Current trends and challenges in post-quantum cryptography

Steven Galbraith

University of Auckland, New Zealand

Thanks

- Eric Bach, Joshua Holden, Jen Paulhus, Andrew Shallue, Renate Scheidler, Jonathan Sorenson.
- Hilary Heffley.
- David Kohel, Bryan Birch, Victor Miller, Florian Hess, Nigel Smart, Alfred Menezes, Scott Vanstone, David Jao, Drew Sutherland, Gaetan Bisson, Christophe Petit, Luca de Feo.
- Anton Stolbunov, Ilya Chevyrev, Chang-An Zhao, Fangqian (Alice) Qiu, Christina Delfs, Barak Shani, Yan Bo Ti, Javier Silva, Joel Laity.
- Thanks to you for waking up after the banquet.

Plan

- Post-quantum cryptography and the NIST “process”
- Computational problems from isogenies
- Crypto based on group actions/homogeneous spaces
- Crypto based on homomorphisms with co-prime kernels
- Open problems

Intended audience: experts in elliptic curves who don’t know much crypto.

Goal: Convince you to work on PQ Crypto and isogenies.

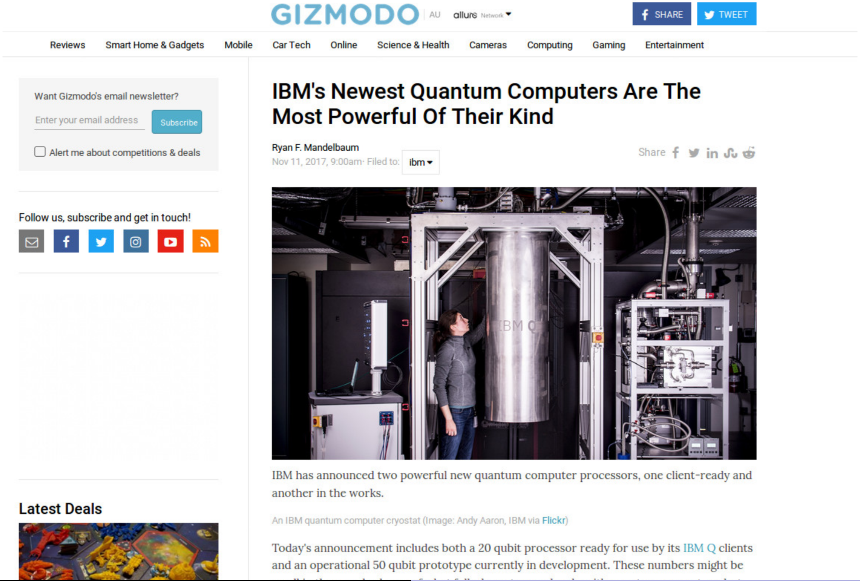
*** Footnotes are corrections added after the talk. ***

Quantum Computing

- Quantum computing was proposed by: Paul Benioff (1980), Yuri Manin (1980), Richard Feynman (1982) and David Deutsch (1985). [wikipedia]
- Peter Shor (1994): polynomial-time quantum algorithm for integer factorisation and discrete logs.
- Late 1990s: Breakthrough in quantum computing around "10 years away".
- Dave Wecker (Microsoft) invited talk at PQ Crypto 2018: Microsoft will have a quantum computer suitable for chemistry applications within 5 years and "something of interest to this crowd" in 10 years.

Quantum computer or microbrewery?

Quantum computer or microbrewery?



IBM's Newest Quantum Computers Are The Most Powerful Of Their Kind

Ryan F. Mandelbaum
Nov 11, 2017, 9:00am· Filed to: ibm

IBM has announced two powerful new quantum computer processors, one client-ready and another in the works.

An IBM quantum computer cryostat (Image: Andy Aaron, IBM via Flickr)

Today's announcement includes both a 20 qubit processor ready for use by its IBM Q clients and an operational 50 qubit prototype currently in development. These numbers might be

Interesting quantum computer algorithms for number theory

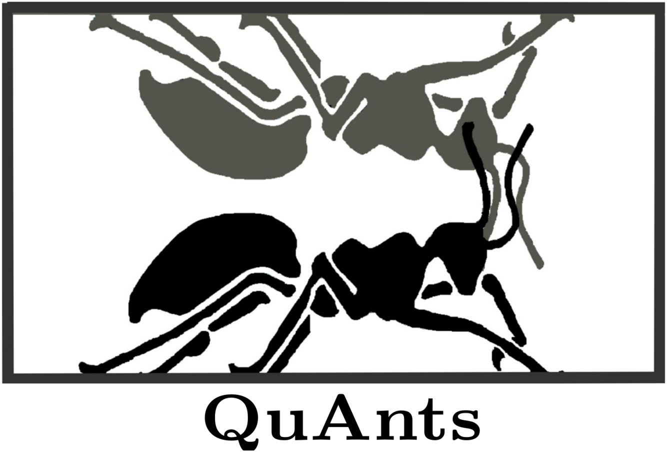
- Integer factoring record by Shor's algorithm on a quantum computer is 21.

  The integer 56153 has been factored using an "adiabatic quantum computer".
- Computing class group and unit group structure, generators for principal ideals etc.

  Nice survey: Childs and van Dam "Quantum algorithms for algebraic problems" (2010).
- Given p and $f(x) = (\frac{x+s}{p})$ to compute s.

  Efficient quantum algorithm due to van Dam, Hallgren and Ip.
- What else will quantum computers do for Algorithmic Number Theory?

QUANTS



NIST standardisation process

- August 2015: NSA Information Assurance Directorate proposed “a transition to quantum resistant algorithms in the not too distant future”.
- February 2016: NIST preliminary announcement of standardization plan.
- December 2016: Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms
- November 2017: Submission deadline
- April 2018: First NIST PQC Standardisation Conference
- Mid-late 2019: Selections to the second round
- Draft standards expected around 2023-2025

NIST submissions

- 69 submissions accepted, 5 withdrawn already.
- Roughly $\frac{2}{3}$ are key exchange/public key encryption schemes, and roughly $\frac{1}{3}$ are public key signatures.
- Mathematical foundation: Lattices, coding-theory, multivariate polynomial systems, hash trees, non-abelian groups, isogenies.
- Each offers different tradeoff between speed, key sizes, ciphertext/signature size, etc.
- This talk is not giving an overview of the whole field. I'm focussing on isogenies.

Lattice crypto

- Pros: Lattice crypto gives good solutions to both encryption and signatures, plus fancy gadgets like IBE and homomorphic encryption.
- Generally fast.
- Cons: may have large public keys/ciphertexts/signatures.[1]
- Problem: Estimating lattice attacks (basis reduction/enumeration/sieving) and choosing key sizes.
- Mersenne prime cryptosystem: A great target for cryptanalysis. (Aggarwal, Joux, Prakash, Santha, CRYPTO 2018)

[1] Someone on twitter disagrees with this statement.

Discrete Logarithm Problem and Diffie-Hellman

(Pre-quantum crypto)
Let G be a subgroup of $\mathbb{F}_q^*$ or $E(\mathbb{F}_q)$ of prime order p.
Given $g \in G$ and $h = g^a$ for $a \in \mathbb{Z}$, it is hard to compute a.

Diffie-Hellman key exchange:

- Alice chooses a and sends $t_A = g^a$ to Bob.
- Bob chooses b and sends $t_B = g^b$ to Alice.
- Alice computes $t_B^a = g^{ab}$.
- Bob computes $t_A^b = g^{ab}$.

Diffie-Hellman key exchange

$$\begin{tikzcd}
 & g^a \arrow[dr] & \\
g \arrow[ur] \arrow[dr] & & g^{ab} \\
 & g^b \arrow[ur] &
\end{tikzcd}$$

Generalised Discrete Logarithm Problem 1: Homogenous Spaces

(Couveignes 1997)
Let G be a subgroup of $\mathbb{F}_q^*$ or $E(\mathbb{F}_q)$ of prime order p.
For $a \in \mathbb{Z}_p$ and $g \in G$ define $a * g := g^a$.
Given $g \in G$ and $h = a * g$, hard to compute a.

Generalised Diffie-Hellman key exchange:

- Alice chooses $a \in \mathbb{Z}_p$ and sends $t_A = a * g$ to Bob.
- Bob chooses $b \in \mathbb{Z}_p$ and sends $t_B = b * g$ to Alice.
- Alice computes $a * t_B$.
- Bob computes $b * t_A$.

Generalised Discrete Logarithm Problem 2: Group homomorphisms

Let G be a subgroup of $\mathbb{F}_q^*$ or $E(\mathbb{F}_q)$ of prime order p.
Let $\phi : G \to G$. Given $g \in G$ and $h = \phi(g)$, hard to compute the group homomorphism ϕ.

Generalised Diffie-Hellman key exchange:

- Alice chooses ϕ_A and sends $t_A = \phi_A(g)$ to Bob.
- Bob chooses ϕ_B and sends $t_B = \phi_B(g)$ to Alice.
- Alice computes $\phi_A(t_B)$.
- Bob computes $\phi_B(t_A)$.

We can compose these homomorphisms, and they commute: $\phi_A(\phi_B(g)) = \phi_B(\phi_A(g))$.

Isogenies

- An **isogeny** $\phi : E_1 \to E_2$ of elliptic curves is a (non-constant) morphism and a group homomorphism.
- An isogeny has finite kernel.
- Given a finite subgroup $G \subseteq E_1(\overline{\mathbb{F}}_q)$ there is a (unique separable) isogeny $\phi_G : E_1 \to E_2$ with kernel G.
  Can compute ϕ_G using Vélu.
- We will write $E_2 = E_1/G$.
- We focus on separable isogenies, in which case $\deg(\phi) = \#\ker(\phi)$.
- $\mathrm{End}(E) = \{\text{isogenies } \phi : E \to E \text{ over } \overline{\mathbb{F}}_q\} \cup \{0\}$.

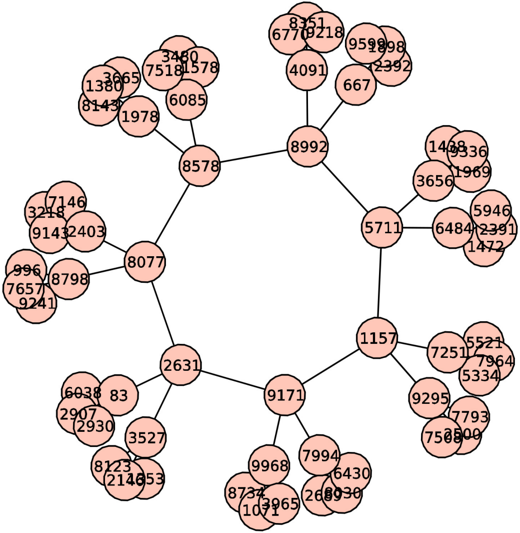
Main Computational Problem Regarding Isogenies

Given E_1, E_2 elliptic curves over $\mathbb{F}_q$ such that there is an isogeny between them (i.e., $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$), find an isogeny $\phi : E_1 \to E_2$.

Issues:

- Unique?
- Representation?
- Size?
- Algorithms?
- Classical or Quantum algorithms?

Ordinary Isogeny Graph



Credit: Dustin Moody

Abelian group action

(Kohel 1996, Couveignes 1997, Rostovtsev-Stolbunov 2006, Stolbunov 2010)

- Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with $\mathrm{End}(E) \cong \mathcal{O}$ an order in an imaginary quadratic field.
- Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal.
- Can define the subgroup

  $$E[\mathfrak{a}] = \{P \in E(\overline{\mathbb{F}}_q) : \phi(P) = 0 \ \forall \phi \in \mathfrak{a}\}.$$

  (Waterhouse 1969)
- There is an isogeny $E \to E'$ with kernel $E[\mathfrak{a}]$. Define $\mathfrak{a} * E$ to be $E' = E/E[\mathfrak{a}]$.
- $\mathfrak{a} * E$ depends only on the ideal class of $\mathfrak{a}$.
- This gives an action of ideal class group $\mathrm{Cl}(\mathcal{O})$ on set of E with $\mathrm{End}(E) \cong \mathcal{O}$.

Cryptography from Abelian group actions

- Couveignes describes a Diffie-Hellman-type key exchange based on group actions.
  He also sketched two interactive authentication protocols.
- Rostovtsev and Stolbunov give key exchange and encryption.
- Stolbunov's thesis describes an interactive authentication protocol and mentions signatures.
- Couveignes does not mention post-quantum security.
- Stolbunov (Advances Math. Comm. 2010) discusses quantum algorithms.[2]
  "Besides being interesting from the theoretical point of view, the proposed cryptographic schemes might also have an advantage against quantum computer attacks."

[2] Also eprint 2006/145 suggests isogenies could be post-quantum secure.

Generalised Diffie-Hellman 1: Group action

$$\begin{tikzcd}
 & \mathfrak{a} * E \arrow[dr] & \\
E \arrow[ur] \arrow[dr] & & \mathfrak{a}\mathfrak{b} * E \\
 & \mathfrak{b} * E \arrow[ur] &
\end{tikzcd}$$

Computational problems and algorithms

- Given E and $E' = \mathfrak{a} * E$ to determine the ideal (class) $\mathfrak{a}$.
- Classical algorithms due to Galbraith and Galbraith-Hess-Smart in time $\tilde{O}(\sqrt{\#G})$ (bug fixed by Stolbunov).
- Hidden shift problem: G an abelian group and $f, g : G \to S$ such that, for some $s \in G$, $g(x) = f(xs)$ for all $x \in G$. Problem: find s.
- Idea: Given $(E, E' = \mathfrak{a} * E)$ define $f(\mathfrak{b}) = \mathfrak{b} * E$ and $g(\mathfrak{b}) = \mathfrak{b} * E' = f(\mathfrak{b}\mathfrak{a})$.

Quantum algorithms for hidden shift

- Kuperberg (2004, 2011) gave subexponential-time quantum algorithms for hidden shift. Complexity[3] $2^{O(\sqrt{\log(\#G)})}$.
- Require massive quantum storage, which may be unrealistic.
- Regev (2004) gave low quantum storage variant.

[3] This is taking cost $O(1)$ for the functions f and g.

Kuperberg for isogenies

- Childs, Jao and Soukharev were the first to analyse Kuperberg's algorithm in the isogeny setting.
- Subexponential complexity arises twice in their work:
  - Computing $\mathfrak{a} * E$ requires smoothing the ideal class over a factor base.[4]
  - Kuperberg itself.
- Bonnetain and Schrottenloher, "Quantum Security Analysis of CSIDH and Ordinary Isogeny-based Schemes", eprint 2018/537.

  Gives more efficient action $\mathfrak{a} * E$ and gives variant of Kuperberg with heuristic running time[5] $\tilde{O}(2^{\sqrt{\log(\#G)}})$.
- Also see Biasse, Iezzi and Jacobson, "A note on the security of CSIDH", arXiv:1806.03656.

[4] This step improved by Biasse, Fieker and Jacobson in ANTS 2016.

[5] Again, taking cost $O(1)$ for $\mathfrak{a} * E$.

Open problems

- The Kuperberg and Regev algorithms mostly classical and combinatorial.

  Very like the Blum-Kalai-Wasserman (BKW) and Wagner algorithms.
- Regev ("Quantum computation and lattice problems", SIAM J. Comput. 2004) reduces shortest vector problem in lattice to dihedral hidden subgroup.

  Conversely, should be able to improve Kuperberg by using lattice methods.
- Algorithmic number theorists should study these algorithms.
- Kuperberg/Regev has only been used as a black box. Are there further optimisations/approaches/algorithms that exploit the specific features of isogenies?

Efficient computation of DH protocol

- Need to sample ideal class as product of powers of small prime ideals:
$$\mathfrak{a} \equiv \prod_i \mathfrak{l}_i^{e_i}$$
where $\mathfrak{l}_i$ are non-principal $\mathcal{O}$-ideals of small prime norm.
- Then need to compute corresponding isogenies.
- Couveignes and Stolbunov do this by just choosing random small "Elkies primes", using modular polynomials and action of Frobenius on kernels.
- Couveignes: time required "a few hours".
- Stolbunov: compute $\mathfrak{a} * E$ in 4 minutes or so.
- De Feo, Kieffer and Smith (eprint 2018/485) discuss choosing a special curve to make the isogeny computations faster.

CSIDH (Castryck, Lange, Martindale, Panny, Renes 2018)

- Let X be the set of isomorphism classes of supersingular elliptic curves E with j-invariant in $\mathbb{F}_p$.
- All $E \in X$ have $\mathrm{End}_{\mathbb{F}_p}(E)$ an order in $\mathbb{Q}(\sqrt{-p})$.
  Here $\mathrm{End}_{\mathbb{F}_p}(E) = \{\phi : E \to E \text{ defined over } \mathbb{F}_p\}$.
- Delfs-Galbraith showed that one can define class group actions on X.
- CSIDH is an instantiation of group action crypto using supersingular curves, which gives **massive** performance improvements.
- Advantages over SIDH (see later in talk) include:
  - No public key validation needed, so can do non-interactive key exchange.
  - Better bandwidth.
- Still only sub-exponentially quantum secure due to hidden shift algorithms.

Open problems

- How close to uniform is the distribution

$$\mathfrak{a} \equiv \prod_i \mathfrak{l}_i^{e_i}$$

  over uniform $e_i \in [-B, B]$, for fixed small prime ideals $\mathfrak{l}_i$? (Let's assume $\{\mathfrak{l}_i\}$ generates the class group.)
- Can small prime factors of $\#\mathrm{Cl}(\mathcal{O})$ be determined? Can subgroups of ideal class group be exploited?
- (Boneh): Find other homogeneous spaces/torsors for group actions that are efficient and secure for crypto.

Candidate post-quantum pairing

Very new paper by Boneh, Glass, Krashen, Lauter, Sharif, Silverberg, Tibouchi and Zhandry (eprint 2018/665).

- Fix ordinary $E/\mathbb{F}_q$
- Fact: $(\mathfrak{a}_1 * E) \times (\mathfrak{a}_2 * E) \cong (\mathfrak{a}_1\mathfrak{a}_2 * E) \times E$ as unpolarized abelian varieties.
  (Result holds more generally for n terms; see Kani 2011.)
- This is essentially a bilinar pairing (resp. multilinear map). Note: Not used for key exchange, but other more complex protocols.
- **Open problem:** To find a computable invariant of the isomorphism class.

Generalised Diffie-Hellman 2: Endomorphisms

Fix an element g in a group G.

$$\begin{tikzcd}
 & \phi_A(g) \arrow[dr] & \\
g \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & \phi_A(\phi_B(g)) \\
 & \phi_B(g) \arrow[ur] &
\end{tikzcd}$$

The maps $\phi_A(x) = x^a$ and $\phi_B(x) = x^b$ are group homomorphisms such that $\phi_A \circ \phi_B = \phi_B \circ \phi_A$.

Generalised Diffie-Hellman 2: Homomorphisms

Let E be an elliptic curve and G_A, G_B finite subgroups such that $G_A \cap G_B = \{0\}$.

$$\begin{tikzcd}
 & E_A = E/G_A \arrow[dr] & \\
E \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E/\langle G_A, G_B \rangle \\
 & E_B = E/G_B \arrow[ur] &
\end{tikzcd}$$

Alice and Bob need to give each other enough information that they can compute $\phi_A(G_B)$ and $\phi_B(G_A)$.
Alice computes $E_B/\phi_B(G_A)$ and Bob computes $E_A/\phi_A(G_B)$.

Why supersingular?

- The endomorphism ring of a supersingular elliptic curve is a maximal order in a quaternion algebra.
- The set of (approx $p/12$) supersingular elliptic curves in characteristic p is not a homogeneous space for a group action.
- Hence can hope to avoid subexponential attacks, such as based on Kuperberg's algorithm.

Jao and De Feo key exchange

- Let $p = \ell_1^{e_1} \ell_2^{e_2} f \pm 1$ be prime.
- Let E over $\mathbb{F}_{p^2}$ be a supersingular elliptic curve.
- Then group structure of $E(\mathbb{F}_{p^2})$ is a product of two cyclic groups of order $\ell_1^{e_1} \ell_2^{e_2} f$.
- Fix points $R_1, S_1 \in E[\ell_1^{e_1}]$ such that $\langle R_1, S_1 \rangle = E[\ell_1^{e_1}]$.
- Fix R_2, S_2 such that $\langle R_2, S_2 \rangle = E[\ell_2^{e_2}]$.
- The **system parameters** are (E, R_1, S_1, R_2, S_2).

Jao and De Feo key exchange

- Alice chooses a secret subgroup of $E[\ell_1^{e_1}]$ by choosing an integer $0 \leq a < \ell_1^{e_1}$ and setting $T_1 = R_1 + [a]S_1$.
- Alice computes an isogeny $\phi_A : E \to E_A$ with kernel generated by T_1 and publishes $(E_A, \phi_A(R_2), \phi_A(S_2))$.
- Bob chooses $0 \leq b < \ell_2^{e_2}$, computes $\phi_B : E \to E_B$ with kernel generated by $T_2 = R_2 + [b]S_2$ and publishes $(E_B, \phi_B(R_1), \phi_B(S_1))$.
- Alice computes

  $$T_1' = \phi_B(R_1) + [a]\phi_B(S_1) = \phi_B(R_1 + [a]S_1) = \phi_B(T_1)$$

  and then computes an isogeny $\phi_A' : E_B \to E_{AB}$ with kernel generated by T_1'.
- Bob computes an isogeny $\phi_B' : E_A \to E_{AB}'$ with kernel $\langle \phi_A(R_2) + [b]\phi_A(S_2) \rangle$.

Jao and De Feo key exchange

- The composition $\phi'_A \circ \phi_B : E \to E_{AB}$ has kernel $\langle T_1, T_2 \rangle$.
- The elliptic curve equations E_{AB} and E'_{AB} computed by Alice and Bob are isomorphic.
- The shared key for Alice and Bob is $j(E_{AB}) = j(E'_{AB})$.
- Can use for encryption, but need to avoid an active attack due to Galbraith, Petit, Shani, Ti (2016).
  Hence can't use this for static non-interactive key exchange.

SIKE submission to NIST

- SIKE = Supersingular Isogeny Key Exchange.
- Submission to the NIST standardization process on post-quantum cryptography.
- Authors: Jao, Azarderakhsh, Campagna, Costello, De Feo, Hess, Jalali, Koziel, LaMacchia, Longa, Naehrig, Renes, Soukharev and Urbanik.
- Submission contains specification of an IND-CCA KEM.
- `http://sike.org/`
- Advantage over lattice crypto: very short ciphertexts. CSIDH is even better.

Special Case of Isogeny Problem

- Given: $E, \ R_2, S_2, \ E_A, \ R_2', S_2'$.
- Know there is an isogeny $\phi : E \to E_A$ of degree $\ell_1^{e_1}$.
- Have exponentially many interpolation points

$$\phi([a]R_2 + [b]S_2) = [a]R_2' + [b]S_2'.$$

- Easy to solve if given $\phi(R_1)$, $\phi(S_1)$.
- Attack on extreme variant: C. Petit "Faster Algorithms for Isogeny Problems Using Torsion Point Images", ASIACRYPT 2017.
- Is this a hard problem?
- Decisional variant is equivalent to the computational problem.

Special Case of Isogeny Problem

- Classical meet-in-middle algorithm with time and space complexity $\tilde{O}(\ell_1^{e_1/2})$.
- **Open problem:** Low storage algorithm with this time complexity.
  See Adj, Cervantes-Vázquez, Chi-Domínguez, Menezes and Rodríguez-Henríquez, eprint 2018/313.
- Quantum "claw" algorithm. See Jao, de Feo and Plût (2014) for analysis.
- Biasse, Jao, and Sankar give a quantum algorithm for the general supersingular isogeny problem.

More open problems

- New quantum or classical algorithms?
- Find a random-self-reduction for this isogeny problem. This is easy in the group action setting: Given $(E, E_A = \mathfrak{a} * E)$ then $(\mathfrak{b} * E, \mathfrak{b}' * E_A)$ is a uniformly chosen instance.
- Find an efficient public key signature scheme. See Yoo et al (2017) and Galbraith, Petit, Silva (2017).

Quaternion Analogues

- Given two supersingular elliptic curves E_1, E_2 in characteristic p let $\mathcal{O}_1 = \mathrm{End}(E_1)$ and $\mathcal{O}_2 = \mathrm{End}(E_2)$.
- Then $\mathrm{Hom}(E_2, E_1)$ is a left-$\mathcal{O}_1$ module and a right-$\mathcal{O}_2$-module.
  Since if $\alpha \in \mathcal{O}_1, \rho : E_2 \to E_1$ and $\beta \in \mathcal{O}_2$ then $\alpha\rho\beta$ maps

$$E_2 \xrightarrow{\beta} E_2 \xrightarrow{\rho} E_1 \xrightarrow{\alpha} E_1.$$

- If $\phi : E_1 \to E_2$ is an isogeny of elliptic curves then $I = \mathrm{Hom}(E_2, E_1)\phi$ is a left-$\mathcal{O}_1$-ideal with right order $\mathcal{O}_2$.
- Conversely a left-$\mathcal{O}_1$-ideal I defines an isogeny with kernel

$$E_1[I] = \cap_{\phi \in I} \ker(\phi).$$

Quaternion Analogues

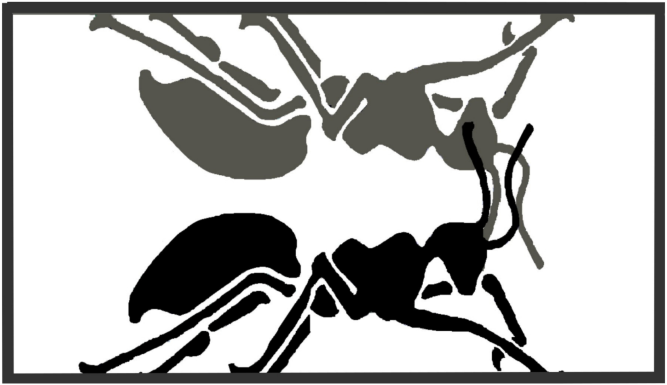
- Quaternion analogue of the isogeny problem: Given maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$, find a left-$\mathcal{O}_1$-ideal I with right order $\mathcal{O}_2$.
- This problem is easy. Can even find such an ideal I of two-power or power-smooth norm.

  D. Kohel, K. Lauter, C. Petit and J.-P. Tignol, On the quaternion ℓ-isogeny path problem, ANTS 2014.
- Indeed, can convert an ideal to an isogeny between the corresponding curves.
- Given an arbitrary supersingular curve E_1 it is hard to compute the maximal order $\mathcal{O}_1 = \mathrm{End}(E_1)$.
- Hence, hard to transform an isogeny problem (E_1, E_2) to a quaternion order problem $(\mathcal{O}_1, \mathcal{O}_2)$.
- K. Eisenträger, S. Hallgren, K. E. Lauter, T. Morrison, C. Petit, Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions, EUROCRYPT 2018.

Conclusion

- Post-quantum crypto is very active.
- There are plenty of good problems for arithmetic geometers and algorithmic number theorists to study.
- I'm happy to discuss these problems with you during the conference.

Thank You



QuAnts