

平成24年度「セキュアフォトリ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

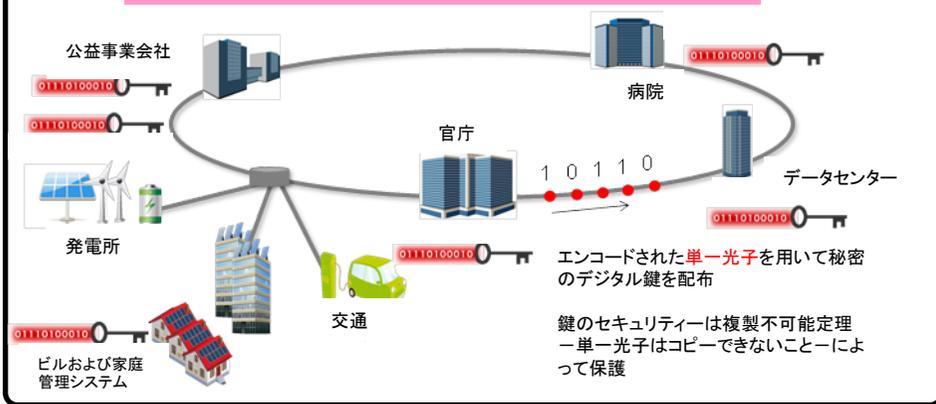
- 実施機関: 株式会社 東芝
- 研究開発期間: 平成23年度から平成28年度(5年間)
- 研究開発費: 総額 376.97 百万円(平成24年度 80 百万円)

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)、サイドチャン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。

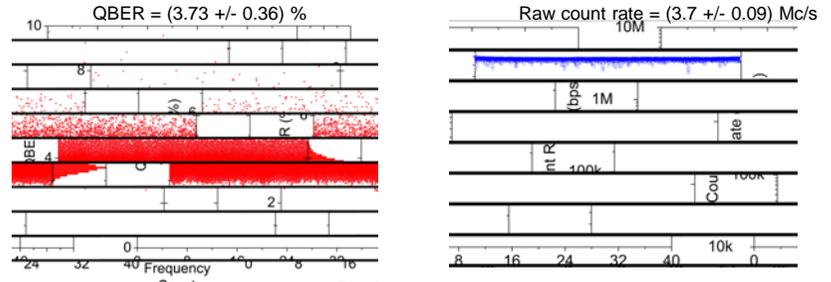
3. 研究開発の成果

(1) 量子鍵配送によってスマートコミュニティの安全性を向上



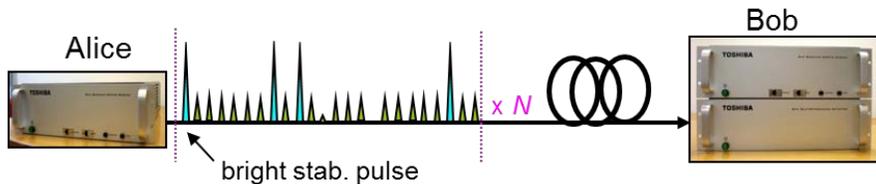
研究開発成果: 能動安定化機構の研究室レベルの試験

- » 安定化のパルス位置をランダムに変えることにより、固定位置の場合に比べて量子ビット誤り率(QBER)の変動が減少
- » 10dBを超える損失(50kmのファイバースプールを使用)において、40時間以上の安定動作を確認



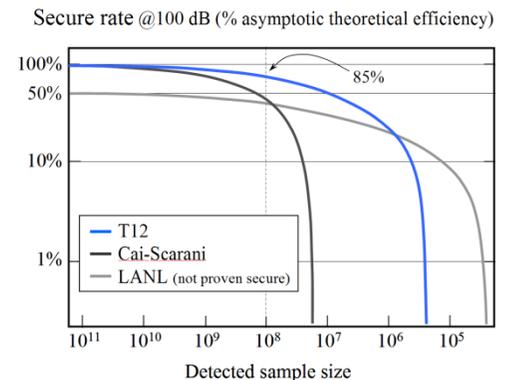
(2) 能動安定化技術

- » 明るい安定化パルスを用いた干渉計の位相の動的安定化
- » 明るいパルスは、変調パターン内でランダムに配置
- » 明るいパルスの配置は、あらかじめ共有されている鍵を用いて決定
- » 安定化パルスの生起率は1%未満であり、安全な鍵レートはほとんど低下しない



研究開発成果: T12 量子鍵配送プロトコル

- » より高速で安全なQKDプロトコルを開発!
- » 安全性を ϵ 値で定量化:
 $\epsilon=100$ dBの場合, 毎 10^2 秒、 10^8 ビットを配送するシステムは、30,000年に1度しか情報リークしない
- » 妥当なサンプルサイズにおいて、高い漸近的鍵レートパーセントを達成



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)	2 (1)	7 (6)	0 (0)	4 (1)	0 (0)

5. 研究成果発表会等の開催について

(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. Shields, M. Lucamarini, B. Frohlich, Z. Yuan, J. Dynes, H. Sato, S. Kawamura and A. Dixon, **Next Generation Quantum Key Distribution Networks**, *NICT Forum*, Tokyo, Japan, October, 2012

(2) 国際会議等の開催

なし

6. 今後の研究開発計画

課題ア 能動安定化技術の開発

安定した連続運転の基本要素として、参照パルスを用いた能動安定化技術を開発する。具体的には、単一光子と共に、ランダムに配置された強い参照パルスを送信し、その検出信号をフィードバックして光子の遅延や極性、さらにマッハ-ツェンダー干渉計の位相トラッキングを安定化する。

課題ア-3 (1) 量子コアネットワーク

平成24年度に、有限の鍵サイズの影響を考慮したT12 QKDプロトコルを開発した。このプロトコルは高い伝送レートを維持しつつ、コンポーザブルで定量的なセキュリティを担保する。平成25年度はT12プロトコルをQKDシステムに統合し、高いビットレートと高いセキュリティを達成する。またQKD構成部品のセキュリティ解析を実施し、構成部品の選択のガイドラインを設定する。特定できたセキュリティ上の欠陥に対しては、その都度対策を検討する。さらに、フィールド試験において重要と特定された部品に対して動作をモニターする機構を導入する。

課題ア-3 (2) 量子アクセスネットワーク

平成25年度は、量子アクセスネットワークの原理を実証する。最初の実験は、2つの送信機と1つの受信機を用いて光学台上で実施する。種類の異なるファイバー多重化技術を用いて比較調査を行う。

課題ア-4 次世代QKDシステムをJGN-Xで連続運転

平成24年度は、JGN-Xネットワーク上に平成25年1月に設置したQKDシステムを用いて、予備的な伝送実験を実施した。平成25年度は第二世代QKDシステムをJGN-Xネットワークで連続1カ月動作させることを目指す。さらに、構成部品の故障頻度に留意し、重要と考えられる部品に対してモニター機構の導入を検討する。