Secure sequential transmission of quantum information

Kabgyun Jeong[1,*] and Jaewan Kim[1,†]

[1] *School of Computational Sciences, Korea Institute for Advanced Study, Hoegiro 87, Dongdaemun, Seoul 130-722, Korea*

(Dated: June 14, 2013)

In this paper, we suggest a quantum protocol to transmit any quantum information, namely, quantum sequential ε-secure transmission scheme. The scheme is constructed via some modified quantum secret (or state) sharing method. Actually, these schemes significantly rely on the idea of approximation of the well-known private quantum channel using randomly selected n-qubit Pauli matrices. We focus on describing the protocol structure, security argument, and efficiency of the quantum sequential transmission in-depth, relatively more than modified quantum secret sharing protocols.

PACS numbers: 03.67.Hk

- *Introduction*: One of the most popular quantum cryptographic primitives, except quantum key distribution, is the quantum secret (or state) sharing (QSS) protocol [1, 2]. The primitive known as QSS is a process of splitting a quantum information into several parts, and then securely reconstructing the information, but certain subparts are impossible to restoring the information. (In the strict sense, the secret sharing is different from the state sharing on its goal [3], but we treat the same category.) There are huge number of theoretical studies on QSS protocols and, also exist experimental demonstrations on QSS scheme in continuous-variable regime e.g., Ref. [4, 5].

In this paper we will deform the original QSS scheme to other one, and propose an information transmission protocol so-called "ε-secure quantum sequential transmission" (QST$_\varepsilon$), via some modified QSS scheme, (ε-secure) information splitting-reconstruction (ISR$_\varepsilon$) method. The ε implies that security and efficiency of the protocols are dealt with an asymptotic consideration. Shortly speaking, the quantum sequential transmission protocol (see Fig. 1) can transmit any quantum states, one party to another, under the consent of all authorized participants having classical secrets. Thus we hope that the protocol, QST$_\varepsilon$, is applied to certain scheme such as quantum sealed-bid auction [6] or, namely, *quantum email* protocol. Furthermore, with the proposed scheme, we study the question of finding the minimal resources required to split and reconstruct of quantum information and to transfer any quantum information sequentially.

First of all, we define a quantum one-time

*Electronic address: kgjeong6@kias.re.kr
†Electronic address: jaewan@kias.re.kr

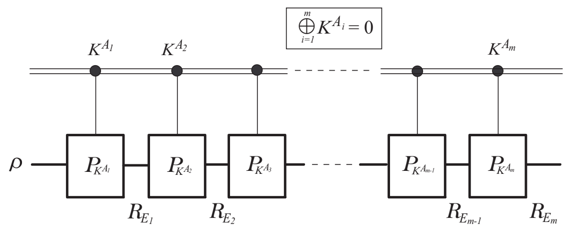

FIG. 1: Approximate m-party quantum sequential transmission protocol: Using their secret classical information K, a sender transmits a quantum information ρ securely and efficiently through the $m-1$ ε-randomizing maps $\mathcal{R}_{E_j}$. Boxes with P_K represent the (appointed) n-qubit Pauli operations.

pad. Ambainis *et al.*, [7] have first proposed a quantum primitive known as private quantum channel (PQC) for secure transmission of quantum states, and have proven its security including the optimality [8, 9]. Their complete randomization scheme naturally gives birth to *approximate* approaches for quantum state randomization [10–12]. We here adapt the approximate version of the Dickinson and Nayak's PQC [12] having relatively few Pauli operations on a multi-qubit encoding. By exploiting the following conventions and definitions, we will present two quantum communication protocols of which are efficient in the view point from minimal resources and security from a small information leakages ($\varepsilon < 1$). But, in this paper, we mainly concentrate our attention to the ε-secure quantum sequential transmission scheme.

- *Main protocol*: If each ε-randomizing maps between two users $(j, j+1)$, for every quantum state $\rho \in \mathcal{B}(\mathbb{C}^{2^n})$, satisfy

$$\left\| \mathcal{R}_j(\rho) - \frac{\mathrm{id}}{2^n} \right\|_1 \le \varepsilon^{\frac{1}{m}}, \tag{1}$$

then we can always consist of QST$_\varepsilon$ protocol via APQC they having

$$\left\| \mathcal{R}(\rho) - \frac{\mathrm{id}}{2^n} \right\|_1 \le (\varepsilon^{\frac{1}{m}})^m = \varepsilon, \tag{2}$$

and consuming only $O(n)$ secret classical keys with $\bigoplus_{i=1}^m k_i = 0$.

The estimation of Eq. (2), for any ε, allows us to only use the classical key as $n + 2\log\frac{1}{\varepsilon} + 4$ [12]. Notice that Dickinson and Nayak's efficient construction for the approximate private quantum channel on n-qubit relies on McDiarmid's inequality in probability analysis and a net argument on discretizing pure quantum states. Strict security analyzes of the approximate private quantum channel in security parameter ε are renowned at Ref. [9], and see also Ref. [13].

- *Summary*: We have proposed a quantum protocol for quantum sequential and ε-secure transmission scheme via some modified quantum secret sharing method. This scheme exploits a relatively small (correlated) classical information such as $O(n)$ bits, about half of perfect PQC case of $2n$-bits, and transmit any n-qubit state securely, so it is efficient. The security argument only depends on small ε (it is small value, $\varepsilon \ll 1$, for sufficiently large d in Hilbert space $\mathbb{C}^d$) in which an approximate private quantum channel guarantee its security. Finally, we point out that the security of the protocol must be systematically analyzed depending on the type of attackers, and be studied a noise stability. We hope that the quantum sequential transmission, QST_ε, can be used and applied to quantum information processing.

---

[1] M. Hillery, V. Bužek, and A. Berthiaume, *Quantum secret sharing*, Phys. Rev. A **59**, 1829 (1999).

[2] R. Cleve, D. Gottesman, and H. K. Lo, *How to share a quantum secret*, Phys. Rev. Lett. **85**, 648 (1999).

[3] A. Karlsson, M. Koashi, and N. Imoto, *Quantum entanglement for secret sharing and secret splitting*, Phys. Rev. A **59**, 162 (1999).

[4] W. Tittel, H. Zbinden, and N. Gisin, *Experimental demonstration of quantum secret sharing*, Phys. Rev. A **63**, 042301 (2001).

[5] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and, P. K. Lam, *Tripartite Quantum State Sharing*, Phys. Rev. Lett. **92**, 177903 (2004).

[6] M. Naseri, *Secure quantum sealed-bid auction*, Opt. Commun. **282**, 1939 (2009).

[7] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, *Private quantum channels*, In *IEEE Symposium on Foundations of Computer Sciences (FOCS)*, p. 547, (2000).

[8] D. Nagaj and I. Kerenidis, *On the optimality of quantum encryption schemes*, J. Math. Phys. **47**, 092102 (2006).

[9] J. Bouda and M. Ziman, *Optimality of private quantum channels*, J. Phys. A **40**, 5415 (2007).

[10] P. Hayden, D. Leung, P. W. Shor, and A. Winter, *Randomizing quantum states: Constructions and applications*, Commun. Math. Phys. **250**, 371 (2004).

[11] A. Ambainis and A. Smith, *Small Pseudo-Random Families of Matrices: Derandomizing Approximate Quantum Encryption*, In *Proceedings of RANDOM.* p. 249 (2004).

[12] P. A. Dickinson and A. Nayak, *Approximate Randomization of Quantum States With Fewer Bits of Key*, AIP Conference Proceedings **864**, 18 (2006).

[13] M. Ziman and V. Bužek, *All (qubit) decoherences: complete characterization and physical implementation*, Phys. Rev. A **72**, 022110 (2005).