Enhanced Quantum Key Distribution Protocols Using BB84 and B92

(*Submitted for Cryptography and Information Security*)

Ching-Nung Yang and Chen-Chin Kuo
Department of Computer Science & Information Engineering,
National Dong Hwa University,
1, Sec. 2, Da Hsueh Rd., Shou-Feng, Hualien,
Taiwan, Republic of China
TEL: 886-3-8662500 Ext-22120 FAX: 886-3-8662781
E-mail: cnyang@mail.ndhu.edu.tw

Abstract

Four-state quantum key distribution (QKD) protocol BB84 [1] and two-state QKD protocol B92 [2] can let Alice and Bob share the secret key with idealized maximum efficiencies 50% and 25% over quantum channel, respectively. However, for these two polarization-based systems, the polarization states need to be maintained stable and against the noise of photon over a long distance optical fiber. Due to the alignment of polarization and the need of apparatus, the complexity of a four-state protocol is greater than that of two-state protocol. We herein use average number of polarization states in a QKD protocol as the complexity order. In this paper, we propose two enhanced QKD protocols. One is to enhance the idealized maximum efficiency to 28.6% with the average complexity order 2, and the other has the efficiency 42.9% and the average complexity order 2.86.

Keywords: Quantum cryptography, quantum key distribution, uncertainty principle, BB84, B92.

Contact author:
Ching-Nung Yang
E-mail: cnyang@mail.ndhu.edu.tw

1. Introduction

A QKD protocol can provide real-time key distribution over a quantum channel between Alice and Bob who have a need to communicate secretly. The principle of QKD is based on the uncertainty principle of quantum physics; however, the conventional key distribution protocols such as Diffie-Hellman and RSA key exchange protocols are based on computation infeasibility of certain problems in number theory. So, QKD can provide perfect secrecy, since the cryptanalytic tools in conventional cryptography will be of no use for quantum cryptography [3]. The first demonstration of QKD protocol was over 30 cm of free-space [2], and recently it was extended to 1.9km free-space [4]. Now QKD is successfully performed over a long optical fiber [5]. QKD is not only a point-to-point key distribution protocol, but also the any-to-any or any-to-many key distribution in passive optical network [6], [7], [8]. It is believed that QKD protocol will play an important role in future networks [6].

The first QKD protocol was introduced in 1984 [1], termed as the BB84 protocol. BB84 uses two polarization bases, rectilinear (*R*) basis and diagonal (*D*) basis, and the single photon may be polarized with four states: |*h*⟩, |*v*⟩, |*lcp*⟩, and |*rcp*⟩. Polarization state |*h*⟩ (|*v*⟩) in *R-basis* reveals "0" ("1") and polarization state |*lcp*⟩ (|*rcp*⟩) in *D*-basis reveals "0" ("1"). The italic letters *h*, *v*, *lcp*, *rcp* mean *horizontal*, *vertical*, *left circle polarized*, *right circle polarized*.

In [2], a two-state B92 protocol can be regarded as "half" of the BB-84 protocol. Alice and Bob first have agreement that Alice uses |*h*⟩*-photon* and |*rcp*⟩*-photon* to represent "0" and "1". Bob uses |*lcp*⟩*-basis* and |*v*⟩*-basis* as "0" and "1". Table 1 and Table 2 show B92 and BB84 in detail.

B92 QKD protocol :

B92 protocol (see Table 1) begins with Alice sending a random sequence of photons, |*h*⟩*-photon* and |*rcp*⟩*-photon*. Bob randomly chooses one of his detector basis, |*lcp*⟩*-basis* or |*v*⟩*-basis* and records his measurement results (Yes or No). Bob sends a copy of his results to Alice through the public channel. Finally, Alice and Bob will keep the bits where the results are "Y", discarding all other bits.

Table 1. A 12-bit sample of Alice (A) and Bob (B) for B92 protocol

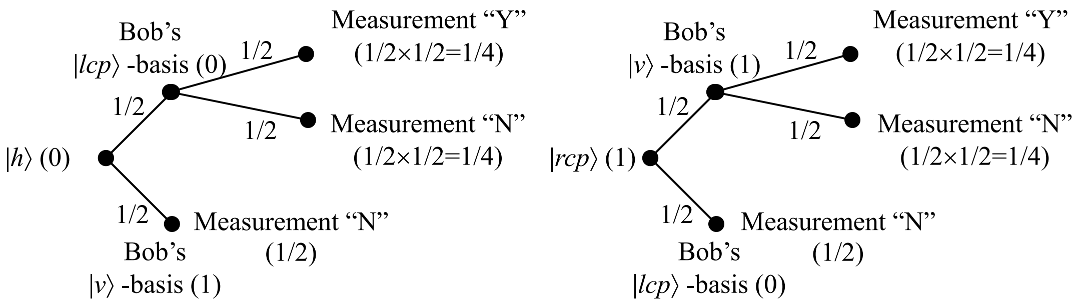
Sequence of bits		1	2	3	4	5	6	7	8	9	10	11	12
(1)	A's bit	1	1	0	0	1	0	1	0	0	0	1	1
	A's polarization	|*rcp*⟩	|*rcp*⟩	|*h*⟩	|*h*⟩	|*rcp*⟩	|*h*⟩	|*rcp*⟩	|*h*⟩	|*h*⟩	|*h*⟩	|*rcp*⟩	|*rcp*⟩
(2)	B's detector basis	|*lcp*⟩	|*v*⟩	|*lcp*⟩	|*v*⟩	|*lcp*⟩	|*lcp*⟩	|*lcp*⟩	|*v*⟩	|*lcp*⟩	|*lcp*⟩	|*v*⟩	|*lcp*⟩
	B's bit	0	1	0	1	0	0	0	1	0	0	1	0
(3)	B's measurement	N	Y	N	N	N	Y	N	N	Y	N	N	N
	Shared secret key	–	1	–	–	–	0	–	–	0	–	–	–

(1) Alice sends a random sequence of photons, |*h*⟩*-photon* and |*rcp*⟩*-photon*.

(2) Bob randomly chooses his detector basis from |*lcp*⟩*-basis* or |*v*⟩*-basis* to measure each photon, and the bases are interpreted as a binary sequence.

(3) Results of Bob's measurement. Alice and Bob will share the bits where the measurement results are "Y", discarding all other bits.

For example, in Table 1, only three bits (2, 6, and 9) are shared by Alice and Bob as the secret key. In this 12-bit example, the efficiency is 3/12=25%. In fact, an idealized maximum efficiency is 25% for B92 protocol. The formal analysis of the efficiency is shown in Figure 1. Suppose that Alice sends $|h\rangle$-*photon*, i.e., "0" (Figure 1(a)). Bob will randomly choose $|lcp\rangle$-*basis* or $|v\rangle$-*basis*. If Bob chooses the wrong basis, i.e., $|v\rangle$-*basis*, he cannot detect the photon. If Bob chooses the correct basis, i.e., $|lcp\rangle$-*basis*, he has 50% probability to detect the photon; however he also has 50% probability to detect nothing even choosing correct basis. Finally, Bob will have the idealized maximum efficiency 25% to share the correct bits between Alice. Figure 1(b) is the case that Alice sends $|rcp\rangle$-*photon*.



(a) Alice sends $|h\rangle$-*photon* (b) Alice sends $|rcp\rangle$-*photon*

Figure 1. Analysis of idealized maximum efficiency for B92 protocol.

BB84 QKD protocol :

The formal description of BB84 protocol is shown in Table 2 . Figure 2 is its analysis of efficiency.

Table 2. A 12-bit sample of Alice (A) and Bob (B) for BB84 protocol

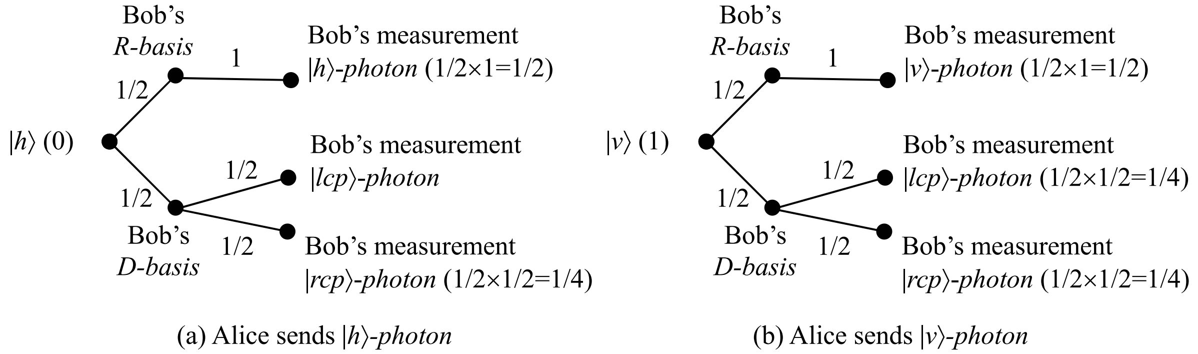
Sequence of bits		1	2	3	4	5	6	7	8	9	10	11	12
(1)	A's bit	1	1	0	0	1	0	1	0	0	0	1	1
	A's source basis	*D*	*R*	*R*	*R*	*D*	*D*	*R*	*D*	*R*	*D*	*R*	*D*
	A's polarization	$\|rcp\rangle$	$\|v\rangle$	$\|h\rangle$	$\|h\rangle$	$\|rcp\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|lcp\rangle$	$\|h\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|rcp\rangle$
(2)	B's detector basis	*D*	*D*	*R*	*R*	*R*	*R*	*R*	*D*	*D*	*R*	*D*	*D*
(3)	B's measurement	$\|rcp\rangle$	$\|lcp\rangle$	$\|h\rangle$	$\|h\rangle$	$\|h\rangle$	$\|v\rangle$	$\|v\rangle$	$\|lcp\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|rcp\rangle$	$\|rcp\rangle$
	B's bit	1	0	0	0	0	1	1	0	0	1	1	1
(4)	B reports basis	*D*	*D*	*R*	*R*	*R*	*R*	*R*	*D*	*D*	*R*	*D*	*D*
(5)	A's response	Y	N	Y	Y	N	N	Y	Y	N	N	N	Y
(6)	Shared secret key	1	–	0	0	–	–	1	0	–	–	–	1

(1) Alice sends a random sequence of photons, $|h\rangle$-*photon*, $|v\rangle$-*photon*, $|lcp\rangle$-*photon*, and $|rcp\rangle$-*photon*.

(2) Bob randomly chooses his detector basis from *R-basis* or *D-basis* to measure each photon.

(3) Results of Bob's measurement. Then, the states are interpreted as a binary sequence.
(4) Bob reports his detector bases for each photon.
(5) Alice tells Bob which bases were correct.
(6) Finally, Alice and Bob will share the bits where A's response is "Y", discarding all other bits.

In Figure 2, if Bob chooses the correct basis, then he will detect the correct polarized photon. However, if Bob chooses the wrong basis, he knows that his result is inconclusive. So the idealized maximum efficiency is 50% for BB84. Figure 2 shows the case that Alice use *R-basis*. Figure 2(a) is that Alice sends $|h\rangle$*-photon* and Figure 2(b) is that Alice sends $|v\rangle$*-photon*.



(a) Alice sends $|h\rangle$*-photon* (b) Alice sends $|v\rangle$*-photon*

Figure 2. Analysis of idealized maximum efficiency for BB84 protocol with Alice using *R-basis*.

If an eavesdropper Eve intercepts the quantum channel, Alice and Bob will find a large part of errors of their shared keys. Thus, in BB84 and B992, Alice and Bob will choose some bits in the shared secret key for verification to find whether Eve eavesdrops or not. We can also add parity bits or error correcting codes through public channel to ensure that the key is error free.

Efficiencies 25% for B92 and 50% for BB84 (see Figure 1 and Figure 2) are the price that these two QKD protocols must pay for secrecy. Here, we will propose two-way transmission over quantum channel (Alice→Bob and Bob→Alice) instead of one-way transmission (Alice→Bob). Our enhanced QKD protocols have two stages. In the first stage, Alice sends a random sequence of photon according B92, and in the second stage, Bob will use BB84 or B92 to send the photons in which Bob's measurement results are "N" in the first stage.

Our enhanced protocol enhances the efficiency to 28.6% with the average complexity order 2 when using B92 in the second stage. When use BB84 in the second stage, the idealized maximum efficiency can reach 42.9% and the average complexity order is 2.86.

2. Our Enhanced QKD Protocols

2.1 The First Enhanced QKD Protocol (B92+BB84)

In B92 protocol, Alice sends a sequence of photons through optical fiber. Bob always randomly chooses the detector bases and measures the photons. If the measurement results are “N”, i.e., we do not detect the photon, then the choice of Bob’ detector bases may be wrong. However, Eve does not know Bob’s basis for the “N” case. Bob herein chooses the *R-basis* (or *D-basis*) when B’s bit (Step (2) in Table 3) is “0” (or “1”) to send the photons. The detector basis of Alice is determined by A’s bit (Step (1) in Table 3). If A’s bit is “1”, then Alice chooses *R-basis* and otherwise *D-basis*. For the first enhanced QKD (FEQKD) protocol, the first stage is same as B92, and in the second stage Bob uses BB84 to resend the photons where he cannot measure correctly in the first stage.

Table 3 shows the FEQKD protocol step by step, Step (1)~(3) are same as Step (1)~(3) in Table 1, and Step (4)~(9) areBB84, but now Bob sends the photons to Alice. Nine bits (1, 3, 4, 5, 7, 8, 10, 11, and12) are resent for this example and in six positions (1, 4, 5, 7, 8, and 12) Alice and Bob have the same bases. We will get the final secret key by combining secret keys in 1st stage and 2nd stage. In this 12-bit example, the finale secret key is “110001101” where positions are 1, 2 , 4, 5, 6, 7 ,8, 9, and 12.

Table 3. A 12-bit sample of Alice (A) and Bob (B) for the FEQKD protocol

	Sequence of bits		1	2	3	4	5	6	7	8	9	10	11	12
1st Stage (A→B)	(1)	A’s bit	1	1	0	0	1	0	1	0	0	0	1	1
		A’s polarization	$\lvert rcp\rangle$	$\lvert rcp\rangle$	$\lvert h\rangle$	$\lvert h\rangle$	$\lvert rcp\rangle$	$\lvert h\rangle$	$\lvert rcp\rangle$	$\lvert h\rangle$	$\lvert h\rangle$	$\lvert h\rangle$	$\lvert rcp\rangle$	$\lvert rcp\rangle$
	(2)	B’s detector basis	$\lvert lcp\rangle$	$\lvert v\rangle$	$\lvert lcp\rangle$	$\lvert v\rangle$	$\lvert lcp\rangle$	$\lvert lcp\rangle$	$\lvert lcp\rangle$	$\lvert v\rangle$	$\lvert lcp\rangle$	$\lvert lcp\rangle$	$\lvert v\rangle$	$\lvert lcp\rangle$
		B’s bit	0	1	0	1	0	0	0	1	0	0	1	0
	(3)	B’s measurement	N	Y	N	N	N	Y	N	N	Y	N	N	N
		Shared secret key in 1nd stage	–	1	–	–	–	0	–	–	0	–	–	–
2nd Stage (B→A)	(4)	B’s source basis	*R*	–	*R*	*D*	*R*	–	*R*	*D*	–	*R*	*D*	*R*
		B’s bit	1	–	0	0	0	–	1	1	–	1	1	1
		B’s polarization	$\lvert v\rangle$	–	$\lvert h\rangle$	$\lvert lcp\rangle$	$\lvert h\rangle$	–	$\lvert v\rangle$	$\lvert rcp\rangle$	–	$\lvert v\rangle$	$\lvert rcp\rangle$	$\lvert v\rangle$
	(5)	A’s detector basis	*R*	–	*D*	*D*	*R*	–	*R*	*D*	–	*D*	*R*	*R*
	(6)	A’s measurement	$\lvert v\rangle$	–	$\lvert lcp\rangle$	$\lvert lcp\rangle$	$\lvert h\rangle$	–	$\lvert v\rangle$	$\lvert rcp\rangle$	–	$\lvert rcp\rangle$	$\lvert h\rangle$	$\lvert v\rangle$
		A’s bit	1	–	0	0	0	–	1	1	–	1	0	1
	(7)	A reports basis	*R*	–	*D*	*D*	*R*	–	*R*	*D*	–	*D*	*R*	*R*
	(8)	B’s response	Y	–	N	Y	Y	–	Y	Y	–	N	N	Y
	(9)	Shared secret key in 1nd stage	1	–	–	0	0	–	1	1	–	–	–	1
	(10)	The final shared secret key	1	1	–	0	0	0	1	1	0	–	–	1

(1)~(3) Same in Table 1.

(4) Bob choose his basis according B’s bit in Step (2), and then he sends a random sequence of photons, $\lvert h\rangle$*-photon*, $\lvert v\rangle$*-photon*, $\lvert lcp\rangle$*-photon*, and $\lvert rcp\rangle$*-photon* where his measurement results are “N” in Step (3).

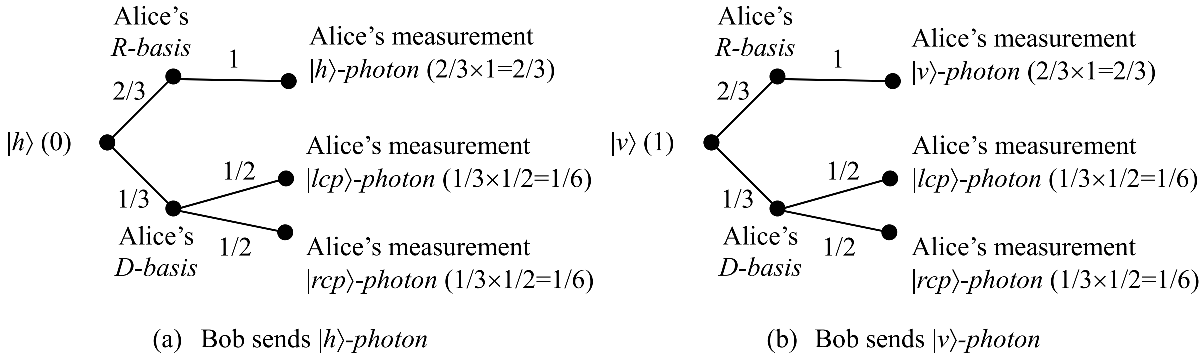
(5) Alice chooses her detector bases according A’s bits in Step (1) to measure each photon.

(6) Results of Alice’s measurement. Then, the states are interpreted as a binary sequence.

(7) Alice reports his detector bases for each photon.
(8) Bob tells Alice which bases were correct.
(9) Alice and Bob will share the bits where the results in Step (3) are "Y" in 2nd stage, discarding all other bits.
(10) Combine Step (3) and (9). Alice and Bob will get the final shared secret key.

From analysis of efficiency for B92 (Figure 1), it is observed that Bob's measurement result is "N" with probability 3/4 (=1/2+1/4), where 1/2 is due to the wrong choice of detector's basis and 1/4 is due to the uncertainty principle. Thus, in the measurement sequence with "N" (Step (3)), there are 2/3 portion of wrong bases and 1/3 portion of correct bases. So, if Bob and Alice choose the bases according B's bit and A's bit in 1st stage, respectively, then they will have same bases with probability 2/3.

Analysis of efficiency for the second stage is shown in Figure 3. When Bob chooses *R-basis* and sends *|h⟩-photon* (Figure 3(a)), Alice may selects the correct basis *R-basis* with probability 2/3 and she will reveal a *|h⟩-photon*. Otherwise, Alice has the wrong basis, *R-basis*, and she will have *|lcp⟩-photon* and *|rcp⟩-photon* with probability 1/6 for each. Efficiency in the second stage will be 2/3 larger than 1/4 in the first stage. Figure 3(b) shows the other case that Bob sends *|v⟩-photon*.



(a) Bob sends *|h⟩-photon* (b) Bob sends *|v⟩-photon*

Figure 3. Analysis of idealized maximum efficiency for FEQKD protocol with Bob using *R-basis*.

2.2 The Second Enhanced QKD Protocol (B92+B92)

For the second enhanced QKD (SEQKD) protocol, the first stage is same as B92 protocol, and in the second stage Bob resends the photons where his detected results are "N".

Same as FEQKD protocol, for the result sequence with "N" in the first stage, there are 2/3 portion of wrong bases and 1/3 portion of correct bases. So, Bob resends a photon in the second stage according the wrong detector's basis. For example, in Table 4, Bob's detection result of the first bit is "N" and Bob's basis is *|lcp⟩*. Thus in the second stage, Bob guesses that he get the wrong basis and then resends a $\lvert rcp\rangle$*-photon* to Alice. However, for the third bit in Table 4, Bob's basis is $\lvert lcp\rangle$ too. He will resend a $\lvert rcp\rangle$*-photon*, but he makes a mistake now. At this time, in the second stage, Alice will choose her detector bases according A's bits (Step (1) in Table 4).

Table 4 shows the SEQKD protocol step by step, Step (1)~(3) is the B92 protocol, where is the first stage in our protocol. Step (4)~(7) is the second stage where Bob resends the photons to Alice. Nine bits (1, 3, 4, 5, 7, 8, 10, 11, and 12) are resent now and six bits (1, 4, 5, 7, 8 and 12) are corrected by Bob; however three bits (3, 10 and 11) are wrong. Combine the shared secret key in Step (3) and Step (6) and we will get the final secret key "110001" for this 12-bit example.

Table 4. A 12-bit sample of Alice (A) and Bob (B) for the SEQKD protocol

	Sequence of bits		1	2	3	4	5	6	7	8	9	10	11	12
1st Stage (A→B)	(1)	A's bit	1	1	0	0	1	0	1	0	0	0	1	1
		A's polarization	$\lvert rcp\rangle$	$\lvert rcp\rangle$	$\lvert h\rangle$	$\lvert h\rangle$	$\lvert rcp\rangle$	$\lvert h\rangle$	$\lvert rcp\rangle$	$\lvert h\rangle$	$\lvert h\rangle$	$\lvert h\rangle$	$\lvert rcp\rangle$	$\lvert rcp\rangle$
	(2)	B's detector basis	$\lvert lcp\rangle$	$\lvert v\rangle$	$\lvert lcp\rangle$	$\lvert v\rangle$	$\lvert lcp\rangle$	$\lvert lcp\rangle$	$\lvert lcp\rangle$	$\lvert v\rangle$	$\lvert lcp\rangle$	$\lvert lcp\rangle$	$\lvert v\rangle$	$\lvert lcp\rangle$
		B's bit	0	1	0	1	0	0	0	1	0	0	1	0
	(3)	B's measurement	N	Y	N	N	N	Y	N	N	Y	N	N	N
		Shared secret key in 1nd stage	–	1	–	–	–	0	–	–	0	–	–	–
2nd Stage (B→A)	(4)	B's bit	1	–	1	0	1	–	1	0	–	1	0	1
		B's polarization	$\lvert rcp\rangle$	–	$\lvert rcp\rangle$	$\lvert h\rangle$	$\lvert rcp\rangle$	–	$\lvert rcp\rangle$	$\lvert h\rangle$	–	$\lvert rcp\rangle$	$\lvert h\rangle$	$\lvert rcp\rangle$
	(5)	A's detector basis	$\lvert v\rangle$	–	$\lvert lcp\rangle$	$\lvert lcp\rangle$	$\lvert v\rangle$	–	$\lvert v\rangle$	$\lvert lcp\rangle$	–	$\lvert lcp\rangle$	$\lvert v\rangle$	$\lvert v\rangle$
		A's bit	1	–	0	0	1	–	1	0	–	0	1	1
	(6)	A's measurement	Y	–	N	N	N	–	N	Y	–	N	N	Y
		Shared secret key in 2nd stage	1	–	–	–	–	–	–	0	–	–	–	1
	(7)	The final shared secret key	1	1	–	–	–	0	–	0	0	–	–	1

(1)~(3) Same in Table 1.

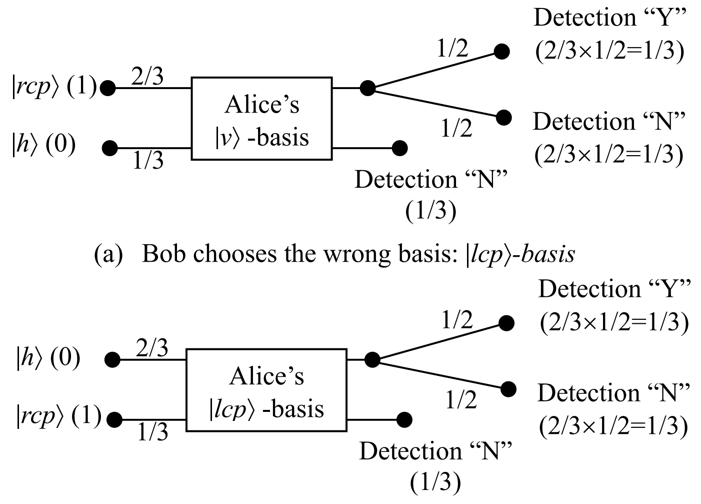
(4) Bob resends a random sequence of photons according B's bits in Step (2) ($\lvert rcp\rangle$*-photon* for "0" and $\lvert h\rangle$*-photon* for "1") in which his measurement results are "N" in Step (3).

(5) Alice chooses her detector basis according A's bit in Step (1) ($\lvert lcp\rangle$*-basis* for "0" and $\lvert v\rangle$*-basis* for "1") to measure each photon.

(6) Results of A's measurement. Then, the states are interpreted as a binary sequence. Alice and Bob will share the bits where the measurement results are "Y", discarding all other bits.

(7) Combine Step (3) and (6). Alice and Bob will get the final shared secret key.

Analysis of the efficiency for the second stage is shown in Figure 4. If Bob chooses the wrong $\lvert lcp\rangle$*-basis* (Figure 4(a)), he will correct the mistake and resend a $\lvert rcp\rangle$*-photon*. Alice always has the correct basis, because she sends the bit first. The efficiency of the second stage will be 1/3 larger than the first stage. Figure 4(b) shows the case that Bob chooses the wrong $\lvert v\rangle$*-basis*.



(a) Bob chooses the wrong basis: $|lcp\rangle$-*basis*

(b) Bob chooses the wrong basis: $|v\rangle$-*basis*

Figure 4. Analysis of idealized maximum efficiency for the SEQKD protocol.

3. Compared Result and Security Analysis

Compared Result:

For a n-bit sequence in the FEQKD protocol, the idealized maximum shared bits between Alice and Bob are n×1/4 in the first stage. Bob resends $3n/4$ bits in the second stage and Alice may get maximum correct $3n/4$ ×2/3 bits (see Figure 3). Finally the efficiency of our FEQKD protocol will be $\frac{n\times 1/4 + 3n/4 \times 2/3}{n + 3n/4} = \frac{3}{7}$=42.9%.

The efficiency 42.9% of FEQKD is larger than 25% of B92 and less than 50% of BB84, and the compromise of efficiency for our FEQKD is that the average number of quantum states in total sent photons. For polarization-based quantum cryptography schemes, the polarization states need to be maintained stable and against the noise of photon over a long optical fiber. Due to the alignment of polarization and the need of apparatus, it is reasonable to use average number of polarization states in a QKD protocol as the complexity order. Thus, the average complexity order of FEQKD is calculated as follows. There are n photons with two polarization states in 1st stage (B92), and $3n/4$ photons with four polarization states in 2nd stage (BB84). The average complexity order is $\frac{2\times n + 4\times 3n/4}{n + 3n/4} = \frac{20}{7}$=2.86.

Same as the above, for the SEQKD protocol, the idealized maximum shared bits between Alice and Bob are n×1/4 in the first stage. Bob resends $3n/4$ bits in the second stage and Alice will get correct $3n/4$ ×1/3 bits (see Figure 4). The efficiency factor of our SEQKD protocol will be $\frac{n\times 1/4 + 3n/4 \times 1/3}{n + 3n/4} = \frac{2}{7}$=28.6%. Because the two stages in SEQKD protocol are all B92, the average complexity order is $\dfrac{2\times n+2\times {}^{3n}\!/_{4}}{n+{}^{3n}\!/_{4}}=2$.

Table 5 gives the compared results for four QKD protocols, BB84, B92, the proposed FEQKD and SEQKD.

Table 5. Compared result for four QKD protocols

	B92	SEQKD	FEQKD	BB84
Complexity order	2	2	2.86	4
Efficiency	25%	28.6%	42.9%	50%

In our proposed FEQKD and SEQKD protocols, we use B92 and BB84 in the second stage to enhance B92. If we use BB84 in the first stage, can we use B92 and BB84 in the second stage to improve BB84? Suppose that we use BB84 first, but now Bob report his detector bases over quantum channel using B92 or BB84 instead of using public channel, the idealized maximum efficiency and average complexity order are given below.

Table 6 shows that Bob uses B92 to report his detector bases in BB84 protocol, and then Alice will have 25% probability to receive the correct bases. Alice tells Bob where his measurement results are "Y", and whether Bob's detector bases were correct or not. Note that Step (6) in Table 6 notation "Y/Y" (resp. "Y/N") means Alice get the correct measurement and Bob chooses the correct (resp. wrong) detector basis. Alice and Bob will share two bits for "Y/Y" case. The first bit is B's bit (Step (4)) and the second bit is B's bit (Step (3)). They will share only one bit (B's bit in Step (4)) for "Y/N" case. It is obvious that there ate 1/2 portion of "Y/Y" and 1/2 portion of "Y/N" in positions "Y". In other positions where Alice's measurement results are "N", Bob will reports his detector bases over public channel like BB84 and then Alice will give her response. So the final shared secret key is to combine Step (6) and Step (9). For this example Alice and Bob totally send 24 photons and the final shared secret key is 8-bit sequence "11000101". The efficiency is 8/24=33.3%.

Table 6. A 12-bit sample of Alice (A) and Bob (B) using B92 to report detector bases in BB84

	Sequence of bits		1	2	3	4	5	6	7	8	9	10	11	12
1^{st} Stage (A→B)	(1)	A's bit	1	1	0	0	1	0	1	0	0	0	1	1
		A's source basis	*D*	*R*	*R*	*R*	*D*	*D*	*R*	*D*	*R*	*D*	*R*	*D*
		A's polarization	$\|rcp\rangle$	$\|v\rangle$	$\|h\rangle$	$\|h\rangle$	$\|rcp\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|lcp\rangle$	$\|h\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|rcp\rangle$
	(2)	B's detector basis	*D*	*D*	*R*	*R*	*R*	*R*	*R*	*D*	*D*	*R*	*D*	*D*
	(3)	B's measurement	$\|rcp\rangle$	$\|lcp\rangle$	$\|h\rangle$	$\|h\rangle$	$\|h\rangle$	$\|v\rangle$	$\|v\rangle$	$\|lcp\rangle$	$\|lcp\rangle$	$\|h\rangle$	$\|rcp\rangle$	$\|rcp\rangle$
		B's bit	1	0	0	0	0	1	1	0	0	0	1	1
2^{nd} Stage	(4)	B's bit (B reports basis using B92)	1	1	0	0	0	0	0	1	1	0	1	1
		B's polarization	$\|rcp\rangle$	$\|rcp\rangle$	$\|h\rangle$	$\|h\rangle$	$\|h\rangle$	$\|h\rangle$	$\|h\rangle$	$\|rcp\rangle$	$\|rcp\rangle$	$\|h\rangle$	$\|rcp\rangle$	$\|rcp\rangle$
	(5)	A's detector basis	$\|v\rangle$	$\|v\rangle$	$\|lcp\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|v\rangle$	$\|v\rangle$	$\|lcp\rangle$	$\|lcp\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|v\rangle$
		A's bit	1	1	0	0	1	1	1	0	0	0	1	1

	(6)	A's measurement / response	N	Y/N	N	Y/Y		N	N	N	N	N	Y/N	N	N
		Shared secret key in B92	–	1	–	0		–	–	–	–	–	0	–	–
			–	1	–	0	0	–	–	–	–	–	0	–	–
	(7)	B reports basis	*D*	–	*R*	–		*R*	*R*	*R*	*D*	*D*	–	*D*	*D*
	(8)	A's response	Y	–	Y	–		N	N	Y	Y	N	–	N	Y
	(9)	Shared secret key In BB84	1	–	0	–		–	–	1	0	–	–	–	1
	(10)	The final shared secret key	1	1	0	0	0	–	–	1	0	–	–	–	1

(1)~(3) Same as BB84.

(4) Bob resends a random sequence of |*rcp*⟩-*photon* ("0") or |*h*⟩-*photon* ("1") over quantum channel according B's detector bases in Step (2) (*R-basis* for "0" and *D-basis* for "1") in all *n* bits.

(5) Alice randomly chooses her detector basis from |*lcp*⟩-*basis* or |*v*⟩-*basis* to measure each photon, and the bases are interpreted as a binary sequence.

(6) Results of Alice's measurement. Alice will check whether Bob's detector bases were correct or not. Alice and Bob will share one or two bits where the measurement results are "Y/N" or "Y/Y", discarding all other bits.

(7) Bob reports his detector bases over public channel where Alice's measurement results are "N" in Step (6).

(8) Alice tells Bob which bases were correct.

(9) Alice and Bob will share the bits where A's response is "Y", discarding all other bits.

(10) Combine Step (6) and (9). Alice and Bob will get the final shared secret key.

For the above case, the idealized maximum shared bits between Alice and Bob are $n\times1/4+n\times1/4\times1/2$ in B92 (Step (6)) for a *n*-bit sequence. They will get $3n/4\times1/2$ bits (Step (9)) in BB84 for other $3n/4$ bits. The total photons that Alice and Bob send are $2n$. Finally the efficiency will be $\frac{n\times {}^{1}\!/_{4}+n\times {}^{1}\!/_{4}\times {}^{1}\!/_{2}+{}^{3n}\!/_{4}\times {}^{1}\!/_{2}}{n+n}=\frac{3}{8}$ = 37.5%. The complexity order is $\frac{2\times n+4\times n}{n+n}$=3. When compared to SEQKD there is no advantage for this protocol, the efficiency 37.5% is less than 42.9% and the complexity order 3 is greater than 2.86.

If we use BB84 to report Bob's detector bases in Table, the QKD protocol is shown in Table 7. The detail steps are similar as Table 6, and omitted here.

Table 7. A 12-bit sample of Alice (A) and Bob (B) using BB84 to report detector bases in BB84

	Sequence of bits		1	2	3	4	5	6	7	8	9	10	11	12
1^{st} Stage (A→B)	(1)	A's bit	1	1	0	0	1	0	1	0	0	0	1	1
		A's source basis	*D*	*R*	*R*	*R*	*D*	*D*	*R*	*D*	*R*	*D*	*R*	*D*
		A's polarization	$\|rcp\rangle$	$\|v\rangle$	$\|h\rangle$	$\|h\rangle$	$\|rcp\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|lcp\rangle$	$\|h\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|rcp\rangle$
	(2)	B's detector basis	*D*	*D*	*R*	*R*	*R*	*R*	*R*	*R*	*D*	*D*	*D*	*D*
	(3)	B's measurement	$\|rcp\rangle$	$\|lcp\rangle$	$\|h\rangle$	$\|h\rangle$	$\|h\rangle$	$\|v\rangle$	$\|v\rangle$	$\|h\rangle$	$\|lcp\rangle$	$\|lcp\rangle$	$\|rcp\rangle$	$\|rcp\rangle$
		B's bit	1	0	0	0	0	1	1	0	0	0	1	1
2^{nd} Stage (B→A)	(4)	B's bit (B reports basis using BB84)	1	1	0	0	0	0	0	0	1	1	1	1
		B's source basis	*R*	*R*	*R*	*D*	*D*	*R*	*R*	*D*	*D*	*D*	*D*	*R*
		B's polarization	$\|v\rangle$	$\|v\rangle$	$\|h\rangle$	$\|lcp\rangle$	$\|lcp\rangle$	$\|h\rangle$	$\|h\rangle$	$\|lcp\rangle$	$\|rcp\rangle$	$\|rcp\rangle$	$\|rcp\rangle$	$\|v\rangle$
	(5)	A's detector basis	*D*	*R*	*R*	*R*	*R*	*D*	*R*	*D*	*D*	*R*	*R*	*R*
	(6)	A's measurement	$\|lcp\rangle$	$\|v\rangle$	$\|h\rangle$	$\|v\rangle$	$\|h\rangle$	$\|rcp\rangle$	$\|h\rangle$	$\|lcp\rangle$	$\|rcp\rangle$	$\|v\rangle$	$\|h\rangle$	$\|v\rangle$
		A's bit	0	1	0	1	0	1	0	0	1	1	0	1
	(7)	A reports basis	*D*	*R*	*R*	*R*	*R*	*D*	*R*	*D*	*D*	*R*	*R*	*R*
	(8)	B's response	N	Y	Y	N	N	N	Y	Y	Y	N	N	Y
	(9)	A's response	–	N	Y	–	–	–	Y	N	N	–	–	Y
	(10)	Shared secret key in 2^{st} BB84	–	1	0 0	–	–	–	0 1	0	1	–	–	1 1
	(11)	B reports basis	*D*	–	–	*R*	*R*	*R*	–	–	–	*D*	*D*	–
	(12)	A's response	Y	–	–	Y	N	N	–	–	–	Y	N	–
	(13)	Shared secret key in 1^{nd} BB84	1	–	–	0	–	–	–	–	–	0	–	–
	(14)	The final shared secret key	1	1	0 0	0	–	–	0 1	0	1	0	–	1 1

Same as the above analysis, we will get the idealized maximum efficiency $\frac{n\times {}^{1}\!/_{2}+n\times {}^{1}\!/_{2}\times {}^{1}\!/_{2}+{}^{n}\!/_{2}\times {}^{1}\!/_{2}}{n+n}=\frac{1}{2}=$ 50%. The complexity order is $\frac{4\times n+4\times n}{n+n}=$ 4. We find that there is no improvement for BB84.

From the above description, if the first stage is BB84, we cannot use BB84 or B92 to improve BB84 protocol like that we improve B92 in FEKQD and SEKQD protocols. In fact, the following theorem shows that use BB84 in the first stage and B92 or BB84 in the second stage will have no advantages. It is same as using BB84 and B92 simultaneously in single stage.

Theorem: The OKD protocol using BB84 in the first stage and B92 or BB84 in the second stage will have the same idealized maximum efficiency and average complexity order when compared to the protocol using BB84 and B92 simultaneously in single stage.

Proof: When use BB84 or B92 to report Bob' detector bases for BB84 protocol, in general, we can use B92 to send *n*' photons and BB84 to send (*n*-*n*') photons, where 0 ≤ *n*' ≤ *n*.

The idealized maximum efficiency will be as follows:

$$\frac{\left[n'\times {}^{1}\!/\!_{4} + n'\times {}^{1}\!/\!_{4} \times {}^{1}\!/\!_{2} + {}^{3n'}\!/\!_{4} \times {}^{1}\!/\!_{2}\right] + \left[(n-n')\times {}^{1}\!/\!_{2} + (n-n')\times {}^{1}\!/\!_{2} \times {}^{1}\!/\!_{2} + {}^{(n-n')'}\!/\!_{2} \times {}^{1}\!/\!_{2}\right]}{n + n' + (n-n')}$$

$$= \frac{{}^{6n'}\!/\!_{8} + (n-n')}{2n} = \frac{n - {}^{n'}\!/\!_{4}}{2n} = \frac{1}{2} - \frac{1}{8}\,(\frac{n'}{n})\,. \qquad (1)$$

The average complexity order will be as follows:

$$\frac{n\times 4 + n'\times 2 + (n-n')\times 4}{n + n' + (n-n')}$$

$$= \frac{8n - 2n'}{2n} = 4 - (\frac{n'}{n})\,. \qquad (2)$$

Use BB84 and B92 simultaneously in single stage. In general, we can use B92 to send *n*” photons and BB84 to send (*n*-*n*”) photons, where 0 ≤ *n*” ≤ *n*.

The idealized maximum efficiency will be as follows:

$$\frac{n''\times {}^{1}\!/\!_{4} + (n-n'')\times {}^{1}\!/\!_{2}}{n'' + (n-n'')}$$

$$= \frac{{}^{n}\!/\!_{2} - {}^{n''}\!/\!_{4}}{n} = \frac{1}{2} - \frac{1}{4}\,(\frac{n''}{n})\,. \qquad (3)$$

The average complexity order will be as follows:

$$\frac{n''\times 2 + (n-n'')\times 4}{n'' + (n-n'')}$$

$$= \frac{4n - 2n''}{n} = 4 - 2(\frac{n''}{n})\,. \qquad (4)$$

We can easily check that if the complexity orders in Eq. (2) and (4) are same then the idealized maximum efficiencies in Eq. (1) and (3) are same too.

If $4 - (\frac{n'}{n}) = 4 - 2(\frac{n''}{n})$, then *n*’ = 2 *n*”.

Substitute *n*’ = 2 *n*” into Eq. (1).

$\frac{1}{2} - \frac{1}{8}\,(\frac{n'}{n}) = \frac{1}{2} - \frac{1}{8}\,(\frac{2n''}{n}) = \frac{1}{2} - \frac{1}{4}\,(\frac{n''}{n})$ is same as Eq. (3).

The proof is completed.

□

Security analysis:

In conventional communication channel, Eve may intercept the channel and reveal Alice’s signal correctly. Thus, she can resend the same copy of signal to Bob. It is, however, impossible to intercept/resend in quantum channel. Thus, if Eve intercepts the quantum channel, Alice and Bob will find a large part of errors in their shared keys.

In 1st stage, the security is same as B92. In 2nd stage, Eve does not know which source bases Bob chooses in the positions where his measurement results are "N" in 1st stage, because Bob may detect nothing when choosing the wrong or even correct bases. Same as BB84 and B92, Alice and Bob can choose some bits in shared secret key of 2nd stage for verification to easily find Eve's eavesdropping activities. We can also add error detecting and correcting codes into our enhanced QKD protocols.

4. Conclusion

We successfully use BB84 and B92 as the second stage to construct our two-stage FEQKD and SEQKD protocols to improve B92. Our FEQKD protocol has the idealized maximum efficiency 42.9% and the average complexity order 2.86. In other words, FEQKD has better efficiency and a little complexity than B92, but when compared to BB84, FEQKD has simpler complexity and a little less efficiency. We find a new QKD protocol to compromise efficiency and complexity. For the SEQKD protocol, we only use B92 protocol and successfully enhance the efficiency for B92 by adding the extra steps.

Our FEQKD and SEQKD protocols use the information when Bob chooses the wrong detector's basis; however the information is discarded in the original B92 protocol.

References

[1] C.H. Bennet and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", *Proceedings of IEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp.175-179, Dec. 1984.

[2] C.H. Bennet, "Quantum cryptography using any two non-orthogonal states", *Physical Review Letters*, Vol. 68, pp.3121-3124, May 1992.

[3] C.H. Bennet, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography", *Journal of cryptology*, Vol. 5, pp. 3-28, 1992.

[4] J.G. Rarity, P.M. Gorman and P.R. Tapster, "Secure key exchange over 1.9 km free-space range using quantum cryptography", *Electronic Letters*, Vol. 37, No. 8, pp. 512-514, April 2001.

[5] P.D. Townsend, "Secure key distribution system based on quantum cryptography", *Electronic Letters*, Vol. 30, No. 10, pp. 809-811, May 1994.

[6] S.J.D. Phoenix and P.D. Townsend, "Quantum cryptography: protecting our future networks with quantum mechanics", *Cryptography and Coding: 5th IMA Conference*, pp. 112-131. Dec. 1995.

[7] P.D. Townsend, S.J.D. Phoenix, K.J. Blow and S.M. Barnett, "Design of quantum

cryptography systems for passive optical network", *Electronic Letters*, Vol. 30, No. 22, pp. 1875-1877, Oct. 1994.

[8] S.J.D. Phoenix, S.M. Barnett, P.D. Townsend and K.J. Blow, "Multi-user quantum cryptography on optical networks", *Journal of Modern Optics*, Vol. 42, No. 6, pp. 1155-1163, 1995.