# 研究開発成果概要図 （目標・成果）



## 1. 研究課題・実施機関・研究開発期間

◆課題名　　：セキュアフォトニックネットワーク技術の研究開発
◆個別課題名　：課題イ：量子暗号安全性評価理論
◆副題　　：量子鍵配送実システムの安全性と安定性の向上及び高速化
◆実施機関　　：日本電信電話株式会社、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：平成23年度～平成27年度（5年間）

## 2. 研究開発の目標

安全強度が高く、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

研究開発目標

### ①データ処理アルゴリズムの研究（1）

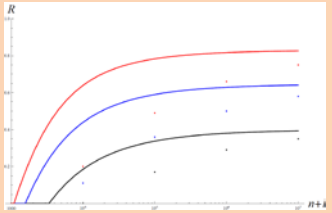
量子鍵配送装置の安全性確保しつつ鍵生成率の高速化を行うためには、装置が行うデータ処理方法を改良する必要がある。更に、データ処理には、装置の不完全性の影響を考慮する必要がある。

課題イ-1　有限長解析の研究

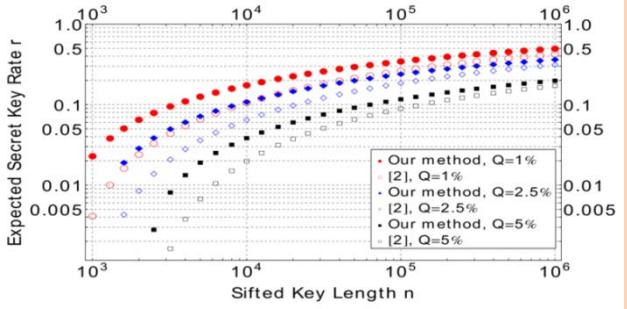
量子鍵配送装置から得られたデータから、高効率で暗号鍵を生成するためには、送信パルス数が有限であることを考慮した高効率なデータ処理アルゴリズムを開発する必要がある。

研究開発成果

有限長理論の改良



・単一光子を用いたBB84プロトコルに対する厳密な有限長解析
・送信者と受信者が、プロトコル実行毎に最適な鍵生成レートを適応的に算出することを特徴する
・ふるい鍵長が短い（$10^6$ビット）場合でも漸近的な鍵生成率（≒理論的限界）の90% 以上が達成可能




上記の結果の更なる改良

研究開発目標

## ①データ処理アルゴリズムの研究（２）

量子鍵配送装置の安全性確保しつつ鍵生成率の高速化を行うためには、装置が行うデータ処理方法を改良する必要がある。更に、データ処理には、装置の不完全性の影響を考慮する必要がある。

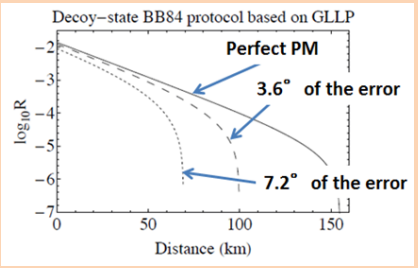
課題イ-3　サイドチャンネルの特定及び対策

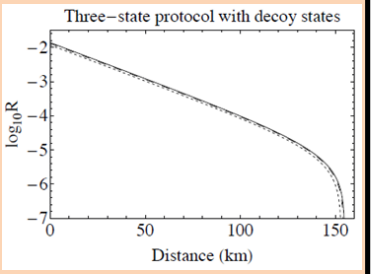
実際のQKD装置の構成部品の性質 ⇔ 安全性理論が仮定するQKD装置の構成部品の性質

装置の雑音、不完全性、サイドチャネルが原因で、安全性証明はそのままでは実際のQKD装置には適用できない。従って、安全性証明を発展・改良する必要がある

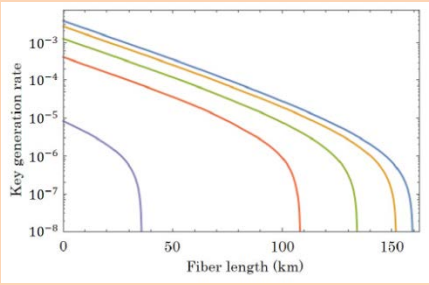
研究開発成果

### 位相変調エラーの影響を劇的に低減

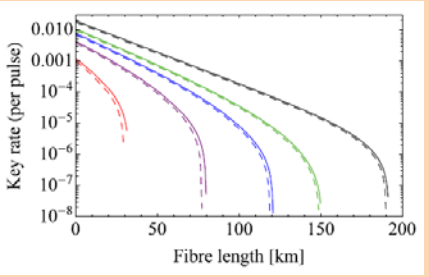



### 状態準備の精度の緩和




### 位相変調エラーを取り入れた有限長理論



研究開発成果

## ①データ処理アルゴリズムの研究（3）

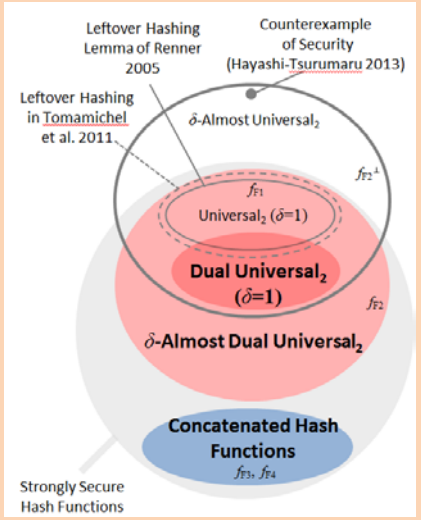
研究開発目標

量子鍵配送装置の安全性確保しつつ鍵生成率の高速化を行うためには、装置が行うデータ処理方法を改良する必要がある。更に、データ処理には、装置の不完全性の影響を考慮する必要がある。

課題イ-2 鍵蒸留処理アルゴリズムの高速化及び簡素化

量子鍵配送の高速化のためには、エラー訂正と秘匿性増強を高効率のものに置き換える必要がある。更に、性能を劣化させずに安価な装置での実装を行い、簡素化を目指す。

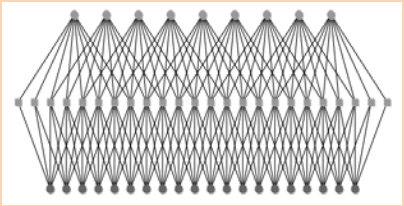
秘匿性増強で用いる関数クラスの拡大とシード乱数量と質の低減




FPGAに比べて安価なGPU上での誤り訂正の実装

課題ウで開発した実機で運用

レートコンパチブルで高速符号化可能な空間結合符号の開発



研究開発目標

## ①サイドチャンネルの特定及び対策（実験的研究）

量子鍵配送装置の安全性確保しつつ鍵生成率の高速化を行うためには、装置が行うデータ処理方法を改良する必要がある。更に、データ処理には、装置の不完全性の影響を考慮する必要がある。

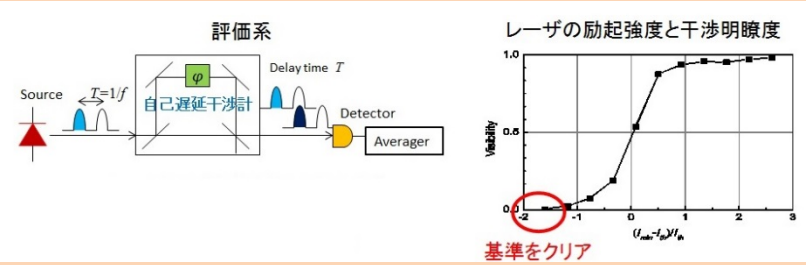
課題イ-3　サイドチャンネルの特定及び対策（実験的研究）

実際のQKD装置の構成部品の性質 ⇔ 安全性理論が仮定するQKD装置の構成部品の性質

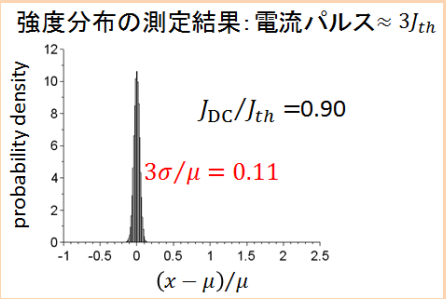
装置の雑音、不完全性、サイドチャネルが原因で、安全性証明はそのままでは実際のQKD装置には適用できない。従って、理論が適用できるようにするために、実際の装置のより詳細な特徴づけや必要とあれば新たな実験装置を提案する必要がある。更に理論が適用できるような装置パラメータを実験的に見出す必要がある。

研究開発成果

今後のひな形となる定量的な安全性保証基準設定と評価系の構築



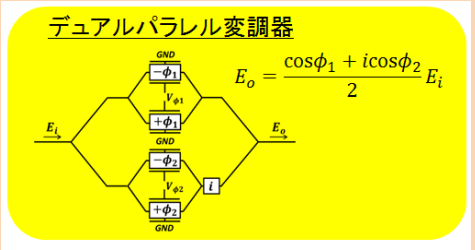

利得スイッチLDの強度揺らぎ評価

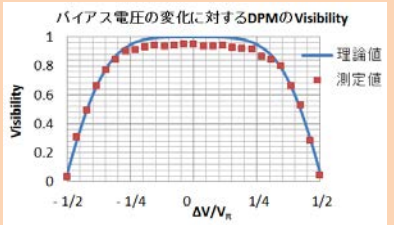



その他の不完全性対策

- テストポイントでの監視機能
- ダークカウントのモニタ
  自動バイアス制御
- 光子検出率制御
（検出率・ダークカウント均等化）
・ トロイの木馬対策

エラーを低減する装置提案



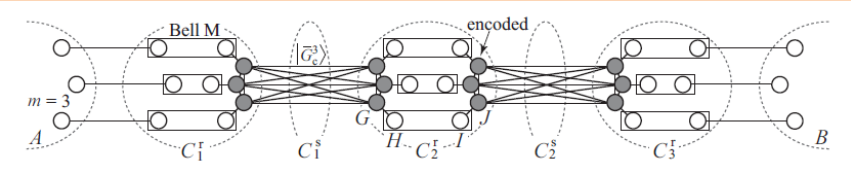
## ①量子鍵配送の多様化へ向けた研究（課題イ-4）

研究開発目標

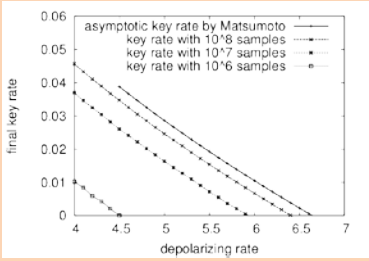
量子鍵配送以外の量子通信の研究を行い、量子通信の多様性を広げることが目標である。特に、現在の量子鍵配送の通信距離はおよそ300km程が限界であり、これ以上の距離の量子通信には量子中継が必要であるが、量子中継には実現が非常に困難な物質量子メモリーが必要であった。
　更に、単一光子B92の有限長安全性解析を行い、BB84型以外のプロトコルがもつ可能性を探った

研究開発成果

物質量子メモリーを使わない、高効率な全光量子中継方式を提案




凸最適化によるB92プロトコルの有限長鍵レートの解明




## ①安全性評価基準の策定（課題イ-5）

研究開発目標

実際の量子鍵配送装置が、どのような基準で安全であるかの基準があいまいであり、また量子鍵配送のユーザ向けの説明や運用方法をまとめた文書がなかった。これは量子鍵配送の実運用ユーザ獲得に向けて大きな障害の1つである。そこで、これらの内容を盛り込んだ安全性評価基準書を作る必要があった。

研究開発成果

安全性評価基準書の第一版を作成した

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<br>（ 1 ） | 0<br>（ 0 ） | 47<br>（ 36 ） | 88<br>（ 31 ） | 2<br>（ 2 ） | 0<br>（ 0 ） | 0<br>（ 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。