On the Security of Supersingular Isogeny Cryptosystems

Yan Bo Ti

Department of Mathematics,
University of Auckland

AsiaCrypt 2016, 5th of December

Outline

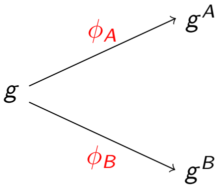
Joint work with **Steven Galbraith**, **Christophe Petit** and **Barak Shani**.

1. Preliminaries
   - Diffie–Hellman
   - Isogenies
   - Supersingular elliptic curves
   - Jao–De Feo key exchange

2. Findings
   - Adaptive attack
   - Reduction to computing endomorphism ring
   - Bit-security result

Diffie–Hellman

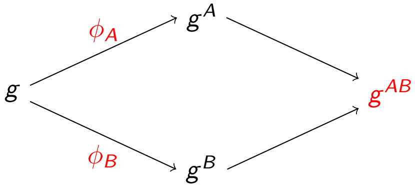
Pick an abelian group $G = \langle g \rangle$.



- Picks secret A which determines $\phi_A : G \to G$, $g \mapsto g^A$.
- Sends g^A.

Diffie–Hellman

Pick an abelian group $G = \langle g \rangle$.



- Receives g^B.
- Computes

$$\begin{aligned}(g^B)^A &= g^{AB} \\ &= (g^A)^B .\end{aligned}$$

- Use g^{AB} as secret key.

- Alice uses long term secret A.
- Adversary will play the role of Bob.
- Adversary sends h instead of g^B, where $\mathrm{ord}(h) = r$ is small.
- Adversary is able to learn $A \pmod{r}$.
- Adversary repeats with different h's to recover all of A.

- Fix a finite field $k = \mathbb{F}_p$ and a finite extension $K = \mathbb{F}_q$ where $q = p^k$.
- Let E_1 and E_2 be elliptic curves over K.

Definition

An isogeny between E_1 and E_2 is a non-constant morphism defined over $\mathbb{F}_q$ that sends $\mathcal{O}_1$ to $\mathcal{O}_2$. We say that E_1 and E_2 are isogenous.

Fun facts:

- Isogenies are group homomorphisms.
- If ϕ is separable, then $\# \ker \phi = \deg \phi$.
- For every finite subgroup $G \subset E_1$, there is a unique E_2 (up to isomorphism) and a separable $\phi : E_1 \to E_2$ such that $\ker \phi = G$. We write $E_2 = E_1/G$.
- The isogeny can be constructed by an algorithm by Vélu.

Definition

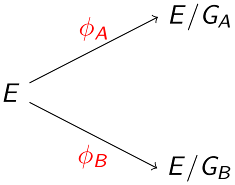
An elliptic curve $E/\mathbb{F}_{p^k}$ is said to be supersingular if $\#E(\mathbb{F}_{p^k}) \equiv 1 \pmod{p}$.

Fun facts:

- All supersingular elliptic curves can be defined over $\mathbb{F}_{p^2}$.
- There are approximately $p/12$ supersingular curves up to isomorphism.

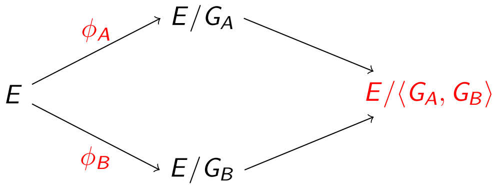
Set up:

- Choose $p = 2^n \cdot 3^m \cdot f - 1$, such that $2^n \approx 3^m$ and f small.
- Choose supersingular elliptic curve E over $\mathbb{F}_{p^2}$.
- Then $E[2^n], E[3^m] \subseteq E(\mathbb{F}_{p^2})$.
- Alice works over $E[2^n]$ with linearly independent points P_A, Q_A.
- Bob works over $E[3^m]$ with linearly independent points P_B, Q_B.



- Picks secret (a_1, a_2) which determines $G_A = \langle [a_1]P_A + [a_2]Q_A \rangle$.
- Computes ϕ_A with $\ker \phi_A = G_A$ via Vélu.
- Sends E/G_A, $\phi_A(P_B)$, $\phi_A(Q_B)$.

Jao–De Feo



- Receives E/G_B, $\phi_B(P_A)$, $\phi_B(Q_A)$.
- Computes

$$\begin{aligned} G'_A &= \langle [a_1]\phi_B(P_A) + [a_2]\phi_B(Q_A)\rangle \\ &= \langle \phi_B([a_1]P_A + [a_2]Q_A)\rangle \\ &= \langle \phi_B(G_A)\rangle \,. \end{aligned}$$

- Uses $j(E_{AB})$ as secret key.

Definition (Supersingular isogeny problem)

Given a finite field K and two isogeneous supersingular elliptic curves defined over K, compute an isogeny $\varphi : E_1 \to E_2$.

Importance of correct isogeny

Definition (Supersingular isogeny problem)

Given a finite field K and two isogeneous supersingular elliptic curves defined over K, compute an isogeny $\varphi : E_1 \to E_2$.

- There are infinitely many isogenies $E \to E_A$.
- We need $E/\langle G_A, G_B \rangle = E_A/\langle \phi_A(G_B) \rangle = E_B/\langle \phi_B(G_A) \rangle$.
- Given some $\phi : E \to E_A$, to complete the square, one needs $\ker \phi \subseteq \langle P_A, Q_A \rangle$.

Importance of correct isogeny

Definition (Supersingular isogeny problem)

Given a finite field K and two isogeneous supersingular elliptic curves defined over K, compute an isogeny $\varphi : E_1 \to E_2$.

Definition (Special supersingular isogeny problem)

Given a special prime p, E and E_A, and generators of a torsion subgroup in E and E_A, and given that there exists $\phi_A : E \to E_A$ with $\deg \phi_A = 2^n$, recover ϕ_A.

- Recall we have E and $P_A, Q_A \in E[2^n]$, and $\ker \phi_A = \langle [a_1]P_A + [a_2]Q_A \rangle$.
- Dishonest user is playing Bob.
- Model: $O(E, R, S, E')$ returns 1 if $j(E') = j(E/\langle [a_1]R + [a_2]S \rangle)$ and 0 otherwise.
  This corresponds to Alice taking Bob's protocol message, completing her side of the protocol, and then performing some operations using the shared key that return an error message if shared key is not $j(E')$.

- Complete honest round of protocol with $(E_B, R = \phi_B(P_A), S = \phi_B(Q_A))$ and obtain E_{AB}.
- In next round, choose suitable integers a, b, c, d and send $(E_B, [a]R + [b]S, [c]R + [d]S)$ to Alice.
- Recover parity of a_2:
  - Query oracle on $(E_B, R, S + [2^{n-1}]R, E_{AB})$.
  - Then subgroup is

$$\langle [a_1]R + [a_2]S + [a_2][2^{n-1}]R \rangle = \begin{cases} \langle [a_1]R + [a_2]S \rangle & \text{if } a_2 \text{ even,} \\ \langle [a_1]R + [a_2 + 2^{n-1}]S \rangle & \text{if } a_2 \text{ odd.} \end{cases}$$

Lemma

Assuming that Alice has chosen (a_1, a_2) *as her private key such that both are not simultaneously even, an attacker may assume that the private key is of the form* $(1, \alpha)$ *or* $(\alpha, 1)$*.*

If a_2 even, then secret key is of the form $(1, \alpha)$. If not, one can take secret key to be of the form $(\alpha, 1)$.

- Suppose secret is $(1, \alpha)$.

Lemma

Assuming that Alice has chosen (a_1, a_2) as her private key such that both are not simultaneously even, an attacker may assume that the private key is of the form $(1, \alpha)$ or $(\alpha, 1)$.

If a_2 even, then secret key is of the form $(1, \alpha)$. If not, one can take secret key to be of the form $(\alpha, 1)$.

- Suppose secret is $(1, \alpha)$.
- Inductively recover all bits of α.
- Recover parity of α:
    - Query oracle on $(E_B, R, [1 + 2^{n-1}]S, E_{AB})$.
    - Then subgroup is

$$\langle R + [\alpha]S + [\alpha][2^{n-1}]R \rangle = \begin{cases} \langle R + [\alpha]S \rangle & \text{if } \alpha \text{ even,} \\ \langle R + [\alpha + 2^{n-1}]S \rangle & \text{if } \alpha \text{ odd.} \end{cases}$$

Implications

- Static key implementations are vulnerable.
- Recovers one bit per hostile interaction (as good as it gets in our model).
- Defeats point order and Weil pairing validations.
- There is a countermeasure by Kirkwood et al. based on the Fujisaki–Okamoto transform. It has 100% overhead.

Previous work [KPLT14]:

- Solved the supersingular isogeny problem in the quaternion case.
- Found an isogeny of degree ℓ^e, but $e \sim \frac{7}{2}\log_\ell p$.
- Need an isogeny of degree ℓ^e, where $e \sim \frac{1}{2}\log_\ell p$.
- Not enough to solve the special supersingular isogeny problem.

Our work:

- Construct ideal of arbitrary norm using methods from above.
- Arbitrary ideal has dimension 4.
- Use lattice methods to find Minkowski reduced basis.
- Hope to find/construct an element with a suitable norm from reduced basis.

Implications:

- Our algorithm allows us to recover Alice's isogeny given the endomorphism rings involved.
- We have shown that the Jao–De Feo cryptosystem is at most as difficult as computing the endomorphism ring.
- Still remains a hard problem.

Definition (Isogeny hidden number problem)

Given all the public parameters of the SIDH key exchange, and some partial information of the shared secret, compute the shared secret.

- We solved this problem for when the partial information is one component of the j-invariant.
- Computing one component of the j-invariant is as hard as computing the entire j-invariant.
- Therefore the two parties can compress (without loss of security) the shared secret into just one component of the j-invariant.

Conclusion

- Shown an adaptive attack that recovers secret isogeny.
  - Lemma to normalise secret key.
  - Static keys are prone to this attack.
- Shown that Jao–De Feo cryptosystem is at most as hard as computing endomorphism ring.
  - Uses equivalence of categories.
  - Perform computations on maximal orders of quaternion.
- Shown a bit-security result.
  - Safe to truncate j-invariants into components.

Conclusion

- Shown an adaptive attack that recovers secret isogeny.
  - Lemma to normalise secret key.
  - Static keys are prone to this attack.
- Shown that Jao–De Feo cryptosystem is at most as hard as computing endomorphism ring.
  - Uses equivalence of categories.
  - Perform computations on maximal orders of quaternion.
- Shown a bit-security result.
  - Safe to truncate j-invariants into components.

THANK YOU!