

# Towards Securing Multi-Agent in Cavity QED via Quantum Protocol

Daniel Adu-Gyamfi<sup>1,2, §</sup>; Fengli Zhang<sup>1,\*</sup>; Zhiguang Qin<sup>1, γ</sup>

University of Electronic Science and Technology of China, Chengdu 610054, China<sup>1</sup>; University of Energy and Natural Resources, Sunyani P O Box 214, Ghana<sup>2</sup>

*E-mail: daniel.adu-gyamfi@uenr.edu.gh<sup>§</sup>; fzhang@uestc.edu.cn<sup>\*</sup>; qinzg@uestc.edu.cn<sup>γ</sup>*

## ABSTRACT

*In this paper, we present quantum secure communication protocol towards securing multi-agent in distributed cavity quantum electrodynamics (CQED) systems. A four-qubit cluster state is used to enable an agent to asymmetrically distribute quantum state to other agents. The protocol allows participating agents to have different levels of rank in hierarchy when reconstructing and sending quantum information secretly across CQED systems through an arbitrary single-qubit state. The protocol has heuristically proven secured, efficient and enabled high speed transmission in CQED systems.*

**Keywords:** Quantum security, Arbitrary single-qubit, Four-qubit cluster state, Multi-Agent, Cavity quantum electrodynamics.

## 1. INTRODUCTION

Quantum cryptography covering quantum key distribution and other cryptographic applications has driven both fundamental and applied researches [1]. Basically, quantum cryptography enables concealing confidential information in network systems via mathematical physics. Among the applications of quantum cryptography include cavity quantum electrodynamics (CQED). The CQED consists of an arbitrary number of emitters interacting with an arbitrary number of cavity quantum states or modes. Securing CQED systems will increasingly contribute to future research and development in designs of products such as modern home security smart gateways and door locks. With the aid of quantum encryption schemes and routing protocols, CQED when interleaved with wireless transmission and other technologies can provide quantum trusted access to networking. Thus, where quantum states can be used as keys to encrypt internet connections and secure them. Meaning that potential application area of

secured CQED include internet-of-things (IoTs) such as smart city and smart home. Where we can achieve secure digital home through quantum secure gateway, quantum secure server, quantum secure cloud across home network space, etc. to enable secure information transmission in smart homes for convenient societal consumption. Moreover, CQED has been among the frontiers of modern science, and thus the application of CQED has quickly entered the engineering domain [1-2]. With the advent of quantum computing, CQED continues to be at the cutting edge of technologies in this area, where it is considered as the most successful commercialized platform. CQED with such a pedestal has paved way to increasing number of quantum sub-systems, and hence the demand for advance secure analytical techniques to comprehend multi-agent systems without losing efficiency and security. In recent time, the entangled quantum states have been applied in quantum communications and information processing [3]. Quantum key distribution has tremendously progressed theoretically and practically. For thorough reviews see [1-2]. Quantum secret sharing in multi-agent systems is a cryptographic primitive activity in which an agent splits a secret quantum state into an arbitrary quantum states and distributes them among other agents such that only legitimate agents who meet an access control structure and requirement can reconstruct the quantum information secrecy. Quantum secret sharing has been applied widely into designs of quantum protocols for digital signature, key management, and secure multi-party transactions, etc. [1]. Originally, quantum secret sharing was proposed by Hillary et al. [4], after the introduction of first quantum teleportation of arbitrary single-qubit state by Bennett et al. [5], where 3-qubit state have been utilized for key distribution. Such that attempts by a third party to reconstruct quantum shared state will prove futile by disrupting the correlation of the quantum states. Making it possible for legitimate

parties to detect such intrusion and announce full outcomes in some trial runs [1,4]. However, a legitimate participant or group of legitimate participants may collude to cheat the system. Therefore, quantum (N;k) threshold scheme [6] was introduced to improve on colluding attack, where a quantum secret state which is split among N parties can be successfully reconstructed if and only if about k parties are capable to combine their shares quantum states, and thus where  $2k > N$ . Recently, quantum secret sharing can be categorized into many forms including hierarchical quantum secret sharing [7], hierarchical dynamic quantum secret sharing [8], and quantum secret sharing based on a d-level particle [9] which differs from not using entanglement of quantum state particles, served the basis for sharing a secret via (N;N) threshold schemes. Similarly, having extended on symmetry of cluster states [10] into asymmetric cluster states, this paper focuses on hierarchical quantum information processing to proof that using four-qubit cluster states as quantum channel is sufficient enough to ensure security of quantum information processing for an arbitrary single-qubit in CQED, and thus participating multi-agent may have either same or different order of rank in hierarchy.

## 2. QUANTUM PROTOCOL DESIGN

Here, we set up the quantum channel for the protocol. Given that quantum information is to be split among three agents in the order of hierarchy. Such that,

$$|\beta^1\rangle = (|000\rangle + |011\rangle)_{234} \text{ and } |\beta^2\rangle = (|100\rangle - |111\rangle)_{234}.$$

The four-qubit cluster state can be established as given in (1).

$$\begin{aligned} |Q\rangle_4 &= \frac{1}{2} (|0000\rangle + |1100\rangle + |0011\rangle - |1111\rangle)_{1234} \\ &= \frac{1}{2} (|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234} \\ &= \frac{1}{2} (|0\rangle(|000\rangle + |011\rangle) + |1\rangle(|100\rangle - |111\rangle))_{1234} \\ &= \frac{1}{2} (|0\rangle(|\beta^1\rangle + |1\rangle(|\beta^2\rangle))_{1234} \end{aligned} \quad (1)$$

Assume that the participating agents in the quantum information secrete sharing include Alice, Bob, Darth and Oscar. Where Alice has the overall authority as the ultimate rank, Bob has high rank than Darth and Oscar who have same level of rank in the hierarchy in terms of revealing quantum information secrecy. Supposing Alice wants to transmit and share her arbitrary single-qubit state such as  $|\psi\rangle_A$  to Bob, Darth and Oscar who happen to be agents. The protocol is such that, Bob having high rank will always need all the agents in the same level of his rank and at least one agent below the level of his rank to cooperate in order to reveal the quantum information secrecy. On the other hand, Darth

and Oscar being in the same level of rank, and considered as low rank will respectively need all the agents in higher rank than them, as well as all the agents in the same level of rank as them to cooperate in order to reveal the quantum information secrecy. Therefore, the arbitrary single-qubit state  $|\psi\rangle_A$  from Alice can be transmitted as given in (2). Such that  $|\alpha_1|^2 + |\alpha_2|^2 = 1$ , where  $\alpha_1$  and  $\alpha_2$  are ordinary complexity numbers.

$$|\psi\rangle_A = \alpha_1 |0\rangle + \alpha_2 |1\rangle \quad (2)$$

Suppose that four-qubit cluster state  $|Q_4\rangle_{1234}$  is to be shared among all the multi-agent, and thus Alice, Bob, Darth and Oscar. The complete state of the system can be established as given in (3). Such that the first particle is linked to Alice, and second particle to Bob, third particle to Darth and fourth particle to Oscar in that order, where A denotes a particle.

$$\begin{aligned} |X\rangle_{A1234} &= |\psi\rangle_A \otimes |Q_4\rangle_{1234} \\ &= (\alpha_1 |0\rangle + \alpha_2 |1\rangle)_A \otimes \frac{1}{2} (|0\rangle|\beta^1\rangle \\ &\quad + |1\rangle(|\beta^2\rangle))_{1234} \\ &= \frac{1}{2} (\alpha_1 |00\rangle|\beta^1\rangle + \alpha_1 |01\rangle|\beta^2\rangle + \\ &\quad \alpha_2 |10\rangle|\beta^1\rangle + \alpha_2 |11\rangle|\beta^2\rangle)_{A1234} \end{aligned} \quad (3)$$

Consider  $n$  as arbitrary number of participating agents in two different order of ranks  $r_1$  and  $r_2$ , such that  $r_1 > r_2$ . First of all, Alice issues the four-qubit cluster states and a single qubit in a form of  $|0\rangle$  in the initial stage. Secondary, Alice applies C-NOT operations on the entangled qubits to establish the cluster states as given in (4). Where  $m$  is an ion.

$$\begin{aligned} |\psi^m\rangle &= \frac{1}{2} (|00 \dots 000 \dots 0\rangle + |00 \dots 011 \dots 1\rangle \\ &\quad + |11 \dots 100 \dots 0\rangle - |11 \dots 111 \dots 1\rangle) \end{aligned} \quad (4)$$

When analyze the cluster states in (4), it can be grouped into two sections. Such that first section has qubits  $|00 \dots 0\rangle$ ,  $|00 \dots 0\rangle$ ,  $|11 \dots 1\rangle$ ,  $|11 \dots 1\rangle$  which corresponds to  $r_1$ . Whereas the second section has qubits  $|00 \dots 0\rangle$ ,  $|11 \dots 1\rangle$ ,  $|00 \dots 0\rangle$ ,  $|11 \dots 1\rangle$ , and corresponds to  $r_2$ . Therefore, the complete system can be established as given in (5).

$$\begin{aligned} |X\rangle &= |\psi\rangle_A \otimes |\psi^m\rangle_{r_1 r_2} \\ &= \frac{1}{4} (\alpha_1 |0\rangle + \alpha_2 |1\rangle) \otimes (|00 \dots 000 \dots 0\rangle \\ &\quad + |00 \dots 011 \dots 1\rangle \\ &\quad + |11 \dots 100 \dots 0\rangle - |11 \dots 111 \dots 1\rangle)_{r_1 r_2} \\ &= \frac{1}{4} (\alpha_1 |000 \dots 000 \dots 0\rangle + \alpha_1 |000 \dots 011 \dots 1\rangle \\ &\quad + \alpha_1 |011 \dots 100 \dots 0\rangle - \alpha_1 |011 \dots 111 \dots 1\rangle) \end{aligned}$$

$$+ \alpha_2 |100 \dots 000 \dots 0\rangle + \alpha_2 |100 \dots 011 \dots 1\rangle \quad (5)$$

As a result, any participating agent in the rank  $r_1$  will be able to reveal the quantum information secrecy through the arbitrary single-qubit state  $|\psi\rangle_A$  shared by

Alice, when any other agents in same  $r_1$  also release their qubit state.

### 3. THE CQED APPLICATION

Assume  $n$  qubits consist of a pair of identical two-level atomic states,  $D_1, D_2$  and  $D_a, D_b$  which interact with the evanescent fields in the cavity [11] simultaneously in a single mode, as shown in Fig. 1. Where the cavity consists of qubits coupled simultaneously to a pair of two-level atoms interacting via dipole-dipole interaction strength,  $\Omega$ , and  $g_1$  and  $g_2$  are eigenvectors. Both the cavity and the atom are coupled to a tapered optical fiber [11]. The fiber modes are described by  $\{a_{in}, a_{out}, b_{in}, b_{out}\}$  and  $\{\sigma_{1,in}, \sigma_{1,out}, \sigma_{2,in}, \sigma_{2,out}\}$  coupled to the cavity and atom respectively, in terms of detectors input-output fields. Where  $\gamma$  is the emission rate when the atoms undergo spontaneous reaction, and  $k$  is rate of cavity decay. The details of the CQED scheme can be found in [11]. Now, Hamiltonian of the whole system for a pair of identical two-level atomic states interactions at frequencies,  $w_c$  and  $f$  can be established as given in (6). Whenever  $f \geq \delta$ , the dynamics of the Hamiltonian system can be expressed as given in (7). The two identical atomic states expressed as ions are varied with parameters  $q_1$  and  $q_2$  respectively. Where  $\lambda = \frac{2(\Omega\eta)^2}{\delta}$ .

$$H = f\alpha^\dagger \alpha + \omega_c \sum_{j=A} \sigma_{2,j} + \Omega \sum_{j=A} [e^{-i[(\omega_c - f - \delta)t - \eta(\alpha + \alpha^\dagger) + \phi]} + \sigma_j^\dagger + H.c.] \quad (6)$$

Where the two atomic ground states have been expressed as follows:

$$\sigma_j^\dagger = |1_j\rangle\langle 0_j|, \sigma_j^- = |0_j\rangle\langle 1_j| \text{ and } \sigma_{2,j} = \frac{1}{2}(|1_j\rangle\langle 1_j| - |0_j\rangle\langle 0_j|), |0_j\rangle$$

And the excited stated for the  $j$ -th atom has been expressed as  $|1_j\rangle$ .

$$H_D = \lambda[\frac{1}{2} \sum_{j=A,1} (|0_j\rangle\langle 0_j|) + (|1_j\rangle\langle 1_j|) + (T_{q_1}^+ T_{q_2}^+ + T_{q_1}^- T_{q_2}^- + H.c.)] \quad (7)$$

The Hamiltonian system dynamics evolves into thermal state,  $E(t)$  which has been expressed in (8).

Where  $H_0 = \sum_{j=A,1} \Omega (T_j^+, T_j^-)$ .

$$E(t) = e^{-i(H_0 t + H_D t)} \quad (8)$$

Moreover, at  $\lambda t = \frac{1}{4} \pi$ , then the evolving state of the CQED system can be given in the expressions as follow:

$$|Q^+\rangle_{A1} \rightarrow |00\rangle_{A1}, |Q^-\rangle_{A1} \rightarrow -i|11\rangle_{A1} \text{ and } |R^+\rangle_{A1} \rightarrow |01\rangle_{A1}, |R^-\rangle_{A1} \rightarrow -i|10\rangle_{A1}$$

As a result, bombarding ions A and 1 whiles discarding the phase factor enables the system to be established. Therefore, it is evidenced that four-qubit cluster state as quantum channel is sufficient enough to ensure security of quantum information processing for an arbitrary single-qubit in CQED.

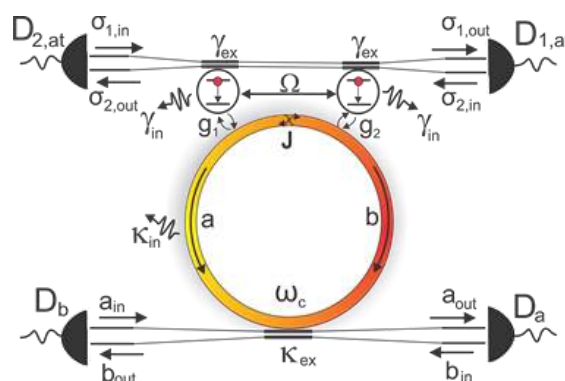


Fig 1: An interactive scheme of atom-cavity system for CQED [11].

### 4. CONCLUSION

In this paper, we have shown that four-qubits cluster states as quantum channel is sufficient to ensure security of quantum information processing for an arbitrary single-qubit in CQED, and thus in terms of order of hierarchy in authority among the participating

multi-agent. Low ranking agents need the cooperation of the rest of other agents in order to reveal the quantum information secrecy. Whereas, high ranking agents need at least a single agent in any level of authority to reveal the quantum information secrecy in the CQED systems. The proposed hierarchical

quantum protocol ensures arbitrary number of quantum states, and provides security, efficiency and high speed information transmissions in a form of qubits cluster of quantum states.

## 5. ACKNOWLEDGMENTS

This research was supported by the National Natural Science Foundation of China [Grant No.61602097, No.61502087, and No.61472064].

## 6. REFERENCES

- [1]. A. Shenoy-Hejamadi, A. Pathak, and S. Radhakrishna, "Quantum Cryptography: Key Distribution and Beyond," in Subhash Kak, Tabish Qureshi & Danko Georgiev edition, 6(1):1, 2017. doi: 10.12743/quanta.v6i1.57
- [2]. E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," NPJ Quantum Information, 2:16025, 2016. doi: 10.1038/npjqi.2016.25
- [3]. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," Physical Review A, 54:3824-3851, 1996. doi:10.1103/PhysRevA.54.3824
- [4]. M. Hillery, V. Bužek, A. Berthiaume, "Quantum secret sharing," Physical Review A, 59(3):1829–1834, 1999. doi:10.1103/PhysRevA.59.1829
- [5]. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Physical review letters, 70(13): 1895, 1993. doi.org/10.1103/PhysRevLett.70.1895
- [6]. R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," Physical Review Letters, 83(3): 648–651, 1999. doi:10.1103/PhysRevLett.83.648
- [7]. C. Shukla, and A. Pathak, "Hierarchical quantum communication," Physics Letters A, 377(19-20):1337–1344, 2013. doi:10.1016/j.physleta.2013.04.010
- [8]. S. Mishra, C. Shukla, A. Pathak, R. Srikanth, and A. Venugopalan, "An integrated hierarchical dynamic quantum secret sharing protocol," International Journal of Theoretical Physics, 54(9): 3143–3154, 2015. doi:10.1007/s10773-015-2552-z
- [9]. A. Tavakoli, and I. Herbauts, M. Zukowski, and M. Bourennane, "Secret sharing with a single d-level quantum system," Physical Review A, 92(3):030302, 2015. doi:10.1103/PhysRevA.92.030302
- [10]. C. H. Bennett, and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theoretical Computer Science, 560(1): 7–11, 2014. doi: 10.1016/j.tcs.2014.05.025
- [11]. E. H. S. Sousa, and J. A. Roversi, "Selective Engineering for Preparing Entangled Steady States in Cavity QED Setup," Quantum Rep. 1, 63–70, 2019. doi:10.3390/quantum1010007