CPPM 型 KCQ 鍵生成における盗聴者の誤り率特性

山下 比呂　　指導教員：臼田 毅

1 はじめに

今現在通信で使用されている暗号は数理暗号と呼ばれるものであり，安全性の根拠が計算量に起因している．数理暗号は鍵長が増えると暗号を解読するのにかかる計算時間も指数的に増えていき，解読するのに相当な時間がかかる．解読される可能性が否定できないが，実用面で有用であるため現在多く利用されている．

しかし数理暗号は今現在安全でも将来的に計算能力の向上，画期的なアルゴリズムの発見等により解読されてしまう危険性が大いにある．そこで絶対盗聴不可能な暗号の開発ということで量子暗号が考案された．量子暗号には大きく分けて二つの方式があるが，従来の方式である量子暗号鍵配布 (QKD) は通信距離，速度ともに現在の通信が果たすべき基準を全く満たしておらず，さらに最近の論文で安全性の理論に疑問がもたれたり，盗聴に成功したという実験報告もある．

しかし Yuen によって新しく提案された KCQ[1] では通信速度，距離共に実用域に達しており，今後実用化に向けて研究がますます進んでいくと思われる．KCQ では安全性の根拠が盗聴者と正規受信者の受信能力の差に基づいており，盗聴者の受信能力を定量的に評価することは重要であるので，本研究では CPPM 型 KCQ 鍵生成において鍵の個数，及びスロット数を変化させた場合についての盗聴者の誤り率特性を考察する．さらに今回扱う信号に対して SRM がどの程度の性能を示しているか確かめるため，盗聴者が量子最適測定を行った場合を SRM を行った場合の誤り率特性と比較する．

2 KCQ 鍵生成プロトコル

KCQ 鍵生成とは，

- Alice(送信者) と Bob(正規受信者) はあらかじめ短いシード鍵 (共通鍵)K を共有している．
- そのシード鍵を疑似乱数生成期を用いて伸長し，それをある長さのビット列に区切ったランニング鍵を生成し，それを使用することにより盗聴者 (Eve) に対しての優位性を確立する．

本研究では鍵の知識を，ユニタリ作用素の選択に用いる CPPM 方式について考察する．

この方式において使用される PPM 信号と CPPM 信号について説明する．N 値 PPM 信号は，1 シンボル内に N 個のスロットを持ち，ある 1 つのスロットにのみコヒーレント光が乗り，ほかのスロットは真空である．

一方 N 値 CPPM 信号は N 個全てのスロットに振幅も位相もバラバラなコヒーレント光が乗り，鍵の知識がなければ元の PPM 信号が何であったのかわからない．Bob は鍵の知識により CPPM 信号を PPM 信号に復号し測定するが，Eve は鍵の知識がないのでより量子雑音の影響を受けた CPPM 信号を測定することとなる．

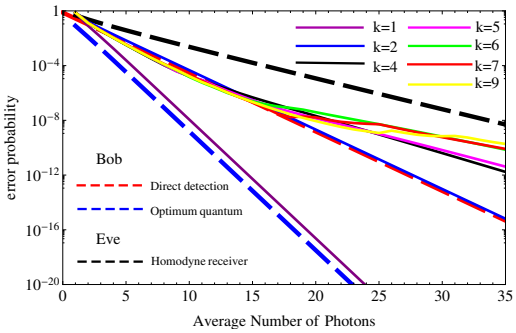

Fig.1. Error performance (case of 4slot)

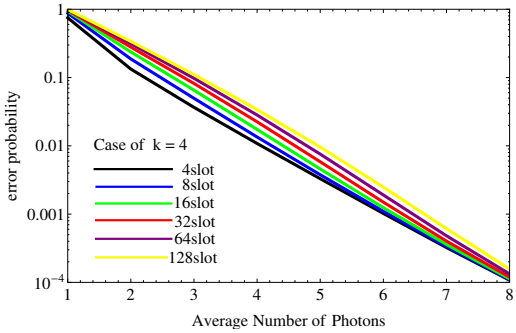

Fig.2. Error performance (case of k=4)

3 CPPM 信号系

3.1 本稿で扱う信号

本稿では位相を固定した場合の CPPM 信号を考える．例として 2 スロットの PPM 信号は，

$$|\phi_1\rangle = |\alpha\rangle_1|0\rangle_2 \qquad |\phi_2\rangle = |0\rangle_1|\alpha\rangle_2 \tag{1}$$

であり，CPPM 信号は，

$$\begin{aligned} |\psi_1(k)\rangle &= U(k)|\phi_1\rangle = |-\sqrt{1-\eta(k)}\alpha\rangle_1|\sqrt{\eta(k)}\alpha\rangle_2 \\ |\psi_2(k)\rangle &= U(k)|\phi_2\rangle = |\sqrt{\eta(k)}\alpha\rangle_1|\sqrt{1-\eta(k)}\alpha\rangle_2 \end{aligned} \tag{2}$$

である．PPM 信号にユニタリ作用素を施すことにより，CPPM 信号に暗号化し，その逆を施すことにより復号を行う．ここで $\eta(k)$ は CPPM 暗号化回路におけるビームスプリッタの透過率で，暗号化鍵 k によって決まる．

3.2 CPPM 暗号化回路

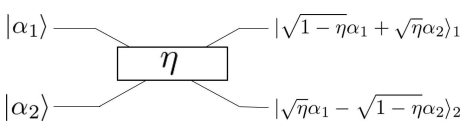

Fig.3. CPPM encryption cirucit

数式ではユニタリ作用素を用いて PPM 信号を CPPM 信号に暗号化するが，実際に実現する場合には，Fig.3 の回路を用いて信号を暗号化する．そしてランニング鍵に応じてビームスプリッタの透過率が決定し，(例 k_1 なら$\eta = 0.1, k_2$ なら$\eta = 0.2$) その透過率に応じた CPPM 信号が出力される．Fig.3 の回路を複数組み合わせることによってスロット数を増幅していくことが可能である．

4 盗聴者の用いる受信機

本研究では盗聴者の誤り率下界を求めるため，盗聴者にとって最良な条件を与えるとする．具体的には，盗聴者に量子状態のフルコピーを与え，信号の測定後に使用した鍵を開示する．本稿では Eve は，信号数を超える出力をもつ量子測定 (SRM) を行った後，古典的最適決定 (最尤検出) により信号を判別する受信機 (半古典的量子受信機 [2]) を用いる．そして 4 スロットの信号に対して，使用する鍵の個数を変化させた場合の誤り率特性を考察する．今回，鍵が x 個 ($k = x$) のとき d 番目の鍵に対応する透過率を，

$$\eta(k_d) = \frac{d}{x} \tag{3}$$

と設定した．例として $k = 4$ の時は $\eta(k_1) = 0.25, \eta(k_2) = 0.5, \eta(k_3) = 0.75, \eta(k_4) = 1.0$ となる．
またスロット数の違いによる誤り率特性を考察するため鍵を 4 個に固定し，スロット数が 2^2〜2^7 の場合の誤り率特性を考察する．

5 盗聴者の誤り率特性

Fig.1 が鍵の個数を変化させた場合の誤り率特性である．なお，比較として Bob が直接検波受信機を用いた場合の誤り率 (赤点線)，量子最適受信機を用いた場合の誤り率 (青点線)，Eve がホモダイン受信機を用いた場合 (黒点線，Eve が PPM 信号と等価の信号をホモダイン測定した場合) の誤り率を示す．
Fig.1 より $k = 1$ のときは Eve は PPM 信号と等価な信号を測定するので Bob が量子最適受信機を用いた場合と近い誤り率を示し，鍵の個数が増えるにつれ，信号数が増加し信号間距離が短くなっていき，量子雑音の影響を受けて信号を正しく復号できない確率が大きくなり誤り率が増加していくことがわかる．
このように盗聴者に最も好条件を与えた場合においても，鍵の個数をある程度増やすことで正規受信者との受信能力に明確な差をつけることができる．
信号数を増やしていくと，連続量を測定しているホモダイン受信機の誤り率に漸近していくと考えられる．
また Fig.2 より鍵の個数を固定し，スロット数の違いのみで比較を行ったところ，平均光子数が小さいところで誤り率に変化がみられ，スロット数が増加するにつれて誤り率が大きくなっていくことがわかった．
これはスロット数が大きくなると CPPM 信号の多値度が増加し，信号がより複雑な信号となり量子雑音の影響を大きく受けるためと考えられる．平均光子数がある程度増加し，量子自身の持つ揺らぎが少なくなってくると，128slot でも 4slot と同程度信号の信号の識別がなされており，今回の解析手法では誤り率にあまり変化がみられなかった．

6 盗聴者が量子最適測定を行った場合

次に今回扱った CPPM 信号に対して SRM がどのくらいの性能を示しているかを確かめるため，Eve が量子最適測定を行った場合の誤り率を示し，SRM と比較を行う．量子受信機による信号の測定過程はヒルベルト空間上に定義される決定作用素で表される．SRM は任意の 2 元信号や M 元の対称信号に対しては最適決定作用素となり量子最適測定となることが知られている．また任意の量子信号系に対しても漸近的に最適な検出になることが知られている．

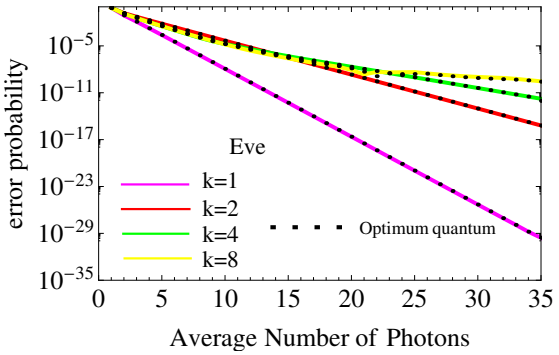

Fig.4. Error performance (Comparison between SRM and Optimum quantum measurement)

つまり正規受信者の Bob は対称性を持つ PPM 信号を測定するので SRM が最適測定となるが，盗聴者の Eve は非対称信号である CPPM 信号を測定するため，最適な決定作用素を求める必要がある．今回はヘルストロムのアルゴリズム [3] を用いて最適な決定作用素を求めた．
Fig.4 より，大まかなプロットではあるがどの暗号化鍵においても SRM と量子最適測定の結果にほとんど違いがないことがわかる．詳細に考察したところ，最大でも約 2% の誤差であることがわかったので，SRM は今回扱った CPPM 信号に対しても最適に非常に近い測定であるといえる．

7 おわりに

本稿では，CPPM 型 KCQ 鍵生成プロトコルにおいて，CPPM 信号の位相を固定した場合の盗聴者の誤り率特性を正規受信者の誤り率と比較し，解析，考察を行った．
今回信号のスロット数，暗号化鍵の個数等，実際に利用するには非現実的なパラメータではあるが，盗聴者に最も好条件を与えた場合においても，鍵の個数を増やしていくと，正規受信者との受信能力に明確な差をつけることができることがわかった．
信号数を増加させていくと最終的に連続量を測定しているホモダイン受信機の誤り率に漸近していくことが考えられる．
さらに Eve が SRM を行った場合と量子最適測定を行った場合を比較し，誤り率の差が最大でも約 2% であったことから CPPM 信号に対しても SRM は非常に最適に近い値を示すことが分かった．今後の課題としてより現実的なパラメータで考察を行うこと，位相も変化させた場合を考察することが挙げられる．

参考文献

[1] H.P. Yuen, IEEE, J. Selected Topics in Quant. Electron., **15**, pp.1630-1645, (2009).
[2] 西田, 竹下, 太田, 臼田, 第 33 回情報理論とその応用シンポジウム, pp.79-82, (2010).
[3] C. W. Helstrom, “Bayes-cost reduction algorithm in quantum hypothesis testing,” IEEE Trans. Inform. Theory, **IT-28**, pp.359-366, (1982).

公表論文

1) **H. Yamashita**, T.S. Usuda, S. Usami Proc. of ISITA2012, pp.308-311, 2012.