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 $\hat{\mathcal{O}}_{\text{Enc}_k}$ maps basis state $|m, c\rangle$ to $|m, c \oplus \text{Enc}_k(m)\rangle$.

**Definition 2.1 (IND-qCPA):** A symmetric encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is said to be IND-qCPA secure if the advantage of any quantum polynomial-time adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$, where $\mathcal{A}_0$ and $\mathcal{A}_1$ are a message generator and a distinguisher, respectively, winning the game is negligible in security parameter $\lambda$.

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

where $\text{Succ}^\text{IND-qCPA}_{\Pi, \lambda}$ is as follows:

$$\Pr\left[k \leftarrow \text{Gen}(\lambda^4); (m_0, m_1, |\text{state}\rangle) \leftarrow \mathcal{A}_0\left(k, \left[0, 1\right]^t\right); c_0 \leftarrow \text{Enc}_k(m_0); b \leftarrow \mathcal{A}_1\left(c_0, |\text{state}\rangle\right); b' = b\right].$$

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 $\mathcal{E} : \mathcal{K} \times \{0, 1\}^t \rightarrow \{0, 1\}^t$, a symmetric encryption scheme with IGE mode $\Pi_{\text{IGE}} = (\text{Gen}, \text{Enc}, \text{Dec})$ is defined such that

- $k \leftarrow \text{Gen}(\lambda^4)$: For a given security parameter $\lambda$, generate key $k \in \mathcal{K}$.
- $c \leftarrow \text{Enc}_k(m)$: Before encryption, $m_0$ and $c_0$ are randomly selected from $\{0, 1\}^t$ as initialization vectors. For a given message $m := m_0m_1 \cdots m_t$, with $n$ a polynomial in $t$, encrypt $m$ using $k$, and output a ciphertext $c := c_0c_1 \cdots c_t$, where $c_i \leftarrow \text{Enc}_k(c_{i-1} \oplus m_i) \oplus m_{i-1}$ for $i \in (0, n]$.
- $m \leftarrow \text{Dec}_k(c)$: For a given ciphertext $c$, decrypt $c$ using $k$, and output a message $m$, with $m_i \leftarrow \text{Dec}_k(c_{i-1} \oplus c_i) \oplus c_{i-1}$ for $i \in (0, n]$.

**Definition 2.3 (sPRF and qPRF):** A pseudorandom function PRF : $\mathcal{K} \times X \rightarrow Y$, where $\mathcal{K}$, $X$, and $Y$ 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 $\text{PRF}_k$ for a random $k$,

$$\Pr_{f \in \mathcal{Y}^t}[\mathcal{A}(f) = 1] - \Pr_{k \in \mathcal{K}}[\mathcal{A}(\text{PRF}_k) = 1] = \text{negl}(\lambda).$$
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 \( H : \{0,1\}^t \rightarrow \{0,1\}^t \) be a random oracle. Consider an oracle algorithm \( \mathcal{A}_{O2H} \) that makes at most \( q_{O2H} \) queries to \( H \). Let \( B \) be an oracle algorithm that on input \( x \) does the following: pick \( i \leftarrow \{1, \ldots, q_{O2H}\} \) and \( y \leftarrow \{0,1\}^t \), run \( A^H_{O2H}(x, y) \) until the \( i \)-th query, measure the argument of the query in the computational basis, and output the measurement outcome. Let

\[
P_{A_{O2H}}^1 := \Pr \left[ H \left( \left( \{0,1\}^t \rightarrow \{0,1\}^t \right); x \leftarrow \{0,1\}^t; b' \leftarrow A^H_{O2H}(x, H(x)) : b' = 1 \right) \right],
\]

\[
P_{A_{O2H}}^2 := \Pr \left[ H \left( \left( \{0,1\}^t \rightarrow \{0,1\}^t \right); y \leftarrow \{0,1\}^t; y' \leftarrow A^H_{O2H}(x, y) : b' = 1 \right) \right],
\]

\[
P_B := \Pr \left[ H \left( \left( \{0,1\}^t \rightarrow \{0,1\}^t \right); x \leftarrow \{0,1\}^t; x' \leftarrow B^H(x, i) : x' = x \right) \right].
\]

Then,

\[
|P_{A_{O2H}}^1 - P_{A_{O2H}}^2| \leq 2q_{O2H}\sqrt{P_B}.
\]

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 \( BC_k(\cdot) \) is constructed as follows:

\[
BC_k(x) := E_{\Pi GIE}(0^l \cdot \text{DropLastBit}(x), x, k),
\]

where \( E : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n \) is a PRF, \( \Pi GIE \) is an IND-qCPA secure cipher, and \( k \) is the secret key. Here, for a string \( x = x_1x_2 \ldots x_n \), where \( x_i \) is the \( i \)-th bit of \( x \), \( \text{DropLastBit}(x) = x_1x_2 \ldots x_{n-1} \). For an \( l \)-bit string \( a \) and a binary variable \( b, a \cdot b = a \) if \( b = 1 \), \( 0 \) otherwise.

In [10], \( BC_k(\cdot) \) is proved to be a sPRF but not a qPRF using O2H lemma, for any quantum adversary with a classical access to \( BC_k(\cdot) \) and a quantum access to the random oracle \( H \). We use this block cipher \( BC_k(\cdot) \) for the construction of \( \Pi GIE \).

**Theorem 3.1:** There exists a sPRF such that \( \Pi GIE \) is IND-qCPA insecure in the QRAM.

**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 messages, i.e. \( \sum_{m_2} 2^{-n/2}|m_2 \rangle \), 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:

\[
|\psi_2 \rangle = \sum_{m_2} 2^{-n/2}|m_0 \rangle |0^n \rangle |m_2 \rangle |c_0 \rangle |BC_k(c_0) \oplus m_0 \rangle |\text{DropLastBit}(BC_k(BC_k(c_0) \oplus m_0 \oplus m_2)) \rangle
\]

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

\[
|\psi_3 \rangle = \sum_{m_2} 2^{-n/2}|m_0 \rangle |0^n \rangle |\alpha \rangle |c_0 \rangle |\alpha \oplus m_2 \rangle |\text{DropLastBit}(BC_k(\alpha)) \rangle
\]

where \( \alpha := BC_k(c_0) \oplus m_0 \oplus m_2 \). In order to use \( BC_k(\cdot) \)’s special property of being \( (k(1)) \)-periodic, we consider another message input \( \sum_{m_2} 2^{-n/2}|m_2 \rangle \oplus (k(1)) \). By a similar calculation as before, and using \( BC_k(x) = BC_k(x \oplus (k(1))) \),

\[
|\psi_3 \rangle = \sum_{m_2} 2^{-n/2}|m_0 \rangle |0^n \rangle |\alpha \rangle |\alpha \oplus m_2 \rangle |\text{DropLastBit}(BC_k(\alpha)) \rangle
\]

Since \( |\psi_3 \rangle = |\psi_1 \rangle ||\psi_2 \rangle )/2 \), \( |\psi_3 \rangle \) is rewritten as

\[
|\psi_3 \rangle = \sum_{m_2} 2^{-(n+1)/2}|m_0 \rangle |0^n \rangle |(\alpha + \alpha \oplus (k(1))) / \sqrt{2} \rangle
\]

\[
|c_0 \rangle |\alpha \oplus m_2 \rangle |\text{DropLastBit}(BC_k(\alpha)) \rangle
\]

The state after applying Hadamard gate on \( |m_2 \rangle \) is

\[
|\psi_4 \rangle = 2^{-n+1/2}(-1)^{\alpha \oplus m_2} \sum_{z} z |m_0 \rangle |0^n \rangle \left[ (1 + (-1)^{k(1)z})/\sqrt{2} \right]
\]

\[
|c_0 \rangle |\alpha \oplus m_2 \rangle |\text{DropLastBit}(BC_k(\alpha)) \rangle
\]

where \( \odot \) denotes bitwise inner product. Finally, if we measure the \( m_2 \) register, we either get a vector \( z \) such that \( (k(1)) \odot z = 0 \), 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 \( \Pi GIE \). □

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 \( Enc^H(m) := c_0c_1 \cdots c_n \), where \( c_j \leftarrow \)}
\[ \{0, 1\}^t \text{ for } j \in \{0, i\} \text{ and } c_j \leftarrow H(c_{j-1} \oplus m_j) \oplus m_{j-1} \text{ for } j \in \{i, n\}. \] In Lemma 4.1, we prove that the probability of distinguishing the output of IGE mode’s \( \text{Enc}^{\text{H}, t} \) from that of \( \text{Enc}^{\text{H}, t+1} \) 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,

\[
\Pr \left[ H \leftarrow \{0, 1\}^t \rightarrow \{0, 1\}^t; \{m_0, m_1\} \leftarrow \mathcal{A}^{\text{Enc}^{\text{H}, t}} \right] - \Pr \left[ H \leftarrow \{0, 1\}^t \rightarrow \{0, 1\}^t; \{m_0, m_1\} \leftarrow \mathcal{A}^{\text{Enc}^{\text{H}, t+1}} \right] \leq \delta(t) \leq O \left( 2^{t+2} p(t)^2 q_{\mathcal{A}}^2 \right),
\]

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 \( m := m_0 m_1 \cdots m_n \), let \( \text{Enc}_i^{H}(m_0, c_1, \cdots, c_i) := \delta_1 \delta_2 \cdots \delta_n \), where \( \delta_j = c_j \) for \( j \in \{0, i\} \) and \( \delta_j = H(c_{j-1} \oplus m_j) \oplus m_{j-1} \) for \( j \in \{i, n\} \). Then we put \( c_i := x \oplus m_{i+1} \) and \( c_{i+1} := y \oplus m_i \), where \( m_i \) is the \( i \)-th block of the message \( m \) and \( x, y \leftarrow \{0, 1\}^t \). By definition of \( \text{Enc}_i^{H} \),

\[
\text{Enc}_i^{H}(m_0, c_0, \cdots, c_i) \triangleq \text{Enc}_i^{H}(m_0, c_0, \cdots, c_i, \cdots, c_{i+1}) \triangleq H(x) \oplus m_i.
\]

We define an adversary \( \mathcal{A}_{\text{O2H}} \) 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 \( y \):

\[
\mathcal{A}_{\text{O2H}}^{H}(x, y) := \{m_0, m_1\} \leftarrow \mathcal{A}^{\text{Enc}^{\text{H}, t}} ; b \leftarrow \{0, 1\}; c_0, \cdots, c_{i-1} \leftarrow \{0, 1\}; c_i := x \oplus \text{Enc}_{i-1}^{H}; c_{i+1} := y \oplus m_i; \text{compute } c := \text{Enc}_{i}^{H}(m_0, c_0, \cdots, c_{i+1}); b' \leftarrow \mathcal{A}^{\text{Enc}^{\text{H}, t}}(c); \text{return } b' = b.
\]

Now we have the equation, by O2H lemma,

\[
\delta(t) = \Pr \left[ H \leftarrow \{0, 1\}^t \rightarrow \{0, 1\}^t; x \leftarrow \{0, 1\}^t \right] - \Pr \left[ H \leftarrow \{0, 1\}^t \rightarrow \{0, 1\}^t; x \leftarrow \{0, 1\}^t \right] \leq \delta(t) \leq O \left( 2^{t+2} p(t)^2 q_{\mathcal{A}}^2 \right).
\]

Note that \( \mathcal{A}_{\text{O2H}} \) can answer \( \mathcal{A} \)’s queries as it has oracle access to \( H \). Let \( q_{\text{O2H}} \) be the number of \( H \)-queries made by \( \mathcal{A}_{\text{O2H}} \), then it is clear that \( q_{\text{O2H}} \leq 3 p(t) q_{\mathcal{A}} \). Let \( q_1, q_2 \), and \( q_3 \) denote the number of queries that \( \mathcal{A}_{\text{O2H}} \) makes to \( H \) before, during, and after the challenge query, respectively. Let \( B \) be an oracle algorithm described in O2H lemma and \( P_{\text{B}} \) be \( p_{\text{B}}^{q_{\text{O2H}}}/q_{\text{O2H}} \). 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 \( P_{\text{B}} \leq O(2^t q_{\text{O2H}}^2) \). Therefore, we have

\[
\delta(t) \leq 2 q_{\text{O2H}} \sqrt{P_{\text{B}}} = O \left( 2^{t+2} q_{\text{O2H}}^2 \right) = O(2^{t+2} p(t)^2 q_{\mathcal{A}}^2), \quad \Box
\]

**Theorem 4.2:** If the function \( E \) is a qPRF, then \( \Pi_{\text{IGE}} \) 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 \( \text{Enc}^{(i), H}(m_b) \) is independent of its argument \( m_b \). Then by Lemma 4.1 and triangle inequality,

\[
\Pr \left[ H \leftarrow \{0, 1\}^t \rightarrow \{0, 1\}^t; \{m_0, m_1\} \leftarrow \mathcal{A}^{\text{Enc}^{\text{H}, t}} \right] - \Pr \left[ H \leftarrow \{0, 1\}^t \rightarrow \{0, 1\}^t; \{m_0, m_1\} \leftarrow \mathcal{A}^{\text{Enc}^{\text{H}, t+1}} \right] \leq p(t) O \left( 2^{t+2} p(t)^2 q_{\mathcal{A}}^2 \right).
\]

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

\[
\Pr \left[ H \leftarrow \{0, 1\}^t \rightarrow \{0, 1\}^t; \{m_0, m_1\} \leftarrow \mathcal{A}^{\text{Enc}^{\text{H}, t}} \right] - \Pr \left[ H \leftarrow \{0, 1\}^t \rightarrow \{0, 1\}^t; \{m_0, m_1\} \leftarrow \mathcal{A}^{\text{Enc}^{\text{H}, t+1}} \right] \leq p(t) O \left( 2^{t+2} p(t)^2 q_{\mathcal{A}}^2 \right).
\]

Since \( \text{Enc}^{H} \) is indistinguishable from Enc of \( \Pi_{\text{IGE}} \) by definition of qPRF, and as \( q_{\mathcal{A}} \) is polynomial in \( t \), we deduce

\[
\text{Adv}_{\mathcal{A}, \Pi_{\text{IGE}}}^{\text{IND-qCPA}} (t) \leq O \left( 2^{t+2} p(t)^2 q_{\mathcal{A}}^2 \right) + \text{negl}(t) = \text{negl}(t)
\]

That is, \( \Pi_{\text{IGE}} \) is IND-qCPA secure. \( \Box \)

**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.
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


