Research Journal of Applied Sciences, Engineering and Technology 6(23): 4381-4386, 2013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: January 31, 2013 Accepted: May 08, 2013 Published: December 15, 2013

Quantum Encoder and Decoder for Secret Key Distribution with Check Bits

T. Godhavari and N.R. Alamelu
Research Scholar, Satyabama University, Chennai-600119, India
SriRamakrishna Engineering College, Coimbatore-641022, India

Abstract: The focus of this study is to develop a novel method of encoding the qubits and use as secret key in public key cryptography. In BB 84 protocol, 50% of the random number (generated at source) is used as secret key and the remaining bits are used as "check bits". The check bits are used to detect the presence of eve as well as the nature of quantum channels. In this protocol, random qubits are encoded using different type of polarizations like horizontal, veritical and diagonal. In the proposed quantum encoder, basic quantum gates are used to encode the random secret key along with the check bits. Quantum key distribution, (a cryptographic mechanism) relies on the inherent randomness of quantum mechanics and serves as an option to replace techniques made vulnerable by quantum computing. However, it is still subject to clever forms of eavesdropping and poses a significant challenge to implementation. To study the challenges, quantum circuits are first simulated using QCAD.

Keywords: Check bits, quantum decryption, quantum encryption, quantum gates

INTRODUCTION

Promising advances in the field of quantum computing indicate a growing threat to cryptographic protocols based on integer factorization. To counter this threat, researchers have already designed and tested alternative protocols that do not rely on factorization (Paterson *et al*., 2004). Quantum information processing a field that includes quantum computing, quantum cryptography and quantum communication. It examines the implications of using a quantum mechanical model for information and its processing. Quantum communications offers many advantages for secure data transmission by encoding the information in quantum bits (qubits), using its intrinsic physical properties, such as polarization of a photon. However, if information is encoded into a property of a quantum object, any attempt to discriminate its non-orthogonal states inevitably changes the original state with a nonzero probability and these changes cause errors in transmissions and reveal the eavesdropper. QKD cannot prevent from eavesdropping, but it enables legitimate users to discover it. If any eavesdropping is detected, the key is simply thrown away and a new one is generated. Quantum Key Distribution (QKD) is one of the innovative methods of information processing that emerged from the properties of quantum mechanics.

LITERATURE REVIEW

Wiesner (1993) reported that if single-quantum states could be stored for long periods of time they could be used as counterfeit proof money (Wiesner 1983). Similarly, Bennet and Brassard (1984) proposed single quanta based information transmission and proposed the Quantum cryptography protocol "BB84". A working prototype system for the BB84 protocol using polarized photons was implemented by Bennet *et al*. (1992) for a propagation distance of 30 cm. Bennet *et al*. (1992) published a "minimal" QKD scheme ("B92") and proposed that it could be implemented using single-photon interference with photons propagating for long distances over optical fibers. Bennett *et al*. (1992) examined the security of even-odd bits of Quantum Cryptography. The aim of these experiments has been to show the conceptual feasibility of QKD. Quantum Key Distribution (QKD) is the best solution of the problem of key distribution in classical cryptography based on quantum mechanics. The above protocols were mostly based on Heisenberg's Uncertainty Principle and Bell's Inequality. Huttner and Peres employed noncoupled photons to exchange keys (Hutter and Peres, 1994). After 20 years of research in QKD development, a group of scholars asserted that key generation is not efficient in practice because only 50% of the qubits transmitted in the quantum channel are utilized. For example, out of 10 qubits, only 5 qubits are used for key generation. QKD mainly applied for one-time pad method and the length of the key must be the same as that of the plaintext, so the number of qubits required far exceeds the length of plaintext. So, the cost of frequent transmission of bulk messages is much too high. Consequently, the new idea of Quantum Secure

Corresponding Author: T. Godhavari, Research Scholar, Satyabama University, Chennai-600119, India

Direct Communication (QSDC) is proposed which transforms plaintext to qubits to replace the key and transmits the messages via the quantum channel. This reduces the number of qubits used and also enables automatic detection of eavesdroppers. Beige *et al*. (1999) transmitted the secure message comprises a single photon with two read-only qubit states. Later Boström and Felbingeer developed a Ping-Pong QSDC Protocol (Bostrom and Felbinger, 2002) that adopts the Einstein-Podolsky-Rosen (EPR) pairs (Einstein, 1935) as the quantum information carriers. So no additional information needs to be transmitted. A QSDC scheme using batches of single photons that acts as a one-time pad (Deng and Long, 2004) is proposed by Deng *et al*. in 2004 and in 2005 Lucamarini and Mancini (2005) presented a protocol for deterministic communication without applying entanglement. Namekata *et al*. (2005) demonstrated the performance of the fiber link by performing quantum key distribution, on the basis of the BB 84 four-state protocol, over 550 m of an installed multimode optical fiber local area network and achieved 1.09% quantum-bit-error rate. Wang *et al*. (2006) proposed a QSDC protocol that uses single photons, of which the concepts were resulted from the order rearrangement and the block transmission of the photons, Cederlof and Larson (2008) analyze security effects of using a key obtained from Quantum Cryptography (QC) for authentication purposes. In particular, the analysis propose a solution if the eavesdropper gains partial knowledge on the key in QC that may have an effect on the security of the authentication in the later round. So the quantum key is also used for authentication purposes. Capmany *et al*. (2009) provides an in-depth theoretical analysis of subcarrier multiplexed quantum key distribution (SCM-QKD) systems, taking into account as many factors of impairment as possible and especially considering the influence of nonlinear signal mixing on the end-to-end Quantum Bit Error Rate (QBER) and the useful key rate. Naor *et al*. (2008) presented an unconditionally secure authentication protocol in the manual channel model, in which the sender manually authenticates only 2 log (1 = ²) + O(1) bits and they proved that one-way functions are essential for the existence of authentication protocols'. Ali and Wahiddin (2010) had simulated the fiber and free-space practical decoy state quantum key distribution for both BB 84 and SARG 04 protocols. Serna (2012) presents a quantum protocol based on public key cryptography for secure transmission of data over a public channel with qubit secret keys. In the Eduin proposed protocol, the transmitted qubit can be in any arbitrary states not only in four states as in BB84 protocol. In this proposed protocol, secret key and the check qubits are encoded using quantum gates. All the existing protocols used polarization or state representations. Encoding and decoding of secret keys using quantum gates is a novel approach. In this method after analyzing the channel with check bits (detection of eavesdroppers/noise) secret key can be transmitted through the quantum channel.

Quantum communication: Conventional secret-key cryptography techniques require the communication of a secret key prior to message exchange. Quantum principles can be used to detect eavesdropping probabilistically when it occurs. A qubit is the precise quantum analogue of a classical bit where it is a two-state quantum system. The two basic orthogonal states of a qubit are represented by vectors labeled |0>and|1>.These states are called the computational basis states and provide analogues of the classical 0 and 1 states. But the analogy is not identity. While a classical bit may only exist in either the 0 or 1 states but qubit may exist in an arbitrary superposition of the computational basis states: |ψ>= α|0>+ β|1>, where α and β are complex numbers whose moduli squared sum to one. Examples to explain the qubit state are the spin degree of freedom of an electron or of a nucleus, or an atom with an excited and an unexcited energy state, or the polarization of a photon. Figure 1 gives the state of qubit representation. This qubits are transmitted as secret key in Quantum Key Distribution (QKD).

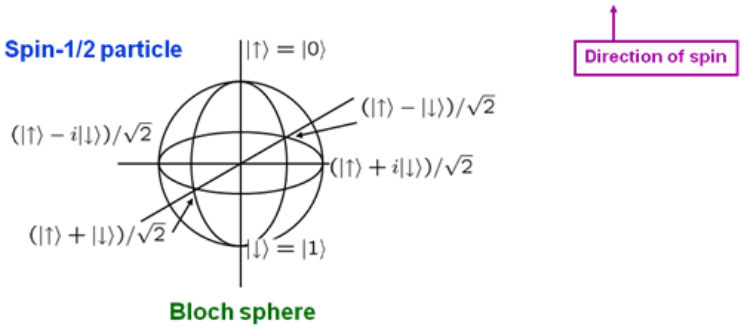

Fig. 1: State of a qubit

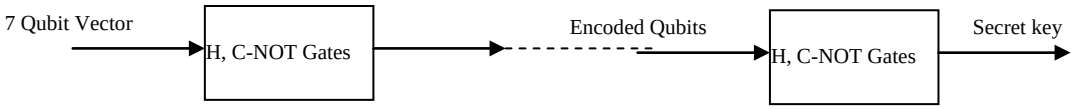

Fig. 2: Integrated encoder and decoder model

Quantum key distribution: Quantum cryptography is the study of the possibilities of secret communication using quantum properties. It holds guaranteed security of communication by the laws of physics, in contrast to the mere computational difficulty in classical methods (Sharbaf, 2009). The no-cloning theorem states that it is impossible to make copies of an unknown quantum state. One can swap $|\psi i$ from one system to another. This property mainly helps in quantum key distribution (Nicolas *et al*., 2007). Quantum Key Distribution (QKD) is an ingenious application of quantum mechanics, in which two remote legitimate users (Alice and Bob) establish a shared secret key through the transmission of quantum signals and use this key to encrypt (decrypt) the secret messages. Quantum secure direct communication is a branch of quantum cryptography, which allows that the sender transmits directly the secret key (not a random key) to the receiver in a deterministic and secure manner. Justin (2008) demonstrated for the first time that it is possible to communicate across thousands of kilometers using unbreakable codes whose security is guaranteed by the laws of quantum physics with the help of satellites. Quantum encryption algorithm has also been investigated. Communication between a sender and a receiver involves a mapping called encoding at the sender and an inverse mapping called decoding at the receiver. An encoder and decoder are designed for sharing the secret key as shown in the following circuit diagrams using QCAD Software (Vishal, 2007). In this study, in addition to the encoded secret key, check bits are used to detect the eavesdropper and the nature (noisy/perfect) of the quantum channel.

Encoder-decoder circuit: The secret key which is to be transmitted is encoded by various quantum gates (Nielsen and Chuang, 2000) like H, C-Not, Swap and controlled rotation gates. This 7 qubit key is encoded around hundred non-zero superposition states arbitrarily. One of the superposed states is selected and transmitted. In the decoder side, the received qubits are decoded by quantum gates like. H, Swap, CNOT, CCNOT. For each encoder superposition states, a unique decoder is needed to decode the secret key. If the secret key is received without noise and eves dropping, decoder decodes the secret key as a single output otherwise multiple output will be received (decoded). The simulation model of the encoder is shown in Fig. 2.

Check bits: A Check Bit is a binary digit used as part of a unit of information that is intended to indicate whether or not an error has occurred in the transmission or storage of the information. These are used to check for an error in data before it is accepted. In QKD check bits are used to estimate the level of noise, or eavesdropping (Marinesu and Marinesu, 2004). The following simulated the encoder and decoder (Godhavari and Alamelu, 2011) circuits used check bits along with the key in order to detect the eavesdropper and to provide secure communication for both sender and receiver.

PROPOSED QKD TRANSMISSION

- To transmit secret key n random numbers are generated by Alice.
- Part of the random number is used as check bits.
- To analyze about the channel, the check bits are encoded using unitary gates.
- Encoded check bits are transmitted through the quantum channel and received by Bob. He decodes the received bits.
- After receiving the check bits, Alice and Bob discuss the details of the check bits using classical channel.
- Error level of the check bits are used to estimate the level of noise, or eves dropping.
- If the check bits are not received properly, then again a fresh communication is established; otherwise the encoded key is transmitted and decoded in the receiver side (Godhavari and Alamelu, 2012).

SIMULATION RESULTS

The proposed 7 Bit Encoder and Decoder circuits are implemented in QCAD using quantum gates as shown in the Fig. 2 and 3. The check bits are also transmitted along with the secret key to detect the eavesdropper and errors that may be introduced during transmission of message from the source to a receiver.

Check bits without input data: The part of the generated random numbers are first transmitted through the channel. In simulation circuit the first 7qubits (Q1-Q7) are used as secret key and the next 4 qubits (Q9-Q12) are used as check bits.

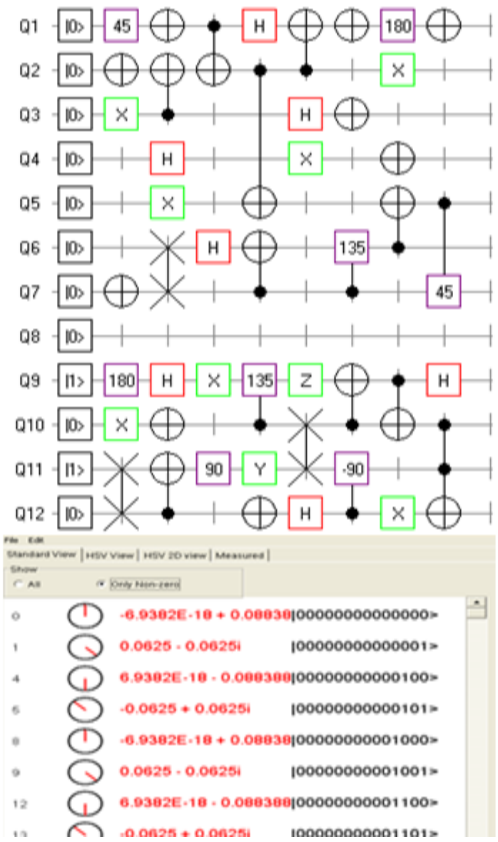

Fig. 3: QCAD simulated encoder with output for input data = 0000000 check bits input = 0101

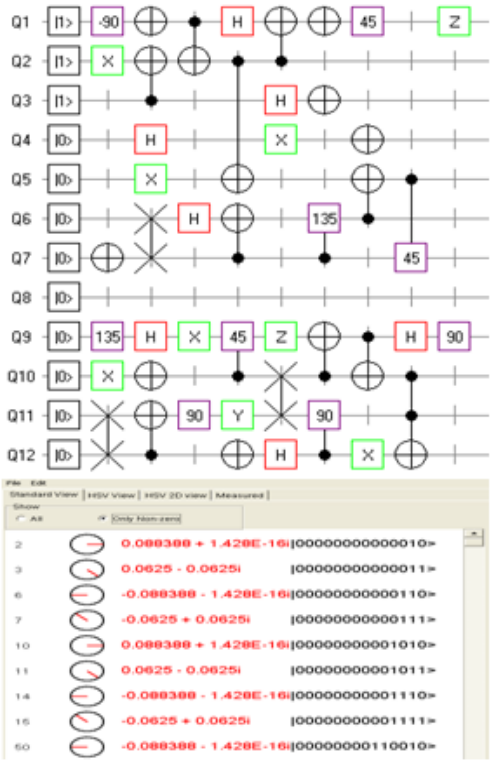

Fig. 4: Encoder output for input = 00000111 check bits input = 0000

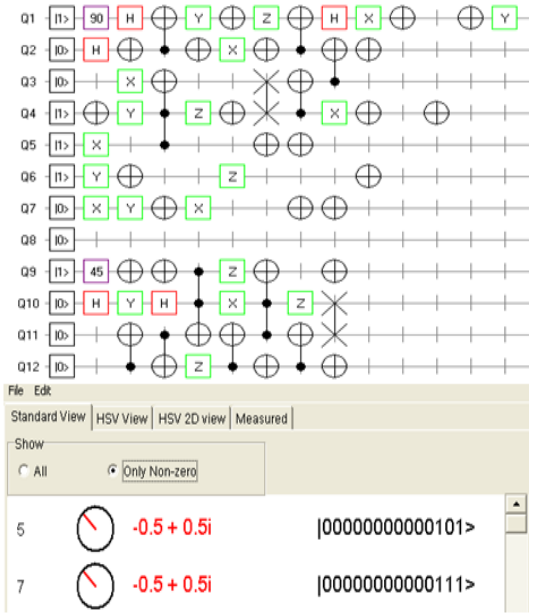

Fig. 5: Decoder output = 00000111 check bits = 00000101 for input data = 000100111001

Encoder with input data: If the channel is free of error and eves presence, the secret key is encoded using the quantum gates and transmitted. The encoded secret key is shown in the simulated result. A qubit |Q = a|0+b|1〉 encoded into an arbitrarily large amount of information (contained in its expansion coefficients a and b as shown in Fig. 4). But at most only one classical bit's worth of information in a qubit is accessible. Because to access the information stored in a qubit, it has to be measured and if it's in a superposition it collapses to either |0〉 or |1〉 , both of which only contain one classical bit of information (i.e., "0" or "1").

Decoder with check bits: It is assumed that the measured secret key from the superposition states is 0 0 0 1 0 0 1 1 1 0 0 1 and it is used as the input to the decoder as shown in Fig. 5. The decoder output is in the reverse order of the transmitted key and the check bits i.e., the decoder output will be the message data 0 0 0 0 1 1 1 and check bits data 0 1 0 1 as shown in the below Decoder output diagram.

CONCLUSION AND FUTURE SCOPE

Quantum technologies will play a very important role in the future and already to date, several companies are commercializing quantum communication systems. In the future [a quantum computer] could do all sorts of things. A quantum computer [would have] massive processing power because it can do computational tasks in parallel and can solve problems which are virtually intractable using an ordinary computer. A quantum simulator is a quantum computer which basically simulates another quantum system. This could help us simulate a new molecule or new nano material and thereby help us to design better materials in the future. Quantum computers are very good at search problems and also for finding the primes of large numbers, which is an important area for cryptography. Also this is going to be one of the great discoveries of the 21st century as these computers will use the techniques of Quantum mechanics and Quantum computing, which will provide more security to the renders for message or information sharing. The proposed method may be implemented in real time applications as it is very simple and the cost may also very less when quantum computer exists.

REFERENCES

Ali, S. and M.R.B. Wahiddin, 2010. Fiber and free-space practical decoy state QKD for both BB84 and SARG04 protocols. Eur. Phys. J. D., 60: 405-410.

Beige, A., B.G. Englert, C. Kurtsiefer and H. Weinfurter, 1999. Secure communication with a publicly known key. Acta Phys. Pol. A., 101: 357.

Bennet, C. and G. Brassard, 1984. Quantum cryptography: Public key distribution and coin tossing. Proceeding of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India, pp: 175-179.

Bennett, C., F. Bessette, G. Brassard, L. Salvail and J. Smolin, 1992. Experimental quantum cryptography. J. Cryptology, 5: 3-28.

Bostrom, K. and K. Felbinger, 2002. Deterministic secure direct communication using entanglement. Phys. Rev. Lett., 89(18): 187902.

Capmany, J., A. Ortigosa-Blanch, J. Mora, A. Ruiz-Alba, W. Amaya and A. Martinez, 2009. Analysis of subcarrier multiplexed quantum key distribution systems: Signal, intermediation and quantum bit error rate. IEEE J. Sel. Topics Quantum. Electron., 15(6): 1607-1621.

Cederlof, J. and A. Larson, 2008. Security aspects of the authentication used in quantum cryptography. IEEE T. Inform. Theory, 54(4): 1735-1741.

Deng, F.G. and G.L. Long, 2004. Secure direct communication with a quantum one-time pad. Phys. Rev. A, 69(5): 052319.

Einstein, A., B. Podolsky and N. Rosen, 1935. Can quantummechanical description of physical reality be considered complete? Phys. Rev., 47(1935): 777-780.

Godhavari, T. and N.R. Alamelu, 2011. Quantum based secure information transmission. Eur. J. Sci. Res., 66(2): 243-254.

Godhavari, T. and N.R. Alamelu, 2012. Noise deduction using quantum check bits. Int. J. Comput. Appl. Special Issue, ISSN: 0975-8887 ICCIA, No: 2.

Hutter, B. and A. Peres, 1994. Quantum cryptography with photon pairs. J. Modern Optics, 41: 2397-2403.

Justin, M., 2008. Breaking quantum cryptography in 150 kilometer. IEEE T. Spectrum, 45(9): 15-15.

Lucamarini, M. and S. Mancini, 2005. Secure deterministic communication without entanglement. Phys. Rev. Lett., 94(14): 140501.

Marinesu, D.C. and G.M. Marinesu, 2004. Approaching Quantum Computing. Prentice Hall, Upper Saddle River, NJ.

Namekata, N., S. Mori and S. Inoue, 2005. Quantum key distribution over an installed multimode optical fiber local area network. Opt. Express, 13(25): 9961-9969.

Naor, M., G. Segev and A. Smith, 2008. Tight bounds for unconditional authentication protocols in the manual channel and shared key models. IEEE T. Inform. Technol., 54(6): 2408-2425.

Nicolas, G., R. Gr´egoire, T. Wolfgang and Z. Hugo, 2007. Quantum cryptography. Submitted Rev. Modern Phys., 1/2: 55.

Nielsen, M.A. and I.L. Chuang, 2000. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge.

Paterson, K.G., F. Piper and R. Schack, 2004. Why quantum cryptography? Quantum Physics, Quant ph/0406147.

Serna, E.H., 2012. Quantum key distribution protocol with private-public key. Vol. 4, [quant-ph] arXiv:0908.2146v4.

Sharbaf, M.S., 2009. Quantum cryptography: A new generation of information technology security system. Proceeding of the IEEE 6th International Conference on Information Technology, pp: 1644-1648.

Vishal, S., 2007. Quantum Computing. Tata McGraw Hill, Delhi.

Wang, J., Q. Zhang and C.J. Tang, 2006. Quantum secure direct communication based on order rearrangement of single photons. Phys. Lett. A, 358(4): 256-258.

Wiesner, S., 1983. Conjugate coding. Sigact News, 15(1): 78-88.

Wiesner, S., 1993. Quantum cryptography with bright light. Manuscript, 1993.