Journal of Computer Science

Original Research Paper

# A Modified Secure Scheme of Quantum Key Distribution Without Public Announcement Bases

[1]Es-Said Chanigui and [2]Abdelmalek Azizi

[1]*Department of Mathematics and Computer Science, FSO, University Mohamed I, Oujda, Morocco*
[2]*Academy Hassan II of Sciences and Technology, Rabat, Morocco*

*Article history*
Received: 25-11-2013
Revised: 17-04-2014
Accepted: 23-10-2014

Corresponding Author:
Es-said Chanigui
Department of Mathematics and Computer Science, FSO,
University Mohamed I, Oujda,
Morocco
Email: chanigui@yahoo.fr

**Abstract:** This study provides a simple variation of the protocol of quantum key expansion proposed by Hwang. Some weaknesses relating to the step of public discussions for error detection are analyzed and an attack strategy, allowing the eavesdropper to get partial information about the used bases, is put forward. Using the One-Time Pad cipher, we propose a possible scheme which is secure against the presented attack.

**Keywords:** Quantum Key Distribution, Quantum Key Expansion, Quantum Cryptography, One-Time Pad

## Introduction

Key distribution is always an important issue in cryptography. One of the earliest discoveries in quantum computation and quantum information was that quantum mechanics can be used to do key distribution in such a way that communication security cannot be compromised. The basic idea is to exploit the quantum mechanical principle that observation disturbs the system being observed. This procedure is known as Quantum Key Distribution (QKD).

QKD protocol enables two remote communicating parties (Bob and Alice) who are authenticated to share a perfectly secure key even in the presence of an Eavesdropper (Eve). The first QKD scheme, BB84 protocol, was proposed by Bennett and Brassard (1984). Since then, many QKD protocols had been suggested, among them the two famous protocols: EPR protocol (Ekert, 1991) based on EPR entangled states and B92 protocol (Bennett, 1992) based on non-orthogonal states. These protocols have been proved secure (Lutkenhaus and Barnett, 1996). Over the last two decades, other QKD protocols (Goldenberg and Vaidman, 1995; Huttner *et al*., 1995; Bechmann-Pasquinucci and Peres, 2000; Gisin *et al*., 2001; Lo *et al*., 2005; Zhao *et al*., 2008; Xiu *et al*., 2009; Sun *et al*., 2009; Sheridan *et al*., 2010) have been proposed and QKD experiments have been demonstrated (Gobby *et al*., 2004; Scheidl *et al*., 2009; Rosenberg *et al*., 2009).

Hwang *et al*. (1998) proposed a variation of the basic ideas of BB84 protocol, in which public announcement bases is eliminated. Hwang protocol provides a higher key generation rate (100%) as compared with BB84 protocol (50%). The efficiency of the scheme is 100% except for the error checking step. The protocol's security has been discussed in ideal condition and has been proved (Hwang *et al*., 2001; 2003; Wen and Long, 2005). Its security in real circumstance is studied in (Lin and Liu, 2012) where two attacks are presented. However, the previous discussions about Hwang protocol security (Hwang *et al*., 2001; 2003; Wen and Long, 2005) did not take into consideration whether a partial information about the encoding bases may be eavesdropped during the error check, that's what will be discussed in greater detail over the course of this article.

This study is organized as follows. In section 2, a brief description of Hwang protocol will be given and the protocol will be analyzed. We will propose an attack on the protocol. Taking into account the flaw of Hwang protocol, we will propose a new secure scheme in section 3 where the subset of cbits (classical bits), that Alice and Bob intend to discuss publically, is encrypted with the One-Time Pad cipher. In section 4, we will show that the modified protocol is more efficient than the original protocol and it can be used securely against the presented attack. Finally, section 5 presents our conclusions.

## Eavesdropping on the Hwang Protocol

### Hwang Protocol

Let us start with the brief description of Hwang protocol (Lin and Liu, 2012).

Alice and Bob share some secure binary random sequence B = ($b_1$ ,$b_2$ ,...,$b_n$), that is known to nobody by the BB84 scheme or by courier and repeat it t times to construct a string C = ( $c_1^1$ ,$c_2^1$,...,$c_n^1$, $c_1^2$ ,$c_2^2$,...,$c_n^2$,…, $c_1^t$, $c_2^t$,...,$c_n^t$) where $c^i_j$ = $b_j$ (for i = 1,...,t).

Alice creates a random N = n×t cbit string X = ($x_1^1$,$x_2^1$,...,$x_n^1$, $x_1^2$ ,$x_2^2$,...,$x_n^2$,…, $x_1^t$ ,$x_2^t$,...,$x_n^t$) and keeps it as the secret key. With the knowledge of two binary strings X and C, Alice prepares a qubit (quantum bit) string $|\varphi x^i_{j,}c^i_j>$ and each qubit is one of the four states: $|\varphi_{0,0}>$ = |0>, $|\varphi_{1,0}>$ = |1>, $|\varphi_{0,1}>$ = |+>, $|\varphi_{1,1}>$ = |−> that is to encode X in the rectilinear basis B⊕ = {|0>,|1>} or the diagonal basis B⊗ = {|+>,|−>} if the corresponding cbit of C is 0 or 1, respectively (The association between the information cbit and the basis are described in Table 1). Then, Alice sends the qubit string to Bob.

After receiving these *N* qubits, Bob measures them in the basis *B*⊕ or *B*⊗ according to the binary string *C*.

If all qubits have been sent, Alice and Bob compare some randomly chosen subset of their key. Bob informs Alice publically whether he obtained 0 or 1 at the subset of instances. Next, Alice compares These data with her ones and checks if there is error. Here what Bob announces is just cbit that the qubit represents but not the exact state of the qubit, which is to prevent the leakage of information.

In this protocol, Alice and Bob have common random sequence *B*. Then, there will be perfect correlation between their measurement results unless the quantum states were perturbed by Eve's attempt at eavesdropping or noise. Thus, it is unnecessary to perform a public announcement bases process, which reduces information about bases that was attained by Eve. However the announcement of cbit 0 or 1 for error check will also leak out information about bases, which we will discuss later.

### Attack Strategy

Now, let us turn to our eavesdropping scheme "Sieving By Difference" attack (SBD attack), which consists of several attacks. For the first series of attacks, Eve will be detected by Alice and Bob and the communication will be abandoned. But for the followed attacks Eve will not be detected and be able to get all the information exchanged subsequently.

Table 1. Qubit preparation according to the choice of basis and cbit value

| | 0 | 1 |
|---|---|---|
| B⊕ | $\|\varphi_{0,0}>$ | $\|\varphi_{1,0}>$ |
| B⊗ | $\|\varphi_{0,1}>$ | $\|\varphi_{1,1}>$ |

Suppose that Eve knows in advance the length of the basis sequence between Alice and Bob (n cbits). If the length of the key that Alice and Bob want to establish is N cbits (N = n × t), then the basis sequence will be used for at least t times. Now, let us induce a method for attack. In the first attack, Eve intercepts all of the photons from Alice to Bob and performs measurement on every photon always along the basis B⊕ or B⊗ which is randomly chosen by Eve (For example B⊕ is chosen) and she sends the measured photons to Bob. Two cases may happen: In the first, which occurs with probability 1/2, the qubit representing the state of the photon sent from Alice to Bob is encoded with a rectilinear basis. In this case, the qubit will not change after measuring by Eve. In the second, which also occurs with half probability, the qubit representing the state of the photon sent from Alice to Bob is |+⟩ = 1/√2×(|0⟩+|1⟩) or |−⟩ = 1/√2×(|0⟩-|1⟩) (the photon state is encoded with a diagonal basis B⊗). Then, when Eve measures this qubit along the basis B⊕ she will get |0⟩ or |1⟩ with probability 1/2. After receiving the photon, Bob should measure it along B⊗ according to the sharing sequence, he will get |+⟩ or |−⟩ with probability 1/2. By the announcement of Bob's result (0 or 1), Eve will find that her measuring result is different from Bob's result with half probability and she will be sure that the basis with which this photon was encoded is B⊗. Then, Eve can get the base state with probability 1/2×1/2 = ¼ like the example shown in Fig. 1. So, to recapitulate, after the first attack averagely 1/4 of the bases corresponding to cbits sacrificed to check for the eavesdropper's activity will be known by Eve.

In the following attacks, Eve invests her knowledge about the basis sequence. She measures the photons of known bases in the right bases and the rest along randomly chosen basis (B⊕ or B⊗). Then Eve will get more and more information about the sharing sequence B and hence get an error rate low enough for eavesdropping without being detected after a certain number of attacks.

Suppose Alice and Bob check error rate for every *n* cbits. Then Eve proceeds through the following steps and will get the following results:

- By eavesdropping on the quantum channel, Eve intercepts all the n photons that Alice sends to Bob. She measures them along the basis $B_{\oplus}$ and sends them to Bob. At the same time, Eve should record the measuring results of all photons
- Eve eavesdrops on the classical channel to get the announcement of the q cbits used for error check by Bob. Then Eve compares her records with Bob's results. If the results of one of the photons are different, Eve can be sure that the base corresponding to this photon must be $B_{\otimes}$ (SBD). As mentioned above, Eve will get different results with Bob for averagely $r_1 = q/4$ photons. Although the error rate induced by Eve, in this first attack, is 25% ($e_1 = 0.25$). Then, Eve will be detected and Alice and Bob will abandon this communication, but Eve will be sure that the bases corresponding to these photons are $B_{\otimes}$
- During another communication for Alice and Bob, Eve performs a second attack. But in this time, Eve knows that the q/4 bases are $B_{\otimes}$, so she measures the q/4 qubits corresponding to these bases along $B_{\otimes}$ and measures the remaining n-q/4 qubits also along $B_{\otimes}$ as indicated in Fig. 2 (for every attack, Eve will use alternatively either $B_{\oplus}$ or $B_{\otimes}$ to measure photons encoded in unknown bases in order to increase the chance of finding more different results from Bob). Then Eve sends all photons to Bob and proceeds exactly like in the first attack. It should be noted that, for every time, Alice and Bob choose q photons randomly for error check. So, on average there will be q/4×q/n photons corresponding to a subset of known bases to be chosen. So, the bases of the q/4×q/n photons is known to Eve and the left q-q/4×q/n photons chosen for error check are still unknown. Similarly, there will be averagely (q-q/4×q/n)×1/4 = (1-q/4n)×q/4 photons that Eve has the different results from Bob, which means that the bases corresponding to these photons are $B_{\oplus}$. At the same time, the error rate induced by Eve is averagely $e_2 = (1\text{-}q/4n)\times 1/4$. After the second attack, Eve will get to know averagely $r_2 = (1\text{-}q/4n)\times q/4 + q/4 = (2\text{-}q/4n)\times q/4$ basis from the basis sequence
- For the next following attacks, the results can be deduced similarly. Let $r_i$ be the number of basis that Eve has got to know after the i-th attack. Let $e_i$ be the error rate in the i-th attack. Then, we have $r_{i+1} = r_i\times(1\text{-}q/4n)+q/4$ , $e_{i+1} = 1/4\times(1\text{-}r_i/n)$, i = 1,2,3,... where q is the number of photons used for error check and n is the length of the basis sequence

*Example*

Suppose the length of the key that Alice and Bob want to establish is $N = 10^5$ and the length of their sharing basis sequence is $n = 10^3$ where q cbits (q = 100, 200, 300) are used for announcement and comparison in the classical channel for error check. Suppose, also, that Eve uses our strategy to attack on Hwang protocol. Then we have the results of the first 100 attacks which are illustrated in Fig. 3 and 4.

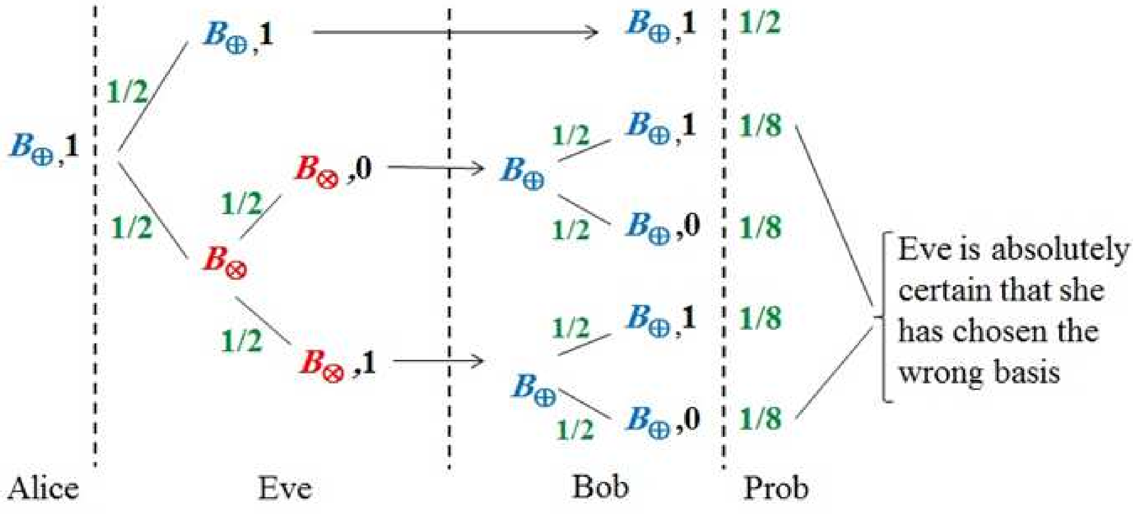

Fig. 1. All possibilities when Alice sends the qubit $|\varphi_{1,0}>$

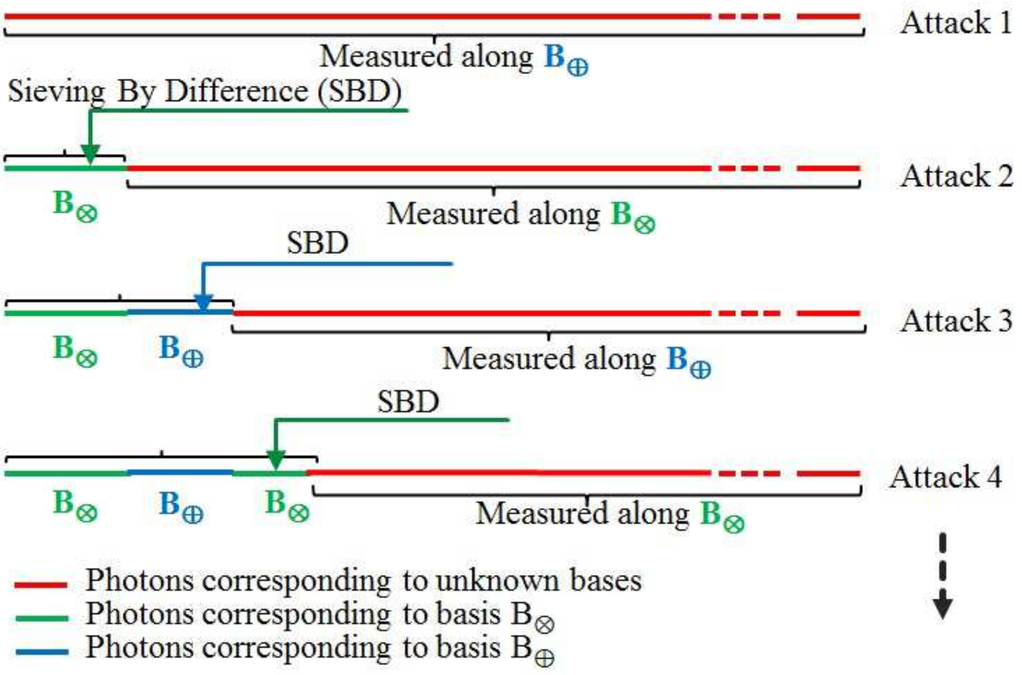
Attack 1
Measured along $B_\oplus$
Sieving By Difference (SBD)
Attack 2
$B_\otimes$
Measured along $B_\otimes$
SBD
Attack 3
$B_\otimes$
$B_\oplus$
Measured along $B_\oplus$
SBD
Attack 4
$B_\otimes$
$B_\oplus$
$B_\otimes$
Measured along $B_\otimes$
Photons corresponding to unknown bases
Photons corresponding to basis $B_\otimes$
Photons corresponding to basis $B_\oplus$

Fig. 2. The first four rounds of SBD attack

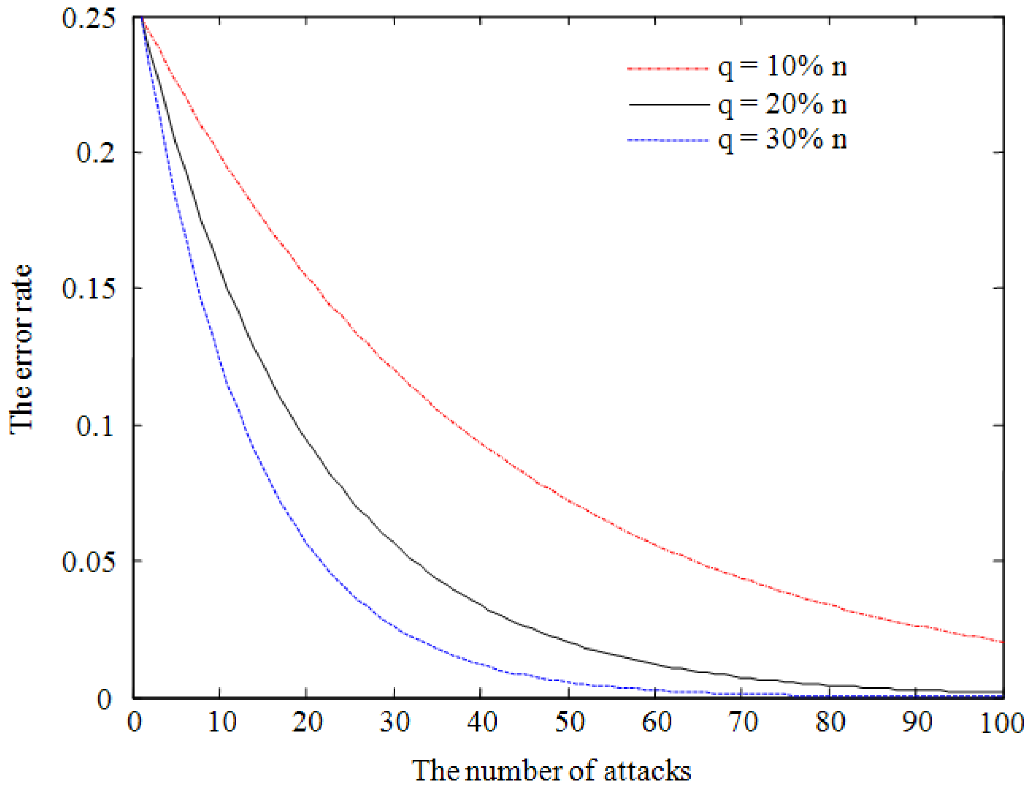

Fig. 3. The error rate as a function of the number of attacks when Eve uses our eavesdropping strategy in order to achieve her attack on the Hwang protocol, for n = 1000 and q = 10, 20 and 30% n

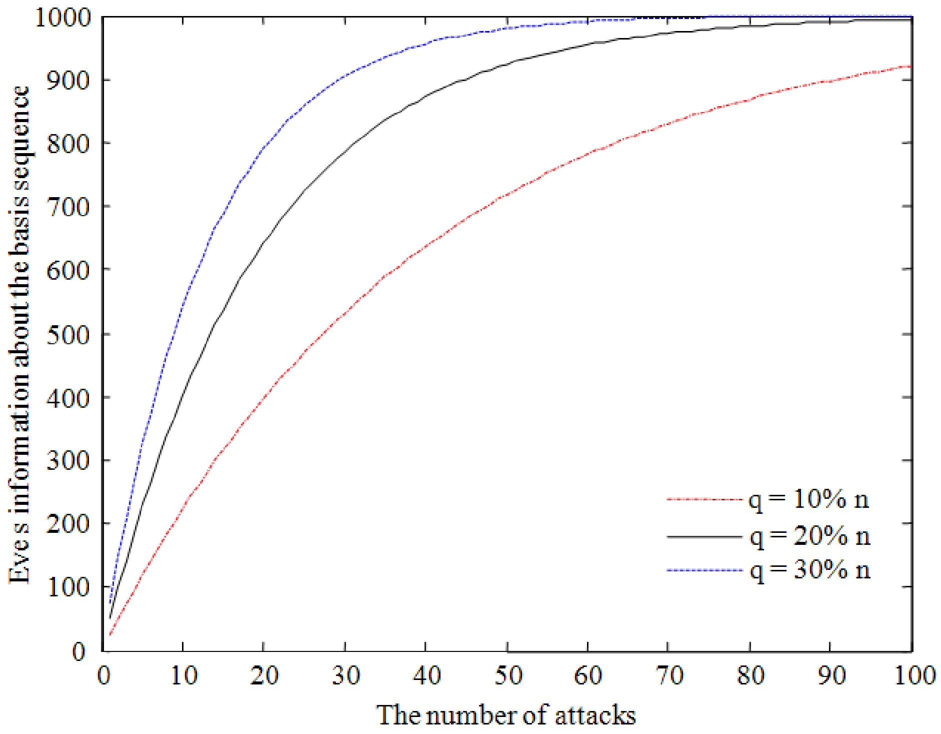

Fig. 4. Eve's information about the basis sequence as a function of the number of attacks when Eve uses our eavesdropping strategy in order to achieve her attack on the Hwang protocol, for n = 1000 and q = 10, 20 and 30% n

## Modified Protocol

In this section, a modified protocol is proposed, which can stand against the attacks depicted in the above section. Here, the One-Time Pad, also called Vernam (1926), which is a provably secure cryptosystem (Shannon, 1949), is utilized to encrypt a public announcement of cbits for error check between Alice and Bob.

One-time pad is a type of symmetric encryption system in which a private key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key.

The modified protocol is described as follows:

- Alice and Bob share two prior random cbit strings. One is the basis sequence B = $(b_1, b_2, ..., b_n)$ with which they construct a cbit string C = $(c_1^{\ 1},c_2^{\ 1},...,c_n^{\ 1},c_1^{\ 2},c_2^{\ 2},...,c_n^{\ 2},..., c_1^{\ t}, c_2^{\ t},...,c_n^{\ t})$ where $c^i_j = b_j$ for I = 1,...,t. The other is a short secret key S = $(s_1,s_2,...,s_q)$ which will be used to encrypt a randomly chosen subset of cbits before being exchanged publicly during the first error check
- For i = 1 to t
- Alice creates a random cbit string $X_i = (x_1^{\ i}, x_2^{\ i},..., x_n^{\ i})$ as the round key and with the knowledge of two binary strings $X_i$ and $C_i$, Alice prepares a qubit string $|\varphi x'^i_{j,} c^i_j>$ as described in Table 1 and sends it to Bob
- After receiving these n qubits, Bob measures them in the basis $B_\oplus$ or $B_\otimes$ according to the binary string $C_i$. Then, he obtains $X'_i$
- Let $S_1$ = S and for i > 1, let $S_i = (s^i_1, s^i_2,..., s^i_q)$ be a subset of q cbits randomly chosen by Bob and Alice from the shared key $X''_{i-1}$($X''$ is the shared key formed after error correction and privacy amplification)

In order to detect Eve's intervention, Alice and Bob compare some randomly chosen subset of received cbits $X'_i$ as follows:

- First, Bob constructs a string $T_i = (x'_1{}^i, x'_2{}^i,..., x'_q{}^i)$ by choosing randomly q cbits into $X'_i$ and records their positions. Then, he encrypts the cbits $x'_j{}^i$ ($\in T_i$), j = 1,…,q, by using the shared key $S_i$ and a One Time Pad cipher. Finally, Bob sends the ciphertext $(x'_j{}^i \oplus s_j{}^i)$, j = 1,…,q publicly to Alice and tells her the positions of chosen cbits

- Alice applies XOR to every cbit of the encrypted message she receives and the corresponding cbit of the One Time Key $S_i$, that is, $x'^{i}_{j} \oplus s_j^i \oplus s_j^i = x'^{i}_{j}$, $j = 1,..., q$ Next, Alice compares These data with her own $(x_j^i)$ $j = 1,…,q$ and checks if there is error
- According to the threshold error rate, Alice and Bob abort the process or execute error correct and privacy amplification to generate the secure key $X''_i$

## Discussion

It's important to note that, in the modifid protocol, the subset $S_i$, used to encrypt the exchanged cbits during the error check operation, should be discarded at the end of each round. The ongoing need to get hold of the short keys $S_i$ may appear as a deficiency of our protocol. But this is not correct because in all of the QKD Protocols and especially Hwang protocol, a subset of cbits used in the error check step (and that has the same length as $S_i$) is discarded as well. In our case, the subset $S_i$, with which we encrypt the announcement of bases in the (i+1)-th round, isn't discarded until we use it to further increase the protocol's security.

In the modified protocol, nothing is changed except the error check process. Hence, the security of the modified protocol is the same as that of Hwang protocol in ideal condition (without taking into consideration its weakness due to the public error check). In addition, the proposed protocol, by using One-Time Pad encryption, makes secure a public comparison between Alice and Bob and deprives Eve of any information at all about Bob's measurements. Eve cannot judge whether her measuring result is different from Bob's result or not because, even by intercepting an encrypted message $T_i \oplus S_i$ exchanged publicly between Alice and Bob during the error check, she cannot attain any information about the subset $T_i$. Then, she will not be able to make any conclusion about prepare basis. Therefore, our scheme is secure against the SBD attack presented in sect. 2.

## Conclusion

In summary, we have analyzed Hwang's Protocol and found that the announcement of cbits over the classical channel for error check is the weakness of the protocol because of the leakage of information about a bases sequence. We propose an eavesdropping strategy for Eve to attack on the protocol and show how she can get more and more information of shared key between Alice and Bob. To overcome this flaw, we propose a new scheme, where the subset of cbits, that Alice and Bob intend to discuss publically, is encrypted with the One-Time Pad cipher. The security of the proposed protocol is discussed and it is shown that the new protocol is secure against the presented attack.

Unfortunately, there is no known way to initiate the modified protocol without initially exchanging a secret key S, which is a weakness. So, finding an efficient QKD Protocol without public announcement of bases, that avoids leaking information (during a public error check) and that doesn't require using a pre-shared key, would be an interesting issue to study.

## Funding Information

The authors have no support or funding to report.

## Author's Contributions

All authors equally contributed in this work.

## Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

## References

Bechmann-Pasquinucci, H. and A. Peres, 2000. Quantum cryptography with 3-state systems. Phys. Rev. Lett., 85: 3313. DOI: 10.1103/PhysRevLett.85.3313

Bennett, C.H. and G. Brassard, 1984. Quantum cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, (SP '84), IEEE Press, New York, pp: 175-179. DOI: 10.1016/j.tcs.2011.08.039

Bennett, C.H., 1992. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 68: 3121-3124. DOI: 10.1103/PhysRevLett.68.3121

Ekert, A.K., 1991. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 67: 661-663. DOI: 10.1103/PhysRevLett.67.661

Gisin, N., G. Ribordy, W. Tittel and H. Zbinden, 2001. Quantum cryptography. Rev. Mod. Phys., 74: 145-145. DOI: 10.1103/RevModPhys.74.145

Gobby, C., Z.L. Yuan and A.J. Shields, 2004. Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett., 84: 3762-3762. DOI: 10.1063/1.1738173

Goldenberg, L. and L. Vaidman, 1995. Quantum cryptography based on orthogonal states. Phys. Rev. Lett., 75: 1239-1243. DOI: 10.1103/PhysRevLett.75.1239

Huttner, B., N. Imoto, N. Gisin and T. Mor, 1995. Quantum cryptography with coherent state. Phys. Rev. A 51: 1863-1869. DOI: 10.1103/PhysRevA.51.1863

Hwang, W.Y., D. Ahn and S.W. Hwang, 2001. Eavesdropper's optimal information in variations of Bennett-Brassard 1984 quantum key distribution in the coherent attacks. Phys. Lett. A, 279: 133-138. DOI: 10.1016/S0375-9601(00)00825-2

Hwang, W.Y., I.G. Koh and Y.D. Han, 1998. Quantum cryptography without public announcement of bases. Phys. Lett., A244: 489-494. DOI: 10.1016/S0375-9601(98)00358-2

Hwang, W.Y., X.B. Wang, K. Matsumoto, J. Kim and H.W. Lee, 2003. Shor Preskill-type security proof for quantum key distribution without public announcement of bases. Phys. Rev., A67: 012302-012302. DOI: 10.1103/PhysRevA.67.012302

Lin, S. and X.F. Liu, 2012. A modified quantum key distribution without public announcement bases against photon-number-splitting attack. Int. J. Theor. Phys., 51: 2514-2523. DOI: 10.1007/s10773-012-1131-9

Lo, H.K., X. Ma and K. Chen, 2005. Decoy state quantum key distribution. Phys. Rev. Lett., 94: 230504-230504. DOI: 10.1103/PhysRevLett.94.230504

Lutkenhaus, N. and S.M. Barnett, 1996. Security against eavesdropping in quantum cryptography. Phys. Rev., A54: 97-111. DOI: 10.1103/PhysRevA.54.97

Rosenberg, D., C.G. Peterson and J.W. Harrington, 2009. Practical long distance quantum key distribution system using decoy levels. New J. Phys., 11: 045009-045009. DOI: 10.1088/1367-2630/11/4/045009

Scheidl, T., R. Ursin, A. Fedrizzi and S. Ramelow, 2009. Feasibility of 300 km quantum key distribution with entangled states. New J. Phys., 11: 085002-085002. DOI: 10.1088/1367-2630/11/8/085002

Shannon, C.E., 1949. Communication theory of secrecy systems. Bell Syst. Technical J., 28: 656-715. DOI: 10.1002/j.1538-7305.1949.tb00928.x

Sheridan, L., T.P. Le and V. Scarani, 2010. Finite-key security against coherent attacks in quantum key distribution. New J. Phys., 12: 123019-123019. DOI: 10.1088/1367-2630/12/12/123019

Sun, S.H., L.M. Liang and C.Z. Li, 2009. Decoy state quantum key distribution with finite resources. Phys. Lett. A, 373: 2533-2536. DOI: 10.1016/j.physleta.2009.05.016

Vernam, G.S., 1926. Cipher printing telegraph systems for secret wire and radio telegraphic communications. J. IEEE, 55: 109-115. DOI: 10.1109/T-AIEE.1926.5061224

Wen, K. and G.L. Long, 2005. Modified bennett-brassard 1984 quantum key distribution protocol with two-way classical communications. Phys. Rev. A, 72: 022336-022340. DOI: 10.1103/PhysRevA.72.022336

Xiu, X.M., L. Dong, Y.J. Gao and F. Chi, 2009. Quantum key distribution protocols with six-photon states against collective noise. Opt. Commun., 282: 4171-4174. DOI: 10.1016/j.optcom.2009.07.012

Zhao, Y., B. Qi and H.K. Lo, 2008. Quantum key distribution with an unknown and untrusted source. Phys. Rev. A, 77: 052327-052340. DOI: 10.1103/PhysRevA.77.052327