量子暗号の開発動向と安全性評価技術

長谷川俊夫*
石塚裕一*
鶴丸豊広**

Research Trend of Quantum Cryptography and Security Anaylsis

Toshio Hasegawa, Hirokazu Ishizuka, Toyohiro Tsurumaru

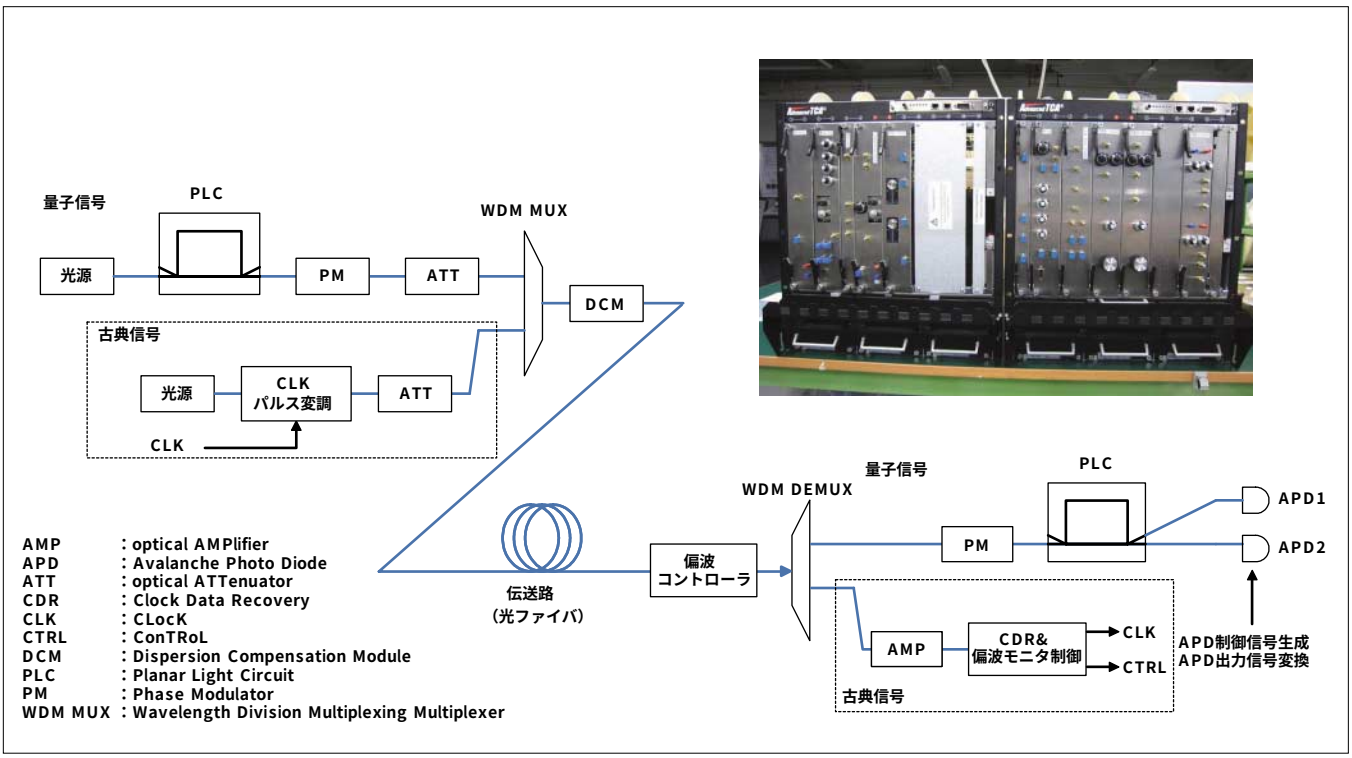
要　旨

量子暗号は物理の基本原理を利用しているため，物理法則で安全性が保証され，究極の安全性を提供する暗号技術である。量子暗号は，量子情報技術の中で最も多く実験や装置開発・フィールド試験が行われており，これまで，光学スキームとして一方向型やプラグアンドプレイ方式などによって100km程度の長距離実験が行われるにいたっている。また最近では，量子暗号の鍵(かぎ)配布プロトコルの中で代表的なBB84を改良し理想的な単一光子源を前提にしなくても，微弱コヒーレント光を用いて長距離での安全性が確保できる方式(例えばデコイ方式，差動位相シフト方式)が提案され期待されている。この場合，実装も比較的容易で，高速化開発に適した方式でもある。ただし，新しい方式に関しては今後まだ安全性の議論を行っていく必要があり，安全性評価技術が非常に重要となってきている。

現在，量子暗号の研究開発は，実用化を目指した装置開発の段階に到達しており，高い安定性を持ち，高速で将来のネットワーク化にも対応可能なものが望まれている。三菱電機が取り組んでいるものも，目標性能として通信距離50km，速度 1Mbpsの実用的な装置で次のような特徴を持っている。

(1)　古典信号と量子信号の時分割伝送(古典信号には，クロック情報及び偏波ゆらぎ補正情報を載せ，量子信号とあわせて送信する。受信側で信号分離し，クロック再生と偏波ゆらぎ補償のフィードバック制御を実施し安定性を高める。将来は経路選択／切替情報を載せることが可能である。)

(2)　BB84，デコイ方式，DPSQKD(Differential−Phase−Shift Quantum−Key−Distribution)の量子暗号プロトコル方式で光源繰り返し速度GHzレベル，数十km伝送対応の高速化に対応



開発中の量子暗号装置の基本構成とATCA規格準拠の量子暗号装置写真

当社が開発中の量子暗号装置の基本構成と装置の外観(右上)を示す。左上が送信側装置，右下が受信側装置である。高い安定性と高速化を特長とする。古典信号と量子信号の時分割多重分離，波長分離技術によって，古典信号に含まれるクロック・偏波情報をモニタし，同期ゲート制御及びフィードバック制御を行う。これによって環境温度変化や偏波ゆらぎを補償し，高い安定性を実現する。また，効率的実装のため，送受信システムをさらに機能分割し，ATCA(Advanced Telecom Computing Architecture)規格準拠の装置を開発した。

*情報技術総合研究所　**同研究所(理博)