SECURITY ANALYSIS OF GENERALIZED CONFIDENTIAL MODULATION

Hidema Tanaka[1]

[1]Department of Computer Science,
National Defense Academy, Yokosuka, Japan
hidema@nda.ac.jp

ABSTRACT

We propose a new evaluation method for 'generalized confidential modulation (GCM)' for quantum communication. Confidential modulation realizes a secret communication by using secret information for modulation and noise in a channel. Y-00 is one of the famous methods of GCM for quantum communication. The existing evaluation methods for GCM are based on stream ciphers. They can estimate its analytical security and the evaluation depends on the security status of pseudo random number generator (PRNG) which controls the modulation. On the other hand, our method is based on mode of operation for block ciphers and clears the weaknesses from structural viewpoint. Using our method, we can compare the security of different GCM structures. Our method of security evaluation and comparison does not depend on the security status of PRNG. From the results of our evaluation, we conclude that the security of GCM is limited to computational security.

KEYWORDS

Quantum communication, Phase Shift Keying, Stream cipher, Mode of operation, Encryption Oracle

1. INTRODUCTION

'Generalized confidential modulation (GCM)' is a modulation method to realize confidential communication by using random noise on a channel. The sender and receiver treat the modulation parameter as common secret information, e.g., a key. We assume that the eavesdropper can observe any signal on the channel and he knows plaintext (known plaintext attack). The purpose of the eavesdropper is to determine the secret information. Further, we assume that the performances of the eavesdropper's equipment conform to physical laws. Although we can use GCM for any communication channel, in this paper, we focus on the quantum communication. An important characteristic of quantum channels is that their quantum noise cannot be removed. Thus, any error propagates to the eavesdropper as well as the receiver. Y-00 is a famous as GCM using such quantum characteristic [9].

In GCM, the almost secret information is provided as the initial value of pseudo random number generator (PRNG). The given random number sequence controls the modulation. Hence, in the sense of conventional cryptography, GCM can be considered as a symmetric key cipher (stream cipher) and can be evaluated using the analysis methods used for stream ciphers. However, such security evaluations depend on the analysis of PRNG of GCM. We conclude that it is not appropriate to analyze the structural security of GCM by using the analysis methods for stream ciphers.

In this paper, we propose a method for analyzing the structural security of GCM; this method does not depend on the security status of the PRNG. There are many methods of modulation for quantum communication; in this paper, we focus on phase shift keying (PSK) because it is most popular methods. From the viewpoint of conventional cryptography, we see the structure of GCM as mode of operation for block cipher. Therefore, we propose an evaluation method developing the following methods for mode of operation for block ciphers: Real_or_Random, Left_or_Right and Find_then_Guess. Our evaluation method enables the comparison among different structures of GCM from the viewpoint of security, effectiveness and implementation performance.

2. GENERALIZED CONFIDENTIAL MODULATION

2.1. Structure and modulation

Figure 1 shows the structure of generalized confidential modulation (GCM) and Table 1 shows the notations. Alice and Bob use the same Modu/DEM and PRNG with the same secret initial value (secret key).

First of all, we show the mechanism of modulation. The basic mechanism underlying GCM is phase shift keying (PSK). PSK is a modulation method to be expressible multi value by one signal. Therefore, it is an appropriate modulation method for broadband communication systems. The details of PSK are shown in [3]. PSK uses $2S$ kinds of signal waves with phase shifted of $n\pi/S$, ($n = 0 \sim 2S\text{-}1$). Let bi be a i-th signal wave whose phase shift is $i\pi/S$. Between bi and $bi+S$, the phase difference is π, thus the waveform is upside down in each other. We give each signal wave bi 'signal value'. How to give signal value can be considered various methods. In this paper, we use the following Yuen's techniques to make discussions simple [9]. Let $< bi > \in \{0, 1\}$ be signal value of bi : for $i = 0\sim S\text{-}1$, $< bi >= 0$ when $i =$even, $< bi >= 1$ when $i =$odd, and $< bi+S >=< bi > \wedge 1$. We call such 'how to give signal value' a signal table. In some cases of GCM, the signal table comprises secret information shared between Alice and Bob [4]. In this paper, we assume that signal table is open to public. In the sense of modern symmetric cipher, this condition is same that the algorithm of encryption function is open to public. A heterodyne detection can express the resultant of modulation by PSK on a phase space as shown in Figure 2(a). Each signal value is a point arranged at equal intervals on the circumference whose semi diameter is amplitude of signal wave. We can use QAM (Quadrature Amplitude Modulation) which uses both shift and amplitude of signal wave [4], in this paper we omit GCM using QAM. But the analysis of security of GCM using QAM is basically same results that we show below. If Bob knows the value of i which Alice used, the message of Alice can recognize '0' or '1' by Bob's measurement of the presence or absence of the signal bi by homodyne detection. The signal transmission repeats following procedure number of times which equals to the length of a message.

(1) Generate $|S|$ [bit] random number r.
(2) Choose wave br or $br+S$ according to the value of message 0 or 1.

According to the procedure, Alice sends a signal to Bob. Bob measures the signal; since there is un-removable quantum noise in the signal (see Figure 2.(b)), he gets s candidates of the signal, such as $\{bj , bj+1, ..., bj+s\text{-}1\}$, ($j \leqq r \leqq j + s\text{-} 1$). In this paper, we assume that the probability of correct signal br is equal for all candidates
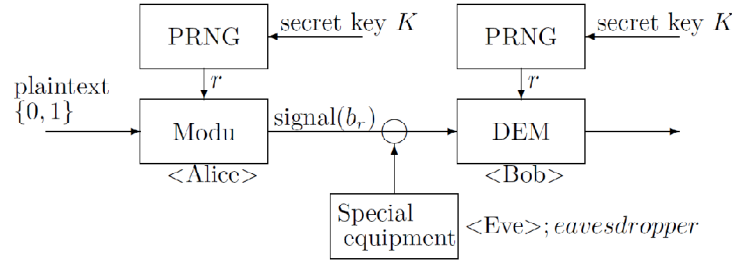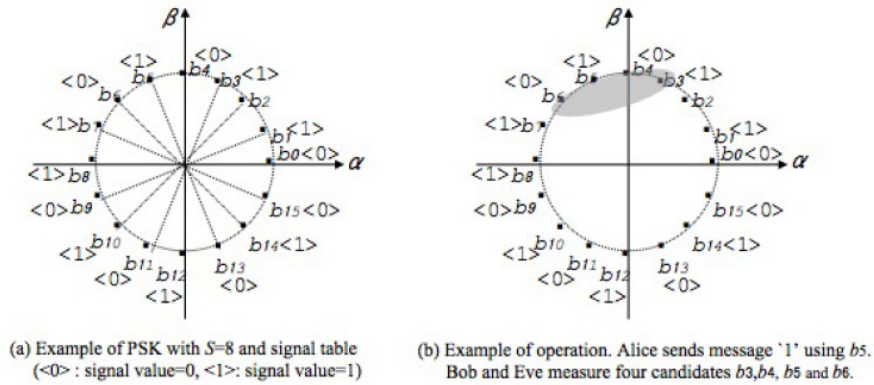
Figure 1. Framework of generalized confidential modulation

(a) Example of PSK with $S=8$ and signal table
($<0>$: signal value=0, $<1>$: signal value=1)

(b) Example of operation. Alice sends message `1' using $b5$.
Bob and Eve measure four candidates $b3, b4, b5$ and $b6$.

Figure 2. Example of measurement and demodulation of PSK on phase space. ($\alpha+i\beta$ where i denotes imaginary number)

$$\text{Prob}\{br = bi\} = \frac{1}{s}, \quad i = j \sim j + s - 1. \tag{2.1}$$

Since Bob knows the value of *r*, he can determine the true value of the signal (0 or 1) from the error in the measurement. On the other hands, the eavesdropper Eve must distinguish the true value from among $\{bj , bj+1, ..., bj+s-1\}$. From eq.(2.1), the probability that Eve successfully distinguishes the true value is $1/s$. Thus, if the purpose of Eve's attack is to determine the secret key, she must determine the true signal at first. GCM makes it difficult for Eve to determine the true signal; hence, when using the same PRNG, GCM can be considered to be more secure than a general communication channel using the conventional information security technologies such as stream cipher.

Table 1. Notations 1

Alice	Sender
Bob	Receiver
Eve	Eavesdropper, Malicious Bob
S	Number of signal waves for PSK
s	Number of candidates for the true signal by the measurement
e	Error rate $e = s/S$
PRNG	Pseudo random number generator whose structure is open to public, output size is m[bit] $(m \geqq 1)$
K	Initial value of PRNG, secret key
Modu/DEM	Modulator/demodulator whose structure is open to public
|*X*| [bit]	Length of binary expression of *X*

2.2. Quantum measurement and error rate

The assumption of the effectiveness of quantum measurement is one of the most important issues. In particular, the effectiveness of quantum detection influences the feasibility of attack scenario. The positive operator valued measure (POVM) is the most general formulation of a measurement in the theory of quantum physics [3] [8]. Although the optimization of POVM and minimization of its error rate have been derived theoretically, such measurement methods and equipment are yet to be realized. In this paper, we assume that the eavesdropper uses optimized equipment. Hence, the specification of her measurement is ambiguous and the results can only be calculated theoretically.

As shown in eq.(2.1), we assume that it is probable for all the candidates to receive the correct signal. In the actual measurement, however, biases are caused in the aforementioned probability. We can consider that the probability of Eve distinguishing the correct signal by using this bias is more advantageous than the probability of our assumption. However, when the size of S is huge, it is not possible to determine the candidate who receives the correct signal even when using such bias. Hence, we consider that the total number of candidates s is equal to the number of resultant candidates after distinguish using such bias.

In this paper, we use a simple quantum measurement model comprising certain parameters. When the effectiveness of the actual measurement is known, we will be able to estimate the actual performance of eavesdropper by using our model.

3. SCENARIOS OF SECURITY ANALYSIS

There are two scenarios for the security analysis of GCM.

1.　Eve observes the channel: on the basis of this assumption, we estimate her computational cost and amount of data (number plaintext-cipher text pairs) to determine the secret key.

2.　'Malicious Bob (Eve)' can obtain the cipher texts for his chosen plaintexts from Alice. In the scenario, we assume that although Eve does not know the key, Alice authenticates Eve (impersonation attack).

In the scenario 1, the goal of the attack is to ensure that the estimated cost becomes lesser than that estimated when using brute force search for obtaining the secret key. Many previous results are based on scenario 1. In scenario 2, we assume that the security of the PRNG is optimum, and hence, we assume that brute force search for the attack is feasible. Ideal security in scenario 2 refers to security against the leaking of information of the secret key to Eve, who can execute a brute force search.

By making estimations on the basis of the above mentioned attack scenarios, we can derive following security results for GCM. From the scenario 1, we have followings:

1-1. Estimation of the upper bound of the security of the GCM by using a specific PRNG.
1-2. Comparison of security among different GCMs by using the same PRNG. The GCM for which the cost estimated for making an attack is the highest is expected to be the most secure.

From the scenario 2, we have followings:

2-1. Estimation of the structural security which does not depends on the security status of PRNG.
2-2. Comparisons of security among the structures that are categorized as GCM.

In the followings, evaluation performed according to scenario 1 is referred to as analytical evaluation, and that performed according to scenario 2 is referred as structural evaluation. As mentioned above, GCM is categorized as a symmetric cipher in the sense of conventional cryptography. As a result, we conclude that it is appropriate to apply the aforementioned evaluation methods as follows.

- Analytical evaluation $\leftarrow$ evaluation method for stream ciphers
- Structural evaluation $\leftarrow$ evaluation method for mode of operation

4. ANALYTICAL EVALUATION

Most of the results of analytical evaluation can be found in previous works. In this section, we categorize and summarize previously mentioned results. Table 2 shows the notations.

We refer to the most effective attack method for using the PRNG in GCM as Algorithm A. Let Π and N be the necessary computational cost and length of the random sequence generated by PRNG, respectively, for determination of the initial value by Algorithm A. The measurement cannot remove the noise in the quantum channel. Thus, Eve gets the output with an error probability ε. The following two attack strategies are proposed.

(1) By using only N of data, apply error correction to get the true output. In this case, the computational cost increases.

(2) Using data of length greater than N, sieve the candidates of initial values. In this case, both the computational cost and data length increase.

Let $R_N(e)$ be an error correction function for a sequence with length N and error rate e. We denote e_c as the successful correction of $R_N(e)$. The necessary computational cost for (1) becomes $O(R_N(e)) \Pi$, and the probability of a successful attack becomes e_c. The value of e_c is lesser than or equals to the probability of successful attack by Algorithm A.

Let $C(e)$, (< 1) be the channel capacity of the binary symmetric channel with an error rate e. The necessary length of the output for (2) becomes $N/C(e)$. The probability of a successful attack is equals to the probability of successful attack by Algorithm A and the computational cost becomes $\Pi/C(e)$.

Because of limited space, we omit the details of estimation of the above mentioned necessary costs. The detailed analysis and estimation are shown in [2], [7], [6], [10] and so on. In many cases, the attack by Algorithm A is either a correlation attack or a fast correlation attack, and the target PRNG is an M sequence generator. From these results of attacks, we expect that GCM for which the cost estimated for making an attack is the highest to be the most secure.

5. STRUCTUAL EVALUATION

5.1. Characteristic of PSK

In this section, we assume that the security of PRNG is optimum, and hence, no attack method other than brute force search can be used for obtaining the secret key. Thus, we need to account for the use of brute force search and estimate the necessary length of the output to execute brute force search.

Because the secret key K is a $|K|$ [bit] unknown value, there are $2^{|K|}$ secret key candidates. The modulator has substantially S kinds of waves, and we can refer to the modulation as a $2^{|K|} \rightarrow 2^{|S|}$ function. From a single modulator output, we get s kinds of candidates (see section 2.1). Therefore, we can derive $2^{|K|} s/S$ secret key candidates in a single measurement.

Table 2. Notations 2

Algorithm A	Most effective attack method for the PRNG used in GCM
N	Necessary length of sequence for Algorithm A
Π	Necessary computational cost for Algorithm A
ε	correct measurement probability for the true signal $\varepsilon = 1/s$

Since the PRNG uses a deterministic algorithm, there exists a correlation between the random sequences. Hence, the number of secret key candidates who do not contradict the results of the continuous measurement is limited. Let t be the number of measurements. We can determine the secret key using t that holds

$$\left(\frac{s}{S}\right)^t \leq \frac{1}{2^{|K|}} \tag{5.1}$$

From this result, we can derive Proposition 1.

Proposition1: *Let S be the number of waves of PSK in GCM, and s be the number of candidates who obtained the true signal in a single measurement. If the size of the secret parameter is n [bit], we can determine the secret value in t times of continuous measurements.*

Algorithm A	Most effective attack method for the PRNG used in GCM
N	Necessary length of sequence for Algorithm A
Π	Necessary computational cost for Algorithm A
ε	correct measurement probability for the true signal $\varepsilon = 1/s$
Algorithm A	Most effective attack method for the PRNG used in GCM
N	Necessary length of sequence for Algorithm A
Π	Necessary computational cost for Algorithm A
ε	correct measurement probability for the true signal $\varepsilon = 1/s$
Algorithm A	Most effective attack method for the PRNG used in GCM
N	Necessary length of sequence for Algorithm A
Π	Necessary computational cost for Algorithm A
ε	correct measurement probability for the true signal $\varepsilon = 1/s$

$$\left(\frac{s}{S}\right)^t \leq \frac{1}{2^{|K|}}$$

In other words, if we can execute brute force search, we can determine the secret key in t times of continuous measurements.
Proof. Trivial

□

Example: In the case of a GCM with a 128[bit] secret key and 64 values PSK, Eve can determine the secret key using 32 times of continuous measurements via a brute force search if she has equipment with $s = 4$.

$$\left(\frac{4}{64}\right)^t \leq \frac{1}{2^{128}} \quad \rightarrow \quad t = 32$$

Note that the computational cost is $O(2^{128})$.

□

From Proposition 1, we can determine the number of measurements (or necessary length of output) necessary for executing brute force search for obtaining the secret key.

5.2. Real_or_Random

Table 3 shows the notations. 'Real_or_Random' is one of the evaluation methods for mode of operation M [1], [5]. The purpose of Eve is to construct a distinguisher A that can distinguish between the following two with a probability $1/2 +\varepsilon$:

- Cipher text for the plaintext, generated by Eve.
- Cipher text for the random number whose size is equal to Eve's plaintext. The random number is chosen using an encryption oracle.

Table3. Notations 3

E	Encryption oracle
P	Pseudo random oracle
m	Message or query to oracle
q	Number of query for oracle
μ [bit]	length of query
$(\cdot)$	Random function whose output size is equals to the size of m
A	Distinguisher whose output is 1 or 0

Note that Eve does not know the secret key. The procedure for Real_or_Random is as follows.

[Step-1] The encryption oracle E randomly chooses the secret key K.
[Step-2] Eve sends encryption oracle E message m as query.
[Step-3] E generates 1[bit] random number b. If $b = 0$ it makes the cipher text $E_K(m)$ according to mode M, else it makes $E_K(\$(\cdot))$ in the same way (where $\$(\cdot)$ is random function). E sends Eve resultant cipher text as c.
[Step-4] Eve uses a distinguisher A. If the distinguisher A judges $c = E_K(m)$, it outputs '1' else it outputs '0'.

Eve repeats above procedure q times with μ [bit] of message. Then, we calculate the advantage as follows:
$$\text{Adv}_A^{rr} = \text{Prob}[a \leftarrow K : A^{E_a(\cdot)} = 1] - \text{Prob}[a \leftarrow K : A^{E_a(\$(\cdot))} = 1] \tag{5.2}$$
If Eve can construct a distinguisher A that holds $\text{Adv}^{rr}_A \geqq \epsilon$, the mode of operation M is not secure against Real_or_Random. Note that the encryption oracle E has ideal security.

In the case of GCM, we use a pseudo random oracle P instead of the encryption oracle E. Moreover, the output is generated in moderation manner instead of mode of operation. The pseudo random oracle P is an ideal secure PRNG; moreover, it is a deterministic algorithm. Therefore, the advantage is calculated as follows:
$$\text{Adv}_A^{rr} = \text{Prob}[a \leftarrow K : A^{P_a(\cdot)} = 1] - \text{Prob}[a \leftarrow K : A^{P_a(\$(\cdot))} = 1] \tag{5.3}$$

We analyze the security of GCM against Real or Random. From Proposition 1, Eve can distinguish by sending a query t times and the length of message (length of query) is 1[bit]. Thus, it is obvious that
$$\text{Adv}_A^{rr} \geq \epsilon \tag{5.4}$$

We conclude that GCM is not secure against Real or Random. However, if the number of times of 1 [bit] encryption with the same key is less than t, GCM has enough Real or Random security. This is the security requirement for GCM.

5.3. Right_or_Left

Table 3 shows the notations. 'Real_or_Random' is one of the evaluation methods for mode of operation M [1], [5]. The purpose of Eve is to construct a distinguisher A that can distinguish between the following two with a probability $1/2 +\varepsilon$:

- Cipher text for the plaintext m_1, generated by Eve.
- Cipher text for the plaintext m_2, generated by Eve.

Note that Eve does not know the secret key. The evaluation procedure of Right_or_Left is as follows.

[Step-1] The encryption oracle E randomly chooses the secret key K.
[Step-2] Eve sends encryption oracle E message m_1 and m_2 as query.
[Step-3] E generates 1[bit] random number b. If $b = 0$ it makes the cipher text $E_K(m_1)$ according to mode M, else it makes $E_K(m_2)$ in the same way. E sends Eve resultant cipher text as c.
[Step-4] Eve uses a distinguisher A. If the distinguisher A judges $c = E_K(m_1)$, it outputs '1' else it outputs '0'.

Eve repeats above procedure q times with μ [bit] of message. Then, we calculate the advantage as follows:
$$\text{Adv}_A^{rl} = \text{Prob}[a \leftarrow K: A^{Ea(m_1)} = 1] - \text{Prob}[a \leftarrow K: A^{Ea(m_2)} = 1] \qquad (5.5)$$
If Eve can construct a distinguisher A that holds $\text{Adv}^{rl}{}_A \geqq \epsilon$, the mode of operation M is not secure against Rightl_or_Left. Note that the encryption oracle E has ideal security.

In the case of GCM, we use a pseudo random oracle P instead of the encryption oracle E. Moreover, the output is generated in moderation manner instead of mode of operation. The pseudo random oracle P is an ideal secure PRNG; moreover, it is a deterministic algorithm.

Therefore, the advantage is calculated as follows:
$$\text{Adv}_A^{rl} = \text{Prob}[a \leftarrow K: A^{Pa(m_1)} = 1] - \text{Prob}[a \leftarrow K: A^{Pa(m_2)} = 1] \qquad (5.6)$$

We analyze the security of GCM against Right_of_ Left. From Proposition 1, Eve can distinguish by t [bit] length of message (or query), and the number of queries is 1. Thus it is obvious that
$$\text{Adv}_A^{rl} \geq \epsilon \qquad (5.7)$$
We conclude that GCM is not secure against Right or Left. However, if the length of the message for encryption with the same key is less than t, GCM has enough Right or Left security. This is the security requirement for GCM or an improvement of its security.

Comparison of the result of Right or Left with that of Real or Random shows that both the results are derived from Proposition 1. The structure of GCM outputs one bit at a time. Therefore the number of operations is equals to the length of the message. Hence, both the results are essentially equivalent in the case of GCM.

5.4. Find_then_Guess

'Find then Guess' is one of the evaluation methods for mode of operation M from the view point of polynomial security [1], [5]. Although evaluation method Find then Guess and Right or Left are basically similar, the distinguishing feature of the former is that Eve can use the knowledge when she executes the distinguisher A. Therefore, Eve is at an advantage. The evaluation procedure of Find then Guess is as follows:
<Find stage>

[Step-1] The encryption oracle E randomly chooses the secret key K.

[Step-2] Eve sends encryption oracle E message m_1 and m_2 as queries and analyze m_1 and m_2 to store the knowledge k. Eve then uses the knowledge k to distinguish the cipher text of m_1 and m_2. <Guess stage>

[Step-3] E generates 1[bit] random number b. If $b = 0$ it makes the cipher text $E_K(m_1)$ according to mode M, else it makes $E_K(m_2)$ in the same way. E sends Eve the resultant cipher text as c.

[Step-4] Eve uses a distinguisher A with knowledge k. If the distinguisher A judges $c = E_K(m_1)$, it outputs '1' else it outputs '0'.

In the case of GCM, we use the pseudo random oracle P instead of the encryption oracle E. The output is generated in moderation manner instead of mode of operation. The pseudo random oracle P is an ideal secure PRNG and it is a deterministic algorithm. Therefore, its advantage is calculated as follows.

$$\mathrm{Adv}_A^{fg} =$$
$$2 \times \mathrm{Prob}\left[a \leftarrow K: (m_1, m_2, k) \leftarrow A^{P_a(\cdot)}(\mathrm{Find}); \; b \leftarrow \{1,2\}; \; c \leftarrow P_a(m_b): A^{P_a(\cdot)}(\mathrm{Guess}, c, k)\right]\text{-}1$$
$$(5.6)$$

If Eve can construct a distinguisher A that holds $\mathrm{Adv}^{fg}{}_A \geqq \epsilon$, the structure of GCM is not secure against Find_then_Guess.

Find then Guess is a weak version of Right or Left in the sense that Eve is at a greater advantage in the former than in the latter. As shown in Section 5.3, if GCM is not secure against Right or Left, it is not practical to adapt Find_then_Guess. Hence, we analyze the GCM whose message length is less than t. Eve uses the information of known plaintexts to measure the output from the modulator and to obtain the random number candidates generated by PRNG. However plaintexts do not influence the resultant outputs from the modulator; the PRNG alone determines the resultant outputs. Therefore, Eve cannot obtain any useful knowledge from the choice of messages. In addition, since the length of the message is less than t, Eve cannot determine the secret key using Proposition 1. Since Eve cannot decrypt c, she cannot distinguish them. As a result, such an improved GCM is secure against Find then Guess.

6. DISCUSSIONS

From the results shown in section 4, the analytical security depends on the choice of PRNG. The condition for attack requires an effective attack method for the target PRNG. If such an effective attack method is not found, it can be concluded that GCM has sufficient analytical security. For example, an effective attack method against AES has not yet been developed. So, if AES is used as the PRNG, we can conclude that any GCM will be analytically secure. Hence, we cannot compare the effectiveness of different structures of GCM from the viewpoint of security. Nevertheless, from these results, practical security can be realized in realistic scenarios. It shall serve as the criteria for choosing the appropriate PRNG.

From the results shown in section 5, we can conclude that the structural security of GCM is limited to computational security. For ideal structural security, it is necessary to achieve A that holds $\mathrm{Adv}_A < \epsilon$ with $q \to \infty$ and $\mu \to \infty$ under the condition that brute force search is executable for obtaining the secret key. Unfortunately, GCM is attackable when $(q \to t, \mu \to 1)$ or $(q \to 1, \mu \to t)$; hence, GCM is not sufficiently secure. Note that this conclusion does not imply that GCM is not realistic secure, but it implies that the basic structure of the GCM is not information

theoretic secure. Therefore, we can conclude that improvement of structural security is important and necessary.

'Semantics' is an important evaluation method for mode of operation. The original semantics is evaluation method for asymmetric key ciphers [6]. For a cryptosystem to be semantically secure, information on the plaintext should not be leaked when the corresponding cipher text and public key are provided. In the case of mode of operation, semantics means that Eve cannot expect to obtain the cipher text corresponding to the plaintext without knowing the secret key. As shown in section 5, our method only evaluates the security of the secret key and does not evaluate the security of the GCM output. The output is secure if information on the plaintext is not leaked. The reason we do not adapt semantics is that the GCM outputs are measured using the information on known plaintexts, and such information does not influence the generation of the output. This is obvious from the function of modulation and Proposition 1. On the other hand, if the GCM has some output function, semantics would be an important evaluation method. For example, we expect that the use of an effective output function leads to privacy amplification.

7. CONCLUSION

In this paper, we define GCM and evaluate its security in the case of quantum communication. We propose a new evaluation method from the viewpoint of mode of operation. Using our method, we can determine the requirements for achieving a GCM with better structural security and compare the security of different GCM structures. Since the results of our method do not depend on the security status of the PRNG, it is possible to develop structurally secure design approach. In section 5, we show the security evaluation of GCM. From the results, we find that a structurally secure GCM needs to have some auxiliary functions to have correlation immunity of output from modulator. We also expect privacy amplification to be one of the strategies for the improvement of GCM. By using privacy amplification, GCM will be able to have information theoretic security. As a result, the following can be realized:

- Information theoretic security against attacks by using brute force search
- Semantic security

These security functions are expected to new GCM. We expect to realize GCM with the abovementioned security features. Further, security requirements for the PRNG can be determined from our evaluation method. The results of evaluation show the necessary key updating period. The maximum length of the message that can be sent in the same secret key and the requirement for secure operation can also be determined by using the proposed evaluation method.

In our future work, we intend to identify the most effective auxiliary function for realizing GCM with information theoretic security. In our next research, we shall analyze and compare the security of existing GCMs.

REFERENCES

[1]   M.Bellare, A.Desai, E.Jokipii & P.Rogaway, "A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation",Proceedings of 38th Annual Symposium on Foundations of Computer Science(FOCS 97),pp. 394-403, IEEE Press, 1997.

[2]   S.Donnet, A.Thangaraj, M.Bloch, J.Cussey, J.M.Merolla and L.Larger,"Security of Y-00 under heterodyne measurement and fast correlation attack",Physics letters A, vol. 356, no.6, 2006, pp. 406-410

[3]   V.Giovannetti, S.Guha, S.Lloyd, L.Maccone, J.H.Shapiro, and H.P.Yuen,"Classical capacity of the lossy bosonic channel: The exact solution",Physical Review Letter 90, 027902, 2004

[4]   O.Hirota and K.Kurosawa, "Immunity against Correlation Attack on Quantum Stream Cipher by Yuen2000 Protocol,Quantum Information Processing, Vol.6, No.2, April 2007 pp.81–91

[5]   ISO/IEC 10116, "Information Technology - Security techniques - Mode of operation for an n-bit block cipher algorithm", 2002-6-26

[6]   M. Mihaljevic, "Generic framework for secure Yuan 2000 quantum encryption protocol employing the wire-tap channel approach", Physical Review A, vol. 75, no. 5, May 2007, pp. 052334-1-5

[7]   T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku and H. Imai, "How much security does Y-00 protocol provide us?," Physical Letters A 327 (2004) 28- 32; quant-ph/0310168.

[8]   J.Preskill, "Lecture note for Physics: Quantum Information and Computation",http://theory.caltech.edu/people/preskill

[9]   H.P.Yuen, "KCQ: A new approach to quantum cryptography I.", General principles and qumode key generation, quant-ph/0311061

[10] H.P.Yuen and R.Naira, "On the security of Y-00 under fast correlation and other attacks on the key", Physics Letters A Volume 364, Issue 2, 23 April 2007, pp. 112–116