SECURITY ANALYSIS OF GENERALIZED CONFIDENTIALMODULATION FOR QUANTUM COMMUNICATION

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 modulationrealizes a secret communication by using secret information for modulationand noise in a channel. Y-00 is one of the famous methods of GCM forquantum communication. The existing evaluation methods for GCM arebased on stream ciphers. They can estimate its analytical security andthe evaluation depends on the security status of pseudo random numbergenerator (PRNG) which controls the modulation. On the other hand,our method is based on mode of operation for block ciphers and clears theweaknesses from structural viewpoint. Using our method, we can comparethe security of different GCM structures. Our method of security evaluationand comparison does not depend on the security status of PRNG.From the results of our evaluation, we conclude that the security of GCMis 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 realizeconfidential communication by using random noise on a channel. The senderand receiver treat the modulation parameter as common secret information,e.g., a key. We assume that the eavesdropper can observe any signal on thechannel and he knows plaintext (known plaintext attack). The purpose of theeavesdropper is to determine the secret information. Further, we assume thatthe performances of the eavesdropper's equipment conform to physical laws.Although we can use GCM for any communication channel, in this paper, wefocus on the quantum communication. An important characteristic of quantumchannels is that their quantum noise cannot be removed. Thus, any errorpropagates to the eavesdropper as well as the receiver. Y-00 is a famous asGCM using such quantum characteristic [16].

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

In this paper, we propose a method for analyzing the structural securityof GCM; this method does not depend on the security status of the PRNG.There are many methods of modulation for

DOI : 10.5121/ijcnc.2013.5509

quantum communication; in thispaper, we focus on phase shift keying (PSK) because it is most popular methods.From the viewpoint of conventional cryptography, we see the structure ofGCM as mode of operation for block cipher. Therefore, we propose an evaluationmethod developing the following methods for mode of operation for blockciphers: Real_or_Random, Left_or_Right and Find_then_Guess. Our evaluation method enables the comparison among different structures of GCM from theview point 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) andTable 1 shows the notations. Alice and Bob use the same Modu/DEM andPRNG with the same secret initial value (secret key).

First of all, we show the mechanism of modulation. The basic mechanismunderlying GCM is phase shift keying (PSK). PSK is a modulation methodto be expressible multi value by one signal. Therefore, it is an appropriatemodulation method for broadband communication systems. The details of PSKare shown in [5]. PSK uses $2S$ kinds of signal waves with phase shifted of$n\pi/S$,(n = 0~$2S$-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 downin each other. We give each signal wave bi 'signal value'. How to give signal valuecan be considered various methods. In this paper, we use the following Yuen'stechniques to make discussions simple [16].Let $< bi > \in \{0, 1\}$be signal valueof bi : for i= 0~S-1, $< bi >= 0$ when i=even, $< bi >= 1$ when i=odd,and $<bi+S>=< bi >$^ 1. We call such 'how to give signal value' a signaltable. In some cases of GCM, the signal table comprises secret informationshared between Alice and Bob [7]. In this paper, we assume that signal tableis open to public. In the sense of modern symmetric cipher, this condition issame that the algorithm of encryption function is open to public. A heterodynedetection can express the resultant of modulation by PSK on a phase space asshown in Figure 2(a). Each signal value is a point arranged at equal intervalson the circumference whose semi diameter is amplitude of signal wave. Wecan use QAM (Quadrature Amplitude Modulation) which uses both shift andamplitude of signal wave [7], in this paper we omit GCM using QAM. But theanalysis of security of GCM using QAM is basically same results that we showbelow. If Bob knows the value of $i$which Alice used, the message of Alice canrecognize '0' or '1' by Bob's measurement of the presence or absence of the signalbi by homodyne detection. The signal transmission repeats following procedurenumber of times which equals to the length of a message.

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

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

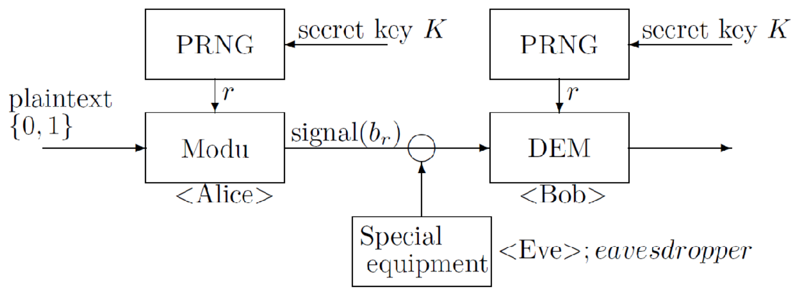

Figure 1. Framework of generalized confidential modulation

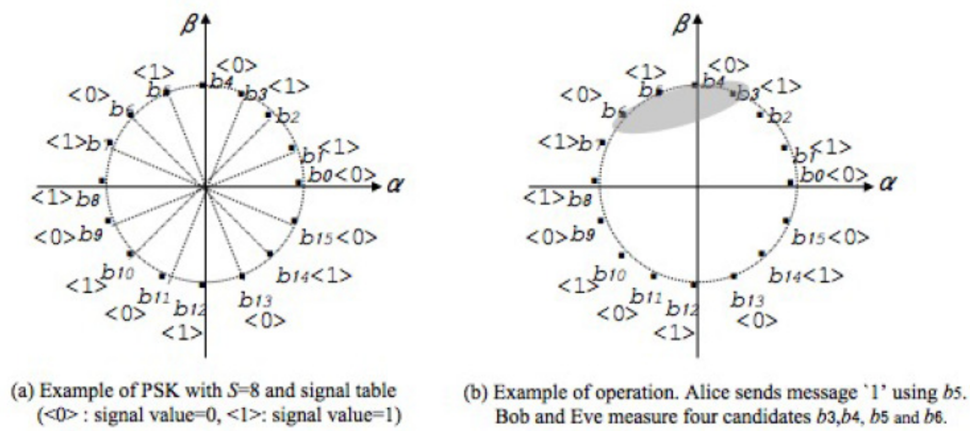

Figure 2.Example of measurement and demodulation of PSK on phase space. (α +i β where i denotes imaginary number)

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

Since Bob knows the value of *r*, he can determine the true value of the signal (0or 1) from the error in the measurement. On the other hands, the eavesdropperEve must distinguish the true value from among $\{bj\ ,\ bj{+}1,\ ....,\ bj{+}s{-}1\}$. Fromeq.(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, shemust determine the true signal at first. GCM makes it difficult for Eve todetermine the true signal; hence, when using the same PRNG, GCM can beconsidered to be more secure than a general communication channel using theconventional 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 opento 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. Pseudo Random Number Generator

Pseudo random number generator (PRNG) is a deterministic algorithm thatgenerates a statistical random sequence. For a PRNG to be used as a streamcipher or information security system, the following conditions must be satisfied:

- The periodicity should be long.
- Its linear complexity should be high.
- It should have good statistical characteristics.
- It should have high non-linearity.
- It should have high correlation immunity.

In addition, PRNG should be secure against general attacking methods suchas correlation attack, generalized correlation attack, algebraic attack and soon. For example, an M-sequence generator comprising a linear feedback shiftregister (LFSR) has good statistical characteristics but is not secure against anyattack algorithm. Therefore, an LFSR alone should not be used as the PRNGfor GCM.

Almost secure PRNGs are provided as a stream cipher, counter mode (CTR)of block cipher, algorithm based on hash function and so on. The standardstream ciphers are listed in eSTREAM project [3], CRYPTREC [2] and ISO [9].Many PRNGs can be obtained from these lists. The securities of these PRNGsare evaluated in each of the above mentioned projects. CTR is a standard modeof operation in FIPS [13] and ISO [8]. AES used by CTR (in following, 'AES'implies 'AES used by CTR') seems to be widely used. FIPS and ISO makePRNG based on hash function SHA-1 to be standard PRNG [12]. For GCM, itis necessary to choose a PRNG that is effective from the viewpoints of securityand implementation.

2.3. Quantum Measurement and Error Rate

The assumption of the effectiveness of quantum measurement is one of the mostimportant issues. In particular, the effectiveness of quantum detection influencesthe feasibility of attack scenario. The positive operator valued measure(POVM) is the most general formulation of a measurement in the theory ofquantum physics [5] [14]. Although the optimization of POVM and minimizationof its error rate have been derived theoretically, such measurement methodsand equipment are yet to be realized. In this paper, we assume that the eavesdropperuses optimized equipment. Hence, the specification of her measurementis ambiguous and the results can only be calculated theoretically.

As shown in eq.(2.1), we assume that it is probable for all the candidatesto receive the correct signal. In the actual measurement, however, biases arecaused in the aforementioned probability. We can consider that the probabilityof Eve distinguishing the correct signal by using this bias is more advantageousthan the probability of our assumption. However, when the size of S is huge, itis not possible to determine the candidate who receives the correct signal evenwhen 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 comprisingcertain parameters. When the effectiveness of the actual measurement is known,we will be able to estimate the actual performance of eavesdropper by using ourmodel.

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 estimateher computational cost and amount of data (number plaintext-ciphertextpairs) to determine the secret key.
2. 'Malicious Bob (Eve)' can obtain the ciphertexts for his chosen plaintextsfrom Alice. In the scenario, we assume that although Eve does not knowthe key, Alice authenticates Eve (impersonation attack).

In the scenario 1, the goal of the attack is to ensure that the estimated costbecomes lesser than that estimated when using brute force search for obtainingthe 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 assumethat 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 havefollowings:

1-1. Estimation of the upper bound of the security of the GCM by using aspecific 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 highestis 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 thesecurity status ofPRNG.
2-2. Comparisons of security among the structures that are categorized asGCM.

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

- Analytical evaluation←evaluation method for stream ciphers
- Structural evaluation ←evaluation method for mode of operation

4. ANALYTICAL EVALUATION

Most of the results of analytical evaluation can be found in previous works. Inthis section, we categorize and summarize previously mentioned results. Table2 shows the notations.

We refer to the most effective attack method for using the PRNG in GCMas Algorithm A. Let Π and N be the necessary computational cost and lengthof the random sequence generated by PRNG, respectively, for determination ofthe initial value by Algorithm A. The measurement cannot remove the noise inthe 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. Inthis 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 $R_N(e)$. Thenecessary computational cost for (1) becomes $O(R_N(e))\ \Pi$, and the probabilityof a successful attack becomes e_c. The value of $e_c$is lesser than or equals to theprobability of successful attack by Algorithm A.

Let $C(e)$, (<1) be the channel capacity of the binary symmetric channel withan 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 successfulattack by Algorithm A and the computational cost becomes $\Pi/C(e)$.

Because of limited space, we omit the details of estimation of the abovementioned necessary costs. The detailed analysis and estimation are shown in[4], [11], [10], [17] and so on. In many cases, the attack by Algorithm A is eithera correlation attack or a fast correlation attack, and the target PRNG is anM sequence generator. From these results of attacks, we expect that GCM forwhich the cost estimated for making an attack is the highest to be the mostsecure.

5. STRUCTUAL EVALUATION

5.1. Characteristic of PSK

In this section, we assume that the security of PRNG is optimum, and hence, noattack method other than brute force search can be used for obtaining the secretkey. Thus, we need to account for the use of brute force search and estimatethe necessary length of the output to execute brute force search.

Because the secret key K is a $|K|$ [bit] unknown value, there are $2^{|K|}$secretkey candidates. The modulator has substantially S kinds of waves, and we canrefer to the modulation as a $2^{|K|}\rightarrow 2^{|S|}$function. From a single modulatoroutput, 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 correlationbetween the random sequences. Hence, the number of secret key candidates whodo 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 thatholds

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

From this result, we can derive Proposition 1.

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

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

In other words, if we can execute brute force search, we can determine the secretkey 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 measurementsvia 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 necessarylength of output) necessary for executing brute force search for obtainingthe secret key.

5.2. Real_or_Random

Table 3 shows the notations. 'Real_or_Random'is one of the evaluation methodsfor mode of operation M[1], [8], [15]. The purpose of Eve is to construct adistinguisher A that can distinguish between the following two with a probability $1/2 + \varepsilon$:

- Ciphertext for the plaintext, generated by Eve.

- Ciphertext 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
\$(・)	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_Randomis 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 ciphertext$E_K(m)$ according to mode *M*, else it makes E_K(\$(・)) in the same way(where \$(・) is random function). *E*sends Eve resultant ciphertext 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 calculatethe advantage as follows:

$$\mathrm{Adv}_A^{rr} = \mathrm{Prob}\left[a \leftarrow K\colon A^{E_a(\cdot)} = 1\right] - \mathrm{Prob}\left[a \leftarrow K\colon A^{E_a(\$(\cdot))} = 1\right] \qquad (5.2)$$

If Eve can construct a distinguisher *A* that holds $\mathrm{Adv}^{rr}{}_A \geqq$□, the mode ofoperation *M* is not secure against Real_or_Random. Note that the encryptionoracle *E* has ideal security.

In the case of GCM, we use a pseudo random oracle *P* instead of the encryptionoracle *E*. Moreover, the output is generated in moderation manner insteadof mode of operation. The pseudo random oracle *P* is an ideal secure PRNG;moreover, it is a deterministic algorithm. Therefore, the advantage is calculatedas follows:

$$\mathrm{Adv}_A^{rr} = \mathrm{Prob}\left[a \leftarrow K\colon A^{P_a(\cdot)} = 1\right] - \mathrm{Prob}\left[a \leftarrow K\colon A^{P_a(\$(\cdot))} = 1\right] \qquad (5.3)$$

We analyze the security of GCM against Real or Random. From Proposition1, 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

$$\mathrm{Adv}_A^{rr} \geq \epsilon(5.4)$$

We conclude that GCM is not secure against Real or Random. However, if thenumber of times of 1 [bit] encryption with the same key is less than *t*, GCM hasenough 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 methodsfor mode of operation *M* [1], [8], [15]. The purpose of Eve is to construct adistinguisher *A* that can distinguish between the following two with a probability $1/2 + \varepsilon$:

- Ciphertext for the plaintext m_1, generated by Eve.
- Ciphertext for the plaintext m_2, generated by Eve.

Note that Eve does not know the secret key. The evaluation procedure ofRight_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 ciphertext$E_K(m_1)$ according to mode *M*, else it makes $E_K(m_2)$ in the same way. *E*sends Eve resultant ciphertext 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 calculatethe advantage as follows:

$$\mathrm{Adv}_A^{rl} = \mathrm{Prob}\left[a \leftarrow K: A^{E_a(m_1)} = 1\right] - \mathrm{Prob}\left[a \leftarrow K: A^{E_a(m_2)} = 1\right] \qquad (5.5)$$

If Eve can construct a distinguisher *A* that holds $\mathrm{Adv}^{rl}_A \geqq$ □, the mode ofoperation *M* is not secure against Rightl_or_Left. Note that the encryptionoracle *E* has ideal security.

In the case of GCM, we use a pseudo random oracle *P* instead of the encryptionoracle *E*. Moreover, the output is generated in moderation manner insteadof mode of operation. The pseudo random oracle *P* is an ideal secure PRNG;moreover, it is a deterministic algorithm. Therefore, the advantage is calculatedas follows:

$$\mathrm{Adv}_A^{rl} = \mathrm{Prob}\left[a \leftarrow K: A^{P_a(m_1)} = 1\right] - \mathrm{Prob}\left[a \leftarrow K: A^{P_a(m_2)} = 1\right] \qquad (5.6)$$

We analyze the security of GCM against Right_of_ Left. From Proposition1, Eve can distinguish by *t* [bit] length of message (or query), and the numberof queries is 1. Thus it is obvious that
$\mathrm{Adv}_A^{rl} \geq \epsilon$(5.7)

We conclude that GCM is not secure against Right or Left. However, if thelength of the message for encryption with the same key is less than *t*, GCM hasenough Right or Left security. This is the security requirement for GCM or animprovement of its security.

Comparison of the result of Right or Left with that of Real or Randomshows that both the results are derived from Proposition 1. The structure ofGCM outputs one bit at a time. Therefore the number of operations is equalsto the length of the message. Hence, both the results are essentially equivalentin 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], [8], [15]. Although evaluationmethod Find then Guess and Right or Left are basically similar, the distinguishingfeature of the former is that Eve can use the knowledge when she executesthe distinguisher A. Therefore, Eve is at an advantage. The evaluationprocedure 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 analyzem_1 and m_2 to store the knowledge k. Eve then uses the knowledge$k$ to distinguish the ciphertext of m_1 and m_2.

<Guess stage>

[Step-3] E generates 1[bit] random number b. If $b = 0$ it makes the ciphertext$E_K(m_1)$ according to mode M, else it makes $E_K(m_2)$ in the same way. Esends Eve the resultant ciphertext as c.
[Step-4] Eve uses a distinguisher A with knowledge k. If the distinguisher Ajudges $c = E_K(m_1)$, it outputs '1' else it outputs '0'.

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

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

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

Find then Guess is a weak version of Right or Left in the sense that Eve isat a greater advantage in the former than in the latter. As shown in Section5.3, if GCM is not secure against Right or Left, it is not practical to adaptFind_then_Guess. Hence, we analyze the GCM whose message length is lessthan t. Eve uses the information of known plaintexts to measure the outputfrom the modulator and to obtain the random number candidates generatedby PRNG. However plaintexts do not influence the resultant outputs from themodulator; the PRNG alone determines the resultant outputs. Therefore, Evecannot 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 secretkey using Proposition 1. Since Eve cannot decrypt c, she cannot distinguishthem. As a result, such an improved GCM is secure against Find then Guess.

6. DISCUSSIONS

6.1. Achievement of Security for GCM

From the results shown in section 4, the analytical security depends on thechoice of PRNG. The condition for attack requires an effective attack methodfor the target PRNG. If such an effective attack method is not found, it can beconcluded that GCM has sufficient analytical security. For example, an effectiveattack method against AES has not yet been developed. So, if AES is used asthe PRNG, we can conclude that any GCM will be analytically secure. Hence,we cannot compare the effectiveness of different structures of GCM from theviewpoint of security.

Nevertheless, from these results, practical security canbe realized in realistic scenarios. It shall serve as the criteria for choosing theappropriate PRNG.

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

'Semantics' is an important evaluation method for mode of operation. Theoriginal semantics is evaluation method for asymmetric key ciphers [6]. Fora cryptosystem to be semantically secure, information on the plaintext shouldnot be leaked when the corresponding ciphertext and public key are provided.In the case of mode of operation, semantics means that Eve cannot expectto obtain the ciphertext corresponding to the plaintext without knowing thesecret key. As shown in section 5, our method only evaluates the security of thesecret key and does not evaluate the security of the GCM output. The outputis secure if information on the plaintext is not leaked. The reason we do notadapt semantics is that the GCM outputs are measured using the informationon known plaintexts, and such information does not influence the generation ofthe output. This is obvious from the function of modulation and Proposition1. On the other hand, if the GCM has some output function, semantics wouldbe an important evaluation method. For example, we expect that the use of aneffective output function leads to privacy amplification.

6.2. Disadvantage of GCM

The disadvantage of GCM is that it is difficult to achieve information theoreticsecurity. By ensuring information theoretic security, it would be impossible todetermine the secret key even if brute force search is executable. Two importantproblems need to be addressed:

(1) Tradeoff between the effectiveness of communication and security
(2) Removal of correlation between outputs from modulation

6.2.1. Tradeoff Between Effectiveness of Communication and Security

From Proposition 1, if the following holds for any t, GCM can be said to haveinformation theoretic security.

$$\left(\frac{s}{S}\right)^t > \frac{1}{2^n} \qquad (6.1)$$

The necessary condition for this is $s/S = 1$. This condition implies that themeasurement is infeasible because Bob cannot receive any signal from Alice.Therefore, when GCM gets information theoretic security, communication becomesimpossible. On the other hand, when $s = 1$ means that error free, then$t$becomes its minimum. Thus, when the effectiveness of communication usingGCM becomes optimum, its security becomes minimum. This is a tradeoffrelationship. The followings are the solutions proposed for this problem:

(1) Compromise on the computational power required to execute brute forcesearch (information theoretic security compromised)
(2) Improvement of security by adding an auxiliary function for output frommodulation

Solution (1) provides computational security. A simple method is to use considerablyhuge size of secret key. A realistic computational security is achievedwhen the execution of brute force search is not realistic. Another solution isto ensure a realistic amount of communication that exceeds the value of t. Apossible solution for the improvement GCM is shown in section 5.3. The improvementis achieved by making the length of the message less than t. Thevalue of t is determined from the values of S and s. Therefore, it is necessary toimprove the implementation of PSK and to determine the physical limitationof the effectiveness of POVM. Solution (2) relates to the correlation of outputsfrom modulation; hence, we show the details in section 6.2.2.

6.2.2. Removal of Correlation Between the Outputs from Modulation

Since there exists a correlation between the outputs of time τ and $\tau +1$, Proposition1 holds. If there is no correlation between them, Proposition 1 does nothold, and the attacks mentioned in section 5 becomes infeasible. One solutionis to add an auxiliary correlation immune function. In [7], the purpose of correlationimmune function is to prevent attacks on the PRNG, and the aim of itto generate no correlation between the resultant outputs from the modulator.Conducting a detailed analysis of this method would be the subject of our futureresearch.

Another solution is to add an auxiliary function based on privacy amplification.In this paper, our definition of the function that is based on privacyamplification is one that removes the correlation between the results of measurementand Alice's signal. Note that in the original GCM, results of measurementare equals to Alice's signal. When using such privacy amplification, we needanother secret information between Alice and Bob. Therefore, Eve needs to determinethe signal using the measurement results with expecting another secretinformation. If the probability of successful determination of the true signal isequals to that of successful expectation of another secret information, we canconclude that there is no correlation. When we realize such privacy amplificationmethod, we can achieve an information theoretic secure GCM.

7. CONCLUSIONS

In this paper, we define GCM and evaluate its security in the case of quantumcommunication. We propose a new evaluation method from the viewpoint ofmode of operation. Using our method, we can determine the requirements forachieving a GCM with better structural security and compare the security ofdifferent GCM structures. Since the results of our method do not depend on thesecurity status of the PRNG, it is possible to develop structurally secure designapproach. In section 5, we show the security evaluation of GCM. From theresults, we find that a structurally secure GCM needs to have some auxiliaryfunctions to have correlation immunity of output from modulator. We alsoexpect privacy amplification to be one of the strategies for the improvement ofGCM. By using privacy amplification, GCM will be able to have informationtheoretic 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 GCMwith the abovementioned security features. Further, security requirements forthe PRNG can be determined from our evaluation method. The results ofevaluation show the necessary key updating period. The maximum length of themessage that can be sent in the same secret key and the requirement for secureoperation can also be determined by using the proposed evaluation method.

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

REFERENCES

[1] M.Bellare, A.Desai, E.Jokipii&P.Rogaway, “A Concrete Security TreatmentofSymmetric 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] CRYPTREC, http://www.cryptrec.go.jp/english/index.html

[3] eSTREAM, http://www.ecrypt.eu.org/stream/

[4] 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

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

[6] S.Goldwasser and S.Micali, “Probabilistic Encryption”, Journal of Computerand System Science, 28: pp.270-299, 1984

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

[8] ISO/IEC 10116, “Information Technology - Security techniques - Mode ofoperation for an n-bit block cipher algorithm”, 2002-6-26

[9] ISO/IEC 18033, “Information technology - Security techniques – Encryptionalgorithms”, 2005-07-15

[10] M. Mihaljevic, “Generic framework for secure Yuan 2000 quantum encryptionprotocol employing the wire-tap channel approach”, Physical ReviewA, vol. 75, no. 5, May 2007, pp. 052334-1-5

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

[12] NIST FIPS 186-2, “Digital Signature Standard (DSS), Appendix 3.1”

[13] NIST, SP800-38A,“Recommendation for Block Cipher Modes of Operation- Methods and Techniques”

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

[15] P.Rogaway, M.Bellare, and J.Black. “OCB: A Block-Cipher Mode of Operationfor Efficient Authenticated Encryption”, ACM Transactions on Informationand System Security (TISSEC), vol. 6, no. 3, August 2003, pp.365-403

[16] H.P.Yuen, “KCQ: A new approach to quantum cryptography I.”, Generalprinciples and qumode key generation, quant-ph/0311061

[17] H.P.Yuen and R.Naira, “On the security of Y-00 under fast correlation andother attacks on the key”, Physics Letters A Volume 364, Issue 2, 23 April2007, pp. 112–116

AUTHORS

Hidema Tanka is an associate professor of National Defense Academy Japan. His main research area is analysis of cryptographic algorithm, code theory, information security and cyber warfare and its domestic laws.