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：

量子セキュアネットワークアーキテクチャの研究開発

研究開発機関名：

独立行政法人　情報通信研究機構

研究開発責任者
佐々木雅英

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

課題１：量子セキュアネットワークアーキテクチャの研究開発

プロジェクトの全参画機関と共同で、量子鍵配送（QKD）された暗号鍵の様々なアプリケーション（端末機器や用途）候補について調査し、実用化ロードマップを策定するとともに、汎用的なアプリケーションインターフェース（Application Programming Interface：API）の仕様をまとめる。それに基づき量子セキュアネットワークアーキテクチャの主要要素を抽出し大枠を定める。

課題２：スマート鍵管理・多層防御システム化技術

盗聴・障害検知機能と複数経路間での自動切り替え機能・鍵リレー機能を実装しスマート鍵管理システムの主要部を完成させる。既存セキュリティ技術と QKD の融合に向け、まず企業チームが現在有している製品（共通鍵暗号やスマートフォンなど）との API を実装し検証して、今後、産学官の様々な機関が有効活用してゆけるようなオープンリソース基盤を構築する。

課題３：適応的物理レイヤ暗号技術

適応的物理レイヤ暗号の要素技術と実証環境の整備を行う。特に、通信路の状況に応じて送信電力や秘匿符号化における誤り訂正／ランダム化比率を自在に調整する技術の基礎実験を行うとともに、高精度光空間通信アライメントシステムの開発と、通信路評価技術に必須の光子検出技術の高度化を行う。光子検出技術は QKD の根幹技術でもあり、競争力のある国産技術に発展させるための産学官連基盤の強化にも取り組む。また、通信路評価のために通信基礎理論と量子通信技術の研究開発を進める。

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

課題１：量子セキュアネットワークアーキテクチャの研究開発

ネットワークの各階層（OSI 参照モデルにおける第 2, 3, 4 層）における既存のセキュリティ技術と QKD の統合法や性能について調査を進め、開発計画のマイルストーンを作成し、ネットワークアーキテクチャの基本構成を導出するとともに、今後、技術検討報告書として公開を想定したドキュメント作成に着手した。

課題２：スマート鍵管理・多層防御システム化技術

QKD システムへの Denial of Service (DoS) 攻撃（例：QKD 装置への明光入射や伝送用ファイバの切断）への耐性とサービスの安定性を向上させるため、システム監視技術の改良とリルーティング機能の強化について検討を進めた。既存の共通鍵暗号システム（データレイヤにおける回線暗号装置）やスマートフォンと QKD を統合するアプリケーションについて、最適な鍵フォーマットと API の設計を行い、実装に着手した。

課題３：適応的物理レイヤ暗号技術

適用的物理レイヤ暗号の実証環境の整備を順調に終了した。秘匿符号化の基礎実験に関しては若干の遅れが生じている。秘匿通信時における送信電力最適化技術に関しては、設計理論の研究の中で教科書を塗り替える重要な新知見が得られた。

高精度光空間通信アライメントシステム、光子検出技術、通信基礎理論、量子通信技術に関して、計画通り順調に進捗した。

2-2 成果

課題１：量子セキュアネットワークアーキテクチャの研究開発

第 2 層（データレイヤ），第 3 層（ネットワークレイヤ）の基本的なプリケーションについてプロトタイプを試作し、潜在ユーザへのデモ環境を構築した。また、防衛、警察、金融分野の潜在ユーザの方々へ見学会を開催し、定期的に情報交換を行うためのスキームを確立した。

課題２：スマート鍵管理・多層防御システム化技術

将来のマルチユーザ化を見据え、任意の 2 拠点間において計 12 パターンの鍵リレールートを設定し、盗聴や障害があった場合に鍵リレー経路を手動及び自動で切り替えできる機能を実装し、エミュレータ上での動作実証に成功した。様々な通信障害やエラーがあった場合でも、2 地点間で正しく認証され同期した暗号鍵が、QKD ネットワーク管理システムからクライアント（ユーザの回線暗号装置やスマートフォン）へ自動で供給される鍵供給 API を開発した。また、QKD ネットワークから複数種類の暗号鍵をスマートフォンへ供給し、情報理論的に安全な認証法と組み合わせることによって、重要データへの安全なアクセス管理とデータの秘匿化を平易に実現するシステムを開発した。

課題３：適応的物理レイヤ暗号技術

通信に利用できる電力に制限が課せられている条件下で最適な符号設計を行うための従来の基礎理論（Gallager 理論）では正しく取り扱えない領域があることを見出し、そのような領域でも信頼性と秘匿性のバランスを正確に定量評価できる新理論を開発した（学会発表、論文準備中）。

ビル間 8 ㎞のレーザー空間通信実証環境において、様々な気象条件下で大気ゆらぎに伴う伝送特性の変動の測定データを蓄積した。10M bps の信号が受信可能な検出器を開発し、疑似乱数列の伝送機能を実証し、信号対雑音比の変化をモニターするシステムを開発した。

2-3 新たな課題など

量子セキュアネットワークアーキテクチャに関して、次々と登場するアプリケーションや OS のバージョンアップに柔軟に対応できる鍵フォーマットや API の開発戦略を練る必要がある。スマート鍵管理・多層防御システム化技術に関して、多数のノードから鍵リレー要求が集中した場合にでも、動作遅延を生じることなく、鍵運用できる効率的な並列処理と安全性を劣化させない鍵管理に向けた新しいネットワークの概念設計が急務である。また一度使用した暗号鍵は確実に強制的に忘却させ、それを担保する技術の開発が必須である。

３．アウトリーチ活動報告

■勉強会および実験装置デモンストレーション

UK-Japan Quantum Technology Workshop(Lab tour)
日時：2015 年 3 月 24 日　11:30～16:00
場所：情報通信研究機構(小金井)
目的：日英間の国際イニシアティブ確立に向けた意見交換及び東京 QKD ネットワークのデモ。
参加者：英国研究機関および英国大使館関係者 7 名