



Title	Quantum Reductions from One-Wayness to Unpredictability and Quantum Public Key Encryption
Author(s)	数藤, 恭平
Citation	大阪大学, 2026, 博士論文
Version Type	VoR
URL	https://doi.org/10.18910/105550
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

Quantum Reductions from One-Wayness to
Unpredictability and Quantum Public Key Encryption

KYOHEI SUDO

MARCH 2026

Quantum Reductions from One-Wayness to
Unpredictability and Quantum Public Key Encryption

A dissertation submitted to
THE GRADUATE SCHOOL OF ENGINEERING SCIENCE
THE UNIVERSITY OF OSAKA
in partial fulfillment of the requirements for the degree of
DOCTOR OF PHILOSOPHY IN SCIENCE

BY

KYOHEI SUDO

MARCH 2026

Abstract

Cryptography is the science and practice of designing computing and communication systems that are secure in the presence of adversaries. Among the central topics in cryptographic research, public-key encryption enables secure communication between two parties, while digital signatures provide guarantees on the authenticity of information.

To prove the security of cryptographic schemes, we use *reductions*. Reduction is a fundamental concept in computer science. When problem A is reduced to problem B, it implies that B is at least as hard as A. To show such a relationship, we usually build a reduction algorithm that solves A efficiently using an algorithm that solves B as a subroutine. Such reductions not only establish the security of the cryptographic primitives, but also give a computational complexity perspective. For example, one can identify the minimal assumption on which cryptographic systems can be based.

The existence of one-way functions is considered a minimal assumption in cryptography. In other words, the existence of one-way functions is essential for the existence of any cryptographic primitive. A function f is said to be one-way if, given $f(x)$, it is computationally infeasible to efficiently recover a corresponding preimage. While one-wayness is a minimal assumption, it is also known to suffice for deriving important cryptographic primitives such as symmetric-key encryption and digital signatures. Cryptographic primitives can thus be divided into those that can be derived from one-way functions and those that cannot. Cryptographic primitives that can be derived from one-way functions are referred to as *Minicrypt*. In this way, one-way functions play a central role in providing a hierarchical understanding of modern cryptographic theory.

When quantum communication and computation are incorporated into cryptographic protocols, it becomes possible to derive a broader class of cryptographic primitives from one-way functions. For example, while there is evidence that public-key encryption cannot be constructed from one-way functions alone in the classical setting, recent works have shown that quantum public-key encryption can be constructed from one-way functions when quantum communication channels are available. Thus, even without altering the classical boundaries, incorporating quantum communication and computation leaves ample room for phenomena that differ from those observed in the classical setting. The class of cryptographic primitives that can be constructed from one-way functions, assuming quantum computation and communication, is referred to as *MiniQCrypt*. As quantum technologies continue to advance and the realization of quantum communication and quantum computers becomes increasingly plausible, the study of one-way functions must be revisited and discussed within these quantum frameworks.

We identify two main challenges in this area. The first challenge is to generalize the quantum reduction from one-wayness to unpredictability. The classical reduction from one-wayness to unpredictability, known as the Goldreich–Levin theorem, is not only fundamental in cryptography but also plays an important role in computational complexity theory. A quantum analogue of this theorem was established by Adcock and Cleve. However, whether the quantum Goldreich–Levin theorem holds not only in the binary setting but also over more general domains such as $\mathbb{Z}_q$ remains a nontrivial open problem. The second challenge

concerns the construction of quantum public-key encryption from one-way functions under more realistic assumptions. Although it is known that quantum public-key encryption can be constructed from one-way functions, an important question is whether such constructions remain possible when practical considerations and realistic security models are taken into account. In particular, prior constructions require the use of powerful quantum computers to generate quantum public keys. From a practical perspective, protocols that use only tensor-product states of single qubits, similar to those employed in quantum key distribution, are more desirable. Moreover, existing security definitions often assume that the generated quantum public key can be transmitted intact, which is unrealistic in practice. Instead, security should be analyzed under the assumption that the quantum channel is insecure and may be subject to tampering or eavesdropping.

In this thesis, we provide affirmative answers to the two challenges in the MiniQCrypt setting described above. First, we present a quantum reduction from one-wayness to unpredictability over the domain $\mathbb{Z}_q$, thereby generalizing the quantum Goldreich–Levin theorem beyond the binary domain. Additionally, as an application of the generalized quantum Goldreich–Levin reduction, we construct a quantum search-to-decision reduction for the *learning with errors* (LWE) problem. The LWE problem is widely regarded as a fundamental computational assumption for post-quantum cryptography. There are two major variants: search LWE and decisional LWE. We establish a reduction between these two variants using quantum computation. Given the central role of LWE in post-quantum cryptography, it is of significant importance to study its structural properties in the quantum setting. Second, we formalize a security notion for quantum public-key encryption and provide a construction satisfying this notion based solely on the assumption of one-way functions. In exchange for achieving an idealized level of security, our construction is based on the assumptions of a random oracle and individual attacks.

These contributions provide a complexity-theoretic understanding of which quantum cryptographic primitives can be reduced to one-way functions. Moreover, the quantum search-to-decision reduction for the LWE problem offers a theoretical analysis of the security of post-quantum cryptography in the presence of quantum adversaries. Finally, the construction of quantum public-key encryption from one-way functions highlights the advantage of quantum communication channels over classical communication channels.

Contents

1	Introduction	3
1.1	Backgrounds	3
1.2	Overview	5
1.3	Outline	6
2	Preliminaries	9
2.1	Basics of Cryptography	9
2.1.1	One-Way Function	11
2.1.2	Minimal Assumption in Quantum Cryptography	12
2.1.3	The Learning with Errors Problem	12
2.2	Quantum Computing	13
2.3	Theoretical Foundations	16
2.4	Notations and Abbreviations	16
3	Quantum Reduction for One-Wayness to Unpredictability	19
3.1	Introduction	19
3.1.1	Backgrounds	19
3.1.2	Our Contributions	19
3.1.3	Concurrent Work of Quantum Goldreich-Levin Theorem	20
3.1.4	Review of the Quantum Goldreich-Levin Theorem	20
3.2	Quantum Goldreich-Levin Theorem over $\mathbb{Z}_q$	23
3.3	Discussions	25
3.3.1	Classical Reduction vs Quantum Reduction	25
3.3.2	Relationship with Bernstein-Vazirani Algorithm	26
4	Quantum Search-to-Decision Reduction for the Learning with Errors Problem	27
4.1	Introduction	27
4.1.1	Backgrounds	27
4.1.2	Our Contributions	28
4.1.3	Technical Overview	30
4.2	Quantum Reduction Algorithms	30
4.2.1	Sample-Preserve Reduction	31
4.2.2	Amplify the Success Probability	33
4.A	Quantum Search-to-Decision Reduction for the LPN Problem	37
4.B	Classical Reduction	38
4.B.1	A Simple Reduction	38
4.B.2	Classical Sample-Preserve Reduction	38

5	Practical Quantum Public Key Encryption from One-way Functions	41
5.1	Introduction	41
5.1.1	Backgrounds	41
5.1.2	Our Contributions	42
5.1.3	Technical Overview	44
5.1.4	Related Work	44
5.2	Quantum Key Encapsulation Mechanism	45
5.3	Building Blocks	47
5.4	Construction	48
5.5	Security Proofs	49
5.6	Discussions	54
5.A	Security against Round Individual Attack	55
6	Conclusion	59
	List of Publications	63
	Bibliography	65

Chapter 1

Introduction

1.1 Backgrounds

When one wishes to transmit a message while hiding it from anyone other than the intended recipient, or to produce evidence that information has not been tampered with, such goals can be achieved by employing cryptographic techniques: encryption schemes in the former case, and digital signatures in the latter. The study of the construction of such protocols, their computational efficiency, and their security properties is known as cryptographic theory. Today, cryptographic protocols whose security is guaranteed by cryptographic theory operate behind the scenes of many everyday technologies, including the Internet, Bitcoin, and electronic payment systems.

In modern cryptography, the security of cryptographic protocols is required to be supported by rigorous theoretical proofs. Unfortunately, establishing such security guarantees inevitably relies on certain computational assumptions [IL89], namely, the presumed hardness of specific computational problems. For example, the security of the RSA cryptosystem [RSA78], a well-known public-key encryption (PKE) scheme, relies on the RSA assumption, a computational hardness assumption that is closely related to the hardness of integer factorization.

To prove the security of cryptographic schemes, we use *reductions*. Reduction is a fundamental concept in computer science. When problem A is reduced to problem B, it implies that B is at least as hard as A. To show such a relationship, we usually build a reduction algorithm that solves A efficiently using an algorithm that solves B as a subroutine. Such reductions not only establish the security of the cryptographic primitives but also give a computational complexity perspective. For example, one can identify the minimal assumption on which cryptographic systems can be based. In fact, one-way functions (OWFs) are known to serve as a minimal assumption in cryptography.

A OWF is a function that is efficiently computable but whose inverse cannot be efficiently computed. It serves as a minimal assumption in cryptography: The existence of any cryptographic primitive implies the existence of OWFs, and conversely, the existence of OWFs enables the construction of many useful cryptographic tools. As shown in Figure 1.1, it is known that a variety of cryptographic primitives can be constructed in a step-by-step manner starting from OWFs. For example, OWFs imply hard-core bit [GL89], pseudorandom generators (PRGs) [BM82; Hås+99], pseudorandom functions (PRFs) [GGM84], symmetric-key encryption (SKE) [GGM84; Hås+99; BN08], and digital signature (DS) [Rom90].

Although many cryptographic primitives can be constructed from OWFs, there exist cryptographic primitives that are unlikely to be derived from them. Impagliazzo and Rudich demonstrated that OWFs are insufficient to imply the existence of PKE in a black-box manner [IR89]. Furthermore, they discussed the implications for computational complexity,

highlighting the distinction between different *possible worlds* in cryptography.

Informally, P and NP are classes of computational problems: P consists of problems that can be solved efficiently, while NP consists of problems whose solutions can be verified quickly given an appropriate hint. It is well known that whether our world satisfies $P \neq NP$ has not yet been proven, although it is widely believed to be true. Moreover, even if $P \neq NP$ holds, there remain multiple possible worlds: one in which PKE exists and another in which OWFs exist but PKE does not (or even one where OWFs themselves do not exist). In cryptography, these possible worlds are clearly distinguished and are referred to as "Cryptomania" and "Minicrypt", respectively. What can(not) be reduced from OWFs is a central subject of study in cryptography, as it helps to computationally distinguish and understand the landscape of cryptographic primitives. We discuss these distinctions more formally in Preliminaries (Chap. 2), where we review the notion of complexity class and the different possible worlds in cryptography.

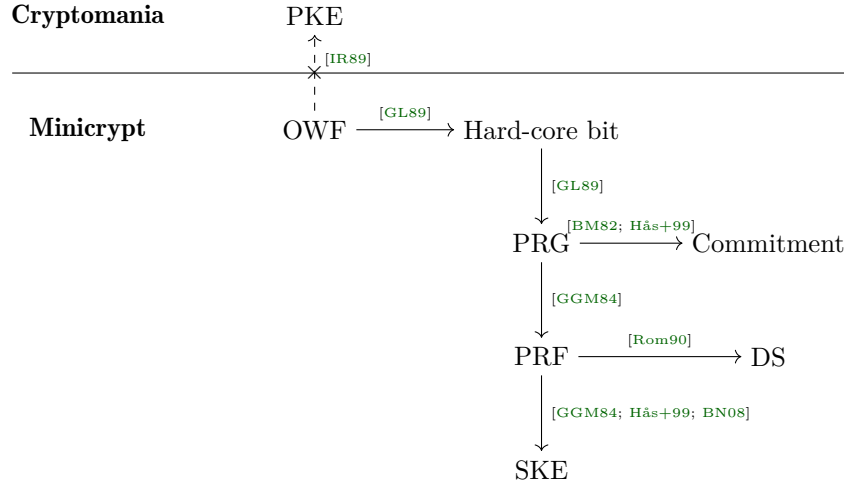


Figure 1.1: Minicrypt : Relationships among cryptographic primitives based on OWFs.

In the classical classification of cryptographic worlds, the so-called Cryptomania includes PKE, key exchange, oblivious transfer, and multi-party computation [IR89]. It has been suggested that these primitives cannot be constructed from OWFs alone; in other words, their construction is believed to require computational assumptions stronger than OWFs.

Although this classification holds in the classical setting, the situation changes significantly when quantum computation and quantum communication are allowed. For instance, key distribution can be achieved with information-theoretic security via quantum key distribution (QKD) [BB84]. Moreover, quantum oblivious transfer and quantum multi-party computation can be constructed from OWFs alone [Gri+21; Bar+21]. In this way, the line of research that investigates which quantum-secure cryptographic primitives can be constructed, and which cannot, starting from one-way functions, is referred to as MiniQCrypt, the quantum analogue of Minicrypt.

Quantum computing has undergone significant development in both theory and experiment since its concept was proposed by Feynman in 1981 [Fey81]. Today, quantum computers consisting of tens to hundreds of qubits, the fundamental units of quantum computation, are gradually being realized, and their potential application is being explored in areas such as quantum system simulation [Llo96], quantum chemistry [Asp+05], and quantum machine learning [Bia+17].

Quantum communication has also been steadily advancing, and some of them are already becoming a reality. For example, in 2017, a Chinese research team successfully demonstrated QKD scheme between a satellite and ground stations [Lia+17].

The impact of quantum computing on cryptography is profound. For example, quantum algorithms pose serious threats to widely deployed classical cryptographic schemes; a prominent example is Shor’s algorithm [Sho99], which enables efficient attacks on RSA and other public-key cryptosystems. On the other hand, if we make use of quantum computing and quantum communication, there are some cryptographic primitives that are classically impossible. For example, quantum money [Wie83], copy protection [Aar09], and certified deletion [BI20].

As quantum technologies mature, bringing large-scale quantum computation and practical quantum communication closer to reality, it becomes essential to re-examine the role of one-way functions within a fundamentally quantum setting. This issue serves as the primary focus of this thesis.

1.2 Overview

This thesis investigates which cryptographic primitives can be constructed from OWFs when quantum computation and quantum communication are available. Our approach is twofold. First, we develop a generalized quantum reduction from one-wayness to unpredictability by extending the quantum Goldreich-Levin theorem by Adcock and Cleve [AC02]. As an application of this result, we also derive a quantum search-to-decision reduction for the Learning with Errors (LWE) problem, illustrating the usefulness of the generalized theorem in concrete cryptographic settings. Second, we give a construction of quantum public-key encryption (QPKE) solely from OWFs, addressing practical limitations that previous works did not consider.

As our first approach, we focus on the generalization of the quantum Goldreich-Levin theorem [GL89]. The Goldreich-Levin theorem has been extensively studied and various generalizations have been proposed. For example, the quadratic Goldreich-Levin Theorems by [TW11], the unpredictability of $x \cdot s \pmod{q}$ shown in [GRS95; Dod+10], and the high-dimensional Goldreich-Levin Theorem by [NRW23]. A quantum analogue of the Goldreich-Levin theorem, which derives a quantum-secure hardcore bit from a quantum one-way function, was given by Adcock and Cleve [AC02]. However, unlike in the classical setting, no generalizations of the quantum Goldreich-Levin theorem were known, leaving open the question of whether other forms of quantum-secure hardcore bits could be derived. In Chapter 3 of this thesis, we address this gap by presenting a generalization of the quantum Goldreich-Levin theorem. Specifically, we show that a quantum-secure hardcore bit of the form $x \cdot s \pmod{q}$ can be constructed from a quantum one-way function. We call this generalized theorem as quantum Goldreich-Levin theorem over $\mathbb{Z}_q$.

The LWE problem is a computational hardness assumption introduced by Regev [Reg05]. The hardness of the LWE assumption enables promising post-quantum cryptographic protocols. For example, CRYSTALS-Kyber [Bos+18], lattice-based public-key cryptography selected in the NIST post-quantum cryptography standardization process.

The LWE problem has two major variants: the search LWE problem and the decisional LWE problem. Informally, the search LWE problem asks one to recover a secret vector from a system of linear equations corrupted by noise, whereas the decisional LWE problem asks one to distinguish the LWE distribution from the uniform distribution. Several classical reductions have been proposed, including Regev’s original reduction [Reg05] and the sample-preserving reductions by Micciancio and Mol [MM11]. However, it remained an open question whether quantum computation could be leveraged to improve such reductions.

Interestingly, a direct application of the quantum Goldreich-Levin theorem over $\mathbb{Z}_q$ is the quantum search-to-decision reduction for the LWE problem. In Chapter 4 of this thesis, we present a new quantum search-to-decision reduction for LWE. By exploiting quantum

computation, our quantum reduction achieves a quantum advantage over classical reductions in multiple respects. This demonstrates that quantum reductions can provide concrete improvements in the theoretical analysis of LWE, strengthening the foundations of post-quantum cryptography.

As our second approach, we focus on the QPKE from the OWFs. The quantum Goldreich–Levin theorem can be seen merely as a refinement of MiniQCrypt. However, MiniQCrypt can even alter the boundary between Cryptomania and Minicrypt. Public-key encryption (PKE) is one of the cryptographic primitives whose boundaries are reshaped by MiniQCrypt. Recently, several works [Bar+23; BS23a; BS23b; Col23; Kit+24; MY24; MW24] have shown, somewhat surprisingly, that “quantum” public-key encryption can be constructed solely from the existence of OWFs. QPKE is a type of public key encryption that uses a quantum channel for public keys (and sometimes also for ciphertexts). This implies that PKE is not contained in Minicrypt, whereas QPKE is contained in MiniQCrypt.

Despite the fact that QPKE can be constructed from one-way functions, this line of research still faces two significant challenges. The first challenge is that generating quantum public keys requires powerful quantum computers. Quantum computers with error correction, called fault-tolerant quantum computers, are widely believed to be at least several decades away from practical realization, and as a result, many existing proposals are not feasible with current or near-term technology. The second challenge is that the security of these schemes is typically analyzed under the assumption of secure quantum communication channels. That is, it is assumed that the generated quantum public keys can be distributed securely without any modification. In more realistic settings, it is necessary to consider stronger security notions that allow adversarial tampering with the distributed quantum public keys.

Motivated by these limitations of existing constructions, in Chapter 5, we formalize such a security notion and construct a QPKE scheme that satisfies this notion based solely on the assumption of OWFs.

1.3 Outline

In this section, we give an outline of the rest of this thesis.

- In Chapter 2, we provide an overview of the fundamental background in cryptography, quantum computation, and information theory required to read this thesis. We also introduce the notation and abbreviations used throughout the thesis. For readability, this thesis revises some notations and phrasings compared to the summarized papers and enriches the preliminaries to make the exposition as self-contained as possible.
- In Chapter 3, we present a generalization of the quantum Goldreich–Levin theorem. The prior work of Adcock and Cleve [AC02] established a quantum reduction from onewayness to unpredictability that exhibits quantum advantages compared to classical reductions. We refer to this result as the quantum Goldreich–Levin theorem over $\mathbb{Z}_2$. For many years, extending this quantum algorithm to more general algebraic settings, namely $\mathbb{Z}_q$, remained an open problem. In this thesis, we resolve this problem by providing such an extension, which we call the quantum Goldreich–Levin theorem over $\mathbb{Z}_q$. This chapter reorganizes [Sudo et al., AFRICACRYPT 2023, LNCS 14064, 395–413] and [Sudo et al., IEICE Trans. 108(2), 104–116 (2025)]. Additionally, as an appendix, we include a new discussion on the quantum reduction algorithm and its relationship with Bernstein–Vazirani’s algorithm [BV93], which is one of the earliest examples of a quantum algorithm exhibiting a quantum advantage.

- In Chapter 4, as a direct application of the result in Chapter 3, we construct a quantum search-to-decision reduction for the LWE problem. Our approach to quantum search-to-decision reduction introduces a prediction problem as an intermediate step between the search LWE problem and the decisional LWE problem. Specifically, we construct a reduction algorithm that uses an algorithm to solve the decisional LWE problem to predict the value of the inner product $a \cdot s \pmod{q}$, where $s \in \mathbb{Z}_q^n$ is the secret string of the LWE instance and $a \in \mathbb{Z}_q^n$ is a randomly chosen string. Once this reduction algorithm is constructed, the quantum Goldreich–Levin theorem over $\mathbb{Z}_q$ as presented in Chapter 3, can be applied to recover the secret string s of the LWE problem. The reduction we provide has the *sample-preserving* property. Specifically, if a distinguisher for the decisional LWE problem requires m LWE samples, then our reduction algorithm uses only m samples to recover the secret s . Compared with classical sample-preserving reductions, our quantum reduction achieves quantum advantages in both the success probability and the number of subroutine calls. We also present a method for efficiently amplifying the success probability of this algorithm. These results provide theoretical insight into the secure design of post-quantum cryptographic schemes, clarifying the relationship between search and decisional hardness in the quantum setting. This chapter reorganizes [Sudo et al., AFRICACRYPT 2023, LNCS 14064, 395–413] and [Sudo et al., IEICE Trans. 108(2), 104–116 (2025)] with slight modifications to fit in the context.
- In Chapter 5, we first introduce a security definition that does not assume a secure quantum channel. Specifically, we consider adversarial tampering on the quantum channel by a third party. This security definition tackles a limitation of prior work by explicitly accounting for adversarial tampering on the quantum communication channel. Then, we present a construction of QPKE from OWFs. We propose a new construction of QPKE that, under the assumptions of a random oracle and individual attacks, does not require powerful quantum computers and remains secure even against tampering of the quantum communication channel. Similarly to the result in Chapter 3, this construction establishes a previously unknown result in the MiniQCrypt setting. This chapter reorganizes [Sudo et al., APKC 2025, 44–53] with slight modifications to fit in the context.
- In Chapter 6, we summarize the thesis and also discuss some further possible research directions.

Chapter 2

Preliminaries

This chapter provides the necessary background for reading this thesis. Readers who are familiar with cryptographic theory and quantum computation may safely skip this chapter. First, we introduce the fundamental concepts required to evaluate the security of cryptographic primitives in a mathematical framework. We next introduce a formal definition of the one-way functions and discuss their complexity-theoretic perspectives. We then present the notation used in quantum information theory. Subsequently, we review some preliminary knowledge from information theory. Finally, we provide notations and a table of abbreviations used in this thesis together with their full forms.

2.1 Basics of Cryptography

Modern cryptographic theory is founded on mathematical rigor. The security of a cryptographic scheme is precisely defined. There is an emphasis on the proofs of security under these definitions. Ideally, we would like to define that a scheme is secure if no adversary can break it. In practice, however, there may be a tiny probability that an adversary succeeds in breaking the scheme. For instance, even a straightforward brute-force attack, where all possible keys are tried, has a non-zero chance of success. Thus, what we truly mean is that the probability that any “*efficient*” adversary breaks the scheme is “*negligible*”. We now proceed to give formal mathematical definitions of these concepts.

Efficiency of Algorithm. We introduce a parameter λ , referred to as the security parameter. This parameter quantifies the desired level of security in a cryptographic scheme. When we design a cryptographic scheme, 1^λ is provided as an input, and other parameters of the scheme, such as the key length, are determined as functions of λ . Here, $1^\lambda = 11 \dots 1$ denotes a unary representation of the security parameter, a string consisting of λ consecutive 1s. Cryptographic protocols and their adversaries are defined as algorithms. We assume that both cryptographic protocols and adversaries take the security parameter as an implicit input. An algorithm is said to be *efficient* if it is a probabilistic polynomial time (PPT) algorithm. An algorithm is said to run in polynomial time if the number of steps it performs is bounded by a polynomial in the length of its input. A probabilistic algorithm is an algorithm that, in addition to its input, takes a randomly chosen string as input. For example, we denote $A(x; r)$ as the output of the probabilistic algorithm A on input x with a random string r . We denote $A(x)$ as a random variable for the output of $A(x; r)$ over a random r . $y \leftarrow A(x)$ denotes that a probabilistic algorithm A outputs y for an input x . Similarly, a quantum polynomial time (QPT) algorithm is a quantum algorithm whose running time is bounded by a polynomial of the size of the input length. Accordingly, an efficient protocol or adversary refers to a PPT algorithm (or a QPT algorithm) whose running time is measured as a function of the security parameter λ .

We adopt the Turing machine as the computational model for algorithms. A Turing machine is a uniform computational model in the sense that the same machine is used to process inputs of all lengths. In contrast, a Turing machine with advice, which receives an advice string a_n depending on the input length n , constitutes a non-uniform computational model and is strictly more powerful than uniform models. We adopt uniform families of quantum circuits as the computational model for quantum algorithms. A family of circuits $\{C_\lambda\}$ is said to be uniform if there exists a polynomial time algorithm A that, on input 1^λ , outputs a description of the quantum circuit C_λ .

Negligible Probability. To formalize the notion of a probability being *negligible*, we introduce the concept of negligible functions. For a function f , we say that $f(\lambda)$ is negligible, denoted $f(\lambda) = \text{negl}(\lambda)$, if $f(\lambda) = \lambda^{-\omega(1)}$. If the security parameter λ is chosen to be sufficiently large, the value of $\text{negl}(\lambda)$ becomes negligibly small. In summary, a cryptographic scheme is secure if for any PPT (or QPT) adversary, the probability of successfully breaking the scheme is negligible as a function of the security parameter λ .

Random Experiment. In order to formalize security definitions in cryptography, it is necessary to consider probabilities of events that involve complex processes. We introduce a random experiment. For a finite set S , $s \xleftarrow{\$} S$ denotes choosing an element s from S uniformly at random. For a distribution or a random variable $\mathcal{D}$, $d \leftarrow \mathcal{D}$ denotes the sampling of an element d according to $\mathcal{D}$. From now on, we will express statements on the probability of events using the notation

$$\Pr[\text{Event} : \text{Random Experiment}],$$

where the random experiment describes how various values are sampled. For example, when an element is chosen uniformly at random from the set $\{0, 1\}$, the probability that it is 0 is $1/2$, which can be expressed as follows,

$$\Pr \left[x = 0 : x \xleftarrow{\$} \{0, 1\} \right] = \frac{1}{2}.$$

Cryptography and the P vs. NP

Cryptography is heavily based on computational complexity. Thus, some background on computational complexity is required for our discussion of cryptography. In this section, we briefly recall the definitions of the complexity classes P and NP.

P and NP are among the concepts known as complexity classes. A complexity class is a collection of computational problems classified according to the computational resources required to solve them, such as running time and memory usage. Informally, the complexity class P is the set of problems that can be decided by deterministic polynomial time algorithms. The letter “P” stands for “polynomial time”. In contrast, the complexity class NP is the set of problems that can be verified by deterministic polynomial time algorithms given an appropriate hint, called a witness. The letter “NP” stands for “non-deterministic polynomial time”. Formal definitions are given as follows. A problem $\mathcal{D}$ is decidable if there exists an algorithm A such that, for every input x , the algorithm $A(x)$ runs and outputs 1 when $x \in \mathcal{D}$, and runs and outputs 0 when $x \notin \mathcal{D}$. The complexity class P is the set of decidable problems. A Problem $\mathcal{V}$ is verifiable if there exists an algorithm A such that, for every input $x \in \mathcal{V}$, there exist a witness w , the algorithm $A(x, w)$ runs and outputs 1, and for every input $x \notin \mathcal{V}$, for any w , the algorithm $A(x, w)$ runs and outputs 0 when $x \notin \mathcal{V}$. The complexity class NP is the set of verifiable problems.

Whether $P \neq NP$ holds is one of the most important open problems in computer science and mathematics. In general, modern cryptography relies on the assumed existence of computational problems that are difficult to solve efficiently; in this sense, the existence

of cryptographic primitives is believed to imply $P \neq NP$. Consequently, at present, it is impossible to prove the security of cryptographic schemes without making any computational assumptions.

A natural next question is whether the assumption $P \neq NP$ alone is sufficient to guarantee the security of cryptographic schemes. That is, can computational security be established solely under this assumption? Unfortunately, most cryptographic constructions require computational hardness assumptions stronger than $P \neq NP$. A representative example of such assumptions is the existence of one-way functions.

2.1.1 One-Way Function

The existence of one-way functions (OWFs) is known as a minimal computational assumption in (classical) cryptography, since it is necessary for the construction of cryptographic schemes and at the same time sufficient for deriving many cryptographic primitives, such as hard-core bit [GL89], pseudorandom generators [BM82; Hås+99], pseudorandom functions [GGM84], symmetric key encryption [GGM84; Hås+99; BN08], and digital signature [Rom90]. A one-way function is a function that can be computed efficiently, while its inverse computation, namely finding a preimage corresponding to a given function value, is computationally hard. We give a formal definition of OWFs as follows.

Definition 2.1. A function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is one-way function if the following holds.

- Easy to compute : For all inputs $x \in \{0, 1\}^*$, $f(x)$ can be computed in polynomial time.
- Hard to invert : For all QPT adversaries $\mathcal{A}$,

$$\Pr \left[f(x') = f(x) : \begin{array}{l} x \xleftarrow{\$} \{0, 1\}^\lambda, \\ x' \leftarrow \mathcal{A}(1^\lambda, f(x)) \end{array} \right] = \text{negl}(\lambda).$$

As a remark, we consider whether it is possible to compute one of the preimages from $f(x)$ for a randomly chosen input x . That is, we do not require the algorithm to recover the original input x itself; rather, given $f(x)$, it is considered successful if the algorithm outputs any x' such that $f(x) = f(x')$.

Impagliazzo's Five Worlds

Investigating what OWFs imply (and equally, what they do not imply) is a central question in modern cryptographic theory. Understanding these implications helps clarify the boundaries between what cryptographic primitives can be constructed under minimal assumptions and what additional assumptions are necessary for more advanced cryptographic goals. A powerful conceptual framework for exploring this landscape is *Impagliazzo's Five Worlds*, proposed by Russell Impagliazzo [Imp95], which classifies possible computational realities based on the hardness of computational problems and the feasibility of cryptographic constructions.

These five hypothetical worlds represent distinct possibilities for the computational nature of our universe, each with its own implications for complexity theory and cryptography. A brief summary of these worlds is as follows:

- Algorithmica: A world where $P=NP$; all NP problems are efficiently solvable, even in the worst case.
- Heuristica: A world where $P \neq NP$, but average-case NP problems are easy; heuristic algorithms succeed in most natural instances, although some inputs remain difficult.

- Pessiland: Average-case hard NP problems exist, but OWFs do not; although some problems are hard, we cannot exploit this hardness for cryptographic purposes.
- Minicrypt: OWFs exist; this world supports symmetric-key cryptography but lacks the tools necessary for public-key schemes.
- Cryptomania: Public-key cryptography is possible; this world enables both symmetric and public-key cryptographic constructions.

Among these, Minicrypt represents the minimal world in which OWFs exist, providing a foundation for a wide class of symmetric-key primitives such as pseudorandom generators, message authentication codes, and shared-key encryption schemes. This indicates that OWFs are a necessary and sufficient assumption for enabling much of symmetric cryptography.

In contrast, Pessiland shows that computational hardness alone is not enough for cryptography, average-case hard problems may exist without enabling any cryptographic functionality. Thus, the existence of OWFs demarcates a fundamental boundary between worlds where cryptography is theoretically impossible and those where it becomes viable.

The distinction between Minicrypt and Cryptomania further reveals that OWFs, while necessary, are not sufficient for public-key cryptography. Public-key constructions often require stronger assumptions, such as trapdoor permutations or additional algebraic structure.

In the quantum setting, a natural analogue of the classical Minicrypt world is referred to as *MiniQCrypt*. In contrast to the Minicrypt, certain primitives that are impossible from OWFs alone in the classical world, such as quantum oblivious transfer and quantum multi-party computation, quantum public-key encryption can be constructed based on post-quantum OWFs [Gri+21; Bar+21; Bar+23; BS23a; BS23b; Col23; Kit+24; MY24; MW24]. Here, quantum primitives refer to primitives that allow both quantum computation and quantum communication.

2.1.2 Minimal Assumption in Quantum Cryptography

Although the present work focuses on MiniQCrypt, we briefly mention another line of research that explores minimal assumptions in a different quantum cryptographic model.

It is known that some quantum cryptographic primitives can be constructed from assumptions weaker than OWFs. In particular, the concept of pseudo-random quantum states was introduced in [JLS18], and it was shown in [Kre21] that such states can exist even in the absence of OWFs. Furthermore, Refs. [MY22; AQY22] demonstrate that quantum commitment schemes and quantum digital signatures can be constructed from pseudo-random quantum states, suggesting that these primitives may not require OWFs at all.

Recent research has focused on the minimal assumptions required for an interesting class of quantum primitives known as quantum-computation classical-communication (QCCC). In this setting, it has been suggested that efficiently verifiable one-way puzzles serve as a natural and central cryptographic primitive [KT24; CGG24]. It was shown in [KT24] that the QCCC versions of symmetric-key encryption, one-time signatures and bit commitments imply efficiently verifiable one-way puzzles. Moreover, it was shown in [CGG24] that the QCCC versions of public-key encryption and pseudorandom generator imply efficiently verifiable one-way puzzles.

2.1.3 The Learning with Errors Problem

Constructing cryptographic primitives such as quantum public-key encryption, that cannot be built from post-quantum OWFs, requires stronger post-quantum assumptions, such as the hardness of the Learning with Errors (LWE) problem. The LWE problem was introduced by

Regev [Reg05]. LWE is a lattice problem that is widely believed to be computationally hard even for quantum computers. For example, the LWE problem serves as the foundation for constructing various cryptographic primitives, such as oblivious transfer [PVW08], identity-based encryption [ABB10; Cas+10; GPV08], and fully homomorphic encryption [BV11]. Two major variants of the problem are known: search LWE and decisional LWE. The search $\text{LWE}_{n,m,q,\chi}$ problem asks to solve a system of noisy linear equations. Formally, it asks to find s chosen uniformly at random from $\mathbb{Z}_q^n$ given m LWE samples. Here the LWE sample is defined as follows,

$$\mathcal{LWE}_{n,s,q,\chi} := \{(a, y) | a \xleftarrow{\$} \mathbb{Z}_q^n, e \leftarrow \chi, y := a \cdot s + e\}$$

where χ is a probability distribution over $\mathbb{Z}_q$ that typically outputs relatively *small* numbers. In the decisional $\text{LWE}_{n,m,q,\chi}$ problem, one is given m samples that are drawn either from the LWE distribution $\mathcal{LWE}_{n,s,q,\chi}$ or from the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$, and the task is to distinguish between the two cases.

Search-to-Decision Reduction for the LWE Problem

A search-to-decision reduction for the LWE problem refers to a reduction from the search LWE problem to the decisional LWE problem. That is, the hardness of search LWE directly implies the hardness of decisional LWE. The proof is typically carried out by constructing a reduction algorithm and arguing via contraposition: if there exists an efficient algorithm for solving decisional LWE, then this algorithm can be employed as a subroutine to construct an efficient solver for search LWE.

Non-uniform Reduction

The quantum search-to-decision reduction we provide (Theorem 4.1) is a non-uniform reduction. Thus we provide an explanation of this notion of uniform and non-uniform reduction. A uniform reduction is an algorithm that operates independently of the input length, using a single efficient procedure to transform any adversary for a target problem into a solver for a source problem. In contrast, a non-uniform reduction allows the use of input-length dependent advice: for each input length λ , the reduction may utilize auxiliary information or a dedicated circuit that is tailored to that particular size. Intuitively, a non-uniform reduction can be viewed as a uniform reduction augmented with a polynomial-length advice string that depends on the input size.

Non-uniform reductions are generally more challenging to construct than uniform reductions, since the reduction must remain correct even when the adversary is optimized individually for each input length. This difficulty is further amplified in the quantum setting. When a quantum adversary is equipped with input-length dependent quantum advice, the reduction faces the additional constraint imposed by the no-cloning theorem [WZ82]: quantum states cannot be copied, and therefore the reduction algorithm cannot reuse the advice multiple times. Consequently, designing quantum non-uniform reductions requires careful management of the quantum advice, making such reductions significantly more delicate than their classical counterparts.

2.2 Quantum Computing

In this section, we briefly review basic notions from quantum information theory that will be used throughout this thesis. Our goal is not to provide a comprehensive introduction to quantum computing, but rather to fix notation and highlight the specific concepts relevant to cryptographic constructions and security proofs.

Quantum States. A pure quantum state is a unit vector in the Hilbert space $\mathbb{C}^N$ for some $N = 2^n$. Here, N denotes the dimension of the Hilbert space. Intuitively, the dimension N corresponds to the number of classical configurations that an n -qubit quantum system can represent simultaneously. For example, for a one-qubit system, $N = 2$; for two qubits, $N = 2^2 = 4$; and for n qubits, $N = 2^n$. For every $x \in [N] = \{0, 1\}^n$, we will denote the state as

$$|x\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

with a 1 in the x -th location and 0 everywhere else. These states correspond to classical bit strings embedded into a quantum state space and form the canonical basis used for measurement and computation. When $n = 1$, we have

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Vectors $\{|x\rangle\}_{x \in [N]}$ form an orthonormal basis for $\mathbb{C}^N$. A general pure state $|\phi\rangle \in \mathbb{C}^N$ can be written as

$$|\phi\rangle = \sum_{x \in [N]} \alpha_x |x\rangle,$$

where $\alpha_x \in \mathbb{C}$ such that $\sum_{x \in [N]} |\alpha_x|^2 = 1$. This representation captures the principle of quantum superposition, which allows a quantum system to encode exponentially many classical states at once. The conjugate transpose of $|\phi\rangle$ is denoted by $\langle\phi|$. $\langle\phi|\psi\rangle$ represents the product of $\langle\phi|$ and $|\psi\rangle$. Besides the computational basis, alternative bases play a crucial role in quantum information, particularly in cryptographic protocols. We adopt the convention that

$$\{|0\rangle, |1\rangle\}, \text{ and } \{|+\rangle, |-\rangle\}$$

denote the computational and Hadamard basis states, respectively, where

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \text{ and } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

The joint state of $|x\rangle \in \mathbb{C}^{N_1}$ and $|y\rangle \in \mathbb{C}^{N_2}$ is $|x\rangle \otimes |y\rangle = |x, y\rangle \in \mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$. In contrast, for any binary string $x = x_1 x_2 \cdots x_n \in \{0, 1\}^n$, $|x\rangle$ can be viewed as $|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$.

Operations. An operation on a quantum state is represented by a unitary transformation $U \in \mathbb{C}^{N \times N}$, which means $UU^\dagger = U^\dagger U = I$, where $U^\dagger$ is the conjugate transpose of U and I is an identity operator. Unitary operations model reversible quantum evolutions and form the basic building blocks of quantum algorithms. The Pauli operators $X, Y, Z \in \mathbb{C}^{2 \times 2}$ are unitary and Hermitian. More specifically:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The X gate transforms $|0\rangle$ into $|1\rangle$ and vice versa. The Z gate keeps $|0\rangle$ the same and turns $|1\rangle$ into $-|1\rangle$. These operators generate fundamental transformations such as bit flips and phase flips, which frequently appear in quantum protocols. The quantum Fourier transformation

QFT over $\mathbb{Z}_q := \{0, 1, \dots, q-1\}$ is determined by $\text{QFT}|j\rangle = \frac{1}{\sqrt{q}} \sum \omega_q^{jk} |k\rangle$. For example, the quantum Fourier transformation QFT over $\mathbb{Z}_2$ is

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \quad (2.1)$$

This operation is specifically known as the Hadamard operation. The Hadamard operation H transforms $|0\rangle$ into $|+\rangle$ and $|1\rangle$ into $|-\rangle$. The QFT is a key ingredient in many quantum algorithms, as it enables the efficient creation and manipulation of superposition states, for example, the preparation of a uniform superposition over computational basis states.

For any binary string $x = x_1x_2 \cdots x_n \in \{0, 1\}^n$, we denote $|\underline{x}\rangle = H^{\otimes n} |x\rangle = H|x_1\rangle \otimes H|x_2\rangle \otimes \cdots \otimes H|x_n\rangle$.

Measurements. When a state $|\phi\rangle$ is measured in the computational basis, the outcome x occurs with probability $|\langle x|\phi\rangle|^2$. When a state $|\phi\rangle$ is measured in the Hadamard basis, the outcome x occurs with probability $|\langle \underline{x}|\phi\rangle|^2$.

Quantum Circuits. To describe how quantum computations are implemented as a sequence of unitary operations and measurements acting on quantum states, it is convenient to use quantum circuit diagrams. In quantum circuit diagrams, time flows from left to right: the initial state appears on the left, followed by the sequence of applied operations. Each qubit is represented as a horizontal wire, and the circuit diagram indicates which quantum gates are applied to which wires. Single-qubit gates, such as the X and H gates, act on only one wire. In contrast, multi-qubit gates, such as the CNOT gate, act simultaneously on multiple wires. When one qubit controls the application of a gate on another qubit, a filled black dot is drawn on the control wire and is connected by a vertical line to the gate applied to the target qubit. A canonical example of this construction is the CNOT gate, in which the single-qubit gate applied to the target qubit is the X gate. If a meter symbol appears at the right end of a wire, it indicates that a measurement of the corresponding register in the computational basis is performed at the end of the circuit. Figure 2.1 illustrates a simple example involving a two-qubit system initially in the state $|00\rangle$. First, an H gate is applied to the first qubit. Next, a CNOT gate is applied to the two qubits, with the first qubit serving as the control qubit. The resulting state is $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. The state transition is given as follows:

$$|00\rangle \xrightarrow{H \otimes I} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

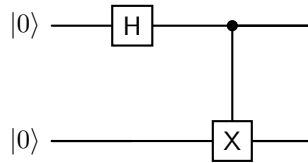


Figure 2.1: A quantum circuit that generates an EPR state.

The state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is called an EPR state [EPR35]. It is a canonical example of an entangled state and plays a central role in many quantum cryptographic protocols, such as entanglement-based protocols [Eke91; BBM92]. Moreover, even in protocols where entanglement is not explicitly employed, such as certain quantum key distribution schemes, EPR states are often used implicitly or virtually in security proofs. This perspective is also adopted in the security proof of the quantum public-key encryption scheme in Chapter 5.

A fundamental property of the EPR state is that when the two qubits are measured independently in the same basis, each outcome is uniformly random, yet the outcomes are perfectly correlated. For example, if both qubits are measured in the computational basis, the outcomes are uniformly random but always identical, yielding either $(0, 0)$ or $(1, 1)$ with equal probability. This is also the case for any other basis. As long as both qubits are measured in the same basis, the outcomes are uniformly random but perfectly correlated.

2.3 Theoretical Foundations

In this chapter, we introduce entropy and the Chernoff bound as basic concepts used throughout this thesis.

Definition 2.2 (Shannon Entropy). Let X be a discrete random variable with support $\mathcal{X}$. The Shannon entropy of X is defined as

$$H(X) = - \sum_{x \in \mathcal{X}} \Pr[X = x] \log \Pr[X = x].$$

Definition 2.3. Let the prediction probability of a random variable X be

$$\text{Pred}(X) = \max_x \Pr[X = x].$$

The min-entropy is defined as

$$H_{\min}(X) = -\log \text{Pred}(X).$$

We note that if two random variables X and Y are independent, we have

$$H_{\min}(XY) = H_{\min}(X) + H_{\min}(Y).$$

The Shannon entropy $H(X)$ measures the *average uncertainty* of the random variable X . It quantifies how much information is revealed, on average, when the value of X is observed. In contrast, the min-entropy $H_{\min}(X)$ captures the *worst-case unpredictability* of X . Specifically, it characterizes the difficulty of guessing the value of X in a single attempt, even for an adversary that knows the full distribution of X .

Next, we introduce the Chernoff bound, a probabilistic inequality that quantifies the strong concentration of the average of a large number of independent random variables around its expected value. In particular, it guarantees that the probability of significant deviation from the expectation decreases exponentially with the number of trials.

Chernoff Bounds. Let $X = \sum_{i=1}^n X_i$, where $X_i = 1$ with probability p_i and $X_i = 0$ with probability $1 - p_i$, and all X_i are independent. Let $\mu = E(X) = \sum_{i=1}^n p_i$. Then for all $0 < \delta < 1$,

$$\Pr[|X - \mu| \geq \delta\mu] \leq 2e^{-\mu\delta^2/3} \tag{2.2}$$

holds.

2.4 Notations and Abbreviations

In this thesis, we use the following notations and definitions. For a positive integer i , we write $[i] = \{1, \dots, i\}$ to denote the set of positive integers less than or equal to i . We denote the concatenation of a string a and a string b by $a||b$. We denote $\mathbb{Z}_q$ for the cyclic group $\{0, 1, \dots, q-1\}$ with addition modulo q . We use standard asymptotic notations $\mathcal{O}(\cdot)$,

$o(\cdot)$, $\Omega(\cdot)$, $\omega(\cdot)$, $\Theta(\cdot)$, etc. Formally, let f, g be functions from the natural numbers to the positive real numbers, we write $f(n) = \mathcal{O}(g(n))$ if there exists a constant $c > 0$ such that $f(n) \leq c \cdot g(n)$ for all sufficiently large n . We write $f(n) = \Omega(g(n))$ if $g(n) = \mathcal{O}(f(n))$, and we write $f(n) = \Theta(g(n))$ if both $f(n) = \mathcal{O}(g(n))$ and $f(n) = \Omega(g(n))$. We write $f(n) = o(g(n))$ if for every $\epsilon > 0$ and all sufficiently large n , $f(n) < \epsilon \cdot g(n)$. We write $f(n) = \omega(g(n))$ if $g(n) = o(f(n))$. We use $\tilde{\mathcal{O}}$ (resp. $\tilde{\Theta}$) notation which overlooks poly-logarithmic quantities 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 : $\omega_n := e^{\frac{2\pi i}{n}}$.

Here we provide a list of abbreviations used in this thesis together with their full names.

Abbreviation	Meaning
CCA	Chosen Ciphertext Attack
CPA	Chosen Plaintext Attack
DS	Digital Signature
sEUF-CMA	Strong-Existentially Unforgeability under Chosen Message Attack
SKE	Symmetric-Key Encryption
IND-pkt-CPA	Indistinguishability against Public-Key Tampering Chosen Plaintext Attack
LPN	Learning Parity with Noise
LWE	Learning with Errors
OWF(s)	One-Way Function(s)
PKE	Public-Key Encryption
PRF	Pseudorandom Function
PPT	Probabilistic Polynomial Time
QCCC	Quantum-Computation Classical-Communication
QKD	Quantum Key Distribution
QKEM	Quantum Key Encapsulation Mechanism
QPKE	Quantum Public-Key Encryption
QPT	Quantum Polynomial Time

Chapter 3

Quantum Reduction for One-Wayness to Unpredictability

The fact that one-wayness can be polynomially reduced to unpredictability is known as the Goldreich–Levin theorem. From a cryptographic perspective, this theorem plays a crucial role in showing that pseudorandom generators and pseudorandom functions can be constructed from any one-way function. Beyond its importance in cryptography, the reduction algorithm introduced in this theorem has had a broad impact on computer science. Its ideas have influenced efficient decoding algorithms for the Walsh–Hadamard code and have found applications in learning theory and related areas. In this chapter, we present a quantum reduction from one-wayness to unpredictability. This chapter reorganizes [Sudo et al., AFRICACRYPT 2023, LNCS 14064, 395–413] and [Sudo et al., IEICE Trans. 108(2), 104–116 (2025)] with slight modifications to fit the context.

3.1 Introduction

3.1.1 Backgrounds

The Goldreich-Levin theorem [GL89] is a cornerstone theorem in Minicrypt. Its significance extends beyond cryptography and has profound implications in information theory. For example, the theorem led to the development of new categories of error-correcting codes [Sud97; KT00] and led to an early success in boolean learning theory [KM91]. This theorem states that any one-way function f can be easily transformed into a function of the required form $g(s||a) := (f(s)||a)$ where $s, a \in \mathbb{Z}_q^n$ and it has a hard-core bit $a \cdot s \pmod{q}$. Roughly speaking, a hard-core bit 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 $1/q$. Adcock and Cleve investigate a quantum Goldreich-Levin theorem over $\mathbb{Z}_2$ [AC02]. Roughly, they show that the reduction from quantum one-way functions to quantum hard-core bits is quantitatively more efficient than the classical version.

3.1.2 Our Contributions

We give a further generalized reduction, that is, the quantum Goldreich-Levin theorem over $\mathbb{Z}_q$. 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 $a \xleftarrow{\$} \mathbb{Z}_q^n$, then we can find s with probability at least $(\frac{q\delta}{q-1})^2$ while accessing the predictor 2 times. The comparison between our results and those of the classical reduction is given in Fig. 3.1 Note that this result is consistent with the quantum Goldreich-Levin theorem by Adcock and Cleve when $q = 2$.

Compared to classical reductions, the quantum algorithm presented in this work achieves a substantial improvement in both success probability and query complexity. In particular, while classical reductions yield a success probability that is polynomial in $1/q$ and a query complexity that is polynomial in q , the quantum algorithm maintains a high success probability even for large q and requires only two queries. That is, the quantum algorithm remains efficient even when q is super-polynomial. Our algorithm employs the quantum Fourier transform (QFT) over $\mathbb{Z}_q$, however, the approximate quantum Fourier transform can be implemented efficiently even when q is super-polynomial in n [Kit95]. Moreover, classically, the number of unpredictably extractable bits from inner products based on the Goldreich-Levin theorem is limited to $\log n$ bits [Gol01]. Our result shows that it is possible to extract super-polynomial unpredictability with respect to n .

Table 3.1: Comparison of the algorithms performance. n is the length of the secret $s \in \mathbb{Z}_q^n$, δ is the advantage of the predictor.

	Success probability	Query complexity
Classical Reduction (over $\mathbb{Z}_q$) [Dod+12]	$\frac{512\delta^3}{nq^2}$	$\text{poly}(n, q, \delta^{-1})$
Quantum Reduction (over $\mathbb{Z}_2$) [AC02]	$4\delta^2$	2
Th.3.1 (over $\mathbb{Z}_q$)	$(\frac{q\delta}{q-1})^2$	2

As mentioned earlier, the reduction from one-wayness to unpredictability has had a significant impact across various areas of computer science. The fact that the quantum reduction of Adcock and Cleve can be further generalized is, in itself, an intriguing and significant result. Furthermore, in Chapter 4, we apply this theorem to establish a search-to-decision reduction for the Learning with Errors (LWE) problem.

3.1.3 Concurrent Work of Quantum Goldreich-Levin Theorem

Recently, Ananth et al. [APV23] 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. [Dod+10] into quantum reduction, by using the recent work of Bitansky et al. [BBK22]. Specifically, they show that a distinguisher, given auxiliary input aux , can distinguish between $(a, a \cdot s)$ and (a, r) where s is randomly chosen from $H \subset \mathbb{Z}_q$ can be converted into a quantum extractor that can extract s given aux . Their quantum algorithm relies on the classical Goldreich-Levin theorem for the field $\mathbb{Z}_q$ by Dodis et al., in which the distinguisher with advantage δ is used $\text{poly}(n, |H|, \frac{1}{\delta})$ times to extract s and its success probability is $\frac{\delta^3}{512nq^2}$.

On the other hand, our quantum algorithm can find s by accessing the distinguisher 2 times with probability $(\frac{q\delta}{q-1})^2$, and it is not necessary to make the subset from which s is chosen small, when q is super-polynomial in n .

3.1.4 Review of the Quantum Goldreich-Levin Theorem

In this section, we first review the quantum Goldreich-Levin theorem from prior work. We then discuss the challenges that arise in extending its algorithm to the general setting and

present the idea used to overcome them.

Quantum Goldreich-Levin theorem over $\mathbb{Z}_2$. Before presenting our generalized Goldreich–Levin theorem, we first recall the Goldreich–Levin theorem over $\mathbb{Z}_2$ by Adcock and Cleve. For simplicity, we consider the uniform case.

We call a unitary operation U_P a quantum (s, q, δ) -predictor, if the second register of $U_P |a\rangle |0\rangle |0^l\rangle$ is measured in computational basis, yielding the value $P(a)$, then

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

holds where $a, s \in \mathbb{Z}_q^n$ and the probability depends on over choice of $a \xleftarrow{\$} \mathbb{Z}_q^n$.

We denote

$$U_P |a\rangle |0\rangle |0^l\rangle = \alpha_{a,0} |a\rangle |a \cdot s\rangle |\eta_{a,0}\rangle + \alpha_{a,1} |a\rangle |a \cdot s + 1\rangle |\eta_{a,1}\rangle$$

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

$$\frac{1}{2^n} \sum_{a \in \{0,1\}^n} |\alpha_{a,0}|^2 \geq \frac{1}{2} + \delta \quad (3.1)$$

and

$$\frac{1}{2^n} \sum_{a \in \{0,1\}^n} |\alpha_{a,1}|^2 < \frac{1}{2} - \delta. \quad (3.2)$$

Figure 3.1 shows the quantum circuit of the Quantum Goldreich-Levin theorem over $\mathbb{Z}_2$. QFT denotes the quantum Fourier transformation over $\mathbb{Z}_2^n$. Ph is the unitary that performs phase kickback depending on the value of the register.

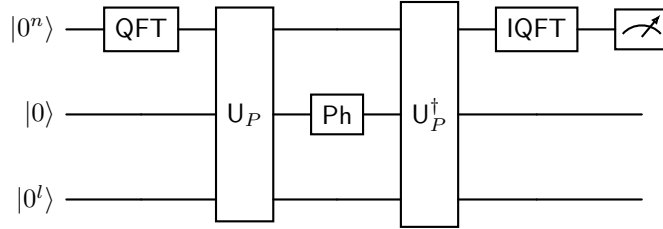


Figure 3.1: Quantum circuit of the quantum Goldreich-Levin theorem over $\mathbb{Z}_2$.

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

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

by QFT and pass through the $(s, 2, \delta)$ -predictor U_P , multiply the phase by $(-1)^y$ according to the value of the second register y . The quantum states are now in a state

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

up to this point. Pass the states through conjugate transpose of the predictor $U_P^\dagger$ and inverse quantum Fourier transformation $\text{IQFT} := \text{QFT}^\dagger$. By measuring the first register in Fourier basis, we could obtain s . The probability of yielding s is greater than

$$\left| \langle s | \langle 0 | \langle 0^l | \text{IQFT} U_P^\dagger | \phi \rangle \right|^2.$$

Let $|\psi\rangle := U_P \text{QFT} |s\rangle |0\rangle |0^l\rangle$, we can compute as follows.

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

Therefore,

$$\begin{aligned} \left| \langle s | \langle 0 | \langle 0^l | \text{IQFT} U_P^\dagger | \phi \rangle \right|^2 &= |\langle \psi | \phi \rangle|^2 \\ &= \left| \frac{1}{2^n} \sum_{a \in \{0,1\}^n} (|\alpha_{a,0}|^2 - |\alpha_{a,1}|^2) \right|^2. \end{aligned} \quad (3.3)$$

Using the fact of (3.1) and (3.2), we can find s with probability at least $\left| \left(\frac{1}{2} + \delta \right) - \left(\frac{1}{2} - \delta \right) \right|^2 = 4\delta^2$.

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

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

$$U_P |a\rangle |0^l\rangle |0\rangle = \alpha_{a,j} |a\rangle |a \cdot s + j\rangle |\eta_{a,j}\rangle.$$

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

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

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

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

If we apply $U_P^\dagger$ and measure the first register in the Fourier basis, the probability of yielding s is greater than the square of the inner product of $|\phi\rangle$ and

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

which is

$$|\langle \psi | \phi \rangle|^2 = \left| \frac{1}{q^n} \sum_{a \in \mathbb{Z}_q^n} \sum_{j \in \mathbb{Z}_q} \omega_q^j |\alpha_{a,j}|^2 \right|^2. \quad (3.4)$$

Define $\text{prb}(j) := \Pr[P(a) = a \cdot s + j : a \leftarrow \mathbb{Z}_q^n]$ as the probability that the gap between the predictor's prediction and the inner product is j , then (3.4) can be written as $|\sum_{j \in \mathbb{Z}_q} \omega_q^j \text{prb}(j)|^2$. This value cannot be guaranteed some lower bound unless the advantage is very high such that $\delta > \frac{1}{2} - \frac{1}{q}$.

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

$$\frac{1}{q-1} \sum_{r \in \mathbb{Z}_q^*} \omega_q^{rj} \text{prb}(j) = \begin{cases} \text{prb}(0) & \text{if } j = 0 \\ \frac{-1}{q-1} \text{prb}(j) & \text{if } j \neq 0. \end{cases} \quad (3.5)$$

We will use this property to improve the algorithm. We carefully control the phase for the associated indices $j \neq 0$. Please refer to Proof 3.2 for the improved reduction algorithm.

3.2 Quantum Goldreich-Levin Theorem over $\mathbb{Z}_q$

We give a formal definition of a predictor.

Definition 3.1. A quantum (s, q, δ) -predictor is unitary operation U_P and an auxiliary $|\text{aux}\rangle$ such that, for $a \xleftarrow{\$} \mathbb{Z}_q^n$, the second register of $U_P |a\rangle |0\rangle |\text{aux}\rangle$ is measured in computational basis, yielding the value $P(a)$, then

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

holds.

Theorem 3.1 (Quantum Goldreich-Levin theorem over $\mathbb{Z}_q$). Let q be a prime. If there is a quantum (s, q, δ) -predictor $(U_P, |\text{aux}\rangle)$, then there is a quantum algorithm that finds s with probability at least $(\frac{q\delta}{q-1})^2$. It invokes U_P and $U_P^\dagger$ once each and uses an auxiliary $|\text{aux}\rangle$.

Proof of Theorem 3.1 We construct a quantum algorithm that finds s using a quantum (s, q, δ) -predictor U_P .

For $a \in \mathbb{Z}_q^n$, we denote the state obtained by applying U_P to $|a\rangle |0\rangle |\text{aux}\rangle$ as follows,

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

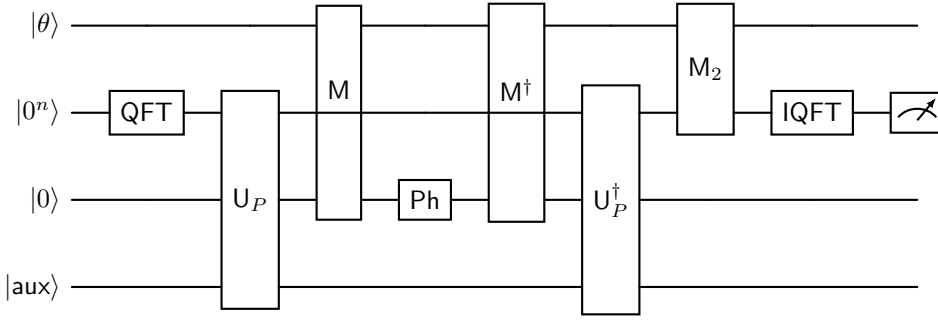
We denote a state $|\theta\rangle = \frac{1}{\sqrt{q-1}} \sum_{r \in \mathbb{Z}_q^*} |r\rangle$.

Consider the following quantum circuit C in Figure 3.2. The QFT is the Fourier transformation over $\mathbb{Z}_q^n$. The unitary M multiplies the first register by the value of the third register. The unitary Ph applies a phase rotation of ω_q^y depending on the value of the third register y . The unitary M_2 multiplies the second register by the value of the first register.

We will show that

$$|\langle \theta | \langle s | \langle 0 | \langle \text{aux} | C | \theta \rangle | 0^n \rangle | 0 \rangle |\text{aux}\rangle|^2 > \left(\frac{q\delta}{q-1} \right)^2.$$

C can be decomposed into the following five operations:

Figure 3.2: Quantum circuit C .

1. Operation C_1 : Apply QFT over $\mathbb{Z}_q^n$ to the second register.
2. Operation C_2 : Apply U_P to the second and third registers.
3. Operation C_3 : Apply multiple operation M to the first and third register.
4. Operation C_4 : Apply a phase kick back operation Ph to the third register.
5. Operation C_5 : Apply multiple operation $M^\dagger$ to the first and third register.
6. Operation C_6 : Apply $U_P^\dagger$ to the second and third registers.
7. Operation C_7 : Apply multiple operation M_2 to the first and second register.
8. Operation C_8 : Apply IQFT to the second register.

First, prepare the superposition states

$$|\theta\rangle |0^n\rangle |0\rangle |\text{aux}\rangle.$$

After passing through the quantum Fourier operation QFT over $\mathbb{Z}_q^n$, the state becomes

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

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

$$\begin{aligned} |\phi\rangle &:= C_5 C_4 C_3 C_2 C_1 |\theta\rangle |0^n\rangle |0\rangle |\text{aux}\rangle \\ &= \frac{1}{\sqrt{q^n(q-1)}} \sum_{a,r,j} \omega_q^{r(a \cdot s + j)} \alpha_{a,j} |r\rangle |a\rangle |a \cdot s + j\rangle |\eta_{a,j}\rangle. \end{aligned}$$

Finally, we apply the states through conjugate transpose of the predictor $U_P^\dagger$ (apply the second to the last register), multiply the second register by the first register (denote this operation as M_2), and measure the second register in Fourier basis. The probability of yielding s is greater than $|\langle \theta | \langle s | \langle 0 | \langle \text{aux} | C | \theta \rangle | 0^n \rangle | 0 \rangle |\text{aux}\rangle|^2$. Therefore, let us consider the

following state.

$$\begin{aligned}
|\psi\rangle &:= C_6^\dagger C_7^\dagger C_8^\dagger |\theta\rangle |s\rangle |0\rangle |\mathbf{aux}\rangle \\
&= U_P M_2^\dagger \text{QFT} \frac{1}{\sqrt{q-1}} \sum_{r \in \mathbb{Z}_q^*} |r\rangle |s\rangle |0\rangle |\mathbf{aux}\rangle \\
&= U_P M_2^\dagger \left(\frac{1}{\sqrt{q^n(q-1)}} \sum_{b \in \mathbb{Z}_q^n} \sum_{r \in \mathbb{Z}_q^*} \omega_q^{b \cdot s} |r\rangle |b\rangle |0\rangle |\mathbf{aux}\rangle \right) \\
&= U_P M_2^\dagger \left(\frac{1}{\sqrt{q^n(q-1)}} \sum_{a \in \mathbb{Z}_q^n} \sum_{r \in \mathbb{Z}_q^*} \omega_q^{r(a \cdot s)} |r\rangle |ra\rangle |0\rangle |\mathbf{aux}\rangle \right) \\
&= U_P \left(\frac{1}{\sqrt{q^n(q-1)}} \sum_{a, r} \omega_q^{r(a \cdot s)} |r\rangle |a\rangle |0\rangle |\mathbf{aux}\rangle \right) \\
&= \frac{1}{\sqrt{q^n(q-1)}} \sum_{a, r, j} \omega_q^{r(a \cdot s)} |r\rangle |a\rangle |a \cdot s + j\rangle |\eta_{a, j}\rangle.
\end{aligned}$$

We get

$$\begin{aligned}
&\Pr[s \text{ is measured}] \\
&\geq |\langle \theta | \langle s | \langle 0 | \langle \mathbf{aux} | C | \theta \rangle | 0^n \rangle | 0 \rangle |\mathbf{aux}\rangle|^2 \\
&= |\langle \psi | \phi \rangle|^2 \\
&= \left| \frac{1}{q^n(q-1)} \sum_{a, r, j} \omega_q^{rj} |\alpha_{a, j}|^2 \right|^2 \\
&= \left| \frac{1}{q^n} \sum_{a \in \mathbb{Z}_q^n} |\alpha_{a, 0}|^2 + \frac{1}{q^n(q-1)} \sum_{a \in \mathbb{Z}_q^n} \sum_{j \in \mathbb{Z}_q^*} (-|\alpha_{a, j}|^2) \right|^2 \tag{3.6} \\
&> \left| \left(\frac{1}{q} + \delta \right) - \frac{1}{q-1} \left(1 - \left(\frac{1}{q} + \delta \right) \right) \right|^2 \\
&= \left(\frac{q\delta}{q-1} \right)^2.
\end{aligned}$$

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.

□ (**Theorem 3.1.**)

The comparison between Eq. (3.4) and Eq. (3.6) highlights the effect of the improvements introduced in our algorithm. Specifically, using the unitaries M and M_2 to control the phases, our algorithm increases the probability of measuring s . We note that this result is consistent with the quantum Goldreich-Levin result where $q = 2$ and is a successful generalization.

3.3 Discussions

3.3.1 Classical Reduction vs Quantum Reduction

Adcock and Cleve [AC02] provided a lower bound on query complexity in classical reductions. We introduce their result (Theorem 3.2) and then compare the quantum reduction that we propose with the classical one.

Let n be a positive integer and $\delta > 0$. Let $s \in \{0, 1\}^n$ and let the information about s be available only from inner product and equivalence queries, which are defined below.

Definition 3.2. A classical inner product (*IP*) query (with bias δ) has input $a \in \{0, 1\}^n$ and outputs a bit that is slightly correlated with $a \cdot s$ (the inner product of a and s modulo two) in the sense that

$$\Pr_a[IP(a) = a \cdot s] \geq \frac{1}{2} + \delta.$$

The above probability is with respect to a random $a \xleftarrow{\$} \{0, 1\}^n$.

Definition 3.3. A quantum equivalence (*EQ*) query has input $a \in \{0, 1\}^n$, and the output is 1 if $a = s$ and 0 otherwise.

Theorem 3.2 ([AC02]). Any classical probabilistic algorithm finding s with success probability $\delta > 0$ requires more than $2^{n/2}$ *EQ* queries or $\Omega(n/\delta^2)$ *IP* queries when $\delta \geq \sqrt{n}2^{-n/3}$.

This theorem shows that, in a black-box framework, a classical reduction has a query complexity more than $\Omega(n/\delta^2)$. On the other hand, the quantum algorithm we present in Section 3.2 achieves a query complexity of 2. Therefore, it is demonstrated that the quantum reduction is quantitatively more efficient than the classical one.

3.3.2 Relationship with Bernstein-Vazirani Algorithm

The Bernstein-Vazirani algorithm [BV93] is one of the foundational early quantum algorithms that demonstrates the utility of quantum computing. When the Bernstein-Vazirani algorithm is constructed using a predictor defined in Definition 3.1 as an oracle that returns the inner product, it can be formalized as the following theorem.

Theorem 3.3 (Bernstein-Vazirani Algorithm [BV93]). If there is a quantum $(s, 2, 1/2)$ -predictor U_P , then there is a quantum algorithm that finds s with probability 1. It invokes U_P and $U_P^\dagger$ once each.

As this theorem indicates, the quantum Goldreich-Levin theorem over $\mathbb{Z}_q$ introduced in this chapter generalizes the Bernstein-Vazirani algorithm. The algorithm in this study extends the oracle, which returns the inner product, to a biased oracle and generalizes the algebra to $\mathbb{Z}_q$, providing a method to find s under these more generalized conditions.

Chapter 4

Quantum Search-to-Decision Reduction for the Learning with Errors Problem

The learning with errors (LWE) problem is considered to be hard even for quantum computers, and it serves as a foundational assumption in the construction of post-quantum cryptographic schemes. Therefore, it is of significant importance to provide an analysis of the LWE problem in the presence of quantum computation. In this chapter, by means of the generalized quantum Goldreich–Levin theorem established in Chapter 3, we present a quantum search-to-decision reduction for the LWE problem as an application. This chapter reorganizes [Sudo et al., AFRICACRYPT 2023, LNCS 14064, 395–413] and [Sudo et al., IEICE Trans. 108(2), 104–116 (2025)] with slight modifications to fit the context.

4.1 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 [Sho99] 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.

4.1.1 Backgrounds

The LWE problem introduced by Regev [Reg05] 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 the 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 LWE search 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 the 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 coordinate 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.

There exist hardness proofs for the search LWE based on reductions from worst-case lattice problems (BDD/gapSVP), which are considered to be hard not only for classical computers but also for quantum computers. Together with the search-to-decision reduction, the fact that the search LWE can be reduced from BDD and gapSVP implies the hardness of decisional LWE. Consequently, the hardness of the decisional LWE problem serves as the security source of many post-quantum cryptographic primitives, such as oblivious transfer [PVW08], identity-based encryption [ABB10; Cas+10; GPV08], fully homomorphic encryption [BV11], etc.

Practical importance of quantum search-to-decision reduction. The LWE challenge [LWE challenge] is the basis to ensure the difficulty of the LWE problem. In practice, the LWE challenge is intended to solve the 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 $\text{loss}_{s2d}(n)$ plus the security loss of the scheme itself, where $\text{loss}_{s2d}(\cdot)$ 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 $\text{loss}_{s2d}(n_Q)$? If we know the efficiency $\text{loss}_{Qs2d}(\cdot)$ of quantum search-to-decision reduction, we know that we can actually implement the scheme with a size based on $\text{loss}_{Qs2d}(n_Q)$, which is expected to partially mitigate the effect of the increase of n_Q over n .

4.1.2 Our Contributions

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 $\mathcal{O}(\frac{q^2 m^2 \log n}{\epsilon^2})$ times.

We additionally give a search-to-decision reduction for the learning parity with noise problem in section 4.A as well. 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 4.1: 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 4.B.

** The success probability and the query complexity of this algorithm are very complex. The specific values are given in 4.B.

	Success probability	Query complexity	Sample complexity
[Reg05]*	$1 - o(1)$	$\tilde{\mathcal{O}}(\frac{nq}{\epsilon^2})$	$\tilde{\mathcal{O}}(\frac{mnq}{\epsilon^2})$
[MM11]**	$\frac{1}{\text{poly}(n)}$	$\text{poly}(n)$	m
Th.4.1	$\frac{4q^2 \epsilon^3}{27(q-1)^5 m^3}$	2	m
Th.4.2	$\Omega(\frac{\epsilon}{qm})$	$\mathcal{O}(\frac{qm}{\epsilon})$	$m + \mathcal{O}(n)$
Cor.4.1	$1 - o(1)$	$\mathcal{O}(\frac{q^2 m^2 \log n}{\epsilon^2})$	$\tilde{\mathcal{O}}(\frac{qm^2}{\epsilon})$

Prior works. There are various incomparable search-to-decision reductions for the LWE problem [Reg05; Pei09; App+09; MM11; MP12; Bra+13]. Regev [Reg05] who introduced the LWE problem showed search-to-decision reduction in [Reg05]. It imposes constraints that modulus q must be prime and bounded by $\text{poly}(n)$. 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 [Pei09] extends Regev’s reduction for the case where q can be expressed as a product of distinct prime numbers in $\text{poly}(n)$, but it requires the error distribution to be Gaussian. Applebaum, Cash, Peikert, and Sahai [App+09] 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 [MP12] give a reduction that runs in $\text{poly}(\log q)$. Micciancio and Mol [MM11] 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. This work aims to leverage quantum computation and quantum queries to the decisional LWE adversary in order to speed up the reduction, using fewer queries and less computation time.

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 [Cha+23] 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 theorem 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.

4.1.3 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 the classical reductions by Micciancio and Mol [MM11], Applebaum, Ishai, and Kushilevitz [AIK07]. 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.

4.2 Quantum Reduction Algorithms

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

The learning parity with noise (LPN) problem is the special case of $\text{LWE}_{n,m,q,\chi}$ 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 [MM11], Applebaum, Ishai, and Kushilevitz [AIK07] and Dötting [Döt15].

We define a quantum distinguisher for the decisional LWE problem.

Definition 4.1. A quantum ϵ -distinguisher for the decisional $\text{LWE}_{n,m,q,\chi}$ problem is unitary operation $\mathbf{U}_D$ and an auxiliary $|\text{aux}\rangle$ such that, the second register of $\mathbf{U}_D |A, y\rangle |0\rangle |\text{aux}\rangle$ is

measured in computational basis, yielding the value $D(A, y) \in \{0, 1\}$, then

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

holds.

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

4.2.1 Sample-Preserve Reduction

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

The following lemmas (4.1, 4.2, 4.3), states that there is a prediction-to-decision reduction for the LWE problem.

Lemma 4.1. For all $s \in \mathbb{Z}_q^n$, $a \in \mathbb{Z}_q^n$,

$$\{(a' + ra, y) | a' \xleftarrow{\$} \mathbb{Z}_q^n, e \leftarrow \chi, r \xleftarrow{\$} \mathbb{Z}_q^n, y = (a' + ra) \cdot s + e\} = \mathcal{LWE}_{n,s,q,\chi} \quad (4.1)$$

and

$$\{(a' + ra, y - r) | a' \xleftarrow{\$} \mathbb{Z}_q^n, e \leftarrow \chi, r \xleftarrow{\$} \mathbb{Z}_q^n, y = (a' + ra) \cdot s + e\} = \mathcal{R}_{n,q} \quad (4.2)$$

holds.

Proof of Lemma 4.1 We begin by proving equation (4.1). Since a' is chosen uniformly at random, $a' + ra$ is also uniformly random. Therefore, distribution $\{(a' + ra, y) | a' \xleftarrow{\$} \mathbb{Z}_q^n, e \leftarrow \chi, r \xleftarrow{\$} \mathbb{Z}_q^n, y = (a' + ra) \cdot s + e\}$ is identical to distribution $\mathcal{LWE}_{n,s,q,\chi}$.

Next, we prove equation (4.2). Since r is chosen uniformly at random, r is also uniformly random. Moreover, $y - r$ is also uniformly random as well. From equation (4.1), it follows that the equation (4.2). $\square$ (**Lemma 4.1.**)

Lemma 4.2. There exists a quantum prediction algorithm P using $(\mathbf{U}_D, |\text{aux}\rangle)$ once, satisfies

$$\Pr[P(a) = a \cdot s] > \frac{1}{q} + \frac{\epsilon}{q}. \quad (4.3)$$

The probability is over choice of random coins $s \xleftarrow{\$} \mathbb{Z}_q^n$, $(A, y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m$ and $r \xleftarrow{\$} \mathbb{Z}_q^m$.

Proof of Lemma 4.2 P is defined by the following procedure.

1. Sample $(A, y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m$.
2. Compute $\mathbf{U}_D |(A + r \cdot a^T, y)\rangle |0\rangle |\text{aux}\rangle$.
3. Measure the second register in the computational base.
4. If the second register is in state $|0\rangle$, output 0, otherwise if it is in state $|1\rangle$, output 1.

Let us analyze the behavior of P . Since equation (4.1) and (4.2),

$$\begin{aligned} & \Pr[P(a) = a \cdot s = 0] \\ &= \Pr[a \cdot s = 0] \Pr[D(A + r \cdot a^T, y) = 0 | a \cdot s = 0] \\ &= \Pr[a \cdot s = 0] \Pr[D(A + r \cdot a^T, A \cdot s + e) = 0 | a \cdot s = 0] \\ &= \Pr[a \cdot s = 0] \Pr[D(A + r \cdot a^T, (A + r \cdot a^T) \cdot s + e) = 0 | a \cdot s = 0] \\ &= \Pr[a \cdot s = 0] \Pr[D(A', y) = 0 : (A', y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m] \\ &= \frac{1}{q} \Pr[D(A, y) = 0 : (A', y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m] \end{aligned}$$

and

$$\begin{aligned}
& \Pr[P(a) = a \cdot s = 1] \\
&= \Pr[a \cdot s = 1] \Pr[D(A + r \cdot a^T, y) = 1 | a \cdot s = 1] \\
&= \Pr[a \cdot s = 1] \Pr[D(A + r \cdot a^T, (A + r \cdot a^T) \cdot s + e - (r \cdot a^T) \cdot s) = 1 | a \cdot s = 1] \\
&= \Pr[a \cdot s = 1] \Pr[D(A + r \cdot a^T, (A + r \cdot a^T) \cdot s + e - r) = 1 | a \cdot s = 1] \\
&= \Pr[a \cdot s = 1] \Pr[D(A', y) = 1 : (A', y) \leftarrow \mathcal{R}_{n,q}^m] \\
&= \frac{1}{q} \Pr[D(A', y) = 1 : (A', y) \leftarrow \mathcal{R}_{n,q}^m]
\end{aligned}$$

holds. Therefore,

$$\begin{aligned}
& \Pr[P(a) = a \cdot s] \\
&= \Pr[P(a) = a \cdot s = 0] + \Pr[P(a) = a \cdot s = 1] \\
&= \frac{1}{q} (\Pr[D(A, y) = 1 : (A, y) \leftarrow \mathcal{LW}\mathcal{E}_{n,s,q,\chi}^m] + \Pr[D(A, r') = 1 : (A, r') \leftarrow \mathcal{R}_{n,q}^m]) \\
&= \frac{1}{q} + \frac{1}{q} (\Pr[D(A, y) = 0 : (A, y) \leftarrow \mathcal{LW}\mathcal{E}_{n,s,q,\chi}^m] - \Pr[D(A, r') = 0 : (A, r') \leftarrow \mathcal{R}_{n,q}^m]) \\
&> \frac{1}{q} + \frac{\epsilon}{q}
\end{aligned}$$

holds.

□ (**Lemma 4.2.**)

Next, let's consider the probability of outputting $a \cdot s$ for a given input a when the random coins used in the prediction algorithm P 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 $\mathcal{U}_P$ to be the same as the algorithm defined in Proof 4.2.1, except for some variables, such as $s, (A, y), r$, are hardwired.

Lemma 4.3. $\mathcal{U}_P$ is a $(s, \frac{2\epsilon}{3q})$ -predictor with probability at least $\frac{\epsilon}{3q}$ over choice of the random coins.

Proof of Lemma 4.3 Firstly, random coins are selected $s \xleftarrow{\$} \mathbb{Z}_q^n$, $L \leftarrow \mathcal{LW}\mathcal{E}_{n,s,q,\chi}^m$ and $r \xleftarrow{\$} \mathbb{Z}_q$. $\mathcal{U}_P$ is defined by the following quantum circuit 4.1.

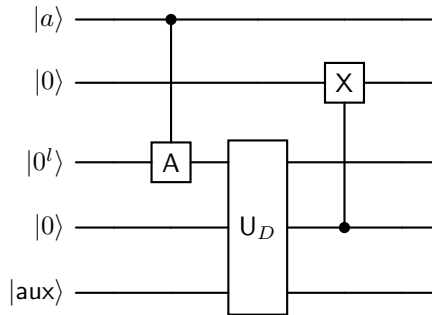


Figure 4.1: Quantum circuit $\mathcal{U}_P$.

$\mathcal{U}_P$ consist of 3 sequence of unitary operations. The control-A operator maps an input state $|a\rangle |0^l\rangle$ to the state $|a\rangle |A + r \cdot a^T, y\rangle$. $\mathcal{U}_D$ is a distinguisher. The control-X operator

maps an input state $|0\rangle|0\rangle$ to the state $|0\rangle|0\rangle$ and $|1\rangle|0\rangle$ to the state $|1\rangle|1\rangle$, where the first register is control state and the second register stores the output.

When the last register of $U_P|a\rangle|0\rangle|0^l\rangle|0\rangle|aux\rangle$ is measured in the computational basis, we denote this as $P(a)$. If U_P be a $(s, \frac{2\epsilon}{3q})$ -predictor, it satisfies the following (4.4).

$$\Pr\left[P(a) = a \cdot s : a \xleftarrow{\$} \mathbb{Z}_q^n\right] > \frac{1}{q} + \frac{2\epsilon}{3q}. \quad (4.4)$$

Define a set $G = \{(s, (A, y), r) | \text{Inequality (4.4) holds}\}$. By the definition of G , when $s \xleftarrow{\$} \mathbb{Z}_q^n$, $(A, y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}$, $r \xleftarrow{\$} \mathbb{Z}_q^m$, then

$$\begin{aligned} & \Pr[P(a) = a \cdot s] \\ &= \Pr[P(a) = a \cdot s \wedge (s, (A, y), r) \in G] \\ & \quad + \Pr[P(a) = a \cdot s \wedge (s, (A, y), r) \notin G] \\ &\leq \Pr[(s, (A, y), r) \in G] \\ & \quad + \Pr[(s, (A, y), r) \notin G] \Pr[P(a) = a \cdot s | (s, (A, y), r) \notin G] \\ &\leq \Pr[(s, (A, y), r) \in G] + \Pr[P(a) = a \cdot s | (s, (A, y), r) \notin G] \\ &\leq \Pr[(s, (A, y), r) \in G] + \frac{1}{q} + \frac{2\epsilon}{3q} \end{aligned}$$

holds. From Lemma 4.2,

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

holds. Therefore,

$$\Pr[(s, (A, y), r) \in G] \geq \frac{\epsilon}{3q}$$

holds.

□ (Lemma 4.3.)

Theorem 4.1. Let q be a prime. If there is a quantum ϵ -distinguisher $(U_D, |aux\rangle)$ for the decisional $\text{LWE}_{n,m,q,\chi}$ problem, then there is a quantum algorithm that solves the search $\text{LWE}_{n,m,q,\chi}$ problem with probability at least $\frac{4\epsilon^3}{27q(q-1)^2}$ using U_D and $U_D^\dagger$ once each and an auxiliary $|aux\rangle$.

Proof of Theorem 4.1 This theorem follows immediately from Lemma 4.3 and Theorem 3.1.

□ (Theorem 4.1.)

We stress that Theorem 4.1 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.

4.2.2 Amplify the Success Probability

We show how to amplify the success probability of the reduction algorithm given in Section 4.2.1. However, this process increases query complexity and sample complexity.

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

We propose an algorithm **Verify**, which tests a candidate solution for the LWE problem. We first sample $(a_i, y_i)_{i \in [\mathcal{O}(n)]} \leftarrow \mathcal{LWE}_{n,s,q,\chi}^{\mathcal{O}(n)}$ 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 $\alpha < \frac{1}{8}$. We remind the definition of discrete Gaussian distribution. We denote $\mathbb{T}$ for $\mathbb{R}/\mathbb{Z}$, in other words, the segment $[0, 1)$ with addition modulo 1. 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),

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

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,

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

Lemma 4.4. 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 (4.5) with probability $1 - \text{negl}(n)$ (resp. any desired constant $0 < p < 1$)

$$\text{Verify}(s') = \begin{cases} 1 & \text{if } s' = s \\ 0 & \text{if } s' \neq s. \end{cases} \quad (4.5)$$

The description of the algorithm **Verify** that satisfies the conditions of (4.5) can be given as follows:

Initially, sample $(a_i, y_i)_{i \in [cn]} \leftarrow \mathcal{LWE}_{n,s,q,\chi}^{cn}$. Upon receiving input $s' \in \mathbb{Z}_q^n$, **Verify** works as follows.

Verify(s') :

$count = 0$
for $i \in \{1, 2, \dots, cn\}$
 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 of Lemma 4.4 Let us analyze the probability that the **Verify** satisfies the condition (4.5).

Let $\beta = \Pr[|\chi| \geq \frac{q}{8}] (< \frac{1}{2})$, $\delta = \frac{1}{2\beta} - 1$.

$$\begin{aligned} & \Pr[\text{Verify satisfies (4.5)}] \\ &= \Pr[\text{Verify}(s) = 1 \wedge \forall s' \neq s, \text{Verify}(s') = 0] \\ &\geq \Pr[\text{Verify}(s) = 1] \cdot \Pr[\forall s' \neq s, \text{Verify}(s') = 0] \\ &\geq (1 - \Pr[\text{Verify}(s) \neq 1]) \cdot \left(1 - \sum_{s' \neq s} \Pr[\text{Verify}(s') = 1]\right) \\ &\geq (1 - \exp\left(-\frac{\delta^2 \beta cn}{2 + \delta}\right)) \cdot \left(1 - (q^n - 1) \exp\left(-\frac{cn}{24}\right)\right) \\ &= 1 - \text{negl}(cn) \end{aligned}$$

The third inequality follows from the Chernoff bound (2.2). Therefore, **Verify** satisfies (4.5) with probability $1 - \text{negl}(n)$ for a 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 . $\square$ (**Lemma 4.4**.)

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 [Bra+02]” than by simply judging the answer each time. We define a unitary $U_{\text{Reflection}}$, referred to as a reflection oracle in the context of amplitude amplification.

Definition 4.2. A quantum reflection algorithm is a unitary operation $U_{\text{Reflection}}$ such that the following holds (4.6)

$$U_{\text{Reflection}} = I - |s\rangle\langle 0^l| \langle s| \langle 0^l| \quad (4.6)$$

holds.

Lemma 4.5. We can construct a quantum algorithm $U_{\text{Reflection}}$ from **Verify** that satisfies the condition (4.5).

Proof of Lemma 4.5 This lemma can be achieved by phase kickback. From Lemma 4.4 there exists a verification algorithm satisfying (4.5), then there exist an unitary operation such that

$$U_{\text{Verify}} |x\rangle |y\rangle |0\rangle = \begin{cases} |x\rangle |y\rangle |1\rangle & \text{if } x = s \wedge y = 0^l \\ |x\rangle |y\rangle |0\rangle & \text{if } x \neq s \vee y \neq 0^l \end{cases} \quad (4.7)$$

holds.

Consider the following quantum operation $U_{\text{Reflection}}$. When given $|x\rangle |y\rangle |0\rangle$, apply U_{Verify} , multiply the phase by $(-1)^z$ according to the value of the last register z and apply $U_{\text{Verify}}^\dagger$. 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. $\square$

Theorem 4.2. 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 $\text{LWE}_{n,m,q,\chi}$ problem, then there is a quantum algorithm that solves the search $\text{LWE}_{n,m',q,\chi}$ problem with probability $\Omega(\frac{\epsilon}{qm})$ using U_D and $U_D^\dagger$ $\mathcal{O}(\frac{qm}{\epsilon})$ times, where $m' = m + \mathcal{O}(n)$.

Proof of Theorem 4.2 Initially, s is chosen uniform random from $\mathbb{Z}_q^n$, we get $(A, y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m$ and samples random coins. From Lemma 4.1 and Theorem 4.1 we can construct a quantum algorithm U_S using U_D and $U_D^\dagger$ once each, and that satisfies

$$|\langle s| \langle 0^l| U_S |0^n\rangle |0^l\rangle|^2 > \frac{4q^2\epsilon^2}{9(q-1)^4m^2} \quad (4.8)$$

with probability $\frac{\epsilon}{3m(q-1)}$ over choice of $s \xleftarrow{\$} \mathbb{Z}_q^n$, $(A, y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m$ and random coins. From Lemma 4.4 and Lemma 4.5 we can construct a verification algorithm **Verify** (resp. a quantum algorithm $U_{\text{Reflection}}$) that satisfies (4.5) (resp. (4.6)) with constant probability using $\mathcal{O}(n)$ samples of $\mathcal{LWE}_{n,s,q,\chi}$.

Assuming that U_S satisfies (4.8), **Verify** satisfies (4.5), and $U_{\text{Reflection}}$ satisfies (4.6), consider the following procedure. The procedure is to compute

$$(-U_S(I - |0^n\rangle\langle 0^l| \langle 0^n| \langle 0^l|)U_S^\dagger U_{\text{Reflection}})^k U_S |0^n\rangle |0^l\rangle, \quad (4.9)$$

measures states in the computational basis, test it by `Verify`. As shown in [Bra+02], 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 $U_S^\dagger$ 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 $U_D^\dagger$ $\mathcal{O}(\frac{qm}{\epsilon})$ times, and with sample complexity $m + \mathcal{O}(n)$.

□ (**Lemma 4.5.**)

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 4.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 4.2.1.

- Whether the predictor U_P has desired property(condition (4.4)) depends on the choice of $s \xleftarrow{\$} \mathbb{Z}_q^n$ (see Lemma 4.1).
- 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 re-randomize 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. 4.2.

Reduction Algorithm with high success probability
Choose $\tilde{\mathcal{O}}(n)$ samples from $\mathcal{LWE}_{n, s, q, \chi}$, and construct <code>Verify</code> .
for $i = 1, \dots, \lceil \frac{3qm \log n}{\epsilon} \rceil$:
Choose m samples of LWE instances (A_i, y_i) .
Sample a random vector $s_i^* \xleftarrow{\$} \mathbb{Z}_q^n$,
set $(A_i, y'_i) := (A_i, y_i + A_i \cdot s_i^*)$, and construct $U_{P,i}$
Construct $\text{Verify}_i(x) := \text{Verify}(x - s_i^*)$ and $U_{\text{Verify}, i}$.
Run the second reduction algorithm in parallel.
If there is a s_j that passes the j -th verification test Verify_j ,
then output $s = s_j - s_j^*$.

Figure 4.2: Reduction Algorithm with high success probability

From Lemma 4.4, we can construct a verification algorithm `Verify` that satisfies (4.5) 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.

Corollary 4.1. 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 $\text{LWE}_{n, m, q, \chi}$ problem, then there is a quantum algorithm that solves the search $\text{LWE}_{n, m', q, \chi}$ problem with probability $1 - o(1)$ using U_D and $U_D^\dagger$ $\mathcal{O}(\frac{q^2 m^2 \log n}{\epsilon^2})$ times, where $m' = \tilde{\mathcal{O}}(\frac{qm^2}{\epsilon})$.

Appendix

4.A Quantum 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 (LPN) problem (Table 4.2). First, from Theorem 4.1 we immediately obtain the following corollary.

Table 4.2: 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
[KS06]	$\frac{\epsilon}{4}$	$\mathcal{O}(\frac{n \log n}{\epsilon^2})$	$\mathcal{O}(\frac{mn \log n}{\epsilon^2})$
[AIK07]	$\Omega(\frac{\epsilon^3}{n})$	$\mathcal{O}(\frac{n^2}{\epsilon^2})$	m
Cor.4.2	$\frac{16\epsilon^3}{27m^3}$	2	m
Cor.4.3	$\Omega(\frac{\epsilon}{m})$	$\mathcal{O}(\frac{m}{\epsilon})$	$m + \mathcal{O}(n)$

Corollary 4.2. If there is a quantum ϵ -distinguisher U_D for the decisional $\text{LWE}_{n,m,2,\text{Ber}_\mu}$ problem, then there is a quantum algorithm that solves the search $\text{LWE}_{n,m,2,\text{Ber}_\mu}$ problem with probability at least $\frac{16\epsilon^3}{27m^3}$ using U_D and $U_D^\dagger$ 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 4.6. We can construct an algorithm $\text{Verify}_{\text{LPN}}$, and it satisfies the following functionality (4.10) with desired probability $0 < c < \frac{2^n - 1}{2^n}$.

For all $x \in \{0, 1\}^n$,

$$\text{Verify}_{\text{LPN}}(x) = \begin{cases} 1 & \text{if } x = s \\ 0 & \text{if } x \neq s. \end{cases} \quad (4.10)$$

Proof of Lemma 4.6. Initially, sample $(A, y) \leftarrow \mathcal{LPN}_{s,\mu}^l$, where $A \in \{0, 1\}^{l \times n}$ is a random Boolean matrix, $l = \left\lceil -\left(\frac{6}{(\frac{1}{2}-\mu)^2} \log_e(\frac{1}{2}(\frac{1}{2^n} - \frac{c}{2^n-1}))\right) \right\rceil = \mathcal{O}(n)$ and $y = A \cdot s \oplus e$ is a noisy inner products, note that $e \in \{0, 1\}^l$ is errors distributed from Ber_μ^l . Upon receiving input $x \in \{0, 1\}^n$, $\text{Verify}_{\text{LPN}}$ works as follows.

$$\begin{aligned} &\text{Verify}_{\text{LPN}}(x) : \\ &\text{if } |\text{weight}(A \cdot x + y) - \mu l| < \frac{1}{2}(\frac{1}{2} - \mu)l \\ &\quad \text{then output 1} \\ &\quad \text{else output 0.} \end{aligned}$$

Note that the function $\text{weight}(\cdot)$ 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_μ^l , $\mathbb{E}(\text{weight}(A \cdot x + y)) = \mathbb{E}(\text{weight}(e)) = \mu l$. If $x \neq s$, $A \cdot x + y$ is uniformly random, since

A is sampled uniformly random. Therefore $\mathbb{E}(\text{weight}(A \cdot x + y)) = \frac{1}{2}l$. Let us analyze the probability that the $\text{Verify}_{\text{LPN}}$ satisfies the condition (4.10).

$$\begin{aligned}
& \Pr[\text{Verify}_{\text{LPN}} \text{ satisfies (4.10)}] \\
&= \Pr[\text{Verify}_{\text{LPN}}(s) = 1 \wedge \forall s' \neq s, \text{Verify}_{\text{LPN}}(s') = 0] \\
&\geq \Pr[\text{Verify}_{\text{LPN}}(s) = 1] \cdot \Pr[\forall s' \neq s, \text{Verify}_{\text{LPN}}(s') = 0] \\
&\geq \Pr[\text{Verify}_{\text{LPN}}(s) = 1] \left(1 - \sum_{s' \neq s} \Pr[\text{Verify}_{\text{LPN}}(s') = 1] \right) \\
&\geq \left(1 - 2 \exp\left(-\frac{l}{12\mu} \left(\frac{1}{2} - \mu\right)^2\right) \right) \left(1 - (2^n - 1) \left(2 \exp\left(-\frac{l}{6} \left(\frac{1}{2} - \mu\right)^2\right) \right) \right) \\
&\geq \left(1 - \left(\frac{1}{2^n} - \frac{c}{2^n - 1} \right)^{\frac{1}{2\mu}} \right) \left(1 - (2^n - 1) \left(\frac{1}{2^n} - \frac{c}{2^n - 1} \right) \right) \\
&\geq \left(1 - \left(\frac{1}{2^n} - \frac{c}{2^n - 1} \right) \right) \left(1 - 2^n \left(\frac{1}{2^n} - \frac{c}{2^n - 1} \right) \right) \\
&\geq \left(1 - \frac{1}{2^n} \right) \frac{2^n c}{2^n - 1} \\
&= c
\end{aligned}$$

The second inequality follows from union bound, and the third inequality follows from the Chernoff bound (2.2). $\square$ (**Lemma 4.6.**)

Corollary 4.3. If there is a quantum ϵ -distinguisher $\mathcal{U}_D$ for the decisional $\text{LWE}_{n,m,2,\text{Ber}_\mu}$ problem, then there is a quantum algorithm that solves the search $\text{LWE}_{n,m',2,\text{Ber}_\mu}$ problem with probability $\Omega(\frac{\epsilon}{m})$ using $\mathcal{U}_D$ and $\mathcal{O}(\frac{m}{\epsilon})$ times, where $m' = m + \mathcal{O}(n)$.

The proof of this corollary is given in the same way as in Theorem 4.2.

4.B Classical Reduction

4.B.1 A Simple Reduction

In this section, we give a simple classical search-to-decision reduction for the LWE problem by [Vai]. It is based on the reduction given by Regev [Reg05] and is useful to compare efficiency.

Definition 4.3. A (classical) algorithm D is said to be a ϵ -distinguisher for the decisional $\text{LWE}_{n,m,q,\chi}$ problem if

$$\left| \Pr_s[D(A, y) = 1 : (A, y) \leftarrow \mathcal{LWE}_{n,s,q,\chi}^m] - \Pr\left[D(A, r) = 1 : A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}, r \xleftarrow{\$} \mathbb{Z}_q^m \right] \right| > \epsilon$$

holds.

The algorithm described in Fig. 4.3 solves the search $\text{LWE}_{n,m',q,\chi}$ 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, refer to [Vai].

4.B.2 Classical Sample-Preserve Reduction

In this section, we give a brief analysis of the search-to-decision reduction by Micciancio and Mol [MM11]. Their search-to-decision reduction for LWE is shown via search-to-decision

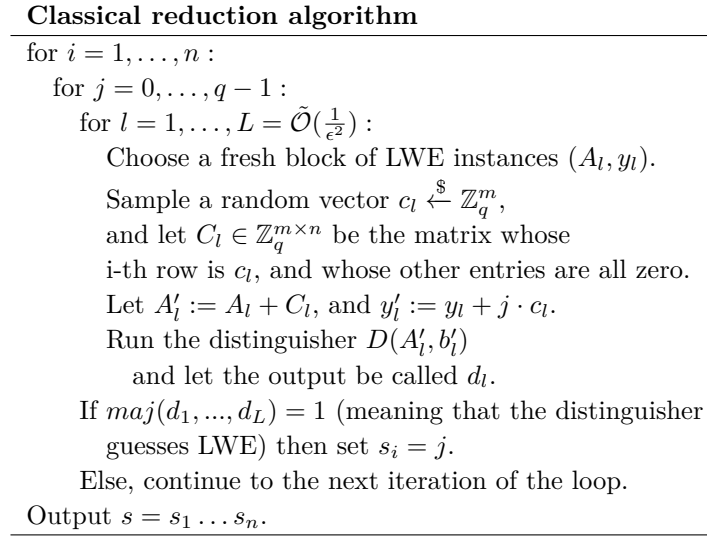


Figure 4.3: Reduction Algorithm with high success probability

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 ([MM11], Proposition 3.9 and Lemma 3.4) the success probability of the search-to-decision reduction for the knapsack functions is $\frac{\epsilon}{3}$ where $\epsilon \geq \left(\frac{d^{*3}\tilde{\delta}}{d^3(d^*-1)}\right)(2 - \frac{\pi^2}{6})$ 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 $\Omega(\frac{\tilde{\delta}}{m^3q^4}) - \text{negl}(n)$.

In ([MM11], Lemma 3.4), they use Significant Fourier Transform [Aka08] with $\tau = \frac{\epsilon^2}{4}$, $N = |\mathbb{Z}_{d^*}^l|$ and $\|f\|_2 = \|f\|_\infty = 1$. The running time of the Significant Fourier Transform is at most $\tilde{\mathcal{O}}(\log N (\frac{\|f\|_2^2}{\tau})^{1.5} (\frac{\|f\|_\infty^2}{\eta^2})^2 \lg \frac{1}{\mu})$ 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 $\tilde{\mathcal{O}}(\log N (\frac{\|f\|_2^2}{\tau})^{1.5} (\frac{\|f\|_\infty^2}{\eta^2})^2 \lg \frac{1}{\mu}) = \tilde{\mathcal{O}}(\frac{\log(d^*l)}{\epsilon^{11}})$. Hence From ([MM11], Proposition 3.9 and Lemma 3.4), the query complexity of the search-to-decision reduction for LWE is $\tilde{\mathcal{O}}(\frac{\log(d^*m)}{\epsilon^{11}})$ $\mathcal{O}(1) = \tilde{\mathcal{O}}(\frac{\log(d^*m)}{\epsilon^{11}})$ where d^* is some polynomial such that $d^* \geq q$.

Chapter 5

Practical Quantum Public Key Encryption from One-way Functions

Just as Cryptomania and Minicrypt are distinguished, it has long been believed that public-key encryption cannot be constructed from one-way functions alone. However, recent studies have shown that by leveraging quantum computation and communication, it is indeed possible to construct quantum public-key encryption schemes from one-way functions.

Nevertheless, the quantum public-key encryption schemes proposed in these works suffer from two major limitations that prevent them from serving as true analogues of classical public-key encryption: practical infeasibility of implementation and the lack of verifiability of quantum public keys. In this chapter, we address these challenges. This chapter reorganizes [Sudo et al., APKC 2025, 44–53].

5.1 Introduction

5.1.1 Backgrounds

Quantum information theory has revolutionized the field of cryptography. For example, there are quantum attacks on cryptosystems based on integer factorization or discrete logarithms, which are believed to be classically secure, due to Shor’s algorithm [Sho99]. In addition, there are some cryptographic primitives that are classically impossible, such as quantum money [Wie83], copy protection [Aar09], and certified deletion [BI20].

One of the most promising applications of quantum cryptography is the quantum key distribution (QKD) [BB84], which provides information-theoretic security and its security is based on the principles of quantum mechanics. Research in quantum public key cryptography is also being actively pursued. Quantum public key encryption (QPKE) is a type of public key encryption that uses a quantum channel for public keys (and sometimes also for ciphertexts). Although Impagliazzo and Rudich demonstrated in the classical setting that one-way functions (OWFs) are insufficient to imply the existence of public key encryption (PKE) in a black-box manner [IR89], there are some recent results showing that QPKE can be constructed from OWFs (or even weaker assumptions) [Bar+23; BS23a; BS23b; Col23; Kit+24; MY24; MW24]. However, there are some drawbacks in their studies. In the following paragraph, we highlight the main challenges in this field.

Difficulty of Implementation. Some previous research provides the construction of QPKE from OWFs as stated above. However, their constructions are all difficult to implement with current technology. This is because they use coherent superpositions of many-qubit states as quantum public keys, which play a crucial role in ensuring the security of the schemes. Generating such quantum states would require fault-tolerant quantum computers, which might be achievable decades from now. A protocol that can be implemented through the transmissions and measurements of just single-qubits, like BB84 protocol [BB84], is the most desirable because it allows for the experimental realization of the protocol on the present-day hardware.

Authentication of Quantum Public Keys. When we consider public key cryptosystems, we must think about how to securely distribute the public key. If the public key is a classical string, its authenticity can be easily verified by digital signatures. However, this method cannot be used if the public key is quantum states. In fact, it is well known that quantum states are impossible to sign digitally [Bar+02; AGM21]. Nevertheless, some previous research assumes the existence of secure quantum channels. This assumption is unrealistic.

In certain quantum cryptographic primitives, authentication does not necessarily require digital signatures on quantum states. For QPKE, it is sufficient to ensure that the protocol can filter out noisy quantum public keys which do not provide correctness and security. Kitagawa et al. [Kit+24] introduced the concept of decryption error detectability and mentioned an even stronger variant of decryption error detectability, which we call strong error detectability. They also introduced a security notion called indistinguishability against public key tampering chosen plaintext attack (IND-pkT-CPA) security. These notions take into account the adversary's tampering of the public key. Decryption error detectability guarantees that a legitimate receiver of a ciphertext can detect if the decrypted message is different from the message intended by the sender. Strong error detectability guarantees that a sender can notice if a given quantum public key does not provide decryption correctness.

Strong error detectability is a more desirable requirement for QPKE compared to decryption error detectability. This is because a QPKE scheme that only satisfies the decryption error detectability may require an additional step for the receiver, who must send a confirmation after decrypting the ciphertext to notice whether the message was successfully shared. In such a case, the protocol would become a 3 round interaction, diminishing the advantage of PKE, which essentially has the ability to share a message in 2 round. Kitagawa et al. only provide a construction of QPKE with decryption error detectability. There is no established technique to authenticate the quantum public keys non-interactively.

5.1.2 Our Contributions

We construct a QPKE from OWFs in the random oracle model [BR93] to address the challenges that we previously mentioned. It offers ease of implementation and authentication of the quantum public keys, but its security holds against restricted adversaries, who perform individual attacks and only have classical access to the random oracle. A detailed comparison is presented in Related Work 5.1.4.

We assume authenticated classical channels, and we consider that the quantum channels may be exposed to an eavesdropping or a tampering by a third party. In our protocol, the receiver, who issues public keys, only requires probabilistic polynomial-time (PPT) computation and the ability to generate and transmit a single-qubit, while the sender, who sends an encrypted message by using the public key, also needs PPT computation and the ability to perform projective measurement on a single-qubit. Our QPKE scheme satisfies two security properties: strong error detectability and IND-pkT-CPA security. The IND-pkT-CPA

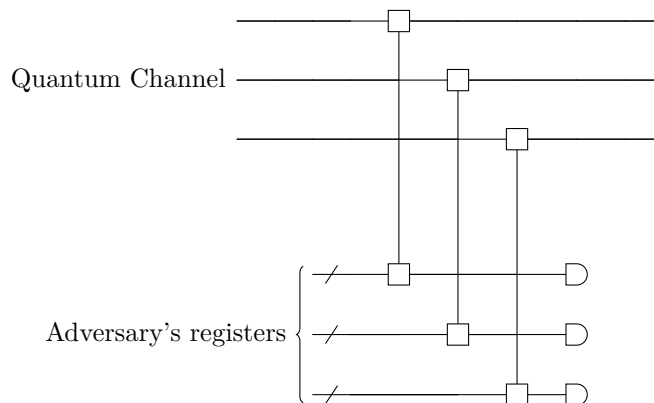


Figure 5.1: Individual Attack.

security ensures that the indistinguishability holds even if a message is encrypted by a public key tampered with by an adversary. Note that IND-pkT-CPA security alone does not guarantee that the message can be shared at the end of the protocol. A QPKE that satisfies these two security requirements enables the message to be securely shared when the protocol completes (i.e., when the sender does not discard the public key as invalid). However, our construction of QPKE only satisfies the IND-pkT-CPA security against adversaries with weak quantum capabilities. Specifically, it is secure against restricted QPT adversaries that perform an individual attack and have “classical” access to the random oracle.

In the individual attack, the adversary independently entangles a quantum register for each qubit on the quantum channel. Figure 5.1 illustrates the individual attack on the quantum channel. The concept of individual attack was introduced in the context of QKD. Individual attacks align with realistic attack scenarios. The capabilities required for general coherent attacks exceed current technological limits. This is because the speed of quantum communication can be arbitrarily set, forcing the attacker to maintain coherence for the corresponding duration, but this is not feasible with current technology.

A random oracle is typically instantiated by a hash function, and the inability of the adversary to make quantum queries can be viewed as a scenario where the given hash function cannot be implemented in the adversaries’ quantum computer. This class of adversaries includes polynomial-time algorithms with some quantum memory. In other words, an adversary is required to have quantum capabilities higher than those of an honest participant. In our construction, the input length of the random oracle can be polynomially increased to force the adversaries to require more and more powerful quantum hardware, while keeping the protocol qubit-wise. Since quantum computers face scalability challenges, we believe that such restrictions are reasonable for near-term quantum adversaries.

We note that these restrictions are essential for the security of our scheme. There exists an effective attack for our scheme that does not have these restrictions, which we provide in Section 5.6. We also note that there is a significant difference between the threat posed by advancements in quantum computing to classical cryptography and its impact on quantum cryptography. For example, it is possible to break RSA encryption using quantum computers developed decades from now. However, it is impossible to break quantum cryptography using quantum computers built in the future. In this case, the adversary requires maintaining the coherence for a long time, but it cannot be feasible by current technology.

5.1.3 Technical Overview

We sketch the key idea of the construction. We construct a QPKE scheme from pseudorandom functions PRF and digital signatures DS. Let H be a random oracle. We use λ as a security parameter. The public key in our construction consists of a classical public key $\mathbf{cpk}$ and a quantum public key $\mathbf{qpk}$. The classical public key $\mathbf{cpk}$ consists of $(r, z_1, z_2, \dots, z_d)$. The value r acts as a label characterizing this public key $(\mathbf{cpk}, \mathbf{qpk})$, and each z_j is given by $z_j = H(x_j) \oplus (k_j || \sigma_j)$, where x_j is a randomly chosen sample, $k_j := \text{PRF}_{\text{KPRF}}(r || j)$ and σ_j is a signature of k_j . The quantum public key $\mathbf{qpk}$ consists of d blocks of n -qubits $(\mathbf{qpk}_1, \mathbf{qpk}_2, \dots, \mathbf{qpk}_d)$. Here, each $\mathbf{qpk}_j$ is either $|x_j\rangle$ or $|\bar{x}_j\rangle$, and the basis is chosen randomly. The sender randomly chooses the computational basis or the Hadamard basis to measure each $\mathbf{qpk}_j$ and can obtain around $d/2$ instances of k_j , and can verify success or failure to obtain this value k_j through the signatures σ_j . The XOR of these values $\{k_j\}$ is used as the key K . The ciphertext $\text{ct} = (r, \{j\}_{\text{suc}}, K \oplus m)$ consists of the tag r , the set of indices j where the measurement was successful, and an encrypted message $K \oplus m$. An important point is that if the sender cannot obtain a sufficient number (for example $d/3$) of these values, he discards the public key as invalid. When the receiver receives ct , compute the key K by the indices $\{j\}_{\text{suc}}$ and decode m .

When the protocol completes successfully (i.e., when the sender does not discard the public key as invalid), the sender's key and the receiver's key match, which is ensured by the unforgeability of the digital signature. Therefore, it offers strong error detectability. If a third party wishes to learn information about the key K , they would need to obtain x_j or disrupt $\mathbf{qpk}_j$ for the j -th instance where the sender's and the receiver's chosen basis match. However, for anyone with only weak quantum capabilities, the probability of obtaining x_j from $\mathbf{qpk}_j$ is about $1/2$, and if too many $\mathbf{qpk}_j$ instances are interrupted, the sender will discard the public key as invalid. In this way, the secrecy of the message m is maintained.

Our proof technique for the IND-pkT-CPA security relies on a hybrid argument. We consider an entanglement-based game in a hypothetical setting where the quantum public key is replaced with halves of the Einstein-Podolsky-Rosen (EPR) pairs [EPR35]. In this hypothetical game, we use the appropriate uncertainty relation to prove its security and show that the actual protocol is equally secure.

5.1.4 Related Work

QKD [BB84] enables two parties to share a key using an untrusted quantum channel and an authenticated classical communication channel, in the same setting as in this work. Also, similar to our construction, QKD has the practical advantage of using only products of single-qubit states. Most importantly, QKD offers information-theoretic security, while our QPKE is based on OWFs and offers security against limited quantum adversaries. The advantage of our work is that it is a public key encryption. The protocol can be completed in two messages and there is no need to record interactions from previous sessions, while in QKD, the secret information from the previous sessions needs to be recorded. Additionally, since our scheme has strong error detectability, invalid quantum public keys are simply discarded by the sender. There is no need for interactive communication for tampered quantum states or noisy quantum states.

Kawachi et al. [Kaw+12] formally define QPKE (with quantum public key and quantum ciphertext) and propose a concrete construction from a newly introduced hardness assumption, related to the graph automorphism problem. Morimae and Yamakawa [MY24] show that the QPKE defined in [Kaw+12] can be achieved by classical symmetric key encryption. Coladangelo [Col23] and Barooti et al. [Bar+23] independently study QPKE from OWFs or even weaker assumptions. These constructions rely on the existence of an authenticated quantum channel. Kitagawa et al. [Kit+24] and Malavolta and Walter [MW24] construct

QPKE with security against the tampering of quantum public keys, based on OWFs. The former constructs a QPKE scheme with detection error detectability and CCA security. The latter constructs a QPKE scheme with an everlasting security. The everlasting security means that the message remains information-theoretically hidden, provided that the adversary was computationally bounded during the execution of the protocol, and even if it has unbounded computational power later. Their constructions satisfy stronger security notions, such as the CCA security and everlasting security, which we do not consider in this work. However, they do not offer strong error detectability. Similarly to our work, Barhoush and Salvail [BS23b] study QPKE against restricted adversaries. They construct a QPKE scheme with CCA1 security in the bounded quantum storage model. In this model, the quantum memory required by honest users is significantly smaller than that required by adversaries. However, they assume an authenticated quantum channel. In their companion work [BS23a], they address the problem of quantum public key distribution through time-dependent signatures. Time-dependent signatures can be constructed from OWFs, but the verification key needs to be continuously updated.

5.2 Quantum Key Encapsulation Mechanism

We introduce a quantum key encapsulation mechanism (QKEM), which is a quantum analog of a key encapsulation mechanism (KEM). KEM is a type of public-key cryptography that enables key sharing between two parties. PKE can be constructed by combining key sharing via KEM and a one-time pad. Since KEM can be seen as a more fundamental primitive than PKE, this work focuses on QKEM rather than QPKE. The definition of QKEM is based on the definition of QPKE by Kitagawa et al. [Kit+24]. A minor difference is that, in our definition, we separate the classical part of the public key, referred to as cpk , and the quantum state part, referred to as qpk . Additionally, we specify the challenge public key that the adversary attacks in the IND-pkT-CPA game.

Definition 5.1. (Quantum Key Encapsulation Mechanism.) A quantum key encapsulation mechanism (QKEM) scheme is defined as a tuple of QPT algorithms ($\text{Gen}, \text{PKGen}, \text{Encaps}, \text{Decaps}$).

- $\text{Gen}(1^\lambda) \rightarrow (\text{sk}, \text{vk})$: Given a security parameter 1^λ as input, the secret key generation algorithm outputs a secret key sk and a verification key vk .
- $\text{PKGen}(\text{sk}) \rightarrow (\text{cpk}, \text{qpk})$: Given a secret key sk as input, the public key generation algorithm outputs a classical string cpk and a quantum public key qpk .
- $\text{Encaps}(\text{vk}, (\text{cpk}, \text{qpk})) \rightarrow (\text{K}, \text{ct})/\perp$: Given a verification key vk and a public key (cpk, qpk) as input, the encapsulation algorithm outputs key K and its encapsulation ct or a rejection symbol $\perp$.
- $\text{Decaps}(\text{sk}, \text{ct}) \rightarrow \text{K}$: Given a secret key sk and a encapsulation ct , the decapsulation algorithm outputs a key K .

We require the following correctness.

Correctness. A QKEM satisfies the correctness if,

$$\Pr \left[\begin{array}{l} (\text{sk}, \text{vk}) \leftarrow \text{Gen}(1^\lambda), \\ (\text{cpk}, \text{qpk}) \leftarrow \text{PKGen}(\text{sk}), \\ (\text{K}, \text{ct}) \leftarrow \text{Encaps}(\text{vk}, (\text{cpk}, \text{qpk})), \\ \text{K}' \leftarrow \text{Decaps}(\text{sk}, \text{ct}) \end{array} \right] \geq 1 - \text{negl}(\lambda).$$

We require the following strong error detectability for QKEM. The strong error detectability guarantees that a sender can notice if a given quantum public key, tampered by a third party, does not provide decryption correctness.

Strong Error Detectability The strong error detectability for QKEM is defined by the following game between a challenger $\mathcal{CH}$ and a QPT adversary $\mathcal{A}$.

1. $\mathcal{CH}$ runs $(\text{sk}, \text{vk}) \leftarrow \text{Gen}(1^\lambda)$, creates m public keys $(\text{cpk}^i, \text{qpk}^i)_{i \in [m]}$ by executing $\text{PKGen}(\text{sk})$, and gives $(\text{vk}, (\text{cpk}^i, \text{qpk}^i)_{i \in [m]})$ to $\mathcal{A}$.
2. $\mathcal{A}$ outputs $(\text{cpk}^i, \text{qpk}')$, for some $i \in [m]$.
3. $\mathcal{CH}$ computes $\text{Encaps}(\text{vk}, (\text{cpk}^i, \text{qpk}'))$, if it outputs $\perp$, abort this game. If it outputs $(\text{K}, \text{ct}) \leftarrow \text{Encaps}(\text{vk}, (\text{cpk}^i, \text{qpk}'))$, $\mathcal{CH}$ computes $\text{K}' \leftarrow \text{Decaps}(\text{sk}, \text{ct})$.

A QKEM satisfies the strong error detectability if for all QPT adversaries $\mathcal{A}$ and for all polynomial $m(\lambda)$,

$$\Pr[\text{K} \neq \text{K}'] \leq \text{negl}(\lambda)$$

holds.

We require the following indistinguishability against public key tampering chosen plain-text attack (IND-pkT-CPA) security for QKEM. The IND-pkT-CPA security guarantees that no QPT adversary can distinguish between the shared key and a random string.

IND-pkT-CPA Let k to be the length of the shared key of QKEM. The IND-pkT-CPA security for QKEM is defined by the following indistinguishability game between a challenger $\mathcal{CH}$ and a QPT adversary $\mathcal{A}$.

$\text{Game}_{\text{QKEM}, b^*}^{\text{indcpa}}$:

1. $\mathcal{CH}$ runs $(\text{sk}, \text{vk}) \leftarrow \text{Gen}(1^\lambda)$, creates m public keys $(\text{cpk}^i, \text{qpk}^i)_{i \in [m]}$ by executing $\text{PKGen}(\text{sk})$, and creates challenge public key $(\text{cpk}, \text{qpk}) \leftarrow \text{PKGen}(\text{sk})$, and gives $(\text{vk}, (\text{cpk}^i, \text{qpk}^i)_{i \in [m]}, (\text{cpk}, \text{qpk}))$ to $\mathcal{A}$.
2. $\mathcal{A}$ outputs qpk' .
3. $\mathcal{CH}$ computes $\text{Encaps}(\text{vk}, (\text{cpk}, \text{qpk}'))$, if it outputs $\perp$, abort this game. If it outputs $(\text{K}_0, \text{ct}) \leftarrow \text{Encaps}(\text{vk}, (\text{cpk}, \text{qpk}'))$, $\mathcal{CH}$ samples $\text{K}_1 \xleftarrow{\$} \{0, 1\}^k$, and gives $(\text{K}_{b^*}, \text{ct})$ to $\mathcal{A}$.
4. $\mathcal{A}$ outputs a guess b .

A QKEM satisfies the IND-pkT-CPA security if for all QPT adversaries $\mathcal{A}$ which performs an individual attack and for all polynomial $m(\lambda)$,

$$\left| \Pr \left[b = 1 : \text{Game}_{\text{QKEM}, 0}^{\text{indcpa}} \right] - \Pr \left[b = 1 : \text{Game}_{\text{QKEM}, 1}^{\text{indcpa}} \right] \right| \leq \text{negl}(\lambda)$$

holds.

Remark 1. In the definition of Kitagawa et al. [Kit+24], the adversary receives a polynomial number of public keys $(\text{cpk}^i, \text{qpk}^i)_{i \in [m]}$ and outputs a tampered public key $(\text{cpk}^j, \text{qpk}')$ for some $j \in [m]$. In our definition, the adversary receives a polynomial number of public keys $(\text{cpk}^i, \text{qpk}^i)_{i \in [m]}$ and the challenge public key (cpk, qpk) , but tampers with only one of them, the challenge public key. Such a change incurs a polynomial security loss, but it does not cause any essential difference.

5.3 Building Blocks

We give formal definitions for the following cryptographic primitives as building blocks.

Definition 5.2. (Pseudorandom Functions.) We say that a keyed function $\text{PRF}_k : \{0, 1\}^{m(\lambda)} \rightarrow \{0, 1\}^{n(\lambda)}$ that is classical deterministic polynomial time algorithm is a secure pseudorandom function if for any QPT adversary $\mathcal{A}$,

$$\left| \Pr \left[1 \leftarrow \mathcal{A}^{\text{PRF}_k(\cdot)}(1^\lambda) \right] - \Pr \left[1 \leftarrow \mathcal{A}^f(1^\lambda) \right] \right| \leq \text{negl}(\lambda)$$

holds, where $k \xleftarrow{\$} \{0, 1\}^\lambda$ and $f : \{0, 1\}^{m(\lambda)} \rightarrow \{0, 1\}^{n(\lambda)}$ is a function chosen uniformly random.

Definition 5.3. (Digital Signatures.) A digital signature scheme DS with a message space $\mathcal{M}$ is a tuple of PPT algorithms (Gen, Sign, Verify).

- $\text{Gen}(1^\lambda) \rightarrow (\text{sk}, \text{vk})$: Given a security parameter 1^λ as input, the key generation algorithm outputs a signing/verification key pair (sk, vk) .
- $\text{Sign}(\text{sk}, m) \rightarrow \sigma$: Given a signing key sk and a message m as input, the signing algorithm outputs a signature σ .
- $\text{Verify}(\text{vk}, m, \sigma) \rightarrow \top / \perp$: Given a verification key vk , a message m , and a signature σ as input, the verification algorithm outputs $\top$ or $\perp$.

We require the following correctness for DS.

Correctness DS satisfies correctness if for all $m \in \mathcal{M}$,

$$\Pr \left[\text{Verify}(\text{vk}, m, \sigma) = \top : \begin{array}{l} (\text{sk}, \text{vk}) \leftarrow \text{SigGen}(1^\lambda), \\ \sigma \leftarrow \text{Sign}(\text{sk}, m) \end{array} \right] = 1$$

holds.

We require the following strong-existentially unforgeability under chosen message attacks (sEUF-CMA) security for DS.

sEUF-CMA The sEUF-CMA security for DS is defined by the following game between a challenger $\mathcal{CH}$ and a QPT adversary $\mathcal{A}$.

1. $\mathcal{CH}$ runs $(\text{sk}, \text{vk}) \leftarrow \text{SigGen}(1^\lambda)$, initializes a list $Q = \{\}$, and gives vk to $\mathcal{A}$.
2. Throughout the entire game, $\mathcal{A}$ is given access to signing oracle $\text{Sign}(\text{sk}, \cdot)$. Given an input m , the signing oracle runs $\sigma \leftarrow \text{Sign}(\text{sk}, m)$, updates $Q \leftarrow Q \cup \{(m, \sigma)\}$, and returns σ to $\mathcal{A}$.
3. $\mathcal{A}$ outputs a forgery (m', σ') .

DS satisfies the sEUF-CMA security if for all QPT adversaries $\mathcal{A}$,

$$\Pr [\text{Verify}(\text{vk}, m', \sigma') = \top] \leq \text{negl}(\lambda)$$

where $(m', \sigma') \notin Q$ holds.

We note that secure pseudorandom functions and sEUF-CMA secure digital signatures exist if OWFs exist [Gol04; Zha12].

5.4 Construction

In this section, we give a construction of QKEM from secure pseudorandom functions and a sEUF-CMA secure digital signature scheme. We remind that these primitives exist if OWFs exist. Let $\text{PRF}_{\text{kPRF}} : \{0, 1\}^{d+\lceil \log d \rceil} \rightarrow \{0, 1\}^k$ be a secure pseudorandom function, where $d = \omega(\log \lambda)$, $\text{DS} = (\text{SigGen}, \text{Sign}, \text{Verify})$ be a sEUF-CMA secure digital signature scheme whose signature length is l , and $H : \{0, 1\}^n \rightarrow \{0, 1\}^{k+l}$ be a hash function modeled as a random oracle, where $n = \omega(\log \lambda)$. k is the length of the shared key offered by the QKEM. Our construction of the QKEM scheme $\text{QKEM} = (\text{Gen}, \text{PKGen}, \text{Encaps}, \text{Decaps})$ is given as follows.

- $\text{Gen}(1^\lambda)$:
 1. Generate $(\text{sk}_{\text{Sig}}, \text{vk}_{\text{Sig}}) \leftarrow \text{SigGen}(1^\lambda)$.
 2. Sample $\text{kPRF} \xleftarrow{\$} \{0, 1\}^\lambda$.
 3. Output $(\text{sk}, \text{vk}) = ((\text{sk}_{\text{Sig}}, \text{kPRF}), \text{vk}_{\text{Sig}})$.
- $\text{PKGen}(\text{sk})$:
 1. Parse $\text{sk} = (\text{sk}_{\text{Sig}}, \text{kPRF})$.
 2. Sample $r \xleftarrow{\$} \{0, 1\}^d$, $\theta = \theta_1 \theta_2 \cdots \theta_d \xleftarrow{\$} \{0, 1\}^d$.
 3. For $j \in [d]$.
 - (a) Sample $x_j \xleftarrow{\$} \{0, 1\}^n$.
 - (b) Compute $y_j = \text{PRF}_{\text{kPRF}}(r||j)$, $\sigma_j \leftarrow \text{Sign}(\text{sk}_{\text{Sig}}, r||j||\theta_j||y_j)$, $z_j = H(x_j) \oplus (y_j||\sigma_j)$.
 4. Output $\text{cpk} = (r, (z_j)_{j \in [d]})$ and $\text{qpk} = (\text{qpk}_j)_{j \in [d]}$, where $\text{qpk}_j = |x_j\rangle$ if $\theta_j = 0$, otherwise $\text{qpk}_j = |\underline{x_j}\rangle$.
- $\text{Encaps}(\text{vk}, (\text{cpk}, \text{qpk}'))$:
 1. Parse $\text{vk} = \text{vk}_{\text{Sig}}$, $\text{cpk} = (r, (z_j)_{j \in [d]})$, $\text{qpk}' = (\text{qpk}'_j)_{j \in [d]}$.
 2. Sample $\theta = \theta_1 \theta_2 \cdots \theta_d \xleftarrow{\$} \{0, 1\}^d$.
 3. Initialize a list $\text{IDX} = \{\}$, set $\text{K} = 0$, and set a counter $\text{count} = 0$.
 4. For $j \in [d]$.
 - (a) If $\theta_j = 0$, measure qpk'_j in the computational basis and get x'_j .
 - i. Compute $y'_j||\sigma'_j = z_j \oplus H(x'_j)$.
 - ii. If $\text{Verify}(\text{vk}_{\text{Sig}}, r||j||0||y'_j, \sigma'_j) = \top$, update $\text{K} \leftarrow \text{K} \oplus y'_j$, $\text{IDX} \leftarrow \text{IDX} \cup \{j\}$, and $\text{count} \leftarrow \text{count} + 1$.
 - (b) If $\theta_j = 1$, measure qpk'_j in the Hadamard basis and get x'_j .
 - i. Compute $y'_j||\sigma'_j = z'_j \oplus H(x'_j)$.
 - ii. If $\text{Verify}(\text{vk}_{\text{Sig}}, r||j||1||y'_j, \sigma'_j) = \top$, update $\text{K} \leftarrow \text{K} \oplus y'_j$, $\text{IDX} \leftarrow \text{IDX} \cup \{j\}$, and $\text{count} \leftarrow \text{count} + 1$.
 5. If $\text{count} \geq \frac{d}{3}$, output K and $\text{ct} = (r, \text{IDX})$, otherwise output $\perp$.
- $\text{Decaps}(\text{sk}, \text{ct})$:
 1. Parse $\text{sk} = (\text{sk}_{\text{Sig}}, \text{kPRF})$, $\text{ct} = (r, \text{IDX})$.
 2. Set $\text{K} = 0$.
 3. For $j \in \text{IDX}$, compute $y_j = \text{PRF}_{\text{kPRF}}(r||j)$ and update $\text{K} \leftarrow \text{K} \oplus y_j$.

4. Output K.

We note that QKEM is relatively easy to implement. It only requires participants to perform PPT computations and single-qubit operations (qubit-wise transmissions and projective measurements).

Theorem 5.1. If DS satisfies the correctness, then the QKEM scheme presented above satisfies the correctness.

Proof of Theorem 5.1 Let $\theta = \theta_1\theta_2 \dots \theta_d$ be the bases chosen in PKGen, and let $\theta' = \theta'_1\theta'_2 \dots \theta'_d$ be the bases chosen in Encaps. We recall that PRF is a deterministic algorithm. From the correctness of DS, for all j , where $\theta_j = \theta'_j$, $\text{PRF}_{\text{kPRF}}(r||j)$ can be shared. The probability that the number of matching bases falls below $d/3$ is negligible with respect to λ , easily followed by the Chernoff bound (2.2). Therefore, QKEM satisfies the correctness.

□ (Theorem 5.1.)

Theorem 5.2. If DS satisfies the sEUF-CMA security, then the QKEM scheme presented above satisfies the strong error detectability.

Theorem 5.3. If PRF is a secure pseudorandom functions, DS satisfies the sEUF-CMA security, and $n = \omega(\log \lambda)$, then the QKEM scheme presented above satisfies the IND-pkT-CPA security in the classical random oracle model.

We will prove the strong error detectability and the IND-pkT-CPA security in the next section.

5.5 Security Proofs

In this section, we give formal proofs of Theorems 5.2 and 5.3.

We introduce the uncertainty principle, which expresses the trade-off that measuring one physical quantity with high precision necessarily increases the uncertainty in another.

Entropic Uncertainty Relation [Deu83; Col+17] Let ρ be an arbitrary single-qubit state, X be an outcome when ρ is measured in the computational basis, and Z be an outcome when ρ is measured in the Hadamard basis. Then the following inequality holds.

$$H_{\min}(X) + H_{\min}(Z) \geq -2 \log \frac{1 + \sqrt{\frac{1}{2}}}{2} \quad (5.1)$$

Proof of Theorem 5.2 We give a proof by contradiction. Suppose that there exists an adversary that can break the strong error detectability of QKEM. If the sender's key K and the receiver's key K' do not match, it means that a message not signed by the sender has passed verification within the Encaps algorithm. In other words, a signature for a message different from $\text{PRF}_{\text{kPRF}}(r^i||j)$ has been forged for some $j \in [d]$. Therefore, an adversary that can break the strong error detectability can easily be used to construct an adversary that breaks the sEUF-CMA security of DS. However, this contradicts the sEUF-CMA security of DS. Thus, QKEM satisfies the strong error detectability.

□ (Theorem 5.2.)

We provide an outline of the proof of Theorem 5.3. The proof uses a hybrid argument and consists of two major steps. First, we change the target key that the adversary attempts to gain information about in the security game from the sender's key to the receiver's key. This change is justified by the strong error detectability. Next, we replace the challenge

quantum public key with halves of the EPR pairs. The security in this EPR-based game is proved by the uncertainty principle. By the hybrid argument, the security of the original protocol is ensured.

Proof of Theorem 5.3 We give a proof by a hybrid argument. In the following, we assume that PRF is a secure pseudorandom function, DS satisfies the security of sEUF-CMA, $n = \omega(\log \lambda)$, and $m(\lambda)$ is a polynomial. We note that, by Theorem 5.2, the QKEM scheme satisfies the strong error detectability. We define $\text{Hyb}(0, b^*)$, which coincides with the IND-pkT-CPA game $\text{Game}_{\text{QKEM}, b^*}^{\text{indcpa}}$ in the classical random oracle model.

$\text{Hyb}(0, b^*) :$

1. $\mathcal{CH}$ runs $(\text{sk}, \text{vk}) \leftarrow \text{Gen}(1^\lambda)$, creates m public keys $(\text{cpk}^i, \text{qpk}^i)_{i \in [m]}$ by executing $\text{PKGen}(\text{sk})$, and creates challenge public key $(\text{cpk}, \text{qpk}) \leftarrow \text{PKGen}(\text{sk})$, and gives $(\text{vk}, (\text{cpk}^i, \text{qpk}^i)_{i \in [m]}, (\text{cpk}, \text{qpk}))$ to $\mathcal{A}$.
2. $\mathcal{A}$ is given classical access to the random oracle H throughout the game.
3. $\mathcal{A}$ outputs qpk' .
4. $\mathcal{CH}$ computes $\text{Encaps}(\text{vk}, (\text{cpk}, \text{qpk}'))$, if it outputs $\perp$, abort this game. If it outputs $(K_0, \text{ct}) \leftarrow \text{Encaps}(\text{vk}, (\text{cpk}, \text{qpk}'))$, $\mathcal{CH}$ samples $K_1 \xleftarrow{\$} \{0, 1\}^k$, and gives (K_{b^*}, ct) to $\mathcal{A}$.
5. $\mathcal{A}$ outputs a guess b .

$\text{Hyb}(1, b^*) :$ Step (1) to (3) and (5) are the same as $\text{Hyb}(0, b^*)$. In step (5) of $\text{Hyb}(1, b^*)$, the adversary distinguishes between the sender's key (instead of the receiver's key) and a uniformly random string. Formally, we define step (4) as follows.

4. $\mathcal{CH}$ computes $\text{Encaps}(\text{vk}, (\text{cpk}, \text{qpk}'))$, if it outputs $\perp$, abort this game. If it outputs $(K, \text{ct}) \leftarrow \text{Encaps}(\text{vk}, (\text{cpk}, \text{qpk}'))$, $\mathcal{CH}$ computes $K_0 \leftarrow \text{Decaps}(\text{sk}, \text{ct})$, $K_1 \xleftarrow{\$} \{0, 1\}^k$, and gives (K_{b^*}, ct) to $\mathcal{A}$.

Lemma 5.1. For all QPT adversaries $\mathcal{A}$, the following holds.

$$|\Pr[b = 1 : \text{Hyb}(1, b^*)] - \Pr[b = 1 : \text{Hyb}(0, b^*)]| \leq \text{negl}(\lambda).$$

Proof of Lemma 5.1 $\text{Hyb}(0, b^*)$ and $\text{Hyb}(1, b^*)$ are different when the sender's key and the receiver's key do not match. This event occurs with a negligible probability because of the strong error detectability. Therefore,

$$|\Pr[b = 1 : \text{Hyb}(1, b^*)] - \Pr[b = 1 : \text{Hyb}(0, b^*)]| \leq \text{negl}(\lambda)$$

holds. $\square$ (**Lemma 5.1.**)

We define $\text{Gen}'(\cdot)$ the same as $\text{Gen}(\cdot)$, except for sampling $f(\cdot)$ uniformly instead of $k_{\text{PRF}} \xleftarrow{\$} \{0, 1\}^\lambda$. Formally, as follows.

- $\text{Gen}'(1^\lambda) :$
 1. Generate $(\text{sk}_{\text{Sig}}, \text{vk}_{\text{Sig}}) \leftarrow \text{SigGen}(1^\lambda)$.
 2. Sample $f \xleftarrow{\$} \{f | f : \{0, 1\}^{d+\lceil \log d \rceil} \rightarrow \{0, 1\}^k\}$.
 3. Output $(\text{sk}, \text{vk}) = ((\text{sk}_{\text{Sig}}, f), \text{vk}_{\text{Sig}})$.

We define $\text{PKGen}'(\cdot)$ the same as $\text{PKGen}(\cdot)$, except that we use $f(\cdot)$ instead of $\text{PRF}_{k_{\text{PRF}}}(\cdot)$. Formally, as follows.

- $\text{PKGen}'(\text{sk})$:
 1. Parse $\text{sk} = (\text{sk}_{\text{sig}}, f)$.
 2. Sample $r \xleftarrow{\$} \{0, 1\}^d$, $\theta = \theta_1 \theta_2 \cdots \theta_d \xleftarrow{\$} \{0, 1\}^d$.
 3. For $j \in [d]$.
 - (a) Sample $x_j \xleftarrow{\$} \{0, 1\}^n$.
 - (b) Compute $y_j = f(r||j)$, $\sigma_j \leftarrow \text{Sign}(\text{sk}_{\text{sig}}, r||j||\theta_j||y_j)$, $z_j = H(x_j) \oplus (y_j||\sigma_j)$.
 4. Output $\text{cpk} = (r, (z_j)_{j \in [d]})$ and $\text{qpk} = (\text{qpk}_j)_{j \in [d]}$, where $\text{qpk}_j = |x_j\rangle$ if $\theta_j = 0$, otherwise $\text{qpk}_j = |\underline{x_j}\rangle$.

$\text{Hyb}(2, b^*)$: all the same as $\text{Hyb}(1, b^*)$, except for using $\text{Gen}'(\cdot)$ and $\text{PKGen}'(\cdot)$ instead of $\text{Gen}(\cdot)$ and $\text{PKGen}(\cdot)$.

Lemma 5.2. For all QPT adversaries $\mathcal{A}$, the following holds.

$$|\Pr[b = 1 : \text{Hyb}(2, b^*)] - \Pr[b = 1 : \text{Hyb}(1, b^*)]| \leq \text{negl}(\lambda).$$

Proof of Lemma 5.2 Since PRF is secure pseudorandom functions, no QPT adversary can distinguish these hybrids with noticeable probability. $\square$ (**Lemma 5.2.**)

$\text{Hyb}(3, b^*)$: Step (3) to (5) are all the same as $\text{Hyb}(2, b^*)$. The difference between $\text{Hyb}(3, b^*)$ and $\text{Hyb}(2, b^*)$ is that, in $\text{Hyb}(3, b^*)$, z_j is determined first, and then the output of the random oracle $H(x_j)$ is decided. Formally, we define step (1) and (2) of $\text{Hyb}(3, b^*)$ as follows.

1. $\mathcal{CH}$ does as follows.

- (a) Run $(\text{sk}, \text{vk}) \leftarrow \text{Gen}'(1^\lambda)$, create m public keys $(\text{cpk}^i, \text{qpk}^i)_{i \in [m]}$ by executing $\text{PKGen}'(\text{sk})$.
- (b) Parse $\text{sk} = (\text{sk}_{\text{sig}}, f)$.
- (c) Sample $r \xleftarrow{\$} \{0, 1\}^d$, $\theta = \theta_1 \theta_2 \cdots \theta_d \xleftarrow{\$} \{0, 1\}^d$.
- (d) For $j \in [d]$.
 - i. Sample $x_j \xleftarrow{\$} \{0, 1\}^n$, $z_j \xleftarrow{\$} \{0, 1\}^{k+l}$.
 - ii. Compute $y_j = f(r||j)$, $\sigma_j \leftarrow \text{Sign}(\text{sk}_{\text{sig}}, r||j||\theta_j||y_j)$, $w_j = z_j \oplus (y_j||\sigma_j)$.
- (e) Give vk , $(\text{cpk}^i, \text{qpk}^i)_{i \in [m]}$, $\text{cpk} = (r, (z_j)_{j \in [d]})$ and $\text{qpk} = (\text{qpk}_j)_{j \in [d]}$ to $\mathcal{A}$, where $\text{qpk}_j = |x_j\rangle$ if $\theta_j = 0$, otherwise $\text{qpk}_j = |\underline{x_j}\rangle$.

2. $\mathcal{A}$ is given classical access to the oracle H' throughout the game. The oracle H' responds as follows.

$$H'(x) = \begin{cases} H(x) & \text{if } x \neq x_j \text{ for all } j \in [d] \\ w_j & \text{if } x = x_j \text{ for some } j \in [d] \end{cases}$$

Lemma 5.3. For all adversaries $\mathcal{A}$, the following holds.

$$|\Pr[b = 1 : \text{Hyb}(3, b^*)] - \Pr[b = 1 : \text{Hyb}(2, b^*)]| \leq \text{negl}(\lambda).$$

Proof of Lemma 5.3 $\text{Hyb}(2, b^*)$ and $\text{Hyb}(3, b^*)$ are different when the x_j is used to construct the public keys $(\text{cpk}^i, \text{qpk}^i)_{i \in [m]}$. Since $n = \omega(\log \lambda)$ and $m(\lambda)$ is a polynomial, the probability of such an event occurs is negligible with respect to λ . $\square$ (**Lemma 5.3.**)

$\text{Hyb}(4, b^*)$: Step (2) to (5) are all the same as $\text{Hyb}(3, b^*)$. The difference between $\text{Hyb}(4, b^*)$ and $\text{Hyb}(3, b^*)$ is that, instead of sending the products of single-qubit states as the challenge quantum public key, sending halves of the EPR pairs and measuring the other halves. Formally, we define step (1) of $\text{Hyb}(4, b^*)$ as follows.

1. $\mathcal{CH}$ does as follows.

Step (a) to (c) are all the same as $\text{Hyb}(3, b^*)$.

- (d) Create dn EPR pairs. Each pair is referred to as the (j, j') -th EPR pair, where $j \in [d]$ and $j' \in [n]$.
- (e) Give vk , $(\text{cpk}^i, \text{qpk}^i)_{i \in [m]}$, $\text{cpk} = (r, (z_j)_{j \in [d]})$ and the second halves of each EPR pairs to $\mathcal{A}$.
- (f) For $j \in [d]$.
 - i. If $\theta_j = 0$, measure his second halves of (j, j') -th EPR pairs for all $j' \in [n]$ in the computational basis and get x_j .
 - ii. If $\theta_j = 1$, measure his second halves of (j, j') -th EPR pairs for all $j' \in [n]$ in the Hadamard basis and get x_j .

Lemma 5.4. For all adversaries $\mathcal{A}$, the following holds.

$$\Pr[b = 1 : \text{Hyb}(4, b^*)] = \Pr[b = 1 : \text{Hyb}(3, b^*)].$$

Proof of Lemma 5.4 These hybrids are totally equivalent. $\square$ (**Lemma 5.4.**)

$\text{Hyb}(5, b^*)$: This hybrid is all the same as $\text{Hyb}(4, b^*)$ except for step (1)(c). In $\text{Hyb}(5, b^*)$, $\mathcal{CH}$ aborts when r overlaps. Formally, we define step (1)(c) of $\text{Hyb}(5, b^*)$ as follows.

- 1. (c) Sample $r \xleftarrow{\$} \{0, 1\}^d$, $\theta = \theta_1 \theta_2 \cdots \theta_d \xleftarrow{\$} \{0, 1\}^d$. If for some $i \in [m]$, $r = r^i$ holds, abort this game.

Lemma 5.5. For all adversaries $\mathcal{A}$, the following holds.

$$|\Pr[b = 1 : \text{Hyb}(5, b^*)] - \Pr[b = 1 : \text{Hyb}(4, b^*)]| \leq \text{negl}(\lambda).$$

Proof of Lemma 5.5 $\text{Hyb}(4, b^*)$ and $\text{Hyb}(5, b^*)$ are different when the tag of the public key r overlaps. Such an event occurs with a negligible probability because $d = \omega(\log \lambda)$ is sufficiently large. $\square$ (**Lemma 5.5.**)

Lemma 5.6. For all adversaries $\mathcal{A}$ with polynomial number (with respect to λ) of queries for the random oracle, the following holds.

$$|\Pr[b = 1 : \text{Hyb}(5, 0)] - \Pr[b = 1 : \text{Hyb}(5, 1)]| \leq \text{negl}(\lambda).$$

Proof of Lemma 5.6 Let $\rho_{j, j'}$ denote a posteriori state, which was half of the (j, j') -th EPR pair held by the challenger, after a measurement performed by the adversary on his register. Then, apply the uncertainty principle for $\rho_{j, j'}$, the following inequality holds.

$$H_{\min}(X_{j, j', 0}) + H_{\min}(X_{j, j', 1}) \geq -2 \log \frac{1 + \sqrt{\frac{1}{2}}}{2},$$

where $X_{j, j', 0}$ be an outcome when $\rho_{j, j'}$ is measured in the computational basis, and $X_{j, j', 1}$ be an outcome when $\rho_{j, j'}$ is measured in the Hadamard basis. Since $\mathcal{A}$ performs an individual

attack, for all $k, l \in [n]$, $b \in \{0, 1\}$, $X_{j,k,b}$ and $X_{j,l,b}$ are independent. Therefore, by additivity of min-entropy,

$$H_{\min}(X_{j,0}) + H_{\min}(X_{j,1}) \geq -2n \log \frac{1 + \sqrt{\frac{1}{2}}}{2}$$

holds, where $X_{j,0} = (X_{j,1,0}, X_{j,2,0}, \dots, X_{j,n,0})$ and $X_{j,1} = (X_{j,1,1}, X_{j,2,1}, \dots, X_{j,n,1})$. It indicates that, either $H_{\min}(X_{j,0})$ or $H_{\min}(X_{j,1})$ is greater than $-n \log \frac{1 + \sqrt{\frac{1}{2}}}{2}$. We note that $-\log \frac{1 + \sqrt{\frac{1}{2}}}{2} > 0$.

Since $H_{\min}(X_{j,0})$ ($H_{\min}(X_{j,1})$) corresponding to the probability that the adversary guesses $X_{j,0}$ ($X_{j,1}$) correctly, if the adversary only makes polynomial number of classical queries to the random oracle, for all $j \in [d]$, $\Pr[\mathcal{A} \text{ queries } x_j \text{ to the oracle}] = \frac{1}{2} + \text{negl}(\lambda)$ holds, and each event is independent of the others. We denote this probability by p .

Let θ' be the bases of the measurement chosen in the **Encaps** in the step (4), **IDX** be the part of the output of the **Encaps**, $c = \theta \oplus \theta'$, c_j be the j -th character of c , $S = \{j | c_j = 0\}$, and E be an event that $\mathcal{A}$ makes at least $\frac{d}{3}$ independent queries x_j for $j \in S$.

Hyb(5, 0) and **Hyb**(5, 1) are different when $\mathcal{A}$ makes queries x_j for all $j \in \text{IDX}$. Since the signature σ_j also guarantees the validity of the basis θ_j , such an event is included in event E . The probability that event E occurs is

$$\begin{aligned} \Pr[E] &= \Pr \left[|S| > \frac{5d}{8} \right] + \sum_{i=\frac{d}{3}}^{\frac{5d}{8}} \Pr[|S| = i] \Pr[E | |S| = i] \\ &\leq \Pr \left[|S| > \frac{5d}{8} \right] + \sum_{i=\frac{d}{3}}^{\frac{5d}{8}} \Pr[|S| = i] 2 \exp \left(-pi \left(\frac{d - 3pi}{3pi} \right)^2 / 3 \right) \\ &= \Pr \left[|S| > \frac{5d}{8} \right] + \sum_{i=\frac{d}{3}}^{\frac{5d}{8}} \Pr[|S| = i] 2 \exp \left(-\frac{(d - 3pi)^2}{27pi} \right) \\ &\leq \Pr \left[|S| > \frac{5d}{8} \right] + \sum_{i=\frac{d}{3}}^{\frac{5d}{8}} \Pr[|S| = i] 2 \exp \left(-d \frac{(8 - 15p)^2}{1080p} \right) \\ &= \Pr \left[|S| > \frac{5d}{8} \right] + \Pr \left[|S| \leq \frac{5d}{8} \right] 2 \exp \left(-d \frac{(8 - 15p)^2}{1080p} \right) \\ &\leq \Pr \left[|S| > \frac{5d}{8} \right] + 2 \exp \left(-d \frac{(8 - 15p)^2}{1080p} \right) \\ &\leq 2 \exp \left(-\frac{d}{2} \left(\frac{1}{4} \right)^2 / 3 \right) + 2 \exp \left(-d \frac{(8 - 15p)^2}{1080p} \right) \\ &= \text{negl}(\lambda). \end{aligned}$$

We used the Chernoff bound (2.2) in the second and seventh inequality. The last equation holds because p is negligibly close to $1/2$ and $d = \omega(\log \lambda)$. Therefore,

$$|\Pr[b = 1 : \text{Hyb}(5, 0)] - \Pr[b = 1 : \text{Hyb}(5, 1)]| \leq \text{negl}(\lambda)$$

holds. □ (Lemma 5.6.)

Applying the triangle inequality to the results of the lemmas 5.1 to 5.6, the following holds. For all QPT adversary $\mathcal{A}$,

$$|\Pr[b = 1 : \text{Hyb}(0, 0)] - \Pr[b = 1 : \text{Hyb}(0, 1)]| \leq \text{negl}(\lambda).$$

Since **Hyb**(0, b^*) coincides with $\text{Game}_{\text{QKEM}, b^*}^{\text{indcpa}}$, this shows that QKEM satisfies the IND-pkT-CPA security.

□ (Theorem 5.3.)

5.6 Discussions

In this section, we give some discussions. We first discuss how to make the assumptions, where the adversary performs individual attack and can only make classical queries to the random oracle more realistic. Next, we present a specific attack on the QKEM given in Section 5.4 by allowing coherently attacking on the quantum channel and quantum access to the random oracle. Finally, we give some open problems.

Against more powerful quantum computation. The QKEM we proposed offers desirable properties such as the strong error detectability and ease of implementation. However, in the IND-pkT-CPA security, it imposes that the adversary attacks each qubit on quantum channel individually and cannot make quantum queries to the random oracle.

One of the challenge for near-term quantum computers is the short coherence time. If the transmission rate of the quantum communication channel slows down, the attacker needs to maintain entanglement for a longer period. On the other hand, our scheme is entirely qubit-wise for honest users.

In practice, the random oracle is replaced by a hash function like SHA256. Therefore, an adversary who cannot make quantum queries to the random oracle can be interpreted as one cannot implement the hash function on their quantum computers. The quantum public key $\mathbf{qpk}$ in this study consists of d blocks of n -qubit states $(\mathbf{qpk}_j)_{j \in [d]}$. The input length of the random oracle is determined by this n . For the protocol to run in polynomial time, n must be a polynomial in the security parameter λ , but it can be set to be relatively large. In this case, the difficulty for an adversary to implement the hash function on his quantum computer increases. On the other hand, the hardware requirement for honest participants remains the same, a classical computer and single-qubit devices. Since the study of quantum computers faces scalability challenges, we believe such a countermeasure is effective.

Coherent attack. We show a specific attack for our construction. The attack treats the entire quantum transmission as one system and coherently queries to the random oracle. A state transition as shown below can be realized by quantum query to the random oracle H and the verification algorithm.

$$\begin{aligned}
 |x\rangle &\mapsto |x\rangle |H(x)\rangle \\
 &\mapsto |x\rangle |H(x) \oplus z_j\rangle \\
 &= |x\rangle |y'_j| |\sigma'_j\rangle \\
 &\mapsto |x\rangle |y'_j| |\sigma'_j\rangle |\text{Verify}(\mathbf{vk}_{\text{Sig}}, r || j || 0 || y'_j, \sigma'_j)\rangle
 \end{aligned}$$

Suppose that the above state transition is performed on the j -th quantum public key $\mathbf{qpk}_j$. If we measure the third register and if it outputs $\top$, then we get x_j by measuring the first register. If it outputs $\perp$, it indicates that the public key is sent in a Hadamard basis. Due to the unforgeability of the signature, the state at this point is negligibly close to the state $\sum_{x'} (-1)^{x_j \cdot x'} |x'\rangle |H(x') \oplus z_j\rangle |\perp\rangle$. It is reasonable to consider that the system is in this state. Then, using the random oracle again to compute

$$\begin{aligned}
 \sum_{x'} (-1)^{x_j \cdot x'} |x'\rangle |H(x') \oplus z_j\rangle |\perp\rangle &\mapsto \sum_{x'} (-1)^{x_j \cdot x'} |x'\rangle |H(x')\rangle |\perp\rangle \\
 &\mapsto \sum_{x'} (-1)^{x_j \cdot x'} |x'\rangle |0\rangle |\perp\rangle \\
 &= |x_j\rangle |0\rangle |\perp\rangle
 \end{aligned}$$

, and measuring the first register in the Hadamard basis and get x_j . This attack requires quantum computation over $n + k + l + 1$ qubits.

Open Problems. From a practical perspective, security against chosen ciphertext (CCA) attacks is widely regarded as an essential requirement for PKE. In contrast, the present work focuses only on security against chosen plaintext attacks (CPA). In classical cryptography, there exist generic transformations, such as the Fujisaki-Okamoto transformation [FO99], that convert CPA secure PKE schemes into CCA secure ones in the random oracle model. However, such transformations rely on classical rewinding techniques and do not directly extend to the setting of QPKE. In particular, achieving CCA security while simultaneously preserving strong error detectability for QPKE from OWFs remains an open problem. We leave the construction of QPKE schemes that satisfy both strong error detectability and CCA security remains an open problem.

Appendix

5.A Security against Round Individual Attack

In Section 5.5, we demonstrate that our QPKE construction is IND-pkT-CPA secure against individual attacks. In this section, we further show that it satisfies a stronger and more generalized notion of security. In our construction, quantum public keys consist of d blocks of n -qubits each. We prove that the construction achieves indistinguishability against a model in which an adversary attacks each n -qubit block individually. We refer to this as a round individual attack.

Entropic Uncertainty Relation Let ρ be an arbitrary n -qubit state, X be an outcome when ρ is measured in the computational basis, and Z be an outcome when ρ is measured in the Hadamard basis. Then the following inequality holds.

$$H(X) + H(Z) \geq n$$

Lemma 5.6’. For all adversaries $\mathcal{A}$ with a polynomial number (with respect to λ) of queries for the random oracle, the following holds.

$$|\Pr[b = 1 : \text{Hyb}(5, 0)] - \Pr[b = 1 : \text{Hyb}(5, 1)]| \leq \text{negl}(\lambda).$$

Proof of Lemma 5.6’ Let ρ_j denote a posteriori state, which was halves of the j -th EPR pairs held by the challenger, after a measurement performed by the adversary on his register. Then, applying the uncertainty principle for ρ_j , the following inequality holds.

$$H(X_{j,0}) + H(X_{j,1}) \geq n,$$

where $X_{j,0}$ be an outcome when ρ_j is measured in the computational basis, and $X_{j,1}$ be an outcome when ρ_j is measured in the Hadamard basis. It indicates that either $H(X_{j,0})$ or $H(X_{j,1})$ is greater than $\frac{n}{2}$.

Consider the probability of correctly guessing x , which is chosen from a distribution X , where $H(X) \geq \frac{n}{2}$ within a polynomial number of queries. Let $x_1, x_2, \dots, x_l$ be the elements of the distribution X arranged in the descending order of their probabilities. In other words, $p_{x_1} \geq p_{x_2} \geq \dots \geq p_{x_l}$, where $p_{x_j} := \Pr[X = x_j]$. Since $H(X) \geq \frac{n}{2}$, we have $|X| > 2^{\frac{n}{2}}$, which implies $2^n \geq l > 2^{\frac{n}{2}}$.

In the following, we proceed by contradiction. Assume that the probability of x being chosen from among the most likely elements (i.e., the probability that x_1 or x_2 , or $x_3, \dots$, or $x_{2^{\frac{n}{4}}}$ are chosen) exceeds $3/4$. We denote this probability by q . For sufficiently large n , by

the definition of the entropy,

$$\begin{aligned}
H(X) &= - \sum_{j=1}^l p_{x_j} \log p_{x_j} \\
&= - \sum_{j=1}^{2^{\frac{n}{4}}} p_{x_j} \log p_{x_j} - \sum_{j=2^{\frac{n}{4}}+1}^l p_{x_j} \log p_{x_j} \\
&\leq -2^{\frac{n}{4}} \frac{q}{2^{\frac{n}{4}}} \log \frac{q}{2^{\frac{n}{4}}} - (2^l - 2^{\frac{n}{4}}) \frac{1-q}{2^l - 2^{\frac{n}{4}}} \log \frac{1-q}{2^l - 2^{\frac{n}{4}}} \\
&= -q(\log q - \log 2^{\frac{n}{4}}) - (1-q)(\log(1-q) - \log(2^l - 2^{\frac{n}{4}})) \\
&= -q \log q - (1-q) \log(1-q) + q \log 2^{\frac{n}{4}} + (1-q) \log(2^l - 2^{\frac{n}{4}}) \\
&\leq 1 + \frac{qn}{4} + (1-q) \log 2^n \\
&= 1 + (1 - \frac{3q}{4})n \\
&< 1 + \frac{7n}{16} \\
&< \frac{n}{2}.
\end{aligned}$$

This contradicts $H(X) \geq \frac{n}{2}$. Therefore, the assumption is rejected. In conclusion, when an element is chosen from a distribution X such that $H(X) > \frac{n}{2}$, the probability that the chosen element belongs to the top $2^{\frac{n}{4}}$ most probable elements is less than $3/4 + \text{negl}(\lambda)$.

From the above discussion, if the adversary only makes polynomial number of classical queries to the random oracle, for all $j \in [d]$,

$$\begin{aligned}
\Pr[\mathcal{A} \text{ queries } x_j \text{ to the oracle}] &\leq \frac{1}{2} + \frac{1}{2} \left(\frac{3}{4} + \text{negl}(\lambda) \right) \\
&= \frac{7}{8} + \text{negl}(\lambda)
\end{aligned}$$

holds, and each event is independent of the others. We denote this probability by p .

Let θ' be the bases of the measurement chosen in **Encaps** in step 4. **IDX** be the part of the output of **Encaps**, $c = \theta \oplus \theta'$, c_j be the j -th character of c , $S = \{j | c_j = 0\}$, and E be an event that $\mathcal{A}$ makes at least $\frac{15d}{32}$ independent queries x_j for $j \in S$.

Hyb(5,0) and **Hyb**(5,1) are different when $\mathcal{A}$ queries x_j for all $j \in \text{IDX}$. Since the signature σ_j also guarantees the validity of the basis θ_j , such an event is included in the

event E . The probability that the event E occurs is

$$\begin{aligned}
\Pr[E] &= \Pr\left[|S| > \frac{17d}{32}\right] + \sum_{i=\frac{15d}{32}}^{\frac{17d}{32}} \Pr[|S| = i] \Pr[E \mid |S| = i] \\
&\leq \Pr\left[|S| > \frac{17d}{32}\right] + \sum_{i=\frac{15d}{32}}^{\frac{17d}{32}} \Pr[|S| = i] 2e^{-pi(\frac{15d-32pi}{32pi})^2/3} \\
&= \Pr\left[|S| > \frac{17d}{32}\right] + \sum_{i=\frac{15d}{32}}^{\frac{17d}{32}} \Pr[|S| = i] 2e^{-\frac{(15d-32pi)^2}{3072pi}} \\
&\leq \Pr\left[|S| > \frac{17d}{32}\right] + \sum_{i=\frac{15d}{32}}^{\frac{17d}{32}} \Pr[|S| = i] 2e^{-d\frac{(15-17p)^2}{1632p}} \\
&= \Pr\left[|S| > \frac{17d}{32}\right] + \Pr\left[|S| \leq \frac{17d}{32}\right] 2e^{-d\frac{(15-17p)^2}{1632p}} \\
&\leq \Pr\left[|S| > \frac{17d}{32}\right] + 1 \cdot 2e^{-d\frac{(15-17p)^2}{1632p}} \\
&\leq 2e^{-\frac{d}{2}(\frac{1}{32})^2/3} + 2e^{-d\frac{(15-17p)^2}{1632p}} \\
&= \text{negl}(\lambda).
\end{aligned}$$

We used the Chernoff bound (2.2) in the second and seventh inequality. The last equation holds because p is less than $7/8 + \text{negl}(\lambda)$ and $d = \omega(\log \lambda)$. Therefore,

$$|\Pr[b = 1 : \text{Hyb}(5, 0)] - \Pr[b = 1 : \text{Hyb}(5, 1)]| \leq \text{negl}(\lambda)$$

holds. □ (Lemma 5.6'.)

Applying the triangle inequality to the results of the lemmas 5.1 to 5.5 and 5.6', the following holds. For all QPT adversary $\mathcal{A}$ who performs round-individual attack,

$$|\Pr[b = 1 : \text{Hyb}(0, 0)] - \Pr[b = 1 : \text{Hyb}(0, 1)]| \leq \text{negl}(\lambda).$$

Since $\text{Hyb}(0, b^*)$ coincides with $\text{Game}_{\text{QKEM}, b^*}^{\text{indcpa}}$, this shows that QKEM satisfies the IND-pkT-CPA security against round-individual attacks.

Chapter 6

Conclusion

In this thesis, by assuming access to quantum computation and quantum communication, we derive several cryptographic primitives from one-way functions (OWFs). These derivations are not known classically and appear to be inherently difficult to obtain in the classical setting.

In Chapter 3, we present a quantum Goldreich–Levin theorem over $\mathbb{Z}_q$. This result generalizes the prior quantum Goldreich–Levin theorem over $\mathbb{Z}_2$. Additionally, unlike the classical reduction, its efficiency does not depend on q . Consequently, even when q is super-polynomial in n , the reduction remains efficient. This implies that the unpredictability of the inner product guaranteed by the Goldreich–Levin theorem continues to hold against quantum (and even classical) adversaries for super-polynomially large q .

In Chapter 4, we give a quantum search-to-decision reduction for the Learning with Errors (LWE) problem. Our reduction proceeds by reducing the inner-product prediction problem to decisional LWE, and then invoking the quantum GL theorem over $\mathbb{Z}_q$ (from Chapter 3) as a reduction from the search LWE problem to the inner-product prediction problem. A key feature of our reduction is that it is sample-preserving: it introduces no loss in the number of LWE samples when reducing search LWE to decisional LWE. Compared with the classical sample-preserving reduction, our quantum reduction achieves a higher success probability and fewer queries. We further analyze the version with amplified success probability and show that it still reduces the required number of samples. These results collectively demonstrate that security loss in reductions can be significantly reduced, providing theoretical guidelines for setting parameters that ensure the hardness of decisional LWE and, consequently, secure post-quantum cryptography.

In Chapter 5, we construct a QPKE scheme from OWFs. A notable feature of our scheme is that it uses only tensor products of single-qubit states, making it implementable on current quantum hardware. Moreover, unlike previous work, we do not assume secure quantum channels. Instead, we work in a setting where quantum communication may be subject to tampering or eavesdropping, and we construct a scheme that is secure under this model. Our construction relies on a random oracle and the assumption of individual attacks. Avoiding secure quantum channels is a crucial property, and we argue that it is essential for QPKE to be regarded as a genuine quantum analogue of classical public-key encryption. Thus, our construction takes a step toward making QPKE not only theoretically meaningful but also practically applicable.

Overall, this thesis demonstrates that the range of cryptographic primitives derivable from OWFs can be significantly broadened when quantum computation and communication are incorporated. The results obtained in this thesis go beyond a mere extension of the MiniQCrypt. In particular, the quantum Goldreich–Levin theorem over $\mathbb{Z}_q$ not only provides a new perspective on the analysis of hardcore properties, but has also been shown to have

applications to security proofs in Unclonable Cryptography [APV23; AB24]. Furthermore, in Chapter 4, we present a theoretical analysis in the form of a quantum search-to-decision reduction for the LWE problem, which serves as a foundational assumption for post-quantum cryptographic primitives. Although the generalization of the quantum Goldreich–Levin theorem is a fundamentally theoretical result, it has close connections to ongoing research on the security of post-quantum cryptography.

In prior work, the construction of QPKE from OWFs has largely focused on theoretical interest. Indeed, many *quantum* cryptographic protocols, including QPKE, assume the existence of secure quantum communication channels. However, when quantum cryptography is viewed as an analogue of classical cryptography, this assumption is not necessarily justified. In classical cryptography, it is reasonable to assume secure classical communication channels because there exist well-established techniques, such as digital signatures and error-correction, that guarantee the authenticity of classical information. In contrast, it is known that signatures for quantum states are fundamentally impossible [Bar+02; AGM21], which constitutes an essential limitation specific to quantum cryptography.

The security definitions and constructions presented in Chapter 5 are motivated by this observation and aim to go beyond purely theoretical interest by explicitly addressing practical applicability. In particular, a key feature of our construction is that it incorporates mechanisms for verifying the validity of quantum states used within the protocol, thereby enabling a QPKE scheme that does not rely on the assumption of secure quantum communication channels. Cryptographic theory must progress through a balance between theoretical interest and practical applicability. For the continued development of quantum cryptographic protocols, it will become increasingly important to explicitly incorporate mechanisms for verifying the validity of quantum states.

As a direction for future work, an important challenge is to go beyond verification of validity and address robustness against noise arising in quantum communication channels. Validity verification alone only allows one to discard quantum states containing errors by deeming them invalid, which is insufficient in realistic quantum communication settings. To achieve truly practical quantum cryptographic protocols, it will be necessary to design constructions that can tolerate and correct a certain level of errors. Developing such error-tolerant designs remains an important open problem for future research.

Acknowledgments

First and foremost, I would like to thank my supervisor, Prof. Keisuke Fujii. Without his insightful guidance and constant encouragement, it would not have been possible for me to complete this thesis.

I would also like to thank all members of the Fujii Laboratory. In particular, I am deeply grateful to the students with whom I conducted research in the staff room D355–357. Through our daily discussions and interactions, I was able to enjoy a fulfilling and rewarding research life. The time I spent with all of you is an irreplaceable treasure to me.

I would further like to express my sincere appreciation to Prof. Keisuke Tanaka, who introduced me to the world of research. It was a great fortune for me to encounter cryptographic theory through his guidance during my master's program. I am also deeply grateful to Keisuke Hara, Kosuke Ito, Masayuki Tezuka, and Yusuke Yoshida for their valuable insights and contributions, which made my research richer and more substantial.

Finally, I would like to express my deepest gratitude to my parents and family and to Hikari Nakatani for their support and love.

List of Publications

Publications included in thesis

1. Kyohei Sudo, Masayuki Tezuka, Keisuke Hara, and Yusuke Yoshida, “Quantum Search-to-Decision Reduction for the LWE Problem.”, AFRICACRYPT2023, Proceedings, 2023.
2. Kyohei Sudo, Masayuki Tezuka, Keisuke Hara, and Yusuke Yoshida, “Quantum Search-to-Decision Reduction for the LWE Problem.”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Volume 108, 2024.
3. Kyohei Sudo, Keisuke Fujii, Kosuke Ito, Masayuki Tezuka, Keisuke Hara, and Yusuke Yoshida, “Practical Quantum Public Key Encryption from One-way Functions.”, Proceedings of the 12th acm asia public-key cryptography workshop, APKC’25, 2025.

Publications not included in thesis

4. Kyohei Sudo, Masayuki Tezuka, Keisuke Hara, and Yusuke Yoshida, “Watermarkable Signature with Computational Function Preserving.”, Provable and Practical Security - 14th International Conference, ProvSec2020, Singapore, Proceedings, 2020.
5. Kyohei Sudo, Masayuki Tezuka, Keisuke Hara, and Yusuke Yoshida, “Watermarkable Signature with Computational Function Preserving.”, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Volume 104-A, 2021.
6. Yusei Mori, Hideaki Hakoshima, Kyohei Sudo, Toshio Mori, Kosuke Mitarai, Keisuke Fujii, “Quantum Circuit Unoptimization.”, Phys. Rev. Res. 7 (2 May 2025), p. 023139.

Bibliography

- [LWE challenge] *LWE challenge website*. https://www.latticechallenge.org/lwe_challenge/challenge.php.
- [Aar09] Scott Aaronson. “Quantum Copy-Protection and Quantum Money”. In: *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*. IEEE Computer Society, 2009, pp. 229–242.
- [AB24] Prabhanjan Ananth and Amit Behera. “A Modular Approach to Unclonable Cryptography”. In: *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part VII*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14926. Lecture Notes in Computer Science. Springer, 2024, pp. 3–37.
- [ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. “Efficient Lattice (H)IBE in the Standard Model”. In: *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*. Ed. by Henri Gilbert. Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 553–572.
- [AC02] Mark Adcock and Richard Cleve. “A Quantum Goldreich-Levin Theorem with Cryptographic Applications”. In: *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes - Juan les Pins, France, March 14-16, 2002, Proceedings*. Ed. by Helmut Alt and Afonso Ferreira. Vol. 2285. Lecture Notes in Computer Science. Springer, 2002, pp. 323–334.
- [AGM21] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. “Can you sign a quantum state?” In: *Quantum* 5 (2021), p. 603.
- [AIK07] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. “Cryptography with Constant Input Locality”. In: *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*. Ed. by Alfred Menezes. Vol. 4622. Lecture Notes in Computer Science. Springer, 2007, pp. 92–110.
- [Aka08] Adi Akavia. “Learning noisy characters, MPC, and cryptographic hardcore predicates”. PhD thesis. Massachusetts Institute of Technology, Cambridge, MA, USA, 2008.

- [App+09] Benny Applebaum et al. “Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems”. In: *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*. Ed. by Shai Halevi. Vol. 5677. Lecture Notes in Computer Science. Springer, 2009, pp. 595–618.
- [APV23] Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. *Revocable Cryptography from Learning with Errors*. Cryptology ePrint Archive, Paper 2023/325. <https://eprint.iacr.org/2023/325>. 2023.
- [AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. “Cryptography from Pseudorandom Quantum States”. In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13507. Lecture Notes in Computer Science. Springer, 2022, pp. 208–236.
- [Asp+05] Alán Aspuru-Guzik et al. “Simulated Quantum Computation of Molecular Energies”. In: *Science (New York, N.Y.)* 309 (Oct. 2005), pp. 1704–7.
- [Bar+02] Howard Barnum et al. “Authentication of Quantum Messages”. In: *43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings*. IEEE Computer Society, 2002, pp. 449–458.
- [Bar+21] James Bartusek et al. “One-Way Functions Imply Secure Computation in a Quantum World”. In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*. Ed. by Tal Malkin and Chris Peikert. Vol. 12825. Lecture Notes in Computer Science. Springer, 2021, pp. 467–496.
- [Bar+23] Khashayar Barooti et al. “Public-Key Encryption with Quantum Keys”. In: *CoRR* abs/2306.07698 (2023). arXiv: [2306.07698](https://arxiv.org/abs/2306.07698).
- [BB84] Charles H. Bennett and Gilles Brassard. “Quantum cryptography : Public key distribution and coin tossing”. In: *International Conference on Computer System and Signal Processing, IEEE, 1984* (1984), pp. 175–179.
- [BBK22] Nir Bitansky, Zvika Brakerski, and Yael Tauman Kalai. *Constructive Post-Quantum Reductions*. 2022.
- [BBM92] Charles H. Bennett, Gilles Brassard, and N. David Mermin. “Quantum cryptography without Bell’s theorem”. In: *Phys. Rev. Lett.* 68 (5 Feb. 1992), pp. 557–559.
- [BI20] Anne Broadbent and Rabib Islam. “Quantum Encryption with Certified Deletion”. In: *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part III*. Ed. by Rafael Pass and Krzysztof Pietrzak. Vol. 12552. Lecture Notes in Computer Science. Springer, 2020, pp. 92–122.
- [Bia+17] Jacob Biamonte et al. “Quantum machine learning”. In: *Nature* 549.7671 (2017), pp. 195–202.

- [BM82] Manuel Blum and Silvio Micali. “How to Generate Cryptographically Strong Sequences of Pseudo Random Bits”. In: *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982*. IEEE Computer Society, 1982, pp. 112–117.
- [BN08] Mihir Bellare and Chanathip Namprempre. “Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm”. In: *J. Cryptol.* 21.4 (2008), pp. 469–491.
- [Bos+18] Joppe W. Bos et al. “CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM”. In: *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018*. IEEE, 2018, pp. 353–367.
- [BR93] Mihir Bellare and Phillip Rogaway. “Random Oracles are Practical: A Paradigm for Designing Efficient Protocols”. In: *CCS ’93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993*. Ed. by Dorothy E. Denning et al. ACM, 1993, pp. 62–73.
- [Bra+02] Gilles Brassard et al. *Quantum amplitude amplification and estimation*. 2002.
- [Bra+13] Zvika Brakerski et al. “Classical hardness of learning with errors”. In: *Symposium on Theory of Computing Conference, STOC’13, Palo Alto, CA, USA, June 1-4, 2013*. Ed. by Dan Boneh, Tim Roughgarden, and Joan Feigenbaum. ACM, 2013, pp. 575–584.
- [BS23a] Mohammed Barhoush and Louis Salvail. “How to Sign Quantum Messages”. In: *CoRR* abs/2304.06325 (2023). arXiv: [2304.06325](#).
- [BS23b] Mohammed Barhoush and Louis Salvail. “Powerful Primitives in the Bounded Quantum Storage Model”. In: *CoRR* abs/2302.05724 (2023). arXiv: [2302.05724](#).
- [BV11] Zvika Brakerski and Vinod Vaikuntanathan. “Efficient Fully Homomorphic Encryption from (Standard) LWE”. In: *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*. Ed. by Rafail Ostrovsky. IEEE Computer Society, 2011, pp. 97–106.
- [BV93] Ethan Bernstein and Umesh Vazirani. “Quantum complexity theory”. In: *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing*. STOC ’93. San Diego, California, USA: Association for Computing Machinery, 1993, pp. 11–20. ISBN: 0897915917.
- [Cas+10] David Cash et al. “Bonsai Trees, or How to Delegate a Lattice Basis”. In: *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*. Ed. by Henri Gilbert. Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 523–552.
- [CGG24] Kai-Min Chung, Eli Goldin, and Matthew Gray. “On Central Primitives for Quantum Cryptography with Classical Communication”. In: *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part VII*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14926. Lecture Notes in Computer Science. Springer, 2024, pp. 215–248.

- [Cha+23] Orestis Chardouvelis et al. “Quantum Key Leasing for PKE and FHE with a Classical Lessor”. In: *CoRR* abs/2310.14328 (2023). arXiv: [2310.14328](#).
- [Col+17] Patrick J. Coles et al. “Entropic uncertainty relations and their applications”. In: *Rev. Mod. Phys.* 89 (1 Feb. 2017), p. 015002.
- [Col23] Andrea Coladangelo. “Quantum trapdoor functions from classical one-way functions”. In: *CoRR* abs/2302.12821 (2023). arXiv: [2302.12821](#).
- [Deu83] David Deutsch. “Uncertainty in Quantum Measurements”. In: *Phys. Rev. Lett.* 50 (9 Feb. 1983), pp. 631–633.
- [Dod+10] Yevgeniy Dodis et al. “Public-Key Encryption Schemes with Auxiliary Inputs”. In: *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*. Ed. by Daniele Micciancio. Vol. 5978. Lecture Notes in Computer Science. Springer, 2010, pp. 361–381.
- [Dod+12] Yevgeniy Dodis et al. “Message Authentication, Revisited”. In: *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 355–374.
- [Döt15] Nico Döttling. “Low Noise LPN: KDM Secure Public Key Encryption and Sample Amplification”. In: *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*. Ed. by Jonathan Katz. Vol. 9020. Lecture Notes in Computer Science. Springer, 2015, pp. 604–626.
- [Eke91] Artur K. Ekert. “Quantum cryptography based on Bell’s theorem”. In: *Phys. Rev. Lett.* 67 (6 Aug. 1991), pp. 661–663.
- [EPR35] A. Einstein, B. Podolsky, and N. Rosen. “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” In: *Phys. Rev.* 47 (10 May 1935), pp. 777–780.
- [Fey81] R.P. Feynman. “Simulating Physics with Computers”. In: *International Journal of Theoretical Physics* 21.6 (1981), pp. 467–488.
- [FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. “Secure Integration of Asymmetric and Symmetric Encryption Schemes”. In: *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology. CRYPTO ’99*. Berlin, Heidelberg: Springer-Verlag, 1999, pp. 537–554. ISBN: 3540663479.
- [GGM84] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. “How to Construct Random Functions (Extended Abstract)”. In: *25th Annual Symposium on Foundations of Computer Science, West Palm Beach, Florida, USA, 24-26 October 1984*. IEEE Computer Society, 1984, pp. 464–479.
- [GL89] Oded Goldreich and Leonid A. Levin. “A Hard-Core Predicate for all One-Way Functions”. In: *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA*. Ed. by David S. Johnson. ACM, 1989, pp. 25–32.
- [Gol01] Oded Goldreich. *Foundations of Cryptography: Volume 1*. Cambridge University Press, 2001.

- [Gol04] Oded Goldreich. *The Foundations of Cryptography - Volume 2: Basic Applications*. Cambridge University Press, 2004. ISBN: 0-521-83084-2.
- [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, Victoria, British Columbia, Canada, May 17-20, 2008*. Ed. by Cynthia Dwork. ACM, 2008, pp. 197–206.
- [Gri+21] Alex B. Grilo et al. “Oblivious Transfer Is in MiniQCrypt”. In: *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12697. Lecture Notes in Computer Science. Springer, 2021, pp. 531–561.
- [GRS95] Oded Goldreich, Ronitt Rubinfeld, and Madhu Sudan. “Learning Polynomials with Queries: The Highly Noisy Case”. In: *36th Annual Symposium on Foundations of Computer Science, FOCS 1995, Milwaukee, Wisconsin, USA, 23-25 October 1995*. IEEE Computer Society, 1995, pp. 294–303.
- [Hås+99] Johan Håstad et al. “A Pseudorandom Generator from any One-way Function”. In: *SIAM J. Comput.* 28.4 (1999), pp. 1364–1396.
- [IL89] R. Impagliazzo and M. Luby. “One-way functions are essential for complexity based cryptography”. In: *30th Annual Symposium on Foundations of Computer Science*. 1989, pp. 230–235.
- [Imp95] R. Impagliazzo. “A personal view of average-case complexity”. In: *Proceedings of the 10th Annual Structure in Complexity Theory Conference (SCT’95)*. SCT ’95. USA: IEEE Computer Society, 1995, p. 134. ISBN: 0818670525.
- [IR89] Russell Impagliazzo and Steven Rudich. “Limits on the Provable Consequences of One-Way Permutations”. In: *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA*. Ed. by David S. Johnson. ACM, 1989, pp. 44–61.
- [JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. “Pseudorandom Quantum States”. In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. Lecture Notes in Computer Science. Springer, 2018, pp. 126–152.
- [Kaw+12] Akinori Kawachi et al. “Computational Indistinguishability Between Quantum States and Its Cryptographic Application”. In: *J. Cryptol.* 25.3 (2012), pp. 528–555.
- [Kit+24] Fuyuki Kitagawa et al. “Quantum Public-Key Encryption with Tamper-Resilient Public Keys from One-Way Functions”. In: *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part VII*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14926. Lecture Notes in Computer Science. Springer, 2024, pp. 93–125.
- [Kit95] A. Yu. Kitaev. *Quantum measurements and the Abelian Stabilizer Problem*. 1995. arXiv: [quant-ph/9511026](https://arxiv.org/abs/quant-ph/9511026) [quant-ph].

- [KM91] Eyal Kushilevitz and Yishay Mansour. “Learning decision trees using the Fourier spectrum”. In: *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing*. STOC ’91. New Orleans, Louisiana, USA: Association for Computing Machinery, 1991, pp. 455–464. ISBN: 0897913973.
- [Kre21] William Kretschmer. “Quantum Pseudorandomness and Classical Complexity”. In: *CoRR* abs/2103.09320 (2021). arXiv: [2103.09320](https://arxiv.org/abs/2103.09320).
- [KS06] Jonathan Katz and Ji Sun Shin. “Parallel and Concurrent Security of the HB and HB⁺ Protocols”. In: *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*. Ed. by Serge Vaudenay. Vol. 4004. Lecture Notes in Computer Science. Springer, 2006, pp. 73–87.
- [KT00] Jonathan Katz and Luca Trevisan. “On the efficiency of local decoding procedures for error-correcting codes”. In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*. STOC ’00. Portland, Oregon, USA: Association for Computing Machinery, 2000, pp. 80–86. ISBN: 1581131844.
- [KT24] Dakshita Khurana and Kabir Tomer. “Commitments from Quantum One-Wayness”. In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*. Ed. by Bojan Mohar, Igor Shinkar, and Ryan O’Donnell. ACM, 2024, pp. 968–978.
- [Lia+17] Sheng-Kai Liao et al. “Satellite-to-ground quantum key distribution”. In: *Nature* 549.7670 (2017), pp. 43–47.
- [Llo96] Seth Lloyd. “Universal Quantum Simulators”. In: *Science* 273.5278 (1996), pp. 1073–1078. eprint: <https://www.science.org/doi/pdf/10.1126/science.273.5278.1073>.
- [MM11] Daniele Micciancio and Petros Mol. “Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions”. In: *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*. Ed. by Phillip Rogaway. Vol. 6841. Lecture Notes in Computer Science. Springer, 2011, pp. 465–484.
- [MP12] Daniele Micciancio and Chris Peikert. “Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller”. In: *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 700–718.
- [MW24] Giulio Malavolta and Michael Walter. “Robust Quantum Public-Key Encryption with Applications to Quantum Key Distribution”. In: *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part VII*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14926. Lecture Notes in Computer Science. Springer, 2024, pp. 126–151.

- [MY22] Tomoyuki Morimae and Takashi Yamakawa. “Quantum Commitments and Signatures Without One-Way Functions”. In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13507. Lecture Notes in Computer Science. Springer, 2022, pp. 269–295.
- [MY24] Tomoyuki Morimae and Takashi Yamakawa. “One-Wayness in Quantum Cryptography”. In: *19th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2024, September 9-13, 2024, Okinawa, Japan*. Ed. by Frédéric Magniez and Alex Bredariol Grilo. Vol. 310. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024, 4:1–4:21.
- [NRW23] Parker Newton, Silas Richelson, and Chase Wilson. “A High Dimensional Goldreich-Levin Theorem”. In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*. Ed. by Barna Saha and Rocco A. Servedio. ACM, 2023, pp. 1463–1474.
- [Pei09] Chris Peikert. “Public-key cryptosystems from the worst-case shortest vector problem: extended abstract”. In: *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*. Ed. by Michael Mitzenmacher. ACM, 2009, pp. 333–342.
- [PVW08] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. “A Framework for Efficient and Composable Oblivious Transfer”. In: *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*. Ed. by David A. Wagner. Vol. 5157. Lecture Notes in Computer Science. Springer, 2008, pp. 554–571.
- [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, Baltimore, MD, USA, May 22-24, 2005*. Ed. by Harold N. Gabow and Ronald Fagin. ACM, 2005, pp. 84–93.
- [Rom90] John Rompel. “One-Way Functions are Necessary and Sufficient for Secure Signatures”. In: *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*. Ed. by Harriet Ortiz. ACM, 1990, pp. 387–394.
- [RSA78] R. L. Rivest, A. Shamir, and L. Adleman. “A method for obtaining digital signatures and public-key cryptosystems”. In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782.
- [Sho99] Peter W. Shor. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. In: *SIAM Rev.* 41.2 (1999), pp. 303–332.
- [Sud97] Madhu Sudan. “Decoding of Reed Solomon Codes beyond the Error-Correction Bound”. In: *Journal of Complexity* 13.1 (1997), pp. 180–193. ISSN: 0885-064X.
- [TW11] Madhur Tulsiani and Julia Wolf. “Quadratic Goldreich-Levin Theorems”. In: *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*. Ed. by Rafail Ostrovsky. IEEE Computer Society, 2011, pp. 619–628.

- [Vai] Vinod Vaikuntanathan. *Lattices, Learning with Errors and Post-Quantum Cryptography*. <https://people.csail.mit.edu/vinodv/CS294/lecturenotes.pdf>.
- [Wie83] Stephen Wiesner. “Conjugate coding”. In: *SIGACT News* 15.1 (1983), pp. 78–88.
- [WZ82] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. In: *Nature* 299.5886 (Oct. 1982), pp. 802–803.
- [Zha12] Mark Zhandry. “How to Construct Quantum Random Functions”. In: *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*. IEEE Computer Society, 2012, pp. 679–687.