平成26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

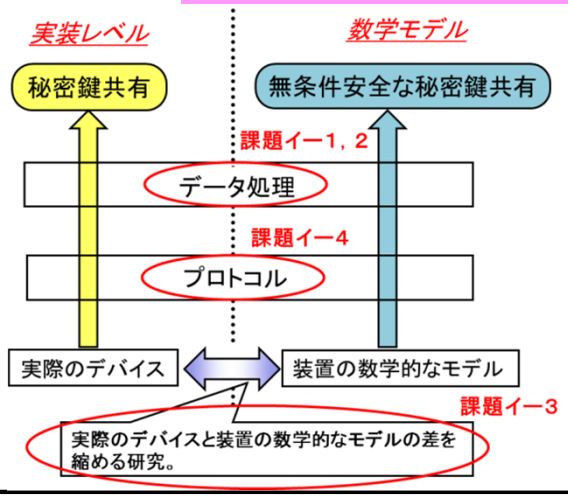
実施機関:　(株) 日本電信電話株式会社　＜幹事＞、（株） 三菱電機株式会社、国立大学法人, 北海道大学、国立大学法人, 名古屋大学、国立大学法人, 東京工業大学
研究開発期間:　H23年度からH27年度（5年間）
研究開発費:　総額61百万円　（H26年度　**8百万円**）

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）

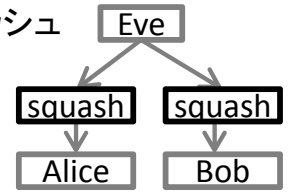


左に記した課題研究はお互いを密に連携させて行われる。これらの成果は最終的には安全性評価基準の策定に用いる（課題イー5）

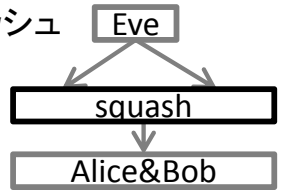
課題イー1のH26年度成果

1．多体スカッシュ演算子の提案とそのDIQKD方式への応用
スカッシュ演算子の手法を多体系に拡張し、装置無依存QKD（DIQKD）の安全性証明のための新たな数学的手法を提案した。この手法により、DIQKD方式の性能（鍵生成率）を、従来論文のものより大幅に向上させることに成功した。

i)従来型スカッシュ演算子の使用例（E91方式）



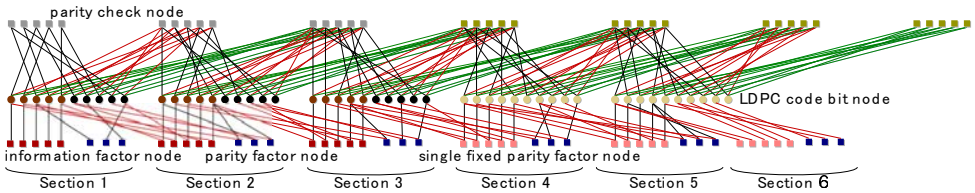
ii)多体スカッシュ演算子の使用例



三菱と学習院（課題ウ）との共同研究

課題イー2のH26年度成果

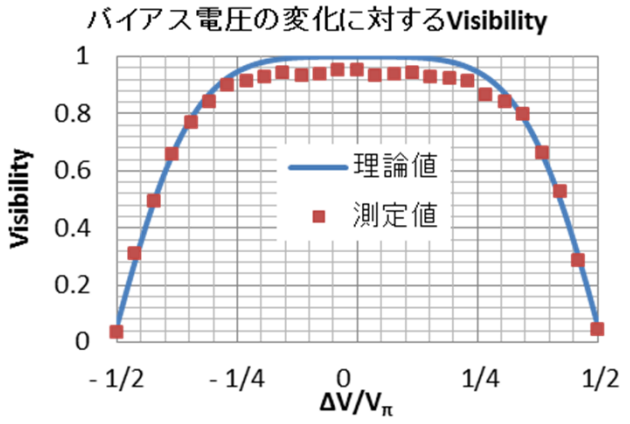
復号アルゴリズムを符号化に利用することで、組織的（エラーのないときには復号処理が不要）でセクション毎にスライド窓復号可能な高速な空間結合符号の符号器と実装方法を考案した。



東工大

課題イー3のH26年度成果

ドライブ電圧の変動に対して安定な変調方式を開発



- 1次の変動の影響を抑圧
- 25%の電圧変動があっても93%の干渉明瞭度（誤り率3.5%以下）を維持

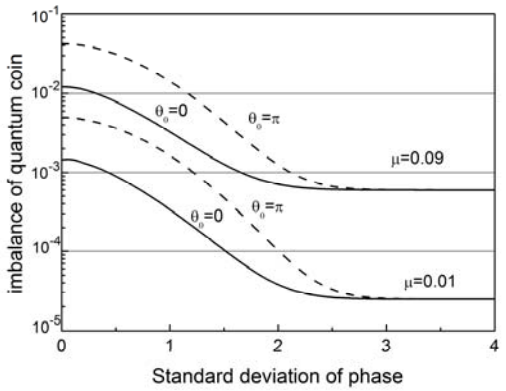
北大

平成26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

課題イー3のH26年度成果

レーザパルスが位相乱雑とみなせる条件を解析

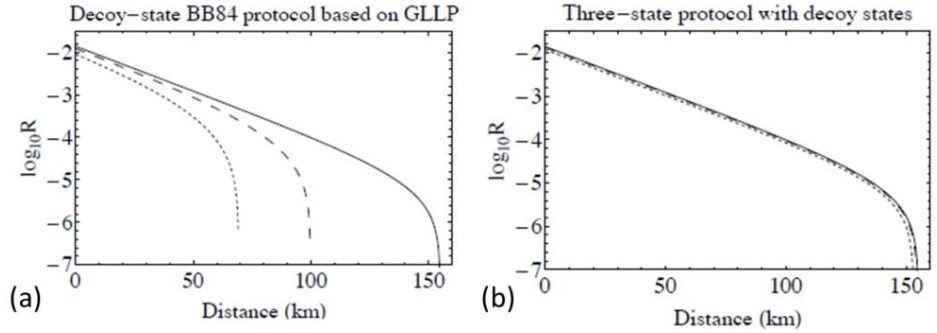


- 位相の確率分布がガウス型であるとした時，標準偏差が2.5程度以上
- 1.25GHzクロックでは利得スイッチ半導体レーザで実現可能
- パルス間干渉のランダム性を実験で確認

北大

課題イー3のH26年度成果

BB84における不完全な状態生成が及ぼす影響を劇的に低減

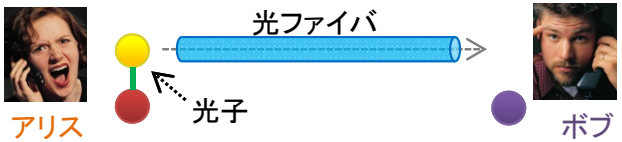


・(a)既存理論 (b)我々の理論
・BB84では3状態のみで十分であることが示された

NTT

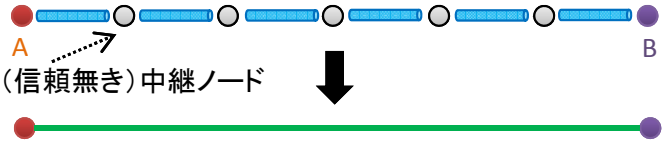
課題イー4のH26年度成果

従来方式:光子の直接伝送



光子損失により通信可能距離に限界

超長距離化技術：量子中継



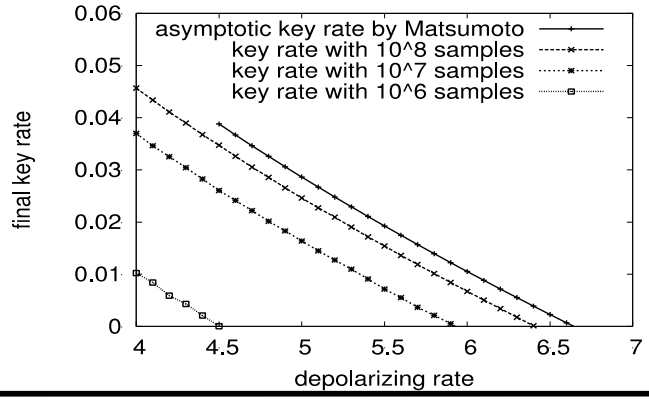
中継ノードを利用し、光子損失からの通信距離限界を打破

物質量子メモリを一切用いず、光学系だけに基づく量子中継方式を構築

NTT

課題イー4のH26年度成果

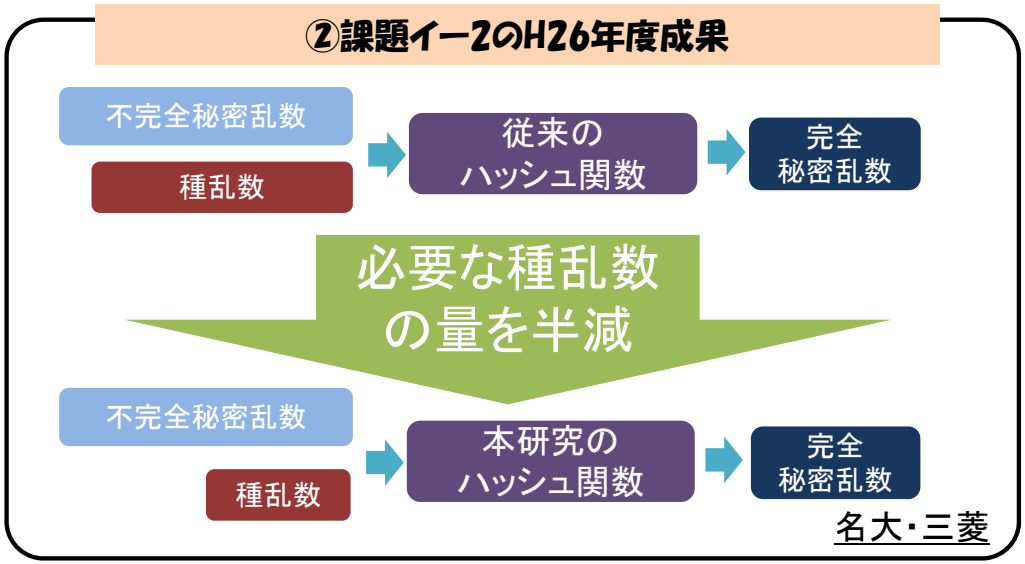
B92プロトコルの送信キュービット数と鍵レートの関係



東工大

平成26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



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(7)	0 (0)	21(10)	101(40)	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. また、安全性評価基準書の執筆に着手し始めた.

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

・・今年度は多体squash演算子の手法を、Ekert 1991 (E91)方式のみに適用し、DIQKD方式の鍵生成率の向上に成功した。今後はこの手法をE91方式以外の様々な方式に適用し、そこでも従来論文を上回る性能を達成することを目指す。

・デコイを用いたBB84方式の効率的パラメータ推定理論:B92プロトコルの鍵レートの導出を改善したRennerらの安全性解析手法(2005)をデコイを用いた有限キュービットの鍵共有プロトコルに適用し、従来の解析手法で得られる鍵レート以上の鍵レートを得る方法を引き続き検討する.

イ―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工学的な研究前年度までに考案した組織的でスライド窓復号可能なレートコンパチブル空間結合符号をCPUまたはGPUに実装する.

・乱数の高速生成のための理論提案及び基礎実験:QKD用乱数発生の実証として高速乱数発生装置のうち光部分のモジュール化を行う.

イ―3

・デバイス評価のためのテストベンチの構築:送信される光の量子状態を測定する方法を開発する.

・QKD実システムでの評価:課題ア、課題エと協力して実システムでのパルスごとの光強度の変化、ダブルパルス間の強度比を測定する.

・より一般的な状態準備の不完全性を取り入れた理論を構築する.

イ―4

・プロトコルの性能向上基礎提案:平成26年度の研究では、与えられた通信路に対してどのようなパラメータが高い鍵レートを与えるか特定に至らなかったので、それを特定する.

・全光量子中継方式は、送受信者を結ぶパス上に存在する中継器だけを利用し、送受信者の量子通信を可能にする。しかしながら、従来のインター ネットがそうであるように、将来の量子通信ネットワークにおいても、送受信者を結ぶ中継器は1つのパス上だけでなく、複数のパス上に存在し得 る。そこで、本年度は、このような2次元的な量子ネットワークを想定し、全光量子ネットワークの可能性を探る。

イ―5

・安全性評価基準書を他の課題と協力し執筆する.