平成25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

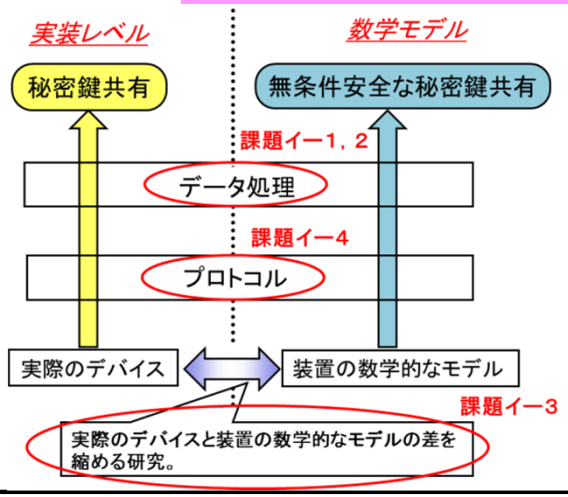
実施機関:　(株) 日本電信電話株式会社　＜幹事＞、（株） 三菱電機株式会社、国立大学法人, 北海道大学、国立大学法人, 名古屋大学、国立大学法人, 東京工業大学
研究開発期間:　H23年度からH27年度（5年間）
研究開発費:　総額62百万円　（H25年度　13百万円）

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

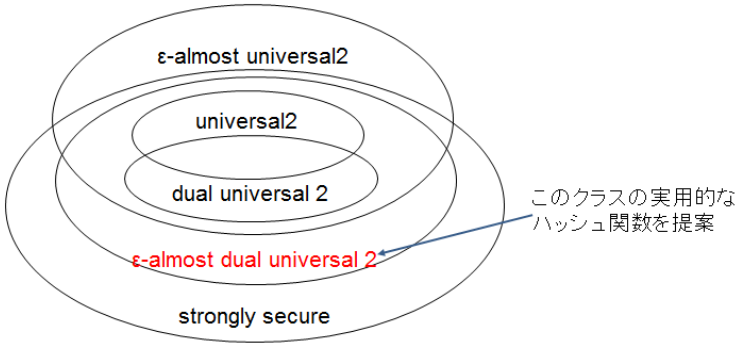
3. 研究開発の成果

①量子鍵配送技術（研究開発目標）



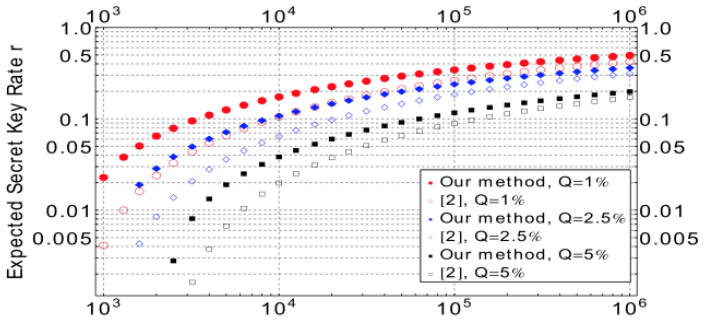
左に記した課題研究はお互いを密に連携させて行われる。これらの成果は最終的には安全性評価基準の策定に用いる（課題イー5）

②課題イー1のH25年度成果



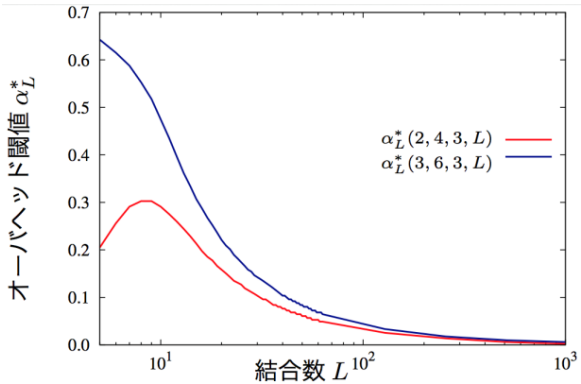
・双対ユニバーサルハッシュ関数の提案
✓　有限長解析を行い、無条件に安全な秘匿性増強をしめした
✓　広いクラスのハッシュ関数が鍵蒸留に使用可能(名大、三菱)

②課題イー1のH25年度成果



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。（東工大）

②課題イー2のH24年度成果

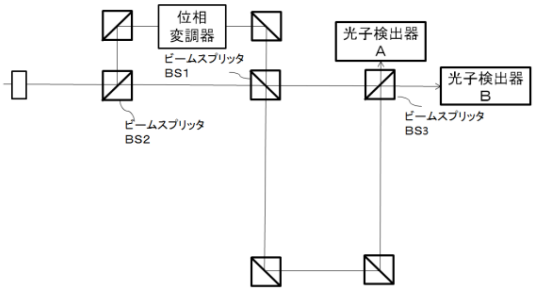


L個のLDPC符号を，結合した誤り訂正符号を考案した．十分大きな結合数Lに対して，考案した符号が，全ての符号化率に対してレートコンパチブルであり，消失通信路のオーバヘッドをゼロにする，つまり通信路容量を達成することを証明した．(東工大)

平成25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

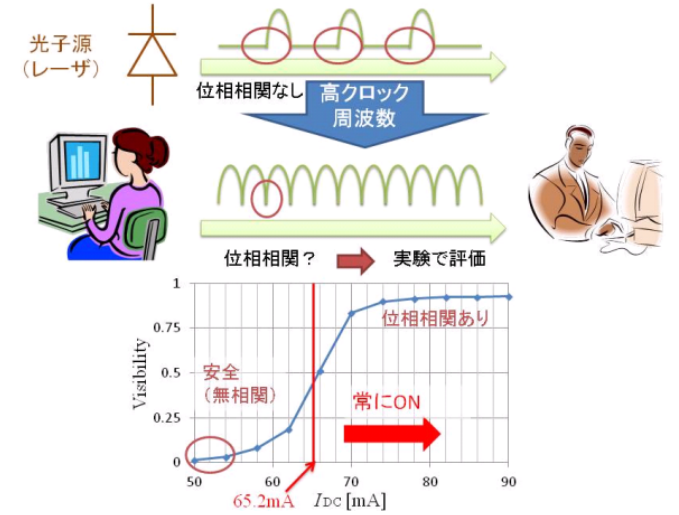
②課題イー3のH25年度成果



安全性理論が実験系に課す大きな要求の一つに、複数の光子検出器の性質の均質性がある。我々は、空間にエンコードされているビット情報を時間情報へ変換することにより、光子検出器の性質の均質性を大きく向上させる提案をした。(NTT)

②課題イー3のH24年度成果

光源のパルス間に位相相関があると効率的な盗聴法があることが知られている



利得スイッチで動作する半導体レーザのパルス間位相相関を測定し，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，クロック周波数10GHz程度までQKD装置に使用可能であることを示した．（北大）

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	7(4)	0 (0)	11(5)	59(35)	0	0(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委託研究チームとNICTの研究者が一同に会し、今後の量子鍵配送システム開発のプラン作りを数回行った。

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
・デコイを用いるBB84方式において，実験グループからの情報をベースに、個々のパラメータが実際のシステムの値である場合において、有限長での鍵生成レートについて数値解析を行う。
・既存のデコイを用いた有限長BB84方式の通信路推定において、改善の余地がある部分を探す。それと同時に、デコイを用いない方式において林・鶴丸らの理論とほぼ同等の 極めて良好な鍵レートを与えるTomamichelらの 安全性証明理論をデコイを用いる方式に拡張できるか否か検討する。
・Squash演算子は、従来型量子暗号の安全性証明における、有用な数学的手法として知られている。2014年度以降の研究では、squash演算子の数学的定義を大幅に拡張し、それが装置無依存量子暗号(DIQKD)の安全性証明に活用できることを示す。
イ―2
・Toeplitz行列を用いたハッシュ関数の場合に、ハッシュ関数を定める乱数が一様でない場合に、秘匿性増強アルゴリズムの性能を評価する。
・高速乱数発生装置を試作し、NIST　SP-800乱数テストを行う.
・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QKDへの適用し，高速な符号器と復号器の実装方法を検討する.
イ―3
・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.
・デュアルバランス変調器を用いた量子暗号送信部を試作し、位相変調の誤差への耐性を実証する。また、パルスごとの光強度の変化、ダブルパルス間の強度比の測定法を確立する。
・課題アと協力して実システムでの出力光強度の変動の測定を行う.
イ―4
・Toeplitz行列を用いたハッシュ関数の場合に、ハッシュ関数を定める乱数が一様でない場合に、秘匿性増強アルゴリズムの性能を評価する。
・Rennerらの安全性解析手法に基づいてB92方式漸近的鍵レートの解析をやりなおし大幅な鍵レートの向上を実現できることを前年度明らかにしたので、漸近論ではなく有限長の場合のB92方式の鍵レートをRennerらの手法に基づいて導出する。
イ―5
・安全性評価基準書を執筆する