On the efficient representation of isogenies

2024/06/24 – NuTMiC, Szczecin

Damien Robert

Canari, Inria Bordeaux Sud-Ouest
http://www.normalesup.org/~robert/

Isogenies

- Elliptic curve: $E/k : y^2 = x^3 + ax + b.$ Algebraic group law!

- Isogeny: $\phi : E_1 \rightarrow E_2$ with $\phi(0_{E_1}) = 0_{E_2}$
- $\phi(P + Q) = \phi(P) + \phi(Q)$

$$\phi(x,y) = \left(\frac{g(x)}{h(x)}, cy \left(\frac{g(x)}{h(x)} \right)' \right)$$

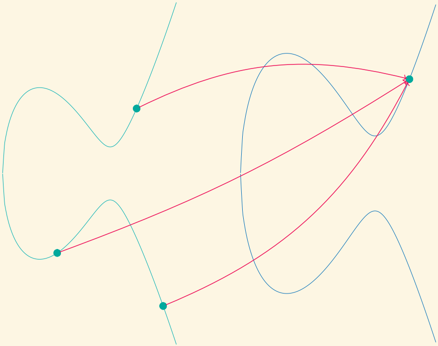
Isogeny based cryptography:

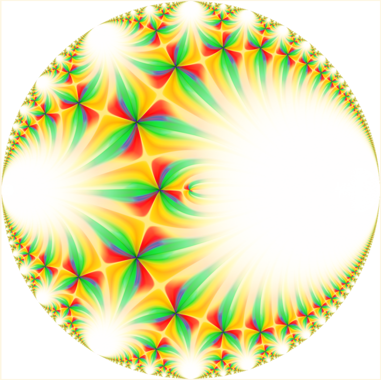
- Computing an isogeny $\phi : E_1 \rightarrow E_2$: Easy!
- Given (E_1, E_2), find an isogeny path $\phi : E_1 \rightarrow E_2$: Hard! (Even for quantum computers!)

$\Rightarrow$ Post quantum cryptosystems

Isogenies

$E_1 : y^2 = x^3 + a_1 x + b_1$ $E_2 : y^2 = x^3 + a_2 x + b_2$





Isogeny paths

Ordinary/Oriented curves:

- ☺ Commutative group action from the class group of R
  $R \subset \mathrm{End}(E)$ primitive orientation by a quadratic imaginary order on E
- ☹ Quantum subexponential $L(1/2)$ algorithm [Kuperberg 2003]
- Examples: CRS [Couveignes 1997; Rostovtsev, Stolbunov 2006], CSIDH [CLMPR 2018], SCALLOP [DFKLMPW 2023], …

Supersingular curves:

- Isogeny graph has good mixing properties
- Best algorithm is essentially exhaustive search (meet in the middle)
- ☺ Quantum exponential time
- ☹ No commutative group action
- Examples: CGL hash function [CGL 2009], SIDH [DJP 2011], SQISign [DKLPW 2020], …

Isogeny representations

- $\phi/\mathbb{F}_q : E_1 \to E_2$ isogeny of degree n (n-isogeny)
- "Evaluating an isogeny is easy"
- Really? Depends on the representation!

- Kernel representation: $K = \operatorname{Ker} \phi$
- Generator(s) representation: $K = \langle T \rangle = \langle T_1, \dots, T_m \rangle$
- Ideal representation: $I \leftrightarrow \phi_I$
- Interpolation representation, Deformation representation, Modular representation… See survey!

- Compact representation: polynomial space in $\log n, \log q$
- Efficient representation: evaluation in polynomial time in $\log n, \log q$

- Previously: only isogenies of smooth degrees had an efficient representation
- SIDH attacks (2022): every isogeny has an efficient HD representation!
- This talk: the HD representation and algorithms to manipulate it

Kernel representation

- $K = \mathrm{Ker}\,\phi$
- $K : h(x) = 0, h(x) = \prod_{P \in K - 0_E} (x - x(P))$

If $E : y^2 = f(x)$, [Kohel 1996]:

$$\phi(x,y) = \left(\frac{g(x)}{h(x)}, y \left(\frac{g(x)}{h(x)} \right)' \right)$$

$$\frac{g(x)}{h(x)} = \#K.x - \sigma - f'(x)\frac{h'(x)}{h(x)} - 2f(x)\left(\frac{h'(x)}{h(x)}\right)'$$

- Space: $O(n \log q)$ = linear space
- Evaluation: $O(n)$ arithmetic operations in $\mathbb{F}_q$ = linear time

Generator representation

- $K = \langle T \rangle$, K defined over $\mathbb{F}_q$, T defined over $\mathbb{F}_{q^d}$, $d = O(n)$, [Vélu 1971]:

$$x(f(P)) = x(P) + \sum_{i=1}^{n-1} (x(P+iT) - x(iT))$$
$$y(f(P)) = y(P) + \sum_{i=1}^{n-1} (y(P+iT) - y(iT))$$

- Space: $O(d \log q)$
  If $d = 1$ (or small): compact representation!
- Evaluation: $O(n)$ operations over $\mathbb{F}_{q^d}$ $\Rightarrow$ linear if d small, quadratic if d large
- $\sqrt{\text{élu}}$ [Bernstein, De Feo, Leroux, Smith 2020]: evaluation in $\widetilde{O}(\sqrt{n})$ over $\mathbb{F}_{q^d}$
  (via a time/memory trade off)

Decomposed representation

- $n = \prod_{i=1}^{m} \ell_i, \phi = \phi_m \circ \ldots \circ \phi_2 \circ \phi_1, \phi_i$ a ℓ_i-isogeny;
- Decomposed representation: complexity for evaluation depends on $\ell_n := \max(\ell_i)$

- Space: $O(m\ell_n \log q)$
- Evaluation: $O(m\ell_n \log q)$
- If n is smooth: compact and efficient!

Decomposing a smooth degree isogeny

- $\phi : E_1 \to E_2, K = \mathrm{Ker}\,\phi = \langle T \rangle$ of degree $n = 2^m, T \in \mathbb{F}_{q^d}$
- $\phi = \phi_1' \circ \phi_1$
- $\phi_1 : E_1 \to E_1'$ of degree 2 with kernel $K_1 = \langle 2^{m-1} T \rangle$
- $\phi_1' : E_1' \to E_2$ of degree 2^{m-1} with kernel $K = \langle \phi_1(T) \rangle$

- Complexity: $O(m^2)$ arithmetic operations in $\mathbb{F}_{q^d}$
- [De Feo, Jao, Plût 2011]: $\widetilde{O}(m)$ operations in $\mathbb{F}_{q^d}$
- d can be large, $d = \Theta(n)$ in the worst case $\Rightarrow$ quasi-linear time

- $n = \prod_{i=1}^m \ell_i^{e_i}$
- CRT representation: $K = \prod_{i=1}^m K[\ell_i^{e_i}] = \langle G_1, \dots, G_m \rangle, G_i \in \mathbb{F}_{q^{d_i}}, d = \max(d_i)$
- Compact representation if the n-torsion is accessible
- Decomposition cost: $\widetilde{O}(m(\sum e_i) d \ell_n \log q)$;
- Efficient if n is smooth (ℓ_n small) and the n-torsion is accessible (d small)
- Example: n powersmooth

Ideal representations

- I ideal in $R \subset \mathrm{End}(E) \Rightarrow \phi_I$ isogeny with kernel $E[I]$.

- Supersingular case: Deuring's correspondance
  $E/\mathbb{F}_{p^2}$ supersingular curve, $R = \mathrm{End}(E)$ quaternion order
- KLPT: smoothening algorithm $I \sim J, N(J)$ smooth

- Oriented case: $R \subset \mathrm{End}(E)$ imaginary quadratic order
- Example: Frobenius orientation. Ordinary curves, $E/\mathbb{F}_p$ supersingular

☹ Smoothening of ideals: subexponential in Δ_R

☹ Restricted class group action

Summary

- Kernel representation: linear space and time
- Generator representation: possibly compact, linear or quadratic time
- If n smooth: decomposed representation = logarithmic space and time

- Decomposition cost given a CRT representation $K = \langle G_1, \dots, G_m \rangle$: polynomial time in $d = \max(d_i)$ and $\ell_n = \max(\ell \mid n)$

$\Rightarrow$ Efficient if n smooth and the n-torsion is accessible

- What if n is a large prime?
- No way to represent ϕ efficiently

Summary

- Kernel representation: linear space and time
- Generator representation: possibly compact, linear or quadratic time
- If n smooth: decomposed representation = logarithmic space and time

- Decomposition cost given a CRT representation $K = \langle G_1, \dots, G_m \rangle$: polynomial time in $d = \max(d_i)$ and $\ell_n = \max(\ell \mid n)$

$\Rightarrow$ Efficient if n smooth and the n-torsion is accessible

- What if n is a large prime?
- ~~No way to represent ϕ efficiently~~

Scalar multiplication

- Scalar multiplication: $[n] : P \mapsto n \cdot P$ is an n^2-isogeny
- Double and add: $O(\log n)$ arithmetic operations, even if n is prime!

- $\Phi : E^2 \to E^2, (P_1, P_2) \mapsto (P_1 + P_2, P_1 - P_2)$ is a 2-isogeny in dimension 2.
- $\Phi = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$
- Double: $\Phi(T, T) = (2T, 0)$.
- Add: $\Phi(T, P) = (T + P, T - P)$.

- We can evaluate $n \cdot P$ as a composition of $O(\log n)$ evaluations of Φ, projections $E^2 \to E$ and embeddings $E \to E^2$.
- Double and add on E = 2-isogenies in dimension 2

The embedding lemma [R. 2022]

- For any $N \geq n$, an n-isogeny $\phi : E_1 \to E_2$ in dimension 1 can always be efficiently embedded into a N-isogeny $\Phi : A_1 \to A_2$ in dimension 8 (and sometimes $4, 2$)

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow & & \uparrow \\ A_1 & \xrightarrow{\Phi} & A_2 \end{array}$$

- Considerable flexibility (at the cost of going up in dimension).
- Breaks SIDH ([Castryck-Decru 2022], [Maino-Martindale 2022] in dimension 2, [R. 2022] in dimension 4 or 8)

- Kani's lemma [1997] + Zarhin's trick [1974]: write $N - n = a_1^2 + a_2^2 + a_3^2 + a_4^2$ and

$$\Phi = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 & \widetilde{\phi} & 0 & 0 & 0 \\ a_2 & a_1 & a_4 & -a_3 & 0 & \widetilde{\phi} & 0 & 0 \\ a_3 & -a_4 & a_1 & a_2 & 0 & 0 & \widetilde{\phi} & 0 \\ a_4 & a_3 & -a_2 & a_1 & 0 & 0 & 0 & \widetilde{\phi} \\ -\phi & 0 & 0 & 0 & a_1 & a_2 & a_3 & a_4 \\ 0 & -\phi & 0 & 0 & -a_2 & a_1 & -a_4 & a_3 \\ 0 & 0 & -\phi & 0 & -a_3 & a_4 & a_1 & a_2 \\ 0 & 0 & 0 & -\phi & -a_4 & -a_3 & a_2 & a_1 \end{pmatrix}$$

Algorithms for N-isogenies in higher dimension

- Analogues of Vélu's formula: [Cosset, R. (2014); Lubicz, R. (2012–2022)]
  An N-isogeny in dimension g can be evaluated in linear time $O(N^g)$ arithmetic operations in the theta model given generators of its kernel.

☺ Work in any dimension

☹ Exponential dependency 2^g in the dimension g.

☹ Need a rational level $\Gamma(2,4)$-structure (automatic for supersingular curves over $\mathbb{F}_{p^2}$)

- Algorithm in $O(N^g)$ in the Jacobian model: [Couveignes, Ezome (2015)]

☺ Rational model

☹ Restricted to $g \leq 3$

Cost of a 2^m-isogeny in dimension g:

g	1	2	4	8
Relative cost	$\times 1$	$\times 4$	$\times 32$	$\times 1024$

Dedicated fast formulas in higher dimension

Dimension 2:

- Fast 2^m-isogenies in the Mumford Jacobian or Kummer model [Kunzweiler 2022] and in the theta model [Dartois, Maino, Pope, R. 2023]

		Codomain			Evaluation		
$\log p$	m	Theta Rust	Theta SageMath	Richelot SageMath	Theta Rust	Theta SageMath	Richelot SageMath
254	126	2.13 ms	108 ms	1028 ms	161 µs	5.43 ms	114 ms
381	208	9.05 ms	201 ms	1998 ms	411 µs	8.68 ms	208 ms
1293	632	463 ms	1225 ms	12840 ms	17.8 ms	40.8 ms	1203 ms

- Fast 3^m-isogenies in the Mumford Jacobian model [Decru, Kunzweiler 2023] and in the theta model [Corte-Real Santos, Costello, Smith 2024]

Dimension 4:

- Fast 2^m-isogenies in the theta model [Dartois 2024]

The HD representation

- Embed $\phi : E_1 \to E_2$ into an N-isogeny Φ in dimension g
- Represent Φ by its kernel Ker Φ:
  Ker Φ is completely determined by n and the action of ϕ on $E_1[N]$
- CRT basis: $N = \prod_{i=1}^m N_i = \prod_{i=1}^m \ell_i^{e_i}$,

$$(P_i, Q_i, \phi(P_i), \phi(Q_i)), \quad \text{for } (P_i, Q_i) \text{ a basis of } E[\ell_i^{e_i}]$$

- Naive algorithm: reconstruct ϕ in $\widetilde{O}(n)$ via rational function interpolation
- HD approach: exploit the N-torsion structure by going to Φ in higher dimension

- Compact representation if the N-torsion is accessible
- Decomposing Φ: efficient if N is smooth and the N-torsion is accessible
- Evaluating the decomposed Φ: efficient if N is smooth

- Can take any $N \geq n$ (Example: N powersmooth)
- Ideal scenario: E_1 has rational $N = 2^m$-torsion and Φ in dimension 2

- Universal: can be efficiently recovered from any other efficient isogeny representation of ϕ
- Philosophy: if we know how ϕ act on sufficiently many nice points, we can efficiently compute $\phi(P)$ for any point P

Application: divisions [R. 2022]

- Is an isogeny $\phi : E_1 \to E_2$ divisible by $[\ell]$?
- Prior art: test if $\phi(E[\ell]) = 0$
- Division polynomial ψ_ℓ: degree $O(\ell^2) \Rightarrow$ exponential time

- HD division algorithm [R. 2022]:
- Given an HD representation $(P_i, Q_i, \phi(P_i), \phi(Q_i))$ with $N_i \wedge \ell = 1$,

$$(P_i, Q_i, \frac{\phi(P_i)}{\ell}, \frac{\phi(Q_i)}{\ell})$$

  is an HD representation of ϕ/ℓ if it exists

$\Rightarrow$ polynomial time (in $\log \ell$) division algorithm

Corollary (Computing the endomorphism ring of ordinary elliptic curves)

If $E/\mathbb{F}_q$ is an ordinary elliptic curve; point counting gives χ_π, hence $K := \mathbb{Q}(\pi_q)$, and we know $\mathbb{Z}[\pi] \subset \mathrm{End}(E) \subset O_K$. Given the factorisation of the conductor $[O_K : \mathbb{Z}[\pi]]$ of $\mathbb{Z}[\pi]$, we can determine $\mathrm{End}(E)$ in polynomial time, via efficient divisions.

- Factorisation: quantum polynomial time, classical subexponential time
- Previously: no quantum polynomial time algorithm known
  Classical algorithm in $L(1/2)$ under GRH [Bisson–Sutherland 2009]

Algorithms for the HD representation

$\phi/\mathbb{F}_q : E_1 \to E_2$ an n-isogeny with an efficient representation

- Equality testing, Validity
- Composition and addition: $\phi_2 \circ \phi_1, \phi_1 + \phi_2$
- Dual isogeny: $\widetilde{\phi} : E_2 \to E_1$
- Divisions: Test if $\phi \stackrel{?}{=} \psi' \circ \psi$ is divisible by ψ, and if so return the HD representation of ψ'
- Lifts and deformations: deform ϕ to $\widetilde{\phi}/R : \widetilde{E_1} \to \widetilde{E_2}$ over $R = \mathbb{F}_q[\varepsilon]/\varepsilon^m$ or $R = \mathbb{Z}_q/p^m\mathbb{Z}_q$
- Splittings: If $n = n_1 n_2, n_1 \wedge n_2 = 1$, split ϕ as $\phi = \phi_2 \circ \phi_1$

$$\phi : E_1 \xrightarrow{\phi_1} E_{12} \xrightarrow{\phi_2} E_2$$

- Pushforwards: compute the pushfoward of ϕ_1 and ϕ_2 if they are of coprime degrees

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_1} & E_1 \\ \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_2'} \\ E_1 & \xrightarrow{\phi_1'} & E_{12} \end{array}$$

- Kernel: return an equation for Ker ϕ in $\widetilde{O}(n)$

Cryptographic applications

- New protocols in isogeny based cryptography: SQIsignHD [DLRW24], FESTA [BMP23] and QFESTA [NO23], the Deuring VRF [Ler23b], SCALLOP-HD [CL23] (efficient representation of orientations), IS-CUBE [Mor23], LIT-SiGamal [Mor24], SILBE [DFV24], POKE [Bas24], SQIsign2d (West and East) [BDD+24; NO24], SQIPrime [DF24]…
- New or improved security reductions in isogeny based cryptography, [MW23; ACD+23; PW24; ES24] and in classical elliptic curve cryptography [Gal24]
- New methods to convert ideals into isogenies [Ler23a; NO23; PR23; ON24; BDD+24]

Examples:

- Clapoti(s) [Page, R. 2023]: computing the class group action for an arbitrary orientation R in polynomial time
- No smoothening needed
- Unrestricted effective group action!

- SQIsignHD, SQIsign2d-West: bypass KLPT's smoothening algorithm for supersingular curves too
- KLPT: $\phi_J : E_1 \to E_2$, smoothened isogeny of degree $O(p^{4.5})$ (or $O(p^3)$ if E_1 is nice)
- HD representation: can use the smallest isogeny $\phi_J : E_1 \to E_2$ of degree $O(\sqrt{p})$ even if it is not smooth!

SQISign2d (West)

	SQIsign	SQIsign2d
Public key	66B	66B
Signatures	177B	148B
Clean security proof	☹	☺
Keygen (Mcycles)	400	60
Sign (Mcycles)	1880	160
Verify (Mcycles)	29	9

- SQIsign2D: signature and verification in dimension 2
- SQIsignHD: signature in dimension 1, verification in dimension 4
  New faster variant compared to the Eurocrypt 2024 version using techniques from SQIsign2d: signatures now use dimension 2 too.

  Bonus: same public key as in SQIsign2d!
- Signature size: 109B
- Signature $\approx 5\times$ faster than SQIsign2d
- Verification expected $\approx 8\times$ slower

Number theoretic applications

- Computing the saturation of a quadratic order R in $\mathrm{End}(E)$
- Compute the canonical lift $\hat{E}/\mathbb{Z}_q$ of an ordinary elliptic curve in polynomial time [R. 2022]
  Previously: $L(1/2)$ under GRH [Couveignes–Henocq 2002]
- Compute the modular polynomial Φ_ℓ by deformation [Kunzweler, R. 2024]

Point counting for $E/\mathbb{F}_q, q = p^n$

- [Schoof 1985]: $\widetilde{O}(n^5 \log^5 p)$ (Étale cohomology)
- [SEA 1992]: $\widetilde{O}(n^4 \log^4 p)$ (Heuristic)

- [Kedlaya 2001]: $\widetilde{O}(n^3 p)$ (Rigid cohomology)
- [Harvey 2007]: $\widetilde{O}(n^{3.5} p^{1/2} + n^5 \log p)$

- [Satoh 2000] (canonical lifts of ordinary curves): $\widetilde{O}(n^2 p^2)$ (Crystalline cohomology)
- [Maiga – R. 2021]: $\widetilde{O}(n^2 p)$
- [R. 2022]: $\widetilde{O}(n^2 \log^8 p + n \log^{11} p)$
  Use an HD representation of the Verschiebung $\hat{\pi}_p$ and canonical lifts

Efficient representation of isogenies

Past:

- Restricted to smooth degree isogenies
- Vélu's / $\sqrt{\text{élu}}$ formulas
- Ideal smoothening

Present:

- The HD representation: recent powerful tool with many applications in isogeny based cryptography and algorithmic number theory
- Use abelian varieties to speed up algorithms on elliptic curves
- Excellent overview in Castryck's invited talk at Eurocrypt 2024: "An attack became a tool: Isogeny based cryptography 2.0"
- Full details in the survey paper:

  http://www.normalesup.org/~robert/pro/publications/articles/isogeny_survey.pdf

Future?

- Switch from ideals equivalences of categories to modules equivalences of categories
  - Handles the higher dimensional isogeny graphs of E^g
  - Handles level structures
  - Go beyond Kani's lemma
- Use cyclic isogenies?

Bibliography

[ACD+23] S. Arpin, J. Clements, P. Dartois, J. K. Eriksen, P. Kutas, and B. Wesolowski. "Finding orientations of supersingular elliptic curves and quaternion orders". In: arXiv preprint arXiv:2308.11539 (2023) (cit. on p. 20).

[Bas24] A. Basso. "POKE: A Framework for Efficient PKEs, Split KEMs, and OPRFs from Higher-dimensional Isogenies". In: Cryptology ePrint Archive (2024) (cit. on p. 20).

[BDD+24] A. Basso, L. De Feo, P. Dartois, A. Leroux, L. Maino, G. Pope, D. Robert, and B. Wesolowski. "SQIsign2D-West: The Fast, the Small, and the Safer". May 2024 (cit. on p. 20).

[BMP23] A. Basso, L. Maino, and G. Pope. "FESTA: fast encryption from supersingular torsion attacks". In: International Conference on the Theory and Application of Cryptology and Information Secu Springer. 2023, pp. 98–126 (cit. on p. 20).

[CL23] M. Chen and A. Leroux. "SCALLOP-HD: group action from 2-dimensional isogenies". In: Cryptology ePrint Archive (2023) (cit. on p. 20).

[DLRW24] P. Dartois, A. Leroux, D. Robert, and B. Wesolowski. "SQISignHD: New Dimensions in Cryptography". In: 14651 (May 2024). Ed. by M. Joye and G. Leander, pp. 3–32. doi: 10.1007/978-3-031-58716-0_1 (cit. on p. 20).

[DF24] M. Duparc and T. B. Fouotsa. "SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies". In: Cryptology ePrint Archive (2024) (cit. on p. 20).

[DFV24] M. Duparc, T. B. Fouotsa, and S. Vaudenay. "Silbe: an updatable public key encryption scheme from lollipop attacks". In: Cryptology ePrint Archive (2024) (cit. on p. 20).

[ES24] K. Eisentraeger and G. Scullard. "Connecting Kani's Lemma and path-finding in the Bruhat-Tits tree to compute supersingular endomorphism rings". In: (2024). arXiv: 2402.05059 (cit. on p. 20).

[Gal24] S. Galbraith. Climbing and descending tall volcanos. Cryptology ePrint Archive, Paper 2024/924. 2024. url: https://eprint.iacr.org/2024/924 (cit. on p. 20).

[Ler23a] A. Leroux. "Computation of Hilbert class polynomials and modular polynomials from supersingular elliptic curves". In: Cryptology ePrint Archive (2023) (cit. on p. 20).

[Ler23b] A. Leroux. "Verifiable random function from the Deuring correspondence and higher dimensional isogenies". In: (2023) (cit. on p. 20).

[MW23] A. H. L. Merdy and B. Wesolowski. "The supersingular endomorphism ring problem given one endomorphism". In: arXiv preprint arXiv:2309.11912 (2023) (cit. on p. 20).

[Mor23] T. Moriya. "IS-CUBE: An isogeny-based compact KEM using a boxed SIDH diagram". In: Cryptology ePrint Archive (2023) (cit. on p. 20).

[Mor24] T. Moriya. "LIT-SiGamal: An efficient isogeny-based PKE based on a LIT diagram". In: Cryptology ePrint Archive (2024) (cit. on p. 20).

[NO23] K. Nakagawa and H. Onuki. "QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras". In: Cryptology ePrint Archive (2023) (cit. on p. 20).

[NO24] K. Nakagawa and H. Onuki. "SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies". In: Cryptology ePrint Archive (2024) (cit. on p. 20).

[ON24] H. Onuki and K. Nakagawa. "Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign". In: Cryptology ePrint Archive (2024) (cit. on p. 20).

[PR23] A. Page and D. Robert. “Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time”. Nov. 2023 (cit. on p. 20).

[PW24] A. Page and B. Wesolowski. “The supersingular endomorphism ring and one endomorphism problems are equivalent”. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer. 2024, pp. 388–417 (cit. on p. 20).