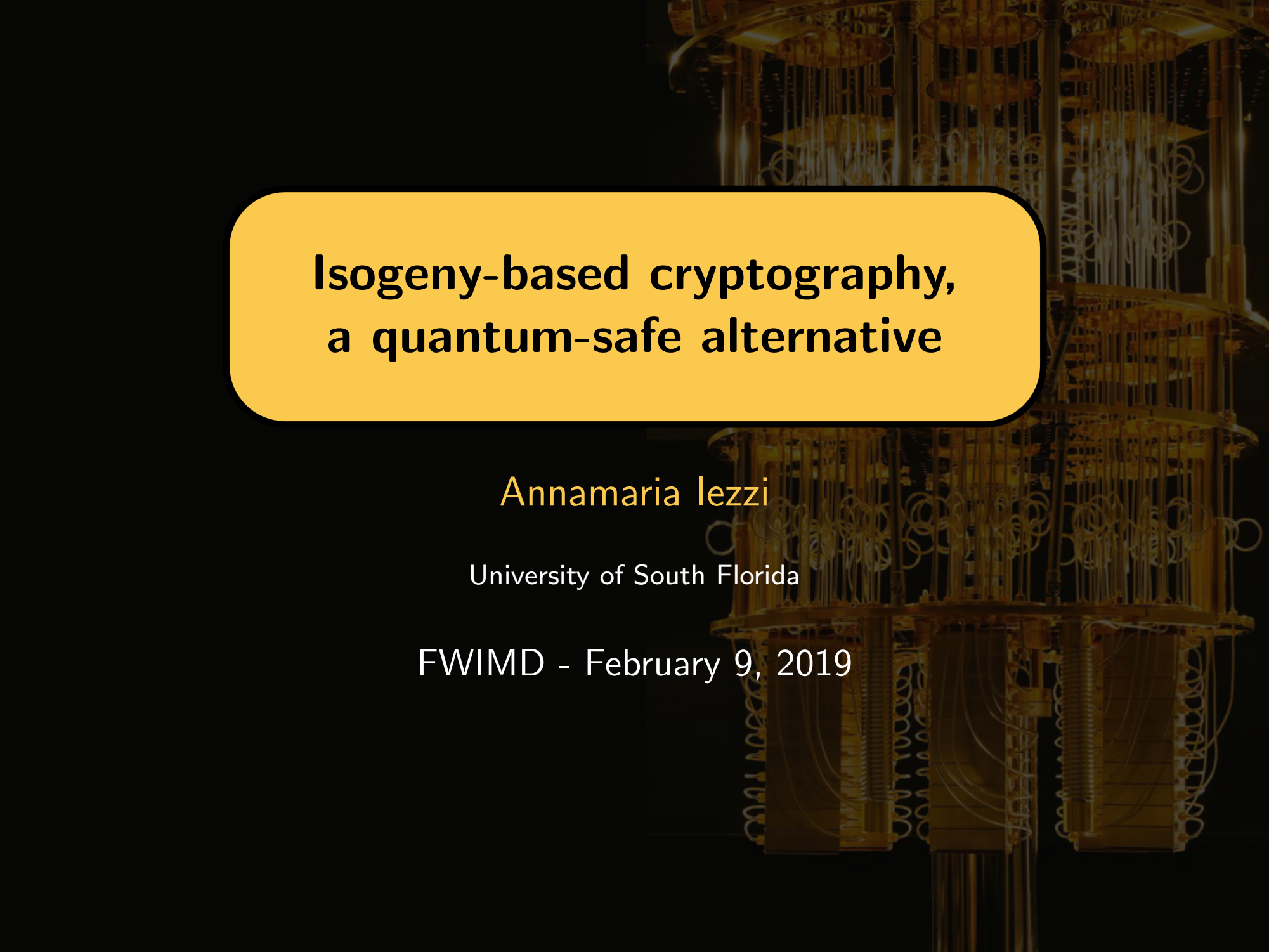


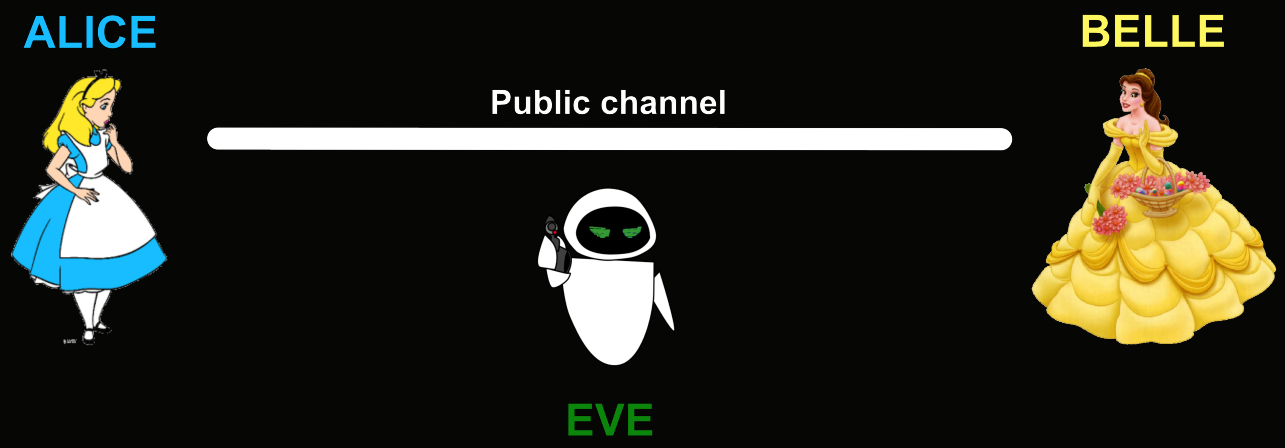
Isogeny-based cryptography, a quantum-safe alternative

Annamaria Iezzi

University of South Florida

FWIMD - February 9, 2019

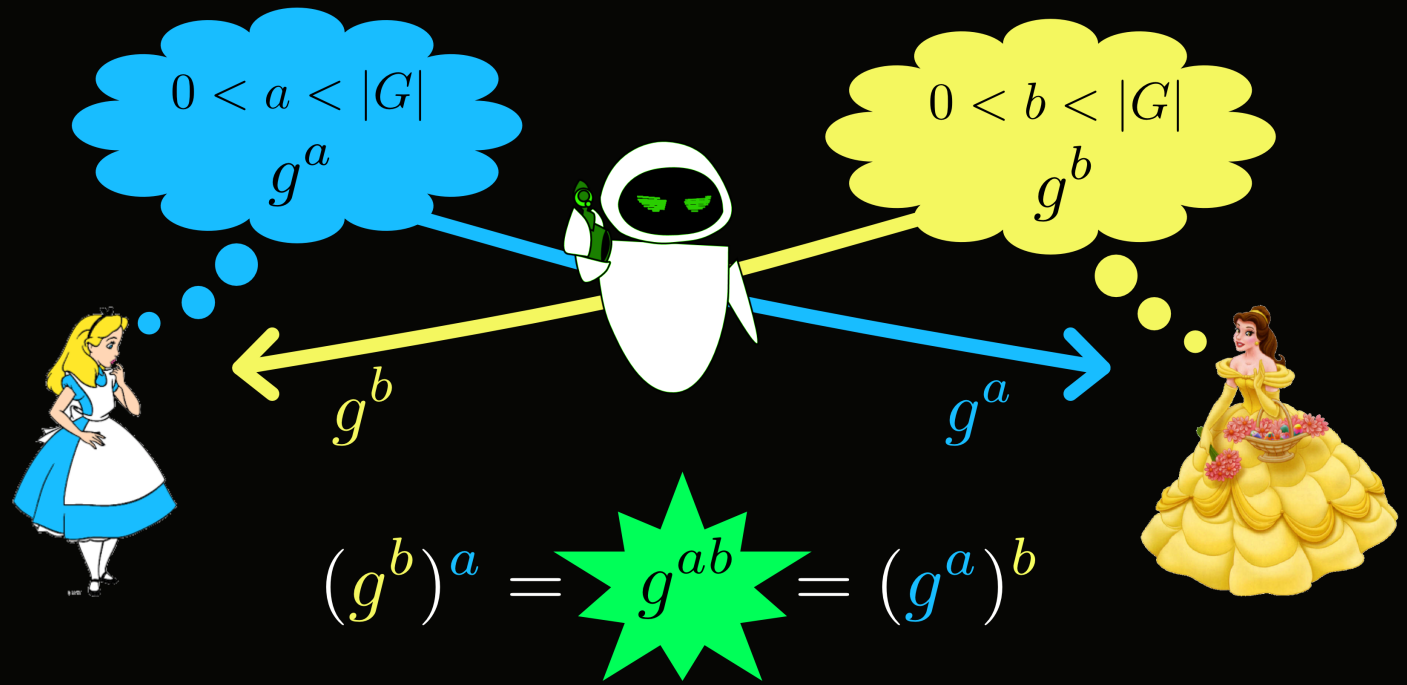
The key exchange problem



ALICE and BELLE, communicating over a public channel, want to agree on a common secret without making it available to EVE.

Diffie-Hellman Key Exchange (1976)

$G =< g >$ a **finite cyclic group**



Discrete Logarithm Problem (DLP): Given g^a find a.

Which group?

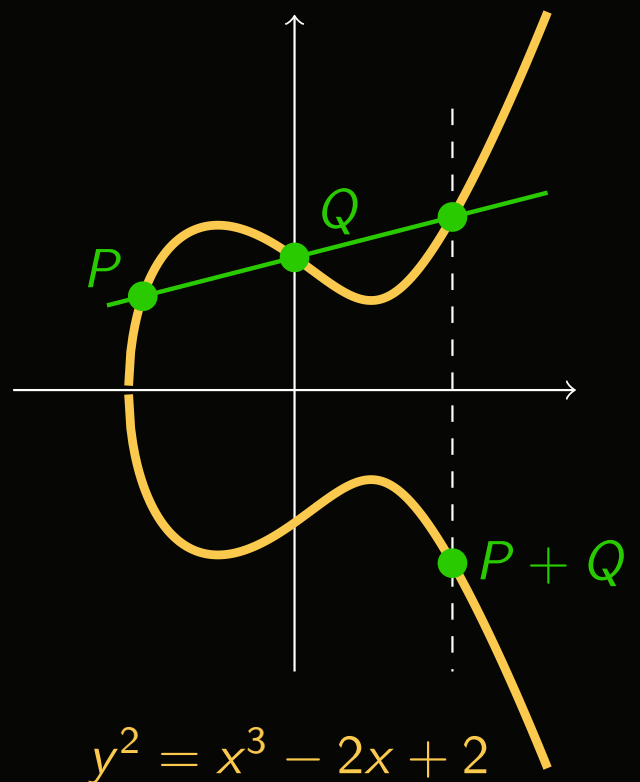
Original protocol
Diffie-Hellman (1976)

$$G = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times} = < g >$$

DLP: Given $g^a \mod p$, find $0 < a < p - 1$.

Which group?

Elliptic-Curve Diffie-Hellman (ECDH)
Koblitz and Miller (1985)



E: elliptic curve over $\mathbb{F}_q$

$G = E(\mathbb{F}_q), P \in G$

DLP
Given $Q = aP$,
find $0 < a < ord(P)$.

Towards the quantum computing era...

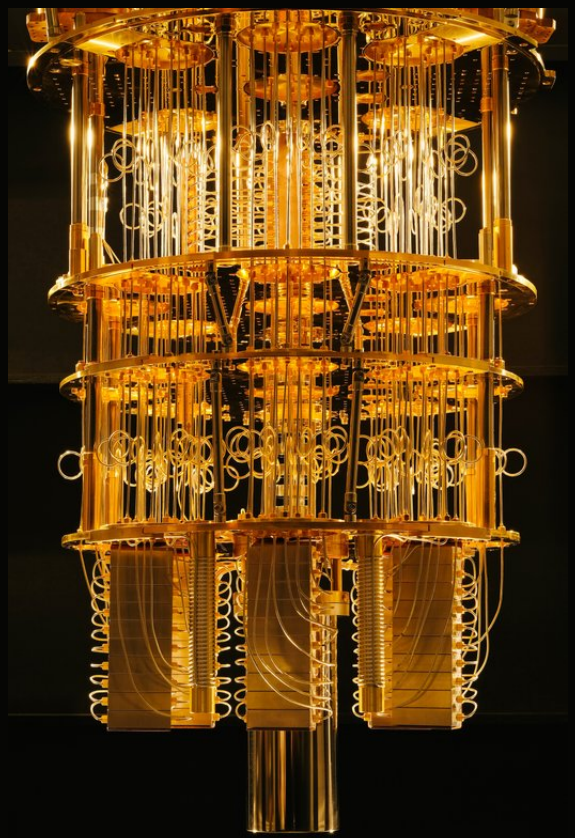
1994 - Peter Shor's quantum polynomial-time for integer factorization.

$\downarrow$ extends to

Resolution of the DLP in all finite groups.

$\downarrow$

All the currently deployed public key infrastructure will need to be replaced.



IBM's 50-qubit quantum computer
March 2, 2018

Credit: IBM Research Flickr

How serious is the threat?

August 2015

NSA announced that it is planning to transition "in the not too distant future" to a new cipher suite that is resistant to quantum attacks.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

November 2017

NIST Post-Quantum Cryptography Competition: "process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms".

What are the quantum-safe alternatives?

- Lattice-based cryptography
  25 candidates (Round one) $\rightarrow$ 12 candidates (Round two)
- Code-based cryptography
  17 candidates (Round one) $\rightarrow$ 7 candidates (Round two)
- Multivariate cryptography
  10 candidates (Round one) $\rightarrow$ 4 candidates (Round two)
- Hash-based cryptography
  2 candidates (Round one) $\rightarrow$ 1 candidates (Round two)
- **Isogeny-based cryptography**
  1 candidate (Round one) $\rightarrow$ 1 candidates (Round two)
- Other
  5 candidates (Round one) $\rightarrow$ 1 candidates (Round two)

Recall

We look for cryptosystems which are **not** based on any discrete logarithm problem

Hard-Homogeneous Spaces (Couveignes, 97)

- G a **group**, X a **set**, an **action**

$$\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & g * x \end{array}$$

  such that

$$\forall\, x, x' \in X,\ \exists!\, g \in G \text{ such that } g * x = x'.$$

- **"Easy"** operation (e.g. polynomial time):

  given $g \in G$ and $x \in X$, compute $g * x$.

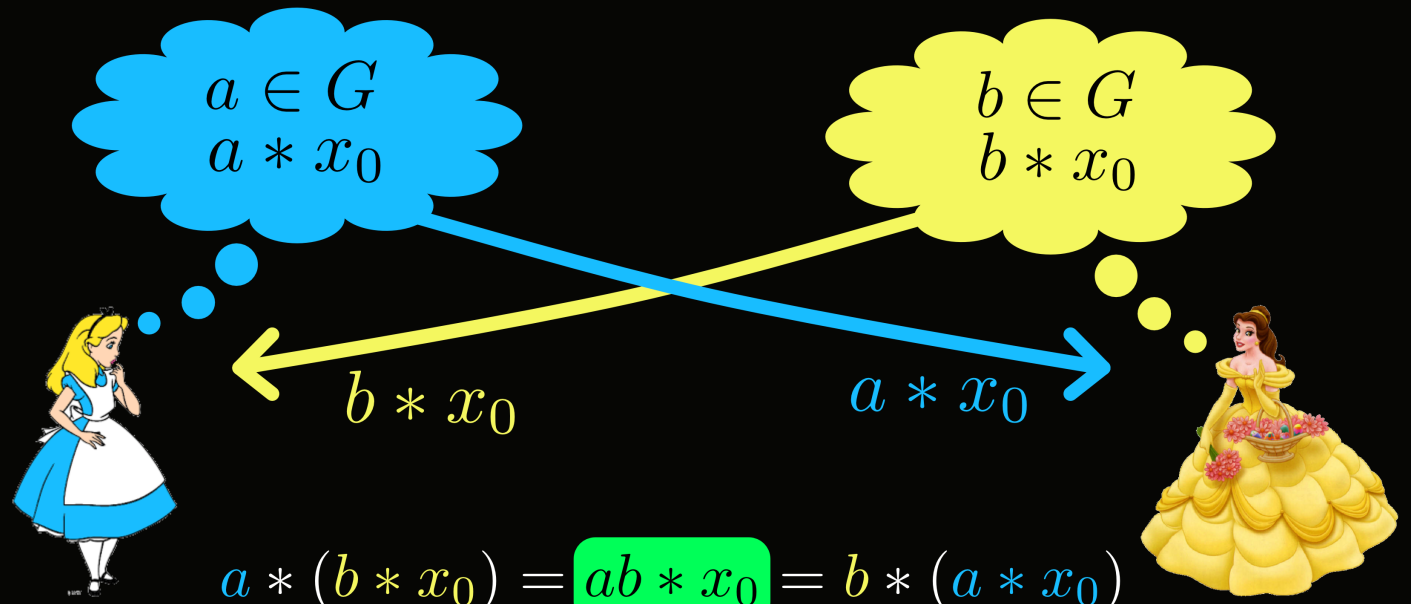
- **"Hard"** operation (e.g. not polynomial time):

  given $x, x' \in X$, find $g \in G$ such that $g * x = x'$.

If G is Abelian $\to$ commutative group action $\to$
$\to$ key exchange based on HHS.

Key exchange based on HHS

public parameter: $x_0 \in X$



Problem: Given $a * x_0$ find a.

Elliptic curves and isogenies

- E, an **elliptic curve** defined over $\mathbb{F}_q$:

$$E : y^2 = ax^3 + bx + c, \quad a, b \in \mathbb{F}_q, \quad 4a^3 + 27b^2 \neq 0$$

- φ, an **isogeny** (non-constant rational map and group homomorphism):

$$\begin{array}{rccc} \varphi : & E & \longrightarrow & E' \\ & (x, y) & \mapsto & \left(\frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)} \right) \end{array}$$

- $\mathcal{O} := \mathrm{End}(E)$, the **ring of endomorphisms** of E.

A commutative group action

$\mathcal{O}$ an order in an imaginary quadratic field

- **Set** X: isomorphism classes $\overline{E}$ of elliptic curves having the same endomorphism ring $\mathcal{O}$.
- **Group** G: ideal class group of $\mathcal{O}$

$$G = \mathrm{Cl}(\mathcal{O}) = \frac{\mathcal{I}(\mathcal{O})}{\mathcal{P}(\mathcal{O})} = \{[\mathfrak{a}] : \mathfrak{a} \text{ is an ideal of } \mathcal{O}\},$$

G is a finite abelian group.

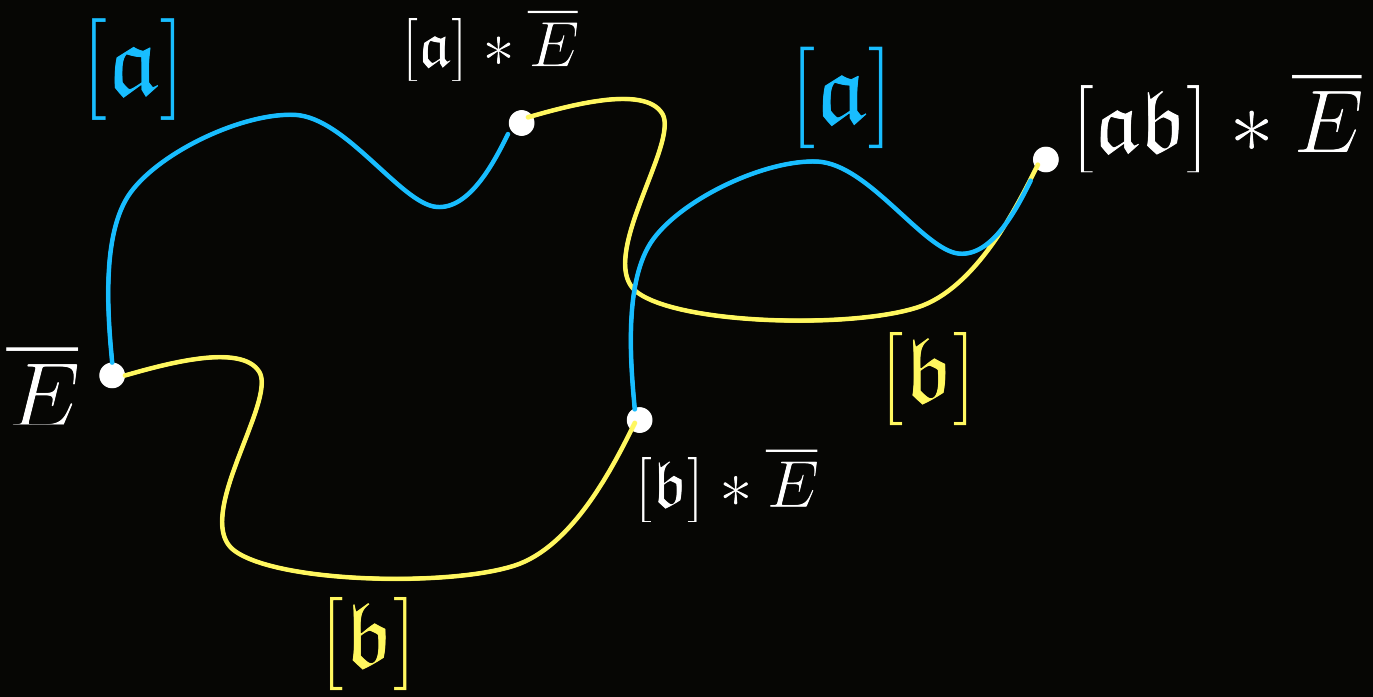
G acts on X:

$[\mathfrak{a}] * \overline{E}_1 = \overline{E}_2$

$\varphi_{\mathfrak{a}} : E_1 \to E_2$

with $\deg(\varphi_{\mathfrak{a}}) = \mathcal{N}(\mathfrak{a})$

Random walks on the isogeny graph



Examples

- Couveignes - 1997
- Rostovtsev and Stolbounov - 2006 and 2010
- De Feo, Kieffer, Smith - 2018
- CSIDH - 2018

The underlying mathematical problem

The security of these cryptosystems relies on the following "hard" mathematical problem:

Let E_1 and E_2 two elliptic curves defined over a finite field such that there exists a imaginary quadratic order $\mathcal{O}$ which satisfies:

$$\mathcal{O} \cong \mathrm{End}(E_i),\ i = 1, 2.$$

Problem: Find ~~an isogeny~~ $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ such that

$$\sout{\phi : E_1 \longrightarrow E_2} \quad [\mathfrak{a}] * \overline{E}_1 = \overline{E}_2.$$

How to tackle the problem?

Problem: Given $\overline{E}_1$ and $\overline{E}_2$, find $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ such that

$$[\mathfrak{a}] * \overline{E}_1 = \overline{E}_2.$$

- Limit the number of tries in $\mathrm{Cl}(\mathcal{O})$:
  $\rightarrow$ **Hidden Shift Problem**
- Compute efficiently $[\mathfrak{a}] * \overline{E}_1$:
  $\rightarrow$ **Factor $[\mathfrak{a}]$ in a "short" product**

Biasse, I., Jacobson (2018):

$N := |\mathrm{Cl}(\mathcal{O})|$
Time: $2^{O\left(\sqrt{\log(N)}\right)}$
Quantum memory: $2^{O\left(\sqrt{\log(N)}\right)}$

Thank you!