SCIS 2018 2018 Symposium on
Cryptography and Information Security
Niigata, Japan, Jan. 23 - 26, 2018
The Institute of Electronics,
Information and Communication Engineers

Validating IGE Mode of Block Cipher from Quantum Adversaries

Sungsook Kim [*] Jeeun Lee[*] Rakyong Choi[*] Kwangjo Kim[*]

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

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 [1]. 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 very popular and widely used for secure applications. The computational security of public key cryptosystem based on the difficulty of the number theory relies on mathematical hard problems such as the integer factorization problem(IFP), the discrete logarithm problem(DLP), and the elliptic-curve discrete logarithm problem(ECDLP). However these problems can be solved within polynomial time using a powerful quantum computer by Shor's algorithm [2]. 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 [3] can find the correct member given unstructured database in complexity $O(\sqrt{N})$ compared to $O(N)$ in classical world. The suggested countermeasure against quantum computer attack needs to double the key size; use 256 bit key instead of 128 bit key in AES.

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, uses Infinite Garble Extension(IGE) [4] mode in their customized protocol called MTProto. IGE mode is not classified as standard mode of operation by National Institute of Standards and Technology(NIST) [5]. However, this Telegram is claimed to be secure even though they use IGE mode. Even Telegram got great score by Electronic Frontier Foundation(EFF) in 2014 [6] by evaluating the security requirements among secure IM's. Different to other IM's, Telegram has special policy to 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 sufficiently 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-

[*] School of Computing, KAIST. 291, Daehak-ro, Yuseong-gu, Daejeon, South Korea 34141. $\{kusino, jeeun.lee, thepride, kkj\}$@kaist.ac.kr)

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

2 Preliminaries

2.1 Notation

$y \leftarrow A(x)$ means an algorithm A that takes the input x outputs a value and this value is assigned to y. We write A^H when A can access to an oracle H. $(A \leftarrow B)$ denotes 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 $x = x_1 x_2 x_3 \cdots x_n$ where x_i is the $i\text{-}th$ bit, we use function $lastbit(x) = (x_n)$, $droplastbit(x) = x_1 x_2 x_3 \cdots x_{n-1}$.

2.2 Quantum Computation

A quantum system A is a complex Hilbert space $\mathcal{H}$ with 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 b_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

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

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.

2.3 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 [7]. 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 [7]). *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* $k \xleftarrow{\$}$ *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:*

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

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

2.4 Standard and quantum security

Definition 3 (Standard-secure PRF [8]). *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 [8]). *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.*

2.5 One way to hiding(O2H) Lemma

This lemma below is devised from Unruh in 2015 [9]. This lemma shows that given a uniformly random value s, to show that $H(x)$ is also uniformly random (indistinguishable from random) we need to show that : 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 Section 5.2 to set up the boundary of probability.

Lemma 1 (One way to hiding(O2H) Lemma [9]). *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 ith 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,

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

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 [10]. 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't read original messages and the messages is not stored in the middle. 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 [4] mode.

3.2 Infinite Garble ExtensionIGE mode

IGE [4] 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.

Definition 5 (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 $k \xleftarrow{\$} K$.

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

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* $0 < i \le n$.

When encrypt the message m_0, 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 a random value like definition 5. But we just take the latter without loss of generality.

3.3 Security of Telegram

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

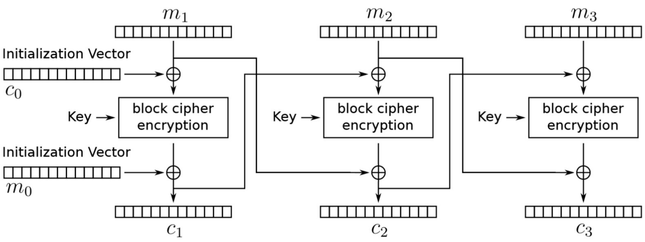


Figure 1: Diagram of IGE mode for encryption. [11]

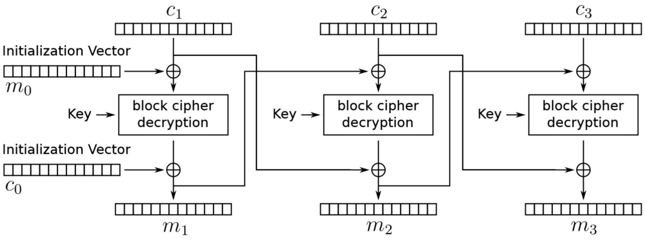
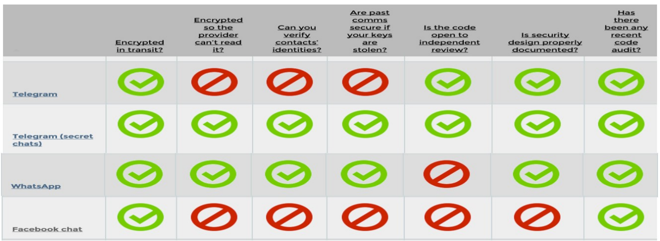


Figure 2: Diagram of IGE mode for decryption. [11]

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.

Meanwhile, Telegram's MTProto has been criticized until now and Jakobsen *et al.* [11, 12] 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.



	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: Secure messaging scorecard. [6]

Also, Electronic Frontier Foundation(EFF) announced "Secure Messaging Scorecard" [6] in 2014 depicted in Figure 3, and Telegram got 4 out of 7 in cloud chat and 7 out of 7 in secret chat whereas Facebook chat got only 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.

4 Insecurity of IGE mode assuming sPRF BC

4.1 Standard-secure PRF

For the first step to construct a sPRF, Anand *et al.* [13] construct a specific block cipher as follows:

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

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 $n-1$ bit in both cases. But we will use some trick to change this incomplete construction to complete block cipher explained later in the second step.)

This block cipher has the special property, which is important in next section, $(k \parallel 1)$-periodic:

- **Case 1 :**
  x is even, $lastbit(x) = 0, lastbit(x \oplus (k \parallel 1)) = 1$, $\mathrm{BC}_k(x \oplus (k \parallel 1)) = E_{H(k)}(droplastbit(x \oplus (k \parallel 1) \oplus (k \parallel 1))) = E_{H(k)}(droplastbit(x))$ $= E_{H(k)}(droplastbit(x \oplus (k \parallel 1) \cdot lastbit(x))) =$ $\mathrm{BC}_k(x)$

- **Case 2 :**
  x is odd, $lastbit(x) = 1, lastbit(x \oplus (k \parallel 1)) = 0$, $\mathrm{BC}_k(x \oplus (k \parallel 1)) = E_{H(k)}(droplastbit(x \oplus (k \parallel 1))) = E_{H(k)}(droplastbit(x \oplus (k \parallel 1) \cdot lastbit(x))) =$ $\mathrm{BC}_k(x)$

Thus we can use this property:

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

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:
$\mathrm{BC}_k(x) := E_{H(k)_1}(droplastbit(x \oplus (k \parallel 1) \cdot lastbit(x)))$ $\parallel t_{H(k)_2}(x \oplus (k \parallel 1) \cdot lastbit(x)) \oplus lastbit(x)$
where $E : \{0,1\}^{n-1} \times \{0,1\}^{n-1} \to \{0,1\}^{n-1}$ is a sPRF, $t : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is a sPRF, $H : \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$ is a random oracle, and the key $k \xleftarrow{\$} \{0,1\}^{n-1}$

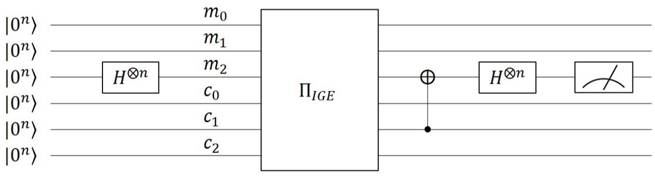


Figure 4: Attack on 1 block IGE using Simon's algorithm

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

$z := x \oplus (k \parallel 1) \cdot lastbit(x)$, then $lastbit(z) = 0$

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

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

$t_{H(k)_2}(z \oplus (k \parallel 1) \cdot lastbit(z)) = t_{H(k)_2}(z)$

This 1 bit is xored with $lastbit(y)$, we can get $lastbit(x)$:

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

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

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

The remaining part is to prove the construction is a sPRF and it is proved in [13]

4.2 Attack on IGE Mode using Quantum Circuit

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 2. *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.

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

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

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

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

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:

$$\sum_{m_2} |m_0\rangle|0^n \parallel m_2 \oplus y\rangle|c_0\rangle|y\rangle$$
$$|droplastbit\{BC_k(y \oplus m_2)\}\rangle|+\rangle \tag{2}$$

Also BC_k is $(k \parallel 1)$-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 :

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

We can modified above equation, we get :

$$= \sum_{m_2} |m_0\rangle|0^n \parallel m_2 \oplus y \oplus (k \parallel 1)\rangle|c_0\rangle|y\rangle$$
$$|droplastbit\{BC_k(y \oplus m_2)\}\rangle|+\rangle \tag{3}$$

Put $\gamma = m_2 \oplus y$ in Eqs. (2) and (3) change Eqs. (4) and (5) respectively :

$$\sum_{\gamma} |m_0\rangle|0^n \parallel \gamma\rangle|c_0\rangle|y\rangle|droplastbit\{BC_k(\gamma)\}\rangle|+\rangle \tag{4}$$

$$\sum_{\gamma} |m_0\rangle|0^n \parallel \gamma \oplus (k \parallel 1)\rangle|c_0\rangle|y\rangle|droplastbit\{BC_k(\gamma)\}\rangle|+\rangle \tag{5}$$

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

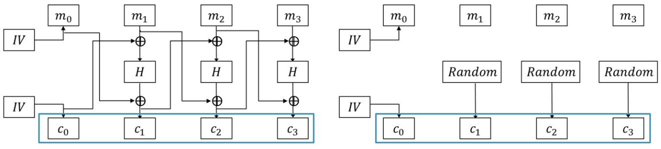
$$\textstyle\sum_{\gamma} |m_0\rangle|0^n\rangle\big(|\gamma\rangle + |\gamma \oplus (k \parallel 1)\rangle\big)$$
$$|c_0\rangle|y\rangle|droplastbit\{BC_k(\gamma)\}\rangle|+\rangle$$

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

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

Now if the adversary measures 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 $(k \parallel 1) \odot z = 1$, the superposition collapses to 0 thus the adversary can get nothing. By doing this attack repeatedly, adversary can get n independent vectors $v_i's$. Remaining part is that using the Gaussian elimination, adversary can retrieve $n-1$ bits of k, thereby breaks the Π_{IGE} scheme.

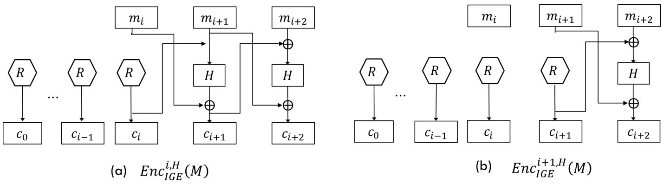
□



(a) Output of IGE mode using qPRF BC

(b) Random string

Figure 5: IGE mode using random function H



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

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

Figure 6: Adversary has to distinguish outputs of (a) and (b) in Eq.(6). R represents randomly chosen value.

5 Security of IGE mode assuming qPRF BC

5.1 Techniques

In the previous section, the IGE mode assuming sPRF can be broken by Simon's algorithm and even the adversary can retrieve the secret key. Thus assuming only the sPRF is weak in quantum setting. However, if we use the qPRF we can overcome this problem which will be described in this section. When proving the random property in cryptography, we usually use the hybrid-game method. That is the one part of the cryptosystem that 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 $\mathsf{Enc}(m_1)$:

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.

Second, when the quantum adversary $\mathcal{A}$ makes challenge queries, we replace the ciphertext with random one one by one. Last, we show the difference is negligible, thus the quantum adversary $\mathcal{A}$ gains only negligible advantage.

But the problem is that how we can show the last one, proving the difference is negligible. For example, we have to show that $c_2 = H(m_2 \oplus c_1) \oplus m_1 (c_1$ 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, the probability that $m_2 \oplus c_1$ collides with other H-queries is negligible, so $H(m_2 \oplus c_1)$ is random, the $H(m_2 \oplus c_1) \oplus m_1$ is random. However this is not in quantum setting; The quantum adversary $\mathcal{A}$ queries in superposition, we can not say H was not queried before. Instead, we use other method, One-way to Hiding(O2H) Lemma mentioned in Section 2.5.

5.2 IND-qCPA security of IGE mode

Define $\mathbf{Enc}^{i,H}_{IGE}(M) := c_0 c_1 \cdots c_n$, where $c_j \xleftarrow{\$} \{0,1\}^t$ for $j \leq i$ and $c_j = H(m_j \oplus c_{j-1}) \oplus m_{j-1}$ for $i < j \leq n$. We want to prove using O2H lemma that for the quantum Adversary $\mathcal{A}$ who can access to oracle $\mathbf{Enc}^{i,H}_{IGE}$, the probability the $\mathcal{A}$ 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 3. *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,*

$$\Big|\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\mathbf{Enc}^{i,H}(M_b))] - \mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\mathbf{Enc}^{i+1,H}(M_b))]\Big| \leq O(\frac{p(t)^3 {q_A}^3}{2^t})$$

where $p(t)$ is the maximum number of blocks in the message M and t is the length of each message block.

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

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

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

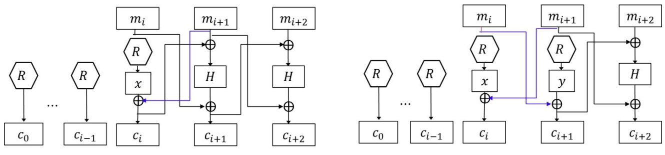
Then we have,

$$\begin{aligned} \varepsilon(t) = \Big|&\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; \\ &M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; c_0, \ldots, c_i \xleftarrow{\$} \{0,1\}^t; \\ &b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}^{i}_{H}(M_b, c_0, \ldots, c_i))] - \\ &\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\}; \\ &M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; c_0, \ldots, c_{i+1} \xleftarrow{\$} \{0,1\}^t; \\ &b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}^{i+1}_{H}(M_b, c_0, \ldots, c_{i+1}))]\Big| \end{aligned} \tag{6}$$

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

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

$$
\begin{aligned}
&\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \to \{0,1\}^t), b \xleftarrow{\$} \{0,1\};\\
&M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; c_0, \dots, c_{i-1} \xleftarrow{\$} \{0,1\}^t;\\
&x \xleftarrow{\$} \{0,1\}^t, c_i := x \oplus m_b^{i+1},\\
&y \xleftarrow{\$} \{0,1\}^t, c_{i+1} := y \oplus m_b^{i},\\
&b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}_H^{i+1}(M_b, c_0, \dots, c_{i+1}))]\Big|
\end{aligned} \tag{7}
$$

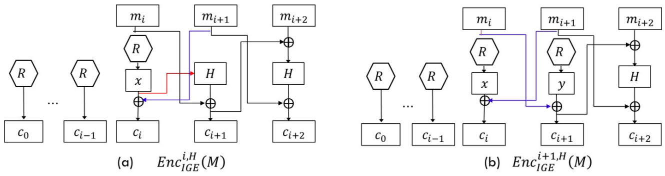


(a) $Enc^{i,H}_{IGE}(M)$ (b) $Enc^{i+1,H}_{IGE}(M)$

Figure 7: Adversary has to distinguish outputs of (a) and (b) in Eq.(7)

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,

$$
\begin{aligned}
\varepsilon(t) = \Big|&\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \to \{0,1\}^t), b \xleftarrow{\$} \{0,1\};\\
&M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; c_0, \dots, c_{i-1} \xleftarrow{\$} \{0,1\}^t,\\
&x \xleftarrow{\$} \{0,1\}^t, c_i := x \oplus m_b^{i+1}, c_{i+1} := H(x) \oplus m_b^i;\\
&b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}_H^{i+1}(M_b, c_0, \dots, c_{i+1}))] -\\
&\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \to \{0,1\}^t), b \xleftarrow{\$} \{0,1\};\\
&M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}; c_0, \dots, c_{i-1} \xleftarrow{\$} \{0,1\}^t;\\
&x \xleftarrow{\$} \{0,1\}^t, c_i := x \oplus m_b^{i+1}, y \xleftarrow{\$} \{0,1\}^t,\\
&c_{i+1} := y \oplus m_b^{i},\\
&b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(\widetilde{\mathbf{Enc}}_H^{i+1}(M_b, c_0, \dots, c_{i+1}))]\Big|
\end{aligned} \tag{8}
$$



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

Figure 8: Adversary has to distinguish outputs of (a) and (b) in Eq.(8).

Now, the difference is when c_{i+1} is $H(x)$ or uniformly random value y, and we can use the O2H lemma. We define an adversary A_{O2H} that makes oracle queries to random function $H \leftarrow (\{0,1\}^t \to \{0,1\}^t)$ with given input x and y does the following:

```
Adversary $A^H_{O2H}(x, y)$ :
$M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}, b \xleftarrow{\$} \{0,1\}$
$c_0, \dots, c_{i-1} \xleftarrow{\$} \{0,1\}^t; c_i = x \oplus m_b^{i+1};$
$c_{i+1} = y \oplus m_b^i;$
compute $C := \widetilde{\mathbf{Enc}}^{i+1}_H(M_b, c_0, \dots, c_{i+1})$
$b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{i,H}}(C)$
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 a number that A_{O2H} query, then $q \leq p(t)q_A$. Also, let q_1, q_2, q_3 be a number that A_{O2H} query before the challenge query, during challenge query and after challenge query, respectively. Then we can get another equation below from Eq. (8).

$$
\begin{aligned}
\varepsilon(t) = \Big|&\mathbf{Pr}[\tilde{b} = 1 : H \leftarrow (\{0,1\}^t \to \{0,1\}^t), x \xleftarrow{\$} \{0,1\}^t,\\
&\tilde{b} \leftarrow A^H_{O2H}(x, H(x)] -\\
&\mathbf{Pr}[\tilde{b} = 1 : H \leftarrow (\{0,1\}^t \to \{0,1\}^t), x \xleftarrow{\$} \{0,1\}^t,\\
&y \xleftarrow{\$} \{0,1\}^t, \tilde{b} \leftarrow A^H_{O2H}(x, y)]\Big|
\end{aligned} \tag{9}
$$

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

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

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

P^j_B is different depending on when is the j-th queries to H(before, during, or after challenge query). And this probability can be calculated similarly as described in [13] except that the quantum encryption oracle when $j \geq q_1 + q_2$ is different from original depicted in Figure 9. Following [13], we have $P^j_B = O(\frac{j^3}{2^t})$, hence by the definition of P_B we have, $P_B \leq O(\frac{q^3}{2^t})$. Therefore, we have :

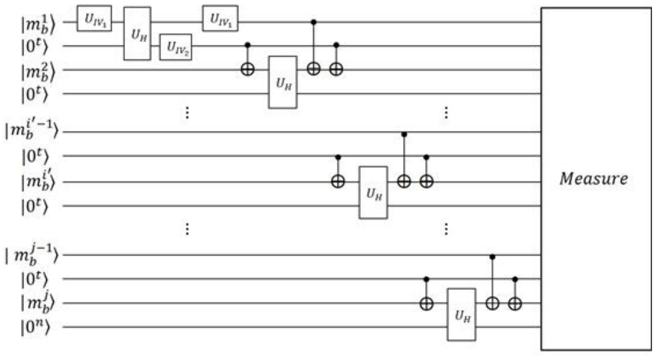


Figure 9: Composition of Encryption Oracle using H oracle.

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

Theorem 1. *If the function E is a quantum-secure PRF then Π_{IGE} is IND-qCPA secure.*

Proof. For any efficient adversary $\mathcal{A}$ making q_A encryption queries using Lemma 3 and triangle inequality we have,

$$\Big|\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\};$$
$$M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}(\mathbf{Enc}^{0,H}(M_b))]$$
$$-\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\};$$
$$M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}(\mathbf{Enc}^{p(t),H}(M_b))]\Big|$$
$$\le nO(\tfrac{p(t)^3 q_A{}^3}{2^t})$$

Outputs of $\mathsf{Enc}^{p(t),H}(M_b)$ are the case when the ciphertext are chosen completely randomly. Therefore,

$$\Big|\mathbf{Pr}[b = b' : H \leftarrow (\{0,1\}^t \rightarrow \{0,1\}^t), b \xleftarrow{\$} \{0,1\};$$
$$M_0, M_1 \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}; b' \leftarrow \mathcal{A}^{\mathbf{Enc}^{0,H}}(\mathbf{Enc}^{0,H}(M_b))] - \frac{1}{2}\Big|$$
$$\le p(t) \cdot O(\tfrac{p(t)^3 q_A{}^3}{2^t})$$

The adversary can't distinguish $\mathsf{Enc}^{0,H}$ from Enc function of Π by definition of qPRF. Therefore,

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

as q_A is polynomial in t we deduce that,

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

□

6 Conclusion and future work

We have shown that quantum security of the IGE mode in block cipher against the quantum adversary $\mathcal{A}$. When assuming sPRF, the IGE mode block cipher does not satisfy IND-qCPA. But assuming qPRF, the IGE mode block cipher is proven IND-qCPA. When we assume the sPRF, especially periodic, we can even 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.

Acknowledgement

This work was partly supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT)(No. 2017-0-00555, Towards Provable-secure Multi-party Authenticated Key Exchange Protocol based on Lattices in a Quantum World) and National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT)(No. NRF-2015R1A2A2A01006812, Design and Security Analysis of Novel Lattice-based Fully Homomorphic Signatures Robust to Quantum Computing Attack).

References

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

[2] 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.

[3] 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.

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

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

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

[7] 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.

[8] 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.

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

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

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

[12] 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.

[13] 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.