(IJIASE) 2019, Vol. No. 5, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

DEVELOPING AN APPLICATION OF QUANTUM COMPUTING THROUGH QUANTUM SECURE DIRECT COMMUNICATION IN VOTING BY LEVERAGING SINGLE QUBIT

Shreya Ahuja

ABSTRACT

An epic quantum parallel democratic plan that utilizations just a solitary qubit is proposed. In particular, the convention is planned by altering a solitary qubit based plan for controlled deterministic secure quantum correspondence. The security of the convention is dissected over some particular assaults. Further, the qubit proficiency of the convention is likewise determined. It is built up that on account of paired democratic, the proposed single qubit based quantum casting a ballot convention is more proficient than a portion of the as of late proposed conventions for parallel democratic. Further, it additionally appears in a portion of the ongoing papers that the first single qubit based quantum secure direct correspondence conspire that has been changed to plan the proposed quantum casting a ballot plot is less influenced than comparing multiqubit based plan. This further sets up the importance of the present outcomes. As the proposed plan doesn't require complex quantum assets like entrapment and qubits, it is by all accounts tentatively feasible utilizing the accessible innovation.

1. INTRODUCTION

The advent of quantum information processing endangered classical cryptography1 (see2,3 for review) Bennett et al.'s key distribution (BB84) protocol4 not only turned out to be a solace for cryptography community, it also opened doors for a whole new field of quantum cryptography. In fact, the BB84 protocol provides unconditional security by using quantum resources, an unachievable feat in the domain of classical physics. The motivation to explore the unconditional security was initially restricted to quantum key distribution (QKD)4-6 Later, possibilities of secure quantum communication without prior sharing of a secure key have also been studied (see7 for review).

Specifically, direct quantum communication without additional classical communication required to decode the message is referred to as quantum secure direct communication (QSDC)8,9 . Similarly, when at least an additional bit of classical communication is required to perform the direct communication, it falls under deterministic secure quantum communication (DSQC)10- 17. The direct communication was later extended to two-way simultaneous communication known as quantum dialogue (QD)18-20. Over the last decade, controlled versions of these various direct communication schemes have also been designed (cf.21,22 and references therein). Recently, the interest of quantum cryptography community has been diverted towards designing quantum schemes for applications in various problems of practical importance, such as socialist millionaire problem19,

quantum private comparison23, e-commerce24, auction25 and voting26-34. Out of all these, voting is relevant to us in more than one way. As also discussed in Ref.34, it forms the backbone of democracy. In this manner, here, our advantage is to structure another quantum casting a vote which can be seen as an altered Controlled Deterministic Secure Quantum Communication it ought to be controlled deterministic secure quantum communication(CDSQC) conspire. The undertaking of a quantum casting a ballot plot is to fulfill security, unquestionable status and protection. The primary quantum casting a ballot plot was proposed26. Simultaneously additionally proposed a democratic scheme28. In the ongoing past, it has just been set up that a CDSQC conspire is a superior decision to plan a quantum casting a ballot scheme34 than a controlled teleportation scheme27. These schemes motivated various quantum voting scheme proposed since then31-33 (and references therein). The fact that most of these schemes either multi-qubit or multi-qudit-based set the motivation for the present paper to accomplish the same task with single qubit states which are relatively easier to generate and maintain. Remaining part of the present paper is organized as follows. A single qubit based quantum voting scheme has been proposed in Sec. 2. Subsequently, the security and efficiency of the proposed protocol are discussed in Sec. 3, where an attempt to compare the efficiency with the existing protocols has also been made. Finally, the paper is concluded in Sec. 4.

2. PROTOCOL OF QUANTUM VOTING USING SINGLE QUBITS

Here, we propose a binary voting protocol, where each voter casts a vote of 1 bit (say yes or no). The same task can also be viewed as voter sending a binary vote in a secure manner to a tallyman controlled by a supervisor. This is the same as the task accomplished by a usual CDSQC scheme21. The difference appears in the security requirement which mentioned that the identity of individual voter is to be concealed. This can be ensured using an additional trusted party (CA), who issues a quantum ID to each voter and later verifies the identity of each voter27,34. The complete voting protocol can be viewed as voters Alice is send each 1-bit vote to the tallyman (Bob), and a scrutineer (Charlie) maintains his supervision. Additionally, each voter shares a unique quantum key with Bob. Here, we attempt to design a CDSQC protocol modified from LM05 protocol9 using only single qubits.

The protocol works as mentioned in the following steps.

CDSQC 1: Charlie sets up a classical channel to make an announcement, which will be called bulletin board.

CDSQC 2: Tallyman verifies the identities of the authorized voters with the help of the trusted party CA, who had issued the quantum IDs.

CDSQC 3: When th voter Alicei requests Charlie to vote, he prepares and sends a single qubit state randomly prepared in either basis to her. Charlie keeps the information of the choice of initial state with himself. Here, it should be noted that the qubit is sent to Alicei in a secure manner using BB84 subroutine, i.e., after adding a decoy qubit to be checked for eavesdropping. For more details of BB84 subroutine see Refs.21,35.

(IJIASE) 2019, Vol. No. 5, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

CDSQC 4: After making sure she has received the qubit in a secure manner Alicei encodes her binary vote by doing nothing to send "no", whereas applying a Pauli Y operation to cast "yes". Finally, she sends the encoded qubit after encrypting with quantum key in a secure way to Bob.

CDSQC 5: Bob can measure the Alicei's qubit only when Charlie shares information on the basis he had chosen to prepare the initial state.

CDSQC 6: Bob knows the quantum key shared with Alicei. He can use this information but will still require the choice of the initial state to decode her vote.

CDSQC 7: Bob and Charlie follow the same procedure to record each voter's choice.

Finally, the authorities proceed to the counting phase. In which, Charlie announces the choice of state of the initially prepared by him. Using this Bob counts the total number of "yes" votes and announces the result.

3. SECURITY AND EFFICIENCY

A quantum voting scheme is desired to satisfy security, verifiability and privacy simultaneously. In the proposed protocol security, that a voter's choice is not disclosed to other voters and each voter can cast only one vote, is maintained by using proper eavesdropping checking strategy for which BB84 subroutine is employed. Additionally, each voter has access to only a single qubit state so she cannot encode more than one bit. The verifiability is also maintained as it can be verified that each vote is counted once all the votes are summarized on the bulletin board. Finally, the privacy is ensured as the identity of each voter is hidden and quantum IDs are issued and verified by a trusted party, who also help on authentication of each voter using zero knowledge proof. Therefore, the quantum scheme proposed here is secure. In the proposed voting scheme, an additional quantum key is used to ensure security against Charlie's attack. Specifically, Charlie has the knowledge of initial quantum state, and if he intercepts the qubits while the voter to Bob transmission and measure both the qubits in the basis he had initially prepared it. Though this will be detected during Alicei's and Bob's eavesdropping checking but Charlie will learn the vote she had cast. The efficiency of the proposed scheme can be calculated using the quantitative measure of efficiency as discussed in 21,36 Here, c is the total no of classical bits transmitted with the help of b bits of classical communication using the q number of qubits. The qubit efficiency of the proposed protocol can be calculated as follows. Each binary vote is transmitted using a single qubit, which also require 2 decoy qubits to ensure security (i.e., . Additionally, each voter shares a unique quantum key with Bob using 2 qubits. Charlie announces the initial state and basis chosen for that in different stages of the protocol with 2 bits of information. Thus, the qubit efficiency of the protocol proposed here is.

The efficiency of the protocols proposed in the past was 9.09% for TZL protocol27, which decreases further to 6.67% when the suitable number decoy qubits, which needs to be used, is considered34. Similarly, in Ref34, a large number of CDSQC based quantum binary voting protocols have been proposed and efficiency of two of them was reported to be 11.11% and 16.67%. However, various ways to increase the efficiency have been discussed for the CDSQC based quantum voting protocols

(IJIASE) 2019, Vol. No. 5, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

in Ref.34, i.e., decreasing classical bits and/or qubits used. Here, we show that the efficiency increases considerably by decreasing the number of qubits required.

4. CONCLUSION

An efficient quantum binary voting scheme is proposed by modifying a standard CQSDC protocol. The security of the scheme proposed has also been established. In particular, a solitary qubit based quantum parallel democratic plan has been structured and proficiency for the equivalent has been determined. In the wake of contrasting the proficiency of the proposed plan with the current plans, it is set up that the proposed plan has higher effectiveness when contrasted and a portion of the as of late proposed plans. Curiously, in37, it is demonstrated that the LM05 protocol9 is less influenced when contrasted and an ensnared state-based QSDC plot, i.e., Ping-pong protocol8, over noisy environment. A similar study over non-Markovian channels38 will be reported elsewhere. Further, it is known that the generation and maintenance of a single qubit state is relatively easier than a multi-qubit (or multi-qudit) quantum state. Therefore, we hope that the feasibility of experimental realization of the proposed quantum voting scheme using single qubits would motivate the experimentalists interested in quantum voting to implementation this scheme.