Breaking SIDH in polynomial time

DAMIEN ROBERT

Abstract. We show that we can break SIDH in polynomial time, even with a random starting curve E_0.

1. Introduction

We extend the recent attacks by [CD22; MM22] and prove that there exists a proven polynomial time attack on SIDH, even with a random starting curve E_0.

Theorem 1.1. *We suppose that we are given the following input: we are given a secret N_B-isogeny over a finite field $\phi_B : E_0 \to E_B$ along with its images on (a basis of) the N_A-torsion points of E_0, where N_A and N_B are smooth coprime integers. Let $\mathbb{F}_q$ be the smallest field such that ϕ_B, and the points of $E_0[N_A N_B]$ are defined*[1]*. Then we can recover ϕ_B in time $\widetilde{O}(\ell_A^8 \log q + \ell_B^2 \log^2 q)$ operations where ℓ_A is the largest prime divisor of N_A and ℓ_B the largest of N_B.*

2. Proof

We suppose here that $N_A > N_B$. Otherwise, in the context of SIDH we would attack ϕ_A. Another solution would be to guess the image of the eN_A-torsion under ϕ_B for the smallest e such that $eN_A > N_B$. Write $N_A = bN_B + a$ for positive integers $a, b > 0$. Since N_A is prime to N_B, the gcds $(N_A, a) = (N_A, b) = (N_A, a, b) := d$, so we get a relation $N_A/d = (b/d)N_B + (a/d)$. Since we know the image of the N_A/d torsion, henceforth, we will assume $d = 1$.

Let α be an endomorphism on E_0^4 given by a matrix $M \in M_4(\mathbb{Z})$ such that α is an a-isogeny, ie $\hat{\alpha}\alpha = a \operatorname{Id}$ where $\hat{\alpha}$ is the dual of α and is simply given by the transpose of M (since integer multiplications are their own dual). Explicitly we write $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$ and take M the matrix of the multiplication of $a_1 + a_2 i + a_3 j + a_4 k$ in the standard quaternion algebra. Likewise we let β be an endomorphism of E_B^4 which is a b-isogeny.

Let $F = \begin{pmatrix} \alpha & \beta\phi_B \\ -\hat{\beta}\hat{\phi_B} & \hat{\alpha} \end{pmatrix}$, where $\hat{\phi_B}$ is the dual isogeny $E_B \to E_0$ of ϕ_B. Since N_A is prime to N_B, we know how $\hat{\phi_B}$ acts on $E_B[N_A]$. Then the dual $\hat{F}$ of F is given by $\hat{F} = \begin{pmatrix} \hat{\alpha} & -\beta\phi_B \\ \hat{\beta}\hat{\phi_B} & \alpha \end{pmatrix}$, and we compute $\hat{F}F = F\hat{F} = \begin{pmatrix} bN_B + a & 0 \\ 0 & bN_B + a \end{pmatrix} = N_A \operatorname{Id}$. Hence F is an N_A-isogeny on $E_0^4 \times E_B^4$ and we can compute its action on the N_A-torsion. It is easy to compute its kernel: using pairings and discrete logarithms in μ_{N_A} (which is easy since N_A is smooth: they cost $O(\sqrt{\ell_A})$) we reduce to linear algebra over $\mathbb{Z}/N_A\mathbb{Z}$. The cost of this step will be dominated by the following isogeny computation.

We can then compute F using an isogeny algorithm in dimension 8. If ℓ is the largest prime divisor of N_A, the complexity will be dominated by $\widetilde{O}(\ell^8)$ operations over $\mathbb{F}_q$ using [LR22].

Given F, we recover $\beta\phi_B$, hence $b\phi_B$ on E_0 (more precisely we recover its kernel via two evaluations of F on a basis of $E_0[N_B]$ suitably embedded into $E_0^4 \times E_B^4$). If b is prime to N_B we directly recover ϕ_B. Otherwise, we only recover $e\phi_B$ where $e = (b, N_B)$ and we have to do a bit of backtracking to recover $\frac{e}{\ell}\phi_B$ on E_0 for ℓ a prime divisor of e and so on until we recover ϕ_B. This involve working over an extension where the points of $E_0[\ell N_B]$ torsion are defined.

Date: August 11, 2022.

[1] We make no further assumptions on E_0 and E_B: we do not require them to be supersingular. In the context of SIDH, k will be the base field $\mathbb{F}_{p^2}$.

More precisely, since $E_0[N_B]$ is defined over $\mathbb{F}_q$ by assumption and $\ell \mid N_B$, this extension is of degree $O(\ell)$ (in fact unless $E_0[N_B]$ is already rational, $E_0[\ell N_B]$ is defined over an extension of degree exactly ℓ). We can compute a basis of $E_0[\ell N_B]$ in time $\widetilde{O}(\ell^2 \log^2 q)$ using [BCR11] (a summary is in [Rob21, §5.6.1]). This is assuming we already know the zeta function of E_0, otherwise we need to compute it in $\widetilde{O}(\log^4 q)$ using the SEA algorithm. We can evaluate $e\phi_B$ on this basis, hence recover the kernel of $\frac{e}{\ell}\phi_B \subset E_0[N_B \frac{\ell}{e}]$.

References

[BCR11] G. Bisson, R. Cosset **and** D. Robert. **?**On the Practical Computation of Isogenies of Jacobian Surfaces**?** 2011. URL: https://www.math.u-bordeaux.fr/~damienrobert/avisogenies/. In preparation.

[CD22] W. Castryck **and** T. Decru. *An efficient key recovery attack on SIDH (preliminary version)*. Cryptology ePrint Archive, Paper 2022/975. https://eprint.iacr.org/2022/975. 2022. URL: https://eprint.iacr.org/2022/975.

[LR22] D. Lubicz **and** D. Robert. **?**Fast change of level and applications to isogenies**?** Accepted for publication at ANTS XV Conference — Proceedings. **august** 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/change_level.pdf.

[MM22] L. Maino **and** C. Martindale. *An attack on SIDH with arbitrary starting curve*. Cryptology ePrint Archive, Paper 2022/1026. https://eprint.iacr.org/2022/1026. 2022. URL: https://eprint.iacr.org/2022/1026.

[Rob21] D. Robert. **?**HDR: Efficient algorithms for abelian varieties and their moduli spaces**?** phdthesis. Université Bordeaux, **june** 2021. URL: http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf. Slides: 2021-06-HDR-Bordeaux.pdf (1h, Bordeaux).

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE
Email address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/

Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex FRANCE