Improved Torsion-Point Attacks On SIDH Variants

Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, Katherine E. Stange

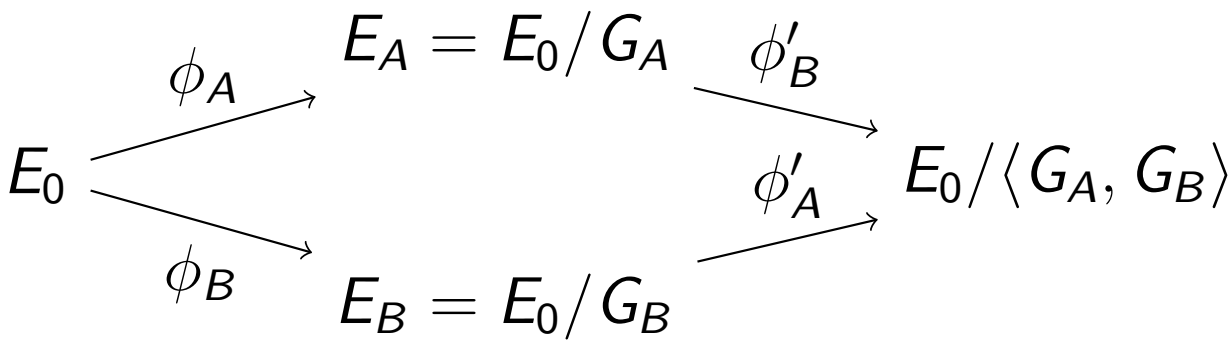
August 9, 2021

Isogeny-based cryptography

- Based on the hard problem of finding isogenies between supersingular elliptic curves.
- Can be interpreted as a path-finding problem in certain expander graphs.
- Best known algorithms for finding a degree-d isogeny between two curves have time complexity $O(\sqrt{d})$.
- Van Oorschot–Wiener gives a time-memory tradeoff.
- Most cryptosystems (most prominently SIDH) are based on a relaxation of this problem.
- Question: Can one exploit the extra information?

Supersingular Isogeny Diffie–Hellman (SIDH)

- Choose a prime p, and $A, B \in \mathbb{N}$ with $\gcd(A, B) = 1$
  Choose E_0 a supersingular curve over $\mathbb{F}_{p^2}$
- Let $E_0[A] = \langle P_A, Q_A \rangle$ and $E_0[B] = \langle P_B, Q_B \rangle$
- Alice picks a cyclic subgroup $G_A \subset E_0[A]$ defining an isogeny $\phi_A : E_0 \to E_A = E_0/G_A$ and she sends E_A to Bob
- Bob picks a cyclic subgroup $G_B \subset E_0[B]$ defining an isogeny $\phi_B : E_0 \to E_B = E_0/G_B$ and he sends E_B to Alice



- Shared key is $E_0/\langle G_A, G_B \rangle$
- To compute the shared key, Alice sends over $\phi_A(P_B), \phi_A(Q_B)$ and Bob sends over $\phi_B(P_A), \phi_B(Q_A)$.

Isogeny problem with torsion information

This motivates the study of the following algorithmic problem:

Problem (SSI-T)

Let ϕ be a secret isogeny of known degree A between supersingular elliptic curves E_0 and E_A as above. Suppose given $\phi(P_B)$ and $\phi(Q_B)$. Compute ϕ.

- Goal: Give conditions on the relationship between A, B, p for which we can solve this problem in polynomial time (or at least improve on generic meet-in-the-middle)
- Generalization of the previously defined CSSI problem.

Remarks on the SSI-T problem

- $E_0[B]$ should be efficiently representable
- SIDH uses A, B which divide $p + 1$
- BSIDH uses A, B which divide $p^2 - 1$
- SIDH and BSIDH use balanced parameters (i.e., $A \approx B$), but that does not provide any efficiency benefit

Petit's attack '17

- Find a special endomorphism θ of E_0 and an integer d such that $\tau = \phi \circ \theta \circ \hat{\phi} + [d]$ can be recovered from its restriction to $E_A[B]$.
- Computing $ker(\tau - d) \cap E_A[A]$ then yields $\hat{\phi}$.
- How to recover τ?
  - Choose θ such that $\deg(\tau)$ is Be where e is small
  - Using torsion-point images we can recover the B part and use meet-in-the-middle to get the e part
  - Question: How to find a suitable θ?

A diophantine equation

- In most applications the special starting curve $E : y^2 = x^3 + x$ is used
- $\mathrm{End}(E)$ contains a subring $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij$ where $i^2 = -1,\ j^2 = -p,\ ij = -ji$
- Finding a suitable θ is equivalent to solving

$$A^2(a^2p + b^2p + c^2) + d^2 = Be$$

- Method for solving the equation: Solve modulo A^2 to get d, then solve modulo p to get a, b, c
- This works roughly when $B > p^2A^2$

Improvements

- Let $\deg(\tau) = B^2 e$. Then $\tau = \psi_1 \circ \eta \circ \hat{\psi}_2 \circ [m]$ where $\deg(\psi_1) = \deg(\psi_2) = B/m$, $\deg(\eta) = e$ and $m \mid 2$
- We can represent τ modulo B as a matrix in $M_2(\mathbb{Z}/B\mathbb{Z})$. The kernel of this matrix is the kernel of ψ_1, the image of this matrix is the kernel of ψ_2
- Alternative: Run Petit's attack with θ and then with $\hat{\theta}$
- Corollary: Finding θ such that $\deg(\phi \circ \theta \circ \hat{\phi} + [d]) = B^2 e$ allows retrieving ϕ (reduction between problems)
- For $y^2 = x^3 + x$ this gives the diophantine equation

$$A^2(a^2 p + b^2 p + c^2) + d^2 = B^2 e$$

- We can solve this when $B > pA$, but solutions should exist for a wider variety of parameters

Improvements II

- Let $\deg(\tau) = B^2pe$. Run the same attack as before; the degree-p part is just a Frobenius isogeny
- Main idea: retrieve isogenies between two curves when one is close to the other's *conjugate*
- This leads to the following equation:

$$A^2(a^2p + b^2p + c^2) + d^2 = B^2pe$$

- Choosing c, d divisible by p leads to the equation

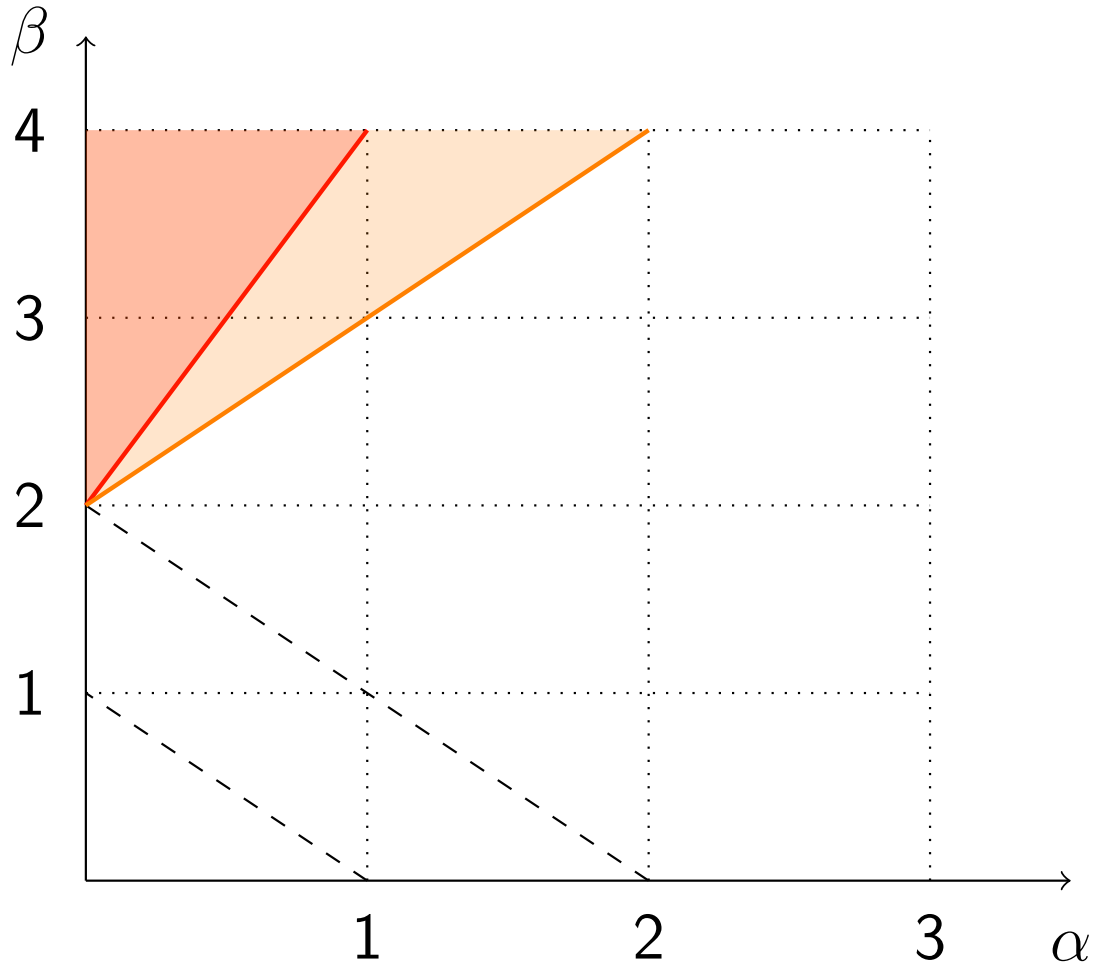
$$A^2(a^2 + b^2 + pc^2) + pd^2 = B^2e$$

- Set $c = 0$, solve modulo A^2, and hope to get a sum of two squares
- This leads to a solution roughly whenever $B > \sqrt{p}A^2$ (modulo technical details)

Exponential-time attacks

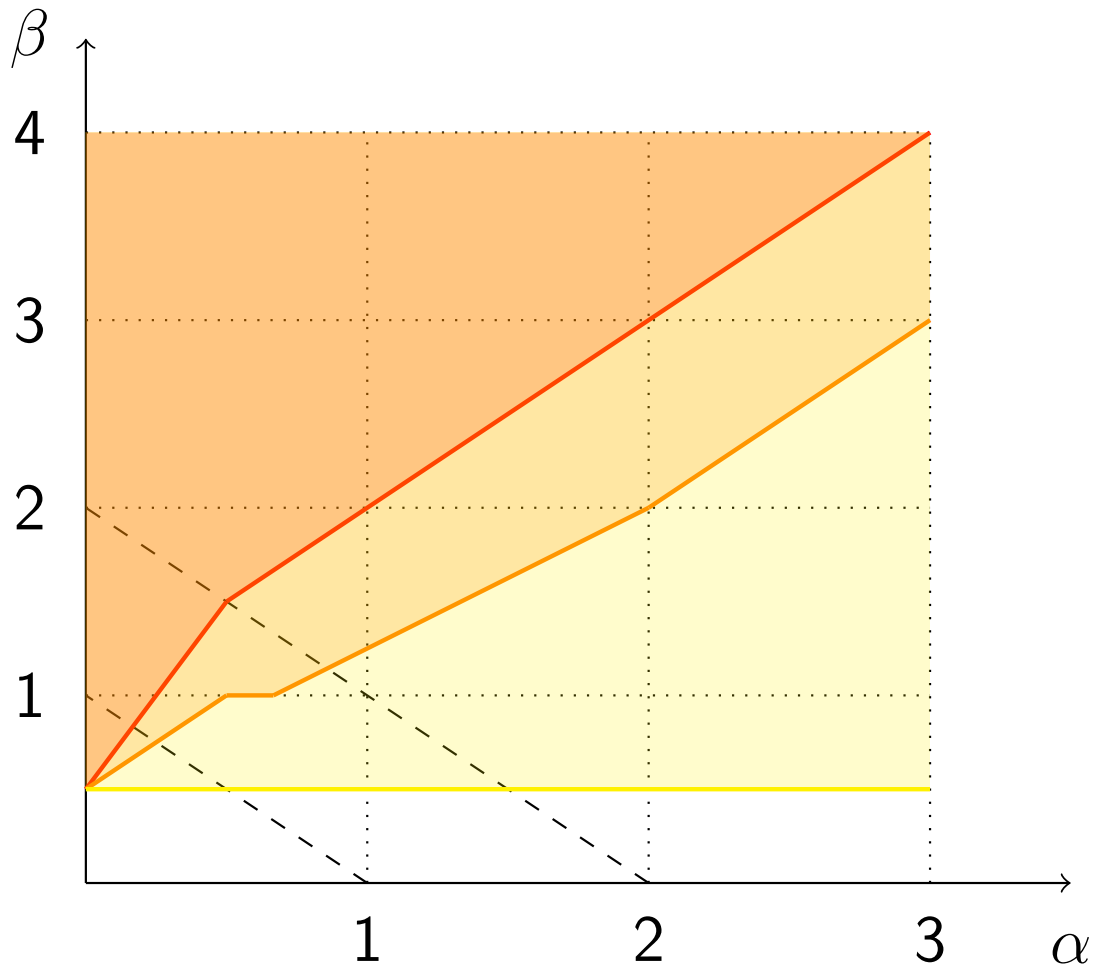
- All previous attacks were focusing on polynomial-time attacks
- One can look at versions where the attack is exponential-time but faster than generic pathfinding
- One can set e to be larger and then the cost of the attack is the cost of finding a degree-e isogeny
- One can also simply guess part of the secret isogeny and run the torsion-point attack (if the attack fails, guess a different isogeny)
- The cost of guessing a degree-d isogeny is a factor $O(d)$

Petit 2017



- $A = p^{\alpha}$, $B = p^{\beta}$
- red: polynomial-time attack
- orange: better than generic attack

Our work



- yellow: better than known quantum attacks

Highlights

- Polynomial-time key recovery when $B > A^5$ and $p \approx AB$ (SIDH-like parameters)
- Polynomial-time key recovery when $B > A^2$ and $p^2 \approx AB$ (BSIDH-like parameters)
- Improved quantum attack when $B > A^2$ and $p \approx AB$

Backdoor attacks I

- Question: Can one specifically design starting curves for which one can solve SSI-T in polynomial time/faster than generic algorithms?
- For $B > A^2$, we construct special starting curves from which one can solve SSI-T in polynomial time (note that this condition is independent of p)
- Key idea: instead of looking for a curve E and then an endomorphism θ, look for the pair together
- $A^2(pa^2 + pb^2 + c^2) + d^2 = B^2$, enough to find integer d and rational a, b, c such that $pa^2 + pb^2 + c^2$ is an integer
- The norm of the θ will be $D = pa^2 + pb^2 + c^2$ and the trace will be zero

Backdoor attacks II

- First solve modulo A^2 (which leads to the $B > A^2$ condition); then need a rational solution to $pa^2 + pb^2 + c^2 = B^2 - d^2$ where d, e are already fixed
- Find a maximal order containing $\mathbb{Z}[\sqrt{-D}]$ and translate it to a supersingular elliptic curve
- (A, B)-backdoor curves have an endomorphism ring which contains a copy of $\mathbb{Z}[\sqrt{-D}]$
- The number of backdoor curves is exponential in $\log(p)$ and they seem hard to distinguish from a random curve
- Using our exponential-time attacks, we construct backdoor curves for balanced parameters $A \approx B$ from which one can beat existing attacks
- We also discuss backdoored parameters A, B and backdoored base-field primes p

Conclusion

- Significant improvement to previous attacks, most prominently our attack when $B > A^5$ and $p \approx AB$
- Introduction of the concept of backdoored curves (which besides leading to attacks can be used constructively)
- Benchmark for SIDH and BSIDH-like parameter choices
- Do not trust starting curves coming from shady sources