平成２６年度研究開発成果概要書

課題名　　：セキュアフォトニ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３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、鍵を生成する際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 26 年度　　８百万円）
※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	0	7
	外国出願	0	0
外部発表	研究論文	21	10
	その他研究発表	101	40
	プレスリリース	2	1
	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)

量子鍵配送(QKD)は理想的な環境ではその安全性は完全に保障されているものの，現実の環境は不完全でそれを考慮した現実的なプロトコルの研究はまだ発展途上である。特に問題となるのが，光源の不完全性と符号長が有限サイズでの安全性の評価である．本年度は，有限長と漸近理論との中間となる二次の漸近論を検討した．

(2)(課題イ－２)

・秘匿増強時に用いるにハッシュ関数をさらに改良した．昨年度の研究では，圧縮率が 1/2 以上の場合にのみ従来法よりも，大幅に必要な種乱数の量を減らすことに成功していた．本年度は，圧縮率が 1/2 以下の場合に，大幅に必要な種乱数の量を減らすことに成功した．これにより，全ての範囲で大幅に必要な種乱数の量を減らすことに成功したことになる．

・ 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

前年度までに考案したレートコンパチブルで高性能な空間結合符号をもとに、組織的でスライド窓復号可能な高速な符号器と復号器の実装方法を考案した。

・高速な乱数生成方式として、利得スイッチ半導体レーザのパルス間位相を干渉計で取り出す方法を提案した。これは発振パルスの位相がランダムであることを利用したもので、ランダム性のメカニズムが自然放出光という量子力学的現象によるため、本質的にランダムであると考えられる。我々は QKD 装置の光源部にファラディミラーと高速フォトデテクタを付加するだけで乱数が得られる実装方式を開発し、発生した乱数が NIST　SP-800 乱数テストに合格することを確かめた。

(3)(課題イ－３) デバイス評価のためのテストベンチの構築

・デバイス評価の対象として、光源のパルス間位相相関を測定する方法を検討した。パルス間の位相は干渉計によって測定されるが、我々はクロック 1GHz 用にマイケルソン干渉計を、さらに 10GHｚではファイバ型マッハツェンダー干渉計を用いる系を開発した。さらに、QKD 装置の光源と一体化可能な乱数発生器としても用いることができる PLC 干渉計を用いる方法を開発した。実験によれば、10GHz まで位相相関を持たないパルスを得ることが可能であり、そのための条件を示した。また、位相相関が QKD の安全性に与える影響を理論的に評価し、位相が乱雑であるとみなすことのできる範囲を干渉の明瞭度として示した。

・課題アと協力して、光源の強度変動を測定する方法を開発し、評価した。変動の詳細、変動のメカニズム、変動の抑圧方法については現在解析中である。また、光子検出器の検出効率のばらつきを測定し、補正する方法の開発も行った。

・従来理論によれば、BB84 プロトコルにおいて状態準備に不完全性がある場合、通信距離が大幅に縮小されてしまうことが知られていた。我々は、既存の方法で捨てられてきた、基底不一致の事象を上手く用いることにより、状態準備の不完全さが通信距離にほとんど影響を与えないプロトコルを提案した。更に、我々の方法により、BB84 では３状態のみを用いれば良いことが示された。

(4)（課題イ－４）

・当研究機関で既に開発した B92 量子鍵配送プロトコルの漸近的鍵レートの解析方法と、Scarani-Renner らの有限長鍵レートの解析方法を組み合わせて、B92 量子鍵配送プロトコルの有限長鍵レートの下界を与えた。

・量子中継は量子通信の長距離化に必須とされている技術であるが、その実現には物質量子メモリが必要だと広く信じられてきた。本プロジェクトで は、そのような分野の常識に反し、一切の物質量子メモリを用いず、光学系だけに基づく量子中継方式の発見に至った。「全光量子中継方式」と名 付けられた本方式は、単一光子源、線型光学素子、光子検出器、アクティブフィードフォワード技術の

みで実現が可能である。そのため、量子中継 を含むような「限界なき量子ネットワーク」は、従来の通信の全光化の流れの究極形に位置し得ることが示唆された。