QKD PROTOCOL BASED ON PHOTON POLARIZATIONWITH 6-BIT PER PHOTON

M. Mohamed [1], T. A. Moniem [2, *]

[1] *Electronics and communication Dept. faculty of Eng. MSA University*
[2] *Faculty of engineering, Communication and Electronics Dept. IAEMS*, Cairo-Egypt

Received 14 October 2012, accepted 3 March 2013

ABSTRACT

The paper introduces a quantum key distribution (QKD) scheme which generates 6-bits per each transmitted photon. The efficiency of our protocol is 100% like quantum dense key distribution but with 6 bits per photon instead of 4-bits per photon. The proposed protocol improves the efficiency of BB84 and the biased BB84 which use 1-bit per photon.

Keywords: Quantum Cryptography, Quantum Key Distribution, Quantum Dense Key distribution.

1. Introduction

QKD is one of the most developed applications of quantum information theory. It is based on the properties of quantum states and allows two parties separated by a distance to generate a shared secret key based on the laws of quantum mechanics.

QKD using entangled photons has been demonstrated in a range of experiments in the literature. Polarization entangled pairs of photons were used as an approximation of a conditional single photon source in the single qubit BB84 protocol [1]. They were also applied to protocols like the Ekert protocol [2] where both photons are used for the key transmission [1] or the "six state protocol" [3]. Another class of experiments uses phase encoding [4], energy-time entanglement [5] or the SARG protocol [6] based on time bin qubits instead of polarization entanglement. QKD via fibers was recently demonstrated beyond 100 km distance with qubit-error rates (QBER) of 8.9 % [7] and 5 % [8] respectively. An overview of methods and techniques in QKD can be found in [9] and [10].

Many OKD schemes were proposed based on quantum mechanics, which provide the unconditional security rather than computational hard problems used in classical cryptography. Some of the QKD schemes used a single polarized photon such as BB84 and the biased BB84 are based on the entanglement systems [11]. The advantage of using single polarized photon is the ease of implementation, but its efficiency is limited. The term efficiency is measured as Bs/(Ba + Ps) [12] where Bs is the number of shared bits, Ba the number of announced bits and Ps is the number of sent photons. The entangled pair systems provide a 100% efficiency but with more complexities and difficulties of implementations. In this paper, we use the idea introduced in [12] which implemented the polarized photon with increasing the efficiency to 100%. It generated 4 bits per photon. Here we generate 6-bits per photon and maintain the same efficiency at 100%.

The proposed protocol (like [12]) improves the efficiency of BB84 [13] (25%) and the biased BB84 (50%). The first quantum dense key distribution (QDKD) protocol introduced in [11] utilized 2-bit per photon but with two entangled photons. Our protocol is based on a

* Corresponding author.
E-mail address: tamerkhawaga@yahoo.com

single polarized photon, polarization is simpler and easier to implement (using Faraday rotators) rather than entanglement which is more complex and difficult for implementation. The efficiency of entanglement systems can be enhanced to 100% but the hardware is complex to implement [12]. The polarized photon systems provide a limited efficiency.

2. Efficient QKD schemes

2.1. BB84

Two users Alice and Bob randomly choose from Rectilinear (R) and Diagonal (D) basis [10]. After transmission over quantum channel, Alice and Bob share their bases through the public channel and discard the wrong bases they used [2]. The single photon may be polarized with four states:

$|h\rangle, |v\rangle, |r_{cp}\rangle and |l_{cp}\rangle.$

- Polarization state $|h\rangle (or |v\rangle)$ in R-basis reveals “0” (or “1”).
- Polarization state $|r_{cp}\rangle (or |l_{cp}\rangle)$ in D-basis reveals “0” (or “1”).

The BB84’s Efficiency is defined in [12] as

$$\eta = \frac{Bs}{Ba + Ps} \tag{1}$$

where:

Bs = number of shared bits.
Ba = number of announced bits.
Ps = number of sent photons

For BB84 protocol, efficiency is equal to:

$$\eta = \frac{0.5}{1+1} = 25\%$$

2.2. Biased BB84 protocol

Bases are chosen with a biased probability as follow:
R-basis is chosen with probability p.
D-basis is chosen with probability 1-p, where $0 \le p \le \frac{1}{2}$.

Biased BB84_Efficiecny [14] is:

$$\eta = \frac{(1-p)^2 + p^2}{1+1} \tag{2}$$

$\eta = 50\%$, when p approaches 0 and
$\eta = 25\%$, when p= 0.5 like the ordinary BB84.

2.3. Quantum Dense Coding (QDC)

Bennett and Wiesner [15] proposed a quantum dense coding protocol which can bring two information bits per photon using entangled Bell-states as follow:

$$\left|\psi_{12}{}^{+}\right\rangle = \frac{1}{\sqrt{2}}[\left|0\right\rangle_1\left|1\right\rangle_2 + \left|1\right\rangle_1\left|0\right\rangle_2] \quad (3)$$

$$\left|\psi_{12}{}^{-}\right\rangle = \frac{1}{\sqrt{2}}[\left|0\right\rangle_1\left|1\right\rangle_2 - \left|1\right\rangle_1\left|0\right\rangle_2] \quad (4)$$

$$\left|\phi_{12}{}^{+}\right\rangle = \frac{1}{\sqrt{2}}[\left|0\right\rangle_1\left|0\right\rangle_2 + \left|1\right\rangle_1\left|1\right\rangle_2] \quad (5)$$

$$\left|\phi_{12}{}^{-}\right\rangle = \frac{1}{\sqrt{2}}[\left|0\right\rangle_1\left|0\right\rangle_2 - \left|1\right\rangle_1\left|1\right\rangle_2] \quad (6)$$

Operation can be stated as follow:

1- Alice and Bob obtain one particle from the entangled pair in the initial state $\left|\psi_{12}{}^{+}\right\rangle$.

2- Bob performs one of four operations on his particle:

$$\left|\psi_{12}{}^{+}\right\rangle \to \left|\psi_{12}{}^{+}\right\rangle \to \textit{Identity operation} \quad (00)$$

$$\left|\psi_{12}{}^{+}\right\rangle \to \left|\phi_{12}{}^{+}\right\rangle \to \textit{Bit flip} \quad (01)$$

$$\left|\psi_{12}{}^{+}\right\rangle \to \left|\psi_{12}{}^{-}\right\rangle \to \textit{Phase flip} \quad (10)$$

$$\left|\psi_{12}{}^{+}\right\rangle \to \left|\phi_{12}{}^{-}\right\rangle \to \textit{Both bit and phase flip} \quad (11)$$

3- Alice encodes the last four operations as 00, 01, 10, and 11 respectively.

The QDC Efficiency is equal to $\eta = \frac{2}{0+2} = 100\%$, since no announced bits and there are two used entangled photons.

2.4. Quantum Dense Key Distribution using entangled photon pair (QDKD)

The protocol of QDC is adopted for QDKD protocol as follow [15]:
Only two states are used: $\left|\psi_{12}{}^{+}\right\rangle$ and $\left|\psi_{12}{}^{-}\right\rangle$ (identity and phase flip), and define two operations as following:

$$u_{o:}\left|\psi_{12}{}^{+}\right\rangle \to \left|\psi_{12}{}^{+}\right\rangle \text{ Identity (0)}$$

$u_{1:}\left|\psi_{12}{}^{+}\right\rangle \rightarrow \left|\psi_{12}{}^{-}\right\rangle$ Phase flip (1)

Alice makes one of the two transformations on the particle and announces measurement result 0 or 1 while Bob measures the particle according to the table (1). If Bob measures the state $\left|\psi_{12}{}^{+}\right\rangle$ and he makes u_o according to the above table he can predict that Alice makes u_o, then they share (00) (so do Alice) and so on. Alice and Bob can share two information bits from their mutual operations (u_o: "0", u_1: "1"). So, the efficiency of QDKD-Entangled Photons Protocol is equal to $\eta = \frac{2}{1+1} = 100\%$

Table 1.

Bob / Alice	u_o	$u_{\underline{1}}$
u_o	$\left\|\psi_{12}{}^{+}\right\rangle$	$\left\|\psi_{12}{}^{-}\right\rangle$
$u_{\underline{1}}$	$\left\|\psi_{12}{}^{-}\right\rangle$	$\left\|\psi_{12}{}^{-}\right\rangle$

3. QDKD protocol using single polarized photon

Bennett [12] combines the concept of QDKD-Entangled photons and the single polarized photon (Biased BB84) in order to achieve high efficiency with simple implementation. The four polarized operations on a single photon are defined as:

u_{oo}: Polarizes the photon with 0^0
u_{o1}: Polarizes the photon with 45^0
u_{10}: Polarizes the photon with 90^0
u_{11}: Polarizes the photon with 135^0

- Thus four photon polarization states are used and Polarization states $\left|h\right\rangle$ and $\left|v\right\rangle$ in the R-basis and Polarization states $\left|r_{cp}\right\rangle$ and $\left|l_{cp}\right\rangle$ in the D-basis
- Alice and Bob uses the operation u_{o1} and u_{10} with probability ($\frac{p}{2}$), while the operation u_{00} and u_{11} with probability of $\left(\frac{1-p}{2}\right)$, where $0 \le p \le \frac{1}{2}$.

The QDKD – polarized photon protocol can be described as the following steps:

1- Alice prepares the photon in the state $\left|v\right\rangle$ and $\left|h\right\rangle$ with equal probability (state $\left|\psi\right\rangle$).

2- Alice randomly polarizes the photon with one of the four operations: u_{oo}, u_{o1}, u_{1o} and u_{11} and sends the photon to Bob.

3- Bob (doesn't measure) polarizes the photon with one of the last mentioned four operations and sends the photon back to Alice $|\psi`\rangle$.

4- Alice (A) randomly uses R-basis and D-basis to measure the photon and announces the result as follow:

If $|\psi`\rangle - |\psi\rangle = 0^o \, or \, 180^o$ Alice announces 00

If $|\psi`\rangle - |\psi\rangle = 45^o \, or \, 225^o$ Alice announces 01

If $|\psi`\rangle - |\psi\rangle = 90^o \, or \, 270^o$ Alice announces 10

If $|\psi`\rangle - |\psi\rangle = 135^o \, or \, 315^o$ Alice announces 11

5- Bob (B) announces the basis bit "0" (for 0° or 90°) and "1" (for 45° or 135°).

6- Alice makes response "Y" for right base she chooses and "N" for wrong base.

7- According to table (2), Alice and Bob can share four information bits from their own operations and announcements:

Table 2.

Bob / Alice	u_{oo}	u_{o1}	u_{11}	u_{10}
u_{oo}	00	01	10	11
u_{o1}	01	10	11	00
u_{11}	10	11	00	01
u_{10}	11	00	01	10

3.1. QDKD protocol using single polarized photon example

Initially, Alice generates $|h\rangle$ polarized photon ($|\psi\rangle$=0°), and makes u_{o1} (polarization with 45°) (the state in $|r_{cp}\rangle$) then, send it to Bob. Bob makes u_{11} on the photon ($|\psi`\rangle = 135^o$) and sends it back to Alice. Alice measures the photon say in the D-basis and calculates $|\psi`\rangle - |\psi\rangle$ $|\psi`\rangle$-$|\psi\rangle$= 135°-0° = 135° then, announces "11". Bob announces the basis bit "0" because he was making u_{11} (90°). Alice knows from Bob announcement that he had made 0° or 90° while the photon was sent at 45° or 135° i.e. in the D-basis thus, Alice was making the right measurement, then respond with "Y". Alice now records "01" (from his operation u_{01}) and according to the above table, Alice can know that Bob makes u_{11} then record "11", finally, Alice now share four information bits "0111". For Bob, he knows his own operation u_{11} and Alice announcement "11", return to the above table, he found that Alice makes u_{01} then record the four shared bits "0111".

If Alice chooses the R-bases and announce "11", Bob will announce a basis bit "0" because he made 90°, when Alice reads this bit, Alice knows that Bob made 0° or 90° while Alice send the photon at 45° this means that the photon was at 45° or 135° and the correct base was D-basis, then respond with "N" to discard this bit.

Finally, Alice and Bob can share four information bits per photon [12]. The efficiency of The QDKD-Polarized Protocol [12] is given as:

$$\eta = \frac{4\times((1-p)^3 + 3p^2(1-p))}{3+1} \tag{7}$$

and there are two cases according to the value of p.

Case 1:

$\eta = 100\%$, when p approaches to 0, and

Case 2:

$\eta = 50\%$, when p=0.5

4. The proposed 6-bit per photon QKD protocol

Alice and Bob use one of eight operations as following steps:
u_{000}: Polarizes the photon with 0^o or 180^o
u_{001}: Polarizes the photon with 22.5^o or 202.5^o
u_{011}: Polarizes the photon with 45^o or 225^o
u_{010}: Polarizes the photon with 67.5^o or 247.5^o
u_{100}: Polarizes the photon with 90^o or 270^o
u_{101}: Polarizes the photon with 112.5^o or 292.5^o
u_{111}: Polarizes the photon with 135^o or 315^o
u_{110}: Polarizes the photon with 157.5^o or 337.5^o
Alice and Bob used four Bases: B_0, B_1, B_2, and B_3 with equal probabilities (25%), where these four bases are the entangled Bell states of four unitary operations on qubit [12].
The steps are as the following:

1- Alice generated at random vertically and horizontally polarized photons with equal probability 120 π $|h\rangle$ ($|4\,\phi\rangle$.
2- Alice performs one of the eights polarization angles u_{000} to → u_{111}.
3- Alice sends the photon to Bob.
4- Bob (doesn't measure) performs one of the eights operations u_{000} to → u_{111} ($|\psi\rangle$.
5- Bob sends the photon back to Alice.
6- Alice measure in 4-basis B_0 , B_1 , B_2 , or B_3 with equal probability (25% for each), and record the phase difference $|\psi`\rangle - |\psi\rangle$ as following:

$$|\psi`\rangle - |\psi\rangle = 0^o \; or\, 180^o \;\; announce \rightarrow 000$$

$$|\psi`\rangle - |\psi\rangle = 22{,}5^o \; or\, 202.5^o \;\; announce \rightarrow 001 \quad = 45^o \; or\, 225^o \;\; announce \rightarrow 010$$

$$= 67.5^o \; or\, 247.5^o \;\; announce \rightarrow 011$$

$$= 90^o \; or\, 270^o \;\; announce \rightarrow 100$$

$$=112.5^o \; or\, 292.5^o \;\; announce \rightarrow 101 = 135^o \; or\, 315^o \;\; announce \rightarrow 110$$

$$=157.5^o \; or\, 337.5^o \;\; announce \rightarrow 111$$

7- B announces (00) gf he did 0^o / 90^o
(01) gf he did 22.5^o / 12.5^o
(10) gf he did 45^o / 135^o
(11) gf he did 67.5^o / 157.5^o

8- Alice compares his measures and B announcement and makes response with "1" → correct Base. "N" → Wrong base. Finally, Alice and Bob can share 6-bits per photon according to table (3)

Comparison among the proposed protocol and other previous protocols are summarized in table (4).

The proposed protocol allows the generation of secure cryptographic keys using only one travelling-qubit for two bit of classical information [16]. The QKD system is capable of continuous and autonomous operation, and generating secret keys in real time [17].

5. Examples for 6-bit per photon QKD protocol

5.1. Example 1

1- Alice generates $\left|h\right\rangle \rightarrow \therefore \left|\psi\right\rangle = 0$
2- A's operation → u_{000} → 0
3- After operation → in B_0 base
4- B's operation → u_{101} (112.5^o)
5- After operation → lies in (B_1)
6- A choose say (B_1) with 25%, and others with 75.
7- A measures $\left|\psi`\right\rangle - \left|\psi\right\rangle = \left|12.5^o\right\rangle$, so that A announces (101)
8- B announce (01) (112.5^o ⇒ 01
9- A's response = "y"
10- Shared bits u_{000}, u_{101}.
Sharing [000 101]

5.2. Example 2

1- A generates $\left|h\right\rangle \rightarrow \left|\psi\right\rangle = o$
2- A's operation → u_{010} → 67.5^o
3- After operation → ψ at B_3 base
4- B's operation → u_{110} → (157.5^o)
5- After operation → $\left|\psi`\right\rangle$ → 225^o Lies at B_1 base.
6- A choose at random say B_3 with 25%.

7- A measure $|\psi`\rangle - |\psi\rangle = 225^{o}$, so that the $announce\, 010$

8- B's basis announce (11) (he did 157.5°)

9- A's response = "N"

10- Discard $\eta = \dfrac{Bs}{Ba + Ps} = \dfrac{6}{5+1} = 100$

Table 3.

Alice /Bob	u_{000}	u_{001}	u_{011}	u_{010}	u_{100}	u_{101}	u_{111}	u_{110}
u_{000}	000	001	010	011	100	101	110	111
u_{001}	001	010	011	100	101	110	111	000
u_{011}	010	011	100	101	110	111	000	001
u_{010}	011	100	101	110	111	000	001	010
u_{100}	100	101	110	111	000	001	010	011
u_{101}	101	110	111	000	001	010	011	100
u_{111}	110	111	000	001	010	011	100	101
u_{110}	111	000	001	010	011	100	101	110

Table 4.

QKD protocol / Measure	BB84	Biased BB84	QDKD (Entangled)	QDKD (Polarized)	Proposed QDKD
Efficiency η	25%	50%	100%	100% (P=0) 50% (p=$\frac{1}{2}$)	100%
No. of bits per photon	1	1	2	4	6
Complexity	Simple	Simple	Complex	Simple	Simple

6. Conclusions

The paper proposes a protocol that embeds the main advantages of two quantum communication applications, namely QKD and QDC. The quantum dense key distribution is presented with 6-bits per photon instead of 4-bits per photon with efficiency 100 %. The proposed system was proven and illustrated with two examples and can be used for continuous and autonomous operation.

7. References

[1] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, A. Zeilinger., *Quantum Cryptography with Entangled Photons*, Phys. Rev. Lett. 84, 4729-4732 (2000)

[2] A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. 67, 661-663 (1991)

[3] D. G. Enzer, P. G. Hadley, R. J. Hughes, C. G. Peterson, P. G. Kwiat, *Entangled-photon six-state quantum cryptography*, New Journal of Physics 4, 45.1-45.8 (2002)

[4] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, H. Zbinden, *Quantum key distribution over 67 km with a plug & play system*, New Journal of Physics 4 41.1-41.8 (2002)

[5] S. Fasel, N. Gisin, G. Ribordy, H. Zbinden, *Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods*, Eur. Phys. J. D 30 143-148 (2004).

[6] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementation*s, Phys. Rev. Lett. 92, 057901 (2004)

[7] C. Gobby, Z. L. Yuan, and A. J. Shields , *Quantum key distribution over 122 km of standard telecom fiber*, Applied Physics Letters 84, 3762 (2004)

[8] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, *Long-distance quantum key distribution in optical fiber*, New Journal of Physics 8, 193 (2006)

[9] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Quantum Cryptography*, Rev. Mod. Phys. Pp. 74 145 (2002)

[10]M. Dusek, N.Lutkenhaus, M. Hendrych, *Quantum Cryptography*, Progress in Optics 49,pp. 381-454 (2006)

[11] C.N. Yang, C.C. Kuo, *Enhanced Quantum Key Distribution Protocols Using BB84 and B92,* International Computer Symposium, vol. 2, pp.951-959, (2002).

[12] C. H. Bennett , G. Brassard, *Quantum Cryptography: Public Key Distribution and coin Tossing*, IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp 175-179. (1984)

[13] C.H. Bennett, G. Brassard, N.D. Mermin., *Quantum cryptography without bell' s theorem*, Phys. Rev. Lett., 68:557, (1992).

[14] H. K. Lo, H. F. Chau, *A Simple Proof of the Unconditional Security of Quantum Key Distribution*, quant-physics Vol. 34, 6957 (2001)

[15] C.H. Bennet, Wiesner, *Communication via one-and two-particle operators on Einstein-Podolsky, Rosen states,* physics letter**,** Vol 69, pp. 2881-2884,(1992).

[16] A. Poppe, A. Fedrizzi, R. Ursin, H. R., *Practical quantum key distribution with polarization entangled photons,* Optic Express Vol. 12, No. 16,pp. 3865-3871, (2004)

[17] D. Stucki, C. Barreiro, S. Fasel, J. D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, H. Zbinden, *Continuous high speed coherent one-way quantum key distribution*, Optic Express, Vol 17, No 16, pp. 13326-13334, (2009)

بروتوكول لمفتاح مستوى طاقه موزع باستخدام استقطاب فوتوني ب 6 بت لكل فوتون

الملخص:

هذه الورقه البحثيه تقدم بروتوكولا لمفتاح مستوى طاقه الكتروني باستخدام 6 بت لكل فوتون مرسل حيث تصل كفاءه النظام المستخدم الى 100% مثل مفتاح مستوى الطاقه الالكتروني المكثف ولكن مع استخدام 6 بت بدلا من 4 بت لكل فوتون ضوئي. البروتوكول المقدم يحسن كفاءه النظامين BB84 و المرافق له ايضا الذي يستخدم 1 بت لكل فوتون ضوئي.