IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

VOL. E102-A NO. 1
JANUARY 2019

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY
The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

IEICE TRANS. FUNDAMENTALS, VOL.E102–A, NO.1 JANUARY 2019

LETTER *Special Section on Cryptography and Information Security*

Post-Quantum Security of IGE Mode Encryption in Telegram*

Jeeun LEE[†a)], **Sungsook KIM**[†], **Seunghyun LEE**[†], ***Nonmembers***, ***and*** **Kwangjo KIM**[†b)], ***Member***

SUMMARY IGE mode used in Telegram's customized protocol has not been fully investigated in terms of post-quantum security. In this letter, we show that IGE mode is IND-qCPA insecure by Simon's algorithm, assuming that the underlying block cipher is a standard-secure pseudorandom function (sPRF). Under a stronger assumption that the block cipher is a quantum-secure pseudorandom function (qPRF), IND-qCPA security of IGE mode is proved using one-way to hiding lemma.

key words: *IGE mode, IND-qCPA, quantum-accessible random oracle, standard/quantum-secure pseudorandom function*

1. Introduction

Telegram, a popular instant messaging (IM) service, uses AES-256 with Infinite Garble Extension (IGE) mode [1] in their customized protocol called MTProto [2]. Although Telegram is widely known as one of the most secure IM services, IGE mode is not a standard mode of operation recommended by the National Institute of Standards and Technology (NIST) [3], nor by the European Union Agency for Network and Information Security (ENISA) [4]. This motivates us to thoroughly examine the security of IGE mode encryption. The classical security of IGE mode was previously reviewed in [5]. To the best of our knowledge, this letter evaluates the post-quantum security of IGE mode against quantum adversaries who use the quantum computers to break our system for the first time.

2. Preliminaries

We consider the post-quantum security notion of *indistinguishability under quantum chosen-plaintext attack* (IND-qCPA) [6] in the *quantum-accessible random oracle model* (QaROM). The model uses an attack scenario where the adversary has a quantum encryption oracle access, with classical challenge queries allowed only. The following is a mathematically formulated definition [7], where $\hat{O}_{\mathsf{Enc_k}}$ maps basis state $|\mathsf{m}, \mathsf{c}\rangle$ to $|\mathsf{m}, \mathsf{c} \oplus \mathsf{Enc_k}(\mathsf{m})\rangle$.

Definition 2.1 (IND-qCPA): A symmetric encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is said to be IND-qCPA secure if the advantage of any quantum polynomial-time adversary $\mathcal{A} = (\mathcal{A}_\mathsf{M}, \mathcal{A}_\mathsf{D})$, where $\mathcal{A}_\mathsf{M}$ and $\mathcal{A}_\mathsf{D}$ are a message generator and a distinguisher, respectively, winning the game is negligible in security parameter λ.

$$\mathsf{Adv}^{\mathsf{IND-qCPA}}_{\mathcal{A},\Pi}(\lambda) := 2\left|\mathsf{Succ}^{\mathsf{IND-qCPA}}_{\mathcal{A},\Pi} - \frac{1}{2}\right| = \mathsf{negl}(\lambda),$$

where $\mathsf{Succ}^{\mathsf{IND-qCPA}}_{\mathcal{A},\Pi}$ is as follows:

$$\Pr\left[\mathsf{k} \xleftarrow{\$} \mathsf{Gen}(1^\lambda); (\mathsf{m}_0, \mathsf{m}_1, |\mathsf{state}\rangle) \xleftarrow{\$} \mathcal{A}_\mathsf{M}^{\hat{O}_{\mathsf{Enc_k}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{c_b} \xleftarrow{\$} \mathsf{Enc_k}(\mathsf{m_b}); \mathsf{b}' \leftarrow \mathcal{A}_\mathsf{D}^{\hat{O}_{\mathsf{Enc_k}}}(\mathsf{c_b}, |\mathsf{state}\rangle) : \mathsf{b}' = \mathsf{b}\right].$$

In order to prove IND-qCPA security of IGE mode, we need certain assumptions regarding the existence of pseudorandom functions, analogous to the classical case—namely, existence of *standard-secure pseudorandom function* (sPRF) and *quantum-secure pseudorandom function* (qPRF) [8]. The former allows quantum adversaries but limits the queries to be classical, whereas the latter allows both quantum adversaries and quantum queries, i.e. quantum superposition of inputs. The formal definitions are as follows:

Definition 2.2 (IGE Mode): For a given permutation $\mathsf{E} : \mathcal{K} \times \{0,1\}^t \to \{0,1\}^t$, a symmetric encryption scheme with IGE mode $\Pi_{\mathsf{IGE}} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is defined such that

- $\mathsf{k} \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$: For a given security parameter λ, generate key $\mathsf{k} \in \mathcal{K}$.
- $\mathsf{c} \xleftarrow{\$} \mathsf{Enc_k}(\mathsf{m})$: Before encryption, m_0 and c_0 are randomly selected from $\{0,1\}^t$ as initialization vectors. For a given message $\mathsf{m} := \mathsf{m}_0\mathsf{m}_1 \cdots \mathsf{m}_n$, where n is a polynomial in t, encrypt m using k, and output a ciphertext $\mathsf{c} := \mathsf{c}_0\mathsf{c}_1 \cdots \mathsf{c}_n$, where $\mathsf{c}_i \leftarrow \mathsf{E_k}(\mathsf{c}_{i-1} \oplus \mathsf{m}_i) \oplus \mathsf{m}_{i-1}$ for $i \in (0, n]$.
- $\mathsf{m} \leftarrow \mathsf{Dec_k}(\mathsf{c})$: For a given ciphertext c, decrypt c using k, and output a message m, where $\mathsf{m}_i \leftarrow \mathsf{E}_\mathsf{k}^{-1}(\mathsf{m}_{i-1} \oplus \mathsf{c}_i) \oplus \mathsf{c}_{i-1}$ for $i \in (0, n]$.

Definition 2.3 (sPRF and qPRF): A pseudorandom function $\mathsf{PRF} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$, where $\mathcal{K}$, $\mathcal{X}$, and $\mathcal{Y}$ are key space, domain, and range, respectively, is said to be sPRF (or qPRF) if no efficient quantum adversary $\mathcal{A}$ making classical (or quantum) queries can distinguish between a truly random function f and the function $\mathsf{PRF_k}$ for a random k,

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

Manuscript received March 22, 2018.
Manuscript revised June 13, 2018.

[†]The authors are with KAIST, Daejeon 34141, South Korea.

[*]A preliminary version of this work was presented at the 35th Symposium on Cryptography and Information Security (SCIS 2018), Niigata, Japan, 23–26 January 2018.

a) E-mail: jeeun.lee@kaist.ac.kr
b) E-mail: kkj@kaist.ac.kr

DOI: 10.1587/transfun.E102.A.148

In order to consider quantum adversaries and quantum queries, the concept of *one-way to hiding* (O2H) [9] is introduced in the security proofs.

Lemma 2.1 (O2H): Let $\mathsf{H} : \{0,1\}^t \to \{0,1\}^t$ be a random oracle. Consider an oracle algorithm $\mathcal{A}_{\mathsf{O2H}}$ that makes at most q_{O2H} queries to H. Let $\mathcal{B}$ be an oracle algorithm that on input x does the following: pick $i \xleftarrow{\$} \{1,\ldots,q_{\mathsf{O2H}}\}$ and $y \xleftarrow{\$} \{0,1\}^t$, run $\mathcal{A}^{\mathsf{H}}_{\mathsf{O2H}}(x,y)$ until the i-th query, measure the argument of the query in the computational basis, and output the measurement outcome. Let

$$P^1_{\mathcal{A}_{\mathsf{O2H}}} := \Pr\left[\mathsf{H} \xleftarrow{\$} (\{0,1\}^t \to \{0,1\}^t); x \xleftarrow{\$} \{0,1\}^t; \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{H}}_{\mathsf{O2H}}(x, \mathsf{H}(x)) : \mathsf{b}' = 1\right],$$

$$P^2_{\mathcal{A}_{\mathsf{O2H}}} := \Pr\left[\mathsf{H} \xleftarrow{\$} (\{0,1\}^t \to \{0,1\}^t); x \xleftarrow{\$} \{0,1\}^t; y \xleftarrow{\$} \{0,1\}^t; \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{H}}_{\mathsf{O2H}}(x,y) : \mathsf{b}' = 1\right],$$

$$P_{\mathcal{B}} := \Pr\left[\mathsf{H} \xleftarrow{\$} (\{0,1\}^t \to \{0,1\}^t); x \xleftarrow{\$} \{0,1\}^t; x' \leftarrow \mathcal{B}^{\mathsf{H}}(x,i) : x' = x\right].$$

Then,

$$\left|P^1_{\mathcal{A}_{\mathsf{O2H}}} - P^2_{\mathcal{A}_{\mathsf{O2H}}}\right| \le 2q_{\mathsf{O2H}}\sqrt{P_{\mathcal{B}}}.$$

3. IND-qCPA Insecurity of IGE Mode Using a sPRF

In order to show that a sPRF is not sufficient for IND-qCPA security of IGE mode, a specific block cipher $\mathsf{BC}_\mathsf{k}()$ is constructed as follows:

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

where $\mathsf{E} : \{0,1\}^{n-1} \times \{0,1\}^{n-1} \to \{0,1\}^{n-1}$ and $t : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ are sPRFs, $\mathsf{H} : \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$ is a random oracle, and $\mathsf{k} \xleftarrow{\$} \{0,1\}^{n-1}$ is the key. Here, for a string $x := x_1x_2\cdots x_n$, where x_i is the i-th bit of x, $\mathsf{LastBit}(x) = x_n$ and $\mathsf{DropLastBit}(x) = x_1x_2\cdots x_{n-1}$. For an l-bit string a and a binary variable b, $a \cdot b = a$ if $b = 1$, 0^l otherwise.

In [10], $\mathsf{BC}_\mathsf{k}()$ is proved to be a sPRF but not a qPRF using O2H lemma, for any quantum adversary with a classical access to $\mathsf{BC}_\mathsf{k}()$ and a quantum access to the random oracle H. We use this block cipher BC_k for the construction of Π_{IGE}.

Theorem 3.1: There exists a sPRF such that Π_{IGE} is IND-qCPA insecure in the QaROM.

Proof. As in previous attacks [10], we use Simon's algorithm [11] to attack IGE mode. The quantum adversary prepares six quantum registers, three of which store messages and the rest three store ciphertexts, as shown in Fig. 1. The adversary then stores the superposition of all possible

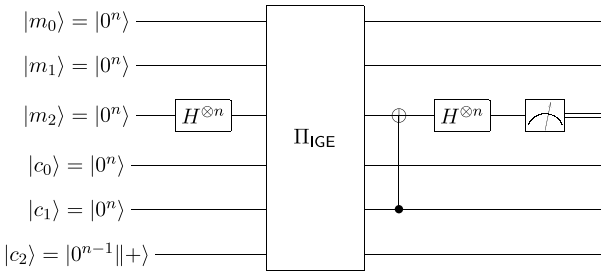

Fig. 1 Attack on 1-block IGE using Simon's algorithm.

messages, i.e. $\sum_{\mathsf{m}_2} 2^{-n/2}|\mathsf{m}_2\rangle$, in the message registers using a Hadamard gate. After an encryption query is made, the corresponding reply is stored in the ciphertext registers as follows:

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

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

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

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

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

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

$$|\psi_3\rangle = \sum_{\alpha} 2^{-(n+1)/2}|\mathsf{m}_0\rangle|0^n\rangle\left[\{|\alpha\rangle + |\alpha \oplus (\mathsf{k}\|1)\rangle\}/\sqrt{2}\right] |\mathsf{c}_0\rangle|\alpha \oplus \mathsf{m}_2\rangle|\mathsf{DropLastBit}(\mathsf{BC}_\mathsf{k}(\alpha))\|+\rangle.$$

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

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

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

4. IND-qCPA Security of IGE Mode Using a qPRF

In order to show that IND-qCPA security of IGE mode is conditional on the existence of a qPRF, we use O2H lemma and prove the bound for any quantum adversary that attacks the system. We define $\mathsf{Enc}^{i,\mathsf{H}}(\mathsf{m}) := \mathsf{c}_0\mathsf{c}_1\cdots\mathsf{c}_n$, where $\mathsf{c}_j \xleftarrow{\$}$

$\{0,1\}^t$ for $j \in [0,i]$ and $\mathsf{c}_j \leftarrow \mathsf{H}(\mathsf{c}_{j-1} \oplus \mathsf{m}_j) \oplus \mathsf{m}_{j-1}$ for $j \in (i,n]$. In Lemma 4.1, we prove that the probability of distinguishing the output of IGE mode's $\mathsf{Enc}^{i,\mathsf{H}}$ from that of $\mathsf{Enc}^{i+1,\mathsf{H}}$ is negligible in security parameter t.

Lemma 4.1: For any $i \in [0,p(t))$ and every quantum adversary $\mathcal{A}$ that makes at most $q_{\mathcal{A}}$ queries in the QaROM,

$$\Big|\Pr\Big[\mathsf{H} \leftarrow (\{0,1\}^t \to \{0,1\}^t); (\mathsf{m}_0,\mathsf{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc}^{i,\mathsf{H}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{Enc}^{i,\mathsf{H}}}(\mathsf{Enc}^{i,\mathsf{H}}(\mathsf{m}_\mathsf{b})) : \mathsf{b}' = \mathsf{b}\Big] - \Pr\Big[\mathsf{H} \leftarrow (\{0,1\}^t \to \{0,1\}^t); (\mathsf{m}_0,\mathsf{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc}^{i,\mathsf{H}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{Enc}^{i,\mathsf{H}}}(\mathsf{Enc}^{i+1,\mathsf{H}}(\mathsf{m}_\mathsf{b})) : \mathsf{b}' = \mathsf{b}\Big]\Big| =: \delta(t) \le O\left(2^{-t/2}p(t)^2 {q_{\mathcal{A}}}^2\right),$$

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

Proof. Using the proof technique as [10], we prove IGE mode case as follows: For a given message $\mathsf{m} := \mathsf{m}_0\mathsf{m}_1\cdots\mathsf{m}_n$, let $\widetilde{\mathsf{Enc}}^i_{\mathsf{H}}(\mathsf{m},\mathsf{c}_0,\mathsf{c}_1,\ldots,\mathsf{c}_i) := \hat{\mathsf{c}}_1\hat{\mathsf{c}}_2\cdots\hat{\mathsf{c}}_n$, where $\hat{\mathsf{c}}_j = \mathsf{c}_j$ for $j \in [0,i]$ and $\hat{\mathsf{c}}_j = \mathsf{H}(\hat{\mathsf{c}}_{j-1} \oplus \mathsf{m}_j) \oplus \mathsf{m}_{j-1}$ for $j \in (i,n]$. Then we put $\mathsf{c}_i := x \oplus {\mathsf{m}_\mathsf{b}}^{i+1}$ and $\mathsf{c}_{i+1} := y \oplus {\mathsf{m}_\mathsf{b}}^i$, where ${\mathsf{m}_\mathsf{b}}^i$ is the i-th block of the message m_b and $x, y \xleftarrow{\$} \{0,1\}^t$. By definition of $\widetilde{\mathsf{Enc}}^i_{\mathsf{H}}$, $\widetilde{\mathsf{Enc}}^i_{\mathsf{H}}(\mathsf{m}_\mathsf{b},\mathsf{c}_0,\mathsf{c}_1,\ldots,\mathsf{c}_i) = \widetilde{\mathsf{Enc}}^{i+1}_{\mathsf{H}}(\mathsf{m}_\mathsf{b},\mathsf{c}_0,\mathsf{c}_1,\ldots,\mathsf{c}_{i+1})$ with $\mathsf{c}_{i+1} := \mathsf{H}(x) \oplus {\mathsf{m}_\mathsf{b}}^i$. We define an adversary $\mathcal{A}_{\mathsf{O2H}}$ that makes oracle queries to the random function H is defined to be the output of the procedure described below for given inputs x and y:

$$\begin{aligned}\mathcal{A}^{\mathsf{H}}_{\mathsf{O2H}}(x,y) :=\ & (\mathsf{m}_0,\mathsf{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc}^{i,\mathsf{H}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{c}_0,\cdots,\mathsf{c}_{i-1} \\ & \xleftarrow{\$} \{0,1\}^t; \mathsf{c}_i := x \oplus {\mathsf{m}_\mathsf{b}}^{i+1}; \mathsf{c}_{i+1} := y \oplus {\mathsf{m}_\mathsf{b}}^i; \\ & \text{compute } \mathsf{c} := \widetilde{\mathsf{Enc}}^{i+1}_{\mathsf{H}}(\mathsf{m}_\mathsf{b},\mathsf{c}_0,\ldots,\mathsf{c}_{i+1}); \\ & \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{Enc}^{i,\mathsf{H}}}(\mathsf{c}); \text{ return } \mathsf{b}' = \mathsf{b}.\end{aligned}$$

Now we have the equation, by O2H lemma,

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

Note that $\mathcal{A}_{\mathsf{O2H}}$ can answer $\mathcal{A}$'s queries as it has oracle access to H. Let q_{O2H} be the number of H-queries made by $\mathcal{A}_{\mathsf{O2H}}$, then it is clear that $q_{\mathsf{O2H}} \le 3p(t)q_{\mathcal{A}}$. Let q_1, q_2, and q_3 denote the number of queries that $\mathcal{A}_{\mathsf{O2H}}$ makes to H before, during, and after the challenge query, respectively. Let $\mathcal{B}$ be an oracle algorithm described in O2H lemma and $P_{\mathcal{B}}$ be $P^j_{\mathcal{B}}/q_{\mathsf{O2H}}$. In all three cases depending upon whether the j-th H-query was made before, during, or after the challenge query, we may show that $P_{\mathcal{B}} \le O(2^{-t}{q_{\mathsf{O2H}}}^2)$. Therefore, we have

$$\begin{aligned}\delta(t) &\le 2q_{\mathsf{O2H}}\sqrt{P_{\mathcal{B}}} \\ &= O(2^{-t/2}{q_{\mathsf{O2H}}}^2) = O(2^{-t/2}p(t)^2{q_{\mathcal{A}}}^2). \quad \square\end{aligned}$$

Theorem 4.2: If the function E is a qPRF, then Π_{IGE} is IND-qCPA secure in the QaROM.

Proof. Using the proof technique as [10], we prove IGE mode case as follows: Let $\mathcal{A}$ be a quantum adversary making $q_{\mathcal{A}}$ queries. Note that $\mathsf{Enc}^{p(t),\mathsf{H}}(\mathsf{m}_\mathsf{b})$ is independent of its argument m_b. Then by Lemma 4.1 and triangle inequality,

$$\begin{aligned}&\Big|\Pr\Big[\mathsf{H} \leftarrow (\{0,1\}^t \to \{0,1\}^t); (\mathsf{m}_0,\mathsf{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}}(\mathsf{Enc}^{0,\mathsf{H}}(\mathsf{m}_\mathsf{b})) : \mathsf{b}' = \mathsf{b}\Big] - \\ &\Pr\Big[\mathsf{H} \leftarrow (\{0,1\}^t \to \{0,1\}^t); (\mathsf{m}_0,\mathsf{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc}^{p(t),\mathsf{H}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{Enc}^{p(t),\mathsf{H}}}(\mathsf{Enc}^{p(t),\mathsf{H}}(\mathsf{m}_\mathsf{b})) : \mathsf{b}' = \mathsf{b}\Big]\Big| \\ &\le p(t)O\left(2^{-t/2}p(t)^2{q_{\mathcal{A}}}^2\right).\end{aligned}$$

One can see that $\mathsf{Enc}^{p(t),\mathsf{H}}(\mathsf{m}_\mathsf{b})$ outputs ciphertext as a completely random string. Hence, the output b' is independent of b. Therefore,

$$\begin{aligned}&\Big|\Pr\Big[\mathsf{H} \leftarrow (\{0,1\}^t \to \{0,1\}^t); (\mathsf{m}_0,\mathsf{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{Enc}^{0,\mathsf{H}}}(\mathsf{Enc}^{0,\mathsf{H}}(\mathsf{m}_\mathsf{b})) : \mathsf{b}' = \mathsf{b}\Big] - \frac{1}{2}\Big| \\ &\le p(t)O\left(2^{-t/2}p(t)^2{q_{\mathcal{A}}}^2\right).\end{aligned}$$

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

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

That is, Π_{IGE} is IND-qCPA secure. $\square$

5. Concluding Remarks

We examined the post-quantum security of IGE mode as a follow-up study of its classical security. Among many post-quantum security notions, we considered IND-qCPA security against the quantum adversary who has a quantum encryption oracle access, with classical challenge queries allowed only. When the underlying block cipher is assumed to be a sPRF only, IGE mode is broken by attacks using Simon's algorithm. However, assuming a qPRF block cipher, IGE mode is proven to be secure.

Acknowledgements

We are very grateful for valuable comments of the anonymous reviewers to improve the readability of this letter. This

work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korean government (MSIT) (No. 2017-0-00555, Towards provable-secure multi-party authenticated key exchange protocol based on lattices in a quantum world).

References

[1] C.M. Campbell, "Design and specification of cryptographic capabilities," IEEE Commun. Soc. Mag., vol.16, no.6, pp.15–19, Nov. 1978.
[2] "MTProto mobile protocol: Detailed description," https://core.telegram.org/mtproto/description
[3] M. Dworkin, "Recommendation for block cipher modes of operation: Methods and techniques," Technical Report, National Institute of Standards and Technology (NIST), Dec. 2001.
[4] N.P. Smart, V. Rijmen, B. Gierlichs, K.G. Paterson, M. Stam, B. Warinschi, G. Watson, and R. Tirtea, "Algorithms, key size and parameters report – 2014," Technical Report, European Union Agency for Network and Information Security (ENISA), Nov. 2014.
[5] J. Lee, R. Choi, S. Kim, and K. Kim, "Security analysis of end-to-end encryption in Telegram," Proc. 34th Symposium on Cryptography and Information Security (SCIS 2017), Naha, Japan, Jan. 2017.
[6] D. Boneh and M. Zhandry, "Secure signatures and chosen ciphertext security in a quantum computing world," Cryptology ePrint Archive, Report 2013/088, 2013. https://eprint.iacr.org/2013/088
[7] J. Lee, S. Lee, and K. Kim, "Security notions for the random oracle model in classical and quantum settings," Proc. 35th Symposium on Cryptography and Information Security (SCIS 2018), Niigata, Japan, Jan. 2018.
[8] M. Zhandry, "How to construct quantum random functions," Proc. 53rd Annual Symposium on Foundations of Computer Science (FOCS 2012), pp.679–687, New Brunswick, NJ, US, Oct. 2012.
[9] D. Unruh, "Revocable quantum timed-release encryption," Cryptology ePrint Archive, Report 2013/606, 2013. https://eprint.iacr.org/2013/606
[10] M.V. Anand, E.E. Targhi, G.N. Tabia, and D. Unruh, "Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation," Cryptology ePrint Archive, Report 2016/197, 2016. https://eprint.iacr.org/2016/197
[11] D.R. Simon, "On the power of quantum computation," Proc. 35th Annual Symposium on Foundations of Computer Science (FOCS 1994), pp.116–123, Santa Fe, NM, US, Nov. 1994.