プログラム名： 量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現
PM 名：山本 喜久
プロジェクト名：量子セキュアネットワーク

委 託 研 究 開 発

実 施 状 況 報 告 書（成果）

平成２７年度

研究開発課題名：

量子鍵配送デバイス安全性評価技術の研究開発

研究開発機関名：

国立大学法人　北海道大学

研究開発責任者
富田　章久

Ⅰ　当該年度における計画と成果

１．当該年度の担当研究開発課題の目標と計画

1. 安全性評価基準のドキュメントの改訂.
   安全性評価基準のドキュメントを関係する他の研究機関と共同して継続的な更新を行う.
2. Decoy-BB84 方式における送信状態の評価と改善手法の検討.
   Decoy-BB84 方式における送信状態を評価し，理想状態からのずれ・揺らぎを定量的に求める.
3. 鍵蒸留のための統計処理の検討.
   理想状態からのずれ・揺らぎの鍵蒸留に対する影響を統計的に推定する手法を検討する.
4. 量子通信のテスト用システム開発
   量子通信のテストに用いるシステムのプロトタイプの製作を行う.
5. 新原理ＱＫＤ実装法検討として，RR-QKD の原理実証のための実験方法の検討
   RR-QKD の原理実証のための実験構成を考案する

２．当該年度の担当研究開発課題の進捗状況と成果

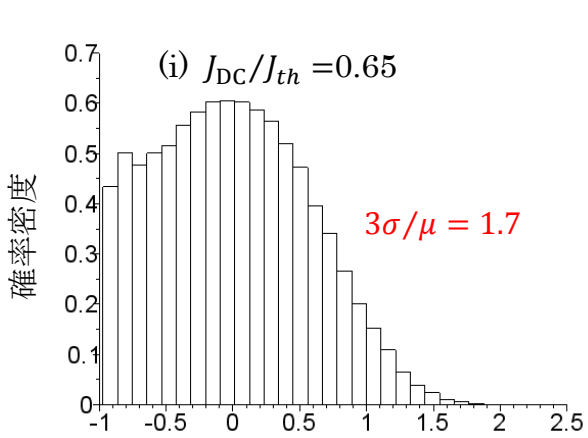
2-1 進捗状況

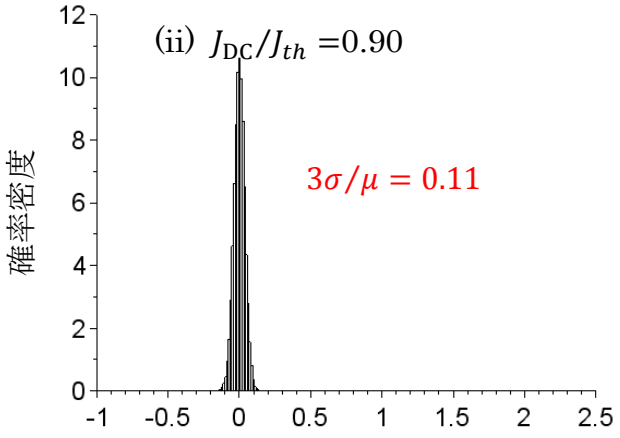
1. 安全性評価基準のドキュメントの改訂.
   安全性評価基準ドキュメントのうち，装置の実験的な安全性保証法を担当している．防衛省における説明会の反応などから，理論的な背景には深入りせず，実際の装置に即した測定方法を記載するマニュアル的なドキュメントの作成を行った.
2. Decoy-BB84 方式における送信状態の評価と改善手法の検討.
   今年度は送信パルスの強度変化に注目し，変動の要因分析と変動の低減手法の提案と実証を行い，光強度変化の問題は解決した.
3. 鍵蒸留のための統計処理の検討
   2 に関連して，有限長の安全性理論を強度変化の影響を取り入れるように拡張した.
4. 量子通信のテスト用システム開発
   QKD 送信機および受信機の量子通信部分のうち，送信状態の評価に必要な部分−光源，送信側干渉計，状態変調器，強度変調器と受信部の干渉計−を抜き出した評価用実験系を構築した.
5. RR-QKD のメカニズムについて検討を行い，より簡略化したプロトコルでも同様の原理に基づいた QKD の可能性があることを指摘した.

2-2 成果

<u>Decoy-BB84 方式における送信状態の評価と改善手法の検討</u>.

- 送信パルスの強度変化にはレーザの強度揺らぎと強度変調器への入力電圧の変動の 2 つの要因があることを示した.
  (a) レーザ強度揺らぎについては利得スイッチレーザの強度変動シミュレーションから動的な不安定現象を見出し，動作条件の最適化によって変動が抑制されることを示した.



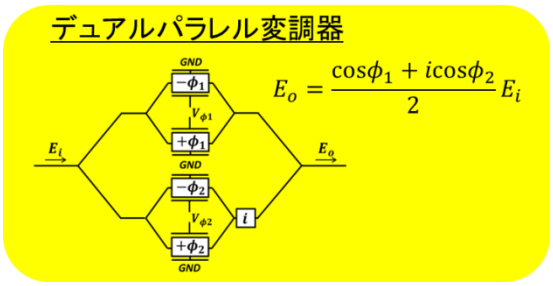


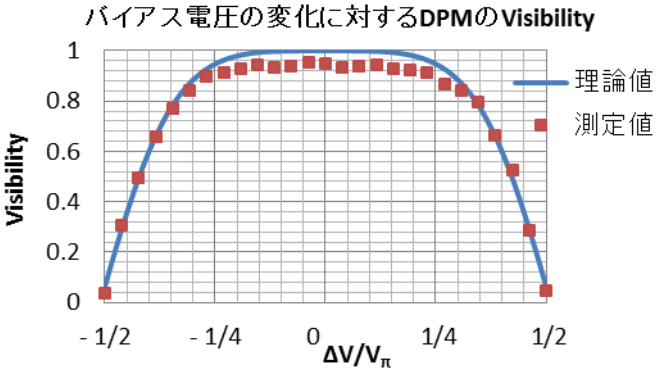
(i)利得スイッチレーザの発振不安定性による揺らぎの増大　(ii)バイアス電流の増加による不安定性の抑制

(b) 強度変調器への入力電圧の変動については，電圧の変動に対して出力光強度の変動が小さい変調法（ネスト型変調器を利用）を提案し，動作の実証を行った．

(c) 送信パルスの光強度変動の影響を見積もるため，C.W. Lim, et al., Phys. Rev. A 89, 022307(2014)が与えた有限長の安全性理論を強度揺らぎを含むように拡張した．

- BB84 に用いる光子状態のずれに関して，変調器の入力信号の揺らぎに対してずれの小さな変調法（デュアルドライブ変調器を利用）を提案し，原理実証を行った．





2-3 新たな課題など

デバイス不完全性により，状態が理想からずれた場合の影響について定量的な評価理論を実験に則して構築する必要がある

3．アウトリーチ活動報告

nano tech 2016 ロボティック・シンポジウムにて講演を行った