平成　27　年　3　月　31 日

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２６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：国立大学法人　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

東工大担当の任務は、NICT と共同で盗聴通信路符号化の設計理論の開発である。符号化が実現するべき機能は、正規受信者の復号誤り確率を減らす誤り訂正機能と、盗聴者への漏洩情報量を減らす秘匿性増強機能である。東工大では、これら二つの機能を実現する符号化・復号方法を別々に設計して組み合わせることにより所望の盗聴通信路符号化を行えることを数学的に証明（これを（１）とする）した後、秘匿性増強を行う符号化・復号方法の設計理論（これを（２）とする）と誤り訂正を行う符号化・復号方法の設計理論（これを（３）とする）を別々に構築することが任務である。その目的のための平成２６年度の年度目標は、既存の研究結果を精査して具体的に何を達成する必要があるか特定することであった。

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

上記の目標（１）に関連する先行研究として、東工大の松本が名古屋大と共同で行っている、離散通信路に対して秘匿性状況と誤り訂正の符号化を分離設計する先行研究を検討した。この研究は本プロジェクトに先立ち行われており本プロジェクトに先立ち論文投稿され現在査読中で査読報告が戻ってきて改訂作業を行っている。この改訂作業で分離設計理論を離散型通信路だけでなく、連続型通信路にも分離設計理論を適用できるように拡張した。ここで、改訂作業を行う前の、名古屋大との先行研究は通信路の入出力アルファベットが有限集合であることを仮定していたので、そのままでは ImPACT の研究対象となる光通信路に適用することが出来なかった。これを受けて以下の 2-2 成果に述べるような作業を目標（１）と（２）について行った。

目標（３）については、本プロジェクトに先立って東工大の笠井が開発していた、理論限界に近い性能を有する高速に復号終端処理が可能な誤り訂正符号をソフトウェアにより実装し、実装上の問題点をシミュレーションを通して検討した。さらに、単純ではあるが広範囲の記憶のある通信路に対して、開発した誤り訂正符号の性能を検討した。

2-2 成果

前小節で述べた名古屋大による連続通信路における分離設計理論は、本プロジェクトの対象である自由空間光通信路に適用できる可能性が高いが、当初は一体どのような条件ならびに連続通信路のクラスに理論を適用できるのか不明瞭な部分があった。これに対して松本が適用できる範囲を明確にした（目標（１）に関する成果)。また本プロジェクトに先立つ名古屋大との共同研究において秘匿性増強のための符号化を離散通信路のために提案していたが、分離設計理論を拡張したことによって連続通信路にも適用できる秘匿性増強のための符号化を提案したことになる（目標（２）に関する成果)。

目標（３）については、理論限界近くで低いエラーレートを達成できることをソフトウェアによるシミュレーションにより確認することができたが、ビットエラーレートで 1.0E-9 程度

のエラーフロアを有することが観測された。さらに、単純ではあるが広範囲の記憶のある通信路に対して、開発した誤り訂正符号の性能が万能に理論限界を達成する性能を有することを理論的に証明した。

2-3 新たな課題など

目標（１）に関して 2-2 に述べた成果が本プロジェクトで扱う自由空間光通信路に適用できるか否かは、自由空間光通信路の統計モデルが現時点では特定できていないためはっきりしない。自由空間光通信路の統計モデルの特定は主として NICT の任務であるが、東工大も NICT と協力して統計モデルを確定し 2-2 の目標（１）に関する成果が十分なのか不足があるのか確定する必要がある。

目標（２）に関して、2-2 で述べた秘匿性状況のための符号化法はメッセージとダミー乱数の組にランダムに選んだ正則行列を掛けることによって実現される。これは計算量がメッセージ長の平方に比例し実装が困難になる可能性が高いため、より少ない計算量を実現する設計方法を解明する必要がある。

目標（３）については、ソフトウェアシミュレーションにより観測したエラーフロアは、符号化の終端処理を高速に行うために導入した符号構造の修正が原因となっている。符号化の終端処理のスピードを損なわないように符号構造をさらに修正し、エラーフロアを改善する必要がある。

３．アウトリーチ活動報告

なし