Helix (2021) 11 (6): 18-23

https://doi.org/10.29042/2021-11-6-18-23

Authenticated Quantum Three Pass Protocol on One-Time Pad Cryptographic Technique

[*1]Gautam Kumar, [2]Hemraj Saini, [3]Vipin Balyan

[*1]Dept. of Computer Science & Engineering, CMR Engineering College, Hyderabad, Telangana, India
gautam21ujrb@gmail.com

[2]Dept. of Computer Science & Engineering, DIT University, Dehradun, UtraKhand, India
hemraj1977@yahoo.co.in

[3]Dept of Electrical, Electronics and Computer Engineering, Cape Peninsula University of Technology, Cape Town, South Africa
balyanv@cput.ac.za

Received: 29th October 2021, Accepted: 30th November 2021, Published: 31st December 2021

Abstract

A double precision security based application is presented on one-time pad (OTP) technique cryptography using quantum three-pass protocol (QTPP) for subsequent encoding and decoding of plaintext(s). The encoding message first transformed to quantum state, called photon particles, used as qubit, and after encoding that quantum state is rotated randomly by an angle Φ_j for each quantum bits. For the same, both parties agree over a random shared secret key generated by the system that are specific to the security services and works as hidden agents for the next session to establish. The encryption and decryption utilizes the quantum three-pass protocol for the OTP, and finally detailed analysis is presented.

Keywords: *QTPP; One-Time Pad; Entanglement; Quantum Cryptography; Qbits*

Introduction

Security and privacy are the heart of cryptography that can practically achieves by modeling the mathematical transformation in references to the applied algorithms. Cryptography is one of core concept in information security that hides the original information when it passes through channels in medium. It is based on art and science on technologies uses to corresponding role responsiveness at each associated resources, where the information during transit to be safe, secure and satisfies the security services like confidentiality, authentication, integrity, and non-repudiation. With modernization of the security needs, cryptography is considered to be a mixed resultant of mathematical principles that can be implemented with science & technology, and finally to test to ensure for end users applicability [1]. The security services are the key ingredients in cryptography, where it can be achieving through the use of key generation, authentication, encryption, decryption, digital signatures etc.

The quantum cryptography consists of the quantum mechanics and considering to be one of the most emerging fields in security. The quantum mechanics basically having an example in flow of information using light and its corresponding properties in the same. Using the same quantum cryptography, the first principle is given by Bennett in 1984 [2] and that has observed to unconditionally secure enough in keys distribution and protocol applicability. In relation to the same, the proposed protocol doesn't allow the parties to share the secret information [3].

In general the information is transformed into the sequence of computer bits {0,1}, known as binary or classical computing. In contrast to the same, quantum computing encodes the classical computing, named as 'qubits', which uses Dirac-Notation, that can be on or off at the same time, and this condition is known as superposition states. The difference and similarity to understand both the approaches on computation basis represented on $\{|0>, |1>\}$, which is applicable both for classical and quantum computing, but quantum uses as pure states as |0 or |1. The quantum

information in contrast to classical information releases probabilistic nature, that acts qubits be kept in superposition states, such as $\{|0>,|1>\}$ represented in $(\alpha|0+\beta|1)$, where $\alpha,\beta \in \mathbb{C}$. Due probabilistic nature with its coefficients $|\alpha|^2+|\beta|^2=1$, theoretically with the same infinite information can be encoded or accumulated into one qubit. But important to know, this is not applicable in integers. Therefore, one qubit is as large as to store key values, which is combinatorial be inaccessible. Instead of the same qubit is sufficient in storing the infinite information. But, there are some limitations; (i) this is not applicable to integers (ii) certain level of noise during transmission channel, and (iii) associated error correction requirements.

The manuscript is organized in sections, section 2 contains the background details, section 3 contains the working principles of quantum three pass protocols, further in section 4, how the one-time pad can be used with quantum cryptography with quantum-three pass protocol works and their security analysis is presented in the next section. At the end work is concluded in last.

Background Details

The quantum cryptography is an innovative approach based on discrete phenomena that works on the laws of quantum mechanics, such as the use of superposition and entanglement operations. The most unique property of quantum cryptography is not only protecting communications channels, but also the detection of a third party trying to break in and gain knowledge of the secret key. It is a method through which two users of a common communication channel generate a body of shared and secret string of information that can be used as a secret key for standard encryption to ensure secure communications.

If we see the progress of quantum cryptography, it is initially be considered based on uncertainty principle of nondeterministic approach, but later be shown to be deterministic distribution on secure communications for exchanging of photons with classical channels [4] and secure communications using entanglement [5]. The weaknesses of the [5] is resolved out A. Wojcik and Q.Y. Cai in [6] and [7] with the eavesdropping on the quantum cryptography and eavesdropping without Ping-pong.

A Shamir's Quantum Three-Pass protocol is a new kind of quantum cryptography approach based on classical cryptography [8], and then the quantum three-pass protocol (QTPP) based on quantum superposition state is proposed [9] showing that there can be no key shared between the sender and receiver. Due to rapid growth in science and innovation in subsequent years given a wide applicability of quantum algorithms that likely to be working with the classical algorithms in cryptography but the quantum algorithm is based on the quantum laws and its mathematical laws in suggested in [10] a realizable quantum encryption algorithms for qubits and in [11] novel qubit block encryption algorithm with hybrid keys. Further to see in 2015 [12], the quantum cryptography has applied with image correction to proceed with the encryption techniques and quantum cryptography with quantum three pass protocol using the Hill-cipher techniques by Abdullah et all [13].

Quantum Three-Pass Protocol (QTPP)

The Quantum Three-Pass Protocol in cryptography has shown the matured behavior on its applicability in many applications. This protocol is an extension to Shamir's three pass protocol on quantum cryptography. The implementation of the protocol uses quantum channels using the photon as a qubit. The qubit bit is encrypted on the photon by an angle θj rotation, which is chosen randomly on qubit. This rotated operation is described as:

$$R(\theta j)=\begin{bmatrix} cos\theta j & sin\theta j \\ -sin\theta j & cos\theta j \end{bmatrix} \qquad (1)$$

This can be assumed in encryption with θj as the encryption key, where its rotation in decryption is considered with an angle $-\theta j$. In this protocol there is no shared keyed required on both the parties between sender and receiver. This logic is generalized for the sender as generation of secret key $K_{\theta S}$ where $K_{\theta S}=\{\theta_S|0\leq\theta_S<\pi\}$ for each session. At the other end, receiver generates its own secret key $K_{\theta R}$ where $K_{\theta R}=\{\theta_R|0\leq\theta_R<\pi\}$ for each session. The key generation is likely being negligible for the opponent to discover. The key generation for sender and

receiver changes with each qubit and each key is only used twice during key generation (one is used for encryption and second is used for decryption). For the n-qubits of the keys are continued till key generations. Therefore, the used key for both (sender and receiver) will prevent any information release related to the key, as well as data to be being infiltration. Now, if it is assumed that the plaintext P is single photon encrypted to the qubit as $P = |1$, the sender and receiver generate their own key, key of the sender $= K_{\emptyset s}$ and key of the receiver $= K_{\emptyset R}$. The sender encrypts the plaintext P with its generation key as the following:

$$E_{K_{\emptyset s}}[P]: R(\emptyset_S)\left|1 = \begin{bmatrix} cos\emptyset_S & sin\emptyset_S \\ -sin\emptyset_S & cos\emptyset_S \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = sin\emptyset_S\right| 0 + cos\emptyset_S|1\rangle, \qquad (2)$$

where E is the encryption with the sender key $K_{\emptyset s}$, and the resulting is the superposition state $|\emptyset_1>$ where the sender will send it to the receiver. The receiver receives the photon in $|\emptyset_1>$ and encrypts it with its own key as the following:

$$E_{K_{\emptyset R}}\left[E_{K_{\emptyset S}}[P]\right]: R(\emptyset_R)|\emptyset_1\rangle = \sin(\emptyset_R + \emptyset_S)|0\rangle + cos(\emptyset_R + \emptyset_S)|1 = |\emptyset_2\rangle, \qquad (3)$$

where $|\emptyset_2\rangle$ is the superposition state. The receiver sends $|\emptyset_2\rangle$ back to the sender. The sender receives $|\emptyset_2\rangle$ and decrypts it by using the angle $\emptyset_S$ but with rotation of $-\emptyset_S$ because there are decrypts in this case; then the results $\emptyset_3\rangle$ send it back to the receiver as the following:

$$D_{K_{\emptyset S}}\left[E_{K_{\emptyset R}}\left[E_{K_{\emptyset S}}[P]\right]\right] = E_{K_{\emptyset R}}[P]: R(-\emptyset_S) = sin\emptyset_R|0 + cos\emptyset_R|1\rangle = |\emptyset_3\rangle, \qquad (4)$$

where D is the decryption with the sender key $K_{\emptyset s}$. The receiver receives $|\emptyset_3\rangle$ and decrypts it by using the angle $\emptyset_R$ but with rotation of $-\emptyset_R$ because there are decryptions in this case; then the receiver gets the plaintext P that the sender sends it $|1|$as the following:

$$D_{K_{\emptyset R}}\left[E_{K_{\emptyset s}}\right][P]: R(-\emptyset_R)|\emptyset_3\rangle = \begin{bmatrix} cos{-\emptyset_R} & sin{-\emptyset_R} \\ -sin{-\emptyset_R} & cos{-\emptyset_R} \end{bmatrix}\begin{bmatrix} sin\emptyset_R \\ cos\emptyset_R \end{bmatrix} = |1\rangle \quad (5)$$

Finally, the receiver has the plaintext. Further, a proof of QTPP is presented in the next section.

Proof of Quantum Three-Pass Protocol (QTPP)

The use of Quantum Three-Pass Protocol (QTPP) in cryptography is to use encrypted messages as a single particle called quantum bits and then all the quantum bits are received using the QTPP as follows**:**

(i) The sender sends quantum bit as $|1$, after that it encrypts it to the photons by using the angle for the sender; I this proof, our assumption is θ_s=75, then $\theta_1$is:

$$\theta_1 = \begin{bmatrix} cos75 & sin75 \\ -sin75 & cos75 \end{bmatrix}.\begin{bmatrix} 0 \\ 1 \end{bmatrix}=\begin{bmatrix} 0.258 & 0.965 \\ -0.965 & 0.258 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix}=0.965|0\rangle + 0.258|1\rangle \qquad (6)$$

(ii) The receiver receives θ_1 and generate its own session angle as secret key, on θ_R=30; then $\theta_2$is

$$\theta_2 = \begin{bmatrix} cos30 & sin30 \\ -sin30 & cos30 \end{bmatrix}.\begin{bmatrix} 0.965 \\ 0.258 \end{bmatrix}=\begin{bmatrix} 0.866 & 0.5 \\ -0.5 & 0.866 \end{bmatrix}.\begin{bmatrix} 0.965 \\ 0.258 \end{bmatrix}=\begin{bmatrix} 0.964 \\ -0.258 \end{bmatrix}=0.964|0\rangle - 0.258|1\rangle \quad (7)$$

(iii) The θ_2 is sent back to sender, the sender decrypts by rotating θ_s by $-\theta_s$=-75 and sends this superposition state to receiver by:

$$\theta_3 = \begin{bmatrix} cos-75 & sin-75 \\ -sin-75 & cos-75 \end{bmatrix}.\begin{bmatrix} 0.965 \\ -0.258 \end{bmatrix}=\begin{bmatrix} 0.258 & -0.965 \\ 0.965 & 0.258 \end{bmatrix}.\begin{bmatrix} 0.965 \\ -0.258 \end{bmatrix}=\begin{bmatrix} 0.496 \\ 0.865 \end{bmatrix}=0.496|0\rangle + 0.865|1\rangle \quad (8)$$

(iv) Now, the receiver decrypts the same by rotating an angle θ_R by $-\theta_R$. Then afterwards receiver receives the original message.

$$\theta_4 = \begin{bmatrix} cos-30 & sin-30 \\ -sin-30 & cos-30 \end{bmatrix}.\begin{bmatrix} 0.496 \\ 0.865 \end{bmatrix}=\begin{bmatrix} 0.866 & -0.5 \\ 0.5 & 0.866 \end{bmatrix}.\begin{bmatrix} 0.496 \\ 0.865 \end{bmatrix}=\begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad (9)$$

This state $|1\rangle$ represents, this one is sent from sender. In the vice versa, from the receiver to sender works in the similar fashion, but only requirements to change in quantum bits in reverse order, as:

(v) $$\theta_1 = \begin{bmatrix} cos75 & sin75 \\ -sin75 & cos75 \end{bmatrix}.\begin{bmatrix} 1 \\ 0 \end{bmatrix}=\begin{bmatrix} 0.258 & 0.965 \\ -0.965 & 0.258 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix}=0.258|1\rangle - 0.965|0\rangle \quad (10)$$

(vi) $$\theta_2 = \begin{bmatrix} cos30 & sin30 \\ -sin30 & cos30 \end{bmatrix}.\begin{bmatrix} 0.258 \\ -0.965 \end{bmatrix}=\begin{bmatrix} 0.866 & 0.5 \\ -0.5 & 0.866 \end{bmatrix}.\begin{bmatrix} 0.258 \\ -0.965 \end{bmatrix}=\begin{bmatrix} -0.258 \\ -0.964 \end{bmatrix}=-0.258|1\rangle - 0.964|0\rangle \quad (11)$$

(vii) $$\theta_3 = \begin{bmatrix} cos-75 & sin-75 \\ -sin-75 & cos-75 \end{bmatrix}.\begin{bmatrix} -0.258 \\ 0.964 \end{bmatrix}=\begin{bmatrix} 0.258 & -0.965 \\ 0.965 & 0.258 \end{bmatrix}.\begin{bmatrix} -0.258 \\ 0.965 \end{bmatrix}=\begin{bmatrix} -0.997 \\ 0.000 \end{bmatrix}=-0.997|1\rangle + 0.000|0\rangle \quad (12)$$

(viii) $$\theta_4 = \begin{bmatrix} cos-30 & sin-30 \\ -sin-30 & cos-30 \end{bmatrix}.\begin{bmatrix} 0.997 \\ 0.000 \end{bmatrix}=\begin{bmatrix} 0.866 & -0.5 \\ 0.5 & 0.866 \end{bmatrix}.\begin{bmatrix} 0.997 \\ 0.000 \end{bmatrix}=\begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (13)$$

One-Time Pad using QTPP

In cryptography, Gilbert S. Vernam and Joseph O. Mauborgne proposed a truly random security approach, which is an enhancement over the Vernam cipher [14]. The idea suggested in the same is, according to the size of message a system uses a random key of the same size, and this key can be only be applicable to this message only. The security point of view, it is having special significance in correlation to the one-time uses. This can become as a unbreakable, and the given name as One-time pad. During the processing, it produces random output cipher text by bearing not a statistical relationship to the plaintext [15], [16]. Therefore, in a simple sense no way to break the security code, on the chosen plaintext. In cryptography, where perfect security is one of the requirement One-Time Pads is best suitable as it can't be cracked, but in relation to same it is having single-use and message length should not be less than or greater than the message size intake [17], [18]. In this technique, plaintext is shared with random secret key. Here, we can elaborate the same with one of the numerical example. A plaintext of the message is converted into numeric form or many be considered in the form of ASCII format, but here for simplicity purpose it can been considered in numeric form, like a=0, b=1, c=2, etc and a random secret key is considered. The cipher text of the message determines using plain text plus key modulus 26

$$\text{Cipher text} = (Plain\ text + Key)\%26 \quad (14)$$

and further the plaintext of the message generation is using cipher text minus key mod 26.

$$Plain\ \text{text} = (\text{Cipher}\ text - Key)\%26 \quad (15)$$

Example,

Sender

Plaintext:	C O V I D S U P E R H E R O E S A R E T H E I R W A R R I O R S 2 14 21 8 3 18 20 15 4 17 7 4 17 14 4 18 0 17 4 19 7 4 8 17 22 0 17 17 8 14 17 18
Key:	G R E E N W O R L D M O S T L Y A R E S H O W S A F F E C T N E 6 17 4 4 13 22 14 17 11 3 12 14 18 19 11 24 0 17 4 18 7 14 22 18 0 5 5 4 2 19 13 4
Initial Total(IT):	8 31 25 12 16 40 34 32 15 20 19 18 35 33 15 42 0 34 8 37 14 18 30 35 22 5 22 21 10 33 30 22
IT%26: Ciphertext (CT):	8 5 25 12 16 14 8 6 15 20 19 18 9 7 15 16 0 8 8 11 14 18 4 9 22 5 22 21 10 7 4 22 I F C F M Q O I G P U T S J H P A I I L O S E J W F W V K H E W

Transmission Media

Receiver

Ciphertext (CT):	I F C F M Q O I G P U T S J H P A I I L O S E J W F W V K H E W 8 5 25 12 16 14 8 6 15 20 19 18 9 7 15 16 0 8 8 1114 18 4 9 22 5 22 21 10 7 4 22
CT-Key:	2 -12 21 8 3 - 8 -6 -11 4 17 7 4 -9 -12 4 -8 0 -9 4 -7 7 4 -18 -9 22 0 17 17 8 -12 -9 18
(CT-Key)%26: Plaintext:	2 14 21 8 3 18 20 15 4 17 7 4 17 14 4 18 0 17 4 19 7 4 8 17 22 0 17 17 8 14 17 18 C O V I D S U P E R H E R O E S A R E T H E I R W A R R I O R S

Security Analysis

The proposed security is directly augmenting the behavior of Quantum Three Pass Protocol using the qbits, where the opponent is having likely to be impossible to decipher the sender and receiver private keys. The plaintext of the information cannot be find random secret key of the one-time pad too. In addition to the same the entanglement of keys is hard to get for the opponents qbits as the data are transmitted in three states such as sender-to-receiver, receiver-to-sender, and sender-to-receiver. In the transmission medium, the key exchange are applied that gives the benefits of quantum three pass protocols and gets the advantages of one-time pad. Therefore, the double precision security is available by using this hybrid mode.

Conclusion

The quantum technology is an innovative in the sense of propagation of information's using lights and its properties involved. As a security concern, the private data are important for one and all, where quantum cryptography working as one the most challenging to crack for the opponent. The proposed work is simulated with quantum three pass protocols (QTPP) key exchange protocol and key concept one-time pad techniques used are adding the tremendous advantages to use the same with any of the services to use. A double precision value addition in security services are always been a demand to implement for deployment purpose. Here in the work classical encryption techniques by one-time pad and use of QTPP relies on the principles of cryptography. The used protocol is having distinguish properties to apply. The security and implementation are well analyzed to conclude the proposed analogy can be right enough to prevent quantum attacks as well as classified attacks.

References

1. W. Stallings, Cryptography and Network Security: Principles and Practice, Pearson Custom Computer Science Series, Prentice Hall, 5th edition, 2010

2. C. H. Bennett andG. Brassard, "Quantumcryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, New York, NY,USA, 1984.

3. C. H. Bennett, F. Bessette,G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

4. A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter,"Secure communication with a publicly known key," Acta Physica Polonica A, vol. 101, no. 3, pp. 357–368, 2002.

5. K. Bostr¨om and T. Felbinger, "Deterministic secure direct communication using entanglement," Physical Review Letters, vol. 89, no. 18, pp. 187902–187905, 2002.

6. A. W´ojcik, "Eavesdropping on the 'ping-pong' quantum communication protocol," Physical Review Letters, vol. 90, no. 15, Article ID 157901, 2003.

7. Q.-Y. Cai, "The ping-pong protocol can be attacked without eavesdropping," Physical Review Letters, vol. 91, 2003.

8. L. Yang, L.-A. Wu, and S. Liu, "Quantum three-pass cryptography protocol," in Quantum Optics in Computing and Communications, vol. 4917 of Proceedings of the SPIE, pp. 106–111, Shanghai, China, October 2002.

9. Y. Kanamori and S. Moo-Yoo, “Quantum three-pass protocol: key distribution using quantum superposition states,” International Journal of Network Security & Its Applications, vol. 1, no. 2, 2009.

10. N.-R. Zhou and G.-H. Zeng, “A realizable quantum encryption algorithm for qubits,” Chinese Physics, vol. 14, no. 11, pp. 2164–2169, 2005.

11. N. R. Zhou, Y. Liu, G. H. Zeng, J. Xiong, and F. Zhu, “Novel qubit block encryption algorithm with hybrid keys,” Physica A: Statistical Mechanics and its Applications, vol. 375, no.2,pp. 693– 698, 2007.

12. T. Hua, J. Chen, D. Pei, W. Zhang, and N. Zhou, “Quantum image encryption algorithmbased on image correlation decomposition,” International Journal of Theoretical Physics, vol. 54,no. 2, pp. 526–537, 2015.

13. Alharith A. Abdullah,1 Rifaat Khalaf,2 and Mustafa Riza3, “A Realizable Quantum Three-Pass Protocol Authentication Based on Hill-Cipher Algorithm”, Journal of Mathematical Problems in Engineering, Hindawi Publishing Corporation, Volume 2015, Article ID 481824, 2015. http://dx.doi.org/10.1155/2015/481824

14. Menezes, A.J., P.C. van Oorschot and S.A. Vanstone, 1997. Handbook of Applied Cryptography. CRC Press, New York, USA

15. K.V.O. Rabah , Implementation of One-Time Pad Cryptography. Information Technology Journal, Issue 4, pp. 87-95, 2005. DOI: 10.3923/itj.2005.87.95

16. D. Bouwmeester, A. Ekert, and A. Zeilinger, The Physics of Quantum Information, Springer, New York, NY, USA, 2000.

17. Maurer, U.M. and J.L. Massey, 1990. Perfect Local Randomness in Pseudo-Random Sequences. In: Advances in Cryptology-CRYPTO89, Brassard, G. (Ed.). Springer Verlag, Heidelberg and New York, pp: 100-112

18. Parhami, B. (ed.): Computer Arithmetic: Algorithms and Hardware Designs. Oxford University Press, New York (2010).