PRAMANA
— journal of
physics

Vol. 64, No. 1
January 2005
pp. 1–4

Failure of Kak quantum key distribution protocol

CHING-NUNG YANG*, SU-HSUAN CHU and BING-LING LU
Department of Computer Science and Information Engineering, National Dong Hwa University, 1, Sec. 2, Da Hsueh Rd., Shou-Feng, Hualien, Taiwan, Republic of China
*Corresponding author. E-mail: cnyang@mail.ndhu.edu.tw

MS received 24 March 2004; revised 28 August 2004; accepted 8 October 2004

Abstract. Kak's quantum key distribution (QKD) protocol provides not only the distribution but also the integrity of secret key simultaneously in quantum channel. Consequently the additional exchange of information, used to check whether an eavesdropper exists, is unnecessary. In this comment, we will point out the failure of Kak's protocol and show that Kak's protocol does not have the joint distribution and integration that the author declares in [1].

Keywords. Quantum cryptography; quantum key distribution.

PACS No. 03.67.Dd

1. Introduction

As we know, quantum encryption provides more security in a variety of cryptography tasks than conventional methods. There are many interesting topics in quantum information science and how to distribute the secret key is one of the important topics in this area. The most famous QKD protocol, BB84 [2], was invented in 1984 by Bennett and Brassard. It is also the first QKD scheme, which uses the uncertainty principle to reach the perfect secrecy on sharing the secret key.

In BB84 protocol, Alice and Bob randomly choose m bits of the shared key after distribution to test whether there is an eavesdropper (Eve) between them via the public channel. This takes more time and decreases the efficiency of key sharing, because the chosen bits need to be discarded after the test process. To avoid the waste of m test bits, Kak proposed a new QKD protocol using three basis states [1], which is a variant of BB84 protocol. Kak's new protocol is trying to combine the distribution and integration of secret key similar to joint encryption and error-correcting code together in [3]. Although Kak's protocol seems to be a novel idea of joint distribution and integration, it has a serious weakness. In this comment, we will prove that Kak's protocol will become useless, i.e., Alice and Bob cannot know whether they share the correct key or not.

Table 1. Photon and detector states (A: Alice; B: Bob).

A's data	0	0	0	k	k	k	1	1	1
B's filter	0	k	1	0	k	1	0	k	1
B may receive	0	k/e	e	$0/e$	k	$1/e$	e	k/e	1
B's result	Y	Y	N	N	Y	Y	N	N	Y
Secret key	0	–	0	–	k	–	1	–	1

This comment is organized as follows: Kak's QKD protocol is introduced in §2 and §3 shows the failure of Kak's protocol.

2. Quantum key distribution using three basis states

In Kak's QKD protocol, the photons are prepared by Alice in the polarization of 0 (represented as 0), 45 (represented as k) and 90 (represented as l) degrees, respectively. At the destination end, Bob uses the filters (0-filter, 1-filter or k-filter) to detect. After the transmission, Alice and Bob share the filter status from the public channel and then decide the shared secret key. The difference between Kak's protocol and BB84 protocol is that Kak's protocol reduces the number of photon polarization from four to three and changes the number of detector's states from two (which is equivalent to four) to three.

Table 1 summarizes nine different situations of the photons and detector's states. The first row is the data sent from Alice; the second row is Bob's filter setting; the third row shows what Bob may receive. Bob's result (the fourth row) shows whether the photon is detected or not; 'Y' means 'Yes' and 'N' means 'No'. The final shared secret key is shown in the last row.

Here is the detailed description of table 1. In the first column, since Bob detects the light he knows that Alice sends 0; in the mean time although Eve knows Bob's filter, she does not know whether Bob detected the light or not. Therefore, Eve cannot know that the secret key is 0 or 1. In the third column, since Bob does not detect the light he knows that Alice's data is 0, and then he changes the data from e to 0; however Eve does not know whether Bob has detected the light or not and she cannot get the correct data. In the fifth column, since Eve knows that Bob selects the correct k-filter, the k-photon cannot be used to represent the information. When Alice and Bob has not negotiated their filter status yet, Eve has intercepted the photon and compromised the quantum state and so she may not resend the correct one. Thus, although we cannot use the k-photon to represent the information, we can use it to detect the eavesdropping. The situations of the seventh and ninth columns are similar to third and first columns. Other columns in table 1 are the wrong choices of Bob's filter and will not contribute any information.

As we can see, five of the nine bits are useful, but only four bits of them are secure and can be used as the key. The fifth bit (k-photon) helps in authenticating the integrity. When n bits are sent, $4n/9$ bits are used for key and $n/9$ bits for checking interception. Since there is a 1/3 probability that Eve would have used the correct filter when intercepting the photon sequences and resend with her own, the certification probability for n bits will be $1–3^{-n/9}$. Compared to the four-state

BB84 protocol with $(n/2) - m$ key bits and certification probability $1–2^{-m}$, Kak's protocol has more key bits for $n < 18m$ and furthermore the certification probability is higher [1]. The two certification probabilities will be the same when $1–3^{-n/9}$=$1–2^{-m}$, and the certification probability of BB84 is higher for $m > 0.176n$. This is impossible because the effective values of m in the three-state protocol is only $n/9$. Obviously, Kak's protocol provides not only the ability of authentication, but also better efficiency under certain situations.

3. The failure of Kak's protocol

As we know, in a successful quantum key distribution scheme such as BB84 and B92 [4], Alice and Bob can detect Eve by the physical property caused by uncertainty principle, because Eve cannot discriminate among the receiving states. For example, in BB84 protocol, Eve may have intercepted some of the photons that Alice sends to Bob. However, any measurement she makes on photons will inevitably disturb the quantum states. If she chooses the same filter to measure as Bob, Eve will not be detected. However, Eve does not know which filter Bob will choose to measure the photons. If Eve measures in the diagonal filter (45 and 135 degree) and Bob measures in the orthogonal filter (0 and 90 degree) or vice-versa, Bob's result will be random. That means that Alice and Bob can randomly choose m bits from the shared key bits for certification with successful probability $1–2^{-m}$. But in Kak's protocol, there is a trivial method to cause the failure. When Eve always resends k-photons to Bob with 100% probability, Alice and Bob do not know whether an eavesdropper exists because the k-photons will be all correct; this is because k-photon is used for authentication in Kak's protocol. Actually, the trivial method shows that using only a single state, k-polarized state in Kak's protocol, will be a failure. However, if Eve always resends k-photons for all quantum data, Bob can choose k-filter to detect all the quantum bits first. Then, Bob will have 100% probability to get the state k. For the normal transmission ($p_0 = 1/3, p_1 = 1/3$ and $p_k = 1/3$ are the probabilities for 0, 1 and k, respectively), Bob should get the k-photon with $(2/3)(= ((2n/3) \times (1/2) + (n/3))/n)$ probability. Thus by comparing the detection probability, he will detect the eavesdropping. A more reasonable way to resend k-photons by Eve to compromise Kak's protocol is given below.

As shown in figure 1, Eve uses the filter with 135 degree polarization to intercept the quantum data from Alice. If the intercepted data is k-photon, then Eve will not detect the light. If the data is 0 or 1, Eve will have 50% probability to detect the light, and 50% probability to detect nothing. Suppose that Eve resends k-photon to Bob when she detects nothing and randomly resends 0 or 1 if she detects the light. When Alice's data is k-photon Eve will correctly resend k-photon with 100% probability. The information of k-photon is unchanged. Because Kak's protocol uses the strings of k-photon to procure the authentication of the key integrity, Bob's authentication mechanism will not work any more. Finally, Alice and Bob are not sure that they share the correct key unless they use some bits of the shared key to check the correctness like BB84 protocol. The detection probability for this case will be $(5/6)(= ((n/3) \times (1/2) + (2n/3))/n)$ when Bob uses k-filter and thus Bob can use the detection probability to detect whether the eavesdropper exists. For reducing

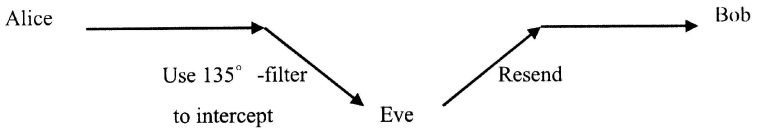

Figure 1. Eavesdropping strategy, intercept-resend strategy of Eve.

the probability to 2/3, the detection probability for a normal transmission, Eve can resend the k-photons with probability q when she detects nothing. The detection probability will be $((((n/3)+(2n/3)\times(1-q))\times(1/2)+(2n/3)\times q)/n) = (3+2q)/6$. Choosing $q = 1/2$, we have $(3+2q)/6 = 2/3$, and since there is a q probability that Eve would resend the correct k-photons, the certification probability for n bits is $1–q^{n/9} = 1–2^{-n/9}$, i.e., Bob needs 1.58 times number of bits to assure the same certification probability ($\because$ $1–2^{-n_1/9}$=$1–3^{-n_2/9}$, $\therefore$ $n_1/n_2 = \log 3/\log 2 = 1.58$).

References

[1] S Kak, *Pramana – J. Phys.* **54**, 709 (2000)
[2] C H Bennett and G Brassard, *Proceedings of the IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984) pp. 175–179
[3] S Kak, *IEEE Trans. Comput.* **C34**, 803 (1985)
[4] C H Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992)