研究開発成果概要書

１　研究開発成果概要書

平成２３年度研究開発成果概要書
「セキュアフォトニックネットワーク技術の研究開発
個別課題：課題イ　量子暗号安全性評価理論」

（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）委託先企業
（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　東北大学、国立大学法人　東京工業大学
（４）研究開発予算（百万円）
平成２３年度　　１５（契約金額）
（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（東北大）
（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　（東北大）
（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	0
	外国出願	0	0
外部発表	研究論文	2	2
	その他研究発表	6	6
	プレスリリース	0	0
	展示会	1	1
	標準化提案	0	0

具体的な成果
(1) Hash 関数を ε-almost dual universal2 hash 関数まで広げた量子暗号の安全性評価に成功．これにより，従来よりも広いクラスの hash 関数が使用可能となる（IEEE Transactions on Information Theory へ投稿し、又 SCIS2012 において発表済み）
(2) 安全性が検出器の性質に無依存な量子鍵配送方式の新たなプロトコルを２つ提案し、光源の位相エラーなどの現実的なエラーを考慮しても無条件に安全な鍵が生成できることを示した(Physical Review A に受理)
(3) 従来のユニバーサルハッシュ関数を拡張した「双対ユニバーサル

ハッシュ関数」 の概念を導入するとともに、その量子暗号および現代暗号への応用を示した。この双対ユニバーサルハッシュ関数を用いることにより、量子暗号で必須のデータ処理（プライバシ増幅）の処理速度や符号化率を向上させることが期待できる（QCRYPT 2011 において発表)。

（７）研究開発イメージ図

別紙の通り