On the Quantum Equivalence between S—LWE⟩ and ISIS

Hermouet Paul*[1]

[1]Inria - COSMIQ – Centre Inria de Paris – France

Résumé

A cornerstone of lattice-based cryptography is Regev's reduction (1) that reduces reduces the Short Integer Solution (SIS) problem to the Learning With Errors (LWE) problem. That is, it shows that given an algorithm solving LWE, one can solve SIS. These are arguably two of the most important problems in post-quantum cryptography and they are somehow dual to each other. LWE asks to find a random secret s given a noisy linear samples (A, As + e), while SIS asks to find a short, non-zero solution x to a linear system Ax = 0 - the short condition being usually defined as an upper-bound on the solution's (l2 or l∞) norm. Regev's reduction uses a (classical or quantum) algorithm solving LWE in order to create a superposition of noisy lattice points and then performs a measurement in the Fourier basis to obtain a short dual lattice point.

As noted in (2), this reduction does not strictly need an LWE solver, but an algorithm solving an easier problem, later defined as S—LWE⟩ (3), where the errors in the samples are in quantum superposition, that is one is given (A, $\sum$f(e)—As+e⟩) where f is an amplitude function that concentrates on small inputs. This was first explicitly used by Brakerski, Kirshanova, Stehlé and Wen (4) where they extend this reduction and introduced the Extended Dihedral Coset Problem.

A few years later, Chen Liu and Zhandry (3) revisited this reduction for algorithmic purposes, and showed that in some regimes, this S—LWE⟩ problem can be significantly easier than the standard LWE problem. They showed how to construct, for some parameters, a quantum polynomial time algorithm for SIS∞ - where the upper-bound is on the l∞ norm of the solution. While these parameters are still very far from those used in lattice-based cryptography, this result shows the very promising nature of this family of algorithms.

This framework has then been successfully used. Yamakawa and Zhandry (5) provided a first quantum advantage without structure in the Random Oracle Model. It was also used in a somewhat different context to construct quantum oblivious sampling (6) and extended to the setting of linear codes (7, 8), as well as structured codes in other to obtain a quantum advantage (9, 10). All these results use an algorithm for S—LWE⟩ to construct an algorithm for SIS and perform an ad hoc analysis of this reduction. This is in part due to the fact that we cannot have a generic reduction from SIS to S—LWE⟩ using this approach (see (8)). The only notable exception is the

work of Chailloux and Tillich (10) that provided the first generic reduction, but from

*Intervenant

Inhomogeneous-SIS (ISIS) to S—LWE⟩ - where ISIS is a variant of SIS that asks to find a short solution to an inhomogeneous linear system Ax = y. This reduction does however have some assumptions on the S—LWE⟩ algorithm, which are satisfied by classical algorithms but not necessarily by quantum algorithms. A first natural question arises :

Is it possible to have a fully generic reduction from ISIS to S—LWE⟩ that is robust to failures in the decoder ?

Also, because of the importance of S—LWE⟩, recent works directly construct quantum algorithms for this problem. First, a generic quantum algorithm for S—LWE⟩ was presented in (11), running in subexponential time and requiring a subexponential number of queries. Then (12) presented a slightly superpolynomial algorithm for S—LWE⟩ in the case the alphabet size q is a small power of 2. These results both use variants of the quantum Kuperberg sieve (13) for the Dihedral Coset Problem. When looking at these algorithms more carefully, one can notice that they are actually very similar to some known classical algorithm for ISIS and this raises a second question :

Can we construct algorithms for S—LWE⟩ from algorithms for ISIS ? More generally, are the problems S—LWE⟩ and ISIS equivalent ?

Contributions

We present three main contributions in our work :

1. First, we construct a fully generic reduction from ISIS to S—LWE⟩. This new reduction is robust to errors in the S—LWE⟩ solver, and removes the assumptions needed in (10).

2. We then tackle the reverse reduction. We introduce a quantum version of ISIS : —ISIS⟩ and show that one can solve S—LWE⟩ given access to a solver for —ISIS⟩. This is, to the best of our knowledge, the first work investigating this direction of the reduction.

3. Finally, we show that such a solver for —ISIS⟩ can be constructed by a solver for its classical counterpart ISIS, provided that this solver meets a specific condition, that we call randomness-recoverability.

In conclusion, our results give for the first time a full forward reduction between ISIS and S—LWE⟩ and a partial reverse reduction. This clarifies the landscape of reductions between S—LWE⟩ and ISIS, as well as the remaining barrier for showing full equivalence.

(Collaboration with André Chailloux)