IEICE TRANS. FUNDAMENTALS, VOL.E82–A, NO.10 OCTOBER 1999

PAPER *Special Section on Information Theory and Its Applications*

Application of Quantum Cryptography to an Eavesdropping Detectable Data Transmission

Takamitsu KUDO[†], ***Nonmember***, **Tsuyoshi Sasaki USUDA**[†], **Ichi TAKUMI**[†], ***and*** **Masayasu HATA**[††], ***Members***

SUMMARY In this paper, we show that the principle of quantum cryptography can be applied not only to a key distribution scheme but also to a data transmission scheme. We propose a secure data transmission scheme in which an eavesdropping can be detected based on sharing the bases Alice (the sender) and Bob (the receiver) have. We also show properties of this scheme.

key words: *quantum cryptography, communication bases, detection of eavesdropping*

1. Introduction

Recently quantum information theory which is based on the quantum mechanics has been developed [1], [2]. Quantum cryptography, one of applications of quantum information theory is a key distribution scheme, the security of which is guaranteed by the laws of the quantum mechanics. Theoretical models for the quantum cryptography have been based on the uncertainty principle [3], EPR states [4] and two nonorthogonal states [5].

In all the quantum cryptographic schemes [3]–[5] until 1998, Alice (the sender) and Bob (the receiver) choose random bases (e.g. polarized single photons) before communicating in quantum channel, and can detect eavesdropping by inspecting the bases via classical channel. In these schemes, we need public announcement of bases via classical channel. So we call these schemes "Announcement of bases scheme."

On the other hand, a quantum cryptographic schemes without public announcement of bases was recently proposed [6]. In this scheme, Alice and Bob share the bases by the preliminary communication and don't inspect the bases via classical channel. In this scheme, since Alice and Bob use the same bases, there will be perfect correlation between the bits Alice sends and the bit Bob receives if there is no eavesdropper. From this fact, Alice can send Bob key data that Alice intends herself. We call this scheme "No announcement of bases scheme."

Manuscript received January 22, 1999.
Manuscript revised May 24, 1999.

[†]The authors are with the Department of A.I. & Computer Science, Nagoya Institute of Technology, Nagoya-shi, 466–8555 Japan.

[††]The author is with the Department of Applied Information Technology, Aichi Prefectural University, Aichi-ken, 480–1198 Japan.

In this paper, we show that the principle of quantum cryptography can be applied not only to a key distribution schemes but also to a data transmission scheme. Developing the idea in Ref. [6], we propose a secure data transmission scheme in which an eavesdropping can be detected based on sharing the bases Alice and Bob have. We also show properties of this scheme and give some information theoretical discussion.

2. Announcement of Bases Scheme (the BB84 Scheme) [3]

Let us start with the BB84 scheme since No announcement of bases scheme [6] is proposed as a variation of the BB84 scheme [3].

In the BB84 scheme, Alice and Bob communicate over both quantum and classical channels. In quantum channel, Alice sends to Bob a random sequence which is the source of a key. Here Eve (the eavesdropper) can eavesdrop and tamper. But eavesdropping and tampering by Eve reflect Bob's observations, which follows from quantum mechanical laws (the uncertainty principle, in the BB84 scheme). In classical channel, Alice and Bob detect eavesdropper and generate keys using the random sequence obtained from the communication via quantum channel. Here Eve can eavesdrop but cannot tamper. And eavesdropping doesn't reflect Bob's observations.

2.1 Fundamental Principle of the BB84 Scheme

In the BB84 scheme, Alice and Bob share a random sequence using linearly polarized single photons. As polarization directions of photons, $0°, 45°, 90°$ and $135°$ are used. Assume that $0°$ and $45°$ correspond to the message 0 and $90°$ and $135°$ correspond to the message 1. There are two types of the transmitters and the receivers. One corresponds to a type in which the transmitter sends rectilinear polarized photons and the receiver performs a measurement of rectilinear polarization direction. We call it "R type." The other corresponds to a type in which the transmitter sends diagonal polarized photons and the receiver performs a measurement of diagonal polarization direction. We call it "D type."

In R(D) type, the transmitter sends $0°(45°)$ and

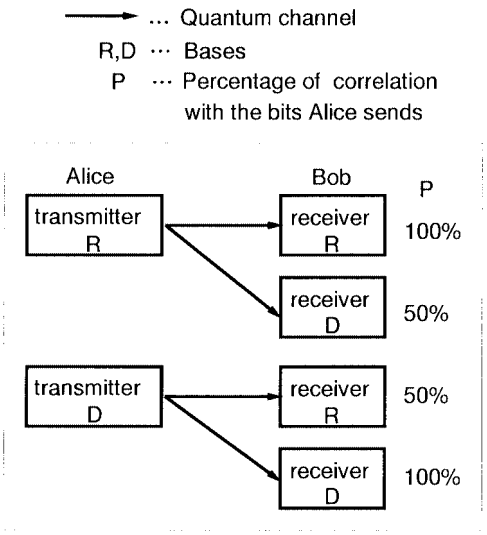


Fig. 1 Relation between the bit and basis in the BB84 scheme.

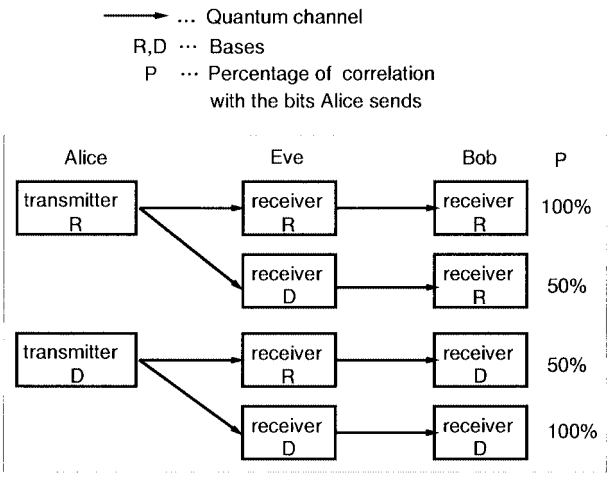


Fig. 2 Relation between bit and basis in case that there is an eavesdropper (Eve).

90°(135°) polarization directions and the receiver detects 0°(45°) and 90°(135°) polarized signals without any error. We call polarization direction of transmitter and receiver "basis." We represent rectilinear basis "R" and diagonal basis "D."

If Bob receives the bits with the same bases as the bases Alice uses, Bob receives the bits which have perfect correlation with the bits Alice sends. But, when Bob receives a bit with basis different from the basis Alice uses, Bob receives the bit which has only half correlation (probability 50%) with the bits Alice sends (Fig. 1).

Consequently, if Alice and Bob choose the bases randomly, Bob receives the bits with 75% correlation with the bits Alice sends. In other words, the bits Bob receives include 25% errors.

When Eve exists between Alice and Bob, even if Alice and Bob use same bases, Bob receives the bits which include 25% errors by Eve's bases (Fig. 2). Alice and Bob can detect eavesdropping by using this fact.

2.2 Protocol of the BB84 Scheme

Table 1 illustrates the protocol of the BB84 scheme. The numbers in this section correspond to the numbers in the Table 1.

(1) Alice chooses some bits which are 0 or 1 randomly. (2) Alice chooses some bases randomly, too. (3) Alice decides polarization directions of the single photons based on (1) and (2), and sends them. (4) Bob chooses bases of receiver randomly, and observes each photon. (5) If Bob uses the same bases as Alice uses, the received bits have perfect correlation with the bits Alice sends. But, if Bob uses the bases different from the bases Alice uses, the bits have only half correlation with the bits Alice sends by uncertainty principle (the underline in Table 1 shows this fact). (6) Bob sends Alice bases of received bits by classical channel. (7) Alice tells Bob which bases were correct. (8) Alice and Bob throw away the bits corresponding to wrong bases.

Table 1 Protocol of the BB84 scheme.

In quantum channel								
(1)Alice's random bits	0	0	0	0	1	1	1	1
(2)Random sending bases	R	R	D	D	R	R	D	D
(3)Photons Alice sends	→	→	↗	↗	↑	↑	↖	↖
(4)Random received bases	R	D	R	D	R	D	R	D
(5)Bits as received by Bob	0	1	0	0	1	0	0	1
In classical channel								
(6)Bob reports bases of received bits	R	D	R	D	R	D	R	D
(7)Alice says which bases were correct	○	×	×	○	○	×	×	○
(8)Presumably shared information (if no eavesdrop)	0			0	1			1
(9)Bob reveals some bits at random				0	1			
(10)Alice confirms them				○	○			
(11)Remaining shared secret bits	0							1

2.3 Detection of Eavesdropping

If Eve eavesdrops, Bob receives the bits include 25% errors as shown in Fig. 2. Because of this fact, (9) Bob sends Alice some of bits (k bits) in the bits corresponding to the correct bases. (10) Alice inspects all the bits Bob sends whether the bits are correct. (11) If all the bits are correct, Alice and Bob judge that there is no eavesdropping, and accept the remaining bits as a key.

If there is eavesdropping, the error probability of the bits Alice inspected in (10) is $1 - (\frac{3}{4})^k$. We can detect eavesdropping with sufficiently higher probability if we set k large number. The other side, Eve obtains some information of random bits by comparing the bases obtained in classical channel with the bases used in quantum channel herself and examining the bits obtained in quantum channel. Therefore when Alice

and Bob detect eavesdropping, they throw away all bits and repeat this protocol again, or they use "privacy amplification" [7] scheme.

Thus the safety key distribution scheme in which one can detect eavesdropping is realized.

3. No Announcement of Bases Scheme [6]

As a variation of the BB84 scheme, the scheme that Alice and Bob don't inspect the bases via classical channel is proposed [6] (No announcement of bases scheme). In this section, We briefly survey this scheme.

3.1 The Protocol of No Announcement Bases Scheme

In No announcement of bases scheme, first, Alice and Bob share the short secure random sequence that is known to nobody by a preliminary communication (the BB84 scheme and so on). The random sequence is used as bases repeatedly. For example, when Alice and Bob share 50 bits of the random sequence (short sequence) and Alice sends Bob 1000 bits of the other random sequence (long sequence), they used the short sequence 20 times repeatedly. It is proved that even if Alice and Bob use the short sequence as bases repeatedly, Eve can obtain no information about the bases [6].

Table 2 illustrates the protocol of No announcement of bases scheme. The numbers in this section correspond to the numbers in the Table 2.

(1) Alice chooses some bits which are 0 or 1 randomly. (2) Alice uses the bases decided by the preliminary communication, and (3) she decides polarization directions of the single photons based on (1) and (2), and sends them. (4) Bob uses the bases decided by the preliminary communication, and observe each photons. (5) If Eve doesn't eavesdrop, the received bits have perfect correlation with the bit Alice sends because Alice and Bob use the same bases.

(6) Bob sends Alice some of bits obtained in (5). (7) Alice inspects all the bits Bob sends whether they are correct. Eve can obtain no information about the bases in (7) because they don't inspect the bases in classical channel. (8) If all the bits are correct, Alice and Bob judge that there is no eavesdropping and accept the remaining bits as a key. If Alice and Bob detect eavesdropping, they use privacy amplification scheme.

Table 2 Protocol of No announcement of bases scheme.

In quantum channel						
(1)Alice's random bits	0	0	0	1	1	1
(2)Sending bases	R	D	R	R	D	D
(3)Photons Alice sends	→	↗	→	↑	↖	↖
(4)Received bases	R	D	R	R	D	D
(5)Bits as received by Bob	0	0	0	1	1	1
In classical channel						
(6)Bob reveals some bits at random			0	1		
(7)Alice confirms them			○	○		
(8)Remaining shared secret bits	0	0			1	1

When Alice and Bob use the key shared by this scheme in classical channel, the bases are thrown away. Because Eve may obtain some information about the bases by eavesdropping (classical) cryptograms encrypted by the distributed key.

3.2 Advantages and Disadvantage in the Scheme

According to Ref. [6], there are three significant advantages of the No announcement of bases scheme. First, the protocol can be easier than the BB84 scheme because public announcement of bases is not needed. Second, it reduces information about bases to which Eve has access. Third, there is no discarded data in ideal case, while in the BB84 scheme about half of data is discarded.

There is also a disadvantage of the scheme as Alice and Bob must prepare a short random sequence to be used as a bases sequence. But it is a characteristic of the scheme that Alice and Bob can share a long sequence by preparing a short sequence.

4. Application to a Data Transmission Scheme

It is clear that No announcement of bases scheme has the feature that there is perfect correlation between the random sequence Alice sends and that Bob receives and just the same sequence can be used as a cryptographic key when Eve doesn't eavesdrop.

This implies that Alice can send Bob data quite correctly by sharing the bases. Here we try to construct a secure data transmission scheme in which we can detect eavesdropping by using the idea in Ref. [6].

4.1 The Protocol of Data Transmission Scheme

Table 3 illustrates the protocol of data transmission scheme based on sharing the bases. In this protocol, Alice and Bob share a short random sequence by a preliminary communication just like No announcement of bases scheme. After that they communicate data. Here we assume that they also share the location of "inspection bit" included in the data Alice sends in the preliminary communications. The numbers in this section correspond to the numbers in the Table 3.

Table 3 The protocol of proposed data transmission scheme.

In quantum channel						
(1)Alice's data bits	0	0		1	1	
(2)inspection bits			0			1
(3)Sending bases	R	D	R	R	D	D
(4)Photons Alice sends	→	↗	→	↑	↖	↖
(5)Received bases	R	D	R	R	D	D
(6)Bits as received by Bob	0	0	0	1	1	1
In classical channel						
(7)Bob reveals inspection bits			0			1
(8)Alice confirms them			○			○
(9)Remaining shared secret bits	0	0		1	1	

(1) Alice sets the data bits which are 0 or 1. (2) Alice mixes inspection bits with data bits. (3) Alice uses the bases decided by the preliminary communication, and (4) she decides polarization directions of the single photons based on (1), (2) and (3), and sends them. (5) Bob uses the bases decided by the preliminary communication and observes each photons. (6) Because Alice and Bob use the same bases, the received bits have perfect correlation with the bits Alice sends if Eve doesn't eavesdrop.

(7) Bob sends Alice inspection bits. (8) Alice inspects whether all inspection bits are correct. In this case, just like No announcement of bases scheme, Eve can obtain no information about the bases in (8). (9) If all inspection bits are correct, Alice and Bob judge that there is no eavesdropping, and accept the remaining bits as the data.

4.2 Advantages in the Scheme

There are three significant advantages of this data transmission scheme. First, one can detect eavesdropping, which classical data transmission protocols never have so far. Second, Alice and Bob don't need to replace a key (bases) periodically because they can detect eavesdropping. This contrasts well with classical cryptographic schemes (including a case of using keys distributed by quantum cryptography) in which Alice and Bob must replace a key periodically because they cannot detect Eve's eavesdropping, and therefore, they have to assume cryptograms are always eavesdropped by Eve. In this protocol, it is sufficient for them to replace the key after they detect eavesdropping. Third, Alice and Bob don't need to save a long key. They only use a short key repeatedly.

5. Properties of the Data Transmission Scheme

In the previous section, we showed the protocol of a secure data transmission scheme and its advantages. But we should consider some points in this protocol.

In No announcement of bases scheme, it is sufficient for Alice and Bob to share the noncommittal random sequence. They can share the random sequence by privacy amplification even if there is an eavesdropper although they may not share the same random sequence as Alice sends. But in the data transmission scheme, it is useless that Alice and Bob cannot share the same data as Alice sends. So privacy amplification cannot be used in this scheme.

When Eve eavesdrops, there is a secure but not efficient way that Alice and Bob replace the bases and Alice retransmits the data. There may be more efficient way even if there is an eavesdropper. To obtain better way, we need to study properties of this data transmission scheme. In the following, we study properties of this scheme in detail and consider how it influences this scheme that privacy amplification cannot be used.

5.1 Information Theoretical Investigation

In No announcement of bases scheme, privacy amplification is used to eliminate discrepancy in bits. And Eve can obtain no information about the random bits. But in the data transmission scheme, we cannot use the privacy amplification. So we first estimate how much information Eve can obtain.

We assume that Alice sends x bits and Eve eavesdrops n bits ($n \leq x$). Since bit error rate is 25% for an eavesdropped bit on the channel between Alice and Bob, the entire bit error rate is $\frac{n}{x} \times 0.25$ [bits/symbol]. Therefore, the mutual information $I(A;B)$ between Alice and Bob is

$$\begin{aligned} I(A;B) &= H(A) - H(A|B) \\ &= 1 + \left\{ \left(\frac{n}{x} \times 0.25\right) \log_2 \left(\frac{n}{x} \times 0.25\right) \right. \\ &\quad \left. + \left(1 - \frac{n}{x} \times 0.25\right) \log_2 \left(1 - \frac{n}{x} \times 0.25\right) \right\}. \end{aligned} \tag{1}$$

On the other hand, the mutual informations $I(A;E)$ between Alice and Eve and $I(E;B)$ between Bob and Eve are $I(A;E) = I(E;B) = 0.189$ [bits/symbol] since the bit error rates in the channel between Alice and Eve and that between Eve and Bob are both 0.25 [bits/symbol] when Eve eavesdrops choosing bases randomly for each eavesdropped bit.

Figure 3 shows mutual information with respect to $\frac{n}{x}$ for each channel.

In Fig. 3, we can see $I(A;E) = I(E;B) \leq I(A;B)$. If $n = x$, $I(A;E) = I(E;B) = I(A;B)$. This is the case that Eve eavesdrops all bits. In this case, bit error rate of channel between Alice and Bob is 0.25

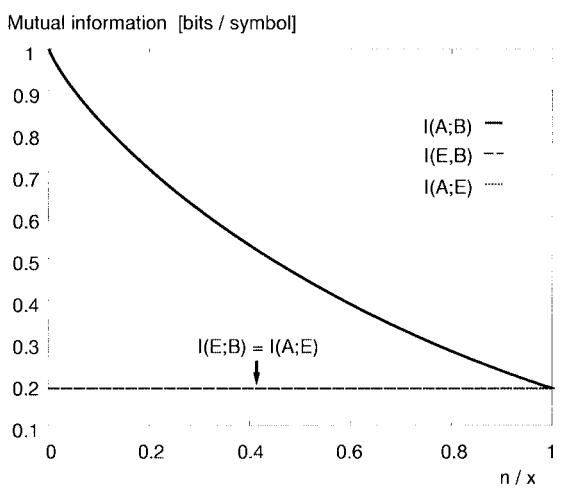


Fig. 3 Mutual informations for Alice-Bob, Eve-Bob, and Alice-Eve channels as functions of eavesdropping rate $\frac{n}{x}$.

[bits/symbol]. So mutual informations $I(A;B), I(A;E)$ and $I(E;B)$ are $I(A;B) = I(A;E) = I(E;B) = 0.189$ [bits/symbol].

5.1.1 Channel Coding Theorem

The classical channel coding theorem shows that there is a code with probability of error $\epsilon \to 0$ if transmission rate R is $R \leq C$ when we send information via the channel whose capacity is C. But if $R > C$, such a code never exists.

From this fact, if the channel capacity C between Alice and Bob is larger than the channel capacity C_E between Alice and Eve, Alice can send information to Bob without errors and Eve can obtain no information. Since the occurrence probabilities of bits 0 and 1 are assumed to be $\frac{1}{2}$ in this data transmission scheme, the mutual informations shown in Fig. 3 are just the same as the channel capacities.

We can see from Fig. 3 that $I(A;E) < I(A;B)$ when $r \neq x$, and therefore $C_E < C$. So we can say that there is a coding in which Alice can send Bob information safely by setting R at $C_E < R < C$ if Eve doesn't eavesdrop all bits.

5.2 The Number of Bits Which have Perfect Correlation

In this subsection, we consider this scheme from another point of view. In particular cases, Eve can judge some eavesdropped bits to have perfect correlation with the bits Alice sends. We consider the number of the bits which Eve can judge to have perfect correlation. That is, how many bits can Eve get with zero-errors.

If Eve eavesdrops, 25% bit errors occur in A-E and A-B channels. So Alice cannot send Bob data correctly even if they share the bases. Eve also cannot obtain the bits which have perfect correlation with the bits Alice sends when only once she eavesdrops the bits. Because Alice and Bob don't inspect the bases via classical channel. Since privacy amplification cannot be used, Alice must retransmit the data to share it with Bob.

So we consider whether Eve can obtain the bits which have perfect correlation with the bits Alice sends when Alice sends the same information more than twice. For simplicity, we assume that Alice and Bob don't change the values of the bases and the inspection bits.

Suppose that Eve eavesdrops them with the same bases as the first bases when Alice retransmits the data bits. If Eve uses the same basis as Alice used, Eve detects the same bit as the first absolutely. If Eve uses the basis different from Alice used, Eve detects the bit different from the first with probability 50%. Therefore if Eve detects the bit different from the first, she can find that she used wrong basis for the bit (Fig. 4).

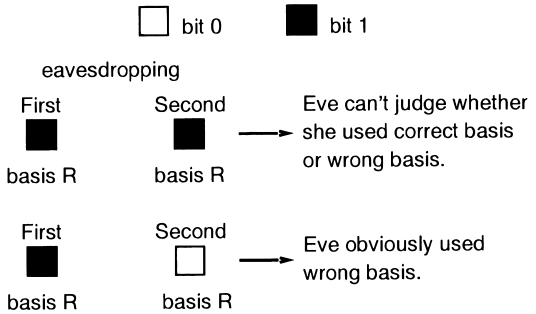


Fig. 4 An example that Eve can find correct bases.

Therefore Eve can obtain correct bases with probability $\frac{1}{4}$. Because the probability Eve uses the different bases from Alice's is $\frac{1}{2}$ and then in second eavesdropping, the probability Eve obtains the different bit from the first one is $\frac{1}{2}$.

If Alice sends data three times and Eve eavesdrops, Eve can obtain the "true" data bits with probability $\frac{1}{4}$ by using correct bases.

5.3 Relation between Number of Inspection Bits and Probability of Detecting Eavesdropping

In the proposed data transmission scheme, Alice mixes data bits and inspection bits and Alice and Bob detect eavesdropping by inspecting the inspection bits. In this subsection, we consider relation between the proportion of inspection bits to the data bits and probability of detecting eavesdropping.

Assume that Alice sends x bits, inspection bits are included r bits in x, and Eve eavesdrops n bits. Then we consider the probability of including inspection bits in eavesdropped bits.

The number of combinations of choosing k inspection bits in eavesdropped bits are ${}_rC_k$, the number of combinations of choosing $n-k$ expecting inspection bits in eavesdropped bits are ${}_{x-r}C_{n-k}$, and the number of combinations of choosing eavesdropped bits in all bits are ${}_xC_n$. Therefore the probability of including $k(k \leq n)$ inspection bits in the eavesdropped bits is $\frac{{}_rC_k \times {}_{x-r}C_{n-k}}{{}_xC_n}$.

When Eve eavesdrops k inspection bits, the probability of detecting eavesdropping is $1-(\frac{3}{4})^k$. Therefore the probability of detecting eavesdropping P_n is

$$P_n = \sum_{k=1}^{n} \frac{{}_rC_k \cdot {}_{x-r}C_{n-k}}{{}_xC_n} \left\{ 1 - \left(\frac{3}{4}\right)^k \right\}. \tag{2}$$

Using this equation, we show relation between the number of eavesdropped bits and the probability of detecting eavesdropping in the case of including 5,10,20,40 and 50 inspection bits in 100 bits Alice sends (Fig. 5).

From Fig. 5, Alice and Bob can detect eavesdropping with almost probability 100% by mixing 20 inspection bits in 100 bits if Eve eavesdrops all bits. However, Alice needs to mix many inspection bits in 100 bits to

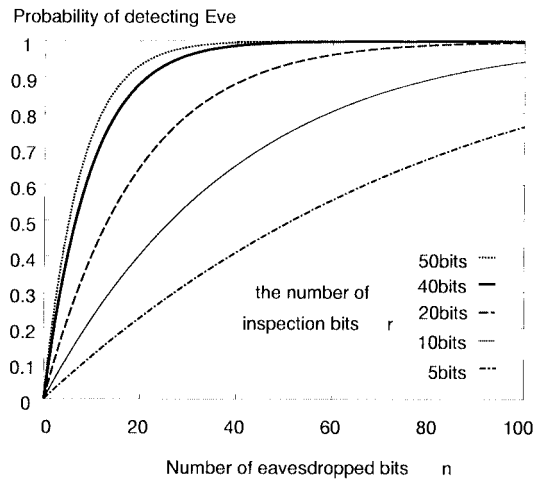


Fig. 5 Relation between the number of eavesdropped bits and the probability of detecting eavesdropping when $x = 100$.

detect eavesdropping certainly if Eve eavesdrops only several bits.

5.4 Discussion

According to the above discussions, Eve can obtain bases with probability $\frac{1}{4}$ for eavesdropped bits when Alice sends the same data twice in the case that Eve eavesdrops all bits. Moreover, when Alice sends data three times, Eve can obtain true data bits with probability $\frac{1}{4}$ for eavesdropped bits. However if Alice sends data one-time, Eve can obtain no data without any error. Since Alice and Bob can detect eavesdropping with high probability by mixing sufficient inspection bits, the data transmission system is secure if Alice stops the transmission as soon as she detects eavesdropping.

Moreover, in the case that Eve doesn't eavesdrop all bits, information Bob obtains is larger than that Eve can obtain. So Alice can (in principle) send Bob data safely (i.e., Eve can obtain no information) by setting transmission rate properly. But we don't know a code which works under the condition such that bit error rate nearly equals to 25%. Further work is needed to find such a code.

On the other hand, Eve trades the amount of information by eavesdropping and a risk to be detected the eavesdropping.

6. Conclusion

In this paper, we apply the method in Ref. [6] to construct a data transmission scheme with detecting eavesdropping. As a result, it is shown that the data transmission scheme may be useful by combining sharing the bases and a coding scheme based on classical channel coding theorem.

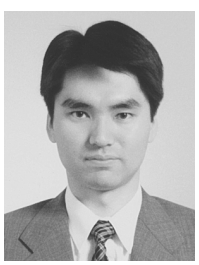
This scheme is not complete still now. But we hope our result will open new possibility of quantum cryptography, that is, the principle of quantum cryptography can be applied not only to key distribution schemes but also to the other secure schemes.

There are two further problems. First one is that how can we estimate the number of bits and the amount of information Eve obtains and how can we construct the error correcting code. Second one is to give the method in which one can protect the data from various eavesdropping strategies [8].

References

[1] C.H. Bennett and P. Shor, "Quantum information theory," IEEE Trans. Inf. Theory, vol.44, pp.2724–2742, 1998.
[2] Special Section on Quantum Information Theory and Its Applications, IEICE Trans., vol.J81-A, no.12, 1998.
[3] C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," International Conference on Computers, Systems & Signal Processing, Bangalore, pp.175–179, India, 1984.
[4] A.K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol.67, pp.661–663, 1991.
[5] C.H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., vol.68, pp.3121–3124, 1992.
[6] W.Y. Hwang, I.G. Koh, and Y.D. Han, "Quantum cryptography without public announcement of bases," Phys. Lett., vol.A244, pp.489–494, 1998.
[7] C.H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer, "Generalized privacy amplification," IEEE Trans. Inf. Theory, vol.41, pp.1915–1923, 1995.
[8] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy," Phys. Rev., vol.A56, pp.1163–1172, 1997.

Takamitsu Kudo received the B.E. degree from Nagoya Institute of Technology, Nagoya, Japan in 1998, in Department of Artificial Intelligence and Computer Science. He has been attending Department of Artificial Intelligence and Computer Science, Nagoya Institute of Technology as a master course student. His current research is quantum information theory.



Tsuyoshi Sasaki Usuda received the B.E., M.E., and Ph.D. degrees in information and communication engineering from Tamagawa University, Tokyo Japan, in 1990, 1992, and 1995, respectively. Since 1995 he has been with Department of Artificial Intelligence and Computer Science, Nagoya Institute of Technology, Nagoya Japan, where he is presently an Assistant. His current research interests are in quantum information and communication theories and their applications.

Ichi Takumi received the B.E. degree and the M.S. degree from Nagoya Institute of Technology, Nagoya, Japan in 1982 and 1984 respectively, both in electronic engineering. After graduation he joined Oki Electric Co. He has a Doctor of Eng. degree from Nagoya Institute of Technology. Since December 1985 he has been with Nagoya Institute of Technology, where he is now an Associate Professor of Department of Artificial Intelligence and Computer Science. His current research interests include digital signal processing and its applications. He is a member of the Society of Instrument and Control Engineerings of Japan.

Masayasu Hata graduated in 1958 from Department of Electronic Engineering, Faculty of Engineering, Nagoya Institute of Technology, and affiliated with Oki Electric Co. He has a Doctor of Eng. degree from Tokyo Institute of Technology. He was engaged in R&D of digital communication system, application of electronic circuits and millimeter wave communication equipment. Retired from Oki Electric Co. in 1985 and became a Professor in the Department of Artificial Intelligence and Computer Science, Nagoya Institute of Technology. Since 1998 he has been with Aichi Prefectural University as a Professor in the Department of Applied Information Technology. He is engaged in research on digital signal processing and information communication.