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２９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

量子鍵配送に必要な条件としてシステムの安全性基準を明確化し，これに則してデバイスの特性を実験的に評価する方法を開発するという研究課題達成のため，今年度は以下の目標を定め，研究を行った.

(1)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：

(a)光パルス中の光子数分布のうち，デコイ法に必要な 0 光子，1 光子，2 光子以上の確率を定量的に評価する.

(b)光パルス中の光子数が 0 光子，1 光子，2 光子以上となる確率が任意に与えられたときのデコイ法による犠牲ビットの算定法を得る.

(c)装置に組み込みが可能な乱数生成装置への応用を念頭においた利得スイッチ半導体レーザのダイナミクスのシミュレーションを行い，位相乱雑なパルスを安定して得られる条件を明らかにする.

(d)強い参照光によって偏光制御を行った場合に可能な盗聴とそれによる情報の利得を求める.

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については新たな知見を取り入れて担当部分を改訂した.

(2a) 光子数分布を 2 つの光子検出器で推定するため，ビームスプリッタの分岐比を変えて同時計数を測定する方法を考案した.

(2b) 光子数分布がポワソンでない場合のデコイ法による犠牲ビット算定法を求めた．さらに，光子数分布を制御する方法として，BBM92 プロトコルにおいて 2 光子パルスを含む確率を低減するプロトコルを提案した.このプロトコルに上記の犠牲ビット算定法を適用し,性能のシミュレーションを行った.

(2c) 利得スイッチ半導体レーザのダイナミクスのレート方程式によるシミュレーションを行い,励起強度と光パルス強度揺らぎの関係を検討し，実験データと比較した.

(2d) 強い参照光を盗聴者が自由に制御できるとき,受信機の位相変調器のもつ偏波依存性を利用すると受信者の基底選択を無効にできる（常に同じ基底で光子検出させる）ことを示した．これにより，盗聴者と受信者の測定結果を常に一致させることが可能になり，有効な盗聴となる．このことは偏波依存性がある受信機を用いる場合，偏波変動の補正を強い参照光で行えないことを示している.

(2e) 位相変調器に印加する制御電圧がジッタなどの影響で変動する場合，状態生成エラーがおき，生成される鍵レートが小さくなる．これに対して，デュアルパラレル変調器を用いることで制御電圧が変動しても状態生成エラーを小さくできることを提案した．さらに，状態トモグラフィを行って状態の密度行列を推定してデュアルパラレル変調器の効果を実証した.

(2f) 強度変調器に印加する制御電圧がジッタなどの影響で変動する場合,強度が設定値からずれる現象が観測された．強度のずれは信号のパターン（シグナル，デコイ，真空）によって変動する，相関を

持った変動であることが明らかになった．このことは従来の安全性理論の仮定が満たされなくなり，安全性保証ができなくなることを示している．この問題に対して，相関を消去するために decoy sift 法を提案した．さらに，理論グループとの協力によって安全性が保証できることを明らかにした．

2-2 成果　（主要な成果なもの 2 点）

- **2 光子パルスを含む確率を低減する BBM92 を改良したプロトコルの提案**

提案するプロトコルの実装は図 1 の通り従来の BBM92 とほぼ同じである．ただし，光子対源は送信（Alice）側にある．提案するプロトコルでは，Alice の光子検出器のどちらか一方が光子を検出した時のみを鍵生成に用いる．つまり，光子検出なし（真空），2 重検出（2 光子以上）の状態が鍵生成に用いられる確率を低減できる．デコイ法による鍵生成レートの推定にあたり，ポアソン分布以外の光子数分布にも適用できるように Lim らが提案している方法を拡張した．シミュレーションの結果，図 2 のように同条件の BB84 プロトコルに対して鍵生成レート，最大伝送距離のいずれも改善された．

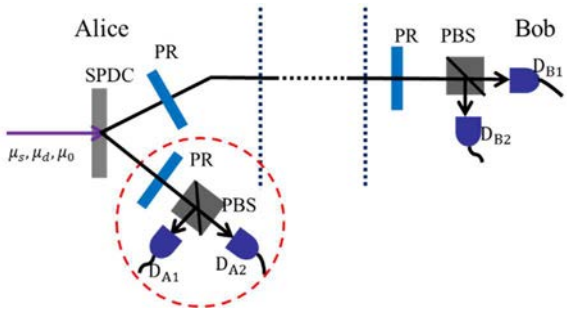

図 1　提案したプロトコル実装の原理図

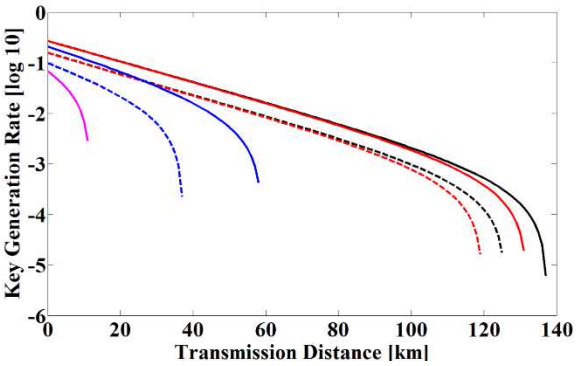

図 2　シミュレーション結果．実線は提案プロトコル，破線は BB84．色は符号長の違い

- **デュアルパラレル変調器による状態生成エラーの低減**

状態トモグラフィによって密度行列を実験的に推定し，鍵生成レートのシミュレーションを行った．印加する制御電圧が 10%変動しても鍵生成レートはほとんど影響を受けないことが示された．

2-3 新たな課題など

(2a) 今回考案した方法を実際に適用するため，所要の推定精度（これ自体安全性保証の要求から決定する）を得るためのサンプル数，分岐比の数をシミュレーションにより決定する必要がある．

(2b) 新たに提案したプロトコルを実証するために，最適な光子数をシミュレーションで求める．また，高効率の 2 波長エンタングル光子対源を開発する必要がある．

(2c) 励起強度について，位相乱雑性と強度の安定性にトレードオフがあることが分かったので，半導体レーザ単体で両立可能か，あるいは新しいデバイスを導入する必要があるかを見極める．

(2e) 最近報告された理論では位相のずれの範囲を限定する必要がある．現在の状態評価の精度を向上させ，測定値のばらつきの影響を減らして，高い信頼度で範囲を限定する方法を開発する必要がある．

3．アウトリーチ活動報告

特に無し