Evaluation of quantum gain for KCQ protocol using best multi-ary codes in high or low rate

Mana Yoshida[1] * Shogo Usami[2] † Tsuyoshi Sasaki Usuda[1] ‡

[1] *Graduate School of Information Science and Technology, Aichi Prefectural University,*
1522-3 Ibaragabasama, Nagakute-shi, Aichi, 480-1198, Japan
[2] *School of Science and Engineering, Meijo University,*
1-501 Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi 468-8502, Japan

Abstract. In AQIS2019, we evaluated keyed communication in quantum noise (KCQ) protocols using binary codes that are the best in terms of reliable communications. In this paper, we consider the best 'multi-ary' codes. As a result, it is clarified that the best codes in reliable communications are not good for KCQ protocols, also in the case of 4-ary signals.

Keywords: quantum cryptography, KCQ protocol, quantum gain, reliability function

1 Introduction

Quantum gain is a key concept not only for quantum communications but also for quantum cryptography. As the latter applications, there is a keyed communication in quantum noise (KCQ) [1]. Its security is based on the difference in performance of an optimum measurement by the presence of a key. There are many realization methods of the KCQ [1]∼[6]. We are interested in an asymptotic property of the KCQ by using classical codes [5, 6]. In AQIS2019, we considered the best binary codes, which corresponds to [5]. In this paper, we consider the best multi-ary codes, which corresponds to [6].

2 Overview of Reliability Function

To consider an asymptotic property of the KCQ by using classical codes, we compute upper and lower bounds of the reliability function $E(R)$. Here, we briefly introduce $E(R)$. Let $P_{\rm e}^{\rm opt}(n,R)$ be the best error probability for n and R, where n and R are the length and the rate of the code, respectively. Then it is expressed by the so-called *reliability function* $E(R)$ as

$$P_{\rm e}^{\rm opt}(n,R) = e^{-nE(R)}. \qquad (1)$$

For both classical and quantum cases, the tight upper and lower bounds of $E(R)$ are known [7]∼[11]. Therefore, we can say $E(R)$ is obtained in sufficient accuracy. Let $P_{\rm C}$ and $P_{\rm Q}$ be the best error probabilities obtained by (1) for classical and quantum cases, respectively.

3 Quantum Gain

In this study, we consider 4PSK (4-ary phase shift keying) coherent-state signals. The signals are characterized by the average number of photons $N_{\rm s}$.

The quantum gain can be expressed using $N_{\rm s}$ in the quantum and classical cases when their error probabilities P have the same value [12]:

$$\text{Gain} = 10\log_{10}\frac{N_{\rm s}^{\rm C}(\text{When } P_{\rm C}=P)}{N_{\rm s}^{\rm Q}(\text{When } P_{\rm Q}=P)} \quad [\text{dB}]. \qquad (2)$$

4 Result and Summary

Table 1 shows quantum gain property of 4PSK signals in high and low rates. From Table 1, quantum gain with $n = 10000$ is almost same as that with $n = 1000000$. This means we cannot expect to obtain huge quantum gain by the best code even if we lengthen the codeword length. Therefore, what we need is not the best code but other codes to obtain large quantum gain.

Table 1: Quantum gain [dB] of 4PSK signals.

R	P	Gain	Gain
		$n = 10000$	$n = 1000000$
0.3	10^{-12}	7.716	7.868
0.3	1	7.499	7.890
0.2	10^{-12}	8.018	8.291
0.2	1	8.329	8.329
0.1	10^{-12}	8.415	8.949
0.1	1	9.031	9.031

Acknowledgments: This work has been supported in part by JSPS KAKENHI Grant Number JP20H00581, JP20K20397.

* im191013@cis.aichi-pu.ac.jp
† susami@meijo-u.ac.jp
‡ usuda@ist.aichi-pu.ac.jp

References

[1] H.P. Yuen, "KCQ: A new approach to quantum cryptography I. General principles and key generation," arXiv:quant-ph/0311061v6, (2004).

[2] E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen, "Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks," Phys. Rev. **A71**, 062326, (2005).

[3] O. Hirota, M. Sohma, M. Fuse, and K. Kato, "Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme," Phys. Rev. **A72**, 022335, (2005).

[4] K. Kato and O. Hirota, "Quantum quadrature amplitude modulation system and its applicability to coherent-state quantum cryptography," Proc. SPIE 5893, Quantum Communications and Quantum Imaging III, (2005).

[5] A. Kadoya, Y. Umemura, S. Asano, N. Iwata, and T.S. Usuda, "KCQ using binary linear code and its performance," Proc. of AQIS2015, pp.161-162, (2015).

[6] A. Kadoya and T.S. Usuda, "Quantum gain for KCQ protocol using multi-ary equidistant code," Proc. SITA2016, pp.360-365, (2016). (in Japanese)

[7] R.G. Gallager, "Information Theory and Reliable Communication," John Wiley & Sons, Inc., New York, (1968).

[8] M.V. Burnashev and A.S. Holevo, "On reliability function of quantum communication channel," Probl. Peredachi Inform. **34**, 2, pp.1-13, (1998).

[9] M. Dalai, "Lower bounds on the error probability for classical and classical-quantum channels," IEEE Trans. on Inform. Theory **59**, 12, pp.8027-8056, (2013).

[10] K. Kato, "Error exponents of quantum communication system with M-ary PSK coherent state signal," Tamagawa Univ. Quant. ICT Res. Inst. Bulletin, **1**, 1, pp.33-40, (2011).

[11] K. Kato, "A note on the reliability function for M-ary PSK coherent state signal," Tamagawa Univ. Quant. ICT Res. Inst. Bulletin, **8**, 1, pp.21-25, (2018).

[12] K. Kurokawa and O. Hirota, "Properties of quantum reliability function and its applications to several quantum signals," IEICE Trans. on Fundamentals. **J83-A**, pp.57-66, (2000). (in Japanese)