平成２７年　3月３１日

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２６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。平成 26 年度では、送信光パルス強度の揺らぎが暗号鍵生成特性に与える影響について調査・分析し、その結果を元に光パルス強度揺らぎの許容範囲を特定する。

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。平成 26 年度では、光子検出データから安全な暗号鍵を抽出するまでの鍵蒸留処理全体のアーキテクチャと、鍵蒸留処理に含まれる各部分処理（基底照合・誤り訂正・秘匿増強）の方式について検討する。

スマート鍵管理実装技術に関して、平成 26 年度は、量子鍵配送装置とスマート鍵管理システムの連携インタフェースの検証等に必要な波長多重型高速量子鍵配送システムにおいて、NEC が研究開発した量子鍵配送システムを構成する部位のうち、「制御基板」の信頼性向上設計を行う。

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 年度は、量子鍵配送装置及びスマート鍵管理システムと、NEC が開発した秘匿携帯アプリケーション（スマートフォン）との連携インタフェースを実装し、実運用環境で安定に動作しかつ信頼性の高いシステムを検討する。

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

高秘匿量子光送信技術の研究では、量子鍵配送システムにおける送信光パルス強度の揺らぎが暗号鍵生成特性に与える影響について調査・分析を行った。また、その結果を元に、光パルス強度揺らぎの許容範囲を特定した。フレキシブル秘匿増強処理実装アーキテクチャの研究では、光子検出データから安全な暗号鍵を抽出するまでの鍵蒸留処理全体のアーキテクチャについて検討した。また、鍵蒸留処理に含まれる各部分処理（基底照合・誤り訂正・秘匿増強）の方式について検討した。スマート鍵管理実装技術の研究では、NEC が研究開発した量子鍵配送システムを構成する部位のうち、「制御基板」の信頼性を向上するため、電源回路及び内部クロックの回路設計方針を検討し、設計仕様を作成した。量子鍵配送装置と秘匿携帯アプリケーション（スマートフォン）との連携インタフェースの研究では、複数の鍵管理技術及び鍵更新技術の向上を目的としたアーキテクチャの仕様調査を行った。

４課題とも、平成 26 年度の計画通りに進捗した。

2-2 成果

高秘匿量子光送信技術の研究では、光パルス強度の揺らぎが暗号鍵生成特性に与える影響について調査･分析を行った。Hayashi らの論文の方法に基づき、光パルス強度揺らぎの標準偏差が平均強度の０％（揺らぎなし）、１０％、３０％の場合の暗号鍵生成レートを見積もった（図１）。その結果、暗号鍵生成レートの低

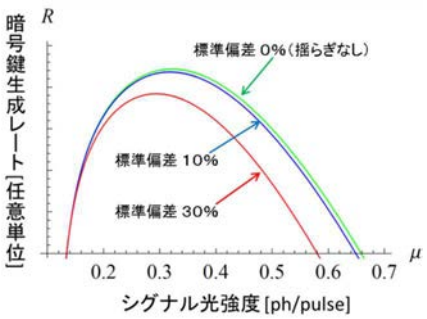

図１：光パルス強度揺らぎを 0%、10%、30%とした場合の暗号鍵生成レート

下をほとんど無視できる程度に抑制するためには、光パルス強度揺らぎを１０％以下に抑える必要があることが明らかとなった。

フレキシブル秘匿増強処理実装アーキテクチャの研究では、光子検出データから安全な暗号鍵を抽出するまでの鍵蒸留処理全体のアーキテクチャについて検討した（図２）。各部分処理の方式については、鍵抽出効率やこれまでの開発実績を元に検討した結果、基底照合には非対称基底選択方式、誤り訂正には LDPC 符号、秘匿増強には Toeplitz 行列を用いた方式が有効であることが分かり、これらの方式を採用することとした。

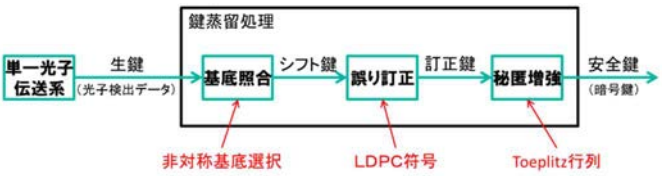

図２：鍵蒸留処理の全体アーキテクチャと各部分処理の方式

スマート鍵管理実装技術の研究では、NEC が研究開発した量子鍵配送システムを構成する部位のうち、量子鍵配送装置と鍵管理部のインタフェースである「制御基板」の信頼性を向上するため、電源回路および内部クロックの回路設計方針を検討し、以下の２点を明らかとした。

①電源回路に関しては、信頼性及び特性向上の為に回路変更が必要なことを明らかにした。

②内部クロックに関しては、内部クロックに関する懸案事項を改善するため、回路変更が必要なことを明らかにした。

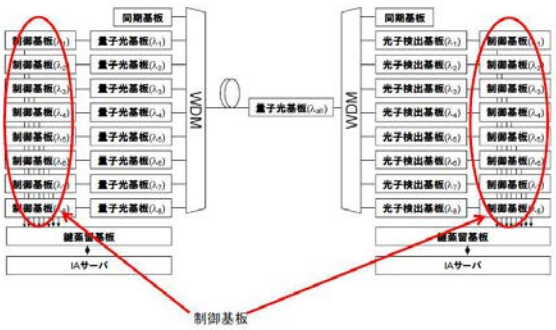

図３　NEC QKD 装置における制御基板

量子鍵配送装置と秘匿携帯アプリケーション（スマートフォン）との連携インタフェースでは、機能向上を目的としたアーキテクチャ（図４）の仕様調査を行い、以下の２点を明らかとした。

①複数の量子鍵配送装置から供給され暗号鍵の一元管理機能向上が必要なことを明らかとした。

②量子暗号と現代暗号を統合したセキュリティ技術として、鍵更新インタフェースの機能向上が必要なことを明らかとした。

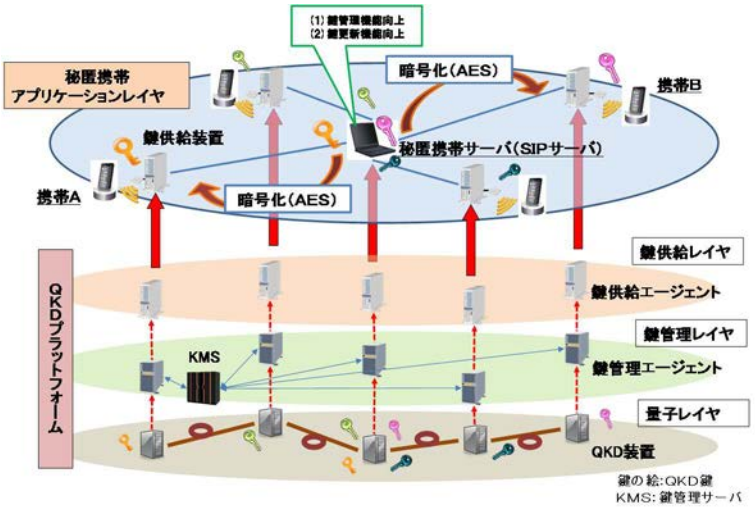

図４　量子鍵配送装置と秘匿携帯アプリケーションとの連携インタフェース

2-3 新たな課題など

平成 26 年度の研究活動において、新たに発生した課題はありません。

３．アウトリーチ活動報告

平成 26 年度の研究活動において、アウトリーチ活動はありません。