On Quantum Double-Lock Encryption

Ahmed E*

Mathematics department, Faculty of Science, Mansoura 35516, Egypt

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)… 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)…qba'(s), qbb(s+1)…qbb(s+r)\}. When the sender A receive it the correct subset of \{qba'(1), qba'(2)…qba'(s)\} will form her key. The extended string is sent back to the receiver B and he gets \{qba'(1), qba'(2)…qba'(s), qbb'(s+1)…qbb'(s+r)\}. The correct subset of the string \{qbb'(s+1)…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


*Corresponding author email: magd45@yahoo.com