光通信量子暗号における盗聴者と正規受信者の誤り率特性

土本 敏之 *(名工大), 宇佐見庄五 (名城大), 臼田 毅 (愛県大, CREST), 内匠 逸 (名工大)

Error performance of Eve and Bob for quantum cryptographic protocol Y-00

Toshiyuki Tsuchimoto(Nagoya Inst. of Tech.), Shogo Usami(Meijo Univ.),
Tsuyoshi Sasaki Usuda(Aichi Pref. Univ., CREST), Ichi Takumi(Nagoya Inst. of Tech.)

1. はじめに

光通信量子暗号とは，光通信技術と融合した新量子暗号のことである．我々は，次世代の光通信量子暗号の開発を目指し，現在実用化研究が進められている Y-00 プロトコル [1,2] を調査している．

最近，文献 [1] において，盗聴者から共有鍵を守るための DSR という新たな手法が提案された．本稿では，DSR を用いたときの盗聴者と正規受信者の誤り率特性について示し，そこから DSR の適切な使用方法を考察する．

2. DSR と誤り率

Y-00 において，送信者 (以下 Alice) は，信号 (1 or 0) を送信するため，正規受信者 (以下 Bob) との共有鍵を使い，M-PSK から位相ペアを選択し，BPSK により信号を送信する．通常は，その位相を使って Bob に信号を送信するが，盗聴者 (以下 Eve) の共有鍵への攻撃を防ぐため，意図的に信号をランダム化し，真の位相を含むその周辺の位相から 1 つを選んで送信する．そのような手法を DSR と言う．本稿では以下の 3 パターンの DSR を使い，位相 0[rad] の信号を送信することにする．

パターン 1　位相 0[rad] とその周りの位相を含む $\frac{M}{2}$ 個のうち 1 つを，ランダムに等確率で送信する．

パターン 2　位相 0[rad] とその前後 2 つの位相を含む 5 個のうち 1 つを，ランダムに等確率で送信する．

パターン 3　位相 0[rad] とその前後 $\frac{\pi}{4}$ を含む $\frac{M}{2}+1$ 個のうち 1 つを，ランダムに等確率で送信する．

本稿では，実際的な検出方法について考察する．まず，Eve は共有鍵の情報を知らないので，ヘテロダイン検出で M-PSK を識別する．そのとき誤り率は以下のようになる．

$$P_{\mathrm{e}} = \int\int_{D} \frac{1}{\pi} \exp[-(x-A)^2 - y^2]\mathrm{d}x\mathrm{d}y \qquad (1)$$

ここで，A は平均光子数である．一方，Bob は共有鍵を知っているので，ホモダイン検出で信号を識別する．そのとき誤り率は以下のようになる．

$$P_{\mathrm{e}} = \int_{-\infty}^{\infty}\int_{-\infty}^{0} \frac{1}{\sqrt{2\pi * \frac{1}{4}}} \exp\left[-\frac{(x-A)^2}{2*\frac{1}{4}}\right]\mathrm{d}x\mathrm{d}y \qquad (2)$$

3. 各パターンの考察

Eve と Bob について，DSR の各パターンにおける誤り率をプロットした (Fig.1,2)．ここで，$A=\sqrt{10}$ であり，パターン 1(青)，2(緑)，3(赤) である．また，比較のため DSR を行わない場合 (ピンク) をプロットした．

パターン 1(青) について見ると，Eve の誤り率は，位相数の小さいところでも十分 1 に近づいているが，同時に本来なら限りなく 0 に近い Bob の誤り率も劣化させてしまう．パターン 1(青) は，正規受信者の誤り率を大きく劣化させても，盗聴者の誤り率をほぼ 1 としたい場合に，使用を限定すべきであると考えられる．

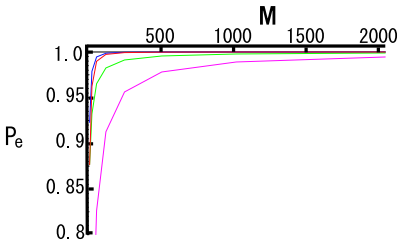

Fig.1. Eve's Error rate in the case that $A=\sqrt{10}$

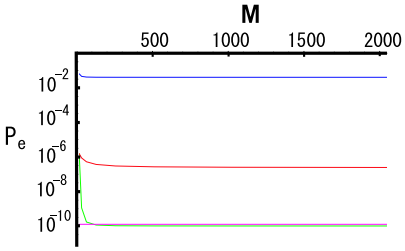

Fig.2. Bob's Error rate in the case that $A=\sqrt{10}$

次にパターン 2(緑) について見ると，位相数の小さいところで Eve の誤り率はやや低いものの，位相数の大きいところではほぼ 1 であり，Bob の誤り率は DSR を行わない場合とほぼ等しい．パターン 2(緑) を位相数の大きいところで使用すれば，効果的な撹乱が行えると考えられる．

パターン 3(赤) では，Eve の誤り率をパターン 1(青) と同程度に劣化させ，また，Bob の誤り率もパターン 2(緑) 程ではないが，まずまずのオーダである．以上より，パターン 1(青) は効果的な DSR の使用法とは言えない．

4. まとめ

光通信量子暗号において，DSR を使用したときの盗聴者と正規受信者の誤り率特性について考察した．発表では，最適受信機の特性も示し比較を行う．

今後の課題として，光通信量子暗号の実装に向けた更なる基礎データの蓄積，これらの知見を生かした新たなプロトコルの提案が考えられる．

謝辞　本研究の一部は，総務省の「戦略的情報通信研究開発推進制度」による研究成果であり，財団法人 堀情報科学振興財団の助成を受けた．

文　献

(1) H.P.Yuen, "KCQ : A New Approach to Quantum Cryptography I. General Principles and Qumode Key Generation," quant-ph/0311061 v6, (2004).

(2) G.A.Barbosa, E.Corndorf, P.Kumar, and H.P.Yuen, "Secure Communication Using Mesoscopic Coherent State," Phys. Rev. Lett. **90**, 227901, (2003).