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：

国立研究開発法人　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 Interfac : 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携基盤の強化にも取り組む。また、高精度の通信評価技術の確立に向け通信基礎理論と量子通信技術の融合に関する研究開発を進める。

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

物理層/鍵管理層/アプリケーション層の 3 階層構造に基づくアーキテクチャの基本設計と、鍵管理層とアプリケーション層間インターフェースの開発を完了した。これらを東京 QKD ネットワークに実装し基本動作の検証を完了した。

課題２：スマート鍵管理・多層防御システム化技術

盗聴・障害検知機能と経路切替機能を開発し、Tokyo QKD Network への実装を完了した。

NEC チームで開発している共通鍵暗号化装置(COMCIPHER)や秘匿スマートフォンへの API を開発し、Tokyo QKD Network へ実装した。また、小型無人航空機ドローンの制御通信を秘匿化するための暗号鍵供給プロトコル及び機器認証プロトコルを開発し、ドローンコントローラへ実装した。

インターネット上の web ブラウザやクラウドサービスが利用しているトランスポートレイヤセキュリティの各種プロトコルに対して QKD プラットフォームから鍵供給を実現するインターフェースを開発した。

課題３：適応的物理レイヤ暗号技術

NICT（小金井市）-電気通信大学（調布市）のビル間約 8km の光空間伝送路（Tokyo FSO Testbed）において、1550nm の通信波長帯で 10 MHz に変調した PN15 段疑似乱数列を送受信するシステムを完成させた。NICT 建屋屋上に設置した全天候型光受信システムに加え、同建屋内部、前記光受信システムから約 10 m 離れた場所に新たに光受信システムを設置し、１送信２受信系にて疑似乱数列のビットパターンを検出する光送受信システムを構築した。それぞれを正規受信者と想定できる最大の能力を有した盗聴者と見立てることにより、各受信系における相互情報量から通信路評価パラメーター（秘匿レート，秘匿アウテージ確率等）を算出し、ビル間光空間通信路の評価を行った。

また，送受信した疑似乱数列に対し，秘匿レートと誤り率から得られたパラメーターを用いて鍵蒸留処理（誤り訂正と秘匿性増強）を施すことにより、大気ゆらぎに伴う受信パワー変動が大きい光空間通信路であっても、送受信者間で情報理論的に安全な乱数列を共有することができる秘密鍵共有の手法の原理実証ついて検討した。

光空間通信用高速光送受信機の設計・仕様検討と整備を行い、実験室内環境にて基本性能の検証を行った。

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

東京 QKD ネットワークに実装した API により複数のアプリケーションで動作・機能の検証を完了し、その結果を基に汎用的な API 仕様を策定し、ドキュメント化した。

課題２：スマート鍵管理・多層防御システム化技術

データレイヤ（いわゆるレイヤ２）で直接機器間をつなぎ秘匿通信するための暗号鍵供給 API を開発し、回線暗号化装置(COMCIPHER)、秘匿スマートフォンシステム、電子カルテシステム、ドローン制御通信の暗号化を実現して、国際会議(Updating Quantum Cryptography and Communications 2015：UQCC2015)での公開実証実験やプレスリリースを実施した。

また、レイヤ４であるトランスポートレイヤへの鍵供給を実現する API も開発したことで、レイヤ２～レイヤ４まで全てのレイヤの API を東京 QKD ネットワーク上に実装する事ができた。（レイヤ３は開発済み）

課題３：適応的物理レイヤ暗号技術

日没後の測定データから算出した秘匿レートはほぼ一定値（5.25～8.30 Mbps）を示し、安定したメッセージ伝送が可能である一方、日没前の秘匿レートは変動が大きく、一時的にゼロを示す時間帯もあった。日没前のように大気ゆらぎに伴う受信パワーの強度変化が激しく、重大な情報漏えいが懸念

されるような場合、秘匿レートがある閾値未満になる確率（秘匿アウテージ確率）を見積もることにより、通信の可否を判断することができることが示唆された。

また，送受信した乱数列に対し、秘匿レートをパラメーターとした鍵蒸留処理により秘匿性を強化した秘密鍵を共有することができ、最大 4 Mbps での秘密鍵共有を実行することが可能であった。

約 8 km のビル間光空間通信用に最適な高速光送受信機を基本から設計し、仕様検討と整備を行い、システムの初期的動作確認に成功した。

2-3 新たな課題など

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

システム全体において安全性に対する脅威の分析・モデル化・評価を実施し脆弱な点を見極める必要がある。その結果をフィードバックし、システム及びネットワークにおける対策の検討を進める。

課題２：スマート鍵管理・多層防御システム化技術

国家機密やゲノムデータなど、重要情報が次々とクラウド上に蓄積されており、これらのセキュリティを超長期間（世紀単位）に渡って守るためのセキュリティ技術の開発が望まれている。これらへの一つの有望な解決策として、情報理論的安全性を持つ秘密分散プロトコルや秘密計算機能（完全準同型）のアプリケーション実装を検討する。

課題３：適応的物理レイヤ暗号技術

伝送レートを高速化（> GHz）した際の秘匿レートとその大気揺らぎの影響について検討する。

３．アウトリーチ活動報告

第４回量子暗号・量子通信国際会議(Updating Quantum Cryptography and Communications 2015 (UQCC 2015)）を 9 月 28 日午前、東京竹橋の一橋講堂において開催し、「量子セキュアネットワーク」プロジェクトの成果の一端を紹介した。本会議は、内外の大学、研究機関、産業界および省庁から３３４名の参加があった。

NICT は、様々な QKD 装置を接続しネットワーク化する鍵管理システム、及び QKD とスマートフォンを組み合わせた電子カルテシステムをステージ上に組み上げて、QKD の発明者であるベネット博士とブラサール教授とともに寸劇を交えて紹介した。

これらの発表は ImPACT 山本プログラムが目指す、都市圏での量子セキュアネットワークを実現する上でキーとなる QKD 技術とアプリケーションインターフェース技術が実サービスに近い環境での実証段階にあることを示した。