Constructing elliptic curve isogenies in quantum subexponential time

Andrew M. Childs[1,2], David Jao[1], and Vladimir Soukharev[1]

[1] Department of Combinatorics and Optimization, University of Waterloo

[2] Institute for Quantum Computing, University of Waterloo

Quantum computation has the potential for dramatic impact on cryptography. Shor's algorithm [16] breaks the two most widely used public-key cryptosystems, RSA encryption and elliptic curve cryptography. Related quantum algorithms could break other classical cryptographic protocols, such as Buchmann-Williams key exchange [8] and algebraically homomorphic encryption [5]. Thus there is considerable interest in understanding which classical cryptographic schemes are or are not secure against quantum attacks, both from a practical perspective and as a potential source of new quantum algorithms that outperform classical computation.

While it is well known that quantum computers can efficiently solve the discrete logarithm problem in elliptic curve groups, other computations involving elliptic curves may be significantly more difficult. In particular, Couveignes [4] and Rostovtsev and Stolbunov [15, 17] proposed public-key cryptosystems based on the presumed difficulty of constructing an isogeny between two given elliptic curves. Informally, an isogeny is a map between curves that preserves their algebraic structure. Isogenies play a major role in classical computational number theory, yet as far as we are aware they have yet to be studied from the standpoint of quantum computation.

In this work, we present a quantum algorithm for constructing an isogeny between two ordinary elliptic curves. The isogenies from an elliptic curve E to itself form the endomorphism ring of the curve; this ring is an imaginary quadratic order $\mathcal{O}_\Delta$ of discriminant $\Delta < 0$. Given two isogenous ordinary elliptic curves E_0, E_1 over $\mathbb{F}_q$ with the same endomorphism ring $\mathcal{O}_\Delta$, we show how to construct an isogeny $\phi : E_0 \to E_1$ (specified by its kernel, represented by a smooth ideal class $[\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O}_\Delta)$). The output of this algorithm is sufficient to recover the private key in all proposed isogeny-based public-key cryptosystems [4, 15, 17].

The running time of our algorithm is subexponential—specifically, assuming the Generalized Riemann Hypothesis (GRH), it runs in time $L(\frac{1}{2}, \frac{\sqrt{3}}{2})$, where

$$L(\tfrac{1}{2}, c) := \exp\left[(c + o(1))\sqrt{\ln q \ln\ln q}\right].$$

Although subexponential-time attacks do not necessarily render a cryptosystem useless, our result suggests that isogeny-based approaches are unlikely to be competitive with other proposed quantum-resistant cryptosystems such as lattice-based cryptography. Furthermore, we hope that our work leads to other quantum algorithms for computations involving elliptic curves, a direction that appears to be a natural target for future quantum speedups.

Our algorithm works by reducing the problem of isogeny finding to the abelian hidden shift problem. When computing isogenies, it suffices to consider curves up to isomorphism, where curves are considered isomorphic if their defining equations are related by a change of variables. Let $\mathrm{Ell}_{q,n}(\mathcal{O}_\Delta)$ denote the set of isomorphism classes of elliptic curves over $\mathbb{F}_q$ with n points and endomorphism ring $\mathcal{O}_\Delta$, as represented by a function called the j-invariant of a curve. There is an action of the ideal class group $\mathrm{Cl}(\mathcal{O}_\Delta)$ on $\mathrm{Ell}_{q,n}(\mathcal{O}_\Delta)$ defined as $[\mathfrak{b}] * j(E) = j(E_\mathfrak{b})$, where $E_\mathfrak{b}$ is the elliptic curve reached from E by an isogeny corresponding to the ideal $\mathfrak{b} \in \mathcal{O}_\Delta$. This action is free and transitive, which implies that the functions $f_0, f_1 : \mathrm{Cl}(\mathcal{O}_\Delta) \to \mathrm{Ell}_{q,n}(\mathcal{O}_\Delta)$ defined as $f_0([\mathfrak{b}]) = [\mathfrak{b}] * j(E_0)$ and $f_1(E) = [\mathfrak{b}] * j(E_1)$ form an instance of the hidden shift problem

in the abelian group $\mathrm{Cl}(\mathcal{O}_\Delta)$. Thus, using Kuperberg's subexponential-time algorithm for the abelian hidden shift problem [12], we can find $[\mathfrak{s}] \in \mathrm{Cl}(\mathcal{O}_\Delta)$ such that $[\mathfrak{s}] * j(E_0) = j(E_1)$, thereby constructing an isogeny from E_0 to E_1.

While the reduction from isogeny finding to the hidden shift problem in $\mathrm{Cl}(\mathcal{O}_\Delta)$ is fairly straightforward, implementing this reduction in subexponential time is nontrivial. Previously, the best known algorithm for computing the action $*$ ran in exponential time (roughly $q^{1/4}$) [7]. We give a new classical algorithm for evaluating this action in time $L(\frac{1}{2}, \frac{\sqrt{3}}{2})$, assuming GRH. Since Kuperberg's sieve runs in time $L(\frac{1}{2}, 0)$, the overall running time is dominated by the time to compute the group action. (We also employ a quantum procedure to determine the structure of the group $\mathrm{Cl}(\mathcal{O}_\Delta)$ [3], but since this can be done in polynomial time, its cost is negligible.)

Our work apparently represents the first nontrivial application of Kuperberg's algorithm to a non-oracular problem. Note that although there is a reduction from certain lattice problems to the hidden shift problem [14], the overhead involved in this reduction makes the resulting algorithms for lattice problems no better than the best known classical algorithms.

Kuperberg's algorithm for the abelian hidden shift problem uses superpolynomial space (specifically, space $2^{O(\sqrt{\log q})}$), so the same is true of the most straightforward version of our algorithm. However, we also obtain an algorithm using polynomial space by taking advantage of an alternative approach to the abelian hidden shift problem introduced by Regev [13]. Regev's polynomial-space variant runs slightly slower than Kuperberg's original algorithm, and consequently the costs of computing the group action and solving the hidden shift problem both contribute to the asymptotic running time in this case. In particular, the version of our algorithm using polynomial space constructs an isogeny in time $L(\frac{1}{2}, \frac{\sqrt{3}}{2} + \sqrt{2})$, again assuming GRH.

Note that Regev only explicitly considered the case of the hidden shift problem in a cyclic group whose order is a power of 2, and even in that case did not compute the constant c in the running time $L(\frac{1}{2}, c)$. As a side result, we fill both of these gaps, showing that the hidden shift problem in any finite abelian group can be solved in time $L(\frac{1}{2}, \sqrt{2})$ using only polynomial space. The group $\mathrm{Cl}(\mathcal{O}_\Delta)$ may not even be cyclic, so this extension is necessary for our application.

Our algorithm for computing the action of the class group on elliptic curves is based on the idea of factoring the ideal class corresponding to the isogeny into a product of ideal classes corresponding to prime ideals, where the powers of the prime ideals and the primes themselves are not too large. Related ideas have appeared in previous classical algorithms for computations involving isogenies [1, 2, 6, 7, 10]. However, in all cases except the algorithm of [2] (which is restricted to curves with small $|\Delta|$), the running times of these algorithms depend on heuristic assumptions that go beyond GRH. In contrast, by taking advantage of expansion properties of a certain Cayley graph of $\mathrm{Cl}(\mathcal{O}_\Delta)$ [9], the analysis of our algorithm only needs to assume GRH. This also allows us to give a new classical algorithm for evaluating a given isogeny on a given curve, with the same performance as a previous algorithm [10], but only assuming GRH.

To break the proposed isogeny-based cryptosystems [4, 15, 17], it is sufficient to assume that the discriminant Δ of the endomorphism ring of the curves is known. Those proposals assume that $\mathcal{O}_\Delta$ is a maximal order, in which case Δ can easily be computed. However, we also give a version of our algorithm that works when Δ is unknown. This algorithm operates in a larger group than $\mathrm{Cl}(\mathcal{O}_\Delta)$ and makes use of other previous quantum algorithms for abelian groups [11, 18].

This work raises many questions about the power of quantum computers for solving problems involving elliptic curve isogenies. Of course, it is natural to ask whether our algorithm can be improved to use only polynomial time. Another potential target for quantum algorithms is the problem of determining the endomorphism ring of an ordinary elliptic curve. The best known classical algorithm for this problem takes time $L(\frac{1}{2}, \frac{\sqrt{3}}{2})$ under fairly aggressive heuristic assumptions

[1]; it would be interesting even to match the performance of this algorithm with a quantum approach requiring fewer assumptions. One might also consider quantum algorithms for constructing isogenies between ordinary elliptic curves of different endomorphism ring or between supersingular curves.

[1] Gaetan Bisson and Andrew V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *J. Number Theory*, to appear, 2009.

[2] Reinier Bröker, Denis Charles, and Kristin Lauter. Evaluating large degree isogenies and applications to pairing based cryptography. In *Pairing '08: Proceedings of the 2nd International Conference on Pairing-Based Cryptography*, pages 100–112, 2008.

[3] Kevin K. H. Cheung and Michele Mosca. Decomposing finite abelian groups. *Quantum Inform. Comput.*, 1(3):26–32, 2001.

[4] Jean-Marc Couveignes. Hard homogeneous spaces, 2006. http://eprint.iacr.org/2006/291.

[5] Wim van Dam, Sean Hallgren, and Lawrence Ip. Quantum algorithms for some hidden shift problems. In *Proceedings of the 14th ACM-SIAM Symposium on Discrete Algorithms*, pages 489–498, 2002.

[6] Steven D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS J. Comput. Math.*, 2:118–138 (electronic), 1999.

[7] Steven D. Galbraith, Florian Hess, and Nigel P. Smart. Extending the GHS Weil descent attack. In *Advances in Cryptology—EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Comput. Sci.*, pages 29–44, 2002.

[8] Sean Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *J. ACM*, 54(1):article 4, 2007. Preliminary version in STOC '02.

[9] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. *J. Number Theory*, 129(6):1491–1504, 2009.

[10] David Jao and Vladimir Soukharev. A subexponential algorithm for evaluating large degree isogenies. In *Algorithmic number theory: Proceedings of ANTS-IX*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 219–233, 2010.

[11] Alexei Yu. Kitaev. Quantum measurements and the abelian stabilizer problem. arXiv:quant-ph/9511026.

[12] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, 2005.

[13] Oded Regev. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. arXiv:quant-ph/0406151.

[14] Oded Regev. Quantum computation and lattice problems. *SIAM J. Comput.*, 33(3):738–760, 2004.

[15] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies, 2006. http://eprint.iacr.org/2006/145.

[16] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. Preliminary version in FOCS '94.

[17] Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Adv. Math. Commun.*, 4(2):215–235, 2010.

[18] John Watrous. Quantum algorithms for solvable groups. In *STOC '01: Proceedings of the 33rd ACM Symposium on Theory of Computing*, pages 60–67, 2001.