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：鍵管理アーキテクチャの研究開発

鍵管理処理速度を従来比の 10 倍まで高速化する。東京 QKD ネットワークの内部に仮想攻撃者を設け、攻撃耐性を検証する。また、乱数ダウンロードサービス運用時に想定されるネットワークセキュリティ上のリスク分析を行い、対処法を抽出する。

課題２：QKD 装置の評価・校正技術の研究開発

安全性評価・校正技術の共通規格化に向けて、日本語のドキュメントを作成し、ウェブ公開に向けた最終仕上げを行う。また、ETSI（欧州電気通信標準化機関）の下で開催される QKD 関連の会議で英語化したドキュメントを発表し、国際的な合意形成に取り組む。

課題３：QKD プラットフォームのアプリケーションの研究開発

分散ストレージネットワークに関して、医療情報を想定したケーススタディを行い、ユーザニーズに適したファイル構造、データ階層化を実装し、将来の潜在ユーザに向けて分散・復元動作の実証デモを行う。また、IPsec や TLS への鍵供給インターフェースを鍵管理層(特に鍵供給エージェントサーバ)へ実装し、基本動作の検証を完了する。

秘匿ドローン通信技術に関しては、屋内、屋外フィールドの様々な電波環境で試験運用を行い、重要インフラ監視や警備用途へ展開するために必要となる品質保証データを蓄積する。

また、物理乱数発生器の乱数性強化アルゴリズムの基本動作を実証する。光空間リンク上での物理乱数配送技術に関しては、10MHz の繰り返しレートで 8km 圏での伝送を実証するとともに大気条件との相関を解明する。

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

課題１：鍵管理アーキテクチャの研究開発

Tokyo QKD Network でのセキュリティ再診断、鍵管理処理高速化の実証までは至らなかったが、信頼できるノード（トラステッドノード）内トポロジーの再構成により攻撃耐性を向上させた。ただし一部再構成未了（大手町ノード）である。また、不特定多数ユーザへの乱数ダウンロード GUI を開発し、その機能を応用して乱数をプラットフォーム外部ユーザ、例えばドローン等ポータブル機器へ安全に配給する鍵搬送デバイス管理システムのプロトタイプを開発し実用化へ向けた検証評価を進めている。

課題２：QKD 装置の評価・校正技術の研究開発

NEC の開発した高速 QKD 装置による Tokyo QKD Network 上での長期安定性試験を引き続き実施するとともに、装置を構成するコンポーネントの数学モデルからの乖離の評価を進めた。また、NICT、NEC、北大で特許出願した（特願 2016-176364）パルス強度の生成パターンを用いたポストセレクシ

ョンと東大が発案した鍵蒸留処理を組み合わせて、相関のあるパルスから安全な鍵を生成する手法の原理実証を進めた。

課題３：QKD プラットフォームのアプリケーションの研究開発

将来の安全性脅威に怯えることなく長期にわたって伝送・保存・処理できるストレージネットワークにおいて、分散したデータ（シェア）を定期的に更新する際、シェアサーバ間で相互に改竄を検知できる認証機能を実装した分散ストレージネットワークの試験システムを構築し基本機能の検証を行った。また IPsec 、TLS、及びレイヤ２回線への鍵供給インターフェースを開発した。さらに QKD の要素技術を用いて生成した暗号鍵を NICT が有する研究開発テストベッド（JGN）上に設置した IPsec およびレイヤ２の回線暗号装置に供給し、広域分散バックアップシステムとしての機能実証を進めた。

秘匿ドローン通信技術ではデータ欠損の検知と効率的な鍵同期フレーム構造を開発し、これをドローンにより撮影した動画データの完全秘匿中継技術へ実装し屋内外で実証実験を行った。また、公開鍵暗号と共通鍵暗号の組み合わせから成る Transport Layer Security（TLS）ソフトウェアの高セキュリティ版モジュールを新たに用意し，これを鍵授受のインターフェースに実装した鍵供給システムを構築した。

また、物理乱数発生器を装置実装する際に生じる乱数性の偏りを取り除き、乱数性を高める技術として NICT が独自に開発した物理乱数蒸留手法（特願 2017-039437）を熱雑音を用いた物理乱数源からの乱数蒸留時に適用し、乱数生成を行った。

光空間リンク上での物理レイヤ暗号技術に関しては、物理乱数源からの乱数を 10MHz の繰り返しレートで 8km 伝送させ、送受信間でのクロック同期、フレーム同期を実証し、送受信間での誤り率と大気条件との相関測定を行った。

2-2 成果

課題１：鍵管理アーキテクチャの研究開発

Tokyo QKD Network の更なる安全性向上策としてトラステッドノード内にセキュアルータを追加設置することでファイアウォールを機能させるトポロジー更改を引続き実施し、ノード外の脅威に対する堅牢性を高めた。また、QKD プラットフォームから QKD リンク網外にある鍵利用機器へ乱数データを搬送し、ユーザ認証、機器認証を共に行う事で共通鍵データを共有する鍵搬送デバイス管理システムのプロトタイプを開発した。本ソフトウェアを複数のドローンとの秘匿通信実証実験に援用する実地検証を実施した。これらの活動により得られた新たな課題、知見を実用化へ向けた改修懸案とした。

課題２：QKD 装置の評価・校正技術の研究開発

ＮＥＣの開発したデコイ BB84QKD 装置の長期安定性試験を Tokyo QKD Network 上およびＮＥＣ社内において引き続き行った。また、昨年度発見した高速 QKD 装置において普遍的に発生するデコイパルス生成時の短期的強度揺らぎが新たなサイドチャネルになりえる問題を Tokyo QKD Network 上にて検証した。この課題に対して以下の様に対応した。まず光パルスの強度の測定機器を送信側に設置し、

光パルス強度が設定値の許容幅を超える強度変調パターンを鍵蒸留時に排除する。（ＮＩＣＴ、ＮＥＣ、北大で特許出願済み：特願 2016-176364）更に、東大が発案したパルス列に対して偶数イベントと奇数イベントとを分けて鍵蒸留処理を行う手法（命名：alternate key distillation ）を組合せる。

この手法により有限長の鍵であっても強度相関のあるパルス列から安全な鍵を生成することが可能となり、その結果を npj Quantum Information 誌に論文発表した。論文化した内容を含め、各参画機関の協働でサイドチャネル攻撃対策等の安全性評価基準策定を進めた。

課題３：QKD プラットフォームのアプリケーションの研究開発

分散ストレージネットワークの開発では、長期データ保存時におけるハッキング脅威等により危殆化されるサーバ数の継時的増加に対処する機能として、秘密分散時のデータが加法準同型であることを利用し、ダミーの秘密情報の分散データを現有の分散データに加算することにより更新を行う機能を実装した。更にその加算用の分散データが元のダミーの秘密情報の分散データであることをサーバ間で相互確認できる機能も実装し、昨年度開発した情報理論的な認証機能を有するストレージネットワークと組み合わせたデモンストレーションに成功した。秘密データ復元に必要な分散データのすべてをハッキングされる前にデータ更新を行うことにより、データ漏洩の脅威を排除することに成功した。また高知医療センターと協力し、高知・大阪・名古屋・大手町・小金井に QKD の要素技術である物理乱数源と共通鍵暗号技術を組合せた分散ストレージネットワークを構築し、南海トラフ地震などの広域災害対策として、電力圏を 2 つ以上またぐ広域での高秘匿分散バックアップシステムの動作確認に成功した。

秘匿ドローン通信技術ではドローンにおける無線通信の誤り耐性向上と鍵同期の信頼性向上を実現し、真性乱数を用いたワンタイムパッド暗号による完全秘匿データ中継技術を屋外フィールド実験と屋内実験によって実証した。また、新たに構築した鍵供給システムには高セキュリティ版 TLS モジュールとグラフィカルインターフェイス，Wegman-Carter 認証に基づく相互機器認証を実装し，高い安全性、高操作性、高信頼性を兼ね備えた鍵供給を可能にした。

また、乱数性を向上させるために使用するエクストラクタを自ら生成した乱数で構成し、一定期間でエクストラクタを更新するシステムを開発した。その結果、10Mbits の自己相関がエクストラクタを更新することにより減少する傾向が確認され、乱数性向上の原理実証に成功した。

また光空間リンクでの伝送実験では受信パワー、誤り率が日照や天候等の影響により数分から数時間の長時間スケールで変動する現象を確認した。また、msec 単位の短時間スケールの中でも受信パワーの急激な変化により誤り率が上昇する現象を確認し、誤り訂正符号を実装した場合であっても残留誤りが発生する場合が有ることを見出し、その発生確率を計測した。

2-3 新たな課題など

課題１：鍵管理アーキテクチャの研究開発

量子セキュアネットワークのオープンソース化によるセキュリティ技術研究開発への活用を促進するために、セキュリティ対策改善実装を継続的に進める。また、具体的脅威、脆弱性への対策を施しながら、QKD プラットフォーム内外での実際的なアプリケーション応用例を実証実験により示し、ユー

ザ認知度向上、ユーザ適用事例開拓を推進する必要がある。また、オープンソース化に必須となる技術の一般化へ向け、標準化文書、解説書などを提示し、ユーザ啓蒙を推進すると同時に世界的な標準としての基礎確立活動も具体的に進める必要がある。

課題２：QKD 装置の評価・校正技術の研究開発

これまで明らかになったサイドチャネルへの対策、特に送信状態の特性についてのモニタ機能、変調器動作マージンの拡大のためのハードウェア対策を早急に実装し、フィールド環境での評価を進める必要がある。我々の提案したサイドチャネル対策手法を低コストで QKD 装置に実装する方法を検討する必要がある。

課題３：QKD プラットフォームのアプリケーションの研究開発

物理乱数源に関しては、QKD 装置への接続に向けて、今年度開発した原理実証系を小型化かつ高速化し、なおかつリアルタイムに乱数を生成可能な装置実装が急務となる。

３．アウトリーチ活動報告

10 月 5 日、11 月 13 日、2018 年 1 月 31 日の 3 回にわたって次世代暗号化技術（量子暗号）に関する勉強会を警察庁情報通信局の方々と中央合同庁舎（霞が関）にて開催した。量子セキュアネットワークプロジェクトからはＮＩＣＴ、北海道大学、東京大学、ＮＥＣのメンバーが参画し、量子暗号の基礎理論から実用化に向けた取り組みについて討議した。

8 月 8 月および 11 月 16 日に重要通信分野のユーザ様に向けた量子暗号に関する研修会、および意見交換会をＮＩＣＴ（小金井）にて開催した。量子暗号に関する最新の技術動向から、実機によるデモを含む各種アプリケーションの紹介を行うとともに、今後の実用化に向けた討議を行った。