Learning with Errors is easy with quantum samples

Alex B. Grilo*[1] and Iordanis Kerenidis†[1,2]

[1]IRIF, CNRS, Université Paris Diderot, Paris, France
[2]Centre for Quantum Technologies, National University of Singapore, Singapore

Learning with Errors is one of the fundamental problems in computational learning theory and has, in the last years, become the cornerstone of post-quantum cryptography [Reg05, GPV08]. In LWE, given a secret s, one is provided samples of the form

$$(a, a \cdot s + e \pmod q),$$

where $a \in \mathbb{F}_q^n$ is picked uniformly at random and $e \in \mathbb{F}_q$ is an 'error' term drawn from some distribution χ. The goal is to output s, while minimizing the number of samples used and the computation time.

In this work we study quantum algorithms for solving LWE with quantum samples. Let us be more explicit on the definition of a quantum sample for the LWE problem. We assume that the quantum learning algorithm receives samples in the form

$$\frac{1}{\sqrt{q^n}} \sum_{a \in \mathbb{F}_q^n} |a\rangle \, |a \cdot s + e_a (mod\, q)\rangle,$$

where e_a are iid random variables from some distribution χ over $\mathbb{F}_q$.

As expected, the performance of the learning algorithm, both in the classical and quantum case, is sensitive to the noise model adopted, i.e. to the distribution χ. When LWE is used in cryptographic schemes, the distribution χ has support on a small interval around 0, either uniform or a discrete gaussian [BV14]. We prove that for such distributions, there exists an efficient quantum learner for LWE.

Main Result(informal) *For error distributions χ used in cryptographic schemes, and for any $\epsilon > 0$, there exists a quantum learning algorithm that solves LWE with probability $1 - \eta$ using $O(n \log \frac{1}{\eta})$ samples and running time $poly(n, \log \frac{1}{\eta})$.*

Our quantum learner is a simple generalisation of Bernstein-Vazirani algorithm [BV97]: we start with a quantum sample, apply a Quantum Fourier Transform over $\mathbb{F}_q$ on each of the qudit registers, and then, we measure in the computational basis. Our analysis shows that, when the last qudit is not 0, which happens with high probability, the value of the remaining registers gives s with constant probability. We can then repeat this process so that our algorithm outputs s with high probability.

While our quantum learning algorithm does not break the proposed LWE-based encryption schemes, it does have some interesting implications for cryptography: first, one needs to be careful about the access to the public-key generation algorithm that is given to the adversary; second, our algorithm shows a possible way for attacking LWE-based encryption by using classical samples to approximate the quantum sample state, since then using our quantum learning algorithm would solve LWE.

*abgrilo@irif.fr
†jkeren@irif.fr

References

[BV97] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26(5), October 1997.

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing*, 43(2):831–871, 2014.

[CSS15] Andrew W Cross, Graeme Smith, and John A Smolin. Quantum learning robust against noise. *Physical Review A*, 92(1):012327, 2015.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC 2008*, pages 197–206, 2008.

[RdSR$^+$15] Diego Rist, Marcus P. da Silva, Colm A. Ryan, Andrew W. Cross, John A. Smolin, Jay M. Gambetta, Jerry M. Chow, and Blake R. Johnson. Demonstration of quantum advantage in machine learning. *CoRR*, abs/1512.0606G9, 2015.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, STOC 2005*, pages 84–93, 2005.