On the Security of Supersingular Isogeny Cryptosystems

Steven D. Galbraith

University of Auckland

Plan

Joint work with **Christophe Petit**, **Barak Shani** and **Yan Bo Ti**.

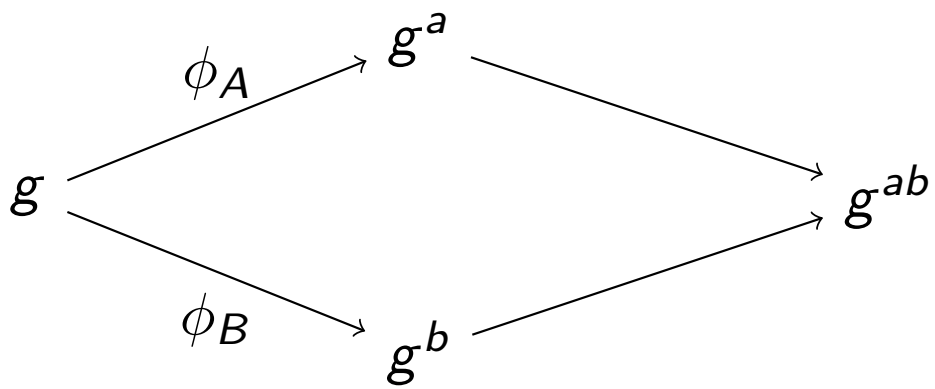
- Diffie-Hellman key exchange
- Small subgroup attacks
- Generalisations
- Isogenies
- Isogeny cryptosystems
- Adaptive attacks

Executive Summary

- These cryptosystems are not broken.
- They might be post-quantum secure.
- Lots of research still to be done.

Diffie-Hellman Key Exchange

Fix an element g in a group G.



The maps $\phi_A(x) = x^a$ and $\phi_B(x) = x^b$ are group homomorphisms.

Elgamal encryption (Static Diffie-Hellman)

- Static Diffie-Hellman key exchange is where Alice uses a fixed key $h = g^a$.
- Bob sends g^b and the shared key is g^{ab}.
- This gives Elgamal encryption:
  - Alice has public key $h = g^a$.
  - Bob sends $(c_1, c_2) = (g^b, mg^{ab})$.
  - Alice decrypts as $m = c_2 c_1^{-a}$.

Small subgroup/invalid group attack

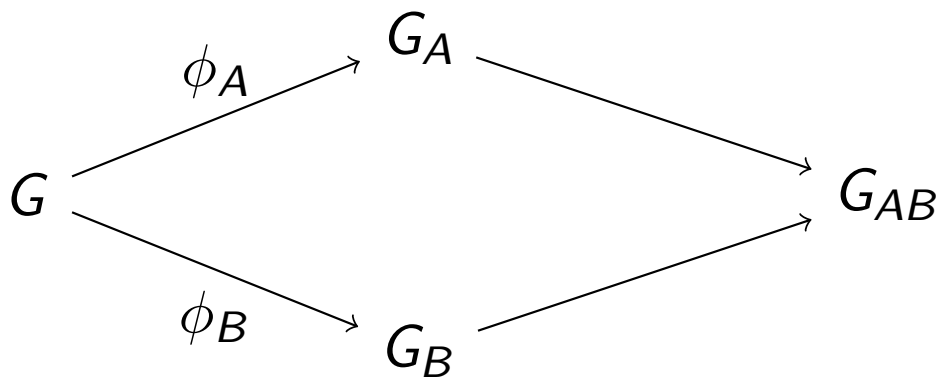
- First analysed by Lim and Lee.
- Suppose malicious Bob wants to learn Alice's long-lived secret key a.
- Bob chooses $\bar{g}$ with small order ℓ and sends $(c_1, c_2) = (\bar{g}, \bar{g}^r)$ for some random r.
- Alice computes $c_2 c_1^{-a} = \bar{g}^{r-a}$.
- Bob hopes that his future interactions with Alice allow him to learn $r - a \pmod{\ell}$ and hence $a \pmod{\ell}$.
- Repeating the attack for different ℓ and using Chinese remainder theorem allows Bob to learn a.

Validation

- Alice can prevent the attack by checking that Bob's values (c_1, c_2) lie in the correct group and have the correct order.
- This process is sometimes called "validation".
- The cost of validation depends on the groups being used.
- For small subgroups of $\mathbb{F}_p^*$ validation can be quite expensive.
- For prime order elliptic curves validation can be quite cheap.

Generalisations of Diffie-Hellman

Consider a group homorphism $\phi_A : G \to G_A$ where $G_A \cong G/\ker(\phi_A)$. Similarly, $\phi_B : G \to G_B$.



Two difficult problems to solve:

- Need to be able to "complete the square" and compute a well-defined shared secret.
- Need to represent $G_A = G/\ker(\phi_A)$ in a way that does not leak ϕ_A.

Isogenies

- Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over a field $\mathbb{F}_q$.
- If H is a finite subgroup of E then there is an elliptic curve E' and a morphism

$$\phi : E \to E'$$

  such that ϕ is a group homomorphism and $\ker(\phi) = H$.
- This is called an **isogeny** and we may denote E' as E/H.
- The isogeny can be computed in time $O(|H|)$ field operations.

Example of an isogeny

- Let $A, B \in \mathbb{F}_q$ be such that $B \neq 0$ and $D = A^2 - 4B \neq 0$.
- Define $E : y^2 = x(x^2 + Ax + B)$.
- The point $(0, 0)$ has order 2.
- Let $E' : Y^2 = X(X^2 - 2AX + D)$.
- The map

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(B - x^2)}{x^2} \right) = \left(\frac{x^2 + Ax + B}{x}, y \frac{B - x^2}{x^2} \right)$$

maps E to E' and has kernel $\langle (0, 0) \rangle = \{(0, 0), 0\}$.

Isogeny version of Diffie-Hellman

- Alexander Rostovtsev and Anton Stolbunov, ePrint 2006/145.
- Anton Stolbunov, Advances in Mathematics of Communications, 2010.
- Fix a curve E over $\mathbb{F}_q$.
- Alice and Bob choose subgroups $G_A, G_B \subseteq E(\mathbb{F}_q)$.
- Alice publishes the image curve $E_A \cong E/G_A$.
- Bob publishes $E_B \cong E/G_B$.
- If there is a way for Alice to compute $\phi_B(G_A) \subseteq E_B(\mathbb{F}_q)$ then Alice computes

$$E_B/\phi_B(G_A) \cong E/\langle G_A, G_B \rangle.$$

- Similarly, if Bob can compute $\phi_A(G_B)$ then he computes

$$E_A/\phi_A(G_B) \cong E/\langle G_A, G_B \rangle.$$

Security

- Public: E, E_A.
  Private: ϕ_A, G_A such that $\phi_A : E \to E_A = E/G_A$.
- This assumption also used by Charles, Lauter and Goren "Cryptographic hash functions from expander graphs", Jornal of Cryptology, 2009.
- Classical security: Find path in isogeny graph.
  The best general algorithm runs in time approx square-root of the size of the isogeny graph.
- Quantum algorithms:
  - Ordinary case: Sub-exponential complexity.
    Andrew M. Childs, David Jao, and Vladimir Soukharev, J. Mathematical Cryptology, 2014.
  - Supersingular case: Exponential complexity.
    De-Feo, Jao, Plût, J.Math.Crypt. 2014.
    Jean-Francois Biasse, David Jao, Anirudh Sankar, INDOCRYPT 2014.

Supersingular Elliptic Curves

- An elliptic curve E over $\mathbb{F}_{p^n}$ is supersingular if $\#E(\mathbb{F}_{p^n}) \equiv 1 \pmod{p}$.
- The endomorphism ring is non-commutative.
- All supersingular elliptic curves mod p can be defined over $\mathbb{F}_{p^2}$.
- There are approximately $p/12$ supersingular curves.

De Feo and Jao Key Exchange Scheme

- Choose prime $p = 2^n 3^m f \pm 1$, where f is small and $2^n \approx 3^m$.
- Choose a supersingular curve $E/\mathbb{F}_{p^2}$.
- Then $\#E(\mathbb{F}_{p^2}) = (2^n 3^m f)^2$ and $E[2^n], E[3^m] \subseteq E(\mathbb{F}_{p^2})$.
- Fix linearly independent points $P_A, Q_A \in E[2^n]$ and $P_B, Q_B \in E[3^m]$.

De Feo and Jao Key Exchange Scheme

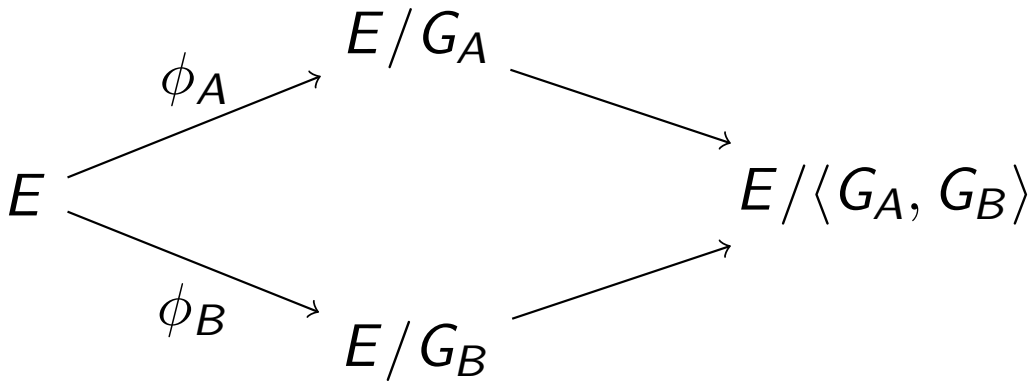
- Alice picks random integers $0 \leq a_1, a_2 < 2^n$ (not both divisible by 2) and computes
$$G_A = \langle [a_1]P_A + [a_2]Q_A \rangle.$$
- Alice now has an isogeny $\phi_A : E \to E_A$.
- Bob picks random integers $0 \leq b_1, b_2 < 3^m$ (not both divisible by 3) and computes
$$G_B = \langle [b_1]P_B + [b_2]Q_B \rangle.$$
- Bob now has an isogeny $\phi_B : E \to E_B$.

De Feo and Jao Key Exchange Scheme

- Let $E_A = \phi_A(E) = E/G_A$, and $E_B = \phi_B(E) = E/G_B$.
- Alice sends message $E_A, \phi_A(P_B), \phi_A(Q_B)$ to Bob.
- Bob sends $E_B, \phi_B(P_A), \phi_B(Q_A)$ to Alice.
- Alice can then compute $\phi_B(G_A)$, while Bob can compute $\phi_A(G_B)$.
- The shared key is $E_{AB} = E_A/\phi_A(G_B) = E_B/\phi_B(G_A)$ (up to isomorphism).
- Actually, shared key is the j-invariant $j(E_{AB})$.

De Feo and Jao Key Exchange Scheme

This can be summarised in the following diagram, where we use the notation from above.



Parameter sizes

- Recall $p = 2^n 3^m f \pm 1$.
- There is a classical attack on Alice's key that takes about $2^{n/2}$ operations.
- Similarly, there is an attack on Bob using about $3^{m/2}$ operations.
- To balance cost we take $2^n \approx 3^m$.
- For 128-bit security take $n = 256$, $m = 161$ giving $p \approx 2^{512}$.
- The classical attack therefore has complexity $O(p^{1/4})$.
- The fastest quantum attack in this specific case (De-Feo, Jao, Plût) has complexity $O(p^{1/6})$.

Implementation Details

- De Feo, Jao and Plût, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", J. Mathematical Cryptology, 2014.
- Yoshida and Takashima, "Computing a Sequence of 2-Isogenies on Supersingular Elliptic Curves" IEICE 2013.
- Azarderakhsh, Fishbein and Jao, "Efficient implementations of a quantum- resistant key-exchange protocol on embedded systems", Technical report 2014.
- Azarderakhsh, Jao, Kalach, Koziel and Leonardi, "Key Compression for Isogeny-Based Cryptosystems", AsiaPKC '16.
- Costello, Longa and Naehrig, "Efficient algorithms for supersingular isogeny Diffie–Hellman", CRYPTO 2016.

Costello-Longa-Naehrig Validation

- We now focus on attacking Alice with a static key E_A. We want to compute Alice's subgroup $G_A = \langle [a_1]P_A + [a_2]Q_A \rangle$.
- Active attacks have been expected.
- Two requirements are: that the points P, Q in the public key have full order and that they are independent.
- CLN use the Weil pairing of the two points to check independence.
- Not necessary to use the Weil pairing.
  Suffices to check $[2^{n-1}]P \neq [2^{n-1}]Q$ and neither 0.
- Weil pairing can be used to check a lot more than just independence.
  A natural validation step for Alice is

$$e_{2^n}(\phi_B(P_A), \phi_B(Q_A)) = e_{2^n}(P_A, Q_A)^{3^m}.$$

Security: Importance of correct isog

- This problem is different to general isogeny problem: special primes; auxiliary points; very strong constraint on the isogeny degree.
- Suppose an attacker given E, E_A, E_B can compute an isogeny $\phi' : E \to E_A$.
- A natural approach is to compute $\phi_B(\ker(\phi'))$, and then compute an isogeny from E_B with this kernel.
- However, the attacker only has the points $\phi_B(P_A), \phi_B(Q_A)$, so can only compute $\phi_B(\ker(\phi'))$ if $\ker(\phi') \subseteq \langle P_A, Q_A \rangle$.
- A random isogeny ϕ' is unlikely to have this property.

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 $(\alpha, 1)$.

Adaptive attack models

- We assume that Alice is using a static key $(1, \alpha)$.
- Dishonest user is playing the role of Bob.
- Model 1: $O(E, R, S) = E/\langle R + [\alpha]S \rangle$.
  This corresponds to Alice taking Bob's protocol message, completing her side of the protocol, and outputting the shared key.
- Model 2: $O(E, R, S, E')$ returns 1 if $j(E') = j(E/\langle R + [\alpha]S \rangle)$ 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 $j(E')$.
- Our main attack works with both models, so we assume the weaker Model 2.

First Step of the Attack

- To differentiate between $(1, \alpha)$ and $(\alpha', 1)$:
- Attacker honestly generates ephemeral values $(E_B, R = \phi_B(P_A), S = \phi_B(Q_A))$ and computes E_{AB}.
- Attacker sends $(E_B, R, S + [2^{n-1}]R)$ to Alice and tests the resulting j-invariant.
- Note that if $(1, \alpha)$ with α even then

$$R + [\alpha](S + [2^{n-1}]R) = R + [\alpha]S.$$

- This means that $E_B/\langle R + [\alpha]S \rangle = E_B/\langle R + [\alpha](S + [2^{n-1}]R) \rangle$.

Continuing the Attack

- Wolog assume $(a_1, a_2) = (1, \alpha)$
- Write $\alpha = K_i + 2^i \alpha_i + 2^{i+1} \alpha'$ where K_i is known but $\alpha_i \in \{0, 1\}$ and $\alpha' \in \mathbb{Z}$ are not known.
- Attacker honestly generates random $E_B, R = \phi_B(P_A), S = \phi_B(Q_A)$ and E_{AB}.
- Instead of sending (E_B, R, S) to Alice, choose suitable integers a, b, c, d and send $([a]R + [b]S,\ [c]R + [d]S)$ to Alice.

Required Conditions for Attack

- If $\alpha_i = 0$, then $\langle [a + \alpha c]R + [b + \alpha d]S \rangle = \langle R + [\alpha]S \rangle$,
- If $\alpha_i = 1$, then $\langle [a + \alpha c]R + [b + \alpha d]S \rangle \neq \langle R + [\alpha]S \rangle$,
- $[a]R + [b]S$ and $[c]R + [d]S$ both have order 2^n,
- The Weil pairing $e_{2^n}([a]R + [b]S, [c]R + [d]S)$ is equal to

$$e_{2^n}(\phi_B(P_A), \phi_B(Q_A)) = e_{2^n}(P_A, Q_A)^{\deg \phi_B} = e_{2^n}(P_A, Q_A)^{3^\ell}.$$

Solution

The following integers satisfy the first three conditions:

$$a_i = 1, \qquad b_i = -2^{n-i-1} K_i,$$
$$c_i = 0, \qquad d_i = 1 + 2^{n-i-1}.$$

To satisfy the fourth condition we need to use a scaling by θ, which is a square root of $1 + 2^{n-i-1}$ modulo 2^n.

Analysis and Complexity of the Attack

- The attack requires fewer than $n \approx \frac{1}{2}\log_2(p)$ interactions with Alice.
- This seems close to optimal for the weak attack model.
- We can reduce the number of queries by doing more computation (increasing the range of the brute-force search).
- The attack is not detected by the validation steps of Costello et al.

Kirkwood, Lackey, McVey, Motley, Solinas and Tuller validation

- General method to secure any key exchange protocol of a certain type.
- Bob chooses a random seed r_B to derive his ephemeral values in the key exchange protocol.
- Alice and Bob engage with the protocol as usual.
- On completion, they derive an additional verification key VK.
- Bob encrypts his seed using VK and sends to Alice.
- Alice decrypts to get the seed, then re-computes all Bob's ephemeral values and terminates if they do not agree.

Further results in our paper

- We show that if one can compute $\mathrm{End}(E)$ and $\mathrm{End}(E_A)$ then one can break the scheme.
- We give a method to determine the secret key from partial knowledge of the secret key.
- We formalise this problem as a variant of the "hidden number problem".
- This results can be viewed as a bit security result, or as a tool for a side channel attack.

Isogeny hidden number problem

- Let E_s be an unknown supersingular elliptic curve over $\mathbb{F}_{p^2}$.
- The *isogeny hidden number problem* is to compute the j-invariant $j(E_s)$ given an oracle $\mathcal{O}$ such that $\mathcal{O}(r)$ outputs partial information on $j(E')$ for some curve E' which is r-isogenous to E_s.

Algorithm for the Isogeny Hidden Number Problem

- Let $\mathbb{F}_{p^2} = \mathbb{F}_p(\theta)$, where $\theta^2 + A\theta + B = 0$, with $A, B \in \mathbb{F}_p$.
- We write supersingular j-invariants as $j = j_1 + j_2\theta$.
- we consider two leakage models:
  1. Oracle returns an entire component j_i of the j-invariant.
  2. Oracle returns the most significant bits of both components.
- Algorithm is based on modular polynomials $\Phi_r(x, y)$.
  There is an isogeny $\phi : E \to E'$ of degree r with cyclic kernel if and only if $\Phi_r(j(E), j(E')) = 0$.

Theorem

- Let oracle $\mathcal{O}$ in the isogeny hidden number problem output one component of the finite field representation of $j(E') \in \mathbb{F}_{p^2}$.
- Then there is an algorithm to solve the isogeny hidden number problem that makes two queries to $\mathcal{O}$ and succeeds with probability at least $1/18$.
- Proof: Call oracle $\mathcal{O}(1)$ and $\mathcal{O}(2)$, do Weil descent, get two polynomial equations in 2 variables, take resultants, compute roots.

Open Questions

- Classically secure?
- Quantumly secure?
- Side-channel attacks?
- Fault attacks?
- Security analysis of the Kirkwood et al validation.

Thank you for your attention.