多元 PSK 信号に対する信頼性関数を用いた KCQ プロトコルの安全性評価

森本 絵偉　　指導教員：臼田 毅

1 はじめに

信頼性関数は，十分に長い符号長 n と与えられた符号化率 R において，復号誤り率を最小とする符号を用いた場合の復号誤り率を $P_{\mathrm{e}}^{\mathrm{opt}}(n,R)$ としたとき，

$$P_{\mathrm{e}}^{\mathrm{opt}}(n,R) = e^{-nE(R)} \tag{1}$$

となる $E(R)$ として定義される [1]．信頼性関数の上下界は導出されており，その上下界が一致する場合は $E(R)$ そのものの値を得ることができる．

先行研究 [2] では，信頼性関数の上下界を，KCQ プロトコルと呼ばれる量子暗号プロトコルの安全性評価に応用している．その際，4 元 PSK 信号を用いる場合の量子信頼性関数の上界が数値計算上で発散した．しかし，同一設定の古典信頼性関数の上界は発散しないことが示されている [1]，よって本研究では，多元 PSK 信号による量子信頼性関数の上界の発散を数式で確認する．次に，量子信頼性関数の上界も利用し KCQ プロトコルの安全性評価を行う．

2 量子信頼性関数の上界

今回利用する量子信頼性関数の上界については，パラメータ s，量子情報源の密度作用素 ρ，信号の生起確率 ξ を用いて以下の式で表される [3]．

$$E_{\mathrm{QU}}(R) = \max_{0\le s}\max_{\xi}\left[\mu(s,\xi) - sR\right] \tag{2}$$

$$\mu(s,\xi) = -\ln \mathrm{Tr}\,\rho^{1+s} \tag{3}$$

また，関数 μ の内部は，密度作用素 ρ の各固有値 λ_i によって，

$$\mathrm{Tr}\,\rho^{1+s} = \sum_{i=1}^{M}\lambda_i^{1+s} \tag{4}$$

として計算可能である．

3 多元 PSK 信号に対する量子信頼性関数の上界の発散

量子信頼関数の上界 $E_{QU}(R)$ の内部を

$$f(s) = \mu(s,1/M) - sR \tag{5}$$

とする．なお，今回用いる対称信号においては，各生起確率 ξ が等確率であるときに最適化するため，$\xi = \left\{\frac{1}{M}\right\}$ としている．$f(s)$ の下界は密度作用素の最大固有値 $\lambda_{\max}$ を用いて，

$$\begin{aligned} g(s) &= -\ln M\lambda_{\max}^{1+s} - sR \\ &= -\ln M - (1+s)\ln\lambda_{\max} - sR \\ &= -\ln M - \ln\lambda_{\max} + s(\ln\lambda_{\max}^{-1} - R) \end{aligned} \tag{6}$$

と定義される．ここで，s が係数となる項に注意すると，R が閾値 $R_\infty = \ln\lambda_{\max}^{-1}$ よりも小さければ，$g(s)$ は十分大きな s について発散することがわかる．よって，$g(s)$ の上界である $f(s)$ も発散するため，量子信頼性関数の上界も

$$\max_{0\le s}\left[f(s)\right] = \infty \tag{7}$$

となり，発散することが示された．

4 KCQ プロトコルの安全性評価

KCQ プロトコルの安全性は，通信過程で生じる正規受信者と盗聴者の間の復号能力差により保たれている [4]．本研究では，正規受信者が量子最適受信機，盗聴者が古典最適受信機を利用できると仮定し，各受信機の能力差を示す指標 (量子利得) を求めることで安全性評価を行う．量子利得は，各受信機が同じ誤り率 P を達成する際の平均光子数 N_{s} の比として次式で表される．

$$\mathrm{Gain} = 10\log_{10}\frac{N_{\mathrm{s}}^{\mathrm{C}}(\mathrm{When}\ P^{\mathrm{C}}=P)}{N_{\mathrm{s}}^{\mathrm{Q}}(\mathrm{When}\ P^{\mathrm{Q}}=P)}\quad[\mathrm{dB}] \tag{8}$$

なお，上付き文字の C は古典，Q は量子の場合のパラメータであることを示す．また，P^{C}, P^{Q} の表現に，多元 PSK 信号による古典及び量子信頼性関数の上下界を用いるとする．

今回は多元 PSK 信号を用いた KCQ プロトコルによる量子利得の計算を行った．その際，古典，量子ともに達成する誤り率を $P = 10^{-12}$ としたときの平均光子数を利用している．また，符号化率 R は 0.1，0.2，0.3，符号語長 n は 10^4, 10^5, 10^6 としてそれぞれ設定した．計算の結果，符号化率 R を小さく符号語数 n を大きく設定するほど，量子利得が増加する傾向が見られた．量子利得が最大となった R, n の設定による結果を，元数 M ごとに表 1 に示す．全体的に量子利得の上下界はほぼ一致し．8dB〜9dB 程度となった．すなわち，正規受信者と盗聴者の能力差は 6〜8 倍程度といえる．また，元数 M が小さいほど量子利得が僅かに大きくなる様子が見られた．

表 1　Quantum gain [dB]

M	R	n	Gain(Lower)	Gain(Upper)
2	0.1	10^6	9.001	9.004
4			8.940	8.944
8			8.275	8.279

5 まとめ

本研究では，多元 PSK 信号の場合の量子信頼性関数の上界が発散する性質を持つことを示した．また，多元 PSK 信号を用いた KCQ プロトコルについて，量子利得による安全性評価を行った．

参考文献

[1] R.G. Gallager, *Information Theory and Reliable Communication*, John Wiley & Sons, Inc., New York, (1968).

[2] 吉田真菜, 宇佐見庄五, 臼田毅, 第 42 回情報理論とその応用シンポジウム, pp.129-134, (2019).

[3] M. Dalai, IEEE Trans. on IT **59**, pp.8027-8056, (2013).

[4] H.P. Yuen, arXiv:quant-ph/0311061v6, (2004).

公表論文

1. **森本 絵偉**, 中川 綾太, 王 天澄, 臼田 毅, 令和 3 年度東海支部連合大会, D5-2, (2021).
2. **森本 絵偉**, 中川 綾太, 王 天澄, 臼田 毅, 第 44 回情報理論とその応用シンポジウム, 2.2.1, (2021).