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：

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
笠井健太

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、情報通信研究機構と協力し、通信路の妥当な統計的モデルを明らかにし、その統計的モデルに従って安全性を保障する具体的な鍵共有のプロトコルを提案することを当該年度の目標とした。

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

「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、統計的なモデルとしてどのようなモデルを想定すると通信路を実際に測定して得られる測定データをよく説明するか明らかにした。また、そのモデルに対して安全性を保障する鍵共有プロトコルを明らかにした。

2-2 成果

情報通信研究機構と協力のうえ、実際の自由空間光通信路で測定したデータから、通信路をよく説明できる統計的モデルとして Bi-Gaussian 分布（２つのガウス分布の重ね合わせとして確率密度関数が与えられる分布）が妥当であることを明らかにした。また、このモデルについて安全性をもつ鍵共有プロトコルを開発し、実環境で１秒当たりに共有できる秘密鍵の量を明らかにした。

同期誤りを訂正可能な誤り訂正符号の理論的な性能評価を行うために、密度発展を開発した。開発した密度発展によってパラメータを最適化し、従来困難であった対象情報レートに接近する性能を有する誤り訂正符号を構成することができた。

2-3 新たな課題など

前節で述べた成果を対外的に公表して社会に還元していくことが必要である。また前節でのべた安全性の解析は、標本数の有限性を無視した解析となっているが、実際には標本数は有限であるから、有限性を考慮に入れた安全性の解析を行う必要がある。

前節で報告した提案誤り訂正符号に関して、パリティ検査行列の構成法にランダム性が含まれているので、装置化する際にはこのランダム性を取り除き規則的なパリティ検査行列で構成される必要がある。

３．アウトリーチ活動報告

該当する活動なし