

平成24年度研究開発成果概要書

「セキュアフォトリックネットワーク技術の研究開発」
(課題エ セキュアフォトリックネットワークアーキテクチャ)

(1) 研究開発の目的

情報の安全な共有を実現するための基盤としてのセキュアフォトリックネットワークを構築するにあたっては、安全な通信網の構築技術として、量子鍵配送ネットワーク制御技術、量子暗号安全性評価論、連続量量子鍵配送技術及びその他、最新のネットワーク理論、認証技術等の周辺関連技術を有機的に融合させ、高度化、多様化している盗聴攻撃や攪乱法に対抗可能なセキュアなネットワークアーキテクチャの研究開発を実施する必要がある。このため、量子暗号技術の安定化等の研究を進めるとともに、実際の環境における周辺関連技術との融合、動作検証等を実施し、各種研究成果を有機的に融合させセキュアなネットワークアーキテクチャとして確立する必要がある。

(2) 開発期間

平成23年度から平成27年度（5年間）

(3) 委託先企業

日本電気株式会社<幹事>
国立大学法人北海道大学

(4) 研究開発予算（百万円）

平成23年度	30（契約金額）
平成24年度	29（ 〃 ）
平成25年度	27（ 〃 ）
平成26年度	25（ 〃 ）
平成27年度	24（ 〃 ）

(5) 研究開発課題と担当

課題エ-1 ベースラインモデルの研究（日本電気株式会社）
課題エ-2 周辺関連技術の適用研究（日本電気株式会社）
課題エ-3 量子暗号技術の適用研究（国立大学法人北海道大学）
課題エ-4 環境構築／動作検証（日本電気株式会社）

(6) これまで得られた研究開発成果

		(累計) 件	(当該年度) 件
特許出願	国内出願	0	0
	外国出願	0	0
外部発表	研究論文	0	0
	その他研究発表	5	3
	プレスリリース	0	0
	展示会	0	0
	標準化提案	0	0

具体的な成果

(1) 日本電気

セキュアフォトリックネットワークのベースラインモデルを策定した。量子鍵配送装置で生成した鍵をアプリケーションレイヤーへ配送する仕組みを検討し、具体的な鍵配送インタフェースの設計を実施した。今後は、当該インタフェースを実装し、相互接続試験で実証する予定である。

気象変化及び装置周辺の温度変化が、量子鍵配送装置の鍵生成に影響を与える要因と想定されたが、気象センサーを設置し一定期間モニターした結果、気象変化が鍵生成へ大きな影響を及ぼさないことを確認した。また、赤外線サーモグラフィ装置を設置し一定期間モニターした結果、装置周辺の温度変化が鍵生成へ影響を及ぼさないことを確認した。

(2) 北海道大学

昨年度提案した量子グループ秘密分散技術と分散コンピューティング技術を用いた量子リレープロトコルの安全性を、単純に複数経路で量子リレーを行って XOR をとるプロトコルと比較した。ある確率で一つの中継点が支配されたとき鍵が奪われる確率は、本研究開発での提案プロトコルの方が小さく、優位性が示された。また、量子グループ秘密分散を用いずに QKD ベースでもほぼ同等のプロトコルが実現できることを明らかにした。

(7) 研究開発イメージ図

※別添をご参照くださいますよう、お願いいたします。