2015 The 5th International Workshop on Computer Science and Engineering
doi: 10.18178/wcse.2015.04.085

Analysis on the Effect of Polarization Drift on the Efficiency of Generating Keys in a Quantum Communication System Based on the B92 Protocol

Zhiyong Zhang[1], Yanbo Wang[1], Min He[1], Yong Zhu[1], Zhiyong Xu[1], Jian Wang[1], Liucun Cao[2]

[1]Institute of Communication Engineering, PLA University of Science and Technology, Nanjing, 210007, china

[2] Zibo City Public Security Bureau, Shandong Province, Zibo, 255000, China

Keywords: B92 protocol; quantum communication; polarization drift; quantum key distribution.

Abstract. Focusing on the polarization drift in a practical quantum communication system, analyze the effect on the efficiency of producing key and mutual information in a quantum communication system based on B92 protocol. Results show that when the polarization drift angle is 0°, the probability receiver can obtain measurement respond comes to minimum value: 0.25, while the mutual information between the sender and the receiver gets the maximum value: 1; When the angle is 90°, the probability reaches the maximum value: 0.75, while the mutual information gets the minimum value: 0.0817; The probability receiver correctly measures the state actually is constantly 0.25. Comparing to BB84, the variation of mutual information in B92 is violent from 0.0817 to 1.

Quantum cryptography communication which is one way realizing one-time -pad unconditional security, relies on the random shared keys. The B92 protocol[1] is one of the classical protocols generating keys randomly. Currently, quantum cryptography communication systems[2][3][4][9] based on B92 protocol are many, and coding ways are different. Papers[5][6][7][8] are based on the polarization code, and papers[4][9] are about phase code. We will analyze how the polarization drift affects the error deviation and the efficiency of generating keys in a QKD system with polarization code based on the B92 protocol.

Introduction

B92 protocol uses two non-orthogonal quantum states $|\psi\rangle$ and $|\varphi\rangle$ in Hilbert space with 45 °angle, and satisfies:

$$\langle\psi|\varphi\rangle=\frac{1}{\sqrt{2}},\ \langle\psi|\psi\rangle=\langle\varphi|\varphi\rangle=1, \tag{1}$$

Build two non-commutative projection operators using states $|\psi\rangle$ and $|\varphi\rangle$,

$$M_{\psi}=1-|\varphi\rangle\langle\varphi|,\quad M_{\varphi}=1-|\psi\rangle\langle\psi|. \tag{2}$$

States $|\psi\rangle$ and $|\varphi\rangle$ are projected to orthogonal subspace by M_{ψ} and M_{φ}, then:

$$\langle\psi|M_{\psi}|\psi\rangle=\frac{1}{2},\langle\varphi|M_{\psi}|\varphi\rangle=0,\langle\psi|M_{\varphi}|\psi\rangle=0,\langle\varphi|M_{\varphi}|\varphi\rangle=\frac{1}{2}. \tag{3}$$

Formulas above show that, from one side, operator M_{ψ} acting on state $|\varphi\rangle$ will eliminate it, while obtain a definitive measurement with probability 0.5 if the operator acts on $|\psi\rangle$, from another side, operator M_{φ} acting on state $|\psi\rangle$will eliminate it, while obtain a definitive measurement probability 0.5 if the operator acts on $|\varphi\rangle$.

Assumes legitimate communication partners: sender named Alice and receiver named Bob. Alice sends a quantum state randomly from $|\psi\rangle$ and $|\varphi\rangle$, while Bob measures receiving states with projection operators M_{ψ} or M_{φ} randomly in the transmission process.

Analysis on the Efficiency of Generating Key

Supposes two states used in the B92 protocol are: $|\psi\rangle=|x\rangle$, $|\varphi\rangle=|u\rangle$($|x\rangle$ is on behalf of 0 and $|u\rangle$ expresses 1). States $|y\rangle$ and $|v\rangle$ are the orthogonal states respectively, then: $M_\psi = M_x = |v\rangle\langle v|$, $M_\varphi = M_u = |y\rangle\langle y|$. Alice sends signal $|l\rangle$(angle to *x* axis is *l*), and it has shifted angle θ before Bob measures the signal, as shown in fig. 1.

Sign the signal Bob measures as $|l_\theta\rangle$ or $|l+\theta\rangle$, then:

$$|l_\theta\rangle = \cos(l+\theta)|x\rangle + \sin(l+\theta)|y\rangle, \tag{4}$$

$$\text{Or } |l_\theta\rangle = -\sin(l+\theta-\pi/4)|v\rangle + \cos(l+\theta-\pi/4)|u\rangle. \tag{5}$$

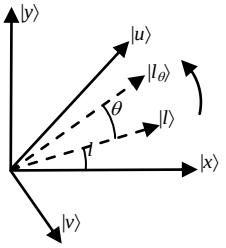

Fig.1: Picture for polarization shift

When *l*=0 °, 45 °, states from signal source are $|x\rangle$ and $|u\rangle$, while the states Bob measures are $|x_\theta\rangle$, $|u_\theta\rangle$.

$$|x_\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle \text{ or } |x_\theta\rangle = -\sin(\theta-\pi/4)|v\rangle + \cos(\theta-\pi/4)|u\rangle, \tag{6}$$

$$|u_\theta\rangle = -\sin(\theta-\pi/4)|x\rangle + \cos(\theta-\pi/4)|y\rangle \text{ or } |u_\theta\rangle = -\sin\theta|v\rangle + \cos\theta|u\rangle. \tag{7}$$

Alice sends quantum states $|x\rangle$ and $|u\rangle$ to Bob through quantum channel. P_M^{AB} is the probability Bob chooses a projection operator, $M\in\{M_x,\ M_u\}$. $P_{|s\rangle}^{AB}$ expresses the probability Alice sends state $|s\rangle$, $s\in\{x,\ u\}$. Coding method is C: $|x\rangle\to 0$; $|u\rangle\to 1$. The probability Bob detects state $|x\rangle$ or $|u\rangle$ is $P_{|s\rangle M|s\rangle}^{AB} = \langle s_\theta|M|s_\theta\rangle$, $P_{|s\rangle M|\bar{s}\rangle}^{AB} = \langle s_\theta|\bar{M}|s_\theta\rangle = 1 - P_{|s\rangle M|\bar{s}\rangle}^{AB}$, $s=x$, u , $M\in\{M_x$, $M_u\}$. P_{ij}^{AB} is the probability Alice sends information *i* and measurement of Bob is information *j*, *i* , *j*=0 , 1, then:

$$P_{iMj}^{AB} = \sum_{s\in C^{-1}(i)} P_{|s\rangle}^{AB} P_M^{AB} \sum_{t\in C^{-1}(j)} P_{|s\rangle M|t\rangle}^{AB} = \frac{1}{4}\sum_{s\in C^{-1}(i)}\sum_{t\in C^{-1}(j)} P_{|s\rangle M|t\rangle}^{AB}, \tag{8}$$

The probability Bob obtains detection responds form Alice is shown in table 1.

The quantum states Bob receives has drifted θ, which makes Bob obtain a measurement response even he wrongly selects the projection operator. P_d^{AB} expresses the probability Bob can obtain the measurement response, then:

$$\begin{aligned} P_d^{AB} &= P_{0M_x0}^{AB} + P_{0M_u1}^{AB} + P_{1M_x0}^{AB} + P_{1M_u1}^{AB} = \frac{1}{4}\left(\frac{1-\sin 2\theta}{2}\right) + \frac{1}{4}\left(\frac{1-\cos 2\theta}{2}\right) + \frac{1}{4}\left(\frac{1-\cos 2\theta}{2}\right) \\ &+ \frac{1}{4}\left(\frac{1+\sin 2\theta}{2}\right) = \frac{1}{4}(2-\cos 2\theta) \end{aligned} \tag{9}$$

Table 1: Probability Bob obtains detection responds form Alice

$P_{\|s\rangle M\|t\rangle}^{AB}$	$t=x$, M_x	u, M_x	$t=x$, M_u	u, M_u
$s=x$	$\frac{1-\sin 2\theta}{2}$	$\frac{1+\sin 2\theta}{2}$	$\frac{1+\cos 2\theta}{2}$	$\frac{1-\cos 2\theta}{2}$
u	$\frac{1-\cos 2\theta}{2}$	$\frac{1+\cos 2\theta}{2}$	$\frac{1-\sin 2\theta}{2}$	$\frac{1+\sin 2\theta}{2}$

According to the B92 protocol, Bob reserves bits with measurement response and abandons others. Considering the states sending from Alice is transparent to Bob, P_{cd}^{AB} is the probability Bob thinks his measurement is right, then:

$$P_{cd}^{AB} = P_{d}^{AB} = \frac{1}{4}\left(2-\cos 2\theta\right) \tag{10}$$

Actually, the probability Bob correctly(right projection operator and measurement response) measures states from Alice is P_{c}^{AB}, then:

$$P_{c}^{AB} = P_{0M_x 0}^{AB} + P_{1M_u 1}^{AB} = \frac{1}{4}\left(\frac{1-\sin 2\theta}{2}\right) + \frac{1}{4}\left(\frac{1+\sin 2\theta}{2}\right) = \frac{1}{4}. \tag{11}$$

According to the results above, when polarization drift angle $\theta = 0^\circ$, $P_{d}^{AB} = P_{cd}^{AB} = P_{c}^{AB} = \frac{1}{4}$, which is reasonable; when polarization drift angle $\theta \neq 0^\circ$, $P_{d}^{AB} = P_{cd}^{AB} \neq P_{c}^{AB} = \frac{1}{4}$, and P_{d}^{AB} changes along with the polarization drift angle.

Define a coefficient of proportionality D_{cd}^{c} which means the ratio of the probability Bob correctly measures states from Alice to the probability Bob thinks his measurement is right, then:

$$D_{cd}^{c} = \frac{P_{c}^{AB}}{P_{cd}^{AB}} = \frac{1}{2-\cos 2\theta}. \tag{12}$$

When the polarization drift angle $\theta = 0^\circ$, $D_{cd}^{c} = 1$, which means the probability Bob correctly measures states from Alice is equal to the probability Bob thinks his measurement is right; When the polarization drift angle $\theta \neq 0^\circ$, $D_{cd}^{c} < 1$, which means there exists wrong bits in the results Bob thinks his measurement is right, and the probability is:

$$P_{cd}^{AB} - P_{c}^{AB} = \frac{1}{4}\left(1-\cos 2\theta\right). \tag{13}$$

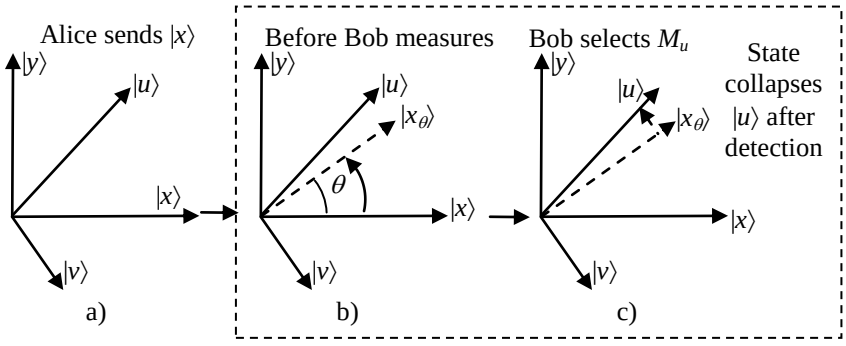

Fig. 2: Picture for showing detection collapsing of Alice and Bob

Analysis on the Quantity Of Information

Analyze the mutual information between Alice and Bob in the sifted data after response confirming. In the sifted data, the probability Bob selects projection operator M_x is 0.5, and the probability Bob gets response is P_1; The probability Bob selects projection operator M_u is 0.5, and the probability Bob gets response is P_2, then:

$$P_1 = \frac{\frac{1-\sin 2\theta}{2}}{\frac{1-\sin 2\theta}{2} + \frac{1-\cos 2\theta}{2}}, \quad P_2 = \frac{\frac{1+\sin 2\theta}{2}}{\frac{1+\sin 2\theta}{2} + \frac{1-\cos 2\theta}{2}} \tag{14}$$

$$
\begin{aligned}
H(A|B) &= \frac{1}{2}H(P_1)+\frac{1}{2}H(P_2) \\
&= \frac{1}{2}\left(\frac{1-\sin 2\theta}{2-\sin 2\theta-\cos 2\theta}\log_2\frac{2-\sin 2\theta-\cos 2\theta}{1-\sin 2\theta}\right. \\
&\left.+\frac{1-\cos 2\theta}{2-\sin 2\theta-\cos 2\theta}\log_2\frac{2-\sin 2\theta-\cos 2\theta}{1-\cos 2\theta}\right) \\
&+\frac{1}{2}\left(\frac{1+\sin 2\theta}{2+\sin 2\theta-\cos 2\theta}\log_2\frac{2+\sin 2\theta-\cos 2\theta}{1+\sin 2\theta}\right. \\
&\left.+\frac{1-\cos 2\theta}{2+\sin 2\theta-\cos 2\theta}\log_2\frac{2+\sin 2\theta-\cos 2\theta}{1-\cos 2\theta}\right)
\end{aligned} \tag{15}
$$

The mutual information between Alice and Bob is:

$$
I(A,B)=H(A)-H(A|B)=1-\frac{1}{2}H_1 . \tag{16}
$$

From the formula above can we see, the mutual information is related to the polarization drift angle. When the angle $\theta=0^\circ$, the mutual information $I(A,B)_{\max}=1$, which indicates the data of the partners is the same without any uncertainty in the sifted data and the mutual information reached its maximum value; When the angle $\theta\neq 0^\circ$, the mutual information $I(A,B)$ changes along with the polarization drift angle, that is, the quantity of mutual information of Alice and Bob in per symbol changes. Especially, when the angle $\theta=90^\circ$, the mutual information $I(A,B)_{\min}=\frac{5}{3}-\log_2 3=0.0817$, which reaches its minimum value. The relationship is shown in fig. 3. Through computing the mutual information in BB84 protocol with polarization drift, obtain the variation is from 0.4 to 0.5. Comparing to BB84, the variation of mutual information in B92 is violent from 0.0817 to 1, which indicates that the effect of polarization drift is higher in system based on B92 protocol than that in BB84 protocol.

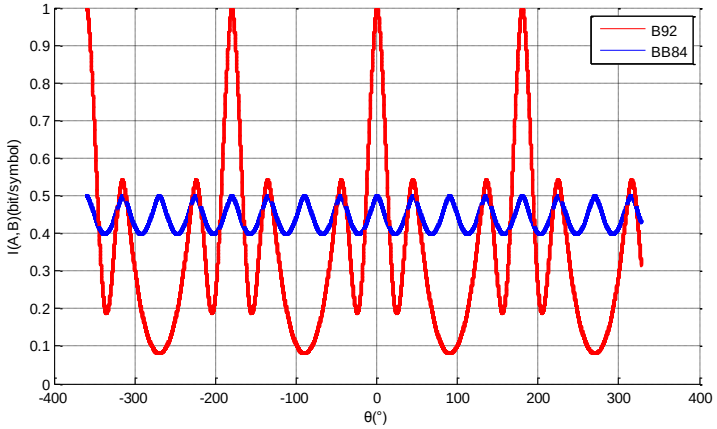

Fig. 3: Picture for showing the relationship between the mutual information and the polarization drift angle

Analysis on the Comparison to the Ideal Channel

Table 2 shows the comparison results of efficiency of keys and the quantity of information in a practical quantum communication system with polarization drift, and the results in the ideal channel.

The comparison results show that, duo to polarization drift in the quantum communication channel, the probability Bob obtains the measurement response with a projection operator(the probability Bob thinks his measurement is right) P_{cd}^{AB} changes along with the polarization drift angle θ. When the angle is 0 °, the probability above is minimum: 0.25; When the angle is 90 °, the probability reaches the

maximum value 0.75; Actually the probability Bob really correctly measures the states is 0.25 and invariant; While the coefficient of proportionality of the two probability above is closely related to the angle. When the angle θ is 90 °, the coefficient of proportionality is minimum： $1/3$; When the angle θ is 0 °, the coefficient of proportionality reaches its maximum value: 1.

Summary

Analyze how the polarization drift affects the efficiency of generating keys and the mutual information in a practical quantum communication system based on the B92 protocol and contrast results above with the ideal condition. Obtain that, when the polarization drift angle is 0 °, results accords with the ideal condition; when the polarization drift angle is not 0 °, corresponding results changes and provide the peak interval. If the eavesdropper is introduced, how the polarization drift affects the eavesdropping needs to be further analyzed.

Table2: The contrast to the ideal condition

Terms	Ideal channel	Drift channel
P_{cd}^{AB}	$\frac{1}{4}$	$\frac{1}{4}\left(2-\cos 2\theta\right)$
P_{c}^{AB}	$\frac{1}{4}$	$\frac{1}{4}$
D_{cd}^{c}	1	$\frac{1}{2-\cos 2\theta}$
$I\left(A,B\right)$	1	$1-\frac{1}{2}H_1$

References

[1] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(21): 3121.

[2] Xiaonan Sun. Analysis and realizing on the QKD system with polarization code based on the B92 protocol[D]. Xi'an Electronic and Science University, 2012

[3] Zheng'an Xiao. Analysis and computer simulation on the quantum keys based on the B92 protocol[D]. Wuhan University of Technology, 2005

[4] Lavale M. Analysis of Differential Phase Shift Quantum Key Distribution[J]. arXiv preprint arXiv:1110.4820, 2011.

[5] Buttler W T, Hughes R J, Kwiat P G, et al. Practical free-space quantum key distribution over 1 km[J]. arXiv preprint quant-ph/9805071, 1998.

[6] Lee S Y, Ji S W, Lee H W, et al. Quantum key distribution using vacuum-one-photon qubits: maximum number of transferable bits per particle[J]. Journal of the Physical Society of Japan, 2009, 78(9).

[7] Yang C N, Kuo C C. Enhanced quantum key distribution protocols using BB84 and B92[C]//Proceedings of the 2002 International Computer Symposium. 2002, 2: 951-959.

[8] Mendonça F A, de Brito D B, Silva J B R, et al. Experimental implementation of B92 Quantum key distribution protocol[C]//Telecommunications Symposium, 2006 International. IEEE, 2006: 712-717.

[9] Inoue K, Waks E, Yamamoto Y. Differential-phase-shift quantum key distribution using coherent light[J]. Physical Review A, 2003, 68(2): 022317.