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：

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」

平成 27 年度に検討した機能要件に従い、Android スマートフォン上で動作する量子暗号ネットワークサービスのプロトタイプ（ソフトウェア)、量子暗号ネットワークサービスと暗号通信を行う PC 用のプロトタイプ（ソフトウェア）を開発する。これにより、Android スマートフォンと PC 間でワンタイムパッドによる暗号通信を実現する。

２.「現代暗号と量子暗号の融合技術」

量子乱数生成器においても秘匿性増強アルゴリズムが重要な役割を果たす。我々はその秘匿性増強アルゴリズムを改良することにより、量子物理乱数の生成速度の理論値の向上、または実装コストの削減を実現することを目指す。またそれと並行して、装置無依存安全性を実現するための方式検討も行う。得られた成果を論文投稿または特許出願することを目指す。

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」

Android スマートフォン上で動作する量子暗号ネットワークサービスのプロトタイプ（ソフトウェア)、量子暗号ネットワークサービスと暗号通信を行う PC 用のプロトタイプ（ソフトウェア）を開発した。

２.「現代暗号と量子暗号の融合技術」

秘匿性増強に関する理論研究を実施した。秘匿性増強の安全性解析については、異なる 2 種類の手法が長年独立に使われてきており、なおかつ両者の関係は不明だった。今年度我々は、ある限定された状況についてではあるものの、両手法を数学的に統一することに成功した。

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、当該年度に開発した量子暗号ネットワークサービスのプロトタイプ（ソフトウェア)、量子暗号ネットワークサービスと暗号通信を行う PC 用のプロトタイプ（ソフトウェア）の概要を記す。

量子暗号ネットワークサービスは、暗号化 IP 通信機能、仮想ネットワークアクセス機能及び鍵管理機能を持つ、クライアントアプリケーションとして実装し、量子暗号ネットワークサービスと暗号通信を行う PC 用のプロトタイプは、暗号化 IP 通信機能、仮想ネットワーク構成機能、サーバ管理機能、IP パケットフラグメント化／再構築機能を持つ、サーバアプリケーションとして実装した。

以下では、主機能である暗号化 IP 通信機能について説明する。

本機能は、クライアントーサーバ間の通信において、両者から送出される IP パケットを秘密鍵によって暗号化/復号を行うものである。本機能のイメージを図 1 に示す。

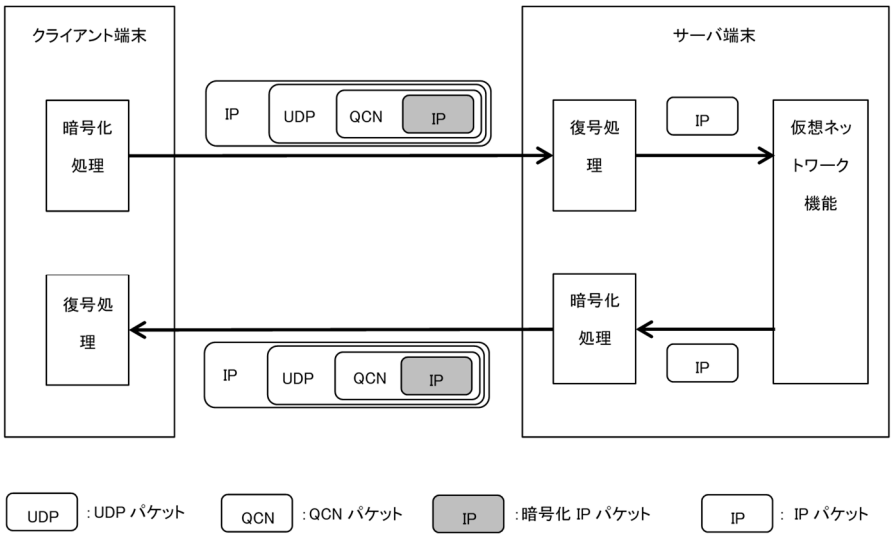

図 1：暗号化 IP 通信機能の概要

本機能ではクライアントーサーバ間で送出された IP パケットを暗号化する。具体的には、暗号化に使用した暗号アルゴリズムおよび認証アルゴリズムや鍵情報などを QCN ヘッダ(*1)に記載し暗号化された IP パケットをカプセル化する。作成された QCN パケットを UDP/IP 通信を行うことで暗号化 IP 通信が実現される。

*1：QCN ヘッダ：本機能を実現するために独自に定義したヘッダ。

2．「現代暗号と量子暗号の融合技術」

秘匿性増強の安全性解析では通常、以下の異なる 2 つの数学的手法のうち、いずれか一方が用いられている：

- 量子誤り訂正符号(QECC)による手法（Mayers 1997, Shor-Preskill 2000 ほか）
- Leftover Hashing Lemma (LHL)の手法（Bennett et al. 1988, Renner 2005 ほか）

これらの手法どうしの数学的な関係は未だ解明されておらず、それぞれが独立な手法と考えられている。そのため同じ問題であっても、異なる手法で解けば独立な成果とみなされ、別個の論文として発表されることがしばしばある。ただし経験的には、どちらの手法を用いようとも、殆ど全ての問題の答えは同じになることが知られている。

今年度我々は、この 2 つの手法どうしの関係を明らかにすべく、理論研究を実施した。そしてその結果、ある限定された状況に対してのみではあるものの、両者を数学的に統一することに成功した。ここでいう限定された状況というのは、具体的には、（量子暗号におけるように）送信者と受信者が協力して秘匿性増強を実施しつつ、シールド状態が存在しない状況を指している。この状況において我々は、LHL の手法における最小エントロピーが、仮想 QECC における位相誤り分布の Renyi エントロピーに対応することを示した。さらにそれを用いて LHL を、仮想的 QECC の帰結として導出することに成功した。これは LHL, QECC の両手法の結果を、QECC の手法のみから導出できたことを意味する。

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」

今年度開発したプロトタイプは、試験環境での簡易な動作検証では滞りなく動作することが確認できているが、実用的な環境での検証は未実施であるため、一般的に利用されているアプリケーションや通信プロトコルでの検証が必要と考える。そのため、次年度では検証用アプリケーションを開発し、様々なパターンの通信形式において、開発した機能が有効であることを確認する。

2.「現代暗号と量子暗号の融合技術」

今後は、上記で得られた結果（LHL, QECC の手法の数学的統一）を、限定なしの一般的な状況に拡張することを計画している。そして両手法の長所を併せ持つ新手法を開発するとともに、それをワイヤタップ通信路、物理乱数生成器といった現実の暗号方式に応用し、性能改善に役立てることを目指している。

3．アウトリーチ活動報告

該当する活動なし