Optics Communications 283 (2010) 1192–1195

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

# Quantum key agreement protocol based on BB84

Song-Kong Chong, Tzonelih Hwang *

*National Cheng-Kung University, Department of Computer Science and Information Engineering, No. 1, Ta-Hsueh Road, Tainan City 701, Taiwan, ROC*

ARTICLE INFO

*Article history:*
Received 26 May 2009
Received in revised form 10 November 2009
Accepted 10 November 2009

*Keywords:*
Quantum key agreement
BB84

ABSTRACT

This work presents a quantum key agreement (QKA) based on the BB84 protocol. The newly proposed QKA protocol enables two involved parties to jointly establish a shared secret key in such a way that the shared secret key cannot be fully determined by one party alone. In contrast to the traditional key agreement protocols that must be based on some mathematical difficulties, the security of the newly proposed protocol is based on the quantum phenomena, which allows unconditional security as well as detection of eavesdroppers. With the technique of delayed measurement, the proposed protocol has 50% qubit efficiency. Therefore, it is very efficient and feasible for practical applications.



## 1. Introduction

A key agreement protocol is one whereby two or more parties agree upon a key over insecure communication channels based on their exchanged messages [1,2]. In contrast to the key distribution [2–4], where one party decides the key and then distributes it to the other parties, each party in a key agreement protocol contributes its part to the shared key [3,5,6], and the shared key should not be determined fully by any party alone [5,7].

Traditionally, the security of key agreement protocols must be based on some mathematical difficulties [8–12], e.g. solving the discrete logarithm problem or factoring large numbers. However, it is believed that these mathematical difficulties may be fragile in the future with the presence of quantum computers [13–15]. Therefore, the development of quantum key agreement protocols which are secure against quantum computations becomes a significant research topic.

The study of quantum key agreement protocols (QKA) was first tried by Zhou et al. [16] in 2004. Their protocol uses the quantum teleportation technique to generate a secret key over public channels. However, Zhou et al.'s protocol was later pointed out by Tsai and Hwang [17] that a party can fully determine the shared key alone and then distribute it to the other party without being detected. Therefore, Zhou et al.'s protocol is not a fair QKA. Tsai and Hwang considered that their improvement still is not a QKA because the shared secret key is a sequence of random measurement results without being negotiated by both involved parties.

This work employs the unitary operations and the delayed measurement technique [18] to modify the BB84 protocol [19] so that both parties can negotiate a shared secret key. The proposed QKA protocol allows a sender, say Alice, to encode her contribution into photons and to send them to a receiver, say Bob, via a quantum channel. After that Bob will encode his contribution into the received photons (by using unitary operations). After announcing his contribution to Alice, Bob receives the original polarization basis information from Alice through the classical channel. Finally, both parties negotiate a shared key accordingly. This proposed protocol has the following advantages:

(1) The outcome of the protocol is influenced by both parties; no one can determine the shared key alone.
(2) The protocol has 50% qubit efficiency after the random sampling discussion; and
(3) It provides the unconditional security.

The rest of this paper is structured as follows: The BB84 protocol and the quantum unitary operations will be introduced in the next section. Section 3 presents the proposed QKA protocol. Then, the security analysis is given in Section 4. Section 5 concludes our result.

## 2. Preliminaries

The BB84 protocol [19] is one of the best known unconditional secure QKD protocols whose security has been proved by many studies. Two polarization bases, the rectilinear basis (R_basis) and the diagonal basis (D_basis), are used in the protocol. In R_basis, a photon is polarized to $|0\rangle$ or $|1\rangle$, in D_basis, $|+\rangle$ or $|-\rangle$. The participants must agree on how to encode each polarization state $(|0\rangle, |1\rangle, |+\rangle, |-\rangle)$ in binary representation. For instance, $|0\rangle$ or $|+\rangle$ can be used to code "0" bit, and, $|1\rangle$ or $|-\rangle$, the "1" bit.

The BB84 is classified as a quantum key distribution (QKD) protocol because a party, say Alice, can decide a key alone and then

* Corresponding author.
*E-mail address:* hwangtl@ismail.csie.ncku.edu.tw (T. Hwang).

0030-4018/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2009.11.007

distribute it to the other party, say Bob. Although Alice cannot know which transmitted qubits will be used as a key and which will be used in the random sampling discussion, in the extreme case, she can set the key as all "1" bits (or all "0" bits) and then polarize the photons to $|1\rangle$ or $|-\rangle$ ($|0\rangle$ or $|+\rangle$). Accordingly, the shared key will be decided by Alice.

In this paper, the quantum unitary operations, $I$, $X$ and $Z$ are used to change the state of a qubit from $|\psi\rangle$ to $|\psi'\rangle$, where

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$
$$X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Notice that the state of $|\psi\rangle$ will remain unchanged in $I$ gate, i.e. $I|\psi\rangle \mapsto |\psi\rangle$. But if applying unitary operator $XZ$ to $|\psi\rangle$, the state is changed, i.e., $XZ|\psi\rangle \mapsto |\psi'\rangle$. More precisely, $XZ|0\rangle \mapsto |1\rangle, XZ|1\rangle \mapsto |0\rangle$, $XZ|+\rangle \mapsto |-\rangle$, and $XZ|-\rangle \mapsto |+\rangle$. (Note that the global phase introduced by the operator $XZ$ is ignored because it does not affect the statistics of a measurement [20].)

## 3. The proposed protocol

The proposed QKA protocol utilizes two unitary operations, $I$ and $XZ$, for Bob to modify the polarization states of Alice's quantums randomly. Additionally, with the delayed measurement technique [18], Bob can measure and decode each qubit sent by Alice. Similar to Zhou et al.'s protocol [16] as well as most of the existing QKD protocols [19,21–24], the classical communication channels are assumed to be authenticated in the proposed QKA protocol, in which the identity of the communicating parties have been verified and the integrity of the transmitted messages is promised. The details of the proposed QKA protocol are described as follows.

Suppose that there are two parties, Alice and Bob, involving in a QKA protocol. Alice is equipped with a quantum generator. Bob is with a quantum state storage and quantum logic gates, $I$ and $XZ$. The purpose of this protocol is for Alice and Bob to agree upon a secret key over an insecure quantum channel wherein no one can determine the shared key alone. The agreed key can be used later to secure their subsequent communications. The proposed QKA protocol proceeds in the following steps (see also Fig. 1):

**Step 1** Alice randomly selects two $n$-bit strings $K_A = \{k_A^1, k_A^2, \ldots, k_A^n\}$ and $B_A = \{b^1, b^2, \ldots, b^n\}$, where $k_A^i$ and $b^i$ denote the $i$th bit of the $K_A$ and $B_A$, respectively, for $1 \leqslant i \leqslant n$. $K_A$ represents Alice's contribution and $B_A$ signifies the polarization bases used to encode $K_A$.

**Step 2** Alice generates the corresponding photons into one of the following four photon states $|\psi_{k_A^i,b^i}\rangle$ according to the bit information of every pair of $k_A^i$ and $b^i, 1 \leqslant i \leqslant n$:

$$|\psi_{0,0}\rangle = |0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle),$$
$$|\psi_{1,0}\rangle = |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle),$$
$$|\psi_{0,1}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$|\psi_{1,1}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

In the above encoding process, if $b^i = 0, k_A^i$ is encoded by using R_basis, and if $b^i = 1$, D_basis is used. After that, Alice sends the photons to Bob in sequence through a quantum channel.

**Step 3** Upon receiving the photons, Bob randomly selects an $n$-bit contribution $K_B = \{k_B^1, k_B^2, \ldots, k_B^n\}$ to change the states of the photons received from Alice as follows, for $1 \leqslant i \leqslant n$:

- If $k_B^i = 0$, then $I|\psi\rangle \mapsto |\psi\rangle$
- If $k_B^i = 1$, then $XZ|\psi\rangle \mapsto |\psi'\rangle$

Then, Bob preserves all these $n$ photons into a quantum memory.

**Step 4** Bob randomly chooses $m$ out of $n$ photons as a checking set $C$ for public discussion. He announces the positions of the selected $m$ photons and $K_B$ to Alice via an authenticated classical channel.

**Step 5** According to the bits value of $K_B$, Alice derives the raw key as $K_{AB} = K_A \oplus K_B = \{k_A^1 \oplus k_B^1, k_A^2 \oplus k_B^2, \ldots, k_A^n \oplus k_B^n\}$. Afterward she sends $B_A$, and the contents of $C$ ($C$'s values are extracted from $K_{AB}$ according to the position announced by Bob) to Bob via the authenticated classical channel.

**Step 6** Upon receiving the messages from Alice, Bob measures all preserved photons according to the values of $B_A = \{b^1, b^2, \ldots, b^n\}$, i.e., if $b^i = 0$, R_basis is used, and if $b^i = 1$, D_basis is used, for $1 \leqslant i \leqslant n$. Bob decodes his measurement results as the raw key $K_{AB}$. Then, he compares the corresponding measurement results with the received $C$. If the comparing results are identical, then there is no eavesdroppers and Bob sends an acknowledgment to Alice via the authenticated classical channel. Then the shared key is $K = K_{AB} - C$, which denotes those remaining bits of $K_{AB}$ removing those positions of bits in $C$. Otherwise, Bob informs Alice to terminate the protocol if the errors reach a predetermined level.

**Step 7** If Alice confirms that there is no eavesdropping, she derives the shared key as $K = K_{AB} - C$.

## 4. Security analysis

### 4.1. Security against eavesdropping

In the BB84 protocol [19], Alice and Bob must randomly choose a number of transmitted photons as a checking set for detecting the presence of eavesdroppers. Similarly, in the newly proposed QKA protocol, Bob will choose $m$ out of $n$ transmitted photons to form the checking set $C$. After receiving the information of $C$ as well as $K_B$, Alice will send $B_A$ and the contents of $C$ to Bob. By comparing the measurement result with the received $C$, Bob can detect the eavesdropping in the quantum channel. Accordingly, if the quantum channel is influenced by eavesdroppers, Bob will discover errors of the transmitted photons. In fact, the process of the eavesdropping check is identical to that in the BB84 protocol.

### 4.2. Security of the key agreement

In the proposed QKA protocol, $K_B$ is announced by Bob via the authenticated classical channel. However, it does not affect the unconditional security of the shared secret key $K$. Since $K_{AB} = K_A \oplus K_B$ and $K = K_{AB} - C$, if $K_A$ is kept secret, an attacker is unable to derive $K_{AB}$ as well as $K$ due to the one-time pad security. In this case, $K_{AB} = K_A \oplus K_B$ can be rewrited as $K_B = K_A \oplus K_{AB}$. Given $K_B$, it is impossible to find out $K_{AB}$ if $K_A$ is generated independently, randomly, and $|K_A| \geqslant |K_{AB}|$. The security of the one-time pad had been proven by Shannon [25]. Accordingly, if $K_{AB}$ is secure, then the attacker is unable to obtain the shared secret key $K$wherein the unconditional security of $K_{AB}$ is inherited by $K$.

Although the attacker is unable to derive the shared secret key $K$, however, a legitimate but malicious party in the QKA may wish

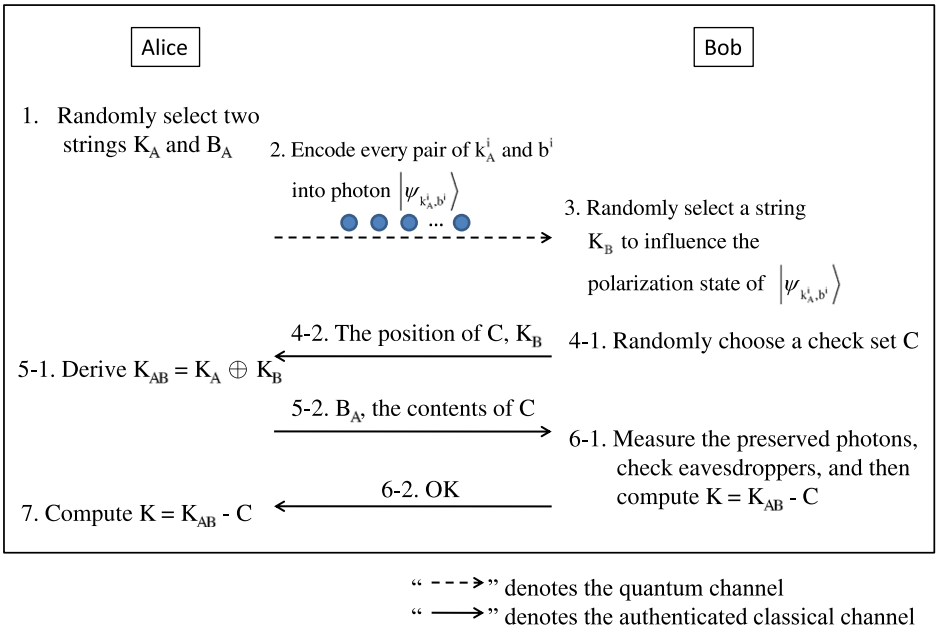


**Fig. 1.** The proposed QKA protocol.

to control the shared key without being detected by the other. The related security analyses are discussed as follows.

*4.2.1. Security against possible malicious Bob*

Although Bob can decode $K_A$ by measuring the photons once they are received, and then decide the corresponding $K_B$ to generate his favorite $K_{AB}$, however without the correct basis $B_A$ of Alice, he can only accurately decode $K_A$ with the probability $(\frac{3}{4})^n$. More precisely, the probability that Bob correctly guesses the measurement basis is $\frac{1}{2}$ for each photon. According to the quantum phenomena, if the measurement basis is correct, he can decode the bit of Alice accurately. Even though Bob uses the wrong basis for measurement, he also has probability $\frac{1}{2}$ to obtain the correct bit. Accordingly, the probability that Bob correctly decodes one bit of Alice is $\frac{3}{4}$. To control the $(n-m)$-bit shared key $K$ as well as to perform the eavesdropping check (via $m$-bit checking set $C$), Bob is only with the probability $(\frac{3}{4})^{n-m+m}$, which is negligible.

*4.2.2. Security against possible malicious Alice*

Upon receiving $K_B$ from Bob, if Alice wants to control $K_{AB}$, she needs to modify the transmitted photon states $(K_A)$ appropriately. In order to pass the verification of Bob on the checking set $C$, Alice can only modify those transmitted photon states which do not belong to $C$. Therefore Alice needs to modify quantum bases from $B_A$ to $B'_A$, where the basis of $C$ should remain unchanged in $B'_A$. For instance, to modify a bit of $K_A$ from "0" bit (assume the original photon is polarized to $|0\rangle$) to"1" bit (in this case, the desired polarization state is $|-\rangle$), Alice should send the D_basis to Bob for measurement. Bob will has the probability $\frac{1}{2}$ to decode the measurement result as "1" bit, and $\frac{1}{2}$ to decode the measurement result as "0" bit (if Alice send the R_basis to Bob, then Bob will surely decode the measurement result as "0" bit). Therefore, if Alice wants to modify a bit of $K_A$, she should send the basis contrary to the original one. In the worst case, Alice has the probability $(\frac{1}{2})^{n-m}$ to fully modify $(n-m)$ bits of $K_A$ to the desired one. In the average case, she has the probability $(\frac{1}{2})^{\frac{n-m}{2}}$ to succeed her attack, which is negligible.

*4.2.3. Advantage of Bob in controlling one bit of K*

Note that, although Bob cannot fully control $K$, he may control one bit of $K$ through his contribution $K_B$. That is, he can measure one of the received photon directly with his randomly selected basis with the probability $\frac{3}{4}$ to obtain that bit of Alice. By adjusting the corresponding bit of $K_B$, he may control that bit of $K$ with a non-negligible probability $\frac{3}{4}$.

## 5. Conclusions

This paper proposes a QKA based on the BB84 protocol that enables two involved parties to jointly negotiate a shared secret key. It precludes any communication party from determine the shared key alone. In contrast to the traditional key agreement protocols that must be based on some mathematical difficulties, the security of the new proposed protocol is based on the quantum phenomena, which instead guarantees unconditional security.

The proposed protocol utilizes two unitary operations and the delayed measurement (the quantum state storage) to modify the BB84 protocol. Both parties can influence the outcome of the proposed QKA protocol to establish a shared secret key wherein no one can decide the shared key alone. On the other hand, the utilization of the quantum state storage enables the protocol to achieve 50% qubit efficiency after the process of the random sampling discussion. Although the techniques for quantum state storage may not be practical so far, it is believed to be available in the future [18,26]. (As for the state of the art of quantum state storage, one can further refer to [27–31].) As for now, however, it is quite challenging to design a QKA without quantum state storage.

Conventionally, it is required that no party in a key agreement protocol can predetermine the resulting value of a negotiated key [32–34]. However, as mentioned in Section 4.2.3, a malicious Bob in the proposed protocol can predetermine $K$ with one bit advantage. It is quite interesting to design a fair QKA to avoid the problem.

## Acknowledgements

The authors thank the National Science Council of the Republic of China, Taiwan for financially supporting this research under Contract No. NSC 95-2221-E-006-147-MY3.

## References


[1] Y.M. Tseng, Electronics Letters 36 (1) (2000) 48.
[2] W. Trappe, Y. Wang, K.J.R. Liu, IEEE/ACM Transactions on Networking 13 (1) (2005) 134.
[3] J. Pieprzyk, C.H. Lin, IEE Proceedings-Computers and Digital Techniques 147 (14) (2000) 229.
[4] M. Steiner, G. Tsudik, M. Waidne, IEEE Transactions on Parallel and Distributed Systems 11 (8) (2000) 769.
[5] G. Ateniese, M. Steiner, G. Tsudik, IEEE Journal on Selected Areas in Communications 18 (4) (2000) 628.
[6] P.P.C. Lee, J.C.S. Lui, D.K.Y. Yau, IEEE/ACM Transactions on Networking 14 (2) (2006) 263.
[7] C.J. Mitchell, M. Ward, P. Wilson, Electronics Letters 34 (10) (1998) 980.
[8] L. Harn, W.J. Hsin, M. Mehta, IEE Proceedings Communications 152 (4) (2005) 404.
[9] C.L. Lin, H.A. Wen, T. Hwang, H.M. Sun, IEICE Transactions on Fundamentals of Electronics Communications and Computers E87-A (11) (2004) 2990.
[10] H.M. Sun, B.C. Chen, T. Hwang, Journal of Systems and Software 75 (1–2) (2005) 63.
[11] H.T. Yeh, H.M. Sun, T. Hwang, International Journal of Information and System Engineering 19 (6) (2003) 1059.
[12] H.A. Wen, T.F. Lee, T. Hwang, IEE Proceedings Communications 152 (2) (2005) 138.
[13] I.C. Chen, T. Hwang, C.M. Li, Physica Scripta 78 (3) (2008) 035005.
[14] M. Naor, B. Pinkas, in: Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, Atlanta, Georgia, United States, 10-4, May, 1999, pp. 245–254.
[15] P.W. Shor, in: Proceedings of 35th Annual Symposium on Foundations of Computer Science, Los Alamitos, CA, 20–22 November, 1994, pp. 124–134.
[16] N. Zhou, G. Zeng, J. Xiong, Electronics Letters 40 (18) (2004) 1149.
[17] C.W. Tsai, T. Hwang, On quantum key agreement protocol, Technical Report, C-S-I-E, NCKU, Taiwan, ROC, 2009.
[18] F.G. Deng, G.L. Long, Y. Wang, L. Xiao, Chinese Physics Letters 21 (2004) 2097.
[19] C.H. Bennett, G. Brassard, in: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December, 1984, pp. 175–179.
[20] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[21] C.H. Bennett, Physical Review Letter 68 (1992) 3121.
[22] A.K. Ekert, Physical Review Letters 67 (1991) 661.
[23] H.K. Lo, H.F. Chau, Science 283 (1999) 2050.
[24] G.L. Long, X.S. Liu, Physical Review A 65 (2002) 0323021.
[25] C. Shannon, Bell System Technical Journal 28 (4) (1949) 656.
[26] T. Hwang, C.M. Li, International Journal of Modern Physics C 19 (4) (2008) 625.
[27] T. Chaneliére, D.N. Matsukevich, S.D. Jenkins, S.Y. Lan, T.A.B. Kennedy, A. Kuzmich, Nature 438 (7069) (2005) 833.
[28] C.S. Chuu, T. Strassel, B. Zhao, M. Koch, Y.A. Chen, S. Chen, Z.S. Yuan, J. Schmiedmayer, J.W. Pan, Physical Review Letters 101 (12) (2008) 120501.
[29] A.E. Kozhekin, K. Molmer, E. Polzik, Physical Review A 62 (3) (2000) 033809.
[30] C. Liu, Z. Dutton, C.H. Behroozi, L.V. Hau, Nature 409 (6819) (2001) 490.
[31] D.F. Phillips, A. Fleischhauer, A. Mair, R.L. Walsworth, M.D. Lukin, Physical Review Letter 86 (5) (2001) 783.
[32] International Organization for Standardization, ISO/IEC 11770-3:2008, Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques,second ed., 15 June, 2008.
[33] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001. <http://www.cacr.math.uwaterloo.ca/hac/>.
[34] B. Preneel, V. Rijmen, State of the Art in Applied Cryptography: Course on Computer Security and Industrial Cryptography, Leuven, Belgium, 1997 (Revised Lectures, Lecture Notes in Computer Science, vol. 1528, Springer, 1998).