論 文 の 内 容 の 要 旨

論文題目　Security of Quantum Key Distribution with Weak Coherent Pulses
（微弱コヒーレント光を用いた量子鍵配送の安全性証明）

氏　名　川上　駿

この論文では、微弱コヒーレント光を用いた量子鍵配送の安全性について解析する。第一に、差動四値位相シフト(DQPS)量子鍵配送プロトコルの安全性を証明する。DQPSプロトコルは現在広く実装が行われている位相変調型BB84（PE-BB84）プロトコルと本質的に同じ装置で実装可能である利点に加え、PE-BB84プロトコルよりも高い効率で鍵共有が可能であることが期待された。我々は、簡潔なBB84プロトコルの安全性証明を応用することによってDQPSプロトコルの安全性を証明し、二者間でやりとりする鍵長さを無限にした極限ではDQPSプロトコルの鍵生成レートがPE-BB84プロトコルを8/3倍上回ることを示した。

第二に、微弱コヒーレント光を用いた量子鍵配送プロトコルに有効な有限鍵長解析の手法を提案する。これまでの有限鍵長解析で多く用いられてきた超幾何分布を用いた手法に代わり、我々は単純な二項分布を用いた手法を提案し、実際に微弱コヒーレント光を用いたBB84プロトコルとDQPSプロトコルの安全性証明を行った。BB84プロトコルでは超幾何分布の手法に比べて推定数の少ない解析が可能となり、先行のBB84プロトコルの結果に比べて鍵生成に必要な検出シグナル数が10^7程度から10^4程度へと大幅に減少した。DQPSプロトコルに対しては、有限鍵長の影響を取り入れてもPE-BB84に対する鍵生成レートの優位性が依然として保たれていることを示した。