

平成25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 62百万円（平成25年度 13百万円）
※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	7	4
	外国出願	0	0
外部発表	研究論文	11	5
	その他研究発表	59	35
	プレスリリース	0	0
	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) 有限体の構造を用いて、これまでのハッシュ関数よりも、必要なランダムシードの数が少ないハッシュ関数を ϵ almost dual universal hash function の具体例として構成した。そして、そのハッシュ関数を少ない計算量で効率的に実行するためには、その乗算の計算量が小さい有限体が必要となるが、そのような有限体の構成方法を与えた。なお、その構成には Artin 予想が重要な役割を果たす。
- (2) 量子鍵配送は物理暗号であるので、安全性を確保するためには実験装置にはいくつかの条件が満たされる必要がある。我々は『盗聴者がプローブ光を当てることにより送信者や受信者の装置の内部状態を監視できない』という条件と『光子検出器の量子効率はそのまらっていないなければならない』という二つの条件を実際のデバイスで高いレベルで達成するための実験装置を提案した。
- (3) Tomamichel らの安全性解析手法の統計的推定の手続きを見直し改善することによって、従来最も長い秘密鍵長を保証していた林・鶴丸らの安全性解析手法と比べて遜色ない秘密鍵レートを得られることを明らかにした。
- (4) 誤り訂正技術に関して、 L 個の LDPC 符号を、結合した誤り訂正符号を考案した。十分大きな結合数 L に対して、考案した符号が、全ての符号化率に対してレートコンパチブルであり、消失通信路のオーバーヘッドをゼロにする、つまり通信路容量を達成することを証明した。
- (5) パルス発振半導体レーザに着目し、パルス間の干渉信号を乱数として用いることを提案した。干渉信号の自己相関関数が速やかに減衰することを確かめた。
- (6) クロック周波数 10GHz でパルス発振するレーザのパルス間位相相関を測定し、レーザに印加する直流電流との関連を明らかにした。レーザがオフになる時間が 25ps 程度あればパルス間の位相相関はなく、QKD 装置に使用可能であることを示した。