QAM 型 KCQ 鍵生成における盗聴者の誤り率特性

情報科学科　梅村 勇貴　　指導教員：臼田 毅

1　はじめに

現在主に使われている暗号は数理暗号と呼ばれ，その安全性の根拠は計算量的な困難さに基づいている．しかし，将来的に計算能力が向上した場合に，その安全性が破綻することが危惧されている．そこで，量子力学的に不可避な性質を安全性の根拠に持つ量子暗号が新たに提案された．

本研究では，新量子暗号である KCQ(Keyed Communication in Quantum noise) 方式における量子鍵生成を対象とし，先行研究 [2] で考察されていなかった QAM(Quadrature Amplitude Modulation: 直交振幅変調) 方式を用いたタイプの安全性を盗聴者の受信能力 (誤り率) を示すことで評価する．

2　QAM 型 KCQ 鍵生成

KCQ 鍵生成 [1] では，正規送受信者間であらかじめ短い秘密鍵を共有することで，正規受信者と盗聴者の受信能力に差をつけ，盗聴者が正確な送信データを入手できないことを安全性の根拠としている．そのため，盗聴者の受信能力の上界を調べることは，プロトコルの安全性を評価するには重要なことである．本研究では，盗聴者の受信能力の上界を見積もるために，先行研究 [1, 2] で用いられている，盗聴者に送信量子状態のフルコピーを与え，かつ，盗聴者の信号測定後に仮想的に鍵の情報を開示するという盗聴者に有利な状況を想定した手法を用いて盗聴者の受信能力の上界を見積もることとする．

本研究で用いる QAM 方式は，2 つの直交振幅成分である $X_{\mathrm{C}}, X_{\mathrm{S}}$ の両方に情報を載せる変調方式である．それぞれ互いに独立に値を決定することができるが，本研究ではそれぞれが L 個の値をとる場合のみを考える．この場合，状態数 M は

$$M = L^2, L = 2, 3, 4, 5, \cdots \tag{1}$$

となる．M 元 QAM コヒーレント状態信号の各信号は次式で表される．

$$|\alpha_{pq}\rangle = |\alpha(p + iq)\rangle,\ p, q \in \Omega \tag{2}$$

$$\Omega = \{-(L-1) + 2(l-1) \mid l = 1, 2, \cdots, L\} \tag{3}$$

ここで，α は信号を配置した格子状の単位であり，長さなので非負の実数である．また，$i = \sqrt{-1}$ である (図 1)．

送信者は，M 個の状態のうち，秘密鍵に基づいて定められた 2 つの状態 (赤色，青色) のうちのいずれかを 2 値信号として送り，正規受信者は，鍵の情報を用いて，その 2 つの信号の信号間距離 $\beta = \sqrt{2M\alpha^2}$ の識別を行う．一方，盗聴者は鍵の知識がないため，いったん M 値信号の測定を行わなければならない．盗聴者は信号の測定後，安全性解析のために仮想的に鍵の開示を受けるので，それを用いて図 1 のような黒破線を閾値とした最尤決定を行う．このような決定法と測定として SRM(Square-root measurement) を行う受信機を半古典的量子受信機 [2] と呼ぶ．

3　盗聴者の誤り率特性

本研究では，盗聴者に与える鍵を固定し，状態数 M を増加させていった場合の盗聴者 (Eve) の誤り率特性を調べた．Eve は先述した半古典的量子受信機の他に，古典の受信機として振幅，

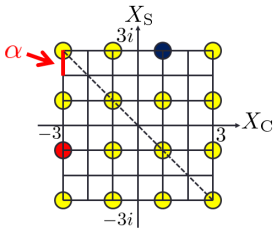

図 1　16-QAM の場合の送信信号例 (ある鍵に固定)

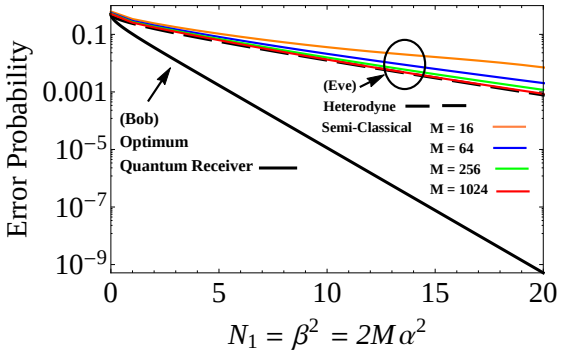

図 2　M-QAM における誤り率特性

位相などが測定できるユニバーサルなヘテロダイン受信機 [1] を用いるものとする．その結果が図 2 となる．図 2 の縦軸は誤り率，横軸は鍵とした信号間の距離 β の 2 乗に当たる $N_1 = 2M\alpha^2$ である．この結果から，半古典的量子受信機の誤り率特性はヘテロダイン受信機の誤り率特性に漸近しており，状態数が 1024 でほぼ同じ特性を示すことがわかった．これは状態数が，1024 で，漸近的に連続量とみなせることを示している．

4　まとめ

本稿では，QAM 型 KCQ 鍵生成における盗聴者の誤り率特性をその状態数を変化させて示した．その結果，鍵を固定した場合，盗聴者の誤り率特性がヘテロダイン受信機の誤り率特性に収束するような特性を示すことがわかった．今後の課題として，盗聴者にすべての鍵を与えた場合の誤り率特性の平均を調べる．それが本稿のような結果であれば，ヘテロダイン受信機の誤り率特性を調べることで盗聴者の受信能力をおよそ見積もることができる．

参考文献

[1] H.P. Yuen, quant-ph/0311061v6, (2004).
[2] M. Takeshita, M. Ota, and T.S. Usuda, Proc. of AQIS2011, pp.137-138, (2011).

公表論文

[1] 梅村 勇貴, 山下 比呂, 臼田 毅, 平成 25 年度電気関係学会東海支部連合大会, 講演論文集, F3-7, (2013.9).
[2] 梅村 勇貴, 山下 比呂, 臼田 毅, 第 36 回情報理論とその応用シンポジウム (SITA2013), pp.615-620, (2013.11).