平成２４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（157 イ 01）
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（百万円単位切上げ）
　　平成２３年度　　１５（契約金額）
　　平成２４年度　　１４（　〃　　）
（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	3	3
	外国出願	0	0
外部発表	研究論文	9	7
	その他研究発表	27	21
	プレスリリース	0	0
	展示会	1	0
	標準化提案	0	0

具体的な成果

(1) 本年度はデコイ法を有限サイズで実装するための研究を行った.

具体的には，区間推定で強度ごとの検出レートなどを推定し，デコイ法で状態ごとの検出レートを導き，最後にパーセント点を用いて，生鍵の内訳を推定した．有限サイズでの漏洩情報評価理論を生鍵の内訳に適用し最終的に犠牲ビット数を求めた．さらに，大規模データでの区間推定及びパーセント点の計算方法を検討した．

(2)量子鍵配送システムでは、情報の符号化のために位相変調器を用いるが、実際に施す位相変調の値には避けられない誤差がある．安全性を保障するためには、実際に施した位相変調の値をリアルタイムで監視する必要がある．今年度はこの位相変調のリアルタイム監視のための実験的な手法を提案した．

(3) レーザのパルス間に位相相関が存在すると漏えい情報量が増大することが知られている．今回繰り返し１GHｚで発振する半導体レーザのパルス間位相相関をパルス間の干渉性で評価する実験系を開発した．クロック周波数 1GHz においても，利得スイッチによってパルス発振させたレーザの隣接パルス間に位相相関は現れないことを示した．一方，連続発振するレーザを強度変調器でパルス化した光源では強い位相相関が表れた．

（７）研究開発イメージ図

平成24年度「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に関する研究開発」の研究開発目標・成果と今後の研究計画

1. 実施機関・研究開発期間・研究開発費

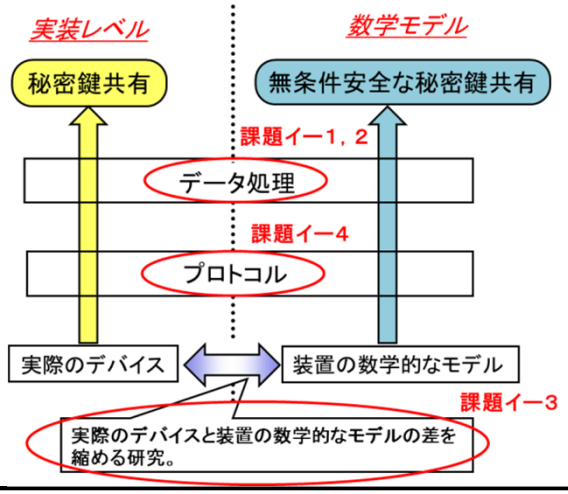
実施機関:　(株) 日本電信電話株式会社　＜幹事＞、（株） 三菱電機株式会社、国立大学法人, 北海道大学、国立大学法人, 名古屋大学、国立大学法人, 東京工業大学
研究開発期間:　H23年度からH27年度（5年間）
研究開発費:　総額67百万円　（H24年度　14百万円）

2. 研究開発の目標

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理論の発展・確立を目指す

3. 研究開発の成果

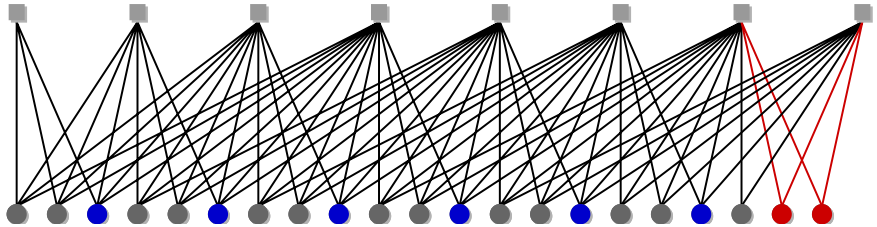
①量子鍵配送技術（研究開発目標）



左に記した課題研究はお互いを密に連携させて行われる。これらの成果は最終的には安全性評価基準の策定に用いる（課題イー5）

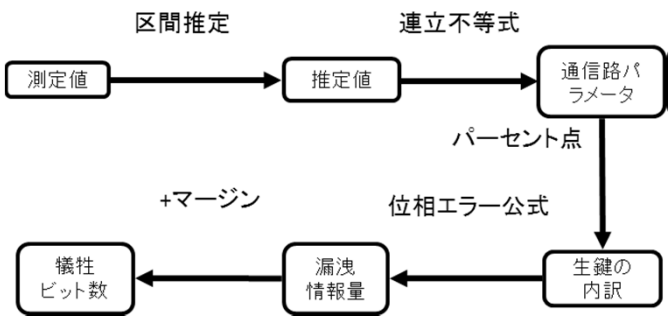
②課題イー2のH24年度成果

空間結合符号（畳み込みLDPC符号）の高速な符号化法を開発した



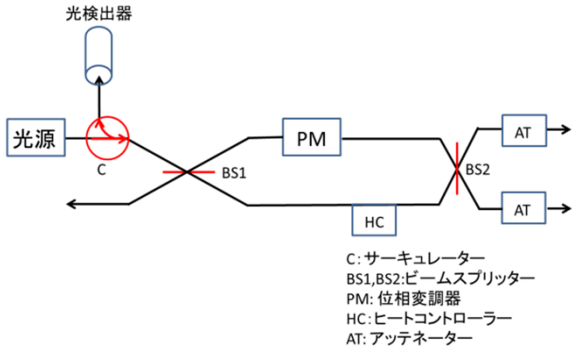
空間結合符号を表すプロトグラフ：グレーの情報ビットノードから青と赤のパリティビットノードを高速に求めることができる.
（東工大）

②課題イー1のH24年度成果



デコイ法を有限サイズで実装するための研究を行った。有限サイズにおいてのパラメータ推定の流れ及び用いる手法は左図のようにまとめられる。（名古屋大）

②課題イー3のH24年度成果

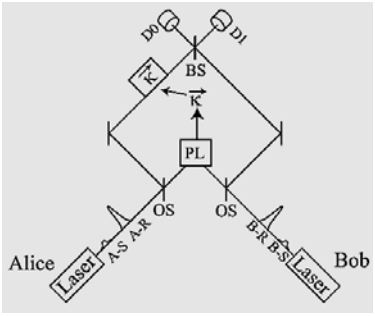


量子鍵配送において、実際に施した位相変調の正確なリアルタイム測定技術を提案した。また、安全な鍵生成のためには、ひたすら正確な位相変調を目指さなくても、ノイズを意図的に印加することも選択肢の一つだということを示した。(NTT)

平成24年度「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に関する研究開発」の研究開発目標・成果と今後の研究計画

3. 研究開発の成果

②課題イー3のH24年度成果

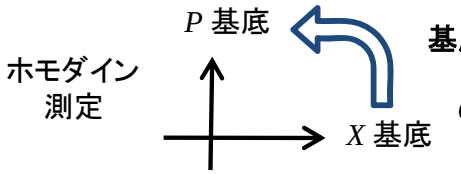


検出器測の不完全性が安全性に全く影響を及ぼさない測定装置無依存量子鍵配送において、送信するパルスの不完全性を定量化するパラメータは、フィデリィティーと送信パルスの密度行列の特定の純粋化状態の内積との積であることを示した。(NTT)

②課題イー4のH24年度成果

（課題イ-1-4, 三菱電機）

1. ホモダイン検出のsquash演算子が存在する十分条件を与えた。
（学習院大学との共同研究）

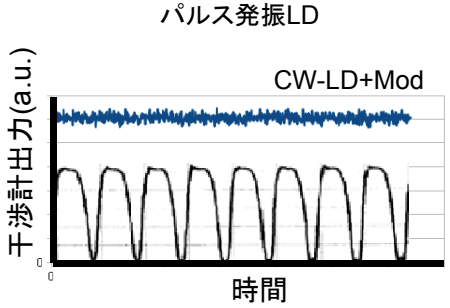


基底変換 ＝ フーリエ変換
これをユニタリ変換とみなすとC_4対称性が自動的に表れる。

ホモダイン測定に内在する対称性を利用し、squash演算子の構成に成功。
⇒ CVQKD方式とBB84方式の安全性が等価であることを示唆する。

2. CVKQD方式に用いる鍵蒸留アルゴリズムの最適化について検討した。
（学習院大学、東工大と共同）

②課題イー3のH24年度成果

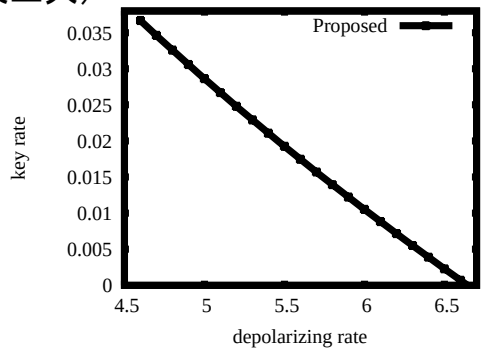


イ-3　パルス間位相評価

QKD装置光源のパルス間位相相関評価系を開発し，以下のことを見出した
- 1GHz程度の繰り返しではパルス発振レーザでは位相相関は現れない
- 連続光を変調してパルス化した光源は位相相関を持つ（北大）

②課題イー4のH24年度成果

単一光子B92プロトコルの漸近鍵レートを凸最適化問題として定式化し直すことにより、従来よりも長い鍵を漸近的に得られる（東工大）



4. これまで得られた成果（特許出願や論文発表等）　※成果数は累計件数と（ ）内の当該年度件数です。

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース	展示会	標準化提案
量子暗号安全性評価理論に関する研究開発	3(3)	0 (0)	9(7)	27(21)	0	1(0)	0(0)

5. 研究成果発表会等の開催について

（1）産学官連携のための量子鍵配送システム及び理論研究運営会議を毎年主催し、All Japanの取り組みを牽引

NICT委託研究課題イ、課題アとNICTの研究者が一同に会し、最新の研究成果を発表し合うとともに、今後の量子鍵配送システム開発へ最新理論の結果を反映させるべくオープンな議論を行った。

6. 今後の研究開発計画

この成果により、今後、どのような研究を行うのかを例示を上げながら、具体的、かつ簡潔に記載して下さい。

イ―1
・今年度は有限長での統計誤差を考慮に入れたデコイ法のプロトコルを作成した．しかしながら，このプロトコルについては十分な検討がなされていない．次件度は，このプロトコルについて，実装のための改良点の有無を含め十分に検討し，改良すべき点が見つかれば改良を行う．
イ―2
・空間結合符号を利用したQKDに適した誤り訂正技術を開発する．
イ―3
・光源のパルス間位相相関に関してレーザの励起条件，動作周波数に対する依存性を評価する．また，パルスごとに位相を測定し，ランダムになっていることを確認する．
・送信パルスや検出器等に存在する更なる不完全性の模索及びその対策を提案する．
イ―4
・CVQKDについて： squash演算子の存在する必要十分条件を明らかにする。またその結果をCVQKD方式の安全性証明に適用し、無条件安全性を証明する。さらにその知見を元に、最適な鍵蒸留方式を考案する。
・DPSQKDの無条件安全性を証明する。
・レーザの位相乱雑性を利用する乱数発生法の原理実証を行う
・単一光子B92プロトコルの有限長における安全性解析を行う。