박 사 학 위 논 문
Ph.D. Dissertation

블록암호 운용모드의 양자 안전성 분석

Quantum Resistance on Modes of Operation in Block Ciphers

2021

이 지 은 (李 知 恩 Lee, Jeeun)

한 국 과 학 기 술 원

Korea Advanced Institute of Science and Technology

박 사 학 위 논 문

블록암호 운용모드의 양자 안전성 분석

2021

이 지 은

한 국 과 학 기 술 원

전산학부

블록암호 운용모드의 양자 안전성 분석

이 지 은

위 논문은 한국과학기술원 박사학위논문으로
학위논문 심사위원회의 심사를 통과하였음

2020년 12월 15일

심사위원장 김 광 조 (인)

심 사 위 원 권 대 성 (인)

심 사 위 원 이 주 영 (인)

심 사 위 원 이 준 구 (인)

심 사 위 원 최 두 호 (인)

Quantum Resistance on Modes of Operation in Block Ciphers

Jeeun Lee

Advisor: Kwangjo Kim

A dissertation submitted to the faculty of
Korea Advanced Institute of Science and Technology in
partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Computer Science

Daejeon, Korea
December 15, 2020

Approved by

Kwangjo Kim
Professor of Computing

The study was conducted in accordance with Code of Research Ethics[1].

[1] Declaration of Ethical Conduct in Research: I, as a graduate student of Korea Advanced Institute of Science and Technology, hereby declare that I have not committed any act that may damage the credibility of my research. This includes, but is not limited to, falsification, thesis written by someone else, distortion of research findings, and plagiarism. I confirm that my thesis contains honest conclusions based on my own careful research under the guidance of my advisor.

DCS 이지은. 블록암호 운용모드의 양자 안전성 분석. 전산학부 . 2021년. 39+iii 쪽. 지도교수: 김광조. (영문 논문)
Jeeun Lee. Quantum Resistance on Modes of Operation in Block Ciphers. School of Computing . 2021. 39+iii pages. Advisor: Kwangjo Kim. (Text in English)

초 록

양자 컴퓨팅에 대한 개념이 처음 제안된 1980년대부터 양자 컴퓨터의 실제적 구현과 양자 특성을 이용한 알고리즘의 개발에 대해 많은 연구가 있었다. 이 중 양자 알고리즘은 큐비트의 양자역학적 성질을 이용하여 기존의 고전 컴퓨터가 해결하지 못하는 문제를 뛰어난 성능으로 해결할 수 있다는 점을 보였다. 양자 계산 능력을 가진 양자 공격자의 등장은 암호학계에도 큰 영향을 주었다. 기존 컴퓨터에 기반하여 설계된 현재 암호체계가 더 이상 안전하지 않을 수 있다는 점이 문제로 나타났으며, 이는 다양한 암호체계에 대한 양자 안전성 연구 필요성을 대두시켰다.

이 연구에서는 가장 널리 쓰이고 있는 암호 기법 중 하나인 블록암호 운용방식들, 예를 들어 CBC, IGE, CFB, OFB, CTR의 양자 안전성을 연구하였다. 먼저, 양자계산능력에 따라 양자 공격자를 Q0, Q1, Q2로 분류한 뒤, 이러한 분류에 따라 양자 안전성에 대한 새로운 증명기법과 그것의 응용을 제시하였다. 운용되는 블록암호의 안전성 또한 Q0, Q1, Q2로 분류하여 가정하였고, 분석의 용이를 위해 각 운용방식을 양자 회로로 표현하였다. 다음으로, 목표하는 안전성 개념을 기존의 비구별성(indistinguishability, IND)과 선택 평문 공격(chosen-plaintext attack, CPA)을 양자 환경으로 확장하여 양자 선택 평문 공격에 대한 비구별성(IND-qCPA), 양자 선택 평문 공격에 대한 약한 양자 비구별성(wqIND-qCPA), 그리고 양자 선택 평문 공격에 대한 양자 비구별성(qIND-qCPA)를 정의하였다. 마지막으로, 이러한 다양한 양자 안전성 정의들에 따라 각 운용방식들이 Q0, Q1, Q2 블록암호를 쓸 때 어떤 양자 안전성을 갖는지 비교 및 분석하였다.

핵 심 낱 말 양자 공격자; 양자 안전성; 양자 회로; 블록암호; 운용방식

Abstract

Since quantum computing was proposed in the early 1980s, quantum computers and their novel algorithms have been developed. There are known advantages that quantum computers have over classical computers due to their quantum-mechanical properties using qubits. The fact that there may be more powerful adversaries capable of quantum computation has had a huge impact on the field of cryptography; The security of the existing cryptosystems is no longer guaranteed against quantum adversaries. The research on quantum security of cryptosystems, therefore, should be thoroughly investigated.

In this research, as one of the most widely used cryptographic primitives, confidentiality modes of operation in block ciphers are examined: CBC, IGE, CFB, OFB, and CTR. First, quantum adversaries are classified as Q0, Q1, and Q2 depending on their ability to perform quantum computation. The corresponding new quantum proof techniques are also presented. Then the underlying block ciphers are assumed as pseudorandom functions which are Q0, Q1, and Q2 secure. Also, modes of operation to be investigated are represented in the quantum circuit. Next, our desired security notions are considered in terms of quantum version of indistinguishability (IND) and chosen-plaintext attack (CPA): IND under quantum CPA (IND-qCPA), weak-quantum IND under quantum CPA (wqIND-qCPA), and quantum IND under quantum CPA (qIND-qCPA). In conclusion, the security of each mode in Q0-, Q1-, or Q2-secure block ciphers is analysed and compared in these various quantum security game scenarios.

Keywords quantum adversaries; quantum security; quantum circuits; block ciphers; modes of operation

Contents

Contents i
List of Figures iii

Chapter 1. Introduction **1**
1.1 Related Work 1
1.2 Our Contribution 2

Chapter 2. Quantum Adversaries **3**
2.1 Modelling Quantum Adversaries 3
2.2 Quantum Query Algorithms 3
2.3 Quantum Proof Techniques 4
2.3.1 Adaptive Programmability 4
2.3.2 Rewinding 7
2.3.3 Extractability 9
2.3.4 Challenge injection 11
2.3.5 Efficient Simulation 13
2.4 Quantum Security Notions 14
2.4.1 IND-qCPA 17
2.4.2 wqIND-qCPA 18
2.4.3 qIND-qCPA 18

Chapter 3. Modes of Operation in Block Ciphers **19**
3.1 Electronic Codebook (ECB) 19
3.2 Cipher Block Chaining (CBC) 19
3.3 Infinite Garble Extension (IGE) 20
3.4 Simplified Cipher Feedback (CFB) 20
3.5 Output Feedback (OFB) 20
3.6 Counter (CTR) 21
3.7 Modelling Block Ciphers 21

Chapter 4. Quantum Security of Modes of Operation **24**
4.1 IND-qCPA 24
4.1.1 Insecurity of CBC/IGE/CFB Mode under Q1-secure PRF 24
4.1.2 Security of OFB/CTR Mode under Q1-secure PRF . . . 26

4.1.3 Security of CBC/IGE/CFB/OFB/CTR Mode under Q2-secure PRF 26
4.2 (w)qIND-qCPA 29
4.2.1 Insecurity of CBC/IGE/CFB/OFB/CTR Mode under Q2-secure PRF 29

Chapter 5. Concluding Remarks 30

Bibliography 31

Acknowledgements 35

Curriculum Vitae 36

List of Figures

2.1 Modelling quantum adversaries as Q0, Q1, and Q2 3
2.2 Quantum circuit diagram for BZ attack 15
2.3 Security tree for checking all possible notions. Excluding 9 unreasonable notions (written in grey) and 3 unachievable notions (crossed out) leaves 4 notions. 17

3.1 CBC/IGE/CFB mode encryption in quantum circuits 22
3.2 OFB/CTR mode encryption in quantum circuits 23

4.1 Quantum circuits for an attack on each mode using Simon's algorithm 24
4.2 Quantum adversary's advantage to distinguish the challenge ciphertext and truly random string. 26
4.3 Quantum circuits for an attack on each mode 29

5.1 Summary 30

Chapter 1. Introduction

1.1 Related Work

As more and more refined classical, i.e. non-quantum, computers are developed, several problems have been encountered. Since the number of transistors in a dense integrated circuit has doubled approximately every 18 months [Moo65], the gaps between transistor terminals would shrink to the classical limits at some point. Then the electrons are able to move between terminals by quantum tunnelling phenomenon, that is, a transistor in an off state could be unexpectedly switched on even if it is not supposed to be. Also, classical computers use logically irreversible manipulation of information where the output of a device does not uniquely define the inputs, for example, by erasing a bit or merging two computation paths. This necessarily implies physical irreversibility and corresponding heat increase by $nkT \ln 2$ for erasure of n-bit known information, where k is the Boltzmann constant and T is the temperature of the heat sink in kelvins [Lan61].

Quantum computers have been proposed as a natural solution to circumventing the aforementioned problems since 1980s [Man80, Fey82, Ben80]. Quantum computers are based on quantum mechanics, which applies to all systems ranging from micro to macro scales, and use quantum bits, i.e. qubits, to create quantum logic gates for quantum computing. A pure qubit can be represented as a linear superposition of the basis states, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where the complex numbers α and β satisfy $|\alpha|^2 + |\beta|^2 = 1$. We may then use n qubits to represent either 2^n different superposed states, or entangled states. Besides, quantum computers use logically reversible manipulation where the output of a device always uniquely determines its input, by using an injective function for mapping old states to new ones. Such manipulation requires no release of heat in principle [Lan61]. For these reasons, quantum computing has attracted research interest both academically and commercially since its initial proposal.

The corresponding quantum algorithms were also proposed: After the publication of Deutsch's groundbreaking paper [Deu85], many quantum algorithms have been introduced, the most famous of which are Simon's algorithm [Sim94, Sim97], Shor's algorithm [Sho94, Sho97], and Grover's algorithm [Gro96, Gro97]. Using these algorithms, there are known advantages that quantum computers have over classical computers. Shor's algorithm could break classical asymmetric encryption and digital signature schemes based on integer factorization and discrete logarithm problems in polynomial time.

Also, classical symmetric encryption schemes would not be safe due to Grover's and Simon's algorithms. It has been believed until recently that doubling the key size would provide security against Grover's algorithm [CJL+16, ABB+15], however, widely used modes of operation for authenticity and authenticated encryption have proved to be completely broken using Simon's algorithm [KLLNP16, SS17]. The fact that there may be more powerful adversaries capable of quantum computation has had a huge impact on the field of cryptography; The security of the existing cryptosystems is no longer guaranteed against quantum adversaries when large-scale quantum computers are available. Accordingly, quantum security of the current cryptosystems should be thoroughly investigated. The cryptographic community has started to develop new security notions and proof models [BDF+11, BJ15, GHS16, Gag17, SLL16].

1.2 Our Contribution

In this work, we investigated many known quantum concepts that were extended from the classical ones. For a systematic study, we first classified *quantum adversaries* as Q0, Q1, and Q2 depending on their ability to perform quantum computation. The corresponding useful quantum proof techniques were introduced, which are used in our security proof later. The security games are extended to quantum case, then, their security notions are defined in terms of quantum version of indistinguishability (IND) and chosen-plaintext attack (CPA): IND under quantum CPA (IND-qCPA), weak-quantum IND under quantum CPA (wqIND-qCPA), and quantum IND under quantum CPA (qIND-qCPA). Since we chose our target as confidentiality modes of operation in block ciphers, we described some of known modes such as cipher block chaining (CBC), infinite garble extension (IGE), simplified cipher feedback (CFB), output feedback (OFB), and counter (CTR) modes. They were represented in quantum circuit diagrams for their quantum security analysis. Finally, quantum security analysis of given modes of operation was done under the assumption that the underlying block cipher is Q0-, Q1-, or Q2-secure pseudorandom functions (PRFs): Their quantum attacks using quantum circuits or provable security was given. All results were discussed and compared at the very end.

Chapter 2. Quantum Adversaries

2.1 Modelling Quantum Adversaries

As shown in Figure 2.1, the quantum adversaries can be classified as Q0, Q1, and Q2 depending on their ability to perform quantum computation. The Q0 adversary, i.e. classical adversary, has no access to an oracle quantumly nor power to do quantum computation. The Q1 adversary makes classical queries to an oracle and processes classical data with quantum computation locally. The powerful Q2 adversary can make quantum queries, i.e. superposition-based queries, and receives quantum states to perform quantum computation. This work is concentrated on Q1 and Q2 adversaries.

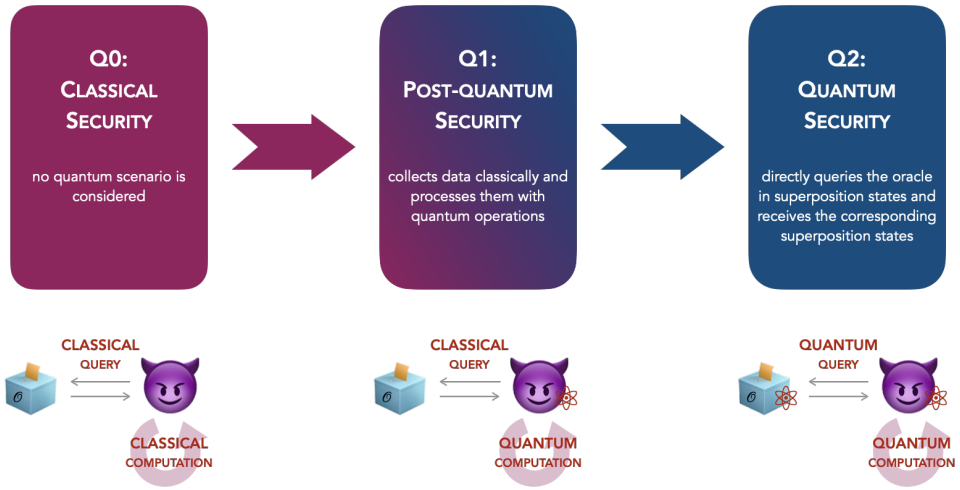


Figure 2.1: Modelling quantum adversaries as Q0, Q1, and Q2

2.2 Quantum Query Algorithms

As we considered quantum queries in Q2 adversary, quantum query algorithms should be investigated. In security analysis, the query model is useful because the number of queries an adversary needs to break a scheme corresponds to the time the attack succeeds. Consider a classical query algorithm that computes a Boolean function by using oracle queries, which is called a decision tree. It can be represented as a binary tree where each node represents a query, and its two children represent the two possible outcomes of the query. A leaf node represents the final answer 0 or 1. The depth of the tree, i.e. the number of queries needed to compute the function, is the cost of an algorithm.

According to [BBC+98], a quantum query algorithm with q queries is a quantum analogue of a classical query algorithm with q queries, where we use the power of quantum parallelism by making queries and operations in superposition. This can be represented in quantum circuits as a sequence of unitary transformations: $U_q O_f \ldots U_1 O_f U_0$. Here, U_i's are fixed unitary transformations that do not depend on inputs, and the (possibly) identical O_f's are unitary transformations that correspond to an oracle. For a general function $f : \{0,1\}^n \to \{0,1\}^m$, the oracle *standard* transformation O_f, called *quantum-accessible oracle*, maps basis state $|x, y\rangle$ to $|x, y \oplus f(x)\rangle$. Besides the standard transformation, there can be different transformations to implement an oracle such as *Fourier phase* oracle $|x, y\rangle \to e^{2\pi i f(x)y/2^m}|x, y\rangle$ and *minimal* oracle $|x\rangle \to |f(x)\rangle$ [KKVB02]. For constructing quantum security notions, the following quantum encryption oracles are defined respectively using standard and minimal oracles: one oracle mapping basis state $|\mathsf{m}, \mathsf{c}\rangle$ to $|\mathsf{m}, \mathsf{c} \oplus \mathsf{Enc}_\mathsf{k}(\mathsf{m})\rangle$ and the other mapping basis state $|\mathsf{m}\rangle$ to $|\mathsf{Enc}_\mathsf{k}(\mathsf{m})\rangle$. Then, the *quantum adversary* is defined to have an access to the quantum encryption oracle, i.e. be able to make queries and operations in superposition.

2.3 Quantum Proof Techniques

As classical random oracle (CRO) model has been regarded as an efficient security proof tool, [BDF+11] introduced quantum-accessible random oracle (QaRO) model to prove quantum security of classical cryptosystems. The QaRO model allows quantum adversaries' access to quantum computation such as superposition of inputs to random oracle, which gives quantum advantages, however, there are some weaknesses that cannot be extended naturally from CRO model. We investigated the difficulties of security reduction in the QaRO model, which caused by quantum mechanical properties such as no-cloning theorem and collapse during measurement: adaptive programmability, rewinding, extractability, challenge injection, and efficient simulation of QaRO.

2.3.1 Adaptive Programmability

Following [Nie02, FLR+10, BM15], as an important feature of the CRO model, *programmability* allows security reductions to dynamically select the outputs of an ideal hash function. For a standard security reduction technique, where the reduction tries to break the underlying hardness assumption, the reduction having oracle access to the adversary simulates the random oracle by answering queries made by the adversary. A random oracle can be simulated by adaptively setting or programming the outputs to a value of reduction's choice. As long as the distribution of the programmed output is uniform on the

specified range, any method for selecting these values is permitted.

If a reduction in the CRO model is *history-free*, then it can also be carried out in the QaRO model as in Theorem 2.3.1. History-free reductions basically answer random oracle queries independently of the history of previous queries. Since many signature schemes have security reductions involving reprogramming in the CRO model, i.e. not history-free, security reductions in the QaRO model is not known to hold. For reductions that are not history-free, adaptive reprogramming of the QaRO is required.

Theorem 2.3.1 ([BDF+11, Theorem 1]). *Let $\mathcal{S} = (G, S, V)$ be a signature scheme. Suppose that there is a history-free reduction that uses a classical PPT adversary A for $\mathcal{S}$ to construct a PPT algorithm B for a problem P. Further, assume that P is hard for polynomial-time quantum computers, and that quantum-accessible pseudorandom functions exist. Then $\mathcal{S}$ is secure in the QaRO model.*

The CRO model allows adaptive programming, i.e. the reduction can program the random oracle adaptively in the online phase of the security game depending on the query received from the adversary. In the QaRO model, however, it was considered to be difficult to program the random oracle adaptively since the quantum adversary can query the random oracle with a superposed state and get information about all exponentially many values right at the beginning.

Using One-way to Hiding Lemma

In order to program adaptively in the QaRO model, new techniques were developed by [Unr14] for the first time. It allows us to reduce the probability that the adversary notices that a random oracle has been reprogrammed to the probability of said adversary querying the oracle at the programmed location. It might be relatively trivial in the CRO model, but becomes non-trivial when the adversary can query superposed states:

Theorem 2.3.2 (Adaptive Programming of QaRO [Unr14, Theorem 10]). *Let $H : M \to N$ be a random oracle for finite M, N. (Infinite $M \subseteq \{0,1\}^*$ is also permissible.) Consider the following algorithms:*

- *The oracle algorithm A_0 that makes at most q_0 queries to H.*
- *The classical algorithm A_C that may access the classical part of the final state of A_0. Assume that for every initial state, the output of A_C has collision entropy at least k.*
- *The oracle algorithm A_1 that may access the final states of A_0 and A_C.*
- *The oracle algorithm A_2 that may access the final state of A_1; and A_1 and A_2 together perform at most q_{12} queries to H.*

- *Let C_1 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, output the measurement outcome. (When A_1 makes less than j queries, C_1 outputs $\perp \notin \{0,1\}^l$.)*

Let

$$
\begin{aligned}
P_A^1 \coloneqq \quad & \Pr\Big[b' = 1 : H \xleftarrow{\$} (M \to N),\ A_0^H(),\ x \leftarrow A_C(), \\
& \qquad A_1^H(x, H(x)),\ b' \leftarrow A_2^H(x, H(x))\Big] \\
P_A^2 \coloneqq \quad & \Pr\Big[b' = 1 : H \xleftarrow{\$} (M \to N),\ A_0^H(),\ x \leftarrow A_C(), \\
& \qquad B \xleftarrow{\$} N,\ A_1^H(x, B),\ H(x) \coloneqq B,\ b' \leftarrow A_2^H(x, B)\Big] \\
P_C \coloneqq \quad & \Pr\Big[x = x' : H \xleftarrow{\$} (M \to N),\ A_0^H(),\ x \leftarrow A_C(), \\
& \qquad B \xleftarrow{\$} N,\ j \xleftarrow{\$} \{1, \ldots, q_{12}\},\ x' \leftarrow C_1^H(j, B, x)\Big]
\end{aligned}
$$

Then $|P_A^1 - P_A^2| \leq (4 + \sqrt{2})\sqrt{q_0}2^{-k/4} + 2q_{12}\sqrt{P_C}$.

Using Hardness of Witness-Search Game

In Theorem 2.3.2, the oracle is queried at an adversarially chosen x which is *information-theoretically* undetermined, possessing a high min-entropy, $\min_x(-\log \Pr[X = x])$. By extending it to a computational setting, [ES15] came up with a new technique when the input is *computationally* difficult to decide by the adversary. They formalized a probabilistic game called *witness-search* and showed the computational hardness of witness-search allows for adaptively programming a QaRO.

Let Samp be an instance-sampling algorithm. On input 1^n, Samp generates public information pk, description of a predicate P, and a witness w satisfying $P(pk, w) = 1$. The witness-search game WS is defined as below:

Definition 2.3.1 (Witness-Search Game [ES15])**.**

- *Challenger C generates $(pk, w, P) \leftarrow \mathsf{Samp}(1^n)$. Ignore w. Let $W_{pk} \coloneqq \{w : P(pk, w) = 1\}$ be the collection of valid witnesses.*
- *$\mathcal{A}$ receives pk and produces a string $\hat{w}$ as output.*
- *We say $\mathcal{A}$ wins the game if $\hat{w} \in W_{pk}$.*

Lemma 2.3.3 (Hardness of WS to Programming QaRO [ES15, Lemma 5])**.** *Let two experiments E and E' be as below. If WS is hard, then* $\mathsf{Adv} \coloneqq |\Pr_E[b = 1] - \Pr_{E'}[b = 1]| \leq \mathsf{negl}(n)$.

- *Experiment E:*
  - *Generate* $(pk, w, P) \leftarrow \mathsf{Samp}(1^n)$.
  - $O \leftarrow \mathcal{F}$ *is drawn uniformly at random from the collection of all functions* $\mathcal{F}$.
  - $\mathcal{A}_1$ *receives* pk *as input and makes at most* q_1 *queries to* O. $\mathcal{A}_1$ *produces a classical string* x.
  - *Set* $z := O(x\|w)$.
  - $\mathcal{A}_2$ *gets* (x, w, z) *and may access the final state of* $\mathcal{A}_1$. $\mathcal{A}_2$ *makes at most* q_2 *queries to* O. *It outputs* $b \in \{0, 1\}$ *at the end.*
- *Experiment E':*
  - *Generate* $(pk, w, P) \leftarrow \mathsf{Samp}(1^n)$.
  - $O \leftarrow \mathcal{F}$ *is drawn uniformly at random from the collection of all functions* $\mathcal{F}$.
  - $\mathcal{A}_1$ *makes at most* q_1 *queries to* O. $\mathcal{A}_1$ *produces a classical string* x.
  - *Pick a random* $z \in_R \mathsf{Range}(O)$. *Reprogram* O *to* O': $O'(y) = O(y)$ *except that* $O'(x\|w) = z$.
  - $\mathcal{A}_2$ *gets* (x, w, z) *and may access the final state of* $\mathcal{A}_1$. $\mathcal{A}_2$ *makes at most* q_2 *queries to* O'. *It outputs* $b \in \{0, 1\}$ *at the end.*

Lemma 2.3.3 shows the computational assumption implies indistinguishability of two functions which a distinguisher has quantum access to: one is the zero function and the other marks a set of strings that could be used to break the computational assumption. Since the two functions are indistinguishable, any efficient quantum algorithm querying the random oracle cannot notice whether they have reprogrammed the QaRO.

Adaptive Reprogramming in TESLA

[ABB+17] gave a concrete tight security reduction for a signature scheme called TESLA, a lattice-based digital signature scheme, in the QaRO model. Their security reduction from learning with errors assumption adaptively reprograms QaRO using a technique from [BBBV97].

2.3.2 Rewinding

The CRO model uses *rewinding* [PS96] as a powerful tool to construct an extractor which extracts the witness w from the prover. Rewinding is a proof technique where the state of the adversary is stored and reproduced later, that is, it should be possible to make snapshots of the state and then later to go back to that snapshot.

In the QaRO model, however, it is difficult to rewind by reversing the unitary transformation or taking snapshots in a quantum setting due to no-cloning theorem and collapse during measurement: snapshots cannot be copied and interacting with a simulated machine may destroy information that would be needed later [vdG97, Proposition 4.5].

Watrous' Rewinding

In order to resolve this issue, [Wat09] introduced a specific type of quantum rewinding: whenever some machine rewinds another machine to an earlier point, the rewinding machine forgets everything it learned after that point. [Wat09, Lemma 9] was reformulated as below:

Lemma 2.3.4 (Quantum Rewinding with Small Perturbations [Unr10, Corollary 17])**.** *Let C, Z, E, Y be quantum registers, where C is one qubit register. Let S_1 be a unitary transformation operating on C, Z, Y and let $\mathbf{M}$ be a measurement in the computational basis on register C.*

For a quantum state $|\Psi\rangle$, let $p(|\Psi\rangle) \coloneqq \Pr[\mathsf{Succ} = 1 : S_1(CZY), \mathsf{Succ} \leftarrow \mathbf{M}(C)]$ where Z, E are jointly initialized with $|\Psi\rangle$ and Y, C are initialized with $|0\rangle$. In the same situation, let the density operator ρ^1_Ψ denote the state of ZE in the case of $\mathsf{Succ} = 1$.

Let $\varepsilon \in (0, 1/2)$. Let $q \in (\varepsilon, 1/2]$. Assume that for all $|\Psi\rangle$, $|p(|\Psi\rangle) - q| \leq \varepsilon$.

Then there exists a quantum circuit S operating on Z of size $O\left(\frac{\log(1/\varepsilon)\mathsf{size}(S_1)}{(q-\varepsilon)(1-q+\varepsilon)} =: k\right)$. S is a general quantum circuit, which may create auxiliary qubits, destroy them, and perform measurements. S can be computed in time $O(k)$ given the description of S_1. And for any $|\Psi\rangle$,

$$\mathrm{TD}(\rho^1_\Psi, \rho^2_\Psi) \leq 4\sqrt{\varepsilon}\frac{k}{\mathsf{size}(S_1)},$$

where the density operator ρ^2_Ψ denotes the state of ZE after execution of S when ZE is initialized with $|\Psi\rangle$.

Unruh's Rewinding

A rewinding technique in the context of a specific two-prover commitment scheme was developed in [CSST11, Lemma 1], which was reformulated as below:

Lemma 2.3.5 (Rewinding of mBQKW Commitment [Unr10, Lemma 10])**.** *Consider two projectors P_0 and P_1 of the form $P_i = U_i^\dagger(|\hat{w}_i\rangle\langle\hat{w}_i| \otimes I)U_i$. (Here U_0, U_1 are unitaries and $\hat{w}_0, \hat{w}_1 \in \{0,1\}^n$ for some n.) Consider a state $|\psi\rangle$. Let $p_i \coloneqq \||P_i|\psi\rangle\|^2$. (That is, p_i is the probability of measuring $\hat{w}_i$ in the first register after applying U_i to $|\psi\rangle$.) Let $p_\oplus \coloneqq \||P_1P_0|\psi\rangle\|^2$. (That is, $p_\oplus$ is the probability of measuring $\hat{w}_0$ after applying U_0 to $|\psi\rangle$ and subsequently measuring $\hat{w}_1$ after applying $U_1U_0^\dagger$.)*

Assume that $p_0 + p_1 \geq 1 + \varepsilon$ *for some* $\varepsilon \geq 0$. *Then* $p_\oplus \geq \varepsilon^2/4$.

[Unr10] pointed out that Lemma 2.3.4 technique only can be used to backtrack if the rewinding machine made a mistake that should be corrected, but cannot be used to collect and combine information from different branches of an execution. Also, Lemma 2.3.5 is specific to the case where there are only two possible measurements, i.e. $\#C = 2$. [Unr10] developed a new rewinding technique, by showing that the output that is measured contains little information about the state and thus does not disturb the state too much, of which core lemma is as below:

Lemma 2.3.6 (Extraction via Quantum Rewinding [Unr10, Lemma 8])**.** *Let* C *be a set with* $\#C = c$. *Let* $(P_i)_{i \in C}$ *be orthogonal projectors on a Hilbert space* $\mathcal{H}$. *Let* $|\Phi\rangle \in \mathcal{H}$ *be a unit vector. Let* $V := \sum_{i \in C} \frac{1}{c} \| P_i |\Phi\rangle \|^2$ *and* $E := \sum_{i,j \in C, i \neq j} \frac{1}{c^2} \| P_i P_j |\Phi\rangle \|^2$. *Then, if* $V \geq \frac{1}{\sqrt{c}}$, $E \geq V(V^2 - \frac{1}{c})$.

It should be noted that strict soundness is additionally required while only special soundness is needed in a classical setting.

Definition 2.3.2 (Special Soundness [Unr10, Definition 5])**.** *We say a* Σ*-protocol* (P, V) *for a relation* R *has special soundness if there is a deterministic polynomial-time algorithm* K_0 *(the special extractor) such that the following holds: for any two accepting conversations* $(\mathsf{com}, \mathsf{ch}, \mathsf{resp})$ *and* $(\mathsf{com}, \mathsf{ch}', \mathsf{resp}')$ *for* x *such that* $\mathsf{ch} \neq \mathsf{ch}'$ *and* $\mathsf{ch}, \mathsf{ch}' \in C_x$, *we have that* $w := \mathsf{K}_0(x, \mathsf{com}, \mathsf{ch}, \mathsf{resp}, \mathsf{ch}', \mathsf{resp}')$ *satisfies* $(x, w) \in R$.

Definition 2.3.3 (Strict Soundness [Unr10, Definition 6])**.** *We say a* Σ*-protocol* (P, V) *has strict soundness if for any two accepting conversations* $(\mathsf{com}, \mathsf{ch}, \mathsf{resp})$ *and* $(\mathsf{com}, \mathsf{ch}, \mathsf{resp}')$ *for* x, *we have that* $\mathsf{resp} = \mathsf{resp}'$.

2.3.3 Extractability

The *extractability* or *pre-image awareness*, i.e. the simulator learns the pre-images the adversary is interested in, is crucial to simulate decryption queries in the security proof for OAEP in the CRO model [Fis05]. In the QaRO model, it is unclear how to extract the right query since the actual query may be hidden in a superposition of exponentially many states. The different definition is needed in a quantum setting; we do not give the extractor the power to see the oracle queries.

Unruh's extractability

The *online extractability* was defined for an extractor, an algorithm $E(H, x, \pi)$ where H is assumed to be a description of the random oracle, x a statement and π a proof of x as below. E is supposed to output a witness. Inputs and outputs of E are classical.

Definition 2.3.4 (Online Extractability [Unr14, Definition 3]). *A non-int-eractive proof system (P, V) is online extractable with respect to S_{init} iff there is a polynomial-time extractor E such that for any quantum-polynomial-time oracle algorithm A, we have that*

$$\Pr[\text{ok} = 1 \wedge (x, w) \notin R \quad : \quad H \leftarrow S_{\text{init}}(), (x, \pi) \leftarrow A^H(), \\ \text{ok} \leftarrow V^H(x, \pi), w \leftarrow E(H, x, \pi)]$$

is negligible. We assume that both S_{init} and E have access to and may depend on a polynomial upper bound on the runtime of A.

The definition implies that it is impossible for an adversary to produce a proof for a statement for which he does not know a witness. The case, when the adversary can take one proof π_1 for one statement x_1 and transform π_1 into a valid proof for another statement x_2, however, is not excluded as long as a witness for x_2 could efficiently be computed from a witness for x_1. It is usually referred to as malleability. Therefore, simulation soundness, i.e. extraction of a witness from the adversary-generated proof should be successful even if the adversary has access to simulated proofs, is adapted to online extractability to avoid malleability:

Definition 2.3.5 (Simulation-sound Online Extrac-tability [Unr14, Definition 4]). *A non-interactive proof system (P, V) is simulation-sound online extractable with respect to (S_{init}, S_P) iff there is a polynomial-time extractor E such that for any quantum-polynomial-time oracle algorithm A, we have that*

$$\Pr\ [\ \text{ok} = 1 \wedge (x, \pi) \notin \mathsf{simproofs} \wedge (x, w) \notin R : \\ H \leftarrow S_{\text{init}}(), (x, \pi) \leftarrow A^{H, S_P}(), \\ \text{ok} \leftarrow V^H(x, \pi), w \leftarrow E(H, x, \pi)]$$

is negligible. Here $\mathsf{simproofs}$ is the set of all proofs returned by S_P (together with the corresponding statements).

We assume that both S_{init}, S_P and E have access to and may depend on a polynomial upper bound on the runtime of A.

The simulation-sound online extractability allows us to extract a witness from a successful adversary without measuring or rewinding, and avoids the problem of determining the query inputs by including its outputs in the proof and inverting them in the security proof. We do not need to operate in any way on

the quantum state of the adversary and get the witness purely by inspecting the classical proof/signature. It avoids the usual problem of disturbing the quantum state while trying to extract a witness.

2.3.4 Challenge injection

In the CRO model, many reductions succeed by injecting a challenge into one of the responses to the random oracle; a random query was selected, and rather than responding in the usual way, the reduction algorithm responded with the element r that was provided by the challenger [Eat17]. In the QaRO model, a random query cannot be simply responded to by returning the classical element r.

Zhandry's Technique

One possible solution is to choose a random subset D of the domain $\mathcal{D}$ and define the oracle H so that for any $d \in D$, $H(d) = y$, the challenge point. The question then is if it is possible to choose D in such a way that it is large enough so that we can reasonably hope for the forgery to be associated with y, but not so large that the adversary notices that our oracle isn't a true random oracle. This was possible by defining a construction called *semi-constant distribution* as below:

Definition 2.3.6 (Semi-constant Distribution [Zha12, Definition 4.1])**.** *The semi-constant distribution $\mathsf{SC}_{\lambda,y}$ is a distribution on mappings from a domain $\mathcal{D}$ to a range $\mathcal{R}$. It is parameterized by a value $\lambda \in [0,1]$ and an element $y \in \mathcal{R}$. The distribution is defined by how it is sampled. For each $d \in \mathcal{D}$, with probability λ set $H(d) = y$. Otherwise set it to a uniformly random element of $\mathcal{R}$.*

Then the following theorem was proved:

Theorem 2.3.7 ([Zha12, Corollary 4.3])**.** *If y is a uniformly random element of $\mathcal{R}$, then the distribution of any quantum algorithm that makes q queries to a random oracle has distance at most $\frac{8}{3}q^4\lambda^2$ from the distribution generated when $\mathsf{SC}_{\lambda,y}$ is used instead.*

Using the above technique regarding indistinguishability of oracles against quantum adversaries, [Zha12] provided the security of [GPV08]'s identity-based encryption (GPV-IBE) scheme in the QaRO model. Though Zhandry's technique is general and useful, a huge reduction loss and a wide gap between the concrete efficiency and security level in the CRO and QaRO model are unavoidable because the reduction algorithm has to abort with high probability.

KYY's Technique

Recently, [KYY18] provided a much tighter security proof for single-challenge GPV-IBE scheme in the QaRO model as in Theorem 2.3.8. Also, multi-challenge GPV-IBE scheme has an almost tight reduction in the QaRO model as in Theorem 2.3.9. KYY's technique uses completely different approach from Zhandry's by simulating in a way so that exactly one valid secret key for every identity can be created.

Theorem 2.3.8 ([KYY18, Theorem 2])**.** *The GPV-IBE scheme is adaptively-anonymous single-challenge secure assuming the hardness of* $\mathsf{LWE}_{n,m,q,\chi}$ *in the QaRO model, where* $\chi = D_{\mathbb{Z},\alpha q}$*. Namely, for any quantum adversary* $\mathcal{A}$ *making at most* Q_{H} *queries to* $|\mathsf{H}\rangle$ *and* Q_{ID} *secret key queries, there exists a quantum algorithm* $\mathcal{B}$ *making* $Q_{\mathsf{H}} + Q_{\mathsf{ID}}$ *QaRO queries such that*

$$\mathsf{Adv}^{\mathsf{IBE}}_{\mathcal{A},\mathsf{GPV}}(\lambda) \leq \mathsf{Adv}^{\mathsf{LWE}_{n,m,q,\chi}}_{\mathcal{B},\mathsf{QaRO}_{l_{\mathsf{ID}},l_r}}(\lambda) + (Q_{\mathsf{H}}^2 + Q_{\mathsf{ID}}) \cdot 2^{-\Omega(n)}$$

and

$$\mathsf{Time}(\mathcal{B}) = \mathsf{Time}(\mathcal{A}) + (Q_{\mathsf{H}} + Q_{\mathsf{ID}}) \cdot \mathsf{poly}(\lambda),$$

where l_r *denotes the length of the randomness for* $\mathsf{Sample}\mathbb{Z}$*.*

Theorem 2.3.9 ([KYY18, Theorem 4])**.** *The GPV-IBE scheme is adaptively-anonymous multi-challenge secure assuming the hardness of* $\mathsf{LWE}_{l,m,q,\chi}$ *in the QaRO model, where* $\chi = D_{\mathbb{Z},\alpha q}$*. Namely, for any quantum adversary* $\mathcal{A}$ *making at most* Q_{H} *queries to* $|\mathsf{H}\rangle$*,* Q_{ch} *challenge queries, and* Q_{ID} *secret key queries, there exists a quantum algorithm* $\mathcal{B}$ *making at most* $3Q_{\mathsf{H}} + 6Q_{\mathsf{ch}} + 2Q_{\mathsf{ID}}$ *QaRO queries such that*

$$\begin{aligned}\mathsf{Adv}^{\mathsf{IBE}}_{\mathcal{A},\mathsf{GPV}_{\mathsf{mult}}}(\lambda) \quad \leq \quad & 3n \cdot \mathsf{Adv}^{\mathsf{LWE}_{l,m,q,\chi}}_{\mathcal{B},\mathsf{QaRO}_{l_{\mathsf{ID}}+2,\max\{l_r,(\lfloor \log q \rfloor + 2\lambda)\times n\}}}(\lambda) \\ & + (Q_{\mathsf{H}} + Q_{\mathsf{ch}} + Q_{\mathsf{ID}}) \cdot 2^{-\Omega(n)}\end{aligned}$$

and

$$\mathsf{Time}(\mathcal{B}) = \mathsf{Time}(\mathcal{A}) + (Q_{\mathsf{H}} + Q_{\mathsf{ch}} + Q_{\mathsf{ID}}) \cdot \mathsf{poly}(\lambda),$$

where l_r *denotes the length of the randomness for* $\mathsf{Sample}\mathbb{Z}$*.*

2.3.5 Efficient Simulation

In the CRO model, simulating an exponential-size random oracle is efficient via *lazy sampling*. As queries to the random oracle are received, a table is built up of queries and responses. When a query is submitted that isn't in the table, a random output is generated as a response, and the query and the output are recorded in the table. By doing this, the simulation is entirely indistinguishable from a truly random oracle, and the reduction algorithm only needs to maintain a table with size at most q [Eat17]. However, in the CRO model, managing such a table is infeasible because the adversary can submit a superposition of all inputs as his first query, which requires the oracle to be defined for all possible inputs when the first query is made.

The *quantum-accessible pseudorandom functions* are proposed as a solution in [BDF+11], where the distinguisher is given quantum access to O or f by way of the unitary mapping U_O or U_f. Although they are an efficient and flexible replacement for a QaRO, an additional computational assumption should be introduced whereas the CRO model does not need such assumption as queries can be answered as they are made in a uniform and independent way.

As another solution, [Zha12] proposed k-wise independent functions to simulate the QaRO.

Definition 2.3.7 ([Zha12])**.** *A family of k-wise independent functions is a set $\mathcal{F}$ of functions $f : \mathcal{D} \to \mathcal{R}$ such that if $d_1, \ldots, d_k$ are any k different elements of $\mathcal{D}$ and $r_1, \ldots, r_k$ are any k elements of $\mathcal{R}$ (possible with repeats), then*

$$\Pr_{f \xleftarrow{\$} \mathcal{F}}[f(d_1) = r_1 \wedge f(d_2) = r_2 \wedge \cdots \wedge f(d_k) = r_k] = \frac{1}{|\mathcal{R}|^k}.$$

Intuitively, a k-wise independent function is a function that appears perfectly uniform and independent if you look at no more than k input/output pairs. The following theorem establishes how these functions may be used to replace the QaRO.

Theorem 2.3.10 ([Zha12])**.** *Let $\mathcal{A}$ be a quantum algorithm outputting some classical state z, that makes q quantum queries to a random oracle $O : \mathcal{D} \to \mathcal{R}$, drawn uniformly from the set of all such functions. If $\mathcal{F}$ is a family of $2q$-wise independent functions $f : \mathcal{D} \to \mathcal{R}$, then*

$$\Pr[\mathcal{A}^O \to z] = \Pr_{f \xleftarrow{\$} \mathcal{F}}[\mathcal{A}^f \to z].$$

2.4 Quantum Security Notions

Here, security notions for symmetric encryption scheme is organised below:

Definition 2.4.1 (Symmetric Encryption)**.** *A symmetric encryption scheme* Π_{sym} *is a tuple of classical probabilistic polynomial-time algorithms* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *and sets called key space* $\mathcal{K}$*, message space* $\mathcal{M}$*, and ciphertext space* $\mathcal{C}$ *such that*

- $\mathsf{k} \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$*: the key generation algorithm* Gen *receives a security parameter* λ *and outputs key* $\mathsf{k} \in \mathcal{K}$*.*
- $\mathsf{c} \xleftarrow{\$} \mathsf{Enc}_\mathsf{k}(\mathsf{m})$*: the encryption algorithm* Enc *uses the key* k *to encrypt a message* $\mathsf{m} \in \mathcal{M}$ *and outputs a ciphertext* $\mathsf{c} \in \mathcal{C}$*.*
- $\mathsf{m} \leftarrow \mathsf{Dec}_\mathsf{k}(\mathsf{c})$*: the decryption algorithm* Dec *uses the key* k *to decrypt a ciphertext* $\mathsf{c} \in \mathcal{C}$ *and outputs a message* m *or* $\perp$ *denoting* c *is invalid.*

For any k *and any* m*, the scheme should satisfy* $\Pr\left[\mathsf{Dec}_\mathsf{k}(\mathsf{Enc}_\mathsf{k}(\mathsf{m})) \neq \mathsf{m}\right] = \mathsf{negl}(\lambda)$*.*

Let us consider classical security games first: In formal definitions of classical security [GM84, BDPR98], a game between an adversary and a challenger formalises the security notions by pairing of a particular goal and a particular attack model. *Indistinguishability* (IND) is one of possible security goals, with regard to an adversary's advantage to distinguish the encryptions of two plaintexts of the same length. As possible attack models, three different attacks are considered depending on an adversary's attack capabilities: *chosen-plaintext attack* (CPA), *non-adaptive chosen-ciphertext attack* (CCA1), and *adaptive chosen-ciphertext attack* (CCA2). Under CPA, the adversary has an encryption oracle access and obtains ciphertexts for plaintexts of its choice. Under CCA1, the adversary has an additional decryption oracle access before the challenge phase, whereas under CCA2, the adversary has an additional decryption oracle access before and after the challenge phase. The CCA2 adversary, however, is not allowed to query the challenge ciphertext itself to the decryption oracle. Hence, the decryption oracle after the challenge phase is modified as follows:

$$\mathsf{Dec}_\mathsf{k}^{\mathsf{c}_\mathsf{b}}(\mathsf{c}) = \begin{cases} \perp & \text{if } \mathsf{c} = \mathsf{c}_\mathsf{b}, \\ \mathsf{Dec}_\mathsf{k}(\mathsf{c}) & \text{otherwise.} \end{cases}$$

Then, for example, a symmetric encryption scheme is said to be *indistinguishability under chosen-plaintext attack* (IND-CPA) secure if the advantage of any classical probabilistic polynomial-time adversary

winning the game is negligible. Quantum security notions are newly suggested by extending this classical case.

Definition 2.4.2 (IND-CPA for Π_{sym})**.** *A symmetric encryption scheme Π_{sym} is said to be IND-CPA secure if the advantage of any classical probabilistic polynomial-time adversary $\mathcal{A} = (\mathcal{A}_{\mathsf{G}}, \mathcal{A}_{\mathsf{D}})$, where $\mathcal{A}_{\mathsf{G}}$ and $\mathcal{A}_{\mathsf{D}}$ are a message generator and a distinguisher, respectively, winning the game is negligible.*

$$\mathsf{Adv}^{\mathsf{IND-CPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}}(\lambda) := 2\left|\mathsf{Succ}^{\mathsf{IND-CPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}} - \frac{1}{2}\right| = \mathsf{negl}(\lambda), \text{ where } \mathsf{Succ}^{\mathsf{IND-CPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}} \text{ is as follows:}$$

$$\Pr\left[\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda); (\mathsf{m}_0^*, \mathsf{m}_1^*, \mathsf{state}) \xleftarrow{\$} \mathcal{A}_{\mathsf{G}}^{\mathcal{O}_{\mathsf{Enc_k}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{c}_{\mathsf{b}}^* \xleftarrow{\$} \mathcal{O}_{\mathsf{Enc_k}}(\mathsf{m}_{\mathsf{b}}^*); \mathsf{b}' \leftarrow \mathcal{A}_{\mathsf{D}}^{\mathcal{O}_{\mathsf{Enc_k}}}(\mathsf{state}) : \mathsf{b}' = \mathsf{b}\right].$$

The most naturally emerging concept for a quantum security game is that replacing all classical communication with quantum communication by allowing an adversary to have both quantum encryption oracle access and quantum challenge queries. In this case, the adversary and the challenger are modelled as quantum circuits sharing a certain number of qubits. For this model, one of the first attempts to extend at defining a quantum security notion was to extend IND-CPA to *fully-quantum IND under quantum CPA* (fqIND-qCPA), which renames [BZ13, Definition 4.1] for consistency. However, no symmetric encryption scheme satisfies fqIND-qCPA security as shown in Theorem 2.4.1, which brings the need to limit quantum adversaries' power to find weaker but achievable security notions.

Theorem 2.4.1 (BZ Attack [BZ13, Theorem 4.2])**.** *No symmetric encryption scheme achieves fqIND-qCPA security.*

Proof. The proof [GHS16, Proof 2.7] can be interpreted as follows: as shown in Figure 2.2, the generic adversary $\mathcal{A}$ prepares three quantum registers, two message registers and an ancilla register for storing ciphertext.

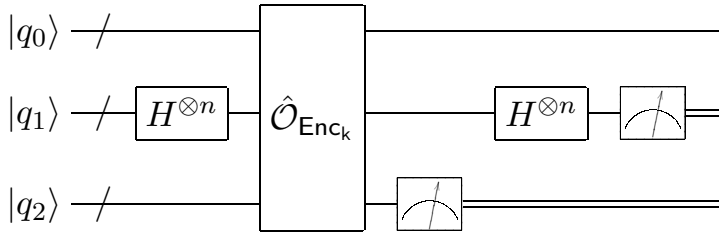


Figure 2.2: Quantum circuit diagram for BZ attack

- They are initialized as $|0^n\rangle$ and the initial quantum state is $|\varphi_0\rangle = |0^n\rangle|0^n\rangle|0^n\rangle$.

- To put superposition of all possible messages in the second register, the Hadamard gate acts on $|q_1\rangle$ and the state becomes $|\varphi_1\rangle = |0^n\rangle \sum_{x\in\{0,1\}^n} 2^{-n/2}|x\rangle|0^n\rangle$.

- When $\mathcal{A}$ challenges fqIND game and gets a quantum encryption oracle access mapping basis state $|q_0, q_1, q_2\rangle$ to $|q_0, q_1, q_2 \oplus \mathsf{Enc}_\mathsf{k}(q_b)\rangle$, then we have two cases as below:

$$|\varphi_2\rangle = \begin{cases} |0^n\rangle \sum_{x\in\{0,1\}^n} 2^{-n/2}|x\rangle|\mathsf{Enc}_\mathsf{k}(0^n)\rangle & \text{if } b = 0 \\ |0^n\rangle \sum_{x\in\{0,1\}^n} 2^{-n/2}|x\rangle|\mathsf{Enc}_\mathsf{k}(x)\rangle & \text{if } b = 1. \end{cases}$$

- Measurement on $|q_2\rangle$ gives

$$|\varphi_3\rangle = \begin{cases} |0^n\rangle \sum_{x\in\{0,1\}^n} 2^{-n/2}|x\rangle|\mathsf{Enc}_\mathsf{k}(0^n)\rangle & \text{if } b = 0 \\ |0^n\rangle|x\rangle|\mathsf{Enc}_\mathsf{k}(x)\rangle \text{ with prob. } 2^{-n} & \text{if } b = 1. \end{cases}$$

- Acting the Hadamard on $|q_1\rangle$ again gives

$$|\varphi_4\rangle = \begin{cases} |0^n\rangle|0^n\rangle|\mathsf{Enc}_\mathsf{k}(0^n)\rangle & \text{if } b = 0 \\ |0^n\rangle(|+\rangle^{n_0}|-\rangle^{n-n_0})|\mathsf{Enc}_\mathsf{k}(x)\rangle & \text{if } b = 1. \end{cases}$$

- Finally, the measurement on $|q_1\rangle$ gives

$$|\varphi_5\rangle = \begin{cases} |0^n\rangle|0^n\rangle|\mathsf{Enc}_\mathsf{k}(0^n)\rangle & \text{if } b = 0 \\ |0^n\rangle|i\rangle|\mathsf{Enc}_\mathsf{k}(x)\rangle \text{ for } i \in \{0,1\}^n & \\ \qquad\qquad \text{with prob. } 2^{-n} & \text{if } b = 1. \end{cases}$$

For $b = 0$, the measurement on $|q_1\rangle$ yields $|0^n\rangle$ with probability 1. For $b = 1$, the measurement on $|q_1\rangle$ yields $|0^n\rangle$ with probability 2^{-n}. The $\mathcal{A}$ outputs $b' = 0$ iff the last outcome is $|0^n\rangle$, otherwise $b' = 1$. □

The possible quantum security notions weaker than fqIND-qCPA were found by spanning the security tree in four criteria: relaying of challenge message states (no N vs yes Y); type of unitary transformation in challenge phase (standard s vs minimal m); game model (challenger C vs oracle O); and challenge messages (classical description c vs quantum states q) [GHS16], which resets orders and symbols here for systematic visibility. In Figure 2.3, out of all 16 possible notions, 9 unreasonable notions (written in grey)

and 3 unachievable notions (crossed out) are excluded, and the following notions are left: $NsCc$, $NsCq$, $NmCc$, and $NmCq$. These are correspond to the definition of

- IND under quantum CPA (IND-qCPA),
- weak-quantum IND under quantum CPA (wqIND-qCPA), and
- quantum IND under quantum CPA (qIND-qCPA).

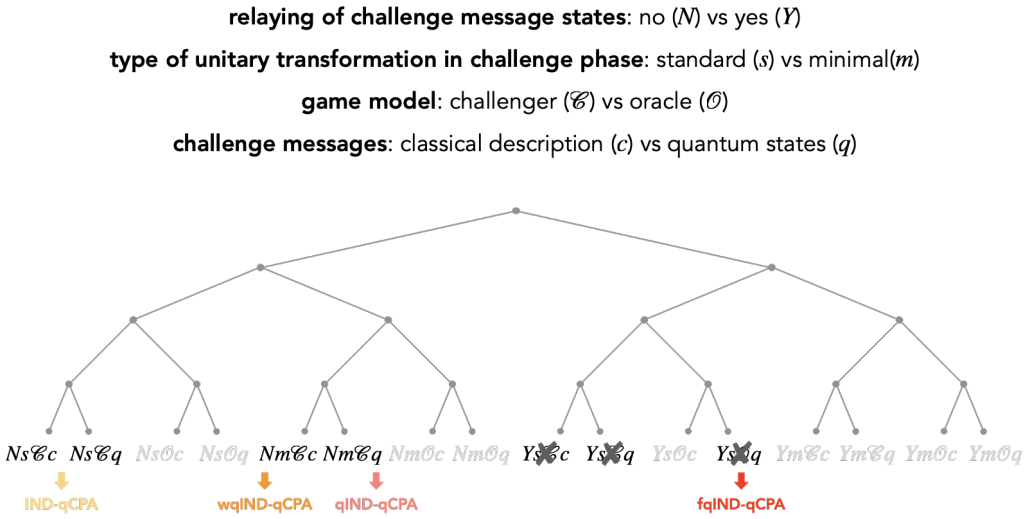


Figure 2.3: Security tree for checking all possible notions. Excluding 9 unreasonable notions (written in grey) and 3 unachievable notions (crossed out) leaves 4 notions.

2.4.1 IND-qCPA

The definition of IND-qCPA was discussed in [BZ13, Definition 4.5].

Definition 2.4.3 (IND-qCPA for Π_{sym})**.** *A symmetric encryption scheme Π_{sym} is said to be IND-qCPA secure if the advantage of any quantum probabilistic polynomial-time adversary $\mathcal{A} = (\mathcal{A}_{\mathsf{G}}, \mathcal{A}_{\mathsf{D}})$, where $\mathcal{A}_{\mathsf{G}}$ and $\mathcal{A}_{\mathsf{D}}$ are a message generator and a distinguisher, respectively, winning the game is negligible.*

$$\mathsf{Adv}^{\mathsf{IND-qCPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}}(\lambda) := 2\left|\mathsf{Succ}^{\mathsf{IND-qCPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}} - \frac{1}{2}\right| = \mathsf{negl}(\lambda), \text{ where } \mathsf{Succ}^{\mathsf{IND-qCPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}} \text{ is as follows:}$$

$$\Pr\left[\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda); (\mathsf{m}_0^*, \mathsf{m}_1^*, |\mathsf{state}\rangle) \xleftarrow{\$} \mathcal{A}_{\mathsf{G}}^{O_{\mathsf{Enc}_\mathsf{k}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{c}_\mathsf{b}^* \xleftarrow{\$} O_{\mathsf{Enc}_\mathsf{k}}(\mathsf{m}_\mathsf{b}^*); \mathsf{b}' \leftarrow \mathcal{A}_{\mathsf{D}}^{O_{\mathsf{Enc}_\mathsf{k}}}(|\mathsf{state}\rangle) : \mathsf{b}' = \mathsf{b}\right].$$

2.4.2 wqIND-qCPA

The definition of wqIND-qCPA was discussed in [GHS16, Definition 3.1] and [Gag17, Definition 5.26].

Definition 2.4.4 (wqIND-qCPA for Π_{sym})**.** *A symmetric encryption scheme Π_{sym} is said to be wqIND-qATK secure if the advantage of any quantum probabilistic polynomial-time adversary $\mathcal{A} = (\mathcal{A}_{\mathsf{G}}, \mathcal{A}_{\mathsf{D}})$, where $\mathcal{A}_{\mathsf{G}}$ and $\mathcal{A}_{\mathsf{D}}$ are a message generator and a distinguisher, respectively, winning the game is negligible.*

$$\mathsf{Adv}^{\mathsf{wqIND-qCPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}}(\lambda) := 2\left|\mathsf{Succ}^{\mathsf{wqIND-qCPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}} - \frac{1}{2}\right| = \mathsf{negl}(\lambda), \text{ where } \mathsf{Succ}^{\mathsf{wqIND-qATK}}_{\mathcal{A},\Pi_{\mathsf{sym}}} \text{ is as follows:}$$

$$\Pr\left[\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda); (\mathsf{Dsc}(\rho_{\mathsf{m}^*_0}), \mathsf{Dsc}(\rho_{\mathsf{m}^*_1}), \rho_{\mathsf{state}}) \xleftarrow{\$} \mathcal{A}_{\mathsf{G}}^{\mathcal{O}_{\mathsf{Enc}'_{\mathsf{k}}}}; \mathsf{b} \xleftarrow{\$} \{0,1\};\right.$$
$$\left.\rho_{\mathsf{m}^*_{\mathsf{b}}} \xleftarrow{\$} \mathsf{Qbd}(\mathsf{Dsc}(\rho_{\mathsf{m}^*_{\mathsf{b}}})); \rho_{\mathsf{c}^*_{\mathsf{b}}} \xleftarrow{\$} \mathcal{O}'_{\mathsf{Enc}_{\mathsf{k}}}(\rho^*_{\mathsf{m}_{\mathsf{b}}}); \mathsf{b}' \leftarrow \mathcal{A}_{\mathsf{D}}^{\mathcal{O}_{\mathsf{Enc}'_{\mathsf{k}}}}(\rho_{\mathsf{state}}) : \mathsf{b}' = \mathsf{b}\right].$$

2.4.3 qIND-qCPA

The definition of qIND-qCPA was discussed in [BJ15, Definition B.1], [GHS16, Definition 3.2], and [Gag17, Definition 5.15].

Definition 2.4.5 (qIND-qCPA for Π_{sym})**.** *A symmetric encryption scheme Π_{sym} is said to be qIND-qCPA secure if the advantage of any quantum probabilistic polynomial-time adversary $\mathcal{A} = (\mathcal{A}_{\mathsf{G}}, \mathcal{A}_{\mathsf{D}})$, where $\mathcal{A}_{\mathsf{G}}$ and $\mathcal{A}_{\mathsf{D}}$ are a message generator and a distinguisher, respectively, winning the game is negligible.*

$$\mathsf{Adv}^{\mathsf{qIND-qCPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}}(\lambda) := 2\left|\mathsf{Succ}^{\mathsf{qIND-qCPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}} - \frac{1}{2}\right| = \mathsf{negl}(\lambda), \text{ where } \mathsf{Succ}^{\mathsf{qIND-qCPA}}_{\mathcal{A},\Pi_{\mathsf{sym}}} \text{ is as follows:}$$

$$\Pr\left[\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda); (\rho_{\mathsf{m}^*_0}, \rho_{\mathsf{m}^*_1}, \rho_{\mathsf{state}}) \xleftarrow{\$} \mathcal{A}_{\mathsf{G}}^{\mathcal{O}'_{\mathsf{Enc}_{\mathsf{k}}}}; \mathsf{b} \xleftarrow{\$} \{0,1\};\right.$$
$$\left.\rho_{\mathsf{c}^*_{\mathsf{b}}} \xleftarrow{\$} \mathcal{O}'_{\mathsf{Enc}_{\mathsf{k}}}(\rho_{\mathsf{m}^*_{\mathsf{b}}}); \textit{trace out } \rho_{\mathsf{m}^*_{1-\mathsf{b}}}; \mathsf{b}' \leftarrow \mathcal{A}_{\mathsf{D}}^{\mathcal{O}'_{\mathsf{Enc}_{\mathsf{k}}}}(\rho_{\mathsf{state}}) : \mathsf{b}' = \mathsf{b}\right].$$

Chapter 3. Modes of Operation in Block Ciphers

One of the symmetric encryption schemes, block ciphers are widely used as cryptographic primitives in the build of many cryptographic protocols. Since their operations only work on a fixed-length group of bits called a block, *modes of operation* have been suggested to combine repeated operations for multiple blocks and provide confidentiality or authenticity. There are three types of modes of operation in block ciphers: confidentiality modes, authenticity modes, and combined (or authenticated encryption) modes. The confidentiality modes are introduced here. Also, Figure 3.1 and 3.2 give their representation in quantum circuits for quantum security analysis.

3.1 Electronic Codebook (ECB)

ECB mode is the simplest mode where the message is divided into blocks and each block is encrypted independently, hence the same ciphertext blocks are generated from the same plaintext blocks. This property makes the system highly vulnerable and insecure.

- Key generation: $\mathsf{k} \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$. For a given security parameter λ, generate key $\mathsf{k} \in \mathcal{K}$.
- Encryption: $\mathsf{c} \xleftarrow{\$} \mathsf{Enc}_\mathsf{k}(\mathsf{m})$. For a given message $\mathsf{m} := \mathsf{m}_1 \dots \mathsf{m}_L$, where L is a polynomial in n, encrypt m using k, and output a ciphertext $\mathsf{c} := \mathsf{c}_1 \dots \mathsf{c}_L$, where $\mathsf{c}_i \leftarrow \mathsf{BC}_\mathsf{k}(\mathsf{m}_i)$ for $1 \le i \le L$.
- Decryption: $\mathsf{m} \leftarrow \mathsf{Dec}_\mathsf{k}(\mathsf{c})$. For a given ciphertext c, decrypt c using k, and output a message m, where $\mathsf{m}_i \leftarrow \mathsf{BC}_\mathsf{k}^{-1}(\mathsf{c}_i)$ for $1 \le i \le L$.

3.2 Cipher Block Chaining (CBC)

- Key generation: $\mathsf{k} \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$. For a given security parameter λ, generate key $\mathsf{k} \in \mathcal{K}$.
- Encryption: $\mathsf{c} \xleftarrow{\$} \mathsf{Enc}_\mathsf{k}(\mathsf{m})$. $\mathsf{c}_0 \xleftarrow{\$} \{0,1\}^n$ as an IV. For a given message $\mathsf{m} := \mathsf{m}_1 \dots \mathsf{m}_L$, where L is a polynomial in n, encrypt m using k, and output a ciphertext $\mathsf{c} := \mathsf{c}_1 \dots \mathsf{c}_L$, where $\mathsf{c}_i \leftarrow \mathsf{BC}_\mathsf{k}(\mathsf{c}_{i-1} \oplus \mathsf{m}_i)$ for $1 \le i \le L$.
- Decryption: $\mathsf{m} \leftarrow \mathsf{Dec}_\mathsf{k}(\mathsf{c})$. For given IV and ciphertext c, decrypt c using k, and output a message m, where $\mathsf{m}_i \leftarrow \mathsf{BC}_\mathsf{k}^{-1}(\mathsf{c}_i) \oplus \mathsf{c}_{i-1}$ for $1 \le i \le L$.

3.3 Infinite Garble Extension (IGE)

IGE mode was initially introduced by Campbell in 1978 to prevent spoofing attacks [Cam78]. It has the property that errors are propagated forward indefinitely, and any difference in ciphertext changes (or garbles) the decryption of all subsequent ciphertext. It is similar to CBC mode and known for being used in Telegram's MTProto.

- Key generation: $\mathsf{k} \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$. For a given security parameter λ, generate key $\mathsf{k} \in \mathcal{K}$.
- Encryption: $\mathsf{c} \xleftarrow{\$} \mathsf{Enc}_\mathsf{k}(\mathsf{m})$. $\mathsf{c}_0 \xleftarrow{\$} \{0,1\}^n$ and $\mathsf{m}_0 \xleftarrow{\$} \{0,1\}^n$ as IVs. For a given message $\mathsf{m} := \mathsf{m}_1 \dots \mathsf{m}_L$, where L is a polynomial in n, encrypt m using k, and output a ciphertext $\mathsf{c} := \mathsf{c}_1 \dots \mathsf{c}_L$, where $\mathsf{c}_i \leftarrow \mathsf{BC}_\mathsf{k}(\mathsf{c}_{i-1} \oplus \mathsf{m}_i) \oplus \mathsf{m}_{i-1}$ for $1 \le i \le L$.
- Decryption: $\mathsf{m} \leftarrow \mathsf{Dec}_\mathsf{k}(\mathsf{c})$. For given IVs and ciphertext c, decrypt c using k, and output a message m, where $\mathsf{m}_i \leftarrow \mathsf{BC}_\mathsf{k}^{-1}(\mathsf{m}_{i-1} \oplus \mathsf{c}_i) \oplus \mathsf{c}_{i-1}$ for $1 \le i \le L$.

3.4 Simplified Cipher Feedback (CFB)

- Key generation: $\mathsf{k} \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$. For a given security parameter λ, generate key $\mathsf{k} \in \mathcal{K}$.
- Encryption: $\mathsf{c} \xleftarrow{\$} \mathsf{Enc}_\mathsf{k}(\mathsf{m})$. $\mathsf{c}_0 \xleftarrow{\$} \{0,1\}^n$ as an IV. For a given message $\mathsf{m} := \mathsf{m}_1 \dots \mathsf{m}_L$, where L is a polynomial in n, encrypt m using k, and output a ciphertext $\mathsf{c} := \mathsf{c}_1 \dots \mathsf{c}_L$, where $\mathsf{c}_i \leftarrow \mathsf{BC}_\mathsf{k}(\mathsf{c}_{i-1}) \oplus \mathsf{m}_i$ for $1 \le i \le L$.
- Decryption: $\mathsf{m} \leftarrow \mathsf{Dec}_\mathsf{k}(\mathsf{c})$. For given IV and ciphertext c, decrypt c using k, and output a message m, where $\mathsf{m}_i \leftarrow \mathsf{BC}_\mathsf{k}(\mathsf{c}_{i-1}) \oplus \mathsf{c}_i$ for $1 \le i \le L$.

3.5 Output Feedback (OFB)

- Key generation: $\mathsf{k} \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$. For a given security parameter λ, generate key $\mathsf{k} \in \mathcal{K}$.
- Encryption: $\mathsf{c} \xleftarrow{\$} \mathsf{Enc}_\mathsf{k}(\mathsf{m})$. $\mathsf{r}_0 \xleftarrow{\$} \{0,1\}^n$ as an IV. For a given message $\mathsf{m} := \mathsf{m}_1 \dots \mathsf{m}_L$, where L is a polynomial in n, encrypt m using k, and output a ciphertext $\mathsf{c} := \mathsf{c}_1 \dots \mathsf{c}_L$, where $\mathsf{r}_i \leftarrow \mathsf{BC}_\mathsf{k}(\mathsf{r}_{i-1})$ and $\mathsf{c}_i \leftarrow \mathsf{r}_i \oplus \mathsf{m}_i$ for $1 \le i \le L$.
- Decryption: $\mathsf{m} \leftarrow \mathsf{Dec}_\mathsf{k}(\mathsf{c})$. For given IV and ciphertext c, decrypt c using k, and output a message m, where $\mathsf{r}_i \leftarrow \mathsf{BC}_\mathsf{k}(\mathsf{r}_{i-1})$ and $\mathsf{m}_i \leftarrow \mathsf{r}_i \oplus \mathsf{c}_i$ for $1 \le i \le L$.

3.6 Counter (CTR)

- Key generation: $\mathsf{k} \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$. For a given security parameter λ, generate key $\mathsf{k} \in \mathcal{K}$.
- Encryption: $\mathsf{c} \xleftarrow{\$} \mathsf{Enc}_\mathsf{k}(\mathsf{m})$. $\mathsf{r}_0 \xleftarrow{\$} \{0,1\}^n$ as an IV. For a given message $\mathsf{m} := \mathsf{m}_1 \dots \mathsf{m}_L$, where L is a polynomial in n, encrypt m using k, and output a ciphertext $\mathsf{c} := \mathsf{c}_1 \dots \mathsf{c}_L$, where $\mathsf{r}_i \leftarrow \mathsf{BC}_\mathsf{k}(\mathsf{r}_0 + i)$ and $\mathsf{c}_i \leftarrow \mathsf{r}_i \oplus \mathsf{m}_i$ for $1 \le i \le L$.
- Decryption: $\mathsf{m} \leftarrow \mathsf{Dec}_\mathsf{k}(\mathsf{c})$. For given IV and ciphertext c, decrypt c using k, and output a message m, where $\mathsf{r}_i \leftarrow \mathsf{BC}_\mathsf{k}(\mathsf{r}_0 + i)$ and $\mathsf{m}_i \leftarrow \mathsf{r}_i \oplus \mathsf{c}_i$ for $1 \le i \le L$.

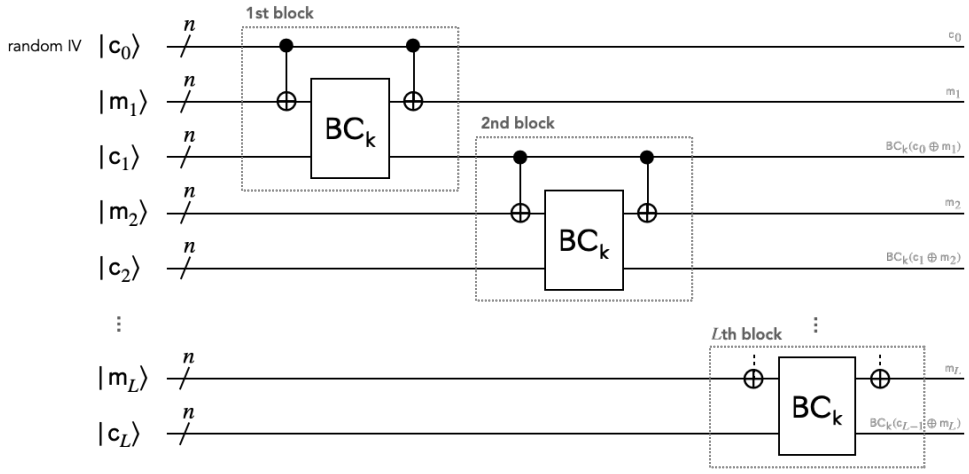
3.7 Modelling Block Ciphers

A keyed block cipher is modelled as a pseudorandom permutation (PRP) operating on fixed-size blocks of bits, $\mathcal{M} = \mathcal{C} = \{0,1\}^n$. By PRP/PRF switching lemma, a PRP is indistinguishable from a PRF in both classical and quantum settings [BR04, Zha13]. It usually turns out to be easier to analyse the security of a block-cipher-based construction assuming the block cipher is secure as a PRF.

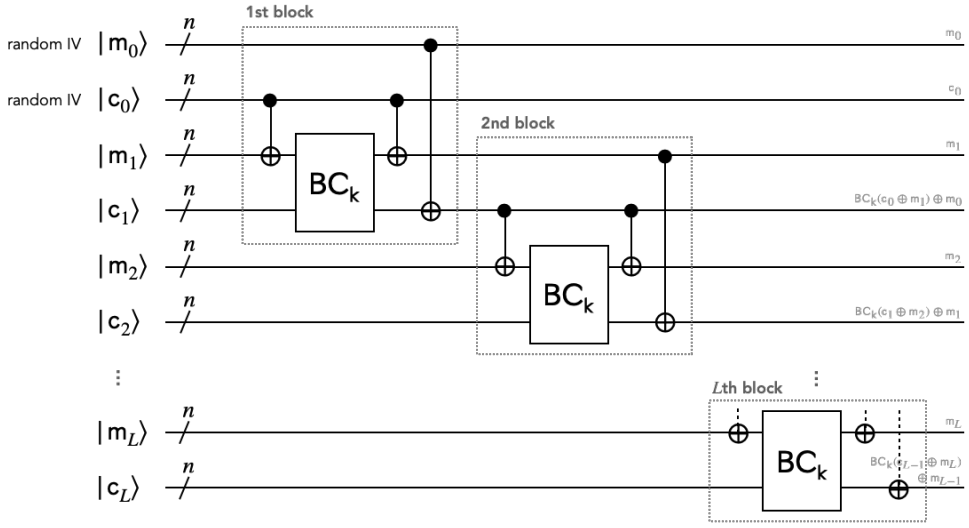
In order to prove quantum security of modes of operation, therefore, we need certain assumptions regarding the existence of PRFs, analogous to the classical case–namely, existence of Q1- and Q2-secure PRFs, which rename standard- and quantum–secure PRFs in [Zha12] for systematic consistency. The former allows quantum adversaries but limits the queries to be classical, whereas the latter allows both quantum adversaries and quantum queries, i.e. quantum superposition of inputs. The formal definitions are as follows:

Definition 3.7.1 (Q1- and Q2-secure PRF)**.** *A pseudorandom function* $\mathsf{PRF} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$*, where* $\mathcal{K}$*,* $\mathcal{X}$*, and* $\mathcal{Y}$ *are key space, domain, and range, respectively, is said to be Q1-secure PRF (or Q2-secure PRF) if no efficient quantum adversary* $\mathcal{A}$ *making classical (or quantum) queries can distinguish between a truly random function* f *and the function* PRF_k *for a random* k*,*

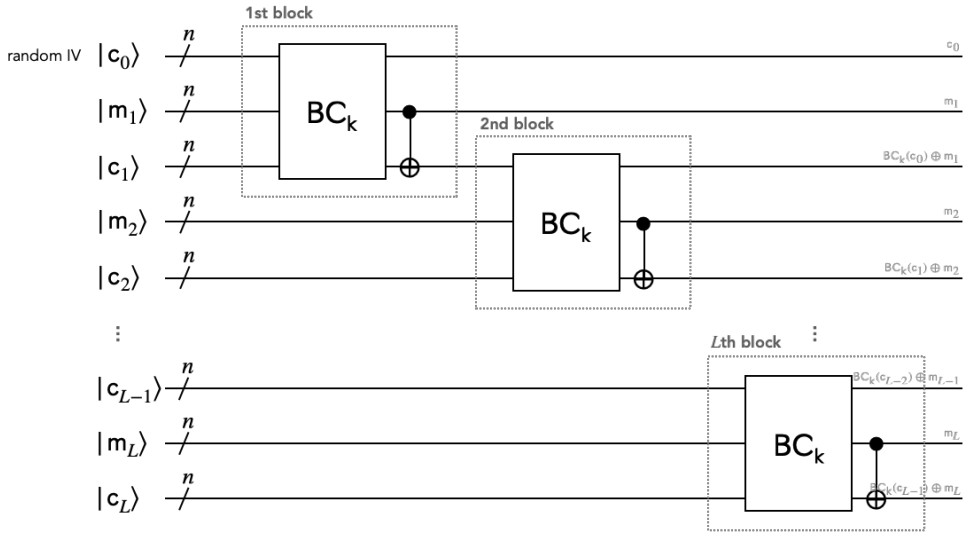
$$\left| \Pr_{f \in \mathcal{Y}^\mathcal{X}} \left[\mathcal{A}^f() = 1 \right] - \Pr_{\mathsf{k} \in \mathcal{K}} \left[\mathcal{A}^{\mathsf{PRF}_\mathsf{k}}() = 1 \right] \right| = \mathsf{negl}(\lambda).$$



(a) CBC mode

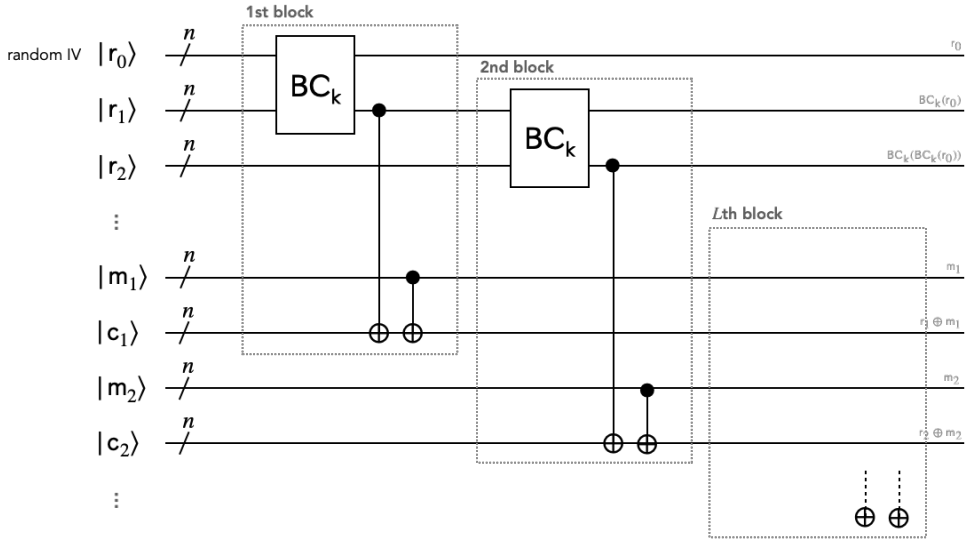


(b) IGE mode

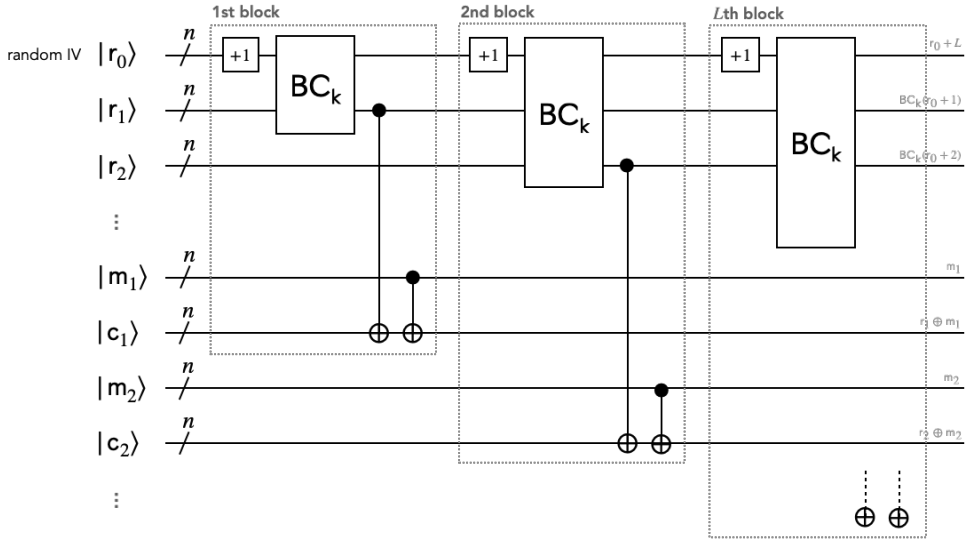


(c) CFB mode

Figure 3.1: CBC/IGE/CFB mode encryption in quantum circuits



(a) OFB mode



(b) CTR mode

Figure 3.2: OFB/CTR mode encryption in quantum circuits

Chapter 4. Quantum Security of Modes of Operation

4.1 IND-qCPA

4.1.1 Insecurity of CBC/IGE/CFB Mode under Q1-secure PRF

Let us give security analysis for IGE mode first: In order to show that a Q1-secure PRF is not sufficient for IND-qCPA security of IGE mode, a specific block cipher $\mathsf{BC}_\mathsf{k}()$ is constructed as follows:

$$\mathsf{BC}_\mathsf{k}(x) \quad := \quad \mathsf{E}_{\mathsf{H}(\mathsf{k})_1}\left(\mathsf{DropLastBit}(x \oplus (\mathsf{k}\|1) \cdot \mathsf{LastBit}(x))\right) \| t_{\mathsf{H}(\mathsf{k})_2}\left(x \oplus (\mathsf{k}\|1) \cdot \mathsf{LastBit}(x)\right) \oplus \mathsf{LastBit}(x),$$

where $\mathsf{E} : \{0,1\}^{n-1} \times \{0,1\}^{n-1} \to \{0,1\}^{n-1}$ and $t : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ are Q1-secure PRFs, $\mathsf{H} : \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$ is a random oracle, and $\mathsf{k} \xleftarrow{\$} \{0,1\}^{n-1}$ is the key. Here, for a string $x := x_1 x_2 \cdots x_n$, where x_i is the i-th bit of x, $\mathsf{LastBit}(x) = x_n$ and $\mathsf{DropLastBit}(x) = x_1 x_2 \cdots x_{n-1}$. For an l-bit string a and a binary variable b, $a \cdot b = a$ if $b = 1$, 0^l otherwise.

Here, if E is efficiently invertible, so is BC. Also, BC has a special property of being $(\mathsf{k}\|1)$-periodic, i.e. $\mathsf{BC}_\mathsf{k}(x) = \mathsf{BC}_\mathsf{k}(x \oplus (\mathsf{k}\|1))$. It is already proved that $\mathsf{BC}_\mathsf{k}()$ is a Q1-secure PRF but not a Q2-secure PRF in [ATTU16], for any quantum adversary with a classical access to $\mathsf{BC}_\mathsf{k}()$ and a quantum access to the random oracle H. We use this block cipher BC_k for the construction of Π_{IGE}.

Theorem 4.1.1. *There exists a Q1-secure PRF such that Π_{IGE} is IND-qCPA insecure in the QaRO model.*

Proof. As in previous attacks [ATTU16], we use Simon's algorithm [Sim94] to attack IGE mode. The

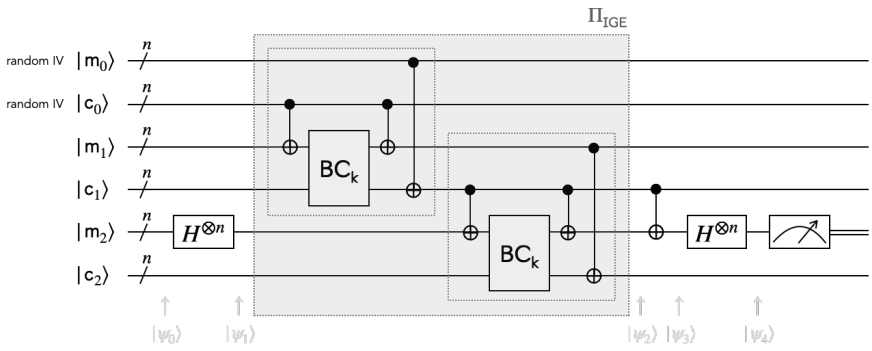


Figure 4.1: Quantum circuits for an attack on each mode using Simon's algorithm

quantum adversary prepares six quantum registers, three of which store messages and the rest three store ciphertexts, as shown in Fig. 4.1. The adversary then stores the superposition of all possible messages, i.e. $\sum_{\mathsf{m}_2} 2^{-n/2}|0^n\rangle|\mathsf{m}_2\rangle$*, in the message registers using a Hadamard gate. After an encryption query is made, the corresponding reply is stored in the ciphertext registers as follows:*

$$|\psi_2\rangle = \sum_{\mathsf{m}_2} 2^{-n/2}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|0^n\rangle|\mathsf{BC}_\mathsf{k}(\mathsf{c}_0)\oplus\mathsf{m}_0\rangle|\mathsf{m}_2\rangle|\mathsf{DropLastBit}(\mathsf{BC}_\mathsf{k}(\mathsf{BC}_\mathsf{k}(\mathsf{c}_0)\oplus\mathsf{m}_0\oplus\mathsf{m}_2))\|+\rangle,$$

where $|+\rangle \coloneqq 2^{-1/2}(|0\rangle+|1\rangle)$*. Now* c_1 *is XOR'ed to* m_2 *using a CNOT gate. More formally,*

$$|\psi_3\rangle = \sum_{\alpha} 2^{-n/2}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|0^n\rangle|\alpha\oplus\mathsf{m}_2\rangle|\alpha\rangle|\mathsf{DropLastBit}(\mathsf{BC}_\mathsf{k}(\alpha))\|+\rangle,$$

where $\alpha \coloneqq \mathsf{BC}_\mathsf{k}(\mathsf{c}_0)\oplus\mathsf{m}_0\oplus\mathsf{m}_2$*. In order to use* BC_k*'s special property of being* $(\mathsf{k}\|1)$*-periodic, we consider another message input* $\sum_{\mathsf{m}_2} 2^{-n/2}|0^n\rangle|\mathsf{m}_2\oplus(\mathsf{k}\|1)\rangle$*. By a similar calculation as before, and using* $\mathsf{BC}_\mathsf{k}(x) = \mathsf{BC}_\mathsf{k}(x\oplus(\mathsf{k}\|1))$*,*

$$|\phi_3\rangle = \sum_{\alpha} 2^{-n/2}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|0^n\rangle|\alpha\oplus\mathsf{m}_2\rangle|\alpha\oplus(\mathsf{k}\|1)\rangle|\mathsf{DropLastBit}(\mathsf{BC}_\mathsf{k}(\alpha))\|+\rangle.$$

Since $|\psi_3\rangle = |\phi_3\rangle = (|\psi_3\rangle+|\phi_3\rangle)/2$*,* $|\psi_3\rangle$ *is rewritten as*

$$= \sum_{\alpha} 2^{-(n/2+1)}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|0^n\rangle|\alpha\oplus\mathsf{m}_2\rangle\left(|\alpha\rangle+|\alpha\oplus(\mathsf{k}\|1)\rangle\right)|\mathsf{DropLastBit}(\mathsf{BC}_\mathsf{k}(\alpha))\|+\rangle.$$

The state after applying Hadamard gate on $|\mathsf{m}_2\rangle$ *is*

$$|\psi_4\rangle = \sum_{\alpha}\sum_{z} 2^{-(n+1)}(-1)^{\langle\alpha,z\rangle}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|0^n\rangle|\alpha\oplus\mathsf{m}_2\rangle\left(\left(1+(-1)^{\langle\mathsf{k}\|1,z\rangle}\right)|z\rangle\right)|\mathsf{DropLastBit}(\mathsf{BC}_\mathsf{k}(\alpha))\|+\rangle,$$

where $\langle *,*\rangle$ *denotes bitwise inner product. Finally, if we measure the* m_2 *register, we either get a vector* z *such that* $\langle\mathsf{k}\|1,z\rangle = 0$*, or an empty string. We repeat the same attack until we get* $n-1$ *independent vectors, thereby recovering* $n-1$ *bits of* k *and breaking* Π_{IGE}*.*

This similar attack can be applied to CBC and CFB modes, which means they are IND-qCPA insecure under the assumption that the underlying block cipher is Q1-secure PRF.

4.1.2 Security of OFB/CTR Mode under Q1-secure PRF

If we look at the definitions and quantum circuit representation of OFB and CTR modes, we know that they have $\mathsf{Enc}_k(\mathsf{m}) = f_k(n;r) \oplus \mathsf{m}$ form for randomness r. For this case, if it is IND-CPA secure then IND-qCPA secure. Therefore, OFB and CTR modes are IND-qCPA secure under the assumption that the underlying block cipher is Q1-secure PRF.

4.1.3 Security of CBC/IGE/CFB/OFB/CTR Mode under Q2-secure PRF

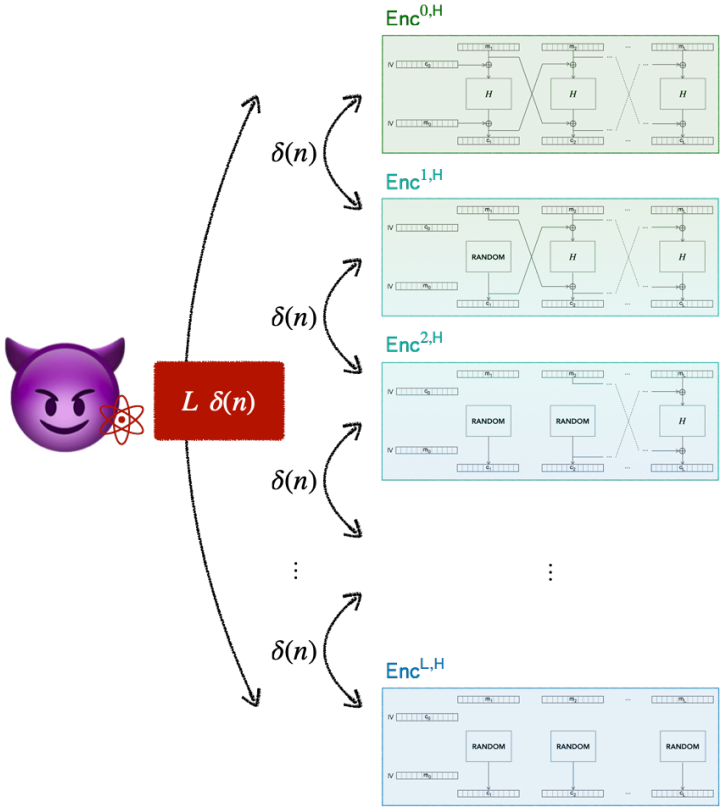


Figure 4.2: Quantum adversary's advantage to distinguish the challenge ciphertext and truly random string.

Let us give security analysis for IGE mode first: In order to show that IND-qCPA security of IGE mode is conditional on the existence of a Q2-secure PRF, we prove the advantage of efficient quantum adversary distinguishing the challenge ciphertext and truly random string is negligible by using O2H lemma.

We define $\mathsf{Enc}^{i,\mathsf{H}}(\mathsf{m}) \coloneqq \mathsf{c}_1 \cdots \mathsf{c}_L$, where $\mathsf{c}_j \xleftarrow{\$} \{0,1\}^n$ for $j \in [1,i]$ and $\mathsf{c}_j \leftarrow \mathsf{H}(\mathsf{c}_{j-1} \oplus \mathsf{m}_j) \oplus \mathsf{m}_{j-1}$ for $j \in (i,L]$. In Lemma 4.1.2, we prove that the probability of distinguishing the output of $\mathsf{Enc}^{i,\mathsf{H}}(\mathsf{m})$ from that of $\mathsf{Enc}^{i+1,\mathsf{H}}(\mathsf{m})$ is negligible in security parameter n.

Lemma 4.1.2. *For any $i \in [0, L)$ and every quantum adversary $\mathcal{A}$ that makes at most $q_{\mathcal{A}}$ queries in the QaRO model,*

$$\left|\Pr\left[\mathsf{H} \leftarrow (\{0,1\}^n \to \{0,1\}^n); (\mathsf{m}_0^*, \mathsf{m}_1^*) \leftarrow \mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}};\ \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}}(\mathsf{Enc}^{i,\mathsf{H}}(\mathsf{m_b}^*)) : \mathsf{b}' = \mathsf{b}\right] - \Pr\left[\mathsf{H} \leftarrow (\{0,1\}^n \to \{0,1\}^n); (\mathsf{m}_0^*, \mathsf{m}_1^*) \leftarrow \mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}}(\mathsf{Enc}^{i+1,\mathsf{H}}(\mathsf{m_b}^*)) : \mathsf{b}' = \mathsf{b}\right]\right| =: \delta(n) \leq O\left(2^{-n/2} L^2 {q_{\mathcal{A}}}^2\right),$$

where L is the maximum number of blocks in the message m and n is the length of each message block.

Proof. *Using the proof technique as [ATTU16], we prove IGE mode case as follows: For a given message $\mathsf{m} := \mathsf{m}_1 \cdots \mathsf{m}_L$, let $\widetilde{\mathsf{Enc}}^i_{\mathsf{H}}(\mathsf{m}, \mathsf{c}_1, \ldots, \mathsf{c}_i) := \hat{\mathsf{c}}_1 \hat{\mathsf{c}}_2 \cdots \hat{\mathsf{c}}_L$, where $\hat{\mathsf{c}}_j = \mathsf{c}_j$ for $j \in [1, i]$ and $\hat{\mathsf{c}}_j = \mathsf{H}(\hat{\mathsf{c}}_{j-1} \oplus \mathsf{m}_j) \oplus \mathsf{m}_{j-1}$ for $j \in (i, L]$. Then we put $\mathsf{c}_i := x \oplus {\mathsf{m_b}}^{i+1}$ and $\mathsf{c}_{i+1} := y \oplus {\mathsf{m_b}}^i$, where ${\mathsf{m_b}}^i$ is the i-th block of the message $\mathsf{m_b}$ and $x, y \xleftarrow{\$} \{0,1\}^n$. By definition of $\widetilde{\mathsf{Enc}}^i_{\mathsf{H}}$, $\widetilde{\mathsf{Enc}}^i_{\mathsf{H}}(\mathsf{m_b}, \mathsf{c}_1, \ldots, \mathsf{c}_i) = \widetilde{\mathsf{Enc}}^{i+1}_{\mathsf{H}}(\mathsf{m_b}, \mathsf{c}_1, \ldots, \mathsf{c}_{i+1})$ with $\mathsf{c}_{i+1} := \mathsf{H}(x) \oplus {\mathsf{m_b}}^i$. We define an adversary $\mathcal{A}_{\mathsf{O2H}}$ that makes oracle queries to the random function H is defined to be the output of the procedure described below for given inputs x and y:*

$$\begin{aligned}\mathcal{A}^{\mathsf{H}}_{\mathsf{O2H}}(x, y) \quad := \quad & (\mathsf{m}_0, \mathsf{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc}^{i,\mathsf{H}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{c}_1, \cdots, \mathsf{c}_{i-1} \xleftarrow{\$} \{0,1\}^n; \mathsf{c}_i := x \oplus {\mathsf{m_b}}^{i+1}; \mathsf{c}_{i+1} := y \oplus {\mathsf{m_b}}^i; \\ & \textit{compute } \mathsf{c} := \widetilde{\mathsf{Enc}}^{i+1}_{\mathsf{H}}(\mathsf{m_b}, \mathsf{c}_1, \ldots, \mathsf{c}_{i+1}); \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{Enc}^{i,\mathsf{H}}}(\mathsf{c});\ \textit{return } \mathsf{b}' = \mathsf{b}.\end{aligned}$$

Now we have the equation, by O2H lemma,

$$\begin{aligned}\delta(n) \quad = \quad & \left|\Pr\left[\mathsf{H} \leftarrow (\{0,1\}^n \to \{0,1\}^n); x \xleftarrow{\$} \{0,1\}^n; \tilde{\mathsf{b}} \leftarrow \mathcal{A}^{\mathsf{H}}_{\mathsf{O2H}}(x, \mathsf{H}(x)) : \tilde{\mathsf{b}} = 1\right] - \right. \\ & \left. \Pr\left[\mathsf{H} \leftarrow (\{0,1\}^n \to \{0,1\}^n); x \xleftarrow{\$} \{0,1\}^n; y \xleftarrow{\$} \{0,1\}^n; \tilde{\mathsf{b}} \leftarrow \mathcal{A}^{\mathsf{H}}_{\mathsf{O2H}}(x, y) : \tilde{\mathsf{b}} = 1\right]\right| \\ = \quad & \left|P^1_{\mathcal{A}_{\mathsf{O2H}}} - P^2_{\mathcal{A}_{\mathsf{O2H}}}\right| \leq 2 q_{\mathsf{O2H}} \sqrt{P_{\mathcal{B}}}.\end{aligned}$$

Note that $\mathcal{A}_{\mathsf{O2H}}$ can answer $\mathcal{A}$'s queries as it has oracle access to H. Let q_{O2H} be the number of H-queries made by $\mathcal{A}_{\mathsf{O2H}}$, then it is clear that $q_{\mathsf{O2H}} \leq 3 L q_{\mathcal{A}}$. Let q_1, q_2, and q_3 denote the number of queries that $\mathcal{A}_{\mathsf{O2H}}$ makes to H before, during, and after the challenge query, respectively. Let $\mathcal{B}$ be an oracle algorithm described in O2H lemma and $P_{\mathcal{B}}$ be $P^j_{\mathcal{B}}/q_{\mathsf{O2H}}$. In all three cases depending upon whether the j-th H-query was made before, during, or after the challenge query, we may show that $P_{\mathcal{B}} \leq O(2^{-n} {q_{\mathsf{O2H}}}^2)$. Therefore,

we have

$$\begin{aligned}\delta(n) &\leq 2q_{\mathsf{O2H}}\sqrt{P_{\mathcal{B}}} \\ &= O(2^{-n/2}{q_{\mathsf{O2H}}}^2) = O(2^{-n/2}L^2{q_{\mathcal{A}}}^2).\end{aligned}$$

Theorem 4.1.3. *If the function* E *is a Q2-secure PRF, then* Π_{IGE} *is IND-qCPA secure in the QaRO model.*

Proof. Using the proof technique as [ATTU16], we prove IGE mode case as follows: Let $\mathcal{A}$ *be a quantum adversary making* $q_{\mathcal{A}}$ *queries. Note that* $\mathsf{Enc}^{L,\mathsf{H}}(\mathsf{m_b})$ *is independent of its argument* $\mathsf{m_b}$*. Then by Lemma 4.1.2 and triangle inequality,*

$$\begin{aligned}&\left|\Pr\left[\mathsf{H}\leftarrow(\{0,1\}^n\to\{0,1\}^n);(\mathsf{m}_0,\mathsf{m}_1)\leftarrow\mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}};\mathsf{b}\xleftarrow{\$}\{0,1\};\mathsf{b}'\leftarrow\mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}}(\mathsf{Enc}^{0,\mathsf{H}}(\mathsf{m_b})):\mathsf{b}'=\mathsf{b}\right]-\right. \\ &\left.\Pr\left[\mathsf{H}\leftarrow(\{0,1\}^n\to\{0,1\}^n);(\mathsf{m}_0,\mathsf{m}_1)\leftarrow\mathcal{A}^{\mathsf{Enc}^{L,\mathsf{H}}};\mathsf{b}\xleftarrow{\$}\{0,1\};\mathsf{b}'\leftarrow\mathcal{A}^{\mathsf{Enc}^{L,\mathsf{H}}}(\mathsf{Enc}^{L,\mathsf{H}}(\mathsf{m_b})):\mathsf{b}'=\mathsf{b}\right]\right| \\ &\leq LO\left(2^{-n/2}L^2{q_{\mathcal{A}}}^2\right).\end{aligned}$$

One can see that $\mathsf{Enc}^{L,\mathsf{H}}(\mathsf{m_b})$ *outputs ciphertext as a completely random string. Hence, the output* b' *is independent of* b*. Therefore,*

$$\begin{aligned}&\left|\Pr\left[\mathsf{H}\leftarrow(\{0,1\}^n\to\{0,1\}^n);(\mathsf{m}_0,\mathsf{m}_1)\leftarrow\mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}};\mathsf{b}\xleftarrow{\$}\{0,1\};\mathsf{b}'\leftarrow\mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}}(\mathsf{Enc}^{0,\mathsf{H}}(\mathsf{m_b})):\mathsf{b}'=\mathsf{b}\right]-\frac{1}{2}\right| \\ &\leq O\left(2^{-n/2}L^3{q_{\mathcal{A}}}^2\right).\end{aligned}$$

Since $\mathsf{Enc}^{0,\mathsf{H}}$ *is indistinguishable from* Enc *of* Π_{IGE} *by definition of Q2-secure PRF, and as* $q_{\mathcal{A}}$ *is polynomial in* t*, we deduce*

$$\mathsf{Adv}^{\mathsf{IND-qCPA}}_{\mathcal{A},\Pi_{\mathsf{IGE}}}(n)\leq O\left(2^{-n/2}L^3{q_{\mathcal{A}}}^2\right)+\mathsf{negl}(n)=\mathsf{negl}(n).$$

That is, Π_{IGE} *is IND-qCPA secure.*

This similar proof can be applied to other modes as well, which means CBC, IGE, CFB, OFB, and CTR modes are IND-qCPA secure under the assumption that the underlying block cipher is Q2-secure PRF.

4.2 (w)qIND-qCPA

4.2.1 Insecurity of CBC/IGE/CFB/OFB/CTR Mode under Q2-secure PRF

Let us give security analysis for IGE mode first: In this security game, the adversary chooses two n-bit challenge messages as $|\mathsf{m}_0^*\rangle := H^{\otimes n}|0^n\rangle$and $|\mathsf{m}_1^*\rangle := H^{\otimes n}|1^n\rangle$for the challenge phase [GHS16].

Then for $b = 0$,

$$|\psi_1\rangle = \sum_{\mathsf{m}_1} 2^{-n/2}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|\mathsf{m}_1\rangle$$

$$|\psi_2\rangle = \sum_{\mathsf{m}_1} 2^{-n/2}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|\mathsf{BC}_\mathsf{k}(\mathsf{c}_0 \oplus \mathsf{m}_1) \oplus \mathsf{m}_0\rangle$$

$$|\psi_3\rangle = \sum_{\mathsf{m}_1} \sum_z (-1)^{\langle \mathsf{BC}_\mathsf{k}(\mathsf{c}_0\oplus\mathsf{m}_1)\oplus\mathsf{m}_0, z\rangle}\ 2^{-n}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|z\rangle$$

The measurement gives 0^n with probability 1.

In the case of $b = 1$,

$$|\psi_1\rangle = \sum_{\mathsf{m}_1} (-1)^{\langle 1^n, m_1\rangle}\ 2^{-n/2}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|\mathsf{m}_1\rangle$$

$$|\psi_2\rangle = \sum_{\mathsf{m}_1} (-1)^{\langle 1^n, m_1\rangle}\ 2^{-n/2}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|\mathsf{BC}_\mathsf{k}(\mathsf{c}_0 \oplus \mathsf{m}_1) \oplus \mathsf{m}_0\rangle$$

$$|\psi_3\rangle = \sum_{\mathsf{m}_1} \sum_z (-1)^{\langle 1^n, m_1\rangle + \langle \mathsf{BC}_\mathsf{k}(\mathsf{c}_0\oplus\mathsf{m}_1)\oplus\mathsf{m}_0, z\rangle}\ 2^{-n}|\mathsf{m}_0\rangle|\mathsf{c}_0\rangle|z\rangle$$

Here, the amplitude of the basis state $|0^n$ becomes $\sum_{\mathsf{m}_1} (-1)^{\langle 1^n, m_1\rangle + \langle \mathsf{BC}_\mathsf{k}(\mathsf{c}_0\oplus\mathsf{m}_1)\oplus\mathsf{m}_0, 0^n\rangle} = \sum_{\mathsf{m}_1} (-1)^{\langle 1^n, m_1\rangle} = 0$. It makes the adversary to distinguish the challenge messages, whose output is 0 when the measurement gives 0^n and 1 otherwise. Therefore, IGE mode encryption scheme is (w)qIND-qCPA insecure. The same attack can be applied to CBC, CFB, OFB, and CTR, which makes them (w)qIND-qCPA insecure, too.

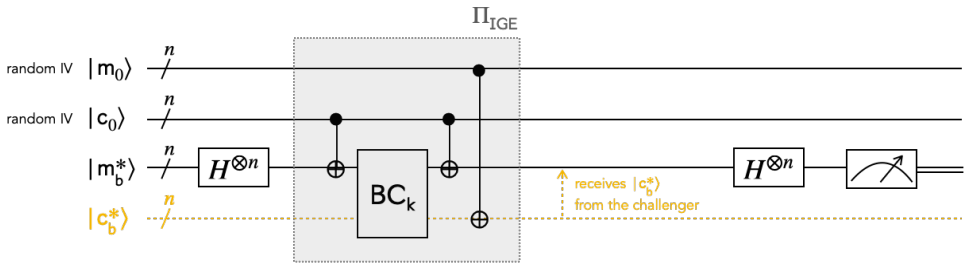


Figure 4.3: Quantum circuits for an attack on each mode

Chapter 5. Concluding Remarks

In this work, we analysed quantum security of some confidentiality modes of operation in block ciphers such as CBC, IGE, CFB, OFB, and CTR. Since the advent of quantum computers and powerful quantum adversaries does not guarantee the security of current modes of operation any more, the systematic approach to analyse quantum security was necessary. For our analysis, we first considered quantum adversaries capable of quantum computation, by classifying them as Q0, Q1, and Q2 depending on their ability. The useful quantum proof techniques were introduced for our quantum security proof. Then, quantum security notions are defined by extending classical case, in terms of quantum IND and CPA: IND-qCPA, wqIND-qCPA, and qIND-qCPA. Our results are summarised in Figure 5.1.

Desired Security	IND-CPA			IND-qCPA		(w)qIND-qCPA	
BC Assumption / Mode of Operation	Q2-secure PRF	Q1-secure PRF	Q0-secure PRF	Q2-secure PRF	Q1-secure PRF	Q2-secure PRF	Q1-secure PRF
ECB	✗	✗	✗	✗	✗	✗	✗
CBC	✓*	✓*	✓ [BDJR97]	✓ [ATTU16]	✗ [ATTU16]	✗	✗
IGE	✓*	✓*	✓†	✓ [LKLK19]	✗ [LKLK19]	✗	✗
CFB	✓*	✓*	✓ [AGPS01]	✓ [ATTU16]	✗ [ATTU16]	✗	✗
OFB	✓*	✓*	✓ [Woo08]	✓ [ATTU16]	✓ [ATTU16]	✗	✗
CTR	✓*	✓*	✓ [BDJR97]	✓ [ATTU16]	✓ [ATTU16]	✗	✗

Figure 5.1: Summary

As future work, we will study more possible confidentiality modes such as propagating cipher block chaining (PCBC) and accumulated block chaining (ABC) or other kinds of block ciphers such as tweakable block ciphers. Their encryption can be also represented in quantum circuits, which can give us some intuition in quantum security analysis. By analysing their quantum security, we may classify all kinds of modes in certain criteria and can suggest which of them has secure structure in quantum settings. There may be some structural features which weaken their security. Classifying will be able to suggest new or improved modes of operation in block ciphers, which are secure even if there are powerful quantum adversaries. We leave it as a follow-up study and suggest this work has potential for further development.

Bibliography

[ABB+15] D. Augot, L. Batina, D. J. Bernstein, J. W. Bos, J. Buchmann, W. Castryck, O. Dunkelman, T. Güneysu, S. Gueron, A. Hülsing, T. Lange, M. S. E. Mohamed, C. Rechberger, P. Schwabe, N. Sendrier, F. Vercauteren, and B.-Y. Yang. Initial recommendations of long-term secure post-quantum systems. PQCRYPTO Post-Quantum Cryptography for Long-Term Security, September 2015. https://pqcrypto.eu.org/docs/initial-recommendations.pdf.

[ABB+17] E. Alkim, N. Bindel, J. Buchmann, Ö. Dagdelen, E. Eaton, G. Gutoski, J. Krämer, and F. Pawlega. Revisiting TESLA in the quantum random oracle model. In *Proceedings of the 8th International Workshop on Post-Quantum Cryptography (PQCrypto 2017)*, pages 143–162, Utrecht, The Netherlands, June 2017.

[ATTU16] M. V. Anand, E. E. Targhi, G. N. Tabia, and D. Unruh. Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. Cryptology ePrint Archive, Report 2016/197, 2016. https://eprint.iacr.org/2016/197.

[BBBV97] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[BBC+98] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS 1998)*, Palo Alto, CA, US, November 1998.

[BDF+11] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In *Proceedings of the 17th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2011)*, pages 41–69, Seoul, South Korea, December 2011.

[BDPR98] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *Proceedings of the 18th Annual International Cryptology Conference (Crypto 1998)*, pages 26–45, Santa Barbara, CA, US, August 1998.

[Ben80] P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22(5):563–591, 1980.

[BJ15] A. Broadbent and S. Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity, June 2015. https://arxiv.org/abs/1412.8766.

[BM15] R. Bhattacharyya and P. Mukherjee. Non-adaptive programmability of random oracle. *Theoretical Computer Science*, 592:97–114, August 2015.

[BR04] M. Bellare and P. Rogaway. Code-based game-playing proofs and the security of triple encryption. Cryptology ePrint Archive, Report 2004/331, 2004. https://eprint.iacr.org/2004/331.

[BZ13] D. Boneh and M. Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. Cryptology ePrint Archive, Report 2013/088, 2013. https://eprint.iacr.org/2013/088.

[Cam78] C. M. Campbell. Design and specification of cryptographic capabilities. *IEEE Communications Society Magazine*, 16(6):15–19, November 1978.

[CJL+16] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone. Report on post-quantum cryptography. Technical report, National Institute of Standards and Technology (NIST), April 2016. http://dx.doi.org/10.6028/NIST.IR.8105.

[CSST11] C. Crépeau, L. Salvail, J.-R. Simard, and A. Tapp. Two provers in isolation. In *Proceedings of the 17th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2011)*, pages 407–430, Seoul, South Korea, December 2011.

[Deu85] D. E. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 400(1818):97–117, July 1985.

[Eat17] E. Eaton. Signature schemes in the quantum random-oracle model. Master's thesis, University of Waterloo, April 2017.

[ES15] E. Eaton and F. Song. Making existential-unforgeable signatures strongly unforgeable in the quantum random-oracle model. In *Proceedings of the 10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015)*, pages 147–162, Brussels, Belgium, May 2015.

[Fey82] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, June 1982.

[Fis05] M. Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In *Proceedings of the 25th Annual International Cryptology Conference (Crypto 2005)*, pages 152–168, Santa Barbara, CA, US, August 2005.

[FLR+10] M. Fischlin, A. Lehmann, T. Ristenpart, T. Shrimpton, M. Stam, and S. Tessaro. Random oracles with(out) programmability. In *Proceedings of the 16th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2010)*, pages 303–320, Singapore, December 2010.

[Gag17] T. Gagliardoni. *Quantum security of cryptographic primitives*. PhD thesis, Technische Universität Darmstadt, February 2017.

[GHS16] T. Gagliardoni, A. Hülsing, and C. Schaffner. Semantic security and indistinguishability in the quantum world. In *Proceedings of the 36th Annual International Cryptology Conference (Crypto 2016)*, pages 60–89, Santa Barbara, CA, US, August 2016.

[GM84] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC 2008)*, pages 197–206, New York, NY, US, May 2008.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC 1996)*, pages 212–219, Philadelphia, PA, US, May 1996.

[Gro97] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79:325–328, July 1997.

[KKVB02] E. Kashefi, A. Kent, V. Vedral, and K. Banaszek. Comparison of quantum oracles. *Physical Review A*, 65:050304, May 2002.

[KLLNP16] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In *Proceedings of the 36th Annual International Cryptology Conference (Crypto 2016)*, pages 207–237, Santa Barbara, CA, US, August 2016.

[KYY18] S. Katsumata, S. Yamada, and T. Yamakawa. Tighter security proofs for GPV-IBE in the quantum random oracle model. In *Proceedings of the 24th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2018)*, pages 253–282, Brisbane, QLD, Australia, December 2018.

[Lan61] R. W. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5(3):183–191, July 1961.

[Man80] Y. Manin. *Computable and uncomputable*. Sovetskoye Radio, Moscow, 1980. (in Russian).

[Moo65] G. E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8):114–117, April 1965.

[Nie02] J. B. Nielsen. Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case. In *Proceedings of the 22nd Annual International Cryptology Conference (Crypto 2002)*, pages 111–126, Santa Barbara, CA, US, August 2002.

[PS96] D. Pointcheval and J. Stern. Security proofs for signature schemes. In *Proceedings of the 15th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 1996)*, pages 387–398, Saragossa, Spain, May 1996.

[Sho94] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS 1994)*, pages 124–134, Santa Fe, NM, US, November 1994.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[Sim94] D. R. Simon. On the power of quantum computation. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS 1994)*, pages 116–123, Santa Fe, NM, US, November 1994.

[Sim97] D. R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, October 1997.

[SLL16] T. Shang, Q. Lei, and J. Liu. Quantum random oracle model for quantum digital signature. *Physical Review A*, 94:042314, October 2016.

[SS17] T. Santoli and C. Schaffner. Using Simon's algorithm to attack symmetric-key cryptographic primitives. *Quantum Information & Computation*, 17(1&2):65–78, February 2017. https://arxiv.org/abs/1603.07856.

[Unr10] D. Unruh. Quantum proofs of knowledge. Cryptology ePrint Archive, Report 2010/212, 2010. https://eprint.iacr.org/2010/212.

[Unr14] D. Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. Cryptology ePrint Archive, Report 2014/587, 2014. https://eprint.iacr.org/2014/587.

[vdG97] J. van de Graaf. *Towards a formal definition of security for quantum protocols*. PhD thesis, Université de Montréal, December 1997.

[Wat09] J. Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, May 2009.

[Zha12] M. Zhandry. Secure identity-based encryption in the quantum random oracle model. In *Proceedings of the 32nd Annual International Cryptology Conference (Crypto 2012)*, pages 758–775, Santa Barbara, CA, US, August 2012.

[Zha13] M. Zhandry. A note on the quantum collision and set equality problems, December 2013. https://arxiv.org/abs/1312.1027.