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：

適応的物理レイヤ暗号の符号化技術の研究開発

研究開発機関名：

東京工業大学

研究開発責任者
松本隆太郎

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

本研究課題は、光空間通信を用いた秘密鍵配送方式を実現することである。当該年度は、盗聴通信路符号化を用いて秘密鍵配送を行う方式の開発を目指し、光空間通信路の統計的モデルとしてポアソン分布・対数正規分布・ガウス分布を想定し、それらの通信路に対応できる符号化方式の開発を目標としている。その目標を実現するために、（1）研究責任者松本が本プロジェクトに先立って明らかにした、誤り訂正機能と情報漏洩防止機能に分離して盗聴通信路符号化法を設計する理論を上記の光通信路の統計モデルのどれか一つに対応出来るように拡張することと、（2）それら統計モデルのどれか一つで適切に動作する誤り訂正符号化方法を開発することを目標としている。

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

上記（1）に関して、前述の本プロジェクトに先立って開発した分離設計理論の正当性を保証する数学的証明を精査し、通信路の条件付き確率が確率密度を有する場合について正当性を保証出来るように議論を拡張した。通信路の統計モデルとして想定していたポアソン分布・対数正規分布・ガウス分布はどれも確率密度を有するため、これらの統計モデルについて分離設計理論を拡張出来たことになる。

（2）については，ガウス分布を想定した誤り訂正符号の汎用 CPU で動作する符号器と復号器を開発した．従来問題となっていた符号構造を原因とするエラーフロア現象を緩和する符号構造を導入した．新たに導入した符号構造によって復号能力が損なわれないことを検証した．

2-2 成果

当該年度の目標（1）については、3 つの統計モデル全てに対し分離設計理論を拡張したことから、目標として掲げたことを完全に達成できた。（2）については、ガウス型の統計モデルに対して、適切に動作する誤り訂正符号化方法を開発したことより、目的を達成できたと判断される。

2-3 新たな課題など

本研究課題と関連して、同じく ImPACT に参加している NICT のほうで、光空間通信を行う送信機と受信機を実際に作成し、通信路の統計モデルの決定に役立つ実測値を収集している。その結果、平成 27 年度に、(a)通信路の時間変動が比較的激しい（速い）、(b)実測値のヒストグラムに良く当てはまる統計モデル（ガウス分布、ガンマ分布等）が、測定を行う時刻や天候に依存して変化することがわかった。

知見(a)により、本研究課題の計画策定時に第一の候補として想定していた盗聴通信路符号化を用いると、通信路状態により定まる通信路容量が符号化器の情報レートを下回るときに通信出来ないことがわかった。そのため、NICT と協議の上、平成 28 年度は通信路状態が悪い場合でも共有できる秘密鍵が短くなるだけで済む「情報理論的鍵共有プロトコル」を光空間通信路に用いて秘密鍵を生成することを、盗聴通信路符号化を用いる方法より優先して研究開発するように計画の変更を行った。

また、「情報理論的鍵共有プロトコル」を用いて秘密鍵を生成するとき、通信路状態に応じて最終的に生成する秘密鍵の長さを調節する。知見(b)のため、通信路状態を推定するときにどのような統計モデルを想定してよいか現時点ではわからないため、標準的な統計学の推定理論を用いることが出来ない。この問題を解決する方法を平成 28 年度に検討するよう計画の変更を行った。

（2）については，誤り訂正符号を定義するパリティ検査行列として，ランダム置換行列を用いたパリティ検査行列の構成を用いているために，さらなる復号の高速化が困難である．疑巡回符号の構造を用いたパリティ検査行列の構成により高速化することが課題としてあげられる．

３．アウトリーチ活動報告

特になし