Computation in supersingular isogeny graphs

Andrew V. Sutherland
MIT

CTNT 2018
University of Connecticut
June 2, 2018

Creating a shared secret

Shared secrets enable fast secure communication. Classical methods:

RSA Alice picks a random $a \in [1, n]$ and sends $a^e \bmod n$ 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 $r^a \bmod p$ to Bob.
Bob picks a random $b \in [1, p]$ and sends $r^b \bmod p$ 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).

Elliptic curve Diffie-Hellman (ECDHE)

Alice picks a random $a \in [1, p]$ and sends aP 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 2017, more than 50% of all internet traffic uses this protocol.

Elliptic curve Diffie-Hellman (ECDHE)

Alice picks a random $a \in [1, p]$ and sends aP 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 2017, more than 50% of all internet traffic uses this protocol.

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

Supersingular elliptic curves

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

1. $E[p]$ is trivial;
2. $\mathrm{End}(E_{\bar{\mathbb{F}}_q})$ is a maximal order in the quaternion algebra $B_{p,\infty}/\mathbb{Q}$;
3. The Hasse-Witt matrix of E is zero;
4. $\#E(\mathbb{F}_q) \equiv 1 \bmod p$;
5. $j(E) \in \mathbb{F}_{p^2}$ and the ℓ-isogeny graph component of $j(E)$ is regular.

Supersingular elliptic curves are rare; the probability that a randomly chosen $E/\mathbb{F}_q$ is supersingular is $O(q^{-1/2})$.

Monte Carlo test to check if $E/\mathbb{F}_{p^2}$ is supersingular: pick a random $P \in E(\mathbb{F}_{p^2})$ and check if $(p+1)P = 0$ or $(p-1)P = 0$.

Schoof's algorithm identifies supersingular curves in $\widetilde{O}(\log^5 p)$ time; this can be improved to $\widetilde{O}(\log^4 p)$, but we will give a faster algorithm.

Constructing supersingular elliptic curves

Let $\mathcal{O}$ be the imaginary quadratic order of discriminant D and let $H_D \in \mathbb{Z}[X]$ be the minimal polynomial of $j(\mathbb{C}/\mathcal{O})$ over $\mathbb{Q}(\sqrt{D})$.

Bröker's algorithm [Br08] to construct a supersingular elliptic curve $E/\mathbb{F}_p$:

1. If $p = 2$ then return $E\colon y^2 + y = x^3$.
2. If $p \equiv 2 \bmod 3$ return $E\colon y^2 = x^3 + 1$.
3. If $p \equiv 3 \bmod 4$ return $E\colon y^2 = x^3 + x$.
4. Let $q \equiv 3 \bmod 4$ be the least prime q that is not a square modulo p and let j_0 be a root of $H_{-q}(X) \bmod p$.
5. Return $E\colon y^2 = x^3 + 3cx + 2c$ where $c := j_0/(1728 - j_0)$.

Why it works: $4p^r = t^2 - v^2D$ has no solutions, so roots of $H_{-q}(X)$ in $\bar{\mathbb{F}}_p$ are supersingular and lie in $\mathbb{F}_{p^2}$, and $h(-q)$ is odd, so root $j_0 \in \mathbb{F}_p$ exists.

Why it's fast: under GRH we have $q = O(\log^2 p)$ and $h(-q) = O(\log p)$. We can then find a root of $H_{-q}(X) \bmod p$ in $\widetilde{O}(\log^3 p)$ expected time.

Modular polynomials

Let $j(z)$ be the modular j-function. For each prime ℓ the minimal polynomial Φ_ℓ of $j(\ell z)$ over $\mathbb{C}(j)$ is the modular polynomial

$$\Phi_\ell \in (\mathbb{Z}[j])[X] \simeq \mathbb{Z}[X, Y].$$

The polynomial $\Phi_\ell(X, Y) = \Phi_\ell(Y, X)$ has degree $\ell + 1$ in both X and Y.

$\Phi_\ell(X, Y)$ is a canonical (singular) model for the modular curve $Y_0(\ell)$.
It parametrizes isogenies $\varphi\colon E_1 \to E_2$ of degree ℓ as points $(j(E_1), j(E_2))$.

This moduli interpretation remains valid over fields k with $\mathrm{char}(k) \neq \ell$.
For any elliptic curve E/k, there are $\ell + 1$ distinct isogenies $\varphi_i\colon E \to E_i$ over $\overline{k}$, corresponding to $\ell + 1$ order ℓ subgroups of $E[\ell]$, and we have

$$\Phi_\ell(j(E), Y) = \prod_{i=1}^{\ell+1} (Y - j(E_i)).$$

Isogeny graph

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

Definition

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

For $j \in \mathbb{F}_q$, let $n(j) = 6, 4, 2$ for $j = 0$, $j = 1728$, $j \neq 0, 1728$. Then

$$m_\ell(j_1, j_2) n(j_2) = m_\ell(j_2, j_1) n(j_1)$$

In particular, $m(j_1, j_2) = m(j_2, j_1)$ whenever $j_1, j_2 \notin \{0, 1728\}$.

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.

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 $P \in E(\bar{k})$ 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 $P := (x_0, 0) \in E(\bar{k})$ 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 $P := (x_0, y_0) \in E(\bar{k})$ 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 $E_0(\mathbb{F}_{p^2}) = E[\ell_A^{e_A}\ell_B^{e_B}]$ (provided $p = \ell_A^{e_A}\ell_B^{e_B} \pm 1$ is prime, such an E_0 exists).
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]).

Computing ℓ-power isogenies

Given $P \in E(\mathbb{F}_q)$ of order ℓ^n and $Q \in E(\mathbb{F}_q)$, compute $E' := E/\langle P \rangle$ and the image Q' of Q under $E \to E/\langle P \rangle$ as follows:

1. Compute $P_n := P$, $P_{n-i} = \ell P_{n-i+1}$ for $1 \leq i < n$, $E_1 := E$, $Q_1 := Q$.
2. For i from 1 to n:
    1. Compute $\varphi_i : E_i \to E_{i+1} := E_i/\langle P_i \rangle$ via Vélu and $Q_{i+1} := \varphi_i(Q_i)$.
    2. For j from $i+1$ to n replace P_j with $\varphi_i(P_j)$.
3. Output $E' := E_n$ and $Q' := Q_n$.

This algorithm is optimized for small ℓ, where evaluating an isogeny of degree ℓ is faster than scalar multiplication by ℓ (true for $\ell = 2, 3$).

For fixed ℓ, it uses $\widetilde{O}(n^2 \log q)$ bit operations, $\widetilde{O}(\log^3 p)$ in SIDH.
For comparison, ECDH uses $\widetilde{O}(\log^2 p)$ bit operations.

Security assumptions

Definition (ℓ-power isogeny path problem)

Given elliptic curves E, $E'/\mathbb{F}_q$ related by an isogeny of ℓ-power degree, compute ℓ-isogenies $\varphi_1 \colon E \to E_2$, $\varphi_2 \colon E_2 \to E_3$, $\ldots$, $\varphi_n \colon E_n \to E'$.

Easy if E is ordinary, polynomial-time in n, ℓ, $\log q$.

Definition (Endomorphism ring problem)

Given $E/\mathbb{F}_q$ compute explicit generators for its endomorphism ring.

For ordinary E, subexponential-time under GRH [B11, BS11].

For supersingular E the problems are polynomially equivalent [KLPT14], [GPST16], [EHLMP18].

Currently the best known algorithms take exponential-time:
$O(p^{1/2})$ classical (meet-in-the-middle), $O(p^{1/3})$ quantum.

Quaternion algebras

Let k be a field of characteristic not 2.
Recall that a quaternion algebra B over k is a k-algebra of the form

$$k\langle i, j\rangle/(i^2 = a, j^2 = b, ij = -ji),$$

with $a, b \in k^\times$. Either $B \simeq \mathrm{M}_2(k)$ (splits) or B is a division algebra.
We have a k-basis $\{1, i, j, ij\}$ and canonical involution $\alpha \mapsto \bar{\alpha}$ that fixes k and negates i, j, ij, and we define $\operatorname{trd}(\alpha) := \alpha + \bar{\alpha}$ and $\operatorname{nrd}(\alpha) := \alpha\bar{\alpha}$.

When k is a global field, we say that B is *ramified* at a place v of k if the quaternion algebra $B_v := B \otimes_k k_v$ is not split. The set Σ of ramified places has finite even cardinality and determines B up to isomorphism; conversely, for every such Σ there is a corresponding B.

For each prime p there is thus a unique quaternion algebra $B_{p,\infty}/\mathbb{Q}$ for which $\Sigma = \{p, \infty\}$. An order in a quaternion algebra $B/\mathbb{Q}$ is a lattice (finitely generated $\mathbb{Z}$-submodule that spans) that is also a ring.

The Deuring correspondence

Theorem (Deuring)

For each prime p there is a bijection

$$\{\textit{maximal orders } \mathcal{O} \subseteq B_{p,\infty}\}/_{\sim} \to \{\textit{supersingular } j \in \mathbb{F}_{p^2}\}/_{\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)}$$

that sends $\mathcal{O}$ to $j(E)$ with $\mathrm{End}(E) \simeq \mathcal{O}$.

Let I be a lattice in $B_{p,\infty}$. The orders

$$\mathcal{O}_L(I) := \{\alpha \in B_{p,\infty} : \alpha I = I\}, \qquad \mathcal{O}_R(I) := \{\alpha \in B_{p,\infty} : I\alpha = I\},$$

are linked by I. Every pair of maximal orders are linked by some I.

Let $\mathrm{nrd}(I) := \gcd\{\mathrm{nrd}(\alpha) : \alpha \in I\}$; $I\bar{I} = \mathrm{nrd}(I)\mathcal{O}_L(I)$ and $\bar{I}I = \mathrm{nrd}(I)\mathcal{O}_R(I)$. Now consider the graph $G_\ell(B_{p,\infty})$ on $\{\text{maximal orders } \mathcal{O} \subseteq B_{p,\infty}\}/_{\sim}$ with edges $(\mathcal{O}, \mathcal{O}')$ whenever $\mathcal{O}$ and $\mathcal{O}'$ are linked by a lattice of norm ℓ.

The Deuring correspondence induces a graph isomorphism*

$$G_\ell(B_{p,\infty}) \xrightarrow{\sim} G_\ell(\mathbb{F}_{p^2})/_{\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)}.$$

More on the Deuring correspondence

Let $E/\mathbb{F}_{p^2}$ is supersingular and let I be a left ideal in $\mathrm{End}(E) \simeq B_{p,\infty}$, with $p \nmid \mathrm{nrd}(I)$. Define the I-torsion subgroup

$$E[I] := \bigcap_{\alpha \in I} \ker(\alpha) = \{P \in E(\bar{\mathbb{F}}_p) : \alpha(P) = 0 \text{ for all } \alpha \in I\}$$

Then $\mathrm{End}(E/E[I]) \simeq \mathcal{O}_R(I)$ and $\varphi_I \colon E \to E/E[I]$ has degree $\mathrm{nrd}(I)$.

Theorem (KLPT14)

Under reasonable heuristics, the analog of the ℓ-power isogeny path problem can be solved in $G_\ell(B_{p,\infty})$ in probabilistic polynomial-time.

Theorem (EHLMP18)

Under reasonable heuristics, the Deuring correspondence can be computed in probabilistic polynomial-time.

The endomorphism ring problem is inverse to the Deuring correspondence.

Ordinary components of $G_\ell(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ be ordinary. Then $\mathrm{End}(E) \simeq \mathcal{O}$ with $\mathbb{Z}[\pi] \subset \mathcal{O} \subset \mathcal{O}_K$.
Here π is the Frobenius endomorphism and $K = \mathbb{Q}(\sqrt{D})$, where

$$4q = \mathrm{tr}(\pi)^2 - v^2 D.$$

Each ordinary component of $G_\ell(\mathbb{F}_q)$ consists of levels $V_0, \ldots, V_d$.
The vertex $j(E)$ belongs to level V_i, where $i = \nu_\ell([\mathcal{O}_K : \mathcal{O}])$.

The vertices in level V_0 form a (possibly trivial) cycle corresponding to the CM action of an invertible $\mathcal{O}$-ideal $\mathfrak{l}$ of norm ℓ (when one exists).

Indeed, if we put

$$E[\mathfrak{l}] := \{P \in E(\bar{\mathbb{F}}_q) : \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{l}\},$$

then $E \to E/E[\mathfrak{l}]$ is a horizontal ℓ-isogeny ($\mathrm{End}(E/E[\mathfrak{l}]) \simeq \mathrm{End}(E)$).
The ideal $\bar{\mathfrak{l}} \subseteq \mathrm{End}(E/E[\mathfrak{l}])$ corresponds to the dual isogeny.

Isogeny volcanoes

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

- The subgraph on V_0 is d-regular with $0 \le d \le 2$.
- 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}

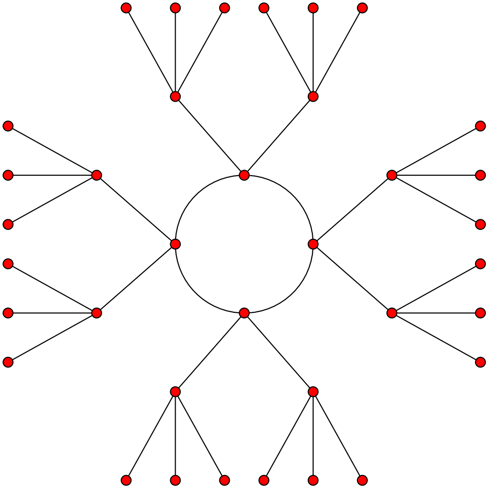
Level V_0 is the *surface* and V_d is the *floor* (possibly $V_0 = V_d$).

Theorem (Kohel)

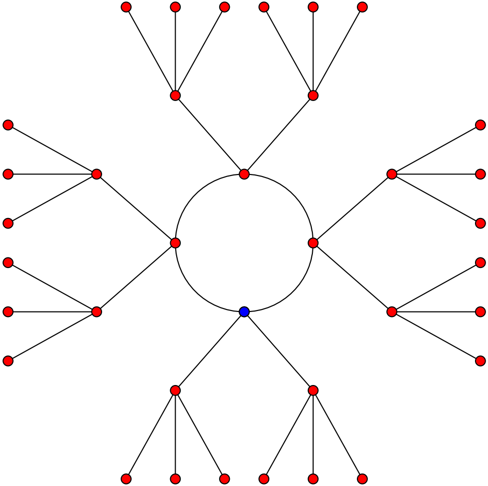
Ordinary components of $G_\ell(\mathbb{F}_q)$ not containing $0, 1728$ are ℓ-volcanoes.

The degree of the subgraph on V_0 is $1 + \left(\frac{D}{\ell}\right)$, the cardinality of V_0 is the order of $\mathfrak{l}$ in $\mathrm{cl}(\mathcal{O})$, and the depth d is the power of ℓ dividing $[\mathcal{O}_K : \mathbb{Z}[\pi]]$.

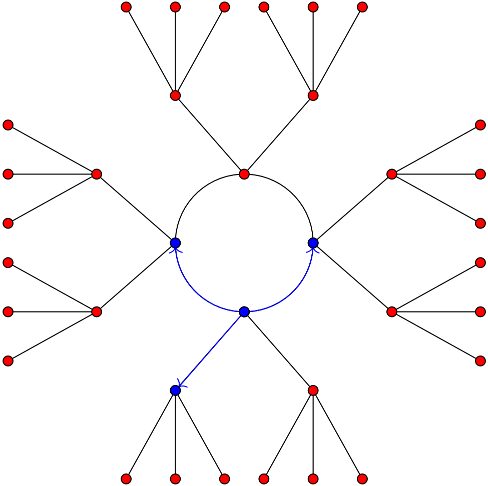
A 3-volcano of depth 2



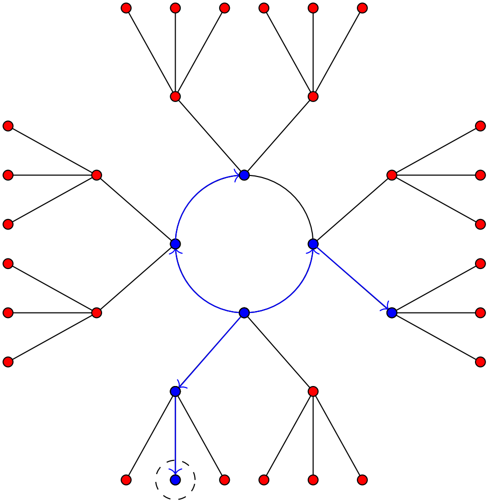
Finding a shortest path to the floor



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

References

- [B11] G. Bisson, *Endomorphism rings in cryptograhy*, Ph.D. thesis, Eindhoven, 2011.
- [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.
- [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.