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

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 28 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について、有効性検証を行う。有効性検証にあたっては、平成 29 年度は、まず、検証用にスマートフォン上で通信を行う検証用アプリケーションを開発する。その後、開発した検証用アプリケーションを用いて、量子暗号ネットワークサービスのプロトタイプが様々な通信を、量子鍵配送で生成した秘密鍵により暗号化できることを検証する。

２.「現代暗号と量子暗号の融合技術」

平成 29 年度の研究開発課題は、平成 28 年度と同様に、秘匿性増強の安全性証明の理論と、そのアルゴリズム（双対ユニバーサルハッシュ関数）の改良検討である。ただしその検討を行うに当たって、平成 28 年度と異なるアプローチをとる。具体的な内容は以下のとおりである。

秘匿性増強の理論研究においては、異なる研究グループ各々の提案による、2 種類の数学的手法(※)が知られている。今年度の研究で我々は、この両者を統合することを目指す。もしこの統合に成功した場合、2 理論の長所を併せ持つ新たな理論的手法が得られる。そしてそれを活用することにより、ワイヤタップ通信路、物理乱数生成器といった、実用的な暗号方式の性能改善にも役立つことが期待できる。

※leftover hashing lemma (LHL)を用いる手法と、量子誤り訂正符号(QECC)を用いる手法

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の有効性検証を行うための検証用アプリケーション（ソフトウェア）を開発した。開発した検証用アプリケーションを用いて、量子暗号ネットワークサービスのプロトタイプが様々な通信を、量子鍵配送で生成した秘密鍵により暗号化できることを検証した。

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際しては、異なる 2 種類の手法が存在し、なおかつ両者の関係はこれまで不明だった。我々は昨年度(2016 年度)の研究において、これら両手法を、条件つきではあるが数学的に統一することに成功した。ひきつづき今年度も研究を継続し、条件なしの一般の場合において統一することに成功した。その結果の一部は国内研究会(2018 年 1 月, SCIS2018)で発表しており、さらに現在は論文投稿の準備を進めている。

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検証用アプリケーション（ソフトウェア）の概要を記す。

検証用アプリケーションは、量子暗号ネットワークサービスの動作検証と機能デモを行うためのサーバソフトウェア（以降、デモサーバ SW と記す）とスマートフォンアプリ（以降、デモアプリと記す）で構成されており、図１のように配置される。

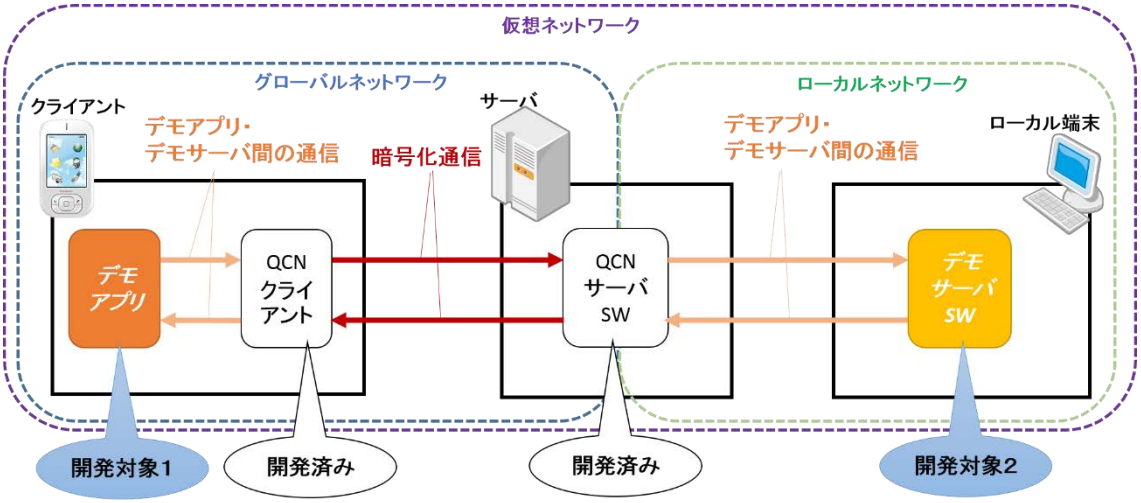

図 1：検証用アプリケーションの配置

デモサーバ SW はローカルネットワーク内にあるローカル端末上で動作し、デモアプリはグローバルネットワークにあるクライアントで動作する。そのため、デモサーバ SW とデモアプリで行う通信は、QCN サーバ SW と QCN クライアントを経由することになり、その結果、量子暗号ネットワークサービスによる暗号化が行われることになる。

デモサーバ SW は、WEB サーバ、メールサーバ及び動画配信サーバの機能を有しており、デモアプリからのリクエストに応答する。デモアプリは、デモサーバ SW に対して WEB 閲覧、メール送受信、動画配信をリクエストすることができ、その結果を画面に表示する。

開発した検証用アプリケーションを用いて量子暗号ネットワークサービスの検証を行い、様々な通信プロトコルによる通信を暗号化できることを確認した。

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が同じになることが知られている。

この問題について、我々は昨年度(2016 年度)から理論研究を継続し、今年度になって、両者を数学的に完全に統一することに成功した。

なおこの成果は量子暗号のみならず、現代暗号にもそのまま適用できる。したがってこの成果を活用することにより、量子暗号のみならず現代暗号の方式をも改良できると考えている。

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」

今年度は、検証用アプリケーションにより量子暗号ネットワークサービスが様々な通信プロトコルによる通信を暗号化できることを確認したが、複数のクライアントが同時に通信する場合や異なる通信プロトコルが同時に通信する場合など、通信負荷が高い状況での検証は未実施である。

そのため、次年度では検証用アプリケーションを活用して、通信負荷が高い状況での動作検証を行い、量子暗号ネットワークサービスの有効性を確認する。

2.「現代暗号と量子暗号の融合技術」

平成 30 年度は、放射線を用いた物理乱数生成器（以下、放射線乱数）に関する理論研究を行う。

物理乱数生成器は現代暗号に不可欠であり、なかでも放射線乱数は、実装が容易性であるという長所があるものの、その安全性はいまだに厳密に証明されていない。そこで我々は、放射線乱数に対して、これまでの量子暗号研究の成果を適用することにより、厳密な安全性証明を与えることを目指す。

それにより、実装が容易かつ推測が絶対に不可能な物理乱数の実現を目指す。

3．アウトリーチ活動報告

該当する活動なし