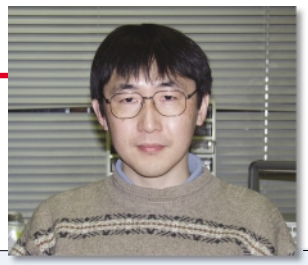
長距離量子暗号通信

― 盗聴を検知できる未来の暗号技術の開発 ―



吉澤 明男（よしざわ あきお）
yoshizawa-akio@aist.go.jp
光技術研究部門

インターネットの普及に伴い研究者や専門家だけではなく一般の利用者にもネットセキュリティーに対する関心が高まっている。

現代暗号は大きな整数の素因数分解など数学的に難しい問題を利用して解読に膨大な時間を要することで安全性を保証するが、急激な計算機技術の技術革新を考慮すれば、いずれ解読される可能性がある。

一方、量子暗号は原理的に盗聴が不可能で極めて安全性が高いとされ、欧州では金融分野への導入を意識した研究が近年活発である。量子暗号通信装置では微弱光パルスである光の粒子(光子)1個の位相や偏光に1ビットの情報を載せるが、盗聴されると状態が変化して誤り率が増大することから盗聴を検知できる。但し、正しく検知するためには装置の不具合など盗聴以外の原因による誤り率を低く抑えることが重要である。また、長距離の量子暗号通信を可能にするにはファイバを経由してくる光子を感度良く検出しなければならない。我々は、低雑音受光素子の採用と検出回路の最適化によりファイバ最低損失波長1550nm帯で電子冷却型単一光子検出器の高感度化と低雑音化を行った。さらに、これを図１に示す量子暗号通信装置に組み込み、装置内の光学素子の配置を工夫して誤り率の増大を抑えた結果、図２に示すように、25.2 kmで誤り率1%という世界一低い誤り率を持つ量子暗号通信装置の開発に成功した。この値は第三者による盗聴行為がない状態で盗聴以外の原因(主に検出器の雑音)による誤り率を測定した結果であるが、盗聴があれば誤り率が増大することから盗聴を検知できる。

図１の量子暗号通信装置において、AはBに光パルスを送り、暗号通信を要請する。これに対して、Bは光パルスを減衰させて単一光子とし、ビット0の場合はそのまま、1の場合は位相を反転させて返送する。反転の有無はAの単一光子検出器で判別する。図２中の白丸は25.2kmに対する単位時間当たりの光子検出数と誤り率を示し、黒丸はファイバを延長する代わりに光減衰器で損失を加えた結果である。

今後、検出器の性能改善を行い、光子検出数の増大と更なる量子暗号通信実験の長距離化を行う予定である。

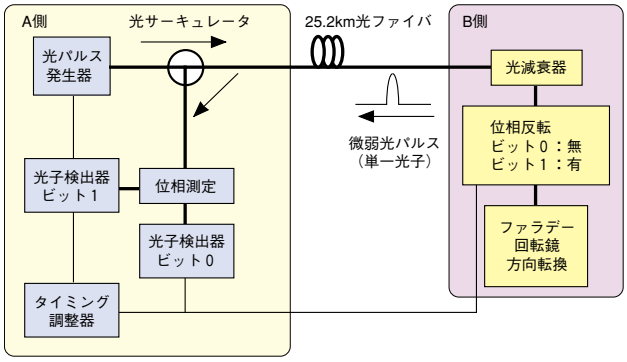


図１　量子暗号通信装置

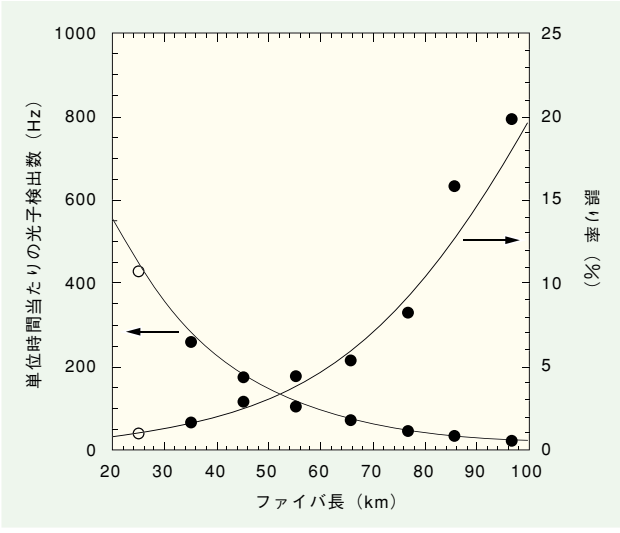


図２　光子検出数と誤り率

関連情報

・http://staff.aist.go.jp/yoshizawa-akio/
・C.H.Bennett : Phys. Rev. Lett., Vol. 68, 3121-3124 (1992).
・A. Yoshizawa and H. Tsuchida : Jpn. J. Appl. Phys., Vol. 40, 200-201 (2001).
・M. Bourennane et al. : Opt. Express, Vol. 4, 383-387 (1999).
・P. Hiskett et al. : J. Mod. Opt., Vol. 48, 1957-1966 (2001).