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」課題ア　量子鍵配送ネットワーク制御技術
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

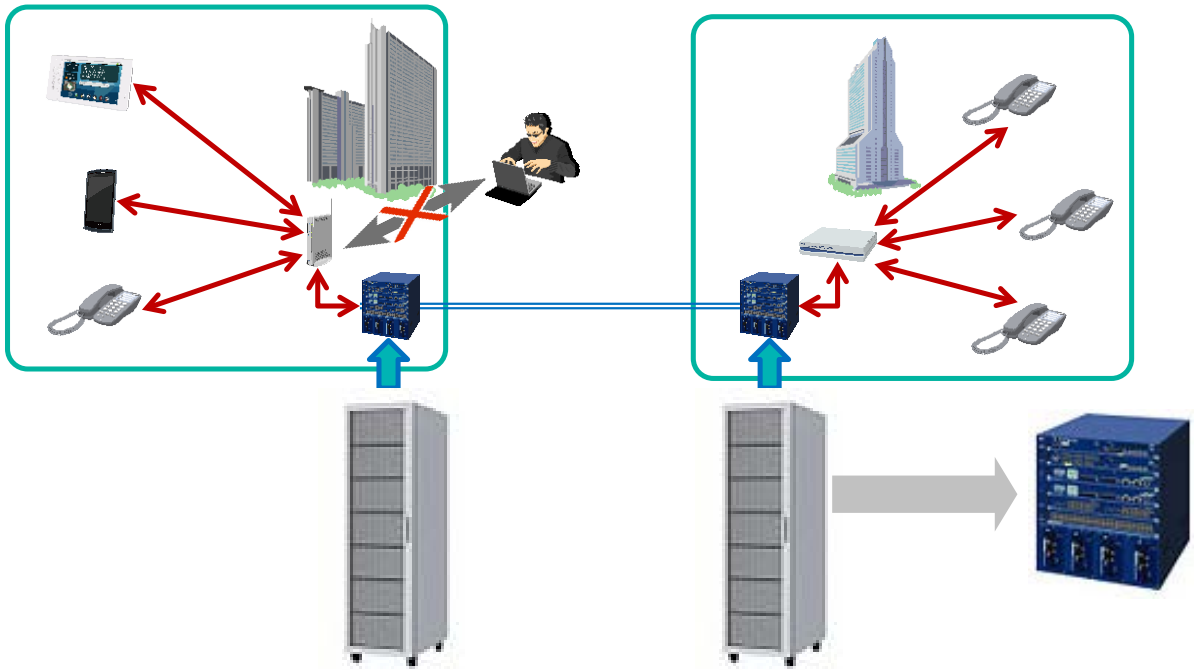
1．実施機関・研究開発期間・研究開発費

■実施機関　　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）
■研究開発費　　総額 426百万円（平成26年度83百万円）

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、量子鍵配送装置の小型化、安定化試作を完了し、暗号鍵生成状況監視システムとの連動、課題（エ）セキュアフォトニックネットワークアーキテクチャとの連携等の長期運転フェーズへの移行準備を完了した。これを基に平成26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する。



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

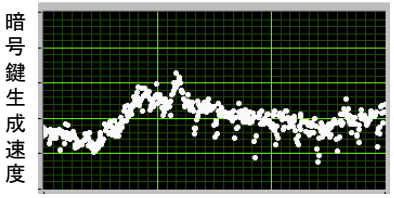
セキュアフォトニックネットワークの構築に向けた量子鍵配送技術の高性能化、安定性向上

3. 研究開発の成果

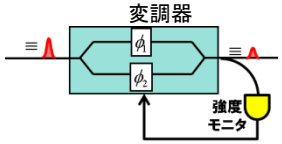
課題ア-1　安定化技術

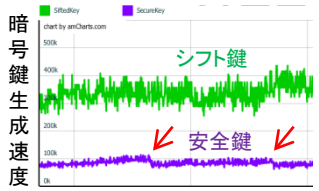
デコイパルス強度の安定化制御

・暗号鍵生成速度の揺らぎ（従来）



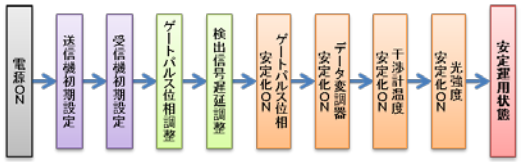
・変調器の能動的制御による揺らぎの抑制



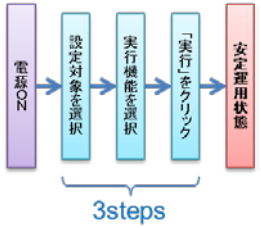


システムの一括起動

・従来の起動手順



・Webブラウザによる3ステップの起動

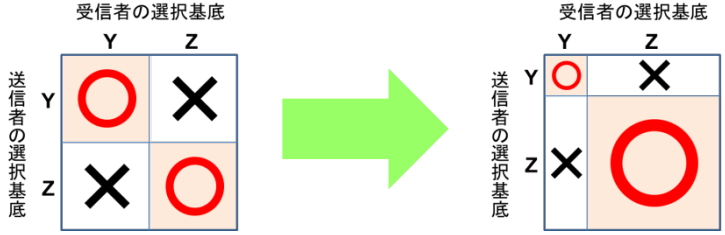


課題ア-3　次世代量子鍵配送システム技術

非対称基底選択方式による鍵蒸留

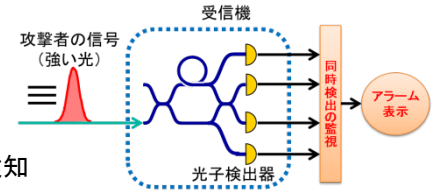
・従来の基底選択
⇒ 利用可能データ＝50%

・非対称基底選択
⇒ 利用可能データ ＞50%



明光攻撃の検知

・複数の光子検出器の同時検出を監視
⇒ 強い光を入射する攻撃を検知



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には各種パラメータの能動的安定化制御が必要であり、H25年度までに誤り率の最小化や光子検出数の最大化といった自動制御機能を開発してきた。しかし、これらの制御のみではデコイBB84プロトコルによる暗号鍵生成速度が大きく揺らぐことが課題であった。また、H25年度にシステム起動時に各種パラメータを最適値に自動調整する機能を開発したが、ユーザが調整順序を考慮した上でパラメータ毎に実行する必要があり、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。

研究開発成果：次世代量子鍵配送システム技術

【課題】

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。鍵生成速度を向上するためには基底選択を各々50%ではなく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。また、近年懸念されているサイドチャネル攻撃の1つとして、受信機に強い光を入射する明光攻撃がある。この攻撃により攻撃者は正規受信者の受信データを操作できてしまう可能性があるため、明光攻撃を検知する必要があった。

【成果】

非対称基底選択方式による鍵蒸留

- 送受信者間の選択基底が一致する確率を高めるため、2種類の基底選択の割合を50%以外にも$1/2^n$の割合に設定可能な鍵蒸留用FPGAを開発した。また、各基底における誤り率を個別に評価し、一方を誤り訂正に、他方を秘匿増強に用いる方式とし、鍵蒸留効率が向上した最新の安全性理論を適用可能とした。

明光攻撃の検知

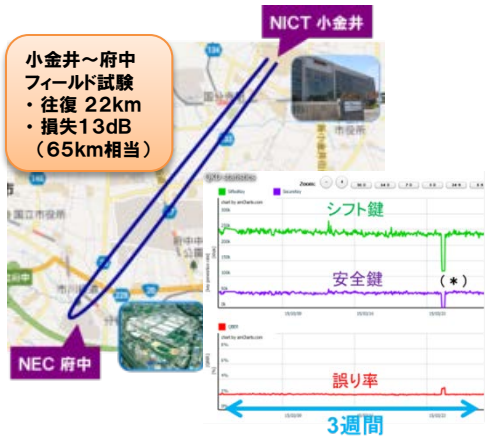
- 攻撃者が受信機に強い光を入射した場合には、複数の光子検出器から同時に検出信号が出力される。この同時検出の発生を監視して明光攻撃を検知する機能を実装した。3台以上の光子検出器で同時検出があった場合には明光攻撃の可能性が高いとしてアラームを表示する。

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

・試作システムによる
1ヶ月間連続運転試験
（50kmファイバスプール）

・デモシステムによる3週間連続運転試験
（22kmフィールドファイバ）



・長期試験結果一覧

No.	期間	条件	特性		
			QBER [%]	Sifted key [kbps]	Secure key [kbps]
1	2012/9/29-30 24時間	2波長（APD+SSPD）	APD 2.02 SSPD 2.49	APD 324 SSPD 279	APD 116 SSPD 92
2	2012/12/7-18 10日間	1波長	2.2	280	100
3	2012/12/28-2013/1/11 2週間	1波長	2.2	320	110
4	2013/2/6-12 5日間	2波長 3 slot 検出器	1.93	441	203
5	2013/4/26-5/27 1ヶ月	2波長 APD 3 slot 検出器	1.70	483.3	229.8
6	2014/12/26-2015/1/26 1ヶ月	1波長 50km スプール 2 slot 検出器	2.1	440	90
7	2015/3/4-27 23日間	1波長 (*)	2.0	240	50

（＊）装置見学対応のため一時的に設定を変更

冗長化試験に向けたデモシステムの追加構築

・冗長化試験や潜在ユーザへの
デモンストレーションに使用
・アプリケーションとして回線暗号装置を組み込み、
現代暗号への鍵供給（課題エと連携）

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。H25年度に1ヶ月間の連続運転試験を行った波長多重対応の試作システムに加え、同年度に開発したコンパクトなデモシステムを用いて1ヶ月程度の連続運転を行う。また、量子鍵配送ネットワークの信頼性を向上するためには複数の量子鍵配送システムを使用し、伝送路および装置を冗長化することが必要である。

【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

- 課題アー1で開発した安定化制御を導入し、長期間の連続運転試験を行った。試作システムの送受信機を50kmのファイバスプールを介して接続し、1ヶ月間の連続運転試験を行った。
また、デモシステムを使用してNICT小金井～NEC府中事業場間の光ファイバ（往復22km、損失13dB＝理想的なファイバでは65kmに相当）を用いた3週間のフィールド試験を行った。
その結果、両システムとも誤り率3%以下の長期間連続安定運転を達成した。

冗長化試験に向けたデモシステムの追加構築

- 複数の量子鍵配送システムによる冗長化試験や潜在ユーザへのデモンストレーションを行うため、1チャンネルに限定したコンパクトなデモシステムを追加構築し、既存システムと同等の特性を得た。
- 量子鍵配送のアプリケーションとして、現代暗号（AES）による暗号化通信で実績のあるレイヤー2回線暗号装置を組み込み、現代暗号への鍵供給による双方向100Mbpsの高速な暗号化通信を実現した（課題エと連携）。

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	7 （3）	2 （0）	1 （0）	13 （4）	2 （1）	0 （0）	0 （0）

5. 研究成果発表会等の開催について

（1）国内学会における発表

2014年8月1日　電子情報通信学会 光通信システム研究会OCS Summer School 2014 「単一光子量子暗号鍵配送技術」を発表
2015年1月28日　光協会フォトニックデバイス応用技術研究会「波長多重による高速量子鍵配送システムを発表」

（2）情報誌掲載

2014年11月21日　日経産業新聞『盗めば壊れる究極の暗号、「光」でも懸念「量子」に注目』掲載

6. 今後の研究開発計画

課題ア-1　安定化技術

微弱コヒーレント光を用いた波長多重量子鍵配送システムの安定化技術を確立する。

課題ア-2　アプリケーションプラットフォームの拡張

前年度に課題エの中で具体化した技術を量子鍵配送ネットワーク上で継続して運用する。

課題ア-3　次世代量子鍵配送システム技術

課題イとの連携により鍵蒸留方式を改良し、生鍵から最終鍵を抽出する効率を30%程度高めて最終鍵の生成速度を向上させる。

課題ア-4　長期運用試験

課題ア-1で確立した安定化技術を課題ア-3で開発した次世代量子鍵配送システムに活用し、フィールド環境において延べ半年以上にわたる長期連続運転を行うことを目標とする。また、システムの信頼性を向上するため、異常発生時の復旧機能を開発するとともに課題エと連携して回線の冗長化を行う。