Ideal to Isogeny: from Qlapoti to qt-Pegasis

Isogeny Days

R. Invernizzi - joint work with many

COSIC - KU Leuven

12 sep 2025

Outline

1. Ideal to Isogeny
2. qlapoti
3. qt-pegasis

Ideal to isogeny

- *Deuring correspondence*
- quaternion ideals $\leftrightarrow$ isogenies
- quaternions are *fast*, isogenies are *slow*
  - perform all computations with quaternions
  - recover isogenies at the end
- *largest component* of most isogeny schemes

Applications

- Sample a *random ideal*, translate it into a *random isogeny*
- the codomain is a *random curve*
  - key generation (SQIsign, PRISM, ...), commitment (SQIsign)
- compute isogenies with *some properties* from ideals
  - respose (SQIsign, PRISM)
- quadratic case: *effective class group actions* (PEGASIS)
- *how?*

Ideal to Isogeny 1

- $\ker(I) = \{P \in E \mid \alpha(P) = 0 \; \forall \; \alpha \in I\}$
- let $\mathrm{nrd}(I) = l$, $E[l] = \langle P, Q \rangle$, $\alpha \in I$
- write $\alpha(P) = aP + bQ$ and $\alpha(Q) = cP + dQ$
- recover R s.t. $\alpha(R) = 0$ by linear algebra
- problem: *requires l small / smooth*

Ideal to Isogeny 2 (KLPT)

- given $\beta \in I$, get *equivalent ideal* $J = I\overline{\beta}/\mathrm{nrd}(I)$
- same domain, same codomain, different degree (norm)
- if $\mathrm{nrd}(\beta) = N \cdot \mathrm{nrd}(I)$ then $\mathrm{nrd}(J) = N$
- look for N smooth ($= 2^e$): *KLPT* $\rightsquigarrow$ *SQIsign v1*
- typically: N *huge* ($\approx p^3$)

Ideal to Isogeny 3 (QFESTA)

- using *HD isogenies* we can compute isogenies of degree $q(2^e - q)$
- it is easy to sample ideals of norm $q(2^e - q)$
- allows to compute isogenies of *any degree*
- requires $q < 2^e < p$
- *does not work with a given ideal*

Ideal to Isogeny 4 (Clapoti)

- generalize the QFESTA equation: enough to solve

  $$u \cdot \mathsf{nrd}(I_1) + v \cdot \mathsf{nrd}(I_2) = 2^e$$

  where I_1, I_2 are equivalent ideals
- need degree u, v isogenies: use QFESTA for that
- works for *every ideal* (*in theory*)

Ideal to Isogeny 4 (Clapoti)

- nrd(I_1), nrd$(I_2) \approx \sqrt{p}$ at least, but $2^e < p$
- equation has a significant *failure rate* (2^{-8})
- SQIsign: reduce it to 2^{-60} with some tricks
- *memory-heavy* and still not cryptographically negligible
- fixed degree isogenies are ok but *costly*

Outline

1. Ideal to Isogeny

2. qlapoti

3. qt-pegasis

A more direct approach

- Clapoti solves $u \cdot \mathrm{nrd}(I_1) + v \cdot \mathrm{nrd}(I_2) = 2^e$
- we can solve $\mathrm{nrd}(I_1) + \mathrm{nrd}(I_2) = 2^e$ instead
- I_1 and I_2 are chosen *random* and *small*
- unlikely to sum to $2^e \rightsquigarrow$ need to be more explicit

A more direct approach

- let $n = \mathrm{nrd}(I)$
- the equation becomes $\mathrm{nrd}(\beta_1) + \mathrm{nrd}(\beta_2) = n2^e$
- write $I = \langle \alpha, n \rangle$ (*many choices* for α)
- $\beta_k = \gamma_k n + \gamma'_k \alpha$
- simplify: $\gamma_k = a_k + ib_k$ and $\gamma'_k = 1$

Solving mod n

- The full equation becomes

$$n(a_1^2 + b_1^2 + a_2^2 + b_2^2) + 2a_\alpha(a_1 + a_2) + 2b_\alpha(b_1 + b_2) = 2^e - 2r$$

- first solve $2a_\alpha x + 2b_\alpha y \equiv 2^e - 2r \mod n$
- find a *short solution* (s, t) using cvp
- replace $a_2 = s - a_1$ and $b_2 = t - b_1$
- we are left with a *sum of squares*

Improvement pt. 1

- no additional fixed degree isogenies
- 2x improvement with direct impact on current schemes

NIST level	Previous work	This work	Improvement
I	0.434s	0.171s	x2.5
III	0.849s	0.446s	x1.9
V	1.143s	0.515s	x2.2

Imrpovement pt. 2

- representation $I = \langle \alpha, n \rangle$ is not unique
- many α to try $\rightsquigarrow$ virtually impossible to fail

NIST Level	p	upper bound on failure rate
I	$2^{248} \cdot 5 - 1$	2^{-197}
III	$2^{376} \cdot 65 - 1$	2^{-312}
V	$2^{500} \cdot 27 - 1$	2^{-438}

Improvement pt. 2

- no need for additional curves
- much simpler code
- less memory usage (x11 to x34)
- cleaner security proofs

Credits

Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies

Join work with: Giacomo Borin, Maria Corte-Real Santos, Jonathan Komada Eriksen, Marzio Mula, Sina Schaeffler and Frederik Vercauteren

Eprint: *2025/1604*
Code: *https://github.com/KULeuven-COSIC/Qlapoti*

Outline

1. Ideal to Isogeny

2. qlapoti

3. qt-pegasis

Revisiting PEGASIS

- PEGASIS: *effective class group actions* from CSIDH
- given an ideal $\mathfrak{a} \in \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ compute the corresponding isogeny
- based on Clapoti: solve $u \cdot n(\mathfrak{b}) + v \cdot n(\mathfrak{c}) = 2^e$ for $\mathfrak{b}, \mathfrak{c} \sim \mathfrak{a}$
- same issues $+$ fixed degree isogenies are *harder*
- partially solved with *Elkies algorithm* and *dimension 4*

Revisiting PEGASIS

- goal: replace *Clapoti* with *qlapoti*
- problem: we are working with $R = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$
- key insight from *KLaPoTi*: "build" i on $E \times E$
- take $\mathcal{O} = R + \mathrm{i}R$ and $\mathcal{I} = \mathfrak{a} + \mathrm{i}\mathfrak{a}$
- apply qlapoti to $\mathcal{I}$

Further optimizations

- $\mathcal{I} = \mathfrak{a} + i\mathfrak{a}$ is far from a random ideal
- different steps can be *simplified*
- we can predict / control the shape of the equation
- *two modular additions* instead of cvp

Comparison with PEGASIS

- no Elkies isogenies
- 1.3x to 2.1x speedup
- much simpler algorithm
- suitable for constant time implementation
- no restriction on primes

Timings

Prime size	Step 1	Step 2	Step 3	Total	Improvement	Step 3 rt.
508	0.027	0.083	1.048	1.16	1.31x	90%
1008	0.06	0.30	2.77	3.13	1.34x	88%
1554	0.09	0.77	6.08	6.94	1.51x	87%
2031	0.55	1.36	10.3	12.17	1.75x	84%
4089	3.15	6.80	47.6	57.5	2.12x	82%

Open Questions

- shorter chains: they should exist, how do we find them?
- move to dimension 2: $\mathfrak{a} + i\mathfrak{a}$ is not a random ideal
- new names: running out of **c** sounds, maybe Clapowtee?

Credits

qt-Pegasis: Simpler and Faster
Effective Class Group Actions

Join work with: Pierrick Dartois, Jonathan Komada Eriksen and Frederik Vercauteren

eprint and code (hopefully) coming soon

Credits: **J**onathan **O**mada **KER**iksen, *street artist*

Thans you for your attention!
Questions?