Hellman.
- It is proposed as a post-quantum drop-in replacement for (EC)DH.
- They use the action of the ideal class group and the supersingular isogeny graph to establish keys.

Isogeny graph used in CSIDH



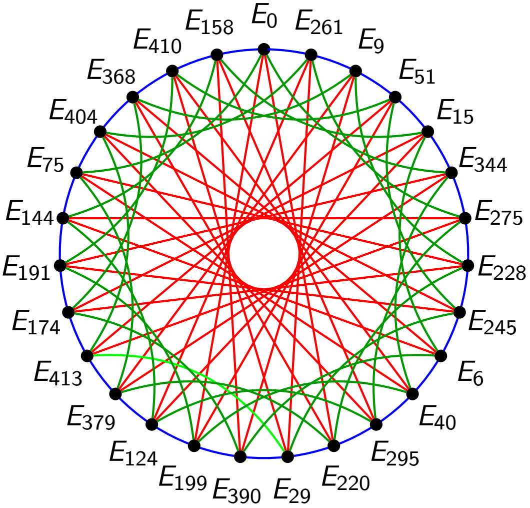
G_3

Isogeny graph used in CSIDH



$G_3 \cup G_5$

Isogeny graph used in CSIDH

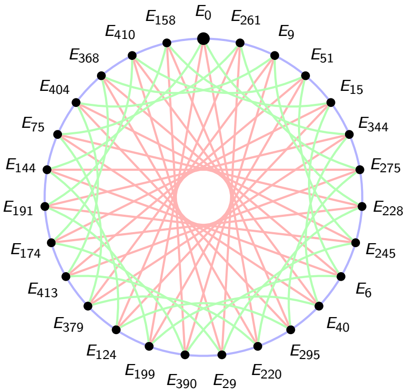


$G_3 \cup G_5 \cup G_7$

Diffie-Hellman with CSIDH

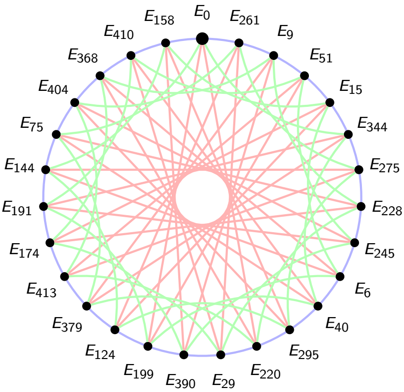
Alice

$a = [+, -, +, -]$



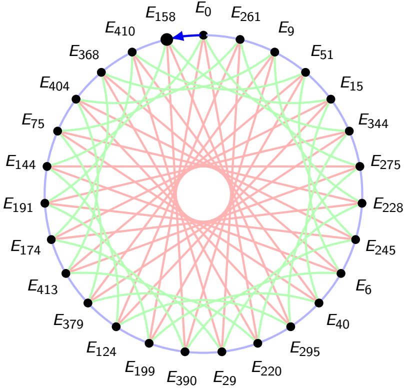
Bob

$b = [+, +, +, -]$



Alice

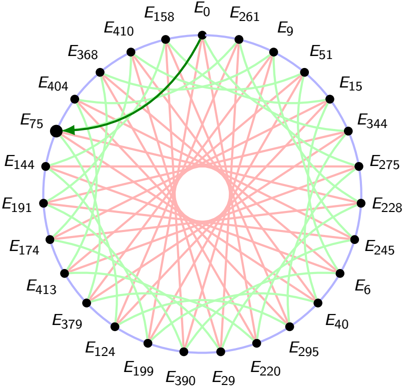
$a = [+, -, +, -]$



$E_{158} = \langle 3, \pi - 1 \rangle * E_0$

Bob

$b = [+, +, +, -]$

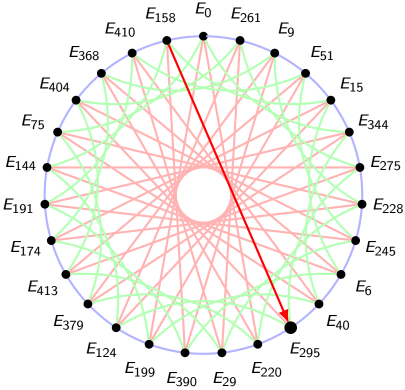


$E_{75} = \langle 7, \pi - 1 \rangle * E_0$

Diffie-Hellman with CSIDH

Alice

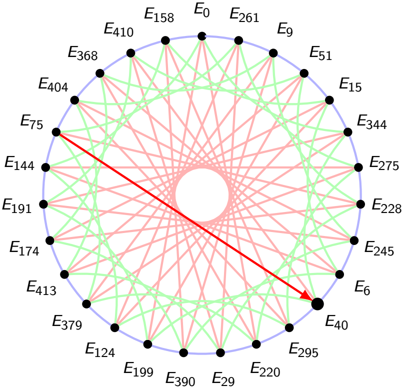
$a = [+, -, +, -]$
$\uparrow$



$$E_{295} = \langle 5, \pi + 1 \rangle * E_{158}$$

Bob

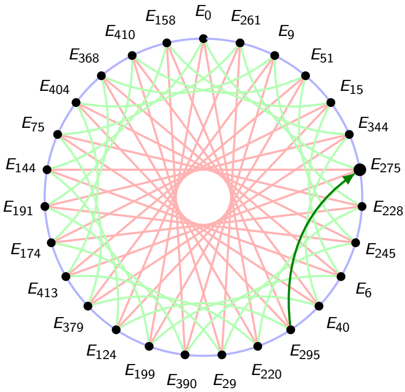
$b = [+, +, +, -]$
$\uparrow$



$$E_{40} = \langle 5, \pi - 1 \rangle * E_{75}$$

Alice

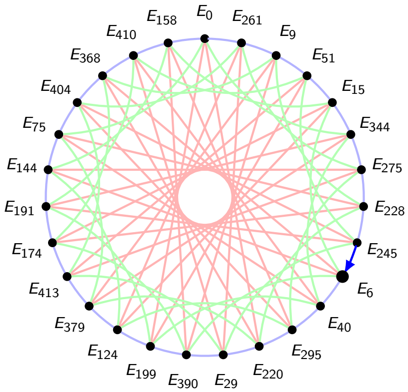
$a = [+, -, +, -]$
$\uparrow$



$E_{275} = \langle 7, \pi - 1 \rangle * E_{295}$

Bob

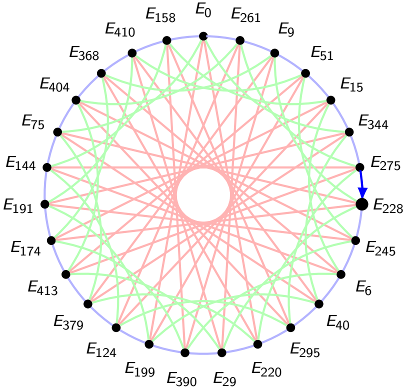
$b = [+, +, +, -]$
$\uparrow$



$E_{6} = \langle 3, \pi - 1 \rangle * E_{245}$

Alice

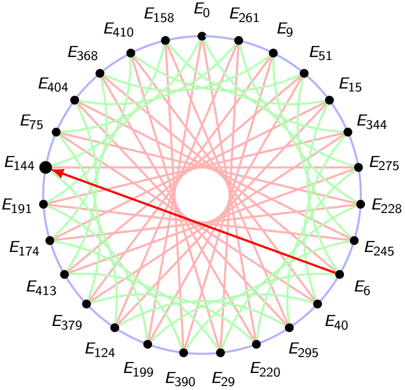
$a = [+, -, +, -]$
$\uparrow$



$E_{228} = \langle 3, \pi + 1 \rangle * E_{275}$

Bob

$b = [+, +, +, -]$
$\uparrow$

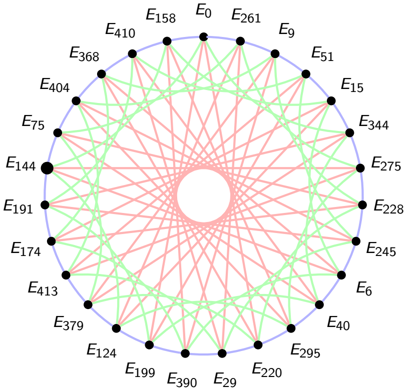


$E_{144} = \langle 5, \pi + 1 \rangle * E_6$

Diffie-Hellman with CSIDH

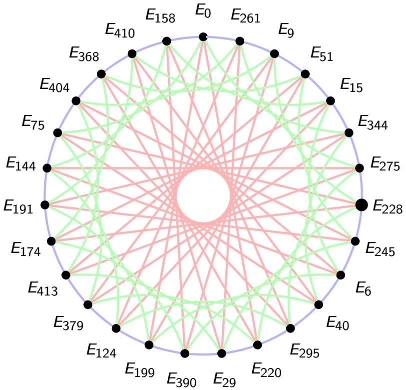
Alice

$a = [+, -, +, -]$



Bob

$b = [+, +, +, -]$

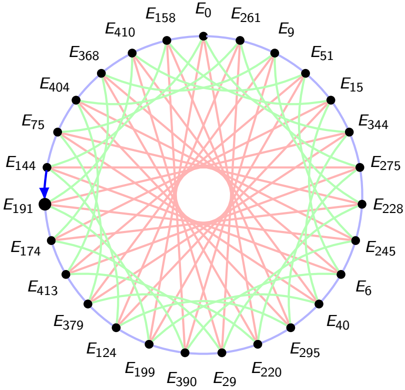


Alice and Bob trade

Diffie-Hellman with CSIDH

Alice

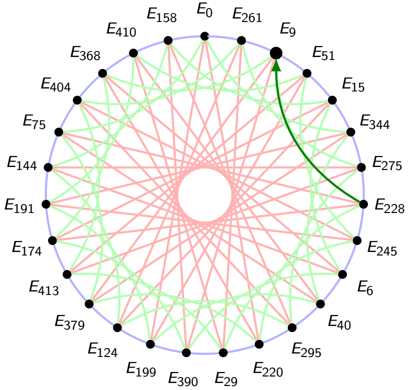
$$a = [+, -, +, -]$$



$$E_{191} = \langle 3, \pi - 1 \rangle * E_{144}$$

Bob

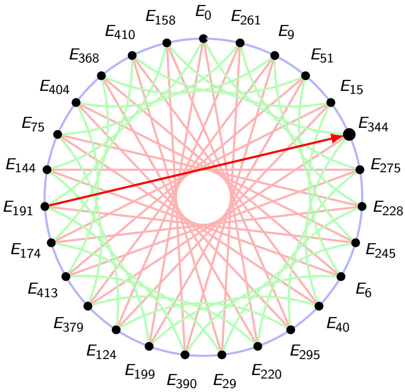
$$b = [+, +, +, -]$$



$$E_9 = \langle 7, \pi - 1 \rangle * E_{228}$$

Alice

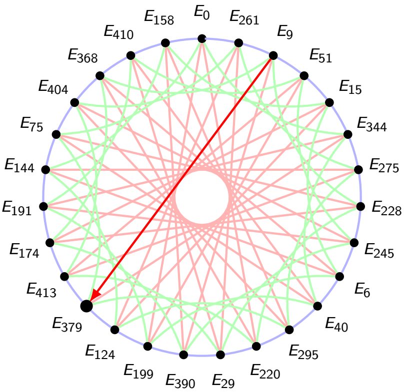
$a = [+, -, +, -]$
$\uparrow$



$$E_{344} = \langle 5, \pi + 1 \rangle * E_{191}$$

Bob

$b = [+, +, +, -]$
$\uparrow$

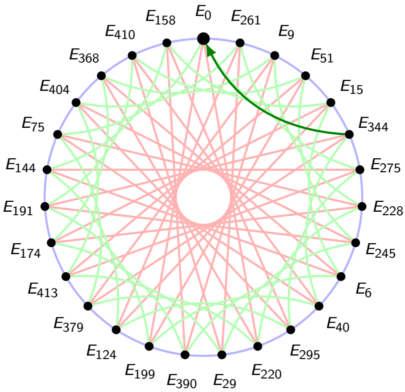


$$E_{379} = \langle 5, \pi - 1 \rangle * E_9$$

Diffie-Hellman with CSIDH

Alice

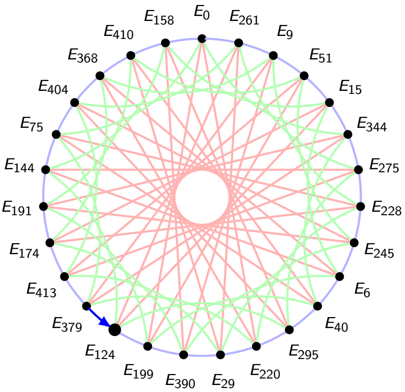
$a = [+, -, +, -]$
$\uparrow$



$E_0 = \langle 7, \pi - 1 \rangle * E_{344}$

Bob

$b = [+, +, +, -]$
$\uparrow$



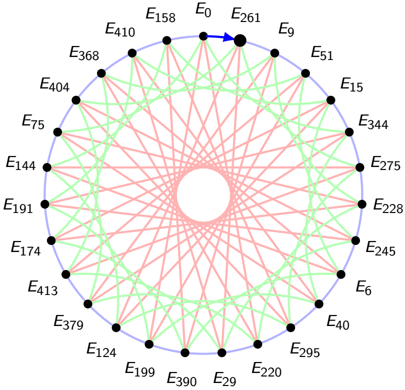
$E_{124} = \langle 3, \pi - 1 \rangle * E_{379}$

Diffie-Hellman with CSIDH

Alice

$a = [+, -, +, -]$

$\uparrow$

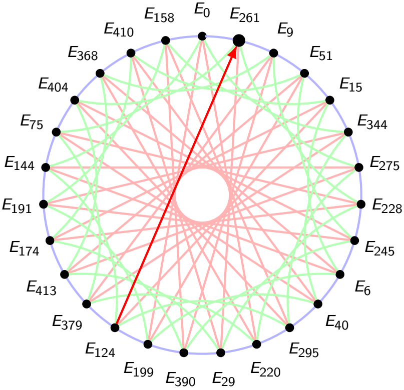


$$E_{261} = \langle 3, \pi + 1 \rangle * E_0$$

Bob

$b = [+, +, +, -]$

$\uparrow$

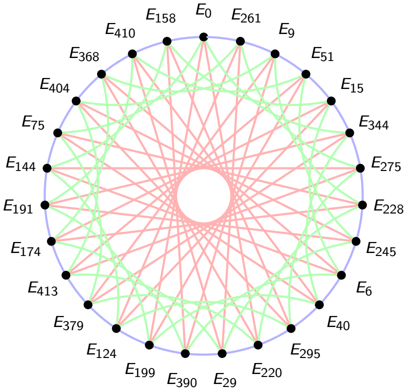


$$E_{261} = \langle 5, \pi + 1 \rangle * E_{124}$$

Diffie-Hellman with CSIDH

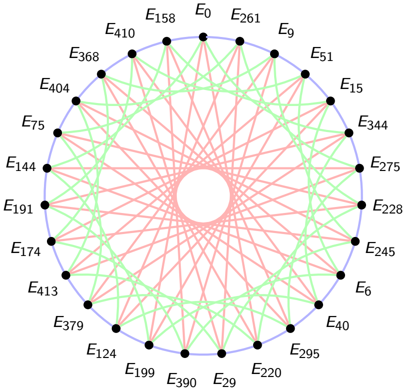
Alice

$a = [+, -, +, -]$



Bob

$b = [+, +, +, -]$



The shared secret key is E_{261}

Thank you!