Supersingular Isogeny Graphs in Cryptography

Kristin Lauter

Director, West Coast Labs

Meta AI Research

September 20, 2022

VANTAGE Seminar

PCMI Lectures Outline, July 2022

TA: Jana Sotáková

- First lecture: cryptography, quantum threat, hash function, SIG
- Second lecture: expander graphs, Ramanujan property, key exchange, generic attacks
- Third lecture: quaternion algebras, KLPT, signatures

Old talk, newer work

WIN4 (2017):

Ramanujan Graphs in Cryptography

Ana Costache, Brooke Feigon, K. Lauter, Maike Massierer, Anna Puskas

WINE3 (2018):

Explicit connections between supersingular isogeny graphs and Bruhat—Tits trees

Laia Amorós, Annamaria Iezzi, Kristin Lauter, Chloe Martindale, and Jana Sotáková

Silverberg (2019):

Adventures in Supersingularland

Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, Jana Sotáková

WIN5 (2020):

Orienteering with one endomorphism

Sarah Arpin, Mingjie Chen, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange, Ha T. N. Tran

Cryptography:

- The science of keeping secrets!
- But more than that…
  - Confidentiality
  - Authenticity
- Tools:
  - Encryption/Decryption
  - Digital signatures
  - Key exchange

Public Key Cryptography

- Key exchange: two parties agree on a common secret using only publicly exchanged information
- Signature schemes: allows parties to authenticate themselves
- Encryption: preserve confidentiality of data

- Examples of public key cryptosystems:

  RSA, Diffie-Hellman, ECDH, DSA, ECDSA

Public Key Cryptography deployed today:

Security is based on hard math problems:

- Factoring large integers
- Discrete logarithm problem in *(Z/pZ)**
- Discrete logarithm problem in elliptic curve groups
- Weil pairing on elliptic curves

Applications:

- Secure browser sessions (https: SSL/TLS)
- Signed, encrypted email (S/MIME)
- Virtual private networking (IPSec)
- Authentication (X.509 certificates)

Elliptic Curve Cryptography

- *p* a large prime of cryptographic size
- Elliptic Curve defined by short Weierstrass equation:

$$E_1 : y^2 = x^3 + ax + b$$

- Labeled by j-invariants: *isomorphism invariant over $F_p$bar*

$$j(E_1)= 1728*4a^3/(4a^3+27b^2)$$

- Algebraic group with group law (chord and tangent method)
- *Supersingular* elliptic curves modulo p: *no p-torsion points over $F_p$bar*

    Isomorphism class has a representative defined over $GF(p^2)$ (or GF(p))

    Endomorphism ring isomorphic to maximal order in definite quaternion algebra

What do we mean by “hard” math problem?

Input represented by *m* bits:

Then the best known attack on the system runs in exponential time in *m*.

exponential time in *m*	$O(2^m)$
sub-exponential time in *m*	$O(e^{c*m\char94 1/3\ (\log m)\char94 2/3})$
polynomial time in *m*	*O(polynomial in m)*

Example: to factor $n = p*q$ where $m = \log n$,

trial division takes *exponential time*

The Quantum threat:

Polynomial time Quantum algorithms for attacking current systems!

m = # bits

- Shor's algorithm for factoring $4m^3$ time and 2m qbits
- ECC attack requires $360m^3$ time and 6m qbits

  [Proos-Zalka, 2004]

Conclusion:

- RSA: m = 2048
- Discrete log m = 2048
- Elliptic Curve Cryptography m = 256 or 384

are not resistant to quantum attacks once a quantum computer exists at scale!

Timeline for Elliptic Curve Cryptography

- (2006) Suite B set requirements for the use of Elliptic Curve Cryptography
- (2016) CNSA requirements increase the minimum bit-length for ECC from 256 to 384. Advises that adoption of ECC not required.
- (2017) NIST international competition to select post-quantum solutions: 5-year PQC Competition

Post-quantum cryptography

Submissions to the NIST PQC competition based on hard math problems:

- Code-based cryptography (McEliece 1978)
- Multivariate cryptographic systems (Matsumoto-Imai, 1988)
- Lattice-based cryptography (Hoffstein-Pipher-Silverman, NTRU 1996)
- Supersingular Isogeny Graphs (Charles-Goren-Lauter 2005)

- Challenge! Need to see if these new systems are resistant to *both* classical and quantum algorithms!

Supersingular Isogeny Graphs

New hard problem introduced in 2005: [Charles-Goren-Lauter]

- *Finding paths between nodes in a Supersingular Isogeny Graph*

Graphs: G = (V, E) = (vertices, edges)

- k-regular, undirected graphs, with optimal expansion
- No known efficient routing algorithm

Application: Cryptographic Hash functions

A *hash function* maps bit strings of some finite length to bit strings of some fixed finite length

$$h : \{0,1\}^n \rightarrow \{0,1\}^m$$

- easy to compute
- unkeyed (do not require a secret key to compute output)
- Collision resistant
- Uniformly distributed output

Collision-resistance

- A hash function *h* is *collision resistant* if it is computationally infeasible to find two distinct inputs, *x, y*, which hash to the same output

$$h(x) = h(y)$$

- A hash function h is *preimage resistant* if, given any output of h, it is computationally infeasible to find an input, x, which hashes to that output.

Application: cryptographic hash function [CGL'06]

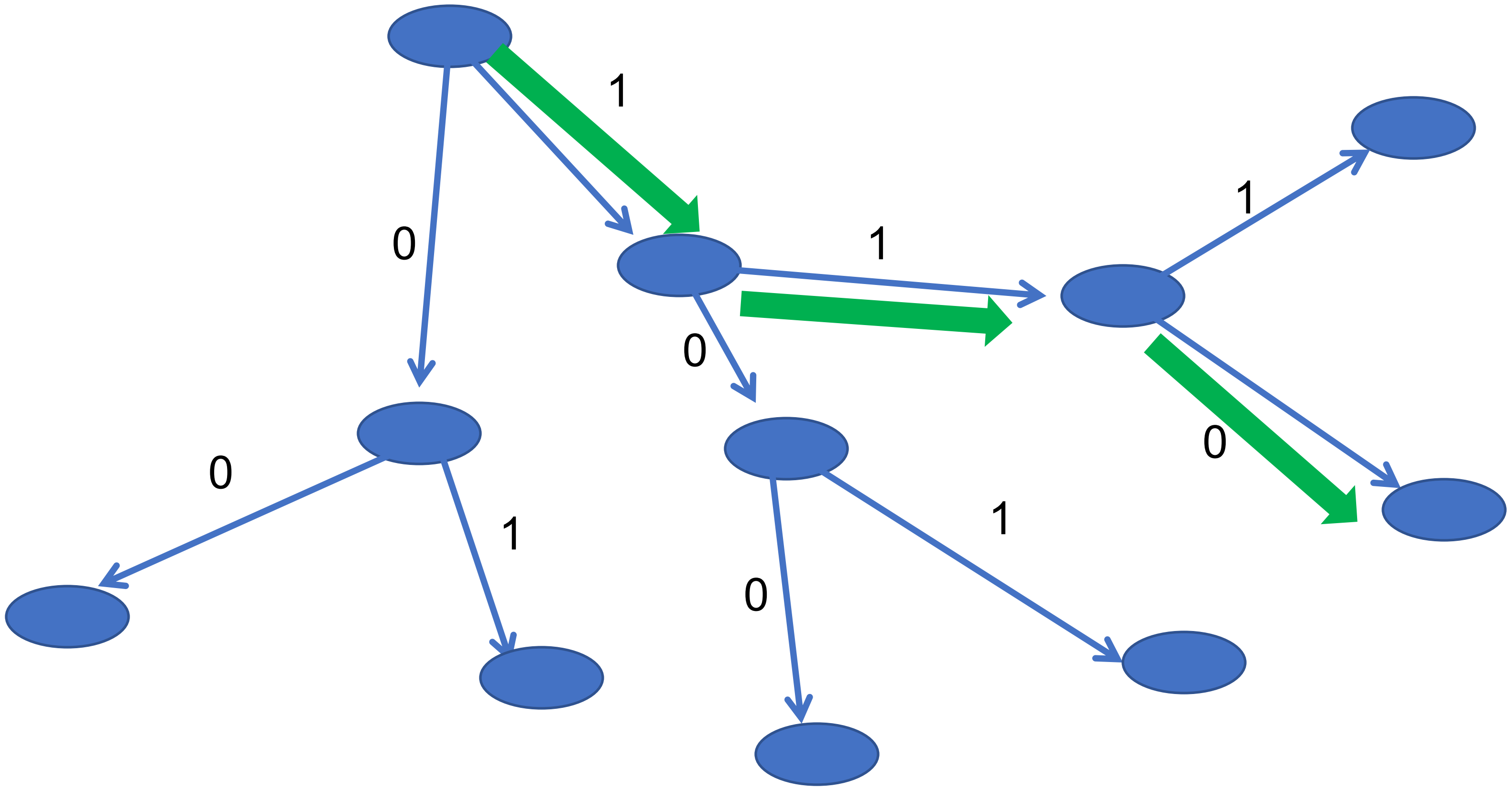
- k-regular graph G
- Each vertex in the graph has a label

Input: a bit string

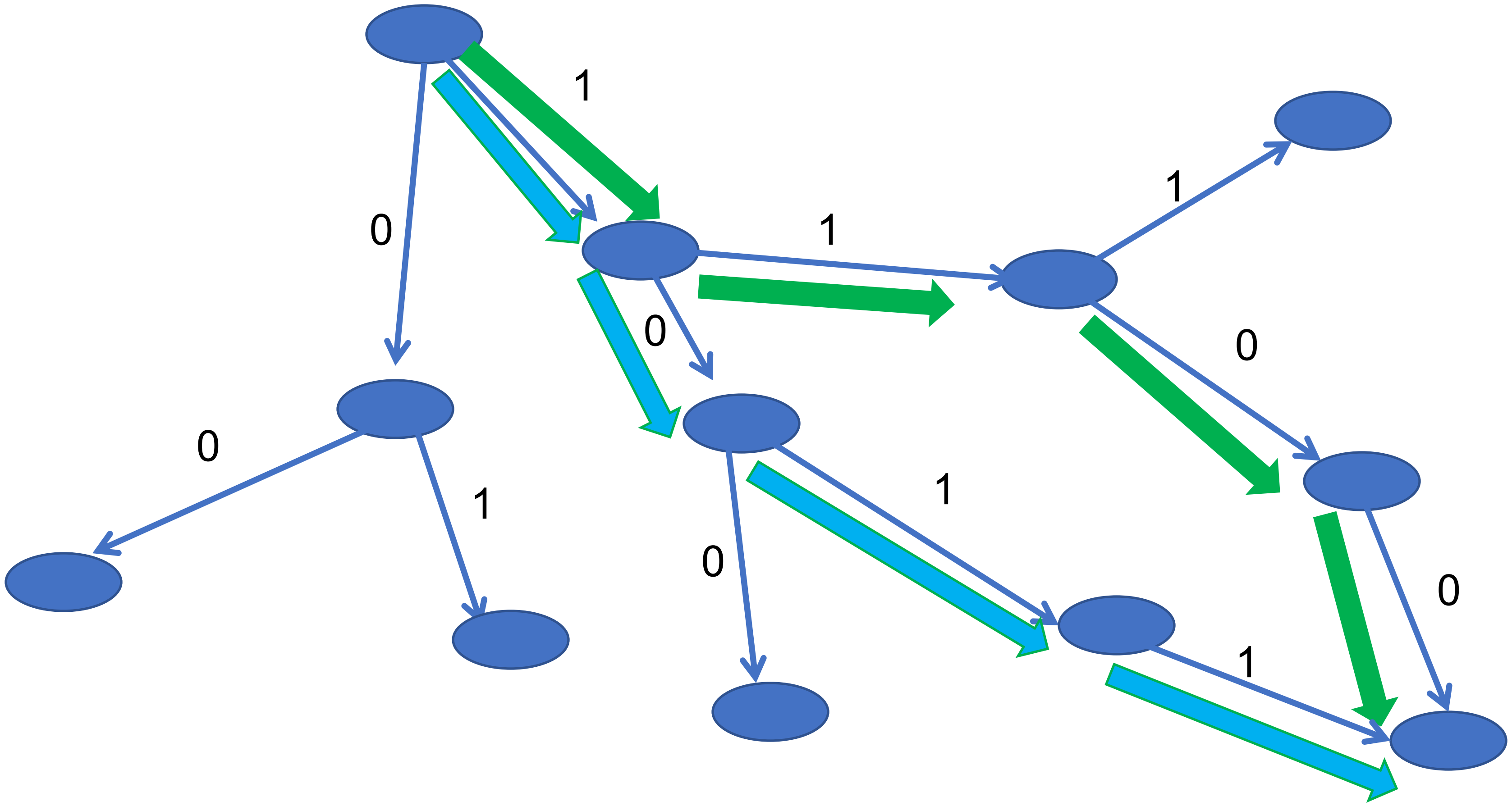
- Bit string is divided into blocks
- Each block used to determine which edge to follow for the next step in the graph
- No backtracking allowed!

Output: label of the final vertex of the walk

Walk on a graph: 110



Colliding walks: 1100 and 1011



Simple idea

- Random walks on *expander* graphs are a good source of pseudo-randomness
- Are there graphs such that finding collisions is hard? (i.e. finding distinct paths between vertices is hard)
- Bad idea: hypercube (routing is easy, can be read off from the labels)

What kind of graph to use?

- Random walks on *expander* graphs mix rapidly: ~log(p) steps to a random vertex, p ~ #vertices

- *Ramanujan* graphs are optimal expanders

- To find a collision: *find two distinct walks of the same length which end at same vertex*

Graph of supersingular elliptic curves modulo p with isogeny edges (Pizer/Mestre graphs)

- Vertices: supersingular elliptic curves mod p
    - Curves are defined over $GF(p^2)$ (or $GF(p)$)

- Labeled by j-invariants
    - $E_1 : y^2 = x^3 + ax + b$
    - $j(E_1)= 1728*4a^3/(4a^3+27b^2)$

- Edges: Isogenies between elliptic curves

Supersingular Isogeny Graphs: edges

- Edges: degree ℓ isogenies between elliptic curves
  - k = ℓ+1 – regular
  - Undirected if we assume p == 1 mod 12
  - Graph is Ramanujan (Deligne, …)

Isogenies

- The degree of a separable isogeny is the size of its kernel
- To construct an ℓ -isogeny from an elliptic curve E to another, take a subgroup-scheme C of size ℓ, and take the quotient E/C.
- Formula for the isogeny and equation for E/C were given by Velu.

One step of the walk: (ℓ=2)

$E_1 : y^2 = x^3 + ax + b$

- $j(E_1)=1728*4a^3/(a^3+27b^2)$
- 2-torsion point $Q = (r, 0)$

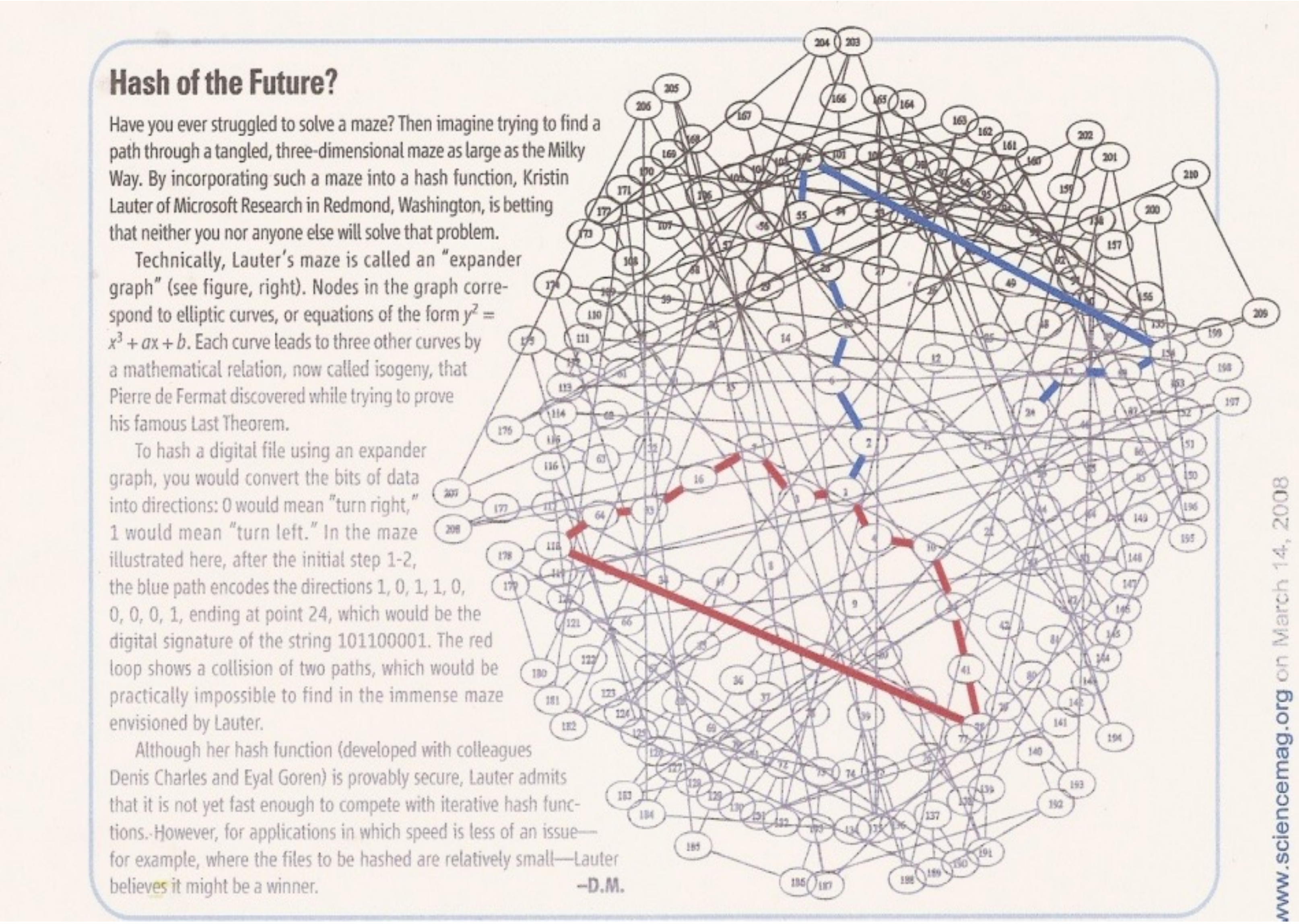
$E_2 = E_1 /Q$ (quotient of groups)

- $E_2 : y^2 = x^3 - (4a + 15r^2)x + (8b - 14r^3)$.

$E_1 \rightarrow E_2$

$(x, y) \rightarrow (x +(3r^2 + a)/(x-r), y - (3r^2 + a)y/(x-r)^2)$

Science magazine 2008



Hash of the Future?

Have you ever struggled to solve a maze? Then imagine trying to find a path through a tangled, three-dimensional maze as large as the Milky Way. By incorporating such a maze into a hash function, Kristin Lauter of Microsoft Research in Redmond, Washington, is betting that neither you nor anyone else will solve that problem.

Technically, Lauter's maze is called an "expander graph" (see figure, right). Nodes in the graph correspond to elliptic curves, or equations of the form $y^2 = x^3 + ax + b$. Each curve leads to three other curves by a mathematical relation, now called isogeny, that Pierre de Fermat discovered while trying to prove his famous Last Theorem.

To hash a digital file using an expander graph, you would convert the bits of data into directions: 0 would mean "turn right," 1 would mean "turn left." In the maze illustrated here, after the initial step 1-2, the blue path encodes the directions 1, 0, 1, 1, 0, 0, 0, 0, 1, ending at point 24, which would be the digital signature of the string 101100001. The red loop shows a collision of two paths, which would be practically impossible to find in the immense maze envisioned by Lauter.

Although her hash function (developed with colleagues Denis Charles and Eyal Goren) is provably secure, Lauter admits that it is not yet fast enough to compete with iterative hash functions. However, for applications in which speed is less of an issue—for example, where the files to be hashed are relatively small—Lauter believes it might be a winner.

–D.M.

History of Isogeny-based Cryptography

- Charles-Goren-Lauter presented at NIST 2005 competition,
  - IACR eprint 2006, published J Crypto 2009
- Later in 2006, two papers on eprint, never published:
  - Couveignes, ordinary case (Hard Homogeneous Spaces)
  - Rostovtsev-Stolbunov, ordinary case (Encryption)
- Ordinary case is very different for many reasons:
  - Volcano structure of graph
  - Action of an abelian class group

Other graphs

- Vary the isogeny degree
- Lubotzky-Phillips-Sarnak graph
  - Cycles found: Eurocrypt 2008, Zemor-Tillich
  - Preimages found: SCN 2008, Petit-Quisquater-Lauter
    - LPS "path-finding" now used for quantum arithmetic (aka Ross-Selinger)
- Morgenstern graph, [Petit-Quisquater-Lauter 08]
- Genus 2 and Higher dimensional analogues
  - Superspecial abelian surfaces [Charles-Goren-L 07]
- Add level structure: [Arpin'22]

Adding Level Structure to Supersingular Elliptic Curve Isogeny Graphs

“Isogenies in Cryptography” ongoing work:

- Alternate graphs/protocols:
  - CSIDH: Castryck-Lange-Martindale-Panny-Renes
- Dimension 2 analogues:
  - Decru, Flynn, Wesolowski, Jetchev, Florit, Smith …
- Signatures:
  - Vercauteren et al., Beullens,…
- Attacks:
  - Petit, Biasse, Bernstein, Stange, …
- Graph structure:
  - Kohel, Arpin et al.

Newer attack strategies:

Adventures in Supersingularland

Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, Jana Sotáková

- SIG has a "spine" and symmetry: an involution which fixes the F_p-points
- Volcanoes from the ordinary graph (fixed CM by an imaginary quadratic field) embed into SIG via "stacking, folding, and attaching"
- Experimental results on:
  - Distance to the spine
  - Mirror paths
  - Expansion constant

Orienteering with one endomorphism

Sarah Arpin, Mingjie Chen, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange, Ha T. N. Tran

- Given one endomorphism, can use the volcanoes corresponding to that CM field to find cycles and paths in the SIG graph

Computing endomorphism rings is hard

Exponential algorithms:

[Kohel 96]: find cycles in the graph via random walks

[Cervino 03], [Lauter-McMurdy 03]: compute # of norm n elements in maximal order, compare with # of isogenies of degree n which are endomorphisms

Recent work on equivalences:

Supersingular isogeny graphs and endomorphism rings: reductions and solutions

K Eisenträger, S Hallgren, K Lauter, T Morrison, C Petit

The supersingular isogeny path and endomorphism ring problems are equivalent

Benjamin Wesolowski

Cycles in the Supersingular ℓ-Isogeny Graph and Corresponding Endomorphisms

E Bank, C Camacho-Navarro, K Eisenträger, T Morrison, J Park

Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs

K Eisenträger, S Hallgren, C Leonardi, T Morrison, J Park

Supersingular Isogeny Graphs in Cryptography

PCMI Lecture #2

Kristin Lauter

Meta (Facebook) AI Research/University of Washington

TA: Jana Sotakova

Expander graphs

G = (V,E) a graph with vertex set V and edge set E.

A graph is k-regular if each vertex has k edges coming out of it.

Def: An *expander graph* with N vertices has *expansion constant or Cheeger constant,* $c > 0$, if for any subset U of V of size

$$|U| \leq N/2,$$

the boundary of U, Γ(U) := neighbors of U not in U, satisfies

$$|\Gamma(U)| \geq c|U|.$$

Expansion constant

The adjacency matrix $A(\ell) = (a_{ij})$ is defined by

$$a_{ij} := \#\text{ edges from } i^{th} \text{ vertex to } j^{th} \text{ vertex in the } \ell\text{-isogeny graph}$$

The adjacency matrix of an undirected graph is symmetric, and therefore all its eigenvalues are real.

For a connected k-regular graph, the largest eigenvalue is k, and all others are strictly smaller

$$k > \mu_1 \geq \mu_2 \geq \cdots \geq \mu_{N-1}$$

Then the expansion constant c can be expressed in terms of the eigenvalues as follows:

$$c \geq 2(k - \mu_1)/(3k - 2\mu_1)$$

Therefore, the smaller the eigenvalue μ_1, the better the expansion constant.

Ramanujan graphs

Theorem (Alon-Boppana)

X_m an infinite family of connected, k-regular graphs, (with the number of vertices in the graphs tending to infinity), then

$$\liminf \mu_1(X_m) \geq 2\sqrt{(k-1)}$$

Definition: A *Ramanujan graph* is a k-regular connected graph satisfying

$$\mu_1 \leq 2\sqrt{(k-1)}$$

In our case $k = \ell + 1$

Ramanujan property for SIG

$S_2(p)$ = vector space of weight-2 cusp forms of level p

Action of Hecke operator T_ℓ given by the Brandt matrix $B(\ell)=A(\ell)$

[Mestre, La Methode des graphes] English translation: https://wstein.org/papers/rank4/mestre-en.pdf

Eigenvalues of this matrix satisfy the Ramanujan condition

For higher-dimensional analogue, see [CGL'07]:

https://www.math.mcgill.ca/goren/PAPERSpublic/FinalRamanujan.pdf

Approximating the uniform distribution

For non-back-tracking walks on a 3-regular graph, if there are no collisions, then you reach

2^n vertices after n steps

So for optimal expander graphs, we expect diameter to be roughly

$\log(|G|)$

Also note: most pairs of vertices are not connected by paths which are significantly shorter than $\log(|G|)$.

Applications of SIG

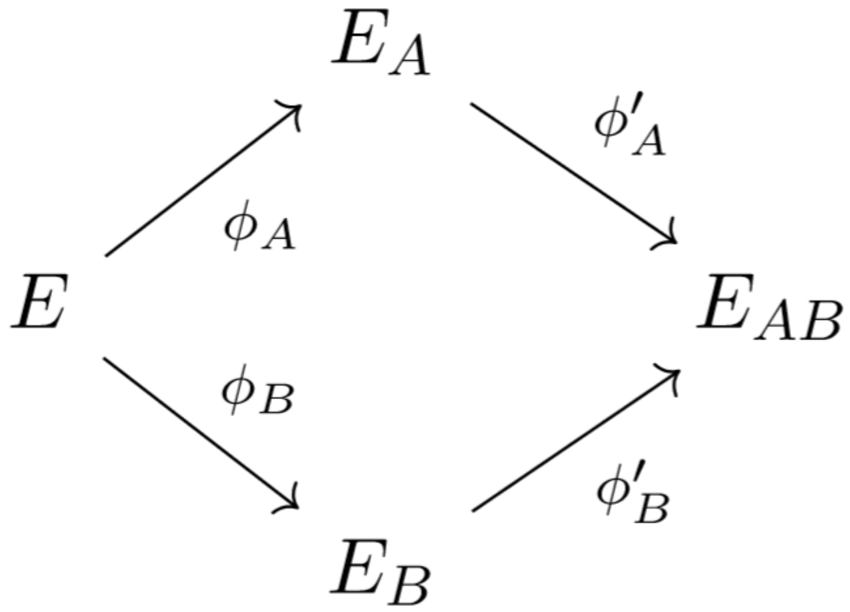
Proposed as basis for other cryptosystems:

Key exchange: Jao-De Feo 2011

Encryption: Jao-De Feo-Plut, 2014

Signatures: Galbraith-Petit-Silva 2016, SQIsign 2020

Key Exchange [Jao-DeFeo-Plut'11]



Key Exchange set-up

E: supersingular elliptic curve over GF(p^2)

$p = \ell_A^m \ \ell_B^n + 1$

ℓ_A and ℓ_B distinct primes (e.g. $\ell_A = 2$ and $\ell_B = 3$)

A and B want to exchange a key.

Public parameters:

A picks P_A, Q_A such that $< P_A, Q_A > = E[\ell_A^m]$

B picks P_B, Q_B such that $< P_B, Q_B > = E[\ell_B^n]$

Key Exchange (continued)

Secret parameters:

A picks two random integers m_A, n_A

A uses Velu's formulas to compute the isogeny

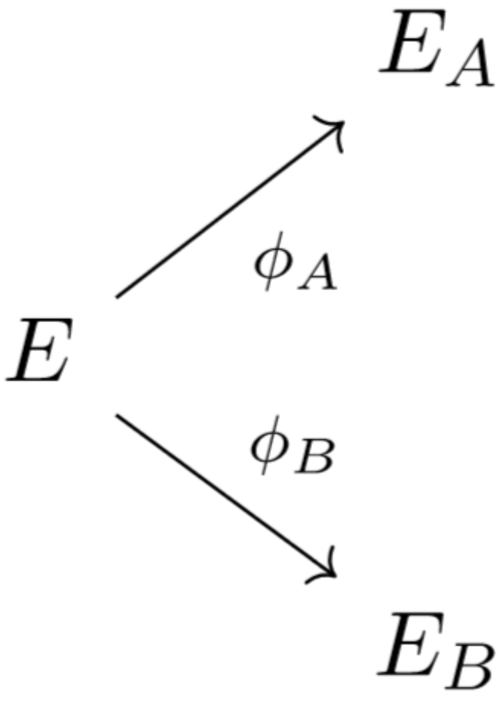
$$\varphi_A : E \longrightarrow E_A := E / < m_A P_A + n_A Q_A >$$

B picks two random integers m_B, n_B

B uses Velu's formulas to compute the isogeny

$$\varphi_B : E \longrightarrow E_B := E / < m_B P_B + n_B Q_B >$$

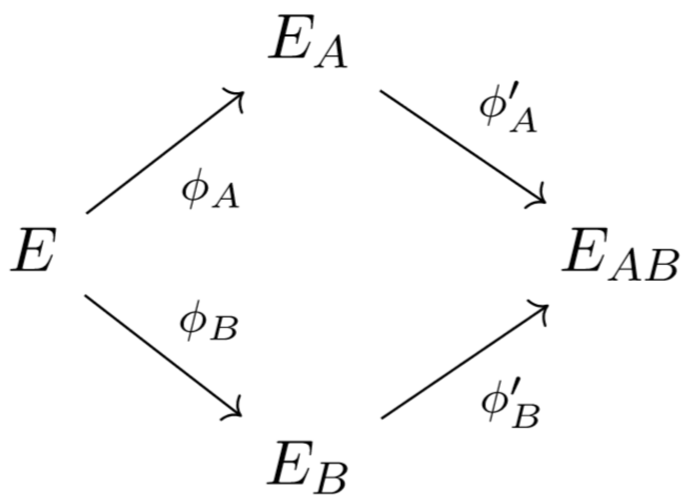
A and B have constructed the following diagram.



To complete the diamond, A and B exchange information:

A computes the points $\varphi_A(P_B)$ and $\varphi_A(Q_B)$ and sends $\{\varphi_A(P_B), \varphi_A(Q_B), E_A\}$ to B

B computes the points $\varphi_B(P_A)$ and $\varphi_B(Q_A)$ and sends $\{\varphi_B(P_A), \varphi_B(Q_A), E_B\}$ to A



The j-invariant of the curve E_{AB} is the shared secret.

Security of Key Exchange:
relies on CGL path-finding problem

If you can find the path between E and $E_{A,}$

then you can break the Key Exchange.

Note that the walks on each stage of the Key Exchange protocol are of *length roughly ½ the diameter*!

- Thus the probability that there exists a path between any 2 nodes is roughly $p^{(-1/2)}$
- So if you can find any path, it is overwhelming likely to be the path used in the Key Exchange.

Reduction result from WIN4 paper 2017

[Costache-Feigon-Lauter-Massierer-Puskas]

Theorem 5.3 *[CFLMP18] Assume as for the Key Exchange set-up that* $p = \ell_A^n \cdot \ell_B^m + 1$ *is a prime of cryptographic size, i.e.* $\log(p) \geq 256$, ℓ_A *and* ℓ_B *are small primes, such as* $\ell_A = 2$ *and* $\ell_B = 3$, *and* $n \approx m$ *are approximately equal. Given an algorithm to solve Problem 3.1 (Path-finding), it can be used to solve Problem 3.2 (Key Exchange) with overwhelming probability. The failure probability is roughly*

$$\frac{\ell_A^n + \ell_A^{n-1}}{p} \approx \frac{\sqrt{p}}{p}.$$

Hard Problems in SIG?

- **Problem 1 (collisions)** Produce a pair of supersingular elliptic curves, E_1 and E_2, and two distinct isogenies of degree ℓ^n between them.

- **Problem 2 (cycles)** Given E, a supersingular elliptic curve, find an endomorphism $f : E \rightarrow E$ of degree ℓ^{2n} , not the multiplication by ℓ^n map.

- **Problem 3 (paths)** Given two supersingular elliptic curves, find an isogeny of degree ℓ^n between them.

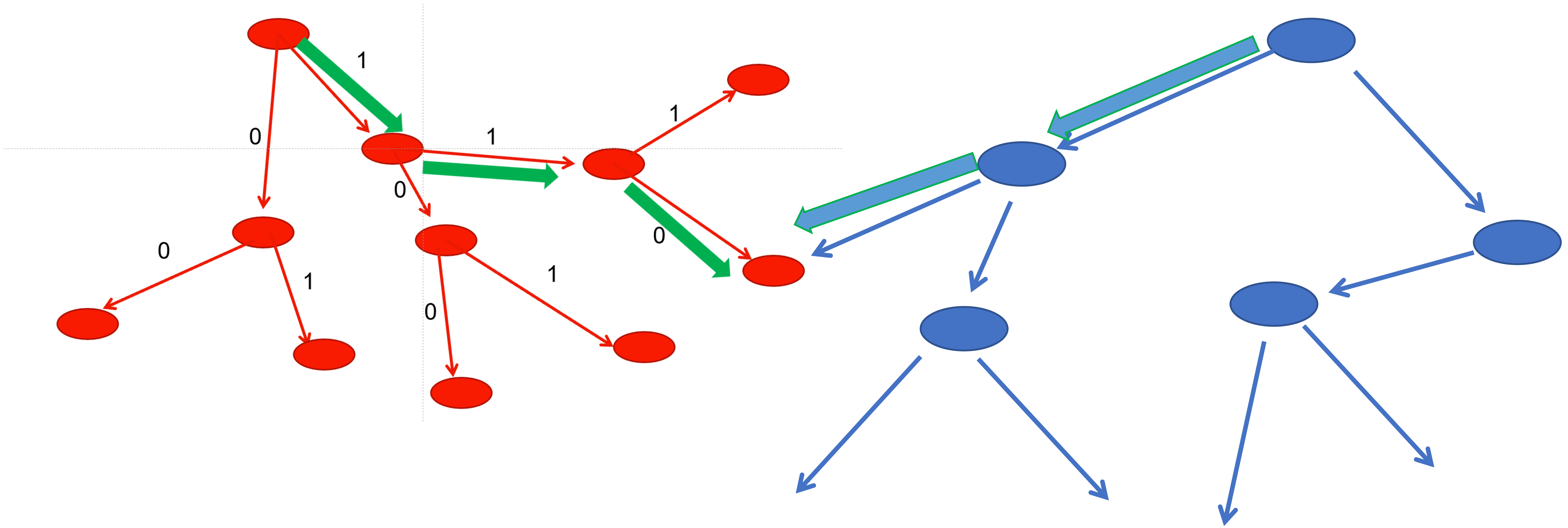
Hardness: Generic attacks

The best known classical attacks are generic square root attacks:

heuristic running time is exponential: $\sqrt{(|G|)}$

Birthday attack: randomly walk from the two endpoints until you find a collision

Generic Square Root Attack



Supersingular Isogeny Graphs in Cryptography

PCMI Lecture #3

Kristin Lauter

Facebook AI Research/University of Washington

TA: Jana Sotakova

Hash of the Future?

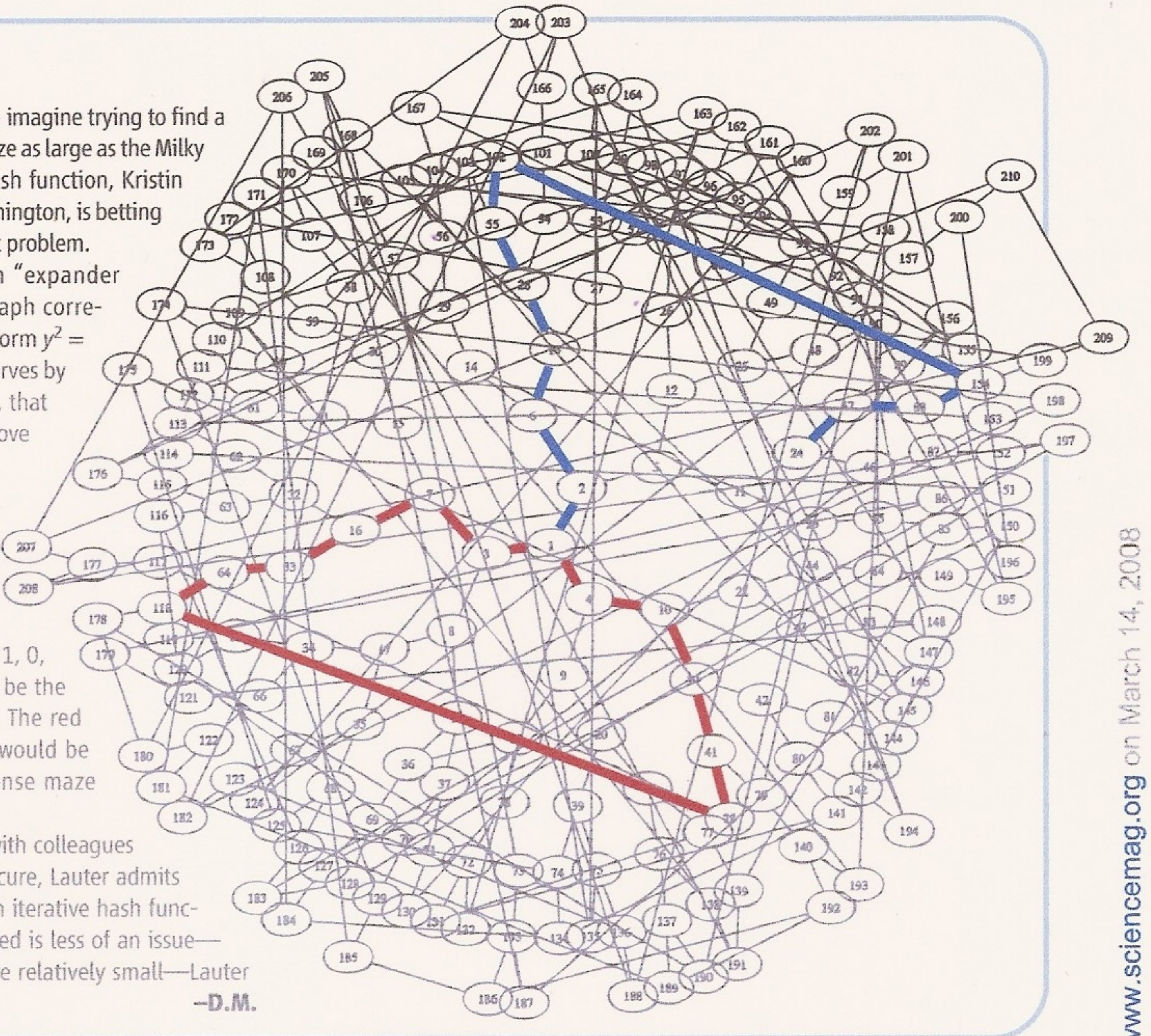
Have you ever struggled to solve a maze? Then imagine trying to find a path through a tangled, three-dimensional maze as large as the Milky Way. By incorporating such a maze into a hash function, Kristin Lauter of Microsoft Research in Redmond, Washington, is betting that neither you nor anyone else will solve that problem.

Technically, Lauter's maze is called an "expander graph" (see figure, right). Nodes in the graph correspond to elliptic curves, or equations of the form $y^2 = x^3 + ax + b$. Each curve leads to three other curves by a mathematical relation, now called isogeny, that Pierre de Fermat discovered while trying to prove his famous Last Theorem.

To hash a digital file using an expander graph, you would convert the bits of data into directions: 0 would mean "turn right," 1 would mean "turn left." In the maze illustrated here, after the initial step 1-2, the blue path encodes the directions 1, 0, 1, 1, 0, 0, 0, 0, 1, ending at point 24, which would be the digital signature of the string 101100001. The red loop shows a collision of two paths, which would be practically impossible to find in the immense maze envisioned by Lauter.

Although her hash function (developed with colleagues Denis Charles and Eyal Goren) is provably secure, Lauter admits that it is not yet fast enough to compete with iterative hash functions. However, for applications in which speed is less of an issue—for example, where the files to be hashed are relatively small—Lauter believes it might be a winner.

–D.M.



Summary:

- First lecture: cryptography, quantum threat, hash function, SIG
- Second lecture: expander graphs, Ramanujan property, key exchange, generic attacks
- Third lecture: quaternion algebras, KLPT, signatures

Quaternionic interpretation

An elliptic curve is supersingular modulo p if its endomorphism ring is a maximal order in the definite quaternion algebra, $B_{p,\infty}$

Beautiful theorems in number theory:

- Deuring's correspondence

  $E \leftrightarrow End(E) := \{\varphi: E \rightarrow E \text{ endomorphism}\}$

  Vertices $\leftrightarrow$ maximal orders in a quaternion algebra

- Eichler class number:

  # vertices ~ p/12

Quaternion Algebras

$B_{p,\infty}$:= definite quaternion algebra ramified at p & infinity

Basis $< 1, i, j, k=ij >$ for $B_{p,\infty}$

$i^2 = a\ ,\ j^2 = b,\ k = ij = -ji$

If $p = 3 \pmod 4$ then $(a,b) = (-p,-1)$

(reduced) norm map

Involution on $B_{p,\infty}$

$x = (1, i, j, k) \quad \rightarrow \quad x^* = (1, -i, -j, -k)$

$\mathrm{Trace}(x) := x + x^* \qquad \mathrm{Norm}(x) := xx^*$

Norm map when *p = 3 (mod 4)* :

$N(c + dj + fi + gij) = c^2 + d^2 + p(f^2 + g^2)$

Norm map on quaternions corresponds to degree map on endomorphisms!

Quaternionic orders and ideals

Fractional ideal $\mathscr{I}$: rank-4 Z-lattice, $\mathscr{I} = \alpha_1 Z + \alpha_2 Z + \alpha_3 Z + \alpha_4 Z$

Norm($\mathscr{I}$) := Z-module generated by reduced norms of elements of $\mathscr{I}$

Order $\mathscr{O}$: a fractional ideal which is also a subring of $B_{p,\infty}$

Quaternion algebras ...

Integral element: reduced norm and trace in Z

Note: integral elements do not necessarily form a ring!

Right order of fractional ideal: $\mathcal{O}_R(\mathcal{I}) = \{\alpha \in B_{p,\infty} \mid \mathcal{I}\alpha \subset \mathcal{I}\}$

Connecting ideal: Given two maximal orders, $\mathcal{O}_1$ and $\mathcal{O}_2$, connecting ideal $\mathcal{I}$ has $\mathcal{O}_R(\mathcal{I}) = \mathcal{O}_1$ and $\mathcal{O}_L(\mathcal{I}) = \mathcal{O}_2$

Can compute (see e.g. Kirschmer-Voigt`08)

$$\mathcal{I} := \mu\, \mathcal{O}_1 + N\, \mathcal{O}_2\, \mathcal{O}_1$$

Deuring's correspondence

{supersingular elliptic curves over $F_p$bar (*up to isomorphism*)}

↔

{maximal orders of $B_{p,\infty}$ (*up to conjugation*)}

supersingular j-invariant *j(E)* ←→ maximal order *O* such that *O = End(E)*

Any left ideal $\mathscr{I}$ of O corresponds to an isogeny

$\phi_{\mathscr{I}}: E \to E_{\mathscr{I}}$ with kernel $\ker \phi_{\mathscr{I}} = \{P \in E \mid \alpha(P) = 0, \forall \alpha \in \mathscr{I}\}$.

1-1 correspondence if degree of $\phi_{\mathscr{I}}$ is coprime to *p*.

The right order of $\mathscr{I}$, $\mathscr{O}_R(\mathscr{I})$ = endomorphism ring of $E_{\mathscr{I}}$

Example:

- If $p = 3 \bmod 4$, $E_0: y^2 = x^3 + x$ is supersingular
- j-invariant $j = 1728$.
- $End(E_0)$ = maximal order $\mathcal{O}_0 = Z\{1, i, (1+k)/2, (i+j)/2\}$

$\theta : B_{p,\infty} \to End(E_0) \otimes Q$ sends $(1,i,j,k)$ to $(1,\varphi,\pi,\pi\varphi)$

- $\pi : (x,y) \to (x^p, y^p)$ is the Frobenius endomorphism
- $\phi : (x,y) \to (-x, \iota y)$ with $\iota^2 = -1$.

KLPT algorithm: quaternionic path-finding [KLPT, ANTS 2014]

Given maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$, find connecting ideal of ℓ-power norm

1. Algorithm for $\mathcal{O}_0$-ideals.
    1. Find connecting ideal $\mathcal{I}$ between $\mathcal{O}_0$ and $\mathcal{O}_1$
    2. Let N = norm($\mathcal{I}$). Find an equivalent ideal of norm ℓ^n
    3. If α is an element of $\mathcal{I}$, then replace by $\mathcal{I}\gamma$, where $\gamma = \alpha^*/N$
    4. To find α of norm prime to N, search through box solving the norm equation using Cornacchia's algorithm
    5. Use Strong approximation to find equivalent ideal with ℓ-power norm
2. Repeat step 1 for $\mathcal{O}_0$ and $\mathcal{O}_2$
3. Concatenate the paths from $\mathcal{O}_1$ to $\mathcal{O}_0$ with the one from $\mathcal{O}_0$ to $\mathcal{O}_2$.

Number theoretic algorithm to find paths

Given E_1, E_2, supersingular elliptic curves over F_{p^2}

- Compute endomorphism rings as maximal orders in $B_{p,\infty}$
- Use path-finding algorithm on maximal orders in the quaternion algebra [Kohel-Lauter-Petit-Tignol]
- Pull back to a path in the SIG graph

Supersingular Isogeny Signature Schemes

[GPS 2016], [SQIsign 2020]

Set-up:

Fix a prime p, supersingular elliptic curve E_0 defined over F_p with known endomorphism ring O_0.

Select an odd smooth number D of log(p) bits.

Key generation:

(pk = E_A, sk = τ) Prover takes a random isogeny walk $\tau : E_0 \rightarrow E_A$

The public key is E_A, and the secret key is the isogeny τ .

Identification protocol: SQIsign

Commitment The prover generates a random (secret) isogeny walk

$\psi : E_0 \to E_1$, and sends E_1 to the verifier.

Challenge The verifier sends the description of a cyclic isogeny

$\varphi : E_1 \to E_2$ of degree D to the prover.

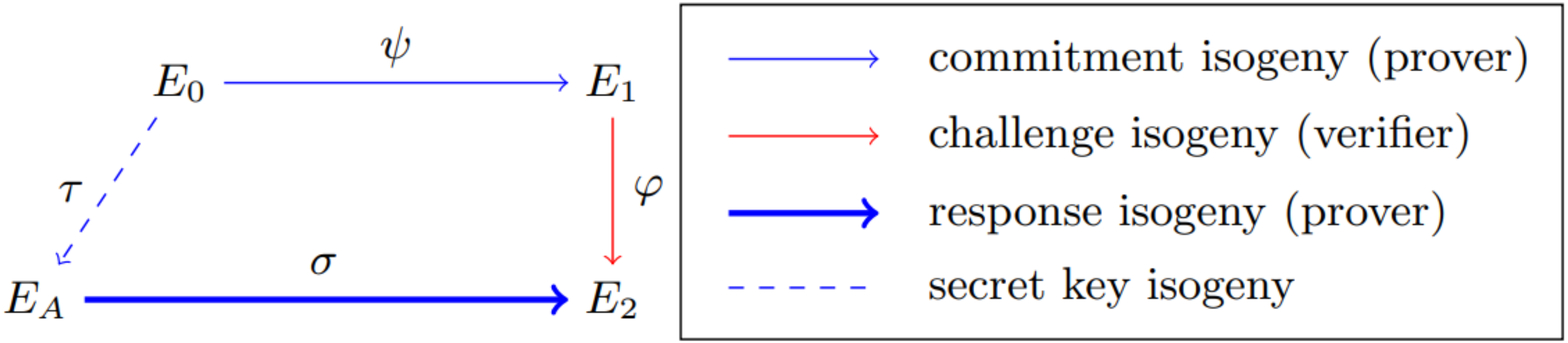
Response From the isogeny $\varphi \circ \psi \circ \hat{\tau} : E_A \to E_2$, the prover constructs a new isogeny

$\sigma : E_A \to E_2$ of degree D

such that $\hat{\varphi} \circ \sigma$ is cyclic, and sends σ to the verifier.

Verification The verifier accepts if σ is an isogeny of degree D from E_A to E_2 and $\hat{\varphi} \circ \sigma$ is cyclic. They reject otherwise.

SQIsign



ψ
E_0
E_1
τ
φ
σ
E_A
E_2
commitment isogeny (prover)
challenge isogeny (verifier)
response isogeny (prover)
secret key isogeny

References for quaternion algebras

- Bible: book by Marie-France Vigneras (in French)

- Short overviews and cryptographic applications (in English)
  - P. Clark lectures: SC9-Orders.pdf (uga.edu)
  - Sharif: sharif-04-05-19.pdf (uci.edu)
  - Kirschmer-Voigt paper: quatideal-fixed-errata-021312.pdf (dartmouth.edu)
  - SQIsign paper: 1240.pdf (iacr.org)
  - Chenevier lectures: chenevier_lecture6.pdf (cnrs.fr)