Biquaternion cryptography

Péter Kutas

30th April 2025

Outline

- KLPT in dimension 2 (joint work with Castryck, Decru, Laval, Petit and Ti) and consequences
- Orientations and Shimura class group actions (ongoing work with Castryck, Dina and Lorenzon) if time permits (but probably won't)
- Talk will focus mostly on the algebraic side and will present recent work, ongoing work and open problems
- Biquaternion algebra: tensor product of two quaternion algebras
- Over $\mathbb{Q}$ a biquaternion algebra is either $M_4(\mathbb{Q})$ or $M_2(B)$ where B is a quaternion algebra
- Many slides are "bonus slides" and are here just for completeness (i.e., don't get scared by the 31 slides)

Deuring correspondence

- Supersingular elliptic curves $\leftrightarrow$ Maximal orders in $B_{p,\infty}$ (this is usually a 2-1 correspondence)
- Isogenies $\leftrightarrow$ connecting ideals
- Degree of an isogeny $\leftrightarrow$ Norm of an ideal
- Everything starts here with understanding the structure of $Hom(E_1, E_2)$ which is a 4-dimensional Euclidean lattice of determinant p^2

Kohel-Lauter-Petit-Tignol

- The Deuring correspondence implies that that every algorithmic problem on the elliptic curve side has a quaternion counterpart
- Isogeny pathfinding problem: Given two supersingular elliptic curves find an isogeny of degree 2^k between them
- Quaternion pathfinding problem: Given two maximal orders find a connecting ideal of norm 2^k between them
- KLPT2014: Quaternion pathfinding problem can be solved in polynomial time
- Many crytpographic applications but in particular it means that given a maximal order one can compute a corresponding supersingular elliptic curve

Brief sketch of KLPT

- Computing any connecting ideal is easy, finding a smooth norm one is the hard part
- Equivalent ideal: I is equivalent to J if $J = I\beta$ for some $\beta \in B_{p,\infty}$
- One computes one ideal I of norm N and then tries to find an equivalent smooth norm one $\leftrightarrow$ finding an element $z \in I$ such that $N(z) = Nl^n$
- Ideal I can be generated by σ, N. The idea is to first solve the problem modulo N and then try to lift the lift the solution (this is called Strong Approximation) to an element of norm l^k

Dimension 2

- What about dimension two Abelian varieties?
- The natural analogue of supersingular curves is going to be superspecial Abelian surfaces which are isomorphic to the product of two supersingular elliptic curves
- Problem 1: Only 1 superspecial surface up to isomorphism
- Solution: You have to view surfaces together with a principal polarization
- How does this translate to the algebra side?

Dimension 2, the algebra side

- Endomorphism rings of superspecial surfaces are maximal orders in $M_2(B_{p,\infty})$
- Problem 1: There is only one maximal order up to isomorphism
- Solution: You have to incorporate principal polarizations
- Ibukiyama, Katsura, Oort: Since every superspecial surface comes from a different principal polarization of $E \times E$, one can associate a 2×2 matrix to every surface
- Fix E^2 together with the product polarization σ_0 and then associate a different principal polarization σ_1 the map $\sigma_1^{-1}\sigma_0$ which is an endomorphism of E^2.

Dimension 2, the algebra side II

- This matrix is going to be quite special and actually of the following form:

$$\begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}$$

  where $End(E) = O$, $r \in O$ and $s, t > 0$ are integers.
- This comes from the fact that $M_2(O)$ has the conjugate transpose as a totally positive involution and the above matrix will be symmetric with respect to that involution
- To get a proper correspondence we need an equivalence relation as polarizations can be composed with automorphisms
- Matrices g_1 and g_2 are equivalent if there exists $u \in GL_2(O)$ such that $g_2 = u^* g_1 u$
- How do you bring isogenies into the picture?

Algebraic polarized isogenies

- Polarized isogenies between g_1, g_2 will correspond to matrices $\gamma \in M_2(O)$ such that $\gamma^* g_2 \gamma = N g_1$

Problem

Given two matrices g_1, g_2 *find* $\gamma \in M_2(O)$ *such that* $\gamma^* g_2 \gamma = 2^k g_1$

- Main result: There exists a polynomial-time algorithm for the above problem with $2^k < p^{25}$
- Note that matrices g could apriori have big coefficients yet the output length of our algorithm only depends on p and not the coefficients of the g_i

Algebraic pathfinding I

- Let $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(O)$. Let
  $\mathcal{N}(u) = N(a)N(d) + N(b)N(c) - Tr(\bar{a}b\bar{d}c)$
- $\mathcal{N}(u)$ is actually the reduced norm of u (reduced norm is multiplicative!)
- $u^{-1}\mathcal{N}(u) \in M_2(O)$

Lemma

Assume that $\delta^* g_1 \delta = N u^* g_2 u$ where $N \in \mathbb{Z}^+$, $u, \delta \in M_2(O)$. Then there exists $\gamma \in M_2(O)$ such that $\gamma^* g_1 \gamma = N\mathcal{N}(u)^2 g_2$.

- This generalizes the equivalence relation and provides more flexibility

Algebraic pathfinding II

Lemma

Let $g_1 = \begin{pmatrix} D & r_1 \\ \bar{r}_1 & u \end{pmatrix}$ *and* $g_2 = \begin{pmatrix} D & r_2 \\ \bar{r}_2 & v \end{pmatrix}$ *such that* $Du - N(r_1) = Dv - N(r_2)$ *where* $D, u, v \in \mathbb{Z}$ *and* $r_1, r_2 \in O$. *Then there exists* $\gamma \in M_2(O)$ *such that*

$$\gamma^* g_1 \gamma = D^2 g_2$$

Proof.

Take $\gamma = \begin{pmatrix} D & r_2 - r_1 \\ 0 & D \end{pmatrix}$ □

Algebraic pathfinding III

- Goal: find u_1, u_2 such that the top left corner of $u_1^* g_1 u_1$ is the same as the top left corner of $u_2^* g_2 u_2$ and is a power of 2
- Problem 1: you have to ensure that $\mathcal{N}(u_1) = \mathcal{N}(u_2) = 2^k$
- You also need bounds on the powers of 2 that do not depend on g_1 and g_2
- Note that this reduces the pathfinding problem to a transformation problem
- What does the top left corner look like after conjugation with u?

Algebraic pathfinding IV

- If $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $g = \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}$, then the top left corner of $u^* g u$ is

$$s' := s \cdot N(a) + t \cdot N(c) + \mathrm{Tr}(\bar{c}\bar{r}a)$$

- Observation 1: This does not depend on b, d!
- Observation 2: This a quadratic form in 8 variables, or one can also look at it as O^2 together with a quadratic module structure $Q(a, c)$
- Interesting fact: The determinant of this quadratic form is p^4 (if $st - N(r) = 1$, in general it is $p^4(st - N(r))^4$) so in particular it does not depend on s, t, r! Furthermore, the form is positive definite.

Algebraic pathfinding V

- Solving $Q(a, c) = A$ where $A \in \mathbb{Z}^+$ can be done efficiently assuming some technical conditions and provided A is big enough
- Problem: Bound will depend on s, t
- Solution: Run LLL and find u_0 such that the top left corner of $u_0^* g u_0$ is smaller than $\sqrt{p}$
- This will only ensure that s is small but using one more step one get every coefficient of the new g to be bounded
- What remains? At every step we only work with a, c and now we have to ensure that we can find a suitable b, d such that $\mathcal{N}(u)$ is a fixed power of 2 whose size is bounded in terms of p

Algebraic pathfinding VI

- Controlling the reduced norm means that given a, c we need to find b, d such that $N(a)N(d) + N(b)N(c) - Tr(\bar{a}b\bar{d}c)$ is a fixed power of 2.
- Assume that $N(a)$ and $N(c)$ are coprime and look at the quadratic form

$$Q(x, y) = N(a)N(y) + N(x)N(c) - Tr(\bar{a}x\bar{y}c)$$

- Instead of starting to write down Diophantine equations we stop and think about what this is algebraically
- O^2 can be viewed with Q as a quadratic right O-module. The submodule $M_1 = (a, c)O$ is going to be the radical, i.e a submodule whose elements are orthogonal to everyone
- Goal: Try to find a right submodule M_2 such that $M_1 \oplus M_2 = O^2$

Algebraic pathfinding VII

- The tactic for finding M_2 is going to be to find a vector w that is $B_{p,\infty}$-independent from (a, c) and look for $M_2 = wB_{p,\infty} \cap O^2$.
- For every such choice M_2 is a right O-module whose intersection with M_1 is trivial, however there is only one choice to ensure that M_1 and M_2 generate O^2
- Let α, β be such that $\alpha N(a) + \beta N(c) = 1$
- $w = (\beta N(c)a, -\alpha N(a)c)$ is going to be an appropriate choice (it is enough to show that together with (a, c) they generate $(1, 0)$ and $(0, 1)$)

Algebraic pathfinding VIII

- What is M_2? Use the duck method (if it quacks like a duck, waddles like a duck, then it has to be a duck)!
- M_2 is going to be an invertible right O-module (i.e., locally free of rank 1)
- It has two elements of coprime norm , namely $(\beta N(c), -\alpha c\bar{a}), (\beta a\bar{c}, -\alpha N(a)) \in M_2$ which actually generate it
- It has to be a $Hom(E, E_1)$
- Actually one has the following formula:

$$Q((\beta N(c), -\alpha c\bar{a})o_1 + (\beta a\bar{c}, -\alpha N(a))o_2) = 1/N(c)N(N(c)o_1 + a\bar{c}o_2).$$

- This formula actually gives a module isomorphism between M_2 and the right ideal generated by $N(c)$ and $a\bar{c}$ which is a $N(c)$ homothethy between quadratic modules. Why do we care about this?

Algebraic pathfinding IX

- The above formula tells me that if I find an element of norm $N(c)N$ in the ideal generated by $N(c)$ and $a\bar{c}$ (an ideal of norm $N(c)$), then I find an element of norm N in M_2
- Hence I onleed need to find an element of norm $N(c)2^k$ in the aforementioned ideal. But how do I do that? Use 1-dim KLPT!
- Since we use O as the nicest maximal order possible KLPT will give as a power of 2 smaller than p^3
- The terrible bound comes from the reduction step and solving the previous norm equation

Potential improvements

- Let's get back to the quadratic form

$$s \cdot N(a) + t \cdot N(c) + \mathrm{Tr}(\bar{c}\bar{r}a)$$

- This is again O^2 with a quadratic module structure
- Would be great to find an equivalent matrix where s, t are small (right now we move out of the equivalence class)
- Even nicer would be to solve

$$s \cdot N(a) + t \cdot N(c) + \mathrm{Tr}(\bar{c}\bar{r}a) = l^k$$

directly where the bound does not depend on s, t

Applications

- Efficient endomorphism ring to surface translation (2-dim ideal to isogeny algorithm)
- Breaking 2-dimensional generalizations of the CGL hash function without trusted setup
- This break involves an isogeny to matrix algorithm which requires solving solving a principal ideal problem in left ideals of $M_2(O)$
- For a chain of (I, I)-isogenies this can be avoided by using a polynomial-time precomputation computing γ matrices for every possible rank 2 kernel (note that in dimension 2, every surface is just E^2 with a different principal polarization)
- Alternatively one can also solve it using algorithms for the principal ideal problem

Speculations on 2-dimensional SQIsign

- KLPT^2 naturally avoids going through a special surface (conjecturally) so SQIsign can be built from it but problems arise
- Paths are too long, so it is not yet clear how to make it practical (very interesting open problem!)
- ZK knowledge assumption needs to be studied
- What about generalizations of SQIsignHD?

Speculations on 2-dimensional SQIsign

- Non-smooth degree matrices can be returned which are much smaller but they go through a special surface
- In theory a (reduced) degree $\approx p$ isogeny should be possible but finding it is not obvious
- Polarized isogenies do not form a lattice, so one can't find the shortest polarized isogeny with lattice reduction
- Interesting to pursue this direction as well as endomorphism ring computation in dimension 2 has $O(p)$ complexity (by recent survey from Anni, Bisson, Garcia, Iezzi, Wesolowski citing Costello-Smith algorithm)

Alternative description of IKO

- IKO paradigm does not seem like the natural generalization of the Deuring correspondence
- One way is to look at totally positive involutions on $M_2(O)$
- Another more natural way is to look at maximal orders together with a totally positive involution (here isogenies will correspond to certain kind of conjugations)
- One can algorithmically navigate between them using the principal ideal problem

Endomorphism ring problems

- Given a surface find a basis of the endomorphism ring
- Given a surface find the corresponding g matrix
- Algorithmically equivalent:
- one finds an isomorphism between the endomorphism algebra and $M_2(B_{p,\infty})$
- Explicit conjugation to $M_2(O)$ using the principal ideal problem
- The g matrix can be read of from the Rosati involution using linear algebra

Group actions

- What other things are posisble with biquaternions?
- One can generalize class group actions to dimension 2 but one has to account for polarizations
- One can view every maximal order as $M_2(O)$ (where $End(E) \cong O$) together with the Rosati involution given by $\sigma(x) = g^{-1}\overline{x}^T g$
- Instead of the class group one can use the Shimura class group of CM orders

Orientations

- Shimura class group actions are in characteristic 0 and they generalize easily to ordinary abelian surfaces. What can we do with superspecial surfaces?
- Orientations are **NOT** just an embedding of a CM order in the endomorphism ring
- Take the endomorphism ring together with the involution. An orientation is a CM order in the endomorphism ring where the involution σ acts as complex conjugation
- Simply put: one has $Z[a, b]$ as a subring where a is real and $\sigma(a) = a$ and $ab = ba$

Ongoing work

- We can create orientations and show that these group actions are free
- Orbits are very interesting and depend on something called CM types which you don't really see in postive characteristic
- One can efficiently compute them á la SCALLOP-HD
- Many open problems still arise

Conclusion

- Biquaternion cryptography poses many open questions
- Does everything we know from the quaternion world generalize to higher dimensions?
- Will there be applications that will outperform 1-dimensional counterparts (e.g., a recent 3-dimensional hash function significantly outperforms CGL)

Orientations II

- Find a symmetric element a
- Compute the centralizer of a in $M_2(B_{p,\infty})$ which will be the quaternion algebra $\mathbb{Q}(a) \otimes B_{p,\infty}$ by the double centralizer theorem
- If one intersects it with the original maximal order, one can prove that σ will act as quaternion conjugation on this quaternion algebra (σ will be a standard involution)
- Just take a quadratic order

Orientations III

- Through lifting to characteristic 0, this will provide a free and transitive group action
- One still has to translate the orientation
- This can be done through interpolation data (like SCALLOP-HD)
- Drawback: one needs 8-dimensional isogenies

Orientations III

- Gives rise to an order embedding problem which can be solved in the smallish cases using lattice reduction details on the board
- Frobenius is not great as it does not generate a CM order almost always. There is a group action of the class group of $\mathbb{Z}[\sqrt{-p}]$ which still provides interesting questions
- Several open questions in terms of security and efficiency