シングルモード型 KCQ における半古典的量子受信機の性能解析

梅村 勇貴　　指導教員：臼田 毅

1 はじめに

インターネット上で通信の安全を保つために，送信される情報には暗号化が施されている．そのため，第三者が盗聴行為に及んだとしても，暗号が解読されない限り情報の機密性は守られる．現在用いられている暗号は数理暗号と呼ばれ，離散対数問題や複雑な計算過程による計算量の膨大さで安全性を確保している．これらは，現在明らかとされている計算能力では，解読には百年以上かかると言われている．しかし，現在研究が進められている量子計算機が実現した場合，数理暗号の安全性が破綻する恐れがある．そこで，計算量に依存しない暗号が必要とされ，研究されている．

KCQ (Keyed Communication in Quantum noise) プロトコル [1] は，Gbps 単位の通信速度と古典情報理論に基づく Shannon 限界を超える安全性の双方を達成可能であることが期待されている現在唯一の量子暗号プロトコルである．KCQ プロトコルでは，正規のユーザ間で予め秘密鍵を共有しておき，その鍵を用いて正規受信者と盗聴者の間に受信能力の差をつけることで，盗聴者に正しい受信データが行き渡らないようにすることを安全性の根拠としている．そのため，KCQ プロトコルの安全性解析では，盗聴者の誤り率の下界を調べることが重要である．KCQ プロトコルの安全性解析では，プロトコルの発案者である Yuen の手法 [1] を踏襲し，盗聴者の誤り率の下界を求める．盗聴者の行う攻撃法として，KCQ に対して最適攻撃と呼ばれるヘテロダイン受信機 [1] とそれを超える可能性のある攻撃として半古典的量子受信機 [2, 3] の 2 つが考えられており，今までに ASK (Amplitude Shift Keying)，PSK (Phase Shift Keying)，QAM (Quadrature Amplitude Modulation) などの様々な信号系に対する各々の受信機の誤り率が示されてきた [2, 3]．しかし，先行研究では，半古典的量子受信機における測定点は信号点の数しか取られていない．本研究では，先行研究で行われてきたシングルモードの信号系である ASK，PSK，QAM 方式に対して信号点以上の測定点を取る半古典的量子受信機の測定の「多様化」を行い，半古典的量子受信機の特性を明らかにして，ヘテロダイン受信機と比較を行った．なお，本稿には振幅のみを変調する ASK と，位相のみを変調する PSK を組み合わせた振幅と位相の両方を変調する QAM 方式の結果のみを記す．

2 本研究の通信プロトコル

QAM 信号は，2 つの直交振幅成分 $X_{\rm c}, X_{\rm s}$ が変調された信号である．本研究では，先行研究 [4] に習い，以下の式で表されるような格子状の最小単位を α_0 とした QAM コヒーレント状態信号を扱う．

$$|\psi_{p,q}\rangle = |\alpha_0(p+\mathbf{i}q)\rangle,\ (p,q)\in\Omega\times\Omega, \tag{1}$$

$$\Omega = \{-(L-1)+2(i-1)\mid i=1,2,\cdots,L\}. \tag{2}$$

ここで，$\mathbf{i}=\sqrt{-1}$ である．また，信号数を M とすると，$M=L^2$ となる．次に，本研究の通信手順を説明していく．

(i) 送信者は，送信データを M 元コヒーレント状態信号のうち，定められた 2 つの状態（信号ペア）のいずれかに変調して送信する．
(ii) 受信者は受信した量子状態信号に対して測定を行う．
(iii) 送信者の使用した信号ペア (図 1 でいうと赤と青の状態) の情報を得る．
(iv) 測定した結果と信号ペアの情報を用いて，測定した信号が信号ペアのどちらである確率が高いか，最尤決定を行い受信データを得る．

本研究では，Yuen の安全性解析の手法 [1] に則っている．Yuen の安全性解析の手法は以下のようになっている．

- 盗聴者に送信量子状態のフルコピーを与える．
- 盗聴者の測定後に鍵を仮想的に開示する．

3 本研究で用いる受信機

本研究で用いる受信機として，KCQ に対して最適な攻撃法と言われているユニバーサルなヘテロダイン受信機 [1] と，KCQ の安全性解析に応用されており，ヘテロダイン受信機を超える可能性が示されている半古典的量子受信機 [2, 3] の 2 つを考える．

3.1 ヘテロダイン受信機

ヘテロダイン受信機は，信号の 2 つの直交振幅成分 $X_{\rm c}, X_{\rm s}$ を同時測定し，その測定結果として，2 次元のアナログ値を得る．その測定結果と信号ペアの情報を用いて閾値を用いた最尤決定を行う．ヘテロダイン受信機の誤り率は以下の式で表せる．

$$P_{\rm e}^{\rm Het} = \frac{1}{2}\left(1-\frac{2}{\sqrt{\pi}}\int_0^{\frac{\sqrt{N_1}}{2}} e^{-t^2}dt\right) \tag{3}$$

ここで，式中の N_1 は信号エネルギーに当たり，信号ペア間の距離の 2 乗に等しく，$N_1=2M\alpha_0^2$ で表される．

3.2 半古典的量子受信機

半古典的量子受信機では，受信者はまず測定として SRM (Square-Root Measurement) を行い，信号系の内積を要素とするグラム行列から最尤決定に用いる条件付き確率を求める．SRM を行った後，受信者は送信に用いた信号ペア (図 1 の場合は赤と青色の信号) の情報を得て，その情報と先ほど SRM で求めた条件付き確率を用いて，自分が検出した信号が信号ペアのどちらである確率が高いのかを決定する最尤決定を行う．半古典的量子受信機で行う最尤決定は古典的最適決定と呼ばれる．古典的最適決定は，図 1 を用いて説明すると，黒破線を閾値として，閾値より左側の信号を検出した場合は赤色の信号に，右側の場合は青色の信号に，閾値上の信号を検出した場合は確率 1/2 で赤もしくは青色の信号に決定を行っている．QAM 方式では，常に閾値上の信号点が存在する．この尤度比 1 の信号点は，半古典的量子受信機の誤り率に大きな影響を与えていることが分かっている．

3.3 半古典的量子受信機の多様化

本研究では，半古典的量子受信機のさらなる性能を見るために，半古典的量子受信機の測定の多様化を行う．本稿で述べる「多様化」とは，半古典的量子受信機の測定である SRM の際の

測定点を増やすことを意味する．また，その呼び方はひとつの信号点に対して増やす測定点の数に対応する．図 1 の場合，一つの信号点に対して 4 つの測定点を増やしているので，本稿ではこれを 4-多様化と呼ぶこととする．16-QAM において半古典的量子受信機を多様化した場合のイメージを図 1 に示す．図中の黒い丸が，基の信号点から増やした測定点である．本研究では，16-QAM に対して，4- 多様化と 8-多様化を行っている．

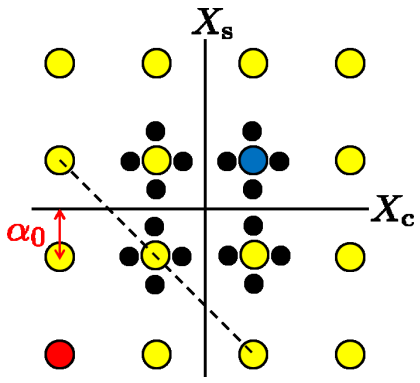

図 1　16-QAM における 4-多様化のイメージ

4　誤り率特性

まずはじめに，半古典的量子受信機における多様化を行っていない場合の QAM 方式における誤り率特性を図 2 に示す．信号数が $M = 16, 64$ のときは，半古典的量子受信機の誤り率がヘテロダイン受信機よりも高い誤り率を示していることがわかる．しかし，信号数を増やすことで，誤り率が低くなっていくことがわかる．この理由としては，全体の信号数と閾値上の信号数の割合が，信号数を増やすことで減って行くことが原因であると考えられる．また，信号数を増やしていくことで，古典最適である受信機の誤り率よりも低くなる結果は，QAM 方式特有の結果であることが判明した．このため，QAM 方式に多様化を行い，全体の測定点を増やした場合も図 2 同様に誤り率が低くなることが予想される．多様化を行った場合の 16-QAM における誤り率特性を図 3 に示す．

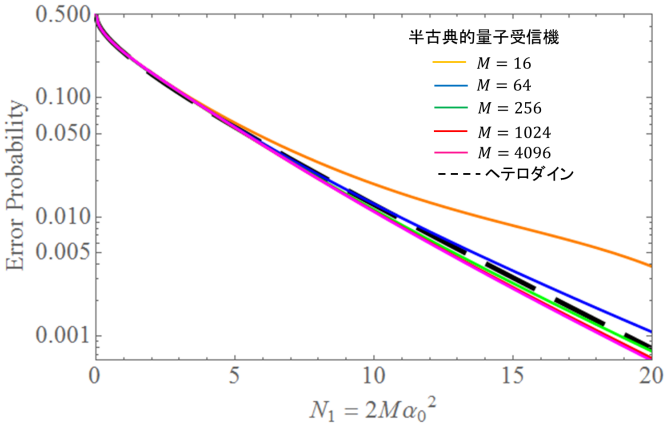

図 2　M-QAM における誤り率 (多様化なし)

図の横軸は信号エネルギー N_1 であり，縦軸は受信機の性能を表す誤り率である．本研究の結果より，図 3 の信号エネルギーの範囲にて，4-多様化した場合の半古典的量子受信機の誤り率

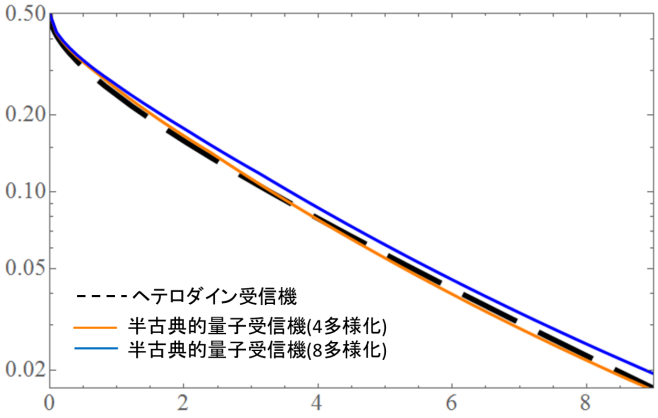

図 3　16-QAM における多様化を行った場合の各受信機の誤り率特性

がヘテロダイン受信機の誤り率よりも低くなっていることが分かった．また今回，8-多様化よりも 4-多様化のほうが誤り率が高いが，これは 8-多様化では，新たにとった測定点が尤度比 1 の点に当たる部分であったため，その点での確率的な決定が誤り率に影響を及ぼしていると考えられる．そのため，QAM 方式における半古典的量子受信機の誤り率には QAM 信号の内部の尤度比が 1 となる信号点が誤り率に影響を与えていることも今回の結果で確認できた．

以上より，半古典的量子受信機の SRM における測定点を増やすことでヘテロダイン受信機の性能を超える可能性があることを示した．

5　おわりに

本研究では，KCQ プロトコルの安全性解析に用いられている半古典的量子受信機の性能を解析するために，SRM の測定点を増やすという多様化を行い，その誤り率特性を調べてヘテロダイン受信機と比較した．その結果，16-QAM 方式において，N_1 が小さい部分で，多様化を行った場合の半古典的量子受信機の性能がヘテロダイン受信機を超える部分を新たに示すことができた．本研究の結果が，KCQ における盗聴者の最適受信機を明らかにする研究の手助けとなれば，本懐である．

今後の課題としてはまず第一により効率の良い測定点のとり方はないか，多くの形で測定点を取る必要性が挙げられる．更に，KCQ プロトコルの安全性解析への応用も重要な課題である．

公表論文

1. **Yuki Umemura**, Tsuyoshi Sasaki Usuda, Shogo Usami, Proc. of ISITA2014, p.346, (2014.10).
2. **梅村　勇貴**，臼田　毅，SITA2015 予稿集，pp.463-467, (2015.11).

参考文献

[1] H.P. Yuen, quant-ph/0311061v6, (2004).
[2] 西田, 竹下, 太田, 臼田, SITA2010 予稿集, pp.79-82, (2010).
[3] M. Takeshita, M. Ota, and T.S. Usuda, Proc. of AQIS2011, pp.137-138, (2011).
[4] K. Kato, O. Hirota, Proc. SPIE 5893, Quantum Communications and Quantum Imaging III, (2005).