様式３

論　文　内　容　の　要　旨

氏　　名　　（ 水谷　明博 ）	
論文題名	Robust and efficient quantum key distribution with practical devices （現実的な装置を用いた堅牢かつ効率的な量子鍵配送）

論文内容の要旨

量子鍵配送(QKD)は、量子状態の伝送、測定と認証された古典通信路を用いることで、離れた2者間に秘密鍵を配布する。この秘密鍵をメッセージの暗号化/復号化に用いることで、情報理論的に安全な通信が可能になる。秘密鍵の配布には、量子通信で盗聴者に漏洩した情報量を推定する安全性証明に基づいたデータ処理が必要である。その際、盗聴者は如何なる盗聴もできるという最悪の状況を考えるが、その一方で送受信者が持つ装置はある性質を満たすと仮定する。この性質が現実の装置の物理特性と食い違う場合、現実のシステムの安全性を保障できないという問題がある。そのため、現実の物理特性を反映した装置モデルで安全性証明を行うことがQKDの実現のために重要である。受信装置に関しては、装置モデルに依存せずに安全なQKDが可能である方式が提案されている一方で、送信装置の不完全さを考慮した安全性理論は十分とは言えなかった。本研究の第1の目標は、この送信装置の不完全さに対して堅牢な安全性理論を構築することである。また、高効率なQKDの実現に向けて、QKDの効率を向上させる理論の構築を第2の目標とした。

第1の目標については、送信状態間の相関を考慮し、送信者の過去の選択に依存しない相関がある枠組みで、典型的な不完全さである位相と強度の揺らぎを考慮した安全性証明を与えた。数値解析を行った結果、現実的な揺らぎと送信パルス数でもQKDが実現可能であることを明らかにした。

また、総当り差動位相シフト方式に対して、送信装置に僅か3つの現実的な仮定を課すだけで安全性が保障されることを示し、この方式が送信装置の不完全性に対して堅牢であることを明らかにした。

第2の目標については、簡易な実験系で実装可能な差動位相シフト(DPS)方式に対して、量子力学の相補性に基づく簡潔な証明を与えた。その結果、先行研究よりも高効率な鍵生成が可能であることを明らかにした。

また、新たなDPS方式としてSmall-number-random DPS方式を提案し、通信路の擾乱情報を用いて安全性証明を行った。その結果、干渉測定にランダムに切り替えられる遅延を少数加えるだけで、DPS方式に比べて高効率な鍵生成が可能であることを明らかにした。

様式７

論文審査の結果の要旨及び担当者

氏　　名　　（ 水谷　明博 ）		
論文審査担当者	（職）	氏　　名
	主 査　　教 授	井元　信之
	副 査　　教 授	関山　明
	副 査　　教 授	石原　一

論文審査の結果の要旨

量子暗号は実地試験に到達している方式がいくつかあるが、そうでないものも含め、最初に提案されたもの（BB84と呼ばれる）から最新のもの（RR-DPS）まで数多くある。その理由は、商用としてどれが生き残るかわからないこともあるが、その安全性（秘匿性）を保証する条件や目的とするところ（遠距離なのか高速なのか等）が異なるためである。特に条件設定は重要であるが、その理論は容易ではないため、量子暗号の研究はまず新方式提案が先になされ、条件設定や安全性証明は後回しという形態をとっている。そのため、提案論文自体に条件設定や安全性証明も書いてあることはあっても多くはなく、むしろ既に提案だけされている方式の条件設定や安全性証明の論文が熱望されることになる。水谷氏の数多くの論文はその両方のケースにまたがる。歴史的にはまず「単一光子源、光伝送路、光子検出器のどれも理想的」というあり得ない条件設定から安全性証明が始まり、徐々に現実性を取り入れながら段階的に安全性証明が進化して来た。このようなハード的現実性を条件設定とするほか、光パルスを無限個使える極限を仮定するか有限のN個から安全鍵を抽出するかという情報理論的条件設定もある。また安全性証明とは、単位時間（単位光パルス）当たりの安全鍵生成率が正となる領域（伝送距離は長くとれないが0でないとかノイズ量は小さい必要があるが0でない等の領域）が存在することを示すことである。この領域がない方式は提案失敗となる。一方、安全性証明理論には優劣がある。劣った証明法では安全サイドを余分に見るため「そういう領域はない」と結論した同一装置が、優れた理論は余計なマージンを取らないので「いや安全である」と判定することがある。すなわちハード的には何ら進歩がなくとも理論の進歩で「より優れた量子暗号に変身する」ことが起きる。

水谷氏の博士論文は全てこうした「初めての証明」「より優れた証明」「条件の緩和」「新方式の提案」を謳ったものである。氏の研究成果を大きく分けるならば、まず[A]光源の完全性を条件から外した安全性証明と[B]DPS（差動位相シフト方式：隣り合う光パルスの相対位相に0と1を符号化する、高効率を特徴とする）方式の安全性証明に分類される。さらに[A]は(A1)損失を許す量子暗号から「位相と強度が一定」という条件を外し、同時に「利用できるパルス個数は無限」も外した安全性証明と(A2)RR-DPS方式は光源の不完全性に対して強い耐性があることを示した理論に分類できる。[B]も二つに分類すると(B1)DPS方式の「より優れた証明」を発見し、（ハード的には変更せず）その効率を上げたことと(B2)DPS方式に新たにランダム遅延を導入することによりエラー耐性が上がることを示した（簡単なハード変更による大きなエラー耐性の獲得)。

以上の研究は量子暗号で有望とされるDPSやRR-DPS方式などの諸方式に理論の面から簡単なハード変更で絶大な効果を生む提案をし、またはハード変更は要求せずその性能だけ大幅に向上させる優れた安全性理論を構築し、さらに現実的条件を取り入れることを可能にするなど、質的にも量的にも大きな進歩を生んだ。よって博士（理学）の学位論文として価値のあるものと認める。