Generalising Fault Attacks to Genus Two Isogeny Cryptosystems

Ariana Goh, Chu-Wee Lim, Yan Bo Ti

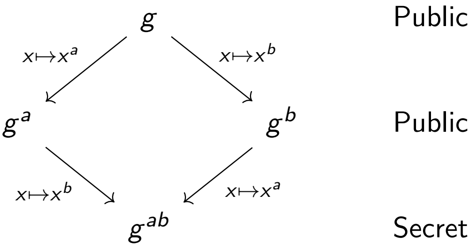
DSO National Laboratories, Singapore

16 September 2022

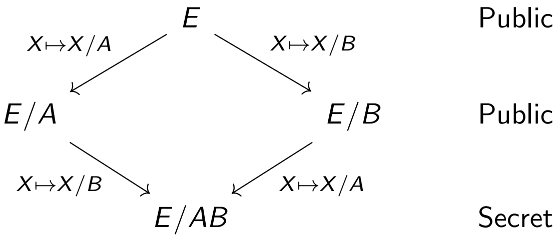
Outline

- Elliptic Curves and Isogenies
- SIDH fault attack
- G2SIDH fault attack

Diffie Hellman



SIDH overview

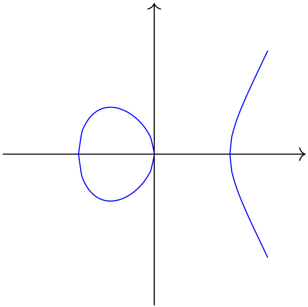


Elliptic Curves

An *elliptic curve* E is a curve given by

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

E.g. $y^2 = x^3 - x$,

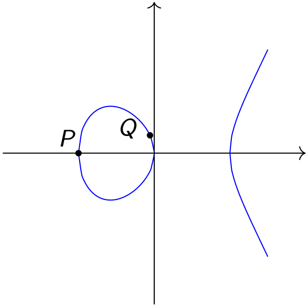


Elliptic Curves

An *elliptic curve* E is a curve given by

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

E.g. $y^2 = x^3 - x$, $P = (-1, 0) \in E(\mathbb{Q})$

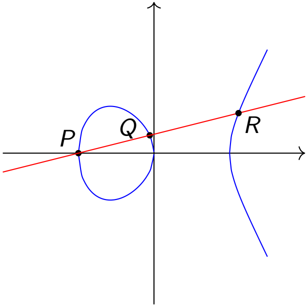


Elliptic Curves

An *elliptic curve* E is a curve given by

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

E.g. $y^2 = x^3 - x$, $P = (-1, 0) \in E(\mathbb{Q})$

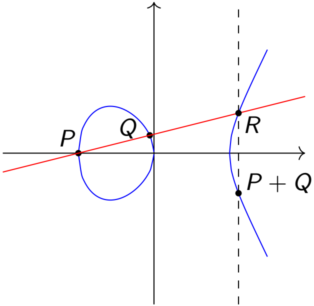


Elliptic Curves

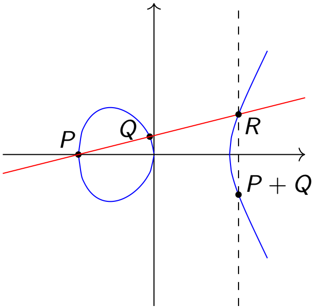
An *elliptic curve* E is a curve given by

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

E.g. $y^2 = x^3 - x$, $P = (-1, 0) \in E(\mathbb{Q})$



Elliptic Curves



Elliptic curves forms an abelian group under modulo p ($\mathbb{F}_p$):

- Group: $(P+Q)+R = P+(Q+R)$, $\mathcal{O}+P = P+\mathcal{O} = P$
- Abelian: $P+Q = Q+P$

Isogenies

Isogenies are maps $\phi : E \to E'$ between elliptic curves such that

$$\phi(P +_E Q) = \phi(P) +_{E'} \phi(Q)$$

Example: $[N] : E \to E$, $P \mapsto [N]P = P \underbrace{+ \cdots +}_{N \text{ times}} P$

For subgroups $A \subset E$, there exists a isogeny $\phi : E \to E/A$ such that $\phi(P) = \mathcal{O}_{E/A} \iff P \in A$, equivalently, if $\ker\phi = A$.

$$E[N] = \ker[N]$$

SIDH Protocol

Choose Elliptic curve $E/\mathbb{F}_{p^2}$ such that

- $E\left[\ell_A^{e_A}\right] = C^2_{\ell_A^{e_A}}$, generated by P_A, Q_A
- $E\left[\ell_B^{e_B}\right] = C^2_{\ell_B^{e_B}}$, generated by P_B, Q_B

Alice	Bob
$A = P_A + [r_A]Q_A$	$B = P_B + [r_B]Q_B$
$\phi_A : E \to E/\langle A\rangle$	$\phi_B : E \to E/\langle B\rangle$

Alice → Bob: $E/\langle A\rangle, \phi_A(P_B), \phi_A(Q_B)$

Bob → Alice: $E/\langle B\rangle, \phi_B(P_A), \phi_B(Q_A)$

Alice	Bob
$\phi_B(A) = \phi_B(P_A) + [r_A]\phi_B(Q_A)$	$\phi_A(B) = \phi_A(P_B) + [r_B]\phi_A(Q_B)$
$E/\langle B\rangle \to E/\langle A, B\rangle$	$E/\langle A\rangle \to E/\langle A, B\rangle$

SIDH Fault Attack

Idea: Given $\phi_A(R)$ for $R \in E[\ell_A^{e_A}]$, if $\langle A, R\rangle = E\left[\ell_A^{e_A}\right]$, then

$$\hat{\phi}_A = (E/\langle A\rangle \to E/\langle A, R\rangle) \cong E$$

Fault attack: Fault the computation of $\phi_A(P_B)$ such that Alice sends $\phi_A(R)$. We can get the image of a point in $E\left[\ell_A^{e_A}\right]$ with

$$\frac{\#E/\mathbb{F}_{p^2}}{\ell_A^{e_A}}\phi_A(R) = \phi_A\left(\underbrace{\frac{\#E/\mathbb{F}_{p^2}}{\ell_A^{e_A}}R}_{R'}\right)$$

SIDH Fault Attack Probabilities

$$\frac{\#E/\mathbb{F}_{p^2}}{\ell_A^{e_A}}\phi_A(R) = \phi_A\left(\underbrace{\frac{\#E/\mathbb{F}_{p^2}}{\ell_A^{e_A}}R}_{R'}\right)$$

$$\frac{\left|E\left[\ell_A^{e_A}\right]\right|}{|\langle A, R'\rangle|} = \ell_A^k \text{ occurs with probability } \frac{\ell_A - 1}{\ell_A^{k+1}}$$

$$\left|E\left[\ell_A^{e_A}\right]\right| = \left|\langle A, R'\rangle\right| \text{ with probability } 1 - \frac{1}{\ell_A}$$

G2SIDH Overview

In genus 2, we can still add points, have isogenies and form quotients $\phi : \mathcal{A} \to \mathcal{A}/G$.
However instead of $E\left[\ell_A^{e_A}\right] = C^2_{\ell_A^{e_A}}$, we have $\mathcal{A}\left[\ell_A^{e_A}\right] = C^4_{\ell_A^{e_A}}$
Kernel of isogeny used in G2SIDH is generated by 2 or 3 elements.

G2SIDH Protocol

1. Choose $\mathcal{A}\left[\ell_A^{e_A}\right] = C^4_{\ell_A^{e_A}} = \langle P_1, P_2, P_3, P_4 \rangle$, $\mathcal{A}\left[\ell_B^{e_B}\right] = C^4_{\ell_B^{e_B}} = \langle Q_1, Q_2, Q_3, Q_4 \rangle$
2. Alice and Bob chooses secret subgroups $A \in \mathcal{A}\left[\ell_A^{e_A}\right]$, $B \in \mathcal{A}\left[\ell_B^{e_B}\right]$ respectively
3. Alice and Bob computes $\phi_A : \mathcal{A} \to \mathcal{A}/A$, $\phi_B : \mathcal{A} \to \mathcal{A}/B$ respectively
4. $\mathcal{A}/A \, , \mathcal{A}/B \, , \phi_A(Q_i) \, , \phi_B(P_i)$ are exchanged publically
5. Alice and Bob computes $\mathcal{A}/(AB)$

G2SIDH Fault Attack Overview

- Idea: Having image of $\mathcal{A}\left[\ell_A^{e_A}\right]$ under ϕ_A is enough to recover ϕ_A
- Fault attack: Force Alice to output the image of random points under ϕ_A
- Need to fault more points to get $\phi_A\left(\mathcal{A}\left[\ell_A^{e_A}\right]\right)$
- Probability of full recovery and how much brute force needed is more intricate

G2SIDH Fault Attack Results

Probability that n faults gives a subgroup of index ℓ_A^k where $\phi_A\left(\mathcal{A}\left[\ell_A^{e_A}\right]\right)$ has m generators is

$$\ell_A^{-nk}\left(\prod_{i=0}^{m-1} 1-\ell_A^{i-m}\right)\left(\prod_{i=1}^{k}\frac{1-\ell_A^{m+k-i}}{1-\ell_A^{i}}\right)$$

Average amount of isogenies to brute force through when $m = n = 2$:

$$\frac{\ell_A^7+16\ell_A^6+75\ell_A^5+176\ell_A^4+219\ell_A^3+176\ell_A^2+65\ell_A+16}{(\ell_A^2-1)^4}$$

G2SIDH Fault Attack Results

If $\phi_A(\mathcal{A}[2^{e_A}])$ has 2 generators, the probability that $2, 3, 4$ faults is enough is $0.38, 0.66, 0.82$

If $\phi_A(\mathcal{A}[2^{e_A}])$ has 3 generators, the probability that $3, 4$ faults is enough is $0.33, 0.62$