平成27年度研究開発成果概要書

課　題　名　：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　：次世代量子コアネットワーク及び量子アクセスネットワークの開発

（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

株式会社　東芝

（4）研究開発予算（契約額）

総額338百万円（平成27年度55百万円）
※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	５	１
	その他研究発表	３４	９
	プレスリリース・報道	３８	３
	展示会	１２	８
	標準化提案	０	０

（7）具体的な実施内容と成果

課題ア-1　能動安定化技術の開発

我々はＱＫＤの能動安定化技術実現のために重要な課題に集中的に取り組んだ。まず、ランダムな位置に明るい安定化用のパルスを挿入することによって、連続的に干渉計のフェーズ調整を行う機構を実装した。次に、改良されたＰＩＤ制御を使うために、位相および偏光のフィードバックアルゴリズムを修正した。最終的なラボでのテストでは、３０７±１４ｋｂｐｓのセキュアビットレートを確認した。これは4．7%の変動に相当し、目標としていた5%以内を達成した。

課題ア-3　次世代ＱＫＤシステムの開発

我々はポイント・ツー・ポイントを繋ぐＱＫＤプロトタイプを開発することにより、量子コアネットワークのニーズの解決に取り組んだ。また、ポイント・ツー・マルチポイントのＱＫＤプロトタイプを構築することで量子アクセスネットワークへのニーズの解決に取り組んだ。

課題ア-3-1…　量子コアネットワークの開発

課題アー１で確立した能動安定化技術に基づいて、次世代ＱＫＤシステムを開発した。最終バージョン（Ｇｅｎ ＩＩＩ）では、有限サイズの影響を考慮すると共に、サイドチャネル攻撃（例えば、トロイの木馬攻撃やＡＰＤブラインディング攻撃）への対策を備えている。さらに、重要部品についての状態モニタリングや、自動スタート機能も実装されている。

課題ア-3-2…　量子アクセスネットワークの開発

我々は、１対多のエンドポイントを結ぶ量子アクセスネットワークのプロトタイプを開発した。これは６４ユーザーまで収容可能であり、Ｎａｔｕｒｅの論文５０１，６９（５ Ｓｅｐ　２０１３）に掲載された。

課題ア-4　ＪＧＮ－ＸネットワークにおけるＱＫＤシステムの評価

我々は、ＪＧＮ－Ｘネットワーク上で評価するために、２０１３年のＧｅｎ ＩＩと２０１５年のＧｅｎ ＩＩＩの2種類のプロトタイプを開発した。最初のフィールド実験では、Ｇｅｎ ＩＩ ＱＫＤシステムにより３４日間に亘る連続動作を確認し、中間評価の目標だった１カ月のフィールドでの動作を達成した。それに続くＧｅｎ ＩＩＩ ＱＫＤシステムでは、７７日に亘る連続動作を行い、鍵消費速度が平均鍵生成速度の８０%以下という条件の下、ＱＫＤを可用性１００%で運用するという最終目標を達成した。