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

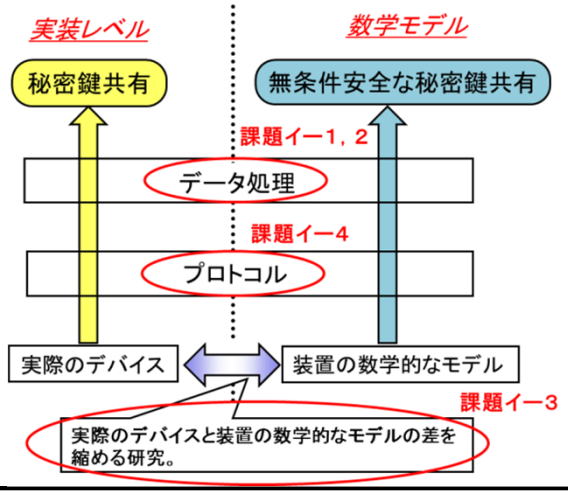
実施機関:　(株) 日本電信電話株式会社　＜幹事＞、（株） 三菱電機株式会社、国立大学法人, 北海道大学、国立大学法人, 名古屋大学、国立大学法人, 東京工業大学
研究開発期間:　H23年度からH27年度（5年間）
研究開発費:　総額67百万円　（H24年度　14百万円）

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

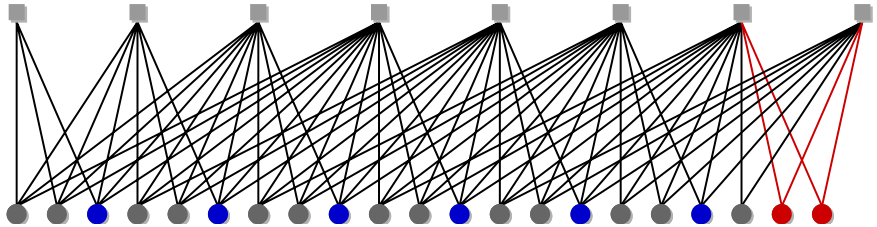
①量子鍵配送技術（研究開発目標）



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）

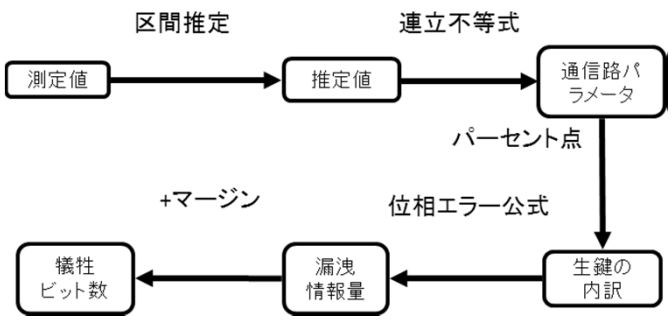
②課題イー2のH24年度成果

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



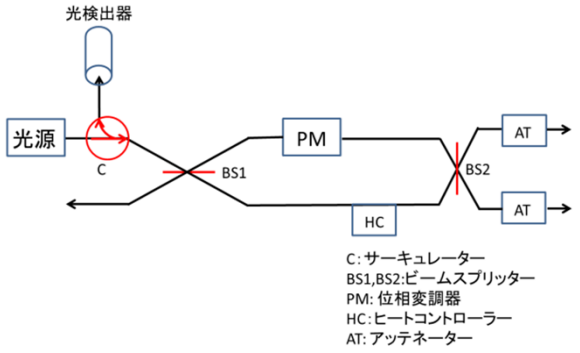
空間結合符号を表すプロトグラフ：グレーの情報ビットノードから青と赤のパリティビットノードを高速に求めることができる.
（東工大）

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

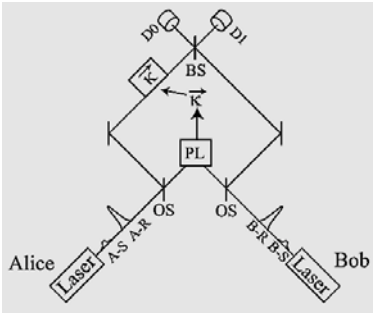


量子鍵配送において、実際に施した位相変調の正確なリアルタイム測定技術を提案した。また、安全な鍵生成のためには、ひたすら正確な位相変調を目指さなくても、ノイズを意図的に印加することも選択肢の一つだということを示した。(NTT)

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

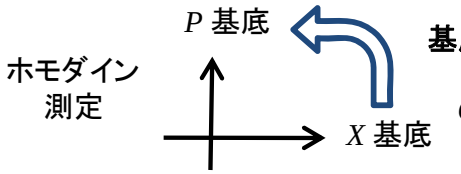


検出器測の不完全性が安全性に全く影響を及ぼさない測定装置無依存量子鍵配送において、送信するパルスの不完全性を定量化するパラメータは、フィデリィティーと送信パルスの密度行列の特定の純粋化状態の内積との積であることを示した。(NTT)

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）

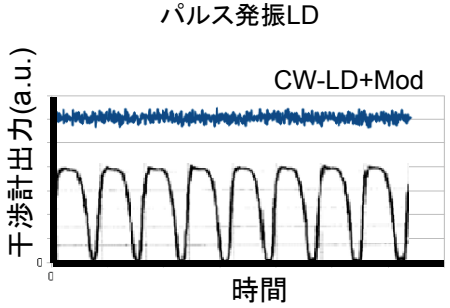


基底変換 ＝ フーリエ変換
これをユニタリ変換とみなすとC_4対称性が自動的に表れる。

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

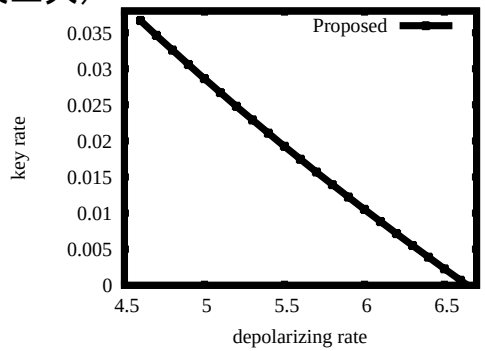


イ-3　パルス間位相評価

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。