論文の内容の要旨

論文題目　Theory and Experiment of the First Decoy State Quantum Key Distribution Guaranteeing Quantitative Security in the Real-World Settings
（現実世界の設定下で定量的な安全性を初めて保証したデコイ法量子鍵配送の理論と実験）

氏名　長谷川　淳

（本文）量子鍵配送(QKD)は 1984 年に Bennett と Brassard によって提案された，量子通信路を用いて離れた 2 人が秘密鍵を共有するためのプロトコル(BB84)である．このプロトコルの重要な性質は，量子力学の基本原理と情報理論によって計算量に依らない無条件安全性が理論的に保証されていることである．さらに近年，現在の技術では完全な単一光子光源を利用できないため, 弱コヒーレント光に対して安全な QKD を実現する現実的な方法として，強度値の異なる複数のパルスによるデコイ法鍵配送プロトコルが提案された．

これらの安全性の多くは，プロトコルの符号長が無限大を仮定した下で行われた Gottesman-Lo-Lutkenhaus-Preskill (GLLP)の安全性議論に基づいている．しかし現実の世界の設定では，符号長は有限長であり，またそのため受信情報に含まれる物理揺らぎやサンプリング誤差といった統計揺らぎを無視することはできない．今までにも有限長符号によるデコイ法 QKD で統計揺らぎの影響を考慮した秘密鍵の生成レート解析及び量子暗号実験も行われているが，彼らの安全性はすべて，本来漸近での安全性しか保証されていない GLLP の議論を拡張して，秘密鍵の生成レートの評価を統計揺らぎを影響を考慮して導出したものであった．したがってそのような ad hoc なアプローチでは，符号長が無限大のときに盗聴者の情報量の極限が 0 であることしか保証できず，本質的に有限長での安全性を保証することはできないものであった．

本論文では, 現実の世界での安全性を初めて厳密に保証したデコイ法 QKD プロトコルを提案する．これは GLLP の漸近での安全性保証に基づくものではなく，林によって提案された有限符号長の下での盗聴情報量評価を拡張することで達成している．そして数値計算を行い，漸近でのデコイ法 QKD との比較を行うことで，提案したデコイ法 QKD の性能や振る舞い，及び光強度値などの本プロトコルのパラメータの最適値を示した．その結果，漸近でのデコイ法 QKD の場合では伝送距離が十分長いときでも秘密鍵の生成に用いる光強度値は 0.3 を取っていたのに対して，本デコイ法 QKD で最大伝送距離を達成するときの最適な光強度値が統計揺らぎの影響から非常に小さな値となることを明らかにした．また実際に量子暗号通実験を行うことで，揺らぎのある装置やファイバの元での本プロトコルの性能も明らかにした．その結果，光ファイバ 20km で真空を含めた 4 種類の強度によるデコイ法 QKD の実験を行い，符号長 10^5 で平均盗聴情報量が 2^-9 ビット以下であることを保証した秘密鍵を，200 bps の速度で伝送することに成功した．さらに数値計算と比較することで，装置やファイバの揺らぎの影響の大きさを示した．