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：

新世代量子セキュリティ技術の研究開発

研究開発機関名：

東京大学

研究開発責任者
小芦 雅斗

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

従来の量子鍵配送とは異なる動作原理に基づく RRDPS 方式においても、通常の量子鍵配送方式と同様に、現実的な光子検出器が到着した光子数を見分けられない（閾値型検出器）という性質をセキュリティ理論に組み込む必要がある。同時検出数の「監視」による手法を前年度に確立したが、RRDPS 本来の長所に沿った監視によらない対処法に基づくセキュリティ理論を構築する。

RRDPS 方式で能動的な遅延路の切り替えを実装する場合、一般に、切り替え速度と損失の間にトレードオフ関係が生じる。そこで、干渉計の遅延の切り替えをパルス列のブロック毎に行えない状況において、秘密鍵を生成するためのセキュリティ理論を構築し、鍵生成レートの切り替え速度依存性を定量的に明らかにする。とくに、受信側の光子検出レートと同程度まで切り替え速度を落とした場合でも秘密鍵の生成を可能にすることを目指す。

RRDPS 方式あるいは密接に関連した方式の様々な実装法の開拓に着手する。とくに、位相変調を２値から４値にした方式について、ハードウェアの簡略化の可能性を念頭に置いて、性能の検討を行う。

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

RRDPS 方式における、監視によらない閾値型検出器の対処法、および、干渉計の遅延の切り替え速度の一般化について、予定通り理論を構築した。とくに、後者については、従来型の量子鍵配送も含めた一般的な形で、測定装置のパラメーター（基底の選択等）の切り替えを遅くできる場合を明らかにする理論に拡張できる可能性が拓けたため、一般的な条件の定式化を引き続き行っている。

RRDPS 方式に関連した方式として、従来型の擾乱監視を併用した場合のセキュリティ理論を構築した。また、遅延切り替えを行わず、位相変調を２値から４値にした方式について、セキュリティ理論を構築した。この方式は、DQPS 方式として従来知られているものにブロック長の概念を導入したものに相当する。この方式のセキュリティ理論が未解決であった背景には、２光子以上を光源が放出した事象に原理的にタグをつけるという汎用的な証明技法(Gottesman らに依る)が適用できない点にあった。今回は、受信者の測定が終了した後で事後的にタグをつけられる点に着目し、事後的であることから生じる問題点を解決することでセキュリティの証明に成功した。さらに、この方式の有限鍵長のセキュリティ理論の構築に取り組んだが、その際、従来の BB84 方式の有限鍵長の議論に冗長な部分があることを見出し、簡潔で汎用性の高い証明技法の提案に結びつけた。

当該年度中に、本プログラムにおけるデコイ BB84 方式の実装で、パルス信号強度の揺らぎが直前のパルス強度と相関を持つ現象が NICT、NEC 社、北大により明らかとなった。その対処法に関して綿密な意見交換を行った。一般に、鍵生成速度を高めるためには、パルスの繰り返し速度を上げるのが効果的であるが、その際に上記のような相関の問題は常に発生すると考えられる。従って、この問題は、デコイ BB84 方式に限らず、様々な量子鍵配送方式に共通の課題であると言える。その重要性に鑑みて、継続してセキュリティ理論の構築を進めることとした。

2-2 成果

受動的な遅延切り替えと閾値型検出器を用いた RRDPS 方式では、多重検出を監視して鍵長を調整することをせずとも、安全な最終鍵が得られることを証明し、その鍵長を与える公式を導いた。実際上は、多くの場合に監視による方法のほうが優れていることが明らかになった。

RRDPS 方式がもともと想定していた、ブロック毎に受信装置の干渉計の遅延量を切り替えるという要求を緩和し、はるかに遅い切り替えを行う場合についてのセキュリティ理論を構築し、受信側の光子検出レートと同程度まで切り替え速度を落とした場合でも、秘密鍵の生成が可能であることがわかった。

RRDPS 方式に従来型の擾乱監視を併用した場合のセキュリティ理論を構築し、漸近的な鍵生成レートの公式を導いた。ブロック長が 6 程度までの短い場合には、擾乱監視を加えることで鍵生成レートが大きく向上することが判明した。ブロック長が大きい場合には、擾乱監視を加えても鍵生成レートの向上はほとんど見られず、RRDPS 方式が鍵を生成する能力は新原理によるものが支配的であることを明らかにした。

DQPS 方式にブロック長の概念を導入した方式のセキュリティ理論を構築し、漸近的な鍵生成レートの公式を導いた。２重パルスの位相差を用いる BB84 方式の実装と比較して、ほぼ同じハードウェアを用いながら、約３倍に近い鍵生成レートが得られることを明らかにした。

従来の BB84 方式の有限鍵長の議論においては、誤り率の推定に単純無作為抽出の理論を用いることが慣例であったが、ベルヌーイ抽出の理論を用いることで証明が簡潔になり、得られる鍵長も改善することを明らかにした。同じ理論を用いて DQPS 方式の有限鍵長の鍵生成レートを導出し、有限鍵長の場合でも２重パルスの位相差を用いる BB84 方式に対する優位性が保たれることを見出した。

NICT、NEC 社、北大との協力により、揺らぎに相関が有る装置から効率よく鍵を生成する手法の提案を行った。

2-3 新たな課題など

光源の揺らぎに相関がある場合のセキュリティ理論については、より一般的な場合に対する処方箋を確立することが求められる。そのような方向性の報告も近年見られるが、光パルスへの攻撃の順番について、現実的な仮定のもとで成立する理論はまだ完成されていない。また、RRDPS 方式は光源の不完全性についての耐性が高いことが期待されるため、従来方式との比較検討も重要である。

３．アウトリーチ活動報告

平成２９年２月２２日に、青山学院中等部にて、「光の正体と究極の暗号」と題した出張講義を行った。小芦雅斗、佐々木寿彦、鈴木泰成の 3 名で担当し、対象者は、同校三年生 26 名。偏光板とレーザーポインタを用いた実演と体験を交えながら、波としての光の性質、特に偏光について理解を深められるようにした。続いて、粒子としての光の性質、量子力学の簡単な導入、量子コンピュータ、微弱な光を利用した解読不可能な暗号である量子暗号について解説し、ImPACT の活動について紹介した。