平成27年度研究開発成果概要図 （目標・成果と今後の成果展開）

採択番号：157ア0301

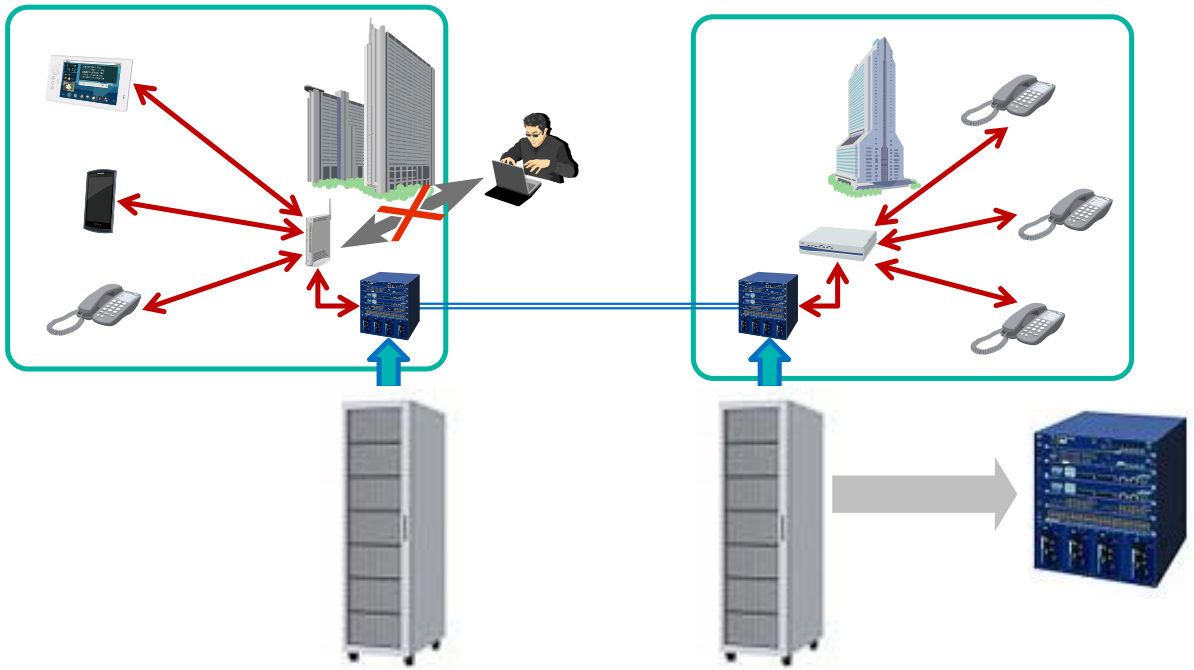
1. 研究課題・実施機関・研究開発期間・研究開発予算

◆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
◆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　　：安全な通信網の構築に向けた量子鍵配送技術の研究開発
◆実施機関　　：日本電気株式会社（幹事者）
◆研究開発期間：平成23年度から平成27年度（5年間）
◆研究開発予算：総額 426百万円（平成27年度62百万円）

2. 研究開発の目標

研究開発課題全体の目標としては、物理的安全性が理論的に保証された量子鍵配送技術をベースとして50km圏内の都市圏ファイバネットワーク上に量子鍵配送ネットワークを構築し、500kbps以上の速度で半年以上にわたって鍵を生成し続け長期運転実績を積むと共に信頼性の確立を行う。
そのため、量子鍵配送ネットワーク制御技術を実現する要件より課題ア「（1）安定化技術　（2）アプリケーションプラットフォームの拡張　（3）次世代量子鍵配送システム技術　（4）長期運用試験」の4つの技術課題を抽出し、研究開発を遂行する。

前年度は、量子鍵配送ネットワーク上での冗長化試験に向け、前年度までに開発した小型化・安定化技術を取り入れた量子鍵配送装置を試作する。また、量子鍵配送の安全性を向上するため、最新の安全性理論を適用した制御FPGAやソフトウェアを課題イと連携して開発した。これを基に平成27年度は、物理的安全性が理論的に保証された量子鍵配送技術をベースとして50km圏内の都市圏ファイバネットワーク上に量子鍵配送ネットワークを構築し、8波長の多重時に500kbps以上に相当する速度で延べ半年以上にわたって鍵を生成し続け長期運転実績を積むと共に、システムの信頼性向上のため課題エと連携して回線の冗長化を行う。



課題ア-1　安定化技術

課題ア-2　アプリケーション プラットフォームの拡張
⇒ 課題エで実運用中

課題ア-3　次世代量子鍵配送 システム技術

課題ア-4　長期運用試験

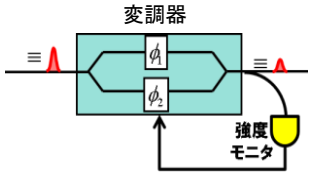
セキュアフォトニックネットワークの構築に向けた量子鍵配送技術の高性能化、安定性向上

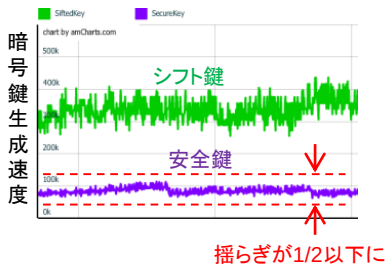
3. 研究開発の成果

課題ア−1　安定化技術

デコイパルス強度の安定化制御

- 変調器の能動的制御による揺らぎの抑制
- 安全鍵生成速度の揺らぎを1/2以下に抑制

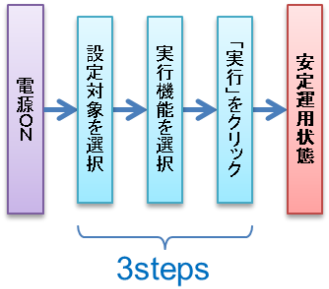




システムの一括起動

- 初期設定やパラメータ自動調整機能を統合
- Webブラウザによる3ステップの起動

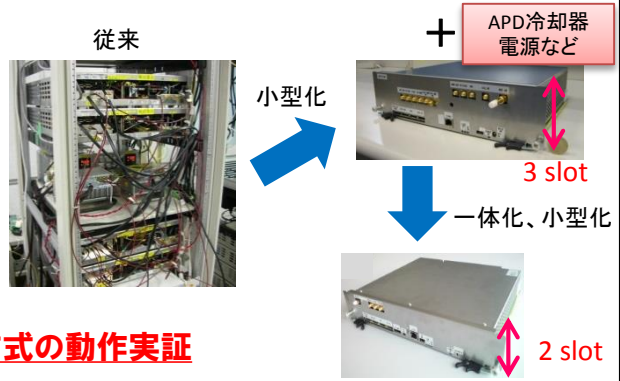
変調器、干渉計、検出器の各種安定化制御を統合したシステムにより、長期間フィールド試験を実施（課題ア−4）
⇒ 鍵生成速度の揺らぎ＜±10%を達成



課題ア−3　次世代量子鍵配送システム技術

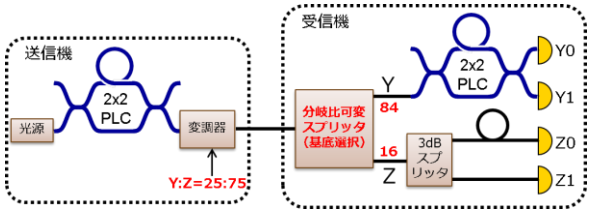
光子検出器の小型化

- APD冷却器、制御回路などの外部機器を検出回路と一体化
- 体積、消費電力ともに従来の1/3以下に
- 8波長多重時でも検出器を19inchラック2本以下に収納



光学的非対称基底選択方式の動作実証

- 基底選択を従来の50:50から非対称に
  ⇒ 基底一致の確率が向上し、鍵生成効率が30%向上
- 分岐比可変スプリッタによる動作実証



研究開発成果：安定化技術

【課題】

量子鍵配送システムを長期間にわたって運用する場合、ファイバ伝送路や装置設置場所の環境変動が安全鍵の生成速度に影響を及ぼす。この影響を抑制するため、各種パラメータの能動的安定化制御機能を開発する必要があった。
また、量子鍵配送システムの起動時には各種パラメータを最適値に調整する必要があり、システムを熟知していないユーザには負担が大きいという課題があった。

【成果】

デコイパルス強度の安定化制御

- 暗号鍵生成速度が揺らぐ原因について調査した結果、揺らぎはデコイパルスの強度と強い相関を持つことが判明した。デコイパルスを生成するための変調器の出力強度をモニタし、それを元に変調器に印加するバイアス電圧を能動的に制御することでデコイパルスの強度を安定化することができ、暗号鍵生成速度の揺らぎを1/2以下に抑制することができた。

システムの一括起動

- 量子鍵配送システムの初期設定やパラメータ自動調整機能を開発・統合し、システム起動を一括で実行するGUIを開発した。Webブラウザ上での3ステップのクリック操作により安定運用状態に到達可能とした。

⇒ 変調器、干渉計、検出器の各種安定化制御を統合したシステムにより長期間のフィールド試験を実施し（課題ア−4）、鍵生成速度の揺らぎ＜±10%を達成した。

研究開発成果：次世代量子鍵配送システム技術

【課題】

量子鍵配送のさらなる高速化のためには波長多重システムが必須となる。その際、波長多重数に比例して光子検出器の必要数が増大するため、光子検出器を小型化する必要があった。
また、オリジナルのBB84プロトコルでは2種類の基底を各々50%の確率で選択し、送受信者間で選択が一致したデータのみを利用するが、鍵生成速度を向上するためには基底選択を一方に偏らせた非対称基底選択方式として、利用できるデータ数を増加させることが有効である。

【成果】

光子検出器の小型化

- 従来、受光素子であるAPDを冷却するための冷却機構と、信号処理のための検出回路が別の筐体に分離していたが、小型冷却機構を内蔵したAPDを検出回路に組み込み1つの筐体とした。これにより光子検出器は体積・消費電力ともに1/3以下に小型化された。さらに、光子検出器を構成する冷却器や電源などの外部装置は全てATCAシャーシに収納され、安定性・可用性・操作性が大幅に向上した。8波長多重時にも光子検出器をラック2本に収容可能となった。
- 小型光子検出器単体で62.5kbps(8波多重時500kbps)以上を達成。

光学的非対称基底選択方式の動作実証

- 基底選択の割合を非対称とした方式に適応した制御ソフトウェアおよびFPGAを開発した。受信機における基底選択には分岐比可変スプリッタを使用して動作実証を行った。これにより鍵生成効率が30%向上した（目標値30%）。

課題ア-4　長期運用試験

光ネットワークテストベッド上での量子鍵配送システム連続運転

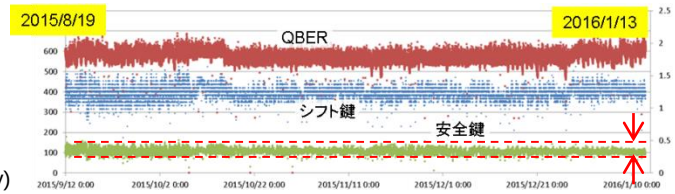
・NICT小金井～NEC府中（2波長WDM）
30日間

QBER: 1.70%
シフト鍵生成速度（2波長）: 483.3 kbps
安全鍵生成速度（2波長）: 112.4 kbps (w/ decoy)
229.8 kbps (w/o decoy)

・サイバーセキュリティ・ファクトリー 21週間

サイバーセキュリティ・ファクトリー
（NECのサイバーセキュリティ対策の中核拠点）

送信機　受信機



揺らぎ±8.6%
（目標＜±10%）

・連続運転試験 結果一覧

No.	期間	条件	特性		
			QBER [%]	Sifted key [kbps]	Secure key [kbps]
1	'12/9/29-30 24時間	2波長 APD、SSPD	APD 2.02 SSPD 2.49	APD 324 SSPD 279	APD 116 SSPD 92
2	'12/12/7-18 10日	1波長 APD	2.2	280	100
3	'12/12/28-'13/1/11 2週間	1波長 APD	2.2	320	110
4	'13/2/6-12 5日間	2波長 3 slot 検出器	1.93	441	203
5	'13/4/26-5/27 1ヶ月	2波長 3 slot 検出器	1.70	483.3	229.8 112.4 †
6	'14/12/26-'15/1/26 1ヶ月	1波長 50 km Spool 2 slot 検出器	2.1	440	90*
7	'15/3/4-27 23日間	1波長 小金井～府中	2.0	240	50*
8	'15/7/17-8/20 1ヶ月	2波長 小金井～府中	3.0	550	140*
9	'15/8/19-'16/1/13 21週間	サイバーセキュリティファクトリ	1.79	393.2	107.7*

† w/ decoy (estimated), * w/ decoy

研究開発成果：長期運用試験

【課題】
量子鍵配送システムの信頼性を確立するためには、実運用に近い環境で長期間にわたる特性評価試験を行う必要がある。伝送路をフィールド敷設ファイバとした場合や、装置の設置場所を実験室ではなく一般的なサーバ室やオフィス環境とした場合の長期間試験を行い、運用実績を蓄積する。

【成果】
光ネットワークテストベッド上での量子鍵配送システム連続運転
- 課題ア－1で開発した能動的安定化制御を導入した2波長多重システムによる、NICT小金井～NEC府中事業場間の光ファイバ（往復22km）を用いたフィールド試験を30日間にわたって行った。その結果、平均QBER1.7%（目標＜3%）、安全鍵生成速度229.8kbps（8波長多重、15dB換算時574.5kbps。目標＞500kbps）の長期間連続安定運転を達成した。
- 単一波長での運用に特化したコンパクトなデモシステムを構築し、NECのサイバーセキュリティ対策の中核拠点であるサイバーセキュリティ・ファクトリーにおいて21週間にわたる長期間連続安定運転を行った。装置の設置場所は送信機がサーバ室、受信機が通常のオフィスであるため室温などの環境変動が大きい。それにも関わらず課題ア－1で開発した能動的安定化制御を適用することにより、デコイ法を実装した場合にも鍵生成速度の揺らぎを±8.6%（目標＜±10%）に抑制することに成功した。
- 上記の他にも長期間連続運転試験を複数回行い、延べ55週間（目標＞26週間）の運用実績を蓄積した。
- 量子鍵配送システムの運用状況をリモートで監視するためのWeb公開システムを開発し、東京QKDネットワークに組み込まれている全てのリンクをリアルタイムに監視可能とした。

追加：　実システムの安全性について(課題間連携)
- 実システムの安全性評価技術について、課題イとの連携。
- 変調器駆動信号波形の歪みなどの装置実装、実機データを課題イへ提供し、その影響の分析・対策検討を行い、課題アでその対策を実装した。

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
新世代ネットワークを支えるネットワーク仮想化基盤技術の研究開発	8 （1）	3 （1）	1 （0）	14 （2）	9 （7）	4 （3）	0 （0）

5. 研究成果発表会等の開催について

（1）国内学会等における発表

・2015年9月10日　電気情報通信学会「量子鍵配送システムにおけるデコイパルス強度の安定化方法」
・2015年9月29日　Qcrypt2015「Quantum key distribution system using wavelength-division multiplexing 」
・2015年9月30日　QCrypt2015 Lab Tour at NICT「Tokyo QKD Network Updated」

（2）情報誌掲載

主なメディア掲載
・2015年9月28日　マイナビニュース「NEC、量子暗号システムの実用化に向けた評価実験を開始」
・2015年9月29日　電波新聞「量子暗号システム　実用化へ評価実験　NECが開始」

• 6. 研究開発成果の展開・普及等に向けた計画・展望

想定市場規模を含む実用化の状況

サイバー攻撃の増加により、サイバーセキュリティ市場は今後も右肩上がりで拡大し続ける。IDC Japan(株)発表によると、国内市場は、2014-2019年CAGR4～5%で成長すると予想されている。市場拡大と共に、セキュリティ対策の高度化が進み、5年後にはQKDをはじめとする現在使われている技術よりはるかに高度な技術導入検討が進められる。

人材育成への貢献の状況

本研究に携わった人材が、研究者、エンジニアとして中心的な役割を担い、国内外機関と連携して、セキュアフォトニックネットワークの研究開発に継続的に貢献していくと考えている。

社会に対する新たな利便性提供に関する状況

本研究開発成果が基盤技術のひとつとなって、より安心・安全なICTインフラとして、社会の利便性向上に貢献することが期待される。