Elliptic Curve Cryptography

an introduction which is entirely too short

by Giacomo Fenzi (ETH Zurich)
on 6 January 2022

» Motivation

'It is possible to write endlessly on elliptic curves.
(This is not a threat.)' Serge Lang

- Elliptic curves are everywhere in cryptography
- Power $\approx 70\%$ of TLS Exchanges
- Coolest post quantum cryptography proposal
- Maths is banging

Outline

- Historical Notes
- Mathematical Background
- Addition on Elliptic Curves
- Discrete Logarithm and Diffie Hellman
- Pairings
- Isogenies

» Diophantine Equations

Historically originated in the context of solving Diophantine equations such as

$$X^n + Y^n = Z^n, \ \ X, Y, Z \in \mathbb{Z}$$

or equivalently

$$x^n + y^n = 1, \ \ x, y \in \mathbb{Q}$$

Often very hard, and in general undecidable[1]!
Let us see what we can do...

[1] In fact, already undecidable with 11 integers variables!

» One variable

$$a_nx^n + a_{n-1}x^{n-1} + \dots a_1x + a = 0$$

Quite easy! We can show that:

Theorem

Let $\frac{p}{q} \in \mathbb{Q}$ be a solution of the above equation. Then q divides a_n and p divides a_0.

Check the finite list of candidates.
Alternatively, solve numerically and find candidate of form $\frac{b}{a_n}$

Linear and Quadratic

$$ax + by = c$$

Theorem

Has infinitely many rational solution. If $\gcd(a, b)$ does not divide c, then no integers solutions. Else, infinitely many.

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

These are rational points on a conic.

* Given a rational point, all of them can be found geometrically
* Hasse principle allows us to test if a rational point exists

» Cubics

What about:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \text{ ?}$$

This is the general form of an elliptic curve! We have that

Theorem (Mordell)

If the curve is non singular, and it has a rational point then the group of rational points is finitely generated

But no equivalent of Hasse principle!

Elliptic Curves $\neq$ Ellipse

» Fields

Definition

A field $\mathbb{F}$ is set together with two operations $+, \cdot$ such that

* $\mathbb{F}$ is an abelian group under $+$ with identity 0
* $\mathbb{F} - \{0\}$ is an abelian group under multiplication with identity 1.
* For every $a, b, c \in \mathbb{F}$ we have that $a(b + c) = ab + ac$
* $0 \neq 1$

Informally, we can add, subtract, multiply and divide non zero elements.

» Finite Fields

We are mostly interested in finite fields. We have that:

Theorem

For every prime p, and every $n \in \mathbb{Z}^+$ there is an unique field of size p^n, which we denote by either $\mathbb{GF}(p^n)$ or $\mathbb{F}_{p^n}$

If $n = 1$, then $\mathbb{F}_p = \mathbb{Z}_p$, if not we can write them as

$$\mathbb{F}_{p^n} = \frac{\mathbb{F}_p[X]}{(f(x))}$$

where $f(x)$ is an irreducible polynomial of degree n.

» Characteristic

For any field, $\mathrm{char}(\mathbb{F})$ is the least integer[2] ℓ such that

$$\underbrace{1 + \ldots 1}_{\ell \text{ times}} = 0$$

We have that $\mathrm{char}(\mathbb{F}_{p^n}) = p$.

[2] Or ∞ if no such integer exists

» Field Extensions

Let k, K be two fields. If there is an homomorphism $k \to K$, we can identify k with a subfield of K. In that case, K is a **field extension** of k which we denote by $k \subseteq K$.
Given any field K we can construct the algebraic closure $\overline{K}$ which is the smallest algebraically closed extension containing K.
Some examples:

* $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
* $\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^3} \cdots \subseteq \overline{\mathbb{F}}_p$

» Weierstrass Form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

$$\downarrow$$

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

$$\Big\downarrow \ \mathrm{char}(\mathbb{F}) \neq 2, 3$$

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

Much easier to manage!

» Elliptic Curves

Definition

Let k be a field. An elliptic curve E defined over k (denoted by E/k) is given by

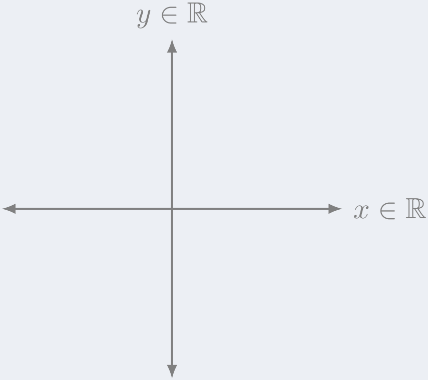
$$E : y^2 = x^3 + ax + b$$

for $a, b \in k$. For any extension $k \subseteq K$ we define

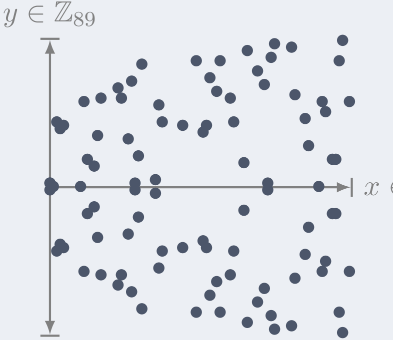
$$E(K) = \left\{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\right\} \cup \{\infty\}$$

Mathematicians are often interested with $E(\mathbb{Q}) \subseteq E(\mathbb{R}) \subseteq E(\mathbb{C})$ but we mostly consider the finite case.

» Elliptic curves



$y^2 = x^3 - 2x + 1$ over $\mathbb{R}$



$y^2 = x^3 - 2x + 1$ over $\mathbb{Z}_{89}$

» Some elliptic curves (In $E(\mathbb{R})$ since they look better...)

TODO: One singular with cusp, one node and three non singular

» Fundamental Quantities

Definition

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve.
The **discriminant** of E is

$$\Delta = -16(4a^3 + 27b^2)$$

A curve is **singular** if $\Delta = 0$.

Alternatively, let $E : y^2 = f(x)$, and let x_1, x_2, x_3 be the roots of f.

$$\Delta = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$$

i.e. $\Delta = 0 \iff f$ has a repeated root.
For now on, all curves are assumed non singular.

» j-invariant

Definition

The j-**invariant** of E is

$$j(E) = -1728\frac{(4A)^3}{\Delta}$$

In fact, an isomorphisms from a curve in short Weierstrass form must necessarily be:

$$(x, y) \mapsto (u^2 x, u^3 y)$$

for $u \in \overline{K}^*$ and this yields:

Theorem

Let E, E' be two elliptic curves over K. Then $E \cong E'$ over $\overline{K}$ if and only if $j(E) = j(E')$.

» The Group Law

TODO: Picture group law

» The Group Law: Formulae

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define

$$-P_0 = (x_0, -y_0)$$

Now, for $P_1 + P_2$:

* If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$
* If $P_1 = \infty$ then $P_1 + P_2 = P_2$, and viceversa.
* Let $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ where λ is defined as:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1}, & \text{otherwise} \end{cases}$$

This makes E into an abelian group with identity ∞

» Scalar multiplication

For $n > 0, P \in E$ we write $[n]P = \underbrace{P + \cdots + P}_{n \text{ times}}$. We then extend the notation by letting $[0]P = \infty$ and $[-n]P = [n](-P)$.
Note that we can compute $[n]P$ in $\Theta(\log n)$ group operations using square and multiply.
For $m \in \mathbb{Z}$ we can define a map $[m] : E \to E$ accordingly, and write:

$$E[m] \coloneqq \ker[m]$$

to be the m-**torsion subgroup** of E.

» Number of Points on a curve

Heuristically, we expect $\approx q+1$ points

Theorem (Hasse)

Let E be an elliptic curve defined over $\mathbb{F}_q$.

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

Exact value can be efficiently found using Schoof's algorithm in $O((\log q)^8)$.

» Discrete Logarithm

Cryptography relies on hardness assumptions.

Definition

Let $\mathrm{Gen}(1^\lambda)$ be a p.p.t. algorithm that returns a group description $\mathbb{G} = (+, P, q)$, where $\mathbb{G} = \langle P \rangle$ and $q = \#\mathbb{G}$. For an attacker $\mathcal{A}$, define

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{dlp}}(\lambda) = \Pr\left[\mathcal{A}\left(1^\lambda, \mathbb{G}, [k]P\right) = k \,\middle|\, \begin{array}{c} \mathbb{G} \leftarrow\$\ \mathrm{Gen}(1^\lambda) \\ k \leftarrow\$\ \mathbb{Z}_q \end{array}\right]$$

We say that the **discrete logarithm assumption** hold with respect to Gen if, for every p.p.t. attacker $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{dlp}}(\cdot)$ is negligible.

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

* CHD: From $[x]P, [y]P$ compute $[xy]P$
* DDH: Distinguish $(P, [x]P, [y]P, [xy]P)$ from $(P, [x]P, [y]P, [z]P)$

In fact, pairings make DDH easy on elliptic curves!

$$\mathrm{DDH} \leq_R \mathrm{CDH} \leq_R {}^3\mathrm{DLP}$$

Representation matters! $\mathbb{Z}_{p-1} \cong \mathbb{Z}_p^*$ as groups but the discrete logarithm is trivial in the former, assumed hard in the latter.

[3] In fact equivalent

» Why elliptic curves?

Assumption	Group	Best Algorithm	$\approx$ Complexity
RSA	$\mathbb{Z}_N$	Number Field Sieve	$\exp(c\sqrt[3]{\log N})$
DLP	$\mathbb{F}_p^*$	Number Field Sieve	$\exp(c\sqrt[3]{\log p})$
DLP	$E(\mathbb{F}_p)$	Pollard Rho	$\sqrt{p}$

Best known attacks against ECC are generic attacks

* Shorter keysizes (≈ 256 vs[4] 3072 bits)
* Faster computation[5]

[4] For 128 bits of security

[5] against other DLP schemes and private RSA ops

» EC Diffie Hellman Key Exchange

Let E be an elliptic curve over $\mathbb{F}_q$. Let p be a large prime dividing $\#E(\mathbb{F}_q)$ and P a point of order p.

Diffie Hellman		
Alice		**Bob**
$x \xleftarrow{\$} \mathbb{Z}_q$		$y \xleftarrow{\$} \mathbb{Z}_q$
$Q_A = [x]P$		$Q_B = [y]P$
	$\xrightarrow{Q_A}$	
	$\xleftarrow{Q_B}$	
$K = [x]Q_B$		$K = [y]Q_A$

Correctness follows since:

$$K = [x]Q_B = [x][y]P = [xy]P = [y][x]P = [y]Q_A = K$$

» Easy Elliptic Curves

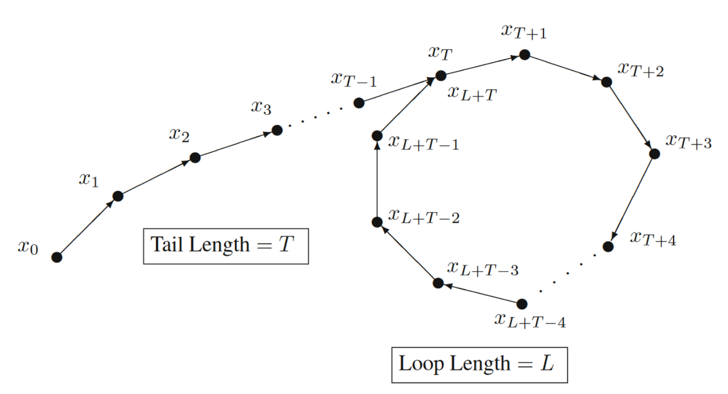
DLP is not equally hard on every curve!

- Singular curves over $\mathbb{F}_p$. Equivalent to DLP in[6] $\mathbb{F}_p^*$ or $\mathbb{F}_p^+$
- Curves and subgroups with small embedding degree. E.g. supersingular and anomalous curves
- Curves that admit pairings to small finite fields.
- Curves defined over $\mathbb{F}_{p^k}$ for k with small factors. GHS Method, Diem's Analysis.

[6] Or in some small extension

» Pollard Rho

Collision search for $f : S \to S$. Let $x_0 \in S$, $x_n = f(x_{n-1})$.
Expected $\sqrt{\pi \# S/2}$ calls to f, constant memory.



» Pollard Rho

Let G be a group of order N. We want to find k s.t. $[k]P = Q$. Split $G = A \sqcup B \sqcup C$ with $\#A \approx \#B \approx \#C$. Define

$$f(X) = \begin{cases} P + X, & X \in A \\ [2]X, & X \in B \\ Q + X, & X \in C \end{cases}$$

Let $X_0 = \infty$, then $X_i = [\alpha_i]P + [\beta_i]Q$ and we can track α_i, β_i. A collision $X_j = X_{j+\ell}$ with $\gcd(\beta_{j+\ell} - \beta_j, N) = 1$ allows us to solve the DLP with

$$k \equiv \frac{\alpha_j - \alpha_{j+\ell}}{\beta_{j+\ell} - \beta_j} \pmod N$$

» Pairings

Definition

Let $\mathbb{G}, \mathbb{G}_T$ be two groups. A **pairing** is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that is:

- Non degenerate:

$$e(S,T) = 1 \; \forall S \in \mathbb{G} \implies T = 0_{\mathbb{G}}$$

- Bilinear:

$$e(S_1 + S_2, T) = e(S_1, T)e(S_2, T)$$

$$e(S, T_1 + T_2) = e(S, T_1)e(S_2, T_2)$$

- Alternating:

$$e(T,T) = 1$$

» Weil Pairing

Every elliptic curve E over K admits an efficiently computable pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

where μ_m is the group of m-th root of unity.
In degenerate on cyclic subgroups of $E[m]$, so use modified Weil pairing

$$\langle \cdot, \cdot \rangle : E[m] \times E[m] \to \mu_m$$
$$\langle P, Q \rangle = e_m(S, \phi(Q))$$

For $\phi : E \to E$ a distorsion map[7]

[7] If it exists

» BLS Signatures

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p. Let P be a generator of $\mathbb{G}$, and e a non degenerate pairing. Also, let $H : \{0,1\}^* \to \mathbb{G}$

$$
\begin{array}{ll}
\underline{\mathrm{Gen}(1^\lambda)} & \underline{\mathrm{Sign}(sk, m)} \\
x \leftarrow\$ \mathbb{Z}_p & Q \leftarrow H(m) \\
pk := [x]P & \sigma \leftarrow [x]Q \\
sk := x & \textbf{return } \sigma \\
\textbf{return } (pk, sk) &
\end{array}
$$

$$
\begin{array}{l}
\underline{\mathrm{Verify}(pk, m, \sigma)} \\
\textbf{return } e(\sigma, P) =_? e(H(m), [x]P)
\end{array}
$$

Correctness by:

$$e(\sigma, P) = e([x]Q, P) = e(Q, P)^x = e(Q, [x]P) = e(H(m), [x]P)$$

» Post Quantum

* Discrete logarithms, RSA, and pairings broken by Shor's algorithm

» Post Quantum

* Discrete logarithms, RSA, and pairings broken by Shor's algorithm
* Can we recover?

Post Quantum

* Discrete logarithms, RSA, and pairings broken by Shor's algorithm
* Can we recover?
* Yes, lattices, codes, multinear maps...

Post Quantum

* Discrete logarithms, RSA, and pairings broken by Shor's algorithm
* Can we recover?
* Yes, lattices, codes, multinear maps...
* **Isogenies!**

» Isogenies

"Nice maps" between elliptic curves.

Definition

Let E_1, E_2 be elliptic curves. An **isogeny** is a morphism

$$\phi : E_1 \to E_2$$

with $\phi(\infty) = \infty$. If $\phi(E_1) \neq \{\infty\}$, E_1 is **isogenous** to E_2.

For example, the curves $y^2 = x^3 + x$ and $y^2 = x^3 - 3x + 3$ are isogenous over $\mathbb{F}_{71}$ via the isogeny

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, y \cdot \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \right)$$

» Properties of isogenies

- Each isogeny is also a group homomorphism
- The map $[m] : E \to E$ is an isogeny
- You can compose isogenies
- Each isogeny has a degree, and it is multiplicative $\deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$
- Each isogeny $\phi : E_1 \to E_2$ has a unique dual $\hat{\phi} : E_2 \to E_1$ such that
$$\phi \circ \hat{\phi} = [\deg(\phi)]$$
- An isogeny between two Weierstrass curves has the form
$$(x, y) \mapsto \left(\frac{f}{h^2}(x), y \cdot \frac{g}{h^3}(x)\right)$$

» Separable and Inseparable Isogenies

Definition

Let $E/k : y^2 = x^3 + ax + b$, with $\mathrm{char}(k) = p$. Define $E^{(p^r)} : y^2 = x^3 + a^{p^r} x + b^{p^r}$. The map:

$$\pi : E \to E^{(p^r)}, (x, y) \mapsto \left(x^{p^r}, y^{p^r}\right)$$

is the (p^r)-**Frobenius isogeny**. Note if $k = \mathbb{F}_{p^r}$ then $E^{(p^r)} = E$

If an isogeny factors trough a Frobenius isogeny it is inseparable. If it is a Frobenius followed by an isomorphisms, it is purely inseparable. We are mostly concerned with the separable case.

» Kernel and Velu

Theorem

There is a one to one correspondence between finite subgroups of elliptic curves and separable isogenies from that curve, up to post-compostion with isomorphisms

$$\textit{kernels} \longleftrightarrow \textit{isogenies}$$

Let E/k, with k a finite field. For any subgroup $H \leq E$ we can find an isogeny with kernel H in $\Theta(\#H)$ using Velu's formulas. We denote the target of that isogeny by E/H

» Computing large degree isogenies

- Velu's formula are too slow for large degree
- Decompose ℓ^k isogenies in k ℓ-isogenies
- Speedup from $\Theta(\ell^k)$ to $\Theta(k^2\ell)$

Take $H \cong \mathbb{Z}_{\ell^k}$. Set $\ker\psi_i = [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(H)$. Then $\deg(\psi_i) = \ell$ and

$$\begin{tikzcd} E \arrow[r, "\psi_1"] \arrow[rrrr, bend left] & E_1 \arrow[r, "\psi_2"] & \cdots \arrow[r, "\psi_{k-1}"] & E_{k-1} \arrow[r, "\psi_k"] & E/H \end{tikzcd}$$

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

- Something something order in a quaternion algebra?
- There are $\approx \lfloor \frac{p}{12} \rfloor$ supersingular curves over $\mathbb{F}_{p^n}$.
- A supersingular curve has $p + 1$ points.
- Insecure for DLP
- Secure for CSSI (later)!

» Isogeny Problems

It is easy to find out if two curves are isogenous

Theorem

Two curves E_1, E_2 over a finite field k are isogenous over k if and only if $\#E_1(k) = \#E_2(k)$.

Finding the isogeny is dramatically harder:

Definition

The **computational supersingular isogeny problem** is as follows: Given two supersingular elliptic curves E, E', find an isogeny between them.

» Isogeny Graphs

TODO: Insert picture

» Isogeny Graphs

Let p, ℓ be a primes.

Definition

The ℓ-**supersingular isogeny graph** has as:

* Vertices: Supersingular Elliptic curves over $\overline{\mathbb{F}}_p$
* Edges: Separable isogenies from $E \to E'$

Both up to isomorphisms (i.e. vertices are j-invariants)

* We can represent vertices as elements of $\mathbb{F}_{p^2}$
* Graph is directed
* Graph has good mixing properties
* Can walk in the graph with Velu's method
* Most vertices have degree $\ell + 1$

» SIDH

TODO: Picture

» SIDH

Picture to keep in mind:

$$\begin{tikzcd} E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A \arrow[d, "\phi'_B"] \\ E_B \arrow[r, "\phi'_A"'] & E_{AB} \cong E_{BA} \end{tikzcd}$$

Details will follow

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\overline{\mathbb{F}}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A \rangle = E[2^{e_A}], \langle P_B, Q_B \rangle = E[3^{e_B}]$.

* Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
* Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A \rangle = E_A$
* Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B \rangle = E_B$
* The public keys are $\mathrm{pk}_X = (E_X, P'_X = \phi_X(P_X), Q'_X = \phi_X(Q_X))$
* Alice computes $S'_A = P'_B + [n_A]Q'_B$, and an isogeny $\phi'_A : E_B \to E/\langle S'_A \rangle = E_{AB}$
* Bob computes $S'_B = P'_A + [n_B]Q'_A$, and an isogeny $\phi'_B : E_A \to E/\langle S'_B \rangle = E_{BA}$
* The final secret is $j(E_{AB}) = j(E_{BA})$

» SIDH and SIKE

* SIDH is vulnerable to active attacks
* SIKE uses the Fujisaki-Okamoto transform to fix this
* SIKE in the Alternate Candidates of Round 3 of the NIST PQC competion
* Very short keys
* Currently slower than most other schemes
* Best known attack is classical

» Security

Best attack is on CSSI problem. Suppose we want to find an ℓ^a-isogeny between $E_0 \to E_1$, both supersingular over $\bar{\mathbb{F}}_p$. Let $k \approx a/2$ and

$$\begin{gathered} S_{i,k} := \left\{ H \leq E_i[\ell^k] \mid \; H \text{ cyclic}, |H| = \ell^k \right\} \\ S := (\{0\} \times S_{0,k}) \sqcup (\{1\} \times S_{1,k}) \\ g : S \to \mathbb{F}_{p^2}, \; (i, H) \mapsto j(E_i/H) \end{gathered}$$

A collision $g(0, H) = g(1, H')$ will solve the isogeny problem. To allow for Pollard-Rho style methods, let $h : \mathbb{F}_{p^2} \to S$ be a hash function, and let:

$$f : S \to S, \; f := h \circ g$$

» Security

h maps a set $\approx p/12$ to S which has size $\approx p^{1/4}$ so introduces a lot of collisions. To find a 'golden' one we use the van Oorschot Wiener (vOW) algorithm. When using m processors and w memory cells, time complexity[8] is

$$\frac{2.5}{m}\sqrt{\#S^3/w} = O(p^{3/8})$$

TODO: Add image

[8] In terms of ℓ^k-isogeny computations

» Conclusion

* Elliptic curves are pretty damn cool
* We only scratched the surface!
* Elliptic Curve Diffie Hellman base of most of web key exchanges
* BLS Pairing based signatures both efficient and secure
* SIKE leverages isogenies for post quantum security

» Resources

- J.H. Silverman, J.T. Tate, Rational Points on Elliptic Curves
- J.H. Silverman, The Arithmetic of Elliptic Curves[9]
- D.A. Cox, Primes of the form $x^2 + ny^2$
- L. Panny, notes: [intro] [isogenies problems]
- C. Costello, Supersingular isogeny key exchange for beginners
- R. Granger, A. Joux, Computing Discrete Logarithms [5.2, 5.3]

[9] The bible