# 多モード量子状態信号を用いた KCQ プロトコルに関する研究

角谷 昭仁　　指導教員：臼田 毅

## 1　はじめに

量子コンピュータは，現在用いられている暗号の多くを多項式時間で解くことができるとされている．そのため，量子コンピュータに対しても安全性を保証できる暗号は，将来の安全なネットワークのために必要不可欠である．そのような暗号の一つに，Keyed Communication in Quantum noise (KCQ) 原理 [1] に基づく量子暗号プロトコル（KCQ プロトコル）がある．KCQ プロトコルの安全性は，正規受信者 Bob と盗聴者 Eve の受信能力の違いに基づいており，この差は，量子利得と呼ばれる指標によって定量化される．

これまでに，Amplitude Shift Keying (ASK) 信号や Phase Shift Keying (PSK) 信号といった単一モード量子状態信号を用いた KCQ プロトコルについて，様々な成果が得られている（例えば [1, 2] など）．一方，多モード量子状態信号を用いた KCQ プロトコルについては，Pulse Position Modulation (PPM) 信号を用いる Coherent PPM (CPPM) 型 KCQ の結果 [3] 以外，ほとんど明らかにされていない．そのため，その他の多モード量子状態信号を用いた KCQ プロトコルについて解析することで，KCQ プロトコル設計の自由度を更に向上できる可能性がある．また，どのような多モード量子状態信号が高い量子利得を示すのかを明らかにすることができる．

我々は，多モード量子状態信号として，線形符号によって符号化されたコヒーレント状態信号を使用し，そのときの KCQ プロトコルの量子利得特性を明らかにしてきた [A, B, C]．本稿では，多元線形符号の一つである多元等距離符号 [4] を用いた KCQ プロトコルを説明する．この方式の量子利得を求め，CPPM 型 KCQ の量子利得との比較を行い，多元等距離符号を用いた KCQ プロトコルの優位性を示す．

## 2　多元線形符号を用いた KCQ プロトコル

### 2.1　プロトコルの手順と Eve の攻撃方法

図 1 に，本研究で考える KCQ プロトコルの大まかな全体像を示す．実行前の準備として，送信者 Alice と Bob はあらかじめ鍵を共有しているものとする．

**Alice の手順:**

1. 送信データ $\boldsymbol{x}$ を多元線形符号によって符号化する．
2. 符号語 $\boldsymbol{w}$ を対応するコヒーレント状態信号 $|\phi_{\boldsymbol{w}}\rangle$ へと写像する．本研究では，符号語の各記号に対応する量子状態を $M$ 元 PSK コヒーレント状態 $\left\{|\alpha e^{\mathbf{i}2\pi l/M}\rangle \,\middle|\, l=0,\ldots,M-1\right\}$ とする．ここで，$\alpha$ は振幅，$\mathbf{i}=\sqrt{-1}$ である．
3. 鍵 $k$ の情報に基づいてユニタリ作用素 $U_k$ を選択し，それを $|\phi_{\boldsymbol{w}}\rangle$ に施して暗号化を行う．暗号化された信号 $|\psi_{\boldsymbol{w},k}\rangle$ は，各モードの振幅と位相がばらばらな信号となる．
4. 信号 $|\psi_{\boldsymbol{w},k}\rangle$ を Bob へ送信する．

**Bob の手順:**

1. Alice から信号 $|\psi'_{\boldsymbol{w},k}\rangle$ を受信する．
2. 鍵 $k$ の情報に基づいてユニタリ作用素 $U_k^\dagger$ を選択し，それを $|\psi'_{\boldsymbol{w},k}\rangle$ に施して復号を行う．
3. 復号された信号 $|\phi'_{\boldsymbol{w}}\rangle$ に対して量子最適測定を行い，受信データ $\boldsymbol{y}$ を得る．量子最適測定とは，量子情報理論において最も低い平均誤り率を達成する測定のことである．

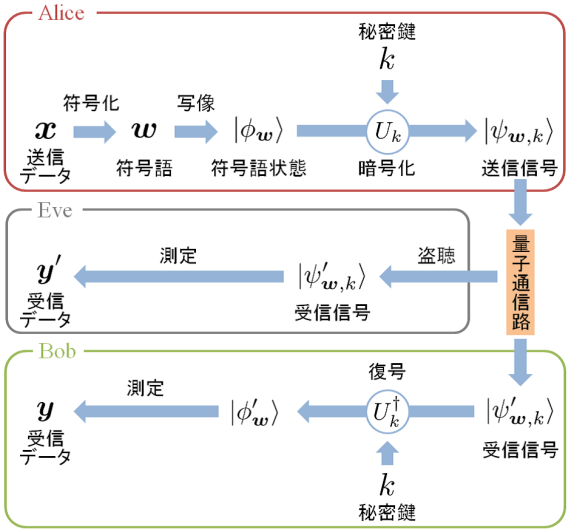


図 1　多元線形符号を用いた KCQ プロトコルの全体像

**Eve の攻撃方法:**

1. 通信路上から Alice の送った信号を盗聴する．
2. Eve は鍵を持たないため，盗聴した信号の復号ができない．そのため，暗号化された信号に対して何らかの測定を行う．
3. 測定によって得られた情報を元に，送信データへの復号を試みる．

### 2.2　量子利得

量子利得 [dB] は，次の式から求めることができる．

$$\mathrm{Gain} = 10\log_{10}\frac{N_{\mathrm{S}}^{\mathrm{Eve}}}{N_{\mathrm{S}}^{\mathrm{Bob}}} \tag{1}$$

ここで，$N_{\mathrm{S}}^{\mathrm{Bob}}, N_{\mathrm{S}}^{\mathrm{Eve}}$ は，Bob と Eve のそれぞれの誤り率 $P_{\mathrm{e}}^{\mathrm{Bob}}$, $P_{\mathrm{e}}^{\mathrm{Eve}}$ が，ある値 $P$ となるときの信号エネルギーである．

### 2.3　多元等距離符号

本研究では，文献 [4] で定義されている $\mathbb{Z}/p\mathbb{Z}$ ($p$ は素数) 上の多元等距離符号を用いる．$m$ をある自然数とすると，$[p^m-1, m]$ 等距離符号の生成行列 $G$ は，次のように定義される．

$$G = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & p-1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & \cdots & p-1 \\ 1 & 2 & \cdots & p-1 & 0 & \cdots & p-1 \end{pmatrix} \tag{2}$$

すなわち，$1,\ldots,p^m-1$ を $m$ 次元の $p$ 進数列ベクトルで表し，それを並べたものである．

## 3　Bob と Eve の測定方法と誤り率

Bob と Eve の測定方法と誤り率について説明する．なお，本研究では，量子通信路は無雑音の通信路，信号の先験確率は等確率を仮定する．

### 3.1 Bob の測定方法と誤り率

Bob は，復号した信号の測定に Square-Root Measurement (SRM) を用いる．SRM は，生起確率が等確率な線形符号に対して量子最適な測定となる [5]．$[p^m-1, m]$ 等距離符号に対する SRM の条件付き確率は文献 [4] で与えられており，今回用いる量子状態が $p$ 元 PSK コヒーレント状態信号であることと合わせて考えると，Bob の誤り率は

$$P_{\mathrm{e}}^{\mathrm{Bob}} = \frac{p^m-1}{p^{2m}}\left\{\sqrt{1+(p^m-1)e^{-p^m N_{\mathrm{S}}}} - \sqrt{1-e^{-p^m N_{\mathrm{S}}}}\right\}^2 \quad (3)$$

となる．ここで，$N_{\mathrm{S}}$ は平均光子数である．

### 3.2 Eve の測定方法と誤り率

Eve の誤り率の解析にあたり，本研究では，Yuen の評価方法 [1] を踏襲する．これは，Eve に送信信号のフルコピーを一つ与え，測定後に仮想的に鍵を開示することで，Eve の受信能力の上界を見積もるというものである．また，本研究では，Eve は，自身にとって最適とされるヘテロダイン攻撃 [1] を行うと仮定する．さらに，鍵を用いた最尤検出を行うと仮定して，Eve の受信能力の上界を見積もる．

ヘテロダイン攻撃を用いたときの誤り率は，シンプレクティック変換と呼ばれる変換を考えることで，暗号化前の信号に対するヘテロダイン攻撃の誤り率に等しくなることが示されている [3]．このシンプレクティック変換の考え方をさらに用いることで，本研究で考える暗号化前の信号（$[p^m-1, m]$ 等距離符号によって符号化された $p$ 元 PSK コヒーレント状態信号）に対するヘテロダイン攻撃の誤り率が，解析解の求められている PPM 信号に対するヘテロダイン攻撃の誤り率に等しくなることを示すことができる．そして，その誤り率は

$$P_{\mathrm{e}}^{\mathrm{Eve}} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\exp\left[-\frac{(y-\sqrt{2p^m N_{\mathrm{S}}})^2}{2}\right]Q_{p^m}(y)dy \quad (4)$$

$$Q_{p^m}(y) = 1-[\Phi(y)]^{p^m-1} \quad (5)$$

$$\Phi(y) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{y}\exp\left[-\frac{v^2}{2}\right]dv \quad (6)$$

となる．

## 4 結果

3 章で求めた正規受信者と盗聴者の誤り率を用いて，多元等距離符号を用いた KCQ プロトコルの量子利得を調べる．図 2 に，$P=0.45$ のときの数値結果を示す．また，図 3 に，[8,2] 等距離符号における，$P$ を変化させたときの数値結果を示す．図 2 より，今回調べた全ての符号長で，多元等距離符号を用いた KCQ プロトコルの量子利得が CPPM 型 KCQ の量子利得を上回っていることがわかる．特に，符号長が短いところでその差が顕著であることが確認できる．また，図 3 より，$P$ を変化させた場合であっても，多元等距離符号を用いた KCQ プロトコルの量子利得の方が常に大きいことが確認できる．これらの結果より，本研究で考えた KCQ プロトコルに優位性があることがわかる．

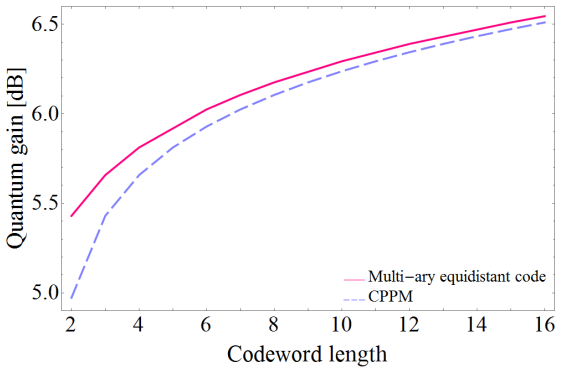


図 2 $P=0.45$ のときの，多元等距離符号を用いた KCQ プロトコルの量子利得（赤実線）と CPPM 型 KCQ の量子利得（青破線）

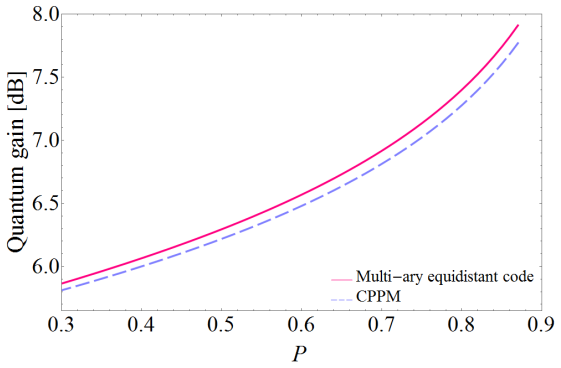


図 3 [8,2] 等距離符号における，多元等距離符号を用いた KCQ プロトコルの量子利得（赤実線）と CPPM 型 KCQ の量子利得（青破線）

## 5 おわりに

多モード量子信号を用いた KCQ プロトコルの性能調査を目的として，多元等距離符号を用いた KCQ プロトコルの量子利得を求め，CPPM 型 KCQ の量子利得との比較を行った．その結果，多元等距離符号を用いた KCQ プロトコルの量子利得が CPPM 型 KCQ の量子利得を上回ることを明らかにした．

今後の課題として，その他の線形符号を用いた KCQ プロトコルの解析を行うこと，そして，それらの結果から高い量子利得を示すための信号の条件を見つけることなどが挙げられる．

## 参考文献

[1] H.P. Yuen, quant-ph/0311061v6, (2004).
[2] K. Kato and O. Hirota, Proc. SPIE, Quantum Communication and Quantum Imaging III, **5893**, (2005).
[3] 相馬正宜, 広田修, 信学技報, ISEC2010-4, pp.17-24, (2010).
[4] 岩田直樹, 臼田毅, 2014 年電子情報通信学会ソサイエティ大会, A-6-4, (2014).
[5] T.S. Usuda, S. Usami, I. Takumi, and M. Hata, Phys. Lett. **A305**, pp.125-134, (2002).

## 公表論文

[A] **A. Kadoya**, Y. Umemura, S. Asano, N. Iwata, and T.S. Usuda, Proc. of AQIS2015, pp.161-162, (2015).
[B] **角谷昭仁**, 臼田毅, SITA2016, pp.360-365, (2016).
[C] **角谷昭仁**, 臼田毅, WiNF2016, C-04, p.29, (2016).

他 4 件 (筆頭著者)，10 件 (第二以降著者)