Information investigation for B92 protocol in quantum cryptography

ZOU Ming[*a,b] ZHANG Guo-ping[a]
a. College of Physics Science and Technology, Central China Normal University, Hubei, Wuhan, 430079,china
b. Department of Physics, Hubei Institute of Nationalities, Hubei, Enshi, 445000，china

ABSTRACT

In this paper, we simulate the quantum channel with a binary symmetric channel and a binary erasure channel, a series channel and a Markovian chain channel in classical information theory, then calculate respectively the mutual information between the signal's deliverer, the legal receiver and the eavesdropper, the bit error rate during propagating the signals with the theory about the quantum measurement channel and the quantum information theory. For B92 protocol, a simple quantum cryptography distribution scheme, we study the bound and the property of mutual information obtained by the legal receiver and the eavesdropper, seek the relationship between the bit error rates and the eavesdropper's way, in two cases of the opaque eavesdropping and the translucent eavesdropping. A new criteria for checking the eavesdropper and ensuring the legal correspondent is estimated. Furthermore, the comparison in bit error rates caused respectively in two different measuring ways indicates that POVM is better than the standard measurement by the way of orthogonal projecting for reducing the bit error rate and increasing effective communication.

Keywords: Quantum information theory, quantum cryptography, mutual information,B92 protocol

1. INTRODUCTION

As the representative of quantum cryptography, the quantum key distribution QKD[1-3] is a successful model that the quantum information technique applies to the conventional communications. The security of the quantum cryptogram is unconditional for the Heisenberg uncertainty principle and quantum state no-cloning theorem, so the quantum cryptogram system has the advantage that former cryptogram system have no, up to now the people have already acquired a series research result in the theories and experiments for the quantum cryptogram, the progress also is very quick to QKD research[4-7], The research have already also launched and the series result was obtained for QKD in our country[8] , we believe that the quantum cryptography may get practical near future.

In the Information theory investigation for the quantum cryptography, how compute the quantity of information that the eavesdropper Eve and legalities receiver Bob acquire, and the characteristic of the quantity of information, the boundary of quantity of information, the containing quantity of information in a parity bit etc, are the key problems to quantum cryptography. Only the one know the quantity of information Eve acquiring, then legality correspondence can adopt the valid measurement, guaranteeing the correspondence safety. B92 protocol, as the representative of quantum cryptographical system based on two nonorthogonal quantum states, needs less equipment and is no complex in experiment, is thought to have a good of applied foreground. In this paper, we will discuss the security of B92 protocol with the theory about the quantum measurement channel and the classic information theory, the theory about Markovian

Quantum Optics and Applications in Computing and Communications II,
edited by G.-C. Guo, H.-K. Lo, M. Sasaki, S. Liu, Proc. of SPIE Vol. 5631
(SPIE, Bellingham, WA, 2005) · 0277-786X/05/$15 · doi: 10.1117/12.569663

chain series channel. A new criteria for checking eavesdropper Eve is estimated.

2 QUANTUM CHANNEL

Quantum transmission system is different with classic communication system, the carrier of information is the particles allowed by the laws of quantum mechanics in it, so the theories foundation of the quantum communication is the quantum information theories. The essential differentiation between the classic information theories and the quantum information theories is the acharacteristic of noise in communication system, the characteristic of the quantum noise obeys the quantum statistics theories. From the quantum mechanics uncertainty principle we can know that the quantum measurement process and its affect is totally different with the classic theories . The classic measurement way can't affect the system under test. That the signal receiver will capture in the quantum correspondence is a quantum signal that will arrive to receiver, but the quantum noise will be produced in the process of capturing the quantum signal, it produce the influence to system under test. So the quantum measurement process equal to a channel in quantum correspondence, the quantum information channel can be regarded as the series-wound channel that make up of the quantum transmission channel and quantum measurement channel. Bases on the model of quantum information channel in reference[9], we assume that the quantum signal is transmitted in a no noisy channel, the quantum states have no change, well then the quantum signal is affected in the quantum measurement channel, the quantum measurement channel can be described by signal quantum state and measurement operator in quantum measurement process. The symbol assemble of input signal is defined by X: $\{a_i\}; i = 1,2,\cdots,r$, respectively, correspond to quantum states $\{\rho_i\}; i = 1,2,\cdots,r$ (namely, the quantum code letter of alphabet system has r kinds of quantum states of different parameter), Also is to adopt r codes, every one occurs with a priori probability $P(a_i)$. Measurement and judgment of the signal is described by a few measurement operator $\{A_i\}$, it satisfies

$$\sum_{i=1}^{r} A_i = I \tag{1}$$

The I is an unit matrix, so the average mutual information caused by quantum measurement is

$$I(X, A) = \sum_{i=1}^{r} \sum_{j=1}^{r} P(a_i) P(b_j / a_i) \log \frac{P(b_j / a_i)}{\sum_{k=1}^{r} P(a_k) P(b_j / a_k)} \tag{2}$$

Assuming $tr(\rho_i A_j)$ is a probability of state ρ_i that was measured with operator A_j, Eqs.(1) can be written as

$$I(X, A) = \sum_{i=1}^{r} \sum_{j=1}^{r} P(a_i) tr(\rho_i A_j) \log \frac{tr(\rho_i A_j)}{\sum_{k=1}^{r} P(a_k) tr(\rho_k A_j)} \tag{3}$$

3 INFORMATION INVESTIGATION FOR B92 PROTOCOL

There are a lot of protocols about the quantum key distribution, The B92 protocol[3] is the most simplest quantum-

cryptographical system, once people put forward a lot of attack strategies to it. In this paper, we analyze B92 protocol's safety based on the information theory under Eve's two eavesdropping strategies.

3.1 Communication protocol[10]

The two legitimate user, traditionally, called Alice and Bob, want to establish a cryptographic key. Alice starts the key distribution with a quantum transmission, sending to Bob a random sequence of quanta in two nonorthogonal states **u** and **v,** which represent bits "0" and "1" respectively. By a suitable choice of phase and the basis, the two quantum states **u** and **v**, whose overlap is $|\langle u|v\rangle|^2 = \sin^2\alpha$, can always be written as

$$|u\rangle = \begin{bmatrix} \cos\alpha \\ \sin\alpha \end{bmatrix} \quad \text{and} \qquad |v\rangle = \begin{bmatrix} \sin\alpha \\ \cos\alpha \end{bmatrix} \tag{4}$$

On the receiving side, Bob has to distinguish between these two nonorthogonal states for each incoming carrier. Of course he cannot do that with certainty for the limit of laws of quantum mechanics, Eve's eavesdropping also will bring influence to Bob's measurement and enhance the error rate in the transmission. In the language of information theory, this situation corresponds to Alice and Bob, Alice and Eve having at their disposal a communication channel known as a "binary erasure channel" and "binary symmetric channel", respectively.

3.2 Opaque eavesdropping

Eve intercepts the quantum carrier on its way from Alice to Bob and performs a measurement that maximizes her information as to which one of the two states, **u** or **v**, was chosen for preparing the carrier. The best procedure in this case is the measurement of a Hermitian operator whose two orthogonal eigenvectors are symmetrically related to the signal states $|u\rangle$ and $|v\rangle$. In the same basis as used in Eqs.(4), this two eigenvectors are simply $|x\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|y\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. The project operator A_u and A_v which project the quantum state to state space that $|u\rangle$ and $|v\rangle$ is orthogonal each other was respectively written as $A_u = |x\rangle\langle x|$, $A_v = |y\rangle\langle y|$. This strategy can be modeled as a flow of information from Alice to Eve through a binary symmetric channel and then from Eve to Bob through a binary erasure channel.

3.2.1 The mutual information between Alice and Eve

When Eve intercepts the quantum carrier on its way from Alice to Bob and performs a measurement, the information communication channel between Alice and Eve can be modeled as a flow of information from Alice to Eve through a binary symmetric channel. Eve uses a projecting measurement for the quantum carrier. The probability measuring $|u\rangle$ and $|v\rangle$ with A_u, A_v respectively is $tr(\rho_u A_u), tr(\rho_u A_v), tr(\rho_v A_u), tr(\rho_v A_v)$. Among them $tr(\rho_i A_j)$ ($i, j = u$ or v) mean a probability that Alice sends out the state $|i\rangle$ and Eve gains state $|j\rangle$,when $i \neq j$,it is an error transmission probability. A transmission matrix of quantum communication channel between Alice and Eve can be got, was written as $P_{AE}(j/i)$, schematized in Table 1.

As the output quantum states of the quantum code letter of alphabet system is a uniform probability, it is $P(a_i) = 1/2$, using it and $P_{AE}(j/i)$ in Eqs.(3),the mutual information between Alice and Eve is given by

$$I_{AE}(X,A) = 1 + \cos^2\alpha \log\cos^2\alpha + \sin^2\alpha \log\sin^2\alpha \tag{5}$$

Moreover, we have the Eve's bits error rate before screening data

$$P_e = \frac{1}{r}\sum_{j=1}^{r}\sum_{i\neq j} P(b_j / a_i) = \frac{1}{2}\sum_{j=1}^{2}\sum_{i\neq j} P_{AE}(j/i) = \sin^2\alpha \tag{6}$$

Eve's bits error rate before screening data is

$$q'_{e(AE)} = \sin^2\alpha . \tag{7}$$

Assuming Eve only intercepts some fraction of all the quantum carriers that Alice sends out, say η $(\eta \le 1)$, the mutual information between Alice and Eve becomes

$$I_{AE}(X,A) = \eta(1 + \cos^2\alpha \log\cos^2\alpha + \sin^2\alpha \log\sin^2\alpha) \tag{8}$$

Eve's bits error rate before screening data is no change, then

$$q_{e(AE)} = q'_{e(AE)} = \sin^2\alpha \tag{9}$$

Table.1 $P_{AE}(j/i)$

The transmission matrix of quantum communication channel between Alice and Eve

i \ j	$\|u\rangle$	$\|v\rangle$
$\|u\rangle$	$\cos^2\alpha$	$\sin^2\alpha$
$\|v\rangle$	$\sin^2\alpha$	$\cos^2\alpha$

3.2.2 The mutual information between Alice and Bob

If Eve only intercepts some fraction η $(\eta \le 1)$ of all the quantum carriers that Alice sends to Bob, after her measurement, sends to Bob another quantum carrier, prepared in state **u** or **v** according to the outcome of her measurement on the real carrier. The information communication channel between Eve and Bob can be modeled as a flow of information from Eve to Bob through a binary erasure channel. Bob uses a positive operator valued measure (POVM) for raising the efficiency he can confirm the quantum state. The measurement operator is $B_u = \frac{1 - vv^+}{1 + \langle u|v\rangle}$ and $B_v = \frac{1 - uu^+}{1 + \langle u|v\rangle}$, $B_? = 1 - B_u - B_v$ respectively, the probability Bob measuring $|u\rangle$ and $|v\rangle$ with them is $tr(\rho_u B_u)$ and $tr(\rho_u B_v)$, $tr(\rho_u B_?)$, $tr(\rho_v B_u)$, $tr(\rho_v B_v)$, $tr(\rho_v B_?)$, here $tr(\rho_i B_?)$ ($i = u$ or v) means a probability that Eve sends out the state $|i\rangle$ and Bob gains a no certain state, $tr(\rho_i B_j)$ ($i,j=u$ or v) means a probability that Eve sends out the state $|i\rangle$ and Bob gains state $|j\rangle$, when $i \neq j$,it is error transmission probability. So we get a transmission matrix of quantum communication channel between Eve and Bob, it was written as $P_{EB}(j/i)$, schematized in Table 2.

For Eve' interception with fraction η, a transmission matrix of quantum communication channel between Alice and

Eve becomes $P'_{AE}(j/i)$ from $P_{AE}(j/i)$, $P'_{AE}(j/i)$ is schematized in Table 3.

Table.2 $P_{EB}(j/i)$

The transmission matrix of quantum communication channel between Eve and Bob

i \ j	$\|u\rangle$	?	$\|v\rangle$
$\|u\rangle$	$1-\sin 2\alpha$	$\sin 2\alpha$	0
$\|v\rangle$	0	$\sin 2\alpha$	$1-\sin 2\alpha$

Table.3 $P'_{AE}(j/i)$

The transmission matrix of quantum communication channel with fraction η between Alice and Eve

i \ j	$\|u\rangle$	$\|v\rangle$
$\|u\rangle$	$1-\eta\sin^2\alpha$	$\eta\sin^2\alpha$
$\|v\rangle$	$\eta\sin^2\alpha$	$1-\eta\sin^2\alpha$

The information communication channel between Alice and Bob can be regard as a Markovian chain series channel that is consist of the information communication channel between Alice and Eve and the information communication channel between Eve and Bob, so the total transmission matrix $P_{AB}(j/i)$ is a product of transmission matrix $P'_{AE}(j/i)$ and $P_{EB}(j/i)$, schematized in table 4.

Table.4 $P_{AB}(j/i)$

The total transmission matrix of quantum communication channel between Alice and Bob

i \ j	$\|u\rangle$	?	$\|v\rangle$
$\|u\rangle$	$(1-\sin 2\alpha)(1-\eta\sin^2\alpha)$	$\sin 2\alpha$	$\eta\sin^2\alpha(1-\sin 2\alpha)$
$\|v\rangle$	$\eta\sin^2\alpha(1-\sin 2\alpha)$	$\sin 2\alpha$	$(1-\sin 2\alpha)(1-\eta\sin^2\alpha)$

Using it and $P(a_i)=1/2$ in Eqs.(3),the mutual information between Alice and Bob is given by

$$I_{AB}(X,B)=1-\sin 2\alpha+(1-\eta\sin^2\alpha)(1-\sin 2\alpha)\log[(1-\eta\sin^2\alpha)(1-\sin 2\alpha)]+ \eta(1-\sin 2\alpha)\sin^2\alpha\log[\eta(1-\sin 2\alpha)\sin^2\alpha]-(1-\sin 2\alpha)\log(1-\sin 2\alpha) \quad (10)$$

The calculation of the bits error rate is similar with the case 3.2.1, we have Bob's bits error rate before screening data

$$q_{e(AB)}=\eta(1-\sin 2\alpha)\sin^2\alpha \quad (11)$$

If Eve intercepts all the quantum carriers that Alice sends to Bob, η=1, the mutual information between Alice and Bob is

$$I_{AB}(X,B) = 1-\sin 2\alpha + \cos^2\alpha(1-\sin 2\alpha)\log[\cos^2\alpha(1-\sin 2\alpha)] \quad (12)$$
$$+(1-\sin 2\alpha)\sin^2\alpha\log[(1-\sin 2\alpha)\sin^2\alpha] - (1-\sin 2\alpha)\log(1-\sin 2\alpha)$$

According to Eqs.(8)~(11), the relation between the mutual information and Eve's interception fraction η, the bits error rate and η, the characteristic and boundary of I_{AE} and I_{AB} all can be given by Fig.1, thus we have part following conclusions

i I_{AE} is minimum and has bottom boundary ($I_{AE}=0$) for $\eta=0$, I_{AE} is maximum and has up boundary ($I_{AE}=1+\cos^2\alpha\log\cos^2\alpha+\sin^2\alpha\log\sin^2\alpha$) for $\eta=1$.

ii I_{AB} is minimum and has bottom boundary ($I_{AB}=1-\sin 2\alpha$) for $\eta=0$, I_{AB} is maximum and has up boundary (Eqs.12) for $\eta=1$.

iii The curve I_{AB} and I_{AE} are intersectant in Fig.1, indicate the quantity of information Eve acquire from Alice can be bigger than that Bob acquire from Alice

iv The relationship $q_{e(AB)} < q_{e(AE)}$ indicate that Bob would rather adopt POVM than projecting measurement for reducing his own bits error rate and enhancing his own efficiency of confirming quantum state.

In checking the eavesdropper Eve, if Bob measure the quantum carrier by POVM and the bits error rate is $q_{e(AB)} \neq 0$, Eve's eavesdropping should be considered occurring according to Eqs.(11).When Bob's measurement way is same as Eve's orthogonal projecting measurement way, his bits error rate before screening data also is $\sin^2\alpha$ in no Eve's eavesdropping, it indicates that Eve's eavesdropping should be occurring on condition that Bob's bits error rate before screening data is $q_{e(AB)} > \sin^2\alpha$.

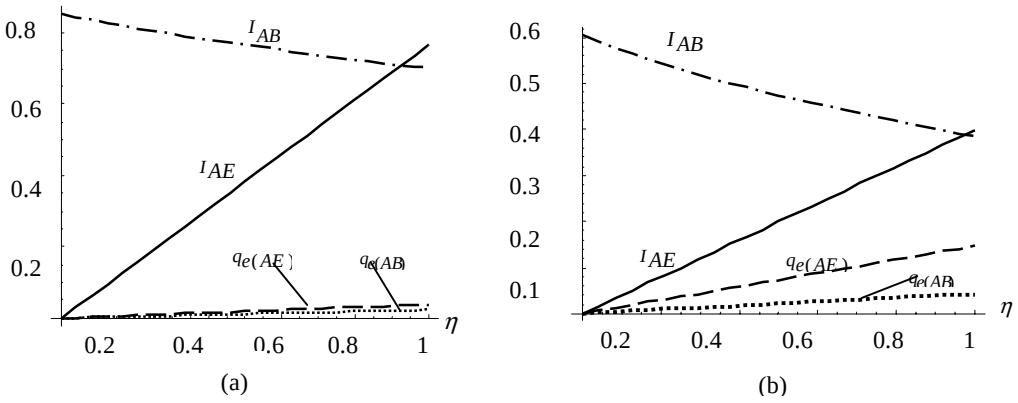

Fig.1 The mutual information and the bits error rate between Alice, Bob, and Eve depend on Bob's eavesdropping rate η. (a) for $\alpha=\pi/16$, (b) for $\alpha=\pi/8$

3.3 Translucent eavesdropping

In this strategy Eve attempts to gain some information on each signal sent by Alice, while minimizing the damage to the state of the signal. Eve make a probe in a known initial state interact with the information carrier. She can perform a Von Neumann measurement or uses a POVM to her probe, part information of every information carrier can be obtained by orthogonal projecting measurement, entire information of part information carrier can be obtained by POVM, Eve

choices orthogonal projecting measurement for gaining maximal information.

Assuming Eve's probe is in a initial state $|\varphi\rangle$, and, according to the state sent by Alice, the combined system evolves either as

$$U(|u\rangle \otimes |\varphi\rangle) = \left|u'\right\rangle \otimes e_u = \begin{pmatrix}\cos\beta\\ \sin\beta\end{pmatrix} \otimes \begin{pmatrix}\cos\gamma\\ \sin\gamma\end{pmatrix} \tag{13}$$

or as

$$U(|v\rangle \otimes |\varphi\rangle) = \left|v'\right\rangle \otimes e_v = \begin{pmatrix}\sin\beta\\ \cos\beta\end{pmatrix} \otimes \begin{pmatrix}\sin\delta\\ \cos\delta\end{pmatrix} \tag{14}$$

This evolution is unitary provided that

$$\sin 2\alpha = \sin 2\beta \sin(\gamma + \delta),\ (\beta \geq \alpha, \gamma \geq \alpha) \tag{15}$$

As $\sin 2\beta$ would be only slightly larger than $\sin 2\alpha$, the idea is to cause minimal damage to the information carrier. In the following discussion, we shall assume that $\gamma = \delta$, for the sake of symmetry. After evolution the signal quantum state is $\left|u'\right\rangle$ and $\left|v'\right\rangle$, probe state is e_u or e_v, Eve's measurement for the probe state is equal to it for signal quantum state.

3.3.1 The mutual information between Alice and Eve

Here, in order to acquire information as more as possible, Eve uses the same measurement way in the case 3.2.1, The probability that e_u or e_v was measured with A_u, A_v is respectively $tr(\rho_{e_u} A_u)$, $tr(\rho_{e_v} A_u)$, $tr(\rho_{e_u} A_v)$, $tr(\rho_{e_v} A_v)$ (equivalent to the probability measuring $|u\rangle$, $|v\rangle$), Among them $tr(\rho_i A_j)$, ($i, j = e_u$ or e_v) means a probability that Alice sends out the state $|i\rangle$ and Eve gains state $|j\rangle$, when $i \neq j$, it is error transmission probability. The transmission matrix of quantum communication channel between Alice and Eve can be got, and written as $P_{ae}(j/i)$, schematized in Table 5

Table.5 $P_{ae}(j/i)$

The transmission matrix of quantum communication channel between Alice and Eve

i \ j	e_u	e_v
e_u	$\cos^2\gamma$	$\sin^2\gamma$
e_v	$\sin^2\gamma$	$\cos^2\gamma$

As same as the calculation in 3.2.1, the mutual information between Alice and Eve is given by

$$I_{ae}(X, A) = 1 + \cos^2\gamma \log\cos^2\gamma + \sin^2\gamma \log\sin^2\gamma \tag{16}$$

The Eve's bits error rate before screening data

$$q_{e(ae)} = \frac{1}{r}\sum_{j=1}^{r}\sum_{i\neq j} P(b_j / a_i) = \frac{1}{2}\sum_{j=1}^{2}\sum_{i\neq j} P_{ae}(j/i) = \sin^2\gamma \tag{17}$$

Actually, Eve's bits error rate before screening data is

$$q'_{e(ae)} = \sin^2\gamma . \tag{18}$$

3.3.2 The mutual information between Alice and Bob

Because Eve is no intercept directly the quantum carrier sent by Alice, the information communication channel between Alice and Bob can be modeled as a flow of information from Alice to Bob through a binary erasure channel. Bob uses a POVM for raising the efficiency he can confirm the quantum state. The measurement operator is $B_{u'} = \frac{1-v'v'^{+}}{1+\langle u'|v'\rangle}$, $B_{v'} = \frac{1-u'u'^{+}}{1+\langle u'|v'\rangle}$, $B_? = 1 - B_{u'} - B_{v'}$ respectively. The probability Bob measuring $|u'\rangle$ and $|v'\rangle$ with them is $tr(\rho_{u'}B_{u'})$ and $tr(\rho_{u'}B_{v'})$, $tr(\rho_{u'}B_?)$, $tr(\rho_{v'}B_u)$, $tr(\rho_{v'}B_{v'})$, $tr(\rho_{v'}B_?)$. Among them $tr(\rho_i B_?)$ ($i = u'$ or v') means a probability that Alice sends out the state $|i\rangle$ and Bob gains a no certain state, $tr(\rho_i B_j)$ ($i, j = u'$ or v') means a probability that Alice sends out the state $|i\rangle$ and Bob gains state $|j\rangle$,when $i \neq j$, it is error transmission probability. We have a transmission matrix of quantum communication channel between Alice and Bob, it was written as $P_{ab}(j/i)$, schematized in Table 6.

Table.6 $P_{ab}(j/i)$

The transmission matrix of quantum communication channel between Alice and Bob

i \ j	$\|u'\rangle$	?	$\|v'\rangle$
$\|u'\rangle$	$\frac{\cos^2(\alpha+\beta)}{1+\sin 2\alpha}$	$\frac{(1+\sin 2\beta)\sin 2\alpha}{1+\sin 2\alpha}$	$\frac{\sin^2(\alpha-\beta)}{1+\sin 2\alpha}$
$\|v'\rangle$	$\frac{\sin^2(\alpha-\beta)}{1+\sin 2\alpha}$	$\frac{(1+\sin 2\beta)\sin 2\alpha}{1+\sin 2\alpha}$	$\frac{\cos^2(\alpha+\beta)}{1+\sin 2\alpha}$

Using it and $P(a_i) = 1/2$ in Eqs.(3), the mutual information between Alice and Bob is given by

$$\begin{aligned} I_{ab}(X,A) = \frac{1}{1+\sin 2\alpha}[&1 - \sin 2\alpha\sin 2\beta + \cos^2(\alpha+\beta)\log\cos^2(\alpha+\beta) + \\ &\sin^2(\alpha-\beta)\log\sin^2(\alpha-\beta) - (1-\sin 2\alpha\sin 2\beta)\log(1-\sin 2\alpha\sin 2\beta)] \end{aligned} \tag{19}$$

We have the Bob's bits error rate before screening data

$$q_{e(ab)} = \frac{\sin^2(\alpha-\beta)}{1+\sin 2\alpha} \tag{20}$$

According to Eqs.(16)～(20), the relation between the mutual information and angle γ of Bob's probe state, the bits error rate and γ, the characteristic and boundary of I_{ae} and I_{ab} all can be given in Fig.2, we have a few another following conclusions

i . I_{ae} is minimum and has bottom boundary ($I_{ae}=0$) for $\gamma=\frac{\pi}{4}$, I_{ae} is maximum and has up boundary ($I_{ae}=1$) for $\gamma=0$.

ii . I_{ab} is minimum and has bottom boundary ($I_{ab}=0$) for $\gamma=\alpha$; I_{ab} is maximum and has up boundary ($I_{ab}=1-\sin 2\alpha$) for $\gamma=\frac{\pi}{4}$.

iii.With increasing γ, I_{ab} is more and more bigger and Bob's error rate $q_{e(ab)}$ is decrescent.

iv.With increasing γ, I_{ae} is decrescent and Eve's error rate $q_{e(ae)}$ is more and more bigger

v .While $\gamma\to 0$, we know that $I_{ab}<I_{ae}(=1)$, it indicates this strategy is "strong" eavesdropping. When $\gamma\to\pi/4$, $I_{ab}(=1-\sin 2\alpha)>I_{ae}(=0)$ was given and indicate this strategy is "weak" eavesdropping.

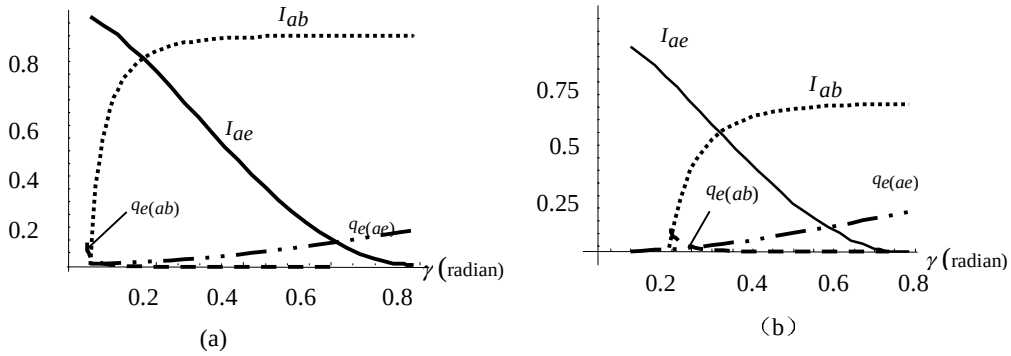

Fig.2 The mutual information and the bits error rate between Alice, Bob, and Eve depend on the angle γ of Bob's probe state (a) for $\alpha=\pi/32$, (b) for

In checking the eavesdropper Eve, if Bob measures the quantum carrier by POVM and the bits error rate before screening data is $q_{e(ab)}\neq 0$ (while $\gamma\neq\frac{\pi}{4}$), Eve's eavesdropping should be considered occurring according to Eqs.(15) and Eqs.(20). When Bob's measurement way is same as Eve's orthogonal projecting measurement way, his bits error rate before screening data also is $\sin^2\alpha$ in no Eve's eavesdropping, it indicates that Eve's eavesdropping should be considered occurring on condition that Bob's error rate before screening data is $q_{e(ab)}>\sin^2\alpha$ as same as the case 3.2.1.

4 CONCLUSIONS

Now, it was gained that if Bob's bits error rate before screening data is $q_e \neq 0$ by POVM or $q_e > \sin^2 \alpha$ by orthogonal projecting measurement way, Eve's eavesdropping should be considered occurring in the previous two case of Eve's eavesdropping. After discarding the inconclusive results, Bob, in public discussion with Alice, will estimate his bits error rate with $Q = q/(1-R)$, ($R = \langle u | A? | v \rangle$ or $R = \langle u' | B'? | v' \rangle$). An criteria of another form for checking the eavesdropper and ensuring the legal correspondent can be given, we will discuss it in other paper.

In actual correspondence system, the influence of the environment noise and the detecting efficiency of Bob's detector, will bring the rising of Bob's error rate. Under the condition that we can't make sure completely whether the information have been eavesdropped, in order to prevent the eavesdropper from acquiring as more information as possible, after completing the quantum states deliver, we must still complete a few processes the data filtration, the data error correction and privacy amplification, can make the information that Eve acquire minimum or her don't know. In a word, we will achieve improving the safety of the cryptography or information and the safety of the quantum cryptography correspondences.

In this paper, we study respectively the mutual information between the signal's deliverer, the legal receiver and the eavesdropper, the bit error rate before screening data during propagating the signals with the theory about the quantum measurement channel and the quantum information theory, for B92 protocol. A new criteria for checking the eavesdropper and ensuring the legal correspondent is estimated. Of course, the mutual information that Eve and Bob acquire respectively is variational and the relation between them is different under the different attack method.

The quantum cryptographical system is a kind of all new concepts to the encryption system, currently its best application is in the quantum key distribution. Certainly the application of the quantum cryptography is not only in this aspect, other for example unconditional and safe quantum attestation, keeping secret of personal information etc. In the practical aspect, we think the quantum cryptography system has been start head for practical turn, hope to enter the company to be used before long, especially while the quantum computer becomes the actuality, the encryption system of past will have no any secret. At that time the quantum cryptography system may become one of the best choices, thus there are the really fine market foreground and science values for it.

REFERENCES

1 C H Bennett, G Brassard. *Proceedings of IEEE International Conf. Computer, Systems, and signal Processing*[M].Bangalore, India(IEEE, New York,)1984 ,175

2 A K Ekert. Quantum cryptography based on Bell's theorem[J]. *Phys.Rev.lett,*1991,67: 661～663

3 C H Bennett. Quantum cryptography using two non-orthogonal states[J]. *Phys.Rev.lett,*1992,68 : 3121～3124

4 H K Lo, H F Chau. Unconditional Security of Quantum Key Distribution over Arbitrary Long Distances[J]. *Science,*1999, 283 : 2050～2056

5 D Mayers. On the security of the quantum oblivious transfer and key distribution protocol [J]. *Proc. Crypto,*1996 ,343

6 P W Shor, J Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol[J] . *Phys .Rev. Lett,*2000, 85: 441

7 R J Hughes, G L Morgan, C G Peterson. Quantum key distribution over 48km optical fibre network[J].

J.*Mod.Opt*,2000, 47 : 533

8 Zhi-xin CHEN, Zhi-lie TANG, et al. Quantum Cryptography and Secure Communications [J]. *CHINESE JOURNAL OF QUANTUM ELECTRONICS*. 2003,Vol 20, (385)

9 Gui-hua ZENG, Xin-mei WANG, Hong-wen ZHU. Information investigation for BB84 protocol in quantum cryptography[J].*Journal of China Institute of Communications*. 2000,Vol 21,6(2000)

10 A K Ekert, B Huttner, *et al.* Eavesdropping on quantum cryptographical systems [J]. *Phys .Rev. A*,1994,50:1047—1055

*Email:zming394@yahoo.com.cn; **phone:**027-87150886