DISSERTATIONES
INFORMATICAE
UNIVERSITATIS
TARTUENSIS
3

EHSAN EBRAHIMI

Post-Quantum Security in the Presence of Superposition Queries

DISSERTATIONES INFORMATICAE UNIVERSITATIS TARTUENSIS

3

DISSERTATIONES INFORMATICAE UNIVERSITATIS TARTUENSIS

3

EHSAN EBRAHIMI

Post-Quantum Security in the Presence of Superposition Queries

1632

UNIVERSITY OF TARTU
Press

Institute of Computer Science, Faculty of Science and Technology, University of Tartu, Estonia.

Dissertation has been accepted for the commencement of the degree of Doctor of Philosophy (PhD) in informatics on 13th of November, 2018 by the Council of the Institute of Computer Science, University of Tartu.

Supervisor

Prof. Dominique Unruh
University of Tartu
Tartu, Estonia

Opponents

PhD. Frédéric Dupuis
CNRS, LORIA, Université de Lorraine
Nancy, France

PhD. Marc Kaplan
VeriQloud
Montrouge, France

The public defense will take place on January 21, 2019 at 16:15 in Liivi 2-405.

The publication of this dissertation was financed by the Institute of Computer Science, University of Tartu.

ISSN 2613-5906
ISBN 978-9949-77-934-5 (print)
ISBN 978-9949-77-935-2 (PDF)

University of Tartu Press
http://www.tyk.ee/

To my family and friends

ABSTRACT

As we are going toward the quantum era, the need to revisit the security of cryptographic constructions against a quantum adversary is getting more appreciable. Post-quantum cryptography is an emerging discipline that deals with classical cryptographic constructions that remain secure against a quantum adversary. In this setting, the honest parties are willing to communicate using only classical devices while the adversary may have a quantum computing device. Due to the breaking of many public-key cryptosystems based on the factoring and discrete logarithm problems by Shor's quantum algorithm, to achieve the post-quantum security, it is necessary to substitute those hard problems with some quantum-hard problems. Then we need to design the cryptographic construction based on quantum hard problems. Finally, we have to prove mathematically the security of the new constructions. The classical security proof techniques may fail against a quantum adversary due to some strange properties of a quantum adversary, therefore, even if we design a cryptographic construction based on a quantum-hard problem, proving the security of the construction remains a challenging task. In this thesis, we focus on proving the quantum security of some cryptographic constructions. We also present some quantum attacks to argue the insecurity of some constructions.

We prove the post-quantum security of a slightly modified version of the Fujisaki-Okamoto (FO) construction that transforms two weakly secure encryption schemes into a strongly secure one using three hash functions in the quantum random oracle model. In the quantum random oracle model the quantum adversary has superposition (quantum) access to the random oracles. In order to prove the security of the FO construction, we need to study the properties of hash functions in the quantum setting. The Indifferentiability Framework has been used to prove the soundness of some hash function constructions when underlying primitive used in the construction is modeled as an ideal primitive. In the quantum setting, a quantum adversary can evaluate an ideal primitive in superposition, therefore we need to redefine the Indifferentiability Framework for a quantum adversary. We define the quantum indifferentiability and show that most of classical constructions of hash functions are not perfectly-quantum indifferentiable from a random oracle under some conjecture. Our quantum definition of indifferentiability allows superposition access to the underlying primitive used in the construction, however, since we claim the impossibility of quantum indifferentiability, we consider a classical access to the construction and this leads to a stronger impossibility result. In other words, our impossibility result will hold if we consider a quantum indifferentiability definition in which the adversary has superposition access to both the construction and the underlying primitive because this definition is stronger than ours. Also, we study the collision-resistance property of a function whose outputs are chosen according to some non-uniform distribution against a quantum adversary that has quantum access to the function. We obtain some upper and lower bounds

that depend on the min-entropy and collision-entropy of the outputs distribution of the function. We use the quantum collision-resistance property of a function whose outputs are chosen according to a distribution with high min-entropy to prove the security of the FO construction in the quantum random oracle model. We use the same techniques to prove the post-quantum security of the OAEP transformation in the quantum random oracle model. Finally, we study the security of modes of operations in the quantum chosen plaintext attack model (qCPA) in which the quantum adversary may have quantum access to the encryption oracle, but, it is only allowed to submit classical challenge queries. We prove that OFB and CTR are secure against qCPA using a block cipher that is secure against a quantum adversary with classical access to the block cipher (this block cipher is called standard secure block cipher). We show CBC, CFB and XTS modes can be insecure when using standard secure block ciphers by constructing separating examples. Finally, we prove the IND-qCPA security of CBC and CFB using a block cipher that is secure against a quantum adversary with quantum access.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

		Page
FO construction:	Fujisaki-Okamoto construction	6
OAEP:	Optimal Asymmetric Encryption Padding	6
IND-CCA:	Indistinguishability under Chosen Ciphertext Attack	16
IND-CPA:	Indistinguishability under Chosen Plaintext Attack	17
ECB:	Electronic Codebook	28
CBC:	Cipher Block Chaining	28
CFB:	Cipher Feedback	28
OFB:	Output Feedback	28
CTR:	Counter	29
XTS:	XEX-based tweaked-codebook mode with ciphertext stealing	29
ENISA:	European Union Agency for Network and Information Security	63
NIST:	National Institute of Standard and Technology	70

LIST OF ORIGINAL PUBLICATIONS

Publications included in the thesis

1. Tore Vincent Carstens , Ehsan Ebrahimi, Gelo Noel Tabia, and Dominique Unruh: On Quantum Indifferentiability, IACR Cryptology ePrint Archive 2018: 257 (2018).

2. Ehsan Ebrahimi and Dominique Unruh: Quantum Collision-Resistance of Non-uniformly Distributed Functions: Upper and Lower Bounds, IACR Cryptology ePrint Archive 2017: 575 (2017). Submitted to Quantum Information & Computation Journal.

3. Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh: Quantum Collision-Resistance of Non-uniformly Distributed Functions. In Tsuyoshi Takagi, editor, PostQuantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings, volume 9606 of Lecture Notes in Computer Science, pages 79–85. Springer, 2016.

4. Ehsan Ebrahimi Targhi and Dominique Unruh: Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms. In Martin Hirt and Adam D. Smith, editors, Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II, volume 9986 of Lecture Notes in Computer Science, pages 192–216, 2016.

5. Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh: Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation. In Tsuyoshi Takagi, editor, Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings, volume 9606 of Lecture Notes in Computer Science, pages 44–63. Springer, 2016.

1. INTRODUCTION

Quantum computing is a new paradigm to do computation that employs some strange properties of quantum mechanics. Due to those strange properties, a large-scale quantum computer can solve some specific problems much faster than a classical computer. This is due to the existence of some efficient quantum algorithms that can solve some problems that there is not an efficient classical algorithm to solve them. For instance, we can name the factoring problem and discrete logarithm problem as two important intractable problems for a classical computer that can be solved by a quantum computer [59]. Since the factoring problem and discrete logarithm problem have been used to construct many cryptographic protocols, the interest in verifying the security of cryptosystems in the presence of a quantum adversary increased after the celebrated paper of Shor [59]. To address the threat posed by a large-quantum computer, there are two trends among scientists: Post-Quantum cryptography and Quantum Cryptography. Even though these two trends look similar but there is a subtle difference between them. Namely, in the post-quantum cryptography setting, users are willing to communicate securely using their classical devices in the presence of an adversary that possesses a quantum computing device. In contrast, in the quantum cryptography users also use quantum devices to communicate securely and of course in the presence of an adversary with the quantum computing power. The quantum security can also be achieved by combining two secure schemes in the aforementioned realms. For instance, two parties can use Quantum Key Distribution scheme to share a secret key using quantum devices and then use the secret key to communicate using their classical schemes and devices. In this thesis, we focus on post-quantum cryptography.

To achieve post-quantum security, the research community should build confidence on some intractable problems for a quantum computer. Exploring such quantum-hard problems and designing a cryptographic protocol based on them is the halfway of constructing a secure cryptographic protocol that can be used in practice. In addition, we need to prove, mathematically, the security of the cryptographic construction and this might be a challenging task since the adversary may possess a quantum computing device.

Many security proofs in the classical cryptography have to be revisited for the reason that the classical security techniques may not work against a quantum adversary. For instance, "rewinding" technique that has been used in classical interactive proof systems is quiet problematic to use in the quantum case [10]. Also, we need to modify the classical security notions to encounter the quantum attacks. For instance, we need to consider adversarial superposition queries in the security notions in the quantum case. A quantum adversary with superposition access to an oracle can evaluate the oracle on exponentially many inputs in each query. In contrast, a classical adversary only learn the output of the oracle on one input in each query. This can have some consequences. Namely, a quantum adversary may obtain more information about the oracle compared to a classical adversary. Another challenge caused by superposition queries is the incapability of some classical security techniques to prove the quantum security. Now some questions may arise: What would be the impact of superposition queries on the security of classical constructions? What are the challenges that may arise when one wants to prove the security of classical constructions considering adversarial superposition queries? What would be solutions to the challenges? How can one justify a new security notion that is defined to encounter superposition attacks?

To name a few examples of the security proofs in the presence of adversarial superposition queries, we can mention the security proofs in the random oracle model [14] where a quantum adversary has superposition access to the random oracle, the security of the cryptosystems against the chosen-plaintext attack in which the adversary is allowed to submit superposition queries to the encryption algorithm [18], the collision-resistance property of hash functions when the adversary has superposition access to the hash function and the security of the constructions based on Indifferentiability Framework [54] when the adversary has superposition access to the public interface of the construction (these new quantum definitions will be discussed in details in next chapters).

1.1. Our Contribution

In this thesis, we study the impact of superposition queries to the security of classical constructions. These include the security of hash functions, the security of modes of operation and the security of public-key encryption schemes against superposition queries. In the following, we give a short overview of our result in each chapter.

Chapter 3 [On Quantum Indifferentiability]. The primary goal of the "Indifferentiability Framework" introduced in [54] was to provide a simplified explanation of the impossibility of instantiating a random oracle by a hash function [26]. However, subsequently, many classical construction have been studied in the indifferentiability framework [16, 32, 33, 35] to prove their soundness. Indifferentiability is a generalization of indistinguishability in which the adversary may have access to additional information of involved systems. In this thesis, we redefine the Indifferentiability Framework considering a quantum adversary. Our new definition allows a quantum distinguisher to submit superposition queries to the primitive that has been used in the construction as a building block. In contrast, since we claim the impossibility of quantum indifferentiability in many cases, queries to the construction are classical and this definition (with classical queries to the construction) leads to a stronger impossibility result. In other words, our impossibility result will hold if we consider a quantum indifferentiability definition that allows superposition queries to both the construction and the underlying primitive.

We show that almost all classical constructions (that are classically indifferetiable from a random oracle (or ideal cipher)) are not "perfectly" quantum indifferentiable from a random oracle (or ideal cipher). We show our result using a conjecture. Informally, the conjecture says that whenever we have N orthogonal projectors that pairwise commute over a subspace $\mathcal{V}$ of a Hilbert space $\mathcal{H}$, then there are N new orthogonal projectors that pairwise commute everywhere (over $\mathcal{H}$) and operate the same as the old projectors over $\mathcal{V}$ (refer to the Conjecture 1 for its mathematical representation).

Chapter 4 [Quantum Collisions for Non-uniform Functions]. A cryptographic hash function is a fundamental primitive in cryptology and it has to fulfil some properties according to its applications. The indifferentiability of a hash function from a random oracle is a desirable property for a cryptographic hash function that has been studied in [16,32]. In the chapter 3, we prove that most famous constructions, Merkle-Damgard and Sponge construction, are not "perfectly" quantum indifferentiable from a random oracle. However, in many applications, even a weaker property like collision-resistance is sufficient. Informally, the collision-resistance property guarantees that it is computationally infeasible to find two distinct inputs that hash to the same output. In this thesis, we study the collision-resistance property of hash functions considering a quantum adversary that can submit quantum queries to the hash function. We consider the quantum collision problem for a random function whose outputs are chosen according to a non-uniform distribution because the outputs of a hash function usually are not uniformly distributed. We derive some upper and lower bounds for the quantum collision problem applied to a random function whose outputs are chosen according to a distribution with some known entropy (collision-entropy or min-entropy).

Chapter 5 [Post-Quantum Security of Fujisaki-Okamoto and OAEP]. Impact of the quantum computing to the public-key encryption is drastically negative due to breaking the classical cryptosystems based on factoring and discrete logarithm problems. Also, many efficient classical cryptosystems are proved to be secure in the random oracle model [14] and many of them still lack an equivalent proof in the quantum setting. Therefore, even if we find a cryptographic primitive immune to quantum attacks, to construct an efficient cryptosystem secure against quantum adversaries, we may have to consider its security in the quantum random oracle model in which the adversary has quantum access to the random oracle. In this thesis, we analyse the security of two well-known transformations, Fujisaki-Okamoto (FO) [42] and OAEP [60] constructions, in the quantum random oracle model. The FO construction is a transformation from two weakly secure encryption schemes to a strongly secure one (IND-CCA secure) using two random oracles. We modify the FO construction and prove the security of our modified construction in the quantum random oracle model. OAEP is a transformation from a one-way trapdoor permutation to IND-CCA secure encryption scheme using two random oracles. We modify the OAEP construction and prove its security in quantum random oracle model.

Chapter 6 [Post-quantum Security of Modes of Operations]. The impact of a large-scale quantum computer to the private-key encryption schemes is the necessity to use a larger key size (or a larger output size for hash functions) [1]. However, the security of the private-key encryption schemes has to be revisited considering the new security definitions that are defined against a quantum adversary. For instance, the IND-qCPA security notion introduced in [18] considers superposition queries to the encryption algorithm with classical queries during the challenge phase. In contrast, in the IND-CPA security notion (the classical security notion) both learning queries and challenge queries are classical. Block ciphers are one of the most fundamental primitives used in private-key encryption schemes in which two parties can communicate securely using a shared secret key. Block ciphers are usually used in so called "modes of operation" in order to encrypt a message with larger size. In this thesis, we study the IND-qCPA security of the recommended list of modes of operation published by the European Union Agency for Network and Information Security [41]. Classically, OFB, CTR, CBC and CFB modes of operation are IND-CPA secure if the underlying block cipher is a classical secure pseudo-random function (a function that is indistinguishable from a truly random function when the distinguisher is classical). In the quantum setting, we prove that OFB and CTR are IND-qCPA secure if the underlying block cipher is a standard secure PRF, that is, a PRF that is indistinguishable from a truly random function when the distinguisher is quantum but it is only allowed to make classical queries to the function. In contrast, we show that CBC, CFB and XTS modes of operation are not IND-qCPA secure using a standard secure block cipher. We prove the IND-qCPA security of CBC and CFB when the underlying block cipher is a quantum secure PRF, that is, a PRF that is indistinguishable from a truly random function when the quantum distinguisher can make superposition queries to the function.

Connections between the chapters. In order to prove the quantum security of the FO and OAEP construction, we need to study the security of hash functions against superposition attacks since our modified version of the FO and OAEP construction use three hash functions. We revisit the property of hash functions, indifferentiability from a random oracle and collision-resistance, when an adversary has superposition access to the hash function. We use our result on collision-resistance of a non-uniformly distributed function to prove the FO construction in Chapter 5. The FO construction is a transformation from IND-CPA to IND-CCA secure encryption scheme, therefore for the future work, we may need an

[1] Initial recommendations of long-term secure post-quantum systems:
https://pqcrypto.eu.org/docs/initial-recommendations.pdf

IND-qCPA secure private-key encryption scheme in order to prove the security of FO construction against an adversary that makes superposition queries to the encryption and decryption oracles [4]. In other words, we may prove that the FO construction is a transformation from IND-qCPA to IND-qCCA and the existence of IND-qCPA secure private encryption scheme make the result more useful.

2. PRELIMINARIES

In this chapter, we present the preliminaries that are used throughout this thesis. We give a short introduction to the quantum computing in Section 2.2. Then, we present some definitions and theorems that are needed in each chapter.

2.1. Notation

Asymptotic Notations. We define $\mathsf{negl(n)}$ to be any non-negative function that is smaller than the inverse of any non-negative polynomial $p(n)$ for sufficiently large n. That is, $\lim_{n\to\infty} \mathsf{negl(n)}p(n) = 0$ for any polynomial $p(n)$. We write $f(n) = O(g(n))$ iff the absolute value of f is bounded above by g (up to a constant factor asymptotically), that is, $\lim_{n\to\infty} \sup \frac{|f(n)|}{g(n)} < \infty$. We write $f(n) = \Omega(g(n))$ iff f is bounded below by g asymptotically , that is, $\lim_{n\to\infty} \inf \frac{f(n)}{g(n)} > 0$. We say $f(n) = \theta(g(n))$ iff $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.

Probability Notations. The notation $x \overset{\$}{\leftarrow} X$ means that x is chosen uniformly at random from the set X. If $\mathcal{D}$ is a distribution over Y, then the notation $y \leftarrow \mathcal{D}$ means that y is chosen at random according to the distribution $\mathcal{D}$. Sup($\mathcal{D}$) is the set of all elements $y \in Y$ such that $\mathcal{D}(y) \neq 0$. By $f \leftarrow \mathcal{D}^X$, we mean a function whose outputs are chosen independently according to the distribution $\mathcal{D}$, that is, f is a function from X to Sup($\mathcal{D}$) such that for any $x \in X$, $f(x) = y$ where $y \leftarrow \mathcal{D}$. $\Pr[P : G]$ is the probability that the predicate P holds where free variables in P are assigned according to the description of G.

Other Notations. We represent the set $\{1,\ldots,m\}$ by $[m]$. By $a \oplus b$, we mean the "Exclusive or" of a and b that is 1 if a and b differ.

2.2. Quantum Computing Background

In this section, we present some introductory information about quantum computing that are needed in the thesis. We refer the interested reader to [56] for more information.

For a complex number $\psi = x + yi$, $\psi^* := x - yi$ is the complex conjugate of ψ. The n-dimensional Hilbert space $\mathcal{H}$ is the complex vector space $\mathbb{C}^n$ with the inner product defined as

$$\langle \Psi, \Phi \rangle := \sum_i^n \psi_i^* \phi_i.$$

The norm of a vector $|\Psi\rangle \in \mathcal{H}$ is defined by $||\Psi|| = \sqrt{\langle \Psi, \Psi \rangle}$. We say that vectors $|\Psi\rangle$ and $|\Phi\rangle$ are orthogonal iff $\langle \Psi, \Phi \rangle = 0$. We say that B is a basis for $\mathcal{H}$ if every vector in $\mathcal{H}$ can be written as a unique linear combination of vectors in B. B is an orthonormal basis if its elements have norm 1 and they are pairwise orthogonal. A quantum system is the Hilbert space $\mathcal{H}$ and a quantum state is a vector in $\mathcal{H}$ with norm 1. For two quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$, the composition of them is defined by a tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$. If $B_1 = \{|b_1\rangle, \dots, |b_n\rangle\}$ and $B_2 = \{|b'_1\rangle, \dots, |b'_m\rangle\}$ are bases for $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, then

$$B = \{|b_i\rangle \otimes |b'_j\rangle\}_{i=1,\cdots,n, j=1,\cdots,m}$$

is a basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$. We may use the abbreviation $|b_i b'_j\rangle$ instead of $|b_i\rangle \otimes |b'_j\rangle$.

For a quantum state $|\Psi\rangle$, the linear operator $|\Psi\rangle\langle\Psi| : \mathcal{H} \to \mathcal{H}$ is defined as:

$$|\Psi\rangle\langle\Psi|(|\Phi\rangle) = \langle\Psi, \Phi\rangle |\Psi\rangle.$$

We say the linear transformation $U : \mathcal{H} \to \mathcal{H}$ is unitary if it preserve the inner product:

$$\langle U\psi, U\phi\rangle = \langle\psi, \phi\rangle.$$

For an unitary transformation U, $UU^\dagger = I$ where $U^\dagger$ is the conjugate-transpose of U. If U_1 and U_2 are some unitaries on $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, then $U_1 \otimes U_2$ is the corresponding unitary on $\mathcal{H}_1 \otimes \mathcal{H}_2$ that is defined by

$$(U_1 \otimes U_2)(|v\rangle \otimes |w\rangle) = U_1(|v\rangle) \otimes U_2(|w\rangle).$$

A linear operator A is Hermitian if $A = A^\dagger$ where $A^\dagger$ is the conjugate-transpose of A. An orthogonal projector P is a Hermitian operator that satisfies $P^2 = P$. A projective measurement is a family $\{P_j\}_{j \in J}$ of orthogonal projectors such that $P_i P_j = 0$ for any $i \neq j$ and $\sum_{j \in J} P_j = I$. The measurement applied to $|\Psi\rangle$ returns outcome "j" with probability $\|P_j |\Psi\rangle\|^2$ and the post-measurement state is

$$\frac{P_j |\Psi\rangle}{\|P_j |\Psi\rangle\|}.$$

For an orthonormal basis $B = \{|b_1\rangle, \dots, |b_n\rangle\}$ and a given state $|\Psi\rangle$, the result of measurement in the basis B applied to $|\Psi\rangle$ is b_i with probability $\|\langle b_i, \Psi\rangle\|^2$ and the post-measurement state will be $|b_i\rangle$. This is a special case of a projective measurement where $P_i = |b_i\rangle\langle b_i|$ and it is called a complete measurement. The basis $B = \{|n\rangle\}_{n \in \{0,1\}^n}$ is called the computational basis and the measurement with respect to the computational basis is called computational basis measurement.

The set $E = \{(|\Psi_i\rangle, p_i)\}_i$ is an ensemble over a Hilbert space $\mathcal{H}$ if it satisfies the following two items.

1. For all i, $|\Psi_i\rangle \in \mathcal{H}$ and $\|\Psi_i\| = 1$
2. For all i, $p_i \geq 0$ and $\sum_i p_i = 1$.

The density operator corresponding to the ensemble E is

$$\rho = \sum_i p_i \left|\Psi_i\right\rangle \left\langle\Psi_i\right| .$$

The Hadamard operator H is an unitary operator on $\mathbb{C}^2$ such that

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) \text{ and } H\left|1\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle).$$

The Controlled-Not operator is an unitary operator on $\mathbb{C}^4$ such that it flips the second bit only if the first bit is 1.

$$CNOT\left|00\right\rangle = \left|00\right\rangle, CNOT\left|01\right\rangle = \left|01\right\rangle, CNOT\left|10\right\rangle = \left|11\right\rangle \text{ and } CNOT\left|11\right\rangle = \left|10\right\rangle.$$

A general quantum circuit can be represented by a circuit consists of unitary operations on larger systems. This procedure is called unitary purification of a general quantum circuit [70]. We say that a quantum algorithm $\mathcal{A}$ has quantum access to the oracle $O : \{0,1\}^{n_0} \to \{0,1\}^{n_1}$ (O might be chosen randomly according to some distribution), denoted by $\mathcal{A}^O$, where $\mathcal{A}$ prepares two registers X and Y for inputs and outputs respectively. Then $\mathcal{A}$ can submit superposition queries $(\sum_{x,y} \alpha_{x,y} \left|x,y\right\rangle)$ and the oracle O applies an unitary transformation that maps $\left|x,\ y\right\rangle$ to $\left|x,\ y \oplus O(x)\right\rangle$ to registers X and Y .

2.3. Preliminaries for Chapter 4

We define the min-entropy and collision entropy of a distribution in the following:

Definition 1. *Let $\mathcal{D}$ be a distribution on a set X. The min-entropy and collision-entropy of the distribution $\mathcal{D}$ is defined as the following, respectively.*

$$H_\infty(\mathcal{D}) = -\log \max_{x \in X} \mathcal{D}(x), \quad H_2(\mathcal{D}) = -\log \sum_{x \in X} \mathcal{D}(x)^2.$$

A collision for a function h is a pair of two distinct inputs, let say (x,x'), such that $h(x) = h(x')$. The theorem below proves that an uniformly random function is collision-resistant even against a quantum adversary. By an uniformly random function $h : X \to Y$, we mean a function that is chosen uniformly at random from the set of all functions with domain X and co-domain Y. We reduce the quantum collision problem for a random function whose outputs are chosen according to a non-uniform distribution to the quantum collision problem for an uniformly random function and use the following theorem.

Theorem 1 (Theorem 7 [75]). *Let $h \leftarrow \mathcal{D}^X$ where $\mathcal{D}$ is the uniform distribution over Y. Then any quantum algorithm making q queries to h outputs a collision for h with probability at most $\frac{C(q+2)^3}{|Y|}$ where C is a universal constant.*

Definition 2 (Universal Hash Function [28])**.** *A family of functions $H = \{h : \{0,1\}^n \to \{0,1\}^m\}$ is called a family of universal hash functions if for all distinct $x, y \in \{0,1\}^n$:*

$$\Pr\Big[h(x) = h(y) : h \xleftarrow{\$} H\Big] \leq 2^{-m}.$$

Definition 3. *Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be distributions on a set X. The statistical distance between $\mathcal{D}_1$ and $\mathcal{D}_2$ is*

$$\mathrm{SD}(\mathcal{D}_1, \mathcal{D}_2) = \frac{1}{2} \sum_{x \in X} \Big| [\mathcal{D}_1(x)] - [\mathcal{D}_2(x)] \Big|.$$

Lemma 2 (Leftover Hash Lemma [46])**.** *Let $\mathcal{D}$ be a distribution with collision-entropy k over set X and e be a positive integer. Let $h : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^{k-2e}$ be a universal hash function. Then,*

$$\mathrm{SD}\Big(\big(h(y,x), y\big), \big(z, y\big)\Big) \leq 2^{-e-1}$$

where $x \leftarrow \mathcal{D}, y \xleftarrow{\$} \{0,1\}^m$ and $z \xleftarrow{\$} \{0,1\}^{k-2e}$.

The following lemma gives an upper bound on the success probability of a quantum adversary in distinguishing a zero function from a random function that outputs 1 with some probability γ independently for any input and outputs 0 otherwise.

Lemma 3 (Lemma 3 in [48])**.** *For $0 \leq \gamma \leq 1$, we define distribution $\mathcal{D}_\gamma$ of functions $F : X \to \{0,1\}$ where $F(x) := 1$ with probability γ, and $F(x) := 0$ otherwise. Then for any oracle algorithm $\mathcal{A}$ making q queries,*

$$\Big| \Pr\big[b = 1 : b \leftarrow \mathcal{A}^F\big] - \Pr\big[b = 1 : b \leftarrow \mathcal{A}^N\big] \Big| \leq 8q^2\gamma,$$

where N is the zero function on X and F is chosen randomly according to the distribution $\mathcal{D}_\gamma$.

The lemma below proves that if two distributions are indistinguishable for a quantum distinguisher then they are "oracle-indistinguishable".

Lemma 4 ([74])**.** *Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be efficiently sampleable distributions over some set Y, and let X be some other set. Then if A is a quantum algorithm that distinguishes $f_1 \leftarrow \mathcal{D}_1^X$ from $f_2 \leftarrow \mathcal{D}_2^X$ by making q queries and with probability ε, we can construct a quantum algorithm $\mathcal{B}$ that distinguishes samples from $\mathcal{D}_1$ and $\mathcal{D}_2$ with probability at least $\dfrac{3\varepsilon^2}{64\pi^2 q^3}$.*

2.4. Preliminaries for Chapter 5

In this section, we present some notations, definitions and existing results that are needed in Chapter 5. In the following lines, we define the notion of the symmetric and asymmetric encryption scheme.

Definition 4. *A symmetric encryption scheme* Π *consists of three polynomial time (in the security parameter n) algorithms,* $\Pi = (Gen, Enc, Dec)$*, described below.*

1. *Gen, the key generation algorithm, is a probabilistic algorithm which on input* 1^n *outputs a key,* $sk \leftarrow Gen(1^n)$.
2. *Enc, the encryption algorithm, is a probabilistic algorithm which takes as input a key k and a message* $m \in \mathtt{MSP}$ *and outputs a ciphertext* $c \leftarrow Enc_k(m)$*. The message space can be infinite and may depend on the security parameter.*
3. *Dec, the decryption algorithm, is a deterministic algorithm that takes as input a key k and a ciphertext c and returns the message* $m := Dec_k(c)$*. Here we assume that decryption algorithm returns the original message, i.e.,* $Dec_k(Enc_k(m)) = m$*, for every* $k \in \mathtt{KSP}$ *and every* $m \in \mathtt{MSP}$.

Definition 5. *An asymmetric encryption scheme* Π *consists of three polynomial time (in the security parameter n) algorithms,* $\Pi = (Gen, Enc, Dec)$*, described below.*

1. *Gen, the key generation algorithm, is a probabilistic algorithm which on input* 1^n *outputs a pair of keys,* $(pk, sk) \leftarrow Gen(1^n)$*, called the public key and the secret key for the encryption scheme, respectively.*
2. *Enc, the encryption algorithm, is a probabilistic algorithm which takes as input a public key pk and a message* $m \in \mathtt{MSP}$ *and outputs a ciphertext* $c \leftarrow Enc_{pk}(m)$*. The message space* $\mathtt{MSP}$ *may depend on pk.*
3. *Dec, the decryption algorithm, is a deterministic algorithm that takes as input a secret key sk and a ciphertext c and returns message the* $m := Dec_{sk}(c)$*. It is required that the decryption algorithm returns the original message, i.e.,* $Dec_{sk}(Enc_{pk}(m)) = m$*, for every* $(pk, sk) \leftarrow Gen(1^n)$ *and every* $m \in \mathtt{MSP}$*. The algorithm Dec returns* $\perp$ *if ciphertext c is not decryptable.*

We define the security notions for encryption schemes, e.g, One-time security, One-way security and IND-CCA in the quantum random oracle model.

Definition 6 (One-time secure)**.** *A symmetric encryption scheme* $\Pi = (Enc, Dec)$ *is one-time secure if no* ***quantum*** *polynomial time adversary* $\mathcal{A}$ *can win in the* $PrivK^{OT}_{\mathcal{A},\Pi}(n)$ *game, except with probability at most 1/2 + negl(n):*

$\boldsymbol{PrivK^{OT}_{\mathcal{A},\Pi}}(n)$ *game:*

Key Gen: *The challenger picks up a key k from* $\mathtt{KSP}$ *uniformly at random, i.e.,* $k \xleftarrow{\$} \mathtt{KSP}$.

Query: *The adversary* $\mathcal{A}$ *on input* (1^n) *chooses two messages* m_0, m_1 *of the same length and sends them to the challenger. The challenger chooses* $b \xleftarrow{\$} \{0,1\}$ *and responds with* $c^* \leftarrow Enc_k(m_b)$.

Guess: *The adversary* $\mathcal{A}$ *produces a bit* b'*, and wins if* $b = b'$.

Definition 7 (One-way secure)**.** *An asymmetric encryption scheme* $\Pi = (Gen, Enc, Dec)$ *is one-way secure if no* ***quantum*** *polynomial time adversary* $\mathcal{A}$ *can win in the* $PubK^{OW}_{\mathcal{A},\Pi}(n)$ *game, except with probability at most negl(n):*

$\boldsymbol{PubK^{OW}_{\mathcal{A},\Pi}}(n)$ *game:*

Key Gen: *The challenger runs* $Gen(1^n)$ *to obtain a pair of keys* (pk, sk)*.*

Challenge Query: *The challenger picks a uniformly random* x *from the message space, i.e.,* $x \overset{\$}{\leftarrow} \mathtt{MSP}$*, and encrypts it using* pk *to obtain the ciphertext* $y \leftarrow Enc_{pk}(x)$*, and sends* y *to the adversary* $\mathcal{A}$*.*

Guess: *The adversary* $\mathcal{A}$ *on input* (pk, y) *produces a bit string* x'*, and wins if* $x' = x$*.*

Random Oracle Model. In the random oracle model, the assumption is every party, even adversary, has access to a truly random function H that has been used in a cryptographic construction. By access to H, we mean that every party can query H on some inputs x and gets $H(x)$ back. It is easier to prove the security of construction when H is modeled as a random function, however, in a real life application one has to substitute the random function with a hash function.

Quantum Random Oracle Model. Since in a real life application H is a hash function that adversary knows its description, a quantum adversary can implement H on his quantum computing device and evaluates H on some quantum states. Therefore, we need to consider the quantum random oracle model instead of random oracle model to prove the security of cryptographic constructions in the presence of a quantum adversary. In the quantum random oracle model the adversary has superposition access to H but honest parties have classical access to H.

Definition 8 (IND-CCA in the quantum random oracle model)**.** *An asymmetric encryption scheme* $\Pi^{asy} = (Gen, Enc, Dec)$ *is IND-CCA secure if no* ***quantum*** *polynomial time adversary* $\mathcal{A}$ *can win in the* $PubK^{CCA-QRO}_{\mathcal{A},\Pi}(n)$ *game, except with probability at most 1/2 + negl(n):*

$\boldsymbol{PubK^{CCA-QRO}_{\mathcal{A},\Pi}}(n)$ *game:*

Key Gen: *The challenger runs* $Gen(1^n)$ *to obtain a pair of keys* (pk,sk) *and chooses random oracles.*

Query: *The adversary* $\mathcal{A}$ *is given the public key pk and with* ***classical*** *oracle access to the decryption oracle and* ***quantum*** *access to the random oracles chooses two messages* m_0,m_1 *of the same length and sends them to the challenger. The challenger chooses* $b \xleftarrow{\$} \{0,1\}$ *and responds with* $c^* \leftarrow Enc_{pk}(m_b)$.

Guess: *The adversary* $\mathcal{A}$ *continues to query the decryption oracle and the random oracles, but may not query the ciphertext* c^* *in a decryption query. Finally, the adversary* $\mathcal{A}$ *produces a bit* b'*, and wins if* $b = b'$.

Note that in the definition above, the adversary is only allowed to make superposition queries to the random oracle. In contrast, the encryption and decryption queries are classical.

Definition 9 (Quantum partial-domain one-way function)**.** *We say a function* $f : \{0,1\}^{n+k_1} \times \{0,1\}^{k_0} \to \{0,1\}^m$ *where* k_0*,* k_2 *may depend on n is partial-domain one-way if for any polynomial time quantum adversary A,*

$$\Pr\Big[\tilde{s} = s : s \xleftarrow{\$} \{0,1\}^{n+k_1},\ t \xleftarrow{\$} \{0,1\}^{k_0},\ \tilde{s} \leftarrow A(f(s,t))\Big] \leq \textsf{negl(n)}.$$

2.4.1. One-way to Hidding Lemmas

The following lemmas give us a way to reprogram a random oracle in the security proof. A classical adversary with access to the random oracle H can not distinguish $(x,H(x))$ from (x,y) where x and y are chosen uniformly at random unless the adversary queries H on input x. If the adversary makes q queries, the probability that one of them is on input x is $\frac{q}{|X|}$. In the quantum case, the same argument does not hold because a quantum adversary A can query the random oracle on superposition of all inputs (that includes x as well). Therefore in our quantum security proof, we use the following lemma. Informally, the lemma says that the success probability of A in distinguishing two cases is upper bounded by the success probability of another algorithm C that runs A and measures the input of a randomly chosen query of A and declares success if the result of measurement is x.

Lemma 5 (One way to hiding (O2H) [67])**.** *Let* $H : \{0,1\}^n \to \{0,1\}^m$ *be a random oracle. Consider an oracle algorithm A that makes at most q queries to H. Let C be an oracle algorithm that on input x does the following: pick* $i \xleftarrow{\$} \{1,\ldots,q\}$ *and* $y \xleftarrow{\$} \{0,1\}^m$*, run* $A^H(x,y)$ *until (just before) the i-th query, measure the argument of the query in the computational basis, and output the measurement outcome. (When A makes less than i queries, C outputs* $\perp \notin \{0,1\}^n$*.) Let* $FALL\{n,m\}$ *be the set of all functions from* $\{0,1\}^n$ *to* $\{0,1\}^m$*.*

Let $P_A^1 := \Pr\Big[b' = 1 : H \xleftarrow{\$} FALL\{n,m\}, x \xleftarrow{\$} \{0,1\}^n, b' \leftarrow A^H(x,H(x))\Big]$,

$$P_A^2 := \Pr\left[b' = 1 : H \xleftarrow{\$} FALL\{n,m\}, x \xleftarrow{\$} \{0,1\}^n, y \xleftarrow{\$} \{0,1\}^m, b' \leftarrow A^H(x,y)\right],$$
$$P_C := \Pr\left[x' = x : H \xleftarrow{\$} FALL\{n,m\}, x \xleftarrow{\$} \{0,1\}^n, x' \leftarrow C^H(x)\right].$$

Then

$$\left|P_A^1 - P_A^2\right| \leq 2q\sqrt{P_C}.$$

The following lemma is a generalization of the lemma above. In the security proof, we use it to replace $H(x\|m)$ with a random element when x is chosen uniformly at random, but m is chosen adaptively based on earlier random oracle queries.

Lemma 6 (One way to hiding, adaptive (O2HA) [66]). *Let $H : \{0,1\}^* \to \{0,1\}^n$ be a random oracle. Consider an oracle algorithm A_0 that makes at most q_0 queries to H. Consider an oracle algorithm A_1 that uses the final state of A_0 and makes at most q_1 queries to H. Let C be an oracle algorithm that on input (j,B,x) does the following: run $A_1^H(x,B)$ until (just before) the j-th query, measure the argument of the query in the computational basis, and output the measurement outcome. (When A_1 makes less than j queries, C outputs $\perp \notin \{0,1\}^\ell$.)*
Let

$$P_A^1 := \Pr\Big[b' = 1 : H \xleftarrow{\$} (\{0,1\}^* \to \{0,1\}^n), m \leftarrow A_0^H(), \\ x \xleftarrow{\$} \{0,1\}^\ell, b' \leftarrow A_1^H(x, H(x\|m))\Big]$$

$$P_A^2 := \Pr\Big[b' = 1 : H \xleftarrow{\$} (\{0,1\}^* \to \{0,1\}^n), m \leftarrow A_0^H(), \\ x \xleftarrow{\$} \{0,1\}^\ell, B \xleftarrow{\$} \{0,1\}^n, b' \leftarrow A_1^H(x,B))\Big]$$

$$P_C := \Pr\Big[x = x' \wedge m = m' : H \xleftarrow{\$} (\{0,1\}^* \to \{0,1\}^n), m \leftarrow A_0^H(), x \xleftarrow{\$} \{0,1\}^\ell, \\ B \xleftarrow{\$} \{0,1\}^n, j \xleftarrow{\$} \{1,\cdots,q_1\}, x'||m' \leftarrow C^H(j,B,x)\Big]$$

Then

$$\left|P_A^1 - P_A^2\right| \leq 2q_1\sqrt{P_C} + q_0 2^{-\ell/2+2}.$$

2.5. Preliminaries for Chapter 6

We define the IND-CPA security and IND-qCPA security of a symmetric encryption scheme as follows. We may use the notation $c = \mathsf{Enc}_k(m;r)$ instead of $c \leftarrow \mathsf{Enc}_k(m)$ when the randomness r used by the encryption algorithm explicitly has defined.

Definition 10 (IND-CPA)**.** *A symmetric encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is indistinguishable under chosen plaintext attack (IND-CPA secure) if no classical poly-time adversary* $\mathcal{A}$ *can win in the* $PrivK^{CPA}_{\mathcal{A},\Pi}(n)$ *game, except with probability at most 1/2 + negl(n):*
PrivK$^{\boldsymbol{CPA}}_{\boldsymbol{\mathcal{A},\Pi}}(n)$ *game:*

Key Gen: *The challenger picks a random key* $k \leftarrow \mathsf{Gen}(1^n)$.

Encryption Queries: *Adversary may make polynomial number of encryption queries.*

Challenge Query: *Adversary* $\mathcal{A}$ *chooses two messages* m_0, m_1 *and sends them to the challenger. The challenger chooses* $b \overset{\$}{\leftarrow} \{0,1\}$ *and* $r \overset{\$}{\leftarrow} \{0,1\}^*$ *and responds with* $c^* = \mathsf{Enc}_k(m_b; r)$.

Encryption Queries: *Adversary makes polynomial number of encryption queries.*

Guess: *Adversary* $\mathcal{A}$ *produces a bit* b'*, and wins if* $b = b'$.

In the definition below, a quantum adversary is allowed to query encryption oracle in superposition but challenge queries have to be classical.

Definition 11 (IND-qCPA [19])**.** *A symmetric encryption scheme* Π = *(Gen,Enc, Dec) is indistinguishable under quantum chosen message attack (IND-qCPA secure) if no efficient adversary* $\mathcal{A}$ *can win in the* $PrivK^{qCPA}_{\mathcal{A},\Pi}(n)$ *game, except with probability at most 1/2 + negl(n):*
PrivK$^{\boldsymbol{qCPA}}_{\boldsymbol{\mathcal{A},\Pi}}(n)$ *game:*

Key Gen: *The challenger picks a random key* $k \leftarrow \mathsf{Gen}(1^n)$.

Challenge Queries: $\mathcal{A}$ *sends two messages* m_0, m_1 *to which the challenger responds with* $c^* = \mathsf{Enc}_k(m_b; r)$ *where* $b \overset{\$}{\leftarrow} \{0,1\}$ *and* $r \overset{\$}{\leftarrow} \{0,1\}^*$.

Encryption Queries: *For each such query, the adversary* $\mathcal{A}$ *provides the register M, containing message, and the register C, to store ciphertext. Then, the challenger chooses randomness r, and encrypts each message in the superposition using r as randomness:*

$$\sum_{m,c} \psi_{m,c} \big| m, c \big\rangle \rightarrow \sum_{m,c} \psi_{m,c} \big| m, c \oplus Enc_k(m; r) \big\rangle,$$

and gives back M and C registers to the adversary.
Guess: $\mathcal{A}$ *produces a bit* $b^{'}$*, and wins if* $b = b^{'}$.

2.5.1. Modes of Operation

Let $E : \mathcal{K} \times \{0,1\}^t \to \{0,1\}^t$ be a block cipher and n be a polynomial in t in the following definitions. We define different modes of operation using E. Every mode consists of three algorithms $\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}$ that are defined below for each mode.

Definition 12 (ECB mode of operation)**.** $\Pi_{ECB} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$*:*
Gen*: Pick a random key* $k \leftarrow \mathsf{Gen}(1^t)$.
Enc*: For a given message* $M = m_1 m_2 \ldots m_n$*;*

$$\mathsf{Enc}_k(M) := c_1 \cdots c_n, \text{ where } c_i = E(k, m_i) \text{ for } 0 < i \leq n.$$

Dec*: For a given cipher-text* $C = c_1 \ldots c_n$ *and key* k*;*

$$\hat{m}_i := E^{-1}(k, c_i) \text{ for } 0 < i \leq n.$$

Definition 13 (CBC mode of operation)**.** $\Pi_{CBC} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$*:*
Gen*: Pick a random key* $k \leftarrow \mathsf{Gen}(1^t)$.
Enc*:: For a given message* $M = m_1 m_2 \ldots m_n$*;*

$$\mathit{Enc}_k(M) := c_0 c_1 \ldots c_n, \text{ where } c_0 \xleftarrow{\$} \{0,1\}^t \text{ and } c_i = E(k, m_i \oplus c_{i-1}) \text{ for } 0 < i \leq n.$$

Dec*: For a given cipher-text* $C = c_0 c_1 \cdots c_n$ *and key* k*;*

$$\hat{m}_i := E^{-1}(k, c_i) \oplus c_{i-1} \text{ for } 0 < i \leq n.$$

Definition 14 (CFB mode of operation)**.** $\Pi_{CFB} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$*:*
Gen*: Pick a random key* $k \leftarrow \mathsf{Gen}(1^t)$.
Enc*: For a given message* $M = m_1 m_2 \ldots m_n$*;*

$$\mathsf{Enc}_k(M) := c_0 c_1 \ldots c_n, \text{ where } c_0 \xleftarrow{\$} \{0,1\}^t \text{ and } c_i = E(k, c_{i-1}) \oplus m_i \text{ for } 0 < i \leq n.$$

Dec*: For a given cipher-text* $C = c_0 c_1 \ldots c_n$ *and key* k*;*

$$\hat{m}_i := E(k, c_{i-1}) \oplus c_i \text{ for } 0 < i \leq n.$$

Definition 15 (OFB mode of operation)**.** $\Pi_{OFB} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$*:*
Gen*: Pick a random key* $k \leftarrow \mathsf{Gen}(1^t)$.
Enc*: For a given message* $M = m_1 m_2 \ldots m_n$*;* $\mathsf{Enc}_k(M) := c_0 c_1 \ldots c_n$,

$$\text{where } c_0 = r_0 \xleftarrow{\$} \{0,1\}^t, \; r_i = E(k, r_{i-1}) \text{ and } c_i = r_i \oplus m_i \text{ for } 0 < i \leq n.$$

Dec*: For a given cipher-text* $C = c_0 c_1 \ldots c_n$ *and key* k*;*

$$\hat{m}_i := E(k, c_{i-1}) \oplus c_i \text{ for } 0 < i \leq n.$$

Definition 16 (CTR mode of operation)**.** $\Pi_{CTR} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$*:*
Gen*: Pick a random key* $k \leftarrow \mathsf{Gen}(1^t)$ *.*
Enc*: For a given message* $M = m_1 m_2 \ldots m_n$*;*

$$\mathsf{Enc}_k(M) := c_0 c_1 \ldots c_n, \textit{ where } c_0 \xleftarrow{\$} \{0,1\}^t \textit{ and } c_i = E(k, c_0 + i) \oplus m_i \textit{ for } 0 < i \leq n.$$

Dec*: For a given cipher-text* $C = c_0 c_1 \ldots c_n$ *and key* k*;*

$$\hat{m}_i := E(k, c_0 + i) \oplus c_i \textit{ for } 0 < i \leq n.$$

Definition 17 (XTS mode of operation)**.** $\Pi_{XTS} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$*:*
Gen*: Pick two random keys* $k_1, k_2 \leftarrow \mathsf{Gen}(1^t)$ *.*
Enc*: For a given message* $M = m_1 m_2 \ldots m_n$*;*

$$\mathsf{Enc}_k(M) := c_0 c_1 \ldots c_n,$$

where $c_0 \in \{0,1\}^t$ *(and will be different in different ciphertext),* $c_i = E(k_1, m_i \oplus \Delta_i) \oplus \Delta_i$ *for* $0 < i \leq n$*,* $\Delta_i = \alpha^{i-1} L$*,* $L = E(k_2, c_0)$ *and* α *is the primitive element of the field* $\mathbb{F}_2^n$*.*
Dec*: For a given cipher-text* $C = c_0 c_1 \ldots c_n$*; and keys* k_1 *and* k_2*;*

$$\Delta_i = \alpha^{i-1} E(k_2, c_0) \textit{ and } \hat{m}_i := E(k, c_i \oplus \Delta_i) \oplus \Delta_i \textit{ for } 0 < i \leq n.$$

3. ON QUANTUM INDIFFERENTIABILITY

3.1. Motivation

The “Indifferentiability Framework” introduced in [54] is a generalization of the concept of indistinguishability of two systems in which the adversary is assumed to have access to the additional information of involved systems. It is a security notion that allows us to compare the implementation of a cryptosystem (called a “construction” in the following) to an ideal representation. For example, the indifferentiability framework allows us to say that a certain hash function construction that is constructed from a smaller idealized primitive is indifferentiable from a random oracle. This means that we can use this hash function in any setting in which a random oracle can be used, without loss of security.[1] In particular, showing indifferentiability of a specific construction immediately implies a number of other security properties. For example, if a hash function is indifferentiable from a random oracle, we immediately get that it is one-way, collision-resistant, a pseudo-random-function, etc. Indifferentiability is most often applied in settings where a larger primitive (say a hash function) is constructed from a smaller idealized primitive (say a random oracle with short input/output as a block function).

In [54], constructions can be arbitrary interacting systems. In our paper, we consider a special case, namely where constructions are stateful oracles.[2] To make this more formal, we need to first introduce two types of “interfaces” to a construction, the private and the public interface. In our view (where constructions are oracles), these simply represent two types of queries, and we write $\mathcal{T}^{priv}$ for $\mathcal{T}$ restricted to its private interface (i.e., ignoring all queries that are not of the private type), and $\mathcal{T}^{pub}$ for $\mathcal{T}$ restricted to its public interface. The idea behind private and public interfaces is that private interfaces model the access the user of a construction has (e.g., input/output via an API), while the public interface represents what access an adversary has (e.g., network communication, or, in our case, publicly available random oracles).

The primary goal of the indifferentiability framework was to provide a simplified explanation of the impossibility of instantiating a random oracle by a hash function [26]. However, subsequently, many classical constructions have been revisited based on indifferentiability framework to prove their soundness. To name a few, the Luby-Rackoff construction (Feistel Network) [53] that constructs a pseudo-random permutation from pseudo-random functions has been studied based on the indifferentiability framework in multiple research works [33,35,37]. In [32], the authors revisited the Merkle-Damgård construction based on the indif-

[1] Within limitations. There are certain settings in which indifferentiability is not enough for this purpose. See [58]. In most settings, however, a construction that is indifferentiable from a random oracle is as good as a random oracle.

[2] That is, whenever a construction is queried with some value x, it returns some value y to the invoking party and possibly updates its internal state.

ferentiability framework. They show that the plain Merkle-Damgård construction is differentiable from a random oracle, but, they modify the MD construction to successfully obtain positive result. The indifferentiability of sponge construction that is used in SHA-3 has been studied in [16].

It is worth mentioning that at least in the case of SHA-3/the Sponge construction, all security properties were derived from its indifferentiability. For example, we are not aware of any proof of the collision-resistance of the Sponge construction that does not rely on first showing indifferentiability.[3]

However, all of these results are in the classical setting. To the best of our knowledge, no results on indifferentiability are known in the quantum setting.[4] Especially in the case of the Sponge construction, this is quite problematic since no direct proofs of the security properties of the Sponge construction are known in the case of a random permutation as block function. That means, we do not even know whether SHA-3 is post-quantum secure.

3.2. Our Contribution

We translate the indifferentiability framework to the quantum case. In the definition below, $\mathcal{C}[f]$ (that can be any of mentioned constructions above, e.g. Sponge) is a construction that uses a primitive function f as a building block. $\mathcal{D}(X,Y)$ means the quantum distinguisher $\mathcal{D}$ has oracle access to X and Y. We denote non-superposition access using "overline" and no overline over constructions means superposition access.

Definition 18 (Quantum indifferentiability)**.** $\mathcal{C}[f]$ *is quantum indifferentiable from H iff for any quantum-polynomial-time distinguisher $\mathcal{D}$, there exists a quantum-polynomial-time simulator* Sim *such that*

$$|\Pr[\mathcal{D}(\overline{\mathcal{C}[f]},f)=1]-\Pr[\mathcal{D}(\overline{H},\mathsf{Sim}(H))=1]| \tag{3.1}$$

is negligible. We say $\mathcal{C}[f]$ is perfectly quantum indifferentiable from H if that difference is 0*.*

[3] [34] shows the (quantum) collision-resistance of the Sponge construction in the case where the underlying block function is a random function, but this does not apply to SHA-3 which uses an invertible random permutation instead.

[4] In [76], Zhandry proved the Quantum Indifferentiability of Merkle-Damgård construction using a "compressed standard oracle". However, it is not clear that their compressed standard oracle is an unitary operation. Since a non-unitary operation is not a valid quantum operation, their result might not hold.

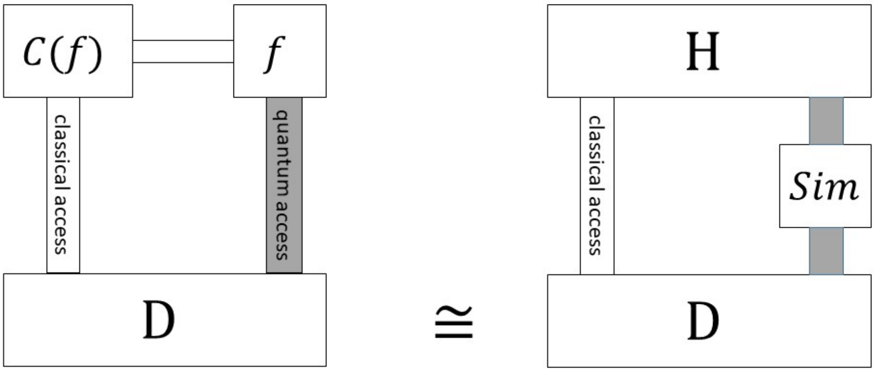


Figure 3.1: Quantum Indifferentiability Definition. Quantum access has highlighted by gray rectangles.

Here, we explain the ideas behind the definition above. Since f (public interface) represents a globally known function (e.g., the block function of a hash function construction modeled as a random oracle), we have to model the fact that an adversary can evaluate that function in superposition[5]. (See [17] for additional discussion on why random oracles should be modeled with superposition queries.) Since we will give evidence that indifferentiability is not achievable in many cases (stated below), we consider queries to $\mathcal{C}[f]$ (private interface) to be classical and consequently this weaker variant of the definition (with classical queries) yields a stronger claim.

We give some evidence why there is a lack of proofs of quantum indifferentiability. Precisely, we show that under a certain assumption (stated below as a conjecture), perfectly secure quantum indifferentiability is impossible in a wide variety of cases (including the Sponge construction and Feistel networks). This holds even in the weaker setting where the construction is accessed classically, and the adversary merely has superposition access to the underlying primitive (e.g., the random oracle). We give an overview of the impossibility result in the following subsection.

Concurrent Work. Concurrently in [76], Zhandry proved the Quantum Indifferentiability of Merkle-Damgåd construction using a “compressed standard oracle”. However, it is not clear that their compressed standard oracle is an unitary operation and this means that their result might not hold. Even if it is an unitary operation, it does not reject our conjecture and result since we show the impossibility of Quantum Indifferentiability respected to a perfect simulator. We would like to thank Mark Zhandry for valuable discussion about his work.

[5] An oracle implementing f with classical queries will measure its input register in the computational basis, resulting in a value x, and then prepare its output register in the state $|f(x)\rangle$. An oracle implementing f with superposition queries will apply the unitary U_f to a pair of registers, where U_f is defined by $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$.

3.2.1. Proof Overview for the Impossibility of Perfect Indifferentiability

We skip the details of the proof and the interested reader can refer to [27] for more information. The highlighted part of the proof:

- We show that if two constructions $\mathcal{C}[f]$ and H are perfectly quantum indifferentiable, then they are perfectly classical indifferentiable with respect to a stateless classical simulator. By a stateless simulator, we mean a simulator that chooses the primitive function f according to some distribution at the beginning, before any queries have been made, and answers to a query on input x by $f(x)$. We show that the existence of a perfect quantum simulator implies the existence of a stateless one (to show the result stated above) by defining a class of distinguishers, named $\mathbb{D}$, that limit the behaviour of the quantum simulator. Inside the class, there is a classical distinguisher $\mathcal{D}_{cl}$ that we will give its description later in the proof. Using $\mathbb{D}$, we transform a quantum simulator to a (stateless) classical simulator that is perfect for $\mathcal{D}_{cl}$.
- Finally, we show that many classical constructions are not perfectly indifferentiable from H with respect to stateless simulators (using $\mathcal{D}_{cl}$) and therefore they are not perfectly quantum indifferentiable (since perfect quantum indifferentiability implies perfect classical indifferentiability with respect to stateless classical simulators.).

The following theorem is our main theorem. We show the theorem under a certain assumption (see the Conjecture 1.) By an one-sided distinguisher, we mean a distinguisher $\mathcal{D}$ that outputs 1 with probability 1 when it interacts with the real case, that is, $\Pr[\mathcal{D}(\overline{\mathcal{C}[f]}, f) = 1] = 1$.

Theorem 7. *If two construction $\mathcal{C}[f]$ and H are **perfectly quantum** indifferentiable then for any classical "one-sided" distinguisher $\mathcal{D}_{cl}$ (cl stands for classical), there exists a stateless simulator Sim_{sl} (sl stands for stateless) such that*

$$|\Pr[\mathcal{D}_{cl}(\overline{\mathcal{C}[f]}, \overline{f}) = 1] - \Pr[\mathcal{D}_{cl}(\overline{H}, \overline{\mathsf{Sim}_{sl}(H)}) = 1]| = 0.$$

We prove the theorem above for a primitive f that has one bit output. The result can be generalized easily for a function with n bit output. To prove the theorem above, we start with arbitrary one-sided classical distinguisher $\mathcal{D}_{cl}$ that makes at most $q-2$ queries. Then, we define a class of one-sided distinguishers

$$\mathbb{D} = \bigcup_{i=1}^{6} \mathbb{D}_i \cup \{\mathcal{D}_{cl}\}$$

that limits the behaviour of the simulator. These distinguishers can be defined now but we present them step by step in the following.

High-level proof of Theorem 7. In the following lemma we show that for the finite class of one-sided distinguishers, the perfect quantum indifferentiability implies the existence of a simulator that is perfect for all distinguishers inside the class. Then, we show that a quantum simulator that is perfect for the class $\mathbb{D}$ has some properties. Namely, we show that there is a quantum simulator Sim_3 that is perfect for $\mathbb{D}$ and in each query operates as follows:

$$\mathsf{Sim}_3 \left|x, b, \psi\right\rangle_{XYS} = \left|x\right\rangle \otimes \left|b\right\rangle P_x \left|\psi\right\rangle + \left|x\right\rangle \otimes \left|1-b\right\rangle (I - P_x) \left|\psi\right\rangle ,$$

where X is the input register, Y is the output register, S is the internal register of simulator, and P_x is a projector (see Property 8). This property can be obtained using distinguishers in $\mathbb{D}_1, \ldots, \mathbb{D}_5$. Then we use distinguishers in $\mathbb{D}_5$ and $\mathbb{D}_6$ to show that the projectors $\{P_x\}_{x \in X}$ pairwise commute on some specific subspace $\mathsf{Span}\, V_{q-3}^{\mathsf{Sim}_3}$ (see Definition 21). We conjecture that there are some projectors $\{\hat{P}_x\}_{x \in X}$ that commute everywhere and they operate the same as P_x on subspace $\mathsf{Span}\, V_{q-3}^{\mathsf{Sim}_3}$. Since the projectors commute, they are diagonalizable and therefore a complete measurement on the register S can be commuted to the beginning before any query has been made. This intuitively means that the internal register of the simulator will not change during the queries (simulator does not have a memory). From this we construct a classical stateless simulator that is perfect for $\mathcal{D}_{cl}$.

Lemma 8. *Let $\mathbb{D}$ be a finite class of "one-sided" distinguishers that make polynomial number of queries. If the construction $\mathcal{C}[f]$ is perfectly quantum indifferentiable from H, then there exists a quantum-polynomial time simulator* Sim *such that for any $\mathcal{D} \in \mathbb{D}$,*

$$|\Pr[\mathcal{D}(\overline{\mathcal{C}[f]}, f) = 1] - \Pr[\mathcal{D}(\overline{H}, \mathsf{Sim}(H)) = 1]| = 0.$$

Proof. Let $\mathcal{D}^*$ be a distinguisher that chooses a distinguisher $\mathcal{D}$ from $\mathbb{D}$ uniformly at random, runs $\mathcal{D}$ and outputs its result. Then, the perfectly quantum indifferentiability of $\mathcal{C}[f]$ and H implies the existence of a simulator Sim that is perfect for $\mathcal{D}^*$. Since $\mathbb{D}$ is a class of one-sided distinguishers, we can conclude that Sim is a perfect simulator for any $\mathcal{D} \in \mathbb{D}$.

□

We use the following definition for the sate of a simulator that has been queried by a distinguisher. Since queries made by the distinguisher can be randomized, the state of simulator after being queried by the distinguisher is represented as a density operator.

Definition 19. *For a given simulator* Sim, *and for a given algorithm $\mathcal{D}$ querying the simulator, let*

$$\rho_S^{\mathsf{Sim},\mathcal{D}} := \sum_j \lambda_j \left|\Psi_j\right\rangle \left\langle\Psi_j\right| ,$$

where $\lambda_i > 0$ and $\{\left|\Psi_j\right\rangle\}_j$ is an orthonormal set of vectors, denote the inner state of Sim *after running D.*

Definition 20. *We define $V^{\mathcal{D},\mathsf{Sim}} := \{\left|\Psi_j\right\rangle\}_j$ where for any j, $\left|\Psi_j\right\rangle$ is defined in the definition above. That is, $V^{\mathcal{D},\mathsf{Sim}}$ is defined such that the state of* Sim *after running $\mathcal{D}$ is a mixture of pure states in $V^{\mathcal{D},\mathsf{Sim}}$.*

Definition 21. *Let*

$$V_i^{\mathsf{Sim}} := \bigcup_{\mathcal{D}} V^{\mathcal{D},\mathsf{Sim}}$$

where the union ranges over all $\mathcal{D} \in \mathbb{D}$ that makes i queries. We omit Sim *from* V_q^{Sim} *wherever* Sim *is clear. Note that $V_0 = \{|\Phi\rangle\}$ where $|\Phi\rangle$ is the initial state of the simulator.*

To prove Theorem 7, in the following, we present our distinguishers and the properties that they enforce to a perfect simulator. The discussion here lacks a lot of details and interested reader can refer to [27] for more detailed proofs.

Property 1. *The simulator is perfect for the class of distinguishers $\mathbb{D}$, that is, the simulator is a perfect simulator for any $\mathcal{D} \in \mathbb{D}$.*

Claim 1. *There exists a simulator* Sim_1 *that has Property 1.*

Proof. Since $\mathbb{D}$ is a finite class of one-sided distinguishers, there exists Sim_1 that is perfect for any $\mathcal{D} \in \mathbb{D}$ by Lemma 8. □

Property 2. *The simulator is a unitary transformation, i.e., his operation in the i-th query is given by an unitary $U^{(i)}$ that may depend on the primitive that is queried by the simulator and it is applied to the registers X (input register), Y (output register), S (internal register of simulator).*

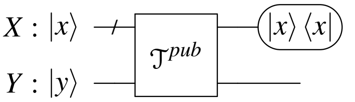
Claim 2. *There exists a simulator that has the Properties 1 and 2.*

Proof. Let Sim_2 be a purification of Sim_1. It is clear that it fulfils Properties 1 and 2. □

The class $\mathbb{D}_1$ of distinguishers:

$$\mathbb{D}_1 = \{\mathcal{D}_1^{(1)}, \ldots, \mathcal{D}_1^{(q)}\},$$

where for any $i \in [q]$, $\mathcal{D}_1^{(i)}$ is a distinguiser that queries the public interface of the primitive on a random input x in the i-th query. After getting a response, it measures the input wire to test if it gets the input back.



It is clear that when $\mathcal{D}_1$ interacts with the public interface of the real case (or f), it measures $|x\rangle$ with probability 1. This is because $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$. Since Sim_2 is perfect for $\mathcal{D}_1$, then $\mathcal{D}_1$ forces the simulator Sim_2 to have the following property.

Property 3. *For any $i \in [q]$ and $x \in X$, there exists an unitary $U_x^{(i)}$ such that for any $|\Psi\rangle \in V_{i-1}$, $y \in Y$:*

$$U^{(i)}|x,y,\Psi\rangle = |x\rangle \otimes U_x^{(i)}|y,\Psi\rangle,$$

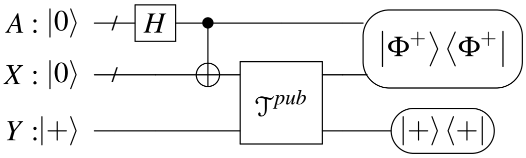
where $U^{(i)}$ is the unitary from Property 2.

Note that if a distinguisher interacts with the public interface of the construction (or f) and queries $|x\rangle_X |+\rangle_Y$, then it will get $|x\rangle_X |+\rangle_Y$ back from the construction. Then in the following, we present two class of distinguishers $\mathbb{D}_2$ and $\mathbb{D}_3$ that test if simulator do the same or not and of course a perfect simulator has to return $|x\rangle_X |+\rangle_Y$ back.

The class $\mathbb{D}_2$ of distinguishers:

$$\mathbb{D}_2 = \{\mathcal{D}_2^{(1)}, \ldots, \mathcal{D}_2^{(q)}\},$$

where for any $i \in [q]$, the distinguisher $\mathcal{D}_2^{(i)}$ (the i-th query) prepares an ancillary wire A and does the following:



where

$$|\Phi^+\rangle = \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle |x\rangle .$$

(In the circuit above, the Hadamard operation H is applied to each wire.) $\mathcal{D}_2^{(i)}$ measures if it gets back $|\Phi^+\rangle$ and $|+\rangle$ states in AX and Y wires, respectively.

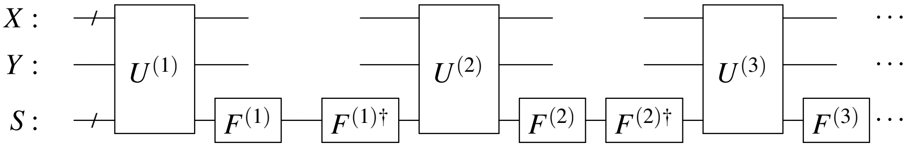
A simple calculation shows that if $\mathcal{D}_2^{(i)}$ interact with the public interface of the real case (or f), it measures $|\Phi^+\rangle$ and $|+\rangle$ with probability 1. Since Sim_2 is perfect for $\mathbb{D}_2$, the class $\mathbb{D}_2$ ensures that if the output register Y sets to $|+\rangle$ in any query, then the simulator has to return $|+\rangle$ in output wire. In other words, the inner state of the simulator is not entangled with input and output wires in this case. We can show that $\mathbb{D}_2$ is a class of distinguishers that forces Sim_2 to have the following property.

Property 4. *For any $i \in [q]$ and $|\Psi\rangle \in V_{i-1}$, there exists $|\Psi'\rangle$ such that*

$$\forall x : \ U_x^{(i)}(|+\rangle_Y \otimes |\Psi\rangle_S) = |+\rangle_Y \otimes |\Psi'\rangle_S ,$$

where $U_x^{(i)}$ is the unitary from Property 3.

Let Sim_3 be a simulator that is the same with Sim_2 except it applies a unitary operator $F^{(i)}$ that maps $|\Psi'\rangle$ to $|\Psi\rangle$ to the internal register in i-th query and, the inverse of $F^{(i)}$ before the $(i+1)$-th query. So, Sim_3 applies the operation $F^{(i-1)\dagger}U^{(i)}F^{(i)}$ in the i-th query where $F^{(0)} = I$ and $U^{(i)}$ is defined in Property 2.



Intuitively, since Sim_3 undoes the operator $F^{(i)}$, then it has all the properties so far and in addition it has the following property.

Property 5. *For any $i \in [q]$ and $|\Psi\rangle \in V_{i-1}$, $\forall x:$ $U_x^{(i)}(|+\rangle_Y |\Psi\rangle_S) = |+\rangle \otimes |\Psi\rangle$.*

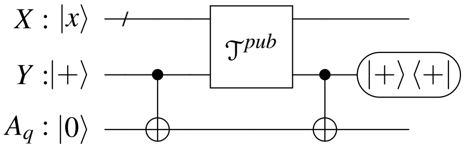
The class $\mathbb{D}_3$ of distinguishers. For any $i \in [q]$ and any distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$ that makes $i-1$ queries, let $\mathcal{D}_3^{(i)}(\mathcal{D}^{(i-1)})$ be a distinguisher that runs the distinguisher $\mathcal{D}^{(i-1)}$ and then additionally queries with $XY = |0\rangle |+\rangle$. The class $\mathbb{D}_3$ is consists of all such distinguishers.

Claim 3. *For any $i \in [q]$, $V_{i-1}^{\mathsf{Sim}_3} \subseteq V_i^{\mathsf{Sim}_3}$.*

Proof. Note that the state of simulator stays the same if distinguisher queries $|0\rangle_X |+\rangle_Y$ by Property 5, therefore we get every state in $V_i^{\mathsf{Sim}_3}$ using $\mathcal{D}_3$.

□

The class $\mathbb{D}_4$ of distinguishers. For any $i \in [q]$ and any distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$ that makes $i-1$ queries, let $\mathcal{D}_4^{(i)}(\mathcal{D}^{(i-1)})$ be an i-query distinguisher that prepares an ancillary wire A_q, queries the public interface of the construction for uniformly random x, and measures the outputs wire Y to see if it gets $|+\rangle$ back as follows:



A simple calculation shows that if $\mathcal{D}_4$ interacts with the public interface of the real case, it measures $|+\rangle$ with probability 1. Since Sim_3 is perfect for $\mathcal{D}_4$, then with probability 1 the measurement outputs $|+\rangle$ in the ideal case as well. Using this, we can show the following property for Sim_3.

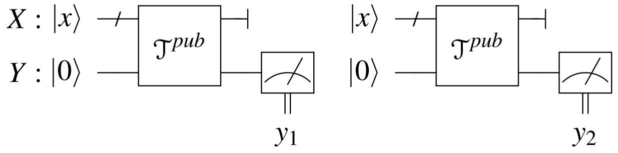
Property 6. *For any $i \in [q]$ and $|\Psi\rangle \in V_{i-1}$, and any x, $U_x^{(i)} |1\rangle_Y |\Psi\rangle = (X \otimes I_S) U_x^{(i)} |0\rangle_Y |\Psi\rangle$. Here X is the bitflip (Pauli X matrix).*

The following property can be concluded by Property 5 and Property 6.

Property 7. *For any $i \in [q]$, $|\Psi\rangle \in V_{i-1}$ and x, there are non-normalized $|\Psi_{x0}\rangle, |\Psi_{x1}\rangle$ such that:*

$$U_x^{(i)} |b\rangle |\Psi\rangle = |b\rangle |\Psi_{x0}\rangle + |\bar{b}\rangle |\Psi_{x1}\rangle \text{ and } |\Psi_{x0}\rangle + |\Psi_{x1}\rangle = |\Psi\rangle .$$

The class $\mathbb{D}_5$ of distinguishers. For any $i \in [q]$ and any distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$ that makes $i-1$ queries, let $\mathcal{D}_5^{(i+1)}(\mathcal{D}^{(i-1)})$ be an $(i+1)$-query distinguisher that runs $\mathcal{D}^{(i-1)}$ and queries the same input in two subsequent queries, i-th and $(i+1)$-th queries, and measures if their outputs are the same (checks if $y_1 = y_2$ in the following circuit).

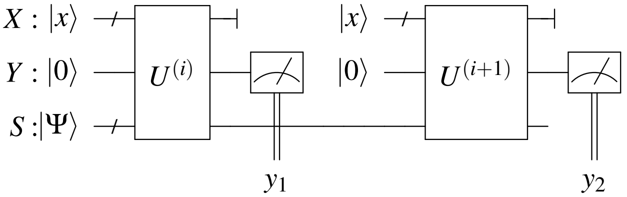


Using the distinguisher $\mathcal{D}_5$ and the previous properties, we can conclude:

Property 8. *For any $i \in [q]$, $x \in X$, and $|\Psi\rangle \in V_{i-1}$, the states $|\Psi_{x0}\rangle$ and $|\Psi_{x1}\rangle$ defined in Property 7 are orthogonal. In addition, for any x there exists a projector $P_x^{(i)}$ such that for any $|\Psi\rangle \in \mathsf{Span}\, V_{i-1}$, we have $U_x^{(i)} : |b\rangle |\Psi\rangle \mapsto |b\rangle P_x^{(i)} |\Psi\rangle + |1-b\rangle \overline{P_x^{(i)}} |\Psi\rangle$ where $\overline{P_x^{(i)}} := I - P_x^{(i)}$.*

Claim 4. Sim_3 *has the Property 8.*

Proof. We depict the distinguisher above in the ideal case:



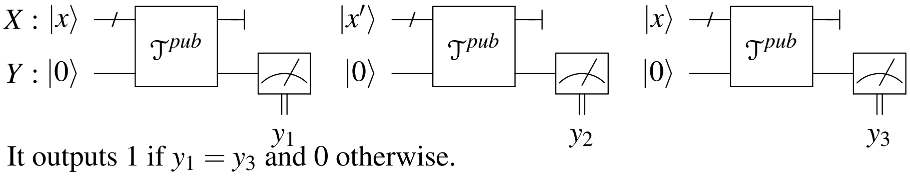
Intuitively, we show that the second measurement can distinguish $|\Psi_{x0}\rangle$ and $|\Psi_{x1}\rangle$ defined in Property 7 perfectly and therefore they are orthogonal and consequently we can write $U_x^{(i)} : |b\rangle |\Psi\rangle \mapsto |b\rangle P_x^{(i)} |\Psi\rangle + |1-b\rangle \overline{P_x^{(i)}} |\Psi\rangle$ where $\overline{P_x^{(i)}} := I - P_x^{(i)}$. □

In the following, we show that the projectors defined in Property 8 will pairwise commute.

Property 9. *For any $i \in [q]$, $|\Psi\rangle \in \mathsf{Span}\, V_{i-1}$, and $x \in X$, $P_x^{(i)} |\Psi\rangle = P_x^{(i+1)} |\Psi\rangle$, where $P_x^{(i)}$ and $P_x^{(i+1)}$ are the projectors from Property 8.*

Proof. This also can be proven by the distinguisher $\mathcal{D}_5$. □

The class $\mathbb{D}_6$ of distinguishers. For any $i \in [q-1]$ and any distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$ that makes $i-1$ queries, let $\mathcal{D}_6^{(i+2)}(\mathcal{D}^{(i-1)})$ be an $(i+2)$-query distinguisher that runs $\mathcal{D}^{(i-1)}$, then makes three subsequent queries as follows.



It outputs 1 if $y_1 = y_3$ and 0 otherwise.

Using the distinguisher $\mathcal{D}_6$, we can conclude the following property. The following property is needed to prove the Lemma 9 that is crucial to prove the Property 11 that states the commutativity property for the projectors over a subspace.

Property 10. *For any $i \in [q-2]$, $|\Psi\rangle \in V_{i-1}$ and x, x', $\overline{P_x^{(i+2)}} P_{x'}^{(i+1)} P_x^{(i)} |\Psi\rangle = 0$ and $P_x^{(i+2)} P_{x'}^{(i+1)} \overline{P_x^{(i)}} |\Psi\rangle = 0$.*

Lemma 9. *Let P and Q be rank-one projectors over a two dimensional Hilbert space $\mathcal{H}$ such that for any $|\Psi\rangle \in \mathcal{H}$, $\bar{Q}PQ|\Psi\rangle = 0$ and $QP\bar{Q}|\Psi\rangle = 0$. Then, P and Q commute on $\mathcal{H}$, i.e, $\forall\ |\Psi\rangle \in \mathcal{H},\ PQ|\Psi\rangle = QP|\Psi\rangle$.*

Proof. The proof is straightforward by writing $P = |\alpha\rangle\langle\alpha|$ and $Q = |\beta\rangle\langle\beta|$ for some normalized vectors $|\alpha\rangle$ and $|\beta\rangle$. Then using the assumption $\bar{Q}PQ|\Psi\rangle = 0$ and $QP\bar{Q}|\Psi\rangle = 0$. □

Property 11. *For any $i \in [q-2]$, $|\Psi\rangle \in V_{i-1}$, x, x': $P_{x'}^{(i+1)}P_x^{(i)}|\Psi\rangle = P_x^{(i+1)}P_{x'}^{(i)}|\Psi\rangle$.*

Proof. The proof uses Jordan's Lemma [49] that says two orthogonal projectors are simultaneously block diagonalizable with block of size ≤ 2 and then the commutativity property follows from Lemma 9. □

Corollary 1. *For any $|\Psi\rangle \in \mathsf{Span}\, V_{q-3}^{\mathsf{Sim}_3}$, x, x': $P_{x'}^{(q-1)}P_x^{(q-1)}|\Psi\rangle = P_x^{(q-1)}P_{x'}^{(q-1)}|\Psi\rangle$.*

Proof. By Property 11 and Property 9, it is clear that for any $|\Psi\rangle \in V_{q-3}^{\mathsf{Sim}_3}$, x, x': $P_{x'}^{(q-1)}P_x^{(q-1)}|\Psi\rangle = P_x^{(q-1)}P_{x'}^{(q-1)}|\Psi\rangle$. The result follows by the linearity of $P_x^{(q-1)}$. □

Conjecture 1. *Let $\mathcal{V}$ be a strict subspace of Hilbert space $\mathcal{H}$. Let $\{P_x\}_{x\in X}$ be a family of orthogonal projectors such that*

$$\forall|\Psi\rangle \in \mathcal{V},\ x \neq x' \in X, P_xP_{x'}|\Psi\rangle = P_{x'}P_x|\Psi\rangle.$$

Then, there exists a family of projectors $\{\hat{P}_x\}_{x\in X}$ such that

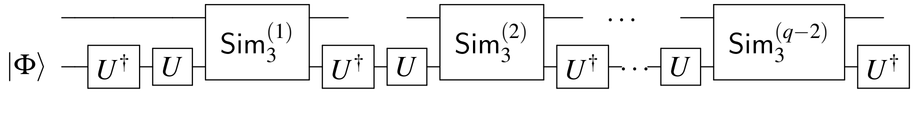
1. *For any $|\Psi\rangle \in \mathcal{V}$ and $x \in X$, $\hat{P}_x|\Psi\rangle = P_x|\Psi\rangle$.*
2. *$\forall|\Psi\rangle \in \mathcal{H},\ x \neq x' \in X,\ \hat{P}_x\hat{P}_{x'}|\Psi\rangle = \hat{P}_{x'}\hat{P}_x|\Psi\rangle$.*

Now using the conjecture above and the Corollary 1, there is a family of projectors $\{\hat{P}_x^{(q-1)}\}_{x\in X}$ such that it has the following two properties.

1. For any $|\Psi\rangle \in \mathsf{Span}\, V_{q-3}^{\mathsf{Sim}_3}$, $\hat{P}_x^{(q-1)}|\Psi\rangle = P_x^{(q-1)}|\Psi\rangle$.
2. Projectors in $\{\hat{P}_x^{(q-1)}\}_{x\in X}$ pairwise commute everywhere.

Claim 5. *There exists a perfect simulator Sim_6 for $\mathbb{D}$ such that it chooses a classical value s in the first invocation according to some probability distribution μ^H. It then applies some unitary $U_{\mathsf{Sim}_6}|x,y\rangle = |x\rangle \otimes U_x^s|y\rangle$ in every query.*

Proof. Since the projectors $\{\hat{P}_x^{(q-1)}\}_{x\in X}$ pairwise commute, they are simultaneously unitarily diagonalizable [45], that is, there exists an unitary matrix U such that $U^\dagger\hat{P}_x^{(q-1)}U$ is diagonal for any $x \in X$. We define $\mathsf{Sim}_4^{(1)} := (I_{XY} \otimes U^\dagger)\mathsf{Sim}_3^{(1)}$ and for $2 \leq i \leq q-2$, $\mathsf{Sim}_4^{(i)} := (I_{XY} \otimes U^\dagger)\mathsf{Sim}_3^{(i)}(I_{XY} \otimes U)$. The simulator Sim_4 is depicted in the following circuit.



where for any x,y and $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$,

$$\mathsf{Sim}_3^{(i)} |x,y,\Psi\rangle := |x\rangle \otimes U_x^{(i)} |y,\Psi\rangle = |x\rangle \otimes \big(|y\rangle P_x^{(i)} |\Psi\rangle + |\bar{y}\rangle \bar{P}_x^{(i)} |\Psi\rangle\big).$$

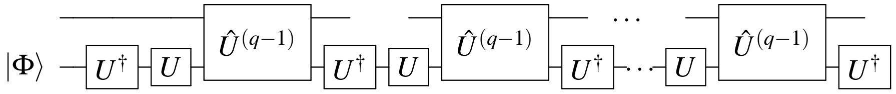
By definition of Sim_4, it is clear that Sim_4 is perfect for $\mathcal{D}_{cl}$. Let $\hat{U}^{(q-1)}$ be the following unitary:

$$\hat{U}^{(q-1)} |x,y,\Psi\rangle := |x\rangle \otimes \hat{U}_x^{(q-1)} |y,\Psi\rangle = |x\rangle \otimes \big(|y\rangle \hat{P}_x^{(q-1)} |\Psi\rangle + |\bar{y}\rangle \bar{\hat{P}}_x^{(q-1)} |\Psi\rangle\big).$$

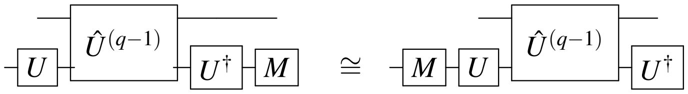
By Property 4 and Property 8, for any $i \in [q-2]$ and $|\Psi\rangle \in \mathsf{Span}\, V_{i-1}^{\mathsf{Sim}_3}$, $P_x^{(i)} |\Psi\rangle = P_x^{(q-1)} |\Psi\rangle$ and by Conjecture 1, $P_x^{(q-1)} |\Psi\rangle = \hat{P}_x^{(q-1)} |\Psi\rangle$ therefore we can conclude that

$$\forall\, x,y,\ \forall\ |\Psi\rangle \in \mathsf{Span}\, V_{i-1}^{\mathsf{Sim}_3} :\ \mathsf{Sim}_3^{(i)} |x,y,\Psi\rangle = \hat{U}^{(q-1)} |x,y,\Psi\rangle\,. \tag{3.2}$$

Let Sim_5 be the same with Sim_4 except it applies the unitary $\hat{U}^{(q-1)}$ instead of $\mathsf{Sim}_3^{(i)}$ in each query:



By Equation 3.2, it is clear that Sim_5 fulfils Property 1. Now since $U^\dagger \prod\limits_{x \in X} \hat{P}_x^{(q-1)} U$ is diagonal, we show a complete measurement in computational basis on S-register at the end of the circuit above can be moved to the beginning of the circuit (right after $U^\dagger$). To show that, we prove that the following two circuits output the same result:



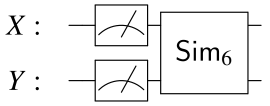
Let $M_j := |j\rangle\langle j|$ be the measurement operator corresponding to the outcome j. We start with the circuit in the left side. For any x,y and $|\Psi\rangle$:

$$\begin{aligned}
&(I_{XY} \otimes M_j)(I_{XY} \otimes U^\dagger)\hat{U}^{(q-1)}(I_{XY} \otimes U)\,|x,y,\Psi\rangle \\
&\quad = (I_{XY} \otimes M_j)(I_{XY} \otimes U^\dagger)\hat{U}^{(q-1)}\big(|x,y\rangle \otimes U\,|\Psi\rangle\big) \\
&\quad = (I_{XY} \otimes M_j)(I_{XY} \otimes U^\dagger)\big(|x\rangle \otimes \hat{U}_x^{(q-1)}(|y\rangle \otimes U\,|\Psi\rangle)\big) \\
&\quad = (I_{XY} \otimes M_j)(I_{XY} \otimes U^\dagger)\big(|x\rangle \otimes (|y\rangle \otimes \hat{P}_x^{(q-1)} U\,|\Psi\rangle + |\bar{y}\rangle \otimes \bar{\hat{P}}_x^{(q-1)} U\,|\Psi\rangle)\big) \\
&\quad = |x\rangle \otimes (|y\rangle \otimes M_j U^\dagger \hat{P}_x^{(q-1)} U\,|\Psi\rangle + |\bar{y}\rangle \otimes M_j U^\dagger \bar{\hat{P}}_x^{(q-1)} U\,|\Psi\rangle) \\
&\quad \overset{(*)}{=} |x\rangle \otimes (|y\rangle \otimes U^\dagger \hat{P}_x^{(q-1)} U M_j\,|\Psi\rangle + |\bar{y}\rangle \otimes U^\dagger \bar{\hat{P}}_x^{(q-1)} U M_j\,|\Psi\rangle) \\
&\quad = (I_{XY} \otimes U^\dagger)\big(|x\rangle \otimes (|y\rangle \otimes \hat{P}_x^{(q-1)} U M_j\,|\Psi\rangle + |\bar{y}\rangle \otimes \bar{\hat{P}}_x^{(q-1)} U M_j\,|\Psi\rangle)\big) \\
&\quad = (I_{XY} \otimes U^\dagger)\big(|x\rangle \otimes \hat{U}_x^{(q-1)}(|y\rangle \otimes U M_j\,|\Psi\rangle)\big) \\
&\quad = (I_{XY} \otimes U^\dagger)\hat{U}^{(q-1)}(I_{XY} \otimes U)(I_{XY} \otimes M_j)\,|x,y,\Psi\rangle\,,
\end{aligned}$$

where $(*)$ holds because $U^\dagger \hat{P}_x^{(q-1)} U$, $U^\dagger \bar{\hat{P}}_x^{(q-1)} U$ and M_j are diagonal. We have proven that the (non-normalized) post-measurement state corresponding to outcome j is the same in two circuit. This also shows that the probability of getting output j is the same in two circuits. Therefore the measurement can be moved to the beginning of the circuit right after $U^\dagger$ and the output of the circuit stays the same. Let Sim_6 be a simulator that measures the inner state in the computational basis right after applying $U^\dagger$. (Sim_6 is the same with Sim_5 except the measurement has been moved to the beginning.) By the construction, Sim_6 has *Property* 1. Therefore, the inner state of the simulator collapses to a classical value s. □

Claim 6. *There exists a stateless classical simulator* Sim_8 *that is perfect for* $\mathcal{D}_{cl}$*. That is* Sim_8 *chooses a random function* $f : X \to \{0,1\}$ *at the beginning and answers to any query on input* x *by* $f(x)$*.*

Proof. Let Sim_7 be a simulator that upon receiving a query from the distinguisher, measures the input and output wires in the computational basis measurement and then invokes Sim_6 (or forwards the input and output wire to Sim_6).



It is clear that for any distinguisher $\mathcal{D}$ that makes classical queries, the circuit above is indistinguishable from Sim_6. Let Sim_8 be a classical simulator that upon receiving a classical query on input x, invokes Sim_7 on input $|x,0\rangle$ to get the answer $\mathsf{Sim}_7 |x,0\rangle = U_{\mathsf{Sim}_6} |x,0\rangle = |x\rangle \otimes U_x^s |0\rangle = |x\rangle \otimes |y'\rangle$. It then returns the output y' to the distinguisher. We define $f(x) := y'$. Since U_x^s only depends on the values s and x, then this is equivalent to saying that Sim_8 chooses a function $f : X \to \{0,1\}$ at the beginning and answers to any query on input x by $f(x)$. □

3.2.2. Discussion on the Conjecture

This subsection is based on a public communication with the mathematics community [1]. The following lemma prove that the conjecture holds for two projectors.

Lemma 10. *Let P and Q be two orthogonal projectors over Hilbert space $\mathcal{H}$ such that they commute over a strict subspace $\mathcal{V} < \mathcal{H}$. There are two projectors $\hat{P}$ and $\hat{Q}$ such that they commute over $\mathcal{H}$ and for all $|\Psi\rangle \in \mathcal{V}$,*

$$\hat{P}|\Psi\rangle = P|\Psi\rangle \text{ and } \hat{Q}|\Psi\rangle = Q|\Psi\rangle .$$

Proof. Poof follows using Halmos' two projections theorem [25]. Let $\operatorname{Im} P := L$ and $\operatorname{Im} Q := N$. We can decompose $\mathcal{H}$ as

$$\mathcal{H} = (L \cap N) \oplus (L \cap N^\perp) \oplus (L^\perp \cap N) \oplus (L^\perp \cap N^\perp) \oplus (M_1 \oplus M_2).$$

Halmos's theorem says that M_1 is nontrivial iff M_2 is nontrivial and if one of them is nontrivial, then we can write

$$P = (I, I, 0, 0) \oplus U^\dagger \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix} U,$$

$$Q = (I, 0, I, 0) \oplus U^\dagger \begin{pmatrix} I-H & W \\ W & H \end{pmatrix} U,$$

where $U = \mathrm{Diag}(I, R)$, $W = \sqrt{H(I-H)}$, $R : M_2 \to M_1$ is a unitary operator and $H : M_1 \to M_1$ is a selfadjoint operator such that $0 \le H \le I$ and $\mathrm{Ker} H = \mathrm{Ker}(I - H) = \{0\}$. For any $|\Psi\rangle \in \mathcal{V}$, let $|\psi_1\rangle \in M_1$ and $|\psi_2\rangle \in M_2$ be the last components of $|\Psi\rangle$. A simple calculation shows that

$$QP|\Psi\rangle = \begin{pmatrix} (I-H)|\psi_1\rangle \\ R^\dagger W|\psi_1\rangle \end{pmatrix} \text{ and } PQ|\Psi\rangle = \begin{pmatrix} (I-H)|\psi_1\rangle + WR|\psi_2\rangle \\ 0 \end{pmatrix}$$

where we only consider the operation over two last components of $|\Psi\rangle$. Since P and Q commute over $\mathcal{V}$ we can conclude

$$R^\dagger W|\psi_1\rangle = 0 \text{ and } WR|\psi_2\rangle = 0,$$

and from this we can obtain $|\psi_1\rangle = |\psi_2\rangle = 0$. This means that $\mathcal{V}$ is contained in the sum of first four expressions. We consider projectors $\hat{P}$ and $\hat{Q}$ that are modification of P and Q by replacing $M_1 \oplus M_2$ with zero. □

It is not clear how one can generalize this proof idea to more than two projectors to prove the Conjecture 1. In order to prove the Conjecture 1 for three projectors P_1, P_2 and P_3, one idea will be to use the lemma to obtain projectors $\hat{P}_1$ and $\hat{P}_2$ that commute everywhere and operate the same as P_1 and P_2 on $\mathcal{V}$. Then we may use the lemma again for $\hat{P}_i$ (for an $i \in [2]$) and P_3, however, we can not apply the lemma because it is not clear if $\hat{P}_i$ and P_3 commute on $\mathcal{V}$. Another idea would be to apply the lemma to pairs (P_1, P_2), (P_2, P_3) and (P_3, P_1) to obtain projectors $(\hat{P}_1, \hat{P}_2)$, (P_2', P_3') and $(\bar{P}_3, \bar{P}_1)$, respectively. But it is not clear if three of transformed projectors have the properties stated in the Conjecture.

3.2.3. The Impossibility Results

In the following, we present the description of $\mathcal{D}_{cl}$. We argue that $\mathcal{D}_{cl}$ can distinguish $(\mathcal{C}[f], f)$ from $(H, \mathsf{Sim}_{sl}(H))$. This shows that any constructions that is not perfectly indifferentiable from the real case with respect to classical stateless simulators is not perfectly quantum indifferentiable by Theorem 7.

Construction of $\mathcal{D}_{cl}$. The distinguisher $\mathcal{D}_{cl}$ that wants to distinguish $(\mathcal{C}[f], f)$ from $(H, \mathsf{Sim}(H))$ picks a random element x from the domain. Then it evaluates $\mathcal{C}[f](x)$ without querying x to the public interface of the construction and only using queries to f (this is possible since the construction has been built from f). We call this value y. Then it queries x to the public interface of the construction to get $\mathcal{C}[f](x)$. Finally, it outputs 1 if $y = \mathcal{C}[f](x)$ and 0 otherwise. It is clear that in the real case, when $\mathcal{D}_{cl}$ interacts with $(\mathcal{C}[f], f)$, the output of $\mathcal{D}_{cl}$ is 1 with probability 1.

Argument on impossibility results. In the ideal case, the simulator has access to the H and answers to the queries that distinguisher makes to f. Since the simulator is stateless, it chooses a function f at the beginning (before any query has been made to f) and according to some distribution that can depend on H and answers to the distinguisher queries using f. Intuitively, since H is a random primitive with larger domain and co-domain compare to f, then a stateless simulator that does not record the list of queries can not simulate a bigger function with a smaller one. So, any constructions that is not perfectly indifferentiable from the real case limited to classical stateless simulator is not perfectly quantum indifferentiable as well. For instance, Sponge Construction [16] and Feistel Networks [53].

3.3. Discussion: Open Problems and Related Works

Indifferentiability is a well-studied notion for cryptographic constructions in the classical setting. We initiate the study of Indifferentiability notion in the quantum setting. We study the quantum indifferentiability notion with respect to a perfect simulator. We show the impossibility of quantum indifferentiability notion with respect to a perfect simulator for many classical constructions of hash functions under a conjecture. Proving or rejecting our conjecture is an interesting open problem. The main challenge in proving the quantum indifferentiability of a construction from an ideal primitive is the incapability of a quantum simulator to record quantum queries. In the classical setting, the simulator can record list of queries to the underlying function f used in the construction $\mathcal{C}[f]$. Then the simulator can respond to queries to the construction $\mathcal{C}[f]$ by looking at the list of queries to f to guarantee the consistency of responses to f and $\mathcal{C}[f]$ queries. Concurrently, Zhandry [76] presents a technique to record quantum queries. He uses the technique to prove the quantum indifferentiability of the Merkle-Damgård construction. Our impossibility result remains unaffected by Zhandy's work because we show the impossibility with respect to a perfect simulator. There are many open questions in this realm. For instance, the indifferentiability of Sponge construction and Feistel construction with respect to a non-perfect simulator is open.

4. QUANTUM COLLISION FOR NON-UNIFORMLY DISTRIBUTED FUNCTIONS

4.1. Motivation

Hash functions are crucial cryptographic primitives that are used to construct many encryption schemes and cryptographic schemes. They usually compress a large input to a smaller output. In many applications, collision-resistance is a vital property for a cryptographic hash function. A collision for a hash function H is a pair of two distinct inputs that map to the same output under the hash function, that is, $x \neq x'$ such that $H(x) = H(x')$. Since it is mainly the case that the input size of a hash function is much larger than its output size, a collision is inevitable, however, the design of the hash function has to guarantee that the hash function is collision resistant. In other words, it has to be computationally infeasible to find a collision.

As we move toward the quantum era, we have to prove it is computationally hard to find a collision using a quantum computing device. This is formulated as a quantum query complexity problem, that is, how many quantum queries to the hash function are needed in order to find a collision with constant probability. This gives us a lower bound on the required number of queries to solve the collision problem. The other question is to present a quantum algorithm that solves the collision problem using certain number of queries. This gives us an upper bound on the sufficient number of queries to solve the collision problem.

Usually, hash functions are modelled as random functions in the random oracle model [14] to achieve provable secure schemes. It is easier to prove the security of the scheme if we model the underlying hash function as a random function. It has been proven in [75] that a random function is quantum collision-resistant. However in some cryptographic constructions, they are composed with other functions and the security of the construction relies on the collision resistance property of the composition. Therefore the output of combination of a function f and a random function H may not be distributed uniformly and finding a collision for this non-uniformly distributed $f \circ H$ may break the security of the scheme. For example, the well-known Fujisaki-Okamoto construction [42] uses a random function H to produce the randomness for an encryption scheme f. The security relies on the fact that the adversary can not find two inputs of the random function that lead to the same ciphertext. This is roughly equivalent to saying that $f \circ H$ is collision resistant. In fact, our result is a crucial ingredient for analyzing a variant of Fujisaki-Okamoto construction in the quantum setting. See Chapter 5 for more details.

Lower bound			Upper bound		
Quantifier	$H_\infty(\mathcal{D})$	$H_2(\mathcal{D})$	Quantifier	$H_\infty(\mathcal{D})$	$H_2(\mathcal{D})$
$\forall\,\mathcal{A}\,\forall\,\mathcal{D}$	$\Omega(2^{H_\infty(\mathcal{D})/5})$	$\Omega(2^{H_2(\mathcal{D})/9})$	$\exists\,\mathcal{A},\,\exists\,\mathcal{D}$	$O(2^{H_\infty(\mathcal{D})/3})$	$O(2^{H_2(\mathcal{D})/4})$
$\exists\,\mathcal{D}\,\forall\,\mathcal{A}$	$\mathbf{\Omega(2^{\frac{H_\infty(\mathcal{D})}{2}})}$	$\Omega(2^{\frac{H_2(\mathcal{D})}{3}})$	$\forall\,\mathcal{D}\,\exists\,\mathcal{A}$	$\mathbf{O(2^{\frac{H_\infty(\mathcal{D})}{2}})}$	$O(2^{\frac{H_2(\mathcal{D})}{4}})$
$\forall\,\mathcal{A}\,\exists\,\mathcal{D}$	$\Omega(2^{\frac{H_\infty(\mathcal{D})}{2}})$	$\mathbf{\Omega(2^{\frac{H_2(\mathcal{D})}{3}})}$	$\exists\,\mathcal{A}\,\forall\,\mathcal{D}$	$O(2^{\frac{2H_\infty(\mathcal{D})}{3}})$	$\mathbf{O(2^{\frac{H_2(\mathcal{D})}{3}})}$

Table 1: Summary of the bounds achieved in this Chapter. The columns marked $H_\infty(\mathcal{D})$, $H_2(\mathcal{D})$ give lower/upper bounds on the number of queries needed for finding a collision in terms of the min-entropy and the collision-entropy, respectively. The "quantifier" column indicates for what quantification of collision-finding algorithm $\mathcal{A}$ and distribution $\mathcal{D}$ the respective bound is achieved. For example, a lower bound $\Omega(B)$ with quantifiers $\forall\mathcal{A}\,\exists\mathcal{D}$ means that for any adversary $\mathcal{A}$, there exists a distribution $\mathcal{D}$ such that $\mathcal{A}$ needs at least $\Omega(B)$ queries to find a collision.

4.2. Our Contribution

We study the quantum query complexity of finding a collision for a function f whose outputs are chosen according to a non-uniform distribution $\mathcal{D}$. We derive some upper bounds and lower bounds depending on the min-entropy and collision-entropy of $\mathcal{D}$ that are denoted by $H_\infty(\mathcal{D})$ and $H_2(\mathcal{D})$, respectively. Table 1 summarizes our results.

We study the problem for two entropy measures that are mostly occurred in cryptographic context, namely, collision-entropy and min-entropy. We present twelve bounds (see Table 1) that contains all possible quantifiers. The motivation for different quantifiers can be:

- $\forall\mathcal{A}\forall\mathcal{D}$. This is motivated by some cryptographic use cases. We may encounter a cryptosystem that is insecure if a quantum algorithm finds a collision for a non-uniformly distributed function f. Then, in order to claim the security of cryptosystem, we need to show that for any quantum adversary $\mathcal{A}$ and any distribution $\mathcal{D}$ the necessary number of queries to find a collision for a random function f whose outputs are chosen independently according to $\mathcal{D}$ is large. For instance, in Chapter 5, we show the security of FO construction using our result in the row marked $\forall\mathcal{A}\forall\mathcal{D}$ and column marked $H_\infty(\mathcal{D})$.
- $\forall\mathcal{D}\,\exists\mathcal{A}$. We may be motivated from the algorithmic point of view. Namely, we might be interested to give an quantum algorithm that finds a collision for a random function whose outputs are chosen according to a distribution $\mathcal{D}$ with a specific entropy measure. In this case, the algorithm can be dependent on the distribution $\mathcal{D}$. This kind of bounds are needed to compare the quantum computing power with classical computing for a specific problem.
- $\exists\mathcal{A}\forall\mathcal{D}$. We might be interested in a quantum algorithm that finds a collision and it is universal for any distribution with specific entropy measures. In the previous case, the quantum algorithm can be dependent on the dis-

tribution. In contrast, in this case we are interested to give a quantum algorithm that is universal and works for any distribution with a known entropy measure.

Remaining quantifiers. In each item above, we are interested to know if our bound is tight or not. Therefore, we study the negation of the aforementioned quantifiers. We make the tight bounds bold in the Table 1.

4.2.1. Proof Overview for Upper Bounds

We present the sketch of the proofs for the bounds that are more challenging and an interested reader may refer to [63] to find the proofs of other bounds. The core idea of the proofs for upper bounds is to use Grover's search algorithm [21,43], Ambainis' element distinctness algorithm [9] and Theorem 6 in [75] as a black box. In the following, we present the proof for the upper bound for two cases.

Quantifier order $\exists\ \mathcal{A}\ \exists\ \mathcal{D}$ and the collision-entropy. The idea is to use Grover's search algorithm [21,43] to find a collision. To do that, we need to define a distribution $\mathcal{D}$ with $H_2(\mathcal{D}) \geq k$ such that one of the elements in the support of $\mathcal{D}$ (the target element that Grover's algorithm would search for its pre-image) occurs with considerably high probability and other elements of the support occur with relatively small probability. Therefore, we define a distribution $\mathcal{D}$ such that $\mathcal{D}(0) = 1/2^{(k+1)/2} := \gamma$ and it is an uniform distribution over non-zero elements. We show the bound for $f \leftarrow \mathcal{D}^{\mathbb{N}}$ where $\mathbb{N}$ is the set of natural numbers. We choose a subset N_1 of size $\lceil 2/\gamma \rceil$ from $\mathbb{N}$. Then we use Chernoff inequality, Theorem 4.5 in [55], to show that there exists at least one pre-image of 0 in N_1 with high probability. Now, Grover's algorithm [21,43] applied to $f\restriction_{N_1}$ returns a pre-image of 0 using $O(\sqrt{|N_1|})$ queries with constant probability. We choose a subset N_2 of size $\lceil 2/\gamma \rceil$ from $\mathbb{N} \setminus N_1$ and apply Grover's algorithm to $f\restriction_{N_2}$ to obtain another pre-image of 0 and this finishes our proof.

Quantifier order $\exists\ \mathcal{A}\ \forall\ \mathcal{D}$ and the collision entropy. The proof follows by the reduction technique used in [3,75] and using Ambainis's algorithm [9] for the element distinctness as a black box. Let S be a random subset of $\mathbb{N}$ of size $2^{k/2}+1$. By Theorem 3 in [72], $f' := f|_S$ has at least one collision with probability at least $1-2/e$. Now, invoking Ambainis's algorithm [9] for f' returns a collision with bounded error. The query complexity of Ambainis's algorithm is $O(|S|^{2/3}) = O(2^{k/3})$. By repeating this procedure on distinct subset of the domain of f, we can amplify the success probability arbitrary close to 1.

4.2.2. Proof Overview for Lower bounds

Our result are stated in the from of an upper bound for the success probability of an adversary making q queries. We present these bounds in Table 2. The lower

Upper bound for the Success Probability Using q Queries		
Quantifier	$H_\infty(\mathcal{D}) \geq k$	$H_2(\mathcal{D}) \geq k$
$\forall\, \mathcal{A}\, \forall\, \mathcal{D}$	$O\Big(\frac{q^{5/2}}{2^{k/2}}\Big)$	$O\Big(\frac{q^{9/5}}{2^{k/5}}\Big)$
$\exists\, \mathcal{D}\, \forall\, \mathcal{A}$	$O\Big(max\{\frac{q^2}{2^k}, \frac{q^3}{2^{3k/2}}\}\Big)$	$O\Big(\frac{q^3}{2^k}\Big)$
$\forall\, \mathcal{A}\, \exists\, \mathcal{D}$	$O\Big(max\{\frac{q^2}{2^k}, \frac{q^3}{2^{3k/2}}\}\Big)$	$O\Big(\frac{q^3}{2^k}\Big)$

Table 2: An upper bound for the probability of finding a collision using q queries have been presented in this table. For instance, for any quantum adversary ($\forall \mathcal{A}$) that makes q queries and for any distribution $\mathcal{D}$ ($\forall\, \mathcal{D}$) with $H_\infty \geq k$, the success probability of finding a collision is less than or equal to $O\Big(\frac{q^{5/2}}{2^{k/2}}\Big)$.

bounds in Table 1 can be derived from the upper bound on the success probabilities stated in Table 2.

High-level idea of reduction proof. Since the collision problem is hard for a uniformly at random function [75], we reduce the quantum collision problem for non-uniformly at random function to a uniformly at random function as follows. In a very high level, the reduction proof is constructing a quantum adversary B that finds a collision for a uniformly at random function f from a quantum adversary A that finds a collision for a non-uniformly at random function h. So basically, B runs A and has to simulate the function h using his oracle f. The simulation of f by B follows the similar line as the classical proofs, namely, B has to answer to A's queries in such a way that is indistinguishable from A's point of view. To do that, B (using his oracle h) has to come up with a function f' that its outputs are distributed as f (classically). Then $U_{f'}$ is indistinguishable from U_f from A's point of view. The last point to check is that the output of A (that is a collision for h) has to be a collision for target function f. Since it is hard to find a collision for f, we conclude that it is hard to find a collision for non-uniformly at random function h.

We present the high-level proof of quantifier order $\exists\, \mathcal{D}\ \forall \mathcal{A}$ and the proofs for "every adversary and every distribution" quantifier that are more challenging for both the collision-entropy and the min-entropy.

Quantifier order $\exists \mathcal{D} \forall \mathcal{A}$ and min-entropy. We present the proof for "there exists a distribution $\mathcal{D}$ of min-entropy k and any adversary $\mathcal{A}$ making q queries". We define a distribution $\mathcal{D}$ over $\{0,1\}^n \cup \{a\}$ such that $\mathcal{D}(a) = 1/2^k$ and $\mathcal{D}(y) = (1-1/2^k)/2^n$ for $y \in \{0,1\}^n$. Let $\mathcal{A}$ be a quantum adversary that makes q queries to $f \leftarrow \mathcal{D}^X$ and outputs a collision with probability ε. There are two cases:

- $\mathcal{A}$ finds two pre-images of the element "a". Let say with probability ε_1
- $\mathcal{A}$ finds $x \neq x'$ such that $f(x) = f(x') \neq a$. Let say with probability ε_2

Note that we can write $\varepsilon = \varepsilon_1 + \varepsilon_2$. Then, we obtain some upper bounds for ε_1

and ε_2. Since $\mathcal{D}$ over $\{0,1\}^n$ is a distribution close to a uniformly at random distribution, we can reduce it to the collision problem for a uniformly at random function and obtain the upper bound $\varepsilon_2 \leq \frac{C(q+2)^3}{2^n}$ using Lemma 1 in Section 2.3. To conclude an upper bound for ε_2, we construct an adversary $\mathcal{B}$ that runs $\mathcal{A}$ and using the output of $\mathcal{A}$ distinguishes a zero-function from a function that outputs 1 with probability $1/2^k$ and outputs zero otherwise. Then, using Lemma 3 in Section 2.3 we can conclude $\varepsilon_1 \leq 8(2q+2)^2/2^k$. Finally, when $n \geq 3k/2$ we can conclude

$$\varepsilon \leq O\Big(max\{\frac{q^2}{2^k}, \frac{q^3}{2^{3k/2}}\}\Big).$$

Lower bound based on collision-entropy. We would prove that if there exists a quantum adversary that outputs a collision for $f \leftarrow \mathcal{D}^X$, then we can construct a quantum adversary $\mathcal{B}$ that finds a collision for $h \circ f$ in which h is a universal hash function. Since by the Leftover Hash Lemma [46], $h \circ f$ is indistinguishable from a truly random function, we can conclude that $h \circ f$ is collision-resistant simply because a truly random function is collision-resistant [75]. Therefore, we have shown that f is collision-resistant. The proof procedure is as follows. Let f be a random function whose outputs are chosen independently according to a distribution with collision-entropy k. We apply the Leftover Hash Lemma [46] to the function f to extract the number of bits that are indistinguishable from uniformly random bits. After applying the Leftover Hash Lemma, the output distribution of $h \circ f$, where h is a universal hash function, is indistinguishable from the uniform distribution. Note that a collision for function f is a collision for $h \circ f$. Let A be a quantum adversary that has quantum access to f and finds a collision for $h \circ f$. Using the existence of A, we show that there exists a quantum algorithm B that has quantum access to $h \circ f$ and finds a collision for $h \circ f$ with the same probability and the same number of queries as algorithm A. By [74], two distribution are indistinguishable if and only if they are oracle-indistinguishable. Therefore, $h \circ f$ is indistinguishable from a random function (recall that the output of $h \circ f$ is indistinguishable from the uniform distribution by Leftover Hash Lemma) and as a result any quantum algorithm B is unable to differentiate between $h \circ f$ and a random function. This means that the success probability of finding a collision for $h \circ f$ has to be close to the success probability of finding a collision for a random function otherwise a collision finding algorithm can distinguish the two cases. By using an existing result for finding a collision for a random function [75], we obtain an upper bound for the probability of finding a collision for function $h \circ f$. Therefore, we get an upper bound for the probability of success for the quantum collision problem applied to the function f.

Lower bound based on min-entropy. Since every distribution with min-entropy k can be written as a convex combination of some flat distributions on a subset of size at least $\{0,1\}^k$ [31], one can obtain a lower bound for the quantum collision problem for a function $f \leftarrow \mathcal{D}^X$ by reducing the quantum collision problem for f to the quantum collision problem for an uniformly distributed function and use the existing result on collision-resistance of random functions [75]. In more details, assume that the distribution $\mathcal{D}$ is written as convex combination of the flat distributions $\mathcal{D}_1, \ldots, \mathcal{D}_N$. One can use a reduction algorithm that converts a quantum algorithm $\mathcal{A}$ that finds a collision for f to a quantum algorithm that finds a collision for at least one of $f_i \leftarrow \mathcal{D}_i^X$. However, the final bound might be the multiplication of N to the existing bound for a random function, i.e, $O(N(q+2)^3/2^k)$, and that bound is not suitable when N is exponentially large. To circumvent this problem, we write the distribution $\mathcal{D}$ as a convex combination of some nearly flat distributions $\mathcal{D}_i$ for $i = k, \ldots, m$ where the value of m will be fixed at the end of proof. For $i = k, \ldots, m$, we define the distributions $\tilde{\mathcal{D}}_i$ as the following:

$$\tilde{\mathcal{D}}_i(y) := \frac{\mathcal{D}_i(y)}{\sum_{y \in \{0,1\}^n} \mathcal{D}_i(y)},$$

where for $i = k, \ldots, m-1$,

$$\mathcal{D}_i(y) := \begin{cases} \mathcal{D}(y), & \text{if } \mathcal{D}(y) \in \left(2^{-(i+1)}, 2^{-i}\right] \\ 0, & \text{otherwise} \end{cases}$$

and

$$\mathcal{D}_m(y) := \begin{cases} \mathcal{D}(y), & \text{if } \mathcal{D}(y) \in \left(0, 2^{-m}\right] \\ 0, & \text{otherwise} \end{cases}.$$

For all $i \in [m]$, let Y_i be the set of all elements y such that $\tilde{\mathcal{D}}_i(y) \neq 0$. We define the distribution

$$\alpha(i) := \sum_{y \in \{0,1\}^n} \mathcal{D}_i(y)$$

over $\{k, \ldots, m\}$. We show that the distribution $\mathcal{D}$ is equivalent to the distribution $\mathcal{D}''$ obtained by choosing i according to the distribution α and then picking an element according to the distribution $\tilde{\mathcal{D}}_i$. (Note that there are no values i with $\mathcal{D}(i) > 2^{-k}$ since $H_\infty(\mathcal{D}) \geq k$.)

$$\begin{aligned} &\Pr\left[y = y' : i \leftarrow \alpha, y' \leftarrow \tilde{\mathcal{D}}_i\right] \\ &\quad = \sum_{i=1}^{k} \Pr\left[i = i' : i' \leftarrow \alpha\right] \Pr\left[y = y' : y' \leftarrow \tilde{\mathcal{D}}_i\right] \\ &\quad = \sum_{i=1}^{k} \mathcal{D}_i(y) = \mathcal{D}(y). \end{aligned}$$

The high-level overview for the proof. We would prove an upper bound for the probability of finding a collision for the function $f \leftarrow \mathcal{D}^X$. Since $Y_i \cap Y_j = 0$ for any $i \neq j$, the probability of finding a collision for $f \leftarrow \mathcal{D}^X$ can be written as the sum of the probability of finding a collision inside Y_i:

$$\begin{aligned}
&\Pr\bigl[f(x) = f(x') \wedge x \neq x' : f \leftarrow \mathcal{D}^X,\ (x,x') \leftarrow \mathcal{A}^f\bigr] \\
&\quad = \sum_{i=k}^{m} \Pr\bigl[f(x) = f(x') \wedge x \neq x' \wedge f(x) \in Y_i : f \leftarrow \mathcal{D}^X,\ (x,x') \leftarrow \mathcal{A}^f\bigr] := (\varepsilon_i)
\end{aligned}$$

We would obtain an upper bound for each expression in the sum (ε_i) in the following steps.

First step. We prove that the probability of finding a pre-image of Y_i (an x such that $f(x) \in Y_i$) is upper bounded by $O(q^2\alpha(i))$ for any quantum adversary A^f with $f \leftarrow \mathcal{D}^X$. In other words, we prove

$$\delta_i := \Pr\bigl[f(x) \in Y_i : f \leftarrow \mathcal{D}^X, x \leftarrow \mathcal{A}^f\bigr] \leq O\bigl(q^2\alpha(i)\bigr), \tag{4.1}$$

and therefore $\varepsilon_i \leq O\bigl(q^2\alpha(i)\bigr)$. To prove the above, we show that a quantum algorithm $\mathcal{B}$ that has oracle access either to the zero function over X or the function $g : X \to \{0,1\}$:

$$g(x) := \begin{cases} 1, & \text{with probability } \alpha(i) \\ 0, & \text{otherwise} \end{cases},$$

can run $\mathcal{A}$, properly simulates f and using $\mathcal{A}$'s output distinguishes the zero function over X from g making $O(q^2)$ queries to its oracle. Therefore, $\delta_i \leq O(q^2\alpha(i))$ by Theorem 3 in Section 2.3 that gives an upper bound for the success probability of $\mathcal{B}$ that tries to distinguish a zero function from g. Note that the bound might not be useful if $\alpha(i)$ be large for some i. Therefore, we obtain the second bound in the second step.

Second step. We would prove a different abound for ε_i in the following. We reduce the collision problem for $f \leftarrow \mathcal{D}^X$ to collision problem for $f \leftarrow \tilde{\mathcal{D}}_i^X$. Since the distribution $\mathcal{D}$ is equivalent to the distribution $\mathcal{D}''$ obtained by choosing i according to the distribution α and then picking an element according to the distribution $\tilde{\mathcal{D}}_i$, we can prove that

$$\begin{aligned}
&\Pr\bigl[f(x) = f(x') \wedge x \neq x' \wedge f(x) \in Y_i : f \leftarrow \mathcal{D}^X,\ (x,x') \leftarrow \mathcal{A}^f\bigr] \\
&\quad \leq \Pr\Bigl[\tilde{f}(x) = \tilde{f}(x') \wedge x \neq x' : \tilde{f} \leftarrow \tilde{\mathcal{D}}_i^X,\ (x,x') \leftarrow \mathcal{A}^{\tilde{f}}\Bigr].
\end{aligned} \tag{4.2}$$

We show that the probability of finding a collision for function $f_i \leftarrow \tilde{\mathcal{D}}_i^X$ is upper bounded by $O\bigl(\frac{q^3}{2^i\alpha(i)}\bigr)$ for any $i = 1, \cdots, m-1$ with non-empty Y_i:

$$\Pr\Bigl[\tilde{f}(x) = \tilde{f}(x') \wedge x \neq x' : \tilde{f} \leftarrow \tilde{\mathcal{D}}_i^X,\ (x,x') \leftarrow \mathcal{A}^{\tilde{f}}\Bigr] \leq O\bigl(\frac{q^3}{2^i\alpha(i)}\bigr). \tag{4.3}$$

To prove the bound in 4.3, we define the new distributions $\mathcal{D}_i^* : Y_i \cup \{\perp\} \rightarrow [0,1]$ as the following:

$$\mathcal{D}_i^*(y) := \begin{cases} \frac{2^i}{|Y_i|}\mathcal{D}_i(y), & \text{if } y \in Y_i \\ 1 - \frac{2^i}{|Y_i|}\alpha(i), & \text{if } y = \perp \end{cases}.$$

Next we prove that the function $f^* \leftarrow \mathcal{D}_i^{*X}$ is collision-resistant by reducing it to the collision problem for a random function. Since a random function is collision-resistant [75], f^* is collision-resistant as well. And finally, we reduce the collision problem for $\tilde{f} \leftarrow \tilde{\mathcal{D}}_i^X$ to the collision problem for $f^* \leftarrow \mathcal{D}_i^{*X}$. (If it is not clear from this sketch how we get Equation 4.3, an interested reader can refer to [63] for details.)

Final step. In the following, we use the bound derived above to show our final bound. We use the inequalities 4.1, 4.2 and 4.3 to prove that the probability of returning a collision for $f \leftarrow \mathcal{D}^X$ is upper bounded by $O\big(\frac{q^{5/2}}{2^{k/2}}\big)$ as follows:

$$\begin{aligned} &\Pr\big[f(x) = f(x') \wedge x \neq x' : f \leftarrow \mathcal{D}^X,\ (x,x') \leftarrow \mathcal{A}^f\big] \\ &\quad = \sum_{i=k}^{m} \Pr\big[f(x) = f(x') \wedge x \neq x' \wedge f(x) \in Y_i : f \leftarrow \mathcal{D}^X,\ (x,x') \leftarrow \mathcal{A}^f\big] \\ &\quad \leq \sum_{i=k}^{m-1} O\Big(\min\Big\{\frac{q^3}{2^i\alpha(i)}, q^2\alpha(i)\Big\}\Big) + O\big(q^2\alpha(m)\big) \\ &\quad \overset{(*)}{\leq} (m-k-1)O\Big(\frac{q^{5/2}}{2^{k/2}}\Big) + O\big(q^2\alpha(m)\big) \end{aligned}$$

where $(*)$ holds because $\min\Big\{\frac{q^3}{2^i\alpha(i)}, q^2\alpha(i)\Big\}$ will be maximised when $\frac{q^3}{2^i\alpha(i)} = q^2\alpha(i)$ and the maximum value is $q^{5/2}/2^{i/2}$. Choosing $m = n+k$ results in $q^2\alpha(m) \leq q^2|Y_m|/2^m \leq q^2 2^{n-m} \leq q^2/2^k$ and this proves the bound stated in Table 1.

4.3. Discussion: Open Problems and Related Works

“Collapsing” property introduced by Unruh [68] is a strengthening of quantum collision resistance property of hash functions. Unruh shows that a collapsing hash function is collision-resistant. In particular, he shows that a random oracle is collapsing and therefore it is collision-resistant. It is open to verify the collapsing property for a non-uniformly distributed function.

Subsequent Work. In subsequent but independent work, Balogh et al. [13] study the quantum-collision problem for non-uniformly distributed functions. They have obtained similar bounds as ours except for general two lower bounds ($\forall\mathcal{A}\forall\mathcal{D}$) and for an upper bound in case of $\exists\mathcal{A}\exists\mathcal{D}$ and collision-entropy. Their general lower bounds, $\Omega(2^{\frac{H_\infty}{3}})$ and $\Omega(2^{\frac{H_2}{6}})$ improve upon our bounds, using a completely different proof. Our upper bound in case of $\exists\mathcal{A}\exists\mathcal{D}$ and collision-entropy is $O(2^{\frac{H_2}{4}})$ which is stronger than their corresponding bound $O(2^{\frac{H_2}{3}})$.

Previous Works. The quantum collision problem has been studied in various previous works. All of the following results are proven for random functions.

In the following, we mention the existing results on the number of queries that are necessary to find a collision. An $\Omega(N^{1/3})$ lower bound for function f is given by Aaronson and Shi [3] and Ambainis [8] where f is a two-to-one function with the same domain and co-domain and N is the domain size. Yuen [73] proves an $\Omega(N^{1/5}/\text{polylog}N)$ lower bound for the quantum collision problem for a random function f with same domain and co-domain. He reduces the distinguishing between a random function and a random permutation problem to the distinguishing between a function with r-to-one part and a function without r-to-one part. His proof is a combination of using the r-to-one lower bound from [3] and using the quantum adversary method [7]. Zhandry [75] improves Yuen's bound to the $\Omega(N^{1/3})$ and also removes the same size domain and co-domain constraint. He uses the existing result from [74] to prove his bound.

The sufficient number of quantum queries to find a collision has given in the following works. A quantum algorithm that requires $O(N^{1/3})$ quantum queries and finds a collision for any two-to-one function f with overwhelming probability is given by Brassard, Hϕyer and Tapp [23]. Ambainis [9] gives a quantum algorithm that requires $O(N^{2/3})$ queries to find two equal elements among N given elements and therefore it is an algorithm for finding a collision in an arbitrary function f given the promise that f has at least one collision. Yuen [73] shows that the collision-finding algorithm from [23] is able to produce a collision for a random function with same domain and co-domain using $O(N^{1/3})$ queries. Zhandry shows that $O(M^{1/3})$ queries are adequate to find a collision for a random function $f:[N]\to[M]$ where $N=\Omega(M^{1/2})$. He uses Ambainis's element distinctness algorithm [9] as a black box in his proof. Zhandry's bound also implies that we can not expect a lower bound for the query complexity of finding a collision for a non-uniform function better than $O(2^{k/3})$.

5. POST-QUANTUM SECURITY OF FUJISAKI-OKAMOTO AND OAEP TRANSFORMS

5.1. Motivation

The fascinating idea of a public-key encryption scheme that guarantees secure communication between two parties even though they have not shared any key in advance was publicly introduced in 1976 by Whitfield Diffie and Martin Hellman. Since then there have been tremendous efforts to construct public-key encryption schemes based on multiple hard assumptions. However, there are few examples of cryptosystems that are both provably secure against chosen ciphertext attacks (IND-CCA) in the standard model and efficient.

The random oracle model [14] in which there is a truly random function that all parties, including an adversary, can query on some desired inputs and get back the corresponding outputs is a method to achieve a trade-off between the security and the efficiency of encryption schemes. However, in the real world applications, the random oracle is instantiated by a hash function. Consequently in the advent of quantum computers, the security proofs in the random oracle model have to be revisited for the reason that a quantum adversary might implement the hash function (since it is public) and therefore can evaluate the hash function on some quantum superposition of inputs. Proving security of constructions in the quantum random oracle model is more challenging since queries to the random oracle can be in superposition and classical security proof techniques may not work. In [17], Boneh et al. present a separating scheme that is secure when adversary has classical access to the random oracle and is insecure if adversary can submit quantum queries. They construct an identification scheme that has two stages. In the first stage, the verifier checks if the prover is able to find enough collisions for some hash function. In the second stage, the prover and verifier run a quantum secure identification scheme. At the end, the verifier accepts if the prover can find enough collisions in the first stage or the prover can identify itself in the second stage. It is clear that if the prover is not able to find enough collisions in the first stage, then the security of the scheme follows from the security of the quantum secure identification in the second stage. They use the polynomial gap between a quantum collision finding algorithm based on Grover's search algorithm and birthday attack to argue that the scheme is insecure if a malicious prover can evaluate the hash function on quantum states. For the positive result, they show that every classical security reduction in which the answer to a new oracle query is independent of the history of previous queries implies quantum security. However, their techniques can not imply the security of the famous construction of Fujisaki-Okamoto (FO construction) [42]. Whereas the Fujisaki-Okamoto transformation, for example in [57], has been used to construct an actively secure encryption scheme based on the lattice-based assumptions that are believed to be intractable even for a quantum computer.

Fujisaki and Okamoto [42] constructed a hybrid encryption scheme that is secure against chosen ciphertext attacks (IND-CCA), i.e., the most desirable security notion for encryption schemes, in the random oracle model. Their scheme is a combination of a symmetric and an asymmetric encryption scheme using two hash functions where the symmetric and asymmetric encryption schemes are secure in a very weak sense. However, their proof of security only works against classical adversaries and it is not clear how one can fix their proof in the quantum setting. In the following, we mention the parts of the classical proof that may not work in the quantum setting.

Challenges. The following challenges will occur if one wants to prove the security of FO transformation in the quantum random oracle model.

(a) The classical proof uses the list of all queries made to the random oracles to simulate the decryption algorithm without possessing the secret key of the asymmetric encryption scheme. In the quantum case, where the adversary has quantum access to the random oracles and submits queries in superpositions, such a list is not a well-defined concept.

(b) Also, the classical proof uses the fact that using a random value h^* instead of a given random oracle output $H(x)$ cannot be noticed by the adversary, provided that the adversary never queries x from the random oracle. In the quantum setting, the adversary may in a certain sense always query all values x by querying the random oracle on the superposition $\sum_x |x\rangle$ of all values. The situation gets especially difficult since the value x depends in turn on messages produced by the adversary.

(c) Finally, the classical proof uses the fact that for a randomized encryption scheme, it is hard to find values $x \neq x'$ such that encrypting message m with randomness $H(x)$ and $H(x')$ leads to the same ciphertext, $Enc(m;H(x)) = Enc(m;H(x'))$. (Note: this does not follow directly from the collision resistance of the random oracle H since we may have $Enc(m;H(x)) = Enc(m;H(x'))$ for $H(x) \neq H(x')$.)

5.2. Our Contribution

Our solutions. We show how to circumvent those problems. Problem (c) is solved by using our result showing the collision resistance of random functions with outputs sampled from a non-uniform distribution that we discussed in Chapter 4. Problem (b) is solved by the "one-way to hiding" lemmas from [66, 67] (Lemma 5 and Lemma 6 in Subsection 2.4.1) which gives us a tool for handling the reprogramming of the random oracle. Problem (a) remains. In fact, we do not have a proof for the unmodified Fujisaki-Okamoto scheme. However, we show how to solve the problem by adding one more hash value $H'(\delta)$ to the ciphertext. Although in general, it may not be well-defined in the quantum setting what the list of queries to the random oracle is, we can show it to be well-defined in this case, using the fact that range and domain of H' have the same size.

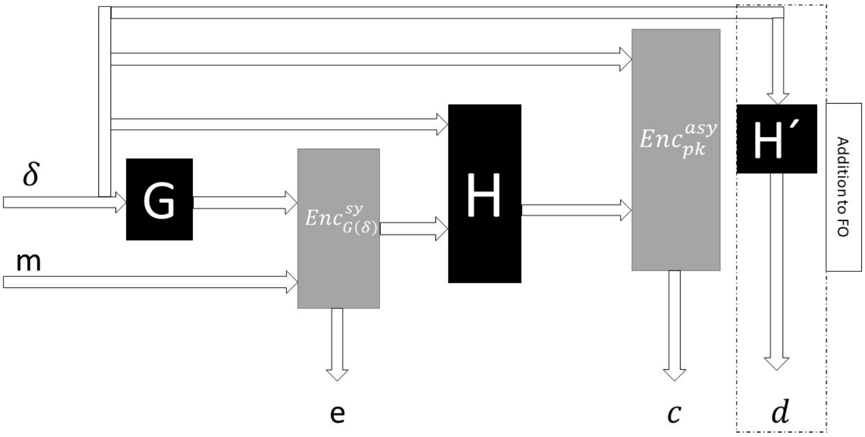


Figure 5.1: Our modified Fujisaki-Okamoto transformation

We modify the hybrid encryption scheme presented by Fujisaki and Okamoto using an extra hash function H'. We prove that our scheme is indistinguishable secure against chosen ciphertext attacks in the quantum random oracle model. For a message m, the encryption algorithm of our scheme, Enc^{hy}_{pk}, works as follows:

$$Enc^{hy}_{pk}(m;\delta) = \left(Enc^{sy}_{G(\delta)}(m),\ Enc^{asy}_{pk}\left(\delta;H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ H'(\delta)\right)$$

where pk and sk are the public key and the secret key of the asymmetric encryption scheme. Enc^{asy}_{pk} and Enc^{sy}_{sk} are the asymmetric and symmetric encryption algorithms respectively and δ is a random element from the message space of the asymmetric encryption scheme. H, G and H' are random oracles. The asymmetric encryption scheme is one-way secure, that is, informally the adversary can not decrypt the encryption of a random message. The symmetric encryption scheme is one-time secure, that is, informally the adversary can not distinguish between the encryptions of two messages when a fresh key is used for every encryption. In addition, the asymmetric encryption scheme is well-spread, i.e. any message can lead to at least $2^{\omega(\log n)}$ potential ciphertexts.

Note that our modification increases the ciphertext size by only a single hash value $H'(\delta)$ and is computationally inexpensive.

As already mentioned above, the added hash value $H'(\delta)$ solves problem (a) because given $H'(\delta)$, it is well-defined what δ is. This is because H' is chosen to have the same domain and range size, and hence is indistinguishable from a permutation [73]. However, we need to efficiently invert H' in the formal proof, therefore we do not directly use that fact, instead our proof goes along the following lines: We replace H' with a random polynomial to force the adversary to submit the input that has been used to obtain the ciphertext. This can be done due to a result by Zhandry [74] that shows a random oracle is indistinguishable from a

$2q$-wise independent function where q is the number of queries that the adversary makes to the oracle function. As soon as H' is implemented as a polynomial, we can use the fact that roots of a polynomial can be found in polynomial-time; this allows us to efficiently get all candidates for δ given $H'(\delta)$.

We present the formal definition of our modified Fujisaki-Okamoto construction in the following. The definition contains the description of key generation, encryption and decryption algorithms.

Modified Fujisaki-Okamoto Construction. Let $\Pi^{asy} = (Gen^{asy}, Enc^{asy}, Dec^{asy})$ be an asymmetric encryption scheme with the message space $\mathtt{MSP}^{asy} = \{0,1\}^{n_1}$ and the coin space $\mathtt{COIN}^{asy} = \{0,1\}^{n_2}$. Let $\Pi^{sy} = (Enc^{sy}, Dec^{sy})$ be a symmetric encryption scheme where $\mathtt{MSP}^{sy}$ and $\mathtt{KSP}^{sy} = \{0,1\}^m$ are its message space and key space, respectively. The parameters n_1, n_2 and m depend on the security parameter n. We define three hash functions:

$$G : \mathtt{MSP}^{asy} \to \mathtt{KSP}^{sy},\ H : \{0,1\}^* \to \mathtt{COIN}^{asy} \text{ and } H' : \mathtt{MSP}^{asy} \to \mathtt{MSP}^{asy}.$$

These hash functions will be modeled as random oracles in the following.

The hybrid scheme $\Pi^{hy} = (Gen^{hy}, Enc^{hy}, Dec^{hy})$ is constructed as follows, with $\mathtt{MSP}^{hy}$ as its message space:

1. Gen^{hy}, the key generation algorithm, on input 1^n runs Gen^{asy} to obtain a pair of keys (pk, sk).
2. Enc^{hy}, the encryption algorithm, on input pk and message $m \in \mathtt{MSP}^{hy}$ $(= \mathtt{MSP}^{sy})$ does the following:
   - Select $\delta \xleftarrow{\$} \mathtt{MSP}^{asy}$.
   - Compute $c \leftarrow Enc^{sy}_a(m)$, where $a := G(\delta)$.
   - Compute $e := Enc^{asy}_{pk}(\delta; h)$, where $h := H(\delta \| c)$.
   - Finally, output (e, c, d) as $Enc^{hy}_{pk}(m; \delta)$, where $d := H'(\delta)$.
3. Dec^{hy}, the decryption algorithm, on input sk and ciphertext (e, c, d) does the following:
   - Compute $\hat{\delta} := Dec^{asy}_{sk}(e)$.
   - If $\hat{\delta} = \perp$: abort and output $\perp$.
   - Otherwise set $\hat{h} := H(\hat{\delta} \| c)$.
   - If $e \neq Enc^{asy}_{pk}(\hat{\delta}; \hat{h})$: abort and output $\perp$.
   - Else if $d = H'(\hat{\delta})$:
     - Compute $\hat{a} := G(\hat{\delta})$ and output $Dec^{sy}_{\hat{a}}(c)$.
   - Else output $\perp$.

Also, we modify OAEP-cryptosystem [60] using an extra hash function and prove its security in the quantum random oracle model based on the existence of a partial-domain one-way trapdoor injective function secure against quantum adversaries. This will remain theoretical until a candidate for a quantum secure partial-domain one-way trapdoor injective function is discovered. The proof follows similar lines as that of the Fujisaki-Okamoto transform.

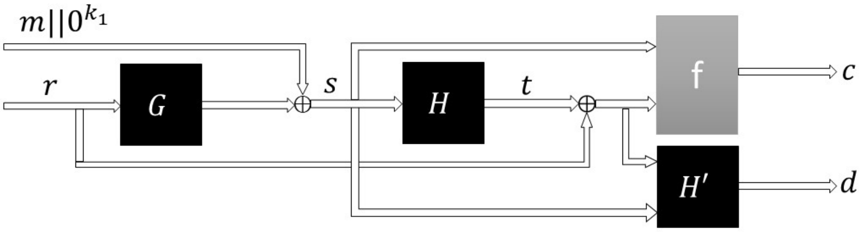


Figure 5.2: Our modified OAEP transformation. H' has been added to OAEP.

Modified OAEP Transform. Let

$$G : \{0,1\}^{k_0} \to \{0,1\}^{k-k_0} \text{ and } H : \{0,1\}^{k-k_0} \to \{0,1\}^{k_0}$$

be random oracles. We modify the OAEP construction using an extra hash function $H' : \{0,1\}^k \to \{0,1\}^k$. The Q-OAEP $= (Gen, Enc, Dec)$ encryption scheme is defined as:

1. **Gen**: Specifies an instance of the injective function f and its inverse f^{-1}. Therefore, the public key and secret key are f and f^{-1} respectively.
2. **Enc**: Given a message $m \in \{0,1\}^n$, the encryption algorithm computes
$$s := m||0^{k_1} \oplus G(r) \quad \text{and} \quad t := r \oplus H(s),$$
where $r \xleftarrow{\$} \{0,1\}^{k_0}$, and outputs the ciphertext $(c,d) := \Big(f(s,t), H'(s\|t)\Big)$.
3. **Dec**: Given a ciphertext (c,d), the decryption algorithm does the following:
   - When $c \notin \operatorname{Im} f$, return $\perp$.
   - When $c \in \operatorname{Im} f$, the decryption algorithm extracts $(s,t) = f^{-1}(c)$. If $H'(s\|t) \neq d$ it returns $\perp$, otherwise it does the following:
     (a) query the random oracle H on input s and compute $r := t \oplus H(s)$.
     (b) query the random oracle G on input r and compute $M := s \oplus G(r)$.
     (c) if the k_1 least significant bits of M are zero then return the n most significant bits of M, otherwise return $\perp$.

Note that k_0 and k depend on the security parameter n. The modification is adding $H'(s\|t)$ to the ciphertext.

On the necessity of our modifications. We have slightly modified both the Fujisaki-Okamoto and the OAEP-cryptosystem by adding one additional hash to the ciphertexts. Although these additions are not very costly, it is a natural question whether they are necessary, especially in light of the question whether existing implementations are post-quantum secure. Although it is clear that our

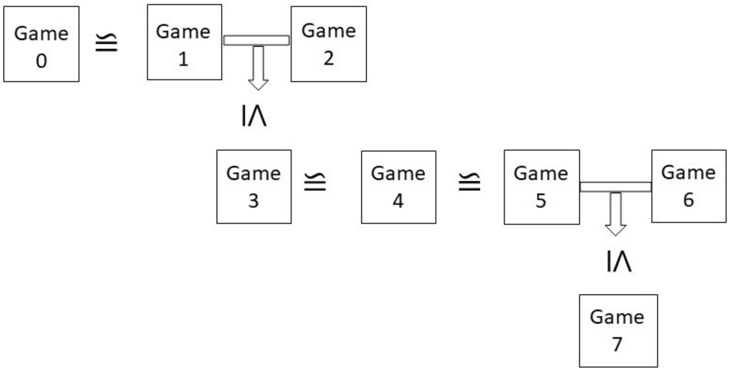


Figure 5.3: The relation between the success probability of Games in the proof of FO construction. The symbol $\cong$ indicates that two games are indistinguishable. The symbol $\leq$ indicates the upper bound, for instance, the difference between the success probability of Game 1 and Game 2 is upper bounded by the success probability of Game 3.

proof technique strongly relies on these additional hashes (to overcome the challenge (a) stated above), this does not mean that the original schemes are insecure. However, we urge the reader not to assume that they are post-quantum secure just because they are classically secure. For example, in [11] it was shown that (at least relative to a specific oracle) the Fiat-Shamir transform is insecure in the quantum setting (using quantum random oracles)even though it is secure classically. Their setting is similar to ours, so while there are no known quantum attacks on Fujisaki-Okamoto or OAEP, we should not rely on their security until a security proof is found. We leave finding either an attack or a proof as a (highly non-trivial) open problem.

5.2.1. Proof Overview

Proof overview for FO construction: The proof consists of several subsequent games in which we start with the IND-CCA game for the hybrid encryption scheme and end with a game whose success probability is negligibly close to $1/2$. In Figure 5.3, we sketch the relation between the games described in the proof. The description of Games are presented in the following. We discuss the differences between two subsequent games and the reason behind the relation in Figure 5.3.

Game 0: This game corresponds to the IND-CCA game. The adversary A that has oracle access to the decryption algorithm wins if he can distinguish between the encryption of two messages m_0, m_1 of his choice (but can not submit the challenge query $Enc^{hy}_{pk}(m_b;\delta^*) := (e^*, c^*, d^*)$ for decryption).

Game 1: We modify the decryption algorithm such that it returns $\perp$ if it receives a decryption query with the first coordinate e^*. Roughly speaking, the adversary may have a chance to distinguish these two games by querying (e^*, c, d^*) to the decryption oracle for a suitable c. Note that the decryption algorithm in Game 1 returns $\perp$ in this case, in contrast, the decryption algorithm in Game 0 will not return $\perp$ if $e^* = Enc^{asy}_{pk}(\delta^*; H(\delta^* \| c))$. Since c is used to produce the randomness for the asymmetric encryption scheme that is well-spread, this roughly leads to a collision for a function whose output is chosen according to a distribution with high min-entropy, that is, $Enc^{asy}_{pk}(\delta^*; H(\delta^* \| c)) = Enc^{asy}_{pk}(\delta^*; H(\delta^* \| c^*))$. Therefore, Game 0 and Game 1 are roughly equivalent by the result showing collision resistance of random functions with outputs sampled from a non-uniform distribution in Chapter 4.

Game 2: In this game, we use a random key a^* to obtain the second coordinate of the challenge ciphertext, and we replace the last coordinate of the challenge ciphertext with a random element, that is, $c^* := Enc^{sy}_{a^*}(m_b)$ and d^* is chosen uniformly at random. Since a^* is a random key to encrypt m_b, we can reduce the success probability of the adversary in Game 2 to the one-time security of the symmetric encryption scheme and consequently its success probability is negligibly close to $1/2$. It is left to prove that Game 1 and Game 2 have negligible difference. Classically (when queries to the random oracles are classical), Game 1 and Game 2 are equivalent unless the adversary queries the random oracles G or H' on input δ^* (the bad event). This argument does not work for quantum queries since every quantum query may contain δ^* in some sense and the bad event is not well-defined concept in quantum case. For this reason, we use the "one-way to hiding" lemma 5 in Subsection 2.4.1, which give us a tool for handling the reprogramming of the random oracle and get an upper bound for the difference between the success probabilities of Game 1 and Game 2. The upper bound that we obtain is roughly the square root of the success probability of the next game.

Game 3: Roughly speaking, in this game, the adversary A_m runs the adversary A, and it measures the argument of a randomly chosen query that adversary A makes to the random oracles G and H' and outputs the measurement result.The game succeeds if A_m outputs δ^* . The success probability of this game may not be negligible since δ^* is used to obtain $e^* := Enc^{asy}_{pk}(\delta^*; H(\delta^* \| c^*))$ and the adversary may obtain some information about δ^* from e^*. The following sequence of games deals with this issue by introducing a new decryption algorithm that does not need the secret key of the asymmetric encryption scheme and consequently we can use the one-way security of the asymmetric encryption scheme to prove that this game has a negligible success probability.

Game 4: In this game, we replace H' with a random polynomial. Due to a result by Zhandry [74] that shows a random oracle is indistinguishable from a $2q$-wise independent function where q is the number of queries that the adversary makes to the oracle function, Game 3 and Game 4 are indistinguishable.

Game 5: In this game, we modify the decryption algorithm in a way that does not need the secret key of the asymmetric encryption scheme for decryption. Vaguely speaking, this can be done by solving the equation $H' - d = 0$ where d is the last coordinate of the decryption query and H' is a polynomial. Still we are not yet able to reduce the success probability of this game to the one-way security of the asymmetric encryption scheme for the reason that the randomness used to obtain e^* ($H(\delta^*\|c^*)$) is dependent on δ^*.

Game 6: We use a fresh randomness to obtain $e^* := Enc_{pk}^{asy}(\delta^*;\$)$ (that is $H(\delta^*\|c^*)$ is replaced by \$) and consequently the success probability of Game 6 can be reduced to the one-way security. Intuitively, since δ^* is not used anywhere else then if A_{m1} measures δ^*, it corresponds to inverting e^*. However, the Game 5 and Game 6 are indistinguishable unless the adversary notices that we replace $H(\delta^*\|c^*)$ with a random element. Classically (when queries to the random oracles are classical), Game 5 and Game 6 are equivalent unless the adversary queries the random oracles G or H' on input δ^* (the bad event). Similar to the discussion in Game 2, this argument does not work for quantum queries. For this reason, we again use the adaptive "one-way to hiding" lemma 6 in Subsection 2.4.1, which gives us a tool for handling the reprogramming of the random oracle and get an upper bound for the difference between the success probability of Game 5 and Game 6. The upper bound that we obtain is roughly the square root of the success probability of the next game.

Game 7: Roughly speaking, in this game, the adversary A_{m2} runs the adversary A_{m1}, and measures the argument of a random query that the adversary A_{m1} makes to the random oracles H and outputs the result. The game succeeds if A_{m2} obtains δ^* and c^* after the measurement. Intuitively, obtaining δ^* is corresponding to inverting e^* and therefore the success probability is negligible by one-way security of the asymmetric encryption scheme.

5.3. Discussion: Open Problems and Related works

We did prove the IND-CCA security of modified FO and OAEP constructions in the quantum random oracle model. Recently, Zhandry [76] shows the IND-qCCA security (Definition 4.6 in [19]) of FO construction (without modification) using a technique to record superposition queries. In the IND-qCCA security notion, the adversary is allowed to submit superposition queries to the decryption oracle. The challenger stores the challenge ciphertexts in a set C and the decryption algorithm returns $\perp$ if the adversary ask for the decryption of a challenge ciphertext in C. A natural question might be: why are the challenge queries only allowed to be classical? and in contrast, the decryption queries can be in superposition. The way they handle the issue of submitting a challenge ciphertext to the decryption oracle by the adversary only works when the challenge queries are classical. In [5], authors study a quantum counterpart of IND-CCA security notion for quantum encryption schemes that encrypt quantum data. Presenting a justified quantum IND-CCA security notion for a classical encryption scheme is open. Then we may verify if the FO construction is a transformation from quantum IND-CPA to quantum IND-CCA in the quantum random oracle model.

Related works. We mention the use of the quantum random oracle model in some previous constructions. Quantum random oracles have been used to explore the limitation of the quantum computing in [15], i.e., relative to a random oracle not all of NP can be solved by a quantum computing device. In [2], they use quantum random oracles to construct publicly-verifiable quantum money. The quantum random oracles have been used in [22, 24] to provide some level of security to the quantum counterpart of Merkle's Puzzles. The first secure identity-based encryption in the quantum random oracle model was proposed in [74] by Zhandry. Unruh [67] constructed a non-interactive zero-knowledge proof system in the quantum random oracle model. A quantum position verification scheme that is secure in the quantum random oracle model was presented in [66]. The security of the Fiat–Shamir transformation [39] in the quantum random oracle model has been studied in multiple research works [10, 36, 69].

Subsequent Works. Subsequently, our transformation has been used in multiple research works [6, 20, 44, 47] to present an IND-CCA secure Key Encapsulation Mechanism (KEM) in quantum random oracle model. Also, our conversion has been used in [29, 30] to propose post-quantum secure public-key encryption scheme.

6. POST-QUANTUM SECURITY OF MODES OF OPERATION

6.1. Motivation

A block cipher is a type of private-key encryption scheme in which the sender and the receiver use a shared secret key to communicate. Block ciphers are one of the most fundamental primitives in cryptography, however, it can only encrypt messages of a fixed (and usually very short) length. This drawback reduces the use of a block cipher significantly. To make the block ciphers more applicable, they are usually used in so-called "modes of operation" that extend the message space of the block cipher. The security of many encryption schemes used in practice are dependent on the security of modes of operation. Classically, the indistinguishability against chosen plaintext attack (IND-CPA) is a desirable notion for the security of a mode of operation. It usually is proven that a mode of operation is IND-CPA secure under the assumption that the underlying block cipher is a pseudo-random function (PRF).

We investigate the security of modes of operation against a quantum adversary. So far in the quantum case, there are two variants of the IND-CPA notion: "standard IND-CPA" and "IND-qCPA". In the standard IND-CPA notion, the quantum adversary performs only classical encryption queries, and in the IND-qCPA notion (as defined by [19]), the adversary is allowed to perform quantum encryption queries. However, the challenge queries are required to be classical.

We enumerate some motivations to consider such a security notion.

- In the future, we might want to encrypt the superposition of messages using quantum devices. (That is, a protocol that actively uses quantum communication, not just a classical protocol secure against quantum adversaries.)
- A second argument (made in [38]) is that with continuing miniaturization, supposedly classical devices may enter the quantum scale, and thus "accidentally" encrypt messages in superposition. (We have doubts how realistic this case is, but we mention it for completeness.)
- A third argument (made in [12]) is that the security of an encryption scheme in IND-qCPA notion might help to prove the quantum security of a classical protocol that uses the encryption scheme as a part of its construction. If a classical protocol is proven secure (with respect to a quantum adversary), intermediate games in the security proof may actually contain honest parties that run in superposition. This happens in particular if zero-knowledge proof systems or similar are involved [64, 71]. For example, in [65, Section 5], the security proof of a classical protocol did not go through because the signature scheme was not secure under quantum queries (they had to change the protocol considerably instead). Encryption schemes that are not just standard IND-CPA, but IND-qCPA might help in similar situations.

Mode of operation	Classical IND-CPA?	Standard (quantum) IND-CPA?	IND-qCPA? (with sPRF)	IND-qCPA? (with qPRF)
ECB	no	no	no	no
CBC	yes	yes	no	yes
CFB	yes	yes	no	yes
OFB	yes	yes	yes	yes
CTR	yes	yes	yes	yes
XTS	unknown	unknown	“no in spirit”	unknown

Table 3: Summary of our results in this Chapter. “No in spirit” means that there is an attack using superposition queries that does not formally violate IND-qCPA.

6.2. Our Contribution

We investigate the quantum security of common modes of operation, namely those listed in the 2013 ENISA[1] report on recommended encryption algorithms [41]: CBC, CFB, OFB, CTR, and XTS. Classically, CBC, CFB, OFB, CTR modes of operation are IND-CPA secure under the assumption that the underlying block cipher is a pseudo-random function (PRF). ECB is known not to have reasonable security for most applications, while the security of XTS, as far as we know, is an open question. The standard IND-CPA security of CBC, CFB, OFB, CTR modes of operation is essentially the same with the classical case under the assumption that the underlying block cipher is a PRF that is secure against a quantum adversary that only makes classical queries to the PRF. Such a PRF is called standard secure pseudo-random function, sPRF.

However, the IND-qCPA security of the aforementioned modes of operation is more challenging since the quantum adversary has superposition access to the encryption scheme. In this setting, we show that OFB and CTR modes of operation can be proven IND-qCPA secure using a standard secure PRF. In contrast, we show that CBC and CFB modes of operation are not IND-qCPA secure in general when using a standard secure PRF in the quantum random oracle model, but they are secure when the underlying block cipher is qPRF. For XTS, we show that the adversary can recover the second half of a plaintext if he can choose the first half of the plaintext (and the adversary can recover half of the key).

We summarize the results in Table 3. Our counter-examples are in the quantum random oracle model, but our positive results are in the standard model (no random oracle). For the counter-example, we construct a block cipher that is periodic in the secret key using a random oracle. We show that our construction is standard secure in the quantum random oracle model. In contrast, when adversary has a superposition access to the block cipher, we can recover the secret key using Simon’s algorithm [61]. For a function $f : \{0,1\}^n \to \{0,1\}^n$ such that

[1] European Union Agency for Network and Information Security. We chose this list as a basis in order to investigate a practically relevant and industrially deployed set of modes of operations.

$f(x \oplus k) = f(x)$ for any $x \in \{0,1\}^n$ and a fixed and unknown $k \in \{0,1\}^n$, Simon's algorithm finds k with polynomial number of queries ($O(n)$ queries) to f.

6.2.1. Proof Overview

Notations. In the following, droplastbit is a function that removes the last bit of the input bit-string, that is, for a bit-string $BS = (b_1, \ldots, b_n)$, $\mathsf{droplastbit}(BS) = (b_1, \ldots, b_{n-1})$. The function lastbit outputs the last bit of the input, for instance $\mathsf{lastbit}(BS) = b_n$. The operator $\cdot$ is defined as $BS \cdot b = BS$ if $b = 1$ and $BS \cdot b = (0,0,\ldots,0)$ (zero bit-string of length n) if $b = 0$.

Insecurity of CBC and CFB modes of operation using a standard secure PRF: In order to show the insecurity of CBC and CFB, we construct a standard secure BC_k that is k-periodic (where k is the secret key). We show the adversary can use Simon's algorithm [61] to find the period (the secret key) of BC_k using learning queries to $\mathrm{CBC}_{\mathsf{BC}_k}$ and $\mathrm{CFB}_{\mathsf{BC}_k}$. This allows the adversary to break the IND-qCPA security of $\mathrm{CBC}_{\mathsf{BC}_k}$ and $\mathrm{CFB}_{\mathsf{BC}_k}$ by decrypting the challenge ciphertext in the challenge phase. BC_k is constructed as follows. First we construct a standard secure PRF as follows.

$$\mathsf{PRF}_k(x) := E_{H(k)}\big(\mathsf{droplastbit}\,(x \oplus (k\|1) \cdot \mathsf{lastbit}(x))\,\big),$$

where H is a random oracle and $E : \{0,1\}^{n-1} \times \{0,1\}^{n-1} \to \{0,1\}^{n-1}$ is a standard secure PRF. We show that $\mathsf{PRF}_k(x) = \mathsf{PRF}_k(x \oplus (k\|1))$. There are two cases:

1. If the last bit of x is 1, then the last bit of $x \oplus (k\|1)$ is 0 and we can write

$$\mathsf{PRF}_k(x \oplus (k\|1)) = E_{H(k)}\big(\mathsf{droplastbit}\,(x \oplus (k\|1))\,\big) = \mathsf{PRF}_k(x)$$

2. If the last bit of x is 0, then the last bit of $x \oplus (k\|1)$ is 1 and we can write

$$\mathsf{PRF}_k(x \oplus (k\|1)) = E_{H(k)}\big(\mathsf{droplastbit}\,(x)\,\big) = \mathsf{PRF}_k(x).$$

Note that the construction above is not decryptable, therefore we modify it to the construction below.

$$\begin{aligned}\mathsf{BC}_k(x) = E_{H(k)_1}\big(&\mathsf{droplastbit}(x \oplus (k\|1) \cdot \mathsf{lastbit}(x))\big)\\ &\big\| t_{H(k)_2}\big(x \oplus (k\|1) \cdot \mathsf{lastbit}(x)\big) \oplus \mathsf{lastbit}(x),\end{aligned}$$

where $H : \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$ is a random oracle, $t : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is a standard secure PRF, and the key is $k \xleftarrow{\$} \{0,1\}^{n-1}$. We prove that BC is a standard secure PRF in the quantum random oracle model. The proof uses the O2H lemma, Lemma 5 in chapter 2, to substitute $H(k)$ by a random element and then the rest of the proof is classical.

By definition of CBC, CBC $_{\mathsf{BC}_k}(m) := (c_0, \mathsf{BC}_k(m \oplus c_0))$ where $m \in \{0,1\}^n$ and $c_0 \xleftarrow{\$} \{0,1\}^n$. Then the adversary can prepare two registers M and C for messages and ciphertexts, respectively, and query CBC on a superposition of messages. Since $\mathsf{BC}_k(m \oplus c_0)$ is $(k\|1)$-periodic when restricted to the first $n-1$ bit of output, the adversary can use Simon's algorithm to output k using a polynomial number of quantum queries. Note that the adversary needs to ignore the last bit of $\mathsf{BC}_k(m \oplus c_0)$ (in order to use Simon's algorithm) by putting $|+\rangle$ as the last bit of the register C (refer to [12] for more detail.).

By definition of CFB, $\mathsf{CFB}_{\mathsf{BC}_k}(m_1) := (c_0, \mathsf{BC}_k(c_0) \oplus m_1)$ and clearly the first message block m_1 in superposition does not lead to a superposition query to BC_k. Therefore, the adversary uses two message blocks to attack. The first block m_1 is in superposition and m_2 is classical. By definition,

$$\mathsf{CFB}_{\mathsf{BC}_k}(m_1, m_2) := \Big(c_0,\ \mathsf{BC}_k(c_0) \oplus m_1,\ \mathsf{BC}_k(\mathsf{BC}_k(c_0) \oplus m_1) \oplus m_2\Big)$$

where $c_0 \xleftarrow{\$} \{0,1\}^n$ and adversary can obtain k similar to the CBC case using the last block of the ciphertext.

The insecurity of XTS mode using a standard PRF: By definition of XTS, the i-th ciphertext block is $c_i := \alpha^{i-1}L \oplus \mathsf{BC}_{k_2}(m_i \oplus \alpha^{i-1}L)$ where $L := \mathsf{BC}_{k_1}(c_0)$ for a nonce c_0 and α is the primitive element of the field $\mathbb{F}_2^n$. (Where k_1 and k_2 are independent part of the key.) If we use the block cipher constructed above (used to prove the insecurity of CBC and CFB) in XTS mode, the Simon attack will only reveal the key k_2 and the key k_1 remains secret since c_0 is a classical value that the adversary has no control over it. In other words, superposition queries to $\mathrm{XTS}_{\mathsf{BC}}$ mode of operation will not result in superposition queries to BC_{k_1} by the definition of XTS. Therefore we can not apply Simon's algorithm to BC_{k_1} and k_1 remains secret. Consequently, L remains unknown and we can not decrypt the mode without knowing L. Instead, we use the following block cipher.

$$\begin{aligned}\mathsf{BC}_{k_2}(x\|y) := E_{H(k_2)}\Big(&\mathsf{droplastbit}\big(x \oplus (k_2\|1) \cdot \mathsf{lastbit}(x)\big)\,\|\\ &\mathsf{droplastbit}\big(y \oplus f_{k_2}(x) \cdot \mathsf{lastbit}(y)\big)\Big),\end{aligned}$$

where f_{k_2} is a suitable function depending on k_2 with the property that $\mathsf{lastbit}(f_{k_2}(x) = 1)$. A simple calculation shows that

$$\mathsf{BC}_{k_2}(x\|y) = \mathsf{BC}_{k_2}(x \oplus (k_2\|1), y) \text{ and } \mathsf{BC}_{k_2}(x\|y) = \mathsf{BC}_{k_2}(x\|y \oplus f_{k_2}(x)).$$

Similar to the previous case, we add two extra bits to make it decryptable (refer to [12] for details). Now, we use Simon's algorithm to recover the key k_2 by querying the superposition of all messages as x-part of input and fixing the second half on the input ($y = 0$). This can be done by polynomial number of message blocks. Then, we recover L used in the encryption query. Note that if we insert 0 as x-part of the input in the i-th query and the superposition of all messages as the y-part, then BC_{k_2} is $f_{k_2}(\mathsf{firsthalf}(\alpha^{i-1}L))$-periodic because the XTS construction invokes BC_{k_2} with the input $(\alpha^{i-1}L \oplus x)\|y$. Therefore, we can recover one bit of $f_{k_2}(\mathsf{firsthalf}(\alpha^{i-1}L))$ from the cipher blocks i and using Simon's algorithm and since k_2 is known, we can recover one bit of $\alpha^{i-1}L$. Using different ciphertext block i, we can compute L and this allows us to decrypt the rest of the ciphertext in this block. Since in each ciphertext , a different L is used, we can not decrypt another ciphertext using L recovered from one ciphertext. Consequently, this attacks does not violate the IND-qCPA security notion because the challenge query is classical and knowing k_2 will not help to distinguish the encryption of two messages M_0 and M_1 when L used in the ciphertext is secret.

The security of OFB and CTR. By definition of OFB and CTR, we can represent them generally as $\mathsf{Enc}_k(M) = G_k(|M|;r) \oplus M$, where G is a pseudorandom bit generator that depends on the block cipher BC. For instance for OFB mode, the pseudo-random bit-string is generated as

$$\mathsf{BC}_k(r), \mathsf{BC}_k(\mathsf{BC}_k(r)), \mathsf{BC}_k\big(\mathsf{BC}_k(\mathsf{BC}_k(r))\big), \ldots$$

and its size depends on the size of the message block. For an encryption scheme of the form $\mathsf{Enc}_k(M) = G_k(|M|;r) \oplus M$, we can reduce the IND-qCPA security to the standard IND-CPA security, since a superposition query $\sum_i \alpha_i |M_i\rangle$, to the encryption scheme can be simulated using a classical encryption query on zero-bit-string of length $|M_i|$ and then calculating $\sum_i \alpha_i |M_i \oplus \mathsf{Enc}_k(0)\rangle$. Therefore, OFB and CTR are IND-qCPA secure if they are standard IND-CPA secure. The standard IND-CPA security of the underlying block cipher follows from the standard security of the PRF.

The security of CBC and OFB. Since a quantum query to the CBC and OFB modes of operation in the IND-qCPA security notion results in a quantum query to the underlying block cipher, their security will not follow using a standard secure PRF as shown above. However, we prove that CBC and OFB are IND-qCPA secure using a quantum secure PRF. The proof overview is as follows. We explain the proof for the CBC mode, and it is similar for OFB. By definition of CBC encryption, the encryption of $M = m_1 \ldots, m_n$ is $Enc_k^{(CBC)}(M) := c_0, \ldots, c_n$ where c_0 is a random string and $c_i = PRF_k(m_i \oplus c_{i-1})$ for $0 < i \leq n$. In the IND-qCPA notion, the adversary given oracle access to Enc_k^{CBC} tries to distinguish the encryption of two message blocks of its choice, let say $Enc_k^{CBC}(M_0)$ and $Enc_k^{CBC}(M_1)$. In other words, the adversary wins if he can guess the random bit b given the challenge ciphertext $C^* = (c_0^*, c_1^*, \ldots, c_n^*) = Enc_k^{CBC}(M_b)$. We show that replacing c_i^* by randomness step by step in the challenge ciphertest C^* will change the advantage of the adversary negligibly. More precisely, we define n hybrid games such that in i-th game, $c_0^*, c_1^*, \ldots, c_i^*$ are random elements and $c_{i+1}^*, \ldots, c_n^*$ are computed by Enc_k^{CBC}. Then, we show that the two successive games have negligible difference. Since in the last game the challenge ciphertext is a random string and it is independent of M_0 and M_1, the advantage of the adversary is $1/2$ in the last game. This proves that the advantage of the adversary in the first game (IND-qCPA) is at most $1/2 + \mathsf{negl}$. Now we show why two consecutive games have a negligible difference. Since the situation is similar for any two consecutive games, we look at the first game where Game 0 is the IND-qCPA game and in the Game 1, c_0^*, c_1^* are random elements and the rest are computed by Enc_k^{CBC}. In the proof, we use the One-way to Hiding (O2H) Lemma, Lemma 5 in chapter 2, that states for a random input $c_0^* \oplus m_1^b$ and random oracle PRF_k, the advantage of a quantum adversary $\mathcal{A}$ making at most q queries to PRF_k, in distinguishing $PRF_k(c_0^* \oplus m_1^b)$ from a random element is bounded approximately by the success probability of an adversary B that chooses a random query $i \xleftarrow{\$} [q]$ of $\mathcal{A}$, measures the input of the i-th query and returns 1 if the measurement output is $c_0^* \oplus m_1^b$. To be accurate syntactically in using the One-way to Hiding (O2H) Lemma, we need to define a adversary $\mathcal{A}_{o2h}$ that is constructed from $\mathcal{A}$ as follows: The adversary $\mathcal{A}_{o2h}$ given oracle access to PRF and on input (x, y) runs the adversary $\mathcal{A}$. It is clear that $\mathcal{A}_{o2h}$ can answer to $\mathcal{A}$'s learning queries using his oracle PRF. In the challenge query, $\mathcal{A}_{o2h}$ picks a random bit and responds with $C^* = (c_0^*, c_1^*, \ldots, c_n^*)$ where $c_0^* = x \oplus m_1^b$, $c_1^* = y$ and the rest of challenge ciphertext are computed similar to Enc_{CBC}^{PRF}. At the end, $\mathcal{A}_{o2h}$ returns 1 if $\mathcal{A}$ guesses b correctly and it return 0 otherwise. It is clear that the success probability in Game 0 is exactly the same as the success probability of $\mathcal{A}_{2oh}$ given input $(x, PRF(x))$ for random x and the success probability of Game 1 is the same as the success probability of $\mathcal{A}_{2oh}$ given input (x, y) for random x and y. Therefore using O2H lemme we can argue that the difference between the success probability of two games 0 and 1 is upper bounded by the success probability of the adversary B that runs $\mathcal{A}_{o2h}$, measures the argument of a random query to PRF and declares success if it measures x. We have three cases based on the random query (i-th query) that is measured by the adversary B.

- If i-th query occurs before the challenge query, then obviously the advantage of two games are negligible because $m_1^b \oplus c_0^*$ is a random element since c_0^* is a uniformly random element and m_1^b is chosen after the i-th query. In other words, the input that is measured in the i-th query is independent of $m_1^b \oplus c_0^*$, therefore the probability of success for B (the probability that the measurement output of B is $m_1^b \oplus c_0^*$) is negligible.
- B measures a query during the challenge query. Note that c_0^* and c_1^* are computed using the input (x, y) of $\mathcal{A}_{o2h}$ and to compute the rest of challenge ciphertext, $\mathcal{A}_{o2h}$ queries its oracle PRF. The queries are :

  $PRF(m_2^b \oplus y), PRF(m_3^b \oplus PRF(m_2^b \oplus y)), PRF(m_4^b \oplus PRF(m_3^b \oplus PRF(m_2^b \oplus y))), \ldots$

  Since the challenge query is purely classical and x is a uniformly random element, then the probability of success is negligible for B.

- The i-th query occurs after the challenge query has been made. The queries to *PRF* are in superposition and we can not use the argument above. Instead we show that a measurement on input registers and on computational basis can commute with the unitary gates used to evaluate the encryption algorithm. Therefore, the measurement performed by B can be made at the beginning of the encryption circuit and we can assume that the queries are classical. Then we use the argument made in the second bullet point above to show that the probability of measuring x is negligible.

These three cases show that the success probability of B is negligible. Sine the difference between the success probability of Game 0 and Game 1 are upper bounded by the success probability of B, Game 0 and Game 1 are indistinguishable.

6.3. Discussion: Open Problems and Related Works

We verify the security of Modes of operation against IND-qCPA that is defined in [19] by Boneh and Zhandry. In the case of XTS mode, we present an attack to XTS_{BC} where BC is constructed in a way that leaks half of the secret key to a quantum adversary. The adversary can decrypt the remaining part of the ciphertext that is under the attack and has not been used to obtain the secret key k_2 and the parameter L. However, we could not show that this attack violates the IND-qCPA notion of XTS because the challenge query is classical (while learning queries can be in superposition) and L used in the challenge query remains secret. This issue may raise some questions: Has IND-qCPA notion been defined properly in [19]? Why quantum learning queries but classical challenge queries? Authors in [19] justify the classical challenge queries in IND-qCPA notion by defining two other notions "IND-fqCPA" (Definition 4.1 in [19]) and "IND-lrCPA" (Definition 4.3 in [19]) with superposition queries during the challenge phase. Then, they show that no encryption scheme satisfies these two security notions. Even though this might help to understand the reason behind the classical restriction to adversarial queries during the challenge phase, but it is not a comprehensive justification because there are some other potential security definitions that they have not discussed. One needs to define all possible security notions and compare them to have a complete study. A comprehensive study of all possible quantum counterpart of IND-CPA notion is an open problem.

Simon's algorithm has been used in multiple research works to attack classical cryptographic constructions. Authors in [51] show that the 3-round Feistel cipher is distinguishable from a truly random permutation if one allows superposition queries to the construction. Their quantum algorithm uses Simon's algorithm to notice the periodicity caused by the Feistel construction. Since a random permutation is an one-one function with no period, their quantum algorithm can distinguish the 3-round Feistel cipher from a random permutation. In contrast in the classical setting, Luby and Rackoff prove the 3-round Feistel cipher is indistinguishable from a truly random permutation when in each round a truly random function is used [53]. The security or the insecurity of 4-round Feistel cipher against superposition queries is an interesting open problem. Simon's algorithm has been used in [52] to attack Even-Mansour block cipher. Their algorithm is allowed to make superposition queries to the construction and to the internal permutation used in the construction. One may suggest the use of constructions above in modes of operation as the block-cipher and show the insecurity. However, it is not clear how we can use the aforementioned result to violate IND-qCPA of modes of operations. Instead, we define some standard secure block-ciphers in the quantum random oracle model that are periodic in the secret key. Our insecurity result are in quantum random oracle model and constructing a counter example in the standard model is open.

In [50], Simon's algorithm has been used to attack many message authentication codes that are constructed by modes of operation. In particular, authors present a forgery attack to CBC-MAC. In contrast, we show that CBC modes of operation is IND-qCPA secure when underlying block cioher is qPRF. It is clear that their forgery attack can not be used to violate IND-qCPA security because *IV* is chosen randomly in each query in CBC mode of operation and it is not in control of adversary while in CBC-MAC, *IV* is fixed to zero bit-string. It easy to get around their forgery attack if one make CBC-MAC signing algorithm a randomized algorithm as following. We present three algorithms *Gen*, *Sign* and $Verify$ of RCBC-MAC.
Gen : It outputs two secret keys k, k'.
Sign : On input k,k' and message $M := m_1, m_2, \dots, m_\ell$ chooses random $c_0 \in \{0,1\}^n$ and calculates $c_i = \mathsf{BC}_k(c_{i-1} \oplus m_i)$ for $i \in [\ell]$. Finally, it returns $t = (c_0, \mathsf{BC}_{k'}(x_\ell))$
$Verify$: On input $(M, t = (c_0, t_2))$ it outputs 1 if $c_i = \mathsf{BC}_k(c_{i-1} \oplus m_i)$ for $i \in [\ell]$ and $t_2 = \mathsf{BC}_{k'}(x_\ell)$. Otherwise it returns 0.

7. CONCLUSION

In this thesis we discuss the challenges caused by adversarial superposition queries to the security of multiple fundamental cryptographic constructions. On the positive side, we prove the post-quantum security of Fujisaki-Okamoto construction, OAEP construction and some modes of operation. In the light of NIST[1] competition, our result has been used in multiple candidates to propose an IND-CCA secure scheme for the competition. To achieve post-quantum security, we overcome some challenges in the quantum security proofs, for instance, how to reprogramme a random oracle when adversary has superposition access to the oracle, how to extract the input of a superposition query that the adversary makes to the random oracle in a specific case, etc. We study the collision-resistance property of non-uniformly distributed functions when the adversary has superposition access to the function. Our result consists of many security proof techniques. For instance, we show how to decompose a non-uniform distribution to some nearly flat distributions and use this decomposition to reduce the quantum collision problem for a non-uniformly distributed function to the quantum collision problem for a uniformly distributed function, etc. On the negative side, we discuss the difficulties in proving the quantum indifferentiability of classical constructions. We present some quantum attacks to modes of operation that indicates the power of superposition queries.

In more details, we defined the indifferentiability in the quantum setting and showed that most of classical constructions are not perfectly quantum indifferentiable from a random oracle using a conjecture. We studied the quantum query complexity of collision problem for a non-uniformly distributed function. We used the quantum collision-resistance property of a function whose outputs are chosen according to a distribution with high min-entropy to prove the security of our modified version of Fujisaki-Okamoto construction in the quantum random oracle model. We present both upper bounds and lower bounds for the collision problem. We studied the IND-qCPA security of modes of operation. We showed that OFB and CTR modes are IND-qCPA when underlying block cipher is standard secure. In contrast, CBC and OFB modes are not secure using standard secure block cipher and we showed their security using a quantum secure block cipher. For XTS, we present an attack using superposition queries that does not formally violate the IND-qCPA.

[1] National Institute of Standards and Technology

BIBLIOGRAPHY

[1] https://mathoverflow.net/questions/286152/the-generalization-of-commutative-property-of-orthogonal-projectors-on-a-subspac. Accessed: 2017-10-17.

[2] 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*, pages 229–242. IEEE Computer Society, 2009.

[3] Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *J. ACM*, 51(4):595–605, July 2004.

[4] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Unforgeable quantum encryption. *CoRR*, abs/1709.06539, 2017.

[5] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Unforgeable quantum encryption. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 489–519. Springer, 2018.

[6] Martin R. Albrecht, Emmanuela Orsini, Kenneth G. Paterson, Guy Peer, and Nigel P. Smart. Tightly secure ring-lwe based key encapsulation with short ciphertexts. In *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part I*, pages 29–46, 2017.

[7] Andris Ambainis. Quantum lower bounds by quantum arguments. In F. Frances Yao and Eugene M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 636–643. ACM, 2000.

[8] Andris Ambainis. Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range. *Theory of Computing*, 1(1):37–46, 2005.

[9] Andris Ambainis. Quantum walk algorithm for element distinctness. *SIAM J. Comput.*, 37(1):210–239, 2007.

[10] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, pages 474–483. IEEE Computer Society, 2014.

[11] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems (the hardness of quantum rewinding). In *FOCS 2014*, pages 474–483. IEEE, October 2014.

[12] Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh. Post-quantum security of the cbc, cfb, ofb, ctr, and XTS modes of operation. In Tsuyoshi Takagi, editor, *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, volume 9606 of *Lecture Notes in Computer Science*, pages 44–63. Springer, 2016.

[13] Marko Balogh, Edward Eaton, and Fang Song. Quantum collision-finding in non-uniform random functions. In *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, pages 467–486, 2018.

[14] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993.*, pages 62–73. ACM, 1993.

[15] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997.

[16] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the indifferentiability of the sponge construction. In Nigel P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 181–197. Springer, 2008.

[17] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.

[18] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *Crypto 2013*, 2013. Full version at IACR ePrint 2013/088.

[19] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. `https://eprint.iacr.org/2013/088`, 2013. The definition of IND-qCPA only appear in this eprint, not in the conference version.

[20] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, and Damien Stehlé. CRYSTALS

- kyber: a cca-secure module-lattice-based KEM. *IACR Cryptology ePrint Archive*, 2017:634, 2017.

[21] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, 46(4-5):493–505, 1998.

[22] Gilles Brassard, Peter Høyer, Kassem Kalach, Marc Kaplan, Sophie Laplante, and Louis Salvail. Merkle puzzles in a quantum world. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 391–410. Springer, 2011.

[23] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum algorithm for the collision problem. *ACM SIGACT News (Cryptology Column)*, 28:14–19, 1997.

[24] Gilles Brassard and Louis Salvail. Quantum merkle puzzles. In *Second International Conference on Quantum, Nano, and Micro Technologies, ICQNM 2008, February 10-15, 2008, Sainte Luce, Martinique, French Caribbean*, pages 76–79. IEEE Computer Society, 2008.

[25] A Böttcher and Ilya Spitkovsky. A gentle guide to the basics of two projections theory. 432:1412–1459, 03 2010.

[26] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited (preliminary version). In Jeffrey Scott Vitter, editor, *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, pages 209–218. ACM, 1998.

[27] Tore Vincent Carstens, Ehsan Ebrahimi, Gelo Noel Tabia, and Dominique Unruh. On quantum indifferentiability. *IACR Cryptology ePrint Archive*, 2018:257, 2018.

[28] Larry Carter and Mark N. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18(2):143–154, 1979.

[29] Jung Hee Cheon, Kyoohyung Han, Jinsu Kim, Changmin Lee, and Yongha Son. A practical post-quantum public-key cryptosystem based on \textsf splwe. In Seokhie Hong and Jong Hwan Park, editors, *Information Security and Cryptology - ICISC 2016 - 19th International Conference, Seoul, South Korea, November 30 - December 2, 2016, Revised Selected Papers*, volume 10157 of *Lecture Notes in Computer Science*, pages 51–74, 2016.

[30] Jung Hee Cheon, Duhyeong Kim, Joohee Lee, and Yong Soo Song. Lizard: Cut off the tail! // practical post-quantum public-key encryption from LWE and LWR. *IACR Cryptology ePrint Archive*, 2016:1126, 2016.

[31] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM J. Comput.*, 17(2):230–261, 1988.

[32] Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya. Merkle-damgård revisited: How to construct a hash function. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 430–448. Springer, 2005.

[33] Jean-Sébastien Coron, Thomas Holenstein, Robin Künzler, Jacques Patarin, Yannick Seurin, and Stefano Tessaro. How to build an ideal cipher: The indifferentiability of the feistel construction. *J. Cryptology*, 29(1):61–114, 2016.

[34] Jan Czajkowski, Leon Groot Bruinderink, Andreas Hülsing, Christian Schaffner, and Dominique Unruh. Post-quantum security of the sponge construction. *IACR Cryptology ePrint Archive*, 2017:771, 2017.

[35] Dana Dachman-Soled, Jonathan Katz, and Aishwarya Thiruvengadam. 10-round feistel is indifferentiable from an ideal cipher. In Fischlin and Coron [40], pages 649–678.

[36] Özgür Dagdelen, Marc Fischlin, and Tommaso Gagliardoni. The fiat-shamir transformation in a quantum world. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part II*, volume 8270 of *Lecture Notes in Computer Science*, pages 62–81. Springer, 2013.

[37] Yuanxi Dai and John P. Steinberger. Indifferentiability of 8-round feistel networks. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 95–120. Springer, 2016.

[38] Ivan Damgård, Jakob Funder, Jesper Buus Nielsen, and Louis Salvail. Superposition attacks on cryptographic protocols. In *ICITS 2013*, volume 8317 of *LNCS*, pages 142–161. Springer, 2014. Online version IACR ePrint 2011/421.

[39] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer, 1986.

[40] Marc Fischlin and Jean-Sébastien Coron, editors. *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*. Springer, 2016.

[41] European Union Agency for Network and Information Security (ENISA). Algorithms, key sizes and parameters report - 2013 recommendations. October 2013. Available at `https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report`.

[42] 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, pages 537–554, London, UK, UK, 1999. Springer-Verlag.

[43] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996.

[44] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the fujisaki-okamoto transformation. In Yael Kalai and Leonid Reyzin, editors, *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I*, volume 10677 of *Lecture Notes in Computer Science*, pages 341–371. Springer, 2017.

[45] Roger A. Horn and Charles R. Johnson. *Matrix analysis*. Cambridge University Press, 1990.

[46] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Construction of a pseudo-random generator from any one-way function. *SIAM Journal on Computing*, 28:12–24, 1993.

[47] Andreas Hülsing, Joost Rijneveld, John M. Schanck, and Peter Schwabe. High-speed key encapsulation from NTRU. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 232–252. Springer, 2017.

[48] Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. *IACR Cryptology ePrint Archive*, 2015:1256, 2015.

[49] C. Jordan. In *Bulletin de la S. M. F.*, pages 3,103, 1875.

[50] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 207–237. Springer, 2016.

[51] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round feistel cipher and the random permutation. In *IEEE Interna-*

tional Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings, pages 2682–2685. IEEE, 2010.

[52] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type even-mansour cipher. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, pages 312–316. IEEE, 2012.

[53] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[54] Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In Moni Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2004.

[55] Michael Mitzenmacher and Eli Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, New York, NY, USA, 2005.

[56] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[57] Chris Peikert. Lattice cryptography for the internet. In Michele Mosca, editor, *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings*, volume 8772 of *Lecture Notes in Computer Science*, pages 197–219. Springer, 2014.

[58] Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton. Careful with composition: Limitations of the indifferentiability framework. In *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, pages 487–506, 2011.

[59] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[60] Victor Shoup. OAEP reconsidered. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 239–259. Springer, 2001.

[61] Daniel R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, 1997.

[62] Ehsan Ebrahimi Targhi and Dominique Unruh. Post-quantum security of the fujisaki-okamoto and OAEP transforms. In Martin Hirt and Adam D. Smith, editors, *Theory of Cryptography - 14th International Conference,*

TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II, volume 9986 of *Lecture Notes in Computer Science*, pages 192–216, 2016.

[63] Ehsan Ebrahimi Targhi and Dominique Unruh. Quantum collision-resistance of non-uniformly distributed functions: Upper and lower bounds. *IACR Cryptology ePrint Archive*, 2017:575, 2017.

[64] Dominique Unruh. Quantum proofs of knowledge. In *Eurocrypt 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, April 2012.

[65] Dominique Unruh. Everlasting multi-party computation. In *Crypto 2013*, volume 8043 of *LNCS*, pages 380–397. Springer, 2013. Preprint on IACR ePrint 2012/177.

[66] Dominique Unruh. Quantum position verification in the random oracle model. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II*, volume 8617 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2014.

[67] Dominique Unruh. Revocable quantum timed-release encryption. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 129–146. Springer, 2014.

[68] Dominique Unruh. Computationally binding quantum commitments. In Fischlin and Coron [40], pages 497–527.

[69] Dominique Unruh. Post-quantum security of fiat-shamir. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 65–95. Springer, 2017.

[70] John Watrous. Quantum computational complexity. In Robert A. Meyers, editor, *Encyclopedia of Complexity and Systems Science*, pages 7174–7201. Springer, 2009.

[71] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009.

[72] Michael J. Wiener. Bounds on birthday attack times. *IACR Cryptology ePrint Archive*, 2005:318, 2005.

[73] Henry Yuen. A quantum lower bound for distinguishing random functions from random permutations. *Quantum Information & Computation*, 14(13-14):1089–1097, 2014.

[74] 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*, pages 679–687. IEEE Computer Society, 2012.

[75] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Information & Computation*, 15(7&8):557–567, 2015.

[76] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. *IACR Cryptology ePrint Archive*, 2018:276, 2018.

ACKNOWLEDGEMENT

I appreciate the support of my supervisor, Dominique Unruh, during my PhD studies. Many thanks to him for his incredible teaching, incredible analytical mind, thoughtful guidance, and humble patience.

I would like to thank the reviewers, Frédéric Dupuis, Marc Kaplan, and Sven Laur (alphabetical order) for their detailed and useful comments and suggestions. Their comments and suggestions have improved the thesis considerably.

I would like to thank the administrative staff at the University of Tartu. The time needed for an administrative task is negligible! at the University of Tartu. Many thanks to Janno Siim for his Estonian translation of the abstract of the thesis. Many thanks to whom that I have learned from, these include the teaching and the research staff of the university and my co-authors.

This work was supported by the Estonian ICT program 2011-2015 (3.2.1201.13 0022), the European Union through the European Regional Development Fund through the sub-measure "Supporting the development of R&D of info and communication technology", by the Estonian Center of Excellence in Computer Science, EXCS, by institutional research funding IUT2-1 of the Estonian Ministry of Education and Research.

SUMMARY IN ESTONIAN

Krüptograafiliste konstruktsioonide turvalisus superpositsioonpäringute vastu

Kvantajastu lähenedes on tekkinud vajadus analüüsida olemaolevate krüptograafiliste konstruktsioonide turvalisust kvantruünnete vastu. Postkvantkrüptograafia on tärkav valdkond, mis klassikalise krüptograafia konstruktsioonide vastupidavust kvantrünnetele. See tähendab, et ausad osapooled kasutavad ainult klassikalisi seadmeid, samas kui ründaja võib kasutada ka kvantarvutusvõimekusega seadmeid. Kuna mitmed avaliku võtme krüptosüsteemid, mis põhinevad algarvudeks lahutamisel või diskreetse logaritmi leidmisel, on murtavad Shori algoritmiga, tuleks need eeldused asendada kvantturvaliste eeldustega ning seejärel välja pakkuda neil eeldustel põhinevad konstruktsioonid ja matemaatiliselt tõestada nende turvalisus. Kvantründajate ebatavalise olemuse tõttu ei pruugi klassikalistest tõestusvõtetest piisata ning seega võib konstruktsioonide turvalisuse tõestamine osutuda suureks väljakutseks. Antud väitekirjas keskendume mitme erineva krüptograafilise konstruktsiooni kvantturvalisuse tõestamisele. Tõestame, et modifikatsioon Fujisaki-Okamoto (FO) konstruktsioon, mis teisendab kaks nõrgalt turvalist krüpteerimisalgoritmi tugevalt turvaliseks krüpteerimisalgoritmiks kasutades kolme räsifunktsiooni kvantjuhuoraakli mudelis, kus kvantründaja saab juhuoraaklile esitada superpositsioonpäringuid, on postkvant-turvaline. Selleks, et tõestada FO konstruktsiooni turvalisus, peame uurima räsifunktsioonide omadusi kvantkeskkonnas. Defineerime Eristamatuse Raamistiku kvantkeskkonnas ja näitame, et klassikalised räsifunktsioonide konstruktsioonid ei ole juhuslikust oraaklist perfektselt kvanteristamatud. Meie kvantdefinitsioon eristamatusest on rakendatav postkvantkeskkonnas, kus kvantründajal on klassikaline ligipääs konstruktsioonile ja kvantligipääs konstruktsioonis kasutatavale krüptograafilisele primitiivile. Negatiivsete tulemuste tõttu uurime funktsioonide kvantkollisioonikindluse omadust, kus funktsiooni väljundid ei ole ühtlase jaotusega ja kvantründajal on kvantligipääs funktsioonile. Tuletame alam- ja ülempiirid funktsiooni väljundi jaotise miinimumentroopia ja kollisioonientroopia kohta. Kasutame mitte-ühtlase jaotusega funktsioonide kollisioonikindluse omadust, kus väljundil on kõrge miinimumentroopia, et näidata FO konstruktsiooni turvalisust kvantjuhuoraakli mudelis. Kasutame samu võtteid, et tõestada OAEP teisenduse turvalisus kvantjuhuoraakli mudelis. Lõpetuseks uurime plokkšifri tööviiside turvalisust superpositsiooniliste tavateksti rünnete tavateksti rünnete (*quantum chosen plaintext attack*, edaspidi IND-qCPA) vastu, kus kvantründajal on kvantligipääs krüpteerimisoraaklile, kuid ta võib edastada vaid klassikalisi päringuid. Kasutades plokkšifrit, kus kvantründaja saab teha klassikalisi päringuid (standardne turvaline plokkšiffer), tõestame, et OFB ja CTR on turvalised IND-qCPA vastu. Konstrueerime näite, mis demonstreerib, et CBC, CFB ja XTS tööviis võivad standardseid turvalisi plokkšifreid kasutades olla ebaturvalised. Lõpuks näitame, et CBC ja CFB töörežiimid on IND-qCPA turvalised eeldusel, et kasutatav plokkšiffer on turvaline kvantrünnete vastu.

PUBLICATIONS

CURRICULUM VITAE

Personal data

Name:	Ehsan Ebrahimi
Birth:	September 11th, 1986
Citizenship:	Iranian
Language:	Persian, English
Contact:	ehasan.ebrahimi.targhi@ut.ee, ebrahimi.math@gmail.com

Education

2013–	University of Tartu, Institute of Computer Science, PHD student
2009–2012	M.Sc. In Mathematics, Shahid Beheshti University, Tehran, Iran
2005–2009	B.Sc. In Pure Mathematics, Shahrood University of Technology, Shahrood, Iran.

Employment

01.09.2016- 31.02.2019	University of Tartu, Research Project Specialist (0.5 p)
01.09.2014-31.08.2016	University of Tartu, Junior Research Fellow in Cryptography (0.5 p)
01.10.2013-31.08.2014	University of Tartu, Research Project Specialist (0.5 p)

Scientific work

Main fields of interest:

- Cryptography
- Quantum Computing
- Cryptocurrencies

Main scientific talks:

- Quantum Collision-Resistance of Non-uniformly Distributed Functions. Post-Quantum Cryptography Conference, 2016
- Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms, Theory of Cryptography Conference, 2016-B

ELULOOKIRJELDUS

Isikuandmed

Nimi:	Ehsan Ebrahimi
Sünniaeg ja-koht	11. september 1986
kodakondsus:	Iraani
Language:	pärsia, inglise
kontakt:	ebrahimi.math@gmail.com, ehasan.ebrahimi.targhi@ut.ee

Haridus

2013–	Tartu Ülikool
2009–2012	M.Sc. Matemaatika, Shahid Beheshti Ülikool, Teheran, Iraan
2005–2009	B.Sc. puhas matemaatika, Shahroodi Tehnoloogiaülikool, Shahrood, Iraan.

Teenistuskäik

01.09.2016- 31.02.2019	Tartu Ülikool, teadusprojekti spetsialist 0,5 k
01.09.2014-31.08.2016	Tartu Ülikool, krüptograafia nooremteadur 0,5 k
01.10.2013-31.08.2014	Tartu Ülikool, teadusprojekti spetsialist 0,5 k

Teaduslik töö

Peamised huvialad:

- krüptograafia
- kvanttehnoloogia
- krüptokursused

Peamised teaduslikud ettekanded:

- Quantum Collision-Resistance of Non-uniformly Distributed Functions. Post-Quantum Cryptography Conference, 2016
- Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms, Theory of Cryptography Conference, 2016-B

DISSERTATIONES INFORMATICAE PREVIOUSLY PUBLISHED IN DISSERTATIONES MATHEMATICAE UNIVERSITATIS TARTUENSIS

19. **Helger Lipmaa.** Secure and efficient time-stamping systems. Tartu, 1999, 56 p.
22. **Kaili Müürisep.** Eesti keele arvutigrammatika: süntaks. Tartu, 2000, 107 lk.
23. **Varmo Vene.** Categorical programming with inductive and coinductive types. Tartu, 2000, 116 p.
24. **Olga Sokratova.** Ω-rings, their flat and projective acts with some applications. Tartu, 2000, 120 p.
27. **Tiina Puolakainen.** Eesti keele arvutigrammatika: morfoloogiline ühestamine. Tartu, 2001, 138 lk.
29. **Jan Villemson.** Size-efficient interval time stamps. Tartu, 2002, 82 p.
45. **Kristo Heero.** Path planning and learning strategies for mobile robots in dynamic partially unknown environments. Tartu 2006, 123 p.
49. **Härmel Nestra.** Iteratively defined transfinite trace semantics and program slicing with respect to them. Tartu 2006, 116 p.
53. **Marina Issakova.** Solving of linear equations, linear inequalities and systems of linear equations in interactive learning environment. Tartu 2007, 170 p.
55. **Kaarel Kaljurand.** Attempto controlled English as a Semantic Web language. Tartu 2007, 162 p.
56. **Mart Anton.** Mechanical modeling of IPMC actuators at large deformations. Tartu 2008, 123 p.
59. **Reimo Palm.** Numerical Comparison of Regularization Algorithms for Solving Ill-Posed Problems. Tartu 2010, 105 p.
61. **Jüri Reimand.** Functional analysis of gene lists, networks and regulatory systems. Tartu 2010, 153 p.
62. **Ahti Peder.** Superpositional Graphs and Finding the Description of Structure by Counting Method. Tartu 2010, 87 p.
64. **Vesal Vojdani.** Static Data Race Analysis of Heap-Manipulating C Programs. Tartu 2010, 137 p.
66. **Mark Fišel.** Optimizing Statistical Machine Translation via Input Modification. Tartu 2011, 104 p.
67. **Margus Niitsoo**. Black-box Oracle Separation Techniques with Applications in Time-stamping. Tartu 2011, 174 p.
71. **Siim Karus.** Maintainability of XML Transformations. Tartu 2011, 142 p.
72. **Margus Treumuth.** A Framework for Asynchronous Dialogue Systems: Concepts, Issues and Design Aspects. Tartu 2011, 95 p.
73. **Dmitri Lepp.** Solving simplification problems in the domain of exponents, monomials and polynomials in interactive learning environment T-algebra. Tartu 2011, 202 p.

74. **Meelis Kull.** Statistical enrichment analysis in algorithms for studying gene regulation. Tartu 2011, 151 p.
77. **Bingsheng Zhang.** Efficient cryptographic protocols for secure and private remote databases. Tartu 2011, 206 p.
78. **Reina Uba.** Merging business process models. Tartu 2011, 166 p.
79. **Uuno Puus.** Structural performance as a success factor in software development projects – Estonian experience. Tartu 2012, 106 p.
81. **Georg Singer.** Web search engines and complex information needs. Tartu 2012, 218 p.
83. **Dan Bogdanov.** Sharemind: programmable secure computations with practical applications. Tartu 2013, 191 p.
84. **Jevgeni Kabanov.** Towards a more productive Java EE ecosystem. Tartu 2013, 151 p.
87. **Margus Freudenthal.** Simpl: A toolkit for Domain-Specific Language development in enterprise information systems. Tartu, 2013, 151 p.
90. **Raivo Kolde.** Methods for re-using public gene expression data. Tartu, 2014, 121 p.
91. **Vladimir Šor.** Statistical Approach for Memory Leak Detection in Java Applications. Tartu, 2014, 155 p.
92. **Naved Ahmed.** Deriving Security Requirements from Business Process Models. Tartu, 2014, 171 p.
94. **Liina Kamm.** Privacy-preserving statistical analysis using secure multi-party computation. Tartu, 2015, 201 p.
100. **Abel Armas Cervantes.** Diagnosing Behavioral Differences between Business Process Models. Tartu, 2015, 193 p.
101. **Fredrik Milani.** On Sub-Processes, Process Variation and their Interplay: An Integrated Divide-and-Conquer Method for Modeling Business Processes with Variation. Tartu, 2015, 164 p.
102. **Huber Raul Flores Macario.** Service-Oriented and Evidence-aware Mobile Cloud Computing. Tartu, 2015, 163 p.
103. **Tauno Metsalu.** Statistical analysis of multivariate data in bioinformatics. Tartu, 2016, 197 p.
104. **Riivo Talviste.** Applying Secure Multi-party Computation in Practice. Tartu, 2016, 144 p.
108. **Siim Orasmaa.** Explorations of the Problem of Broad-coverage and General Domain Event Analysis: The Estonian Experience. Tartu, 2016, 186 p.
109. **Prastudy Mungkas Fauzi.** Efficient Non-interactive Zero-knowledge Protocols in the CRS Model. Tartu, 2017, 193 p.
110. **Pelle Jakovits.** Adapting Scientific Computing Algorithms to Distributed Computing Frameworks. Tartu, 2017, 168 p.
111. **Anna Leontjeva.** Using Generative Models to Combine Static and Sequential Features for Classification. Tartu, 2017, 167 p.
112. **Mozhgan Pourmoradnasseri.** Some Problems Related to Extensions of Polytopes. Tartu, 2017, 168 p.

113. **Jaak Randmets.** Programming Languages for Secure Multi-party Computation Application Development. Tartu, 2017, 172 p.
114. **Alisa Pankova.** Efficient Multiparty Computation Secure against Covert and Active Adversaries. Tartu, 2017, 316 p.
116. **Toomas Saarsen.** On the Structure and Use of Process Models and Their Interplay. Tartu, 2017, 123 p.
121. **Kristjan Korjus.** Analyzing EEG Data and Improving Data Partitioning for Machine Learning Algorithms. Tartu, 2017, 106 p.
122. **Eno Tõnisson.** Differences between Expected Answers and the Answers Offered by Computer Algebra Systems to School Mathematics Equations. Tartu, 2017, 195 p.

DISSERTATIONES INFORMATICAE UNIVERSITATIS TARTUENSIS

1. **Abdullah Makkeh**. Applications of Optimization in Some Complex Systems. Tartu 2018, 179 p.
2. **Riivo Kikas.** Analysis of Issue and Dependency Management in Open-Source Software Projects. Tartu 2018, 115 p.