平成26年度「セキュアフォトニックネットワーク技術の研究開発」の研究開発目標・成果と今後の研究計画

1. 実施機関・研究開発期間・研究開発費

- 実施機関: 株式会社　東芝
- 研究開発期間: 平成23年度から平成27年度（5年間）
- 研究開発費:総額 363 百万円（平成26年度 58百万円）

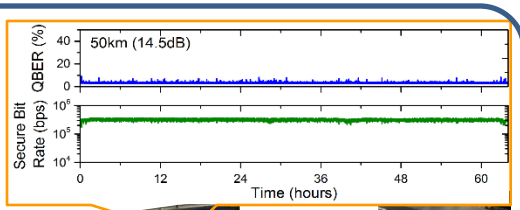
2. 研究開発の目標

- 安定で（安全なビットレートの標準偏差5%未満）、サイドチャネル攻撃に対して安全で信頼性のある（可用性= 100%）次世代QKDシステムを開発し配備する

3. 研究開発の成果

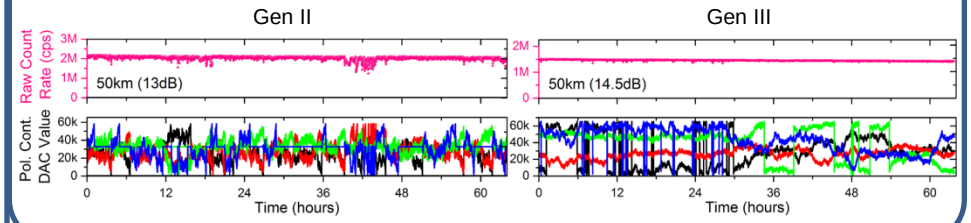
第三世代システム（Gen-III）

従来システム（Gen-II)の改良版としてGen-IIIシステム（写真）の開発を行った。これは、安定性の改善、システム故障への耐性、サイドチャネル攻撃に対する安全性という特徴を持つ。14.5dBの回線損失において、平均300kpbsの鍵配送レートと量子ビット誤り率3.3% を達成(上部の図).



能動安定化

QKDの安定性を向上するために、能動安定化システムの精度向上を行った。幾つかのフィードバック制御の再設計と改良をおこなった。具体的として、偏光を調整するために、新型のPID制御機構を開発した。これによって、従来よりも幅広い変動を補償することが可能となり（図下）、鍵ビットのカウントレートは、従来に比べてはるかに均一となった（図上）。



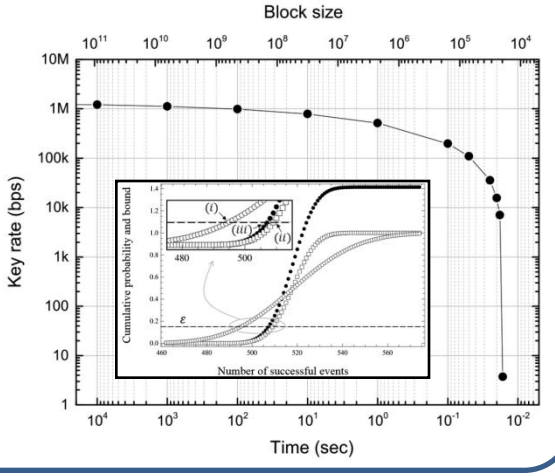
トロイの木馬攻撃対策

トロイの木馬対策ユニット

トロイの木馬攻撃による情報漏えい（最下部に図示）を、定量化し（中央の図）、対策を開発した（左上の写真）

QKD プロトコル

QKDプロトコルの改良を行い、いわゆる「コヒーレント攻撃」に対して、コンポーザブルセキュリティを保証できるようになった。これは、QKD実験に現れる異なる確率分布（右グラフに挿入された図）を関係づける新しい数学的な写像を用いたことによりもたらされた。新プロトコルは、有限長の影響に対しても性能改善効果がある（メインのグラフ）



4. これまで得られた成果（特許出願や論文発表等）　※成果数は累計件数と（ ）内の当該年度件数です。

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース	展示会	標準化提案
セキュアフォトニックネットワーク技術の研究開発	0（0）	0（0）	3（1）	25（9）	35（2）	3（1）	0（0）

5. 研究成果発表等について

（1） NICTが開催した量子ICTフォーラムにおいて、研究成果を発表し意見交換を行った

A. Dixon, M. Lucamarini, A. Plews, M. Brice, Z. Yuan, S. Tam, S. Kawamura, H. Sato, A. Shields, ***Secure Photonic Network Project --- Yearly Review Presentation ---,*** *NICT Quantum ICT Forum,* Tokyo, Japan, September, 2014

（2） 国際会議等の開催

なし

6. 今後の研究開発計画（平成27年度末）

1　研究開発課題全体（量子鍵配送ネットワーク制御技術）

安定（セキュアビットレート標準偏差＜5%）かつ安全で、信頼性の高い（可用性＝100%）次世代QKDシステムを開発及び展開する。

2　課題別

課題ア-1　能動的安定化技術の開発

QKDシステムにおける干渉計のアーム長、偏光、及び検出同期を能動的に安定させ、セキュアビットレートの標準偏差を＜5%に低減する技術を開発する（目標1）。

課題ア-3　次世代QKDシステムの開発

課題ア-3-1　量子コアネットワークの開発

実用的なセキュリティ規準を満たし、有限の鍵サイズの影響を考慮した鍵蒸留システムと、サイドチャネル攻撃に対して安全となる対策を組み込んだQKDプロトタイプを開発する。故障と自動スタート手続きに関係する重要部品をモニターする方法を導入する（目標2）

課題ア-3-2　量子アクセスネットワークの開発

量子アクセスネットワークの研究は27年度委託研究では実施しない

課題ア-4　JGN－XネットワークにおけるQKDシステムの評価

敷設ファイバーネットワークにおいて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（目標4）。