A new attack strategy for BB84 protocol based on Breidbart basis

LIU Dan, PEI Chang-xing, QUAN Dong-xiao, HAN Bao-bin, ZHAO Nan
State Key Lab. of Integrated Services Networks, Xidian Univ.
Xi'an, 710071,China
secret_ren@sohu.com, chxpei@xidian.edu.cn, dxquan@xidian.edu.cn
hanbaobin@163.com, zhaonanonline@hotmail.com

***Abstract*—A new eavesdropping strategy for BB84 quantum key distribution protocol is proposed. This scheme is a new kind of intercept/resend strategy based on Breidbart basis. Under this scheme, eavesdropper can not only exactly obtain the exchanged information between legitimate users but also decrease the probability of being detected.**

Keywords-Eavesdropping strategy; BB84 protocol; quantum cryptography; Breidbart basis

I. INTRODUCTION

Quantum key distribution (QKD), which enables two legitimate users to share a secure key, has attracted more and more interests for its unconditional security guaranteed by Heisenberg uncertainty principle and quantum no-cloning theory. The first QKD protocol was proposed in 1984 by Charles H. Bennett and Gilles Brassard [1]. In BB84 protocol, Alice sends Bob a sequence of single photons each of which is randomly prepared in one of the two conjugate bases. Bob measures each photon randomly in one of these two conjugate bases. Alice and Bob then compare the bases by public channel and keep only those bits sent or measured in the same bases. They randomly test a subset of those bits to evaluate the quantum bit error rate (QBER). If the QBER is larger than the threshold, they abort the protocol. Otherwise, they proceed to the classical data post-processing (which consists of error correction and privacy amplification) and generate a secure key.

The crucial issue of the QKD protocol is its security. The realistic apparatus are imperfect and therefore such imperfection may be utilized by an eavesdropper, Eve, to eavesdrop on the communication. Assuming that Eve is only limited by the laws of quantum mechanics, and she is able to use any unitary interaction. The analysis of the types of attacks that Eve can make on quantum key distribution protocols is the subject of intense research [2-5]. An important goal of this research is to find upper bounds on the amount of secret key information that may be eavesdropped by Eve. Here we consider eavesdropping attacks on BB84 protocols that Alice uses a single photon source to send photons to Bob.

The simplest incoherent attack strategy is intercept/resend scheme. In this scheme, Eve intercepts selected photons and measures them in the bases that she randomly chooses. When this occurs, Eve sends fake photons of the same polarization as she detected to Bob. However, due to uncertainty principle, at least 25% of the photons Eve fabricates will yield the wrong results if later successfully measured by Bob.

In this paper we propose a novel intercept/resend strategy for BB84 protocol based on Breidbart basis [2]. The scheme can be described as follows: Eve intercepts and keeps the photons Alice sends to Bob in the quantum memory. Then she randomly sends a sequence of photons polarized with Breidbart basis to Bob. When Alice and Bob communicate in public channel, Eve can know which basis is correct and measures the photons that she kept to get the right information.

II. NEW ATTACK SCHEME ON BB84

With the development of technology, the realization of single photon source and quantum memory are just around the corner [6,7,8]. Eve can use these new technologies and Breidbart basis to eavesdrop and get more information [9-15]. The new attack scheme, as shown in Figure1, can be described as follows:

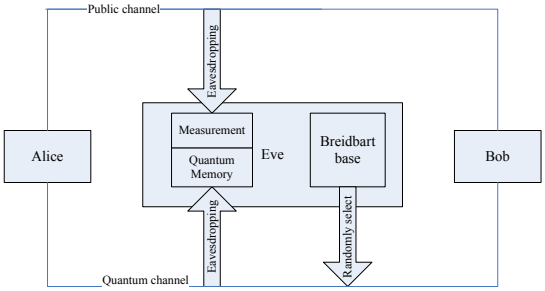

Figure 1. new attack on BB84

Project supported by the National Natural Science Foundation of China (Grant No. 60572147，No. 60672119), the 111 Project(B08038) and the State Key Lab. of Integrated Services Networks(ISN 02080002)

1. Alice prepares a random sequence of photons polarized with one of the two conjugate bases and sends them to Bob;
2. Eve intercepts and stores photons in quantum memory, and she sends a sequence of photons polarized with Breidbart basis randomly, which will decreases the probability of being detected;
3. Bob measures received photons using a random sequence of basis. Bob's measurement results show that some photons are lost owing to channel losses and imperfect detector efficiency;
4. Bob tells Alice which basis he used for each received photon; Alice tells him which bases are correct. Alice and Bob keep only the data from these correctly measured photons, discarding all the rest;
5. By eavesdropping on public channel, Eve can also know the right basis, then she measures the photons that she kept in quantum memory, and she will get the right result;
6. Alice and Bob randomly test a subset of those bits and determine the QBER. If the QBER is larger than some prescribed value, they abort the protocol. Otherwise, they proceed to the classical data post-processing and generate a secure key.

III. SECURITY ANALYSIS

The four states Alice sends to Bob in the BB84 protocol are:

$$|x\rangle = \frac{1}{\sqrt{2}}\left(|u\rangle + |v\rangle\right)$$

$$|y\rangle = \frac{1}{\sqrt{2}}\left(|u\rangle - |v\rangle\right)$$

$$|u\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle + |y\rangle\right)$$

$$|v\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle - |y\rangle\right)$$

In traditional intercept/resend attack, Eve measures one photon that Alice sends to Bob and gets the result, and then she prepares one of the two states and sends it to Bob. The two measurement operators Eve used must satisfy: $M_0 + M_1 = I$ ($M_0 = \langle 0|0\rangle$, $M_1 = \langle 1|1\rangle$). The probability with which Eve gets the correct result is

$$P_c = \frac{1}{4}\left[\langle x|M_0|x\rangle + \langle v|M_0|v\rangle + \langle y|M_1|y\rangle + \langle u|M_1|u\rangle\right] \quad (1)$$

The two states $|0\rangle$ and $|1\rangle$ are given by:

$$|0\rangle = \cos\theta|x\rangle - \sin\theta|y\rangle$$

$$|1\rangle = \sin\theta|x\rangle + \cos\theta|y\rangle$$

Where θ is a variable angle taken clockwise from horizontal direction. Substituting the forms of M_0 and M_1 into equation can get:

$$P_c = \frac{1}{2} + \frac{1}{4}\left(\sin 2\theta + \cos 2\theta\right) \quad (2)$$

TABLE I. THE DETERMINE PROBABILITY OF BREIDBAT BASIS $p(b_j|a_i)$

	0	$\frac{\pi}{4}$	$\frac{\pi}{2}$	$\frac{3\pi}{4}$
	a_1	a_2	a_3	a_4
b_1	$\cos^2(\theta)$	$\cos^2(\theta+\frac{\pi}{4})$	$\cos^2(\theta+\frac{\pi}{2})$	$\cos^2(\theta+\frac{3\pi}{4})$
b_2	$\cos^2(\theta-\frac{\pi}{2})$	$\cos^2(\theta-\frac{\pi}{4})$	$\cos^2(\theta)$	$\cos^2(\theta+\frac{\pi}{4})$

To maximize P_c with respect to θ we can get

$\frac{dP_c}{d\theta} = -\frac{1}{2}\left(\sin 2\theta - \cos 2\theta\right) = 0$, $\theta = 22.5^\circ$, be known as Breidbart basis, $P_c = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right)$。

With Breaibart basis the table can be simplified as：

TABLE II. THE DETERMINE PROBABILITY OF BREIDBAT BASIS $p(b_j|a_i)$

	0	1
$\frac{\pi}{8}$	$\cos^2(\frac{\pi}{8})$	$\sin^2(\frac{\pi}{8})$
$\frac{5\pi}{8}$	$\sin^2(\frac{\pi}{8})$	$\cos^2(\frac{\pi}{8})$

The probability with which Eve causes a disturbance can be present as:

$$D = P_c\langle 0|M_y|0\rangle + (1-P_c)\langle 1|M_y|1\rangle \quad (3)$$

$M_y = \langle y|y\rangle$ is the outcome of Bob's measurement. Being sent if $|0\rangle$ and $|1\rangle$ are equal, it reduced to：

$$D = 2P_c\left(1 - P_c\right) \qquad (4)$$

Alice and Bob check for Eve's presence by measuring the error rates of their sifted key after the public announcement of the basis. So we get $D(\varepsilon) = \frac{\varepsilon}{4}$, and $D_{\max} = \frac{1}{4}$, when $\varepsilon = 1$.

The traditional intercept/resend attack tells Eve the value of Alice's bits with the probability at most 85%, while inducing an error with probability at most 25% for each fabricated photons that later successfully measured by Bob in the correct original basis.

In the new scheme, after Bob has made his measurement, Alice reveals the bases in which she prepared her photons through a public channel. Bob then tells her whether or not he measured in the same bases. If he did not detect a photon, the bits are discarded but if the same bases were used they keep the bit and both parties should now hold the same results of the bit's value. The procedure is repeated until Alice and Bob hold a long string of bits.

Eve keeps the photons Alice sends to Bob in quantum memory, and sends photons prepared randomly with Breidbart basis to Bob. So after intercepting communication between Alice and Bob in public channel, Eve can get the right measure bases and get the correct information.

The probability of every bit with which sent by Eve and measured correctly by Bob is $\cos^2(\frac{\pi}{8})$, the probability D is a disturbance or error caused by Eve, can be given as:

$$D = \frac{\varepsilon}{2}\left(1 - \cos^2\left(\frac{\pi}{8}\right)\right) \qquad (5)$$

$D = 0.1357$, when $\varepsilon = 1$

This new attack tells Eve the value of Alice's bits with the probability at most 100%, while inducing an error with probability at most 13.57% for each fabricated photons that later successfully measured by Bob in the correct original basis, smaller than 25%, a traditional error rate threshold Alice and Bob will detect if Eve is existing. The difference between this new strategy and traditional intercept/resend strategy is Eve resends the photons with Breidbart basis to Bob, which will cause an error rate smaller than traditional threshold and would not be detected, while she keeping photons sent from Alice in quantum memory. After Alice and Bob compare measurement basis, Eve can intercept again and get all correct measurement basis, then she measures the kept photons and gets keys almost 100%. The only way to prevent this new eavesdropping strategy is to choose a suitable error rate threshold.

IV. CONCLUSION

In conclusion, we proposed a new intercept/resend attack strategy based on Breidbart basis for BB84 key distribution protocol in the quantum cryptography. Under this strategy, the BB84 quantum cryptographic protocol is at risk. The eavesdropper can not only exactly obtain the information between the legitimate users but also decrease the probability of being detected. Eve can be detected only if Alice and Bob choose a suitable error rate threshold. Of course, the presented strategy is only valid for the case that the quantum state is encoded in transit.

REFERENCES

[1] C H Bennett, G. Brassard Quantum Cryptography: Public Key Distribution and Coin Tossing［A］. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing［C］. Bangalore: IEEE, 1984. 175-179.

[2] C H Bennett, F Bessette, G Brassard, et al. Experimental quantum cryptography. Journal of Cryptology, 1992, **5**(1):3-28

[3] 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 (A) ,1997 ,**56** (2) :1163-1172

[4] Williamson M , Vedral V. Eavesdropping on practical quantum cryptography. J ournal of Modern Opt ics , 2003 ,50 (13) :1989-2011

[5] G Gilbert, M Hamrick, Constraints on Eavesdropping on the BB84 Protocol, arXiv: 0106034v2, 2001, http://arxiv.org/PS_cache/quant-ph/pdf/0106/0106034v2.pdf

[6] S. Chen, Y-A Chen, T. Strassel, Z-S Yuan, B Zhao, J. Schmiedmayer, J-W Pan, Deterministic and Storable Single-Photon Source Based on Quantum Memory, Phys. Rev. Lett **97**, 173004 (2006)

[7] C S Chuu, T Strassel, B Zhao, M Koch, Y A Chen, S Chen, Z S Yuan, J Schmiedmayer, and J W Pan, Quantum memory with optically trapped atomsvol. Physical Review Letters, 101, 120501(2008)

[8] B Zhao, Y-A Chen, X-H Bao, T Strassel, C-S Chuu, a-M Jin, J Schmiedmayer, Z-S Yuan, S Chen, and J-W Pan, A millisecond quantum memory for scalable quantum networks, arXiv:0807.5064v1, 2008 ,http://arxiv.org/PS_cache/arxiv/pdf/0807/0807.5064v1.pdf

[9] M A Nielsen and I L Chuang , Quantum Computation and Quantum Information Cambridge University Press, Cambridge, Unites Kingdom,2000

[10] 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, Vol21 (6),70-73

[11] YANG LI, Ling-An Wu, Song-Hao Liu, et al. On the Breidbart eavesdropping problem of the extend BB84 QKD protocol. Acta Physica Sinica,2002, **51**(5):961-965

[12] Jing-Feng Liu, Zhi-Lie Tang, Song-Hao Liu, et al. Eavesdropping on practical QKD system based on six-state protocol. Acta Physica Sinica, 2005, **54**(2):517-521

[13] Jing-Feng Liu, Rui-Sheng Liang, Zhi-Lie Tang, et al. Eavesdropping of practical QKD system based on BB84 protocol. Acta Photonica Sinica, 2004 **33**(11):1356-1359

[14] Zhi-Xin Chen, Zhi-Lie Tang, Song-Hao Liu, et al. On the Breidbart eavesdropping information problem of BB84 QKD protocol. Acta Photonica Sinica, 2004 **33**(12):1469-1472

[15] Zhi-Xin Chen, Zhi-Lie Tang, Song-Hao Liu, et al. Practical security problem of six-state QKD protocol. Acta Photonica Sinica, 2006 **35**(1):126-129