平成 26 年度研究開発成果概要書

課題名　　：セキュアフォトニ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なく、このビットレートが常に一毎日２４時間一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一代表的なものでは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一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２７年度（５年間）

（３）実施機関

（株）東芝

（４）研究開発予算（契約額）

総額３６３百万円（平成 26 年度５８百万円）
※百万円未満切り上げ

（５）研究開発課題と担当

課題　：　量子鍵配送ネットワーク制御技術

1. 課題ア-1　能動的安定化技術の開発（(株）東芝）
2. 課題ア-3　　次世代ＱＫＤシステムの開発（(株）東芝）
3. 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）これまで得られた成果（特許出願や論文発表等）

		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	3	1
	その他研究発表	２５	9
	プレスリリース・報道	３５	2
	展示会	3	1
	標準化提案	0	0

（７）具体的な実施内容と成果

課題ア―1：　能動安定化の制御アルゴリズムを高精度化し、厳しい気象条件でもＱＫＤシステムの安定性が持続するようにした。その効果を研究室内でテストし、従来よりも安定性が向上することを確認した。

課題ア－３－１：実装攻撃と部品故障のモニタリングの課題に取組み、送信側ユニットにトロイの木馬攻撃対策を実装し、検出器にブラインディング攻撃を検出するためのモニターを導入した。ＱＫＤプロトコルを改良し、コヒーレント攻撃に対処できるようにした。第３世代プロトタイプ（Gen-Ⅲ）が完成し、今後フィールド試験等を行う。

課題ア－３－２：当該年度の開発なし。

課題ア－４：ネットワークの上位レイヤーに鍵を渡すためのアプリケーションプログラムインタフェースを設計・試験した。また前年度のフィールド試験で得られたデータに詳細な解析を加え、第３世代プロトタイプの能動安定化機構の改良に反映させた。