

# 伝令付き単一光子源による量子暗号実験

西岡 毅\*  
鶴丸豊広\*

Quantum Key Distribution Experiment with the Heralded Single Photon Source

Tsuyoshi Nishioka, Toyohiro Tsurumaru

## 要 旨

近年量子暗号通信実験が相次いで報告されているが、そのほとんどは光子源として微弱レーザ光源を用いたものである。一方で、装置の不完全さがどのようなセキュリティホールをもたらすかも研究されている。この研究によると、微弱レーザ光源のように光子を2個以上放出する場合のある不完全な光子源は、光子数分割攻撃と呼ばれる攻撃によって盗聴が可能になることが分かってきた。このため、安全性の保証される通信距離が25km前後と予想外に短いことが指摘されている。

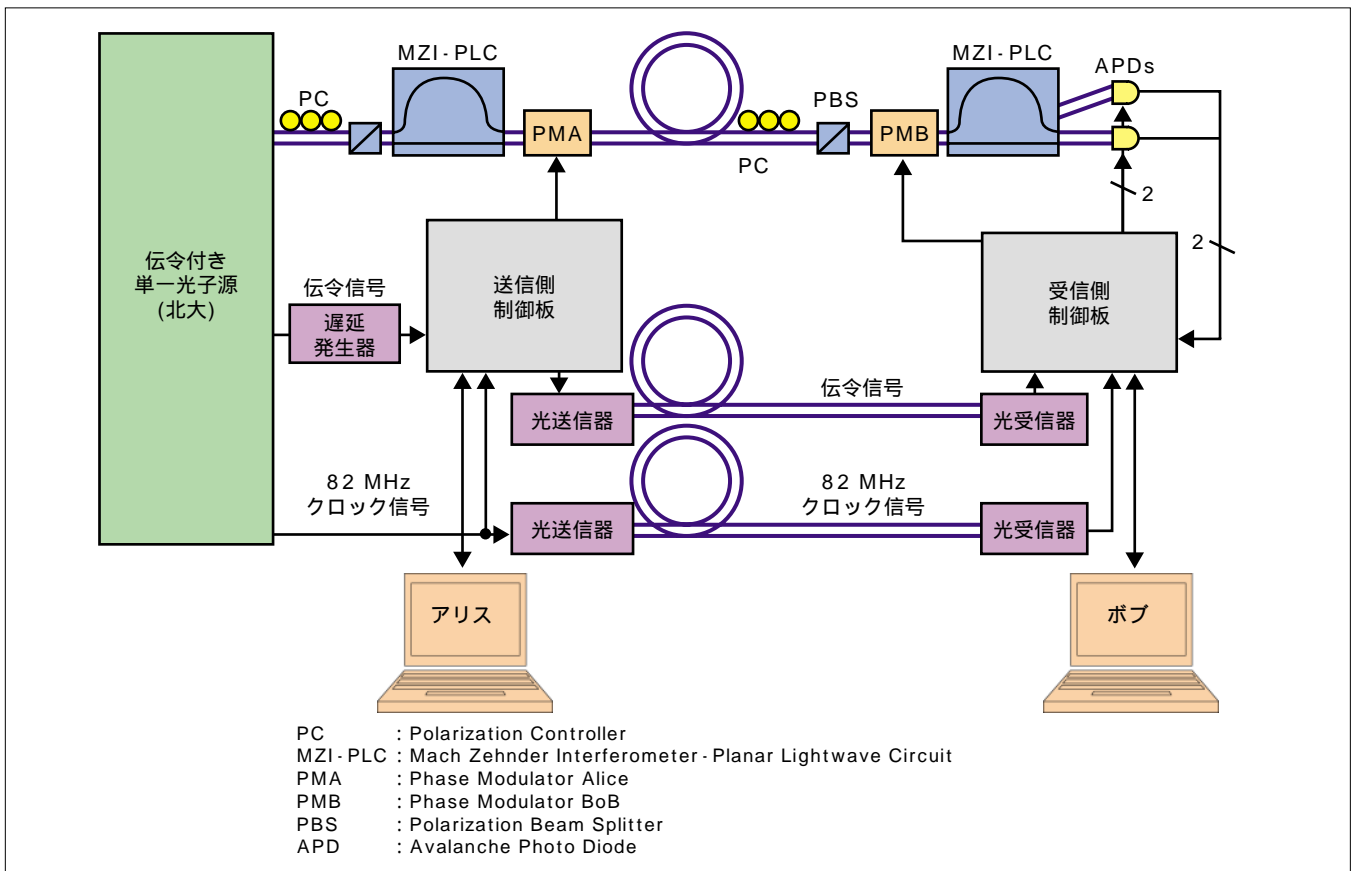
本稿では、このような脅威への対策として光子源をより完全に近づける方針を採用し、北海道大学電子科学研究所の竹内繁樹教授グループが開発した伝令付き単一光子源を

用いた量子暗号システムを開発し、量子暗号実験に成功したことについて述べる。

この量子暗号システムでは伝令信号と呼ばれる制御信号に加えて、クロック信号も制御信号として用いることでシステムの信頼性を向上させている。

これによって安全性の保証された通信距離の大幅な延伸を達成し、通信距離40kmでは量子鍵(かぎ)配布実験に、通信距離80kmでは原理検証実験に成功した。

また、厳密な意味での安全性の評価手法を確立し、この開発した評価手法で上記2つの実験についての安全性を確認することができた。



## 伝令付き単一光子源を組み込んだ量子暗号システム

左端の伝令付き単一光子源からは、上から順に単一光子、伝令信号、クロック信号が出力されている。単一光子は偏波制御子(PC)、偏光ビームスプリッタ(PBS)、マッハツェンダ干渉計を構成する石英平面光回路(MZI-PLC)を通して、位相変調器(PMA, PMB)でランダム変復調を受け光子検出器(APD)で検出される。この単一光子に先立って伝令信号が出力される。クロック信号と単一光子とのジッタは極めて小さい。