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：

量子鍵配送プラットフォームの研究開発

研究開発機関名：

日本電気株式会社

研究開発責任者
中村 祐一

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

高秘匿量子光送信技術に関して、平成 26 年度、平成 27 年度では送信光パルスの強度揺らぎをはじめとする重要パラメータの測定と分析を行い、その測定結果に基づいて高精度 Decoy を実現するための光強度・位相変調技術を検討する。この中で平成 27 年度では、高精度 Decoy を実現するための光強度・位相変調技術について検討し、量子鍵配送装置の光学基板の設計を完了する。

フレキシブル秘匿増強処理実装アーキテクチャに関して、平成 26 年度、平成 27 年度では秘匿増強処理単位を拡大した場合の回路規模および実行時間の見積もりを行い、その結果に基づいてリアルタイム処理を実現するための実装検討を行う。この中で平成 27 年度では、リアルタイム処理を実現するための実装方法について検討し、鍵蒸留ソフトウェアの設計を完了する。

スマート鍵管理実装技術に関して、平成 26 年度、平成 27 年度は、異なるベンダーの量子鍵配送装置から供給される鍵を一元管理し、盗聴や障害時に鍵配送経路を切り替える高信頼な鍵管理システムの実装アーキテクチャおよび量子鍵配送装置とのインタフェースの検討を、取り纏めを担当する NICT と連携して行う。この中で平成 27 年度では、鍵管理システムの実装アーキテクチャの検討を行う。

現代暗号と量子暗号の統合による新しいセキュリティ技術に関して、平成 26 年度、平成 27 年度は要求されるセキュリティレベルや通信速度に応じて暗号鍵を活用するためのアプリケーションインタフェース技術の設計・開発を行う。この中で平成 27 年度では、高速回線暗号装置やスマートフォンで、現代暗号の鍵更新を行うアプリケーションの設計・開発を行う。

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

高秘匿量子光送信技術に関して、平成 27 年度は高精度 Decoy を実現するための光強度・位相変調技術について検討し、量子鍵配送装置の光学基板の設計を完了した（計画通りに進捗）。

フレキシブル秘匿増強処理実装アーキテクチャに関して、リアルタイム処理を実現するための実装方法について検討し、鍵蒸留ソフトウェアの設計を完了した（計画通りに進捗）。

スマート鍵管理実装技術に関して、実装アーキテクチャ策定にくわえ、実証検証のための高秘匿量子鍵配送装置を構成する各種基板の基本仕様設計を完了した（計画通りに進捗）。

現代暗号と量子暗号の統合による新しいセキュリティ技術に関して、秘匿携帯アプリケーションの開発と動作確認および回線暗号装置アプリケーションの実装方式検討を完了した（計画を見直した）。

2-2 成果

高秘匿量子光送信技術に関して、高精度 Decoy 変調を実現するための光学基板の設計を行った。図１にブロック図を示す。D/A コンバータやノイズフィルタの検討によりデコイ用強度変調器のバイアス電圧の調整精度を 10 倍以上向上し、デコイパルス強度の揺らぎを１％以下に抑制できる設計とした。平成 28 年度にはこの設計に基づいて光学基板の試作を行う。

フレキシブル秘匿増強処理実装アーキテクチャに関して、リアルタイム処理を実現する際のボトルネックの１つは最も取り扱うデータ量の多いデータ受信部（図２の①）であることが判明した。そこで、データ受信部にはデータの高速転送が可能である DPDK ライブラリ（Data Plane Development Kit）を用いることとした。また、後段②～⑤の処理に関しても実装検討を行い、ソフトウェアの詳細設計まで完了した。平成 28 年度にはソフトウェアの試作を行う。

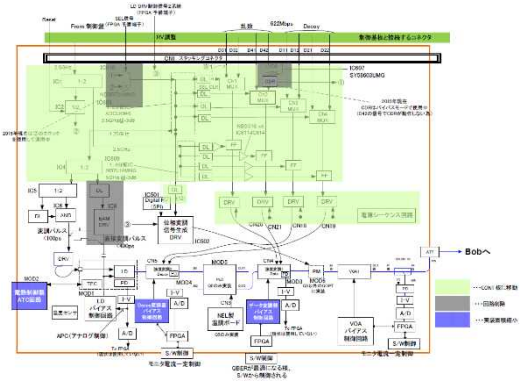

図１：光学基板のブロック図

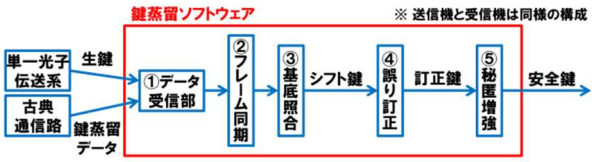

図２：鍵蒸留処理のブロック図

スマート鍵管理実装技術に関して、NICT と連携して量子鍵配送装置とのインタフェース方式を含め鍵管理システムのアーキテクチャを策定した（図３）。また、実証検証に必要な高秘匿量子鍵配送装置の製造に向け、装置の主要構成要素である各種回路基板および光子検出器の仕様設計を行った。平成 28 年度には、高秘匿量子鍵配送装置を製造し、鍵管理システムの実装設計や機能試作を通して安定性・高信頼性のための実装技術と課題を明らかにする。

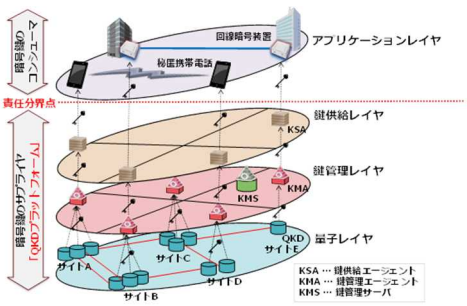

図３：鍵管理システムアーキテクチャ概要

現代暗号と量子暗号の統合による新しいセキュリティ技術に関して、回線暗号装置アプリケーションにつき、実利用に際し有用な多拠点間通信の実現のため、装置の具備するマルチキャスト機能と多拠点間ユニキャスト機能の活用可能性を比較し、実用性と鍵供給・同期インタフェースの実装方式において当初想定の前者より後者が優位であることを明らかにした。秘匿携帯アプリケーションにつき、マルチユーザに対応した、スマートフォンと鍵管理層の連携インタフェースについて開発・動作確認を完了すると共に、継続的な運用面での評価及び実利用に向けた高速化、ユーザーインタフェース向上を含む機能向上が望ましいことを明らかにした。平成 28 年度は評価試験等を通し、鍵の使用量や管理方法、高負荷時の通信処理や実運用面での課題点を抽出し、実用化に向けた機能向上の検討を行う。

2-3 新たな課題など

現代暗号と量子暗号の統合による新しいセキュリティ技術に関して、上記から明らかになった事項から、研究開発スケジュールの見直しを図った。具体的には、回線暗号装置アプリケーションは、比較検討結果を反映して開発着手時期を変更し、秘匿携帯アプリケーションは、多岐にわたる運用面での評価を反映させた機能向上を行うため、複数回の設計・開発・評価をプロジェクト期間を通して実施することとした。

３．アウトリーチ活動報告

大型潜在ユーザである官公庁向け展示会において、量子暗号の紹介と共に研究開発状況を説明した。また、同官公庁との量子暗号に関する勉強会を平成 28 年度上期に開催することを目標として、主体となる NICT と説明方針及び具体的テーマについて検討を開始した。