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：量子暗号と現代暗号の融合に関する研究開発

研究開発機関名：三菱電機株式会社

研究開発責任者：松井　充

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

１．「量子暗号と連携可能な新しいアプリケーションの開発」

量子鍵配送で生成した秘密鍵を用いて、スマートフォン上の様々なアプリケーションが行う通信を対象とした暗号化するソフトウェア（以降、量子暗号ネットワークサービスと記す）を実現するため、該当のソフトウェアに必要とされる機能要件を明確にする。

２．「現代暗号と量子暗号の融合技術」

双対ユニバーサルハッシュ関数に関する理論検討を実施し、既存方式の改良を目指す。また、それと並行して、既存方式が、PUF 技術における現実の装置性能（処理速度や補助乱数消費量）の向上に有効であるか否かについて検討する。有効であると判明した場合には、アルゴリズム改良や FPGA 開発に関する次年度のスケジュールを具体的に設定する。有効でないと判明した場合には現状の問題点を列挙し、次年度の理論研究における目標を定める。

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

１．「量子暗号と連携可能な新しいアプリケーションの開発」

量子暗号ネットワークサービスに必要とされる機能要件を明確にし､その検討結果を機能仕様書としてまとめた。

２．「現代暗号と量子暗号の融合技術」

多体スカッシュ演算子と呼ばれる数学的手法を活用することにより、装置無依存量子暗号(device-independent quantum key distribution, DIQKD)の秘密鍵生成率を改良した。

2-2 成果

１．「量子暗号と連携可能な新しいアプリケーションの開発」

以下に、当該年度に検討した機能仕様の概要を記す。

本システムでは量子鍵配送装置によって配布された秘密鍵を用いることで、スマートデバイス上の任意の通信を暗号化できるシステムを構成する。量子暗号ネットワークサービスはクライアント、サーバおよびローカル端末からなるシステムである（図 1 参照)。

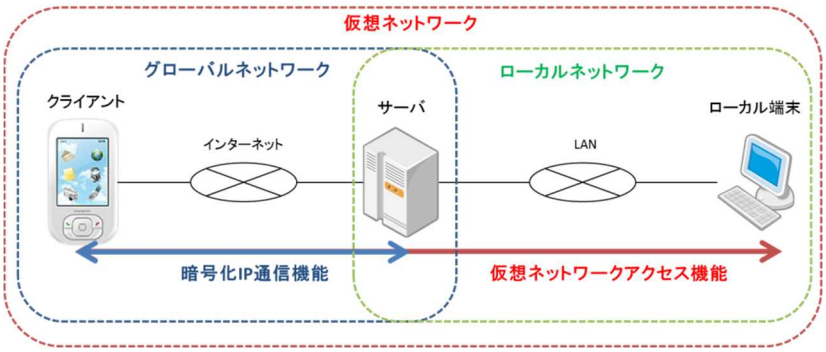

図 1　システム構成図

量子暗号ネットワークサービスは以下の 2 つの機能を提供する。

1. クライアント・サーバ間での暗号化 IP 通信機能

クライアント・サーバ間で通信される任意の IP パケットを、クライアント・サーバ間で共有された秘密鍵を用いて暗号化/復号する。

2. クライアントからローカル端末への、サーバを経由した IP 通信機能

クライアントから受信した IP パケットの情報に基づいてサーバでルーティングを行い、暗号化通信路を介したローカルネットワークへの仮想的なアクセスを実現する。

２.「現代暗号と量子暗号の融合技術」

多体スカッシュ演算子を利用して、Ekert 1991 (E91)プロトコルで無記憶検出器を仮定した場合の、装置無依存な安全性証明を行った（文献[T. Tsurumaru and T. Ichikawa, arXiv:1502.04802v3]）。その結果、図２に示す通り、秘密鍵生成率が既存文献よりも改良された。黒い太線が我々の文献による生成率であり、それ以外は既存文献によるものである。なお黄線、灰色線の文献が高い生成率を達成できているのは、我々よりも強い物理的仮定を置いているためである。

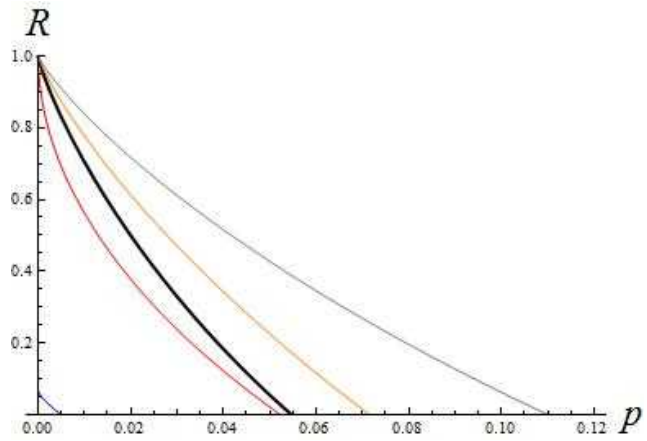

図２：E91 プロトコルの秘密鍵生成率の比較。

2-3 新たな課題など

１.「量子暗号と連携可能な新しいアプリケーションの開発」

機能要件を明確化する過程で、システム構成の詳細を検討した結果、スマートフォンに加えてサーバのソフトウェア開発も必要となった。

そのため、今年度はサーバの機能検討も実施した。次年度以降についても、サーバの設計及び開発を追加実施することで対応する。

２.「現代暗号と量子暗号の融合技術」

今年度の MPSO を用いた成果を、今後は、物理乱数生成器の性能向上に役立てることを計画している。MPSO は量子情報理論の手法であり、物理乱数生成器は現代暗号システムの重要な構成要素である。したがってこの方向性を追求することにより、量子情報理論が、現代暗号の性能向上に役立つことになる。

３．アウトリーチ活動報告

該当する活動なし