IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2024EAP1004

Publicized:2024/08/16

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

Quantum Search-to-Decision Reduction for the LWE Problem*

Kyohei SUDO[†,††a)], **Keisuke HARA**[†††,††††b)], *Nonmembers*, **Masayuki TEZUKA**[†††††c)], *Member*, *and* **Yusuke YOSHIDA**[†††††d)], *Nonmember*

SUMMARY The learning with errors (LWE) problem is one of the fundamental problems in cryptography and it has many applications in post-quantum cryptography. There are two variants of the problem, the decisional-LWE problem, and the search-LWE problem. LWE search-to-decision reduction shows that the hardness of the search-LWE problem can be reduced to the hardness of the decisional-LWE problem. The efficiency of the reduction can be regarded as the gap in difficulty between the problems.

We initiate a study of quantum search-to-decision reduction for the LWE problem and propose a reduction that satisfies sample-preserving. In sample-preserving reduction, it preserves all parameters even the number of instances. Especially, our quantum reduction invokes the distinguisher only 2 times to solve the search-LWE problem, while classical reductions require a polynomial number of invocations. Furthermore, we give a way to amplify the success probability of the reduction algorithm. Our amplified reduction is incomparable to the classical reduction in terms of sample complexity and query complexity. Our reduction algorithm supports a wide class of error distributions and also provides a search-to-decision reduction for the learning parity with noise problem.

In the process of constructing the search-to-decision reduction, we give a quantum Goldreich-Levin theorem over $\mathbb{Z}_q$ where q is a prime. In short, this theorem states that, if a hardcore predicate $a \cdot s \pmod q$ can be predicted with probability distinctly greater than $1/q$ with respect to a uniformly random $a \in \mathbb{Z}_q^n$, then it is possible to determine $s \in \mathbb{Z}_q^n$.

key words: *Learning with errors, Learning parity with noise , Search-to-decision reduction, Goldreich-Levin theorem, Quantum reduction, Query complexity, Sample complexity*

1. Introduction

Quantum algorithms run on a quantum computer and they have the potential to solve some problems faster than classical computation, for example, Shor's algorithm has been shown to solve factorization efficiently. In the same way, we can investigate a quantum reduction algorithm that could be more efficient than the known classical reduction algorithms. Reduction algorithms play an important role in cryptography to transform one problem into another problem. Intuitively, problem A is reducible to problem B, if an algorithm for solving problem B could also be used as a subroutine to solve problem A. In this sense, search-to-decision reduction for the learning with errors (LWE) problem is to show the decisional-LWE problem is as hard as the search-LWE problem.

The LWE problem introduced by Regev [26] is one of the fundamental computational problems in cryptography. The LWE samples consist of a pair (A, y) of a uniformly random matrix $A \in \mathbb{Z}_q^{m\times n}$ together with $y = A \cdot s + e$ for randomly chosen error term $e \leftarrow \chi^m$ (small Gaussian noise is commonly used) where m is the number of samples. LWE has two main variations: The search-LWE problem asks to find a secret string $s \in \mathbb{Z}_q^n$, given a system of noisy linear equations (A, y), while the decisional-LWE problem asks to distinguish between the distribution of the LWE samples $\{(A, y) | s \xleftarrow{\$} \mathbb{Z}_q^n, A \xleftarrow{\$} \mathbb{Z}_q^{m\times n}, e \leftarrow \chi^m, y := A \cdot s + e\}$ and uniformly random distribution $\{(A, r) | A \xleftarrow{\$} \mathbb{Z}_q^{m\times n}, r \xleftarrow{\$} \mathbb{Z}_q^m\}$.

There are two standard facts in LWE hardness. The first is more trivial, which says that there is a reduction from the decisional-LWE to the search-LWE: Whenever the pair (A, b) is randomly chosen $A \xleftarrow{\$} \mathbb{Z}_q^{m\times n}, b \xleftarrow{\$} \mathbb{Z}_q^m$, then with overwhelming probability the vector b is going to be far away from the lattice, thus there does not exist a coordinates vector s such that $A \cdot s$ is close to b, thus if we can break search-LWE and find s, we can check whether b is close to $A \cdot s$ or not, which constitutes an algorithm that breaks decisional-LWE. The second known fact is less trivial and says that the search-LWE can be reduced to the decisional-LWE. These previously known reductions use a distinguisher for the decisional-LWE to extract the secret string s and break the search-LWE. More delicately, the way that these reductions work is that the search-LWE adversary uses classical oracle access to the distinguisher.

There exist hardness proofs based on reductions from worst-case lattice problems (BDD/gapSVP),

[†] Osaka University, Osaka, 560-0831 Japan.
[††] Research Fellow of Japan Society for the Promotion of Science.
[†††] National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan
[††††] Yokohama National University, Kanagawa, Japan
[†††††] Tokyo Institute of Technology, Tokyo, 152- 8552 Japan.

[*] A preliminary version of this paper was accepted in Africacrypt2023 [27]. This is the full version.

a) E-mail: u358338c@ecs.osaka-u.ac.jp
b) E-mail: hara-keisuke@aist.go.jp
c) E-mail: tezuka.m.ac@m.titech.ac.jp
d) E-mail: yoshida.y.aw@m.titech.ac.jp

which are considered to be hard not only for classical computers but also for quantum computers. As a consequence, the hardness of the decisional-LWE problem serves as the security source of many post-quantum cryptographic primitives, such as oblivious transfer [25], identity-based encryption [3], [12], [16], fully homomorphic encryption [10], etc.

Prior works.

There are various incomparable search-to-decision reductions for the LWE problem [6], [9], [21], [22], [24], [26]. Regev [26] who introduced the LWE problem showed search-to-decision reduction in [26]. It imposes constraints that modulus q must be prime and bounded by $poly(n)$. Research on search-to-decision reduction has been conducted in the direction of loosening the restriction on modulus q, but they incur some loss in the LWE parameters. Peikert [24] extends Regev's reduction for the case where q can be expressed as a product of distinct prime numbers in $poly(n)$, but it requires the error distribution to be Gaussian. Applebaum, Cash, Peikert, and Sahai [6] give a reduction for the case where the modulus can be a prime power $q = p^e$. The above algorithms have the property that the run-time scales linearly with q in common. It could make the reductions meaningless for large q. Micciancio and Peikert [22] give a reduction that runs in $poly(\log q)$. Micciancio and Mol [21] give a search-to-decision reduction in another direction. They show a sample-preserving reduction, which shows that if the pseudorandomness of the LWE problem holds, the LWE problem with the same number of samples is invertible. The state-of-the-art results constitute an adversary that makes polynomially many such classical queries to the distinguisher in order to break search-LWE, and the extra computations that the search-LWE adversary makes on the side (between its queries to the decisional-LWE adversary) are also classical. What this work aims to do is to use quantum computations and quantum queries to the decisional-LWE adversary in order to speed up the reduction - use fewer queries and less computation time.

Practical importance of quantum search-to-decision reduction.

The LWE challenge [1] is the foundation for ensuring the difficulty of the LWE problem. In practice, the LWE challenge is intended to solve search LWE problems. Based on the results of the LWE challenge, the parameter size n is selected, at which we can trust that the search-LWE problem is hard enough.

Suppose that there is a cryptographic scheme whose security is reduced to the hardness of the decisional-LWE problem. Intuitively, if the security of the scheme is to be ensured based on the LWE challenge of size n, the size of the scheme should be $loss_{s2d}(n)$ plus the security loss of the scheme itself, where $loss_{s2d}(\cdot)$ is the reduction loss in a search-to-decision reduction.

When a quantum computer arises, a quantum version of the LWE challenge will be held and the parameter n_Q $(\geq n)$ will be determined for the LWE problem to be hard for the quantum computer. Then, should the size of the scheme be selected based on $loss_{s2d}(n_Q)$? If we know the efficiency $loss_{Qs2d}(\cdot)$ of quantum search-to-decision reduction, we know that we can actually implement the scheme with a size based on $loss_{Qs2d}(n_Q)$, which is expected to partially mitigate the effect of the increase of n_Q over n.

1.1 Our contribution

Quantum search-to-decision reduction.

In this work, we investigate a quantum search-to-decision reduction for the LWE problem and we discuss the efficiency of our algorithm and classical ones. We compare the efficiency of our reduction and the classical ones by three aspects, success probability, query complexity, and sample complexity. We treat the distinguisher as a blackbox and the query complexity of an algorithm is measured by the number of queries to the distinguisher in the algorithm while it finds the secret string s of the search-LWE problem. The sample complexity of an algorithm is measured by the number of LWE instances that it takes. In this paper, we propose three variations of the reduction algorithms.

- The first one is an algorithm that also serves as the basis for the other two. It finds s with probability at least $\frac{4q^2\epsilon^3}{27m^3(q-1)^5}$ using distinguisher 2 times. And it is also a sample-preserve reduction, i.e., it needs m sample of LWE instances to find s where m is the number of instances required by the distinguisher to solve the decisional-LWE problem.
- The second algorithm is an evolution of the sample-preserve one. It amplifies the probability of success of the first algorithm instead of increasing the complexities. It finds s with probability $\Omega(\frac{\epsilon}{qm})$ using distinguisher $\mathcal{O}(\frac{qm}{\epsilon})$ times.
- The third algorithm is a version of a higher probability of success through further iterations. It finds s with probability $1-o(1)$ using distinguisher $\mathcal{O}(\frac{q^2m^2\log n}{\epsilon^2})$ times.

We remark that our reductions have some constraints on parameters. Our reductions require q to be prime. The second and third require that we can verify from the instances of the LWE problem whether it is the correct answer for the LWE problem given some input $s' \in \mathbb{Z}_q^n$. We believe that this condition does not impose a strong limitation on the use of LWE as a basis for cryptographic primitives. The existence of more efficient or less restrictive classical/quantum search-to-decision reduction is an open problem.

Table 1 Comparison of the algorithms performance. n is a size of the LWE problem, m is the number of instances required by the distinguisher to solve the decisional LWE problem, ϵ is the advantage of the distinguisher.
* The numbers in this line are from a simplified version of the reduction by Regev. The specific construction of the algorithm is described in Appendix B.
** The success probability and the query complexity of this algorithm are very complex. The specific values are given in Appendix B.

	Success probability	Query complexity	Sample complexity	Classical/Quantum
Reg05*[26]	$1-o(1)$	$\tilde{\mathcal{O}}(\frac{nq}{\epsilon^2})$	$\tilde{\mathcal{O}}(\frac{mnq}{\epsilon^2})$	Classical
MM11**[21]	$\frac{1}{poly(n)}$	$poly(n)$	m	Classical
Th.2	$\frac{4q^2\epsilon^3}{27(q-1)^5m^3}$	2	m	Quantum
Th.3	$\Omega(\frac{\epsilon}{qm})$	$\mathcal{O}(\frac{qm}{\epsilon})$	$m+\mathcal{O}(n)$	Quantum
Cor.1	$1-o(1)$	$\mathcal{O}(\frac{q^2m^2\log n}{\epsilon^2})$	$\tilde{\mathcal{O}}(\frac{qm^2}{\epsilon})$	Quantum

Quantum non-uniform search-to-decision reduction.

A quantum non-uniform algorithm takes a piece of quantum state as auxiliary input, which only depends on the security parameter. Oftentimes, it is beneficial to consider a reduction for non-uniform distinguisher. Recently, Chardouvelis, Goyal, Jain, and Liu [13] give a quantum search-to-decision reduction with high success probability for non-uniform distinguisher with a dedicated analysis. Our sample-preserving reduction, which is essentially the generalized Goldreich-Levin theorm is adopted for the case of non-uniform distinguisher. However our second and third reductions that involve the success probability amplification remain for uniform distinguisher. We leave future work to upgrade our uniform reductions, or more generally, the process of probability amplification to the non-uniform case.

Extension of quantum Goldreich-Levin theorem.

The Goldreich-Levin theorem [17] is a cornerstone theorem in computer science and has been studied from various aspects [2], [17], [18], [20], [23]. This theorem states that any (strong) one-way function f can be easily transformed into a function of the required form $g(s,a) := (f(s),a)$ where $s,a \in \mathbb{Z}_2^n$ and it has a hard-core predicate $a \cdot s \pmod 2$. Roughly speaking, a (strong) one-way function is a function that can be efficiently computed but is hard to compute in the reverse direction, and a hard-core predicate of a function is a bit that can be efficiently computed from the input to the function and no efficient algorithm can guess it from the output of the function with probability distinctly higher than one-half. Adcock and Cleve investigate a quantum Goldreich-Levin theorem [2]. Roughly, they show that the reduction from quantum one-way functions to quantum hard-core predicates is quantitatively more efficient than the classical version.

In the process of constructing the quantum search-to-decision reduction, we give a further generalized theorem of the quantum Goldreich-Levin theorem by Adcock and Cleve. Namely, we show that if there exists a predictor that predicts $a \cdot s \pmod q$ where $a, s \in \mathbb{Z}_q^n$ and q to be prime with probability $\frac{1}{q}+\delta$ over the choice of $a \leftarrow \mathbb{Z}_q^n$, then we can find s with probability at least $(\frac{q\delta}{q-1})^2$ while accessing the predictor 2 times.

Concurrent work of quantum Goldreich-Levin theorem.

Recently, Ananth et al. [5] independently investigated a quantum Goldreich-Levin theorem for the field $\mathbb{Z}_q$. They obtain this result by converting the classical Goldreich-Levin theorem for the field $\mathbb{Z}_q$ by Dodis et al. [14] into quantum reduction, by using the recent work of Bitansky et al. [8]. Specifically, they show that a distinguisher, given auxiliary input Aux, can distinguish between $(a, a \cdot s + e)$ and (a, r) where s is randomly chosen from $H \subset \mathbb{Z}_q^n$ can be converted into a quantum extractor that can extract s given Aux.

While their quantum algorithm relies on the classical Goldreich-Levin theorem for the field $\mathbb{Z}_q$ by Dodis et al. [14], in which the distinguisher with advantage ϵ is used $poly(n, |H|, \frac{1}{\epsilon})$ times to extract s and its success probability is $\frac{\epsilon^3}{512 \cdot n \cdot q^2}$. On the other hand, our quantum algorithm can find s by accessing the distinguisher 2 times with probability $\frac{4q^2\epsilon^3}{27(q-1)^5}$, and there is no need to make the subset from which s is chosen small.

Improvements from Previous Version.

This paper is the full version of the work published in Africacrypt2023 [27]. As a significant update, while the Africacrypt version included the similar method of a prediction-to-decision reduction as in [7], [15], but it was found that this method had incomplete proof. Therefore, we introduce a modified reduction method in Section 3, Lemma 1, 2, 3. Furthermore, a non-uniform reduction was provided for the sample-preserve reduction. In other words, we construct a solver using a distinguisher that requires an auxiliary.

1.2 Technical overview

We describe our techniques for proving our results on quantum search-to-decision reduction for the LWE problem. Our construction of the search-to-decision reduction consists of two parts. For the first part, we construct a predictor from the distinguisher of the decisional-LWE problem, and for the second part, we construct an algorithm that finds s using the predictor. This reduction strategy can be interpreted as making a prediction-to-decision reduction and a search-to-prediction reduction. We note that the idea of the search-to-decision reduction via unpredictability is the same as that of classical reduction by Micciancio and Mol [21], Applebaum, Ishai, and Kushilevitz [7]. We found a quantum speed-up in the second part of the reduction and we call it as generalized quantum Goldreich-Levin theorem. Then we provide an overview of this theorem. For simplicity, we consider uniform case.

Quantum Goldreich-Levin theorem.

We first review the quantum Goldreich-Levin theorem by Adcock and Cleve [2]. We call a unitary operation U_P is a quantum (s, q, ϵ)-predictor, if the last register of $\mathsf{U}_P \left|a\right\rangle \left|0^l\right\rangle \left|0\right\rangle$ is measured in computational basis, yielding the value $P(a)$, then $\Pr[P(a) = a{\cdot}s \pmod q] > \frac{1}{q}+\epsilon$ holds where $a, s \in \mathbb{Z}_q^n$ and the probability depends on over choice of $a \xleftarrow{\$} \mathbb{Z}_q^n$.

We denote

$$\mathsf{U}_P \left|a\right\rangle \left|0^l\right\rangle \left|0\right\rangle = \alpha_{a,0} \left|\eta_{a,0}\right\rangle \left|a\cdot s\right\rangle + \alpha_{a,1} \left|\eta_{a,1}\right\rangle \left|a\cdot s+1\right\rangle$$

where U_P is a $(s, 2, \epsilon)$-predictor, $\alpha_{a,0}$ and $\alpha_{a,1}$ are complex number. Since for a random uniformly distributed $a \xleftarrow{\$} \{0,1\}^n$, measuring the last register of $\mathsf{U}_P \left|a\right\rangle \left|0^l\right\rangle \left|0\right\rangle$ yields $a \cdot s \pmod 2$ with probability at least $\frac{1}{2}+\epsilon$, it follows that

$$\frac{1}{2^n} \sum_{a\in\{0,1\}^n} \left|\alpha_{a,0}\right|^2 \geq \frac{1}{2}+\epsilon \tag{1}$$

and

$$\frac{1}{2^n} \sum_{a\in\{0,1\}^n} \left|\alpha_{a,1}\right|^2 < \frac{1}{2}-\epsilon. \tag{2}$$

We explain their quantum reduction algorithm step by step. First, pass the superposition states

$$\frac{1}{\sqrt{2^n}} \sum_{a\in\{0,1\}^n} \left|a\right\rangle \left|0^l\right\rangle \left|0\right\rangle$$

through the $(s, 2, \epsilon)$-predictor U_P, multiply the phase by $(-1)^y$ according to the value of the last register y. The quantum states is now in a state

$$\left|\phi\right\rangle := \frac{1}{\sqrt{2^n}} \sum_{a\in\{0,1\}^n} \sum_{b\in\{0,1\}} (-1)^{a\cdot s+b} \alpha_{a,b} \left|a\right\rangle \left|\eta_{a,b}\right\rangle \left|a\cdot s+b\right\rangle$$

up to this point. Pass the states through conjugate transpose of the predictor $\mathsf{U}_P^\dagger$. By measuring the first register in Fourier basis, we could obtain s. The probability of yielding s when the first register is the square of the inner product of this states $\left|\phi\right\rangle$ and

$$\begin{aligned}
\left|\psi\right\rangle &:= \mathsf{U}_P \mathsf{QFT} \left|s\right\rangle \left|0^l\right\rangle \left|0\right\rangle \\
&= \mathsf{U}_P \left(\frac{1}{\sqrt{2^n}} \sum_{a\in\{0,1\}^n} (-1)^{a\cdot s} \left|a\right\rangle \left|0^l\right\rangle \left|0\right\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{a\in\{0,1\}^n} \sum_{b\in\{0,1\}} (-1)^{a\cdot s} \alpha_{a,b} \left|a\right\rangle \left|\eta_{a,b}\right\rangle \left|a\cdot s+b\right\rangle,
\end{aligned}$$

which is

$$\left|\left\langle\psi|\phi\right\rangle\right|^2 = \left| \frac{1}{2^n} \sum_{a\in\{0,1\}^n} \left(\left|\alpha_{a,0}\right|^2 - \left|\alpha_{a,1}\right|^2\right) \right|^2.$$

Using the fact of (1) and (2), we can find s with probability at least $\left|\left(\frac{1}{2}+\epsilon\right) - \left(\frac{1}{2}-\epsilon\right)\right|^2 = 4\epsilon^2$.

Difficulty.

Next, we show that naive expansion of the quantum Goldreich-Levin results in a (s, q, ϵ)-predictor where $q \neq 2$ does not work.

We denote the state obtained by applying U_P to $\left|a\right\rangle \left|0^l\right\rangle \left|0\right\rangle$ as follows,

$$\mathsf{U}_P \left|a\right\rangle \left|0^l\right\rangle \left|0\right\rangle = \alpha_{a,j} \left|a\right\rangle \left|\eta_{a,j}\right\rangle \left|a\cdot s+j\right\rangle.$$

As in the quantum Goldreich-Levin algorithm, pass the superposition states

$$\frac{1}{\sqrt{q^n}} \sum_{a\in\mathbb{Z}_q^n} \left|a\right\rangle \left|0^l\right\rangle \left|0\right\rangle$$

through the predictor U_P, multiply the phase by ω_q^y according to the value of the last register y and we get the states

$$\left|\phi\right\rangle := \frac{1}{\sqrt{q^n}} \sum_{a\in\mathbb{Z}_q^n} \sum_{j\in\mathbb{Z}_q^n} \omega_q^{a\cdot s+j} \alpha_{a,j} \left|a\right\rangle \left|\eta_{a,j}\right\rangle \left|a\cdot s+j\right\rangle.$$

If we apply $\mathsf{U}_P^\dagger$ and measure the first register in the Fourier basis, the probability of yielding s is the square of the inner product of $\left|\phi\right\rangle$ and

$$\begin{aligned}
\left|\psi\right\rangle &:= \mathsf{U}_P \mathsf{QFT} \left|s\right\rangle \left|0^l\right\rangle \left|0\right\rangle \\
&= \mathsf{U}_P \left(\frac{1}{\sqrt{q^n}} \sum_{a\in\mathbb{Z}_q^n} \omega_q^{a\cdot s} \left|a\right\rangle \left|0^l\right\rangle \left|0\right\rangle \right) \\
&= \frac{1}{\sqrt{q^n}} \sum_{a\in\mathbb{Z}_q^n} \sum_{j\in\mathbb{Z}_q} \omega_q^{a\cdot s} \alpha_{a,j} \left|a\right\rangle \left|\eta_{a,j}\right\rangle \left|a\cdot s+j\right\rangle,
\end{aligned}$$

which is

$$|\langle\psi|\phi\rangle|^2 = \left|\frac{1}{q^n}\sum_{a\in\mathbb{Z}_q^n}\sum_{j\in\mathbb{Z}_q}\omega_q^j|\alpha_{a,j}|^2\right|^2 .$$

Define $\Pr(j)$ as a probability of the gap between the predictor's prediction and inner product is j, then this probability can be written as $|\sum_{j\in\mathbb{Z}_q}\omega_q^j\Pr(j)|^2$. This value cannot be guaranteed some lower bound unless the advantage is very high such that $\epsilon > \frac{1}{2}-\frac{1}{q}$.

Solution.

To get around this obstacle, our key idea is to use the property of cyclic group $\mathbb{Z}_q^*$. For all element $j\in\mathbb{Z}_q^*$, j determines a bijection $r\mapsto rj$ on $\mathbb{Z}_q$ and it maps 0 to 0. Using this property, we can say that

$$\frac{1}{q-1}\sum_{r\in\mathbb{Z}_q^*}\omega_q^{rj}\Pr(j) = \begin{cases}\Pr(0) & \text{if } j=0\\ \frac{-1}{q-1}\Pr(j) & \text{if } j\neq 0.\end{cases} \qquad (3)$$

We will use this property to improve the algorithm. First, prepare the superposition states

$$\frac{1}{\sqrt{q^n(q-1)}}\sum_{a\in\mathbb{Z}_q^n}\sum_{\mathsf{r}\in\mathbb{Z}_q^*}|\mathsf{r}\rangle|a\rangle|0^l\rangle|0\rangle$$

through the predictor U_P(apply the second to the last register), multiply the last register by the first register r, multiply the phase by ω_q^y according to the value of the last register y, divide the last register by the first register r(multiply r^{-1}) and we get the states

$$|\phi\rangle := \frac{1}{\sqrt{q^n(q-1)}}\sum_{a,\mathsf{r},j}\omega_q^{\mathsf{r}(a\cdot s+j)}\alpha_{a,j}|\mathsf{r}\rangle|a\rangle|\eta_{a,j}\rangle|a\cdot s+j\rangle .$$

If we apply the states through conjugate transpose of the predictor $\mathsf{U}_P^\dagger$(apply the second to the last register), multiply the second register by the first register r(denote this operation as M), and measure the second register in Fourier basis, the probability of yielding s is the square of the inner product of $|\phi\rangle$ and

$$\begin{aligned}
&|\psi\rangle\\
&:= \mathsf{U}_P\mathsf{M}^\dagger\mathsf{QFT}\frac{1}{\sqrt{q-1}}\sum_{\mathsf{r}\in\mathbb{Z}_q^*}|\mathsf{r}\rangle|s\rangle|0^l\rangle|0\rangle\\
&= \mathsf{U}_P\mathsf{M}^\dagger\left(\frac{1}{\sqrt{q^n(q-1)}}\sum_{a'\in\mathbb{Z}_q^n}\sum_{\mathsf{r}\in\mathbb{Z}_q^*}\omega_q^{a'\cdot s}|\mathsf{r}\rangle|a'\rangle|0^l\rangle|0\rangle\right)\\
&= \mathsf{U}_P\mathsf{M}^\dagger\left(\frac{1}{\sqrt{q^n(q-1)}}\sum_{a\in\mathbb{Z}_q^n}\sum_{\mathsf{r}\in\mathbb{Z}_q^*}\omega_q^{\mathsf{r}a\cdot s}|\mathsf{r}\rangle|\mathsf{r}a\rangle|0^l\rangle|0\rangle\right)\\
&= \mathsf{U}_P\left(\frac{1}{\sqrt{q^n(q-1)}}\sum_{a,\mathsf{r}}\omega_q^{\mathsf{r}(a\cdot s)}|\mathsf{r}\rangle|a\rangle|0^l\rangle|0\rangle\right)\\
&= \frac{1}{\sqrt{q^n(q-1)}}\sum_{a,\mathsf{r},j}\omega_q^{\mathsf{r}(a\cdot s)}|\mathsf{r}\rangle|a\rangle|\eta_{a,j}\rangle|a\cdot s+j\rangle .
\end{aligned}$$

Finally, we get

$$\begin{aligned}
\Pr[s\text{ is measured}] &= |\langle\psi|\phi\rangle|^2\\
&= \left|\frac{1}{q^n(q-1)}\sum_{a,r,j}\omega_q^{rj}|\alpha_{a,j}|^2\right|^2\\
&= \left|\Pr(0)-\frac{1}{q-1}\sum_{j\neq 0}\Pr(j)\right|^2\\
&\geq \left(\frac{q\epsilon}{q-1}\right)^2 .
\end{aligned}$$

This result is consistent with quantum Goldreich-Levin results and is a successful generalization.

2. Preliminaries

2.1 Notation and definitions

In this paper, we use the following notations and definitions. For a finite set S, $s\xleftarrow{\$}S$ denotes choosing an element s from S uniformly at random. For a distribution D, $d\leftarrow D$ denotes sampling an element d according to distribution D. We denote $\mathbb{Z}_q$ for the cyclic group $\{0,1,...,q-1\}$ with addition modulo q. We also denote $\mathbb{T}$ for $\mathbb{R}/\mathbb{Z}$, in other words, the segment $[0,1)$ with addition modulo 1. We use standard asymptotic notations $\mathcal{O}(\cdot)$, $o(\cdot)$, $\Omega(\cdot)$, $\Theta(\cdot)$, etc. We use $\tilde{\mathcal{O}}$ (resp. $\tilde{\Theta}$) notation which overlooks quantities poly-logarithmic in appearing arguments, that is, $\tilde{\mathcal{O}}(x) := \mathcal{O}(x(\log x)^{\Theta(1)})$ (resp. $\tilde{\Theta}(x) := \Theta(x(\log x)^{\Theta(1)})$). We denote by ω_n the complex root of unity of order n: $\omega_n := e^{\frac{2\pi i}{n}}$. For $\alpha\in\mathbb{R}^+$ the distribution Ψ_α is the distribution on $\mathbb{T}$ obtained by sampling from a normal variable with mean 0 and standard deviation $\frac{\alpha}{\sqrt{2\pi}}$ and reducing the result modulo 1 (i.e., a periodization of the normal distribution),

$$\forall r\in[0,1), \Psi_\alpha(r) = \sum_{k=-\infty}^{\infty}\frac{1}{\alpha}\exp -\pi\left(\frac{r-k}{\alpha}\right)^2 .$$

We define its discretization $\overline{\Psi_\alpha}$ as the discrete probability distribution obtained by sampling from Ψ_α, multiplying by q, and rounding to the closest integer modulo q. That is,

$$\overline{\Psi_\alpha}(i) = \int_{(i-\frac{1}{2})/q}^{(i+\frac{1}{2})/q}\Psi_\alpha(x)dx.$$

2.2 Quantum computing

Let I be the identity operator. We denote $\mathsf{U}^\dagger$ as the

Hermitian conjugate of a unitary operation U. For operations that use auxiliary inputs $|0^l\rangle$, we often omit them for simplicity. Quantum Fourier transformation QFT over $\mathbb{Z}_q^n$ is a map $|\boldsymbol{x}\rangle \mapsto \sum_{\boldsymbol{y}\in\mathbb{Z}_q^n} \omega_q^{\boldsymbol{x}\cdot\boldsymbol{y}} |\boldsymbol{y}\rangle$. We use the fact that there is a phase kickback algorithm and it maps $|x\rangle |0^l\rangle \mapsto \omega_q^x |x\rangle |0^l\rangle$. This algorithm can be achieved by controlled-U where unitary U has eigenvalue ω_q.

3. Search-to-decision reduction for the learning with errors problem

The learning with errors (LWE) problem has two main variants, the search-LWE problem and the decisional-LWE problem. The search $\mathsf{LWE}_{n,m,q,\chi}$ problem asks to find s chosen uniformly random from $\mathbb{Z}_q^n$ given m LWE samples $\mathcal{LWE}_{n,s,q,\chi} := \{(a,y) | a \xleftarrow{\$} \mathbb{Z}_q^n, e \leftarrow \chi, y := a\cdot s + e\}$. The decisional $\mathsf{LWE}_{n,m,q,\chi}$ problem asks to distinguish between $\mathcal{LWE}_{n,s,q,\chi}$ and a uniformly random distribution $\mathsf{R} := \{(a,r) | a \xleftarrow{\$} \mathbb{Z}_q^n, r \xleftarrow{\$} \mathbb{Z}_q\}$ by using m samples. We often represented samples from $\mathcal{LWE}_{n,s,q,\chi}^m$ (resp. R^m) in matrix form. For $(A,y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m$, each row of the matrix A and each row of the vector y correspond to an LWE sample.

The learning parity with noise (LPN) problem is the special case of $\mathsf{LWE}_{n,m,q,\chi}$ problem for $q = 2$ and the error distribution χ is the Bernoulli distribution Ber_μ.

In this section, we show a search-to-decision reduction using quantum computing. Our construction of the search-to-decision reduction consists of two parts. For the first part, we construct a predictor from the distinguisher of the decisional-LWE problem, and for the second part, we construct an algorithm that finds s using a predictor. This reduction strategy can be interpreted as making a search-to-prediction reduction and a prediction-to-decision reduction. We note that the idea of the search-to-decision reduction via prediction is the same as that of classical reduction by Micciancio and Mol [21], Applebaum, Ishai, and Kushilevitz [7] and Dottling [15].

We define a quantum distinguisher for the decisional-LWE problem.

Definition 1. *A quantum ϵ-distinguisher for the decisional $\mathsf{LWE}_{n,m,q,\chi}$ problem is unitary operation U_D and an auxiliary $|\mathsf{aux}\rangle$ such that, the last register of $\mathsf{U}_D |A,y\rangle |\mathsf{aux}\rangle |0\rangle$ is measured in computational basis, yielding the value $D(A,y) \in \{0,1\}$, then*

$$\begin{aligned}&\Pr[D(A,y) = 0 | s \xleftarrow{\$} \mathbb{Z}_q^n, (A,y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m] \\ &\quad - \Pr[D(A,r) = 0 | (A,y) \leftarrow \mathsf{R}^m] \\ &> \epsilon\end{aligned}$$

holds.

As in the definition, the last register of $\mathsf{U}_D |A,y\rangle |\mathsf{aux}\rangle |0\rangle$ is measured in the computational basis, in this paper, we denote this as $D(A,y)$.

Next, we define a quantum predictor for the LWE problem.

Definition 2. *A quantum (s,δ)-predictor is unitary operation U_P and an auxiliary $|\mathsf{aux}\rangle$ such that, for $a \xleftarrow{\$} \mathbb{Z}_q^n$, the last register of $\mathsf{U}_P |a\rangle |\mathsf{aux}\rangle |0\rangle$ is measured in computational basis, yielding the value $P(a)$, then*

$$\Pr[P(a) = a\cdot s \pmod q)] > \frac{1}{q} + \delta$$

holds.

3.1 Sample-preserve reduction

In this section, we propose a quantum sample-preserve reduction between the search-LWE and the decisional-LWE.

The following Lemma states that there is a prediction-to-decision reduction for the LWE problem.

We define $\mathsf{X}_{m,j}$ as an intermediate distribution between the LWE distribution $\mathcal{LWE}_{n,s,q,\chi}^m$ and R^m. In other words, $\mathsf{X}_{m,j} := \{(L_{m-j}, R_j) | L_{m-j} \leftarrow \mathcal{LWE}_{n,s,q,\chi}^{m-j}, R_j \leftarrow \mathsf{R}^j\}$. We note that $\mathsf{X}_{m,0}$ is equal to $\mathcal{LWE}_{n,s,q,\chi}^m$, and $\mathsf{X}_{m,m}$ is equal to R^m.

Lemma 1. *For $j \xleftarrow{\$} \{0,1,...,m-1\}$,*

$$\begin{aligned}&\Pr[D(A,y) = 1 | (A,y) \leftarrow \mathsf{X}_{m,j}] \\ &\quad - \Pr[D(A,y) = 1 | (A,y) \leftarrow \mathsf{X}_{m,j+1}] \\ &> \frac{\epsilon}{m}\end{aligned}$$

holds.

Proof. From the definition of the distinguisher U_D,

$$\begin{aligned}&\Pr[D(A,y) = 1 | (A,y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m] \\ &\quad - \Pr[D(A,r) = 1 | (A,y) \leftarrow \mathsf{R}^m] \\ &> \epsilon\end{aligned}$$

holds. From the triangular inequalities,

$$\begin{aligned}&\Pr[D(A,y) = 1 | (A,y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m] \\ &\quad - \Pr[D(A,y) = 1 | (A,y) \leftarrow \mathsf{R}^m] \\ &\leq \sum_{i=1}^{m} (\Pr[D(A,y) = 1 | (A,y) \leftarrow \mathsf{X}_{m,i}] \\ &\quad - \Pr[D(A,y) = 1 | (A,y) \leftarrow \mathsf{X}_{m,i+1}])\end{aligned}$$

holds. Therefore,

$$\begin{aligned}&\Pr[j = i](\Pr[D(A,y) = 1 | (A,y) \leftarrow \mathsf{X}_{m,i}] \\ &\quad - \Pr[D(A,y) = 1 | (A,y) \leftarrow \mathsf{X}_{m,i+1}]) \\ &= \frac{1}{m}(\Pr[D(A,y) = 1 | (A,y) \leftarrow \mathsf{X}_{m,i}]\end{aligned}$$

$$\begin{aligned}&- \Pr[D(A,y)=1|(A,y)\leftarrow \mathsf{X}_{m,i+1}])\\ &> \frac{\epsilon}{m}\end{aligned}$$

holds. □

Lemma 2. *There exists a unitary operation U_P using $(\mathsf{U}_D, |\mathsf{aux}\rangle)$ once, it satisfies for $j \xleftarrow{\$} \mathbb{Z}_q$, $L_{m-j-1} \leftarrow \mathcal{LWE}^{m-j-1}_{n,s,q,\chi}$, $R_j \leftarrow \mathsf{R}^j$, $a \xleftarrow{\$} \mathbb{Z}_q^n$, $c \xleftarrow{\$} \mathbb{Z}_q$, $e \leftarrow \chi$ and $r \xleftarrow{\$} \mathbb{Z}_q \setminus \{c\}$, the last register of $\mathsf{U}_P |L_{m-j-1},(a,c+e),R_j\rangle |\mathsf{aux}\rangle |0\rangle |0\rangle$ is measured in computational base, yielding the value $P(L_{m-j-1},(a,c+e),R_j)$, then*

$$\Pr[P(L_{m-j-1},(a,c+e),R_j)=a\cdot s] > \frac{1}{q} + \frac{\epsilon}{(q-1)m}$$

holds.

In the following, if the last qubit of

$$\mathsf{U}_P |L_{m-j-1},(a,c+e),R_j\rangle + |\mathsf{aux}\rangle |0\rangle |0\rangle$$

is measured in computational base, we denote this as $P(L_{m-j-1},(a,c+e),R_j)$.

Proof. $\mathsf{U}_P |L_{m-j-1},(a,c+e),R_j\rangle |\mathsf{aux}\rangle |0\rangle |0\rangle$ is a unitary operation of the following procedure.

1. Compute $(\mathsf{U}_D |(L_{m-j-1},(a,c+e),R_j)\rangle |\mathsf{aux}\rangle |0\rangle) |0\rangle$.
2. Apply a control unitary operation as follows; if the second-to-last register is in state $|1\rangle$, output c to the last register, else if it is in state $|0\rangle$, output $r \neq c$ to the last register.

Let us analyze the behavior of U_P. Since

$$\begin{aligned}&\Pr[P(L_{m-j-1},(a,c+e),R_j)=a\cdot s \land c=a\cdot s]\\ &=\Pr[c=a\cdot s]\Pr[D(L_{m-j-1},(a,c+e),R_j)=1|c=a\cdot s]\\ &=\frac{1}{q}\Pr[D(L_{m-j},R_j)=1]\end{aligned}$$

and

$$\begin{aligned}&\Pr[P(L_{m-j-1},(a,c+e),R_j)=a\cdot s \land c\neq a\cdot s]\\ &=\Pr[r=a\cdot s](\Pr[D(L_{m-j-1},(a,c+e),R_j)=0]\\ &\quad-\Pr[D(L_{m-j-1},(a,c+e),R_j)=0 \land c=a\cdot s])\\ &=\frac{1}{q-1}\{(1-\Pr[D(L_{m-j-1},R_{j+1})=1])\\ &\quad-\frac{1}{q}(1-\Pr[D(L_{m-j},R_j)=1])\}\end{aligned}$$

holds,

$$\begin{aligned}&\Pr[P(L_{m-j-1},(a,c+e),R_j)=a\cdot s]\\ &=\Pr[P(L_{m-j-1},(a,c+e),R_j)=a\cdot s \land c=a\cdot s]\\ &\quad+\Pr[P(L_{m-j-1},(a,c+e),R_j)=a\cdot s \land c\neq a\cdot s]\\ &=\frac{1}{q}\Pr[D(L_{m-j},R_j)=1]\\ &\quad+\frac{1}{q-1}\{(1-\Pr[D(L_{m-j-1},R_{j+1})=1])\\ &\quad-\frac{1}{q}(1-\Pr[D(L_{m-j},R_j)=1])\}\\ &=\frac{1}{q}+\frac{1}{q-1}(\Pr[D(A,y)=1|(A,y)\leftarrow \mathsf{X}_{m,j}]\\ &\quad-\Pr[D(A,y)=1|(A,y)\leftarrow \mathsf{X}_{m,j+1}])\\ &>\frac{1}{q}+\frac{\epsilon}{(q-1)m}\end{aligned}$$

holds. The last inequality follows from Lemma 1. In conclusion, we get

$$\Pr[P(L_{m-j-1},(a,c+e),R_j)=a\cdot s] > \frac{1}{q}+\frac{\epsilon}{(q-1)m}. \tag{4}$$

□

Next, let's consider the probability of outputting $a\cdot s$ for a given input x when the random coins used in the prediction algorithm is fixed. The following lemma states that, when the random coins used in the prediction algorithm is fixed, then the random coins are good, in a seance that, the predictor predicts inner product for significantly exceeds the $\frac{1}{q}$ of inputs $a \in \mathbb{Z}_q^n$, with some probability. Define the U'_P to be the same as the one construct in Lemma 2, except for some variables, such as j, L, R, c, e, r, are hardwired. The last register of $\mathsf{U}_P |L_{m-j-1},(a,c+e),R_j\rangle |\mathsf{aux}\rangle |0\rangle |0\rangle$ is measured in the computational basis, we denote this as $P'(a)$.

Lemma 3. *U'_P is a $(s, \frac{2\epsilon}{3(q-1)m})$-predictor with probability at least $\frac{\epsilon}{3(q-1)m}$ over choice of the random coins.*

Proof. A $(s, \frac{2\epsilon}{3(q-1)m})$-predictor satisfies the following (5).

$$\Pr[P'(a)=a\cdot s|a\xleftarrow{\$}\mathbb{Z}_q^n] > \frac{1}{q}+\frac{2\epsilon}{3(q-1)m}. \tag{5}$$

Define a set $G=\{(s,j,L,R,c,e,r)|\text{Inequality (5) holds}\}$. By the definition of G, when $s \xleftarrow{\$} \mathbb{Z}_q^n$, $j \xleftarrow{\$}$, $L \leftarrow \mathcal{LWE}^{m-j-1}_{n,s,q,\chi}$, $R \leftarrow \mathsf{R}^j$ and $x \xleftarrow{\$} \mathbb{Z}_q^n$, $c \xleftarrow{\$} \mathbb{Z}_q$ and $e \leftarrow \chi$, $r \xleftarrow{\$} \mathbb{Z}_q \setminus \{c\}$, then

$$\begin{aligned}&\Pr[P(L,(a,c+e),R)=a\cdot s]\\ &=\Pr[P(L,(a,c+e),R)=a\cdot s \land (s,j,L,R,c,e,r)\in G]\\ &\quad+\Pr[P(L,(a,c+e),R)=a\cdot s \land (s,j,L,R,c,e,r)\notin G]\\ &\le \Pr[(s,j,L,R,c,e,r)\in G]+\frac{1}{q}+\frac{2\epsilon}{3(q-1)m}\end{aligned}$$

holds. From Lemma 2,

$$\Pr[P(L,(a,c+e),R)=a\cdot s] > \frac{1}{q}+\frac{\epsilon}{(q-1)m}$$

holds. Therefore

$$\Pr[(s,j,L,R,c,e,r)\in G] \geq \frac{\epsilon}{3(q-1)m}$$

holds. □

We next show a prediction-to-decision reduction, that is, the expansion version of the quantum Goldreich-Levin theorem.

Theorem 1 (Expansion version of quantum Goldreich-Levin theorem)**.** *Let q be a prime. If there is a quantum (s,δ)-predictor $(\mathsf{U}_P, |\mathsf{aux}\rangle)$, then there is a quantum algorithm that finds s with probability at least $(\frac{q\delta}{q-1})^2$. It invokes U_P and $\mathsf{U}_P^\dagger$ once each and uses an auxiliary $|\mathsf{aux}\rangle$.*

Proof. We construct a quantum algorithm that finds s using a quantum (s,δ)-predictor U_P.

We denote the state obtained by applying U_P to $|a\rangle|\mathsf{aux}\rangle|0\rangle$ as follows,

$$\mathsf{U}_P|a\rangle|\mathsf{aux}\rangle|0\rangle = \sum_{j\in\mathbb{Z}_q}\alpha_{a,j}|a\rangle|\eta_{a,j}\rangle|a\cdot s+j\rangle .$$

First, prepare the superposition states

$$\frac{1}{\sqrt{q^n(q-1)}}\sum_{a\in\mathbb{Z}_q^n}\sum_{r\in\mathbb{Z}_q^*}|r\rangle|a\rangle|\mathsf{aux}\rangle|0\rangle$$

through the predictor U_P(apply the second to the last register), multiply the last register by the first register r, multiply the phase by ω_q^y according to the value of the last register y, divide the last register by the first register r(multiply r^{-1}), pass the states through conjugate transpose of the predictor and we get the states

$$|\phi\rangle := \frac{1}{\sqrt{q^n(q-1)}}\sum_{a,r,j}\omega_q^{r(a\cdot s+j)}\alpha_{a,j}|r\rangle|a\rangle|\eta_{a,j}\rangle|a\cdot s+j\rangle .$$

If we apply the states through conjugate transpose of the predictor $\mathsf{U}_P^\dagger$(apply the second to the last register), multiply the second register by the first register(denote this operation as M), and measure the second register in Fourier basis, the probability of yielding s is the square of the inner product of this state $|\phi\rangle$ and

$$\begin{aligned}
&|\psi\rangle\\
&:= \mathsf{U}_P\mathsf{M}^\dagger\mathsf{QFT}\frac{1}{\sqrt{q-1}}\sum_{r\in\mathbb{Z}_q^*}|r\rangle|s\rangle|\mathsf{aux}\rangle|0\rangle\\
&= \mathsf{U}_P\mathsf{M}^\dagger\left(\frac{1}{\sqrt{q^n(q-1)}}\sum_{b\in\mathbb{Z}_q^n}\sum_{r\in\mathbb{Z}_q^*}\omega_q^{b\cdot s}|r\rangle|b\rangle|\mathsf{aux}\rangle|0\rangle\right)\\
&= \mathsf{U}_P\mathsf{M}^\dagger\left(\frac{1}{\sqrt{q^n(q-1)}}\sum_{a\in\mathbb{Z}_q^n}\sum_{r\in\mathbb{Z}_q^*}\omega_q^{r(a\cdot s)}|r\rangle|ra\rangle|\mathsf{aux}\rangle|0\rangle\right)\\
&= \mathsf{U}_P\left(\frac{1}{\sqrt{q^n(q-1)}}\sum_{a,r}\omega_q^{r(a\cdot s)}|r\rangle|a\rangle|\mathsf{aux}\rangle|0\rangle\right)\\
&= \frac{1}{\sqrt{q^n(q-1)}}\sum_{a,r,j}\omega_q^{r(a\cdot s)}|r\rangle|a\rangle|\eta_{a,j}\rangle|a\cdot s+j\rangle .
\end{aligned}$$

Finally, we get

$$\begin{aligned}
&\Pr[s\text{ is measured}]\\
&= |\langle\psi|\phi\rangle|^2\\
&= \left|\frac{1}{q^n(q-1)}\sum_{a,r,j}\omega_q^{rj}|\alpha_{a,j}|^2\right|^2\\
&= \left|\frac{1}{q^n}|\alpha_{a,0}|^2 + \frac{1}{q^n(q-1)}\sum_{j\in\mathbb{Z}_q^*}(-|\alpha_{a,j}|^2)\right|^2\\
&> \left|\left(\frac{1}{q}+\delta\right) - \frac{1}{q-1}\left(1-\left(\frac{1}{q}+\delta\right)\right)\right|^2\\
&= \left(\frac{q\delta}{q-1}\right)^2 .
\end{aligned}$$

The second equality follows by the fact that for all elements $j\in\mathbb{Z}_q^*$, j determines a bijection $r\mapsto rj$ on $\mathbb{Z}_q$ and it maps 0 to 0. This result is consistent with the quantum Goldreich-Levin result where $q=2$ and is a successful generalization. □

Theorem 2. *Let q be a prime. If there is a quantum ϵ-distinguisher $(\mathsf{U}_D, |\mathsf{aux}\rangle)$ for the decisional $\mathsf{LWE}_{n,m,q,\chi}$ problem, then there is a quantum algorithm that solves the search $\mathsf{LWE}_{n,m,q,\chi}$ problem with probability at least $\frac{4q^2\epsilon^3}{27(q-1)^5m^3}$ using U_D and $\mathsf{U}_D^\dagger$ once each and an auxiliary $|\mathsf{aux}\rangle$.*

Proof. This theorem follows immediately from Lemma 3 and Theorem 1. □

We stress that Theorem 2 gives a quantum sample-preserving search-to-decision reduction for the LWE problem, i.e., we can find s with some polynomial probability with sample complexity m, where m is the number of instances required by the distinguisher to solve the decisional-LWE problem. Next, we consider the complexity of obtaining s with high probability using this algorithm in the following section. We use this algorithm as a basic building block of the amplified reduction algorithms.

3.2 Amplify the success probability

We show how to amplify the success probability of the reduction algorithm given in Section 3.1. However, this process increases query complexity and sample complexity.

We only consider a uniform distinguisher. This means that the auxiliary $|\mathsf{aux}\rangle$ is simply the computation space $|0^l\rangle$.

We propose an algorithm, Verify, that tests a candidate solution for the LWE problem. We first sample $(a_i, y_i)_{i\in[\mathcal{O}(n)]} \leftarrow \mathcal{LWE}^{\mathcal{O}(n)}_{n,s,q,\chi}$ and construct Verify to test a candidate s' by simply checking that $a_i \cdot s \approx y_i$. Here, we present the case where the error distribution is the discrete Gaussian distribution $\overline{\Psi_\alpha}$ where $\alpha < \frac{1}{8}$.

Lemma 4. *Let $\chi = \overline{\Psi_\alpha}$ where $\alpha < \frac{1}{8}$, we can construct an algorithm* Verify *using $\mathcal{O}(n)$ samples, and it satisfies the following functionality* (6) *with probability* $1 - \mathsf{negl}(n)$*(resp. any desired constant* $0 < p < 1$*)*

$$\mathsf{Verify}(s') = \begin{cases} 1 & \text{if } s' = s \\ 0 & \text{if } s' \neq s. \end{cases} \tag{6}$$

The description of the algorithm Verify *that satisfies the conditions of* (6) *can be given as follows: Initially, sample $(a_i, y_i)_{i\in[cn]} \leftarrow \mathcal{LWE}^{cn}_{n,s,q,\chi}$. Upon receiving input $s' \in \mathbb{Z}^n_q$,* Verify *works as follows.*

```
Verify($s'$) :
$count = 0$
for $i \in \{1, 2, \ldots, cn\}$
  if $|a_i \cdot s' - y_i| > \frac{q}{8}$, add 1 to $count$
if $count < \frac{cn}{2}$ output 1
  else output 0.
```

Proof. Let us analyze the probability that the Verify satisfies the condition (6).
Let $\beta = \Pr[|\chi| \geq \frac{q}{8}](< \frac{1}{2})$, $\delta = \frac{1}{2\beta} - 1$.

$$\begin{aligned}
&\Pr[\mathsf{Verify}\text{ satisfies (6)}] \\
&= \Pr[\mathsf{Verify}(s) = 1 \wedge \forall s' \neq s, \mathsf{Verify}(s') = 0] \\
&\geq \Pr[\mathsf{Verify}(s) = 1] \cdot \Pr[\forall s' \neq s, \mathsf{Verify}(s') = 0] \\
&\geq (1 - \Pr[\mathsf{Verify}(s) \neq 1]) \cdot \left(1 - \sum_{s' \neq s} \Pr[\mathsf{Verify}(s') = 1]\right) \\
&\geq (1 - e^{-\frac{\delta^2 \beta cn}{2+\delta}}) \cdot \left(1 - (q^n - 1)e^{-\frac{cn}{24}}\right) \\
&= 1 - \mathsf{negl}(cn)
\end{aligned}$$

The third inequality follows from Chernoff bound. Therefore, Verify satisfies (6) with probability $1 - \mathsf{negl}(n)$ for sufficiently large constant c. In addition, by choosing c to be sufficiently large, the success probability of the algorithm can be increased to any desired constant level regardless of n. □

We can use this Verify to amplify the success probability of the sample-preserving reduction algorithm by repetition. However, the success probability of our reduction can be increased more efficiently by the quantum-specific repetition technique "amplitude amplification [11]" than by simply judging the answer each time. We define a unitary $\mathsf{U}_{\mathsf{Reflection}}$, referred to as a reflection oracle in the context of amplitude amplification.

Definition 3. *A quantum reflection algorithm is a unitary operation $\mathsf{U}_{\mathsf{Reflection}}$ such that the following holds* (7)

$$\mathsf{U}_{\mathsf{Reflection}=\mathsf{I}-|s\rangle|0^l\rangle\langle s|\langle 0^l|} \tag{7}$$

holds.

Lemma 5. *We can construct a quantum algorithm $\mathsf{U}_{\mathsf{Reflection}}$ from* Verify *that satisfies the condition* (6)*.*

Proof. This lemma can be achieved by phase kickback. From Lemma 4 there exists a verification algorithm satisfying (6), then there exist an unitary operation such that

$$\mathsf{U}_{\mathsf{Verify}} |x\rangle |y\rangle |0\rangle = \begin{cases} |x\rangle |y\rangle |1\rangle & \text{if } x = s \wedge y = 0^l \\ |x\rangle |y\rangle |0\rangle & \text{if } x \neq s \vee y \neq 0^l \end{cases} \tag{8}$$

holds.

Consider the following quantum operation $\mathsf{U}_{\mathsf{Reflection}}$. When given $|x\rangle |y\rangle |0\rangle$, apply $\mathsf{U}_{\mathsf{Verify}}$, multiply the phase by $(-1)^z$ according to the value of the last register z and apply $\mathsf{U}^\dagger_{\mathsf{Verify}}$. We get $-|x\rangle |y\rangle |0\rangle$ when $x = s$ and $y = 0^l$ otherwise we get $|x\rangle |y\rangle |0\rangle$. This operator is indeed a quantum reflection algorithm.

□

Theorem 3. *Let q be a prime and $\chi = \overline{\Psi_\alpha}$ where $\alpha < \frac{1}{8}$. If there is a quantum ϵ-distinguisher U_D for the decisional $\mathsf{LWE}_{n,m,q,\chi}$ problem, then there is a quantum algorithm that solves the search $\mathsf{LWE}_{n,m',q,\chi}$ problem with probability $\Omega(\frac{\epsilon}{qm})$ using U_D and $\mathsf{U}^\dagger_D$ $\mathcal{O}(\frac{qm}{\epsilon})$ times, where $m' = m + \mathcal{O}(n)$.*

Proof. Initially, s is chosen uniform random from $\mathbb{Z}^n_q$, we get $(A, y) \leftarrow \mathcal{LWE}^m_{n,s,q,\chi}$ and samples random coins. From Lemma 1 and Theorem 2 we can construct a quantum algorithm U_S using U_D and $\mathsf{U}^\dagger_D$ once each, and that satisfies

$$|\langle s| \langle 0^l| \mathsf{U}_S |0^n\rangle |0^l\rangle|^2 > \frac{4q^2\epsilon^2}{9(q-1)^4 m^2} \tag{9}$$

with probability $\frac{\epsilon}{3m(q-1)}$ over choice of $s \xleftarrow{\$} \mathbb{Z}^n_q$, $(A, y) \leftarrow \mathcal{LWE}^m_{n,s,q,\chi}$ and random coins. From Lemma 4 and Lemma 5 we can construct a verification algorithm Verify (resp. a quantum algorithm $\mathsf{U}_{\mathsf{Reflection}}$) that satisfies (6) (resp. (7)) with constant probability using $\mathcal{O}(n)$ samples of $\mathcal{LWE}_{n,s,q,\chi}$.

Assuming that U_S satisfies (9), Verify satisfies (6), and $\mathsf{U}_{\mathsf{Reflection}}$ satisfies (7), consider the following procedure. The procedure is to compute

$$(-\mathsf{U}_S(\mathsf{I} - |0^n\rangle |0^l\rangle \langle 0^n| \langle 0^l|)\mathsf{U}_S^\dagger \mathsf{U}_{\mathsf{Reflection}})^k \mathsf{U}_S |0^n\rangle |0^l\rangle ,$$

measures states in the computational basis, test it by Verify. As shown in [11], if this is carried out for a suitably generated sequence of values of k, we can find s with the expected total number of executions of U_S and $\mathsf{U}_S^\dagger$ until a successful verification occurs is $\mathcal{O}(\frac{qm}{\epsilon})$. From the construction of U_S, we get the following conclusions. We can find s with probability $\Omega(\frac{\epsilon}{qm})$ using U_D and $\mathsf{U}_D^\dagger$ $\mathcal{O}(\frac{qm}{\epsilon})$ times, and with sample complexity $m + \mathcal{O}(n)$. □

We remark that our reduction holds for a variety of other error distributions. It simply requires that we can verify from the samples whether it is the correct answer or not given some input $s' \in \mathbb{Z}_q^n$. For example, the verification algorithm for the case where $q = 2$ and the error distributed from the Bernoulli distribution is given in Appendix A.

Next, we consider how we can raise the success probability of our reduction algorithm to $1 - o(1)$. Simply repeating the algorithm does not efficiently increase the success probability. There are two reasons why we cannot simply repeat the algorithm given in Section 3.1.

- Whether the predictor U_P has desired property(condition (5)) depends on the choice of $s \xleftarrow{\$} \mathbb{Z}_q^n$(see Lemma 1).
- And the amplitude amplification algorithm would keep running until it finds s in time inversely proportional to the advantage of U_P.

We can overcome the first problem by rerandomize the secret s. By sampling $s^* \xleftarrow{\$} \mathbb{Z}_q^n$ and using $(A, y') := (A, y + A \cdot s^*)$, easily follows that, (A, y') can be regarded as the samples of $\mathcal{LWE}_{n,s+s^*,q,\chi}$. The second problem can be overcome by parallel computing. For example, if we produce $\lceil \frac{3qm \log n}{\epsilon} \rceil$ of predictors, then there exist a predictor $U_{P,i}$ that has advantage $\frac{2\epsilon}{3(q-1)m}$ with probability at least $1 - \frac{1}{n}$. If any part of the parallel computation has an output that passes the verification algorithm, it is the answer. Hence we can find s with probability $1 - o(1)$ by computing in parallel. This algorithm is described in the following Fig. 1.

From Lemma 4, we can construct a verification algorithm Verify that satisfies (6) with probability $1 - o(1)$ using $\tilde{\mathcal{O}}(n)$ samples of $\mathcal{LWE}_{n,s,q,\chi}$. Hence, The above algorithm has success probability $1 - o(1)$, invokes U_D $\mathcal{O}(\frac{q^2 m^2 \log n}{\epsilon^2})$ times, and using $\tilde{\mathcal{O}}(\frac{qm^2}{\epsilon}) = \mathcal{O}(\frac{qm^2 \log n}{\epsilon}) + \mathcal{O}(n)$ samples of $\mathcal{LWE}_{n,s,q,\chi}$. We get the following corollary.

Reduction Algorithm with high success probability

```
Choose $\tilde{\mathcal{O}}(n)$ samples from $\mathcal{LWE}_{n,s,q,\chi}$, and construct $\mathsf{Verify}$.
for $i = 1, \ldots, \lceil \frac{3q \log n}{\epsilon} \rceil$ :
    Choose $m$ samples of LWE instances $(A_i, y_i)$.
    Sample a random vector $s_i^* \leftarrow \mathbb{Z}_q^n$,
    set $(A_i, y_i') := (A_i, y_i + A_i \cdot s_i^*)$, and construct $\mathsf{U}_{P,i}$
    Construct $\mathsf{Verify}_i(x) := \mathsf{Verify}(x - s_i^*)$ and $\mathsf{U}_{\mathsf{Verify},i}$.
Run the second reduction algorithm in parallel.
If there is a $s_j$ that passes the $j$-th verification test $\mathsf{Verify}_j$,
then output $s = s_j - s_j^*$.
```

Fig. 1 Reduction Algorithm with high success probability

Corollary 1. *Let q be a prime and $\chi = \overline{\Psi_\alpha}$ where $\alpha < \frac{1}{8}$. If there is a quantum ϵ-distinguisher U_D for the decisional $\mathsf{LWE}_{n,m,q,\chi}$ problem, then there is a quantum algorithm that solves the search $\mathsf{LWE}_{n,m',q,\chi}$ problem with probability $1 - o(1)$ using U_D and $\mathsf{U}_D^\dagger$ $\mathcal{O}(\frac{q^2 m^2 \log n}{\epsilon^2})$ times, where $m' = \tilde{\mathcal{O}}(\frac{qm^2}{\epsilon})$.*

4. Conclusion

In this section, we display the efficiency of our reduction algorithms. We also give the comparisons listed in Table 1. The sample-preserve one shows that we can find s with a probability at least $\frac{4q^2\epsilon^3}{27(q-1)^5 m^3}$ and query complexity 2. Compared to the previous sample-preserve reduction by [21], it dramatically reduces query complexity. The second algorithm give by Theorem 3 performs amplitude amplification and has $\mathcal{O}(\frac{q^2 m^2}{\epsilon^2})$ times higher success probability than the sample-preserve one, but the query complexity is $\mathcal{O}(\frac{qm}{\epsilon})$ times higher and the sample complexity increases by $\mathcal{O}(n)$. We stress that this trade-off is specific to quantum computation. Additionally, we get the reduction algorithm that has success probability $1 - o(1)$ with query complexity $\mathcal{O}(\frac{q^2 m^2 \log n}{\epsilon^2})$ and sample complexity $\tilde{\mathcal{O}}(\frac{qm^2}{\epsilon})$. Unfortunately, when amplifying the success probability to $1 - o(1)$, the advantage in the query/sample complexity compared to classical reductions seems diminishes and the distinguisher needs to be uniform.

Acknowledgements

This research was in part conducted under a contract of “Research and development on new generation cryptography for secure wireless communication services” among “Research and Development for Expansion of Radio Wave Resources (JPJ000254)”, which was supported by the Ministry of Internal Affairs and Communications, Japan. This work also was in part supported by JSPS KAKENHI Grant Numbers JP22H03590 and JP21H03395, JST-CREST JPMJCR22M1, and JST-AIP JPMJCR22U5.

References

[1] LWE challenge website. `https://www.latticechallenge.org/lwe_challenge/challenge.php`.

[2] Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In Helmut Alt and Afonso Ferreira, editors, *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes - Juan les Pins, France, March 14-16, 2002, Proceedings*, volume 2285 of *Lecture Notes in Computer Science*, pages 323–334. Springer, 2002.

[3] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer, 2010.

[4] Adi Akavia. *Learning noisy characters, MPC, and cryptographic hardcore predicates.* PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2008.

[5] Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. Cryptology ePrint Archive, Paper 2023/325, 2023. `https://eprint.iacr.org/2023/325`.

[6] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*, pages 595–618. Springer, 2009.

[7] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography with constant input locality. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, volume 4622 of *Lecture Notes in Computer Science*, pages 92–110. Springer, 2007.

[8] Nir Bitansky, Zvika Brakerski, and Yael Tauman Kalai. Constructive post-quantum reductions, 2022.

[9] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 575–584. ACM, 2013.

[10] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In Rafail Ostrovsky, editor, *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 97–106. IEEE Computer Society, 2011.

[11] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation, 2002.

[12] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 523–552. Springer, 2010.

[13] Orestis Chardouvelis, Vipul Goyal, Aayush Jain, and Jiahui Liu. Quantum key leasing for PKE and FHE with a classical lessor. *CoRR*, abs/2310.14328, 2023.

[14] Yevgeniy Dodis, Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Public-key encryption schemes with auxiliary inputs. In Daniele Micciancio, editor, *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*, volume 5978 of *Lecture Notes in Computer Science*, pages 361–381. Springer, 2010.

[15] Nico Döttling. Low noise LPN: KDM secure public key encryption and sample amplification. In Jonathan Katz, editor, *Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings*, volume 9020 of *Lecture Notes in Computer Science*, pages 604–626. Springer, 2015.

[16] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Cynthia Dwork, editor, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 197–206. ACM, 2008.

[17] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In David S. Johnson, editor, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA*, pages 25–32. ACM, 1989.

[18] Elena Grigorescu, Swastik Kopparty, and Madhu Sudan. Local decoding and testing for homomorphisms. In Josep Díaz, Klaus Jansen, José D. P. Rolim, and Uri Zwick, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, 9th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2006 and 10th International Workshop on Randomization and Computation, RANDOM 2006, Barcelona, Spain, August 28-30 2006, Proceedings*, volume 4110 of *Lecture Notes in Computer Science*, pages 375–385. Springer, 2006.

[19] Jonathan Katz and Ji Sun Shin. Parallel and concurrent security of the HB and HB$^+$ protocols. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 73–87. Springer, 2006.

[20] Hongwei Li. Quantum algorithms for the goldreich-levin learning problem. *Quantum Inf. Process.*, 19(10):395, 2020.

[21] Daniele Micciancio and Petros Mol. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 465–484. Springer, 2011.

[22] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 700–718. Springer, 2012.

[23] P Newton. *Novel Linearity Tests with Applications to Lattices and Learning Problems.* PhD thesis, UC Riverside, 2022.

[24] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 333–342. ACM, 2009.

[25] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In David A. Wagner, editor, *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*, pages 554–571. Springer, 2008.

[26] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93. ACM, 2005.

[27] Kyohei Sudo, Masayuki Tezuka, Keisuke Hara, and Yusuke Yoshida. Quantum search-to-decision reduction for the LWE problem. In Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne, editors, *Progress in Cryptology - AFRICACRYPT 2023 - 14th International Conference on Cryptology in Africa, Sousse, Tunisia, July 19-21, 2023, Proceedings*, volume 14064 of *Lecture Notes in Computer Science*, pages 395–413, Cham, 2023. Springer.

[28] Vinod Vaikuntanathan. Lattices, learning with errors and post-quantum cryptography. `https://people.csail.mit.edu/vinodv/CS294/lecturenotes.pdf`.

Appendix A: Search-to-decision reduction for the LPN problem

We show that there is a quantum search-to-decision reduction for the learning parity with noise problem(Table A· 1). First, from Theorem 2 we immediately obtain the following corollary.

Corollary 2. *If there is a quantum ϵ-distinguisher U_D for the decisional $\mathsf{LWE}_{n,m,2,\mathsf{Ber}_\mu}$ problem, then there is a quantum algorithm that solves the search $\mathsf{LWE}_{n,m,2,\mathsf{Ber}_\mu}$ problem with probability at least $\frac{16\epsilon^3}{27m^3}$ using U_D and $\mathsf{U}_D^\dagger$ once each.*

As in the case of the LWE problem, we can amplify the success probability by constructing an algorithm Verify that judges the solution.

Lemma 6. *We can construct an algorithm Verify_{LPN}, and it satisfies the following functionality (A· 1) with desired probability $0 < c < \frac{2^n-1}{2^n}$.*
For all $x \in \{0,1\}^n$,

$$\mathsf{Verify}_{LPN}(x) = \begin{cases} 1 & \textit{if } x = s \\ 0 & \textit{if } x \neq s. \end{cases} \qquad \text{(A· 1)}$$

(1) Proof of Lemma 6.

Initially, sample $(A, y) \leftarrow \mathcal{LPN}^l_{s,\mu}$, where $A \in \{0,1\}^{l\times n}$ is a random Boolean matrix, $l = \left\lceil -\left(\frac{6}{\left(\frac{1}{2}-\mu\right)^2}\log_e\left(\frac{1}{2}\left(\frac{1}{2^n}-\frac{c}{2^n-1}\right)\right)\right)\right\rceil = \mathcal{O}(n)$ and $y = A \cdot s \oplus e$ is a noisy inner products, note that $e \in \{0,1\}^l$ is errors distributed from Ber^l_μ. Upon receiving input $x \in \{0,1\}^n$, Verify_{LPN} works as follows.

```
$\mathsf{Verify}_{LPN}(x)$ :
if $|weight(A\cdot x+y)-\mu l| < \frac{1}{2}(\frac{1}{2}-\mu)l$
    then output 1
else output 0.
```

Note that the function $weight(\cdot)$ outputs the Hamming distance. If $x = s$, since $A\cdot x + e = y$, $A\cdot x + y = e$. Since e is distributed from the Bernoulli distribution Ber^l_μ, $\mathbb{E}(weight(A\cdot x+y)) = \mathbb{E}(weight(e)) = \mu l$. If $x \neq s$, $A\cdot x + y$ is uniformly random, since A is sampled uniformly random. Therefore $\mathbb{E}(weight(A\cdot x+y)) = \frac{1}{2}l$. Let us analyze the probability that the Verify_{LPN} satisfies the condition (A· 1).

$$\begin{aligned}
&\Pr[\mathsf{Verify}_{LPN} \text{ satisfies (A· 1)}] \\
&= \Pr[\mathsf{Verify}_{LPN}(s) = 1 \land \forall s' \neq s, \mathsf{Verify}_{LPN}(s') = 0] \\
&\geq \Pr[\mathsf{Verify}_{LPN}(s) = 1] \cdot \Pr[\forall s' \neq s, \mathsf{Verify}_{LPN}(s') = 0] \\
&\geq \Pr[\mathsf{Verify}_{LPN}(s) = 1] \\
&\quad \times \left(1 - \sum_{s'\neq s}\Pr[\mathsf{Verify}_{LPN}(s') = 1]\right) \\
&\geq \left(1 - 2e^{-\frac{l}{12\mu}\left(\frac{1}{2}-\mu\right)^2}\right)\left(1 - (2^n-1)\left(2e^{-\frac{l}{6}\left(\frac{1}{2}-\mu\right)^2}\right)\right) \\
&\geq \left(1 - \left(\frac{1}{2^n} - \frac{c}{2^n-1}\right)^{\frac{1}{2\mu}}\right) \\
&\quad \times \left(1 - (2^n-1)\left(\frac{1}{2^n} - \frac{c}{2^n-1}\right)\right) \\
&\geq \left(1 - \left(\frac{1}{2^n} - \frac{c}{2^n-1}\right)\right)\left(1 - 2^n\left(\frac{1}{2^n} - \frac{c}{2^n-1}\right)\right) \\
&\geq \left(1 - \frac{1}{2^n}\right)\frac{2^n c}{2^n-1} \\
&= c
\end{aligned}$$

The second inequality follows from union bound, and the third inequality follows from Chernoff bound. □

Corollary 3. *If there is a quantum ϵ-distinguisher U_D for the decisional $\mathsf{LWE}_{n,m,2,\mathsf{Ber}_\mu}$ problem, then there is a quantum algorithm that solves the search $\mathsf{LWE}_{n,m',2,\mathsf{Ber}_\mu}$ problem with probability $\Omega(\frac{\epsilon}{m})$ using U_D and $\mathsf{U}_D^\dagger$ $\mathcal{O}(\frac{m}{\epsilon})$ times, where $m' = m + \mathcal{O}(n)$.*

The proof of this corollary is given in the same way as in Theorem 3.

Table A· 1 Comparison of the algorithms performance. n is a size of the LPN problem, m is the number of instances required by the distinguisher to solve the decisional LPN problem, ϵ is the advantage of the distinguisher.

	Success probability (at least)	Query complexity	Sample complexity	Classical/Quantum
KS06[19]	$\frac{\epsilon}{4}$	$\mathcal{O}(\frac{n\log n}{\epsilon^2})$	$\mathcal{O}(\frac{mn\log n}{\epsilon^2})$	Classical
AIK07[7]	$\Omega(\frac{\epsilon^3}{n})$	$\mathcal{O}(\frac{n^2}{\epsilon^2})$	m	Classical
Cor.2	$\frac{16\epsilon^3}{27m^3}$	2	m	Quantum
Cor.3	$\Omega(\frac{\epsilon}{m})$	$\mathcal{O}(\frac{m}{\epsilon})$	$m+\mathcal{O}(n)$	Quantum

Appendix B: Classical search-to-decision reduction for the LWE problem

B.1 A simple reduction

In this section we give a simple classical search-to-decision reduction by [28]. It is based on the reduction given by Regev [26] and is useful for comparing efficiency.

Definition 4. *A (classical) algorithm D said to be a ϵ-distinguisher for the decisional $\mathsf{LWE}_{n,m,q,\chi}$ problem if $|\Pr[D(A,y)=1|s \xleftarrow{\$} \{0,1\}^n, (A,y) \leftarrow \mathcal{LWE}^m_{n,s,q,\chi}] - \Pr[D(A,r)=1|A \xleftarrow{\$} \mathbb{Z}_q^{m\times n}, r \xleftarrow{\$} \mathbb{Z}_q^m]| > \epsilon$ holds.*

The algorithm described in Fig. A· 1 solves the search $\mathsf{LWE}_{n,m',q,\chi}$ problem with probability $1-o(1)$ using D $\tilde{\mathcal{O}}(\frac{nq}{\epsilon^2})$ times where $m' = \tilde{\mathcal{O}}(\frac{nmq}{\epsilon^2})$. For a detailed analysis, please refer to [28].

```
Classical reduction algorithm
for $i = 1, \dots, n$ :
  for $j = 0, \dots, q-1$ :
    for $l = 1, \dots, L = \tilde{\mathcal{O}}(\frac{1}{\epsilon^2})$ :
      Choose a fresh block of LWE instances $(A_l, y_l)$.
      Sample a random vector $c_l \leftarrow \mathbb{Z}_q^m$,
      and let $C_l \in \mathbb{Z}_q^{m\times n}$ be the matrix whose
      i-th row is $c_l$, and whose other entries are all zero.
      Let $A'_l := A_l + C_l$, and $y'_l := y_l + j \cdot c_l$.
      Run the distinguisher $D(A'_l, b'_l)$
        and let the output be called $d_l$.
    If $maj(d_1, ..., d_L) = 1$ (meaning that the distinguisher
      guesses LWE) then set $s_i = j$.
    Else, continue to the next iteration of the loop.
Output $s = s_1 \dots s_n$.
```

Fig. A· 1 Reduction Algorithm with high success probability

B.2 Complexity of MM11 [21]

In this section, we give a brief analysis of the search-to-decision reduction by Micciancio and Mol [21]. Their search-to-decision reduction for LWE is shown via search-to-decision reduction for the knapsack functions. This induces a negligible fraction of loss in the success probability. Let δ be an advantage of the distinguisher. From ([21], Proposition3.9 and Lemma3.4) the success probability of the search-to-decision reduction for the knapsack functions is $\frac{\epsilon}{3}$ where $\epsilon \geq \left(\frac{{d^*}^3\tilde{\delta}}{\tilde{d}^3(d^*-1)}\right)(2-\frac{\pi^2}{6})$ and $\tilde{\delta}$ is some noticeable such that $\tilde{\delta} \leq \delta$. Using the fact that $d^* \geq s$ and $\tilde{d} \leq 2ms^2$, we have $\frac{\epsilon}{3} = \Omega(\frac{\tilde{\delta}}{m^3s^4})$. Substituting q for s, we get the success probability of their search-to-decision reduction for LWE $\Omega(\frac{\tilde{\delta}}{m^3q^4}) - \mathsf{negl}(n)$.

In ([21], Lemma3.4), they use Significant Fourier Transform [4] with $\tau = \frac{\epsilon^2}{4}$, $N = |\mathbb{Z}^l_{d^*}|$ and $\|f\|_2 = \|f\|_\infty = 1$. The running time of Significant Fourier Transform is at most $\tilde{\Theta}(\log N(\frac{\|f\|_2^2}{\tau})^{1.5}(\frac{\|f\|_\infty^2}{\eta^2})^2 \lg\frac{1}{\mu})$ for $\eta = \Theta(min\{\tau, \sqrt{\tau}, \frac{\tau}{\|f\|_\infty}\})$ and $\mu = 1/\mathcal{O}((\frac{\|f\|_\infty^2}{\tau})^{1.5}\log N)$. Substituting $\tau = \frac{\epsilon^2}{4}$, $N = d^*m$ and $\|f\|_2 = \|f\|_\infty = 1$, we get $\tilde{\Theta}(\log N(\frac{\|f\|_2^2}{\tau})^{1.5}(\frac{\|f\|_\infty^2}{\eta})^2 \lg\frac{1}{\mu}) = \tilde{\mathcal{O}}(\frac{\log(d^*l)}{\epsilon^{11}})$. Hence From ([21], Proposition3.9 and Lemma3.4), the query complexity of the search-to-decision reduction for LWE is $\tilde{\Theta}(\frac{\log(d^*m)}{\epsilon^{11}})\mathcal{O}(1) = \tilde{\mathcal{O}}(\frac{\log(d^*m)}{\epsilon^{11}})$ where d^* is some polynomial such that $d^* \geq q$.

Kyohei Sudo is now a doctoral student in the Graduate School of Engineering Science, Osaka University. He received the B.S. and M.S. degrees from Tokyo Institute of Technology in 2020 and 2022, respectively.

Keisuke Hara received the B.S., M.S., and Ph.D. degrees from Tokyo Institute of Technology in 2017, 2019, and

2022, respectively. He is currently Researcher in Cryptography Platform Research Team, National Institute of Advanced Industrial Science and Technology (AIST), and also serves as Visiting Assistant Professor at Yokohama National University. His research interests include cryptography and information security.

Masayuki Tezuka is now a project assistant professor of Tokyo Institute of Technology. He received B.S. degree from Tokyo Metropolitan University in 2010. He received M.S. and D.S. degrees from Tokyo Institute of Technology in 2019 and 2022, respectively.

Yusuke Yoshida received the B.S., M.S., and Ph.D. degrees from Tokyo Institute of Technology in 2017, 2019, and 2022, respectively. Currently, he is an assistant professor in the School of Computing, Tokyo Institute of Technology. His interest includes public-key cryptography and information security.