Post Quantum Cryptography, Isogeny Graphgs

Javad Doliskani

Intitiute for Quantum Computing
University of Waterloo

Content

Quantum computers

- Able to run any classical code!
  - In a quantum computer every operation is reversible.
  - Classical operations might not be reversible.
  - Irreversible operations can be made reversible.

Irreversible + extra input and output = Reversible

Quantum computers

- More powerful than classical computers
  - Operations can be performed on registers in **superposed** states.
  - There are problems that a quantum computer can provably solve more efficient than a classical computer.

1. Deutsch 1985
2. Jozsa 1992
3. Bernstein and Vasirani 1997

Quantum computers

Search

- In a list of size n, and element can be found in time $O(\sqrt{n})$
- More generally, if there are m solutions then a solution can be found in time $O(\sqrt{\frac{m}{n}})$

Period finding

- If $f(n+s) = f(n), \forall n$ then s can be found efficiently
  - An n-bit integer can be factored in time $O(n^3)$
  - Discrete logarithm problem in $\mathbb{F}_q^\times$ can be solved in time $O(\log^3 q)$

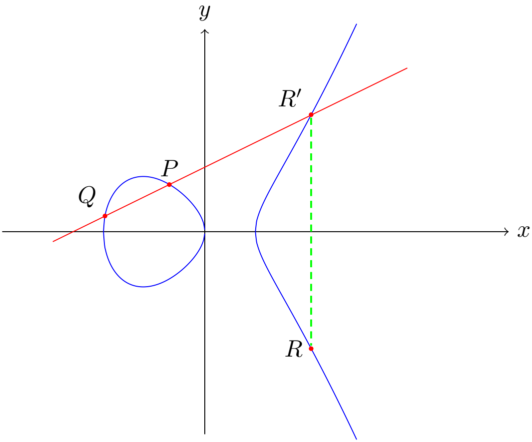
Cryptography

- **Classical cryptography**
  - Cryptography using a classical computer:
    Most known cryptosystems
- **Post quantum cryptography**
  - Classical cryptosystems which seem to resist quantum attacks:
    Lattice based, Code based, Isogeny based, etc.
- **Quantum cryptography**
  - Cryptography using a quantum computer/device:
    Quantum Key Distribution

Post quantum cryptography

- **Lattice based**
  - NewHope, CRYSTALS-KYBER, NTRU, Frodo, etc.
- **Code based**
  - McEliece, BIKE, LAKE, etc.
- **Multivariate**
  - DME, Rainbow, CFPKM, etc.
- **Hash based**
  - Gravity-SPHINCS, SPHINCS+.
- **Isogeny based**
  - SIKE.

Isogeny based cryptography



Elliptic curve E: $y^2 = x^3 + ax + b$

A Graph

Vertices

- The set of all elliptic curves E: $y^2 = x^3 + ax + b$ where a, b are in a given field.
- For example, the curve $y^2 = x^3 + 5x + 13$ is defined over the finite field $\mathbb{F}_{31}$.

Edges

Mappings between elliptic curves are given by rational functions:

$$\begin{array}{rrcl} \psi : & E_1 & \longrightarrow & E_2 \\ & (x, y) & \longmapsto & (R_1(x, y), R_2(x, y)) \end{array}$$

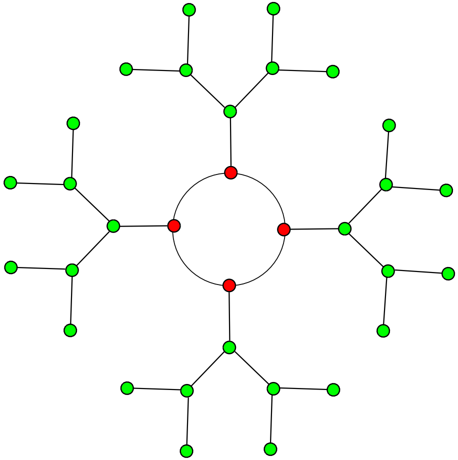
- Isogenies are special kind of such mappings

Isogeny graphs

There are two kinds of elliptic curves over a finite field $\mathbb{F}_q$.

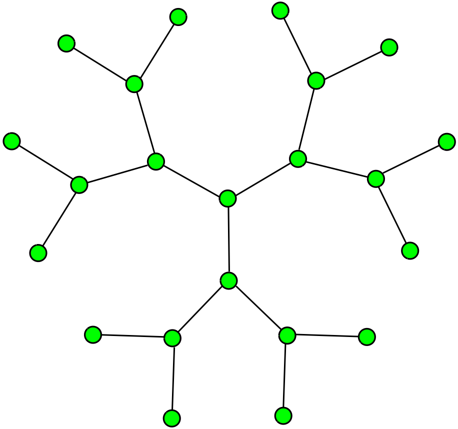
- **Ordinary** elliptic curves
  - Nontrivial p-torsion.
  - Isogeny graphs are called isogeny volcanoes
- **Supersingular** elliptic curves
  - Trivial p-torsion.
  - Isogeny graphs regular graphs
  - For example the graph of 2-isogenies is 3-regular

Isogeny volcanoes



Inner nodes have degree 3 and leaves have degree 1

Supersingular graphs



Connected 3-regular graph.

Supersingular graphs

Over the finite field $\mathbb{F}_{p^2}$:

- The graph is connected.
  - The diameter of the graph is $O(\log p)$.
- The number of vertices in the graph is $\approx \lceil \frac{p}{12} \rceil$.
- The vertices are encoded using j-invariants
  - j-invariants are elements of $\mathbb{F}_{p^2}$.
- The edges are encoded using modular poltnomials.

Taking $p \approx 2^{700}$, the isogenty graph has $\approx 2^{696}$ nodes.

Supersingular isogeny problem

Let G be the isogeny graph of supersingular curves over $\mathbb{F}_{p^2}$. Given two vertices E_1 and E_2 in G, find a path $E_1 \to E_2$.

The endomorphism version:

- Let G be the isogeny graph of supersingular curves over $\mathbb{F}_{p^2}$. Given a vertex E in G, find a nontrivial loop $E \to E$.

A trivial loop is multiplication by an integer

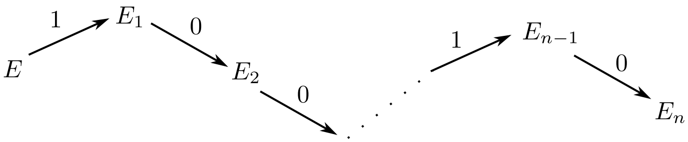
$$\begin{array}{rccc} [m]: & E & \longrightarrow & E \\ & P & \longmapsto & [m]P \end{array}$$

Attacks

- **Pollard-rho**
  - Complexity: $O(\sqrt{p}\log^2 p)$
  - Might not always find the path of correct length
- Quantum **claw finding**
  - Complexity: classical $O(\sqrt{p})$, and quantum $O(\sqrt[3]{p})$
- Using the $\mathbb{F}_p$**-subgraph** and quantum search
  - Complexity: $O(\sqrt[4]{p})$.
  - Usually finds longer paths

Set $p \approx 2^{512}$ to get ≈ 128 bits of security.

Supersingular hash



- Hashing of an n-bit message $M = 100\ldots10$
- Charles, Lauter, Goren 2009

Supersingular Isogeny Diffie-Hellman

$$\begin{tikzcd}[column sep=huge, row sep=huge]
E \arrow[r, squiggly, "\text{Alice}"] \arrow[d, squiggly, "\text{Bob}"'] & E_A \arrow[d, squiggly, "\text{Bob}"] \\
E_B \arrow[r, squiggly, "\text{Alice}"'] & E_{AB}
\end{tikzcd}$$

Shared key: the j-invariant of E_{AB}.

Implementation

Performance (in thousands of cycles) on a 3.4GHz Intel Core i7-6700

Scheme	KeyGen	Encaps	Decaps
SIKEp503	10,134	16,619	17,696
SIKEp751	30,919	50,014	53,838

Size (in bytes) of inputs and outputs

Scheme	secret key	public key	ciphertext	shared secret
SIKEp503	(56+378) 434	378	402	16
SIKEp751	(80+564) 644	564	596	24
SIKEp964	(100+726) 826	726	766	32

See `http://sike.org` for more details.