

平成27年度研究開発成果概要書

課題名 : セキュアフォトリックネットワーク技術の研究開発
採択番号 : 157 イ 01
個別課題名 : 課題イ 量子暗号安全性評価理論
副題 : 量子鍵配送実システムの安全性と安定性の向上及び高速化

(1) 研究開発の目的

(1-1) 研究の概要

離れた場所にいる2者の間に共通で第三者に知られていないビット列の乱数表、すなわち鍵を配送することは秘匿通信やメッセージ認証などの暗号を安全に運用する上で必須となることである。この鍵配送を行う数学的な提案の中で、任意の盗聴に対して安全であることが保障されている唯一の方式が量子鍵配送であり、近年一部で量子鍵配送システムが構築されつつある。しかし、実践的な理論研究の不足や数学モデルと実際の装置との差が原因で、実際の量子鍵配送システムは安全性と通信速度の両面で改善の余地が多く残されている。さらに、量子鍵配送システムはデータ処理を行うための高価なハードウェアを実装した例もあり、システムが複雑で安定性が実用運用に耐えられるレベルではない。

本研究は、実践的な理論や装置の不完全性の取り扱い方の研究などの研究を推進することにより、安全強度が強く、通信速度も速く、かつ実用レベルの運用に耐えられる安定性を有する量子鍵配送システムを構築するための指針を構築することが目標である。ここで与えられた指針は量子鍵配送安全性評価基準として策定し、最終的には、盗聴の心配のない安全な通信を実現することによる社会貢献を主な目的とする。

(1-2) 研究の背景と目的

既存の量子鍵配送システムは、性能が優れているものでは概ね50kmの距離で数100kbit/secの鍵生成率を達成している。単一光子レベルの信号を扱っていることを考えると、この数値は素晴らしいものであるが、その一方で、この数値を達成することに注力しすぎるあまり、おろそかになってしまっている点や若しくはまだ検討の余地がある点が存在する。

1つ目は、そもそも鍵を作る際に用いている理論が未だに発展途上ということである。これは、多くの安全性理論が、データ数の非常に大きい漸近的なことを考えていることが主な原因であり、実際のシステムの安全性を保障するためには、まずは有限のデータから安全な鍵を如何にして生成するかを考える必要がある。

2点目は、鍵を生成するには多くのデータ処理を行う必要があるが、そのデータ処理をより高効率化することにより、更なる高速化が図れる、という点である。この効率化により更なる安定性がもたらされるという結果も大いに期待できる。3点目は、既存のシステムが用いている装置の性質が実は良く分かっていないことが挙げられる。つまり、その装置は量子鍵配送の理論が仮定する数学モデルに厳密に従っているわけではなく、理想モデルとのズレが存在することが考えられる。更に、思いもよらない情報漏れなどを起こしている可能性もある。これらの理想モデルとの実際の装置のズレを一般にサイドチャンネルと呼んでいる。

4点目は、上記の三点の改善を図るためには応用研究を見据えた理論をより発展させる必要があることである。このような理論の発展により、実は装置が大幅に簡素化できる、等という可能性があり、実際量子鍵配送の理論の発展とともに装置への要求は確実に下がってきている、という歴史がある。

最後の点として、量子鍵配送システムと通常の光ネットワークの接続の問題がある。通常の光ネットワークへの量子鍵配送システムの導入はある意味、量子鍵配送の研究者にとって究極の目標である。このことは専用線を使った量子鍵配送システムだけを考えているときには想像もつかないような問題が生じる可能性が多く生じることを意味し、量子鍵配送の研究者と光ネットワークの研究者の協力関係のもと、如何にして量子鍵配送システムを光ネットワークへ導入するかを検討する必要がある。

以上述べた五点を解決しないことには、実運用に耐えられる量子鍵配送システムの実現は無理である。本研究はこれらの五点の問題に対して理論の立場と基礎実験の立場からの解決することを目的とする。

(2) 研究開発期間

平成23年度から平成27年度（5年間）

(3) 委託先

(株) 日本電信電話株式会社 <幹事>、
三菱電機株式会社 (株)、国立大学法人 北海道大学、
国立大学法人 名古屋大学、国立大学法人 東京工業大学

(4) 研究開発予算（契約額）

総額 61 百万円（平成 27 年度 11 百万円）
※百万円未満切り上げ

(5) 研究開発課題と担当

課題イ-1 有限長解析の研究

- (課題イ-1-1) デコイを用いない BB84 方式での効率的パラメータ推定理論 (NTT)
- (課題イ-1-2) デコイ方式の推定精度向上 (名古屋大)
- (課題イ-1-3) デコイを用いた BB84 方式の効率的パラメータ推定理論 (東工大)
- (課題イ-1-4) サイドチャンネルを取り入れた有限長解析及び BB84 方式以外の効率的パラメータ推定理論 (三菱電機)

課題イ-2 鍵蒸留処理アルゴリズムの高速化及び簡素化の評価

- (課題イ-2-1) 有限長符号での効率的な秘匿性増強アルゴリズムの研究 (名古屋大)
- (課題イ-2-2) 誤り訂正の高速化：符号化率と演算速度の向上のための基礎的研究 (三菱電機)
- (課題イ-2-3) 誤り訂正の高速化：符号化率と演算速度の向上のための工学的な研究 (東工大)
- (課題イ-2-4) 乱数の高速生成のための理論提案及び基礎実験 (北大)
- (課題イ-2-5) 認証プロトコル等、量子鍵配送システムが用いる古典通信の高速化及び効率化 (NTT)

課題イ-3 サイドチャンネルの特定及び対策

- (課題イ-3-1) デバイス評価のためのテストベンチの構築 (北大)
- (課題イ-3-2) QKD デバイスのモデル化、評価方法の検討 (三菱電機)
- (課題イ-3-3) QKD 実システムでの評価 (北大)
- (課題イ-3-4) 古典的サイドチャンネルの検討及び、QKD デバイスモデルが与えられた元での、基礎的安全性証明理論の研究 (NTT)

課題イ-4 量子鍵配送の多様化へ向けた研究

- (課題イ-4-1) 最適なプロトコルの選定の研究 (NTT)
- (課題イ-4-2) プロトコルの性能向上基礎提案 (東工大)
- (課題イ-4-3) 安全性証明のフレームワークの精密化及び簡素化の研究 (三菱電機)

課題イ-5 安全性評価基準の策定 (NTT)

(6) これまで得られた研究開発成果

		(累計) 件	(当該年度) 件
特許出願	国内出願	8	1
	外国出願	0	0
外部発表	研究論文	49	38
	その他研究発表	91	34
	プレスリリース	2	2
	展示会	0	0
	標準化提案	0	0

(7) 具体的な成果実施内容と成果

(1) (課題イ-1)

- ・デコイを用いる BB84 方式において、二項分布の議論に帰着させた評価を用い、正規近似を用いないパラメータの推定誤差の見積もりを行う。そして、従来よりも、より現実的な設定で有限長での犠牲ビット数を導出した。特に、今年度は、この提案手法が漸近的にこの評価方法が一定の範囲での最適性能を実現することを示し、漸近特性を明らかにした。

- ・半量子鍵配送プロトコルについて、解析方法を改善して図のような鍵レートを得た。従来 8% 程度の分極レートでしか秘密鍵を生成出来なかったが 11% 以上でも秘密鍵生成出来ることを明らかにした。

(2) (課題イ-2)

- ・有限長符号での効率的な秘匿性増強アルゴリズムの研究 (名古屋大)

- ・秘匿性増強アルゴリズムとしては Toeplitz 行列を用いる方法が知られている。秘匿性増強アルゴリズムの効率を向上させるために、より広いクラスの範囲で秘匿増強のプロトコル探索し、昨年度までの研究で、これまでよりも大きなサイズで実行可能でかつ PC で実装可能な秘匿増強のアルゴリズムを開発していた。本年度は、さらに、秘匿性増強の際に用いる種乱数の数の評価をさらにより緻密に行った。

- ・誤り訂正に関して、符号化を高速に行うと同時に、数ビットのエラービットが残ってしまうエラーフロア現象を解決する方法を提案した。LDPC 符号の特徴として、復号は原理的に高速に行うことができるが、符号化には多くの計算量が必要であった。これまでの LDPC 符号では、符号に構造を持たせることによってエラーフロアを許容することと引き換えに高速化が可能となっていた。本研究結果により、高性能な LDPC 符号である空間結合符号の構造をほとんど変更することなく高速な符号化法を実現することが可能となった。

(3) (課題イ-3)

- ・デコイ状態の光強度揺らぎに関連して、動作電圧の変化に対して出力強度の変化が小さい変調方式を提案した。変調信号電圧の揺らぎの影響を抑えるためネスト型変調器(NM)を用いた強度変調を提案し、実際に強度の揺らぎを大幅に抑えられることを実験で確認した。

- ・課題ア、イ、ウ、エの全機関と協力し、「量子鍵配送技術の標準化と多層防御セキュリティの強化に向けた検討報告書」の執筆を行った。

- ・我々は、昨年度提案した、基底不一致の事象を上手く用いることによる状態準備の不完全さを克服する方法を有限長に拡張し、有限長の枠内でも暗号鍵が生成できることを示した。更に、全ての位相変調器と強度変調器には動作精度に限界がある。我々は、この有限の動作精度を考慮した安全性証明を行った。

(4) (課題イー4)

・(学習院大学との共同研究) 2014年度に我々は「多体 squash 演算子」(MPS0)の手法を提案し、それを可換検出器による装置無依存量子暗号(DIQKD)プロトコルの安全性証明に適用した。それに続き今年度は、MPS0 の適用範囲拡大をめざし、Bennett 1992 (B92)プロトコル、および一般の DIQKD プロトコルの安全性証明に役立てるための検討を行った。そしてその検討を行う中で、2014年に実施した解析の問題点を発見したので、それを修正した。その結果として、DIQKD プロトコルに対する厳密な安全性証明を得ることに成功した。