二元線形符号を用いた量子暗号システムとその特性

情報科学科　角谷 昭仁　　指導教員：臼田 毅

1　はじめに

情報理論的に安全であるとして期待されている暗号に，量子の特性を応用した量子暗号がある．量子暗号 KCQ（Keyed Communication in Quantum Noise）[1] は，盗聴者が正しい暗号文を入手できないことを安全性の根拠とする暗号プロトコルである．これは，優位性確立と呼ばれる過程によって確立されるものであり，どれだけの優位性を確立しているのかは，量子利得によって求めることができる．量子利得は暗号に使用する信号によって決まり，PPM 信号を用いる KCQ は，高い量子利得を示すことが明らかにされている [2]．しかし，十分な優位性を確立するために必要なスロット数が現実的でないことから，この方式よりも高い量子利得を示す信号を見つけることが望まれる．

本研究では，PPM 信号の代わりに二元線形符号によって符号化された量子状態を用いた量子暗号を考える．この量子状態信号に対して，正規受信者，盗聴者が最適な測定を行ったときの量子利得と PPM 信号の量子利得を比較し，その特性を調べる．

2　二元線形符号を用いた量子暗号

本研究では，量子暗号 KCQ に符号による符号化を取り入れる．あらかじめ，送受信者は初期鍵を共有しているものとする．送信者は，ビット列を二元線形符号によって符号化し，符号語を生成する．その符号語を用いて量子符号化を行い，送信信号を生成する．この信号に初期鍵によって暗号化を施し，正規受信者へと送信する．正規受信者は，受信信号に鍵を施して復号を行う．復号された量子状態に対して最適な測定を行い，その結果を得る．盗聴者は，暗号化された量子状態に対して最適な測定を行い，送信されたと思われる信号への復号を試みる．

3　正規受信者と盗聴者の測定方法

量子利得は，正規受信者と盗聴者の測定方法における誤り率の差から求めることができる．なお，盗聴者の上界を評価するために，盗聴者には量子状態のフルコピーを渡し，測定後に仮想的に鍵を開示するものとする．正規受信者は，量子状態の測定に一括 SRM(Square-Root Measurement) を使用する．先験確率が等確率な二元線形符号に対して，一括 SRM は量子最適な測定となる [3]．一方，どのような測定方法が盗聴者にとって最適となるかは明らかではない．そのため，本研究では，古典最適である個別ホモダイン測定 + 軟判定・最尤検出と，ASK 型 KCQ でホモダイン測定を上回ることが知られている個別 SRM+ 最尤検出の，盗聴戦略として現状考えられる二つの測定方法から評価を行う．

1. 個別ホモダイン測定 + 軟判定・最尤検出：信号を構成する各量子状態に対してホモダイン測定を行う．得られた結果から，各信号が送られた場合にこの結果が得られる条件付き確率を求め，最も確率の高い信号に復号する．

2. 個別 SRM+ 最尤検出：基本的な方法は個別ホモダインの場合と同様だが，各量子状態の測定に SRM を用いる．

4　誤り率特性と量子利得

本研究では，二元線形符号にハミング符号，シンプレックス符号，リード・マラー符号を用いる．これらの符号を用いたときの

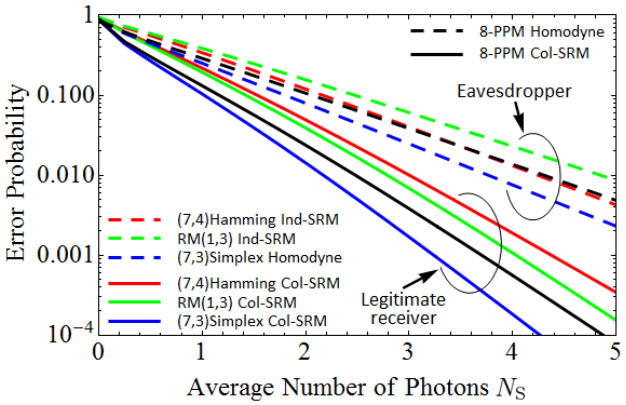

図 1　PPM 信号，各符号に対して，盗聴者と正規受信者が最適な測定を行ったときの誤り率特性

表 1　誤り率 10^{-2} の点における各符号の量子利得

符号	平均光子数			量子利得 [dB]	
	ホモダイン	個別 SRM	一括 SRM	ホモダイン	個別 SRM
8-PPM	4.300	4.692	2.479	2.391	2.770
(7,3)Simplex	3.763	4.106	2.170	2.392	2.770
(7,4)Hamming	5.456	4.241	3.000	2.600	1.503
RM(1,3)	5.079	4.847	2.788	2.605	2.402

正規受信者と盗聴者の誤り率特性を図 1 に示す．ここで，横軸は平均光子数であり，光の強度を表す．量子利得は，次の式で求めることができる．

$$Gain = 10\log_{10}(N_S^{Eve}/N_S^{CS}) \quad (1)$$

ここで，N_S^{Eve}, N_S^{CS} は，個別ホモダインもしくは個別 SRM と一括 SRM において，それぞれある誤り率を達成するときの平均光子数である．本稿では，誤り率 10^{-2} を達成するときの平均光子数から求めた量子利得を表 1 に示す．図と表より，盗聴者の最適となる測定が符号によって異なること，リード・マラー符号が最も量子利得が高くなることがわかる．

5　おわりに

量子暗号 KCQ に二元線形符号を応用し，そのときの正規受信者と盗聴者の誤り率特性を示した．また，そこから量子利得を求め，PPM 信号の量子利得との比較を行った．その結果，今回用いた符号の中では，リード・マラー符号の量子利得が最も高い量子利得を示すことがわかった．今後は，本研究で用いた符号以外について調べるとともに，より高い量子利得を示すための信号の条件を明確化していく．

参考文献

[1] H.P. Yuen, quant-ph/0311061v6, (2004).
[2] M. Sohma *et al.*, Tamagawa University Quantum ICT Research Institute Bulletin, Vol.1, No.1, pp.15-19, (2011).
[3] T.S. Usuda *et al.*, Phys. Lett. **A256**, pp.104-108, (1999).

公表論文

1) 角谷昭仁, 梅村勇貴, 浅野駿吾, 神谷幸宏, 臼田毅, 平成 26 年度電気・電子・情報関連学会東海支部連合大会, J1-3, (2014).
2) 角谷昭仁, 岩田直樹, 臼田毅, 第 37 回情報理論とその応用シンポジウム (SITA2014), pp.248-252, (2014).