KU LEUVEN

fwo

qt-Pegasis: simpler and faster effective class group actions

Eurocrypt '26

R. Invernizzi
Joint work P. Dartois, J. K. Eriksen, F. Vercauteren

COSIC - KU Leuven

12 may 2026

Outline

1. Isogeny based group actions
2. A new solution: qt-Pegasis
3. Implementation results

Outline

1. Isogeny based group actions
2. A new solution: qt-Pegasis
3. Implementation results

Isogeny based group actions

- ideals of certain rings (e.g. $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$) *act* on supersingular elliptic curves
- namely can compute $\mathfrak{a} * E_1 = E_2$
- E_2 is computed via an *isogeny* $\varphi_{\mathfrak{a}}$
- *commutative* (similar to DH) but (moderately) *quantum safe*
- how can we compute $\varphi_{\mathfrak{a}}$?

Isogeny computation

- computing isogenies is linear in the *degree* and exponential in the *dimension*
- degree q isogeny is $O(\sqrt{q})$ for large q but $O(q)$ *for small* q
- isogenies can be composed: a 2^{100} isogeny is 100 2-isogenies
- in dimension g there are 2^g *coordinates* (e.g. 2 in dim 1, 16 in dim 4)

Quantum security

- quantum attack by *Kuperberg*
- *subexponential* in the *discriminant* of the underlying ring
- actual complexity debated (500 to 4000 bits)
- for this talk: discriminant = base field characteristic

History

- first instantiations (CSIDH, CRS): *REGA*
- can act only with small ideals
- limited for applications
- more recently (Clapoti, KLaPoTi, *PEGASIS*): *EGA*

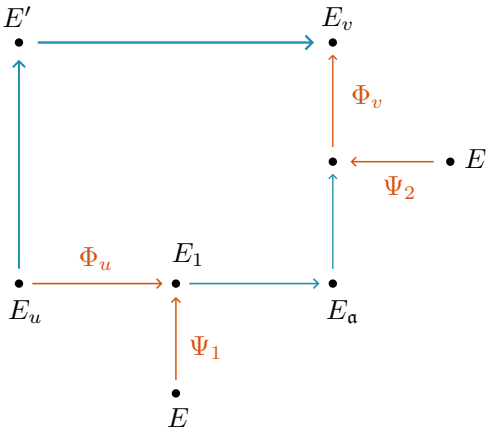
PEGASIS

- PEGASIS: first *practical EGA*
- can act with any target ideal $\mathfrak{a}$
- from $\mathfrak{a}$ sample random elements $\mathfrak{b}, \mathfrak{c}$
- try to solve $uN(\mathfrak{b}) + vN(\mathfrak{c}) = 2^e$ for some u, v, e
- u, v must be sums of squares

PEGASIS

- compute isogeny factors using *Elkies* algorithm
- compute 2^e isogeny in *dimension 4*
- the codomain is the result of the action
- somewhat practical result:
  - 1.5s in sage at 500 bits discriminant
  - first ever instantiation at *4000 bits* (120s)

PEGASIS



Limitations

- Elkies isogenies are *costly* (40% at 4000 bits)
- quite complicated code with *many parameters*
- limitations on the *base prime*
- $\rightsquigarrow$ large margin of improvement

Outline

1. Isogeny based group actions
2. A new solution: qt-Pegasis
3. Implementation results

A more direct approach

- instead of solving $uN(\mathfrak{b}) + vN(\mathfrak{c}) = 2^e$ solve for $N(\mathfrak{b}) + N(\mathfrak{c}) = 2^e$
- instead of sampling $\mathfrak{b}, \mathfrak{c}$ at random *construct them together*
- the full equation becomes

$$N(\mathfrak{a})(b_1^2 + b_2^2 + c_1^2 + c_2^2) + r(d_1^2 + d_2^2) + tr(\alpha)(c_1 d_1 + c_2 d_2) = 2^e$$

- similar to the Qlapoti equation

From quaternions to quadratic ideals

- problem: we are working with *quadratic ideal* $\mathfrak{a} \in \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$
- key insight (KLaPoTi): $\mathfrak{a} + i\mathfrak{a}$ is a *quaternion ideal*
- requires dimension 4 (same as PEGASIS)
- applies directly to our case

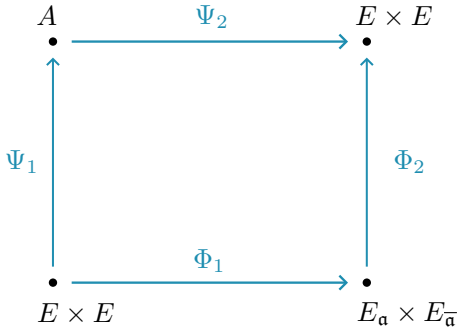
Further optimizations

- the resulting norm equation can be split into a $\bmod N(\mathfrak{a})$ part and a remainder
- a good solution $\bmod N(\mathfrak{a})$ (with cvp) makes the second part easier
- no $u, v \rightsquigarrow$ *no Elkies steps*
- $\mathfrak{a} + \mathfrak{i}\mathfrak{a}$ is far from a random ideal $\rightsquigarrow$ further optimizations

Comparison with PEGASIS

- much simpler and faster
- mostly 4D isogeny computations
- more suitable to constant time

Comparison with PEGASIS



Outline

1. Isogeny based group actions
2. A new solution: qt-Pegasis
3. Implementation results

Timings (s) - sagemath

Prime size	Step 1	Step 2	Step 3	Total	Improvement	Step 3 rt.
508	0.006	0.05	0.79	0.85	1.8×	93%
1008	0.014	0.18	2.29	2.48	1.7×	95%
1554	0.008	0.423	5.10	5.54	1.9 ×	92%
2031	0.06	0.76	8.87	9.69	2.2 ×	92%
4089	0.67	3.83	43.1	47.6	2.6 ×	91%

Recent developements

- *C implementation* [2026/114] with better 4D isogenies
- closer to constant time
- *24ms* for a 500 bit action, 10s for 4000
- PQarrots: NIST submission for threshold primitives

Open Questions

- shorter chains (smaller e): they should exist, how do we find them?
- move to *dimension 2:* $\mathfrak{a} + \mathrm{i}\mathfrak{a}$ is not a random ideal
- apply to discriminant $> p$

Thank you for your attention.
Questions?