# Evaluating isogenies in polylogarithmic time

DAMIEN ROBERT

Abstract. Let $f : E \to E'$ be an $N$-isogeny between elliptic curves (or abelian varieties) over a finite field $\mathbb{F}_q$. We show that there always exist an efficient representation of $f$ that takes polylogarithmic $O(\log^{O(1)} N \log q)$ space and which can evaluate $f$ at any point $P \in E(\mathbb{F}_{q^k})$ in polylogarithmic $O(\log^{O(1)} N)$ arithmetic operations in $\mathbb{F}_{q^k}$.

Furthermore, this efficient representation can be computed by evaluating $f$ on $O(\log N)$ points defined over extensions of degree $O(\log N)$ over $\mathbb{F}_q$. In particular, if $f$ is represented by the equation $H(x) = 0$ of its kernel $K$, then using Vélu's formula the efficient representation can be computed in time $\widetilde{O}(N \log q + \log^2 q)$.

## 1. Introduction

Let $f : E \to E'$ be an $N$-isogeny between elliptic curves, and $K = \operatorname{Ker} f$ its kernel. In the following, we will always assume that $N$ is prime to the characteristic $p$, so our isogenies are separable.

It is well known that the isogeny given by the multiplications $[n]$ by an integer is efficiently evaluable by the double and add algorithm. A natural question is whether a more general isogeny like $f$ can be efficiently evaluated too.

If $N$ is $B$-smooth, then $f$ can be decomposed into a product of $\ell_i$-isogenies $f_i : E_i \to E_{i+1}$, $\ell_i \leq B$. Given this decomposition, the image by $f$ of any point $P \in E(\mathbb{F}_{q^k})$ can then be computed in $O(B \log N)$ arithmetic operations over $\mathbb{F}_{q^k}$.

Furthermore, if $f$ is cyclic and we are given a generator $P$ of $K$, the isogenies $f_i$ and a generator $P_i$ of their kernel $K_i$ can be computed in time $O(\log N(\log N + B))$ using the standard naive algorithm combined with Vélu's formula [Vél71].

**Remark 1.1.**

- Given a generator $P$, this decomposition of $f$ can be optimised by first replacing Vélu's algorithm by the `sqrtVelu` algorithm described in [BDL+20], and secondly by using the optimised decomposition method described in [DJP14, § 4.2.2]. Furthermore, the image of a point can be computed in $\widetilde{O}(\sqrt{B} \log N)$ arithmetic operations over $\mathbb{F}_{q^k}$ using `sqrtVelu`.
- When only given the equation $H(x) = 0$ of the kernel, we can compute the decomposition by treating the point $x \mod H$ as a formal generator, but we cannot hope to compute the decomposition in polylog time (in $N$) since the input is already in $O(N \log q)$. The naive decomposition algorithm in the extension given by $H$ costs $O(N(\log^2 N + B \log N))$ operations in $\mathbb{F}_q$.

*Date*: August 25, 2022.

When $N$ is not smooth, in particular when it is prime, the isogeny $f$ cannot be decomposed as a product of smaller isogenies, so it is not clear that there exists a way to encode $f$ such that it can be evaluated in polylogarithmic time on any point.

As far as I know, when $K$ is given by a generator, the best algorithm is `sqrtVelu`which takes $\widetilde{O}(\sqrt{N})$ arithmetic operations, and when $K$ is given by the equation $H(x) = 0$ of its kernel, the best algorithm is Vélu's formula which takes $O(N)$ arithmetic operations. Indeed, in general a generator of $K$ will live in an extension of degree $\Omega(N)$, so `sqrtVelu`will be slower than Vélu. An alternative, when $\mathrm{End}(E)$ is known, would be to find an ideal representing $f$ and then compute an equivalent ideal of smaller norm, but we do not want to assume $\mathrm{End}(E)$ known here.

The key fact is that if $m$ is any positive integer, we can always embed $f$ into an $N + m$-isogeny $F$ in dimension 8. We recall this construction in Sections 2 and 3, see Lemma 3.2. In particular, the evaluation $f(P)$ can be directly recovered from the evaluation of $F$ on (a suitable embedding of) $P$. Thus, choosing $m$ such that $N' := N + m$ is smooth, we can alway embed $f$ into a smooth isogeny, at the cost of going up in dimension.

This powerful algorithmic tool has been used to devastating effect to break SIDH [CD22; MM22; Rob22]. The purpose of this article is to show that it also allows for interesting constructive algorithmic applications.

We warn that this paper is mostly theoretical: to represent $F$ we need to compute $f$ on (a basis of) $E[N']$. Choosing $N'$ to be power smooth and not just smooth, we can instead compute $f$ on a basis of $E[\ell_i^{e_i}]$ for each prime power dividing $N'$. This requires to evaluate $f$ (using a standard algorithm like Vélu or `sqrtVelu`) on $O(\log N)$ points which live in an extension of degree $O(B^2)$ where $B$ is the powersmooth bound of $N'$. It follows that representing $f$ by $F$ is interesting only if we need to compute it on many more points (or a point of large degree).

In Section 5, taking $B = O(\log N)$, we obtain

**Theorem 1.2.** *An $N$-isogeny $f$ between elliptic curves over a finite field represented by the equation $H(x) = 0$ of its kernel $K$ admits an efficient representation taking $O(\log^3 N \log q)$ bits to encode, and which can evaluate points in $\widetilde{O}(\log^{11} N)$ arithmetic operations over their fields of definition. Furthermore, this efficient representation can be computed in time $\widetilde{O}(N \log q + \log^2 q)$.*

*If we are given a rational generator of the kernel $K$, then the efficient representation can be computed in time $\widetilde{O}(\sqrt{N} \log q + \log^2 q)$.*

Some optimisations are described in Section 6.

We remark that in the particular case that $E(\mathbb{F}_q)$ already contains the full $N'$-torsion for a smooth $N'$, then for any rational $N$-isogeny $f$ with $N < N'$, the efficient representation $F$ can be computed from only two calls of $f$ and a basis of $E[N'](\mathbb{F}_q)$. With this version, we obtain:

**Theorem 1.3.** *Given a basis $(P, Q)$ of $E(\mathbb{F}_q)[N']$ where $N'$ is $B$-smooth, an $N'$-isogeny $f$ between elliptic curves over a finite field with $N < N'$ admits an efficient representation taking $O(\log N \log q)$ bits to encode, and which can evaluate points in $O(B^8 \log B \log N)$ arithmetic operations over their fields of definition. Furthermore, this efficient representation can be computed in $\widetilde{O}(\sqrt{N} + B^8 \log^2 N)$ arithmetic operations in $\mathbb{F}_q$.*

For simplicity we deal with the case of elliptic curves in this paper, the extension to an abelian variety $A/\mathbb{F}_q$ of dimension $g$ is immediate: we can encode a $N$-isogeny-$f$ by an

$N'$-isogeny $F$ of dimension $8g$ which is determined from the image by $f$ of $O(\log N)$ points which live in an extension of degree $O(B^{2g})$.

## 2. Isogeny diamonds

If $f : (A, \lambda_A) \to (B, \lambda_B)$ is an isogeny between principally polarised abelian varieties, we let $\hat{f} : \hat{A} \to \hat{B}$ be the dual isogeny, and define $\tilde{f} : B \to A = \lambda_A^{-1} \hat{f} \lambda_B$ to be the dual isogeny with respect to the principal polarisations. An $N$-isogeny is an isogeny such that $\tilde{f} f = N$.

We recall the following notion from [Kan97, § 2]:

**Definition 2.1.** A $(d_1, d_2)$-isogeny diamond is a decomposition of a $d_1 d_2$-isogeny $f : A \to B$ between principally polarised abelian varieties into two different decompositions $f = f_1' \circ f_1 = f_2' \circ f_2$ where $f_1$ is a $d_1$-isogeny and $f_2$ is a $d_2$-isogeny. (Then $f_1'$ will be a $d_2$-isogeny and $f_2'$ a $d_1$-isogeny.) This decomposition is said to be minimal if $\operatorname{Ker} f_1 \cap \operatorname{Ker} f_2 = \{0\}$ (this is equivalent to the fact that $f_1$ and $f_2$ do not factorize through a common isogeny), and it is said to be orthogonal if $d_1$ is prime to $d_2$ (in which case it is automatically minimal).

$$\begin{tikzcd}
A \arrow[r, "f_1"] \arrow[d, "f_2"] & A_1 \arrow[d, "f_1'"] \\
A_2 \arrow[r, "f_2'"] & B
\end{tikzcd}$$

**Remark 2.2.** If $f$ is a $(d_1 d_2)$-isogeny with $d_1$ prime to $d_2$, then there is an orthogonal $(d_1, d_2)$-isogeny diamond where $\operatorname{Ker} f_1 = \operatorname{Ker} f[d_1]$ and $\operatorname{Ker} f_2 = \operatorname{Ker} f[d_2]$. (These are maximal isotropic since $d_1$ is prime to $d_2$).

**Lemma 2.3** (Kani). *Let $f = f_1' \circ f_1 = f_2' \circ f_2$ be a $(d_1, d_2)$-isogeny diamond as above. Then $F = \begin{pmatrix} f_1 & -\widetilde{f_1'} \\ f_2 & \widetilde{f_2'} \end{pmatrix}$ is a $d$-isogeny $A \times B \to A_1 \times A_2$ where $d = d_1 + d_2$. Furthermore, if $f$ is minimal,* $\operatorname{Ker} F = \{(\tilde{f}_1, -f_1'x), x \in A_1[d]\}$, *and if $f$ is an orthogonal isogeny diamond, then* $\operatorname{Ker} F = \{(d_1 x, -f x), x \in A[d]\}$.

*Proof.* For the product polarisations, the dual isogeny $\tilde{F}$ is given by $\tilde{F} = \begin{pmatrix} \widetilde{f_1} & \widetilde{f_2} \\ -f_1' & f_2' \end{pmatrix}$ and we directly check that $\tilde{F} F = (d_1 + d_2)$ Id. Furthermore, $\operatorname{Ker} F$ is the image of $\tilde{F}$ on $A \times B[d]$, and if $d_1$ is prime to $d_2$ this is also the image of $\tilde{F}$ on $A[d] \times \{0\}$, so $\operatorname{Ker} f = \{(\tilde{f}_1 x, -f_1' x), x \in A[d]\} = \{(d_1 x, -f x), x \in A[d]\}$. □

**Remark 2.4.**

- We can also use the matrix $F = \begin{pmatrix} f_1 & \widetilde{f_1'} \\ -f_2 & \widetilde{f_2'} \end{pmatrix}$, whose kernel, in the case of an orthogonal isogeny diamond, is $\operatorname{Ker} F = \{(d_1 x, f x), x \in A[d]\}$.
- Conversely, given $F = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$ a $d$-isogeny, with $x$ a $d_1$-isogeny, $z$ a $d_2$-isogeny, $y$ a $d_2'$-isogeny and $t$ a $d_1'$ isogeny, the equation $\tilde{F} F = d$ shows that $d_1 = d_1'$, $d_2 = d_2'$ and if $f_1 = x, f_1' = \tilde{y}, f_2 = -z, f_2' = \tilde{t}$, then $f_1' f_1 = f_2' f_2$ so $F$ comes from a $(d_1, d_2)$-isogeny diamond. We refer to [Kan97, § 2] for more details (Kani deals with elliptic curve, but the proofs hold for general abelian varieties).

## 3. Embedding an isogeny

Given $f : E \to E'$ a $N$-isogeny between elliptic curves, and an integer $m$, if we can find a $m$-isogeny $\alpha' : E' \to E''$ with $m$ prime to $N$, then the isogeny $F$ from Lemma 2.3 is a $N + m$-isogeny between abelian surfaces from which we can recover $f$. Taking duals when needed, this also works if we can find a $m$-isogeny $\alpha : E \to E''$.

For our applications, we want $\alpha$ or $\alpha'$ to be efficiently computable, so unless there exist an efficiently computable $m$-endomorphism on $E$ or $E'$, this restricts $m$ to be smooth.

But if $m = m_1^2 + m_2^2$, then the endomorphism $\alpha = \begin{pmatrix} m_1 & m_2 \\ -m_2 & m_1 \end{pmatrix}$ is always an $m$-isogeny on $E^2$ and $E'^2$, which furthermore can be computed in $O(\log m)$ arithmetic operations on $E$. We can then apply Lemma 2.3 to $\alpha$ and $f\,\mathrm{Id}$ to get an $(N + m)$-endomorphism $F = \begin{pmatrix} \alpha & -\tilde{f} \\ f & \tilde{\alpha} \end{pmatrix} : E^2 \times E'^2 \to E^2 \times E'^2$.

Finally, we can always find $m = m_1^2 + m_2^2 + m_3^2 + m_4^2$, then the endomorphism $\alpha = \begin{pmatrix} m_1 & -m_2 & -m_3 & -m_4 \\ m_2 & m_1 & m_4 & -m_3 \\ m_3 & -m_4 & m_1 & m_2 \\ m_4 & m_3 & -m_2 & m_1 \end{pmatrix}$ is an $m$-isogeny on $E^4$, and then $F = \begin{pmatrix} \alpha & -\tilde{f} \\ f & \tilde{\alpha} \end{pmatrix}$ an $(N + m)$-endomorphism on $E^4 \times E'^4$.

Furthermore, if we let $u = \gcd(m_1, m_2, m_3, m_4)$, then if $u$ is prime to $N$, then $\tilde{F}$ is injective on $E^4[N]$. Since $\operatorname{Ker} F$ is given by the image of $\tilde{F}$ on $E^4 \times E'^4[N]$ and is of degree $N^4$, we see that in this case $\operatorname{Ker} F = \{(\tilde{\alpha}x, -f(x)) \mid x \in E^4[N]\}$.

**Remark 3.1.** In the case $u$ prime to $N$, variants for $F$ are given by the kernels: $\{(\tilde{\alpha}x, f(x)) \mid x \in E^4[N]\}$, $\{(\alpha x, -f(x)) \mid x \in E^4[N]\}$ $\{(\alpha x, f(x)) \mid x \in E^4[N]\}$.

Since the same method works for abelian varieties, we have proved the fundamental lemma:

**Lemma 3.2.** *If $f : (A, \lambda_A) \to (B, \lambda_B)$ is an $N$-isogeny between principally polarised abelian varieties, it can be efficiently embedded to an $N'$-endomorphism on $A^4 \times B^4$ for any $N' > N$.*

## 4. Decomposing smooth isogenies

Let $f : (A, \lambda_A) \to (B, \lambda_B)$ be a smooth $N$-isogeny between principally polarised abelian varieties. Here a smooth isogeny means that $N$ is smooth, and we let $B$ be a smoothness bound for $N$.

We study several strategies to decompose $f$ into a product of $\ell_i$-isogenies, $\ell_i \leq B$.

## 5. The algorithm

If necessary, decomposing $f$ along small power divisors of $N$, we may assume that $N$ has no small power divisors.

We fix a $m$ such that $N' = N + m$ is $B$-powersmooth and $m$ is prime to $N$. For instance, if $p_1 < p_2 \ldots$ is a list of distinct primes (prime to $N$), we can take for $N'$ to be the least product $\prod_{i=1}^{j} p_i$ which is larger than $N$. Taking the list of all primes, a standard computation shows that $N'$ is $O(\log N)$ powersmooth.

Let $\alpha$ be the $m$-endomorphism on $E^4$ from Section 3, and $F = \begin{pmatrix} \alpha & -\tilde{f} \\ f & \tilde{\alpha} \end{pmatrix}$ be the 8-dimensional $N'$-endomorphism constructed in Section 3.

We can decompose $F$ as a composition of $\ell_i^{e_i}$-isogenies, $\ell_i^{e_i} \leq B$ as follow. For each prime power factor $\ell_i^{e_i}$, compute a basis of $(P_i, Q_i)$ of $E[\ell_i^{e_i}]$. This requires computing the degree $O(\ell_i^{2e_i})$ division polynomial $\Psi_{\ell_i^{e_i}}$ which can be done in quasi-linear time using the recurrence formula, then to factorize it in time $\widetilde{O}(\ell_i^{3e_i} \log q + \ell_i^{2e_i} \log^2 q)$ over $\mathbb{F}_q$ using [KU11]. The points $P_i, Q_i$ will live in an extension of degree $k_i = O(\ell_i^{2e_i})$ (a more refined bound is $k_i = O(\ell_i^{e_i+1})$, see Lemma 6.1). To check that they form a basis we need to check that the Weil pairing $e_{W,\ell_i^{2e_i}}(P_i, Q_i)$ is of primitive order $\ell_i^{e_i}$, which takes $O(e_i \log(\ell_i))$ operations in this extension. Thus finding these points take $\widetilde{O}(\log N (B^3 \log q + B^2 \log^2 q))$, and they each live in an extension of degree $O(B^2)$ of $\mathbb{F}_q$.

We first let $F_1$ be the isogeny with the kernel generated by the 8-elements $(\alpha(P_1, 0, 0, 0),$ $(-f P_1, 0, 0, 0)), (\alpha(Q_1, 0, 0, 0), (-f Q_1, 0, 0, 0)), (\alpha(0, P_1, 0, 0), (0, -f P_1, 0, 0, 0)), (\alpha(0, Q_1, 0, 0),$ $(0, -f Q_1, 0, 0, 0)), \dots$ To simplify notations, we also let $P_{i,1} = (P_i, 0, 0, 0), P_{i,2} = (0, P_i, 0, 0)$ and so on. We compute the images of the $P_{i,j}, Q_{i,j}$ for $i > 1$ and $j \in \{1, 2, 3, 4\}$ by $F_1$, since $F_1$ is rational these points will live in an extension of degree $k_i$. This requires $O(\log N)$-calls to an $\ell_1^{e_1}$-isogeny algorithm in dimension 8. Using [LR22], each isogeny will cost $O(\ell_1^{8e_1} \log \ell)$ operations in the joint field where $P_1, Q_1, P_i, Q_i$ lives, which is of degree at most $k_1 k_i$.

We now let $F_2$ be the isogeny with kernel generated by the $F_1(P_{2,1}), F_1(Q_{2,1}), F_1(P_{2,2}),$ $F_2(P_{2,2}), \dots$and so on. In the end, we have decomposed $F = F_u \dots \circ F_2 \circ F_1$ where $u \leq \log_2 N'$ and $F_i$ is a $\ell_i^{e_i}$-isogeny represented by 8 generators of its kernel $K_i$ which live in an extension of degree $k_i$ (we could further decompose these isogenies into a product of $e_i$ $\ell$-isogenies).

This decomposition costs us $O(\log^2 N)$ isogeny calls in dimension 8, along with the image of $f$ on the $(P_i, Q_i)$ and the images of $\alpha$ on the $P_{i,j}, Q_{i,j}$ (which has negligible cost).

In summary, the decomposition costs $O(\log^2 N B^8 \log B B^4)$ arithmetic operations in $\mathbb{F}_q$, along with the cost of finding the points $P_i, Q_i$ and evaluating $f$ on these points. The total cost is thus $\widetilde{O}(\log^2 N B^{12} \log q + B^2 \log^2 q) = \widetilde{O}(\log^{14} N \log q + \log^2 N \log^2 q)$ operations, along with the cost of evaluating $f$ on $\log N$ points which live in extensions of degree $O(B^2)$. If $f$ is given by the equation of its kernel, evaluating $f$ on these point take $O(N \log N B^2) = \widetilde{O}(N)$ operations in $\mathbb{F}_q$. The final cost of the decomposition is thus $\widetilde{O}(N \log q + \log^2 q)$. If $f$ is given by a rational generator of its kernel instead, we can use `sqrtVelu`, so evaluating $f$ takes only $O(\sqrt{N} \log N B^2) = \widetilde{O}(\sqrt{N})$ operations in $\mathbb{F}_q$.

Representing $F$ via this decomposition, ie via the kernels $K_i$ thus takes space $O(\log N B^2 \log q) =$ $O(\log^3 N \log q)$, and evaluating $F$ on a point requires evaluating $\log N$ $\ell_i^{e_i}$-isogenies represented by generators of their kernel, living in an extension of degree $O(B^2)$. This take $O(\log N B^{10} \log B) = \widetilde{O}(\log^{11} N)$ arithmetic operations in $\mathbb{F}_q$. This proves Theorem 1.2.

A similar computation proves Theorem 1.3: given our basis $(P, Q)$ of $E(\mathbb{F}_q)[N']$, we just need to compute $f(P), f(Q)$ in $O(N)$ or $\widetilde{O}(\sqrt{N})$ using `sqrtVelu`and then use them to build a decomposition of $F$. The complexity stated in Theorem 1.3 use the naive decomposition method, which could be improved using [DJP14, § 4.2.2].

## 6. Optimisations

We first note that the points $(P_i, Q_i)$ we take do not depend on the isogeny $f$, only on $E$. So it makes sense when constructing $N' > N$ to take prime powers $\ell_i^{e_i}$ such that $E$ admits a basis of $\ell_i^{e_i}$-torsion in a small extension. We can thus add a basic sieving strategy to the primes we use to construct $N'$.

We note that it can make sense to consider small prime powers because of the following standard Lemma 6.1: in general the $\ell$-torsion will live in an extension of degree $k = O(\ell^2)$. But once the $\ell$-torsion is defined, the $\ell^e$-torsion is defined over an extension of degree exactly $(e-1)\ell$ (unless possibly when $\ell = 2$ where it could be defined over a smaller extension).

**Lemma 6.1.** *Assume that $E(\mathbb{F}_q)$ contains the $\ell^e$ $(e \geq 1)$ torsion but not the $\ell^{e+1}$-torsion. Then the smallest extension containing the $\ell^{e+1}$-torsion is of degree $\ell$. Furthermore, unless $\ell = 2$ and $e = 1$, the $\ell^{e+2}$ is not defined over $E(\mathbb{F}_{q^\ell})$.*

*Proof.* If $P$ is a point of $\ell^{e+1}$-torsion, then since $\ell P$ is rational by assumption, $\pi(P) = P + T$, $T$ a point of $\ell$-torsion. Since $e \geq 1$, $T$ is rational, so $\pi^d(P) = P + dT$, hence $\pi^d(P) = P$ if and only if $\ell \mid d$.

Now since $E(\mathbb{F}_q)$ does not contain the full $\ell^{e+1}$-torsion, there is a point $P$ of $\ell^{e+2}$-torsion such that $\pi(P) = P + T$ with $T$ a primitive point of $\ell^2$-torsion. If $e > 1$, $T$ is rational, so $\pi^\ell(P) = P + \ell T \neq P$, hence $P \notin E(\mathbb{F}_{q^\ell})$. If $e = 1$, then $\pi(T) = T + T_0$ with $T_0$ a point of $\ell$-torsion by the reasoning above, so $\pi^\ell(P) = P + \ell T + \ell(\ell-1)/2T_0$. If $\ell > 2$, we have $\pi^\ell(P) = P + \ell T \neq P$ too. □

Also, since the main cost of computing the decomposition of $F$ will be the $O(\log N')$ direct calls to the isogeny $f$ on the points $P_i, Q_i$, it makes sense to batch these calls to a single call of $f$ on $P_{i_1} + P_{i_2} + \cdots + P_{i_k}$ as long as the compositum field containing this sum is not too large.

## 7. Conclusion

The method presented above shows that the efficient computation of isogenies for higher dimensional abelian varieties has interesting algorithmic applications to elliptic curves. Hopefully, this is the start of many new results in this direction.

## References

[BDL+20] D. Bernstein, L. De Feo, A. Leroux, and B. Smith. “Faster computation of isogenies of large prime degree”. 2020.

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

[DJP14] L. De Feo, D. Jao, and J. Plût. “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies”. In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247.

[Kan97] E. Kani. “The number of curves of genus two with elliptic differentials.” In: *Journal für die reine und angewandte Mathematik* 485 (1997), pp. 93–122.

[KU11] K. S. Kedlaya and C. Umans. “Fast polynomial factorization and modular composition”. In: *SIAM Journal on Computing* 40.6 (2011), pp. 1767–1802.

[LR22] D. Lubicz and D. Robert. “Fast change of level and applications to isogenies”. Accepted for publication at ANTS XV Conference — Proceedings. Aug. 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. 2022. URL: https://eprint.iacr.org/2022/1026.

[Rob22] D. Robert. "Breaking SIDH in polynomial time". Aug. 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/breaking_sidh.pdf. eprint: 2022/1038.

[Vél71] J. Vélu. "Isogénies entre courbes elliptiques". In: *Compte Rendu Académie Sciences Paris Série A-B* 273 (1971), A238–A241.

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