Hard Problems on Isogeny Graphs over RSA Moduli and Groups with Infeasible Inversion

Salim Ali Altuğ

Yilei Chen

BOSTON UNIVERSITY

VISA Research

ASIACRYPT 2019 Kobe, Japan

Number Theory is a beautiful garden
– Carl Ludwig Siegel

Slides from a talk of Miller, available at http://2010.eccworkshop.org/slides/Miller.pdf

Number Theory is a beautiful garden – Carl Ludwig Siegel

Oil was discovered in the garden. – Hendrik W. Lenstra, Jr.

Slides from a talk of Miller, available at http://2010.eccworkshop.org/slides/Miller.pdf


A volcano was discovered
in the garden!
- Kohel 1996


Today: A *group with infeasible inversion*
was found in the volcano!


What is a group with infeasible inversion?

Hohenberger and Molnar (2003) propose *groups with infeasible inversion*

Inversion is hard: given [x], compute [-x] is hard.

Composition is easy: given [x], [y], compute [x+y] is easy.

Application: Directed transitive signature.

Another application: Broadcast encryption [Irrer et al. 04].

They did not find out any group (representation) that satisfies this property.

A non-example: over a finite field F_q : $[a] = g^a \bmod q$

given g, g^a, finding a is hard, but computing g^{-a} is simple.

Attempts of constructing groups with infeasible inversion?

Attempt 1: Let G be the multiplicative group “in the exponent”:

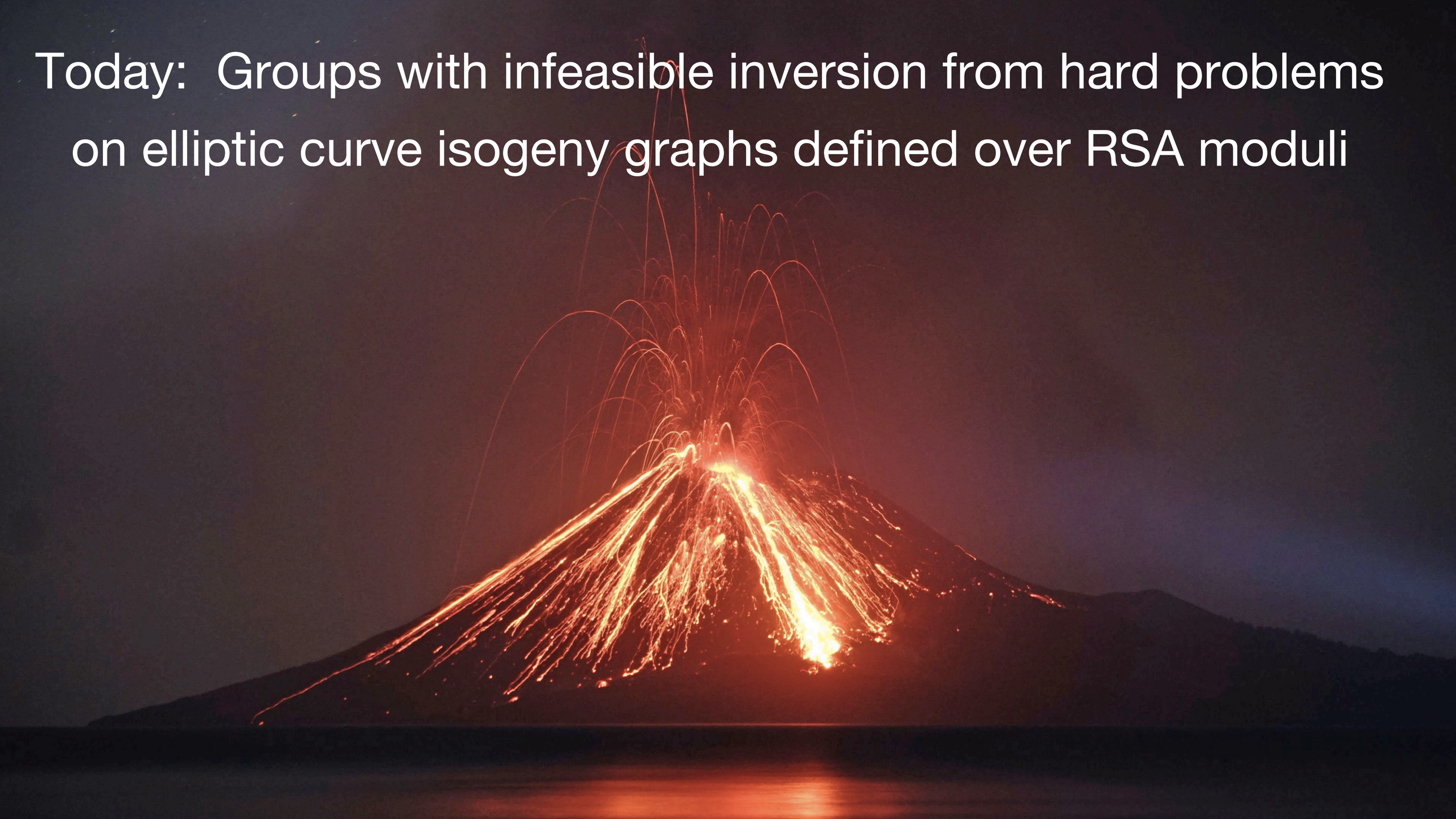
given g, g^a, compute $g^{1/a}$ is hard in many groups.

But … multiplication in the exponent is also hard, cannot compose.

Attempt 2: obfuscate the exponentiation function: Yes [Yamakawa et al. 14]

encoding(a) = { g^a, Obf{a,N}(x) = x^{2a} mod N }

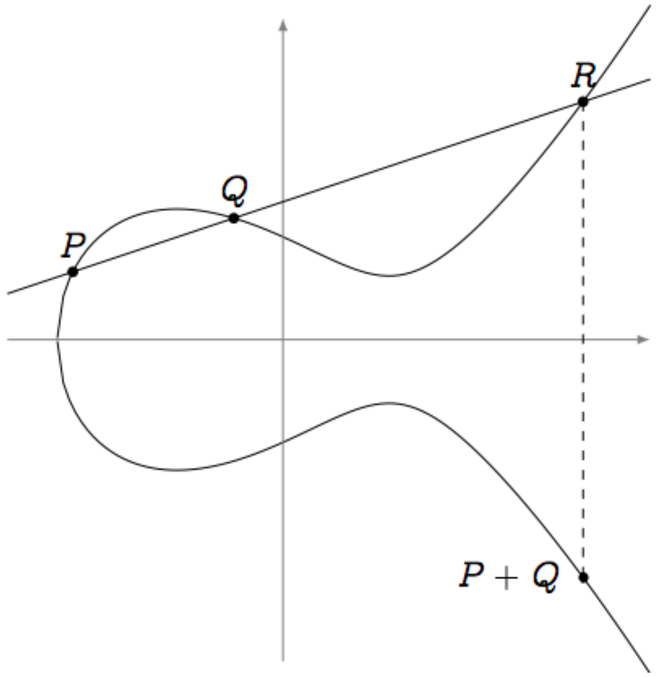
Still, no candidate GII was known without using general purpose obfuscation.


Today: Groups with infeasible inversion from hard problems
on elliptic curve isogeny graphs defined over RSA moduli

Road map

1. Elliptic curve isogenies can be represented by graphs like volcanoes.
2. Isogeny graphs can be used to represent a group.
3. Over finite fields, searching for close neighbors on the graph is easy.
4. Over an RSA modulus N, finding certain neighbors is hard.
5. Hardness of finding certain neighbors => hardness of inverting group elements.

Elliptic curve 101



$E(F_q) = \{ (x, y) \mid y^2 = x^3+ax+b \text{ over } F_q \} \cup \{ O \}$

j-invariant of a curve: $j = 1728 \cdot 4a^3/(4a^3+27b^2)$

Over C, curves with the same j-invariant are isomorphic;

Over F_q they are isomorphic, or the twist of each other.

In this talk let us treat curves with the same j-invariant as the same.

Elliptic curve isogeny

Isogenous is an interesting equivalence relation between elliptic curves.

> “A morphism ϕ from E_1 to E_2 is called an isogeny if it maps O on E_1 to O on E_2.”

Elliptic curve isogeny

Isogenous is an interesting equivalence relation between elliptic curves.

"A morphism ϕ from E_1 to E_2 is called an isogeny if it maps O on E_1 to O on E_2."

[Tate 1966] Two elliptic curves E_1 and E_2 over a finite field F_q are isogenous iff they have the same number of points.

Elliptic curve isogeny

Isogenous is an interesting equivalence relation between elliptic curves.

"A morphism ϕ from E_1 to E_2 is called an isogeny if it maps O on E_1 to O on E_2."

[Tate 1966] Two elliptic curves E_1 and E_2 over a finite field F_q are isogenous iff they have the same number of points.

[Hasse 1933] The number of the points on $E(F_q)$: $[\, q + 1 - 2\sqrt{q} \,,\, q + 1 + 2\sqrt{q} \,]$

[Schoof 1985] given a, b and q, compute $\#E(F_q)$ in time poly(log q).

Elliptic curve isogeny

Isogenous is an interesting equivalence relation between elliptic curves.

"A morphism ϕ from E_1 to E_2 is called an isogeny if it maps O on E_1 to O on E_2."

[Tate 1966] Two elliptic curves E_1 and E_2 over a finite field F_q are isogenous iff they have the same number of points.

[Hasse 1933] The number of the points on $E(F_q)$: $[\, q + 1 - 2\sqrt{q} \,,\, q + 1 + 2\sqrt{q} \,]$

[Schoof 1985] given a, b and q, compute $\#E(F_q)$ in time poly(log q).

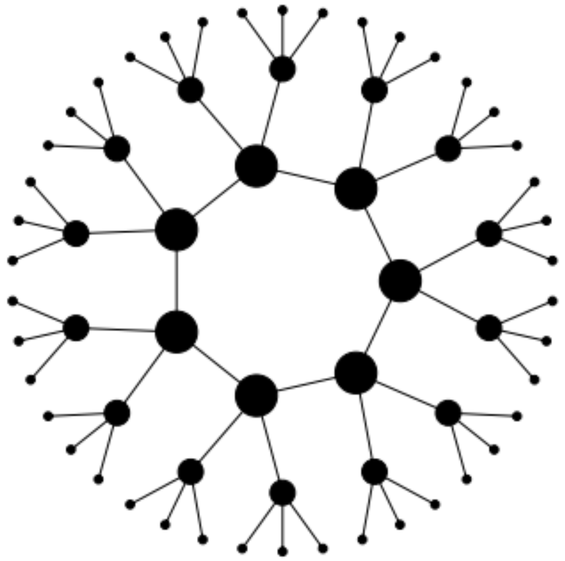
An isogeny ϕ: $E_1 \rightarrow E_2$ can be explicitly written as a rational polynomial.

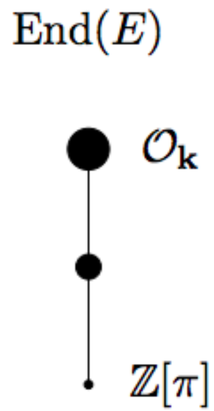
$$\phi: (x, y) \rightarrow \left(f(x)/h^2(x) \,,\, g(x, y)/h^3(x) \right),$$

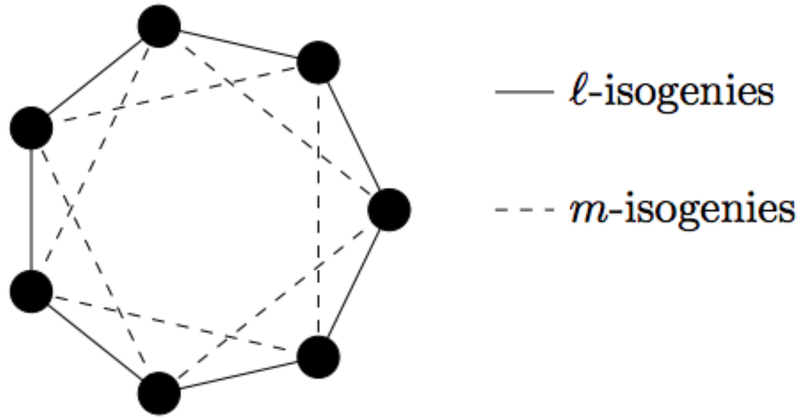
The degree of an isogeny ϕ is the degree of the rational polynomial.

Volcano ahead!

Relation among isogenous curves — isogeny graph







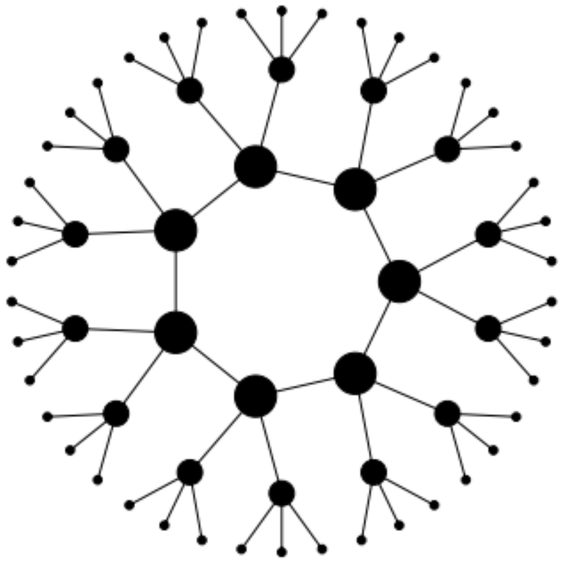
Left: fix a degree L

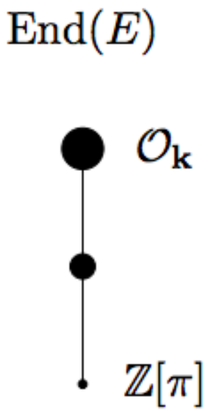
Right: the crater with multiple degrees

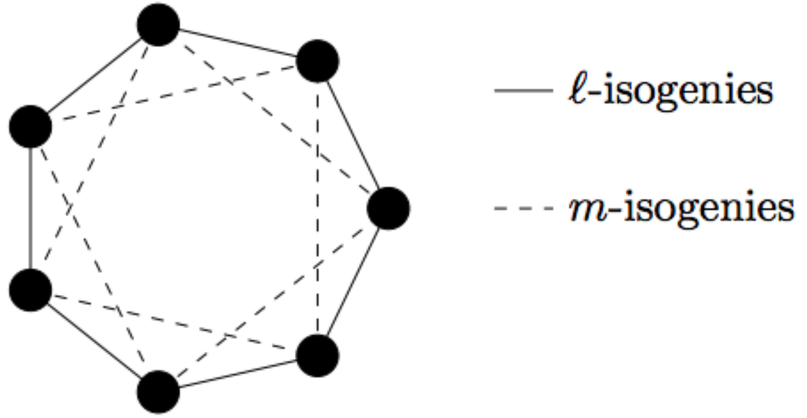
Isogeny graph: each vertex is an elliptic curve; each edge is an isogeny.
The graph structure is described in the PhD Thesis of Kohel (1996).

The term “isogeny volcano” is introduced in [Fouquet, Morain 02].

Representing the ideal class group







Left: fix a degree L

Right: the crater with multiple degrees

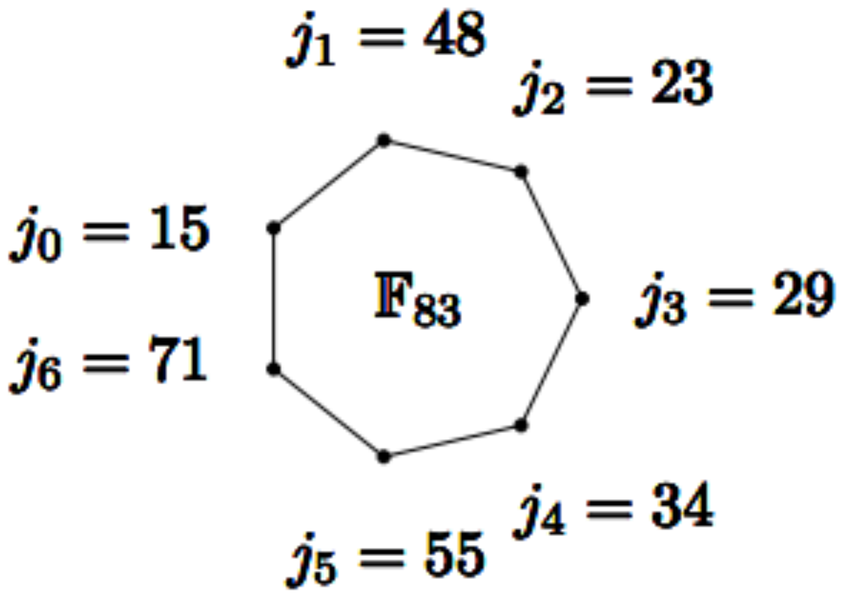
The ideal class group CL(O) acts faithfully and transitively on the set

$$\mathrm{Ell}_O(\mathbb{F}_q) = \{\ j(E) : E \text{ with } \mathrm{End}(E) = O\ \};\quad \#|\mathrm{Ell}_O(\mathbb{F}_q)| = O(\sqrt{q})\ )$$

Faithful: no group elements g (except the identity) satisfies $g*x = x$ for all x in $\mathrm{Ell}_O(\mathbb{F}_q)$.

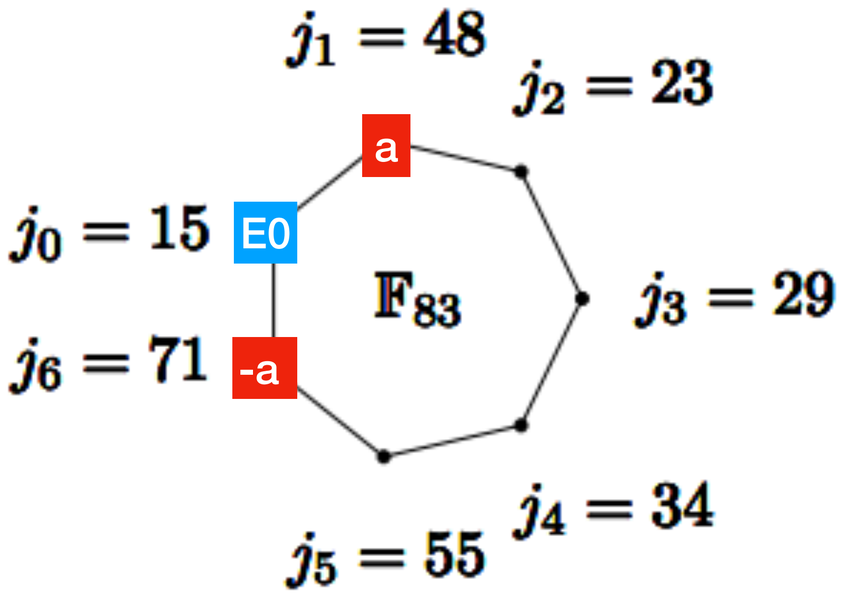
Transitive: for all x, y in $\mathrm{Ell}_O(\mathbb{F}_q)$, there is a g in CL(O) satisfies $g*x = y$.

Example



Example: a connecting component over F_{83}, degree L = 3.

Example



Representing the class group G = CL(D), with D = -251, #|G| = 7

Let j_0 represent the identity of G.

Let j_1 represents an element a of norm 3 in G (i.e. $a * E_0 = E_1$),

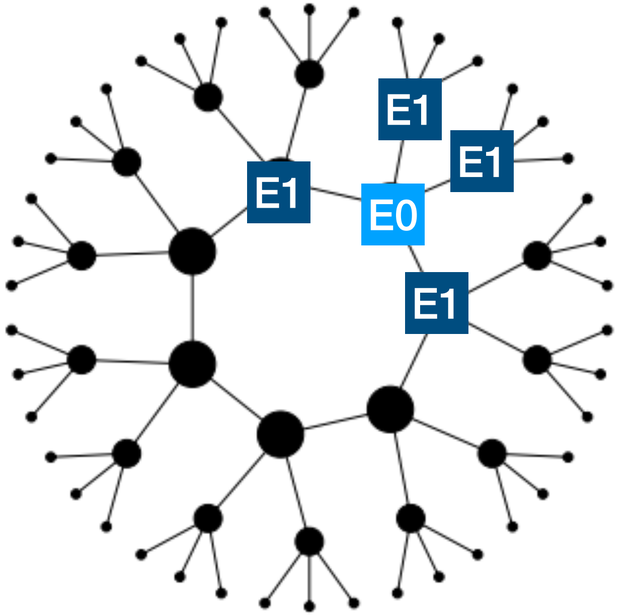
then j_6 represents -a (i.e. $-a * E_0 = E_6$)

Road map

1. ~~Elliptic curve isogenies can be represented by a graph.~~
2. ~~Isogeny graphs can be used to represent a group.~~
3. Over finite fields, searching for close neighbors on the graph is easy.
4. Over an RSA modulus N, finding certain neighbors is hard.
5. Hardness of finding certain neighbors => hardness of inverting group elements

Computational problems for isogeny over a finite field

Q1: Fix a polynomially large degree L, given a curve E_0, is there a polynomial time algorithm that finds all of its L-isogenous neighbors?



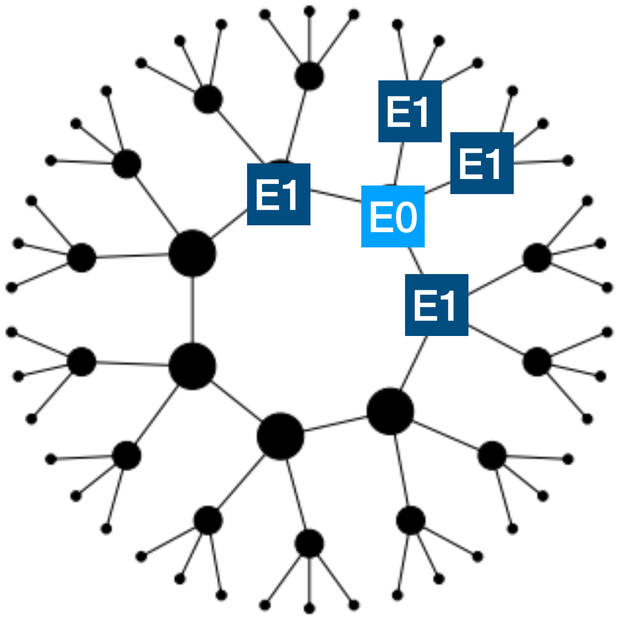
Computational problems for isogeny over a finite field

Q1: Fix a polynomially large degree L, given a curve E_0, is there a polynomial time algorithm that finds all of its L-isogenous neighbors?

Answer: Yes. There are two ways.

(1) Use Velu's formulae

(2) Find (the j invariant of) **E1** by solving modular polynomials,



Modular polynomials

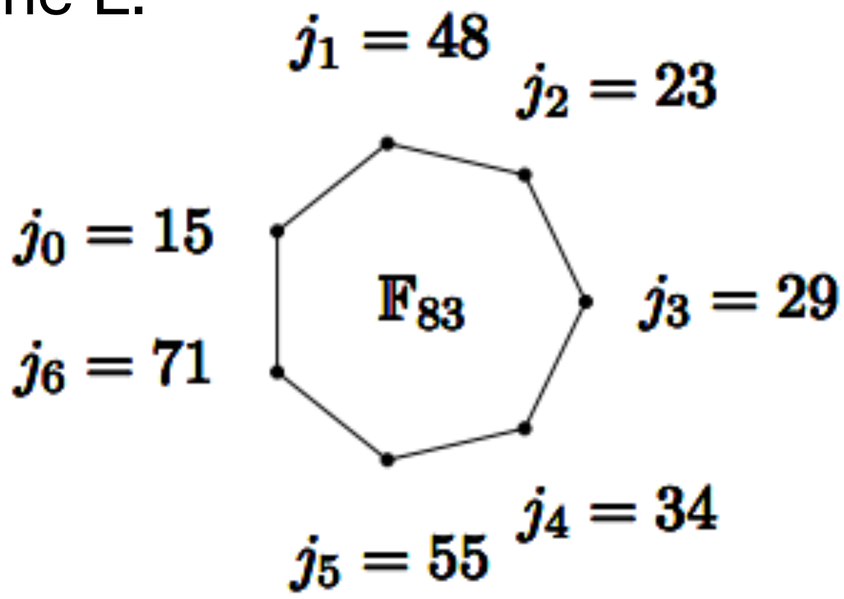
For all L>0, the L-th modular polynomial Ψ_L parameterizes pairs of elliptic curves related by an L-cyclic isogeny:

$\Psi_L(j_1, j_2) = 0$ if j_1 and j_2 are the j-invariants of L-isogenous elliptic curves.

$\Psi_L(x, y)$ has integer coefficients. Has degree L+1 for prime L.

In theory, Ψ_L is computable in polynomial time in L.

In practice, the coefficients are very large.



Computational problems for isogeny over a finite field

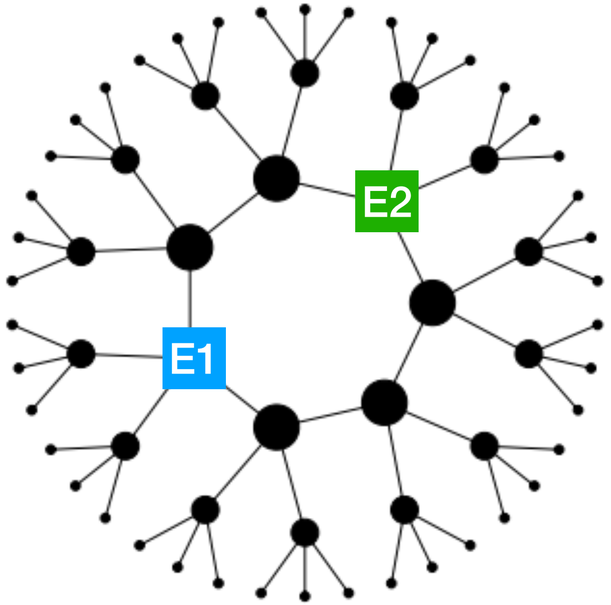
Q2: Randomly select two curves E_1 and E_2 from the graph, find an explicit isogeny between them.

Current status: conjectured to be hard, even for quantum computers.

[Couveignes 97], [Rostovtsev, Stolbunov 06]: post-quantum key-exchange

SIDH [De Feo, Jao 11]

CSIDH [Castryck, Lange, Martindale, Panny, Renes 18]



Road map

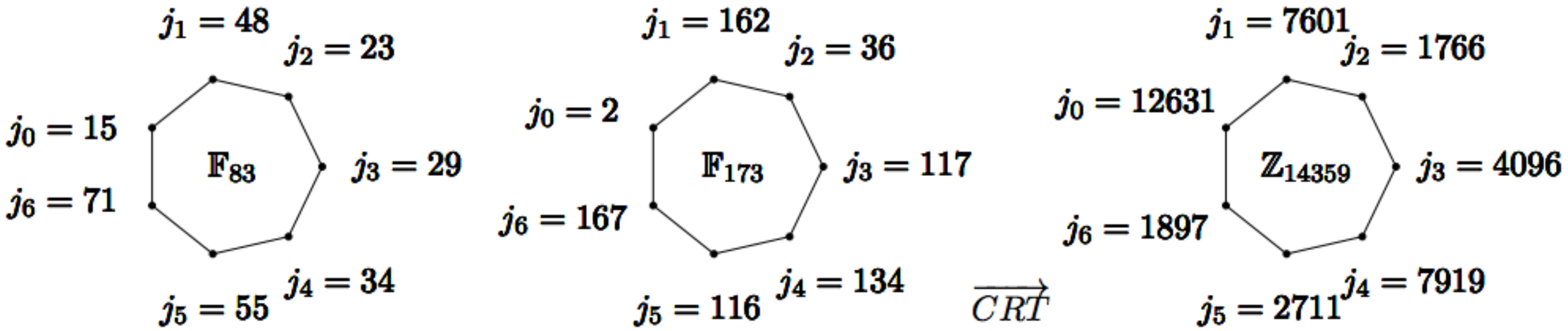
1. ~~Elliptic curve isogenies can be represented by a graph.~~
2. ~~Isogeny graphs can be used to represent a group.~~
3. ~~Over finite fields, searching for close neighbors on the graph is easy.~~
4. Over an RSA modulus N, finding certain neighbors is hard.
5. Hardness of finding certain neighbors => hardness of inverting group elements

Computational problems for isogeny over an RSA modulus N

How to define an isogeny graph mod N:

1. The general case: j_1, j_2 are connected if $\Psi_L(j_1, j_2) = 0 \bmod N$.
2. The special case: Assume the isogeny volcanoes over F_p and F_q have the same structure, then fix j_0 and a direction, take CRT.

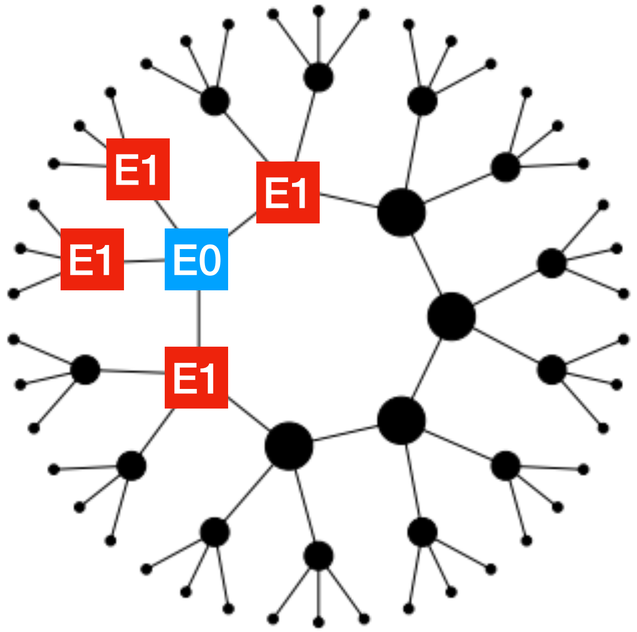
Example: Representing G = CL(-251),



Computational problems for isogeny over an RSA modulus N

Basic neighbor search: Fix a poly degree L, given a curve E_0 (its j-invariant mod N), is there a polynomial time algorithm that finds its L-isogenous neighbors?

Current status: seems to be hard.



Computational problems for isogeny over an RSA modulus N

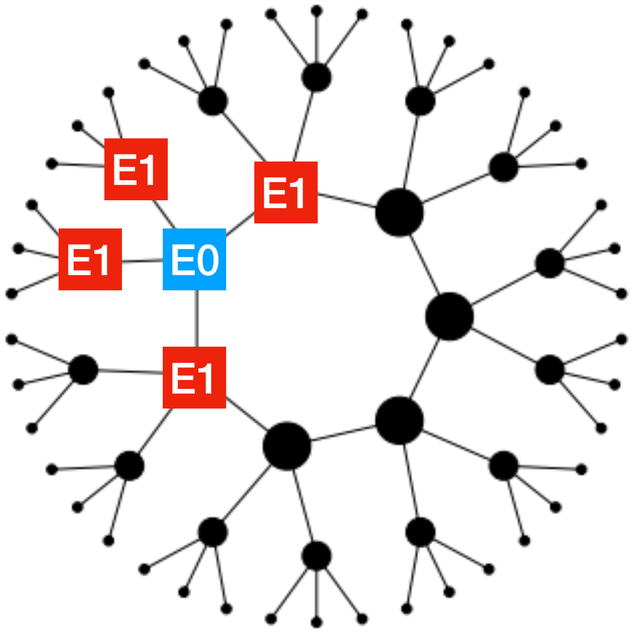
Basic neighbor search: Fix a poly degree L, given a curve E_0 (its j-invariant mod N),

is there a polynomial time algorithm that finds its L-isogenous neighbors?

Current status: seems to be hard.

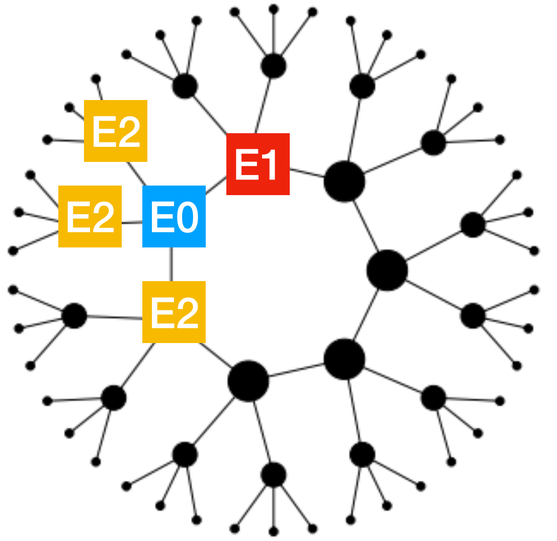
The two methods over the finite field don't work.

Since they both require solving high degree polynomial mod N!



Computational problems for isogeny over an RSA modulus N

Joint-neighbor-search problem: Fix a degree L, given two curves E_0, E_1, find E_2 that is L-isogenous to E_0, and L^2-isogenous to E_1?

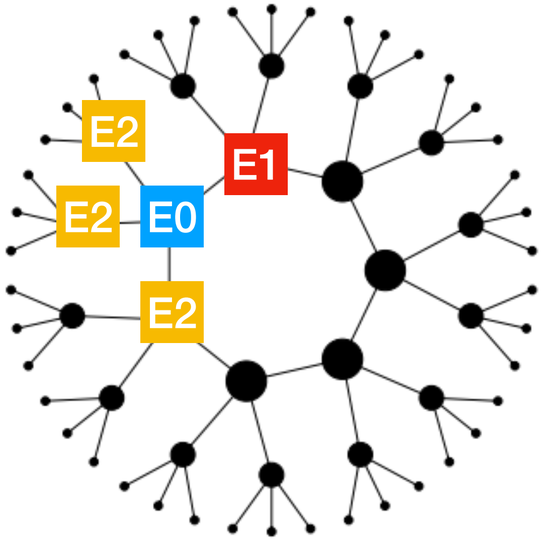


Current status: also seems to be hard.

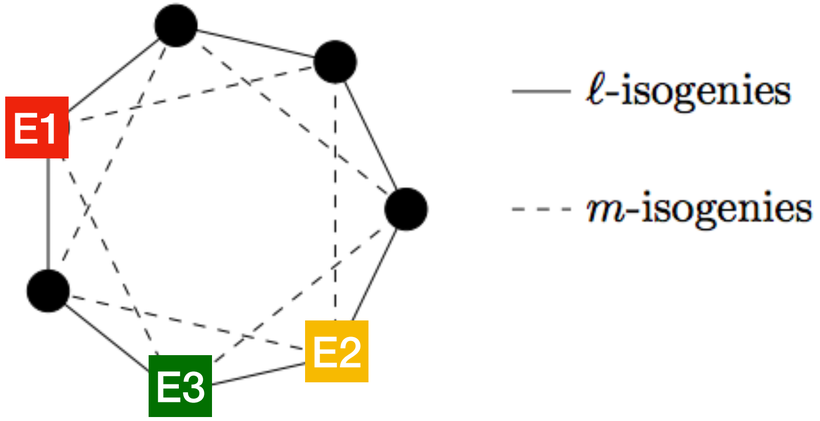
Natural attempt: take the gcd of $\Psi_L(j_0, x)$ and $\Psi_{L^2}(j_1, x)$, but the resulting polynomial has degree L, not 1.

Computational problems for isogeny over an RSA modulus N

Joint-neighbor-search problem: Fix a degree L, given two curves E_0, E_1, find E_2 that is L-isogenous to E_0, and L^2-isogenous to E_1?



Current status: also seems to be hard.



But for ***coprime*** degree joint neighbors,

gcd of $\Psi_M(j_1, x)$ and $\Psi_L(j_2, x)$ gives a linear function

[Enge, Sutherland 10].

Road map

1. ~~Elliptic curve isogenies can be represented by a graph.~~
2. ~~Isogeny graphs can be used to represent a group.~~
3. ~~Over finite fields, searching for close neighbors on the graph is easy.~~
4. ~~Over an RSA modulus N, finding certain neighbors is hard.~~
5. Hardness of finding certain neighbors => hardness of inverting group elements.

Trapdoor group with infeasible inversion

Trapdoor: p, q, the discriminant D (which determines End(E_0)), invariants of CL(D)

Public parameter: $N = pq$, $j_0 = j(E_0)$

Encoding of an class group element **a**:

Canonical encoding of **a**: $j(E_a)$ such that $E_a = a * E_0$

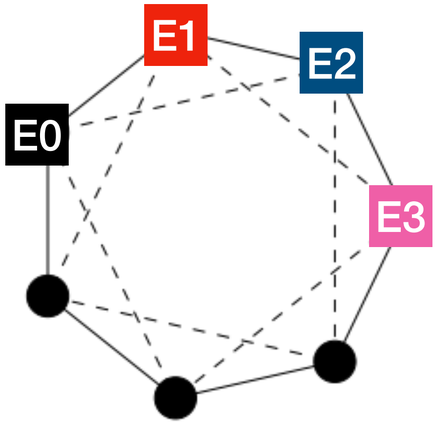
Composable encoding of **a**: factorize **a** into ***poly-smooth ideals***,

publish the canonical encoding and the norm of each of them.

Infeasibility of inversion: (L, L^2)-joint neighbor problem*

Feasibility of composition*: when the norms of the

ideals are ***coprime***, then gcd of modular polys is linear.



The difficulties in generating the parameters efficiently

Parameters: p, q, E_0 s.t. $End(E_0/F_p) = End(E_0/F_q) = O$ of disc D.

Want D to be exponentially large (so that CL(D) is exponentially large).

Problem: how to find E_0, p, q, with a given exponentially large discriminant D.

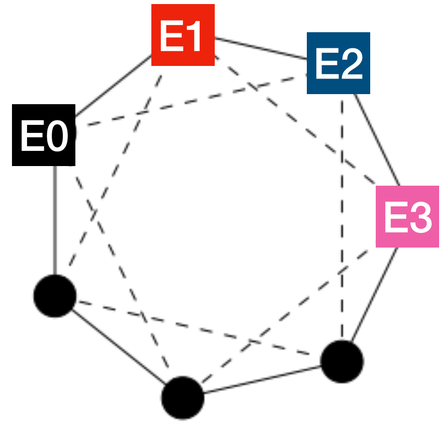
(The CM method only works when |D| is a polynomial, or $<10^{14}$ in practice)

Solution: Can let $D = (f_1 \ldots f_k)^2 \cdot D_0$ s.t. all the factors are poly

=> the order of CL(D) is large but smooth, need to make sure the order is hidden.

=> Also need a short relation basis of CL(D).

New Record: D with 154 digits [Beullens, Kleinjung, Vercauteren 19]



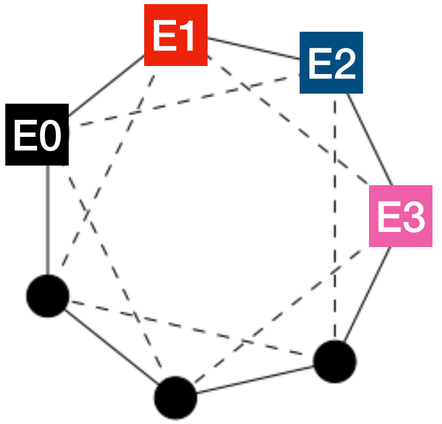
Cryptanalysis attempts (more: Section 5 of the paper)

The attacker sees:

The modulus N, and a bunch of j-invariants of isogenous curves.

We conjecture that the attacker cannot get:

1. p and q such that pq = N
2. The number of points of $E_0(Z_N)$
3. The discriminant D
4. The group size of CL(D)

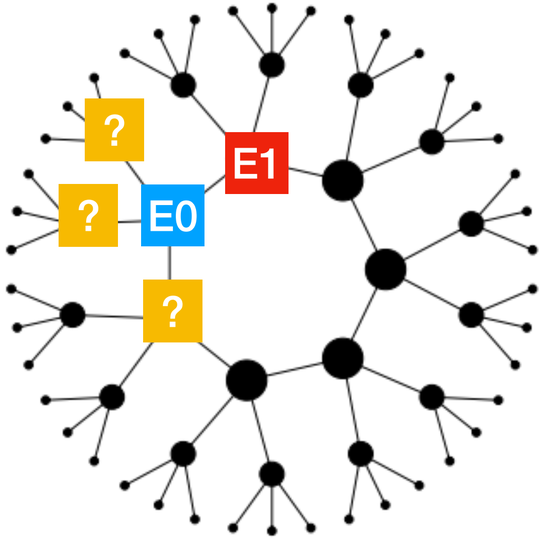


Summary:

We propose a candidate trapdoor group with infeasible inversion from elliptic curve isogeny (available on eprint 2018/926).

Main assumption: (L, L^2)-neighbor search problem on the isogeny graphs defined over RSA moduli

Applications of GII: broadcast encryption, directed transitive signatures, maybe more…



Thanks for your time!