平成27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

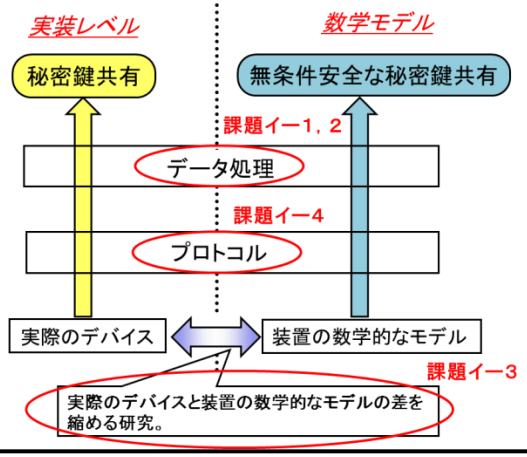
実施機関:　(株) 日本電信電話株式会社　＜幹事＞、（株） 三菱電機株式会社、国立大学法人，北海道大学、国立大学法人，名古屋大学、国立大学法人，東京工業大学
研究開発期間:　H23年度からH27年度（5年間）
研究開発費:　総額61百万円　（H27年度　**10百万円**）

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

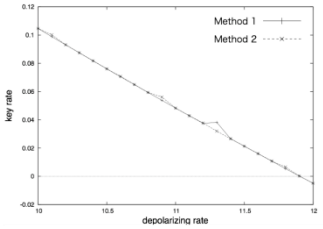
3. 研究開発の成果

①量子鍵配送技術（研究開発目標）



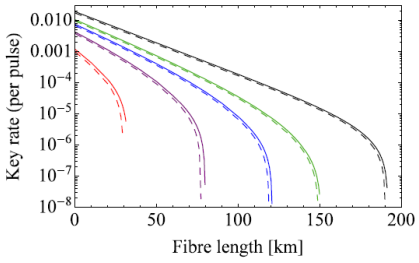
左に記した課題研究はお互いを密に連携させて行われる。これらの成果は最終的には安全性評価基準の策定に用いる（課題イー5）

課題イー1のH27年度成果



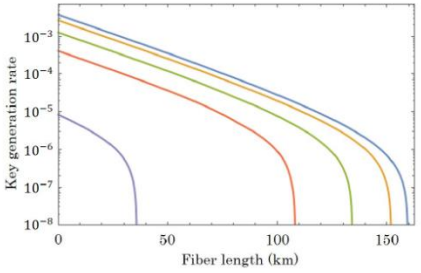
半量子鍵配送プロトコルについて、解析方法を改善して図のような鍵レートを得た。従来8%程度の分極レートでしか秘密鍵を生成出来なかったが11%以上でも秘密鍵生成出来ることを明らかにした。

課題イー1のH27年度成果



位相変調器と強度変調器の雑音による状態準備の不完全性を有限長解析に取り入れ、雑音の度合いに応じて暗号鍵配送可能距離を示した。

課題イー1のH27年度成果



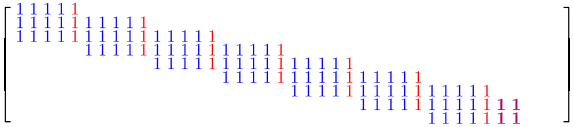
全ての位相変調器と強度変調器には変調精度に限界がある。我々は、この変調精度の有限さを安全性証明に考慮に取り入れ、精度に応じて暗号鍵配送可能距離を示した。

平成27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

課題イー2のH27年度成果

誤り訂正に関して、符号化を高速に行うと同時に、数ビットのエラービットが残ってしまうエラーフロア現象を解決する方法を解決する方法を提案した。図の行列は、エラーフロアの低い高速に符号が可能な空間結合符号のベース行列を表している。空白部分は0を省略している。

$$\hat{B}(3,15,8) =$$

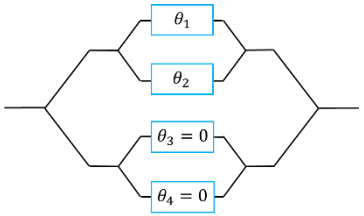


課題イー3のH27年度成果

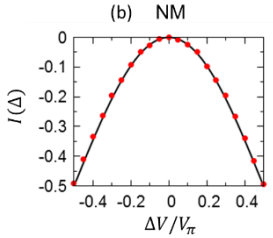
研究開発成果：変調器の出力強度揺らぎを抑制する技術を開発

デコイ法では光強度を正しい値にすることが必要．高速変調ではドライバ帯域が不十分なためパルスパターンによって強度が変動する．

●ネスト型変調器による強度変調を行うことによって，変調器に起因する強度揺らぎをほぼ完全に抑圧することに成功した．



ネスト型変調器の構造図

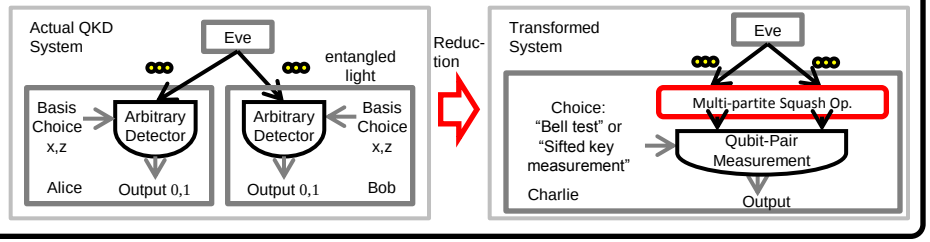


信号電圧に対する出力光強度の依存性

課題イ－1－4のH27年度成果

1．多体スカッシュ演算子を用いた安全性証明手法の研究

2014年度に提案した「多体squash演算子」を、Bennett 1992 (B92)方式、および非可換検出器を用いた装置無依存量子暗号(DIQKD)方式に適用するための検討を実施した。その結果として、DIQKD方式の厳密な安全性証明を得ることに成功した。



4. これまで得られた成果（特許出願や論文発表等）

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース報道	展示会	標準化提案
セキュアフォトニックネットワーク技術の研究開発	8 （ 1 ）	0 （ 0 ）	49 （ 38 ）	91 （ 34 ）	2 （ 2 ）	0 （ 0 ）	0 （ 0 ）

※成果数は累計件数、（ ）内は当該年度の件数です。

（1）

NICT委託研究チームとNICTの研究者間で、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.

（2）

QKDの安全性基準書の第一版を完成させ、QKDを実運用する際に安全性を保証するための基準および、QKDシステムの安定した運用のための指針を与えた. また、本課題の名古屋大のメンバーが日本学術振興会賞及び日本学士院学術奨励賞を受賞した。

5. 研究開発成果の展開・普及等に向けた計画・展望

装置無依存量子暗号（DIQKD）に関する成果は、量子暗号のみならず、（装置無依存な）物理乱数生成器の性能向上にも役立てることができる。また物理乱数生成器は、現代暗号の構成要素としてすでに広く普及している。そこで今後は課題イ-1-4の成果を物理乱数生成器に応用し、さらにそれを現代暗号システムに適用することにより、数年以内の短い期間での社会還元をめざしていきたい。

半量子鍵配送プロトコルは、正規受信者側でZ基底による測定ならびに光の反射しか行わないという点で広く研究ならびに使用されているBB84プロトコルよりも実装が容易になり得るという特徴があるため、この研究成果がBB84プロトコルの代替の一つとして普及する潜在的可能性がある。

LDPC符号の特徴として，復号は原理的に高速に行うことができるが，符号化には多くの計算量が必要であった. これまでのLDPC符号では，符号に構造を持たせることによってエラーフロアを許容することと引き換えに高速化が可能となっていた. 本研究成果により，高性能なLDPC符号である空間結合符号の構造をほとんど変更することなく高速な符号化法を実現することが可能となった. 今後は製品化の可能性を探る。

QKD技術の標準化に向けた検討報告書を製造技術者や想定ユーザに提供し，その評価に対応して内容の改訂を行う. これによって，QKDの安全性を保証するための条件をわかりやすく説明し，安全性保証技術に対する理解を深める. 同時に，安全性保証の基準を定量的に明確化し，評価手法の確立と合わせて，QKD安全性保証技術の標準化を目指す. また、安全性保障に必要な理論も更に発展させる必要がある。

有限長での安全性評価について，上述のように高い評価を得た. 今後，得られた成果を量子暗号に限定せず，より広い範囲での展開の可能性を探ることが，重要であると考える. 事実，我々の成果について，海外の現代暗号の研究者から問い合わせがあったので，このような展開も視野にいれて展開を考えたい.