

平成25年度研究開発成果概要書

課題名 : セキュアフォトリックネットワーク技術の研究開発

採択番号 : 157ア0201

個別課題名 : 課題ア : 量子鍵配送ネットワーク制御技術

副題 :

(1) 研究開発の目的

商用環境でQKDを適用するには、この技術の信頼性と安定性を改善することが最も重要である。顧客は、高いセキュアビットレートを必要とするだけでなく、このビットレートが常に一日24時間利用可能であることも要求する。さらに、現行のQKDハードウェアは、高性能・短時間向けに実現されてきたものであり、保守がまったく不要な、または最低限で済むような長い耐用期間を保証するにはシステムの再設計も必要である。

長期的な展望を備えたQKDはセキュリティへの要求の高いICTシステムを構築する上で重要な暗号化の基礎である。現時点では、金融、医療、エネルギー、及び遠隔通信全般の産業部門において、QKDの暗号用途を開発することが重要である。今後十年間は、世界的なエネルギーの生産・分配・供給ネットワーク内で、通信技術の配備が広く普及するであろう。QKDは、企業・個人情報情報を秘匿し、不可欠なインフラをサイバー攻撃から保護する上で、極めて重要な役割を果たす。これらの応用では、これまで考慮されているコアまたはバックボーンネットワークと共に、QKDをアクセスネットワークへも拡張可能にすることが重要である。

製品化に向けたプロトタイプの開発にあたっては、実際のQKDシステムをより詳しくセキュリティ分析する必要がある。その場合、実システムと理論的プロトコルの違いに起因する実施態様固有のセキュリティホールをいくつか閉じなければならない。また、さまざまなタイプの攻撃に対するハードウェアとソフトウェアの堅牢性に関するセキュリティ上の課題を調べることも重要である。

商用基準までQKDの信頼性、安定性、及びセキュリティを高めるには、現実的な動作条件下で敷設ファイバーによりシステムをテストすることが不可欠である。近年、いくつかの実証実験—代表的なものでは2010年10月に東京で、また2008年10月にウィーンで行われた試験—が注目を集めてきたものの、実証実験数は依然として少ない。さらに、これまでの実証の大半は、数日間または数週間継続したのみであった。数か月及び数年間にわたり、現実的な条件でQKDシステムをテストし、そのデータを使って必要な改善を行うことが急務である。それと同時に、これらのテストベッドにより、QKDの顧客取り込みを推進するための貴重なマーケティングツールが得られるものと期待される。

(2) 研究開発期間

平成23年度から平成28年度（5年間）

(3) 委託先

（株）東芝

(4) 研究開発予算（契約額）

総額 375 百万円（平成 25 年度 75 百万円）

※百万円未満切り上げ

(5) 研究開発課題と担当

課題ア： 研究開発課題全体（量子鍵配送ネットワーク制御技術）

- ・課題ア-1 能動的安定化技術の開発（(株) 東芝）
- ・課題ア-3 次世代QKDシステムの開発（(株) 東芝）
- ・課題ア-4 JGN-XネットワークにおけるQKDシステムの評価（(株) 東芝）

(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	2	1
	その他研究発表	14	8
	プレスリリース	33	33
	展示会	2	1
	標準化提案	0	0

(7) 具体的な成果実施内容と成果

課題ア-1： 能動安定化機構の改良を行い、これを組み込んだ第二世代QKDシステムを完成した。

課題ア-3-1： BB84 プロトコルをベースにして、デコイ方式を採用し、効率的な基底選択を行い、有限サンプルサイズを考慮した T12 プロトコルを設計し、その特性を評価した。

課題ア-3-2： 複数の送信装置（Alice 装置）と、1つの受信装置（Bob 装置）の間で鍵配送する基礎技術を開発。の検証実験を実施し、量子アクセスネットワークの低コスト化の可能性を示した。

課題ア-4： 大手町と小金井間（45km）を結び JG-NX ネットワーク（伝送損失 14.5dB）を用いて、第二世代QKDシステムで1ヶ月以上の連続稼働を確認した。