非線形二元符号を応用した新量子暗号 KCQ の特性

情報科学科　小林 拓也　　指導教員：臼田 毅

1　はじめに

量子暗号の一つに，2000 年に Yuen が提案した KCQ (Keyed Communication in Quantum noise)[1] がある．この暗号は，数理暗号では決して超えることのできない Shannon 限界を超える暗号として期待されている．最近，KCQ に二元線形符号を応用することが提案され [2]，その特性が調べられている．しかしながら，非線形な二元符号を用いた KCQ の特性はまだ研究されていない．

本研究では，二元非線形符号を用いた KCQ における正規受信者 Bob と盗聴者 Eve の誤り率特性と量子利得を求める．そして，二元線形符号を用いたときの量子利得との比較を行う．

2　二元符号を用いた KCQ

KCQ の安全性の根拠は，Eve に正確な暗号文を渡さないことである．そのために，正規送信者 Alice と Bob はあらかじめ秘密鍵を共有する．また，本研究では，送信信号に二元符号によって符号化されたコヒーレント状態を用いる．そして，基本量子状態を BPSK (Binary Phase-Shift Keying) コヒーレント状態とする．

Alice は秘密鍵を用いて送信信号を暗号化する．これにより，信号の各モードが多値のコヒーレント状態となる．Bob は，受信した信号を秘密鍵を用いて復号し，復号された信号に対して測定を行う．一方，Eve は秘密鍵を持っていないため，暗号化された信号に対して復号を試みることになる．このように，Bob と Eve で受信する信号が異なることから，Bob と Eve の使用できる最適な測定方法が変わり，受信能力に差が生まれる．その差は，誤り率規準に基づく量子利得で表される．

3　正規受信者と盗聴者の測定方法

Bob は受信した信号に対して量子最適な測定を行う．一方，Eve は，自身が行える測定の中で最適となるヘテロダイン測定を行うと仮定する [1]．ここで，Eve に信号のフルコピーを一つ与え，さらに Eve の信号測定後に鍵を仮想的に開示するものとする [1]．これにより，Eve は測定後に開示された鍵を用いた最尤検出が可能となる．このように，Eve に有利な状況を想定することによって，Eve の受信能力の上界を調べることができる．

4　誤り率特性と量子利得

図 1 は，符号長 3 の場合の全ての符号における Bob と Eve の誤り率特性を表している．特に，色の濃い線は，量子利得が一番高かった符号におけるそれぞれの誤り率特性を示している．図 1 の結果から，Bob と Eve の受信能力に差が生じていること，すなわち Bob に優位性があることがわかる．

量子利得 Gain [dB] を表す式は次のようになる．

$$\mathrm{Gain} = 10\log_{10}(N_{\mathrm{S}}^{\mathrm{Eve}}/N_{\mathrm{S}}^{\mathrm{Bob}}) \qquad (1)$$

ここで，$N_{\mathrm{S}}^{\mathrm{Bob}}, N_{\mathrm{S}}^{\mathrm{Eve}}$ は，Bob と Eve がそれぞれ量子最適測定，ヘテロダイン測定を用いたときに，ある誤り率を達成するときの平均光子数である．今回はその誤り率を 0.4 とした．表 1 は，符号長 2 から 4 の符号について，量子利得が高かった線形符号と非線形符号を 2 つずつ示している．ただし，符号語間のハミング距離の組み合わせが等しい符号は，量子利得の値が同じ結果

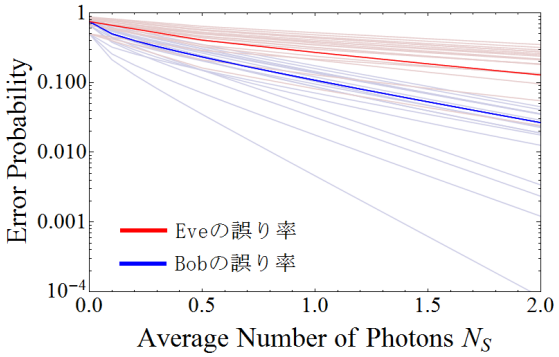

図 1　符号長 3 における Bob と Eve の誤り率特性

表 1　各測定における平均光子数と量子利得

符号長 2				
	符号の一例	$N_{\mathrm{S}}^{\mathrm{Bob}}$	$N_{\mathrm{S}}^{\mathrm{Eve}}$	量子利得 [dB]
線形符号	{00, 01, 10, 11}	0.089745	0.285261	5.02232
	{00, 01}	0.010205	0.032199	4.99029
非線形符号	{00, 01, 10}	0.046097	0.157068	5.32410
	{01, 10}	0.005102	0.016072	4.98329

符号長 3				
	符号の一例	$N_{\mathrm{S}}^{\mathrm{Bob}}$	$N_{\mathrm{S}}^{\mathrm{Eve}}$	量子利得 [dB]
線形符号	{000, 011, 101, 110}	0.045874	0.173492	5.77713
	{000, 001, 010, 011, 100, 101, 110, 111}	0.159562	0.553588	5.40257
非線形符号	{000, 001, 010, 100}	0.066930	0.253192	5.77829
	{000, 001, 010, 101}	0.065793	0.245853	5.72494

符号長 4				
	符号の一例	$N_{\mathrm{S}}^{\mathrm{Bob}}$	$N_{\mathrm{S}}^{\mathrm{Eve}}$	量子利得 [dB]
線形符号	{0000, 0011, 0101, 0110}	0.183500	0.693968	5.77704
	{0000, 0011, 1101, 1110}	0.142944	0.531464	5.70313
非線形符号	{0000, 0001, 0010, 0100, 1000}	0.321224	1.246032	5.88720
	{0000, 0011, 0101, 1001, 1110}	0.201500	0.779760	5.87684

となるため，それらの符号はまとめている．表 1 より，最も量子利得が高かった符号は，どの符号長においても非線形符号であることがわかる．また，それらの符号はいずれも PPM (Pulse Position Modulation) 信号の形に似た符号に全て 0 の符号語を加えた符号であることがわかる．

5　おわりに

本研究では，符号長 2 から 4 のときの二元符号を用いた KCQ の特性を調べ，線形，非線形の場合の比較を行った．その結果，符号長 2 から 4 のいずれの場合においても，非線形符号を応用した KCQ の方が量子利得が高いことが明らかになった．

今後の課題は，より長い符号長における KCQ の特性を調べることである．そのために，より効率よく解析が可能となるような，高い量子利得を示す非線形符号の特徴を明らかにする必要がある．

参考文献

[1] H.P. Yuen, quant-ph/0311061v6, (2004).
[2] A. Kadoya, *et al.*, Proc. of AQIS2015, pp.161-162, (2015).

公表論文

1) **小林拓也**, 角谷昭仁, 梅村勇貴, 臼田毅, 平成 27 年度電気・電子・情報関係学会東海支部連合大会, K1-3, (2015).