平成23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」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

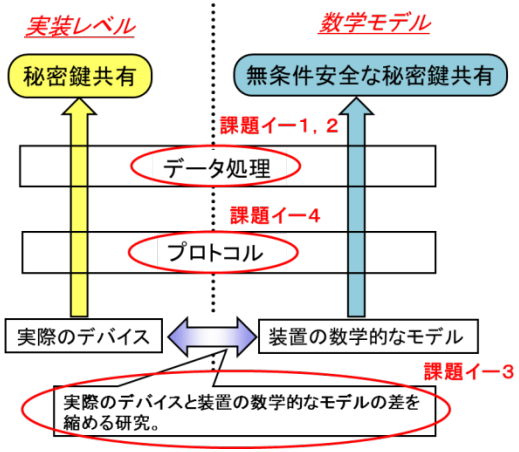
実施機関:　　(株) 日本電信電話株式会社　＜幹事＞、（株） 三菱電機株式会社、国立大学法人　北海道大学、 国立大学法人　東北大学、 国立大学法人　東京工業大学
研究開発期間:　H23年度からH27年度（5年間）
研究開発費:　　総額67百万円　（H23年度　15百万円）

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）

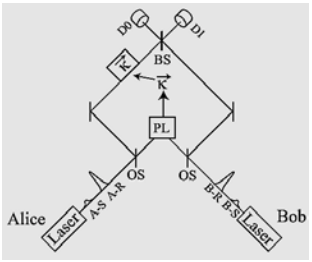
課題イー1、課題イー2のH23年度成果

・より広いクラスの関数を用いて秘匿性増強を行っても安全性が担保できることを示した(Shor-Preskill流の証明方法の枠内). これにより秘匿性増強の高速化が期待できる.

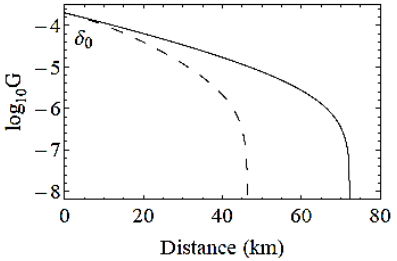
・空間結合符号（LDPC畳み込み符号）や多元LDPC符号を量子鍵配送におけるビットエラー訂正に用いることを検討.

課題イー3、課題イー4のH23年度成果

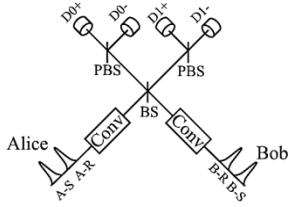
・安全性が検出器の性質に無依存な量子鍵配送方式の新たなプロトコルを2つ提案し、光源の位相エラーなどの現実的なエラーを考慮しても無条件に安全な鍵が生成できることを示した.



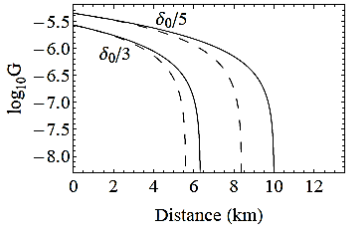
新方式 I



新方式Iの無条件安全な鍵生成率（G）の距離依存性



新方式 II



新方式IIの無条件安全な鍵生成率（G）の距離依存性

・光学系のより詳細なモデル化を行うための前段階として、送信パルス、PLC干渉計，位相変調器の性質をより厳密に測定するための基礎光学系の構築を行った.

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	0	0	2	6	0	1	0

5. 研究成果発表会等の開催について

H23年度は特に開催なし

6. 今後の研究開発計画

課題イ―1、2
- ・エラー訂正符号、秘匿性増強に関しては、更なる高速化及び効率化を目指す
- ・囮状態の推定エラー等を含めたプロトコル全体の有限長効果をより詳細に解析し、鍵生成率の向上を目指す
- ・認証プロトコルを含めた古典通信の高効率化を目指す

課題イ―3
- ・送信機のエラーについてのより詳細な研究を行う
- ・光検出器に対する代表的な攻撃に対しての対策提案を行う

課題イ―4
- ・装置のより詳細な数学モデル化にむけて、装置のテストベンチを構築し、実システムの評価も視野に入れる
- ・乱数の高速生成のための理論提案及び基礎実験を行う