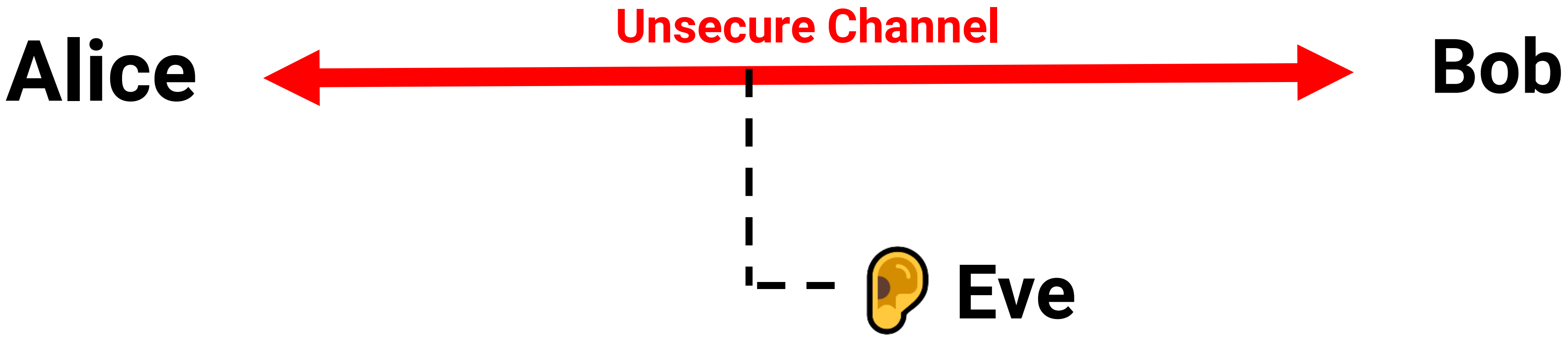
Cryptanalysis of Isogeny-based Cryptography

James Clements

1. Motivation
2. Intro to Isogenies
3. Breaking Decisional DDH
4. Generalizations

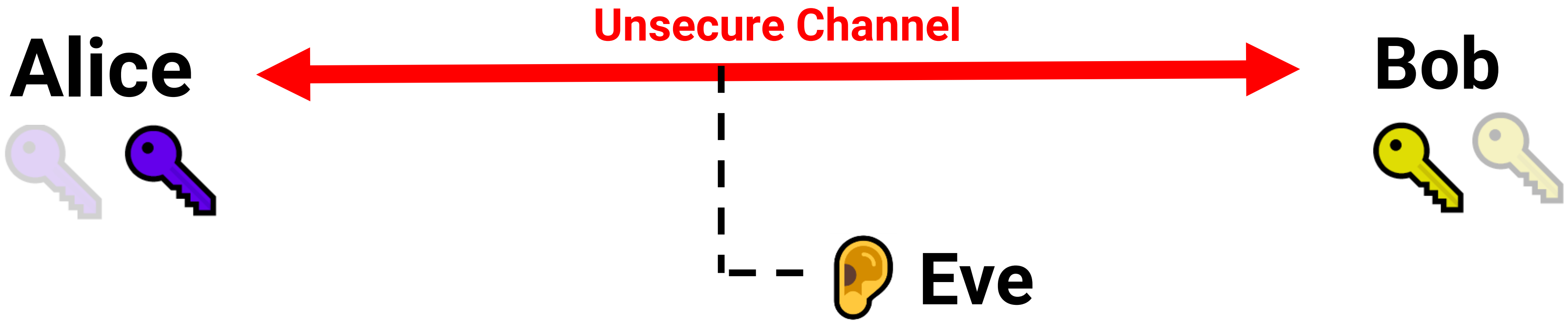
1. Motivation

Public Key Cryptography – Key Exchanges



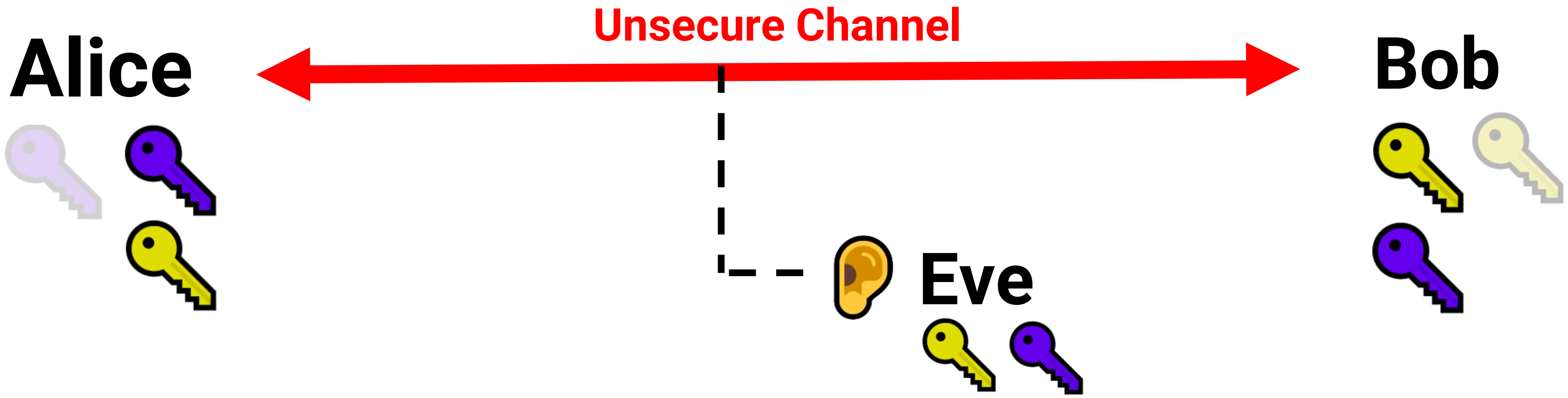
Alice wants a way to communicate with Bob securely.

Public Key Cryptography – Key Exchanges



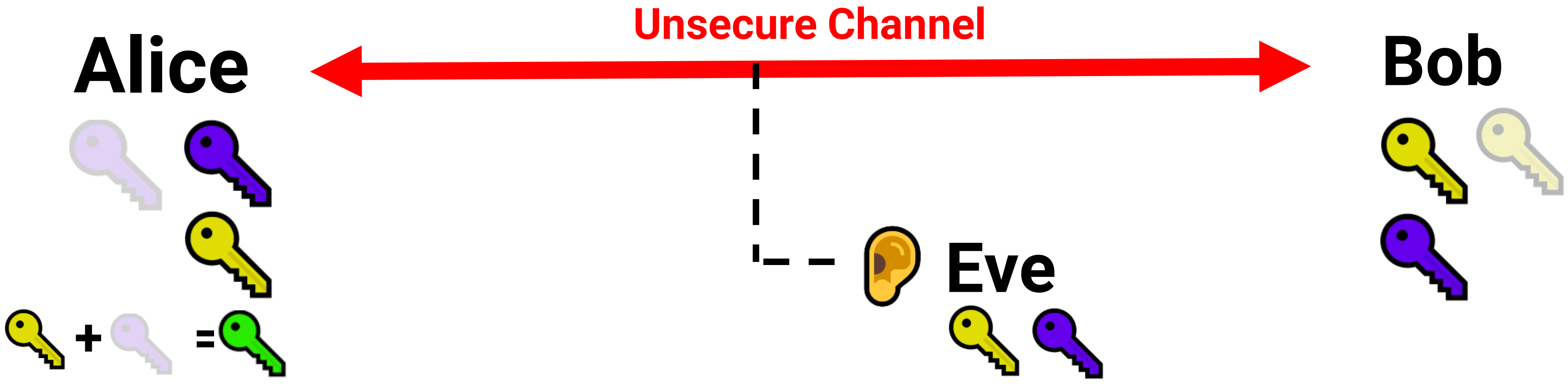
They each have a public key and private key.

Public Key Cryptography – Key Exchanges



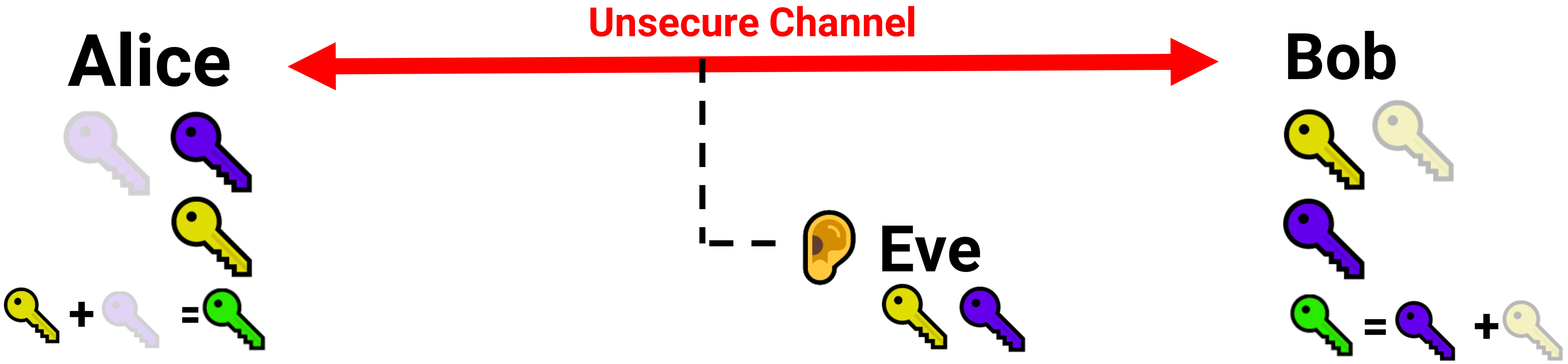
They send their public keys to each other.

Public Key Cryptography – Key Exchanges



Alice uses her private key and Bob’s public key to derive a secret

Public Key Cryptography – Key Exchanges



Unsecure Channel

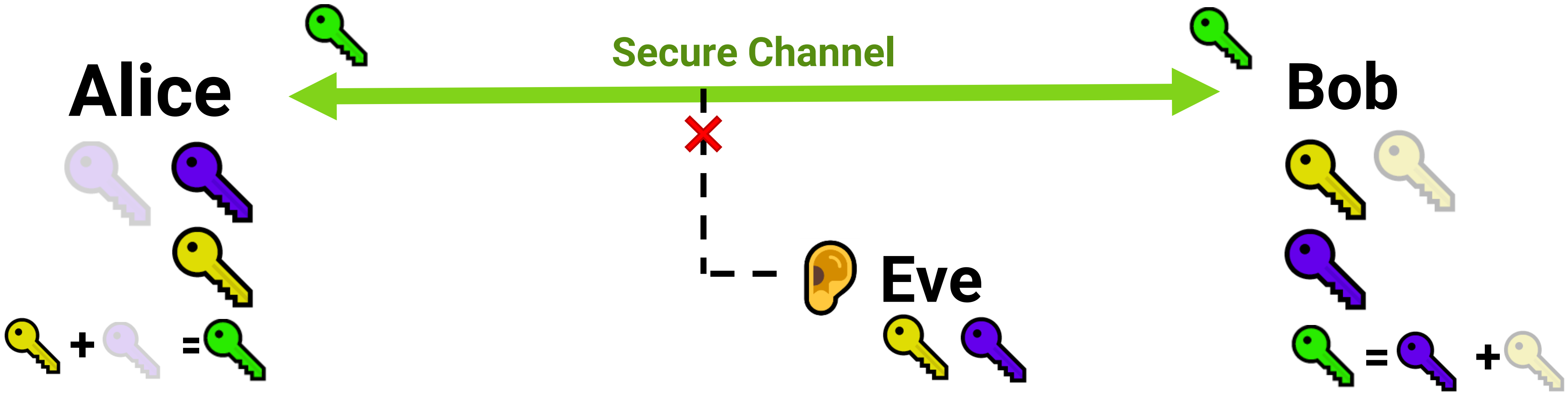
Alice

Bob

Eve

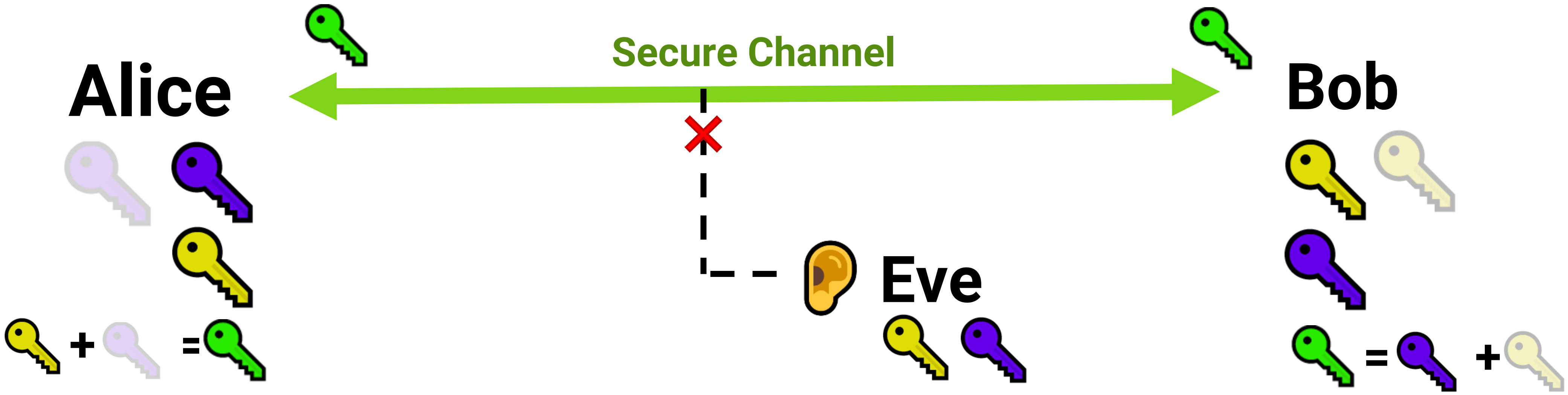
Similarly, Bob uses his private key and Alice’s public key to derive a secret.

Public Key Cryptography – Key Exchanges



Alice and Bob may encrypt messages between them with this secret key.

Public Key Cryptography – Key Exchanges



Eve sees public keys 🔑🔑.

But it must be computationally hard for her to compute the shared secret 🔑.

Hard Problems

Eve sees public keys 🔑🔑.

But it must be computationally hard for her to compute the shared secret 🔑.

Hard Problems

Eve sees public keys 🔑🔑.

But it must be computationally hard for her to compute the shared secret 🔑.

Integer Factorisation Problem

Given an integer N which is the product of two primes $(N = p \times q)$
Find p and q

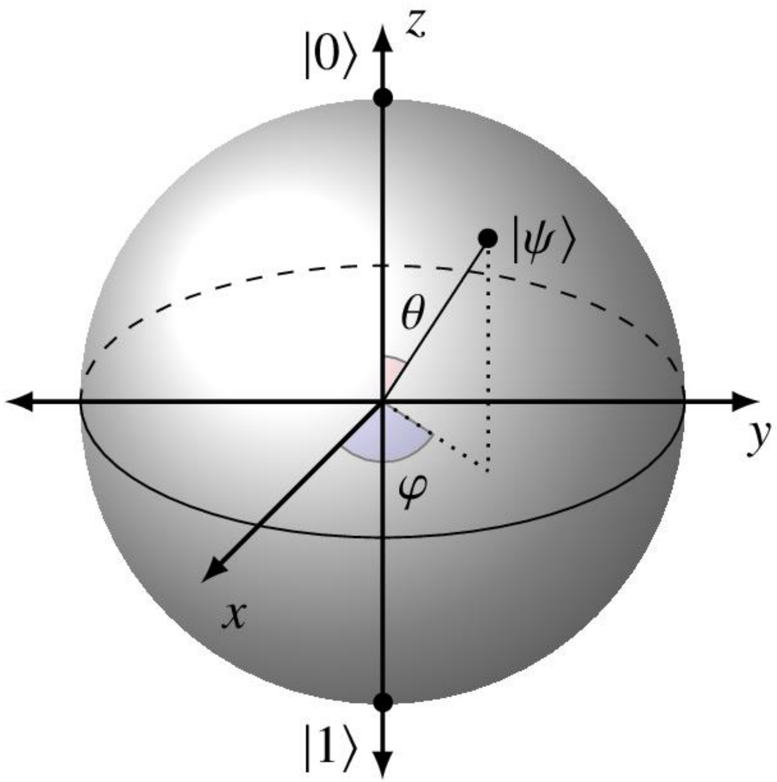
(RSA)

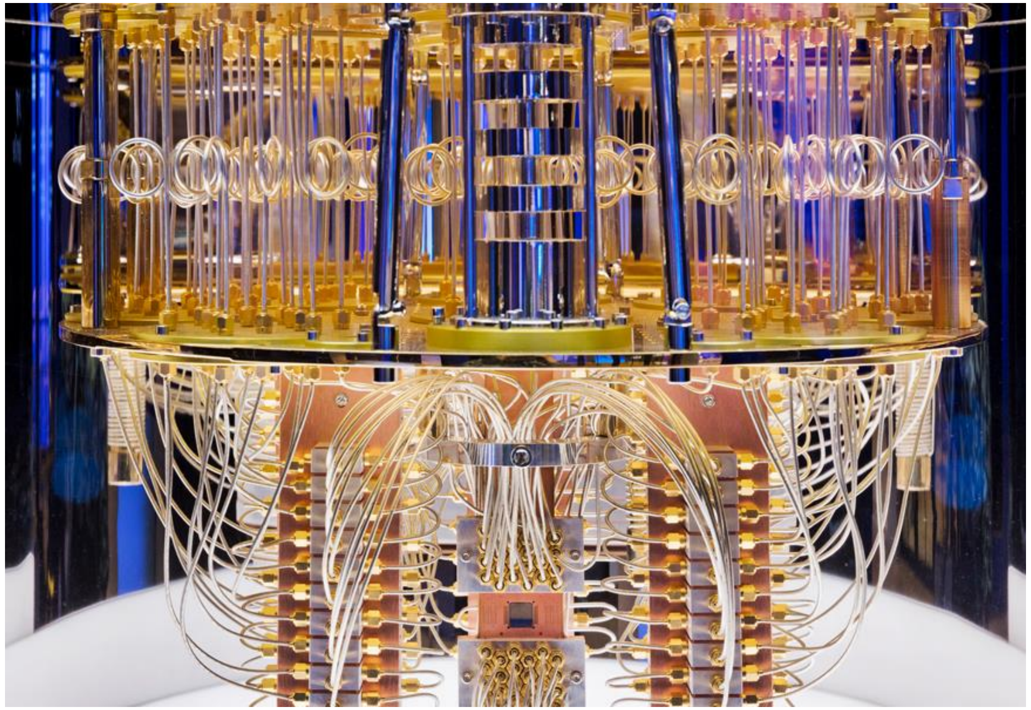
Discrete Logarithm Problem

Given a number N which is a number g to a power a $(N = g^a)$
Find a

(Diffie-Hellman / ECC)

Quantum Computers 😵‍💫





Hard Problems

Eve sees public keys 🔑🔑.

But it must be computationally hard for her to compute the shared secret 🔑.

Integer Factorisation Problem

Given an integer N which is the product of two primes $(N = p \times q)$
Find p and q

(RSA)

Discrete Logarithm Problem

Given a number N which is a number g to a power a $(N = g^a)$
Find a

(Diffie-Hellman / ECC)

Hard Problems

Eve sees public keys 🔑🔑.
But it must be computationally hard for her to compute the shared secret 🔑.

~~Integer Fa torisatio Problem~~

~~Given an inte hich is the~~
~~product of two s $(N = p \times q)$~~
~~Fi p an~~

(RSA)

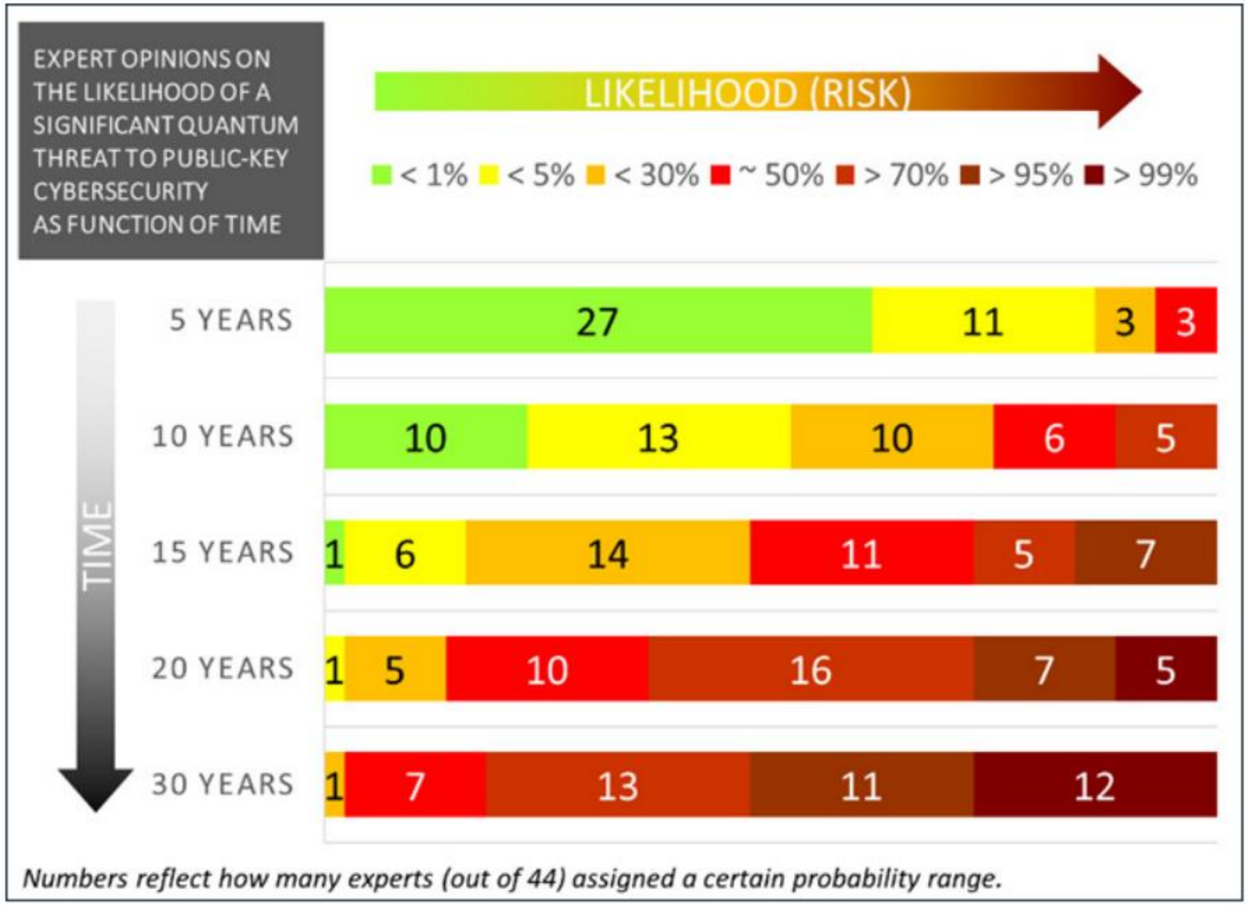
~~Discrete ogarithm Problem~~

~~Given a nu which is a~~
~~number g to r a $(N = g^a)$~~
~~ind a~~

(Diffie-Hellman / ECC)

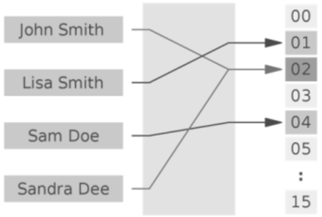
We need new hard problems ...

Timeline ⌚

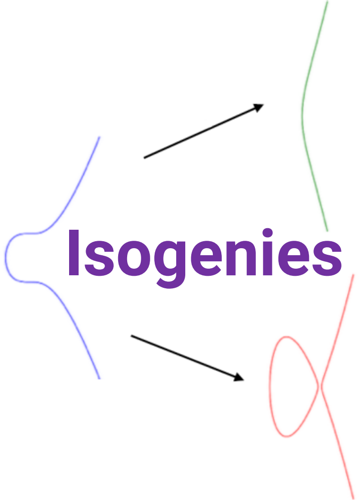


Numbers reflect how many experts (out of 44) assigned a certain probability range.

Source: EvolutionQ: Quantum Threat Timeline Report 2020



Hash Functions

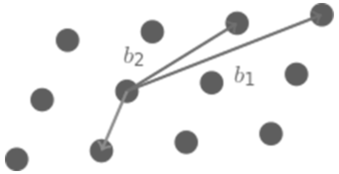


Isogenies

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m, \end{aligned}$$

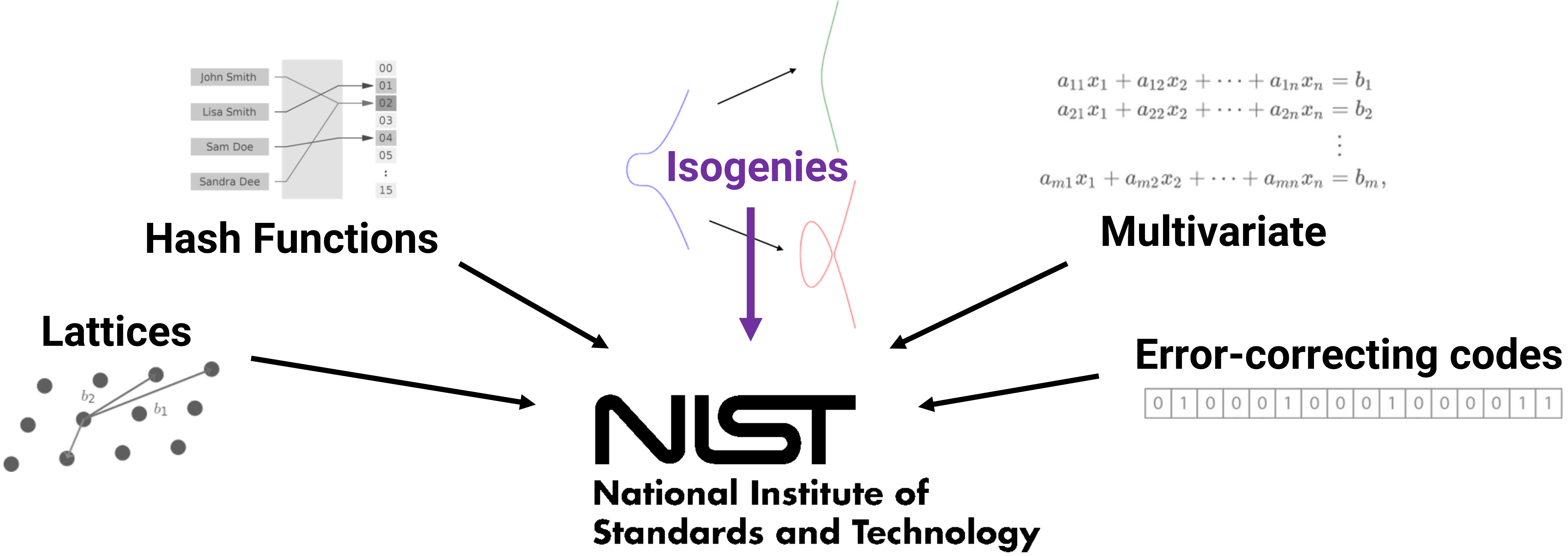
Multivariate

Lattices



Error-correcting codes

0	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1



Hash Functions

Isogenies

Multivariate

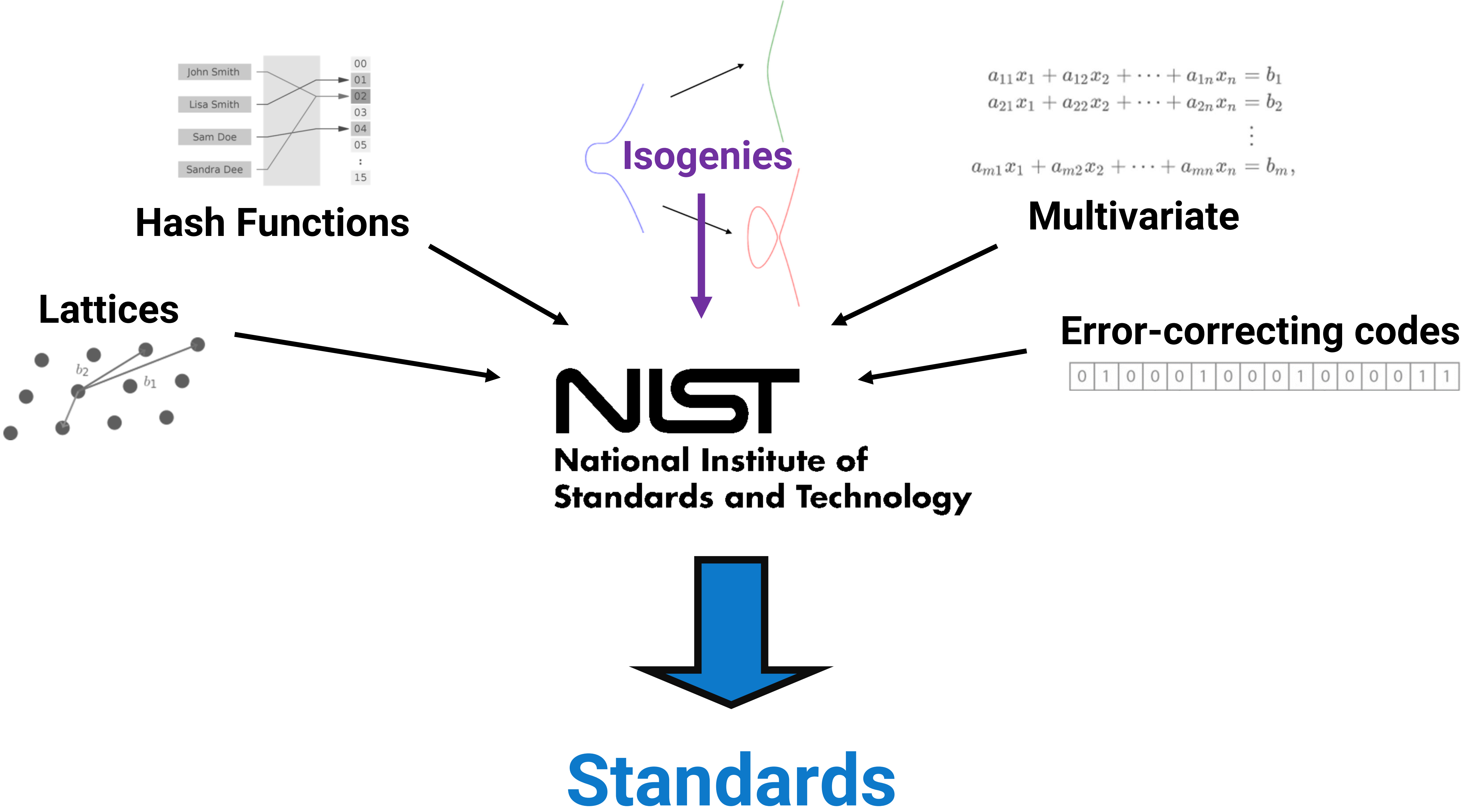
$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m, \end{aligned}$$

Lattices

Error-correcting codes

0	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1

NIST
National Institute of
Standards and Technology



Hash Functions

Isogenies

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\
&\vdots \\
a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m,
\end{aligned}
$$

Multivariate

Lattices

Error-correcting codes

0	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1

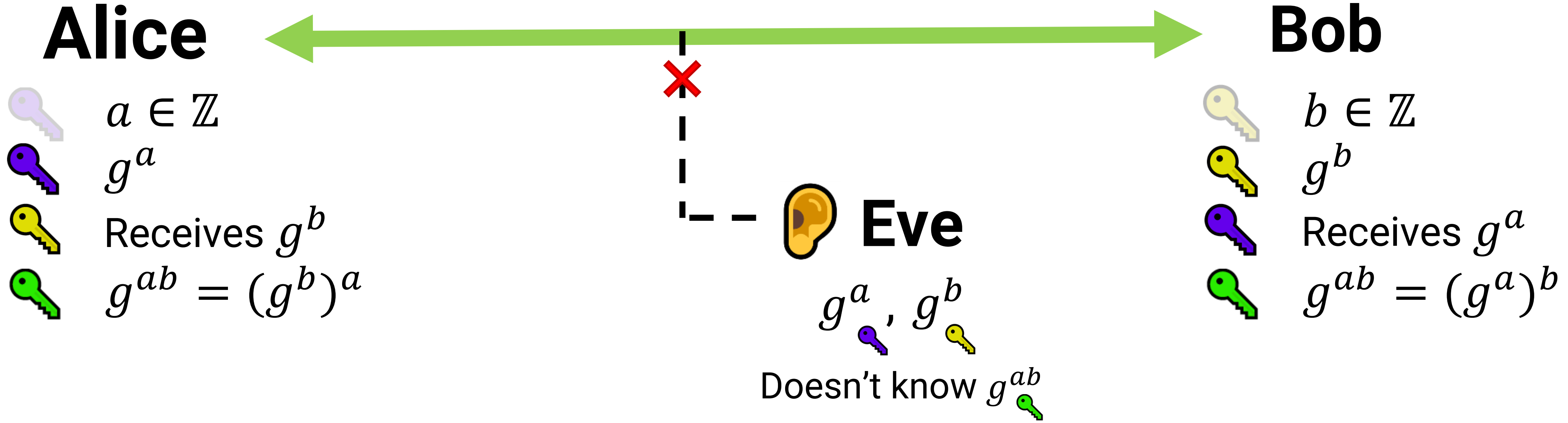
NIST
National Institute of
Standards and Technology

Standards

2. Intro to Isogenies

Diffie Hellman Key Exchange

g is a known generator of $\mathbb{F}_p^*$



Alice

$a \in \mathbb{Z}$

g^a

Receives g^b

$g^{ab} = (g^b)^a$

Bob

$b \in \mathbb{Z}$

g^b

Receives g^a

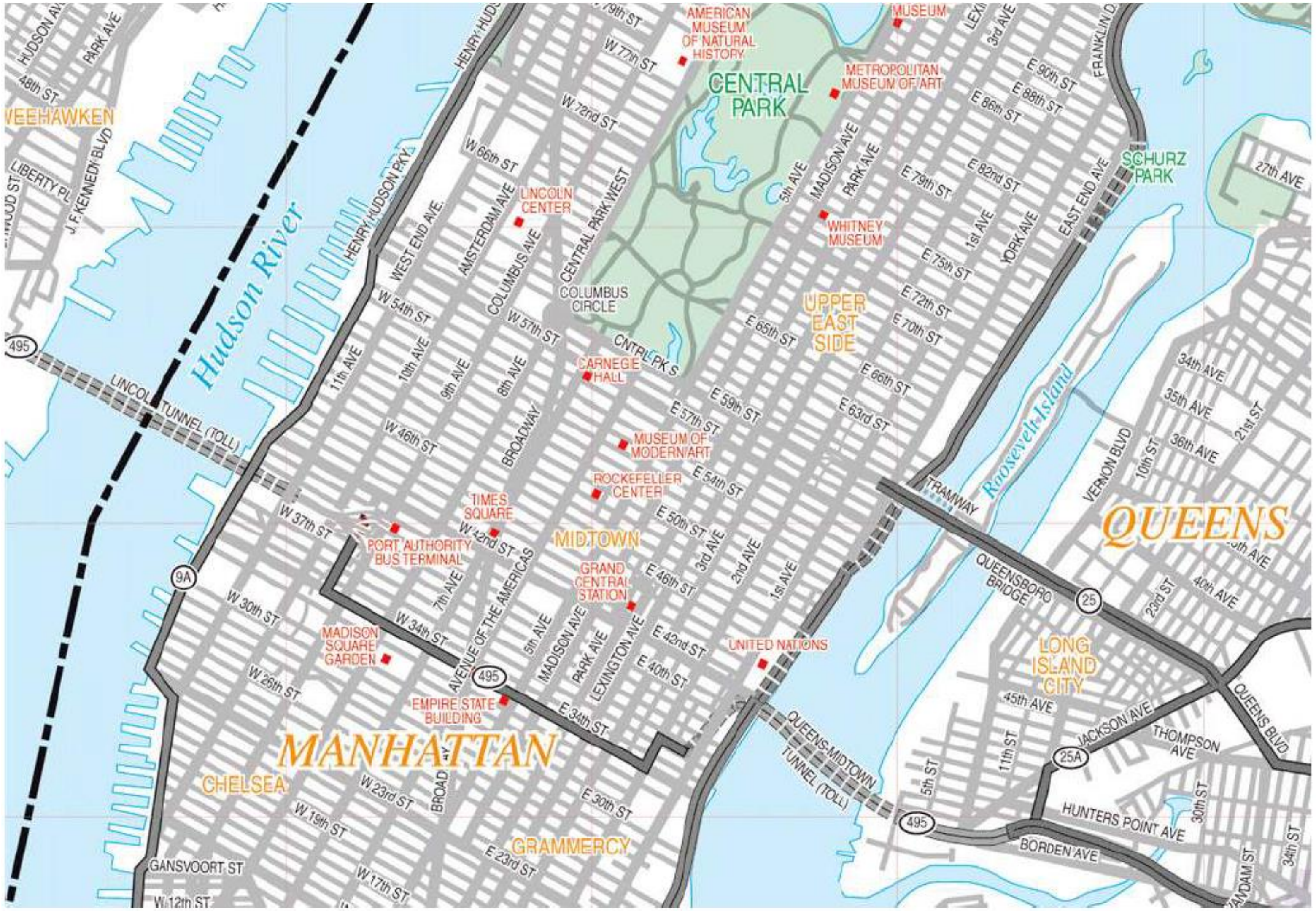
$g^{ab} = (g^a)^b$

Eve

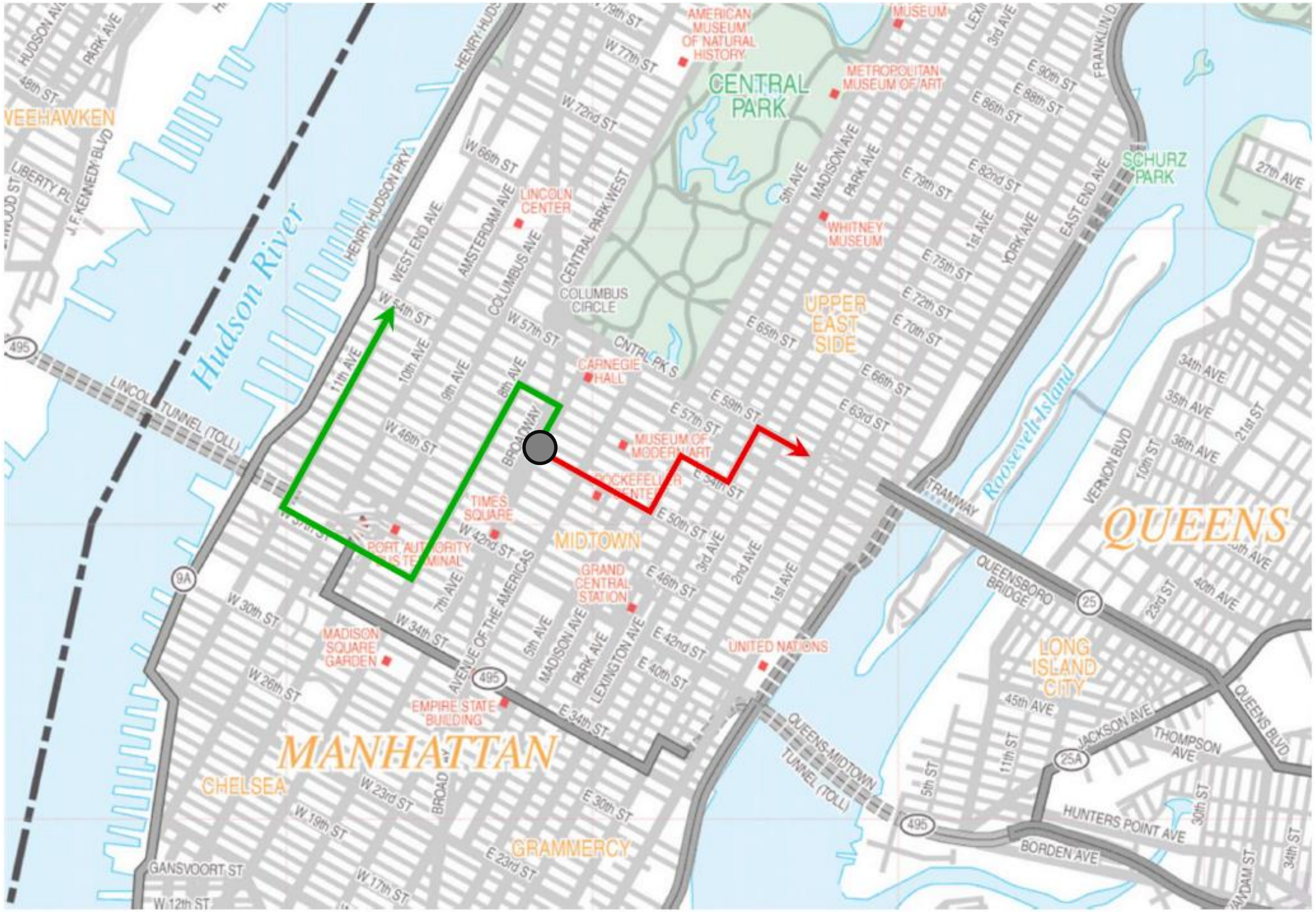
g^a, g^b

Doesn't know g^{ab}

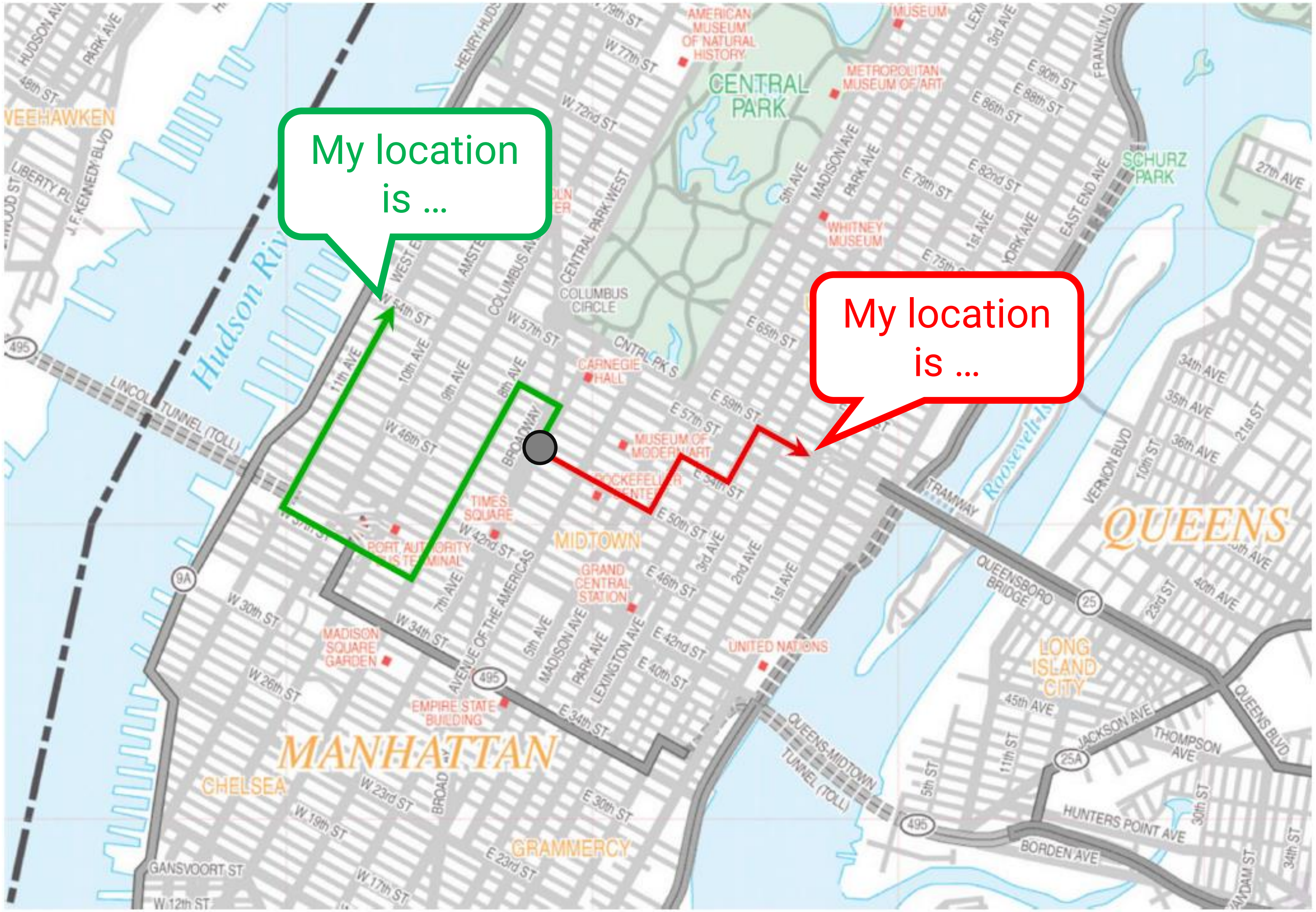
Graph Walking Diffie-Hellman



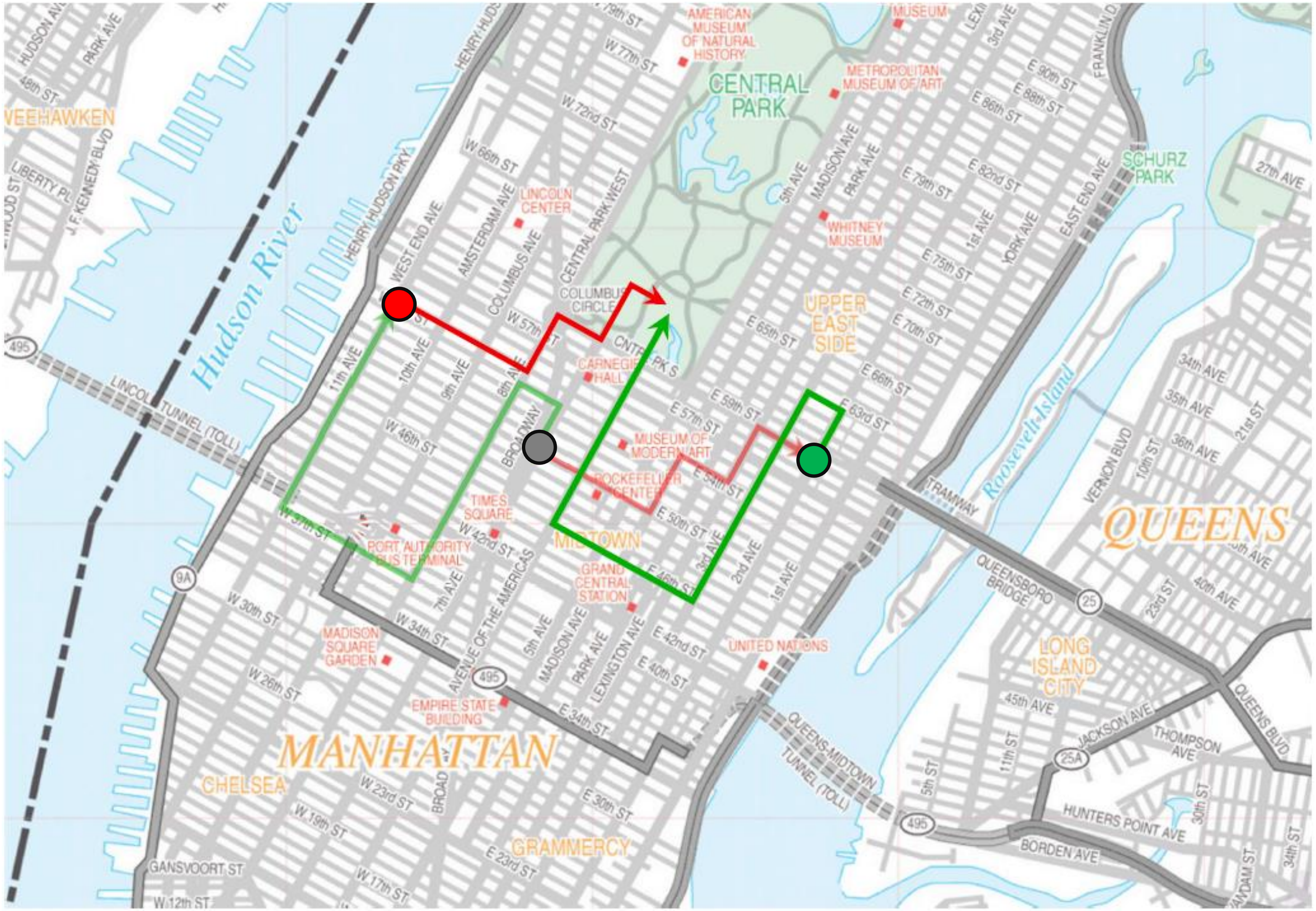
Graph Walking Diffie-Hellman



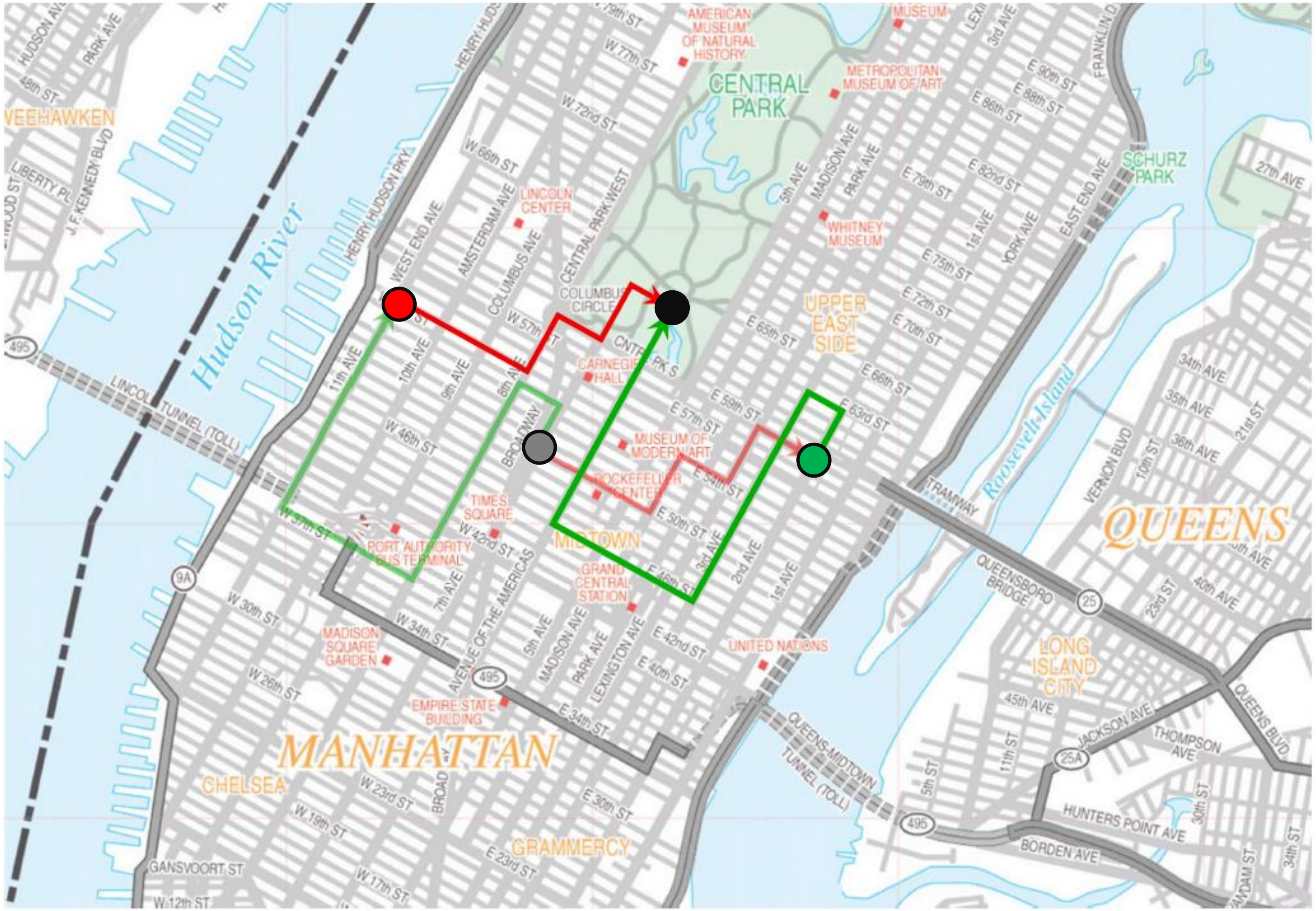
Graph Walking Diffie-Hellman



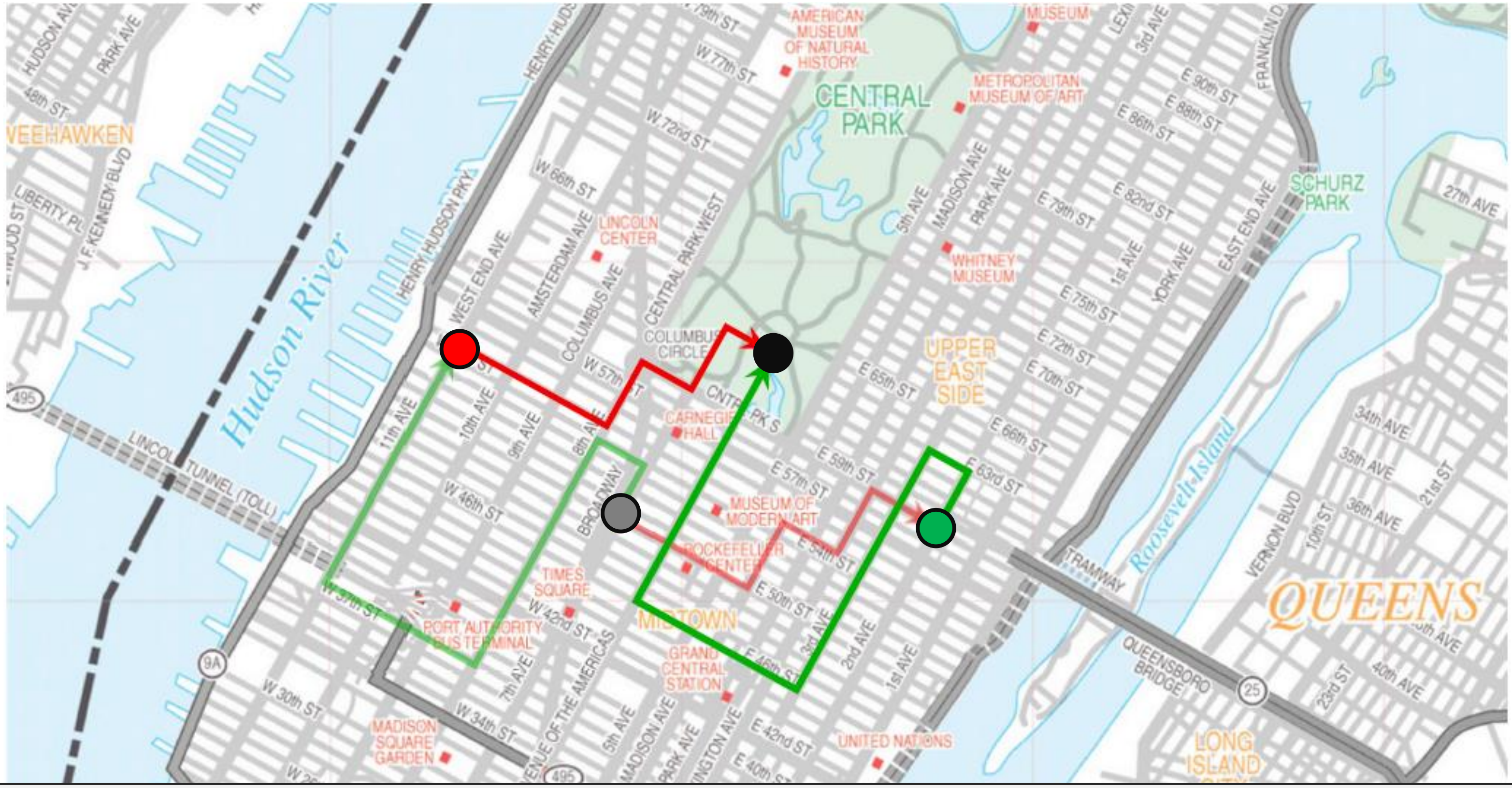
Graph Walking Diffie-Hellman



Graph Walking Diffie-Hellman



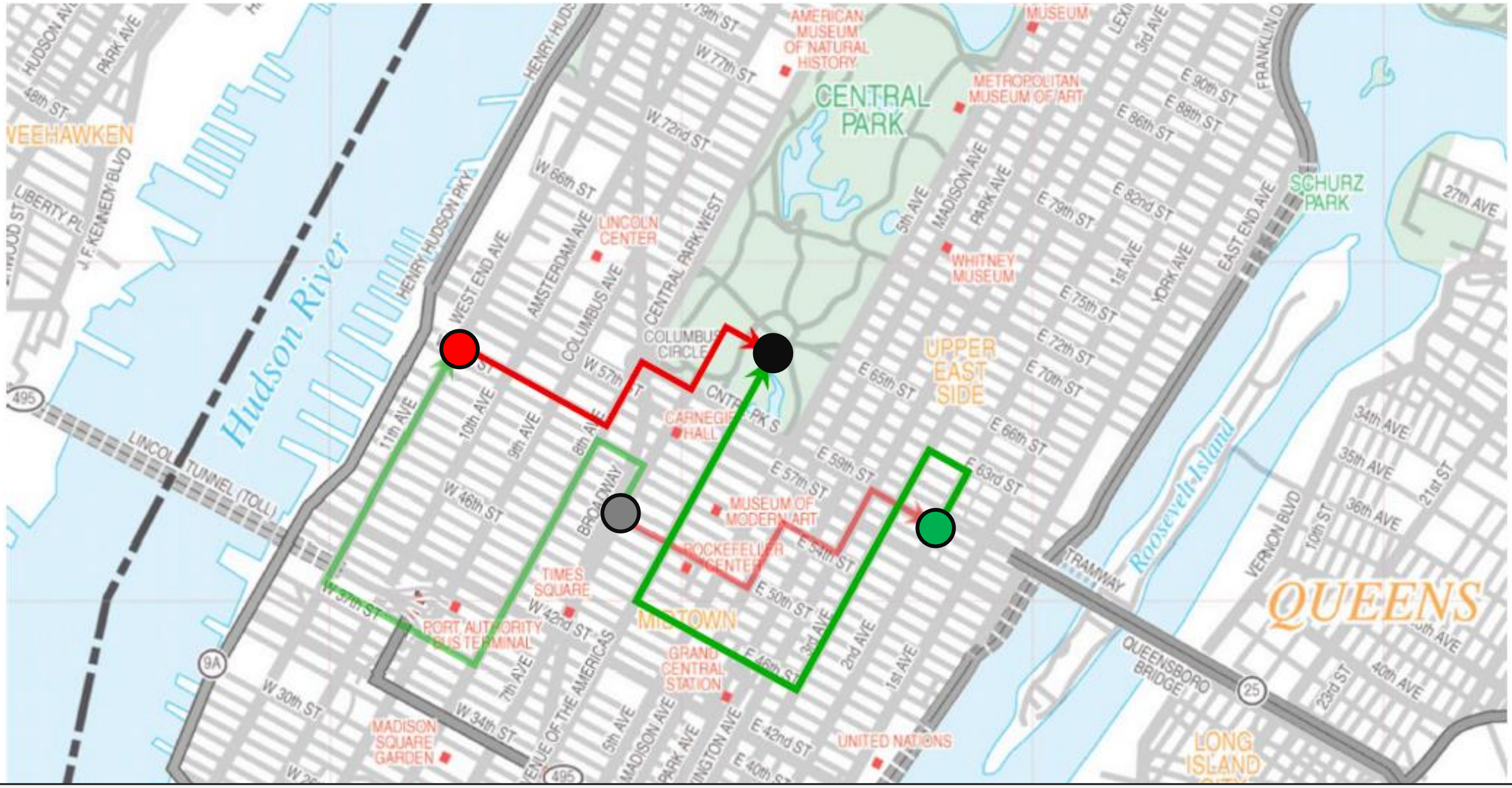
Graph Walking Diffie-Hellman



Eve sees Alice’s point 🟢, and Bob’s point 🔴. She knows where they start ◍.

Shouldn’t be able to find the secret point ⚫ they end up.

Graph Walking Diffie-Hellman



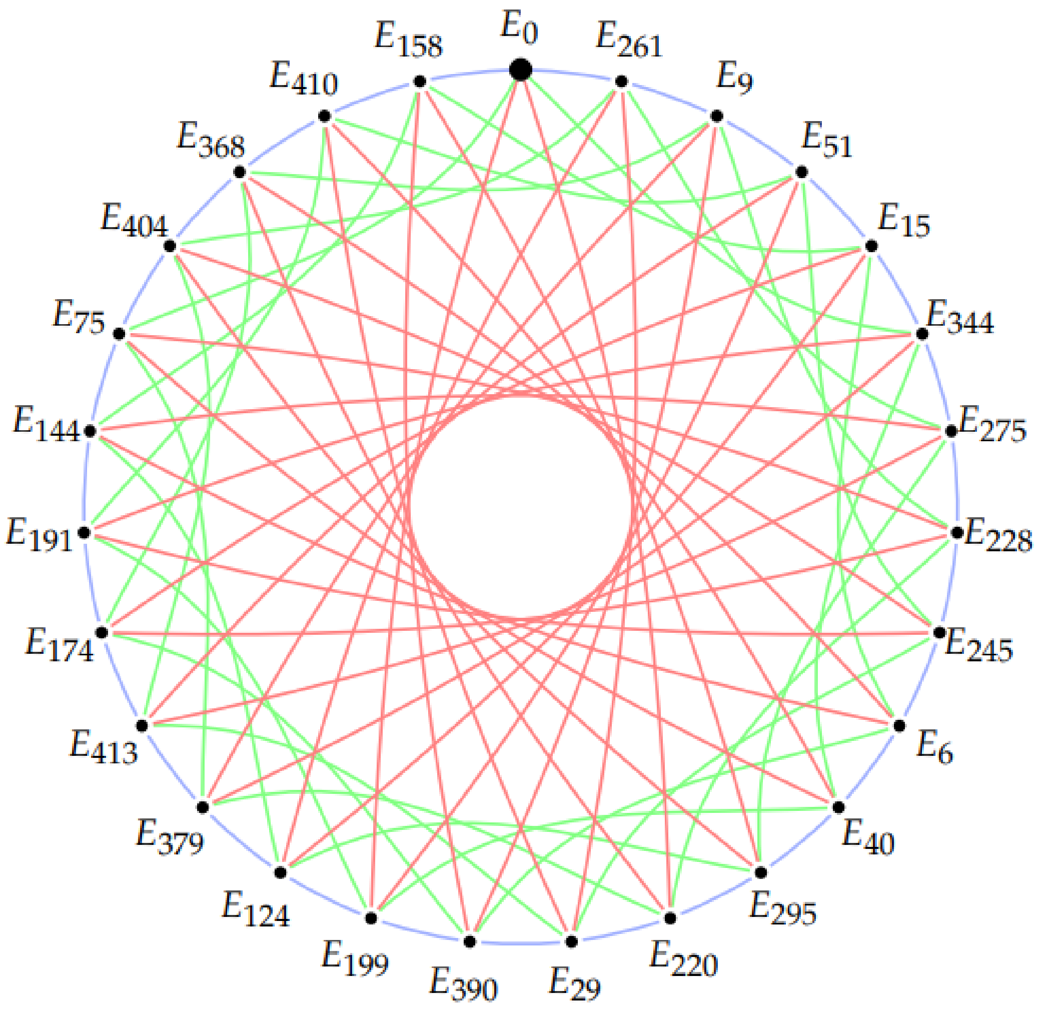
Eve sees Alice’s point 🟢, and Bob’s point 🔴. She knows where they start ⚪.

Shouldn’t be able to find the secret point ⚫ they end up.

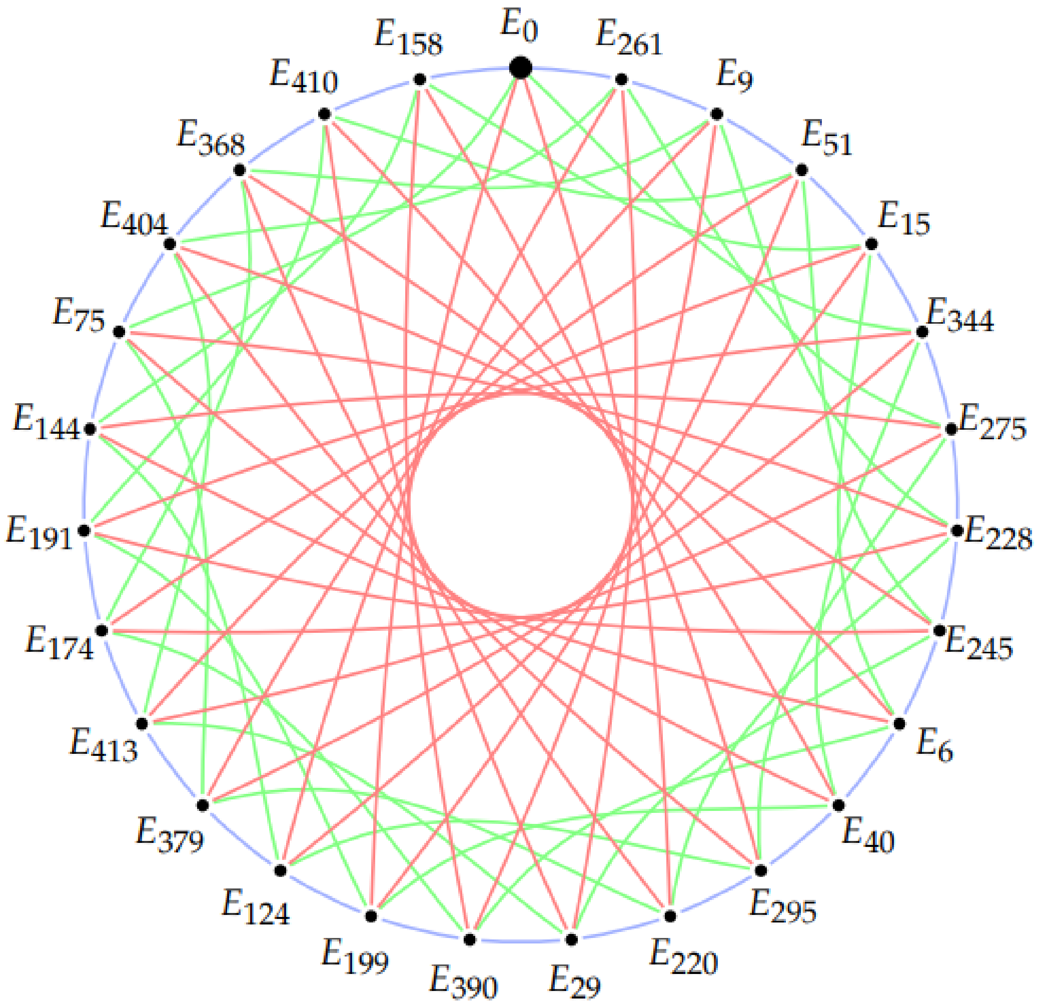
Not a hard problem

Not secure

But for some graphs this works!

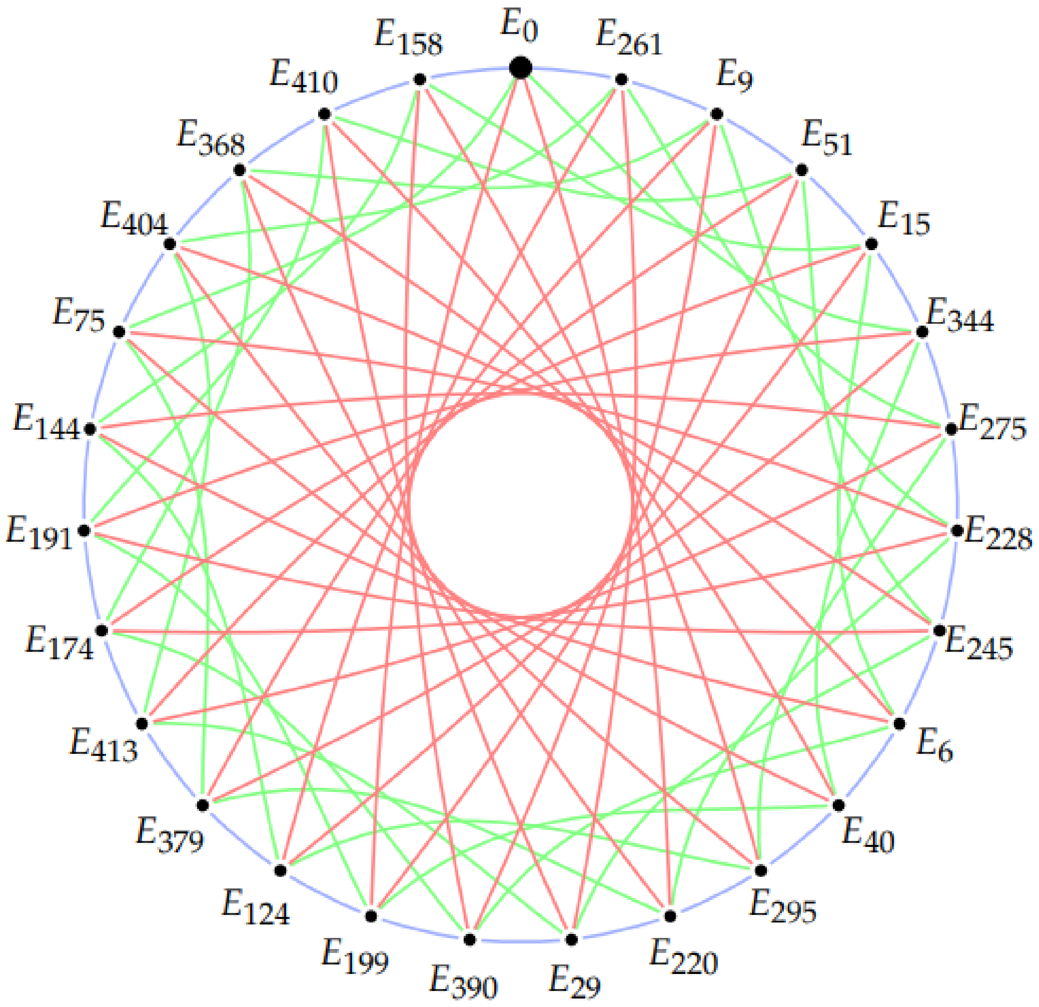


But for some graphs this works!



We need:

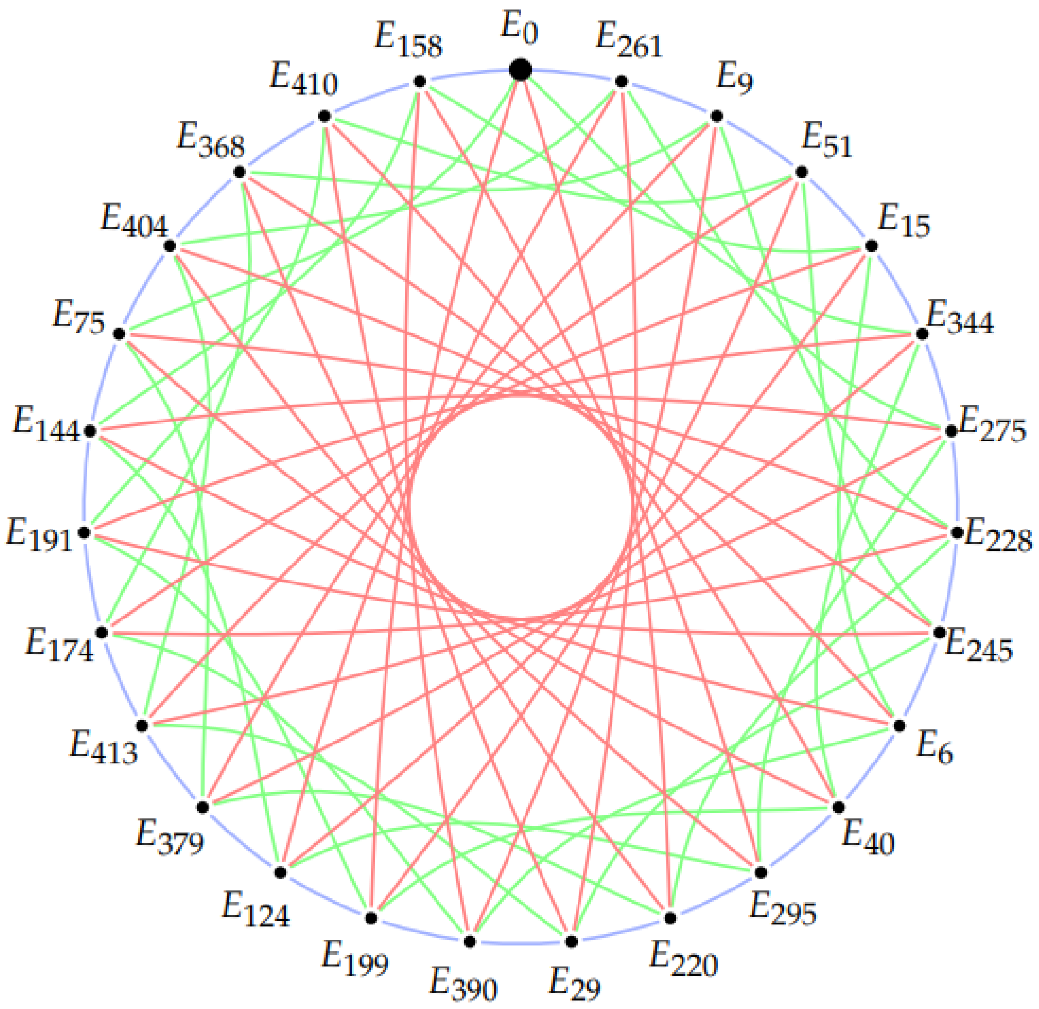
But for some graphs this works!



We need:

- Very large graphs

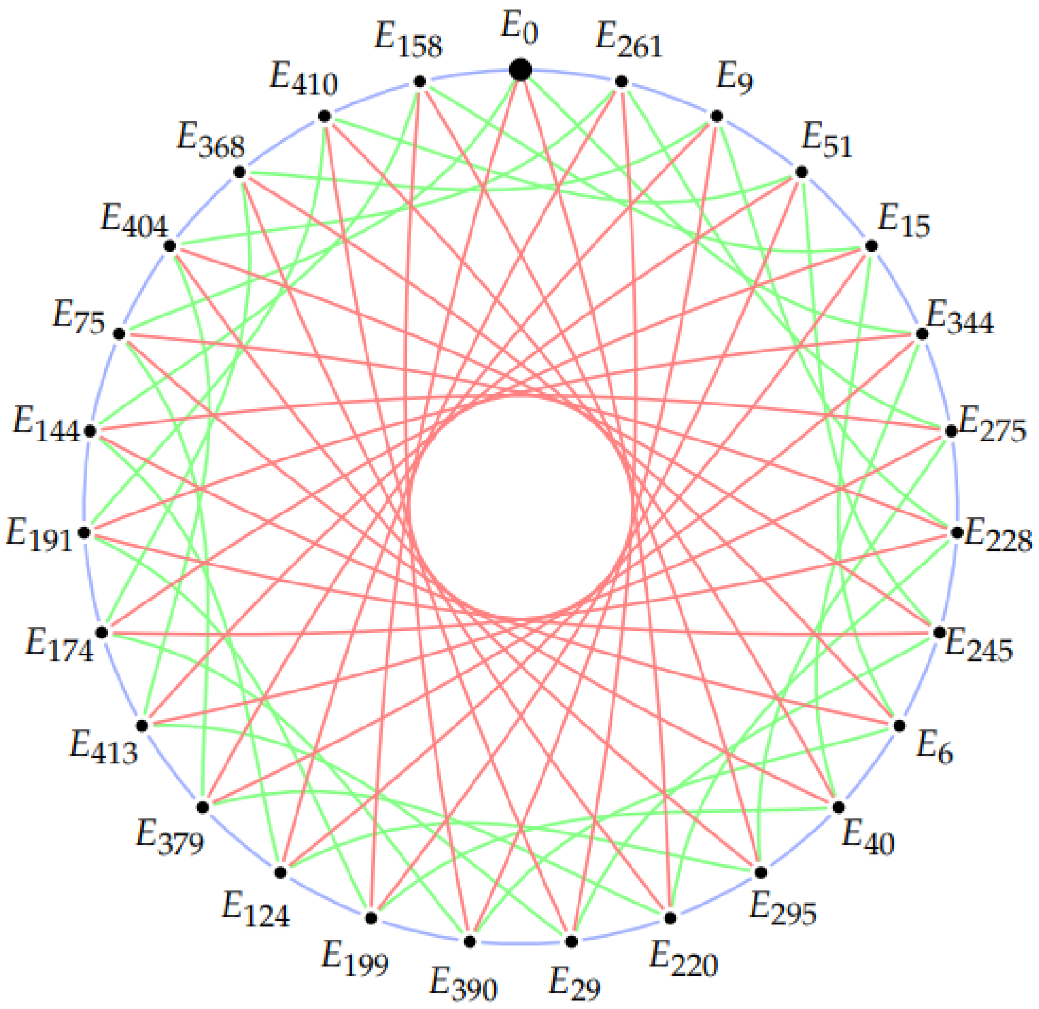
But for some graphs this works!



We need:

- Very large graphs
- A way of traversing the graph, without storing/computing the whole thing

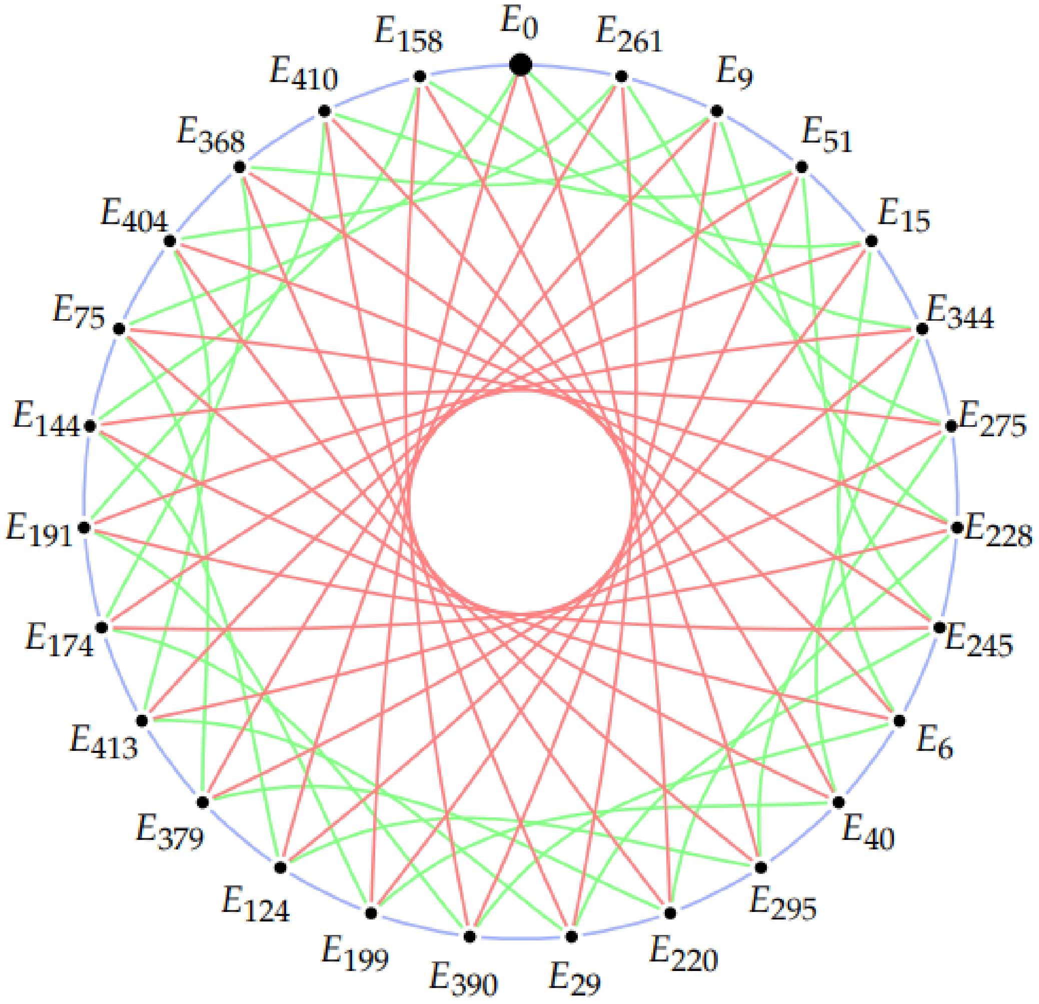
But for some graphs this works!



We need:

- Very large graphs
- A way of traversing the graph, without storing/computing the whole thing
- Vertex labels to look random

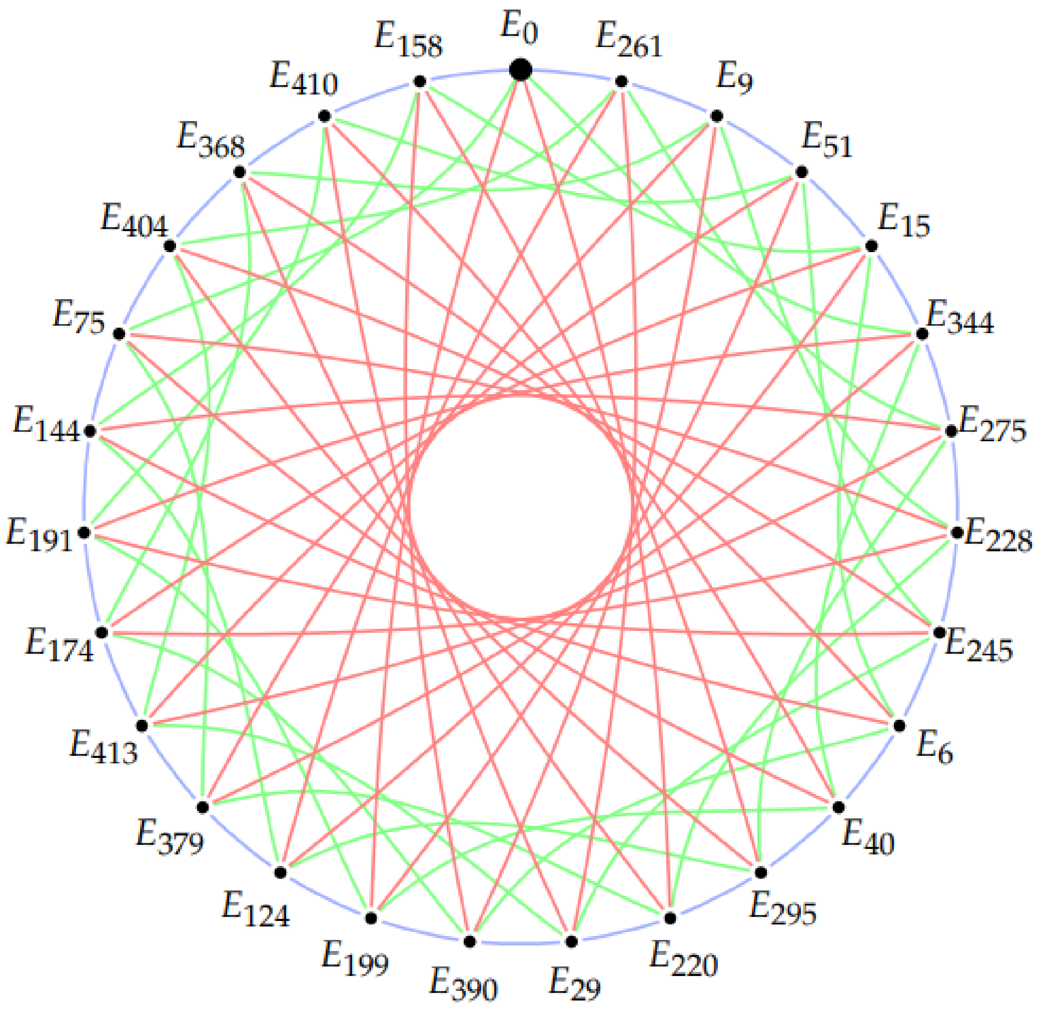
But for some graphs this works!



We need:

- Very large graphs
- A way of traversing the graph, without storing/computing the whole thing
- Vertex labels to look random
- Taking a short walk gets you somewhere uniformly random

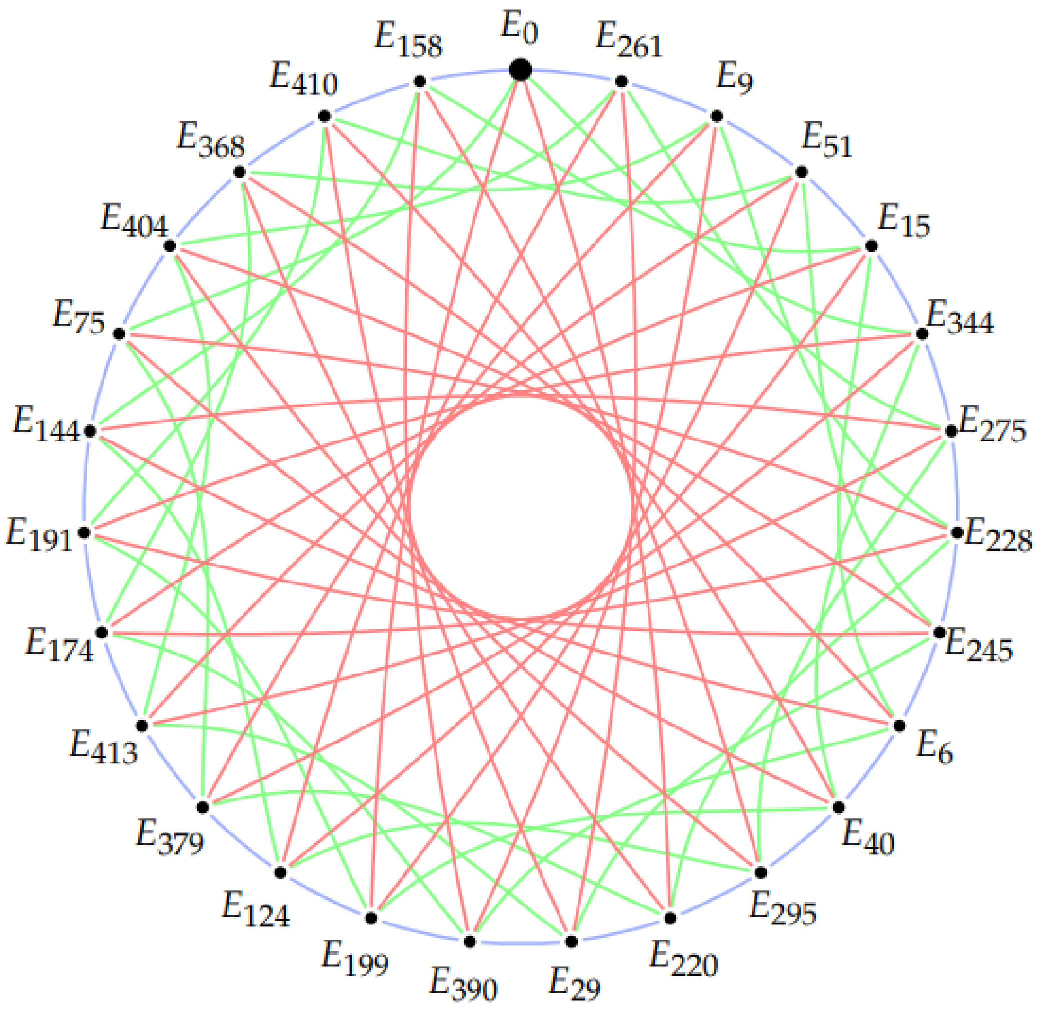
But for some graphs this works!



We need:

- Very large graphs
- A way of traversing the graph, without storing/computing the whole thing
- Vertex labels to look random
- Taking a short walk gets you somewhere uniformly random
- It’s hard to find a walk between two given verticies

But for some graphs this works!



We need:

- Very large graphs
- A way of traversing the graph, without storing/computing the whole thing
- Vertex labels to look random
- Taking a short walk gets you somewhere uniformly random
- It's hard to find a walk between two given verticies

… isogenies!!

Isogenies

- An **elliptic curve** is set of points (x, y) satisfying an equation:

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

Isogenies

- An **elliptic curve** is set of points (x, y) satisfying an equation:

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

- Over a field F, the set of points on an elliptic curve form an **algebraic group**.

Isogenies

- An **elliptic curve** is set of points (x, y) satisfying an equation:

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

- Over a field F, the set of points on an elliptic curve form an **algebraic group**.

- An **isogeny** is a non-zero rational map between two elliptic curves that preserves the group structure. $\varphi : E \to E'$

Isogenies

- An **elliptic curve** is set of points (x, y) satisfying an equation:

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

- Over a field F, the set of points on an elliptic curve form an **algebraic group**.

- An **isogeny** is a non-zero rational map between two elliptic curves that preserves the group structure. $\varphi : E \to E'$

- The **degree** of an isogeny is the size of it's kernel, i.e. the number of points (x, y) on E that get mapped to the identity on E'

Isogenies

Example:

Isogenies

Example:

Let $p = 419$, and E_1, E_2 be elliptic curves over $\mathbb{F}_p$ defined by:

$$E_1\colon\ y^2 = x^3 + 51x^2 + x \qquad E_2\colon\ y^2 = x^3 + 9x^2 + x$$

Isogenies

Example:

Let $p = 419$, and E_1, E_2 be elliptic curves over $\mathbb{F}_p$ defined by:

$$E_1\colon\ y^2 = x^3 + 51x^2 + x \qquad E_2\colon\ y^2 = x^3 + 9x^2 + x$$

Then the following map is an isogeny:

$$\varphi : E_1 \to E_2$$

$$\varphi :\ (x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, y\frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3}\right)$$

Isogeny Graphs

Isogeny Graphs

- Two elliptic curves which are isomorphic are said to be in the same **isomorphism class.**

Isogeny Graphs

- Two elliptic curves which are isomorphic are said to be in the same **isomorphism class.**
- We can think of isogenies acting on isomorphism classes.

  Mapping one isomorphism class to another isomorphism class.

Isogeny Graphs

- Two elliptic curves which are isomorphic are said to be in the same **isomorphism class.**
- We can think of isogenies acting on isomorphism classes.

  Mapping one isomorphism class to another isomorphism class.

- Every isomorphism class has a **j-invariant.** The same for all curves in the class. For a curve in form $y^2 = x^3 + ax + b$:

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

Isogeny Graphs

- A **k-isogeny graph** is a graph where:

  Vertices = isomorphism classes of elliptic curves (labeled by j-invariants)

  Edges = degree k isogenies (and their duals) between classes of elliptic curves over $\mathbb{F}_{p^n}$

Isogeny Graphs

- A **k-isogeny graph** is a graph where:

  Vertices = isomorphism classes of elliptic curves (labeled by j-invariants)

  Edges = degree k isogenies (and their duals) between classes of elliptic curves over $\mathbb{F}_{p^n}$

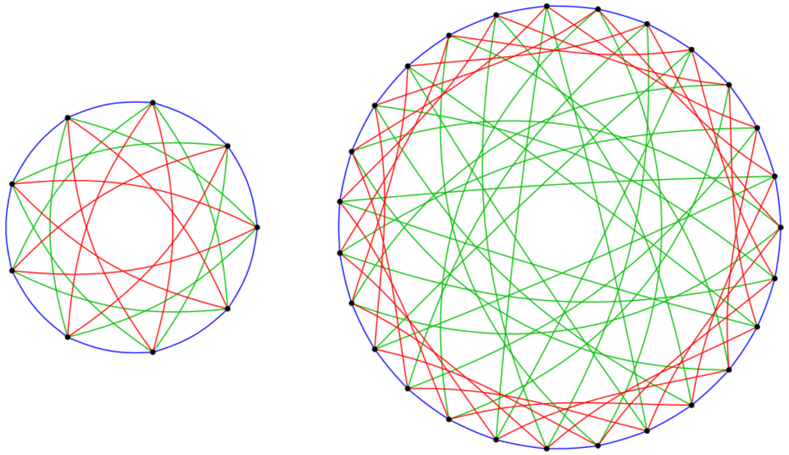


Figure 1. Union of the supersingular ℓ-isogeny graphs for $\ell \in \{3, 5, 7\}$ over $\mathbb{F}_{419}$. CSIDH makes use of the larger component, corresponding to curves whose ring of $\mathbb{F}_{419}$-rational endomorphisms is isomorphic to $\mathbb{Z}[\sqrt{-419}]$.

Isogeny Graphs

- A **k-isogeny graph** is a graph where:

  Vertices = isomorphism classes of elliptic curves (labeled by j-invariants)

  Edges = degree k isogenies (and their duals) between classes of elliptic curves over $\mathbb{F}_{p^n}$

- Isogeny graphs satisfy all the required properties to perform graph walking Diffie-Hellman securely

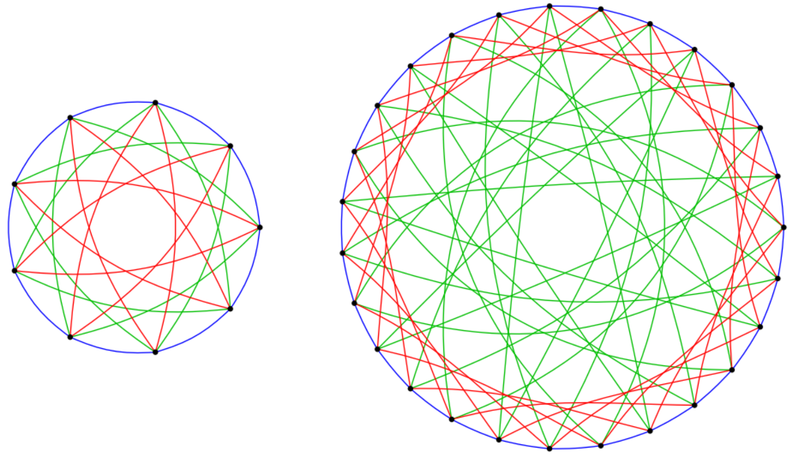
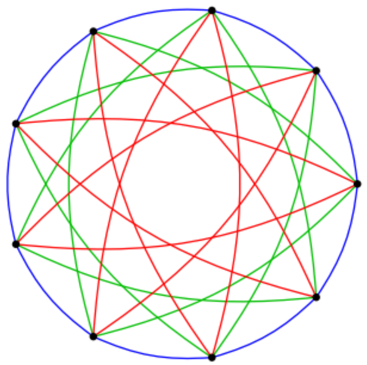


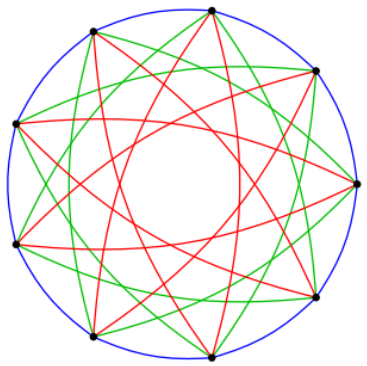
Figure 1. Union of the supersingular ℓ-isogeny graphs for $\ell \in \{3, 5, 7\}$ over $\mathbb{F}_{419}$. CSIDH makes use of the larger component, corresponding to curves whose ring of $\mathbb{F}_{419}$-rational endomorphisms is isomorphic to $\mathbb{Z}[\sqrt{-419}]$.

Walking the graph

- From each vertex of the isogeny graph you can move in a fixed number of directions.



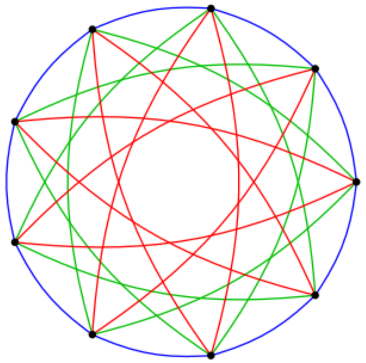
Walking the graph



- From each vertex of the isogeny graph you can move in a fixed number of directions.

- But, the isogenies from E will have completely different formula to the isogenies from a different curve E'.

Walking the graph



- From each vertex of the isogeny graph you can move in a fixed number of directions.

- But, the isogenies from E will have completely different formula to the isogenies from a different curve E'.

- To fix this, there is a method for constructing isogeny walks from ideals of the **ideal class group** $Cl(\mathcal{O})$. *

Given an **ideal class** $[\mathfrak{a}] \in Cl(\mathcal{O})$ and curve E we can compute an isogeny:

$$\varphi : E \to E/[\mathfrak{a}]$$

* Exception: For supersingular curves, to have a group structure you must restrict to a smaller set of (oriented) curves.

Class Group Actions

- Let $Ell(p)$ be the vertex set of the graph.

  i.e. isomorphism classes of curves over $\mathbb{F}_{p^n}$ for prime p.

- Isogenies **act** on this set via a map

$$* : Cl(\mathcal{O}) \times Ell(p) \to Ell(p)$$

$$[\mathfrak{a}] * E = E'$$

Diffie Hellman Key Exchange

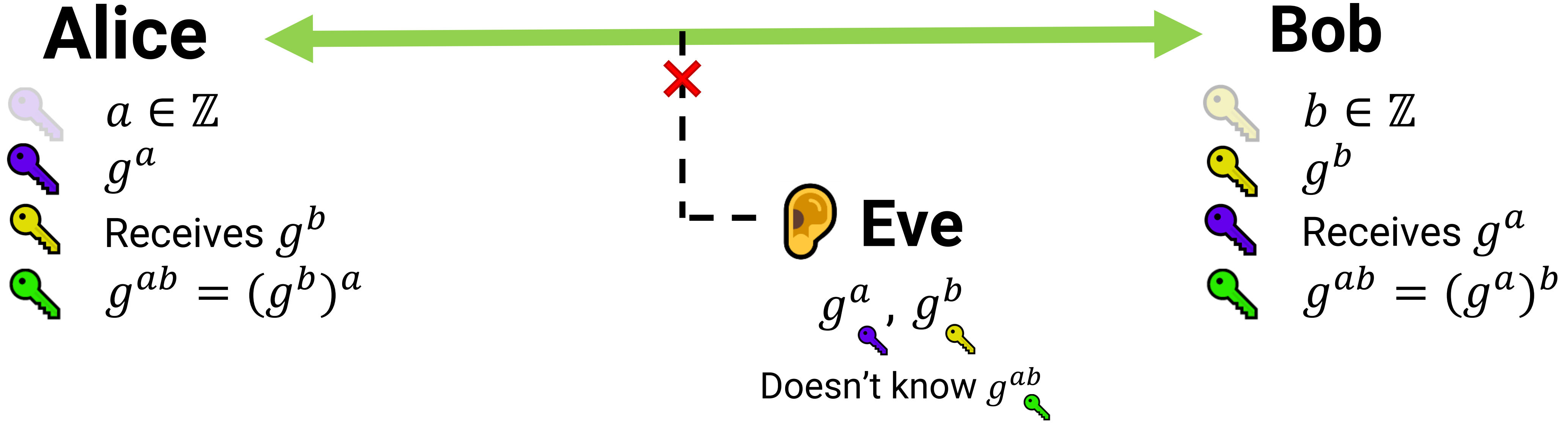
Classical Diffie-Hellman also has a group action:

$$\dagger : \mathbb{Z} \times \mathbb{F}_p \to \mathbb{F}_p$$

$$a \dagger g = g^a$$

Diffie Hellman Key Exchange

g is a known generator of $\mathbb{F}_p^*$



Alice

- $a \in \mathbb{Z}$
- g^a
- Receives g^b
- $g^{ab} = (g^b)^a$

Bob

- $b \in \mathbb{Z}$
- g^b
- Receives g^a
- $g^{ab} = (g^a)^b$

Eve

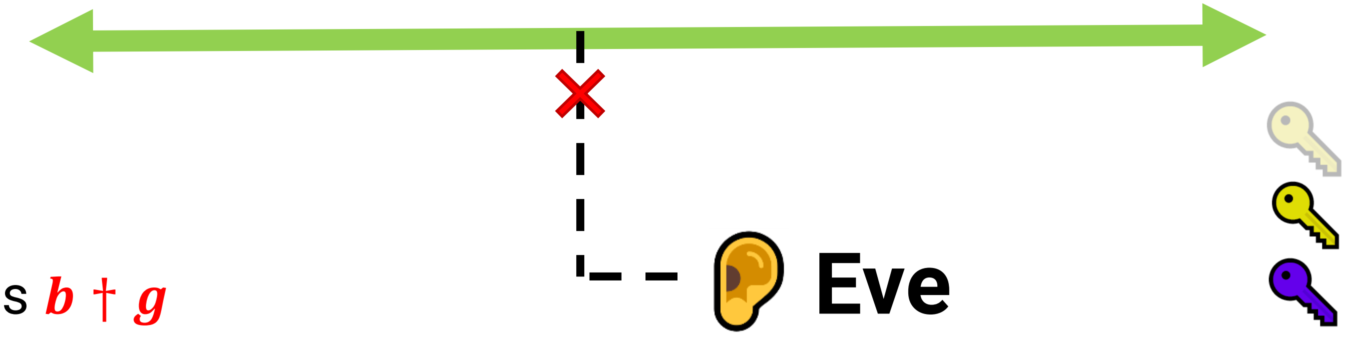
g^a, g^b

Doesn't know g^{ab}

Diffie Hellman Key Exchange

g is a known generator of $\mathbb{F}_p^*$

$\boldsymbol{Action}$: $\boldsymbol{a \dagger g = g^a}$



Alice

- 🔑 $a \in \mathbb{Z}$
- 🔑 $\boldsymbol{a \dagger g}$
- 🔑 Receives $\boldsymbol{b \dagger g}$
- 🔑 $\boldsymbol{ab \dagger g = a \dagger (b \dagger g)}$

Bob

- 🔑 $b \in \mathbb{Z}$
- 🔑 $\boldsymbol{b \dagger g}$
- 🔑 Receives $\boldsymbol{a \dagger g}$
- 🔑 $\boldsymbol{ab \dagger g = b \dagger (a \dagger g)}$

Eve

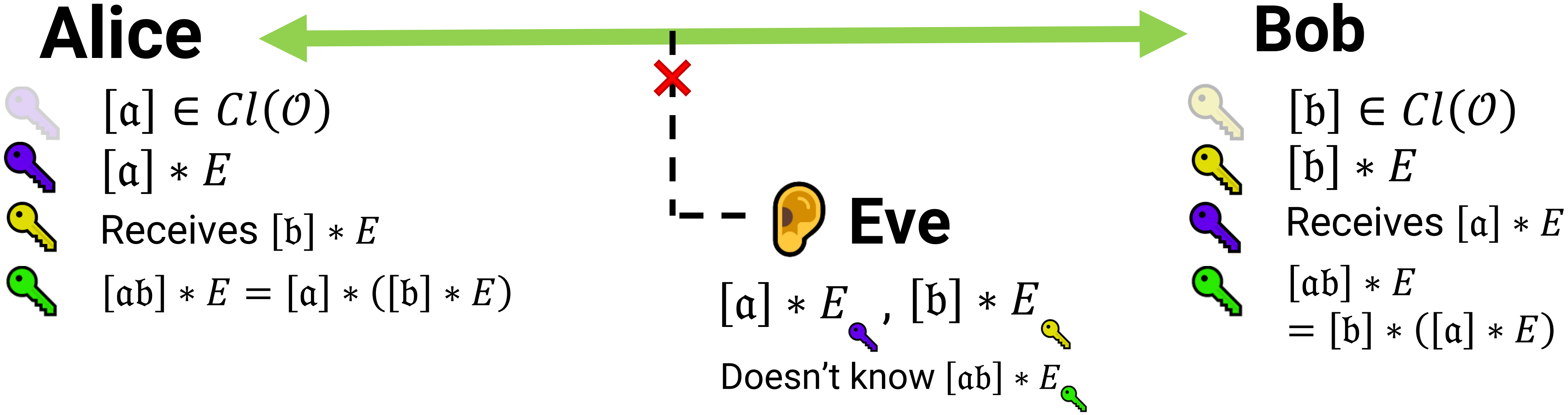
$\boldsymbol{a \dagger g}$ 🔑, $\boldsymbol{b \dagger g}$ 🔑

Doesn't know $\boldsymbol{ab \dagger g}$ 🔑

Isogeny-Based Key Exchange

E is a known starting curve.

$\boldsymbol{Action}$: $[\mathfrak{a}] * E = E'$



Alice

$[\mathfrak{a}] \in Cl(\mathcal{O})$

$[\mathfrak{a}] * E$

Receives $[\mathfrak{b}] * E$

$[\mathfrak{ab}] * E = [\mathfrak{a}] * ([\mathfrak{b}] * E)$

Eve

$[\mathfrak{a}] * E$, $[\mathfrak{b}] * E$

Doesn’t know $[\mathfrak{ab}] * E$

Bob

$[\mathfrak{b}] \in Cl(\mathcal{O})$

$[\mathfrak{b}] * E$

Receives $[\mathfrak{a}] * E$

$[\mathfrak{ab}] * E$
$= [\mathfrak{b}] * ([\mathfrak{a}] * E)$

3. Breaking Decisional DDH

Diffie-Hellman Problems

Diffie-Hellman Problems

Classical Diffie-Hellman Problem:

Given g, g^a, g^b find g^{ab}.

✗ Not secure against quantum computers!

Diffie-Hellman Problems

Classical Diffie-Hellman Problem:

Given g, g^a, g^b find g^{ab}.

✗ Not secure against quantum computers!

Diffie-Hellman for Class Group Actions Problem:

Given $E,\ [\mathfrak{a}] * E,\ [\mathfrak{b}] * E$ find $[\mathfrak{a}\mathfrak{b}] * E$.

☑ Secure against quantum computers*.

* Up to sub-exponential attacks in some cases.

Decisional Diffie-Hellman Problems

Decisional Diffie-Hellman Problems

Classical Decisional Diffie-Hellman Problem:

Distinguish between distributions (g^a, g^b, g^{ab}) and (g^a, g^b, g^c)

DDH-CGA Problem:

Distinguish between distributions $([\mathfrak{a}] * E,\ [\mathfrak{b}] * E,\ [\mathfrak{ab}] * E)$ and $([\mathfrak{a}] * E,\ [\mathfrak{b}] * E,\ [\mathfrak{c}] * E)$.

Decisional Diffie-Hellman Problems

Classical Decisional Diffie-Hellman Problem:

Distinguish between distributions (g^a, g^b, g^{ab}) and (g^a, g^b, g^c)

Easy to break!

Given (g^a, g^b, g^c) need to check if we have g^c in form g^{ab} or not.

Notice that if g^a is a square in $\mathbb{F}_p^*$ **or** g^b is a square, so is g^{ab}.

Then g^c is not a square ⇒ g^c not in form g^{ab}.

Decisional Diffie-Hellman Problems

Classical Decisional Diffie-Hellman Problem:

Distinguish between distributions (g^a, g^b, g^{ab}) and (g^a, g^b, g^c)

Easy to break!

Given (g^a, g^b, g^c) need to check if we have g^c in form g^{ab} or not.

Notice that if g^a is a square in $\mathbb{F}_p^*$ **or** g^b is a square, so is g^{ab}.

g^c in form g^{ab} $\Rightarrow \left(\frac{g^a}{p}\right) \vee \left(\frac{g^b}{p}\right) = \left(\frac{g^c}{p}\right)$

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & \text{if } n \text{ is square} \\ -1 & \text{if } n \text{ is not a square} \\ 0 & \text{if } p \text{ divides } n \end{cases}$$

Decisional Diffie-Hellman Problems

DDH-CGA Problem:

Distinguish between distributions $([\mathfrak{a}] * E,\ [\mathfrak{b}] * E,\ [\mathfrak{a}\mathfrak{b}] * E)$ and $([\mathfrak{a}] * E,\ [\mathfrak{b}] * E,\ [\mathfrak{c}] * E)$.

Can we do something similar for DDH-CGA ?

Decisional Diffie-Hellman Problems

DDH-CGA Problem:

Distinguish between distributions $([\mathfrak{a}] * E,\ [\mathfrak{b}] * E,\ [\mathfrak{a}\mathfrak{b}] * E)$ and $([\mathfrak{a}] * E,\ [\mathfrak{b}] * E,\ [\mathfrak{c}] * E)$.

Can we do something similar for DDH-CGA ?

The hardness of this problem underlies the security of several protocols built on-top of the CSIDH group action.

Breaking Ordinary DDH-CGA

Elliptic Curves are either **supersingular** or **ordinary**. We care more about supersingular curves for cryptography.

Breaking Ordinary DDH-CGA

Elliptic Curves are either **supersingular** or **ordinary**. We care more about supersingular curves for cryptography.

In 2020, Castryck, Sotáková and Vercauteren, found an attack against DDH-CGA for **ordinary** elliptic curves.

Breaking Ordinary DDH-CGA

Elliptic Curves are either **supersingular** or **ordinary**. We care more about supersingular curves for cryptography.

In 2020, Castryck, Sotáková and Vercauteren, found an attack against DDH-CGA for **ordinary** elliptic curves.

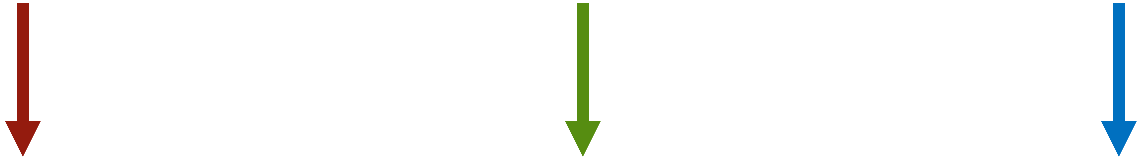
The attack is similar to the attack against Decisional Diffie-Hellman shown previously.

Breaking Ordinary DDH-CGA

$$Cl(\mathcal{O}) \;=\; \{\; [\mathfrak{u}_1], [\mathfrak{u}_2], [\mathfrak{u}_3], \dots, [\mathfrak{u}_4], [\mathfrak{u}_5], [\mathfrak{u}_6], \dots [\mathfrak{u}_7], [\mathfrak{u}_8], [\mathfrak{u}_9], \dots \;\}$$

Breaking Ordinary DDH-CGA

$$Cl(\mathcal{O}) = \{ [\mathfrak{a}_1], [\mathfrak{a}_2], [\mathfrak{a}_3], \dots, [\mathfrak{a}_4], [\mathfrak{a}_5], [\mathfrak{a}_6], \dots [\mathfrak{a}_7], [\mathfrak{a}_8], [\mathfrak{a}_9], \dots \}$$



Take Norms

$N([\mathfrak{a}]) := \left| \frac{\mathcal{O}}{[\mathfrak{a}]} \right|$ ‘size’ of an ideal

Breaking Ordinary DDH-CGA

$$Cl(\mathcal{O}) = \{ \; [\mathfrak{u}_1], [\mathfrak{u}_2], [\mathfrak{u}_3], \dots, [\mathfrak{u}_4], [\mathfrak{u}_5], [\mathfrak{u}_6], \dots [\mathfrak{u}_7], [\mathfrak{u}_8], [\mathfrak{u}_9], \dots \; \}$$

Take Norms

$$N([\mathfrak{u}]) := \left| \frac{\mathcal{O}}{[\mathfrak{u}]} \right|$$

'size' of an ideal

$$\{ N([\mathfrak{u}_1]), N([\mathfrak{u}_2]), \dots \} \qquad \{ N([\mathfrak{u}_4]), N([\mathfrak{u}_5]), \dots \} \qquad \{ N([\mathfrak{u}_7]), N([\mathfrak{u}_8]), \dots \}$$

Breaking Ordinary DDH-CGA

$$Cl(\mathcal{O}) = \{ [\mathfrak{u}_1], [\mathfrak{u}_2], [\mathfrak{u}_3], \dots, [\mathfrak{u}_4], [\mathfrak{u}_5], [\mathfrak{u}_6], \dots [\mathfrak{u}_7], [\mathfrak{u}_8], [\mathfrak{u}_9], \dots \}$$

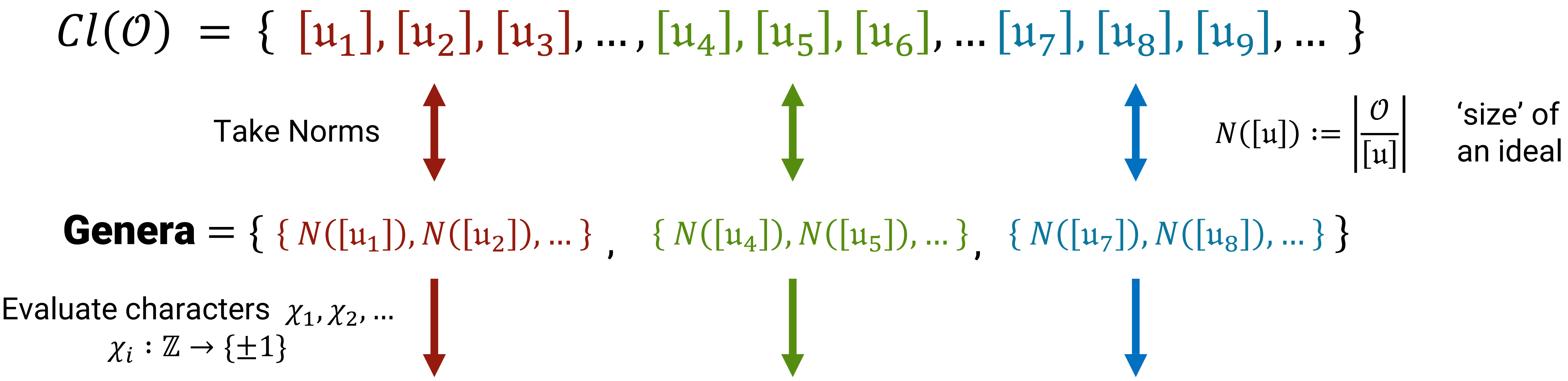
Take Norms

$$N([\mathfrak{u}]) := \left| \frac{\mathcal{O}}{[\mathfrak{u}]} \right|$$

'size' of an ideal

$$\textbf{Genera} = \{ \{ N([\mathfrak{u}_1]), N([\mathfrak{u}_2]), \dots \}, \{ N([\mathfrak{u}_4]), N([\mathfrak{u}_5]), \dots \}, \{ N([\mathfrak{u}_7]), N([\mathfrak{u}_8]), \dots \} \}$$

Breaking Ordinary DDH-CGA



$$Cl(\mathcal{O}) = \{ [\mathfrak{u}_1], [\mathfrak{u}_2], [\mathfrak{u}_3], \ldots, [\mathfrak{u}_4], [\mathfrak{u}_5], [\mathfrak{u}_6], \ldots [\mathfrak{u}_7], [\mathfrak{u}_8], [\mathfrak{u}_9], \ldots \}$$

Take Norms

$N([\mathfrak{u}]) := \left|\frac{\mathcal{O}}{[\mathfrak{u}]}\right|$ 'size' of an ideal

Genera $= \{ \{ N([\mathfrak{u}_1]), N([\mathfrak{u}_2]), \ldots \}, \{ N([\mathfrak{u}_4]), N([\mathfrak{u}_5]), \ldots \}, \{ N([\mathfrak{u}_7]), N([\mathfrak{u}_8]), \ldots \} \}$

Evaluate characters $\chi_1, \chi_2, \ldots$

$\chi_i : \mathbb{Z} \to \{\pm 1\}$

Breaking Ordinary DDH-CGA

$$Cl(\mathcal{O}) = \{ [\mathfrak{u}_1],[\mathfrak{u}_2],[\mathfrak{u}_3],\dots,[\mathfrak{u}_4],[\mathfrak{u}_5],[\mathfrak{u}_6],\dots[\mathfrak{u}_7],[\mathfrak{u}_8],[\mathfrak{u}_9],\dots \}$$

Take Norms

$N([\mathfrak{u}]) := \left|\frac{\mathcal{O}}{[\mathfrak{u}]}\right|$ 'size' of an ideal

Genera $= \{ \{ N([\mathfrak{u}_1]), N([\mathfrak{u}_2]),\dots \}, \{ N([\mathfrak{u}_4]), N([\mathfrak{u}_5]),\dots \}, \{ N([\mathfrak{u}_7]), N([\mathfrak{u}_8]),\dots \} \}$

Evaluate characters $\chi_1,\chi_2,\dots$

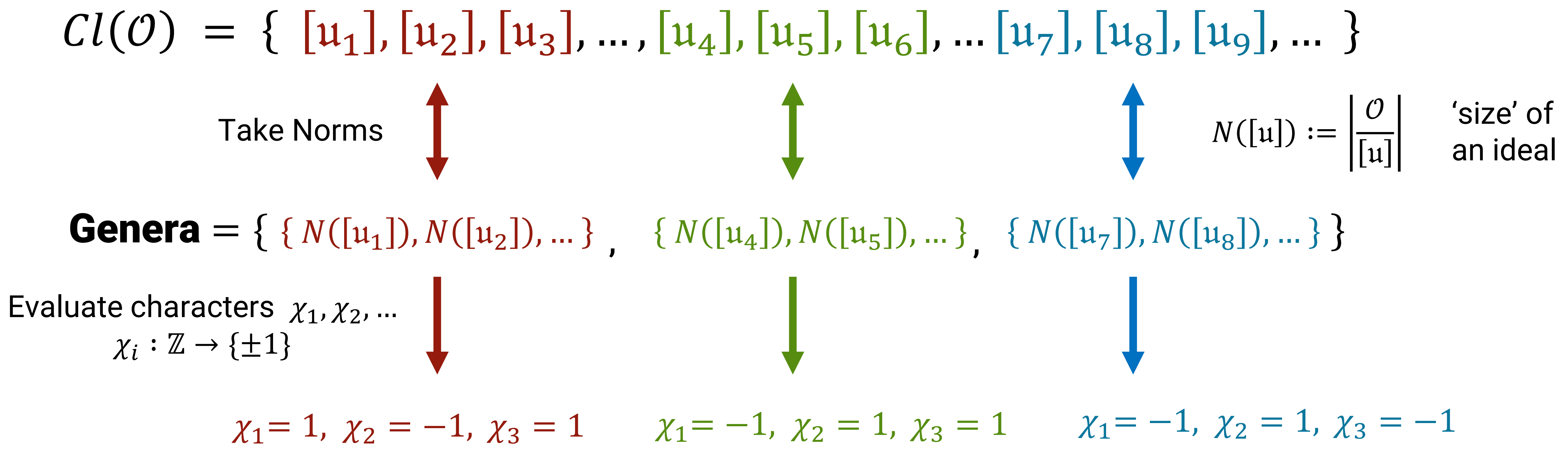
$\chi_i : \mathbb{Z} \to \{\pm 1\}$

$\chi_1 = 1,\ \chi_2 = -1,\ \chi_3 = 1$

$\chi_1 = -1,\ \chi_2 = 1,\ \chi_3 = 1$

$\chi_1 = -1,\ \chi_2 = 1,\ \chi_3 = -1$

Breaking Ordinary DDH-CGA



$Cl(\mathcal{O}) = \{ [\mathfrak{u}_1], [\mathfrak{u}_2], [\mathfrak{u}_3], \ldots, [\mathfrak{u}_4], [\mathfrak{u}_5], [\mathfrak{u}_6], \ldots [\mathfrak{u}_7], [\mathfrak{u}_8], [\mathfrak{u}_9], \ldots \}$

Take Norms

$N([\mathfrak{u}]) := \left|\frac{\mathcal{O}}{[\mathfrak{u}]}\right|$ 'size' of an ideal

Genera $= \{ \{ N([\mathfrak{u}_1]), N([\mathfrak{u}_2]), \ldots \}, \{ N([\mathfrak{u}_4]), N([\mathfrak{u}_5]), \ldots \}, \{ N([\mathfrak{u}_7]), N([\mathfrak{u}_8]), \ldots \} \}$

Evaluate characters $\chi_1, \chi_2, \ldots$

$\chi_i : \mathbb{Z} \to \{\pm 1\}$

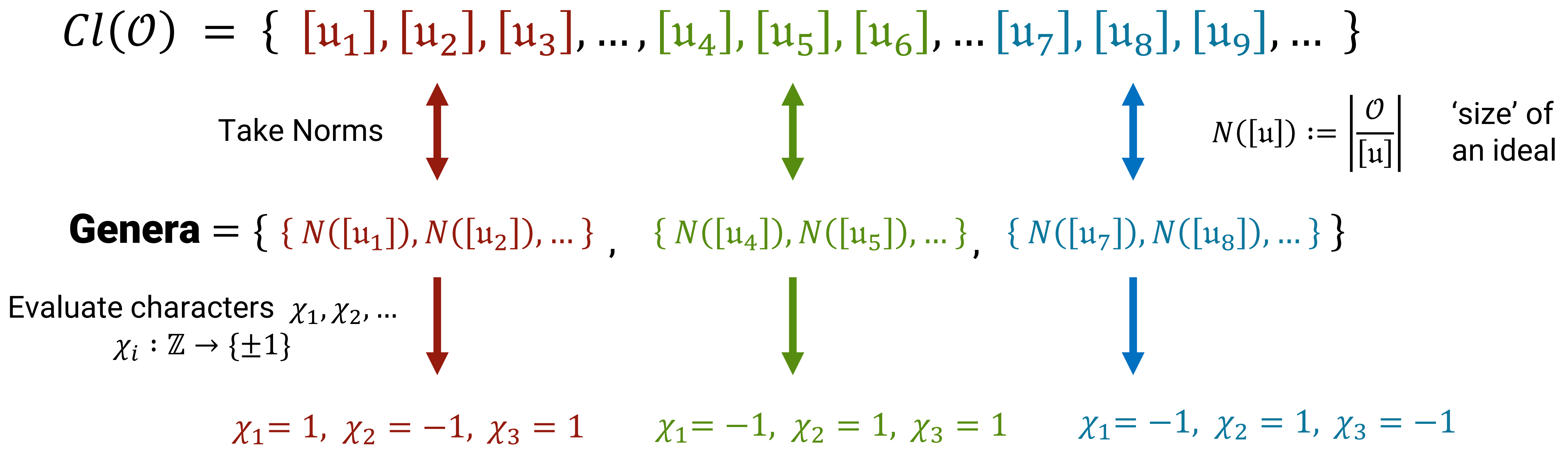
$\chi_1 = 1,\ \chi_2 = -1,\ \chi_3 = 1$

$\chi_1 = -1,\ \chi_2 = 1,\ \chi_3 = 1$

$\chi_1 = -1,\ \chi_2 = 1,\ \chi_3 = -1$

Applying characters to $N([\mathfrak{u}])$ tell us what genera $[\mathfrak{u}]$ lies within.

Breaking Ordinary DDH-CGA



$$Cl(\mathcal{O}) = \{ [\mathfrak{u}_1], [\mathfrak{u}_2], [\mathfrak{u}_3], \ldots, [\mathfrak{u}_4], [\mathfrak{u}_5], [\mathfrak{u}_6], \ldots [\mathfrak{u}_7], [\mathfrak{u}_8], [\mathfrak{u}_9], \ldots \}$$

Take Norms

$N([\mathfrak{u}]) := \left| \frac{\mathcal{O}}{[\mathfrak{u}]} \right|$ 'size' of an ideal

Genera $= \{ \{ N([\mathfrak{u}_1]), N([\mathfrak{u}_2]), \ldots \}, \{ N([\mathfrak{u}_4]), N([\mathfrak{u}_5]), \ldots \}, \{ N([\mathfrak{u}_7]), N([\mathfrak{u}_8]), \ldots \} \}$

Evaluate characters $\chi_1, \chi_2, \ldots$

$\chi_i : \mathbb{Z} \to \{\pm 1\}$

$\chi_1 = 1,\ \chi_2 = -1,\ \chi_3 = 1$ $\chi_1 = -1,\ \chi_2 = 1,\ \chi_3 = 1$ $\chi_1 = -1,\ \chi_2 = 1,\ \chi_3 = -1$

Applying characters to $N([\mathfrak{u}])$ tell us what genera $[\mathfrak{u}]$ lies within.

If $[\mathfrak{a}\mathfrak{b}]$ and $[\mathfrak{c}]$ lie in different genera, then $[\mathfrak{a}\mathfrak{b}] * E$ is not in form $[\mathfrak{c}] * E$

Breaking Ordinary DDH-CGA

Q. How do we group ideal classes into ‘genera’?

Q. What are these characters χ_i?

Q. Ideal classes $[\mathfrak{a}]$ are secret. How do we compute $\chi_q\big(N([\mathfrak{a}])\big)$ just from public curves E and $[\mathfrak{a}] * E$?

Breaking Ordinary DDH-CGA

Q. How do we group ideal classes into ‘genera’?

A **binary quadratic form** is a function of form $f(x, y) = ax^2 + bxy + cy^2$ for integers a, b, c.

It has **discriminant** $b^2 - 4ac$. If $f(x, y) = k$ for $x, y \in \mathbb{Z}$, we say f **represents** k.

Breaking Ordinary DDH-CGA

Q. How do we group ideal classes into 'genera'?

A **binary quadratic form** is a function of form $f(x, y) = ax^2 + bxy + cy^2$ for integers a, b, c.

It has **discriminant** $b^2 - 4ac$. If $f(x, y) = k$ for $x, y \in \mathbb{Z}$, we say f **represents** k.

Two forms are **equivalent** if they have the same discriminant and there is a change of basis between them $(x, y) \mapsto (\alpha x + \beta y, \gamma x + \delta z)$. Equivalent forms represent the same values.

Breaking Ordinary DDH-CGA

Q. How do we group ideal classes into ‘genera’?

A **binary quadratic form** is a function of form $f(x, y) = ax^2 + bxy + cy^2$ for integers a, b, c.

It has **discriminant** $b^2 - 4ac$. If $f(x, y) = k$ for $x, y \in \mathbb{Z}$, we say f **represents** k.

Two forms are **equivalent** if they have the same discriminant and there is a change of basis between them $(x, y) \mapsto (\alpha x + \beta y, \gamma x + \delta z)$. Equivalent forms represent the same values.

Take forms* of discriminant D, group them together into **equivalence classes**. Let $C(D)$ be the set of these classes. It is actually a group. The **form class group**.

* Actually only primitive positive definite forms.

Breaking Ordinary DDH-CGA

Q. How do we group ideal classes into ‘genera’?

A **binary quadratic form** is a function of form $f(x, y) = ax^2 + bxy + cy^2$ for integers a, b, c.

It has **discriminant** $b^2 - 4ac$. If $f(x, y) = k$ for $x, y \in \mathbb{Z}$, we say f **represents** k.

Two forms are **equivalent** if they have the same discriminant and there is a change of basis between them $(x, y) \mapsto (\alpha x + \beta y, \gamma x + \delta z)$. Equivalent forms represent the same values.

Take forms* of discriminant D, group them together into **equivalence classes**. Let $C(D)$ be the set of these classes. It is actually a group. The **form class group**.

Theorem: There is an equivalence, $Cl(\mathcal{O}) \cong C(D)$.

* Actually only primitive positive definite forms.

Breaking Ordinary DDH-CGA

Q. How do we group ideal classes into ‘genera’?

A **binary quadratic form** is a function of form $f(x, y) = ax^2 + bxy + cy^2$ for integers a, b, c.

It has **discriminant** $b^2 - 4ac$. If $f(x, y) = k$ for $x, y \in \mathbb{Z}$, we say f **represents** k.

Two forms are **equivalent** if they have the same discriminant and there is a change of basis between them $(x, y) \mapsto (\alpha x + \beta y, \gamma x + \delta z)$. Equivalent forms represent the same values.

Take forms* of discriminant D, group them together into **equivalence classes**. Let $C(D)$ be the set of these classes. It is actually a group. The **form class group**.

Theorem: There is an equivalence, $Cl(\mathcal{O}) \cong C(D)$.

Genera := Classes of quadratic forms classes representing the same set of values.

* Actually only primitive positive definite forms.

Breaking Ordinary DDH-CGA

Q. How do we group ideal classes into ‘genera’?

Q. What are these characters χ_i?

Simplified a lot.

Breaking Ordinary DDH-CGA

Q. How do we group ideal classes into ‘genera’?

Q. What are these characters χ_i?

Simplified a lot.

For $[\mathfrak{f}] \sim [\mathfrak{a}]$, values represented in $[\mathfrak{f}]$ = norms of ideals in $[\mathfrak{a}]$.

Principal ideals $[\langle 1 \rangle]$ have the set of norms (genera) as squares in $(\mathbb{Z}/d\mathbb{Z})^*$. For other ideals/form classes, genera are cosets of set of squares. We decompose $(\mathbb{Z}/d\mathbb{Z})^*$ by CRT.

For primes $q \mid \Delta_{\mathcal{O}}$ we take $\chi_q : \mathbb{Z} \to \{0, 1\}$ defined by $\chi_q(n) = \left(\frac{n}{q}\right)$

There are exactly 2^μ genera where μ = #characters

⇒ Characters perfectly distinguish between genera

$$\chi_q\big(N([\mathfrak{a}])\big) \times \chi_q\big(N([\mathfrak{b}])\big) = \chi_q\big(N([\mathfrak{a}\mathfrak{b}])\big)$$

Breaking Ordinary DDH-CGA

Q. How do we group ideal classes into ‘genera’?

Q. What are these characters χ_i?

Q. Ideal classes $[\mathfrak{a}]$ are secret. How do we compute $\chi_q\left(N([\mathfrak{a}])\right)$ just from public curves E and $[\mathfrak{a}] * E$?

Isogeny graphs have a volcano-like structure, split into layers with a surface and floor. Starting from curves E and $[\mathfrak{a}] * E$, walk to the floor.

You can recover $\left(\frac{N([\mathfrak{a}])}{q}\right)$ using pairings on q-torsion points. Details omitted.

Breaking Oriented DDH-CGA

Theorem: Let E be an elliptic curve over $\mathbb{F}_{p^n}$. Then:

1. If E is ordinary, $End(E)$ is isomorphic to an **imaginary quadratic order**, $\mathcal{O} = \mathbb{Z}[\omega]$.
2. If E is supersingular, $End(E)$ isomorphic to a **maximal quaternion order.**

Case 1 is where the previous attack applied.

But supersingular curves in case 2 are better for cryptography. How can we attack them instead?

For supersingular curves, the class group action is defined differently …

* specifically, isomorphism $Cl(\mathcal{O}) \cong C(D)$

Breaking Oriented DDH-CGA

Breaking Oriented DDH-CGA

An $\mathcal{O}$**-oriented** elliptic curve is a pair (E, ι) where $\iota : \mathcal{O} \hookrightarrow End(E)$ is an embedding.

Breaking Oriented DDH-CGA

An $\boldsymbol{\mathcal{O}}$**-oriented** elliptic curve is a pair (E, ι) where $\iota : \mathcal{O} \hookrightarrow End(E)$ is an embedding.

The group action of applying isogenies to $\boldsymbol{\mathcal{O}}$**-oriented** curves can similarly be defined using $Cl(\mathcal{O})$. Here $\mathcal{O}$ is also an imaginary quadratic order, just like in the ordinary case.

Breaking Oriented DDH-CGA

An $\mathcal{O}$**-oriented** elliptic curve is a pair (E, ι) where $\iota : \mathcal{O} \hookrightarrow End(E)$ is an embedding.

The group action of applying isogenies to $\mathcal{O}$**-oriented** curves can similarly be defined using $Cl(\mathcal{O})$. Here $\mathcal{O}$ is also an imaginary quadratic order, just like in the ordinary case.

The DDH-CGA attack generalises to this setting.

Breaking CSIDH DDH-CGA?

We have attacks against DDH-CGA for ordinary curves, and oriented supersingular curves.

Breaking CSIDH DDH-CGA?

We have attacks against DDH-CGA for ordinary curves, and oriented supersingular curves.

Doesn’t apply to CSIDH, which uses $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$-oriented supersingular curves.

Breaking CSIDH DDH-CGA?

We have attacks against DDH-CGA for ordinary curves, and oriented supersingular curves.

Doesn’t apply to CSIDH, which uses $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$-oriented supersingular curves.

Recall characters come from primes dividing $\Delta_{\mathcal{O}}$ (ramified). For CSIDH, there is only one prime divisor p. One character. It’s trivial.

4. Generalizations / Variants

From Quadratics to Cubics?

While $Cl(\mathcal{O})[2] \cong \frac{Cl(\mathcal{O})}{Cl(\mathcal{O})^2}$ is trivial for CSIDH, $Cl(\mathcal{O})[3] \cong \frac{Cl(\mathcal{O})}{Cl(\mathcal{O})^3}$ is not.

From Quadratics to Cubics?

While $Cl(\mathcal{O})[2] \cong \frac{Cl(\mathcal{O})}{Cl(\mathcal{O})^2}$ is trivial for CSIDH, $Cl(\mathcal{O})[3] \cong \frac{Cl(\mathcal{O})}{Cl(\mathcal{O})^3}$ is not.

Can we generalise genus theory to get cubes instead of squares?

Consider binary cubic forms:

$$f(x, y) = ax^3 + by^3 + cx^2y + dxy^2$$

Cannot decompose sets of values represented by these forms into cosets of cubes … genus theory breaks. Then cubic residue characters are not consistent across sets of norms of ideal classes.

Higher Dimensional Genus Theory

Higher Dimensional Genus Theory

There is a natural generalization of genus theory. To forms in more variables:

$$f(x_1, \dots, x_n) = \sum_{i,j} a_{ij} x_i x_j$$

E.g. For binary quadratic forms:

$$\begin{array}{ccccc} Cl(\mathcal{O}_K) & \cong & \{K\text{−lattices of order } \mathcal{O}_K\} & \cong & C(\Delta_{\mathcal{O}_K}) \\ \text{ideal } \mathfrak{a} & = & \alpha\mathbb{Z} + \beta\mathbb{Z} & \mapsto & N(\alpha x + \beta y)/N(\mathfrak{a}) \end{array}$$

Genera = Sets of locally isometric lattices.

How about Quaternions?

Recall supersingular curves have endomorphism rings as maximal quaternion orders $\mathcal{O}$, where (left) ideals give isogenies.

How about Quaternions?

Recall supersingular curves have endomorphism rings as maximal quaternion orders $\mathcal{O}$, where (left) ideals give isogenies.

We have higher dimensional genera. Isometry classes of:

$$Cl_{left}(\mathcal{O}) \;\cong\; \{4\text{−dim lattices of order } \mathcal{O}\} \;\cong$$

Non-degenerate quadratic spaces in 4 variables

... but there is no known way to construct multiplicative characters to distinguish between these genera.

Lifting to genus 2?

$\Delta_{\mathcal{O}} = q_1 q_2 \dots q_n$ each q_i gives character as before. Want more.
We can extend our field to split these primes? $q_i = q_i^1 q_i^2$

How to apply this to CSIDH?

Lifting to genus 2?

$\Delta_{\mathcal{O}} = q_1 q_2 \dots q_n$ each q_i gives character as before. Want more.

We can extend our field to split these primes? $q_i = q_i^1 q_i^2$

How to apply this to CSIDH?

… **Weil restrictions**. Elliptic curves can be lifted to principally polarizable abelian surfaces. Endomorphism algebra is a quaternion algebra over number field.

We get splitting. But only for $p \equiv 1\ mod\ 4$, not for CSIDH.

Perhaps we can fix it. The journey continues.

Questions?

Other Projects/Interests

- Hard Problems
  - Reductions between hard isogeny problems. Finding where exactly the hardness lies.
  - Solving quaternion analogues of isogeny problems.
  - Trying to break new hardness assumptions which have some additional structure.
- Finding parameters to improve quantum security of isogeny schemes.
- Using alternative forms of elliptic curves to speed up isogeny schemes or attacks against them.
- Other applications of the link between ideal class groups and quadratic forms.