Elliptic curve cryptography in a post-quantum world: the mathematics of isogeny-based cryptography

Andrew Sutherland

MIT Undergraduate Mathematics Association
November 29, 2018

Creating a shared secret

Shared secrets enable fast secure communication. Classical methods:

RSA Alice picks a random $a \in [1, n]$ and sends a^e mod n to Bob.
Bob computes $(a^e)^d = a$, where $d \equiv e^{-1} \bmod \operatorname{lcm}(p-1, q-1)$.

- n and e are public, while d (and $pq = n$) is secret.
- security: hard to compute d (or p and q).
- 128-bit security: take $n \geq 2^{3072}$.

DH Alice pick a random $a \in [1, p]$ and sends r^a mod p to Bob.
Bob picks a random $b \in [1, p]$ and sends r^b mod p to Alice.
Alice computes $(r^b)^a = r^{ab}$ and Bob computes $(r^a)^b = r^{ab}$.

- r and p are public (no fixed secrets).
- security: hard to compute r^{ab} given r^a, r^b (or a given r^a).
- 128-bit security: take $p \geq 2^{3072}$.

Advantage of DH over RSA: forward secrecy.
Advantage of RSA over DH: no man-in-the-middle attack.
Disadvantage of both: large key size (due to subexponential-time attacks).

Security assumptions

All cryptographic protocols depend on the assumption that some easily computable function is hard to invert.

RSA: For $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ the function $x \mapsto x^e$ is easy to compute but hard to invert if you do not know $\#(\mathbb{Z}/n\mathbb{Z})^\times = (p-1)(q-1)$.

Here the base x is secret; the exponent e and modulus n are public.

DH: For $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ the function $x \mapsto r^x$ is easy to compute but hard to invert. (more precisely, the function $(r^a, r^b) \mapsto r^{ab}$ is hard to compute).

Here the exponent x is secret; the base r and modulus p are public.

The inverse of the function $x \mapsto r^x$ is the discrete logarithm $y \mapsto \log_r y$.

Security assumptions

All cryptographic protocols depend on the assumption that some easily computable function is hard to invert.

RSA: For $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ the function $x \mapsto x^e$ is easy to compute but hard to invert if you do not know $\#(\mathbb{Z}/n\mathbb{Z})^\times = (p-1)(q-1)$.

Here the base x is secret; the exponent e and modulus n are public.

DH: For $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ the function $x \mapsto r^x$ is easy to compute but hard to invert. (more precisely, the function $(r^a, r^b) \mapsto r^{ab}$ is hard to compute).

Here the exponent x is secret; the base r and modulus p are public.

The inverse of the function $x \mapsto r^x$ is the discrete logarithm $y \mapsto \log_r y$.

Both RSA and DH can be broken in $\exp(O(\sqrt[3]{\log n (\log\log n)^2}))$ time using randomized algorithms based on the number field sieve.
This explains the 3072-bit key size needed for 128-bit security.

Elliptic curves

Definition

An elliptic curve over a field k is a smooth projective curve of genus 1 with a distinguished k-rational point.

Provided $\mathrm{char}(k) \neq 2, 3$, every elliptic curve can be written in the form

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

with $a, b \in k$. In projective coordinates this equation becomes

$$E : y^2 z = x^3 + axz^2 + bz^3,$$

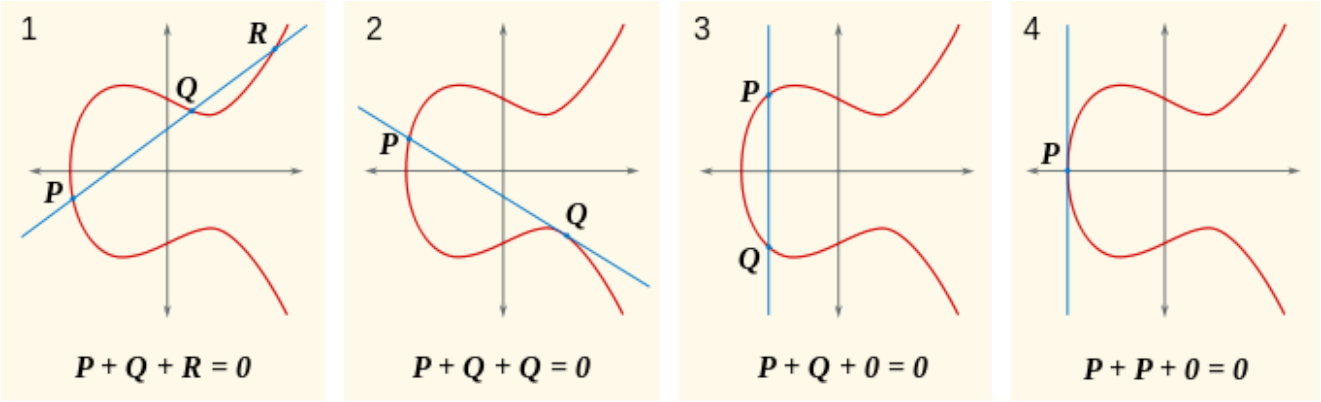
and the point $(0 : 1 : 0)$ "at infinity" is our distinguished rational point.

Theorem

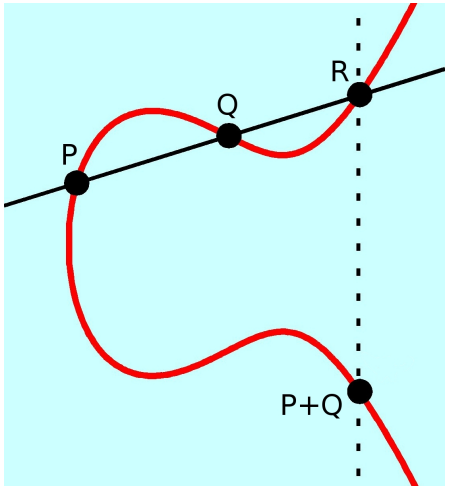
Let E/k be an elliptic curve with distinguished point O. The set $E(k)$ of k-rational points has a natural abelian group structure with identity O.

The elliptic curve group law

Key fact: For $P, Q \in E(k)$ the line $\overline{PQ}$ intersects E in a rational point.



Group law: Three points on a line sum to zero.



Elliptic curve Diffie-Hellman (ECDHE)

Alice picks a random $a \in [1, p]$ and sends $aP := \overbrace{P + \cdots + P}^{a}$ to Bob.
Bob pick a random $b \in [1, p]$ and sends bP to Alice.
Alice authenticates bP and computes abP, Bob computes $baP = abP$.

- $E/\mathbb{F}_p$ with $n = \#E(\mathbb{F}_p)$ and point $P \in E(\mathbb{F}_p)$ are public.
- security: hard to compute abP given aP, bP (or a given aP).
- 128-bit security: take $p \geq 2^{256}$.

All the advantages of DH with much smaller key size.
To avoid man in the middle attack Bob uses private RSA key to sign bP (which Alice authenticates using Bob's certified public RSA key).

ECDHE is a standard part of the transport security layer (TLS) underlying the secure hyper text transfer protocol (https).
As of 2018, more than 70% of all internet traffic uses this protocol.

Elliptic curve Diffie-Hellman (ECDHE)

Alice picks a random $a \in [1, p]$ and sends $aP := \overbrace{P + \cdots + P}^{a}$ to Bob.
Bob pick a random $b \in [1, p]$ and sends bP to Alice.
Alice authenticates bP and computes abP, Bob computes $baP = abP$.

- $E/\mathbb{F}_p$ with $n = \#E(\mathbb{F}_p)$ and point $P \in E(\mathbb{F}_p)$ are public.
- security: hard to compute abP given aP, bP (or a given aP).
- 128-bit security: take $p \geq 2^{256}$.

All the advantages of DH with much smaller key size.
To avoid man in the middle attack Bob uses private RSA key to sign bP (which Alice authenticates using Bob's certified public RSA key).

ECDHE is a standard part of the transport security layer (TLS) underlying the secure hyper text transfer protocol (https).
As of 2018, more than 70% of all internet traffic uses this protocol.

Disadvantage: poly-time quantum attack ($6 \log p$ qbits $\implies \widetilde{O}(\log^3 p)$)

The discrete logarithm problem

In a classical computing model the difficulty of the discrete logarithm problem depends critically on the representation of the underlying group G:

- $G = \mathbb{Z}/p\mathbb{Z}$: Computing $\log_b a = \frac{1}{b}a$ takes quasi-linear time using the fast Euclidean algorithm to compute b^{-1} mod p.
- $G = (\mathbb{Z}/p\mathbb{Z})^\times$: Best known algorithms take subexponential time.
- $G = E(\mathbb{F}_p)$: Best known algorithms take exponential time $O(\sqrt{p})$.
- G a black box group of order p: All algorithms take $\Omega(\sqrt{p})$ time (Shoup 1997).

The discrete logarithm problem

In a classical computing model the difficulty of the discrete logarithm problem depends critically on the representation of the underlying group G:

- $G = \mathbb{Z}/p\mathbb{Z}$: Computing $\log_b a = \frac{1}{b}a$ takes quasi-linear time using the fast Euclidean algorithm to compute b^{-1} mod p.
- $G = (\mathbb{Z}/p\mathbb{Z})^\times$: Best known algorithms take subexponential time.
- $G = E(\mathbb{F}_p)$: Best known algorithms take exponential time $O(\sqrt{p})$.
- G a black box group of order p: All algorithms take $\Omega(\sqrt{p})$ time (Shoup 1997).

In a quantum computing model this is no longer true. Shor's algorithm factors an integer n by using a QFT to compute $\#(\mathbb{Z}/n\mathbb{Z})^\times$ in $O(\log^3 n)$ quantum bit-operations. This algorithm can be generalized to compute discrete logarithms in any cyclic group whose group operation can be computed using modular arithmetic in $O((\log n)^3)$ time.

See arXiv:quant-ph/0301141 and ePrint:2017/598 for ECDLP details.

Post-quantum cryptography

The potential threat of future quantum-based attacks on public-key cryptosystems led NIST to issue a formal Request for Proposal soliciting "post-quantum cryptographic algorithms" in December 2016.

By the December 2017 deadline for round one submissions they had received 69 proposals. Most of these are based on lattice or coding theory problems that are not believed to be susceptible to quantum attacks.

One proposal (SIKE) uses elliptic curves. Rather than working in the group of rational points on a single elliptic curve, it works with isogeny graphs of supersingular elliptic curves a single finite field.

Since then other isogeny-based protocols have been proposed, notably including CSIDH. The main advantage of isogeny-based protocols is that they are well understood, offer an easy to implement drop-in replacement for ECDHE, and have smaller key sizes than lattice-based approaches.

Morphisms and isogenies

Let E_1 and E_2 be elliptic curves over a field k.

A *morphism* $\varphi\colon E_1 \to E_2$ is a map defined by rational functions that sends the distinguished point of E_1 to the distinguished point of E_2.

Morphisms that are not the zero map are called isogenies.
Isogenies induce group homomorphisms $E_1(\overline{k}) \to E_2(\overline{k})$ with finite kernel.
Conversely, every finite subgroup of $E_1(\overline{k})$ is the kernel of an isogeny.

Example: For every nonzero integer n the map $[n]\colon E \to E$ defined by $P \mapsto nP$ is an isogeny whose kernel in $E(\overline{k})$ is denoted $E[n]$.

Example: For $k = \mathbb{F}_p$ the map defined by $(x : y : z) \mapsto (x^p : y^p : z^p)$ is an isogeny with trivial kernel known as the Frobenius endomorphism.

Endomorphism rings

The set of endomorphisms of an elliptic curve E form a ring $\mathrm{End}(E)$:

$$(\varphi+\psi)(P) := \varphi(P)+\psi(P)$$
$$(\varphi\psi)(P) := \varphi(\psi(P)).$$

This ring includes a subring isomorphic to $\mathbb{Z}$ generated by the maps $[n]$, but it may be larger than this (over a finite field it always is).

Theorem

The additive group of $\mathrm{End}(E)$ *is isomorphic to* $\mathbb{Z}^r$ *with* $r = 1, 2, 4$.
For $r = 1, 2$ *the ring* $\mathrm{End}(E)$ *is commutative, but for* $r = 4$ *it is not.*

An elliptic curve E over a finite field $\mathbb{F}_q$ of characteristic p is supersingular if any of the following equivalent conditions holds

$$\text{(a) } E[p] = \{0\}, \qquad \text{(b) } \mathrm{rk}(\mathrm{End}(E_{\overline{\mathbb{F}}_q})) = 4, \qquad \text{(c) } \#E(\mathbb{F}_q) \equiv 1 \bmod p.$$

Otherwise, E is ordinary.

The j-invariant of an elliptic curve

The j-invariant of and elliptic curve E/k defined by $y^2 = x^3 + ax + b$ is

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} \in k.$$

Elliptic curves with the same j-invariant are isomorphic over a finite extension of k, and have isomorphic endomorphism rings $\mathrm{End}(E)$. It thus makes sense to refer to j-invariants as ordinary or supersingular.

Given $j_0 \in k$ it is easy to write down an equation for E/k with $j(E) = j_0$.

We can thus identify k with the set of $\overline{k}$-isomorphism classes of elliptic curves E/k and partition k into ordinary and supersingular subsets.

Modular polynomials

Let N be a positive integer. An N-isogeny is an isogeny of elliptic curves whose kernel is a cyclic group of order N.

Elliptic curves related by an N-isogeny are said to be N-isogenous, as are their j-invariants.

For each integer N there is a modular polynomial

$$\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$$

with the property that $j_1, j_2 \in k$ are N-isogenous iff $\Phi_N(j_1, j_2) = 0$.

The polynomial $\Phi_N(X, Y)$ is symmetric in X and Y.

For any prime ℓ the polynomial Φ_ℓ has degree $\ell + 1$ in both variables.

Isogeny graphs

Let ℓ be a prime and let $\mathbb{F}_q$ be a finite field of characteristic $p \neq \ell$.

Definition

The ℓ-isogeny graph $G_\ell(\mathbb{F}_q)$ is the graph with vertex set $\mathbb{F}_q$ and edges (j_1, j_2) present with multiplicity $m_\ell(j_1, j_2) := \operatorname{ord}_{t=j_2} \Phi_\ell(j_1, t)$.

We have $m(j_1, j_2) = m(j_2, j_1)$ whenever $j_1, j_2 \notin \{0, 1728\}$.
Components not containing $0, 1728$ can be viewed as undirected graphs.

If E_1 and E_2 are isogenous then $\operatorname{End}(E_1) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \operatorname{End}(E_2) \otimes_{\mathbb{Z}} \mathbb{Q}$.

This implies that the connected components of $G_\ell(\mathbb{F}_q)$ can be classified as ordinary or supersingular.

Each component contains only ordinary or supersingular j-invariants.

Note that each $j \in \mathbb{F}_q$ lies in infinitely many $G_\ell(\mathbb{F}_q)$, one for each prime ℓ.

Supersingular ℓ-isogeny graphs

For each prime $\ell \neq p$ the graph $G_\ell(\mathbb{F}_{p^2})$ has a single supersingular component, which is an $(\ell+1)$-regular graph with $N_p \approx \frac{p}{12}$ vertices.

Definition

A d-regular graph is a *Ramanujan graph* if $\lambda_2 \leq \sqrt{d-1}$, where λ_2 is the second largest eigenvalue of its adjacency matrix.

Theorem (Pizer)

The supersingular component of $G_\ell(\mathbb{F}_{p^2})$ is a Ramanujan graph.

Corollary (GPS17)

Fix a supersingular $j_1 \in \mathbb{F}_{p^2}$, and let j_2 be the endpoint of an e-step random walk in $G_\ell(\mathbb{F}_{p^2})$ originating at j_1. For all $j \in \mathbb{F}_{p^2}$:

$$\left|\Pr[j = j_2] - N_p^{-1}\right| \leq \left(\frac{2\sqrt{\ell}}{\ell+1}\right)^e.$$

Vélu's formulas

Given an elliptic curve E/k and a point $P \in E(\overline{k})$ of order n there is a separable isogeny $\varphi_P \colon E \to E/\langle P \rangle$ of degree n, unique up to isomorphism. The isogeny φ_P can be explicitly computed using Vélu's formulas.

If $E \colon y^2 = x^3 + ax + b$ and $P := (x_0, 0) \in E(\overline{k})$ is a point of order 2, then

$$\varphi_P(x, y) := \left(\frac{x^2 - x_0 x + t}{x - x_0}, \frac{(x - x_0)^2 - t}{(x - x_0)^2} y \right)$$

and $E/\langle P \rangle \colon y^2 = x^3 + (a - 5t)x + b - 7x_0 t$, where $t = 3x_0^2 + a$.

For $P := (x_0, y_0) \in E(\overline{k})$ of odd order n there are similar explicit formulas for $\varphi_P(x, y)$ and $E/\langle P \rangle$ as rational expressions in x_0, y_0, a, b over k.

The complexity of computing φ_P depends heavily on the field over which P is defined; ideally one would like $P \in E(k)$.

Supersingular isogeny Diffie-Hellman (SIDH)

Following [DJ11], fix supersingular $E_0/\mathbb{F}_{p^2}$ with $E_0(\mathbb{F}_{p^2}) = E[\ell_A^{e_A}\ell_B^{e_B}]$ (for $p = \ell_A^{e_A}\ell_B^{e_B} \pm 1$ prime, E_0 exists and can be constructed via [Br08]).

Fix public bases $\{P_A, Q_A\}$ for $E[\ell_A^{e_A}]$ and $\{P_B, Q_B\}$ for $E[\ell_B^{e_B}]$.

1. Alice: $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$, let $\varphi_A : E \to E_A := E_0/\langle m_A P_A + n_A Q_A\rangle$, send $\varphi_A(P_B), \varphi_A(Q_B), E_A$ to Bob.
2. Bob: $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$, let $\varphi_B : E \to E_B := E_0/\langle m_B P_B + n_B Q_B\rangle$, send $\varphi_B(P_A), \varphi_B(Q_A), E_B$ to Alice.
3. Alice computes $E_{AB} := E_B/\langle m_A\varphi_B(P_A) + n_A\varphi_B(Q_A)\rangle$.
4. Bob computes $E_{BA} := E_A/\langle m_B\varphi_A(P_B) + n_B\varphi_A(Q_B)\rangle$.

Then $\ker\varphi_{AB} = \langle m_A P_A + n_A Q_A, m_B P_B + n_B Q_B\rangle = \ker\varphi_{BA}$, so $E_{AB} \simeq E_{BA}$, and $j(E_{AB}) = j(E_{BA})$ is a shared secret.[1]

[1] We have omitted verification details important to security. Random integers m_A, n_A, m_B, n_B should always be used (static keys are not secure, see [GPST16]).

Isogeny volcanoes

An ℓ-volcano is a connected graph with vertices partitioned into levels $V_0, \ldots, V_d$ such that

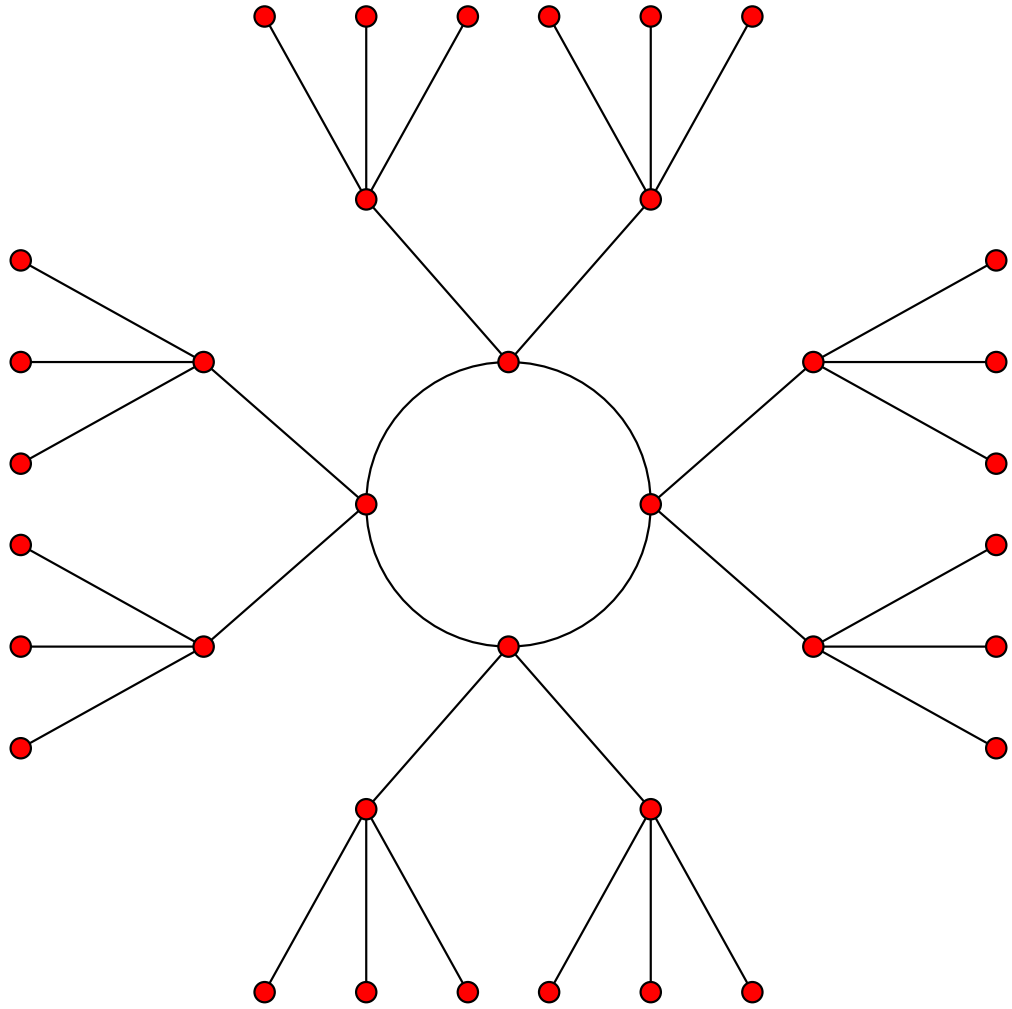
- The subgraph on V_0 is d-regular with $0 \leq d \leq 2$.
- There are no edges contained in level V_i for $i > 0$.
- Vertices on levels V_i with $i < d$ have degree $\ell + 1$.
- Vertices on levels V_i with $i > 0$ have one neighbor in level V_{i-1}

Level V_0 is the *surface* and V_d is the *floor* (possibly $V_0 = V_d$).

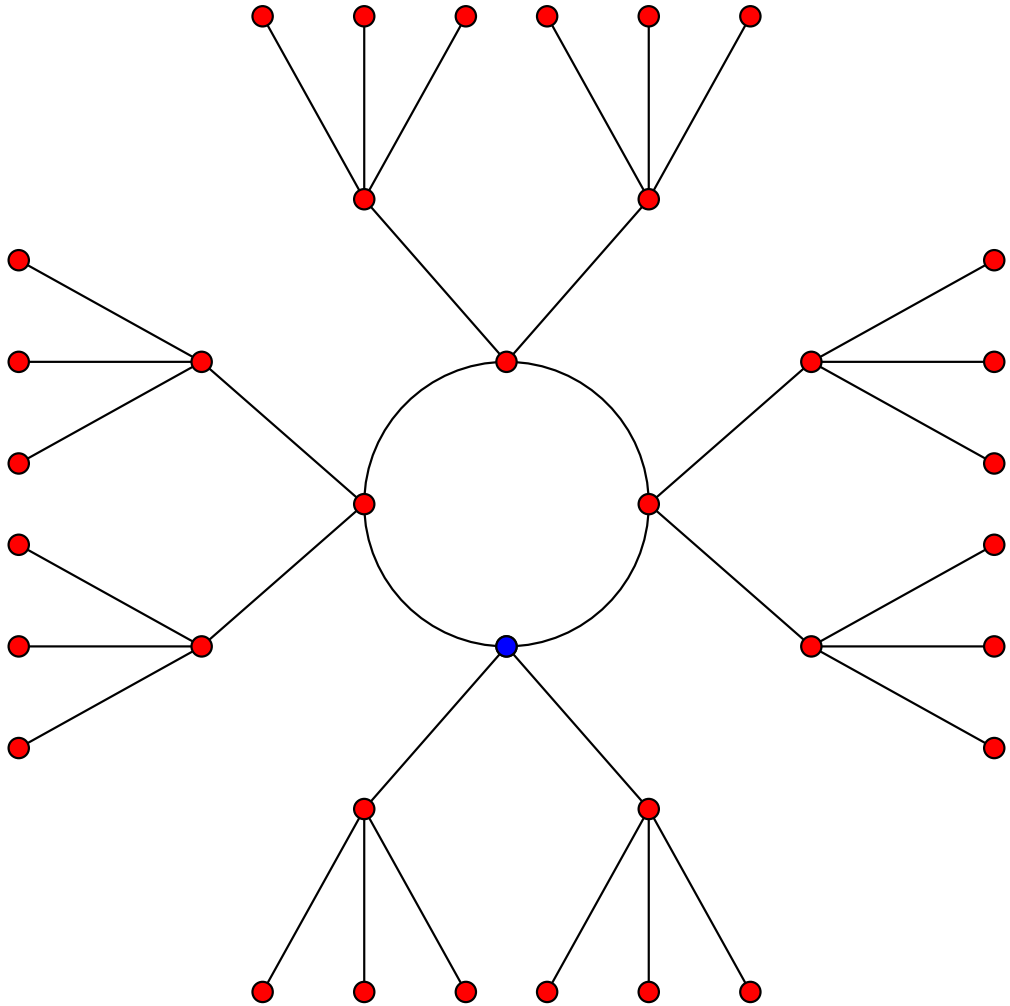
Theorem (Kohel)

Ordinary components of $G_\ell(\mathbb{F}_q)$ not containing $0, 1728$ are ℓ-volcanoes.

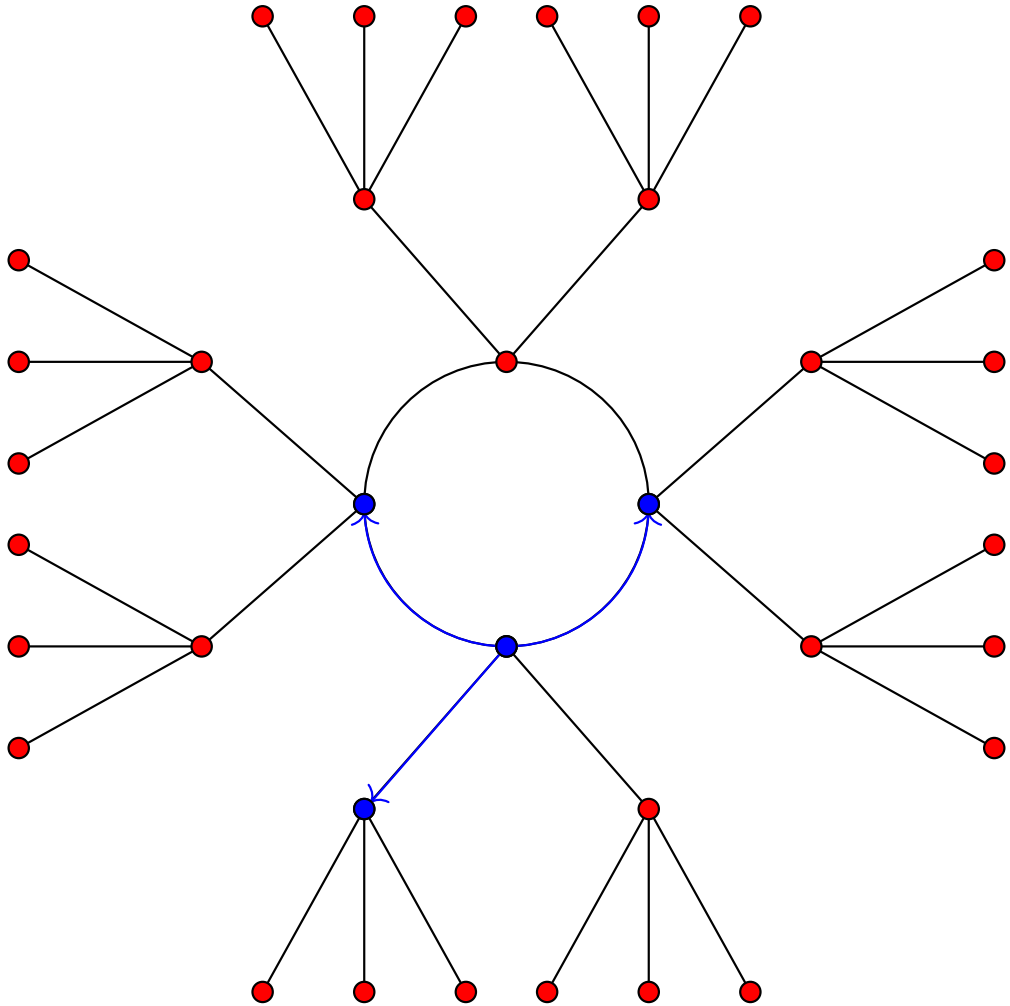
A 3-volcano of depth 2



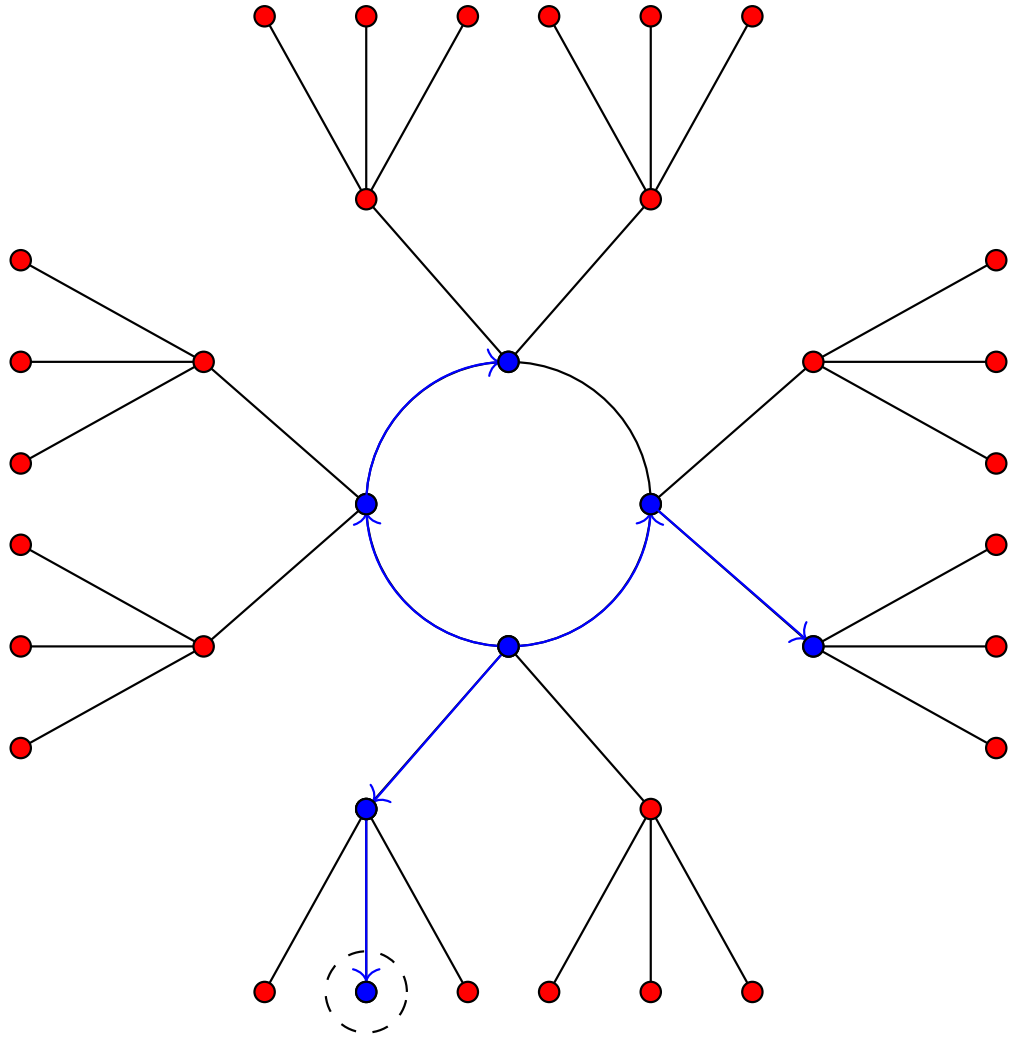
Finding a shortest path to the floor



Finding a shortest path to the floor



Finding a shortest path to the floor



Identifying supersingular curves using isogeny graphs

Given an elliptic curve E over a field of characteristic p, the following algorithm determines whether E is ordinary or supersingular:

1. If $j(E) \notin \mathbb{F}_{p^2}$ then return **ordinary**.
2. If $p \leq 3$ return **supersingular** if $j(E) = 0$ and **ordinary** otherwise.
3. Attempt to find 3 roots of $\Phi_2(j(E), Y)$ in $\mathbb{F}_{p^2}$.
   If this is not possible, return **ordinary**.
4. Walk 3 paths in parallel for up to $\lceil \log_2 p \rceil + 1$ steps.
   If any of these paths hits the floor, return **ordinary**.
5. Return **supersingular**.

$$\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 1488(X^2Y + Y^2X) - 162000(X^2 + Y^2) + 40773375XY + 8748000000(X + Y) - 157464000000000.$$

Complexity analysis

In step 4, we remove the known linear factor so that only a quadratic equation remains, obtaining j_{i+1} as a root of $\Phi_2(j_i, Y)/(Y - j_{i-1})$.
We need to be able to compute square roots (and solve a cubic) in $\mathbb{F}_{p^2}$.

Proposition (S12)

We can identify ordinary/supersingular elliptic curves over $\mathbb{F}_{p^2}$ via

- *A Las Vegas algorithm that runs in $\widetilde{O}(\log^3 p)$ expected time.*
- *Under GRH, a deterministic algorithm that runs in $\widetilde{O}(\log^3 p)$ time*
- *Given quadratic and cubic non-residues in $\mathbb{F}_{p^2}$, a deterministic algorithm that run in $\widetilde{O}(\log^3 p)$ time.*

For a random elliptic curve over $\mathbb{F}_{p^2}$, average running time is $\widetilde{O}(\log^2 p)$.

An alternative algorithm based on polynomial identity testing [D18] achieves a similar complexity (under GRH).

Performance results (CPU milliseconds)

	ordinary				supersingular			
	Magma		**New**		Magma		**New**	
b	$\mathbb{F}_p$	$\mathbb{F}_{p^2}$	$\mathbb{F}_p$	$\mathbb{F}_{p^2}$	$\mathbb{F}_p$	$\mathbb{F}_{p^2}$	$\mathbb{F}_p$	$\mathbb{F}_{p^2}$
64	1	25	0.1	0.1	226	770	2	8
128	2	60	0.1	0.1	2010	9950	5	13
192	4	99	0.2	0.1	8060	41800	8	33
256	7	140	0.3	0.2	21700	148000	20	63
320	10	186	0.4	0.3	41500	313000	39	113
384	14	255	0.6	0.4	95300	531000	66	198
448	19	316	0.8	0.5	152000	789000	105	310
512	24	402	1.0	0.7	316000	2280000	164	488
576	30	484	1.3	0.9	447000	3350000	229	688
640	37	595	1.6	1.0	644000	4790000	316	945
704	46	706	2.0	1.2	847000	6330000	444	1330
768	55	790	2.4	1.5	1370000	8340000	591	1770
832	66	924	3.1	1.9	1850000	10300000	793	2410
896	78	1010	3.2	2.1	2420000	12600000	1010	3040
960	87	1180	4.0	2.5	3010000	16000000	1280	3820
1024	101	1400	4.8	3.1	5110000	35600000	1610	4880

Supersingular isogeny graphs over $\mathbb{F}_p$

Most supersingular curves have j-invariants in $\mathbb{F}_{p^2}$, but an $O(\sqrt{p})$ subset of them actually have j-invariants in $\mathbb{F}_p$.

We know that $G_\ell(\mathbb{F}_{p^2})$ has a single supersingular component, and it is a Ramanujan graph. What about $G_\ell(\mathbb{F}_p)$?

Supersingular isogeny graphs over $\mathbb{F}_p$

Most supersingular curves have j-invariants in $\mathbb{F}_{p^2}$, but an $O(\sqrt{p})$ subset of them actually have j-invariants in $\mathbb{F}_p$.

We know that $G_\ell(\mathbb{F}_{p^2})$ has a single supersingular component, and it is a Ramanujan graph. What about $G_\ell(\mathbb{F}_p)$?

Theorem (Kohel, Delfs-Galbraith)

The supersingular components of $G_\ell(\mathbb{F}_p)$ not containing $0, 1728$ are isogeny volcanoes.

For both ordinary and supersingular elliptic curves $E/\mathbb{F}_p$, if we restrict our attention to endomorphisms defined over $\mathbb{F}_p$, we have $\mathrm{rk}(\mathrm{End}(E)) = 2$ and the endomrophism ring can be embedded in the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{t^2 - 4p})$, where the integer

$$t := p + 1 - \#E(\mathbb{F}_p)$$

is the trace of Frobenius; it satisfies $|t| < 2\sqrt{p}$.

CSIDH

For suitable p every supersingular curve over $\mathbb{F}_p$ has $\mathrm{End}(E) \simeq \mathbb{Z}[\sqrt{p}]$.

For primes $\ell | (p+1)$, the ℓ-isogeny volcano is a cycle and we can compute ℓ-power isogenies very quickly using Velu's formulas working only over $\mathbb{F}_p$ (here we need E to be supersingular).

The ideal class group of $\mathbb{Z}[\sqrt{p}]$ acts on the set S_p of supersingular j-invariants in $\mathbb{F}_p$, whose cardinality is the class number $h(p) \approx \sqrt{p}$.

This makes the set S_p a homogeneous space or torsor for the class group. By exploiting the relationship between ideals that are products of powers of prime ideals of small norms $\ell_1, \ldots, \ell_n$ we can implement an SIDH algorithm without tracking or transmitting generators of isogeny kernels.

This increases security, simplifies implementation, and reduces key sizes. There is an $\exp(O(\sqrt{\log p}))$ quantum attack but it can be protected against with a modest increase in the key size. See ePrint:2018/383.

References

- [BS11] G. Bisson and A.V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, J. Number Theory, **113** (2011), 815-831.
- [Br08] R. Broker, *Constructing supersingular elliptic curves*, J. Comb. Number Theory, **1** (2009), 269–273
- [CGL09] X. Charles, E. Goren, K. Lauter, *Cryptographic hash functions from expander graphs*, J. Cryptol. **22** (2009), 93–113.
- [CLN16] C. Costello, P. Longa, M. Naehrig, *Efficient algorithms for supersingular isogeny Diffie-Hellman*, CRYPTO 2016, LNCS **9814** (2016), 572–601.
- [CLMPR18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, *CSIDH: An efficient post-quantum commutative group action*, ePrint:2018/383.
- [DJ11] De Feo, D. Jao, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Post-quantum Cryptography, LNCS **7071** (2011), 19–34.
- [DJP14] De Feo, L., Jao, D., Plût, J., *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Cryptology **8**, 209–247 (2014)
- [D18] J. Doliskani, *On Division Polynomial PIT and Supersingularity*, arXiv: 1801.02664.
- [EHLMP18] K. Eisentraeger, S. Hallgren, K. Lauter, T. Morrison, and Christophe Petit, *Supersingular isogeny graphs and endomorphism rings: reductions and solutions*, EuroCRYPT 2018, LNCS **10822** (2018), 329–368.
- [KLPT14] D. Kohel, K. Lauter, C. Petit, J.-P. Tignol, *On the quaternion ℓ-isogeny path problem*, LMS J. Comput. Math. **17** (2014), 418–432.
- [GPST16] S. Galbraith, C. Petit, B. Shani, Y. Bo Ti, *On the security of supersingular isogeny cryptosystems*, AsiaCrypt 2014, LNCS **10331** (2016), 63–91.
- [GPS17] S. Galbraith, C. Petit, J. Silva, *Identification protocols and signature schemes based on supersingular isogeny problems*, AsiaCRYPT 2017. LNCS **10624** (2017), 3–33.
- [S12] A.V. Sutherland, *Identifying supersingular elliptic curves*, LMS J. Comput. Math. **15** (2012), 317-325.