International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.293-302
http://dx.doi.org/10.14257/ijsia.2015.9.8.26

Fundamental Two-Party Quantum Secret Sharing Protocol without Quantum Entanglement

Jun-Cheol Jeon

Department of Computer Engineering, Kumoh National Institute of Technology
61, Daehak-ro, Gumi, Gyeongbuk 730-701, Korea
jcjeon@kumoh.ac.kr

Abstract

Quantum key distribution (QKD) protocol techniques are used in the distribution of keys using the laws of physics. Quantum secret sharing (QSS), quantum secure direct communication, and quantum teleportation, which are all included under QKD, are used to share or distribute a secure key in a quantum environment. In QSS, we share a key based on the quantum properties of light. We emphasize cooperation between communicating parties to eliminate untrustworthy members and to improve the strength of the key. The results obtained showed that using the proposed method, it is difficult for eavesdroppers to obtain the key.

Keywords: *Quantum information, Quantum communication, Quantum key distribution, Quantum secret sharing*

1. Introduction

Conventional cryptosystems such as ENIGMA, DES, or even RSA, are based on a mixture of guess-work and mathematics. Information theory shows that traditional secret-key cryptosystems cannot be totally secure unless the key, used once only, is at least as long as the cleartext. On the other hand, the theory of computational complexity is not yet well enough understood to prove the computational security of public-key cryptosystems [1].

In traditional public-key cryptography, trapdoor functions are used to conceal the meaning of messages between two users from a passive eavesdropper, despite the lack of any initial shared secret information between the two users. In quantum public key distribution, the quantum channel is not used directly to send meaningful messages, but is rather used to transmit a supply of random bits between two users who share no secret information initially, in such a way that the users, by subsequent consultation over an ordinary ono-quantum channel subject to passive eavesdropping, can tell with high probability whether the original quantum transmission has been disturbed in transit, as it would be by an eavesdropper (it is the quantum channel's peculiar virtue to compel eavesdropping to be active). If the transmission has not been disturbed, they agree to use these shared secret bits in the well- known way as a one-time pad to conceal the meaning of subsequent meaningful communications, or for other cryptographic applications. If transmission has been disturbed, they discard it and try again, deferring any meaningful communications until they have succeeded in transmitting enough random bits through the quantum channel to serve as an on-time pad [1].

Key distribution is the term applied to techniques allowing two parities to acquire a random bit sequence with a high level of confidence that no one else knows it or has significant partial information about it. One party might generate the key by a physically random process, make a copy of it, and hand deliver the copy to the other party. Such shared secret key bits, although random and meaningless in themselves, are a valuable resource because they allow the communicating parties to achieve, with provable security,

ISSN: 1738-9976 IJSIA

two of the main goals of cryptography: encrypting a subsequent meaningful message to make it unintelligible to a third party [2], and certifying to the legitimate receiver that a message has not been altered in transit [3].

The ability to secure information has been a key objective for many years, and is necessary to prevent the unwanted access by individuals. Suppose Alice, who is the head of a bank, wants an action to be taken on her behalf by two individuals, Bob and Charlie. Alice knows that one of the two individuals is untrustworthy. Therefore, she has to make sure that the untrustworthy individual is not the only one to receive her message, but if both individuals work together, they should be able to receive Alice's message.

One of the techniques used to secure information is secret sharing, which was first proposed independently by Shamir [4] and Blakley [5]. In a (*k*, *n*)-threshold secret-sharing scheme [6], any *k* shares can decrypt a key, but if there are *k*-1 or fewer shares, the information cannot be decrypted. In a similar manner, if *n*-*k* shares are lost, the secret can still be recovered. If an adversary has *k*-1 shares, he/she will not be able to obtain any information about the secret. A similar analogy exists in quantum computing or quantum information processing, and is called quantum secret sharing (QSS), which was proposed in [7, 8].

Most secret-sharing techniques that are currently used rely on classical cryptography to ensure secure message transmission. However, these schemes are vulnerable to technological advancements, which can result in the schemes becoming broken as computational power increases. These schemes are also vulnerable to eavesdropping, and the parties involved in the communication may not be aware that eavesdropping is taking place [9].

QSS, which was first proposed in [7], is a generalization of classical secret sharing, and can be used to distribute both classical messages and quantum information. When QSS is fully realized, it is likely to play a key role in protecting secret quantum information. This may include the secure operations of distributed quantum computation, sharing difficult to construct ancillary states, and the joint sharing of quantum money, among many more applications. There has been a significant amount of research focus on QSS from both a theoretical and experimental perspective. QSS prevents eavesdroppers from obtaining information about the key. It does this by breaking the key into parts, and allowing reconstruction to occur only with the parties working together. There is also a need to check for eavesdroppers during the process [10].

The paper is organized as follows; section 2 gives the related studies including quantum properties and literatures review. Section 3 discusses the proposed quantum secret sharing protocol, section 4 gives a security analysis of our protocol and finally section 5 gives the conclusions.

2. Related Studies

This section shortly mentions the concept of a quantum bit, quantum entanglement, quantum key distribution and typical protocols.

2.1. Quantum Bits

Classical computing represents information in terms of two binary digits, 0 and 1. In quantum computing, there is a similar analogy, which is called a quantum bit or qubit. Qubits can be represented using the Dirac notation. $|0\rangle$ represents bit 0 and $|1\rangle$ represents bit 1, where $|\rangle$ is called "ket". However, a qubit can also exist as a superposition of both states, and this is represented as

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

where $|\alpha|^2 + |\beta|^2 = 1$, and α and β are complex numbers. α represents the probability of measuring a 0, while β represents the probability of measuring a 1. The two qubits $|0\rangle$ and $|1\rangle$ can be represented using ground and excited states, respectively [11]. Qubits can be

generated and measured in two different bases. The Z basis is represented as |0> and |1>, and the other basis is the X basis, which is represented as |+> = 1/(√ 2) (|0>+|1>) and |-> = 1/(√ 2) (|0>-|1>) [12].

Figure 1 shows a qubit in a block sphere, where the two basic states |0> and |1> and a generalization of a quantum superposition state are represented by |ψ> [13].

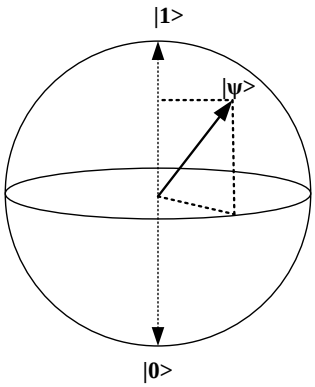

Figure 1. Block sphere representation of a qubit

2.2. Quantum entanglement

In quantum mechanics, quantum entanglement is an important re-source, as well as quantum information processing. It can be implemented in different disciplines such as quantum teleportation and quantum cryptography [14]. In a perfectly correlated quantum entanglement system, one can determine the state of the one qubit once its entangled counterpart has been determined (e.g., a two-qubit system in this case). The examples of a two qubit maximally entangled system are the Bell basis [15]:

$$\begin{aligned} |\Phi^{+}> &= 1/\sqrt{2}\,(|00> + |11>) \\ |\Phi^{-}> &= 1/\sqrt{2}\,(|00> - |11>) \\ |\Psi^{+}> &= 1/\sqrt{2}\,(|01> + |10>) \\ |\Psi^{-}> &= 1/\sqrt{2}\,(|01> - |10>) \end{aligned} \tag{2}$$

For example, in a two-qubit Bell basis (1/√ 2(|00>+|11>)) that is perfectly entangled, assume that two individuals, A and B, share the sys-tem. If A measures the system, then the probability of the system col-lapsing to |0> is 50%. This will let A know that the B's qubit must col-lapse to |0>. Similarly, if the result of A's measurement collapses to |1>, then A will immediately know that B's qubit is |1> with a probability of 50%. This means that in a perfectly correlated quantum system, if the state of one qubit is known, then it is easy to determine the state of the other qubit. This happens regardless of the distance between the two qubits [15, 16].

2.3. Quantum Key Distribution

Charles H. Bennett and Gilles Brassard were the first individuals to introduce quantum key distribution (QKD) in 1984 [1]. QKD uses quantum mechanics to guarantee the security of the secret key. QKD also uses a one-time pad (Vernam cipher) to provide an unconditional secure encryption [17]. The fundamental aim of the QKD protocol is not to use the quantum states directly to share secret information, but to use the quantum states to generate a secret cryptographic key that will be shared among the communicating parties [18].

In general, QKD can be summarized into three phases, the bit-transmission phase, the channel-estimation phase, and the post-processing phase. During bit transmission, the bits

are transmitted between the communicating parties. During channel estimation, the communicating parties estimate the channel and the amount of information that has been leaked to an adversary. The final step is the post-processing phase, where the parties share the secret key depending on the bit sequence used in the bit-transmission phase [19].

QKD systems require the use of dedicated fiber optic cable because QKD is very sensitive to noise and losses. Noise and losses affect the overall performance of the system, so it is very important for them to be minimized [20].

Although QKD shows promising signs of providing unconditional secure key distribution, it still has problems such as low key-generation speeds, costly equipment for key generation, and short transmission distances compared to currently used technologies [21]. It has been reported that there are two important problems that need to be considered in order to achieve high speed QKD systems. These are the key-distillation step (i.e., sifting, privacy amplification, error correction frame synchronization, and random permutation) and the photon-transmission step. Fig. 6 shows an example of a QKD transmission [21].

2.4. BB84 and B92 Protocols

The first QKD protocol was introduced in 1984 which is called BB84 protocol [1]. This protocol uses two polarization bases with four states, rectilinear basis(R basis) and diagonal basis (D basis) which are corresponding to the mentioned Z and X bases, respectively. The next protocol which was proposed in [1] also uses two polarization bases but two states. In these protocols, a single photon may be polarized with four states: $|h\rangle$, $|v\rangle$, $|l\rangle$ and $|r\rangle$. The states $|h\rangle$ and $|v\rangle$ in R basis reveal ‘0’ and ‘1’, and the states $|l\rangle$ and $|r\rangle$ in D basis reveal ‘0’ and ‘1’, respectively [22].

2.4.1. BB84

1) Alice sends a random sequence of photons, one of $|h\rangle$, $|v\rangle$, $|l\rangle$ and $|r\rangle$.
2) Bob randomly chooses his detector basis from R basis or D basis to measure each photon.
3) Results of Bob’s measurement. Then, the states are interpreted as a binary sequence.
4) Bob reports his detector bases for each photon.
5) Alice tells Bob which bases were correct
6) Finally, Alice and Bob will share the bits where A’s response is ‘Y’, discarding all other bits.

Table 1. 12-bit Sample of BB84 Protocol

Sequence of bits		1	2	3	4	5	6	7	8	9	10	11	12
(1)	A’s random bits	1	1	0	0	1	0	1	0	0	0	1	1
	A’s source basis	D	R	R	R	D	D	R	D	R	D	R	D
	A’s polarization	$\|r\rangle$	$\|v\rangle$	$\|h\rangle$	$\|h\rangle$	$\|r\rangle$	$\|l\rangle$	$\|v\rangle$	$\|l\rangle$	$\|h\rangle$	$\|l\rangle$	$\|v\rangle$	$\|r\rangle$
(2)	B’s detector basis	D	D	R	R	R	R	R	D	D	R	D	D
(3)	B’s measurement	$\|r\rangle$	$\|l\rangle$	$\|h\rangle$	$\|h\rangle$	$\|h\rangle$	$\|v\rangle$	$\|v\rangle$	$\|l\rangle$	$\|l\rangle$	$\|v\rangle$	$\|r\rangle$	$\|r\rangle$
	B’s bits	1	0	0	0	0	1	1	0	0	1	1	1
(4)	B reports basis	D	D	R	R	R	R	R	D	D	R	D	D
(5)	A’s response	Y	N	Y	Y	N	N	Y	Y	N	N	N	Y
(6)	Shared secret key	1	-	0	0	-	-	1	0	-	-	-	1

2.4.2. B92

1) Alice sends a random sequence of photons, one of $|h\rangle$ and $|r\rangle$.
2) Bob randomly chooses his detector basis from $|l\rangle$ basis or $|v\rangle$ basis to measure each photon, and bases are interpreted as a binary sequence.
3) Results of Bob's measurement. Alice and Bob will share the bits where the measurement results are 'Y', discarding all other bits.

Table 2. 12-bit Sample of B92 Protocol

Sequence of bits		1	2	3	4	5	6	7	8	9	10	11	12
(1)	A's bits	1	1	0	0	1	0	1	0	0	0	1	1
	A's polarization	$\|r\rangle$	$\|r\rangle$	$\|h\rangle$	$\|h\rangle$	$\|r\rangle$	$\|h\rangle$	$\|r\rangle$	$\|h\rangle$	$\|h\rangle$	$\|h\rangle$	$\|r\rangle$	$\|r\rangle$
(2)	B's detector basis	$\|l\rangle$	$\|v\rangle$	$\|l\rangle$	$\|v\rangle$	$\|l\rangle$	$\|l\rangle$	$\|l\rangle$	$\|v\rangle$	$\|l\rangle$	$\|l\rangle$	$\|v\rangle$	$\|l\rangle$
	B's bits	0	1	0	1	0	0	0	1	0	0	1	0
(3)	B's measurement	N	Y	N	N	N	Y	N	N	Y	N	N	N
	Shared secret key	-	1	-	-	-	0	-	-	0	-	-	-

2.5. Liao *et al.'s* Protocol

In [11], they proposed a quantum secret sharing protocol where they used a bit for steganographic purposes. This bit is used to hide information that an outside observer will not notice that covert communication is taking place. First, Alice generates two random $2n$-bit strings $l = (l_1, l_2,\ldots,l_{2n})$ and $a = (a_1, a_2,\ldots,a_{2n})$. She randomly selects a "steganographic bit" a_q ($1 \le q \le 2n$) whose value equals to the XOR result of Alice's secret bit s and r. $a_q = s \oplus r$.

Table 3. Coding Qubits in the Corresponding Basis

l	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>	|->|->	|+>|->

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 $a_i = b_i \oplus c_i$. Alice sends $2n$-qubit strings $B = (B_1, B_2, \ldots, B_{2n})$ and $C = (C_1, C_2,\ldots, C_{2n})$ to Bob and Charlie, respectively.

1) 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.
2) Alice will select n check bits in a. The first n-1 check bits from the $2n$-1 bits (a_q is excluded from the original $2n$ bits) are randomly selected, while the last one is chosen intentionally. Suppose the remaining n+1 bits are $v = (v_0, v_1, v_2,\ldots, v_n)$ and the "steganographic bit" is v_t (i.e. a_q in a). The last check bit v_x is chosen such that $x = (t\text{-}d) \bmod (n+1)$ Bob and Charlie are required to announce the measurement results of their corresponding check qubits in B and C.
3) If Alice finds the number of agreed values is unacceptably few, she aborts this run and restarts from step 1. Otherwise, she continues to the next step.

4) 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 $k_a = k_b \oplus k_c$.

3. Proposed Protocol

We presented a QSS protocol between two parties. Our protocol does not depend on quantum entanglement, which is used in most QSS protocols; these protocols directly encode the qubits, making them easy to realize and implement. Authentication is done before the parties can start the process. This is done to prevent unauthorized individuals from masquerading and taking part in the key-sharing process [23].

This two-party quantum secret-sharing protocol is described as the basis for the other protocols, where the number of users exceeds two. Suppose we have two individuals, Alice and Bob. Let Alice be the one to initiate the whole process.

1) Alice generates two random 2l-bit strings $m = (m_1, m_2, \dots, m_{2l})$ and $n = (n_1, n_2, \dots, n_{2l})$. For each bit of m and n, Alice creates qubits B_i in the Z basis (if $m_i = 0$) or X basis (if $m_i = 1$), where $b_i = n_i$, and sends 2l-qubit strings $B = (B_1, B_2, \dots, B_{2l})$ to Bob.
2) When Bob announces that he has received the qubit string, Alice announces m. Bob measures each qubit in Z basis or X basis according to the corresponding bit value of m.
3) Bob will then recover the corresponding bit values from the qubits. Alice randomly selects l check bits in n.
4) Bob announces his results to Alice. Alice then compares the result with that of Bob. If Alice finds that the number of agreed values is unacceptably small, this run is aborted and restarted from step 1. Otherwise, two parties recognize the shift amount which is already compromised by the number of the shared secret bits so that shift the result to the right or left as promised, and Alice continues to the next step.
5) They perform information reconciliation and privacy amplification to generate a shared key, k_a and k_b, from the remaining n bits.

Figure 2 illustrates the proposed two party protocol based on shift operation.

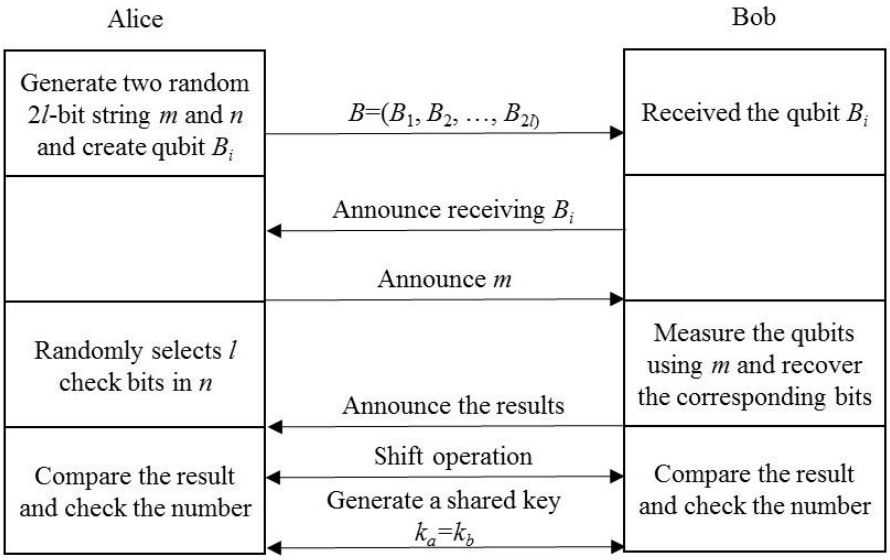

Figure 2. Proposed Two-party QSS Protocol

4. Security Analysis

The security analysis approach that was used is similar to the security analysis used in [11]. This is so because instead of using a steganography bit, we used a shift amount that is unknown to an eavesdropper. This is based on the probability of the attacker obtaining the key and the shift amount (an integer value that is less than n of the bits). Because quantum cryptography uses the laws of physics such that all the eavesdroppers can be revealed, the eavesdropper can be revealed because if they try to measure the qubits, they will disturb the qubits, resulting in an error. The other reason is that the rules of quantum mechanics guarantee that any measurement performed on the qubits modifies the state of those qubits. This can be discovered by both the sender and receiver. The analysis is as follows.

The probability of Eve causing an error is $1/2\times(1/2\times1/2+1/2\times1/2)=1/4$. Therefore, the probability of Eve receiving the right qubit is 1-1/4 = 3/4. According to [11], if θ is the proportion of particles that Eve measures during transmission from Alice to Bob, the probability that Eve knows the value of the qubit is $p=(3/4)\theta+1/2(1-\theta)=\theta/4+1/2$.

Similarly, Eve guesses the probability of the shift amount with probability, $(1/n)p$. The probability that Eve guesses the wrong shift amount is $1/2\,(1-1/n)$. Therefore, the probability of obtaining the value of Bob's qubit is

$$p_b=(1/n)p+1/2(1-1/n)=\Theta^2/4n+1/2.$$

Suppose Eve obtains the value of the qubit of Bob and Charlie with the same probability, i.e., $p_b = p_c$. The probability that Eve knows Alice's qubit is

$$p_a = p_b \times p_c + (1-p_b)\times(1-p_c)=\Theta^2/8n^2+1/2.$$

Therefore, Eve does not know the value of the shift amount of the key, and she cannot determine the value of the key. If the proportion of particles Bob measures from Alice to Charlie is given by β, the probability of obtaining Alice's key is given by $p_b=1/2+\beta/4n$. because Bob does not know the shift amount. Therefore, the probability that Bob obtains the value of Alice's secret shift amount is $P_{Bob} = p_a \times 1/2 + (1-p_a)1/2 = 1/2$. Hence, Bob does not know Alice's secret.

The secrecy of the key is enhanced by the use of the secretive shift amount. The shift amount adds to secrecy enhancement because an eavesdropper does not know the value of the shift. Therefore, it will be difficult for the eavesdropper to know the key. This is so because once the eavesdropper obtains the bits that are being transferred, he/she will not know that that is not the final key. For the attacker to obtain the key, he/she should perform the left cyclic shift with an amount similar to that of the communicating parties.

In the proposed protocol, the assumption is that it is a perfect channel, such that there are no errors. However, if there are errors, the error-correction techniques described in this paper can be used. The errors that occur can also be mistaken as the work of an eavesdropper, which would result in the cancellation of the entire key-distribution protocol. Error correction codes can be used to correct all of the errors that occur as long as the error rate is not higher than what is normal for QKD.

Meanwhile, all of the participants should have mutual information for the entire process to be completed smoothly. Otherwise, if the parties do not have mutual information, then the communication will be aborted because it can be interpreted as an attempt by an eavesdropper to obtain the key.

With the proposed protocols, when the users perform information reconciliation and find that the number of identical bits are below an agreed threshold (whether due to eavesdropping or noise in the channel), they can discard the communication. This can happen in the middle of the process before the key has been communicated. This is an advantage because they will then be able to abort the communication before the key is known.

5. Conclusions

In this paper, we proposed QSS schemes that encourage cooperation between parties. Our protocol has shown a fundamental communication protocol which shares a secret between only two parties. In addition, the security of the key is enhanced by using a secret shift operation of the key. This improves the secrecy of the key in the proposed protocol compared to the case with other protocols. The proposed protocol has a number of advantages, which includes ease of scalability because as the number of parties increases, the complexity of the system will not increase as in other protocols. The communication time of the protocol was also reduced by making sure their certainty. Our protocol can be used as a basic algorithm of multi-party protocols and other applications.

Acknowledgements

This paper was supported by Research Fund, Kumoh National Institute of Technology.

References

[1] C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing, Proc. of IEEE International conf. on computers, systems and signal processing, **(1984)** pp. 175-179.
[2] C. H. Bennett, "Quantum cryptography using any two non-orthogonal states", Physical Review Letters, vol. 68, no. 21, **(1992)** pp. 3121-3124.
[3] M. N. Wegman and J. L. Cater, "New hash functions and their use in authentication and set equality", J. Comput. Syst. Sci., vol. 22, no. 265, **(1981)**, pp. 265-279.
[4] A. Shamir, "How to share a secret", Communications of the ACM, vol. 22, no. 11, **(1979)**, pp. 612-613.
[5] G. R. Blakley and C. Meadows, "Security of ramp schemes", Advances in Cryptology-CRYPTO'84, LNCS 196 **(1985)**, pp. 242-269.
[6] M. Iwamoto, "General Construction Methods of Secret Sharing Schemes and Visual Secret Sharing Schemes, PhD Dissertation", The University of Tokyo, **(2003).**
[7] M. Hillery, V. Bužek and A. Berthiaume, "Quantum Secret Sharing", Phys. Rev. A., vol. 59, no. 3, **(1999),** pp. 1829-1834.
[8] Y. Du and W. Bao, "Multiparty Quantum Secret sharing Scheme Based on the Phase Shift Operations", Optics Communications, vol. 308, **(2013),** pp. 159-163.
[9] S. Muralidharan, S. Jain and P. K. Panigrahi, "Splitting of Quantum Information Using N-qubit Linear Cluster States", Optics Communications, vol. 284, no. 4, **(2011),** pp. 1082-1085.
[10] L. Yanyan and X. Chengqian, "Three-party Quantum Secret Sharing Based on Secure Direct Communication", Proceedings of International Forum on Information Technology and Applications, vol. 1, **(2009),** pp. 126-130.
[11] 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.
[12] 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, no. 5, **(2011),** pp. 630-635.
[13] M. Niemiec, "Design, Construction and Verification of a High-Level Security Protocol Allowing to Apply the Quantum Cryptography in Communication Networks", **(2011)** http://winntbg.bg.agh.edu.pl /rozprawy2/10409/full10409.pdf .
[14] X. P. Zhang, L. T. Shen and Z. B. Yang, "Multi-atom entanglement engineering and phase-covariant quantum cloning with a single resonant interaction assisted by external driving", Optics Communications, vol. 332, **(2014),** pp. 214–218.
[15] E. C. Behrman, R. E. F. Bonde, J. E. Steck, and J. F. Behrman, "On the Correction of Anomalous Phase Oscillation in Entanglement Witnesses Using Quantum Neural Networks", IEEE Transactions on Neural Networks and Learning Systems, vol. 25, no. 9, **(2014),** pp. 1696-1703.
[16] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, "Long-Distance Quantum Communication With Entangled Photons Using Satellites", IEEE Journal of Selected Topics in Quantum Electronics, vol. 9, no. 6, **(2003)** pp. 1541-1551.
[17] T. Honjo, T. Inoue, and K. Inoue, "Influence of light source linewidth in differential-phase-shift quantum key distribution systems", Optics Communications, vol. 284, no. 24, **(2011),** pp. 5856-5859.
[18] L. Lizama, J. M. Lopez, E. De Carlos López, and S. E. Venegas-Andraca, "Enhancing Quantum Key Distribution (QKD) to address quantum hacking", Procedia Technology, vol. 3, **(2012)**, pp. 80-88.
[19] S. Watanabe, R. Matsumoto and T. Uyematsu, "Optimal axis compensation in quantum key distribution protocols over unital channels", Theoretical Computer Science, **(2014).**
[20] J. Martinez-Mateo, A. Ciurana and V. Martin, "Quantum Key Distribution Based on Selective Post-Processing in Passive Optical Networks", IEEE Photonics Technology Letters, vol. 26, no. 9, **(2014)** pp. 881-884.

[21] A. Tanaka, M. Fujiwara, K. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, W. Zhen, M. Sasaki and A. Tajima, "High-Speed Quantum Key Distribution System for 1-Mbps Real-Time Key Generation", IEEE Journal of Quantum Electronics, vol. 48, no. 4, **(2012),** pp. 542-550.
[22] C. N. Yang, "Enhanced quantum key distribution protocols using BB84 and B92", http://www.researchgate.net/publication/228564836.
[23] K. Makanda and J. C. Jeon, "Efficient Two-Party Quantum Secret Key Sharing Protocol", ASTL 109 **(2015)** pp. 10-13.

Author

Jun-Cheol Jeon, he is currently a professor in Department of Computer Engineering at Kumoh National Institute of Technology. He received B.S. degree from Kumoh National Institute of Technology in 2000, the M.S. and Ph.D. degrees from Kyungpook National University in 2003 and 2007 respectively. His current research interests are cryptography, cellular automata, quantum-dot cellular automata, quantum computation and communication.