Security on the Quantum-type Even-Mansour Cipher

Hidenori Kuwakado
Graduate School of Engineering
Kobe University
1-1 Rokkodai-cho Nada-ku Kobe 657-8501, Japan
Email: kuwakado@kobe-u.ac.jp

Masakatu Morii
Graduate School of Engineering
Kobe University
1-1 Rokkodai-cho Nada-ku Kobe 657-8501, Japan
Email: mmorii@kobe-u.ac.jp

***Abstract*—Quantum cryptography such as BB84 is a quantum protocol for sharing classical information, but is not a scheme for encrypting quantum information itself. This paper considers that quantum information is encrypted with the quantum circuit of the Even-Mansour cipher. It has been proved that breaking the Even-Mansour cipher requires exponential time in the key length using any classical algorithm. This paper shows that the quantum version of the Even-Mansour cipher is insecure, that is, a key can be found in polynomial time in the key length. This is an example that the quantum version of a secure classical cipher is not always secure.**

I. Introduction

One important aspect of quantum computation is that quantum computers can be more efficient than anything ever imagined in classical computers for certain computational tasks of considerable practical interest. Since computation is regarded as information processing, a quantum computer is a tool for quantum information processing. Like we currently perform classical information processing using classical computers, we will perform quantum information processing using quantum computers. In fact, the principle of quantum error-correcting codes and that of quantum secret sharing schemes, which are schemes for processing quantum information, have been proposed. Schemes for encrypting quantum information have been studied in the context of private quantum channels and locking of quantum states. Notice that quantum cryptography such as BB84 [1] is a protocol for sharing classical information using quantum technology, but not for encrypting quantum information itself.

On the other hand, research on classical ciphers has a long history. Knowledge on classical ciphers could be useful for constructing a scheme for encrypting quantum information. For example, since AES [7] is a widely-used classical cipher, the quantum version of AES is particularly promising. However, we have no evidence that such a quantum cipher is secure even if AES is secure against any classical adversary. It is worth to study the security of the quantum version of a classical cipher.

The EM cipher is a classical cipher proposed by Even and Mansour [4], and it can be considered as the reduced version of AES. It has been proved that any classical algorithm requires subexponential time in the key length to break the EM cipher. In this sense, the EM cipher is secure against any classical adversary. This paper mainly discusses the security of the quantum version of the EM cipher (the quantum EM cipher), which is defined in Section II. This paper shows that the quantum EM cipher is insecure because a key can be recovered in polynomial time in the key length. This is an example that it is not recommend that a classical cipher is implemented with a quantum circuit. This paper also shows that the security of the EM cipher decreases if an adversary can construct a unitary operator from public information.

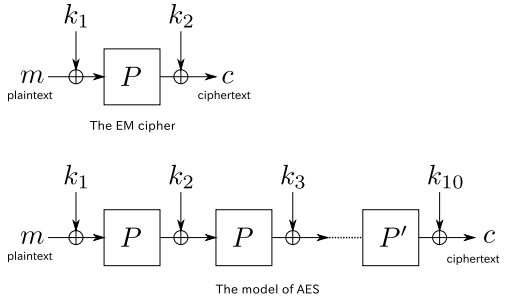

Fig. 1. The EM cipher and the model of AES.

This paper is organized as follows: Section II reviews the EM cipher and its classical security, and defines its quantum version. Section III discusses the complexity for finding a key of the quantum EM cipher. We show a quantum algorithm for finding a key in polynomial queries in the key length. Section IV considers the security of the EM cipher in the model such that a classical encryption oracle is available to an adversary. This model is close to classical computational model. If the adversary can construct a unitary operator from public information about the EM cipher, then the adversary can find the key efficiently, but not in polynomial time. Section V concludes this paper.

II. Preliminaries

A. Even-Mansour Cipher

Even and Mansour [4] have proposed a classical symmetric cipher illustrated in Fig. 1 (the *EM cipher*). The security of the EM cipher is related to that of AES because the EM cipher is considered as the reduced version of AES.

In Fig. 1, P is a public random permutation on $\{0,1\}^{n/2}$ and a key $k = k_1 \parallel k_2$ is n bits where $k_1, k_2 \in \{0,1\}^{n/2}$. The encryption of the EM cipher is defined as

$$\begin{aligned} c &= E_k(m) \\ &= P(k_1 \oplus m) \oplus k_2, \end{aligned}$$

where m, c $(\in \{0,1\}^{n/2})$ are a plaintext and its ciphertext, respectively. The decryption is done as

$$\begin{aligned} m &= D_k(c) \\ &= P^{-1}(k_2 \oplus c) \oplus k_1. \end{aligned}$$

The classical security of the EM cipher has been reported in articles [3], [4]. The results are summarized below.

Lemma 1 ([4]): Suppose that P is a public random permutation on $\{0,1\}^{n/2}$ and k is chosen randomly and uniformly from $\{0,1\}^n$. Suppose that an adversary is allowed to make queries to E_k, D_k, P, and P^{-1}. Then, the probability that the adversary finds the key k is bounded by

$$O\left(\frac{q_e q_p}{2^{n/2}}\right)$$

where q_e is the number of queries to E_k or D_k and q_p is the number of queries P or P^{-1}.

Daemen and Esat [3] have shown a chosen-plaintext attack for finding a key.

Lemma 2 ([3]): The key can be found with $O(2^{n/4})$ complexity. The complexity is dominated by the computation for producing ciphertexts for $2^{n/4}$ chosen plaintexts.

These results show that the EM cipher cannot achieve n-bit security, but breaking it requires subexponential time in n. If n is large, then the EM cipher is computationally secure against any classical adversary.

B. Quantum Even-Mansour Cipher

This paper discusses a quantum version of the EM cipher (the quantum EM cipher). The quantum EM cipher encrypts quantum information. Namely, the quantum EM cipher takes n qubits as a plaintext and outputs n qubits as a ciphertext. This paper assumes that a key is classical information. This is because a key is memorized by a human. This paper does not discuss the case where a key itself is quantum information.

Consider a unitary operator U_{E_k} for the encryption of the EM cipher.

$$U_{E_k}|x\rangle|a\rangle = |x\rangle|a \oplus E_k(x)\rangle,$$

where x is a plaintext and $E_k(x)$ is its ciphertext. This unitary operator is the quantum EM cipher. The objective of an adversary is to find the key k. The adversary is allowed to use the unitary operator U_{E_k}. Namely, the adversary can give any input state $|x\rangle|a\rangle$ to the unitary operator and can take its output state $|x\rangle|a \oplus E_k(x)\rangle$. Since the key length is n, the adversary can find the key k in $O(2^{n/2})$ using the Grover algorithm [5]. We are interested in a more efficient algorithm.

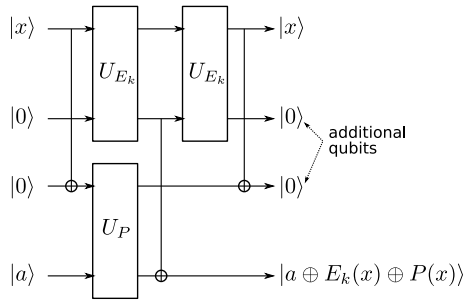

Fig. 2. Quantum circuit for computing F.

III. Chosen Plaintext Attack to the Quantum EM cipher

This section will show a polynomial quantum algorithm for finding a key. The proposed algorithm is similar to Simon's algorithm [8].

A. Algorithm

The proposed algorithm requires the unitary operator U_P for computing the public permutation P.

$$U_P|x\rangle|a\rangle = |x\rangle|a \oplus P(x)\rangle,$$

where P is the public random permutation of the EM cipher. The adversary can construct the unitary operator U_P because P is public. Furthermore, we define a function F as

$$F(x) = E_k(x) \oplus P(x).$$

Figure 2 shows that a unitary operator U_F for computing F can be constructed with U_{E_k} and U_P. Omitting additional qubits in Fig. 2, we can write the application of U_F in a simple way as

$$U_F|x\rangle|a\rangle = |x\rangle|a \oplus F(x)\rangle.$$

The unitary operator U_F plays an important role in the proposed algorithm.

To perform the algorithm, the adversary needs to perform classical operations (e.g., arithmetic operations). Hence, we assume that the adversary can use an auxiliary classical computer for performing them.

We describe an algorithm to find the n-bit key k that runs in polynomial time in n. To simplify the notation, let $\nu = n/2$.

1) Initialize a set $\mathcal{Z}$ to the empty set.
2) Prepare a state
$$|\phi_1\rangle = \frac{1}{\sqrt{2^\nu}} \sum_{x \in \{0,1\}^\nu} |x\rangle|0\rangle.$$
3) Apply U_F to $|\phi_1\rangle$.
$$\begin{aligned} |\phi_2\rangle &= U_F|\phi_1\rangle \\ &= \frac{1}{\sqrt{2^\nu}} \sum_{x \in \{0,1\}^\nu} |x\rangle|F(x)\rangle \end{aligned}$$
4) Measure the second register. Let y be the measurement result and let $\mathcal{X}_y$ denote a set of x such that $y = F(x)$.

By omitting the second register, the resulting state is given by

$$|\phi_3\rangle = \frac{1}{\sqrt{\lambda}} \sum_{x \in \mathcal{X}_y} |x\rangle, \tag{1}$$

where λ denotes the number of elements in $\mathcal{X}_y$.

5) Apply the Hadamard transformation H to $|\phi_3\rangle$.

$$\begin{aligned} |\phi_4\rangle &= H|\phi_3\rangle \\ &= \frac{1}{\sqrt{\lambda 2^\nu}} \sum_{\substack{x \in \mathcal{X}_y \\ z \in \{0,1\}^\nu}} (-1)^{x \cdot z} |z\rangle, \end{aligned}$$

where '$\cdot$' means a bitwise modulo-2 inner product of x and z.

6) Measure the register. Let z_i be the measurement result.

7) Append z_i to the set $\mathcal{Z}$. If $\mathcal{Z}$ does not contain $\nu - 1$ linearly independent z_i's, then go back to step 2. Otherwise solve the following system of equations in a ν-bit sequence $\hat{k}_1$.

$$\begin{cases} z_1 \cdot \hat{k}_1 = 0 \bmod 2 \\ z_2 \cdot \hat{k}_1 = 0 \bmod 2 \\ \cdots \\ z_\nu \cdot \hat{k}_1 = 0 \bmod 2, \end{cases} \tag{2}$$

where z_i's are assumed to be linearly independent.

8) Choose $m \in \{0,1\}^\nu$ at random and make a query m to the classical oracle E_k. Let $\hat{k}_2$ be

$$\hat{k}_2 = E_k(m) \oplus P(m \oplus \hat{k}_1) \tag{3}$$

9) Output $\hat{k}_1 \parallel \hat{k}_2$ as $k = k_1 \parallel k_2$.

B. Analysis of the Algorithm

We justify the output of the above algorithm. Consider the set $\mathcal{X}_y$ in step 4. All the elements x in $\mathcal{X}_y$ satisfy

$$\begin{aligned} y &= E_k(x) \oplus P(x) \\ &= P(x \oplus k_1) \oplus P(x) \oplus k_2. \end{aligned}$$

When x_1 satisfies the above equation, $x_1 \oplus k_1$ always satisfies the above equation. Accordingly, the number of elements in $\mathcal{X}_y$, λ, is even. Equation (1) is rewritten as

$$\begin{aligned} |\phi_3\rangle &= \frac{1}{\sqrt{\lambda}} \sum_{i=1}^{\lambda} |x_i\rangle \\ &= \frac{1}{\sqrt{\lambda}} \sum_{i=1}^{\lambda/2} |x_i\rangle + |x_i \oplus k_1\rangle, \end{aligned}$$

where the indices i were rearranged appropriately. Applying the Hadamard transformation to $|\phi_3\rangle$ in step 5 gives

$$|\phi_4\rangle = \frac{1}{\sqrt{\lambda 2^\nu}} \sum_{\substack{1 \le i \le \lambda/2 \\ z \in \{0,1\}^\nu}} \left((-1)^{x_i \cdot z} + (-1)^{(x_i \oplus k_1) \cdot z} \right) |z\rangle.$$

From this equation, we see that the measurement result z_i in step 6 satisfies

$$z_i \cdot k_1 = 0 \bmod 2,$$

which appeared in Eq. (2). Since k_1 is a ν-bit sequence, solving Eq. (2) yields k_1. When k_1 was obtained correctly, Eq. (3) gives k_2.

Recall that $\nu = n/2$ where n is the key length. The quantum complexity of this algorithm is dominated by obtaining $n/2-1$ independent equations in step 7. To obtain $n/2-1$ independent equations, the adversary must repeat the procedure from step 2 to step 7. Assume that the procedure is repeated $n/2 + \delta$ times. Then, the probability of acquiring enough information to determine k_1 is

$$\prod_{i=\delta+2}^{\delta+\frac{n}{2}} \left(1 - \frac{1}{2^i}\right) > 1 - \frac{1}{2^{\delta+1}},$$

which is independent of n. Hence, the number of repetitions is $O(n)$, which is the quantum complexity of this algorithm. The classical complexity is dominated by solving the system of equations in step 7. It requires $O(n^3)$ modular operations. Hence we conclude that the quantum EM cipher is insecure.

IV. Another Computational Model

The previous section assumes that the unitary operator U_{E_k} is available to an adversary. This section assumes that the classical encryption oracle E_k (instead of the unitary operator U_{E_k} for the encryption) is available to an adversary. This section discusses the security of the EM cipher (not the quantum EM cipher). Unlike classical cryptanalysis in Sect. II-A, the adversary is allowed to use a unitary operator that is related to the public permutation P and is not allowed to use the classical decryption oracle D_k. We note that the unitary operator does not include any information about the key. This section shows that the adversary can find a key more efficiently than the classical attack in Sect. II-A and the straightforward application of the Grover algorithm.

A. Algorithm

Let $\mathcal{D} \subseteq \{0,1\}^{n/2}$ be a set, which will be defined in the following algorithm. For a given $\mathcal{D}$, we define a function $L_\mathcal{D} : \{0,1\}^{n/2} \to \{0,1\}$ as

$$L_\mathcal{D}(x) = \begin{cases} 0 & \text{if } P(x) \oplus P(\overline{x}) \notin \mathcal{D} \\ 1 & \text{if } P(x) \oplus P(\overline{x}) \in \mathcal{D}, \end{cases} \tag{4}$$

where P is a public permutation of the EM cipher and $\overline{x}$ is the bitwise complement of x. Notice that P does not involve any information on the key. We can construct a unitary operator $V_{L_\mathcal{D}}$ as

$$V_{L_\mathcal{D}}|x\rangle = (-1)^{L_\mathcal{D}(x)}|x\rangle.$$

To perform the algorithm, the adversary needs to perform classical operations such as arithmetic operations, a sorting algorithm, and the computation of the public permutation P. Hence, we assume that the adversary can use an auxiliary classical computer for performing them.

We describe the algorithm for finding an n-bit key $k = k_1 \parallel k_2$. In the following, t is a parameter, which is discussed later. This algorithm is similar to a quantum collision-finding algorithm proposed by Brassard, Høyer, and Tapp [2].

1) Choose x_i $(i = 1, 2, \ldots, t)$ from $\{0,1\}^{n/2}$ at random. Assume that $x_i \neq x_j$ for $i \neq j$ and $\overline{x_i} \notin \{x_i \,|\, i = 1, 2, \ldots, t\}$ for any i.
2) For $i = 1, 2, \ldots, t$, compute
$$d_i = E_k(x_i) \oplus E_k(\overline{x_i})$$
by using the classical circuit E_k. Denote by $\mathcal{D}$ a set of d_i, that is,
$$\mathcal{D} = \{d_i \,|\, i = 1, 2, \ldots, t\}.$$
For simplicity, assume that all the elements in $\mathcal{D}$ are distinct. The set $\mathcal{D}$ is used as $\mathcal{D}$ defined in Eq. (4).
3) Sort a table $\mathcal{T}$ where each item holds a pair (d_i, x_i) according to the first entry d_i. Since the table $\mathcal{T}$ is classical, the used sorting algorithm is classical.
4) Find z such that $L_{\mathcal{D}}(z) = 1$ using the Grover algorithm with the unitary operator $V_{L_{\mathcal{D}}}$.
5) After computing
$$d = P(z) \oplus P(\overline{z}), \tag{5}$$
find an item x such that
$$d = E_k(x) \oplus E_k(\overline{x}) \tag{6}$$
from the table $\mathcal{T}$.
6) Compute $\hat{k}_1, \hat{k}_2$ as
$$\begin{aligned} \hat{k}_1 &= x \oplus z \\ \hat{k}_2 &= E_k(x) \oplus P(z). \end{aligned}$$
7) Choose $m' \in \{0,1\}^{n/2}$ at random and obtain $E_k(m')$ by making a query to the classical oracle E_k.
8) If $P(m' \oplus \hat{k}_1) \oplus \hat{k}_2 = E_k(m')$, then output $\hat{k}_1, \hat{k}_2$, as k_1, k_2, respectively. Otherwise output
$$\begin{aligned} k_1 &= \overline{x} \oplus z \\ k_2 &= E_k(\overline{x}) \oplus P(z). \end{aligned}$$

B. Analysis of the Algorithm

We justify the output of the above algorithm. Suppose that z in step 4 satisfies $L_{\mathcal{D}}(z) = 1$. We have, for some item x,
$$\begin{aligned} P(z) \oplus P(\overline{z}) &= d \qquad (7) \\ &= E_k(x) \oplus E_k(\overline{x}) \\ &= (P(k_1 \oplus x) \oplus k_2) \oplus (P(k_1 \oplus \overline{x}) \oplus k_2) \\ &= P(k_1 \oplus x) \oplus P(k_1 \oplus \overline{x}). \qquad (8) \end{aligned}$$
If one of the following equations holds, then we can justify the output.
$$z = \begin{cases} k_1 \oplus x \\ k_1 \oplus \overline{x} \end{cases} \tag{9}$$
Although Eq. (8) does not necessarily mean Eq. (9), we show that Eq. (9) holds with reasonable probability when Eq. (8) holds. For a fixed d, the probability that a randomly-chosen z satisfies Eq. (7) is approximately equal to $2/(2^{n/2}-1)$ because $P(z) \oplus P(\overline{z})$ is approximately regarded as a random function from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2} \setminus \{00\ldots0\}$. This means that few values except for Eq. (9) satisfy Eq. (7). Thus, the output of the above algorithm was justified.

This algorithm is probabilistic because z in step 4 is not always correct. If z is not correct, then the algorithm is repeated from the step 4. It is unnecessary to repeat step 2 and step 3.

We determine the value of t to minimize the complexity of this algorithm. First, consider classical complexity. The dominant factor of classical complexity is step 2 and step 3. Step 2 requires $2t$ invocations of E_k and step 3 requires a running time of $O(t \log t)$ to perform a classical sorting algorithm (e.g., a quick sort). Thus, the classical complexity is given by
$$N_c(t) = 2t + O(t \log t). \tag{10}$$
Next, according to the analysis of the Grover algorithm, the quantum complexity of step 4 is
$$N_q(t) = \frac{\pi}{4}\sqrt{\frac{2^{\frac{n}{2}}}{t}}, \tag{11}$$
which maximizes the probability of obtaining the correct z. The optimal value, t_{opt}, of t to minimize Eq. (10) and Eq. (11) is given by
$$t_{opt} = 2^{\frac{n}{6}}.$$
Substituting t_{opt} into Eq. (10) and Eq. (11) yields
$$N_c(t_{opt}) = O(n2^{\frac{n}{6}}), \quad N_q(t_{opt}) = O(2^{\frac{n}{6}}).$$
The proposed algorithm is more efficient than the straightforward Grover algorithm and the classical attack. However, since the complexity is not a polynomial in n, it is intractable to find the key if the key length is large.

V. Concluding Remarks

This paper has shown the polynomial-time quantum algorithm for finding a key of the quantum EM cipher. Our algorithm is theoretically significant because it is the first instance that exploits the internal structure of a classical symmetric cipher to find a key. Our algorithm is more efficient than the algorithm such that the Grover algorithm is straightforwardly applied. Our algorithm is the application of Simon's algorithm in the cryptanalysis. Although Simon's problem looks like an artificial problem, this paper has shown that Simon's problem is closely related to the key-finding problem on the quantum EM cipher. Another application of Simon's algorithm in the cryptanalysis can be found in article [6]. Simon's algorithm is useful to analyze the quantum version of a classical cipher.

This paper mainly focused on so-called query complexity. In order to perform the proposed quantum algorithms, it is necessary to realize unitary operators. This paper does not consider the complexity for realizing unitary operators.

The quantum EM cipher discussed in this paper is a natural extension of the EM cipher. However, our result does not exclude the possibility of other quantum extension of the EM cipher that could be secure even against a quantum adversary.

The EM cipher is considered as the one-round model of AES. The security analysis of the two-round model of AES is an open problem. Similarly, the security of its quantum version is open. It is significant to study the security of the two (or more)-round model of AES in the context of quantum algorithms.

ACKNOWLEDGMENT

The authors thank anonymous reviewers for their valuable comments. This work was partially supported by JSPS KAKENHI Grant Number (22560376).

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers Systems and Signal Processing, pp. 175–179, 1984.
[2] G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," LATIN'98: Theoretical Informatics, Lecture Notes in Computer Science, vol. 1380, pp. 163–169, 1998.
[3] J. Daemen and L. Esat, "Limitations of the Even-Mansour construction," Advances in Cryptology - ASIACRYPT '91, Lecture Notes in Computer Science, vol. 739, pp. 495–498, 1993.
[4] S. Even and Y. Mansour, "A construction of a cipher from a single pseudorandom permutation," Journal of Cryptology, vol. 10, no. 3, pp. 151–161, 1997.
[5] L. K. Grover, "A fast quantum mechanical algorithm for database search," Proceedings of The 28th ACM Symposium on the Theory of Computing, pp. 212–219, 1996.
[6] H. Kuwakado and M. Morii, "Quantum distinguisher between the 3-round Feistel cipher and the random permutation," Proceedings of the 2010 IEEE International Symposium on Information Theory, 2010.
[7] National Institute of Standards and Technology, "Advanced encryption standard (AES)," Federal Information Processing Standards Publication 197, 2001.
[8] D. R. Simon, "On the power of quantum computing," SIAM Journal of Computing, vol. 26, no. 5, pp. 1474–1483, October 1997.