# Qlapoti:

## Simple and Efficient Translation of Quaternion Ideals to Isogenies

Joint work with: Giacomo Borin, Maria Corte-Real Santos, Riccardo Invernizzi, Marzio Mula, Sina Schaeffler and Frederik Vercauteren

**Jonathan Komada Eriksen,**
**COSIC, KU Leuven**

# Qlapoti:

Homomorphisms between projective modules of rank 1

## Simple and Efficient Translation of ~~Quaternion Ideals~~ to Isogenies

Joint work with: Giacomo Borin, Maria Corte-Real Santos, Riccardo Invernizzi, Marzio Mula, Sina Schaeffler and Frederik Vercauteren

**Jonathan Komada Eriksen,**
**COSIC, KU Leuven**

# The Deuring Correspondence

$$\mathrm{End}(E_0) = \mathcal{O}_0 \subset B_{p,\infty}$$

Projective, left $\mathcal{O}_0$-modules of rank 1 under $\mathcal{O}_0$-module homomorphisms

Supersingular curves $E/\bar{\mathbb{F}}_p$, under isogenies

$$\mathrm{Hom}(E, E_0) \longleftarrow E$$

# The Deuring Correspondence

$$\mathrm{End}(E_0) = \mathcal{O}_0 \subset B_{p,\infty}$$

Projective, left $\mathcal{O}_0$-modules of rank 1 under $\mathcal{O}_0$-module homomorphisms

Supersingular curves $E/\bar{\mathbb{F}}_p$, under isogenies

$$\mathrm{Hom}(E, E_0) \longleftarrow E$$

$$I \longrightarrow E_I := \varphi_\beta(E_0)$$

$\beta \in I$ defines $h_\beta : I \hookrightarrow \mathcal{O}_0$ by $h_\beta(\alpha) = \alpha \dfrac{\bar{\beta}}{n(I)}$

Define $\varphi_\beta$ by $\ker \varphi_\beta = \{P \in E_0 \mid h_\beta(\alpha)(P) = 0, \forall \alpha \in I\}$

# SQIsign - Key Generation

Secret key: $I \subset \mathcal{O}_0$

$$E_0 \dashrightarrow E_{pk} := E_I$$

# SQIsign - Commit

Secret key: $I \subset \mathcal{O}_0$

Commitment: $J \subset \mathcal{O}_0$

$$\begin{tikzcd} E_0 \arrow[r, dotted] \arrow[d, dotted] & E_{pk} := E_I \\ E_{com} := E_J & \end{tikzcd}$$

# SQIsign - Challenge

Secret key: $I \subset \mathcal{O}_0$

Commitment: $J \subset \mathcal{O}_0$

Challenge: $\varphi : E_{com} \to E_{chal}$

$$
\begin{tikzcd}
E_0 \arrow[r, dotted] \arrow[d, dotted] & E_{pk} := E_I \arrow[d] \\
E_{com} := E_J & E_{chal}
\end{tikzcd}
$$

# SQIsign - Response

Secret key: $I \subset \mathcal{O}_0$

Commitment: $J \subset \mathcal{O}_0$

Challenge: $\varphi : E_{com} \to E_{chal}$

Find $h : I \to I'$ corresponding to $\varphi$

$$\begin{tikzcd}
E_0 \arrow[rr, dotted] \arrow[d, dotted] & & E_{pk} := E_I \arrow[d] \\
E_{com} := E_J & & E_{chal}
\end{tikzcd}$$

# SQIsign - Response

Secret key: $I \subset \mathcal{O}_0$

Commitment: $J \subset \mathcal{O}_0$

Challenge: $\varphi : E_{com} \to E_{chal}$

Find $h : I \to I'$ corresponding to $\varphi$

$$
\begin{tikzcd}
E_0 \arrow[r, dotted] \arrow[d, dotted] & E_{pk} := E_I \arrow[d] \\
E_{com} := E_J \arrow[r] & E_{chal}
\end{tikzcd}
$$

Compute some $h : J \to I'$, and translate to corresponding isogeny

# PRISM - Key Generation (Same as SQIsign)

Secret key: $I \subset \mathcal{O}_0$

$$E_0 \cdots\cdots\rightarrow E_{pk} := E_I$$

# PRISM - Signing

Secret key: $I \subset \mathcal{O}_0$

$$\begin{tikzcd} E_0 \arrow[r, dotted] & E_{pk} := E_I \arrow[d, "\sigma"] \\ & E_\sigma \end{tikzcd}$$

Hash message to a random prime q

Compute random $h : I \to I'$ with "degree" $q$

(Same as computing a $J \subset \mathcal{O}_R(I)$ left ideal)

Compute corresponding $\sigma$ with $\deg \sigma = q$

# Part II: Ideals to curves overview

# Direct translation

Given $I \subset \mathcal{O}_0$ find a "nice" homomorphism $h : I \to \mathcal{O}_0$

Index of $h(I)$ in $\mathcal{O}_0$ should be $2^{2e}$

Corresponds to finding $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$

Gives

$$h_\beta : I \to \mathcal{O}_0$$

$$h_\beta(x) = x\overline{\beta}/n(I)$$

# Solvable with KLPT (easy version)

Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$

From this point forward, we fix

$$\mathcal{O}_0 = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2},$$

with

$$i^2 = -1, j^2 = -p$$

# Solvable with KLPT (easy version)

Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$

Let $I = \mathcal{O}_0\langle N, \alpha\rangle$. Look for an element of the form $\beta = (a + ib)N + \lambda\alpha$

Recall $n(\alpha_1 + \alpha_2) = n(\alpha_1) + n(\alpha_2) + t(\alpha_1\bar{\alpha}_2)$

Write $\alpha = a_\alpha + b_\alpha i + c_\alpha j + d_\alpha k$

$$N^2(a^2 + b^2) + \lambda^2 n(\alpha) + 2N\lambda(aa_\alpha + bb_\alpha) = 2^e \cdot N$$

# Solvable with KLPT (easy version)

Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$

Let $I = \mathcal{O}_0\langle N, \alpha\rangle$. Look for an element of the form $\beta = (a + ib)N + \lambda\alpha$

$$N(a^2 + b^2) + \lambda^2 n(\alpha)/N + 2\lambda(aa_\alpha + bb_\alpha) = 2^e$$

# Solvable with KLPT (easy version)

Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$

Let $I = \mathcal{O}_0\langle N, \alpha\rangle$. Look for an element of the form $\beta = (a + ib)N + \lambda\alpha$

$$N(a^2 + b^2) + \lambda^2 n(\alpha)/N + 2\lambda(aa_\alpha + bb_\alpha) = 2^e$$

**Step 2:** Find $\alpha$ with $a_\alpha = b_\alpha = 0$

$$N(a^2 + b^2) + \lambda^2 n(\alpha)/N = 2^e$$

# Solvable with KLPT (easy version)

Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$

Let $I = \mathcal{O}_0\langle N, \alpha \rangle$. Look for an element of the form $\beta = (a + ib)N + \lambda\alpha$

$$N(a^2 + b^2) + \lambda^2 n(\alpha)/N + 2\lambda(aa_\alpha + bb_\alpha) = 2^e$$

**Step 2:** Find $\alpha$ with $a_\alpha = b_\alpha = 0$

$$N(a^2 + b^2) + \lambda^2 n(\alpha)/N = 2^e$$

**Step 3:** Solve for $\lambda$ mod $N$, then $a, b$ by Cornacchia

# Solvable with KLPT (easy version)

Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$

**Step 1:** Choose any $\gamma \in \mathcal{O}_0$ s.t. $n(\gamma) = 2^f \cdot N$

# Solvable with KLPT (easy version)

Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$

**Step 1:** Choose any $\gamma \in \mathcal{O}_0$ s.t. $n(\gamma) = 2^f \cdot N$

**Step 2:** Find $\alpha$ with $a_\alpha = b_\alpha = 0$, s.t. $\gamma\alpha \in I$

Let $I = \mathcal{O}_0\langle N, \gamma\alpha\rangle$. Look for an element of the form $\beta_0 = (a + ib)N + \lambda\alpha$

Such that $\beta = \gamma\beta_0$ is the desired output

$$N^2(a^2 + b^2) + \lambda^2 n(\alpha) = 2^{e-f}$$

# Solvable with KLPT (easy version)

Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$

**Step 1:** Choose any $\gamma \in \mathcal{O}_0$ s.t. $n(\gamma) = 2^f \cdot N$

**Step 2:** Find $\alpha$ with $a_\alpha = b_\alpha = 0$, s.t. $\gamma\alpha \in I$

Let $I = \mathcal{O}_0\langle N, \gamma\alpha\rangle$. Look for an element of the form $\beta_0 = (a + ib)N + \lambda\alpha$

Such that $\beta = \gamma\beta_0$ is the desired output

$$N^2(a^2 + b^2) + \lambda^2 n(\alpha) = 2^{e-f}$$

**Step 3:** Solve for $\lambda$ mod $N^2$, then $a, b$ by Cornacchia

# Solvable with KLPT (easy version)

The proper KLPT algorithm works for $2^e > p^3$

Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$

**Step 1:** Choose any $\gamma \in \mathcal{O}_0$ s.t. $n(\gamma) = 2^f \cdot N$

**Step 2:** Find $\alpha$ with $a_\alpha = b_\alpha = 0$, s.t. $\gamma\alpha \in I$

Let $I = \mathcal{O}_0\langle N, \gamma\alpha\rangle$. Look for an element of the form $\beta_0 = (a + ib)N + \lambda\alpha$

Such that $\beta = \gamma\beta_0$ is the desired output

$$N^2(a^2 + b^2) + \lambda^2 n(\alpha) = 2^{e-f}$$

**Step 3:** Solve for $\lambda$ mod $N^2$, then $a, b$ by Cornacchia

Output size: $N \approx 2^f \approx \sqrt{p}$, $n(\alpha) \approx pN^2 \approx p^2$, $\lambda^2 \approx N^4$, so works when $2^e > p^{4.5}$

# Clapoti (for quadratic or quaternion ideals)

$$\begin{tikzcd} F \arrow[r] & E \\ E \arrow[u] \arrow[r, "\varphi_{\beta_1}"] & E_I \arrow[u, swap, "-\widehat{\varphi_{\beta_2}}"] \end{tikzcd}$$

$$\Phi : \begin{tikzcd} E \arrow[r, "\varphi_{\beta_1}"] \arrow[dr] & E_I \\ E \arrow[ur, "\varphi_{\beta_2}"] \arrow[r] & F \end{tikzcd}$$

~~Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$~~

Given $I \subset \mathcal{O}_0$ find $\beta_1, \beta_2 \in I$ such that $n(\beta_1) + n(\beta_2) = 2^e \cdot n(I)$

$$
\begin{tikzcd}
F \arrow[rr] & & E_v \\
& & E \arrow[u, "\phi_v"'] \\
E_u \arrow[uu] & E \arrow[l, "\phi_u"'] \arrow[r, "\varphi_{\beta_1}"] & E_I \arrow[u, "\widehat{\varphi_{\beta_2}}"']
\end{tikzcd}
\qquad
\Phi : \begin{tikzcd}
E_u \arrow[r, "\phi_{\beta_2} \circ \widehat{\phi_u}"] \arrow[dr] & E_I \\
E_v \arrow[ur, "\phi_{\beta_1} \circ \widehat{\phi_v}"] \arrow[r] & F
\end{tikzcd}
$$

~~Given $I \subset \mathcal{O}_0$ find $\beta \in I$ such that $n(\beta) = 2^e \cdot n(I)$~~

~~Given $I \subset \mathcal{O}_0$ find $\beta_1, \beta_2 \in I$ such that $n(\beta_1) + n(\beta_2) = 2^e \cdot n(I)$~~

Given $I \subset \mathcal{O}_0$ find $\beta_1, \beta_2 \in I$ and $u, v \in \mathbb{Z}_{\geq 0}$, such that $u \cdot n(\beta_1) + v \cdot n(\beta_2) = 2^e \cdot n(I)$

# The norm equation

Given $I \subset \mathcal{O}_0$ find $\beta_1, \beta_2 \in I$ and $u, v \in \mathbb{Z}_{\geq 0}$,
such that $u \cdot n(\beta_1) + v \cdot n(\beta_2) = 2^e \cdot n(I)$

**Step 1:** Find the smallest $\beta_1, \beta_2 \in I$ of coprime norm

**Step 2:** Solve for $u, v$

# The norm equation

Given $I \subset \mathcal{O}_0$ find $\beta_1, \beta_2 \in I$ and $u, v \in \mathbb{Z}_{\geq 0}$,
such that $u \cdot n(\beta_1) + v \cdot n(\beta_2) = 2^e \cdot n(I)$

**Step 1:** Find the smallest $\beta_1, \beta_2 \in I$ of coprime norm

**Step 2:** Solve for $u, v$

Often a bit larger :(

Expected to find $n(\beta_1) \approx n(\beta_2) \approx p$,
and solution is guaranteed when $2^e > n(\beta_1)n(\beta_2)/n(I)^2$

Must be a few bits
smaller than $p$

# Clapoti Issues

The current way of solving the norm equation fails with non-negligible probability

# Clapoti Issues

**The current way of solving the norm equation fails with non-negligible probability**

Leads to a complicated rerandomisation procedure to bring failure probability down to $2^{-60}$

Still not negligible in security parameter leads to gap in security proof

# Clapoti Issues

**The current way of solving the norm equation fails with non-negligible probability**

Leads to a complicated rerandomisation procedure to bring failure probability down to $2^{-60}$

Still not negligible in security parameter leads to gap in security proof

**Random isogenies of degree $u$ and $v$: QFESTA, done by computing an isogeny in dimension 2.**

So currently, translating an ideal to curve requires one $(2^e, 2^e)$-isogeny and two $(2^f, 2^f)$-isogenies ($f \approx e/2$)

# Part III: Qlapoti-with-a-Q

# Clapoti (for quadratic or quaternion ideals)

$$\begin{tikzcd}[column sep=huge, row sep=large]
F \arrow[r] & E \\
E \arrow[u] \arrow[r, "\varphi_{\beta_1}"] & E_I \arrow[u, "-\widehat{\varphi_{\beta_2}}"']
\end{tikzcd}
\qquad
\Phi : \begin{tikzcd}[column sep=huge, row sep=large]
E \arrow[r, "\varphi_{\beta_1}"] \arrow[dr] & E_I \\
E \arrow[ur, "\varphi_{\beta_2}"] \arrow[r] & F
\end{tikzcd}$$

Given $I \subset \mathcal{O}_0$ find $\beta_1, \beta_2 \in I$ such that $n(\beta_1) + n(\beta_2) = 2^e \cdot n(I)$

# Idea: Solve equation directly

Given $I = \mathcal{O}_0\langle N, \alpha\rangle$ find $\beta_1, \beta_2 \in I$ such that $n(\beta_1) + n(\beta_2) = 2^e \cdot n(I)$

# Idea: Solve equation directly

Given $I = \mathcal{O}_0\langle N, \alpha\rangle$ find $\beta_1, \beta_2 \in I$ such that $n(\beta_1) + n(\beta_2) = 2^e \cdot n(I)$

Very easy algorithm that sort of works: Same as $u, v$ method, but restrict $u, v$ to be sums of squares

Failure probability goes from bad to worse...

# Idea: Solve equation directly

Given $I = \mathcal{O}_0\langle N, \alpha\rangle$ find $\beta_1, \beta_2 \in I$ such that $n(\beta_1) + n(\beta_2) = 2^e \cdot n(I)$

~~Very easy algorithm that sort of works: Same as $u, v$ method, but restrict $u, v$ to be sums of squares~~

~~Failure probability goes from bad to worse...~~

# Idea: Solve equation directly

Given $I = \mathcal{O}_0\langle N, \alpha\rangle$ find $\beta_1, \beta_2 \in I$ such that $n(\beta_1) + n(\beta_2) = 2^e \cdot n(I)$

Key: Look for $\beta_1 = (a_1 + ib_1) \cdot N + \alpha$

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

# Idea: Solve equation directly

Given $I = \mathcal{O}_0\langle N, \alpha\rangle$ find $\beta_1, \beta_2 \in I$ such that $n(\beta_1) + n(\beta_2) = 2^e \cdot n(I)$

Key: Look for $\beta_1 = (a_1 + ib_1) \cdot N + \alpha$

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

**Step 1:** Find short $A, B$ such that $2(a_\alpha A + b_\alpha B) \equiv 2^e - 2n(\alpha)/N \pmod{N}$

$$a_1^2 + b_1^2 + (A - a_1)^2 + (B - b_1)^2 = M$$

$$\frac{2^e - 2n(\alpha)/N - 2(a_\alpha A + b_\alpha B))}{N}$$

# Idea: Solve equation directly

Given $I = \mathcal{O}_0\langle N, \alpha \rangle$ find $\beta_1, \beta_2 \in I$ such that $n(\beta_1) + n(\beta_2) = 2^e \cdot n(I)$

Key: Look for $\beta_1 = (a_1 + ib_1) \cdot N + \alpha$

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

**Step 1:** Find short $A, B$ such that $2(a_\alpha A + b_\alpha B) \equiv 2^e - 2n(\alpha)/N \pmod{N}$

$$a_1^2 + b_1^2 + (A - a_1)^2 + (B - b_1)^2 = M$$

**Step 2:** Use Cornacchia to solve

$$(2a_1 - A)^2 + (2b_1 - B)^2 = 2M - A^2 - B^2$$

# Idea: Solve equation directly

Minkowski: $N < 2\sqrt{2p}/\pi$

Given $I = \mathcal{O}_0\langle N, \alpha\rangle$ find $\beta_1, \beta_2 \in I$ such that $n(\beta_1) + n(\beta_2) = 2^e \cdot n(I)$

Choose $n(\alpha)/N < 2^e$ (Not restrictive, expect to find $n(\alpha)/N \approx \sqrt{p}$)

Expect to find $A, B$ with $A \approx B \approx \sqrt{N}$

**Step 1:** Find short $A, B$ such that $2(a_\alpha A + b_\alpha B) \equiv 2^e - 2n(\alpha)/N \pmod{N}$

$$\frac{2^e - 2n(\alpha)/N - 2(a_\alpha A + b_\alpha B))}{N}$$

**Step 2:** Use Cornacchia to solve

$$(2a_1 - A)^2 + (2b_1 - B)^2 = 2M - A^2 - B^2$$

**So all we need is $A^2 + B^2 \lesssim 2^e/N$, and we try new $\alpha$ until this is satisfied**

# Failure probability for SQIsign parameters

| NIST level | $p$ | $c$ | $e$ | upper bound on failure rate |
|---|---|---|---|---|
| I | $2^{248} \cdot 5 - 1$ | 2185 | 246 | $2^{-197}$ |
| III | $2^{376} \cdot 65 - 1$ | 38495 | 374 | $2^{-312}$ |
| V | $2^{500} \cdot 27 - 1$ | 21484 | 498 | $2^{-438}$ |

**Table 3.** The final upper bound of the failure rate of Qlapoti applied to the SQIsign parameters.

# Results in SageMath

| NIST level | Previous work [5] | This work | Improvement |
|---|---|---|---|
| I | 0.415s | 0.160s | x2.595 |
| III | 0.768s | 0.346s | x2.222 |
| V | 1.060s | 0.467s | x2.269 |

**Table 5.** Timings comparing IdealToIsogeny using the technique currently used in SQIsign and the one presented in this work, given in wall-clock time. The final column represents the improvement factor.

# Results in SageMath

| Protocol | Algorithm | Previous work | This work | Improvement |
|---|---|---|---|---|
| SQIsign-LVLI | KeyGen | $0.489s$ | $0.249s$ | x1.961 |
| | Signing | 1.010s | 0.522s | x1.935 |
| PRISM-LVLI | KeyGen | $0.484s$ | 0.252s | x1.929 |
| | Signing | 0.593s | 0.322s | x1.673 |
| PRISM-LVL3 | KeyGen | 0.915s | 0.544s | x1.682 |
| | Signing | 1.328s | 0.808s | x1.644 |
| PRISM-LVL5 | KeyGen | 1.436s | 0.758s | x1.894 |
| | Signing | 2.017s | 1.426s | x1.415 |

**Table 6.** Preliminary benchmarks in SageMath to measure the impact of Qlapoti on the signature schemes SQIsign and PRISM. The comparison with PRISM is with the implementation from [5], while the comparison with SQIsign uses a preliminary proof-of-concept implementation privately shared by the authors.

# Results in C

Coming soon...

| NIST level | Previous work [10] | This work |
|---|---|---|
| I | $75,5$ KiB | $33,5$ KiB |
| III | $337$ KiB | $49,2$ KiB |
| V | $347$ KiB | $64,6$ KiB |

**Table 7.** Heap usage by a reference/Release build of the SQIsign NIST2 implementation with and without Qlapoti. Average over 10 runs. Measures were taken with the sqisign_test_scheme_lvl[x] executable for level x.

# qt-PEGASIS:

## Applying Qlapoti to PEGASIS

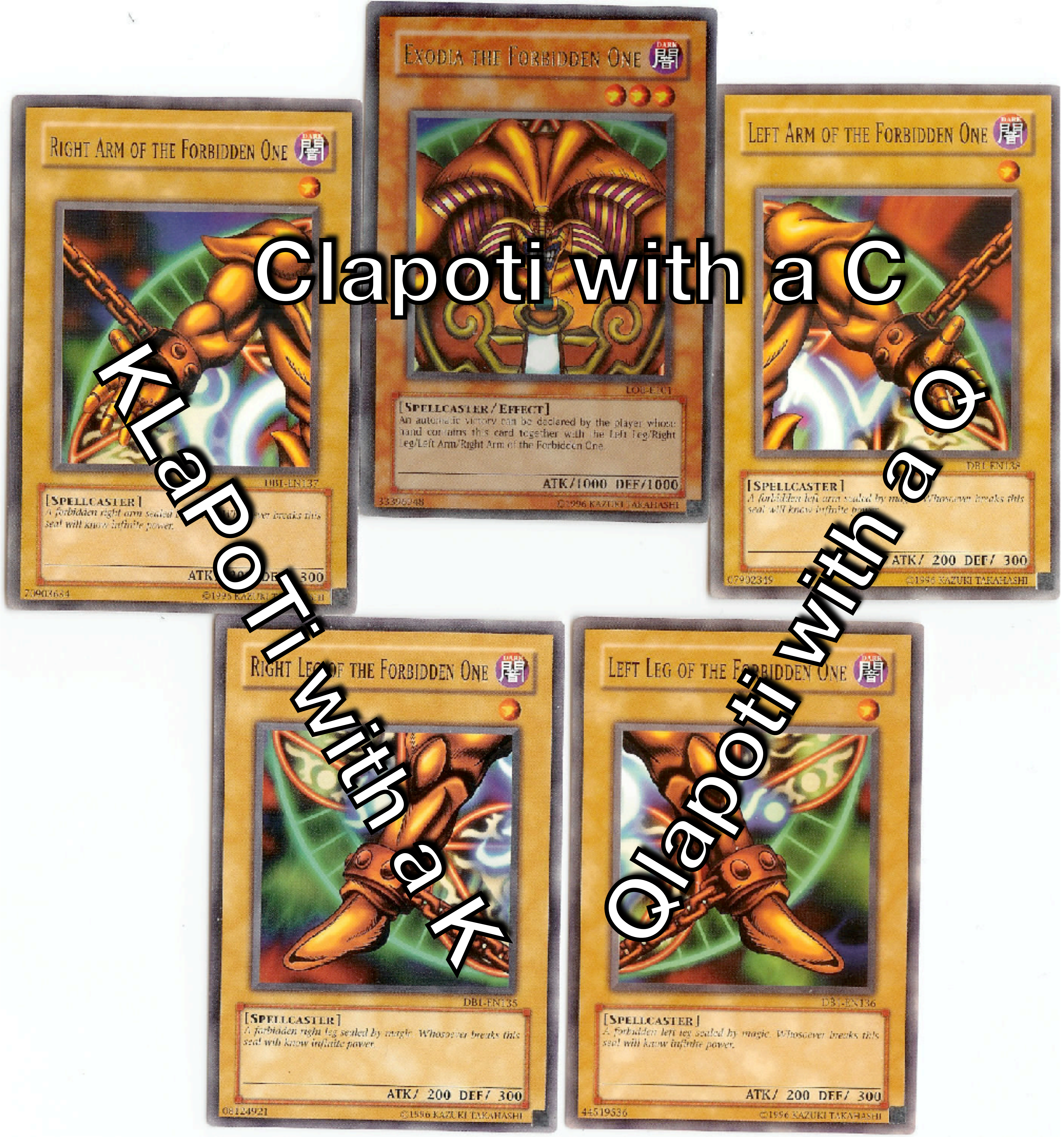
Joint work with Riccardo Invernizzi and Frederik Vercauteren

# PEGASIS

In the quadratic (oriented) setting, the best algorithm is also based on Clapoti

Given $I \subset \mathfrak{O}$ find $\beta_1, \beta_2 \in I$ and $u, v \in \mathbb{Z}_{\geq 0}$,
such that $u \cdot n(\beta_1) + v \cdot n(\beta_2) = 2^e \cdot n(I)$,
and such that $u, v$ can be written as sums of squares

**However, using the starting point of KLaPoTi, it turns out that we can really apply Qlapoti even in the oriented setting!**




# = qt-PEGASIS

Class group actions where essentially the whole cost at all security levels is a single 4-dimensional isogeny!