Quantum Hexagonal Quadrature Amplitude Modulation

YoungJun Kim

School of Electrical Engineering
Korea University
Seoul, South Korea
Email: mkeeper@korea.ac.kr

Young-Chai Ko

School of Electrical Engineering
Korea University
Seoul, South Korea
Email: koyc@korea.ac.kr

***Abstract*—In this paper, we propose the hexagonal quadrature amplitude modulation (QAM)-type modulation for continuous-variable quantum communication systems. Our proposed hexagonal QAM modulation provides less detection error, which occurs in discriminating non-orthogonal quantum states, compared to the previous modulation schemes such as phase shift keying (PSK)-type modulation or rectangular QAM-type modulation. Square root measurement (SRM) is used in the receiver to decrease the detection error probability and receiver complexity. The theoretical detection error rate for the hexagonal QAM modulation is obtained by form of square root of matrix. The detection error rate is verified by Monte Carlo simulation.**

Keywords–Quantum communication, hexagonal QAM, continuous variables, coherent states

I. INTRODUCTION

As the usage of personal communication devices increases, the communication security system becomes more important than ever. The quantum cryptography using quantum key distribution (QKD) is regarded as the future possible technology to guarantee unconditional security [1]. Basically, the quantum cryptography is based on the fact that nonorthogonal quantum states can not be distinguished with certainty [2]. Note that the detection of coherent states is accomplished by quantum measurement which naturally brings about the detection errors.

In this paper, we consider a quantum detection problem. Alice transmits classical information key to Bob through quantum channel. Both Alice and Bob prepare a set of quantum coherent states, and Alice chooses one of the states corresponding to the message. The receiver, Bob, extracts the message from a quantum measurement of the received quantum state. Because the set of coherent states Alice and Bob use are not orthogonal to be general, all measurement can bring about the detection error. Our design goal is to build the shared set of quantum states and to build the quantum measurement.

This quantum detection problem has been researched in many previous papers [3]–[6]. In [6], Yuen contrived a new quantum cryptography which also ensures the unconditional security. The protocol invented by Yuen is called Y-00 protocol named after himself. In Y-00, a set of phase shift keying (PSK) type states is considered. Security is from the detection error rate gap between Bob and Eve, an eavesdropper, where Bob shares an initial secret key string with Alice but Eve does not. Y-00 protocol opened a new type of QKD, *continuous variable quantum key distribution (CV-QKD)*, by using coherent states as information carrier.

Positive operator valued measurement (POVM) is a set of Hermitian positive semidefinite operators. In quantum mechanics, all observable quantity is obtained by a special quantum transaction called *quantum measurement*. By subjecting the state to a quantum measurement, we can obtain a value corresponding to the quantum state. POVM is widely used to measure quantum states because it is easy to realize in a physical system and because it has good mathematical properties for performance analysis [2] [7].

The QAM provides better performance than the PSK in terms of the error probability in higher spectral efficiency case [8]. For this reason, QAM is adopted in many recent communication standards to meet the demand of high speed data rate. The constellation of QAM has several shapes such as square QAM, circular QAM, hexagonal QAM and so on. It is notable that the hexagonal QAM provides the largest minimum Euclidian distance (ED) given the energy constraint compared to other QAM schemes. Hexagonal QAM gives less error rate performance than rectangular QAM but hexagonal QAM is not popular in practical communication systems because of its high implementation complexity compared to other QAM shapes [9].

For PSK scheme, which has the circular symmetric quantum states set, the square root measurement (SRM) detection has been proven to provide the minimum detection error probability [2]. On the other hand, for QAM state, which does not have the circular symmetric quantum states set, the optimum detection scheme in terms of error probability has not been known yet. However, SRM detection can provide quite a good performance when the average number of photons of coherent states, Ns, is sufficiently large based on which the application of SRM detection to QAM has been studied in the literature [10]. The set of QAM state is not circular symmetric but Kato employed SRM for QAM state detection problem. Optimality of SRM for QAM state detection is not proven. But detection probability of QAM state using SRM gives less detection error than PSK state using SRM with same energy constraint.

In SRM detection, the ED between two states is the dominant factor for error detection. In a state set, we have shown in a previous study [11] that the average detection error probability is dominant with the minimum ED among the states of the set. We have shown that circular QAM scheme can reduce the detection error rate by enlarging the minimum ED under a given energy constraint. Moreover, hexagonal QAM scheme has larger minimum ED than circular QAM scheme so we can expect that hexagonal QAM scheme gives less detection error rate than PSK, rectangular QAM and circular QAM.

 ISBN: 978-1-61208-495-4

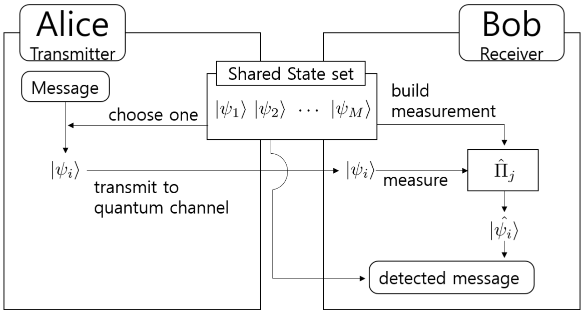

Figure 1. System description

This paper is organized as follows. In Section 2, the mathematical representation of our considering system is described. In Section 3, the SRM detection scheme in the receiver is mathematically described. In Section 4, our new hexagonal QAM scheme is suggested. In Section 5, we show the detection error performance of our hexagonal QAM scheme with SRM detection in a numerical way. Finally, Section 6 concludes the paper.

II. MATHEMATICAL SYSTEM REPRESENTATION

Let us consider the detection problem of quantum states illustrated in Figure. 1. Alice chooses one of pure states in a set of coherent states and sends it to Bob. Then Bob measures the received state and chooses one of the states based on the minimum detection error criterion. Note that an error occurs if the state chosen by Bob is different from Alice's state.

We consider a pure state set ρ of size M in Hilbert space $\mathcal{H}_s$. Each state of ρ is represented by density operator ρ_i which is non-negative and unit trace.

$$\rho_i \geq 0, \qquad \text{Tr}\,[\rho_i = 1] \qquad\qquad (i = 1, 2, \ldots, M). \tag{1}$$

From the pure state assumption, each state can be also represented in vector form such as

$$\rho_i = |\psi_i\rangle \langle\psi_i| \tag{2}$$

where $|\psi_i\rangle$, called *ket* ψ_i, is Dirac's bra-ket notation of the quantum state and $\langle\psi_i|$, called *bra* ψ_i, is the dual state of $|\psi_i\rangle$.

A coherent state $|\alpha\rangle$ is an eigen state of photon annihilation operator, a [12],

$$a\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{3}$$

and can be expressed using the representation in the basis of number states, $|n\rangle$,

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{4}$$

Note that α can be an arbitrary complex value where the real part of α relies on the position of the photon and the imaginary part of α relies on the momentum of the photon [13].

For detection of the received states, we employ the POVM $\hat{\Pi}_j$ which satisfies the following relations

$$\hat{\Pi}_j \geq 0, \tag{5}$$

and

$$\sum_{j=1}^{M} \hat{\Pi}_j = \hat{I}. \tag{6}$$

Let us denote $P(j|i) \triangleq P(\rho_j|\rho_i)$ as the conditional probability that the quantum state ρ_i is decided as ρ_j. Then $P(j|i)$ can be represented as

$$P(j \mid i) = \text{Tr}\,[\hat{\Pi}_j \rho_i]. \tag{7}$$

Note that the value $P(j|i)$ for $(j \neq i)$ represents the decision error probability. Then the average probability of decision error P_e is given by

$$\begin{aligned} P_e &= \sum_{i=1}^{M} q_i \sum_{j=1(\neq i)}^{M} P(j \mid i) \\ &= 1 - \sum_{i=1}^{M} q_i P_i(i \mid i) \end{aligned} \tag{8}$$

where q_i is *a priori* probability of the quantum state ρ_i satisfying

$$\sum_{i=1}^{M} q_i = 1, \qquad\qquad q_i \geq 0. \tag{9}$$

To simplify the discussion, we focus on the equal probable case, that is $q_i = \frac{1}{M}$ for all i.

III. DETECTION ERROR PERFORMANCE OF SQUARE ROOT MEASUREMENT

Quantum measurement is defined as a set of operators. In quantum mechanics, an operator is similar to a system in classical mechanics. As long as the state in quantum is represented in a vector form, the quantum operator can also be represented in a matrix form. POVM is a good example of quantum measurement.

Now, we consider SRM for detection. SRM is known as the optimal detection measurement scheme in distinguishing circular symmetric states, i.e., PSK states, in terms of detection error rate. Note that when the state set is not circular symmetric, the optimal detection measurement scheme is not known yet. However, as shown in [14]–[17], SRM is often employed for non-symmetric case since it can be built by manipulating the shared state set. Here, we also employ SRM for the signal detection of hexagonal states considered in. The hexagonal states set considered in this paper is not circular symmetric. But SRM has been employed in many systems because of its good properties [18].

The detection operator of SRM, denoted as $\hat{\Pi}_j$ for the j-th state is defined as [17]:

$$\begin{aligned} \hat{\Pi}_j &= |\mu_j\rangle \langle\mu_j| \\ |\mu_j\rangle &= \hat{G}^{-1/2}\,|\psi_j\rangle \\ \hat{G} &= \sum_{i=1}^{M} |\psi_i\rangle \langle\psi_i|\,. \end{aligned} \tag{10}$$

We can easily prove that SRM, $\hat{\Pi}_j$, satisfies (5) and (6) just by substituting $\hat{\Pi}_j$ into (5) and (6). It means that SRM is a class of POVM and we can get the advantage of POVM mentioned in Section I.

In the case of using SRM in detection, the conditional detection error probability $P(j|i)$ can be calculated by square root of the Gram matrix G

$$p(j \mid i) = \left|(G^{1/2})_{ji}\right|^2 \tag{11}$$

where the Gram matrix G is the Hermitian matrix whose entries are inner products of coherent states [2]

$$G = \begin{bmatrix} \langle\psi_1|\,\psi_1\rangle & \cdots & \langle\psi_1|\,\psi_M\rangle \\ \vdots & \ddots & \vdots \\ \langle\psi_M|\,\psi_1\rangle & \cdots & \langle\psi_M|\,\psi_M\rangle \end{bmatrix}. \tag{12}$$

From (4), the inner product of two coherent states can be calculated as

$$\begin{aligned} \langle\alpha|\,\beta\rangle &= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} \frac{\alpha^{*m}\beta^n}{\sqrt{m!n!}} \langle m|\,n\rangle \\ &= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{n=0}^{\infty} \frac{(\alpha^*\beta)^n}{n!} \\ &= e^{-\frac{|\alpha|^2+|\beta|^2}{2}+\alpha^*\beta} \\ &= A_{\alpha\beta}\exp \jmath\theta_{\alpha\beta} \end{aligned} \tag{13}$$

where

$$A_{\alpha\beta} = \exp\left[-\frac{1}{2}\left((\alpha_R-\beta_R)^2+(\alpha_I-\beta_I)^2\right)\right] \tag{14}$$

$$\theta_{\alpha\beta} = [\alpha_R\beta_I - \alpha_I\beta_R]\,. \tag{15}$$

and

$$\alpha_R = \mathfrak{Re}\{\alpha\}, \alpha_I = \mathfrak{Im}\{\alpha\}, \beta_R = \mathfrak{Re}\{\alpha\}, \beta_I = \mathfrak{Im}\{\alpha\}.$$

In (11), we point out that the off-diagonal element of square root of the Gram matrix directly influences the conditional detection error probability. In (12), we can see that the off-diagonal elements of the Gram matrix is in inner product form between two different states. In (14), the Euclidian distance between two different states is the dominant factor in the amplitude of inner product between the states. Now, we can say that a states set with large minimum ED can reduce the detection error rate. Hence, it is desired to make the signals spread as far as they can in given signal average energy constraint.

IV. Minimum Euclidian distance Maximizing modulation : Hexagonal QAM

In classical communication systems, the hexagonal QAM scheme is used because of low peak to average power ratio [9] or used in the case considering multiple retransmission system for the automatic repeat request [19]. But hexagonal QAM scheme is rarely used because it can not be demodulated by the two dimensional projective way which deduces the complexity of the receiver.

To detect quantum coherent states, the two dimensional projective way is limited by Heisenberg type uncertainty. In this paper, we consider SRM detection and the detection error performance of SRM is affected by the minimum ED among the states. The hexagonal QAM state gives the largest minimum ED under a given energy constraint.

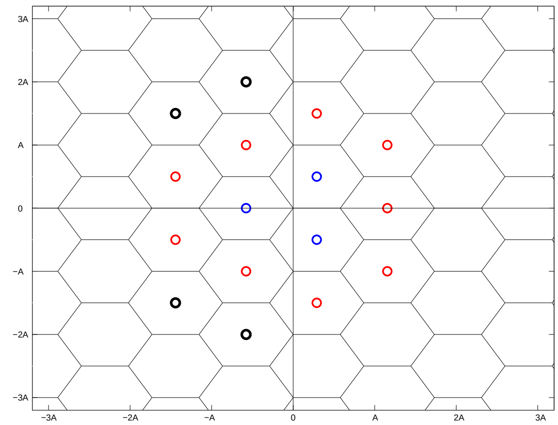

Figure 2. States set for 16-ary hexagonal QAM

The shape of constellation points of Hexagonal QAM is in the form of a shell. We can easily find the number of signals that make the complete shell, and that number is

$$3n^2, n \in \mathbb{N} \tag{16}$$

where n is the number of shells. Figure. 2 shows an example of quantum hexagonal QAM states for $M = 16$ case. States for 16-QAM are denoted as

$$\begin{aligned} |\psi_1\rangle &= |A(-\frac{\sqrt{3}}{3})\rangle \\ |\psi_2\rangle &= |A(\frac{\sqrt{3}}{6}+\jmath\frac{1}{2})\rangle \\ |\psi_3\rangle &= |A(\frac{\sqrt{3}}{6}-\jmath\frac{1}{2})\rangle \\ &\vdots \\ |\psi_{16}\rangle &= |A(-\frac{\sqrt{3}}{3}+\jmath 2)\rangle \end{aligned} \tag{17}$$

where A is a real valued fundamental amplitude. Euclidian distance between most neighboring states is set to be A.

We can see that the first and the second shell is full of states, and the third shell has empty spaces. These empty spaces degrade data rate performance. In our quantum modulation, we consider uncoded classical information so the gap between 2^n for classical bit and (16) for hexagonal QAM symbol degrades the rate.

V. Numerical Result

For comparing the error rate of detection, the average value of the photon number, N_s is a common parameter which is defined as:

$$N_s = \sum_{i=1}^{M} q_i \langle\psi_i|\,\hat{n}\,|\psi_i\rangle \tag{18}$$

where $\hat{n} = \hat{a}^\dagger\hat{a}$ is the number operator of the coherent state. The detection error probability is calculated by substituting (17) to (13), (12), (11) and (8). In (11), square root of Hermitian matrix is calculated by eigen value decomposition in MATLAB.

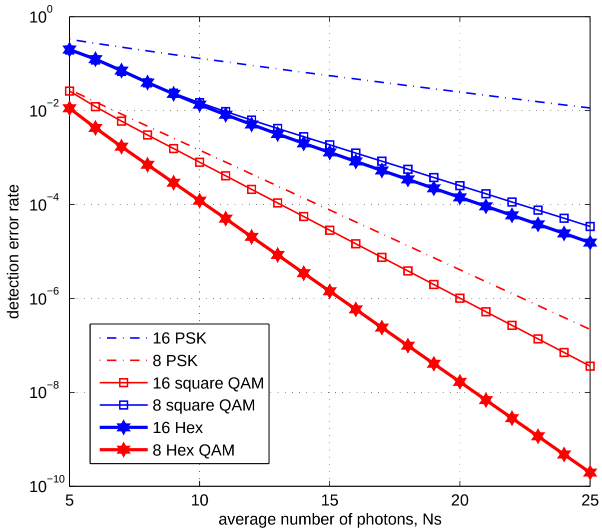

Figure 3. Detection error rate for $M = 8$ and $M = 16$

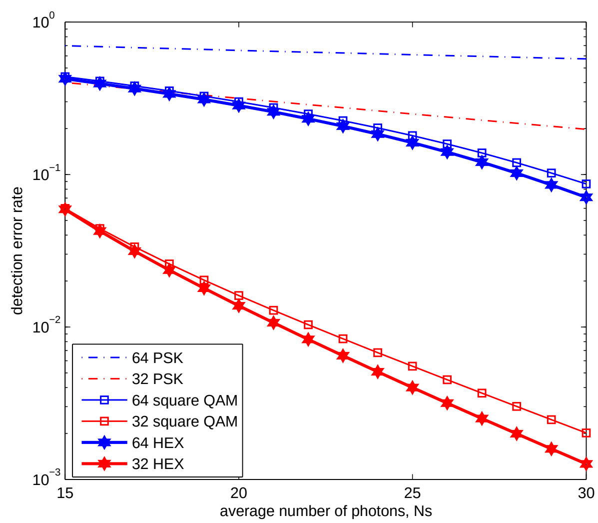

Figure 4. Detection error rate for $M = 32$ and $M = 64$

As seen in Figure 3, we can certify that all types of QAM schemes give less detection error rate than the PSK scheme. The rectangular QAM states are from [17]. The detection error rate of our hexagonal QAM scheme is less than other modulation schemes. And we can also see that the performance gain of our hexagonal QAM scheme is steady compared to the rectangular QAM case which works well in $M = 16$ case but does not work well in $M = 8$ case relatively. Figure 4 shows the detection error rates for higher order cases in large N_s. Our hexagonal QAM scheme also performs better than other schemes in detection error rate in higher order cases. Especially, we can find a cross-over between PSK scheme for $M = 32$ and hexagonal QAM scheme for $M = 64$. It means that our hexagonal QAM state can carry more information bits and can give less detection error performance in some cases.

As the modulation size M grows, we need more photons to meet a certain detection error rate. Our hexagonal QAM scheme still has performance gain in higher modulation cases. The average number of photons to meet a certain detection error rate is still less in our hexagonal QAM state for higher order cases.

VI. CONCLUSION

In this paper, we proposed a new hexagonal QAM scheme that reduces the detection error probability by maximizing the minimum ED between states in the constellation. We used SRM to detect the sent state. Numerical simulation showed that our hexagonal QAM gives less detection error rate under an average photon number constraint in several sizes of modulation.

ACKNOWLEDGMENT

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-R0992-16-1017) supervised by the IITP(Institute for Information & communications Technology Promotion)

REFERENCES

[1] D. Mayers, "Unconditional security in quantum cryptography," *J. of the ACM*, vol. 48, no. 3, pp. 351–406, 2001.

[2] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, "Optimum measurements for discrimination among symmetric quantum states and parameter estimation," *Int. J. of Theoretical Phys.*, vol. 36, no. 6, pp. 1269–1288, 1997.

[3] C. W. Helstrom, "Bayes-cost reduction algorithm in quantum hypothesis testing (corresp.)," *IEEE Trans. Inform. Theory*, vol. 28, no. 2, pp. 359–366, 1982.

[4] K. Kato and O. Hirota, "Quantum quadrature amplitude modulation system and its applicability to coherent-state quantum cryptography," in *Optics & Photonics 2005*. Int. Soc. for Optics and Photonics, 2005, pp. 589 303–589 303.

[5] ——, "Square-root measurement for quantum symmetric mixed state signals," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3312–3317, 2003.

[6] H. P. Yuen, "KCQ: A new approach to quantum cryptography i. general principles and key generation," *arXiv preprint quant-ph/0311061*, 2003.

[7] M. Ziman and V. Bužek, "Realization of positive-operator-valued measures using measurement-assisted programmable quantum processors," *Phys. Rev., A*, vol. 72, no. 2, p. 022343, 2005.

[8] J. G. Proakis, *Digital Communications*. McGraw-Hill, 1995.

[9] S. H. Han, J. Cioffi, and J. H. Lee, "On the use of hexagonal constellation for peak-to-average power ratio reduction of an ODFM signal," *IEEE Trans. Wireless Commun.*, vol. 7, no. 3, pp. 781–786, March 2008.

[10] P. Hausladen and W. K. Wootters, "A pretty goodmeasurement for distinguishing quantum states," *J. of Modern Optics*, vol. 41, no. 12, pp. 2385–2390, 1994.

[11] Y. Kim and Y.-C. Ko, "Detection of quantum circular QAM signals," in *Int. Conv. Inform. and Commun. Technology*, Oct 2013, pp. 1078–1082.

[12] H. P. Yuen, "Two-photon coherent states of the radiation field," *Phys. Rev., A*, vol. 13, no. 6, p. 2226, 1976.

[13] P. Carruthers and M. M. Nieto, "Phase and angle variables in quantum mechanics," *Rev. Mod. Phys.*, vol. 40, pp. 411–440, Apr 1968. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.40.411

[14] A. Peres and W. K. Wootters, "Optimal detection of quantum information," *Phys. Rev. Lett.*, vol. 66, no. 9, p. 1119, 1991.

[15] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, "Quantum channels showing superadditivity in classical capacity," *Phys. Rev., A*, vol. 58, no. 1, p. 146, 1998.

[16] M. Sasaki, T. Sasaki-Usuda, M. Izutsu, and O. Hirota, “Realization of a collective decoding of code-word states,” *Phys. Rev., A*, vol. 58, no. 1, p. 159, 1998.

[17] K. Kato, M. Osaki, M. Sasaki, and O. Hirota, “Quantum detection and mutual information for QAM and PSK signals,” *IEEE Trans. Commun.*, vol. 47, no. 2, pp. 248–254, 1999.

[18] Y. C. Eldar and G. D. Forney Jr, “On quantum detection and the square-root measurement,” *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 858–872, 2001.

[19] L. Snzecinski and M. Bacic, “Constellations design for multiple transmissions maximizing the minimum squared euclidean distance,” in *IEEE conf. Wireless Commun. and Networking*, vol. 2, March 2005, pp. 1066–1071 Vol. 2.