석사학위논문
Master's Thesis

IGE 모드를 사용한 블록암호의 양자 안전성

Validating IGE Mode of Block Cipher from Quantum Adversaries

2018

김성숙 (金成淑 Kim, Sungsook)

한국과학기술원

Korea Advanced Institute of Science and Technology

석사학위논문

IGE 모드를 사용한 블록암호의 양자 안전성

2018

김성숙

한국과학기술원

전산학부

IGE 모드를 사용한 블록암호의 양자 안전성

김 성 숙

위 논문은 한국과학기술원 석사학위논문으로
학위논문 심사위원회의 심사를 통과하였음

2017년 12월 11일

심사위원장 김 광 조 (인)

심 사 위 원 김 동 준 (인)

심 사 위 원 이 주 영 (인)

Validating IGE Mode of Block Cipher from Quantum Adversaries

Sungsook Kim

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
Master of Science in Computer Science

Daejeon, Korea
December 11, 2017

Approved by

Kwangjo Kim
Professor of School 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.

MCS
20163838

김성숙. IGE 모드를 사용한 블록암호의 양자 안전성. 전산학부 . 2018년. 36+iv 쪽. 지도교수: 김광조. (영문 논문)
Sungsook Kim. Validating IGE Mode of Block Cipher from Quantum Adversaries. School of Computing . 2018. 36+iv pages. Advisor: Kwangjo Kim. (Text in English)

초 록

이 논문에서는 블록암호 IGE 모드의 양자 안전성에 대해 다루었다. 블록암호는 일정 블록 단위로 평문을 암호화하고 있으며, 다양한 길이의 평문을 암호화하기 위하여 운영 모드를 사용한다. 널리 알려진 보안 메신저인 텔레그램은 IGE(Infinite Garble Extension)이라는 특수한 운영 모드를 사용하고 있다. IGE 모드는 European Union Agency for Network and Information Security(ENISA)에서 2013년 발표한 표준 모드 5개에 속해있지 않은 운영모드이다. 텔레그램은 표준모드가 아닌 IGE 모드를 사용함에도, 내부 프로토콜을 공개하여 그 안전성을 공개적으로 인정받고 있다. 하지만 최근 양자 컴퓨터에 대한 연구가 활발히 진행됨에 따라 현재 사용되는 블록암호들에 대한 양자안전성 증명에 대한 필요성이 대두되고 있다. 특히, 블록암호의 양자 안전성은 사용하는 암호 알고리즘과 운영모드에 따라 안전성이 결정된다. 본 논문에서는 텔레그램에서 사용되는 IGE 모드가 암호알고리즘이 sPRF(Standard-secure PRF)일 때 양자 안전성(IND-qCPA)을 보장하지 않고, qPRF(quantum-secure PRF)일때 안전성이 보장됨을 증명하였다.

핵 심 낱 말 양자 내성암호, 양자 컴퓨터, IGE 모드, 블록암호, 양자 선택평문공격에 대한 비구별성

Abstract

The Telegram which is a very popular messenger uses a special mode called IGE(Infinite Garble Extension). IGE mode is not included in standard mode of operation recommended by National Institute of Standards and Technology(NIST) in 2001. Block cipher encrypts fixed length of plaintext into the corresponding fixed-length of ciphertext using a secret key shared by two parties and utilizes lots of mode of operation for various length of plaintext. Even though Telegram uses non-standard IGE mode, Telegram is claimed to be secure and demonstrate their security is stronger than other IM's. Thus, we need to verify the security of IGE mode depending on underlying block ciphers. In this paper, we show that IGE mode block cipher used in Telegram assuming sPRF is not IND-qCPA, but assuming qPRF is IND-qCPA.

Keywords Post-quantum cryptography, Infinite Garble Extension(IGE) mode, Telegram, IND-qCPA

Contents

List of Tables

List of Figures

Chapter 1. Introduction

1.1 Post-quantum cryptography

Quantum computers can perform quantum computation using quantum-mechanics happend in quantum states like superposition and entanglement different to the classical computers. Quantum computation uses quantum bits (*i.e.,* qubits) compared to binary bits in classical computations. In general, a quantum computer with n qubits can be in an arbitrary superposition of up to 2^n different state simultaneously[4]. This indicates that qubits can hold exponentially more information than their classical counterpart.

Though the actual quantum computer is not developed yet, many experiments executing on small number of quantum bits imply that the quantum computer will be realized soon. In real, quantum computer is expected to be developed within 15 years. Quantum computers are becoming more and more likely including the recent success of IBM in building 50 qubits.

Modern cryptosystem such as AES, RSA, Diffie-Hellman(DH) and Elliptic Curve Cryptosystem(ECC) are based on cryptographic primitives. For example,in public key cryptosystem, their security relies on one of three hard mathmatical problems such as the integer factorization problem(IFP), the discrete logarithm problem(DLP), and the elliptic-curve discrete logarithm problem. However these problems can be solved within polynomial time using a powerful quantum computer by Shor's algorithm [5]. Thus we need to prepare for cryptosystem secure against the quantum computing attack which we say quantum-safe cryptosystem such like lattice-based, hash-based, code-based, multivariate, and isogeny cryptography.

In symmetric key cyrptosystem, data search algorithm called Grover's algorithm [6] can find the member given database in complexity $O(\sqrt{N})$ compare to $O(N)$ in classical world. The suggested method against quantum computer is doubling the key size; use 256 bits key instead 128 bits key in RSA.

1.2 Motivation

Block ciphers, one of the symmetric key cryptosystem, can only encrypt a fixed length of a message. But for practice we need to encrypt or decrypt for arbitrary-length of message. To meet this, block cipher offers lots of mode of operation like Electronic Codebook(ECB), Output Feedback(OFB), Cipher Feedback(CFB), Cipher Block Chaining(CBC), and XEX-based tweaked-codebook mode with ciphertext stealing(XTS), *etc.* Some mode of operations can increase the message space or provide semantic security depending on the mode of operation.

Telegram, one of the famous instant messaging(IM) services, use Infinite Garble Extension(IGE)[7] mode in their customised protocol called MTProto. IGE mode is not classified as standard mode of operation National Institute of Standards and Technology(NIST)[8]. However this Telegram is claimed to be secure though they use IGE mode. Even Telegram got great score by Electronic Frontier Foundation(EFF) in 2014[3]. Different to other IM's, Telegram open their source code, protocol, and API in order to be made by the public scrutiny of the security experts from the world. This demonstrates indirectly to show that their security is sufficient strong than other IM's. However the overall security of Telegram can be vulnerable against the quantum adversaries. Thus we need to verify the security of Telegram against the quantum adversaries, especially IGE mode used for underlying block ciphers.

In this paper, we focus on the quantum security of IGE mode in block cipher. We will show that (i) if the block cipher is assumed to be standard-secure Pseudo Random Function(sPRF), the block cipher of IGE mode is not IND-qCPA(similar with IND-CPA in classical setting except that the adversary $\mathcal{A}$ has the quantum access). (ii) if the block cipher is assumed to be quantum-secure Pseudo Random Function(qPRF), the block cipher of IGE mode is IND-qCPA.

1.3 Organization

The rest of this thesis is organized as follows: Chapter 2 describes related work about the other study and preliminaries about our definitions and notation used in this thesis. The overview of Telegram, its IGE mode and security are described in Chapter 3. The security proof for sPRF, qPRF is explained in Chapter 4 and 5, respectively. Finally, the conclusion and future work are discussed in Chapter 6.

Chapter 2. Related Work and Preliminaries

2.1 Preliminaries

2.1.1 Notation

$y \leftarrow A(x)$ means that an algorithm A when takes the input x outputs a value and this value is assigned to y. Given an algorithm A, we write A^H if A can access to an oracle H. ($A \leftarrow B$) denote the set of all function from A to B. We write $x \overset{\$}{\leftarrow} A$ if x is uniformly randomly chosen from the set A. $a \parallel b$ represents concatenations of two strings and $\{0, 1\}^n$ represents the n-bit strings. $a \odot b$ means the inner product of two vectors a and b.

We use $\eta(t)$ to denote a function with a security parameter t. If we say a quantity is *negligible*(denoted *negl.*) we mean that it is in $o(\eta^c)$ or $1 - o(\eta^c)$ for all $c > 0$. We use the notation $A \approx B$ to say that quantity A has *negl.* difference with quantity B.

For an n-bit string a and binary variable b, $a \cdot b = a$ if $b = 1$ else $a \cdot b = 0^n$. For a string $x = x_1x_2x_3 \cdots x_n$ where x_i is the $i - th$ bit, we use function $lastbit(x) = (x_n), droplastbit(x) = x_1x_2x_3 \cdots x_{n-1}$.

2.1.2 IND-CPA, IND-qCPA

Definition 1 (IND-CPA)**.** *A symmetric encryption scheme* Π_{IGE} *=(Gen,Enc,Dec) is indistinguishable under chosen message attack(IND-CPA secure) if no classical polynomial time adversary* $\mathcal{A}$ *can win in the* $PrivK^{CPA}_{\mathcal{A},\pi}$ *game, except with probability at most 1/2 + negl.*

$PrivK^{CPA}_{\mathcal{A},\pi}$**(t)** *game:*

> ***Key Gen:*** *The challenger picks a random key* $k \overset{\$}{\leftarrow}$ *Gen and a random bit b.*
>
> ***Query:*** *Adversary* $\mathcal{A}$ *chooses two messages* m_0, m_1 *and sends them to the challenger.*
> *Challenger chooses* $r \overset{\$}{\leftarrow} \{0, 1\}^*$ *and responds with* $c^* =$ *Enc*$_k(m_b; r)$
>
> ***Guess:*** *Adversary* $\mathcal{A}$ *produces a bit* b'*, and wins if* $b = b'$

There are different kinds of definition of IND-qCPA, but we use one in [9]. In the IND-qCPA, the quantum adversary can queries in superposition but the challenge queries are classical as in classical world.

Definition 2 (IND-qCPA[9])**.** *A symmetric encryption scheme* Π_{IGE} *=(Gen,Enc,Dec) is indistinguishable under a quantum chosen message attack(IND-qCPA secure) if no efficient quantum adversary* $\mathcal{A}$ *can win in the* $PrivK^{qCPA}_{\mathcal{A},\pi}$ *game, except with probability at most 1/2 + negl.*

$PrivK^{qCPA}_{\mathcal{A},\pi}$**(t)** *game:*

> ***Key Gen:*** *The challenger picks a random key* $k \overset{\$}{\leftarrow}$ *Gen and a random bit b.*
>
> ***Queries*** $\mathcal{A}$ *is allowed to make two types of queries:*

- **Challenge Queries:** *$\mathcal{A}$ sends two messages m_0, m_1 to challenger and challenger responds with $c* = Enc_k(m_b; r)$.*

- **Encryption Queries:** *For each query, the challenger chooses randomness $r \xleftarrow{\$} \{0,1\}^*$, and encrypts each message in the superposition using r as randomness:*

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

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

2.1.3 sPRF, qPRF

Definition 3 (Standard-secure PRF [10])**.** *A function PRF is a standard-secure PRF if no efficient quantum adversary $\mathcal{A}$ making classical queries can distinguish between a truly random function and a function PRF$_k$ for a random k. That is, for every such $\mathcal{A}$, there exist a negligible function $\epsilon = \epsilon(t)$ such that*

$$|\mathbf{Pr}_{k \leftarrow \mathcal{K}}[A^{PRF_k}() = 1] - \mathbf{Pr}_{\mathcal{O} \leftarrow \mathcal{K}^{\mathcal{X}}}[A^{\mathcal{O}}() = 1]| < \epsilon$$

Definition 4 (Quantum-secure PRF [10])**.** *A function PRF is a standard-secure PRF if no poly-time quantum adversary $\mathcal{A}$ making quantum queries can distinguish between a truly random function and a function PRF$_k$ for a random k.*

2.1.4 Authenticated Encryption

Although the previous modes of operation give confidentiality for block ciphers, much better modes that simultaneously provide confidentiality, integrity, and authenticity known as AE were developed. In 2000, Bellare and Namprempre introduced the notion of AE to guarantee both confidentiality of the message and integrity of the sender while transmission over an insecure channel like mobile network [11]. As a very natural way to construct AE, they suggested a generic composition paradigm on secure encryption and secure MAC protocols such as AES and HMAC. They used indistinguishability under chosen-plaintext attack (IND-CPA), non-malleability under chosen-plaintext attack (NM-CPA), or indistinguishability under chosen-ciphertext attack (IND-CCA) for confidentiality like the classical block ciphers as security requirements of AE, then introduced two notions for integrity, namely integrity of plaintexts (INT-PTXT) and integrity of ciphertexts (INT-CTXT) assuming that the adversary $\mathcal{A}$ is allowed a chosen-message attack as below:

Definition 5 (INT-PTXT)**.** *AE satisfies INT-PTXT security if the advantage of any probabilistic polynomial-time adversary $\mathcal{A}$ to produce a ciphertext $c = \mathcal{E}(m)$, where m is not previously produced by the sender, is negligible.*

Definition 6 (INT-CTXT)**.** *AE satisfies INT-CTXT security if the advantage of any probabilistic polynomial-time adversary $\mathcal{A}$ to produce a ciphertext $c = \mathcal{E}(m)$ not previously produced by the sender is negligible, regardless of whether the underlying plaintext m is new or not.*

From the above security requirements, they designed and analysed three composition methods on encryption and MAC protocols, namely Encrypt-and-MAC (E&M), MAC-then-Encrypt (MtE), and Encrypt-then-MAC (EtM) as below:

E&M: For encryption with authentication, we encrypt a plaintext m as $Enc(m)$ where Enc is an encryption algorithm of secure encryption protocol and append a tag t of m using MAC, *i.e.*, a ciphertext $\mathcal{E}(m) = Enc(m)\|t$. For decryption with verification, we check the validity of the tag as well as the decryption of the ciphertext.

Table 2.1: Security results for the composite AE schemes

	IND -CPA	IND -CCA	NM -CPA	INT -PTXT	INT -CTXT
E&M	insecure	insecure	insecure	secure	insecure
MtE	secure	insecure	insecure	secure	insecure
EtM	secure	secure	secure	secure	secure

MtE: For encryption with authentication, we encrypt a plaintext m as $Enc(m)$ and append a tag t of $Enc(m)$ instead of m, *i.e.*, a ciphertext $\mathcal{E}(m) = Enc(m)\|t_{enc}$ where t_{enc} is a tag of $Enc(m)$. For decryption with verification, we first verify the tag and then decrypt the ciphertext.

EtM: For encryption with authentication, we append a tag t of m first, then encrypt an appended plaintext $m\|t$, *i.e.*, a ciphertext $\mathcal{E}(m) = Enc(m\|t)$. For decryption with verification, we first decrypt the ciphertext to get the plaintext and the tag.

Table 2.1 [11] describes security results for the composite AE schemes when the given MAC is assumed to be strongly unforgeable and shows that EtM can only reach the highest definition of security in AE.

Aside from this research, Bellare & Rogaway and An & Bellare suggested ‘encode-then-encipher’ [12] and ‘encryption with redundancy’ [13] approaches, respectively, but both of them are rather insecure and inefficient than the general composition paradigm [14]. Thus, we focus on a generic composition paradigm for the rest of the paper.

2.2 Quantum security

2.2.1 Quantum computation

A quantum system A is a complex Hilbert space $\mathcal{H}$ together with and inner product $\langle\cdot|\cdot\rangle$. The state of a quantum system is given by a vector $|\psi\rangle$ of unit norm ($\langle\psi|\psi\rangle = 1$). Given quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$, the joint quantum system is given by the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$. Given $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$, the product state is given by $|\psi_1\rangle|\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$. Given a quantum state $|\psi\rangle$ and an orthonormal basis $B = |b_0\rangle, \ldots, |b_{d-1}\rangle$ for $\mathcal{H}$, a measurement of $|\psi\rangle$ in the basis B results in the value i with probability $|\langle b_i|\psi\rangle|^2$, and the quantum state collapses to the basis vector $|b_i\rangle$. If $|\psi\rangle$ actually a state in a joint system $\mathcal{H} \otimes \mathcal{H}'$, then $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |b_i\rangle|\psi_i'\rangle$$

for some complex values α_i and states $|\psi_i'\rangle$ over $\mathcal{H}'$. Then, the measurement over $\mathcal{H}$ obtains the value i with probability $|\alpha_i|^2$ and in this case the resulting quantum state is $|b_i\rangle|\psi_i'\rangle$. A unitary transformation over a d-dimensional Hilbert space $\mathcal{H}$ is a $d \times d$ matrix $\mathbf{U}$ such that $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I}_d$, where $\mathbf{U}^\dagger$ represents the conjugate transpose. A quantum algorithm operates on a product space $\mathcal{H}_{in} \otimes \mathcal{H}_{out} \otimes \mathcal{H}_{work}$ and consists of n unitary transformations $\mathbf{U}_1, \ldots, \mathbf{U}_n$ in this space. $\mathcal{H}_{in}$ represents the input to the algorithm, $\mathcal{H}_{out}$ the output, and $\mathcal{H}_{work}$ the work space. A classical input x to the quantum algorithm is converted to the quantum state $|x, 0, 0\rangle$. Then, the unitary transformations are applied one-by-one, resulting in the final state

$$|\psi_x\rangle = \mathbf{U}_n \ldots \mathbf{U}_i |x, 0, 0\rangle.$$

The final state is then measured, obtaining the tuple (a, b, c) with probability $|\langle a, b, c|\psi_x\rangle|^2$. The output of the algorithm is b. We say that a quantum algorithm is efficient if each of the unitary matrices $\mathbf{U}_i$ come from some fixed basis set, and n, the number of unitary matrices, is polynomial in the size of the input.

Quantum-accessible Oracles. We will implement an oracle $\mathcal{O} : \mathcal{X} \rightarrow \mathcal{Y}$ by a unitary transformation $\mathbf{O}$ where

$$\mathbf{O}|x, y, z_i\rangle = |x, y + O(x), z\rangle$$

where $+ : \mathcal{X} \times \mathcal{X} \rightarrow \mathcal{X}$ is some group operation on $\mathcal{X}$. Suppose we have a quantum algorithm that makes quantum queries to oracles $\mathcal{O}_1, \ldots, \mathcal{O}_q$. Let $|\psi_0\rangle$ be the input state of the algorithm, and let $\mathbf{U}_0, \ldots, \mathbf{U}_q$ be the unitary transformations applied between queries. Note that the transformations $\mathbf{U}_i's$ can be the products of many simpler unitary transformations. The final state of the algorithm will be

$$\mathbf{U}_q\mathbf{O}_q \dots \mathbf{U}_1\mathbf{O}_1\mathbf{U}_0|\psi_0\rangle$$

We can also have an algorithm that makes classical queries to $\mathcal{O}_i$. In this case, the input to the oracle is measured before applying the transformation $\mathbf{O}_i$. We call a quantum oracle algorithm efficient if the number of queries q is polynomial, and each of the transformations $\mathbf{U}_i$ between queries can be written as the product polynomially many unitary transformations from some fixed basis set.

2.2.2 Simon's algorithm

Simon's problem deals with the model of decision tree complexity or query complexity and was conceived by Daniel Simon in 1994 [15]. Simon's problem is then, by querying $f(x)$ to determine whether the function belongs to $s = 0^n$ or $s \neq 0^n$. Sometimes Simon's algorithm is required to find s. Daniel showed that by using Simon's algorithm solving the problem exponentially is faster than any other classical algorithm.

In Simon' problem the function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ is given which satisfies the property that for some $s \in \{0,1\}^n$, we have for all $x, y \in \{0,1\}^n, f(x) = f(y)$ if and only if $x = y$ or $x = y \oplus s$. Classically, order $2^{n/2}$ queries are needed to find s. But in quantum algorithm, only n queries.

Consider quantum circuit as described in 2.1:

Prepare the initial state $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|0^n\rangle$ and call the oracle(U_f) to transform this state to $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$. When $x = y \oplus s$, the first register is $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)$(here x is s-periodic in U_f).

After Hadamard transforms, the state is :

$$\frac{1}{\sqrt{2^{n+1}}} \sum_z \sum_x [(-1)^{x \cdot z} + (-1)^{(x \oplus x) \cdot z}]|z\rangle|f(x)\rangle$$

Since we are working modulo 2, we can factor out the $(-1)^{x \cdot z}$: $\frac{1}{\sqrt{2^{n+1}}} \sum_z \sum_x (-1)^{x \cdot z}[1 + (-1)^{s \cdot z}]|z\rangle|f(x)\rangle$. Then we measure this state in the computational basis, we will obtain uniformly at random a bit string z such that $x \cdot z = 0$. Using this property, we can cuts in half the number of possible s strings only in one query. In classical, we can get nothing in one query. By repeating this query, we can get lineally independent equations $s \cdot z_1 = 0, s \cdot z_2 = 0, \cdots s \cdot z_{n-1} = 0$. Thus using that equations, we can recover s.

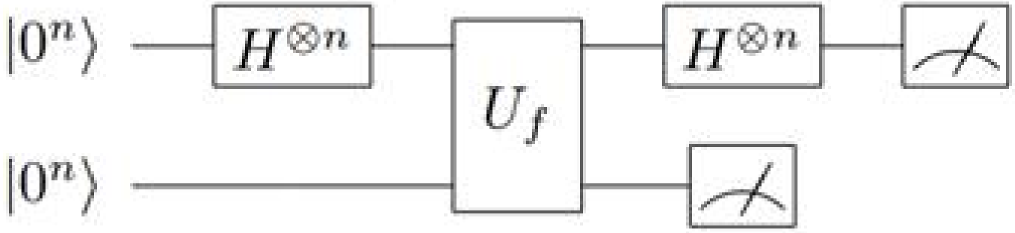


Figure 2.1: Quantum circuit in Simon's algorithm

2.3 One way to hiding(O2H) Lemma

This lemma below is devised from Unruh in 2015[16]. This lemma basically shows that given a uniformly random value s, to show that $H(x)$ is also uniformly random(indistinguishable from random) we need to show this : when adversary queries to oracle, abort the query to H at random point, measure the input to that query(disturbing superposition in quantum), then the probability the input equals x is negligible. This lemma is used in Chapter 5 to set up the boundary of probability.

Lemma 1 (One way to hiding(O2H) Lemma)**.** *Let* $H : \{0,1\}^t \to \{0,1\}^t$ *be a random oracle. Consider an oracle algorithm* A_{O2H} *that makes at most* q_{o2h} *queries to* H*. Let* B *be an oracle algorithm that on input* x *does the following:*

pick $i \xleftarrow{\$} \{1, \cdots, q_{o2h}\}$ *and* $y \xleftarrow{\$} \{0,1\}^t$*, run* $A^H_{O2H}(x, y)$ *until (just before) the* i*th query, measure the argument of the query in the computational basis, output the measurement outcome. (When* A_{O2H} *makes less than* i *queries,*B *outputs* $\perp \notin \{0,1\}^t$*.) Let,*

$P^1_{A_{O2H}} := \mathbf{Pr}[b' = 1 : H \xleftarrow{\$} (\{0,1\}^t \to \{0,1\}^t), x \xleftarrow{\$} \{0,1\}^t, b' \leftarrow A^H_{O2H}(x, H(x))]$,
$P^2_{A_{O2H}} := \mathbf{Pr}[b' = 1 : H \xleftarrow{\$} (\{0,1\}^t \to \{0,1\}^t), x \xleftarrow{\$} \{0,1\}^t, y \xleftarrow{\$} \{0,1\}^t, b' \leftarrow A^H_{O2H}(x, y)]$,
$P_B := \mathbf{Pr}[x' = x : H \xleftarrow{\$} (\{0,1\}^t \to \{0,1\}^t), x \xleftarrow{\$} \{0,1\}^t, x' \leftarrow B^H(x, i)]$.
Then,

$$|P^1_{A_{O2H}} - P^2_{A_{O2H}}| \leq 2q_{o2h}\sqrt{P_B}.$$

2.4 Related Work

A lot of study in the security of cryptography against the quantum computer were done. Boneh *et al.* [17] and Zhandry [18] prove that the signature, encryption, and identity-based encryption scheme is classical secure in the quantum random oracle model where the adversary can query the random oracle in superposition. This paper show some random oracle construction is still secure in the quantum random oracle model.

Also Zhandry [10] showed how to construct pseudorandom functions (PRFs) that remain secure even when the adversary is allowed to issue quantum queries to the PRF. Zhandry showed that certain PRFs are secure even under such a powerful query model.

Anand *et al.* [19] investigated the security of various modes of operations for block cipher against quantum superposition attacks. They show that OFB and CTR modes are secure, while CBC and CFB are not secure in general, but are secure if the underlying PRF is quantum secure.

In [20] Boneh and Zhandry show how to construct the message authentication codes(MACs) that remain secure against a quantum chosen message attack and show that quantum-secure PRF leads to quantum-secure MACs. Also they showed that some classically secure MACs become insecure against quantum adversary.

Chapter 3. Telegram

3.1 Overview

Telegram is known as one of the most popular non-profit cloud-based instant messaging(IM) services for secure communications. Telegram had 100 million monthly active users sending 15 billion messages per day in 2016[21]. People can send messages and exchange photos,video and other files. They offers two modes; regular chat and secret chat mode. In regular chat mode, all messages can be read by server and stored. But secret chat uses an end-to-end encryption(E2EE). In this mode, because all messages are encrypted by the end users, server can not read original messages and the messages is not stored in the middle.

3.1.1 MTProto

Telegram uses a symmetric encryption scheme called MTProto. MTProto uses Diffie-Hellman (DH) key exchange, Secure Hash Algorithm 1(SHA-1), Key Derivation Function(KDF), and AES-256 in IGE[7] mode as cryptographic primitives and the overall process is described in 3.1

Key generation

The DH key exchange is used for generating an ephemeral key. After key exchange, the sender and the receiver share the same 2048-bit symmetric key K. In order to protect past communications, secret key is regenerated once a key has been used for more than 100 messages or more than a week.

The payload x is generated by concatenating some auxiliary information, random bytes, message, and padding such that $|x| \bmod B = 0$ where B is the block length. Then the payload except padding is computed by hash function SHA-1 whose output named tag. This tag is hashed again by KDF for generating AES key and IV. The input of KDF is (K, tag) and the output is (k, c_0, m_0) of the length (κ, B, B) where $\kappa = 256$ bits and B = 128 bits.

Encryption

The AES-256 in IGE mode is used for encryption. Let $x_1, \ldots, x_l$ be the l blocks of the payload, each of length B, then ciphertext is computed as below:

$$c_i \leftarrow F_k(m_i \oplus c_{i`1}) \oplus m_{i`1}$$

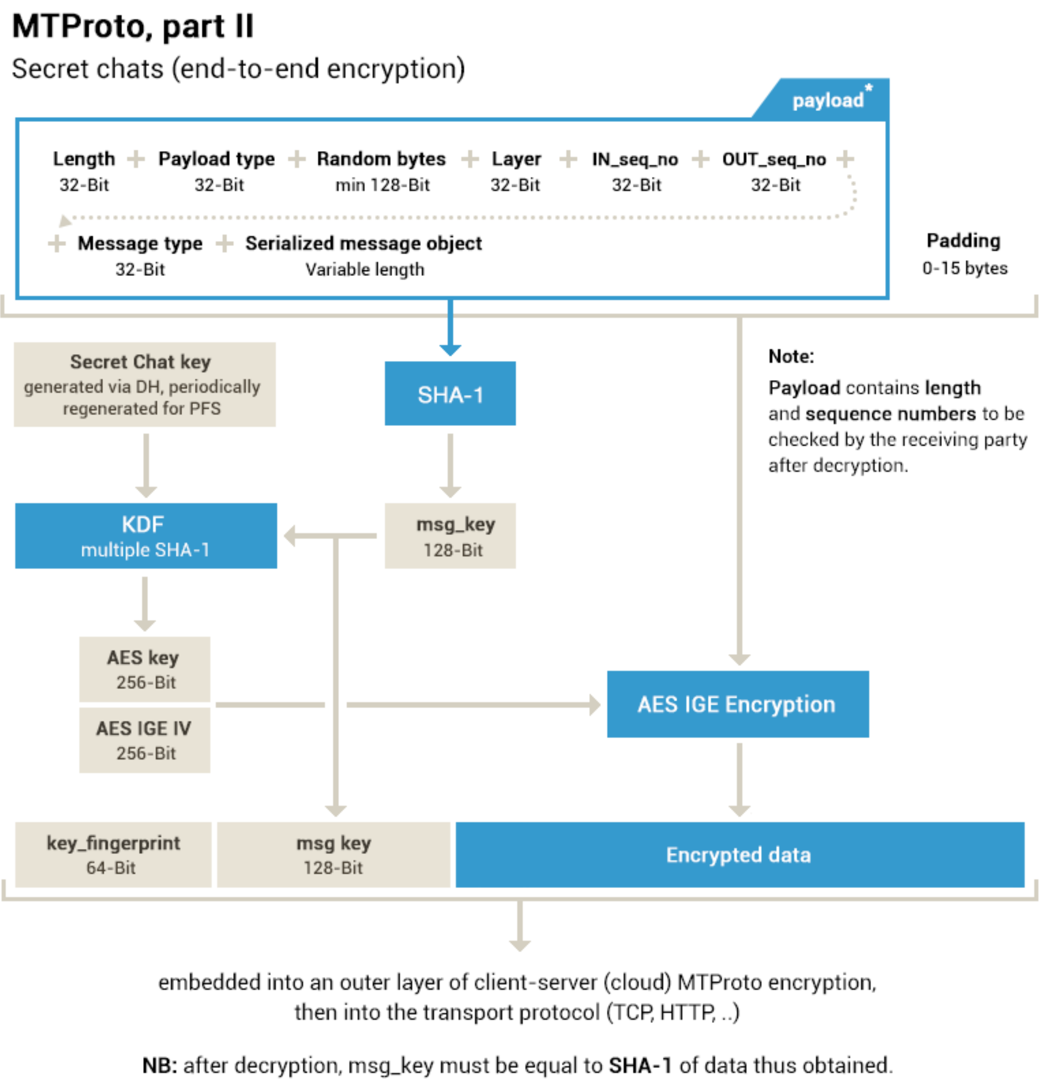

MTProto, part II
Secret chats (end-to-end encryption)
payload*
Length 32-Bit
Payload type 32-Bit
Random bytes min 128-Bit
Layer 32-Bit
IN_seq_no 32-Bit
OUT_seq_no 32-Bit
Message type 32-Bit
Serialized message object Variable length
Padding 0-15 bytes
Secret Chat key generated via DH, periodically regenerated for PFS
SHA-1
Note: Payload contains length and sequence numbers to be checked by the receiving party after decryption.
KDF multiple SHA-1
msg_key 128-Bit
AES key 256-Bit
AES IGE IV 256-Bit
AES IGE Encryption
key_fingerprint 64-Bit
msg key 128-Bit
Encrypted data
embedded into an outer layer of client-server (cloud) MTProto encryption, then into the transport protocol (TCP, HTTP, ..)
NB: after decryption, msg_key must be equal to SHA-1 of data thus obtained.

Figure 3.1: Secret chats in MTProto [1]

where F is a pseudorandom permutation, e.g., AES. The final output of the encryption is c including other information.

$$c = (tag, c_1, \ldots, c_l)$$

Decryption

Given ciphertext c, tag is used again in KDF. Using (tag, K), KDF output is (k, c_0, m_0) same as encryption. Also, the IGE mode is used again for decryption and the payload x is recovered.

$$m_i \leftarrow F_k^{-1}(m_{i-1} \oplus c_i) \oplus c_{i-1}$$

The payload except padding is computed by hash function and checks whether the result is same as tag in ciphertext c. If so, we can verify that the message in payload is original plaintext.

3.1.2 Infinite Garble Extension(IGE) mode

IGE[7] mode was initially introduced by Campbell in 1978 to prevent spoofing attacks. It has the property that errors are propagated forward, that is, any difference in ciphertext changes (*i.e.*, garbles) the decryption of all subsequent ciphertext. The diagrams of IGE mode for encryption and decryption are depicted in Figure 3.2 and 3.3, repectively.

Definition 7 (IGE scheme)**.** *For a given function $E : K \times \{0,1\}^t \to \{0,1\}^t$ we define the symmetric encryption scheme Π_{IGE} =(Gen,Enc,Dec) as follows:*

Gen: Pick a random key $k \overset{\$}{\leftarrow} K$.

Enc: For a given message $M = m_0 m_1 \cdots m_n$, where $m_0 \overset{\$}{\leftarrow} \{0,1\}^t$ and n is a polynomial in t; Enc$_k(M) := c_0 c_1 \cdots c_n$, where $c_0 \overset{\$}{\leftarrow} \{0,1\}^t$ and $c_i = E(k, c_{i-1} \oplus m_i) \oplus m_{i-1}$ for $0 < i \leq n$

Dec: For a given cipher-text $C = c_0 c_1 \cdots c_n$ and the key k; $m_i := E^{-1}(k, c_i \oplus m_{i-1}) \oplus c_{i-1}$ for $0 < i \leq n$

When encrypt the message, the initialisation vector(IV) can be defined using a second key k_0, then the ciphertext will be $c_0 = E(k_0, m_0)$ or random value like definition 7. But we just take the latter without loss of generality.

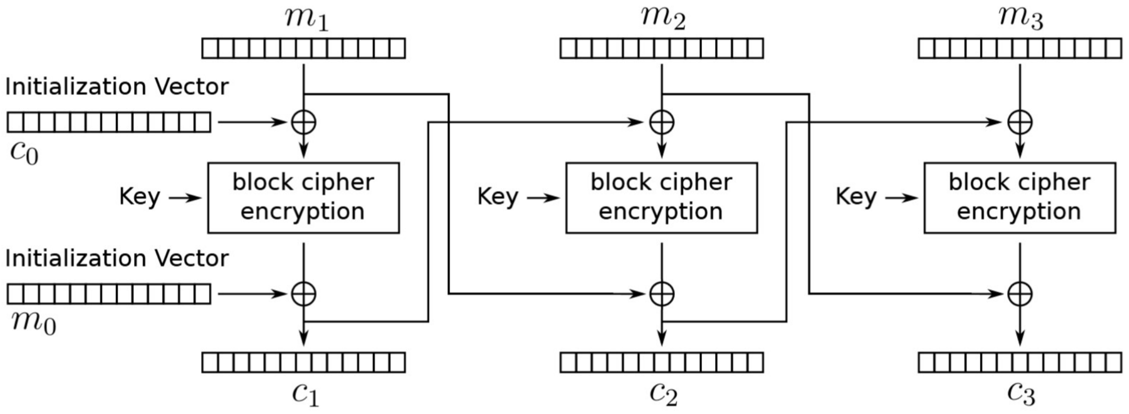


Figure 3.2: Diagram of IGE mode of operation for encryption [2]

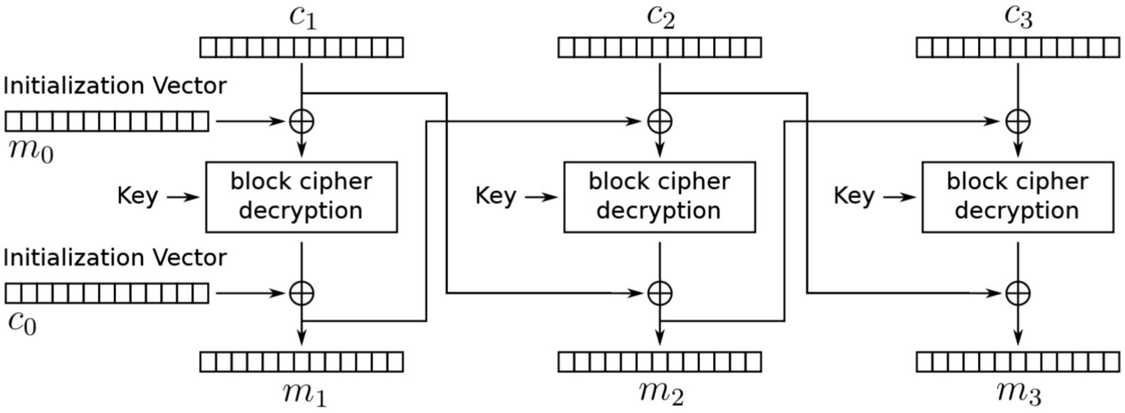


Figure 3.3: Diagram of IGE mode of operation for decryption [2]

3.2 Security of Telegram

As smartphones came into widespread use in the late 2000s, a number of instant messaging (IM) services such as WhatsApp, KakaoTalk, LINE, Facebook Messenger, and Telegram have burst onto mobile app stores. The various IM clients can be classified into three types according to their provided encryption protocols: no encryption, client-to-server encryption, and client-to-client or end-to-end encryption(E2EE). Since the lack of privacy protection has been issued constantly, now the majority of IM services provide E2EE based on verified cryptographic protocols. Telegram is particularly regarded as one of the most secure services in public and has over 100 million active users. Based on Telegram's customized protocol called MTProto, it provides client-to-server encryption in cloud chats for syncing all connected devices and E2EE in secret chats for only two devices that used to initiate or accept the secret chat.

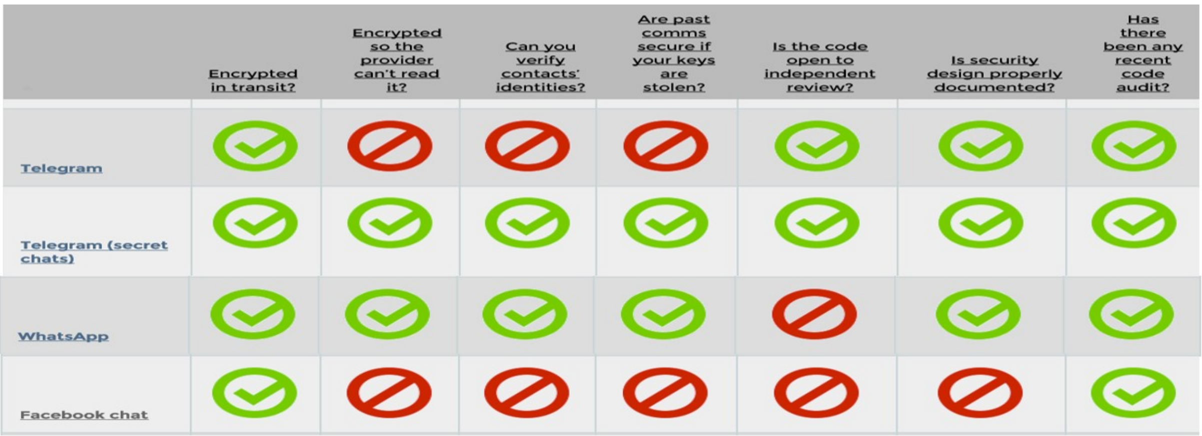
This brand new protocol, however, is actually in doubt and has not been fully scrutinised by cryptanalytic experts yet. Given that there already exist other protocols that thoroughly audited and universally praised as secure, avoiding criticism for MTProto seems unlikely unless extensive investigation is done. One of the most popular cryptographic protocols is Signal Protocol (formerly known as the Axolotl Protocol) developed by Open Whisper Systems in 2013[22] and currently implemented into Signal, WhatsApp,Google Allo, and Facebook Messenger. As of October 2016, its latest version is considered as sound and has no major flaws according to the researchers from three different universities[23].

Meanwhile, Telegram's MTProto has been criticized until now and Jakobsen *et al.*[2, 24] theoretically demonstrated Telegram 2.7.0 (visited GitHub in April 2015) is not indistinguishability under chosen-ciphertext attack

(IND-CCA) and integrity of ciphertexts (INT-CTXT). From the fact that MTProto does not check neither the length nor the content of the padding during block cipher decryption, two attacks were tried: (a) adding a random block at the end of the ciphertext and (b) replacing the last block with a random block. The first weakness can be fixed easily by adding the process to check the length of the padding during decryption and discard the message when it is longer than expected. As for mitigating the second weakness, the encryption process should be changed, which makes communications between patched and unpatched clients difficult. Thus, it is desirable to replace the current scheme with the entirely different, better one that guarantees Authenticated Encryption(AE).

However still Telegram is claimed secure protocol. Though they use IGE mode, it is not broken in their implementation. The fact that they do not use IGE as MAC together with other properties of their system makes the known attacks on IGE irrelevant. IGE mode itself is vulnerable to adaptive CPA, however, the adaptive attack is impossible in Telegram. Because the adaptive attacks are only for the case when the same key is used in several messages, but the key is dependent on the message content in Telegram.

Futhermore Electronic Frontier Foundation(EFF) announced "Secure Messaging Scorecard[3]" in 2014 depicted in figure 3.4, and Telegram got 4 out of 7 in cloud chat and 7 out of 7 in secret chat whereas Facebook chat got onlt 2 out of 7. Telegram opens their source code, protocol and API and holds crypto contest to crack Telegram's encryption so that people can see how everything works and welcome security experts to audit their system and get feedback.



	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Telegram	✓	⊘	⊘	⊘	✓	✓	✓
Telegram (secret chats)	✓	✓	✓	✓	✓	✓	✓
WhatsApp	✓	✓	✓	✓	⊘	✓	✓
Facebook chat	✓	⊘	⊘	⊘	⊘	⊘	✓

Figure 3.4: Secure messaging scorecard [3]

3.2.1 Known attack on telegram

Jakobsen *et al.* theoretically demonstrated that MTProto does not meet IND-CCA and INT-CTXT in 2015[2, 24]. Based on random padding vulnerabilities that MTProto does not check neither the length nor the content of the padding during AES-256 in IGE mode decryption, two attacks were tried: padding length extension and last block substitution.

3.2.2 Attack 1: Padding Length Extension

From **Definition 6**, they created a new ciphertext to break INT-CTXT security of MTProto. In order to understand INT-CTXT security, let us restate why MTProto is not IND-CCA secure using **Lemma 2**.

Lemma 2. *For a probabilistic polynomial-time adversary $\mathcal{A}$, $\mathcal{A}$ always wins the following game, i.e., MTProto is not IND-CCA secure under the following game.*

1. $\mathcal{A}$ outputs different messages M_0 and M_1 of the same length.

2. The challenger $\mathcal{C}$ chooses $b \in \{0, 1\}$ randomly and outputs the ciphertext $C_b \leftarrow \mathcal{E}(M_b)$.

3. $\mathcal{A}$ appends a 128-bit random block c_r to C_b and ask $\mathcal{C}$ to decrypt $C' = C_b \| c_r$.

4. $\mathcal{C}$ returns M' where $M' = M_b$ for any b.

5. $\mathcal{A}$ guesses b as 0 if $M' = M_0$, 1 otherwise.

This attack is possible since extra padding on ciphertext yields only the extension of the padding of plaintext without changing the plaintext. Obviously, $\mathcal{A}$ gets a ciphertext $C' = \mathcal{E}(M_b)$ for M_b and this ciphertext has not been previously produced by the sender because of the random padding.

Corollary 2.1. *MTProto protocol is not INT-CTXT secure from* ***Lemma 2****.*

To be secure against this attack, it is necessary to check the length of padding in M' by modifying the decryption process. Decryption algorithm will discard the message if the length of padding is larger than the block size.

3.2.3 Attack 2: Last Block Substitution

Since the padding is not authenticated in the process of MTProto, it is possible to make a collision with a non-negligible probability as **Lemma 3**, by modifying the last 128-bit (16-byte) blocks.

Lemma 3. *For a probabilistic polynomial-time adversary $\mathcal{A}$, $\mathcal{A}$ wins the following game with a probability at most 2^{-8}, i.e., MTProto is not INT-CTXT secure under the following game.*

1. $\mathcal{A}$ outputs a message M whose length in bytes is equal to $b \bmod 16$.

2. The challenger $\mathcal{C}$ hashes M into the message key $msg\_key \leftarrow$ SHA-1(M) to provide integrity of the plaintext.

3. Before encryption, $16 - b$ random bytes of padding r are added to M, then sends $C = \mathcal{E}(M \| r)$.

4. $\mathcal{A}$ modifies last 16-byte blocks of C to get $C' \neq C$.

5. $\mathcal{A}$ outputs C'.

Proof. From the above game, $\mathcal{C}$ decrypts C' as $M' \| r'$. Then, only the last byte of M' is different from M by the non-malleability of IGE mode.

Thus, they claim that it is possible to have $M' = M$ with the probability at most 2^{-8} when $\mathcal{A}$ chooses a message M with the length in bytes equal to $1 \bmod 16$, *i.e.*, they can generate a valid ciphertext $C' \neq C$ with the probability at most 2^{-8}. □

To make the protocol secure against this attack, it is sufficient to add padding to the computation of the authentication tag. But, since this requires to change the whole encryption with authentication process, it becomes impossible to communicate with the older versions of the protocol due to version compatibility.

Chapter 4. Insecurity of IGE mode using sPRF

In this chapter, we will show that IGE mode block cipher is not secure when we use standard secure PRF. That means, we can attack the IGE mode block cipher and even recover the key within polynomial time. To show that, we first construct a function which is sPRF and not qPRF as described below.

4.1 Standard-secure PRF

For the first step to construct a sPRF, Anand *et al.* construct a specific block cipher follows[19]:

$$\mathrm{BC}_k(x) := E_{H(k)}(\mathit{droplastbit}(x \oplus (k \parallel 1) \cdot \mathit{lastbit}(x)))$$

where E is a sPRF and H refers to a random oracle. Actually this block cipher is not a block cipher because it is not decryptable. (This block cipher's input is x and key k which is n and $n-1$bit respectively, but the outcome is only $n-1$ bit. But we will use some trick to change this incomplete block cipher to complete block cipher explained later in the second step.)

This block cipher has the special property, $(k \parallel 1)$-periodic:

- **Case 1 :** x is even, $\mathit{lastbit}(x) = 0, \mathit{lastbit}(x \oplus (k \parallel 1)) = 1$,

  $\mathrm{BC}_k(x \oplus (k \parallel 1)) = E_{H(k)}(\mathit{droplastbit}(x \oplus (k \parallel 1) \oplus (k \parallel 1))) = E_{H(k)}(\mathit{droplastbit}(x))$

  $= E_{H(k)}(\mathit{droplastbit}(x \oplus (k \parallel 1) \cdot \mathit{lastbit}(x))) = \mathrm{BC}_k(x)$

- **Case 2 :** x is odd, $\mathit{lastbit}(x) = 1, \mathit{lastbit}(x \oplus (k \parallel 1)) = 0$,

  $\mathrm{BC}_k(x \oplus (k \parallel 1)) = E_{H(k)}(\mathit{droplastbit}(x \oplus (k \parallel 1)))$

  $= E_{H(k)}(\mathit{droplastbit}(x \oplus (k \parallel 1) \cdot \mathit{lastbit}(x))) = \mathrm{BC}_k(x)$

Thus we can use this property:

$$\mathrm{BC}_k(x) = \mathrm{BC}_k(x \oplus (k \parallel 1)) \tag{4.1}$$

The second step for sPRF is to make that $\mathrm{BC}_k(x)$ to be decryptable. To do that, additional function t is appended in following construction.

Construction 1:

$$\mathrm{BC}_k(x) := E_{H(k)_1}(\mathit{droplastbit}(x \oplus (k \parallel 1) \cdot \mathit{lastbit}(x))) \parallel t_{H(k)_2}(x \oplus (k \parallel 1) \cdot \mathit{lastbit}(x)) \oplus \mathit{lastbit}(x)$$

where $E : \{0,1\}^{n-1} \times \{0,1\}^{n-1} \rightarrow \{0,1\}^{n-1}$ is a sPRF, $t : \{0,1\}^{n} \times \{0,1\}^{n} \rightarrow \{0,1\}$ is a sPRF, $H : \{0,1\}^{n} \rightarrow \{0,1\}^{n} \times \{0,1\}^{n}$ is a random oracle, the key $k \xleftarrow{\$} \{0,1\}^{n-1}$, and

$H(k) = H(k)_1 \parallel H(k)_2$

We can easily know this construction is permutation by proving that given $\mathrm{BC}_k(x) = y$ and k, we can recover x:

Proof. $z := x \oplus (k \parallel 1) \cdot \mathit{lastbit}(x)$, then $\mathit{lastbit}(z) = 0$

(if x is even, $\mathit{lastbit}(x) = 0, z = x, \mathit{lastbit}(z) = 0$, else $\mathit{lastbit}(x) = 1, z = x \oplus (k \parallel 1), \mathit{lastbit}(z) = 0$)

Since the function E is sPRF, we can get the input of E using $\mathit{droplastbit}(y)$ and $H(k)_1$. Of course the input of E is $\mathit{droplastbit}(x \oplus (k \parallel 1) \cdot \mathit{lastbit}(x)) = \mathit{droplastbit}(z)$. By simply appending 0-bit to $\mathit{droplastbit}(z)$, we can get z. And z is fed into t with key $H(k)_2$ to get 1 bit; $t_{H(k)_2}(z \oplus (k \parallel 1) \cdot \mathit{lastbit}(z)) = t_{H(k)_2}(z)$

This 1 bit is xored with $\mathit{lastbit}(y)$, we can get $\mathit{lastbit}(x)$;

$t_{H(k)_2}(z) \oplus \mathit{lastbit}(y) = t_{H(k)_2}(z) \oplus t_{H(k)_2}(z) \oplus \mathit{lastbit}(x) = \mathit{lastbit}(x)$

So we can finally compute x from $z = x \oplus (k \parallel 1) \cdot \mathit{lastbit}(x)$ and $\mathit{lastbit}(x)$. Thus this construction is injective and invertible.

The remaining part is to prove the construction is a sPRF and it is proved by lemma 4 in [19].

Lemma 4. *Construction 1 is a standard secure PRF for any quantum adversary $\mathcal{D}$ given classical access to BC_k and quantum access to the random oracle H.*

4.2 Attack on IGE mode of operation

We will use the block cipher BC as described in section 4.1 (Construction 1) for the Π_{IGE} scheme. As proved, this BC is sPRF, not qPRF. That is, the BC is secure under the condition that quantum adversary has only classical access to the BC. In this section, we will show the attack using Simon's algorithm to recover the key k.

Lemma 5. *There exists a standard-secure pseudo-random function such that Π_{IGE} is not IND-qCPA secure.(In the quantum random oracle model)*

Proof. Let the Π_{IGE} scheme use the block cipher BC. And we know that the quantum adversary can attack Π_{IGE} using the encryption queries on messages with two blocks. First, the quantum adversary stores random n-bit strings, n-zero strings(0^n) and equal superposition of messages in m_0, m_1 and m_2 blocks of register M, respectively. The quantum adversary initializes the quantum ciphertext register C with string $|0^{3n-1}\rangle|+\rangle$. Now the adversary can make encryption queries to the Π_{IGE} scheme and will get responses with the corresponding ciphertext in quantum register C. This attack is described in Figure 4.1

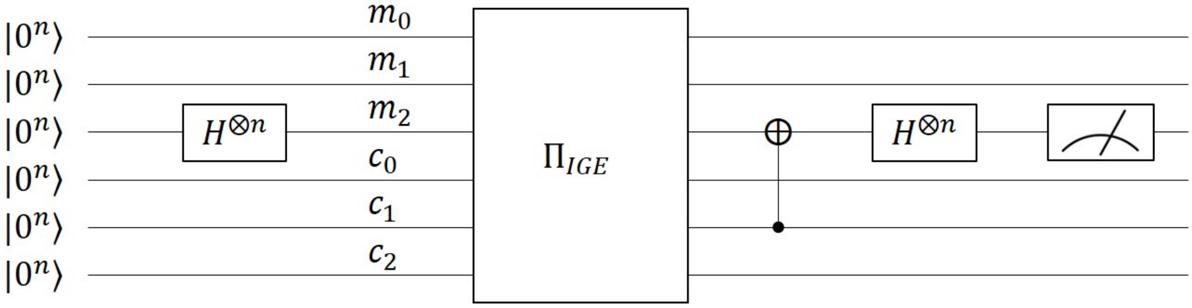


Figure 4.1: Attack on 1 block IGE using Simon's algorithm

After the quantum register M and C are applied encryption algorithm Enc of Π_{IGE}, the message and ciphertext registers becomes(up to normalization):

$|M, C\rangle = \sum_{m_2} |m_0\rangle|0^n \parallel m_2\rangle|c_0\rangle|BC_k(c_0) \oplus m_0\rangle|droplastbit\{BC_k(BC_k(c_0) \oplus m_0 \oplus m_2)\}\rangle|+\rangle$

Put $y := BC_k(c_0) \oplus m_0$, then we have :

$$\sum_{m_2} |m_0\rangle|0^n \parallel m_2\rangle|c_0\rangle|y\rangle|droplastbit\{BC_k(y \oplus m_2)\}\rangle|+\rangle$$

The quantum adversary now xors c_0 to the message register by using a CNOT gate(m_2 is xored with c_1). Then the quantum registers change:

$$\sum_{m_2} |m_0\rangle|0^n \parallel m_2 \oplus y\rangle|c_0\rangle|y\rangle|droplastbit\{BC_k(y \oplus m_2)\}\rangle|+\rangle \tag{4.2}$$

Also BC_k is $(k-1)$-periodic, we can use the property mentioned in Section 4.1 :

$$\mathrm{BC}_k(x) = \mathrm{BC}_k(x \oplus (k \parallel 1))$$

Then the quantum registers are :

$$\sum_{m_2} |m_0\rangle|0^n \parallel m_2 \oplus y\rangle|c_0\rangle|y\rangle|droplastbit\{BC_k(y \oplus m_2 \oplus (k \parallel 1))\}\rangle|+\rangle$$

We can modified above equation, we get :

$$\sum_{m_2} |m_0\rangle|0^n \parallel m_2 \oplus y \oplus (k \parallel 1)\rangle|c_0\rangle|y\rangle|droplastbit\{BC_k(y \oplus m_2)\}\rangle|+\rangle \tag{4.3}$$

Put $\gamma = m_2 \oplus y$, Eqs. (4.2) and (4.3) change Eqs. (4.4) and (4.5), respectively :

$$\sum_{\gamma} |m_0\rangle|0^n \parallel \gamma\rangle|c_0\rangle|y\rangle|droplastbit\{BC_k(\gamma)\}\rangle|+\rangle \tag{4.4}$$

$$\sum_{\gamma} |m_0\rangle|0^n \parallel \gamma \oplus (k \parallel 1)\rangle|c_0\rangle|y\rangle|droplastbit\{BC_k(\gamma)\}\rangle|+\rangle \tag{4.5}$$

Hence the adversary has the state(up to normalization),

$$\textstyle\sum_{\gamma} |m_0\rangle|0^n\rangle\big(|\gamma\rangle + |\gamma \oplus (k \parallel 1)\rangle\big)|c_0\rangle|y\rangle|droplastbit\{BC_k(\gamma)\}\rangle|+\rangle$$

Now the adversary applies n Hadamard gates to the third block of plaintext(m_2) and get the following state(up to normalization):

$$\textstyle\sum_{\gamma}\sum_{z}((-1)^{\gamma \odot z} + (-1)^{\{\gamma\oplus(k\|1)\}\odot z})|m_0\rangle|0^n\rangle|z\rangle|c_0\rangle|y\rangle|droplastbit\{BC_k(\gamma)\}\rangle|+\rangle$$

$$\textstyle= \sum_{\gamma}\sum_{z} (-1)^{\gamma\odot z}(1 + (-1)^{(k\|1)\odot z})|m_0\rangle|0^n\rangle|z\rangle|c_0\rangle|y\rangle|droplastbit\{BC_k(\gamma)\}\rangle|+\rangle$$

Now if the adversary measure n-bit of message register, result is two cases. One is that the adversary can get a vector z such that $(k \parallel 1) \odot z = 0$. The other is when the superposition collapses to 0, the adversary can get nothing. By doing this attack repeatedly until they can get n independent vectors $v_i's$. Remaining part is that using Gaussian elimination, then they can retrieve $n-1$ bit of k, thereby breaking the Π_{IGE} scheme.

□

Chapter 5. Post-quantum security of IGE mode using qPRF

5.1 Techniques

In the previous chapter, the IGE mode assuming sPRF can be broken by Simon's algorithm and even the adversary can retrieve the secret key. Thus using only the standard-secure PRF is weak in quantum setting. However, if only we use the quantum-secure PRF we can overcome this problem which we will show in this chapter. When proving the random property in cryptography, we usually use the hybrid-game method. One part of the cryptosystem which we want to prove randomness is changed with random one, and show this change is so small that we can ignore in the whole cryptosystem. By repeating this, we change original one step-by-step with randomness. Because the change is very small, the total change is also small. Thus we can prove that the cryptosystem is indistinguishable from truly random function.

When proving IND-qCPA security, the quantum adversary $\mathcal{A}$ has to distinguish between IGE mode block cipher and truly random function in the challenge queries. That means, the adversary $\mathcal{A}$ has to distinguish between $\mathsf{Enc}(m_0)$ and $\mathsf{Enc}(m_1)$ in challenge query of IND-qCPA;

First, the function that is used in block cipher is quantum secure PRF, we can substitute the PRF with truly random function H as shown in Figure 5.1.

Second, when the quantum adversary $\mathcal{A}$ makes challenge queries, we replace the ciphertext with random one one by one.

Last, we show replacing one block by randomness is negligible change, thus the quantum adversary $\mathcal{A}$ gains only negligible advantage.

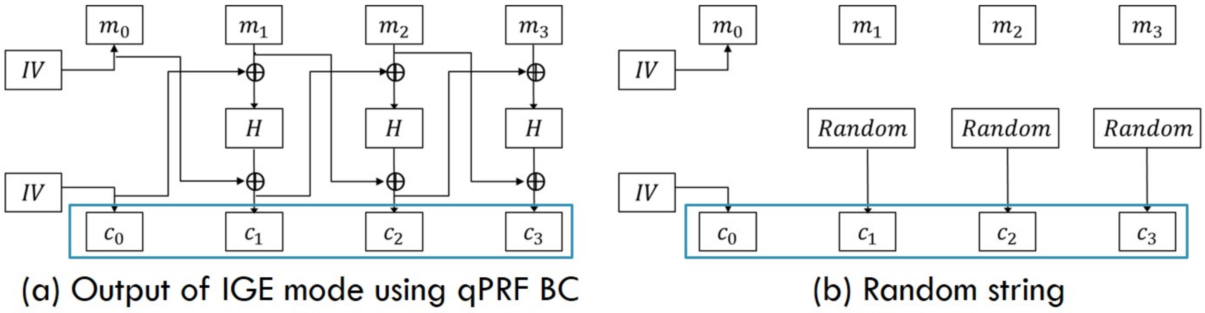


Figure 5.1: IGE mode using random function H

But the problem is that how we can show the last one, proving the difference is negligible. In IGE mode, we have to show that $c_2 = H(m_2 \oplus c_1) \oplus m_1$(when c_1 is random) is indistinguishable from randomly chosen c_2. In the classical setting, we can say that since c_1 is random, $m_2 \oplus c_1$ is also random. And because the probability that $m_2 \oplus c_1$ collides with other H-queries is negligible, the $H(m_2 \oplus c_1)$ is random, thus $H(m_2 \oplus c_1) \oplus m_1$ is random. However this is not in quantum setting. Because quantum adversary $\mathcal{A}$ queries in superposition, we can not say H was not queried before.

Instead, we use other method, One-way to Hidding(O2H) Lemma in Section 2.3. The O2H lemma show that to prove that $H(x)$ is indistinguishable from random given uniformly random x, we only need to show; when the adversary $\mathcal{A}$ performing queries to H, abort the query at random point and measure the input of that query, then the probability that the input of query equals x is negligible.

5.2 IND-qCPA security of IGE mode of operation

Define $\mathbf{Enc}^{i,H}_{IGE}(M) := c_0 c_1 \cdots c_n$, where $c_j \overset{\$}{\leftarrow} \{0,1\}^t$ for $j \leq i$ and $c_j = H(m_j \oplus c_{j-1}) \oplus m_{j-1}$ for $i < j \leq n$. We prove in the next lemma that for the quantum Adversary $\mathcal{A}$ who can access to oracle $\mathbf{Enc}^{i,H}_{IGE}$, the probability the adversary $\mathcal{A}$ distinguish the output of $\mathbf{Enc}^{i,H}_{IGE}$ from $\mathbf{Enc}^{i+1,H}_{IGE}$ is negligible in t, where t is the security parameter. For the sake of simplicity, we use $\mathbf{Enc}^{i,H}$ instead of $\mathbf{Enc}^{i,H}_{IGE}$.

Lemma 6. *For any i with i : $0 \leq i \leq p(t) - 1$, and every quantum adversary $\mathcal{A}$ that makes at most q_A queries,*
$\Big|\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \overset{\$}{\leftarrow} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\mathbf{Enc}^{i,H}(M_b))] - \mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \overset{\$}{\leftarrow} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\mathbf{Enc}^{i+1,H}(M_b))]\Big| \leq O(\frac{p(t)^3 {q_A}^3}{2^t})$
where $p(t)$ is the maximum number of blocks in the message M and t is the length of each message block.

Proof.

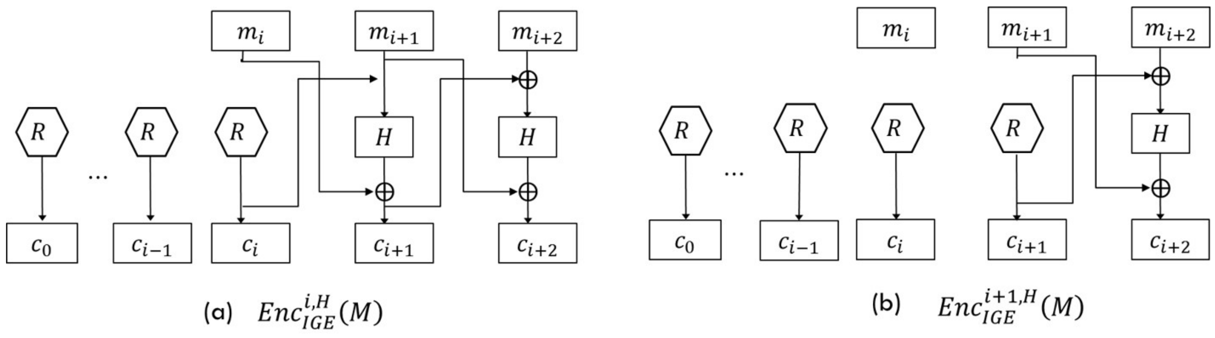
Put $\varepsilon(t) = \Big|\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \overset{\$}{\leftarrow} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\mathbf{Enc}^{i,H}(M_b))] - \mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \overset{\$}{\leftarrow} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\mathbf{Enc}^{i+1,H}(M_b))]\Big|$

For a given message $M = m_0 m_1 \cdots m_n$, let $\widetilde{\mathbf{Enc}}^{i}_{H}(M_b, c_0, \ldots, c_i) := \hat{c_1}\hat{c_2}\cdots\hat{c_n}$ where

$$\hat{c_j} = \begin{cases} c_j & 0 \leq j \leq i \\ H(\hat{c_{j-1}} \oplus m_j) \oplus m_{j-1} & i < j \leq n \end{cases}$$

Then we can substitute $\mathbf{Enc}^i_H$ with $\widetilde{\mathbf{Enc}}^i_H$,

$$\begin{aligned}\varepsilon(t) = \Big|&\mathbf{Pr}[b=b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}};\\ &c_0,\dots,c_i \xleftarrow{\$} \{0,1\}^t; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}^i_H(M_b,c_0,\dots,c_i))]-\\ &\mathbf{Pr}[b=b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}};\\ &c_0,\dots,c_{i+1} \xleftarrow{\$} \{0,1\}^t; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}^{i+1}_H(M_b,c_0,\dots,c_{i+1}))]\Big|\end{aligned} \tag{5.1}$$



(a) $Enc^{i,H}_{IGE}(M)$ (b) $Enc^{i+1,H}_{IGE}(M)$

Figure 5.2: Adversary has to distinguish outputs of (a) and (b) in Eq.(5.1).

In Figure 5.2, R represents randomly chosen value.

We put $c_i := x \oplus m_b^{i+1}, c_{i+1} := y \oplus m_b^i$ where m_b^i and m_b^{i+1} is the i^{th} and $(i+1)^{th}$ block of the message M_b, respectively and $x \xleftarrow{\$} \{0,1\}^t, y \xleftarrow{\$} \{0,1\}^t$. This means that c_i and c_{i+1} are uniformly random as x and y are randomly chosen. Therefore, we have

$$\begin{aligned}\varepsilon(t) = \Big|&\mathbf{Pr}[b=b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}};\\ &c_0,\dots,c_{i-1} \xleftarrow{\$} \{0,1\}^t, x \xleftarrow{\$} \{0,1\}^t, c_i := x \oplus m_b^{i+1}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}^i_H(M_b,c_0,\dots,c_i))]-\\ &\mathbf{Pr}[b=b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}};\\ &c_0,\dots,c_{i-1} \xleftarrow{\$} \{0,1\}^t; x \xleftarrow{\$} \{0,1\}^t, c_i := x \oplus m_b^{i+1}, y \xleftarrow{\$} \{0,1\}^t, c_{i+1} := y \oplus m_b^i,\\ &b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}^{i+1}_H(M_b,c_0,\dots,c_{i+1}))]\Big|\end{aligned} \tag{5.2}$$

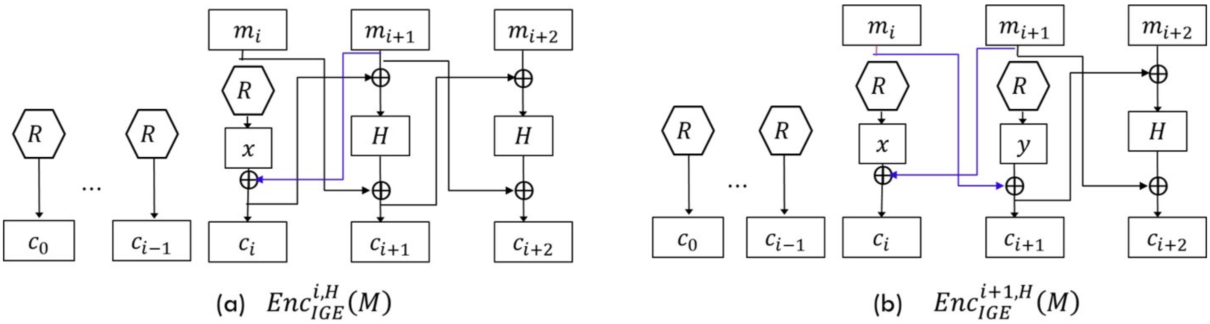


Figure 5.3: Adversary has to distinguish outputs of (a) and (b) in Eq.(5.2).

By definition of $\widetilde{\mathbf{Enc}}^{i}_{H}$, we have $\widetilde{\mathbf{Enc}}^{i}_{H}(M_b, c_0, \dots, c_i) = \widetilde{\mathbf{Enc}}^{i+1}_{H}(M_b, c_0, \dots, c_{i+1})$ with $c_{i+1} := H(x) \oplus m_b^i$. Hence,

$$
\begin{aligned}
\varepsilon(t) = \Big| &\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \to \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}};\\
&c_0, \dots, c_{i-1} \xleftarrow{\$} \{0,1\}^t, x \xleftarrow{\$} \{0,1\}^t, c_i := x \oplus m_b^{i+1}, c_{i+1} := H(x) \oplus m_b^i;\\
&b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}^{i+1}_{H}(M_b, c_0, \dots, c_{i+1}))] -\\
&\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \to \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}};\\
&c_0, \dots, c_{i-1} \xleftarrow{\$} \{0,1\}^t; x \xleftarrow{\$} \{0,1\}^t, c_i := x \oplus m_b^{i+1}, y \xleftarrow{\$} \{0,1\}^t, c_{i+1} := y \oplus m_b^i,\\
&b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}^{i+1}_{H}(M_b, c_0, \dots, c_{i+1}))]\Big|
\end{aligned}
\tag{5.3}
$$

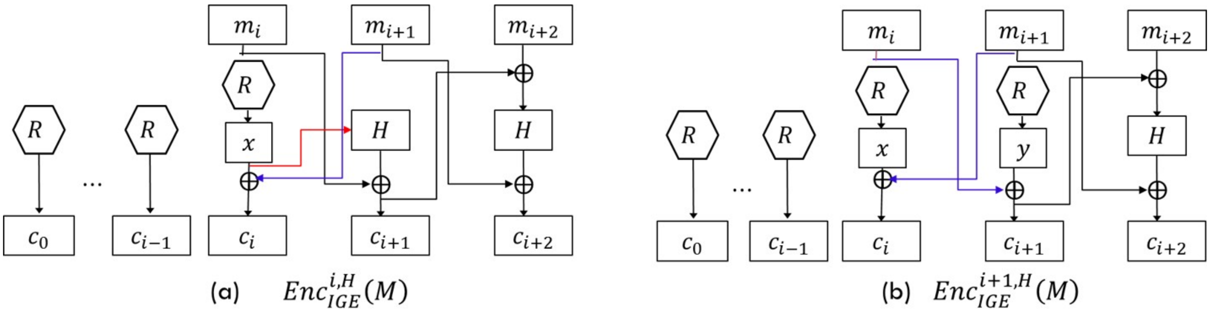


Figure 5.4: Adversary has to distinguish outputs of (a) and (b) in Eq.(5.3).

Now, the difference between two probabilities is that $c_{i+1} = H(x) \oplus m_b^i$ in the former but $c_{i+1} = y \oplus m_b^i$ in the latter. In other words, the difference is c_{i+1} is whether $H(x)$ or uniformly random value y. Thus we can use the O2H lemma. We define an adversary A_{O2H} that makes oracle queries to random function $H \xleftarrow{\$} (\{0,1\}^t \to \{0,1\}^t)$ with given input x and y does the following:

```
$\underline{Adversary A^{H}_{O2H}(x,y)}$ :
$M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}$
$b \xleftarrow{\$} \{0,1\}$
$c_0, \ldots, c_{i-1} \xleftarrow{\$} \{0,1\}^t; c_i = x \oplus m_b^{i+1}; c_{i+1} = y \oplus m_b^i;$
compute $C := \widetilde{\mathbf{Enc}}_H^{i+1}(M_b, c_0, \ldots, c_{i+1})$
$b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(C)$
return $b' = b$
```

Because the A_{O2H} can query to H, A_{O2H} also can answer the adversary $\mathcal{A}$'s query. Let q be the number that A_{O2H} query, then $q \leq 3p(t) \cdot q_A$. Also, let q_1, q_2 and q_3 be the number that A_{O2H} makes queries to random function H before the challenge query, during challenge query and after challenge query, respectively. Then we can get another equation as below from Eq.(5.3).

$$\begin{aligned} \varepsilon(t) = \Big| &\mathbf{Pr}[\tilde{b} = 1 : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), x \xleftarrow{\$} \{0,1\}^t, \tilde{b} \leftarrow A^H_{O2H}(x, H(x))] - \\ &\mathbf{Pr}[\tilde{b} = 1 : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), x \xleftarrow{\$} \{0,1\}^t, y \xleftarrow{\$} \{0,1\}^t, \tilde{b} \leftarrow A^H_{O2H}(x, y)]\Big| \end{aligned} \tag{5.4}$$

Let B be an oracle algorithm described in the O2H Lemma, then we have $\varepsilon(t) \leq 2q\sqrt{P_B}$ with P_B as below:

$$\begin{aligned} P_B &= \mathbf{Pr}[x = x' : j \xleftarrow{\$} \{1, \ldots, q\}, x \xleftarrow{\$} \{0,1\}^t, H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), x' \leftarrow B^H(x, j)] \\ &= \frac{1}{q} \cdot \mathbf{Pr}[x = x' : x \xleftarrow{\$} \{0,1\}^t, H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), x' \leftarrow B^H(x, j)] = \frac{1}{q} \cdot P_B^j \end{aligned}$$

P_B^j is different depending on when the j-th queries to H is done(before, during, or after challenge query).

- **Case 1 :** $j \leq q_1$

  The j-th iteration query to the random oracle H is done before the challenge query. Because the quantum Adversary $\mathcal{A}$ can not access to x during queries, the adversary $\mathcal{A}$'s queries are independent of x. Thus we can fix x to any string because it does not affect argument of the query. Therefore, we fix input x as the null string 0^n.

$$P_B^j = \mathbf{Pr}[x = x' : x \xleftarrow{\$} \{0,1\}^t, H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), x' \leftarrow B^H(0, j)] \leq 2^{-t}$$

- **Case 2 :** $q_1 \leq j \leq q_1 + q_2$

  The j-th iteration query to the random oracle H is computed during the challenge query. Therefore algorithm B can cease adversary $\mathcal{A}$ at any queries:

$$H(m_b^{i+2} \oplus y) \oplus m_b^{i+1}, H(m_b^{i+3} \oplus H(m_b^{i+2} \oplus y) \oplus m_b^{i+1}) \oplus m_b^{i+2}, \cdots ,$$

$$H(m_b^{p(t)} \oplus H(m_b^{p(t)-1} \oplus \cdots H(m_b^{i+2} \oplus y) \oplus m_b^{i+1}) \cdots \oplus m_b^{p(t)-2}) \oplus m_b^{p(t)-1}$$

We use the fact that H is indistinguishable from a random permutation[25]. By using this we have,

$$P_B^j = \mathbf{Pr}[x = x' : x \xleftarrow{\$} \{0,1\}^t, H \xleftarrow{\$} \mathsf{Perm}(), x' \leftarrow B^H(x,j)] + O(\frac{j^3}{2^t})$$

Note that the argument of the j-th iteration query is

$$s := H(m_b^{i+j-q_1+1} \oplus H(m_b^{i+j-q_1} \oplus \cdots H(m_b^{i+2} \oplus y) \oplus m_b^{i+1}) \cdots \oplus m_b^{i+j-q_1-1}) \oplus m_b^{i+j-q_1}$$

As explained in the definition of O2H lemma we know that y is random and y is independent from x and H. And for a fixed message M_b, j-th query s is assigned an output by permutation and it is independent of x but dependent on y, because the input to first call to H is $m_b^{i+2} \oplus y$. Therefore,

$$P_B^j = \mathbf{Pr}[x = x' : x \xleftarrow{\$} \{0,1\}^t, H \xleftarrow{\$} \mathsf{Perm}(), x' = s] + O(\frac{j^3}{2^t}) \leq \frac{1}{2^t} + O(\frac{j^3}{2^t}) \approx O(\frac{j^3}{2^t})$$

- **Case 3 :** $q_1 + q_2 \leq j$

  In this case, the j-th iteration query to the oracle H is done after the challenge query is done. Adversary $\mathcal{A}$, after making some encryption oracle queries, measures the argument of one of the H oracle query and then stops. Assume it measures the argument of the $k^{th} H$ oracle query in j-th encryption query.

$$P_B^j = \mathbf{Pr}[x = x' : x \xleftarrow{\$} \{0,1\}^t, H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), x' \leftarrow B^H(x,j)]$$

Composition of encryption oracle is depicted in Figure 5.5. This circuit diagram represents A_{O2H}'s working. A_{O2H} can answers encryption queries because it has the oracle access to H. Let the quantum message and the corresponding ciphertext are stored in the quantum register M and C, respectively. The encryption circuit consist of the unitary gates $U_{IV}, U_H, CNOT$ and measurements;

$$U_{IV}|M\rangle = |M \oplus IV\rangle, U_H|M, C\rangle = |M, C \oplus H(M)\rangle, CNOT|M, C\rangle = |M, C \oplus M\rangle$$

and the measurements are in the computational basis of the message space.

Measuring can all registers can commutes with other unitary operations performed during encryption, because the unitary gates are diagonal in the computational basis. Hence, we can measure the message register M

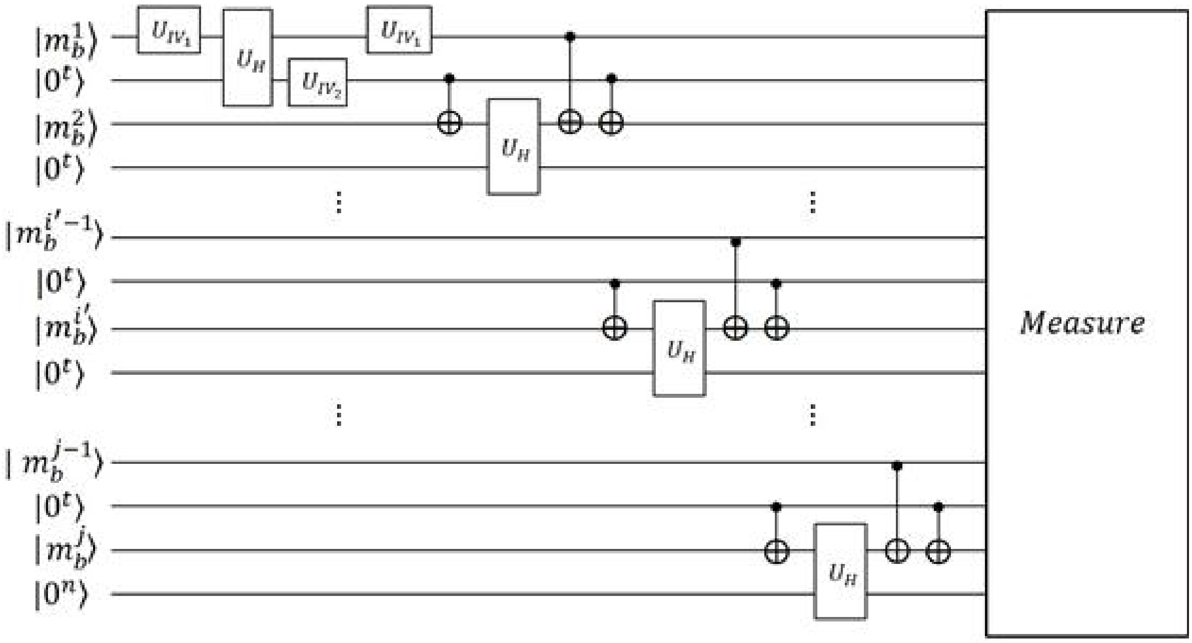


Figure 5.5: Composition of Encryption Oracle using H oracle.

at the beginning of the encryption(before performing the unitary operations). Thus, it is similar to the case when we query on a classical message, Case 2. Therefore, we have $P_B^j = O(\frac{j^3}{2^t})$.

Altogether(case 1,2 and 3), we have $P_B^j \in O(\frac{q^3}{2^t})$. Hence we have, $P_B \leq O(\frac{q^3}{2^t})$ by the definition of P_B. Because the probability of collision in measure is negligible, O2H lemma implies that $\mathbf{Enc}_{IGE}^{i,H}$ is indistinguishable from $\mathbf{Enc}_{IGE}^{i+1,H}$. Therefore, we have :

$$\epsilon(t) \leq q\sqrt{P_B} \leq q\sqrt{O(\frac{q^3}{2^t})} = O(\frac{q^3}{2^t})$$

□

The lemma 6 using O2H lemma show that the quantum adversary $\mathcal{A}$ only get negligible advantage when replacing one block with randomness. And by iterating this, we can replace the whole challenge ciphertext by randomness. And then the adversary has only $\frac{1}{2}$ probability of guessing which challenge plaintext was encrypted in IND-qCPA as proved in below theorem.

Theorem 7. *If the function E is a quantum-secure PRF then Π_{IGE} is IND-qCPA secure.*

Proof.

For any efficient quantum adversary $\mathcal{A}$ making q_A encryption queries to H, the advantage of adversary is calculated using Lemma 6 and triangle inequality;

$$\Big|\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}(\mathbf{Enc}^{0,H}(M_b))]$$

$$-\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}(\mathbf{Enc}^{p(t),H}(M_b))]\Big|$$

$$\leq nO(\tfrac{p(t)^3 {q_A}^3}{2^t})$$

Note that $\mathsf{Enc}^{p(t),H}(M_b)$ outputs completely random string. Hence, the output b' by adversary is independent of b. Therefore,

$$\Big|\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}(\mathbf{Enc}^{0,H}(M_b))] - \frac{1}{2}\Big|$$

$$\leq p(t) \cdot O(\tfrac{p(t)^3 {q_A}^3}{2^t})$$

One can see that $\mathsf{Enc}^{0,H}$ is indistinguishable from Enc function of Π by definition of qPRF. Thus we could replace $\mathsf{Enc}^{0,H}$ by Enc function of scheme Π_{IGE}. Therefore,

$$\Big|\mathbf{Pr}[PrivK^{qCPA}_{\mathcal{A},\Pi_{IGE}}(t) = 1] - \frac{1}{2}\Big| \leq O(\tfrac{p(t)^3 {q_A}^3}{2^t}) + negl(t).$$

Since q_A is polynomial in t, we deduce;

$$\Big|\mathbf{Pr}[PrivK^{qCPA}_{\mathcal{A},\Pi_{IGE}}(t) = 1] - \frac{1}{2}\Big| \leq negl(t).$$

□

Chapter 6. Concluding Remark

This thesis validate the IGE mode of block cipher from quantum adversaries. IGE mode is used in secret chat of Telegram which in very popular IM services. Telegram provide secret chat for protecting personal message and the security of secret chat is claimed to be secure. However this block cipher also need to be verified for security against the quantum computers. Quantum computers can perform quantum computation using quantum-mechanics happened in quantum states like superposition and entanglement different to the classical computers. Since modern cryptosystem can be broken within polynomial time by quantum computers, every cryptosystem need to be evaluated for their security against quantum adversary.

Quantum security of the IGE mode in block cipher against the quantum adversary $\mathcal{A}$ are different depending on the function in the block cipher. When assuming sPRF, the IGE mode block cipher does not satisfy IND-qCPA. But assuming qPRF, the IGE mode block cipher is proven to be IND-qCPA. When we assume the sPRF, especially periodic, we even can recover the secret key k in polynomial time using Simon's algorithm. By making query to oracle, we can get easily information about the secret key. Assuming qPRF, however, the block cipher of IGE mode is proven secure thus the quantum adversary $\mathcal{A}$ can not distinguish the block cipher from truly random function efficiently.

Furthermore, future research is still remaining. Firstly, other modes of operations except IGE mode need to be evaluated their security against quantum adversaries. Secondly the attack used for proving the IND-qCPA assuming sPRF should be implemented when the quantum computers are developed. Lastly, the countermeasure against this attack need to be devised.

Bibliography

[1] "Secret chats, end-to-end encryption." https://core.telegram.org/api/end-to-end.

[2] J. B. Jakobsen and C. Orlandi, *A practical cryptanalysis of the Telegram messaging protocol*. PhD thesis, Master Thesis, Aarhus University (Available on request), 2015.

[3] "Secure messaging scorecard." https://www.eff.org/node/82654, 2014.

[4] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," 2002.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[6] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, ACM, 1996.

[7] C. Campbell, "Design and specification of cryptographic capabilities," *IEEE Communications Society Magazine*, vol. 16, no. 6, pp. 15–19, 1978.

[8] *Recommendation for block cipher modes of operation. methods and techniques*. National Institute of Standards and Technology(NIST), 2001. Special Publication 800-38A.

[9] D. Boneh and M. Zhandry, "Secure signatures and chosen ciphertext security in a quantum computing world," in *Advances in Cryptology–CRYPTO 2013*, pp. 361–379, Springer, 2013.

[10] M. Zhandry, "How to construct quantum random functions," in *Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on*, pp. 679–687, IEEE, 2012.

[11] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," *Advances in Cryptology—ASIACRYPT 2000*, pp. 531–545, 2000.

[12] M. Bellare and P. Rogaway, "Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 317–330, Springer, 2000.

[13] J. H. An and M. Bellare, “Does encryption with redundancy provide authenticity?,” in *Eurocrypt*, vol. 2045, pp. 512–528, Springer, 2001.

[14] H. Kim and K. Kim, “Who can survive in caesar competition at round-zero,” in *The 31th Symposium on Cryptography and Information Security Kagoshima, Japan*, pp. 21–24, 2014.

[15] D. R. Simon, “On the power of quantum computation,” *SIAM journal on computing*, vol. 26, no. 5, pp. 1474–1483, 1997.

[16] D. Unruh, “Revocable quantum timed-release encryption,” *Journal of the ACM (JACM)*, vol. 62, no. 6, p. 49, 2015.

[17] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry, “Random oracles in a quantum world.,” in *Asiacrypt*, vol. 7073, pp. 41–69, Springer, 2011.

[18] M. Zhandry, “Secure identity-based encryption in the quantum random oracle model,” *International Journal of Quantum Information*, vol. 13, no. 04, p. 1550014, 2015.

[19] 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,” in *International Workshop on Post-Quantum Cryptography*, pp. 44–63, Springer, 2016.

[20] D. Boneh and M. Zhandry, “Quantum-secure message authentication codes,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 592–608, Springer, 2013.

[21] M. Burns, “Encrypted messaging app telegram hits 100m monthly active users, 350k new users each day,” *TechCrunch*, Feb. 2016.

[22] “Signal protocol.” `https://whispersystems.org`, 2014.

[23] K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, “A formal security analysis of the signal messaging protocol.,” *IACR Cryptology ePrint Archive*, vol. 2016, p. 1013, 2016.

[24] J. Jakobsen and C. Orlandi, “On the cca (in) security of mtproto,” in *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*, pp. 113–116, ACM, 2016.

[25] M. Zhandry, “A note on the quantum collision and set equality problems,” *arXiv preprint arXiv:1312.1027*, 2013.

Acknowledgments in Korean

이 논문을 작성하기위해 많은 분들의 도움을 받았습니다. 먼저 부족한 저를 잘 이끌어주시고 많은 지식뿐만아니라 인생의 지혜도 알려주시며 항상 저를 믿어주신 김광조 교수님께 감사드립니다. 또한 바쁘신 와중에도 저의 학위논문심사에 참여하셔서 진심어린 조언을 해주신 이주영 교수님과 김동준 교수님께도 감사의 말씀을 드립니다.

그리고 졸업이 다되가서야 반말을 하게된 연구실 친구이자 랩장 최락용, 마지막까지 함께 연구하며 큰 도움을 준 안형철, 양자암호에 대해 많이 알려준 친동생처럼 편하고 착한 이지은, 밤늦게까지 연구실에 같이 있어준 하루살이 동생들 최낙준,한성호, 뒷자리와 옆자리에서 항상 자리를 지켜준 Edwin, Aminanto Erza Muhamad and Harry Chandra, 행정적인 도움을 준 홍지연씨 모두 감사합니다.

또한, 군인으로 학업에 임하며 어려움이 있을때 든든한 멘토가 되어주신 권오정교수님, 카이스트 군위탁생 선후배님들, 외롭지 않게 함께해준 동기 송희진, 김수련에게도 감사의 말씀을 전합니다.

끝으로, 언제나 든든하게 응원해준 부모님, 시부모님, 사랑하는 남편, 루아, 루비에게도 깊은 감사를 드립니다. 앞으로 더 나아진 모습으로 보답하겠습니다. 감사합니다.

Curriculum Vitae in Korean

이름: 김성숙

생년월일: 1989년 2월 23일

전자주소: kusino@kaist.ac.kr

학력

2004. 3. – 2007. 2.	경주여자고등학교
2007. 2. – 2011. 2.	육군사관학교 운영분석학과 (학사)
2016. 3. – 2018. 2.	한국과학기술원 전산학부 (석사)

경력

2011. 3. – 현재	대한민국 육군

연구업적

1. 이지은, **김성숙**, 김광조, "Is Quantum State in BB84 Protocol Really Unclonable?", 한국정보보호학회 하계학술대회(CISC-S'16), 2016.06.23. 국립부경대학교, 부산.

2. Hyeongcheol An, **Sungsook Kim**, Jeeun Lee, Rakyong Choi, and Kwangjo Kim, "Timing and Fault Attacks on Lattice-based Cryptographic Libraries", 2017 Symposium on Cryptography and Information Security, Session 2B3-6 (SCIS 2017), Jan., 24-27, 2017, Naha, Japan.

3. Jeeun Lee, Rakyong Choi, **Sungsook Kim**, and Kwangjo Kim, "Security Analysis of End-to-End Encryption in Telegram", 2017 Symposium on Cryptography and Information Security, Session 3D4-1 (SCIS 2017), Jan., 24-27, 2017, Naha, Japan.

4. 최락용, 안형철, 이지은, **김성숙**, 김광조, "양자 컴퓨터 공격에 안전한 격자 기반 키 교환 방식 비교", 한국통신학회논문지, 제42권, 제11호, pp.2200-2207. 2017.11.30.

5. **김성숙**, 이지은, 김광조, ”IGE 모드의 양자 안전성”, 한국정보보호학회 동계학술대회(CISC-W’17), 2017.12.9. 고려대학교, 서울.

6. **Sungsook Kim**, Jeeun Lee, Rakyong Choi, and Kwangjo Kim, ”Validating IGE Mode of Block Cipher from Quantum Adversaries, 2018 Symposium on Cryptography and Information Security, (SCIS 2018), Jan., 23-26, 2018, Niigata, Japan.