ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2020; 6(5): 465-468
www.allresearchjournal.com
Received: 23-02-2020
Accepted: 26-03-2020

Dr. Vandana Vanegal
Department of Physics, CCS
University Meerut, Utter
Pradesh, India

Corresponding Author:
Dr. Vandana Vanegal
Department of Physics, CCS
University Meerut, Utter
Pradesh, India

Protocols of quantum key agreement solely using bell states and bell measurement

Dr. Vandana Vanegal

Abstract
Two quantum key agreement (QKA) protocols that primarily use Bell State calculation is implied. The first QKA protocol introduced here is intended for two-party QKA, while multi-party QKA is designed for the second protocol. Using a series of multi-party entangled states (e.g., 4-qubit cluster state and Ω state), the proposed protocols are also extended to incorporate QKA. From the monogamy of entanglement, stability of these protocols emerges. This is in contrast to the current QKA protocols, where protection comes from the use of a non-orthogonal condition (principle of non-commutativity). Furthermore, it is shown that it is possible to change all quantum networks that are useful for the implementation of quantum dialogue and most of the stable direct quantum communication protocols to implement QKA protocols.

Keywords: Multi-party key agreement, quantum cryptography and non-orthogonal condition

Introduction
In 2004, Zhou *et al.* [1] implemented the Quantum Key Agreement (QKA) using quantum teleportation. In 2009, however, Tsai and Hwang [2] proved that the Zhou *et al*. protocol based on quantum teleportation was not a true QKA protocol, as the final (shared key can be fully decided by a single user without being detected. Hsueh and Chen [3] have almost simultaneously suggested another QKA protocol. In 2009, however, Tsai and Hwang [2] showed that the Zhou *et al*. protocol based on quantum teleportation was not a true QKA protocol, as the final (shared key can be fully decided by a single user without being detected. Tsai *et al.* [4] showed the following year that even the Hsueh and Chen protocols do not count as QKA protocols. In 2010, a QKA protocol using MUBs was developed by Chong and Hwang [5]. Apparently, the first effective QKA protocol was the Chong Hwang (CH) protocol. They proclaimed that BB84 is the foundation of their protocol. A deeper study will however, reveal that their protocol is similar to the protocol of LM05 [6]. The security of both the LM05 and BB84 protocols, of course, derives from the concepts of non-commutativity and no-cloning. In 2011, an updated variant of the Hsueh and Chen [3] protocol was introduced by Chong, Tsai and Hwang [7] and is free from the restrictions of the original protocol. Both the active and ineffective attempts to establish QKA protocols were limited to two-party cases until the recent past. Recently, there has been an increased interest in multi-party QKA schemes and many protocols have been published. We are guided to the following conclusions by a thorough analysis of all these current works.

Compared to the amount of work published on other areas of quantum cryptography, such as QKD, DSQC, QSDC and QD, the amount of work reported to date on QKA is much smaller. We should also assume that QKA has not been rigorously studied yet, and several further combinations of quantum states and QKA protocols can possibly be discovered.

The security of all 2-party and multi-party QKA protocols mentioned so far is based on conjugate coding, i.e. the security is achieved using two or more MUBs, so the protocols are basically BB84 style protocols. This raises a question: is it appropriate to use non-orthogonal states (two or more MUBs) to design QKA protocols?

Protocol 1: A 2-party protocol of QKA
Alice prepares

$$|\psi^+\rangle^{\otimes n}, \text{ where } |\psi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

She uses first qubits of each Bell state to form an ordered sequence

$$p_A = \{p_A^1, p_A^2, p_A^3, \cdots, p_A^n$$

Similarly, she forms an ordered sequence

$$q_A = \{q_A^1, q_A^2, q_A^3, \cdots, q_A^n\}$$

with all the second qubits. Here,

$$p_A^i, q_A^i$$

first and second particles of i th copy of the Bell state |ψ +, for 1 ≤ i ≤ n. She also prepares a random sequence

KA = $\{K_A^1, K_A^2, K_A^3, \cdots, K_A^n\}$

Alice prepares a sequence of $\frac{n}{2}$ Bell states $|\psi^+\rangle^{\otimes \frac{n}{2}}$ as decoy qubits and concatenates the sequence with qA to form an extended sequence q'_A.

After receiving the authentic acknowledgment of the receipt of the entire sequence q''_A from Bob, Alice announces the coordinates of the qubits (Π2n) sent by her. Using the information, Bob reorders the qubits and performs Bell measurements on the decoy qubits and computes the error rate. Ideally, in absence of Eve, all the decoy Bell states are to be found in |ψ +i. If the error rate is found to be within the tolerable limit, they continue to the next step

Bob drops the decoy qubits to obtain qA. Now, he prepares a new random sequence

$K_B = \{K_B^1, K_B^2, K_B^3, \cdots, K_B^n\}$, where K_B^i denote the i^{th} bit of sequence K_B, for $1 \leq i \leq n$,

He applies a unitary operation on each qubit of sequence qA to encode $K_{B.}$ After receiving the authenticated acknowledgment of the receipt of the entire sequence from q'_A Alice, Bob announces the position of the decoy qubits (note that he does not disclose the actual order of the message qubits) i.e., Πn ∈ Π2n. Alice checks the possibility of eavesdropping by following the same procedure. Alice publicly announces her key KA and Bob uses that and his own key (sequence) KB to form the shared key: K = KA ⨁KB. Bob announces the actual order of the message qubits (Πn ∈ Π2n) and Alice uses that information to obtain qB. Now, she combines pA and qB and performs Bell measurements Using KA and KB Alice prepares her copy of the shared key i.e., K = KA ⨁KB. The protocol discussed above is an orthogonal-state-based 2-party protocol of QKA.

Protocol 2: A multi-party protocol of QKA

In analogy to the previous protocol, Alice, Bob and Charlie produce their secret keys:

$$\begin{aligned} K_A &= \{K_A^1, K_A^2, K_A^3, \cdots, K_A^n\}, \\ K_B &= \{K_B^1, K_B^2, K_B^3, \cdots, K_B^n\}, \\ K_C &= \{K_C^1, K_C^2, K_C^3, \cdots, K_C^n\}, \end{aligned}$$

Where

$$K_A^i, K_B^i, K_C^i \text{ denote } i^{th}$$

bit of key of Alice, Bob and Charlie, respectively[1] and i = 1, 2,⋯

Alice, Bob and Charlie separately prepare

$$|\psi^+\rangle_A^{\otimes n}, |\psi^+\rangle_B^{\otimes n} \text{ and } |\psi^+\rangle_C^{\otimes n},$$

respectively. As in Step 1 of the previous protocol, Alice prepares two ordered sequences

$$p_A = \{p_A^1, p_A^2, p_A^3, \cdots, p_A^n\} \text{ and } q_A = \{q_A^1, q_A^2, q_A^3, \cdots, q_A^n\}$$

composed of all the first and the second qubits of the Bell states that she has prepared. Each of Alice, Bob and Charlie separately prepares sequence of n /2 Bell states $|\psi^+\rangle^{\otimes \frac{n}{2}})_j$ with j ∈ {A, B, C} as decoy qubits and concatenates the sequence with q_j to form extended sequences. After receiving the authentic acknowledgment of the receipt from the receiver (user j +1) corresponding sender (user j) announces the coordinates of the qubits (Π2n)j sent by him/her.

After discarding the decoy qubits, each user j encodes his/her secret bits by applying the unitary operation on each qubit of the sequence received by him/her (i.e., on q_j−1) in accordance with his/her key $_{Kj}$.

After discarding the decoy qubits each user reorders the sequence received by him/her. Now, each user j has two ordered sequences p_j and s_j−1. Each of the users j performs Bell measurements on $p_j^i s_{j-1}^i$. According to the output of the Bell measurement each user j can obtain the secret keys of the other two parties. Hence, the shared secret key K = KA ⨁KB ⨁KC can be generated.

Table 1: Transformation of |ψ +i based on two operations. Here, + refers to modulo 3 operations. j ∈ {A, B, C} where A, B, and C stand for Alice, Bob and Charlie, respectively.

Initial state prepared by user j	First operator applied by user $j+1$	Second operator applied by user $j+2$	Final State
$\|\psi^+\rangle$	$I \otimes I$	$I \otimes I$	$\|\psi^+\rangle$
	$I \otimes I$	$I \otimes Z$	$\|\psi^-\rangle$
	$I \otimes X$	$I \otimes I$	$\|\phi^+\rangle$
	$I \otimes X$	$I \otimes Z$	$\|\phi^-\rangle$

Security and efficiency analysis

Protocol 2 is built with an updated eavesdropping verification technique along the lines of Yin *et al.* [8] current protocol that transforms Yin *et al.* [8] non-orthogonal-state-based protocol into an orthogonal-state-based protocol. Using this technique, we have also established that the safety of this orthogonal-state-based eavesdropping checking technique originates from the monogamy of entanglement. Thus, against external attacks (eavesdropping), the protocol is secure. The remaining part of the protocol is theoretically similar to the Yin Ma Liu (YML) protocol, and the reliability of the YML protocol against internal attacks (i.e. the attempts of malicious Alice, Bob and Charlie to totally monitor the key either independently or through any two users' reciprocal cooperation) is therefore also valid here. Therefore, Protocol 2 is a stable QKA protocol and no separate, extensive discussion is required. Holding this in mind, we have specifically analysed the protection of our 2-party QKA protocol in the remaining part of the present portion.

Security against eavesdropping

QKA's 2-party protocol and also Chong and Hwang's [5] protocol may be viewed as KB's secure direct communication protocols from Bob to Alice, added to KA's classical communication from Alice to Bob. Specifically, Alice and Bob send random keys to one another instead of sending a meaningful message. While Bob sends his key KB through a DSQC or DSQC, QSDC scheme, Alice is publicly announcing her key KA. Thus, Eve has no information about KB. On the other hand the key communicated by Alice (i.e., KA) is a public knowledge. However, it does not affect the secrecy of the shared key as the final shared key to be produced and used is KA $\oplus$KB, knowledge of KA alone does not provide any information about KA $\oplus$ KB. Thus, the shared key produced in this manner is secure from external attacks of Eve.

Security against dishonest Alice

It would be possible for Alice to know Bob's hidden key until she declares KA to connect with KB if Alice and Bob were to use a normal DSQC protocol. In this scenario, by controlling KA as per her wish, she would be able to monitor the shared key entirely. We also changed the protocol to bypass this assault in such a way that Bob does not disclose the coordinates of the qubits submitted by him before he receives KA. This strategy introduces a delay in measurement of Alice and this delayed measurement strategy ensures that Alice cannot control the key by knowing KB prior to her announcement of KA

Turning existing protocols of quantum communication to protocols of QKA

We have shown that a clear relation exists between the protocols of the DSQC/QSDC and the QKA ones. This insight leads to a significant question: can all protocols of stable direct quantum communication be translated into QKA protocols? We plan to address this problem in what follows.

Turning a protocol of QSDC/DSQC to a protocol of QKA

We have shown that any arbitrary orthogonal basis can be used to create maximally efficient protocols for stable direct quantum communication. Both of them though, would not proceed to a QKA protocol. To be exact, in both DSQC and QSDC protocols, eavesdropping can be stopped and we can circumvent the attacks of unethical Alice by randomising the sequence of main encoded bits sent by Bob (i.e. by delaying the calculation to be done by Alice), but it is not enough to construct a protocol. We will need to stop Bob's dishonest assaults. We ought to limit the data available to Bob to do so. In particular, Bob must not have complete baseline information that is used to prepare the qubits on which his key has been encoded. In our Protocol 1 and in all the orthogonal state-based two-way DSQC/QSDC protocols this can be achieved if Alice keeps some of the qubits of each entangled state with herself as that would restrict Bob from changing KB after receiving KA. The above debate demonstrates that the DSQC/QSDC protocol to be used for the implementation of a QKA protocol should not be one-way, since Bob will have direct access to the basis on which the quantum state used for the encoding of his key is prepared (since Bob can prepare the quantum state himself in a one-way protocol). Therefore, neither of the DSQC or QSDC one-way protocols can contribute to QKA. However, QKA will result in most of the two-way protocols of stable quantum communication.

Conclusion

We have suggested two QKA protocols in the present chapter. The first one works in the case of two parties, and the second one works in the case of several parties. Both protocols use only the Bell basis of their original form for the preparing of the encoding states and their decoding and eavesdropping review calculation. Subsequently, it is shown that it is possible to expand the applicability of the proposed protocols to 4-qubit cluster state and |Ω] state. This particular feature that states are calculated and prepared on the same basis ensures that conjugate coding (non-commutativity) is not necessary for QKA to obtain the requisite protection and QKA protocols can be designed entirely orthogonal-state-based. It would be important to note here that the use of entangled states in general and Bell states in particular for the implementation of stable quantum communication protocols is not new. The proposed protocols are the first set of orthogonal-state-based protocols of QKA as all the existing protocols of QKA are based on conjugate coding. Thus, the proposed protocols are fundamentally different from all the existing protocols of QKA. As the orthogonal-state-based protocols show that the use of conjugate coding or in other words use of non-commutativity principle is not essentially required for unconditional security, they require lesser quantum resources in a sense. To be precise, the monogamy of entanglement is sufficient to protect these protocols. We have also shown that much of the current QSDC and DSQC protocols and all the QD protocols can be converted into QKA protocols. This is an interesting finding, since a QSDC, DSQC or QD protocol needs comparatively tighter security compared to a QKD or QKA protocol. The need for comparatively tighter protection comes from the assumption that if we receive eavesdropping signatures in a QKD protocol, or QKA, then we will drop the key and generate a new one. Therefore, because of eavesdropping, we should not care about data loss. As long as we can detect all eavesdropping attempts. However we can not afford to encourage information leakage in a QSDC, DSQC or QD protocol, as in contrast to QKD (where a random sequence is sent) a significant information is sent in a QSDC, DSQC or QD protocol. This argument can be expanded by noticing briefly that a QSDC or DSQC protocol can often be reduced to a QKD protocol, but the opposite is not valid in general.

References

1. Zhou N, Zeng G, Xiong J. Quantum key agreement protocol. Electron. Lett 2004;40:1149-1150.
2. Tsai CW, Hwang T. On Quantum key agreement protocol, Technical Report, C-S-I-E, NCKU. Taiwan, R.O.C, 2009.

3. Hsueh CC, Chen CY. Quantum key agreement protocol with maximally entangled states. In: Proceedings of the 14th Information Security Conference, National Taiwan University of Science and Technology, Taipei, 2004, 236-242.
4. Tsai CW, Chong SK, Hwang T. Comment on quantum key agreement protocol with maximally entangled states. In: Proceedings of the 20th Cryptology and Information Security Conference (CISC 2010), National Chiao Tung University, Hsinchu, Taiwan 2010, 210-213.
5. Chong SK, Hwang T. Quantum key agreement protocol based on BB84. Optic Commun 2010;283:1192-1195.
6. Shi RH, Zhong, H.: Multi-party quantum key agreement with Bell states and Bell measurements. Quantum Inf. Process 2013;12:921-932.
7. Chong SK, Tsai CW, Hwang T. Improvement on Quantum key agreement protocol with maximally entangled states. Int. J Theor. Phys 2011;50:1793-1802.
8. Yin XR, Ma WP, Liu WY. Three-party quantum key agreement with two-photon entanglement. Int. J Theor. Phys 2013;52:3915-3921.