

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意識社会基盤の実現

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 2 9 年度

研究開発課題名：

高速量子鍵配送技術及び安全性評価技術の研究開発

研究開発機関名：

東芝インフラシステムズ株式会社

研究開発責任者

井上 秀行

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

(1) 量子鍵配送装置の開発

東芝は2013年に、大手町ー小金井間45kmの既設ファイバを使用した実証実験を行い、平均ビットレート300kbp/sを達成している。本技術を活用し、量子鍵配送装置の開発を実施する。

平成29年度の研究においては、平成28年度に製造した能動的安定化技術の実装から、新たに開発する量子鍵配送装置2式目の部品手配、組み立て試験を実施する。また、ソフトウェア基本設計、詳細設計、製造、試験を実施する。

(2) 鍵管理アーキテクチャへの鍵供給プログラムのインタフェース設計、ロジック開発及び評価

東芝は、平成28年度に量子鍵配送装置1式目を製造した。

平成29年度の研究においては、量子鍵配送装置1式目を使用し、情報通信研究機構が運用する鍵管理エージェントへの鍵供給動作に必要なインタフェースの実装と相互接続性の評価を行う。

(3) 都市圏量子セキュアネットワークの安全性評価

東芝は、平成28年度に量子鍵配送装置1式目を製造した。

平成29年度の研究においては、研究開発した高速かつ安定動作する量子鍵配送装置を使用し、都市圏量子セキュアネットワークに実装する。実装した量子鍵配送装置の動作検証を行うとともに、過年度に実施したサイドチャネル攻撃に対する対策技術開発で得られた知見を活用し、安全性の評価技術を開発する。

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

(1) 量子鍵配送装置の開発

量子鍵配送装置2式目の部品手配、設計、製造、組み立て試験を完了した。また、ソフトウェア基本設計、詳細設計、製造、試験を完了した。

(2) 鍵管理アーキテクチャへの鍵供給プログラムのインタフェース設計、ロジック開発及び評価

量子鍵配送装置1式目を使用し、情報通信研究機構が運用する鍵管理エージェントへの鍵供給動作に必要なネットワークインタフェースの設定及びソフトウェアの動作設定を実施し、相互接続性の評価を完了した。

(3) 都市圏量子セキュアネットワークの安全性評価

量子鍵配送装置 1 式目を都市圏量子セキュアネットワークに実装した。実装した量子鍵配送装置 1 式目で記録された検証データを使用し、盗聴検知やサイドチャネル攻撃検知などの安全性評価技術を開発した。

2-2 成果

(1) 量子鍵配送装置の開発

量子鍵配送装置 2 式目の部品手配、設計、製造、組み立て試験を完了した。また、ソフトウェア基本設計、詳細設計、製造、試験を完了した。

量子鍵配送装置 2 式目の開発工程の中で、システム構成（ハードウェア構成、ソフトウェア構成）、機能構成、インタフェース（ファイル入出力）と量子鍵配送装置 1 式目と量子鍵配送装置 2 式目の同時接続のための設計結果を資料としてまとめた。

(2) 鍵管理アーキテクチャへの鍵供給プログラムのインタフェース設計、ロジック開発及び評価

量子鍵配送装置 1 式目を使用し、情報通信研究機構が運用する鍵管理エージェントへの鍵供給動作に必要なネットワークインタフェースの設定及びソフトウェアの動作設定を実施し、鍵管理エージェントへの鍵供給動作が正常に行われることを確認した。

(3) 都市圏量子セキュアネットワークの安全性評価

量子鍵配送装置 1 式目を都市圏量子セキュアネットワークに実装した。実装した量子鍵配送装置 1 式目で記録された検証データを使用し、盗聴検知やサイドチャネル攻撃検知などの安全性評価技術を開発した。

開発した安全性評価指標の妥当性を確認するため、量子鍵配送装置 1 式目で記録された数か月分の検証データを用いて分析し、気象条件等の環境変動によって盗聴検知やサイドチャネル攻撃を誤検知しないことを確認した。

2-3 新たな課題など

新たな課題は生じなかった。

3. アウトリーチ活動報告

アウトリーチ活動は実施していない。