

# On Quantum Double-Lock Encryption

Ahmed E\*

Mathematics department, Faculty of Science, Mansoura 35516, Egypt

Received: April 05, 2018; Accepted: April 13, 2018; Published: April 16, 2018

\*Corresponding author: Ahmed E, Mathematics department, Faculty of Science, Mansoura 35516, Egypt, E-mail: magd45@yahoo.com

## Abstract

Cryptography is important for management. Recently new results have posed a serious problem to present cryptography protocols. Quantum Key Distribution (QKD) is one of the most promising solutions to this problem. Some proposed Double-Lock Encryption protocols in QKD assumes that the qbits are 2-component. In this letter we propose a protocol without this assumption.

Cryptography is important for management. Recently it became clear that quantum computers pose a serious threat to the presently used protocols which depend on some difficult mathematical problems e.g. RSA protocol [1]. Quantum Key Distribution (QKD) is one of the most promising solutions to this problem. Its main advantage is that it depends on physical quantum laws e.g. entanglement and uncertainty [2]. Its main disadvantage is that it was difficult to implement in practice. Recently this problem has been solved [3]. QKD has been used for satellite transmission.

Double lock encryption (Zero knowledge) is a protocol that increases the protocol security [4]. Some proposed Double-Lock Encryption protocols in QKD assumes that the qbits are 2-component. In this letter we propose a protocol without this assumption [5,6].

We apply it to the BB84 protocol which is one of the most popular QKD protocols [7].

Quantum Double-Lock (Zero knowledge) Encryption

Recently quantum 3-pass protocol has been proposed [5,6]. It was assumed that the qbits are 2-component hence they use the fact that the group  $SO(2)$  is commutative. This is Not true for  $SO(n)$ ,  $n > 2$ .

Here we propose the following protocol which does not make this assumption:

Assume that sender A sends a string of qbits  $\{qba(1), qba(2), \dots, qba(s)\}$  to a receiver B. He receives them which cause some errors according to Uncertainty principle [2]. The receiver B sends back the extended string

$\{qba'(1), qba'(2), \dots, qba'(s), qbb(s+1), \dots, qbb(s+r)\}$ . When the sender A receive it the correct subset of  $\{qba'(1), qba'(2), \dots, qba'(s)\}$  will form her key. The extended string is sent back to the receiver B and he gets  $\{qba'(1), qba'(2), \dots, qba'(s), qbb'(s+1), \dots, qbb'(s+r)\}$ . The correct subset of the string  $\{qbb'(s+1), \dots, qbb'(s+r)\}$  will be his key. No assumptions are made on the number of components used for each qbit.

These results are also applicable for the E91 protocol.

## References

1. Kraft JS, Washington LC. An introduction to number theory with cryptography. CRC publ. 2014.
2. Pade J. Quantum Mechanics for Pedestrians 2: Applications and Extensions, Springer Publisher. 2014.
3. Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, et al. Satellite-to-ground quantum key distribution. Nature. 2017;549:43-47.
4. Feige U, Fiat A, Shamir A. Zero knowledge proofs of identity. Proceedings of the nineteenth annual acm symposium on theory of computing. 1987:210-217.
5. Kanamori Y, Yoo SM. QUANTUM THREE-PASS PROTOCOL: KEY DISTRIBUTION USING QUANTUM SUPERPOSITION STATES. International Journal of Network Security & Its Applications. 2009;1(2):64-70.
6. Chan KWC, Rifai ME, Verma PK, Subhash K, Chen Y. Multi-Photon Quantum Key Distribution Based on Double-Lock Encryption. arXiv:1503.05793 [quant-ph]. 2015;5(3/4):1-13.
7. Giampouris D. Short Review on Quantum Key Distribution Protocols. GeNeDis. 2016:149-157.

Citation: Ahmed E (2018) On Quantum Double-Lock Encryption. J Comp Sci Appl Inform Technol. 3(1): 1-1.