

光直交振幅変調による量子暗号通信

Quantum cipher communication with optical quadrature amplitude modulation

学習院理¹, 東北大通研² ○平野 琢也¹, 並木亮¹, 中沢正隆², 吉田真人², 廣岡俊彦², 葛西恵介²

Gakushuin Univ.¹, RIEC, Tohoku Univ.², °Takuya Hirano¹, Ryo Namiki¹, Masataka Nakazawa²,

Masato Yoshida², Toshihiko Hirooka², Keisuke Kasai²,

E-mail: takuya.hirano@gakushuin.ac.jp

量子鍵配送(Quantum Key Distribution: QKD)は、微弱な光に情報を載せることにより、盗聴者が正確に情報を読み出せないようにし、加えて、受信者に届く光の状態変化をモニターすることにより、盗聴者の知り得る情報に制限を課し、正規の送受信者のみを知る安全な暗号鍵を共有する通信方法である[1]。微弱な光の測定は、通常は、単一光子検出が用いられる。一方、微弱な光のもう一つの有力な測定方法として、コヒーレント光通信で用いられているホモダイン検出がある。光直交振幅変調による QKD は、やはりコヒーレント光通信との共通の技術である直交振幅変調(Quadrature Amplitude Modulation: QAM)と、ホモダイン検出を組み合わせた QKD である。コヒーレント光通信と共通の技術を用いるので、汎用の部品を用いた実装が可能であるほか、ホモダイン検出は特定のモードの光のみを敏感に測定する技術であるので、漏れ光の影響を受けにくいという特長がある。4 値の位相変調を行う方式は、特に実装が容易であるという特徴があり、市販の部品を用いて実時間動作する QKD 装置を実現可能である[2]。送信光はレーザー光を単一光子レベルまで減衰したコヒーレント状態の光であり、多値変調したコヒーレント状態が互いに重なり合うようにすることで、盗聴者が正確に情報を読み出すことが不可能になる。

QAM と量子雑音ストリーム暗号を組み合わせた QAM 量子雑音暗号伝送技術(QAM/QNSC: QAM/Quantum Noise Stream Cipher)は、多値信号を量子雑音の中に隠すことにより盗聴を困難にした暗号通信技術であり、安全かつ高速・大容量な光秘匿通信システムを実現可能である[3]。伝送距離 480 km の 40 Gbit/s の伝送実験[4]、FPGA を用いた 4~64 QAM (20~60 Gbit/s) の 320km リアルタイム伝送実験に成功している[5]。更に、QAM/QNSC と QKD を融合し、QAM/QNSC で用いる暗号鍵を QKD により生成することにより、極めて安全な暗号通信を実現可能である[6]。

謝辞：本研究は、独立行政法人情報通信研究機構（NICT）の委託研究および革新的研究開発推進プログラム（ImPACT）の支援によって行われた。

[1] V. Scarani, *et al*, Rev. Mod. Phys. **81**, 1301 (2009).

[2] T. Matsubara, *et al.*, Proc. SPIE 9996, Quantum Information Science and Technology II, 99960S, (October 24, 2016).

[3] M. Nakazawa, M. Yoshida, T. Hirooka, and K. Kasai, Opt. Express **22**(4), 4098-4107 (2014).

[4] M. Yoshida, T. Hirooka, K. Kasai, and M. Nakazawa, Opt. Express **24**(1), 652-661 (2016).

[5] M. Yoshida, T. Hirooka, K. Kasai, and M. Nakazawa, ECOC 2015, paper P5.13.

[6] M. Nakazawa, *et al*, ECOC2016, W.4.P1.SC5.59. (2016).