AWS 2026

Lecture 1: Isogeny-based cryptography

Kirsten Eisenträger

One source of computational problems:

- of intrinsic interest to number theorists over $\mathbb{Z}$: primality testing, factoring

  over number fields: compute rings of integers, discriminants, class groups, unit groups

- other source of problems: cryptography

  in public-key cryptography, all known constructions rely on rely on hard number-theoretic problems.

system	underlying hard? problem
RSA	factoring
elliptic curve cryptography (ECC)	ell. curve discrete log problem

broken by quantum algorithm

lattice-based systems Ring-LWE	shortest vector problem in ideal lattices
isogeny-based systems	compute isogenies between supersingular elliptic curves

Post-quantum cryptography

develop public-key crypto secure against quantum computers

NIST competition: seeks to find these

Supersingular isogeny-based cryptography

Fix large prime p: use exponentially large set of ell. curves in char p and isogenies between them

supersingular

$\approx p/12$ supersingular ell. curves in char p

input size: $\log p$

$p/12$ is exponential in $\log p$.

Elliptic curves and isogenies

k = fin. field of char $p > 3$

$E: y^2 = x^3 + ax + b$ $\quad a, b \in k$ s.t. $4a^3 + 27b^2 \neq 0$

is an ell. curve.

Points on E: (x, y) satisfying the curve equation + point at infinity

- points form an abelian group, point at ∞ = identity element

j-invariant $j(E) = \dfrac{256 \cdot 27 \cdot a^3}{4a^3 + 27b^2}$

$j(E_1) = j(E_2) \Leftrightarrow E_1$ and E_2 are isom. over $\bar{k}$.

An **isogeny** $\varphi : E_1 \to E_2$ is a rational map that is also a group homomorphism.

degree of φ = degree of φ as a rational map

When $(\deg \varphi, p) = 1$: φ is separable and $\#\ker \varphi = \deg \varphi$.

Given $\varphi : E_1 \to E_2$, there is an isogeny $\hat{\varphi} : E_2 \to E_1$ s.t. $\hat{\varphi} \circ \varphi : E_1 \to E_1$ mult. by $\deg \varphi$ on E_1.

Thm: Let E/k be an ell. curve and $G \subseteq E(\bar{k})$ a fin. subgp. Then there exists an ell. curve E' and a sep. isogen $\varphi : E \to E'$ with $\ker \varphi = G$. E' and φ are defined over a fin. extn of k and unique up to isomorphism.

Can also factor an isogeny of composite degree into a sequence of isogenies of prime degree.

Supersingular ell. curves

k = finite field E/k.

- an endom. of E is an isogeny $E \to E$
- endomorphisms defined over k form a ring $\mathrm{End}(E)$.

two poss!

$$\mathrm{End}(E) \cong \begin{cases} 1. \text{ order in a quadratic imaginary field} \\ \quad \text{quad.} \\ 2. \text{ order in a quaternion algebra} \rightsquigarrow \text{non. comm.} \end{cases}$$

DEF E is supersingular

$\iff$ $\mathrm{End}(E)$ is an order in a quaterenion algebra

$G(p,\ell)$ supersingular isogeny graph

$\ell \neq p$ primes

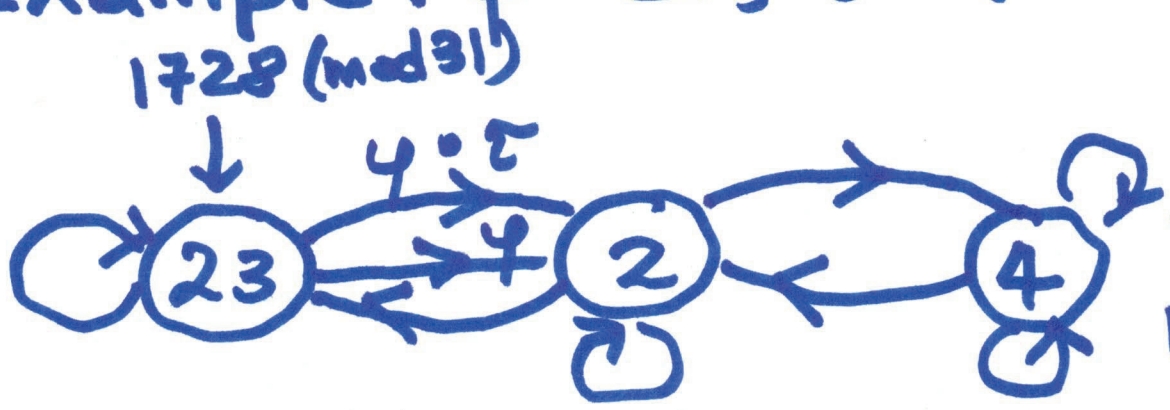
is a directed graph

- vertices : isom classes of supersing. ell. curves in char p
- directed edges from E_1 to E_2 correspond to isogenies of degree ℓ: $E_1 \to E_2$.

Properties of $G(p,\ell)$:

- (j_1, j_2) is connected by an edge $\iff$ (j_2, j_1) connected by an edge.
- $G(p,\ell)$ is $(\ell+1)$-regular for outgoing edges. ($E[\ell] \cong \mathbb{Z}/\ell \times \mathbb{Z}/\ell$ has $\ell+1$ subgroups of order ℓ.

Example: $p = 31$, $\ell = 2$



τ = autom. of E_1, $\deg$ with $j(E_1) = 23$ of order 4

dual isogeny of $\varphi \circ \tau$ and φ have the same kernel, so two edges $(23) \rightleftarrows (2)$, but only one going back.

$p \equiv 1 \pmod{12} \Rightarrow$ neither 0 or 1728 are supersingular j-invariants

$\Rightarrow$ in this case, can think of graph as undirected.

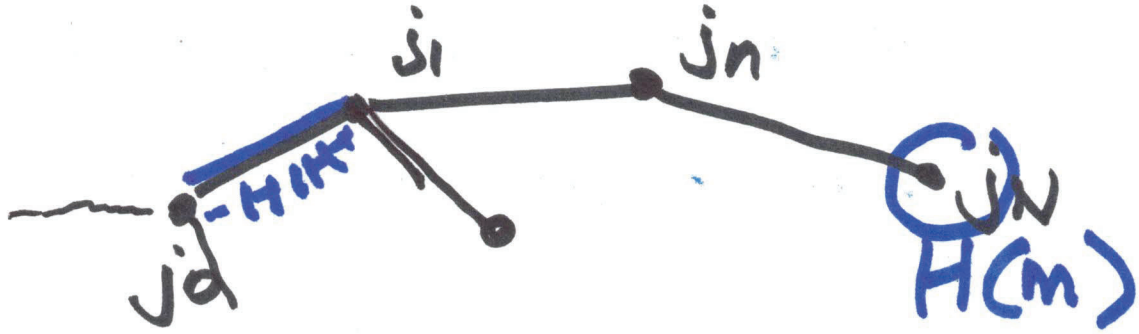
CGL hash function: $p \equiv 1 \pmod 8$

Setup: fix $j_0 \in G(p, \ell)$, $\ell = 2$
(j_0: incoming edge e_0)

Input: message $m = (m_1, \ldots, m_N) \in \{0,1\}^*$

construct a path in $G(p, \ell)$ of length N, label vertices $j_0, \ldots, j_N$.

Output: $H(m) = j_N$.



Goal: collisions should be hard to find for H.

"collision resistant"