International Journal of Control and Automation
Vol. 7, No. 12 (2014), pp. 11-22
http://dx.doi.org/10.14257/ijca.2014.7.12.02

Enhancement of Quantum Secret Sharing Using Exclusive-OR and Shift Operation

Kondwani Makanda and Jun-Cheol Jeon[1]

Department of Computer Engineering, Kumoh National Institute of Technology, Gumi 730-701, Korea
kmakanda@yahoo.com, jcjeon@kumoh.ac.kr

Abstract

We propose quantum secret sharing scheme that emphasizes on the cooperation (*twice*) *of communicating parties to avoid untrustworthy members and improves the strength of the key. The proposed scheme is a new approach in quantum secret sharing in which cooperation of the parties is emphasized at the same time the key is strengthened by performing a shift operation on the received partial keys. In this method, we have managed to achieve the following: security of the key is significantly enhanced; cooperation between parties is also increased* (*to two*) *and improved. This method shows that it is difficult for an eavesdropper to obtain the key easily. It is also hard for the communicating parties to cheat since key verification is done twice and if any member cheats, it can easily be identified and communication can be aborted immediately.*

Keywords: *Cryptography, quantum cryptography, quantum secret sharing*

1. Introduction

Information security is essential when two or more individuals want to transmit sensitive or secretive information; security of the information is of paramount importance. One of the important ways of securing information is by using a method called secret sharing proposed by Shamir [1]. In the method proposed by Shamir, the secret is divided into n shares for n participants, and t is used as a threshold value ($t \leq n$). It was also called a (t, n)-threshold technique which implies that at least t participants of n participants should be gathered to reconstruct the secret. Secret sharing is a method that allows an individual to share a secret to a group of people such that each person has a portion of the secret. Each person's part of the secret will be meaningless until all the individuals in the group work together to reconstruct the secret [2, 3].

Currently, most techniques in secret sharing [17-21] are implemented using the classical cryptographic methods. Classical cryptography is vulnerable to technological advancements. As computing power increases, possibilities of breaking these cryptographic algorithms also increase. The other reason is that the encryption protocols based on mathematical algorithms are vulnerable to security loopholes related to key refresh and key expansion ratio. This then results in most systems not large key-expansion rates that negatively affect the overall security of the system [4, 27]. To maintain the security of secretive information exchange, new ideas based on quantum secret sharing are being proposed. Quantum secret sharing uses the properties of quantum mechanics and classical cryptography to provide a secure method for sharing a secret [11, 14].

[1] Corresponding Author

ISSN: 2005-4297 IJCA

Quantum secret sharing is the generalization of classical secret sharing in a quantum scenario, in terms of which both the classical message and quantum information can be shared. Quantum secret sharing is likely to play a key role in protecting secret quantum information, *e.g.,* in secure operations of distributed quantum computation, sharing difficult-to-construct ancillary states and joint sharing of quantum money, *etc.*, Significant research focused on this issue theoretically and experimentally has been done. Quantum secret sharing prevents eavesdroppers from getting information about the key. It does this by breaking the key into parts allowing reconstruction to occur only with the parties working together [12].

Since Hillery, *et al.,* [22] and Cleve, *et al.,* [23] proposed the first quantum secret sharing scheme based on GHZ and mixed states in 1999, several quantum secret sharing schemes have been proposed. In 2007, Zhang, *et al.,* [28] proposed a multiparty quantum secret sharing scheme based on the concept of Bell states and local unitary operations. These were an improvement on previous schemes, as they were more efficient and more feasible. Thereafter, the Zhang, *et al.,* scheme has had numerous analyses [29-32] and improvements [29, 31] since its inception.

From a theoretical perspective, attack strategies [29-31] consist of the compound entanglement swapping attack, which includes both the intercept-and-resend and entanglement swapping schemes. However, none of them can solve the contradiction between obtaining the entire secret information and introducing no error. The attack [29] presented by Lin, *et al.,* can only obtain half of the secret without any error, while the collective attack [30] presented by Wang, *et al.,* introduces the probabilistic error, and the attack [31] presented by Gao introduces a 25% error rate [32], whereas the Wang, *et al.,* and Gao strategies can obtain the entire secret. In addition, security breach has gained significant attention [33]. Unfortunately, Zhang, *et al.,* scheme and its improvements cannot resist the attack, and therefore is not an improvement on the original strategy. Lin, *et al.,* and Gao's schemes are an improvement, as they increase the sample photon detections between the dealer and agents to improve the authentication of quantum channels. In contrast, Gao's scheme is more secure than Lin, *et al.,*'s scheme because of increasing detection capabilities between the dealer and n, the last agent, which to date has not been successfully breached.

In this paper, we propose an improvement of the quantum secret sharing method in which communication between parties is emphasized; hence, preventing any untrustworthy individuals having access to the key. There are many advantages in quantum cryptography like not being able to measure the system without disturbing it (Heisenberg Uncertainty principle) and the system not being able to be copied without being disturbed (no cloning theorem).

This paper is organized as follows; in Section II, we discuss the preliminaries of quantum cryptography where we talk about basics of quantum computing. In Section III, we provide literature review. Section IV discusses the proposed protocol. Section V talks about the security analysis and finally in Section VI, we give the concluding remarks.

2. Preliminaries

In classical computing, information is represented in terms of binary digits 0 and 1. Although, quantum computing is based on a similar approach, it uses quantum bits (qubits). Qubits have two possible states, 0 represented as |0> and 1 represented as |1>, however we can also have a superposition of both states like (1), where $|\alpha|^2 + |\beta|^2 = 1$ and α and β are complex numbers. α represents the probability of measuring 0 and β represents the probability of measuring 1. The two states |0> and |1> can also represent ground and excited states respectively [7, 8]. Figure 1 shows a qubit in a Block sphere where there are two basic states |0> and |1> and a generalization of a quantum state represented by $|\psi>$ [24].

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

Qubits can be generated and measured in two different bases, the *Z* basis (|0>, |1>) and the *X* basis (|+>, |->), where |+> = (1/√2)(|0> + |1>) and |-> = (1/√2)(|0> - |1>) [9].

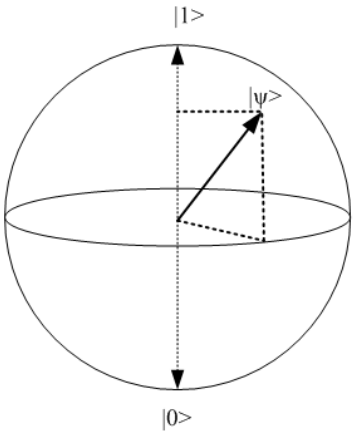

Figure 1. A Block Sphere Showing a Qubit [24]

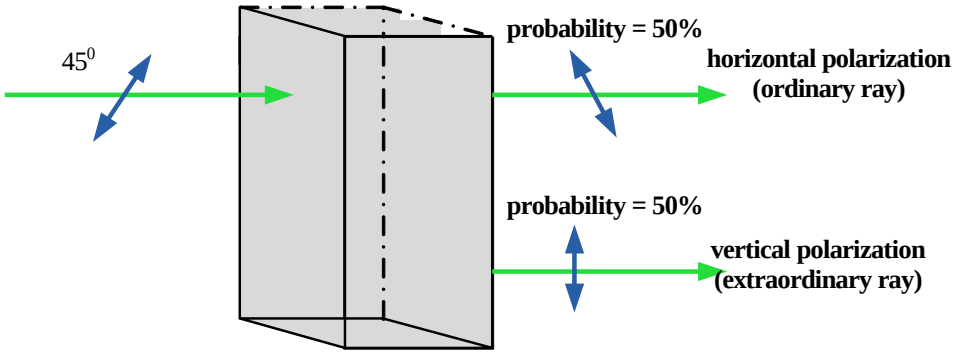

Figure 2. Wave of Polarized Light at 45^0 Entering and Existing Through a Birefringent Calcite Crystal

In quantum secret sharing, two channels are required to transmit and recover the key by all parties involved. The classical channel is used to verify whether there was an eavesdropper on the network attempting to get the key. The quantum channel is used for transmitting the qubits which are used to generate the key [5, 6].

Looking at the experiment where we have polarized photons being transmitted in a birefringent calcite crystal. A birefringent material separates a ray of light into two separate rays which are ordinary ray and an extraordinary ray. The separation depends on how light is polarized. Figure 2 shows polarized light passing through a birefringent calcite crystal material. The light is then split into vertical and horizontal polarization components at the output or extraordinary and ordinary ray respectively [6, 24, 26].

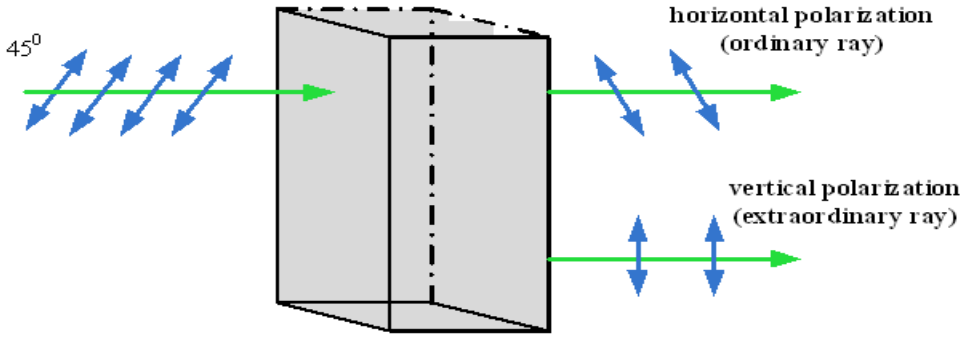

Figure 3. A Single Polarized Photon at 450 Entering and Exiting a Birefringent Calcite Crystal

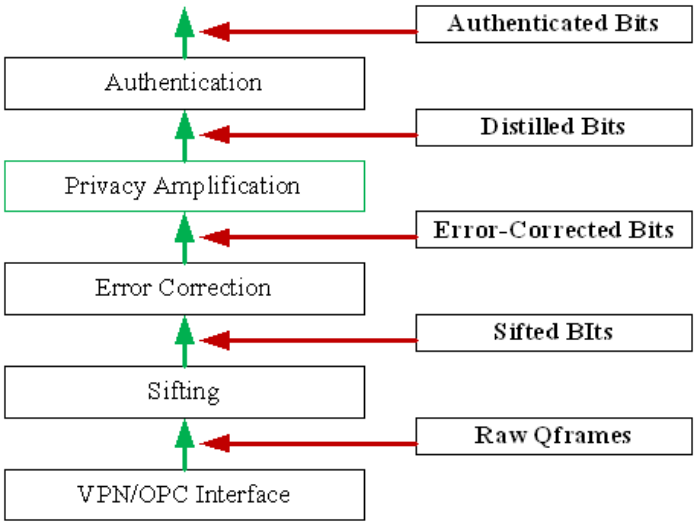

Figure 4. The QKD Protocol Implementation

Figure 3 shows an experiment with a single photon. This photon is also polarized at 45^0 and is passing through a birefringent calcite crystal. The photon cannot be simultaneously vertical and horizontal at the output side. The output will be one of the polarizations with a probability of 50% [6, 24].

Figure 4 gives a general overview of the Quantum key distribution (QKD) protocol as explained in [27]. The Figure shows each step and the output at each step of the process. The Virtual Private Net (VPN)/Optical Process Control (OPC) are where the actual transmission of the qubits takes place. The output of this process is the raw Qframes. These Qframes are the taken to the sifting stage.

The sifting stage allows the sifting of the raw Qframes to allow the removal of bits that have been detected in the wrong basis. This gives the communicating parties to reconcile their secret bits. The output of this stage is the sifted bits.

After getting the sifted bits, the next stage is the error correction stage. The error detection and correction allows the communicating parties to find all the errors in the sifted bits and correct them. This allows the parties to estimate the quantum bit error rate (QBER) on the channel. This stage results in error corrected bits as the output.

After correcting all the errors in the bits, the next stage is the privacy amplification. At this stage, the communicating parties try to reduce the eavesdropper's knowledge of the shared bits to a level that is acceptable.

The final process is that of authentication. Authentication allows parties to prevent against masquerading attacks. This makes sure that the communication parties are really the intended parties [27].

3. Literature Review

Many quantum secret sharing schemes have been proposed. Several of these schemes are based on the entanglement. One example is the one proposed by Ekert which was based on the entanglement of Einstein-Podolsky-Rosen (EPR) pair [13, 15].

In [16], they presented a quantum secret sharing scheme based on the Grover's algorithm where they studied the Hsu protocol.

In [7], they presented a multi-party quantum secret sharing protocol where they emphasized on covertness and steganography. In steganography, Alice selects one secret qubit/bit which is used to check if the communication has been compromised or not.

Table 1. Coding Qubits in the Basis States [7]

m	0		1	
a	0	1	0	1
bc	00	01	00	10
	11	10	11	01
BC	|0>|0>	|0>|1>	|+>|+>	|->|+>
	|1>|1>	|1>|0>	|->|->	|+>|->

In this section, we consider the quantum secret sharing scheme proposed by Guo, *et al.*, as it was presented in [7]. This protocol does not require quantum entanglement to be carried out.

(a) Alice generates two random 2*n*-bit strings $l = (l_1, l_2, l_{3,\ldots}, l_{2n})$ and $a=(a_1,a_2,a_3\ldots,a_{2n})$. For each bit of *l* and *a*, she creates qubits B_i and C_i in the Z basis (if $l_i = 0$) or X basis (if $l_i = 1$), where $b_i \oplus c_i = a_i$. In Table 1, a summary of coding the qubits to corresponding bases is given. Alice knows exactly which pair of qubits she prepares. She sends 2*n*-qubit strings $B = (B_1, B_2,\ldots, B_{2n})$ and $C = (C_1, C_2,\ldots, C_{2n})$ to Bob and Charlie, respectively.

(b) When both Bob and Charlie announce that they have received their strings, Alice announces *l*. Bob and Charlie measure each qubit in the Z basis or X basis according to the corresponding bit value of *l*.

(c) Alice randomly selects *n* check bits in *a*. Bob and Charlie are required to announce the measurement results of their corresponding check qubits in *B* and *C*.

(d) If Alice finds the number of agreed values is unacceptably low, she aborts this run and restarts from step (a). Otherwise, she continues to the next step.

(e) They perform information reconciliation and privacy amplification to generate three m-bit keys k_a, k_b and k_c from the remaining n bits. Alice, Bob and Charlie can obtain k_a, k_b and k_c separately, where $k_a = k_b \oplus k_c$.

4. Proposed Protocol

Quantum key distribution is used to distribute the key and not to transfer any information. This is used to distribute the key for symmetric ciphers [6]. In this section, we will look at the method proposed in [3]. Suppose that Bob cheats during the XOR operation in order to get Charlie's key. Then Charlie will not be able to know that Bob has cheated and that he has managed to get Alice's without Bob's cooperation. To avoid this problem, we implement a new method for key sharing. This method requires Bob and Charlie to cooperate twice, such that if one person cheats in the first part of the process, it can easily be discovered and communication stopped without giving away the key. It can also be extended to more parties (multi-party) without increasing the computation complexity of the whole system.

The proposed scheme is a modification of the protocol presented in [3]. The protocol is outlined below:

(a) Alice generates two random $2n$-bit strings m= (m_1,m_2,m_3,…,m_{2n}) and a=(a_1,a_2,a_3,….,a_{2n}). For each bit of m and a, she creates qubits B_i and C_i in the Z basis (if l_i =0) or X basis (if l_i = 1), where $b_i \oplus c_i = h_i$. She sends $2n$-qubit strings B = (B_1, B_2,…, B_{2n}) and C = (C_1, C_2,…, C_{2n}) to Bob and Charlie, respectively. Alice knows which pairs she has prepared and sent to Bob and Charlie.

(b) When both Bob and Charlie announce that they have received their strings, Alice announces m. Bob and Charlie measure each qubit in the Z basis or X basis according to the corresponding bit value of m.

(c) Alice randomly selects n check bits in a. Bob and Charlie are required to announce the measurement results of their corresponding check qubits in B and C.

(d) If Alice finds the number of agreed values is unacceptably low, she aborts this run and restarts from step (a). Otherwise, she continues to the next step.

(e) Bob and Charlie perform an XOR operation of their check qubits to get an intermediate key h_i.

(f) From the remaining n-bits of h_i, she performs a left cyclic shift of h_i such that the shift is equal to or greater than one but less than n ($1 \leq h_i < n$). Alice does not tell Bob or Charlie in advance how many bits they are supposed to do a left cyclic shift on and this adds to the strength of the key.

(g) She then performs an XOR operation between b_i and h_i as well as c_i and h_i to get new strings bh_i and ch_i.

(h) Alice's key is now obtained by performing an XOR operation between Bob's key (bh_i) and Charlie's key (ch_i) i.e. $bh_i \oplus ch_i = a_i$.

Figure 5 shows steps (g) and (h) from the proposed protocol. After performing a left cyclic shift of the intermediary key (hi) in step (f), the two parties can now individually obtain their keys by performing an XOR of their individual keys (b_i and c_i) with h_i. To obtain Alice's key, the two individuals now have to work together by performing an XOR operation again so that Alice's key can be obtained. A simple example of the protocol is given in Table 2 where m = 1011011110100110 and k = 0010110110010010.

Table 2. An Example of Quantum Key Distribution (Assumption is that it is a Perfect System such that no Error Correction was done and the Communicating Parties know each other)

	Bob's qubits: |+>|1>|+>|+>|1> |->|+>|+>|+>|0>|->|0>|0>|+>|->|1>	Charlie's qubits: |+>|1>|->|+>|0> |+>|+>|->|->|0>|->|1>|0>|+>|+>|1>
Alice selects *n* check qubits (equivalent to *)	B=|+>*|+>**|->|+>***|->|0>*|+>|->* Bob's Qubits =|+>|+>|->|+>|->|0>|+>|->	C = |+>*|->**|+>|+>***|->|1>*|+>|+>* Charlie's qubits = |+>|->|+>|+>|->|1>|+>|+>
The *n*-check qubits (equal to h_i)	h_b = |1>|+>|1>|+>|+>|0>|0>|1>	h_c = |1>|+>|0>|->|->|0>|0>|1>
Bits after $h_i=h_b \oplus h_c$	00111000	
Performs a left cyc shift (by three shifts this example)	11000001	
Performs $b \oplus h$ a also $c \oplus h$ to get session keys	00010011	01110110
Performs $bh \oplus ch$ to get Alice's key	01100101	

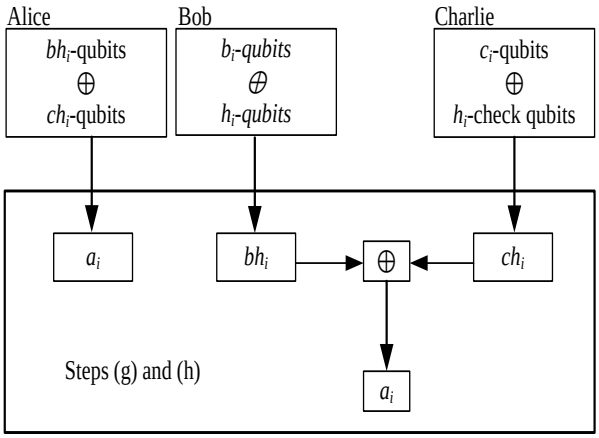

Figure 5. The Steps (g) and (h) from the Proposed Protocol

5. Security Analysis and Discussion

The security of this method depends on a number of factors that include the following:

If one of the Bob, Charlie pair is untrustworthy, then he can easily be identified in the first XOR operation because they will get a different h value. This will result in the communication being terminated without wasting a lot of resources. Even if there was an eavesdropper, they will be discovered in the first phase of the XOR operation. This is an

improvement of the method proposed in [7] that only used one XOR operation in their protocol.

The other main advantage of the proposed method is that the shift operation helps to strengthen the key. This is because the shift amount is only known by Alice alone. This shift operation is used in privacy amplification. Hence, even if an eavesdropper or a member of the Bob/Charlie pair tries to cheat, they will not be able to get the key without the knowledge of the shift amount until Alice tells them. This will give Alice a chance to calculate the values received by Bob and Charlie to determine if they will obtain the same key as her's. It is advantageous because Alice can discover the untrustworthy member in the pair. This can also be extended in a situation where there are many parties in the scheme.

Cooperation of the communicating parties is also emphasized. This is done by making sure that the parties perform an XOR twice so that if one cheats in the first operation he can be detected.

One of the most important properties of quantum cryptography is the no cloning theorem which says that a state cannot be copied and this also applies to this protocol. Using the Heisenberg Uncertainty principle, which states that it is not possible to measure the quantum state of a system without disturbing it, an attacker can easily be detected by the communicating parties once he/she attempts to eavesdrop. The protocol is also easy to extend to multi-parties as [3] explained. By putting an additional XOR operation and the shift operation, we managed to theoretically improve the security of this protocol in comparison to [3].

The other important measure of the proposed scheme is the qubit efficiency. According to [25], methods (3) and (4) are used to measure the qubit efficiency of the protocol where q_u denotes the useful qubits, q_t denotes the total number of transmitted qubits and lastly c_t represents the bit length for classical information (apart from the information for eavesdropping check) [25]. Using equation (3), our proposed scheme is also 100% because the useful qubits transmitted to Bob are 2*n* and also the useful qubits transmitted to Charlie are 2*n*. Total number of transmitted in our case is 4*n* (2*n* to Bob and 2*n* to Charlie) which makes the proposed method to have a 100% qubit efficiency. Using equation (4), the qubit efficiency is at 66.67% since the $c_t + q_t$ is equal to 6*n*.

$$\eta_q = \frac{q_u}{q_t} \tag{3}$$

$$\eta_t = \frac{q_u}{q_t + c_t} \tag{4}$$

From Table 2, our proposed method requires authentication whereas the scheme proposed in [3] does not have an authentication mechanism in it. Both methods require quantum transmission for transmitting qubits. Similarly, the proposed methods use the classical channel for key verification to find if there are eavesdroppers trying to get information about the key.

In terms of secrecy enhancement, our proposed method is very high because to the following reasons:

1. The use of the *n*-check qubits as part of the key helps to amplify the secrecy of the key.

2. The shift operation applied to the check qubits amplifies the key secrecy since the shift amount is not made available to communicating parties such that an eavesdropper cannot know about this amount.

The other parameter which is very important is the verification of the key. In our proposed method, the verification is done twice. The first is during the first XOR operation. If the values after performing the first XOR operation are different then Alice can abort this step even since her values of the first XOR operation are different. The second verification is done during the second XOR operation. All these steps help to prevent an eavesdropper from getting the key.

In all the two protocols, key distribution can be discarded in the middle of process once an eavesdropper has been discovered. This is an advantage because the key will not be disclosed before up until the whole process is finalized.

Our proposed method has more steps (8 in total) needed to be taken in order to complete the whole process than the protocol proposed in [3] which has 5 steps. A summary of all the comparison parameters between our proposal and the method propose in [3] are given in Table 3. These parameters were used in [10] for comparison as well.

Table 3. Comparison of Proposed Method with the One Proposed in [3]

Properties	Proposed Method	Proposed in [3]
Authentication	√	√
Quantum transmission	√	√
Secrecy Enhancement	Very high	High
Decision on Continuation	√	√
Steps required	8	5
Double verification of key	Yes	No
Time needed to Generate Key	More	Less
Ability to discard process in the middle	√	√
Difficult to bypass	Yes	No
Attacker is detected before key generation and distribution	√	√
Use of classical channel	More	Less

6. Conclusions

In this paper, we proposed a quantum secret sharing scheme that encourages parties to cooperate. In addition, the security of the key is enhanced by using a secret shift operation of the intermediate key *h*. This improves the secrecy of the key in the proposed method as compared to the other methods. The proposed method has a number of advantages which including the following; the scheme is easily scalable; this is because as the number of parties increase, the complexity of the system will not increase highly. If the numbers of the parties increase, the security of the key also increases, because of the many XOR operations conducted. The use of the shift operation on the intermediate key (*h*) is also an addition to the security of the key. If one member of the Bob-Charlie pair cheats during the first XOR

operation, he can easily be detected because they will get a different h result and this can alert Alice to abort the communication.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning (2011-0014977).

References

[1] A. Shamir, "How to share a secret", Communications of the ACM. vol. 22, no. 11, **(1979)**, pp. 612-613.
[2] H.-Y. Jia, Q.-Y. Wen, F. Gao, S.-J. Qin and F.-Z. Guo, "Dynamic quantum secret sharing", Physics Letters A. vol. 376, **(2012)**, pp. 1035-1041.
[3] G.-C. Guo, "Quantum secret sharing without entanglement", Physics Letters A. vol. 310, **(2003)**, pp. 247-251.
[4] M. S. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System", Proceedings of the 6th IEEE International Conference on Information Technology: New Generations, **(2009)**, pp. 1644-1648.
[5] A. Sharma, V. Ojha and S. K. Lenka, "Security of entanglement based version of BB84 protocol for Quantum Cryptography", Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology, vol. 9, **(2010)**, pp. 615-619.
[6] M. Niemiec and A. R. Pach, "Management of Security in Quantum Cryptography", IEEE Communications Magazine. vol. 51, no. 8 **(2013)**, pp. 36-41.
[7] X. Liao, Q. Y. Wen, Y. Sun and J. Zhang, "Multi-party covert communication with steganography and quantum secret sharing", Journal of Systems and Software. vol. 83, no. 10 **(2010)**, pp. 1801-1804.
[8] A. Krishnan, An overview of Quantum Wireless Communication using Quantum Cryptography, Proceedings of the 2010 International Conference on Emerging Trends in Robotics and Communication Technologies. **(2010)**, pp. 100-103.
[9] F. Gao, S. J. Qin, F. Z. Guo, and Q. Y. Wen, "Dense-Coding Attack on Three-Party Quantum Key Distribution Protocols," IEEE Journal of Quantum Electronics, vol. 47, **(2011)**, pp. 630-635.
[10] R. D. Sharma. A. De, "A new secure model for quantum key distribution protocol", Proceedings of 6th IEEE International Conference on Industrial and Information Systems (ICIIS), **(2011)**, pp. 462-466.
[11] M. Khorrampanah and M. Houshmand, "An Efficient Quantum Secret Sharing using Secure Direct Communication", Proceedings of Iranian Conference on Electrical Engineering (ICEE), **(2013)**, pp. 1-5.
[12] L. Yanyan and X. Chengqian, "Three-party Quantum Secret Sharing based on Secure Direct Communication", Proceedings of International Forum on Information Technology and Applications (IFITA), **(2009)**, pp. 126-130.
[13] Y. H. Chou, R. K. Fan, S. M. Chen, C. Y. Chen and H. C. Chao "Enhanced Multiparty Quantum Secret Sharing of Classical Messages based on Entanglement Swapping", Proceedings of IET International Conference on Technologies and Applications, **(2010)**, pp. 269-274.
[14] C. S. Moon and S. H. Kim, "A Study on the Integrated Security System based Real-time Network Packet Deep Inspection", International Journal of Security and Its Applications, **(2014)**, pp. 113-122.
[15] H. Ma and B. Chen, "Quantum network based on multiparty quantum secret sharing", Proceedings of Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, **(2007)**, pp. 347-351.
[16] Z. Sakhi, A. Tragha, R. Kabil and M. Bennai, "Quantum Cryptography based on Grover's Algorithm", Proceedings of Second International Conference on Innovative Computing Technology (INTECH), **(2012)**, pp. 33-37.
[17] N. Pakniat, M. Noroozi, and Z. Eslami, "Secret image sharing scheme with hierarchical threshold access structure," Journal of Visual Communication and Image Representation, vol. 25, no. 5, **(2014)**, pp. 1093-1101.
[18] S.-F. Tu and C.-S. Hsu, "Protecting secret documents via a sharing and hiding scheme," Information Sciences, vol. 279, **(2014)**, pp. 52-59.
[19] D. Ou, and W. Sun, "Reversible AMBTC-based secret sharing scheme with abilities of two decryptions," Journal of Visual Communication and Image Representation, vol. 25, no. 5, **(2014)**, pp. 1222-1239.
[20] G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," Computers and security, vol. 30, no. 5, **(2011)**, pp. 320-331.
[21] J. S. Lee and M. H. Hsieh, "An interactive mobile SMS confirmation method using secret sharing technique," Computers and Security, vol. 30, no. 8, **(2011)**, pp. 830-839.

[22] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," Physical Review A, vol. 59, no. 3, **(1999)**, pp. 1829-1834.
[23] R. Cleve, D. Gottesman, and H. K. Lo, "How to share a quantum secret," Physical Review Letters, vol. 83, no. 3, **(1999)**, pp. 648-651.
[24] M. Niemiec, "Design, Construction and Verification of a High-Level Security Protocol Allow to Apply the quantum cryptography in communication networks," http://winntbg.bg.agh.edu.pl/rozprawy2/10409/full10409.pdf.
[25] J. Lin and T. Hwang, An enhanced on Shi, *et al.*,'s multiparty quantum secret sharing protocol, Optics Communications, vol. 284, no. 5, **(2011)**, pp 1468-1471.
[26] R. S. Vignesh, S. Sudharssun and K. J. J. Kumar, "Limitations of Quantum & The Versatility of Classical Cryptography A Comparative Study," Proceedings of Second International Conference on Environmental and Computer Science, **(2009)**, pp. 333-337.
[27] M. S. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System," Proceedings of Sixth International Conference on Information Technology: New Generations (ITNG), **(2009)**, pp. 1644 - 1648.
[28] Z.-J. Zhang, G. Gao, X. Wang, L.-F. Han and S.-H. Shi, "Multiparty quantum secret sharing based on the improved Boström–Felbinger protocol," Optics Communications, vol. 269, no. 2, **(2007)**, pp. 418-422.
[29] S. Lin, Q.-Y. Wen, F. Gao and F.-C. Zhu, "Improving the security of multiparty quantum secret sharing based on the improved Boström–Felbinger protocol," Optics Communications, vol. 281, no. 17, **(2008)**, pp. 4553-4554.
[30] T.-Y. Wang, Q.-Y. Wen, F. Gao, S. Lin and F.-C. Zhu, "Cryptanalysis and improvement of multiparty quantum secret sharing schemes," Physics Letters A, vol. 373, no. 1, **(2008),** pp. 65-68.
[31] G. Gao, "Eavesdropping on the improved three-party quantum secret sharing protocol, Optics Communications," vol. 284, no. 3, **(2011)**, pp. 902-9040.
[32] T.-Y. Wang and Q.-Y. Wen, "Comment on Eavesdropping on the improved three-party quantum secret sharing protocol", Optics Communications, vol. 284, no. 14, **(2011)**, pp. 3664-3666.
[33] Y.-G. Yang, Y.-W. Teng, H.-P. Chai and Q.-Y. Wen, "Verifiable Quantum (k,n)-threshold Secret Key Sharing," International Journal of Theoretical Physics, vol. 50, no. 3, **(2010)**, pp. 792-798.

