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２８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最新の実験的・理論的成果をもとに関係する他の研究機関と共同して継続的に更新する.

2.　デバイス評価技術

・トモグラフィにより，送信光パルスの状態計測を行う：ネスト型変調器の利用による送信光パルスの状態改善効果を理想状態とのフィデリティによって定量的に評価する.

・デバイス不完全性の定量的な評価理論を実験に則して構築する：デバイス不完全性による，状態識別可能性と安全性の関係を定量的に評価する

・新たなデコイ・状態生成方式を開発する：変調器への入力電圧への依存性が小さく，同時に装置構成が簡略化可能なデコイ・状態生成方式を開発する

・受信データの処理方法について検討する

・オンサイト評価技術，テストシステム開発：NEC が開発している QKD 装置の送信状態評価として QKD 装置の送信光強度揺らぎを測定・評価し，安全性を確認する（NICT・NEC と共同）

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

安全性評価基準のドキュメントの改訂をNICT，NTTと共同で進めた．QKD 装置に関する部分を主に担当した.

2. デバイス評価技術

・送信光パルスの状態計測：

デュアルパラレル型変調器の利用による送信光パルスの状態改善効果を示すためにフィデリティを実験から推定し，印加電圧のずれがあった時の最終鍵レートを計算した.

・デバイス不完全性の定量的な評価理論：デバイス不完全性によって状態識別可能性が起きる例として，利得スイッチ半導体レーザの位相乱雑性を取り上げた．位相乱雑性を理論的に検討するために自然放出雑音を考慮したモデルを構築し，シミュレーションを行っている.

・新たなデコイ・状態生成方式：デュアルパラレル変調器を利用した状態生成方式に加え，ネスト型変調器を用いた強度揺らぎの小さなデコイ生成方式の詳細な評価を行った.

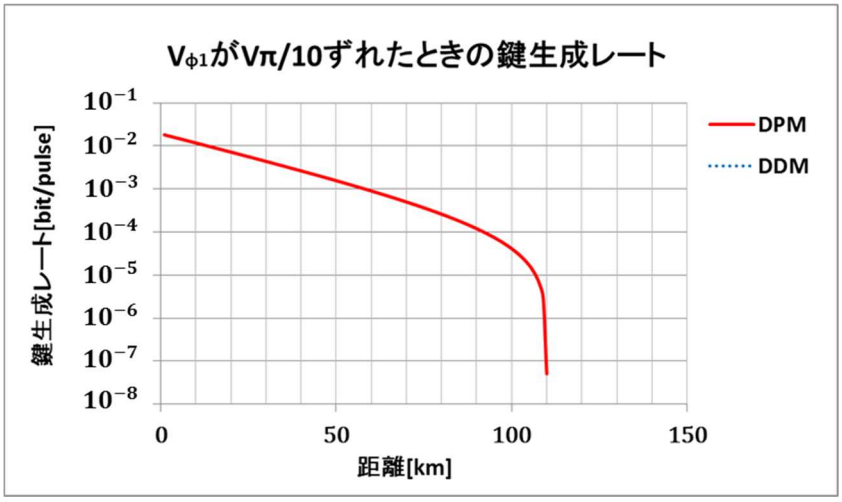
また，強い参照光を用いたB92プロトコルでは盗聴者の測定が完全でないことから盗聴情報量に上限がある．このことを利用したQKDの安全性の検討を進めた．受信再送攻撃，ビームスプリッタ攻撃に加え，ガウシアンクローナーによる攻撃を考えたところ，受信再送攻撃が最も強力であることが分かった.

・受信データの処理方法，オンサイト評価技術：光強度の揺らぎを考慮して犠牲ビットを求める方法を開発し，それに基づいてシミュレーションを行ったところ，装置パラメータの最適化によって鍵生成レート，伝送距離が改善されることを見出した.

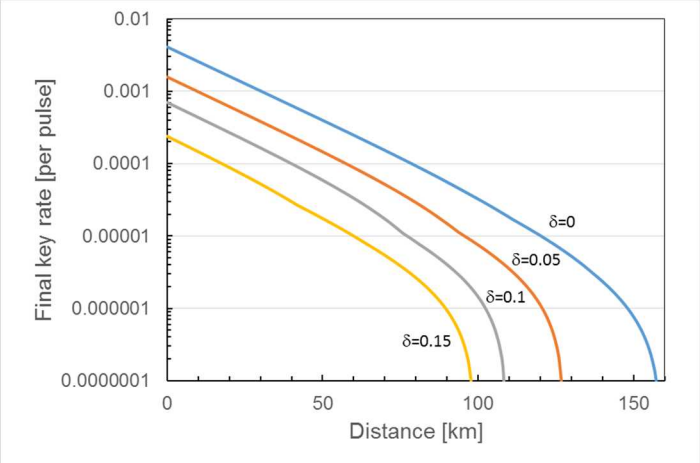
また，NEC，NICT と共同で装置の強度揺らぎを評価し，さらに東大とも共同してソフトウェア的に強度揺らぎの影響を低減する方法を開発した．

2-2 成果

・デュアルパラレル型変調器の利用による印加電圧揺らぎの変動に強い状態生成方法の評価を進めた．実験データから推定されるフィデリティに基づいて，伝送誤り率を推定し，最終鍵レートを計算した．シミュレーション結果によると電圧が 10%程度ずれても デュアルパラレル型変調器を用いると伝送距離が 100km 以上でも鍵生成が可能なことが示された．一方，従来のデュアルドライブ型変調器でこのようなずれがあると鍵生成はできなくなる．



・相関がない強度揺らぎを考慮した犠牲ビットの計算を行った．平均光子数の揺らぎの大きさを・=0,0.05,0.1,0.15 としたときの最終鍵生成レートを下図に示す．ただし，揺らぎの大きさは$\delta = (\mu_k^+ - \mu_k)/\mu_k = (\mu_k - \mu_k^+)/\mu_k$と定義した．簡単のため・は平均光子数によらないものとした．平均光子数の揺らぎは生成レートに大きな影響を及ぼすことがわかる．最適化によって揺らぎが 15%あっても・・・km 程度の鍵生成距離が実現されるが，レートは揺らぎがないときの 4%程度となる．揺らぎが大きくなるにつれて，2 つの基底選択率を等しくし，デコイの平均光子数を小さくすることが必要になることがわかった．



平均光子数揺らぎがあるときの最終鍵生成レートの伝送距離依存性

・実際の装置での光強度を評価し，送信強度選択のパターンに依存した強度のずれが起きることを NEC，NICTと共同で見出した．強度がパターンに依存する(相関を持つ)ため，送信パルスの推定が可能になりうることが東大によって指摘された．強度揺らぎの定量評価と発生原因の検討を行い、強度変調器への配線帯域不足に伴う電気信号の歪みに由来することを明らかにした．この新たなサイドチャネルに対し、NEC，北大、東大グループと協力し揺らぎ・ヒステリシスが有る装置からの安全な鍵生成方法を提案した．この方法を用いればパルス強度の独立性が回復するので上に述べた従来の安全性理論によって鍵生成レートを計算しても問題は起きない．

2-3 新たな課題など

今回の解析は平均光子数の揺らぎはある範囲内にあり，それより大きなずれはないものと仮定している．このことは一般には保証されない．そのため，例えば送信機に強度モニタを設けて各パルスの強度を測定し，基準以上にずれたパルスは基底照合の段階で捨ててしまうといったモニタ機能を装置に実装する必要が生じる．ただし，この方法は高速な検出器を必要とするものの，基準から外れたパルスの位置を記録するだけなので必要なメモリの量や鍵蒸留における古典通信量に与えるインパクトは小さいものと考えられる．

3．アウトリーチ活動報告

特になし