平成23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

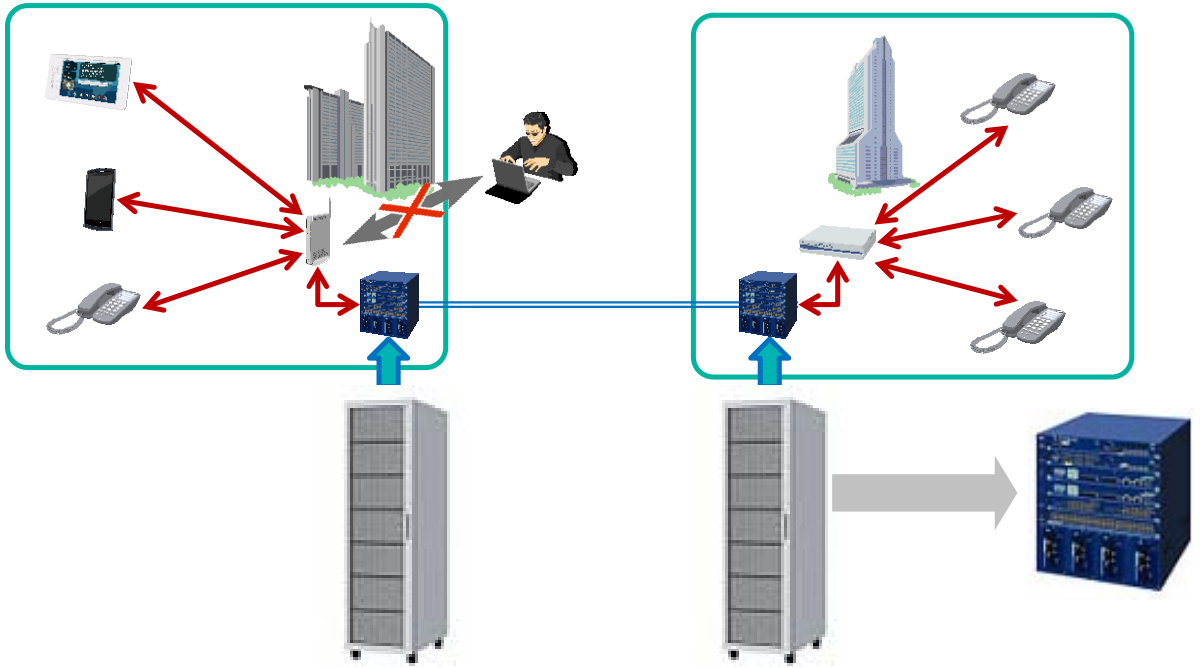
1．実施機関・研究開発期間・研究開発費

■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 438百万円（平成23年度100百万円）

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。

平成23年度の目標としては、量子鍵配送装置の安定化・小型化に向け、現状装置の課題、対策を明らかにする。さらに長期運転性能の特性公開に備えて、公開システムの概要設計を完了する。



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

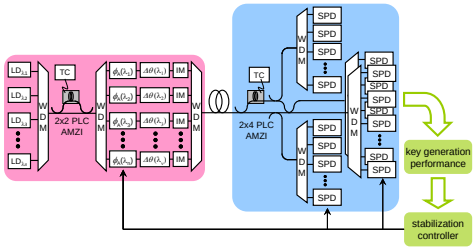
課題ア-4　長期運用試験

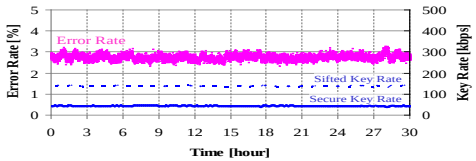
セキュアフォトニックネットワークの構築に向けた量子鍵配送技術の高性能化、安定性向上

3. 研究開発の成果

課題ア-1　安定化技術

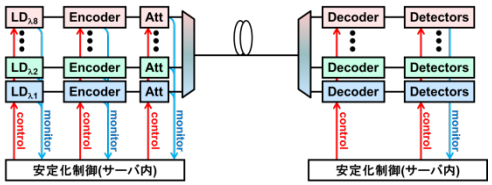
鍵生成特性変動要因の解析





環境温度の変動が光子検出タイミングなどに与える影響について調査。
また、その影響を抑制するソフトウェアに関して基本動作の検証が完了。

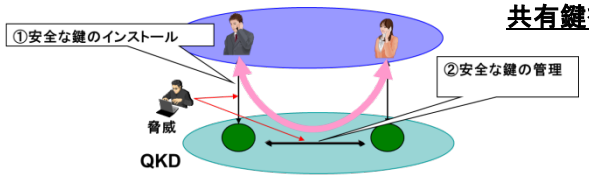
安定性向上に向けた量子鍵配送装置の部分改造試作



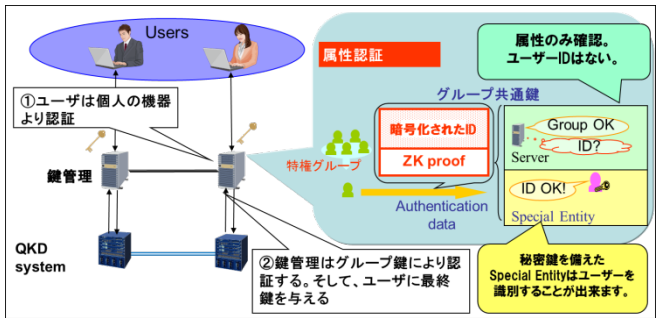
自動的に鍵生成情報を収集してパラメータ調整を行うソフトウェアを開発。
また、パラメータ調整機能の追加、クロック分配方法の改良などのハードウェア改造を実施。

課題ア-2　アプリケーションプラットフォームの拡張

共有鍵を使用できる安全なAP基盤を確立



共有鍵のIDによる管理
属性認証を用いた依頼元認証。



エンドーエンド間の安全な鍵共有機構の設計

鍵管理サーバによる鍵払い出しプロトコルの設計と鍵IDと許可書に用いた暗号データ送受信プロトコルの設計。

研究開発成果：安定化技術

【課題】長時間にわたって量子鍵配送システムの連続運転を行った場合、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問題を解決するため、鍵生成特性変動の要因を特定し、その影響を抑制する安定化機能を開発し、安定な鍵生成を実現。

【成果】

鍵生成特性変動要因の解析

- 恒温槽内に設置した50kmのファイバを伝送路とし、ファイバの環境温度を0℃～50℃で変化させた場合の量子鍵配送システムへの影響を評価。その結果、量子信号光とクロック光を波長多重により同一ファイバで伝送している場合でもファイバ長の伸縮により両者の到着時刻にはずれが生じ、光子検出のタイミングに数十psの調整が必要であることが判明。
  この影響を抑制するための安定化ソフトウェア（後述）を開発し、基本動作の検証を完了。
- 恒温槽内に干渉計を設置し、その環境温度を10℃～40℃で変化させた場合の量子鍵配送システムへの影響を評価。その結果、干渉計が温度安定化されていた場合にも誤り率が10%程度まで上昇することが判明。この影響を抑制する機能についてはH24年度に開発予定。

安定性向上に向けた量子鍵配送装置の部分改造試作

- 自動的に鍵生成情報を収集し、その結果に応じて光子検出のタイミングや変調器のバイアス電圧などのパラメータ調整を行うソフトウェアを開発・実装し、基本動作の検証を完了。
- 量子光基板およびその制御FPGAにパラメータ調整機能を追加し、環境変動があった場合にも外部からの制御が可能となるように改造を実施。
- 基板上のクロック信号の分配方法やタイミング調整方法を改良し、長期間動作時にも安定してデータを供給できるように改造を実施。

研究開発成果：アプリケーションプラットフォームの拡張

【課題】量子鍵配送を用いて安全に共有できた鍵を、アプリケーションで利用する際に安全性を劣化させてはならないという課題を解決するため、共有された鍵の安全な管理と、適切な機器に鍵を安全にインストールすることを可能にするアプリケーション基盤を確立。

【成果】

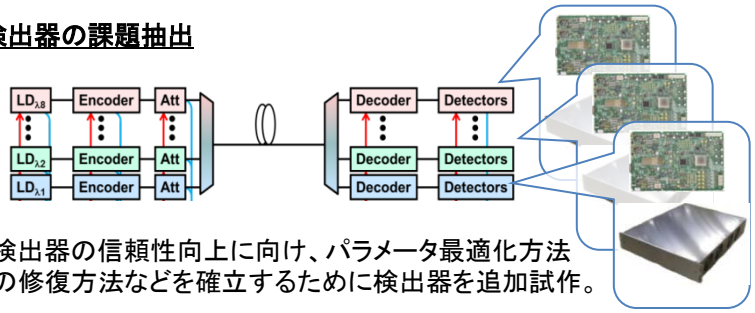
エンドーエンド間の安全な鍵共有機構の設計

- 課題エから提供される課題から、アプリケーションインタフェースとして対応すべきと判断する課題を抽出（データセンタのバックアップ時における2拠点の安全な鍵連携手法、鍵払い出しにおける依頼元認証等）。抽出課題から既存の周辺関連技術を含めて基本的対応策を検討。
  具体的には量子鍵配送を用いて共有できた鍵にIDを付与し、両端で管理し連携することと、属性認証技術を用いた依頼元認証を実施し、認証された依頼元には鍵と鍵IDを送付することを基本的な対応策として考案。
- エンドーエンド間の安全な鍵共有を実現する機構を設計。具体的には上記基本的な対応策を埋め込み、下記のプロトコルを設計。
  -（送信側）鍵払い出し依頼
    鍵管理サーバは、依頼元の属性認証を実施し、鍵と鍵IDを許可書付きで送付
  -(送信側)暗号データ送信
    送信側は、受信した鍵でﾊﾞｯｸｱｯﾌﾟﾃﾞｰﾀを暗号化、受信側に鍵IDと許可書と暗号ﾃﾞｰﾀを送付
  -(受信側)鍵提供依頼
    受信側は、鍵IDと暗号データを受信し鍵管理サーバに鍵IDと許可書を提示。対応する鍵の提供を依頼。鍵管理サーバは許可書に基づき鍵IDと依頼元の属性認証を実施し鍵を提供
  -(受信側)暗号データ復号
    受信側は提供された鍵を用いて暗号データを復号

3. 研究開発の成果

課題ア-3　次世代量子鍵配送システム技術

半導体光子検出器の課題抽出



波長多重時の検出器の信頼性向上に向け、パラメータ最適化方法や動作不良時の修復方法などを確立するために検出器を追加試作。

小型光子検出器の開発

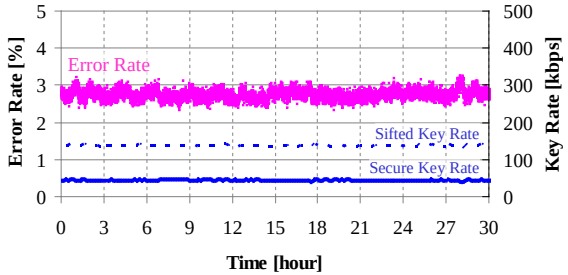
多重化のための光子検出器

高性能で小規模化した多重光子検出器

小型検出器の概要設計を完了し、検出器サイズを1/2に縮小できる見込み。

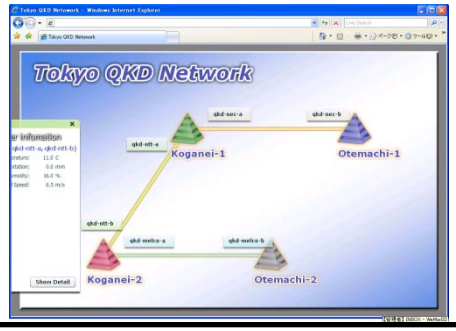
課題ア-4　長期運用試験

光ネットワークテストベッド上での量子鍵配送装置連続運転



NICT構内の光ネットワークに量子鍵配送装置を導入し、2.5日（60時間）にわたる連続運転試験を実施。

暗号鍵生成状況公開システムの開発



暗号鍵生成状況公開システムの基本動作検証を完了。

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。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、光子検出器の信頼性向上および小型化を実現。

【成果】

鍵生成特性変動要因の解析

- 光子検出器の追加試作を行い、検出器の信頼性向上のために必要な課題を抽出。具体的には各種パラメータの最適化方法や動作不良時の修復方法などを確立。
- 来年度の小型光子検出器の開発に向け、オーバースペックおよびアンダースペックの使用部品を抽出。

小型光子検出器の開発

- 「半導体光子検出器の課題抽出」において抽出された課題を踏まえ、筐体内における基板や電源の大きさ、および配置に重点を置いて検討、小型光子検出器の概要設計を完了。
- 本設計による検出器のサイズは現状の1/2であり、8波長多重時にも検出器を2ラックに収納できる見込み。

研究開発成果：長期運用試験

【課題】量子暗号装置の連続運転における暗号鍵生成性能の変化量を見積もるために長期運用試験を実施。量子鍵配送装置の長期運転実績の確立および公開のためには、量子鍵配送装置から統計情報を定期的に収集し、公開サイトに反映させるソフトウェアが必要。

【成果】

光ネットワークテストベッド上での量子鍵配送装置連続運転

- NICT構内に敷設されている光ネットワークに量子鍵配送装置を導入し、2.5日（60時間）にわたる連続運転で稼動。本評価時にはNICT内光ネットワークに50kmのファイバスプールを組み込み、実質的に50km相当の伝送距離として連続運転試験を実施。

暗号鍵生成状況公開システムの開発

- 量子鍵配送装置の長期運転実績を確立および公開するための暗号鍵生成状況公開システムに関し、ネットワーク構成などについての詳細に検討。
  その検討結果に基づいてソフトウェアの試作を行い、基本機能の動作検証を完了。

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	0 (0)	0 (0)	0 (0)	1 (1)	0 (0)	0 (0)	0 (0)

5. 研究成果発表会等の開催について
（1）光通信システム研究会

・課題ア－1，3，4：2012年1月26、27日に伊勢志摩で開催された光通信システム研究会にて、田島が口頭発表。波長多重量子鍵配送システムのフィールド実証実験に関する内容。

6. 今後の研究開発計画
この成果により、今後、どのような研究を行うのかを例示を上げながら、具体的、かつ簡潔に記載して下さい。

課題ア-1　安定化技術

·量子鍵配送装置および制御ソフトウェアに対する能動的安定化機能の追加およびその追加機能を評価するための安定性評価試験の実施

課題ア-2　アプリケーションプラットフォームの拡張

エンドーエンド間の安全な鍵共有を実現する基本アーキテクチャの詳細化と、設計の妥当性の検証。スマートフォンに対する安全な鍵配付を実現する機構の設計。

課題ア-3　次世代量子鍵配送システム技術

·小型光子検出器の試作および評価。また評価結果に基づいてさらに安定性を向上させた光子検出器の設計。

·課題ア-4　長期運用試験

·量子鍵配送システムを用いた連続運転（一週間程度）を行う。また、前年度に試作した公開用基盤ソフトウェアにより暗号鍵生成状況監視システムを構築し、量子鍵配送システムとの連携試験を行う。