Isogeny-based cryptography

Enric Florit Zacarías

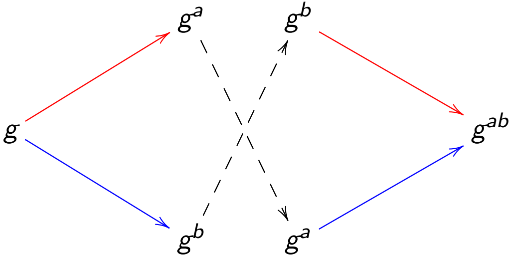
STNB 2020

5 de febrer de 2020

Diffie-Hellman (1976)

Let G be a cyclic group generated by g and with order N.

- **Alice** picks $a \in \mathbb{Z}/N\mathbb{Z}$ and sends $A = g^a$.
- **Bob** picks $b \in \mathbb{Z}/N\mathbb{Z}$ and sends $B = g^b$.
- **Shared secret**: $A^b = B^a = g^{ab}$.



Diffie-Hellman security?

Discrete logarithm problem (DLP)

Given a cyclic group $G = \langle g \rangle$ and an element $A \in G$, find $a \in \mathbb{Z}/N\mathbb{Z}$ such that $A = g^a$.

Algorithm	**Complexity**
Exhaustive search	$O(N)$
Baby step – giant step	Time $O(\sqrt{N})$, memory $O(\sqrt{N})$
Pohlig-Hellman	$O(\sum_{i=1}^{r} e_i(\log N + \sqrt{p_i}))$
Index calculus in $\mathbb{F}_{p^n}^{\times}$	$L_{p^n}[1/2, \sqrt{2}]$
NFS-DLP in $\mathbb{F}_{\mathbf{p^n}}^{\times}$	$\mathbf{L_{p^n}[1/3, c]}$

Table: Algorithms solving DLP in a group of order $N = \prod_{i=1}^{r} p_i^{e_i}$.

- Shor, 1994: polynomial-time quantum algorithms to solve DLP and factorization.

Postquantum Cryptography

A postquantum cryptosystem must meet two requirements:

- It must be efficient to use with existing hardware.
- It must be resistent both to classical and quantum adversaries.

Isogeny-based cryptography is an attempt to develop postquantum cryptography.

Quotient curves

Theorem

Let E be an elliptic curve over K, and let G be a finite subgroup of E. Then, there exist an elliptic curve E' and a separable isogeny $\phi\colon E \to E'$, both unique up to isomorphism, such that $\ker \phi = G$.

- Corollary: isogenies decompose into prime-degree factors.
- Vélu formulas allow us to compute ϕ and E/G in $O(|G|)$ time and memory.

Computational isogeny problems

Problem

Given E, E' isogenous curves, find an isogeny $E \to E'$.

- Exponential complexities, $O(\sqrt{p}\log^2 p)$. See works by Kohel, Galbraith, Delfs, etc. But easier if...
- The degree is known.
- The kernel structure is known (e.g., cyclic kernel).
- The curve is **ordinary** (quantum subexponential time).

Supersingular curves

Theorem

Let E be a curve over a finite field $\mathbb{F}_q$, $q = p^r$. TFAE:

- *E is supersingular.*
- *$E[p] = \{\mathcal{O}\}$.*
- *$[p]$ is purely inseparable.*
- *$\#E(\mathbb{F}_q) = q + 1 - t$, with $t \equiv 0 \mod p$.*
- *$End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion algebra.*

The j invariant of a supersingular curve lies in $\mathbb{F}_{p^2}$. Given a prime p, there are about $p/12$ supersingular elliptic curve isomorphism classes defined over $\bar{\mathbb{F}}_p$.

Protocol parameters

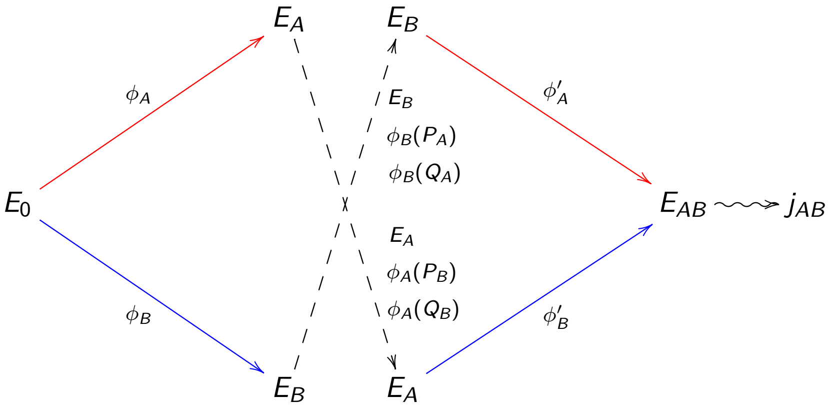
- Choose a prime of the form $p = \ell_A^{e_A}\ell_B^{e_B} f \pm 1$, $\ell_A^{e_A} \approx \ell_B^{e_B}$.
- Initial curve E_0 having $\#E_0(\mathbb{F}_{p^2}) = (\ell_A^{e_A}\ell_B^{e_B} f)^2$ points ($\implies E_0$ supersingular).

Lemma

Let E be an elliptic curve over $\mathbb{F}_q$. Assume π_E is in $\mathbb{Z}$, and let $n \geq 1$ such that $n^2 \mid \#E(\mathbb{F}_q)$. Then $E[n] \subset E(\mathbb{F}_q)$.

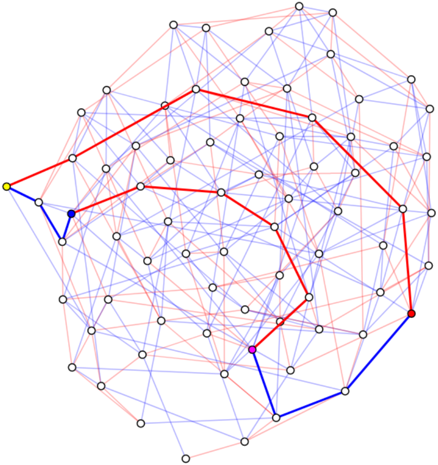
As a consequence, $E_0[\ell_A^{e_A}]$, $E_0[\ell_B^{e_B}] \subset E_0(\mathbb{F}_{p^2})$, and all our isogenies will be defined over $\mathbb{F}_{p^2}$.
Fix bases $E_0[\ell_A^{e_A}] = \{P_A, Q_A\}$, $E_0[\ell_B^{e_B}] = \{P_B, Q_B\}$.

SIDH key exchange (Jao and De Feo, 2011)



SIDH visualization

$$p = 2^5 3^3 - 1 = 863$$



Computation of ℓ^e-isogenies

We want to compute $\phi\colon E \to E/\langle R\rangle$ with $\mathrm{ord}(E) = \ell^e$.
Let $E_0 = E$, $R_0 = R$, and for $0 \le i < e$, let

$$E_{i+1} = E_i/\langle \ell^{e-i-1} R_i\rangle, \quad \phi_i\colon E_i \to E_{i+1}, \quad R_{i+1} = \phi_i(R_i).$$

Then $E/\langle R\rangle = E_e$ and $\phi = \phi_{e-1} \circ \cdots \circ \phi_0$.

Data: E, P, ℓ, e
Result: $\phi\colon E \to E/\langle P\rangle$
$P_0 \leftarrow P$
for $1 \le i \le e-1$ **do**
  $P_i \leftarrow [\ell]P_{i-1}$
end
$\phi \leftarrow id_E$
for $0 \le i \le e-1$ **do**
  $\phi_i\colon E_i \to E_i/\langle \phi(P_{e-1-i})\rangle$
  $\phi \leftarrow \phi_i \circ \phi$
end

Computational problem

Problem (Supersingular Isogeny problem (CSSI))

Let $\phi_A \colon E_0 \to E_A$ be an isogeny with kernel $\langle m_A P_A + n_A Q_A \rangle$, where m_A, n_A are chosen randomly in $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ and not both divisible by ℓ_A. Given the curves E_0, E_A and the values $\phi_A(P_B)$ and $\phi_A(Q_B)$, find a generator R_A of $\langle m_A P_A + n_A Q_A \rangle$.

Analog to DLP in the Diffie-Hellman setting.

SIDH security

- The best strategy to break SIDH is almost brute-force, at $O(\sqrt[4]{p})$ and $O(\sqrt[6]{p})$ (exponential in $\log p \sim e_A, e_B$).
- It looks like the **auxiliary points** ($\phi_A(P_B)$ and so on) are revealing too much information, but so far nobody* has been able to exploit them.

The *claw* algorithm

Problem

Given isogenous curves E, $E/\langle R\rangle$, compute an isogeny $\phi\colon E \to E/\langle R\rangle$ of degree ℓ^e, and compute R.

1. Compute all isogenies $E \to E'$ of degree $\ell^{e/2}$, store the E' in a dictionary.
2. Compute all isogenies $E/\langle R\rangle \to E'$ of degree $\ell^{e/2}$, until some E' is in the dictionary.
3. Compose both isogenies*.

Duals of cyclic isogenies

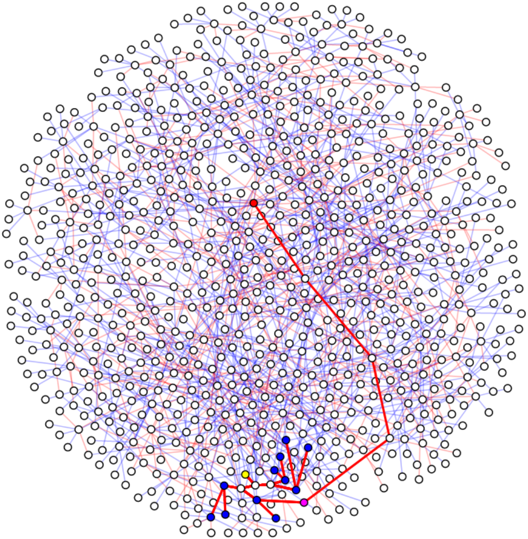
Lemma

Let $\psi\colon E \to E/\langle R\rangle$ be a cyclic ℓ^e-isogeny, with $R \in E[\ell^e]$. Then, its dual isogeny $\hat{\psi}$ is also cyclic. More precisely, if $E[\ell^e] = \langle P, Q\rangle$ and $R = P + \alpha Q$, then $\ker\hat{\psi} = \langle \psi(Q)\rangle$.

Remark

The composition of cyclic isogenies of coprime degree is cyclic.

The *claw* algorithm visualized



Work in progress

- Computation of cyclic isogenies $E_0 \to E_A$, given the degree N.
- Computation of isogenies $E_0 \to E_A$, given the structure of the kernel.
- Given an isogeny $\phi = \phi_{e-1} \circ \cdots \circ \phi_0$, compute its kernel.