Computers, Materials & Continua CMC, vol.61, no.2, pp.759-775, 2019

An Efficient Quantum Key Distribution Protocol with Dense Coding on Single Photons

Hao Xiao[1, *], Jun Zhang[2], Wenhua Huang[3], Mi Zhou[4] and Wencheng Hu[5]

Abstract: Combined with the dense coding mechanism and the bias-BB84 protocol, an efficient quantum key distribution protocol with dense coding on single photons (QDKD-SP) is proposed. Compared with the BB84 or bias-BB84 protocols based on single photons, our QDKD-SP protocol has a higher capacity without increasing the difficulty of its experiment implementation as each correlated photon can carry two bits of useful information. Compared with the quantum dense key distribution (QDKD) protocol based on entangled states, our protocol is more feasible as the preparation and the measurement of a single-photon quantum state is not difficult with current technology. In addition, our QDKD-SP protocol is theoretically proved to be secure against the intercept-resend attack.

Keywords: Quantum key distribution, bias-BB84, dense coding mechanism, quantum dense key distribution, single photons.

1 Introduction

In recent decades, with the development of quantum mechanics, the theory of quantum mechanics has been utilized in the information processing field. Especially, quantum cryptography communication has aroused more and more researchers' interest, and it has been used to complete many tasks, such as quantum key distribution (QKD) [Bennett and Brassard (1984); Bennett and Wiesner (1992); Ekert (1991)], quantum secret sharing(QSS) [Chen, Tang, Xu et al. (2018); Liu, Chen, Xu et al. (2012)], quantum key agreement (QKA) [Chong and Hwang (2010); Huang, Su, Liu et al. (2017); Liu, Xu, Yang et al. (2018)], quantum secure direct communication(QSDC) [Liu, Chen, Li et al. (2008); Liu, Chen, Ma et al. (2009); Xu, Chen, Li et al. (2015)], quantum private comparison(QPC) [Liu, Liu, Wang et al. (2013); Liu, Liu, Chen et al. (2014); Liu, Liu, Liu et al. (2014); Liu, Liu, Wang et al. (2014)], quantum sealed-bid auction(QSBA) [Liu, Wang, Ji et al. (2014); Liu, Wang, Yuan et al. (2016)], quantum remote state preparation (QRSP) [Chen, Sun, Xu et al. (2017);

[1] School of Information Engineering, Huzhou University, Huzhou, 313000, China.

[2] School of Information Engineering, Jiangsu Maritime Institute, Nanjing, 21100, China.

[3] College of Science, Huzhou University, Huzhou, 313000, China.

[4] Virginia Commonwealth University, Richmond Virginia, 23284, USA.

[5] College of Science, Zhongyuan University of Technology, Zhengzhou, 450007, China.

[*] Corresponding Author: Hao Xiao. Email: xiaohao@zjhu.edu.cn.

Liu, Chen, Liu et al. (2015); Qu, Wu, Wang et al. (2017)], quantum steganography [Qu, Chen, Ji et al. (2018); Qu, Cheng, Liu et al. (2018)], delegating quantum computation [Liu, Chen, Ji et al. (2017); Liu, Chen, Liu et al. (2018)], quantum machine learning [Liu, Gao, Yu et al. (2018), Liu, Gao, Wang et al. (2019)], and so on.

As the most basic and important research direction, QKD is used to produce a private key between two legitimate users with the fundamental principles in quantum mechanics or some special features in an entangled quantum system. With the aid of a private key, the two users can communicate their secret message securely. With the unconditional security rather than the infeasible computation in the conventional cryptography, a number of QKD protocols were proposed accordingly. Besides the security, many efforts were made to improve the key distribution efficiency. Generally, these QKD protocols can be divided two categories: the QKD protocols based on single photon (SinglePhoton-QKD) such as BB84 [Bennett and Brassard (1984)], B92 [Ekert (1991)] and their improved schemes [Bechmann-Pasquinucci and Tittel (2000); Lo, Chau, and Ardehali (2005)], and the other QKD protocols based on entangled state (Entangled-QKD) [Bennett and Wiesner (1992); Karimipour, Bahraminasab and Bagherinezhad (2002)]. In the above two categories, SinglePhoton-QKD has the advantage of the simple and feasible experiment implementation but less efficiency, while Entangled-QKD enhances the efficiency but needs more complex quantum resources and equipment.

In 2004, Degiovanni et al. [Degiovanni, Berchera, Castelletto et al. (2004)] proposed a novel QKD protocol, called quantum dense key distribution (QDKD), by using the operations on the Entangled state (i.e., one of the Bell states) to embed the key information. It embeds the benefits of quantum dense coding and quantum key distribution, and can generate shared secret keys four times more efficiently than the BB84 protocol. Although the security of Degiovanni et al.'s QDKD protocol was questioned by Wójcik [Wojcik (2005)], a modified security proof was then given [Degiovanni, Berchera, Castelletto et al. (2005)] and showed that the protocol is able to detect any individual eavesdropping attack including the injecting-subtracting attack proposed in Wójcik's Comment. Since then, this idea of QDKD has been successfully exploited by other scholars, using different entangled states. For example, in 2011, Hwang et al. [Hwang, Hwang and Tsai (2011)] proposed a QKD protocol by utilizing dense coding on three-qubit W state, and Liu et al. [Liu, Chen, Liu et al. (2013)] put forward a quantum simultaneous secret distribution protocol with dense coding on cluster states.

Combined with the bias-BB84 protocol [Lo, Chau and Ardehali (2005)] and the dense coding mechanism in Degiovanni et al.'s QDKD protocol [Degiovanni, Berchera, Castelletto et al. (2004)], we proposed an efficient QKD protocol with dense coding on single photons (QDKD-SP), where two efficiencies of key distribution are used in this paper: (theoretical efficiency) and (practical efficiency). Our QDKD-SP protocol at least has the same practical efficiency like the bias-BB84 protocol, and better practical efficiency than BB84 and Degiovanni et al.'s QDKD protocol. Besides, it has the same theoretical efficiency as Degiovanni et al.'s QDKD protocol, and better theoretical efficiency than BB84 and bias-BB84.

The rest of this paper is organized as follows. In Section 2, we describe the previous QKD protocols: the bias-BB84 protocol (a single-polarized-photon protocol) and

Degiovanni et al.'s QDKD protocol (an entangled-pair protocol). Section 3 introduces the proposed QDKD-SP protocol. Also, two key distribution efficiencies are used to evaluate the proposed QDKD-SP protocol. Security analysis and comparison are given in Section 4. The conclusion is drawn in Section 5.

2 Preliminaries

2.1 BB84 protocol

BB84 [Bennett and Brassard (1984)] is a quantum key distribution protocol developed by Bennett and Brassard in 1984. It is the first quantum cryptography protocol, which is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states one is trying to distinguish are not orthogonal (i.e., no-cloning theorem) and an authenticated public classical channel. It is usually explained as a method of securely communicating a private key from one party to another for use in one-time pad encryption.

In the BB84 protocol, Alice wishes to send a private key to Bob. She begins with two strings of bits, a and b, each $(4+\delta)n$ bits long. She then encodes these two strings as as a block of $(4+\delta)n$ qubits,

$$|\psi\rangle = \bigotimes_{k=1}^{(4+\delta)n} |\psi_{a_k b_k}\rangle \tag{1}$$

where a_k is the kth bit of a (and similarly for b), and each qubit is one of the four states

$$\begin{cases} |\psi_{00}\rangle = |0\rangle \\ |\psi_{10}\rangle = |1\rangle \\ |\psi_{01}\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \\ |\psi_{11}\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \end{cases} \tag{2}$$

The effect of this procedure is to encode a in the base *R*-basis $\{|0\rangle, |1\rangle\}$ or *D*-basis $\{|+\rangle, |-\rangle\}$, as determined by b.

Alice sends the resulting state $|\psi\rangle$ over a public and authenticated quantum channel to Bob. Bob receives the $(4+\delta)n$ qubits, announces this fact, and measures each qubit in the *R*-basis or *D*-basis at random. At the same time, Alice announces b. Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least $2n$ bits left (if not, abort the protocol). They keep $2n$ bits. Alice selects a subset of n bits that will be used to serve as a check on Eve's interference, and tells Bob which bits she selected. Both Alice and Bob announce and compare the values of the n check bits publicly, and run a check to see whether more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques to create on the remaining n bits to obtain m shared key bits. Otherwise, they cancel and start over.

2.2 Bias-BB84 protocol

In 2005, Lo et al. [Lo, Chau and Ardehali (2005)] proposed an efficient QKD protocol to enhance the efficiency of BB84. The major new ingredient of the efficient BB84 protocol is to put a bias in the probabilities of choosing between the two bases, so it is also called bias-BB84.

Recall the fraction of rejected data of BB84 is likely to be 50%. This is because in BB84 Alice and Bob choose between the two bases randomly and independently. The efficiency will be increased if Alice prepares and Bob measures their photons with a bias choice of basis. Specifically, they first agree on a fixed number $0 < p \le \frac{1}{2}$. Alice prepares (Bob measures) each photon randomly and independently in the rectilinear and diagonal basis with probabilities p and $1-p$, respectively. Clearly, the bias-BB84 protocol is insecure when $p = 0$. Nonetheless, in the limit of a large number of photon transfer, this bias-BB84 protocol is secure in the limit of $p \to 0^+$. Hence, the efficiency of bias-BB84 is asymptotically doubled when compared with BB84.

2.3 Degiovanni et al.'s QDKD protocol

The first QDKD protocol [Degiovanni, Berchera, Castelletto et al. (2004)] was proposed by Degiovanni et al., which embeds the benefits of a quantum dense coding and a quantum key distribution and is able to generate shared secret keys four times more efficiently than BB84 one.

In Degiovanni *et al.*'s QDKD protocol, Alice produces pairs of particles in the singlet state $\left|\psi_{AB}^{-}\right\rangle = \frac{\left|0_A 1_B\right\rangle - \left|1_A 0_B\right\rangle}{\sqrt{2}}$, and stores particle A in her lab, whereas she acts randomly with gate I_B or Z_B on particle B and then sends it to Bob. As $Z_B\left|0_B\right\rangle = \left|0_B\right\rangle$, and $Z_B\left|1_B\right\rangle = -\left|1_B\right\rangle$, Alice's random selection of gate I_B or Z_B encodes the bits of her secret key on the EPR pair, with $\left|\psi_{AB}^{+}\right\rangle = \frac{\left|0_A 1_B\right\rangle + \left|1_A 0_B\right\rangle}{\sqrt{2}}$.

$$\begin{cases} I_B\left|\psi_{AB}^{-}\right\rangle = \left|\psi_{AB}^{-}\right\rangle \to bit\,0 \\ Z_B\left|\psi_{AB}^{-}\right\rangle = -\left|\psi_{AB}^{+}\right\rangle \to bit\,1 \end{cases} \tag{3}$$

Bob randomly switches particle B towards either his measurement or his encoding apparatus. In one case Bob projects particle B on the base $\left\{\left|0_B\right\rangle, \left|1_B\right\rangle\right\}$ while in the other case, Bob, analogously to Alice, randomly acts with I_B or Z_B on particle B and then sends it back to Alice.

Alice receives particle B, and her measurement apparatus performs an incomplete Bell's state analysis, i.e., a projection on $\left|\psi_{AB}^{-}\right\rangle$ or $\left|\psi_{AB}^{+}\right\rangle$ of the two-particle state composed by the previously stored particle A and particle B. Then Alice measures particle A on the base $\left\{\left|0_A\right\rangle, \left|1_A\right\rangle\right\}$ instead of performing a Bell's state analysis when Bob's apparatus

projects particle *B*. As Alice prepares only states $\left|\psi_{AB}^{-}\right\rangle$ and $\left|\psi_{AB}^{+}\right\rangle$, Alice and Bob results should be always anti-correlated. The anti-correlation can be checked in Fig. 1, consists in comparing Alice and Bob results, and guarantees the security of the distributed keys against individual eavesdropping attack.

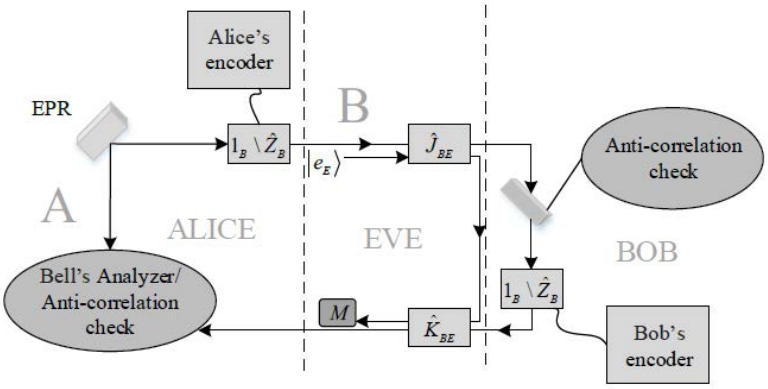

Figure 1: The anti-correlation check process of Degiovanni et al.'s QDKD protocol

3 The proposed efficient QDKD-SP protocol

3.1 The procedures of QDKD-SP protocol

The proposed protocol combines the dense coding mechanism in Degiovanni et al.'s protocol and the bias-BB84 protocol to achieve the advantages of both protocols, i.e., the high efficiency and easy implementation. Suppose Alice and Bob transmit their secret message to each other through the protocol, and *R*-basis $\{|0\rangle,|1\rangle\}$, *D*-basis $\{|+\rangle,|-\rangle\}$. And the specific steps of the proposed QDKD-SP protocol are as follows.

Step 1: Alice randomly prepares a photon $|\varphi\rangle$ in state $|0\rangle$ or $|1\rangle$ with equal probability. Then, Alice randomly uses one of four polarized operations u_{00}, u_{01}, u_{10} and u_{11} to polarize the photon and sends it to Bob. These four polarized operations on the single photon are defined as follows.

$$\begin{cases} u_{00}: \text{ polarizes the photon with } 0^{\circ}, \\ u_{01}: \text{ polarizes the photon with } 45^{\circ}, \\ u_{11}: \text{ polarizes the photon with } 90^{\circ}, \\ u_{10}: \text{ polarizes the photon with } 135^{\circ}. \end{cases} \tag{4}$$

where the operations u_{01} and u_{10} with probability $(p/2)$, respectively, and the operations u_{00} and u_{11} with probability $((1-p)/2)$, respectively, where $0 < p \leq 1/2$.

Step 2: Bob receives the polarized photon, polarizes it in the same strategy as Alice, and then returns it to Alice.

Step 3: Alice receives the polarized photon and measures the photon by using *R*-basis with probability $(1-p)$ or using *D*-basis with the probability p to get the state $|\varphi'\rangle$. After the measurement, she sends the result information to Bob through the classic channel. The result information is determined by $|\varphi'\rangle - |\varphi\rangle$. If $|\varphi'\rangle - |\varphi\rangle = |0\rangle$, the result information is "00"; if $|\varphi'\rangle - |\varphi\rangle = |-\rangle$, the result information is "01"; if $|\varphi'\rangle - |\varphi\rangle = |1\rangle$ the result information is "10"; if $|\varphi'\rangle - |\varphi\rangle = |+\rangle$, the result information is "11".

Step 4: Bob uses the classic channel to inform Alice of the information about polarized operations. Bob announces the bit "0" if he polarizes the photon with 0^o or 90^o and "1" for 45^o or 135^o.

Step 5: Alice determines whether the measurement base used is correct based on the received information. If it is correct, it is marked as "Y"; otherwise, it is marked as "N". Then, Alice sends the location information of "Y" and "N" to Bob.

Step 6: Bob discards all information marked "N" according to the location information sent by Alice.

Step 7: Alice and Bob generate a shared bit string based on their own information and the received information.

3.2 An example of QDKD-SP protocol

We take a 12-bit sample sequence as an example and the detail operation is listed and described in Tab. 1. Suppose Alice has the $|0\rangle$ photon for the first bit after operation. From the announced bit "0" (Alice does not change the basis, i.e., uses *R*-basis), so she knows that she chooses the right basis. Also, Alice checks her measurement result $|1\rangle$, and $|\varphi'\rangle - |\varphi\rangle = |1\rangle - |0\rangle| = |1\rangle$, and then she announces "10". Because Alice and Bob know their own operations, so Alice knows that Bob uses u_{11} and Bob knows that Alice uses u_{00}. Finally, they share four information bits "0011", where "00" is generated by Alice's operation and "11" is generated by Bob's operation.

Because the announcements of Alice and Bob are disclosed publicly, correspondent to the B's announcement "0" or "1" and A's announcement "00", "01", "10", "11", an eavesdropper Eve on the public channel can intercept some information by correlating the two announcements. For example, the announcements of Alice and Bob are "10" and "0" for the first bit in Tab. 1. Eve does not get the direct information on the single key B (the last two bits produced by B), however, she knows the possible key B is "00" or "11". And from the disclosure of A's announcement "10", Eve has the correlation of the single key A (the first two bits produced by A) and the single key B, i.e., she knows the single key A is "11" (resp. "00") when the single key B is "00" (resp. "11"). This obviously induces a lack of security. In fact, the lack of security for our QDKD-SP protocol is the same as Degiovanni et al.'s QDKD protocol. To ensure the security, we can use the single key A and the single key B like the way mentioned in Degiovanni et al. [Degiovanni, Berchera, Castelletto et al. (2004)].

Table 1: A 12-bit sample of Alice (A) and Bob (B) for the proposed QDKD-SP protocol

	Sequence of bits	1	2	3	4	5	6	7	8	9	10	11	12
1	A's initial state	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
2	A's operation	u_{00}	u_{11}	u_{11}	u_{01}	u_{10}	u_{11}	u_{01}	u_{10}	u_{00}	u_{11}	u_{01}	u_{01}
	After operation	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$
3	B's operation	u_{11}	u_{11}	u_{10}	u_{11}	u_{10}	u_{10}	u_{00}	u_{00}	u_{00}	u_{00}	u_{01}	u_{10}
	After operation	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
4	A's basis	*R*	*R*	*D*	*D*	*R*	*R*	*D*	*D*	*R*	*D*	*R*	*R*
	Announce	10	00	01	11	10	01	01	11	00	10	10	00
5	B's Announce	0	0	1	0	1	1	0	0	0	0	1	1
6	A's response	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y
7	Shared bits	0011	1111	1110	0111	1010	–	0100	1000	0000	–	0101	0110

As shown in Fig. 2, the overall correct received probability is to add up Case (1), Case (4), Case (6) and Case (7), and then we obtain $\left((1-p)^3+3p^2(1-p)\right)$. The number of bits and qubits for the proposed QDKD-SP are b_s=4, b_t=3 and $q_t = q_{(A\rightarrow B)} = q_{(A\leftarrow B)} = 1$, where b_t=3 is two bits in Step 4 and one bit in Step 5 (see Tab. 1).

4 Security analysis

Our protocol uses the operations on the single polarized photon with the bias probability to transmit the secret information. Thus, it is compromised by the intercept-resend attack. Similar to bias-BB84, we should do the refined error analysis in our protocol. Suppose that Eve intercepts the photons using *R*-basis or *D*-basis with the probabilities p_R and p_D, respectively, and does nothing with the probability $(1-p_R-p_D)$. By using the intercept-resend attack, Eve has two ways to compromise our QDKD-SP protocol: one is to use the intercept-resend attack in only one stage (Alice→Bob stage or Bob→Alice stage), and the other is to use the intercept-resend attack in both two stages (Alice→Bob stage and Bob→Alice stage). The error rates for these two cases are calculated as follow.

4.1 Single-stage intercept-resend attack

By resending the photon in the Alice→Bob (or Bob→Alice) stage, it may cause the error when choosing the wrong basis to intercept the photon. First, we discuss the interception on the Alice→Bob stage. All erroneous situations are summarized in Tab. 2. Suppose that

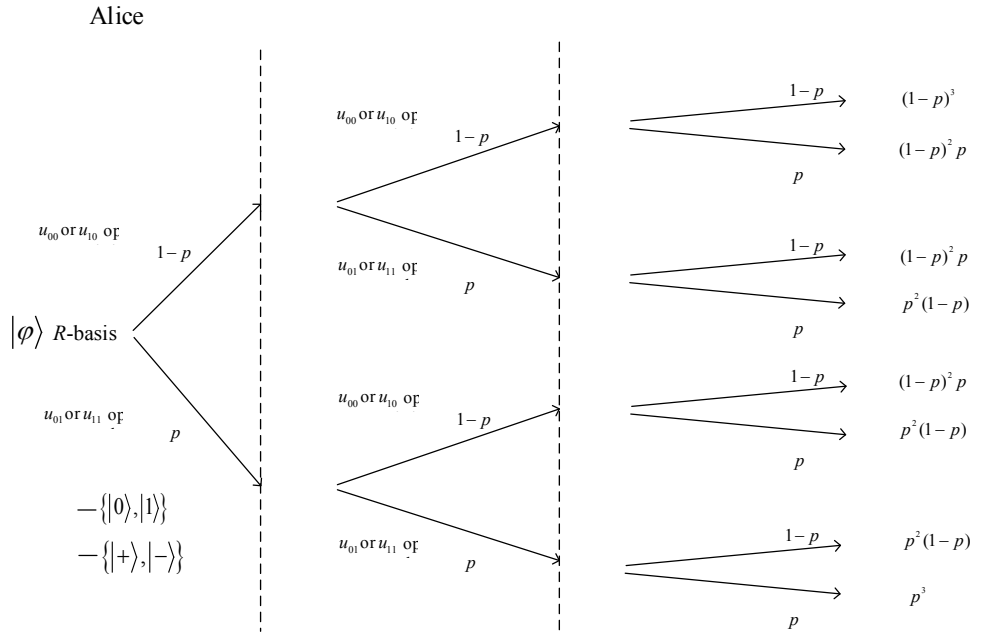

Figure 2: The received probability for all eight cases

Alice prepares the photon $|0\rangle$ and her operation is u_{00} or u_{11}, then the photon is polarized to the photon $|0\rangle$ or $|1\rangle$ which are both in *R*-basis. When Eve uses the *D*-basis to intercept the photon, she obtains the wrong measurement and resends the wrong photon state ($|+\rangle$ or $|-\rangle$). After Bob's announcement, Alice knows that the basis is not changed and she should use the *R*-basis to receive the correct state. However, there is 50% probability to share the wrong photon due to the incorrect one resent by Eve. The probability for this case is $(1-p)\times(p_D)\times(1-p)\times(1-p)\times 1/2=(1-p)^3(p_D/2)$.

Table 2: Eve (E) uses the wrong basis to eavesdrop in the Alice(A)→Bob(B) stage

	A's operation	E's basis	B's operation	A's basis	Error probability
(1)	$(0^\circ, 90^\circ)$ $(1-p)$	D (p_D)	$(0^\circ, 90^\circ)$ $(1-p)$	R $(1-p)$	$(1-p)^3(p_D/2)$
(2)	$(0^\circ, 90^\circ)$ $(1-p)$	D (p_D)	$(45^\circ, 135^\circ)$ (p)	D (p)	$(1-p)p^2(p_D/2)$
(3)	$(45^\circ, 135^\circ)$ (p)	R (p_R)	$(0^\circ, 90^\circ)$ $(1-p)$	D (p)	$(1-p)p^2(p_R/2)$
(4)	$(45^\circ, 135^\circ)$ (p)	R (p_R)	$(45^\circ, 135^\circ)$ (p)	R $(1-p)$	$(1-p)p^2(p_R/2)$

According to the refined error analysis, the error rates $E_R^{(A\to B)}$ and $E_D^{(A\to B)}$ caused by Eve's eavesdropping for the cases that Alice uses *R*-basis and *D*-basis are calculated respectively as follows:

$$E_R^{(\mathrm{A}\to\mathrm{B})} = \left(\frac{\text{the error probability with eavesdropping when Alice uses } R\text{-basis}}{\text{the correct received probability without eavesdropping when Alice uses } R\text{-basis}} \right)$$
$$= \left(\frac{\text{Case (1) + Case (4) in Table 2}}{\text{Case (1) + Case (7) in Fig. 2}} \right)$$
$$= \left((1-p)^3 (p_D/2) + (1-p) p^2 (p_R/2) \right) \Big/ \left((1-p)^3 + (1-p) p^2 \right)$$
$$= \left((1-p)^2 p_D + p^2 p_R \right) \Big/ \left(2\left((1-p)^2 + p^2 \right) \right). \quad (5)$$

$$E_D^{(\mathrm{A}\to\mathrm{B})} = \left(\frac{\text{the error probability with eavesdropping when Alice uses } D\text{-basis}}{\text{the correct received probability without eavesdropping when Alice uses } D\text{-basis}} \right)$$
$$= \left(\frac{\text{Case (2) + Case (3) in Table 2}}{\text{Case (4) + Case (6) in Fig. 2}} \right)$$
$$= \left((1-p) p^2 (p_D/2) + (1-p) p^2 (p_R/2) \right) \Big/ \left(2(1-p) p^2 \right)$$
$$= (p_D + p_R)/4 \quad (6)$$

Therefore, the average rate $\overline{E}^{(\mathrm{A}\to\mathrm{B})}$ for the single-stage (Alice→Bob) intercept-resend attack is

$$\overline{E}^{(\mathrm{A}\to\mathrm{B})} = \left(\frac{\text{the error probability with eavesdropping}}{\text{the correct received probability without eavesdropping}} \right)$$
$$= \left(\frac{\text{Case (1) + Case (2) + Case (3) + Case (4) in Table 2}}{\text{Case (1) + Case (4) + Case (6) + Case (7) in Fig. 2}} \right)$$
$$= \left((1-p)^2 (p_D/2) + p^2 (p_R + p_D/2) \right) \Big/ \left((1-p)^2 + 3p^2 \right). \quad (7)$$

Suppose that Alice always eavesdrops solely along the *R*-basis (i.e., $p_R = 1$ and $p_D = 0$), then

$$\overline{E}^{(\mathrm{A}\to\mathrm{B})} = \left(p^2 \Big/ 2\left((1-p)^2 + 3p^2 \right) \right). \quad (8)$$

Because Alice uses the operations u_{00} and u_{11} with the probability tends to 1, so eavesdropping the quantum channel with the probabilities $p_R = 1$ and $p_D = 0$ is reasonable. The average error rate $\overline{E}^{(\mathrm{A}\to\mathrm{B})} \to 0$ as p tends to 0. Hence Alice and Bob cannot detect Eve's eavesdropping. The refined error analysis can make our protocol against the single-stage (Alice→Bob) intercept-resend attack. It is evident that, from Eq. (6), the error rate $\overline{E}_D^{(\mathrm{A}\to\mathrm{B})}$ is 1/4.

Secondly, we consider the interception on the Bob→Alice stage, and Tab. 3 shows the erroneous situations caused by the eavesdropping in the Bob→Alice stage. For example, Alice prepares the |0⟩-photon, after the operations of Alice and Bob's operation, the photon may be |0⟩-photon or |1⟩-photon which are both in *R*-basis. When Eve uses the *D*-basis to intercept the photon, she gets the wrong measurement and resends the wrong photon state (|+⟩ or |–⟩). After Bob's announcement, Alice knows that the basis is not

changed and she should use the *R*-basis to receive the correct state. However, there is 50% probability to share the wrong photon due to the incorrect one resent by Eve.

Table 3: Eve (E) uses the wrong basis to eavesdrop in the Bob(B)→Alice(A) stage

	A's operation	B's operation	E's basis	A's basis	Error rate
(1)	$(0^\circ, 90^\circ)$ $(1-p)$	$(0^\circ, 90^\circ)$ $(1-p)$	D (p_D)	R $(1-p)$	$(1-p)^3(p_D/2)$
(2)	$(0^\circ, 90^\circ)$ $(1-p)$	$(45^\circ, 135^\circ)$ (p)	R (p_R)	D (p)	$(1-p)p^2(p_R/2)$
(3)	$(45^\circ, 135^\circ)$ (p)	$(0^\circ, 90^\circ)$ $(1-p)$	R (p_R)	D (p)	$(1-p)p^2(p_R/2)$
(4)	$(45^\circ, 135^\circ)$ (p)	$(45^\circ, 135^\circ)$ (p)	D (p_D)	R $(1-p)$	$(1-p)p^2(p_D/2)$

The error rates $E_R^{(\mathrm{B}\to\mathrm{A})}$, $E_D^{(\mathrm{B}\to\mathrm{A})}$ when Alice uses *R*-basis and *D*-basis, and the average error rate $\overline{E}^{(\mathrm{B}\to\mathrm{A})}$ are calculated as Eqs. (9), (10) and (11), respectively.

$$\begin{aligned} E_R^{(\mathrm{B}\to\mathrm{A})} &= \left(\frac{\text{Case (1) + Case (4) in Table 3}}{\text{Case (1) + Case (7) in Fig. 2}}\right) \\ &= \left((1-p)^3(p_D/2)+(1-p)p^2(p_D/2)\right)\Big/\left((1-p)^3+(1-p)p^2\right) \\ &= \left((1-p)^2 p_D + p^2 p_D\right)\Big/\left(2\left((1-p)^2+p^2\right)\right). \end{aligned} \tag{9}$$

$$\begin{aligned} E_D^{(\mathrm{B}\to\mathrm{A})} &= \left(\frac{\text{Case (2) + Case (3) in Table 3}}{\text{Case (4) + Case (6) in Fig. 2}}\right) \\ &= \left((1-p)p^2(p_R/2)+(1-p)p^2(p_R/2)\right)\Big/\left(2(1-p)p^2\right) \\ &= p_R/2. \end{aligned} \tag{10}$$

$$\begin{aligned} \overline{E}^{(\mathrm{B}\to A)} &= \left(\frac{\text{Case (1) + Case (2) + Case (3) + Case (4) in Table 3}}{\text{Case (1) + Case (4) + Case (6) + Case (7) in Fig. 2}}\right) \\ &= \left((1-p)^2(p_D/2)+p^2(p_R+p_D/2)\right)\Big/\left(\left((1-p)^2+3p^2\right)\right) \\ &= p^2\Big/\left((1-p)^2+3p^2\right) \quad \text{for } p_R=1 \text{ and } p_D=0. \end{aligned} \tag{11}$$

From Eq. (11), it is evident that $\overline{E}^{(\mathrm{B}\to\mathrm{A})}\to 0$ as p tends to 0. However, by using the refined error analysis the error rate $\overline{E}_D^{(\mathrm{B}\to\mathrm{A})}$ is 1/2.

4.2 Two-stage intercept-resend attack

Actually, Eve can eavesdrop in both two stages (Alice→Bob and Bob→Alice) simultaneously. Consider the case that Eve at least uses a wrong basis in one of the two stages. The wrong basis polarizes the photon to another basis and results in the possible erroneous situations (see Tab. 4).

Table 4: Eve(E) at least uses a wrong basis in one of the two stages

	A's operation	E's basis	B's operation	E's basis	A's basis	Error rate
(1)	$\begin{matrix}(0^\circ, 90^\circ)\\(1-p)\end{matrix}$	$D(p_D)$	$\begin{matrix}(0^\circ, 90^\circ)\\(1-p)\end{matrix}$	–	$R(1-p)$	$(1-p)^3(p_D^2/2)+$ $(1-p)^3(p_D p_R/4)$
(2)	$\begin{matrix}(0^\circ, 90^\circ)\\(1-p)\end{matrix}$	$D(p_D)$	$\begin{matrix}(45^\circ, 135^\circ)\\(p)\end{matrix}$	–	$D(p)$	$(1-p)p^2(p_D p_R/2)$ $+(1-p)p^2(p_D^2/4)$
(3)	$\begin{matrix}(45^\circ, 135^\circ)\\(p)\end{matrix}$	$R(p_R)$	$\begin{matrix}(0^\circ, 90^\circ)\\(1-p)\end{matrix}$	–	$D(p)$	$(1-p)p^2(p_R^2/2)+$ $(1-p)p^2(p_D p_R/4)$
(4)	$\begin{matrix}(45^\circ, 135^\circ)\\(p)\end{matrix}$	$R(p_R)$	$\begin{matrix}(45^\circ, 135^\circ)\\(p)\end{matrix}$	–	$R(1-p)$	$(1-p)p^2(p_R^2/4)+$ $(1-p)p^2(p_D p_R/2)$
(5)	$\begin{matrix}(0^\circ, 90^\circ)\\(1-p)\end{matrix}$	$R(p_R)$	$\begin{matrix}(0^\circ, 90^\circ)\\(1-p)\end{matrix}$	$D(p_D)$	$R(1-p)$	$(1-p)^3(p_D p_R/2)$
(6)	$\begin{matrix}(0^\circ, 90^\circ)\\(1-p)\end{matrix}$	$R(p_R)$	$\begin{matrix}(45^\circ, 135^\circ)\\(p)\end{matrix}$	$R(p_R)$	$D(p)$	$(1-p)p^2(p_R^2/2)$
(7)	$\begin{matrix}(45^\circ, 135^\circ)\\(p)\end{matrix}$	$D(p_D)$	$\begin{matrix}(0^\circ, 90^\circ)\\(1-p)\end{matrix}$	$R(p_R)$	$D(p)$	$(1-p)p^2(p_D p_R/2)$
(8)	$\begin{matrix}(45^\circ, 135^\circ)\\(p)\end{matrix}$	$D(p_D)$	$\begin{matrix}(45^\circ, 135^\circ)\\(p)\end{matrix}$	$D(p_D)$	$R(1-p)$	$(1-p)p^2(p_D^2/2)$

The error rates $E_R^{(A\rightleftarrows B)}$, $E_D^{A\rightleftarrows B}$ caused by Eve's eavesdropping in both two stages (Alice→Bob and Bob→Alice) when Alice uses *R*-basis or *D*-basis, and the average error rate $\bar{E}^{A\rightleftarrows B}$ are calculated respectively as below,

$$E_R^{(A\rightleftarrows B)} = \left(\frac{\text{Case (1) + Case (4) + Case (5) + Case (8) in Tab. 4}}{\text{Case (1) + Case (4) + Case (6) + Case (7) in Fig. 2}}\right)$$
$$= \left((1-p)^2\left(2p_D{}^2 + 3p_D p_R\right) + p^2\left(p_R{}^2 + 2p_D p_R + 2p_D{}^2\right)\right) \Big/ 4\left((1-p)^2 + p^2\right), \quad (12)$$

$$E_D^{A\rightleftarrows B} = \left(\frac{\text{Case (2) + Case (3) + Case (6) + Case (7) in Tab. 4}}{\text{Case (1) + Case (4) + Case (6) + Case (7) in Fig. 2}}\right)$$
$$= \left((1-p)p^2\left(p_D p_R/2 + p_D{}^2/4 + p_R{}^2/2 + p_D p_R/4 + p_R{}^2/2 + p_D p_R/2\right)\right) \Big/ \left(2(1-p)p^2\right), \quad (13)$$
$$= \left(5p_R p_D + p_D{}^2 + 4p_R{}^2\right)/8$$

$$\overline{E}^{\mathrm{A}\rightleftarrows\mathrm{B}} = \left(\frac{\text{All cases in Tab. 4}}{\text{Case (1) + Case (4) + Case (6) + Case (7) in Fig. 2}} \right)$$
$$= \left((1-p)^2 \left(p_D^2/2 + 3p_D p_R/4 \right) + p^2 \left(5p_R{}^2/4 + 3p_D^2/4 + 7\, p_D p_R/4 \right) \Big/ \left((1-p)^2 + 3p^2 \right) \right). \quad (14)$$
$$= \left(\left(5p^2/4 \right) \Big/ \left((1-p)^2 + 3p^2 \right) \right) \quad \text{for } p_R = 1 \text{ and } p_D = 0$$

$\overline{E}^{(\mathrm{B}\rightleftarrows\mathrm{A})} \to 0$ as p tends to 0. Through the refined error analysis, the error rate $\overline{E}_D^{(\mathrm{B}\rightleftarrows\mathrm{A})}$ is 1/2. Because $\overline{E}_D^{(\mathrm{A}\to\mathrm{B})}$ =1/4, $\overline{E}_D^{(\mathrm{B}\to\mathrm{A})}$ =1/2 and $\overline{E}_D^{(\mathrm{B}\rightleftarrows\mathrm{A})}$ =1/2 are substantially larger than the error rate 1/4 in the original BB84, Alice and Bob can successfully detect Eve's eavesdropping.

5 Efficiency analysis

In this paper, we use two types of key distribution efficiency [Lo, Chau and Ardehali (2005)] to fairly evaluate our QDKD-SP protocol. One is the so-called theoretical efficiency from the point of information theory, and the other is the practical efficiency which is used for precisely measuring the practical protocols.

5.1 Definition of key distribution efficiency

In order to compare the key distribution efficiency of QKD protocol, there is a theoretical definition on the efficiency $\varepsilon_1 = \left(b_s / \left(q_t + b_t \right) \right)$ from the point of information theory, where b_s is the shared bits, b_t is the announced bits per transmission (using the classical channel) and q_t is the number of sent photons per transmission (using the quantum channel). In fact, this definition of efficiency ignores the bits used for checking integration when eavesdropped. This theoretical definition shows a bound of efficiency, but it is not precisely to measure the efficiency for comparing practical QKD protocols.

Another practical key distribution efficiency (more suitably used for evaluating a QKD protocol) is defined as $\varepsilon_2 = \left(b_s / q_{(\mathrm{A}\to\mathrm{B})} \right)$ for one-stage protocol and $\varepsilon_2 = \left(0.5 \times b_s / \left(q_{(\mathrm{A}\to\mathrm{B})} + q_{(\mathrm{A}\leftarrow\mathrm{B})} \right) \right)$ for two-stage protocol, respectively, where $q_{(\mathrm{A}\to\mathrm{B})}$ is the qubits traveling from Alice to Bob in the one-stage protocol and $q_{(\mathrm{A}\leftarrow\mathrm{B})}$ is the qubits traveling from Bob to Alice in the two-stage protocol. Notice that $q_t = q_{(\mathrm{A}\to\mathrm{B})}$ and $q_{(\mathrm{A}\leftarrow\mathrm{B})}$=0 for the one-stage protocol, and $q_t = q_{(\mathrm{A}\to\mathrm{B})} = q_{(\mathrm{B}\to\mathrm{A})}$ for the two-stage protocol.

5.2 Efficiency comparison

The efficiency ε_1 is a theoretical evaluation for a lossless, noiseless quantum channel and perfect detectors. It is valid to show whether the limit of $\varepsilon_1 = 1$ is achieved. This is the most fundamental question in information theory. At this time, the bits and qubits are considered as two types of the same source. However, the efficiency ε_2 is more practical on the efficiency measurement. Both efficiencies have their substance, and we may use each in its proper purpose. For example, the number of bits and qubits for BB84

are: b_s=1, b_t=1, q_t=$q_{(A\to B)}$=1 and $q_{(A\leftarrow B)}$=0. The efficiencies are $\varepsilon_1 = \left(b_s/\left(q_t + b_t\right)\right) = \left(0.5/\left(1+1\right)\right)$ =25% and $\varepsilon_2 = \left(b_s/q_{(A\to B)}\right)$ =0.5/1=50%. It is more reasonable to say that the efficiency of BB84 is ε_2 =50% without privacy amplification when considering the practical application.

According to the example of Section 3.2, we can find out the efficiencies ε_1 and ε_2 of this example. The efficiencies ε_1 and ε_2 are:

$$\begin{aligned}\varepsilon_1 &= b_s/\left(q_t + b_t\right) = 4\times\left(\left(1-p\right)^3 + 3p^2\left(1-p\right)\right)\Big/\left(1+3\right) \\ &= \left(1-p\right)^3 + 3p^2\left(1-p\right)\end{aligned}, \tag{15}$$

$$\begin{aligned}\varepsilon_2 &= 0.5\times b_s/\left(q_{(A\to B)} + q_{(A\to B)}\right) = 0.5\times 4\times\left(\left(1-p\right)^3 + 3p^2\left(1-p\right)\right)\Big/\left(1+1\right) \\ &= \left(1-p\right)^3 + 3p^2\left(1-p\right)\end{aligned}. \tag{16}$$

The values of $\varepsilon_1 = \varepsilon_2$ are about 100% as p tends to 0. The proposed QDKD-SP protocol is dense like Degiovanni et al.'s QDKD because the efficiency ε_1 =100% is the same as Degiovanni et al.'s QDKD protocol.

Comparison among BB84, bias-BB84, Degiovanni et al.'s QDKD and the proposed QDKD protocol is summarized in Tab. 5. Certainly, efficiency is an important point of comparison of QKD protocols. Both efficiencies ε_1 and ε_2 have their own substances, and we may use each in its proper purpose. Our QDKD-SP protocol is a hybrid of two schemes: Degiovanni et al.'s QDKD and bias-BB84. Thus, it has the same advantage of Degiovanni et al.'s QDKD, i.e., the efficiency of our protocol ε_1 =100% (note that ε_1 =25% and 50% for BB84 and bias-BB84). Also, our protocol has the same advantage of bias-BB84, which is implemented by the single polarized photon rather than the Entangled state and the efficiency ε_2 is 100% (Note: ε_2 =50% for BB84 and Degiovanni et al.'s QDKD). Among these four QKD protocols, it is observed that our new protocol is the best choice from either practical or theoretical consideration.

Table 5: Comparison among different QKD protocols

QKD Protocols		BB84	Bias-BB84	Degiovanni et al.'s QDKD	QDKD-SP
Number of bits and qubits	b_s	0.5	2	2	4
	b_t	1	1	1	3
	q_t	1	1	1	1
	$q_{(A\rightarrow B)}$	1	1	1	1
	$q_{(A\leftarrow B)}$	0	1	1	1
Efficiency	ε_1	25%	100%	100%	100%
	ε_2	50%	50%	50%	100%
Extra requirement		None	Refined analysis	Operations on entangled pair and anti-correlation check	Operations on the single photon and refined analysis
Transmitting stage		The single stage (Alice→Bob)		Two stages (Alice→Bob; Bob→ Alice)	
Photon type		Single photon		Entangled state	Single photon

6 Conclusion

As we know, efficiency and security are the main goals of the ongoing research of the QKD protocol. In this paper, through combing the bias-BB84 protocol and dense coding mechanism, we proposed a new efficient protocol with dense coding on single photons, which can achieve the high key distribution efficiencies ($\varepsilon_1 = \varepsilon_2 = 100\%$) and easy implementation (the single photon is more feasible in physical implementation than those entangled quantum resources). Moreover, our protocol is theoretically proved to be secure against the intercept-resend attacks. We believe that our work will have some reference value in the future practical application of quantum key distribution, quantum direct communication, or even the construction of quantum internet.

Acknowledgement: The authors would like to thank the anonymous reviewers and editor for their comments that improved the quality of this paper. This work is supported by the Natural Science Foundation of China under Grant No. 11272120.

References

Bechmann-Pasquinucci, H.; Tittel, W. (2000): Quantum cryptography using larger alphabets. *Physical Review A*, vol. 61, no. 6, 062308.

Bennett, C. H.; Brassard, G. (1984): Quantum cryptography: public key distribution and coin tossing. *International Conference on Computers, Systems & Signal Processing*, pp. 175-179.

Bennett, C. H. (1992): Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, vol. 68, no. 21, pp. 3121.

Bennett, C. H.; Wiesner, S. J. (1992): Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, vol. 69, no. 20, pp. 2881.

Chen, X. B.; Sun, Y. R.; Xu, G.; Jia, H. Y.; Qu, Z. et al. (2017): Controlled bidirectional remote preparation of three-qubit state. *Quantum Information Processing*, vol. 16, no. 10, pp. 244.

Chen, X. B.; Tang, X.; Xu, G.; Dou, Z.; Chen, Y. L. et al. (2018): Cryptanalysis of secret sharing with a single d-level quantum system. *Quantum Information Processing*, vol. 17, no. 9, pp. 225.

Chong, S. K.; Hwang, T. (2010): Quantum key agreement protocol based on BB84. *Optics Communications*, vol. 283, no. 6, pp. 1192-1195.

Degiovanni, I. P.; Berchera, I. R.; Castelletto, S.; Rastello, M. L.; Bovino, F. A. et al. (2004): Quantum dense key distribution. *Physical Review A*, vol. 69, no. 3, 032310.

Degiovanni, I. P.; Berchera, I. R.; Castelletto, S.; Rastello, M. L.; Bovino, F. et al. (2005): Reply to "comment on 'quantum dense key distribution'". *Physical Review A*, vol. 71, no. 1, 016302.

Ekert, A. K. (1991): Quantum cryptography based on Bell's theorem. *Physical Review Letters*, vol. 67, no. 6, pp. 661.

Huang, W.; Su, Q.; Liu, B.; He, Y. H.; Fan, F. et al. (2017): Efficient multiparty quantum key agreement with collective detection. *Scientific Reports*, vol. 7, no. 1, 15264.

Hwang, T.; Hwang, C. C.; Tsai, C. W. (2011): Quantum key distribution protocol using dense coding of three-qubit W state. *European Physical Journal D*, vol. 61, no. 3, pp. 785-790.

Karimipour, V.; Bahraminasab, A.; Bagherinezhad, S. (2002): Quantum key distribution for d-level systems with generalized Bell states. *Physical Review A*, vol. 65, no. 5, 052331.

Liu, W.; Chen, H.; Li, Z.; Liu, Z. (2008): Efficient quantum secure direct communication with authentication. *Chinese Physics Letters*, vol. 25, no. 7, pp. 2354-2357.

Liu, W.; Chen, H.; Ma, T.; Li, Z.; Liu, Z. et al. (2009): An efficient deterministic secure quantum communication scheme based on cluster states and identity authentication. *Chinese Physics B*, vol. 18, no. 10, pp. 4105-4109.

Liu, W.; Liu, C.; Wang, H.; Jia, T. (2013): Quantum private comparison: a review. *IETE Technical Review*, vol. 30, no. 5, pp. 439-445.

Liu, W.; Liu, C.; Chen, H.; Li, Z.; Liu, Z. (2014): Cryptanalysis and improvement of quantum private comparison protocol based on Bell entangled states. *Communications in Theoretical Physics*, vol. 62, no. 2, pp. 210-214.

Liu, W.; Liu, C.; Liu, Z.; Liu, J.; Geng, H. (2014): Same initial states attack in Yang et al.'s quantum private comparison protocol and the improvement. *International Journal of Theoretical Physics*, vol. 53, no. 1, pp. 271-276.

Liu, W.; Liu, C.; Wang, H.; Liu, J.; Wang, F. et al. (2014): Secure quantum private comparison of equality based on asymmetric *W* state. *International Journal of Theoretical Physics*, vol. 53, no. 6, pp. 1804-1813.

Liu, W.; Wang, F.; Ji, S.; Qu, Z.; Wang, X. (2014): Attacks and improvement of quantum sealed-bid auction with EPR pairs. *Communications in Theoretical Physics*, vol. 61, no. 6, pp. 686-690.

Liu, W.; Chen, Z.; Liu, C.; Zheng, Y. (2015): Improved deterministic *N*-to-one joint remote preparation of an arbitrary qubit via EPR pairs. *International Journal of Theoretical Physics*, vol. 54, no. 2, pp. 472-483.

Liu, W.; Wang, H.; Yuan, G.; Xu, Y.; Chen, Z. et al. (2016): Multiparty quantum sealed-bid auction using single photons as message carrier. *Quantum Information Processing*, vol. 15, no. 2, pp. 869-879.

Liu, W.; Chen, Z.; Ji, S.; Wang, H.; Zhang, J. (2017): Multi-party semi-quantum key agreement with delegating quantum computation. *International Journal of Theoretical Physics*, vol. 56, no. 10, pp. 3164-3174.

Liu, W.; Chen, Z.; Liu, J.; Su, Z.; Chi, L. (2018): Full-blind delegating private quantum computation. *Computers, Materials & Continua*, vol. 56, no. 2, pp. 211-223.

Liu, W.; Gao, P.; Yu, W.; Qu, Z.; Yang, C. (2018): Quantum relief algorithm. *Quantum Information Processing*, vol. 17, no. 10, pp. 280.

Liu, W.; Gao, P.; Wang, Y.; Yu, W.; Zhang, M. (2019): A unitary weights based one-iteration quantum perceptron algorithm for non-ideal training sets. *IEEE Access*. https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639.

Liu, W.; Xu, Y.; Yang, C.; Gao, P.; Yu, W. (2018): An efficient and secure arbitrary *N*-party quantum key agreement protocol using Bell states. *International Journal of Theoretical Physics*, vol. 57, no. 1, pp. 195-207.

Liu, Z; Chen, H.; Xu, J.; Liu, W.; Li, Z. (2012): High-dimensional deterministic multiparty quantum secret sharing without unitary operations. *Quantum Information Processing*, vol. 11, no. 6, pp. 1785-1795.

Liu, Z.; Chen, H.; Liu, W.; Xu, J. (2013): Quantum simultaneous secret distribution with dense coding by using cluster states. *Quantum information processing*, vol. 12, no. 12, pp. 3745-3759.

Lo, H. K.; Chau, H. F.; Ardehali, M. (2005): Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, vol. 18, no. 2, pp. 133-165.

Qu, Z.; Wu, S.; Wang, M.; Sun, L.; Wang, X. (2017): Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels. *Quantum Information Processing*, vol. 16, no. 12, pp. 306.

Qu, Z.; Chen, S.; Ji, S.; Ma, S.; Wang, X. (2018): Anti-noise bidirectional quantum steganography protocol with large payload. *International Journal of Theoretical Physics*, vol. 57, no. 6, pp. 1903-1927.

Qu, Z.; Cheng, Z.; Liu, W.; Wang, X. (2018): A novel quantum image steganography algorithm based on exploiting modification direction. *Multimedia Tools and Applications*.

Wójcik, A. (2005): Comment on "quantum dense key distribution". *Physical Review A*, vol. 71, no. 1, 016301.

Xu, G.; Chen, X.; Li, J.; Wang, C.; Yang, Y. et al. (2015): Network coding for quantum cooperative multicast. *Quantum Information Processing*, vol. 14, no. 11, pp. 4297-4322.