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：

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）研究開発責任者松本（平成 28 年度まで）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（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。

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

「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。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 年度に検討を行った。

2-2 成果

秘密鍵共有の際に必要になる、正規ユーザー間の通信路推定について、いかなる統計的モデルも仮定せず、盗聴者のエネルギー分解能の制限を仮定するだけで、鍵の秘匿性を保証できる推定方法を提案し、雑誌論文として発表した。

過去に開発した干渉通信路のための誤り訂正符号を拡張して、同期誤りを訂正可能な誤り訂正符号を検討した。さらに、この通信路の対称情報レートを評価し、提案した同期誤り訂正符号がその対称情報レートに近い符号化率で低い復号誤り確率を達成できることを数値実験により確かめた。

2-3 新たな課題など

前節で報告した通信路推定法を用いたとき、安全に得られる鍵の長さが、推定に用いる標本数が少ない（例えば６４０００個）とき、短くなってしまうことが明らかになった。そこで、安全性を保証できなおかつより長い鍵を取り出せる通信路推定方法の解明が課題としてあげられる。

前節で報告した提案誤り訂正符号に関して、同期誤りが多くなると対称情報レートと符号化率のギャップが大きくなってしまうという現象が観測された。この現象の理論解析と解決が課題としてあげられる。

３．アウトリーチ活動報告

該当する活動なし