Single Wavelength Entangled Pair in Quantum Channel Authentication for QKD

Mohamed Youssef Khalaf Elwadeya[*], Khalid S. A. Al-Khateeb[**], Nurul Fadzlin Hasbullah[**]

[*] Department of Electrical and Computer Engineering, International Islamic University Malaysia
[**] Department of Electrical and Computer Engineering, International Islamic University Malaysia
[***] Department of Electrical and Computer Engineering, International Islamic University Malaysia

Abstract- The photon splitting of an UV into entangled pair of different wavelengths using non-linear crystals is a complicated procedure in the quantum authentication process (QAP) as presented in the six states deterministic protocol (6DP). A simplified process is proposed; the photon splitting process is replaced with basic polarization splitting of a single wavelength in the visible range. The quantum states are prepared, as usual, using retardation wave-plates. The transmitting station sends to the receiver a sequence of random polarized pulses via a quantum channel. The receiver blindly flips the quantum states using half wave-plate before sending back to the transmitter. The transmission of quantum states is made within a secret time interval which, based on preset path length and pulse travel time, triggers the detection device, and eventually achieves authentication after two more iterations.

Index Terms- quantum channel, authentication process, photon polarization, deterministic states.

I. Introduction

Quantum key distribution algorithms are implementations of certain quantum laws and principles for secure cryptographic applications. In QKD systems, users are enabled to have access to a quantum channel through which photons carrying secret information are exchanged securely. Therefore, the establishment of a secure authenticated quantum channel is one characterization of QKD systems which are physically realizable with optical fibers or free space optics (FSO). In general, one station (commonly known as Alice) prepares a sting of photons in certain quantum states and sends them to the intended stations. The receiver (commonly known as Bob), upon reception of photons, examines them in order to extract the encoded cryptographic key. The key is used to decrypt the cihper-text transmitted over the classical channels, e.g. internet. The quantum states according to the no-cloning principle can never be copied which means that any attempt of eavesdropping can be easily detected [1]

In QKD systems, new cryptographic keys are created uniquely and randomly; then automatically shared between Alice and Bob [2]. The key is created from a string of 0s and 1s encoded based on photons' states of polarization. Single photon sources are not physically applicable; however, the additional path loss approximates the single-photon situation.

Quantum bits (qubits) are the basic representation of quantum information. A qubit is a superposition of two different quantum states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

The complex coefficients α and β are related by:

$$|\alpha|^2 + |\beta|^2 = 1$$

Deterministic quantum protocols mostly implements the quantum entanglement phenomenon between two photons such that acting on one of them significantly alters the quantum state of the other; which therefore can be used as a security indicator for several services but more prominently for authentication.

The remainder of this paper is organized as the following; section II presents related QKD work. In section III the simplification on the QAP-6DP is discussed. The results are shown and analyzed in section IV. Finally, discussion over quantum channel and conclusion are presented in sections V and VI respectively.

II. Quantum Protocols

Developing quantum protocols for cryptographic applications started in the 1980s. Different protocols are characterized by different security aspects and limitations. The most obvious limitation of earlier quantum crypto algorithms is mainly the physical realization; for example single photon sources and detectors. Years after, the realization of quantum entanglement has significantly enhanced security (e.g. source authentication) when implemented deterministically.

The first quantum cryptographic protocol is BB84 developed in 1984 and named after Charles Bennett and Gilles Brassard. Both Alice and Bob are connected via two channels; classical channel and a quantum channel [3]:

Alice prepares quantum states on a random rectilinear or diagonal basis then sends it to Bob.

Bob measures the quantum states with a basis he chooses randomly. If the chosen basis matches, the corresponding bit is decoded correctly. Otherwise, a random result (0 or 1) with equal probability of half.

In the public channel, Alice and Bob compare the decoded bits. Bits corresponding to mismatched bases are removed resulting in the shifted key.

Finally, Alice and Bob obtain a joint secret key from the remaining bits by performing error correction.

BB84 exhibit absolute security to most attacks. However, the realization of single photon sources and detectors is still unavailable. Moreover, the quantum communication system is limited to only few thousands bits per second.

In 1991 Artur Ekert [4], proposed a protocol using EPR (Einstein-Podolsky-Rosen) entangled photons' state. An entangled pair of photons hitting two detectors, the measurement gives opposite 100% correlated polarizations.

The entangled photons can be generated by Alice, Bob or a trusted third party such that each station eventually posses one of the entangled photons. The main advantage of the protocol is that the security characterization is realized once the correlation between the entangled photons is maintained. Any attempt to eavesdrop destroys the photons correlation.

Subhash Kak [5], suggests the development of quantum crypto algorithm in which the security is based on the quantity of photons being exchanged during a QKD session. The proposed scheme is (p-k-n) where p is the security threshold of the number of exchanged photons. If the number falls between p and k, the security is partial. Finally, all actions are aborted if the number of photons exceeds k. Single photon sources are not required, which results in longer distances of communications. However, this approach is yet to be much more investigated for theoretical security and practical implementation.

Boyer et al [6] proposed the BKM deterministic quantum scheme a semi-passive Bob. Bob's access to the quantum channel is limited to only acting on photons it receives; i.e. Pass or flip using the identity operator or the NOT operator, respectively. The merits of this approach are; first, quantum sources and detectors are not required in all stations. Second, the protocol provides a simple algorithm for quantum secure direct communication (QSDC) with 'pass' or 'flip' as '0' bit or '1' bit corresponding operators, respectively. Although the BKM scheme with semi-classical receiver exhibits secure nature and efficient performance, the technological support of the optical equipments is still slow-advancing.

Unlike BKM, the LM05 protocol [7], describes Bob as the one who prepares quantum states in one of the four linear polarizations (rectilinear or diagonal bases) and then transmit them to the other station, Alice. A bit is decoded based on which quantum operator Alice has used. If it acted on using the identity operator, decoded bit is '0'. On the other hand, bit '1' is decoded if the NOT operator iY was applied on the photons by Alice. After that, Bob measures the quantum states using the same settings in the preparation stage. The decoded string of bits creates the cryptographic key. This protocol is characterized by a deterministic performance. However, the algorithm is reported to be vulnerable against photon number splitting (PNS) type of attacks.

The six states deterministic protocol (6DP) [8] describes a quantum channel authentication scheme where one station decodes deterministically based on the quantum operation that has been implemented by the other station. In 6DP, Bob prepares an entangled pair of photons; in different wavelengths and bases, then sends them to Alice. Alice acts on the photons blindly and sends them back to Bob's which upon reception examines them using the same preparation settings. Finally, Bob will decide deterministically what operator has been used on the photons by Alice. If the correlation measurement between the prepared and received photons is valid within the secret time interval, the channel is authenticated which enables the key distribution process to begin afterwards. Otherwise the process is aborted. However, the QAP scheme of the 6DP requires a second harmonic generation (SHG) process which results in a complicated and high-cost implementation.

III. Simplification Procedure

The first step in the simplification process is the use of single wavelength in a similar way as proposed by Lucamarini [9]. The result is four possible quantum states of preparation:

$$|z+\rangle = |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad |z-\rangle = |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

$$|x+\rangle = |0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \qquad |x-\rangle = |1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

Alice receives the quantum states and operates on them blindly before she sends them back to Bob. This algorithm exhibits unconditional security according to the author who has also suggested a possible experimental setup [10]. However, complicated and costly type II down conversion process using non-linear crystals such as Beta Barium Borate (BBO3) in the preparation stage is applied. Moreover, the optical fiber as a quantum channel is used which creates the issue of optical activity which severely alters the polarization state of incident light pulses because they experience two different refractive indices (the simplification procedure in this paper uses an FSO quantum channel). Finally, Lucamarini did not specifically provide a mechanism for quantum authentication process (QAP) in his experiment.

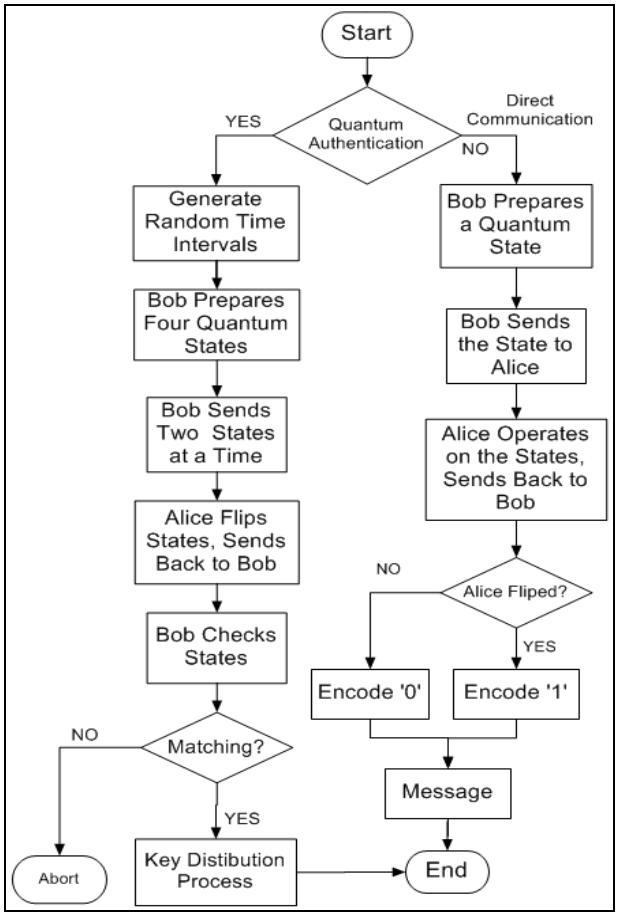
The flipping of the quantum state is physically realized using a half-wave plate which rotates the polarization by 90 degrees as it causes a phase shift of 180 degrees between the components of the incident light. This occurs if it is oriented at 45 degrees. If it is oriented to either of its principal axes, the plate becomes transparent to all incident states of polarization.
Bob prepares two states of polarization of the same wavelength, one after another:

$$\hat{x} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} \qquad \hat{z} = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$$

TABLE I. Quantum states of different quantum baisis

Q. Basis	$\|\psi-\rangle$	$\|\psi+\rangle$
$\hat{z}$	$\|z-\rangle = \begin{pmatrix}0\\1\end{pmatrix}$	$\|z+\rangle = \begin{pmatrix}1\\0\end{pmatrix}$
$\hat{x}$	$\|x-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	$\|x+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$

A. Flowchart



For a QAP session, Alice blindly flips the state of polarization of any photon she receives using the universal NOT gate iY. On the other hand, if the session is for QSDC, the identity operator I is introduced for passing the polarization without flipping (encode bit '0') while the universal NOT gate is used for flipping (encode bit '1').

$$iY = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Bob measures the photons using the exact same settings in the preparation stage. Next, he finds out deterministically which operator has been used by Alice. This process is repeated thrice to ensure authentication before the key distribution process takes place.

TABLE II. Operators for encoding bits '1' or '0'

	I	*iY*
$\hat{z}$	*pass*	*flipped*
$\hat{x}$	*pass*	*flipped*
Code:	*'0'*	*'1'*

B. First Simplification

In the original setup of QAP-6DP, the SHG provides two wavelengths [11]. Consequently, dichroic beam splitting is essential in the preparation process. Moreover, interference filtering is needed upon detection. Two half wave plates are placed in Alice's station; one for each wavelength. Moreover, Bob needs more single photon detectors.

Figure 1 shows the first simplification. a visible laser pulse is initiated within a secret random time interval. A quarter-wave plate is used to set laser polarization to circular polarization. Then, a set of mirrors placed precisely for timing control direct the beam to the Glan Thompson Polarizer (GTP) for beam polarization splitting. Each component (V or H) is then manipulated using wave-plates.

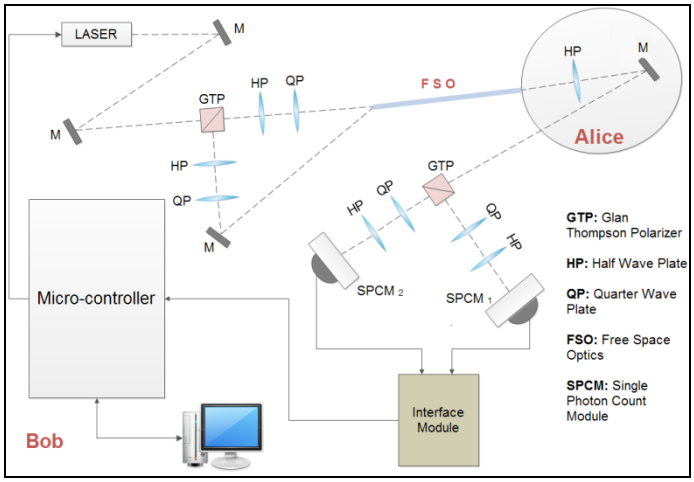


Figure 1: First simplification: neglecting the BBO3, DBSs, and Ifs

C. Second Simplification

Figure 2 shows that the detection settings in Bob are replaced with a quarter wave-plates such that the incoming circularly polarized states are transformed back to linearly polarized states. This allows Bob to check deterministically whether Alice flipped or did not flip the quantum state:

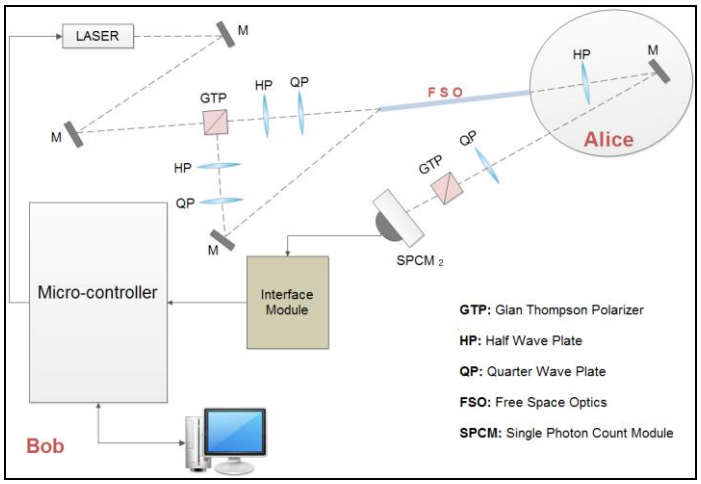


Figure 2: Second simplification: replacing Bob's detection side with a QP

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental setup for the simplified QAP procedure is governed by a MATLAB code which generates the real time charts of one authentication session as well as controlling the various components in the implementation environment such as the laser, photodiodes and Arduino Uno.

Figure 3 is a real time plot of coincidence measurement which correlates the horizontal polarization passed through a transparent HWP/ 90 then through a quarter wave-plate set at 45 degrees resulting in a circular polarization. The amplitude represents the light intensity response by the photo-sensor in units of luminous emittance (lux)

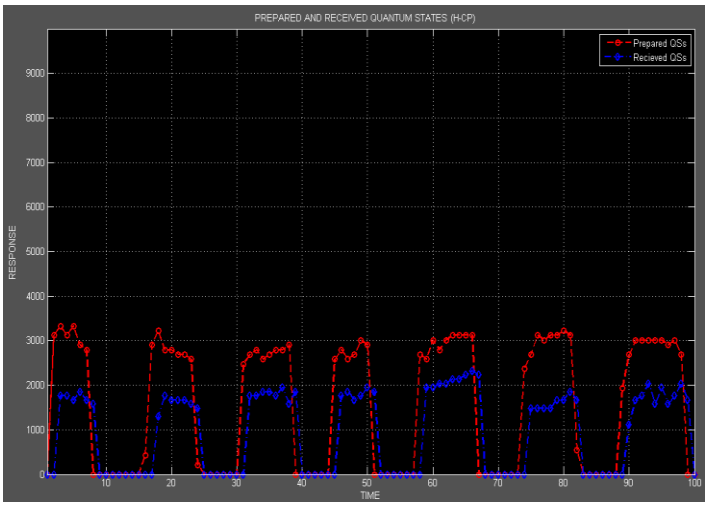


Figure 3: Photon response of prepared state (H-CP)

Similarly, the polarization beam splitter (PBS) is oriented such that the outgoing beam is linearly polarized vertical (LPV). The real time chart of the coincidence measurement is taken in a different time interval of 40s. The LPV pulse is changed to LPH by the HWP/45. Then changed again to circular polarized by the QWP/45. It can be highlighted that the response varies in amplitude from very close to the prepared quantum state to sometimes slightly below half the luminance of the prepared pulse. This can be justified by the path loss that the beam experiences (1m) However; the average response indicates strongly valid correlation.

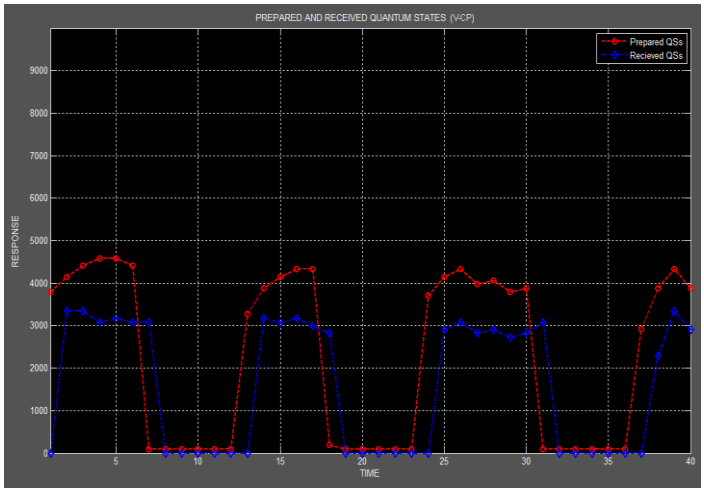


Figure 4: LPV changes to LPH then CP at HWP/45 and QWP/45

V. QUANTUM CHANNEL

A very suitable medium for photonic signals exchange is an optical fiber. Optical fiber repeaters are placed every 32 km which serves for wider areas of communications. However, optical fibers are subjected to optical and thermal activities significantly deform the states of polarization of light pulse launched into the fiber. That is; when the beam of light is launched into the optical fiber, linearly polarized states changes to elliptical states of polarization. The reason behind this is the existence of two different indices of refraction. The result is shifted components; fast component (experiencing the smaller refractive index) and slow component (experiencing the larger refractive index). The phase shift changes the original polarization from linear to elliptical. The elliptical polarization is examined such that it provides information indicating the original polarization.

Birefringence results in breaking the launched beam to its fundamental components with different relative phase shifts and amplitude:

$$E_x = E_{0x}\cos(kz - \omega t) \qquad E_y = E_{0y}\cos(kz - \omega t + \varepsilon)$$

The elliptically polarized state introduces an angle α which determines the amount of rotation of the ellipse from the fundamental *x-y* coordinates:

$$\alpha = \frac{1}{2}\tan^{-1}\left(\frac{2E_{0x}E_{0y}\cos\varepsilon}{{E_{0x}}^2 - {E_{0y}}^2}\right)$$

When α is zero or ε is 90^o; the ellipse principal axes aligns with the fundamental *x-y* coordinates. The analysis of the received ellipse together with the use of a quarter wave-plate gives information about the original transmitted linearly polarized light. Generally, a quarter wave-plate transforms the elliptically polarized light to linear by introducing retardation delay of 90 degrees.

Furthermore, the analysis of the ellipse (ellipsometry) can be used to initially launch an elliptically polarized light into the optical fiber, knowing that a linearly polarized light is going to

be received based on the optical activity analysis and parameters givens.

On the other hand, FSO links are also commonly used quantum channels. FSO is characterized by isotropy, zero-dispersion, and homogeneity.

VI. CONCLUSION

This paper presented a simplified algorithm for secure quantum authentication process (QAP). The original scheme was originally introduced in the six states deterministic quantum protocol (6DP). The simplification replaced the second harmonic generation process with polarization-splitting based procedure. The BBO3 non-linear crystal was disregarded together with dichroic beam splitters and interference filters. The authentication is ensured by providing timing control within secret time intervals of transmission. Initial experimental results proved the viability of the algorithm. Future work is open for technical improvements and implementation settings enhancements.

REFERENCES

[1] D. J. Griffiths, Introduction to Quantum Mechanics, 2 ed., USA: PEARSON, 2005, pp. 93-118.

[2] D. Brub, G. G. Erdelyi, T. Meyer, T. Riege, "Quantum Cryptography: a Survery*," University of Desseldorf, p.9, Germany 2006

[3] M. Scholz, "Quantum Key Distribution via BB84: an Advanced Lab Experiment," University of California, p8, November 2007.

[4] F. Grosshans, P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States,", Phys. Rev. Lett, 88, (057902), January 2002.

[5] Y. Tokunaga, T. Okamoto, N. Imoto, "Threshold Quantum Cryptography", Phys. Rev. A 71 (012314), January 2005.

[6] D. K. T. M. Michel Boyer, "Quantum Key Distribution with Classical Bob," in IEEE First International Conference on Quantum, Nano, and Micro Technologies (ICQNM07), 2007

[7] I. B. M. F. Abdul Khair, "Secure Communication with Practical Two-Way Quantum Key Distribution Protocol and Weak +Vacuum Decoy State," in IEEE, Kuala Lumpur, 2013.

[8] M. L. M. W. J. S. Shaari, "Determinsitic Six State Protocol for Quantum Communication," ELSEVIER, vol. 385, no. Physics Letters A, pp. 85-90, 2006.

[9] S. M. Marco Lucamarini, "Secure Deterministic Communication without Entanglement," PHYSICAL REVIEW LETTERS, vol. 94, p4 15 April 2005

[10] M. L. Alessandro Cere', "Experimental Test of Two Way Quantum Key Distribtuion in the Presence of Controlled Noise," PHYSICAL REVIEW LETTERS, vol 96, no. 200501, p. 4, 26 May 2006.

[11] K. Al-Khateeb, M. Munther, "Secure Protocol Using 6DP for Quantum Authentication and Hash Functions for Key Distribution," International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur 2010.

AUTHORS

First Author – Mohamed Youssef Khalaf Elwadeya, MSc. candidate Communications Engineering, International Islamic University Malaysia (www.mykw_90@hotmail.com)
Second Author – Khalid S. A. Al-Khateeb, PhD, Manchester University, United Kingdom, MSc. Salford University, United Kingdom, BSc, Royal College, United Kingdom. Professor in the faculty of engineering, International Islamic University Malaysia, (khalid@iium.edu.my)
Third Author – Nurul Fadzlin Hasbullah, PhD, University of Sheffield, BSc, University of Wales. Professor in the faculty of engineering, International Islamic University Malaysia, (nfadzlin@iium.edu.my)

Correspondence Author – Mohamed Youssef Khalaf Elwadeya (www.mykw_90@hotmail.com), (mykw90@gmail.com) , +60-0132566070