ON SQUEEZED GAUSSIAN PRIVATE QUANTUM CHANNELS

Kabgyun JEONG [1] , Jaewan KIM [1] and Su-Yong LEE [2]

1) *School of Computational Sciences, Korea Institute for Advanced Study, Hoegiro 85, Dongdaemun, Seoul 130-722, KOREA*

2) *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543 Singapore, SINGAPORE*

Corresponding Author : Kabgyun JEONG, kgjeong6@kias.re.kr

ABSTRACT

We propose a Gaussian private quantum channel with squeezed coherent states, which is a generalization of continuous-variable private quantum channel (CVPQC) [Phys.Rev.A 72, 042313 (2005)]. We show that squeezed coherent states satisfy with the conditions of the CVPQC. In the regime of small squeezing, we can consider even a non-Gaussian regime by replacing the squeezing operation with a superposition operation of two different displacements.

INTRODUCTION

The notion of private quantum channel (PQC) or quantum one-time pad is very useful in quantum information processing, such as superdense coding, quantum data hiding, quantum state sharing protocol (for improving their efficiency), and the proof of additivity counter-example of the classical capacity on quantum channels. The PQC is briefly introduced as follows. If the two communicating parties, Alice and Bob, share a classical secret key (e.g., via quantum key distribution procedure), then PQC can be used to transmit an arbitrary unknown quantum state from Alice to Bob securely. The intermediate state in PQC is close to the maximally mixed state, so the state exhibits almost maximal entropy. The receiver Bob always decrypts the encoded state by using the unitary inverse operations from the pre-shared secret key, whereas no third party (not having the key) can obtain the original quantum state. A discrete version of private quantum protocol was first proposed by Ambainis *et al*. in 2000 [1], and the optimality of PQC was proved that we need exactly d^2 unitary operations to encrypt a d-dimensional quantum state. In the case of approximate encryption, it is sufficient to have the number of unitary operations being less than $d \log d$.

Then, it is natural to ask how we can realize the above mentioned protocols in continuous variable (CV) systems. Previously Brádler proposed CV private quantum channel (PQC) using coherent states that are obtained by displacement operations on the vacuum state [2], where he defined a CV maximally mixed state in Gaussian regime and then constructed CVPQC via the *conformation* method of coherent states. Generally a single-mode Gaussian state is parametrized as a combination of displacement, squeezing operations and a thermal field. Specifically squeezed states, which were considered in CV quantum key distribution, are crucial for a security demonstration of quantum key distribution using coherent states. Moreover squeezed

coherent states are useful for enhancing the security of quantum cryptography, and for improving phase sensitivities of interferometers.

In this paper, we generalize the continuous variable private quantum channel (CVPQC) with a combination of displacement and *squeezing* operations. More explicitly, we show that our construction well represents the dependance of the displacement and the squeezing elements, $\exp\left[-r_p^2\{1-\tanh r\cdot\cos(2\theta_{pq}-\phi)\}\right]$ whereas Brádler's CVPQC only depends on $\exp(-r_p^2)$ term of a coherent state [3]. In the limit of small squeezing, we reach a non-Gaussian regime by replacing the squeezing operation with a non-Gaussian operation, i.e., a superposition operation of two different displacements. Furthermore we propose an implementable scheme for the non-Gaussian operation.

ACKNOWLEDGEMENT

This work was partly supported by the IT R&D program of MOTIE/KEIT [10043464 (2014)]. SYL acknowledges support from FQXI and the National Research Foundation and Ministry of Education in Singapore.

REFERENCES

1. Ambainis A., Mosca M., Tapp A. and de Wolf R., *Private quantum channels*, *IEEE Symposium on Foundations of Computer Sciences* (FOCS) p. 547 (2000).
2. Brádler, K., *Continuous-variable private quantum channel*, *Physical Review A*, Vol. 72, 042313, 2005.
3. Jeong, K., Kim, J. and Lee, S.-Y., *Gaussian private quantum channel with squeezed coherent states*, Submitted (2014).