Quantum Equivalence of the DLP and CDHP for Group Actions

Steven Galbraith[1], Lorenz Panny[2],
Benjamin Smith[3], and Frederik Vercauteren[4]

[1] Mathematics Department, University of Auckland, NZ
s.galbraith@auckland.ac.nz
[2] Department of Mathematics and Computer Science,
Technische Universiteit Eindhoven, The Netherlands
lorenz@yx7.cc
[3] Inria *and* Laboratoire d'Informatique de l'École polytechnique,
Université Paris–Saclay, Palaiseau, France
smith@lix.polytechnique.fr
[4] imec-COSIC, ESAT, KU Leuven, Belgium
frederik.vercauteren@kuleuven.be

Abstract In this short note we give a polynomial-time quantum reduction from the vectorization problem (DLP) to the parallelization problem (CDHP) for group actions. Combined with the trivial reduction from parallelization to vectorization, we thus prove the quantum equivalence of both problems.

Keywords: Quantum reduction, group action, hard homogeneous space, discrete-logarithm problem, computational Diffie–Hellman problem.

1 Introduction

In 1997, Couveignes introduced the notion of a *hard homogeneous space* [2], essentially a free and transitive finite abelian group action $*: G \times X \to X$ which is easy to compute while certain computational problems are hard. In Couveignes' terminology, these problems are *vectorization* and *parallelization*, named by analogy with the archetypical example of a homogeneous space: a vector space acting on affine space by translations (cf. Figure 1). The vectorization problem is: given x and $g*x$ in X, compute $g \in G$. The parallelization problem is: given x, $g*x$, and $h*x$ in X, compute $gh*x \in X$. The group-exponentiation analogues of these problems are more commonly referred to as the *discrete logarithm problem* (DLP) and the *computational Diffie–Hellman problem* (CDHP).

[*] Author list in alphabetical order; see https://www.ams.org/profession/leaders/culture/CultureStatement04.pdf. This work was supported in part by the Commission of the European Communities through the Horizon 2020 program under project number 643161 (ECRYPT-NET), and in part by the Research Council KU Leuven grants C14/18/067 and STG/17/019. Date of this document: 2018.12.12.

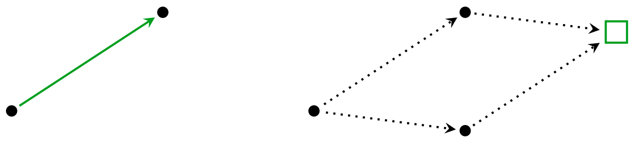

Figure 1. The vectorization and parallelization problems.

It is evident that parallelization reduces to vectorization: recover g from $g*x$, then apply g to $h*x$ to obtain $gh*x$. In the classical group-exponentiation setting, the other direction is much more subtle. The reduction essentially relies on the existence of auxiliary algebraic groups of smooth group order over $\mathbb{F}_{q_i}$, where the q_i are the prime divisors of the order of the group in which the DLP and CDHP are defined. The first result was given by den Boer [4] who showed the DLP and CDHP to be equivalent in $\mathbb{F}_p^\times$ when p is a prime such that the Euler totient $\varphi(p-1)$ is smooth. The auxiliary groups are simply $\mathbb{F}_{q_i}^\times$ for each prime divisor $q_i \mid p-1$, and the smoothness assumption implies that the DLP in each $\mathbb{F}_{q_i}^\times$ is easy. Maurer [6] generalized this result to arbitrary cyclic groups G, assuming that for each large prime divisor q_i of $|G|$, there exists an efficiently constructible elliptic curve $E/\mathbb{F}_{q_i}$ whose group order is smooth. On classical computers, these reductions do not apply in the group-action setting [8, §11].

In this short note, we show that there exists a polynomial-time *quantum* reduction from the vectorization to the parallelization problem for group actions without relying on any extra assumptions, thereby proving the polynomial-time equivalence of both problems in the quantum setting.

For twenty years, there was little interest in the hard-homogeneous-spaces framework, since all known (conjectural) instantiations were either painfully slow to compute with in practice or already captured by the group-exponentiation point of view. However, interest in these one-way group actions has reemerged due to the current focus on post-quantum cryptography. In particular, *CSIDH* [1] is a comparably efficient homogeneous space that appears to be post-quantum secure. The construction is based on the action of the ideal-class group $\mathrm{cl}(\mathcal{O})$ of an imaginary quadratic order $\mathcal{O}$ on the set of elliptic curves with endomorphism ring $\mathcal{O}$ through isogenies (modulo some identifications). Since this scheme and its earlier, less practical, variants [2, 9, 3] are our main applications, we will in the following write $\mathfrak{a}, \mathfrak{b}, \ldots$ for elements of the group G, and let E denote an element of the homogeneous space X.

2 The reduction

Let π be an algorithm that solves the parallelization problem for a homogeneous space $G \times X \to X$. In other words, π takes $\mathfrak{a}*E$ and $\mathfrak{b}*E$ and returns $\mathfrak{ab}*E$. We show that quantum access to a quantum circuit that computes π allows one to solve the vectorization problem in polynomial time.

Lemma. *Given an element $\mathfrak{a}*E \in X$, one can compute $\mathfrak{a}^n * E$ for any integer $n \geq 0$ using $\Theta(\log n)$ queries to π.*

Proof. One performs double-and-add in the "implicit group" [8] using the oracle $\pi\colon (\mathfrak{a}^x * E, \mathfrak{a}^y * E) \mapsto \mathfrak{a}^{x+y} * E$ for addition and doubling. □

Theorem. *Given a perfect (classical or) quantum parallelization algorithm π, there exists a quantum algorithm that recovers $\mathfrak{a}$ from elements E and $\mathfrak{a}*E$ in X in polynomial time.*

Proof. Using only the public description of G, one can compute the group structure $\mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$ of G together with a basis $\{\mathfrak{g}_1, \ldots, \mathfrak{g}_r\} \subseteq G$ in quantum polynomial time using Kitaev's generalisation [5] of Shor's algorithm [7].

Now, for $\underline{x} \in \mathbb{Z}^r$, write $\mathfrak{g}^{\underline{x}} = \prod_{i=1}^{r} \mathfrak{g}_i^{x_i}$ and define

$$\begin{aligned} f\colon\ \mathbb{Z}^r \times \mathbb{Z} &\longrightarrow X \\ (\underline{x}, y) &\longmapsto \mathfrak{g}^{\underline{x}} * (\mathfrak{a}^y * E)\,, \end{aligned}$$

where $\mathfrak{a}^y * E$ is computed using the Lemma.[5] Using the circuit for π one can construct a quantum circuit that computes f. The function f is clearly a group homomorphism (to the implicit group on X), hence defines an instance of the hidden-subgroup problem with respect to its kernel, i.e., the lattice

$$L = \{(x, y) \in \mathbb{Z}^r \times \mathbb{Z} \,:\, \mathfrak{g}^{\underline{x}+y\underline{v}} = 1 \in G\}\,,$$

where $\underline{v} \in \mathbb{Z}^r$ is any vector such that $\mathfrak{a} = \mathfrak{g}^{\underline{v}}$.[6] This (abelian) hidden-subgroup problem can be solved in polynomial time again using Shor's algorithm. Finally, any vector in L of the form $(\underline{x}, 1)$ satisfies $\mathfrak{g}^{-\underline{x}} = \mathfrak{a}$, hence yields a representation of $\mathfrak{a}$, and in particular $\mathfrak{a}$ itself. □

Remark. It is unclear how to perform the reduction above when π is only guaranteed to succeed with non-negligible probability α, meaning that the probability over all triples $(E, \mathfrak{a}*E, \mathfrak{b}*E) \in X^3$ that the oracle outputs $\mathfrak{ab}*E$ is at least α. In the classical setting, it is straightforward to amplify the success probability of π by using random self reduction of problem instances [8, §11]: one computes lists of possible values of $\mathfrak{ab}*E$ by blinding the inputs and unblinding the outputs, and uses majority vote to determine the correct result. Any *non-negligible* failure probability can be achieved using polynomially many queries to π.

However, in Shor's algorithm, it seems that one requires *exponentially* small failure probability: The algorithm works by building a big superposition of all (exponentially many) input-output pairs of the function f, which means that a polynomial number of repetitions is not enough to make all states in the superposition correct with high probability. We leave the analysis of the behaviour of Shor's algorithm in the presence of errors as an open problem.

[5] For negative y, one may generally take a positive representative modulo the exponent $\operatorname{lcm}(d_1, \ldots, d_r)$ of G. This is not needed in the CSIDH setting, since $\mathfrak{a}^{-1} * E$ can be obtained by merely quadratic-twisting $\mathfrak{a}*E$.

[6] Note that $\underline{v}$ is only defined modulo the relation lattice $R = d_1\mathbb{Z} \oplus \cdots \oplus d_r\mathbb{Z}$ of G with respect to $\mathfrak{g}_1, \ldots, \mathfrak{g}_r$. The choice of $\underline{v}$ does not matter since $L \supseteq R \oplus \{0\}$.

References

[1] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *ASIACRYPT (3)*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018. https://ia.cr/2018/383.

[2] Jean-Marc Couveignes. Hard homogeneous spaces. 1997. IACR Cryptology ePrint Archive 2006/291. https://ia.cr/2006/291.

[3] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. In *ASIACRYPT (3)*, volume 11274 of *Lecture Notes in Computer Science*, pages 365–394. Springer, 2018. https://ia.cr/2018/485.

[4] Bert den Boer. Diffie–Hellman is as strong as discrete log for certain primes. In *CRYPTO*, volume 403 of *Lecture Notes in Computer Science*, pages 530–539. Springer, 1988.

[5] Alexei Y. Kitaev. Quantum measurements and the abelian stabilizer problem. *Electronic Colloquium on Computational Complexity (ECCC)*, 3(3), 1996. https://eccc.hpi-web.de/eccc-reports/1996/TR96-003.

[6] Ueli M. Maurer. Towards the equivalence of breaking the Diffie–Hellman protocol and computing discrete logarithms. In *CRYPTO*, volume 839 of *Lecture Notes in Computer Science*, pages 271–281. Springer, 1994.

[7] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. https://arxiv.org/abs/quant-ph/9508027.

[8] Benjamin Smith. Pre- and post-quantum Diffie–Hellman from groups, actions, and isogenies. 2018. IACR Cryptology ePrint Archive 2018/882. https://ia.cr/2018/882.

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