平成25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」
課題エ　セキュアフォトニックネットワークアーキテクチャ
量子暗号技術を活用した安全な通信網の構築技術の研究

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）、北海道大学
■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 165百万円（平成25年度27百万円）

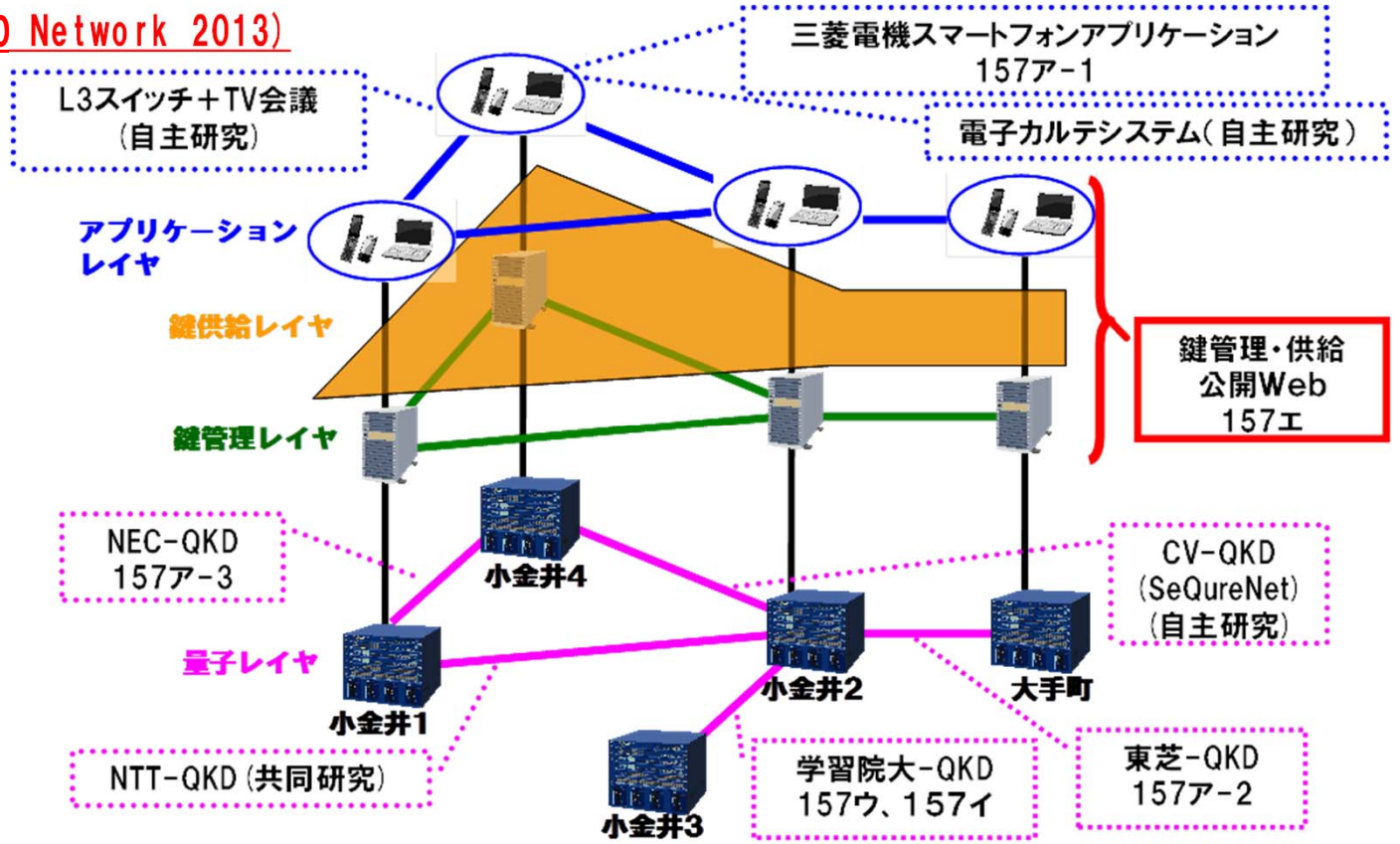
２．研究開発の目標

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エ「(1)ベースラインモデルの研究　(2)周辺関連技術の適用研究　(3)量子暗号技術の適用研究　(4)環境構築／動作検証」の4つの技術課題を抽出し、研究開発を遂行する。

平成25年度の目標は、1対1の通信モデルとして、以下の具体的利用場面を想定し、策定したアーキテクチャの実現性と妥当性を評価することである。

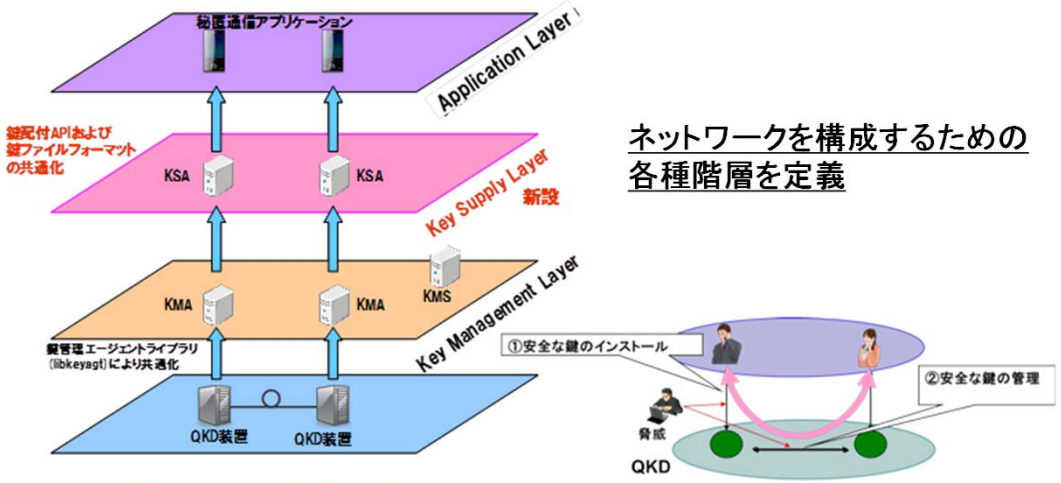
実証環境の構築（Tokyo QKD Network 2013）



3. 研究開発の成果

課題エ-1　ベースラインモデルの研究　　（日本電気株式会社）

量子暗号技術を構成する「量子鍵配送」を独立させ、QKD層として定義、併せて、鍵管理層、鍵供給層及びアプリケーション層の階層構造を考案



ネットワークを構成するための
各種階層を定義

KSA: Key Supply Agent
KMA: Key Management Agent
KMS: Key Management Server

課題エ-2　周辺関連技術の適用研究　　（日本電気株式会社）

課題ア（NEC）及び課題ア（三菱電機）との連携：
アプリケーション層への鍵供給方式の考案

配送先の端末の機種に依らず、また、配送先の端末に鍵を吸い上げるための手段を自由に選択できるようなインタフェースの設計を行った。

研究開発成果：ベースラインモデルの研究

【課題】

H23年度、H24年度に策定したベースラインモデルに、長期的安全性を提供する量子暗号と短期的安全性を提供する現代暗号の概念を追加したが、ベースラインモデルに、現代暗号との連携ができる仕組みを取り込む必要がある。

【成果】

ベースラインモデルの改善

H24年度に長期的安全性を提供する量子暗号と、短期的安全性を提供する現代暗号の概念を追加したベースラインモデルにおいて、生成された量子鍵を組み合わせて暗号鍵として量子鍵の管理や配送を行うキーマネージメントレイヤーを、鍵管理するレイヤー（新しく設定したキーマネージメントレイヤー）と、鍵を供給するレイヤー（キーサプライレイヤー）とに分離した。分離したキーサプライレイヤーに現代暗号と連携できる仕組みを取り込むことによって、アプリケーションレイヤーでワンタイムパッド用の暗号鍵として量子鍵を使用する量子暗号の部分と、安全に共有した量子鍵を共通鍵として使用する現代暗号の部分をアプリケーションレイヤーに提供できるようになった。

研究開発成果：周辺関連技術の適用研究

【課題】

H24年度に、アプリケーションレイヤーへの鍵配送に関して、汎用性の高いインタフェースの設計を実施した。周辺関連技術の評価を実施するためにはキーサプライレイヤーにも汎用性の高いインターフェイスを実装する必要がある。

【成果】

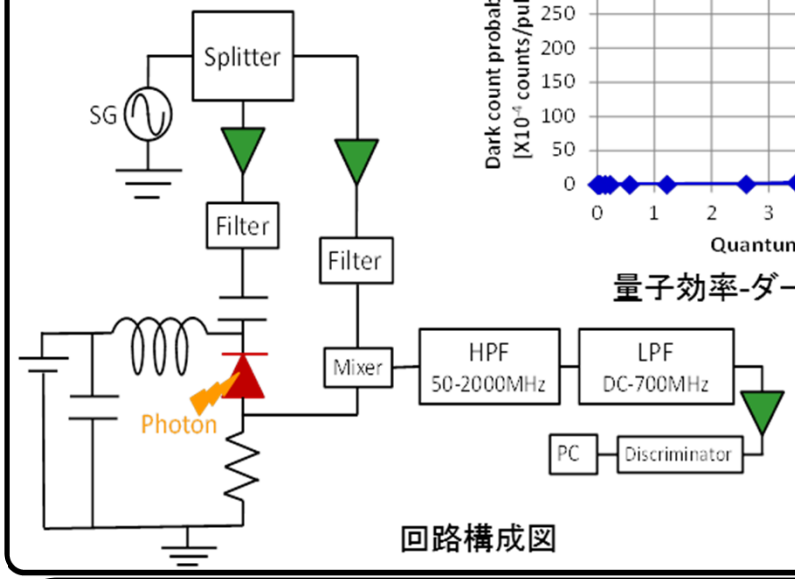
鍵供給のための汎用インターフェイスの実装

実装にあたっては、課題アで開発した三菱電機のスマートフォンアプリケーションへの鍵供給を第一の用途とするが、端末は携帯端末に限定せず、有線、無線（TCP/IPプロトコルによる通信）、USB（TCP・IP over USBによるTCP/IP通信）、FALP（FeliCa Ad-hoc Link Protocolによる通信）を実装した。USBインターフェイスを用いて三菱電機のスマートフォンアプリケーションに鍵供給を行い、セキュアフォトニックネットワークに取り込んだ。
（成果は課題エ－4の実証環境構築へ）

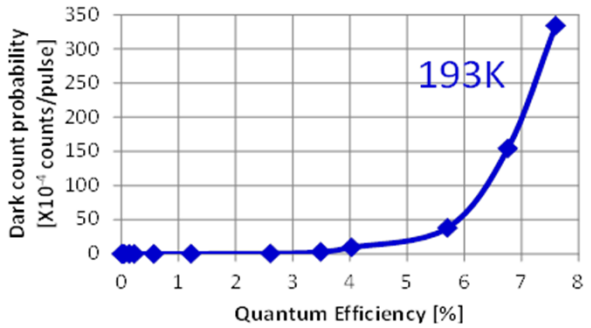
3. 研究開発の成果

課題エ-3　量子暗号技術の適用研究　（北海道大学）

光子検出器の開発



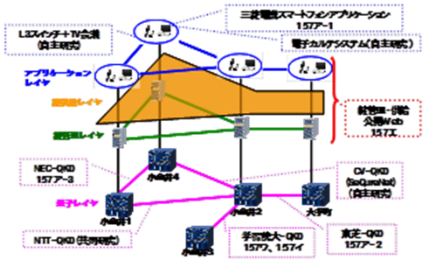
回路構成図



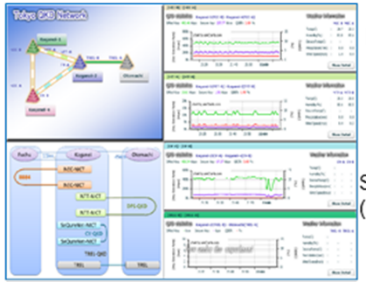
量子効率-ダークカウント特性

課題エ-4　環境構築／動作検証　（日本電気株式会社）

全課題との連携：　実証環境の構築（Tokyo　QKD　Network　2013）



課題ア（NEC）との連携：　公開サイトに反映するソフトウェアを作成

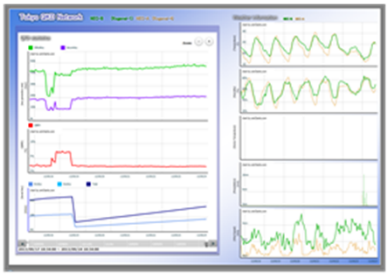


NEC

NTT

SeQureNet
(CV-QKD)

東芝



装置（鍵生成レート、QBER、鍵蓄積量）状況と環境のモニタ

研究開発成果：量子暗号技術の適用研究

【課題】

- 量子暗号装置をモニタするために光子検出器を用いることが検討されているが、現行の光子検出器は高価なAPDを用い、さらに不要信号の除去に高性能のフィルタが必要であり、また製作後の調整も必要であるため、これらを不要にした安価な光子検出器が望まれる。
- QKDでは初期乱数の共有が必要である。情報理論的に安全な初期乱数の共有法が知られているが、効率の向上が必要である。

【成果】

モニタ用光子検出器の開発

- ダブルバランスドミクサを用いる不要信号除去回路を提案した。容易に入手可能な国産APDを用いて試作し、初期的な結果としてゲート周波数1GHzにおいて、温度193 Kで量子効率4.1 %かつダークカウント率 0.001 [counts/pulse]を得た。ここで得られた特性は同種のAPDを用いたゲート周波数 62.5MHz のバランス型光子検出器のものとほぼ同等であり、1GHz 程度のゲート周波数でもこのAPDが使用できることを示した。これにより、QKD装置に組み込む安価なモニタ用光子検出器が実現可能であることが示された。

情報理論的安全な初期乱数共有

- PSMT（Perfectly Secure Message Transfer）プロトコルに量子アルゴリズムの一つであるグローバーアルゴリズムを用いることによって安全な経路を確立するためのラウンド数を低減できることが明らかになった。

研究開発成果：環境構築／動作検証

【課題】

- 課題エ－１で策定したベースラインモデルにおいて、課題エ－２、エ－３で特定した課題解決方式の妥当性を評価するため、実証環境の継続的な改善を実施する必要がある。
- 課題ア、ウで開発する量子鍵配送装置、課題アで開発したスマートフォンアプリケーションを取り込む必要がある。

【成果】

実証環境の構築

- 全課題(ア、イ、ウ、エ)の課題解決方法の実証環境を構築した。
  - ① クァンタムレイヤーに、量子鍵を生成する課題アで開発したNEC、東芝及びNICTとNTT共同研究、NICT自主研究（SeQureNet）の量子鍵配送装置、及び課題ウで開発した学習院の量子鍵配送装置を取り込んだ。（課題ア、ウの成果取込）
  - ② アプリケーションレイヤーに、課題アで開発した三菱電機のスマートフォンアプリケーション、NICT自主研究のL3スイッチ＋TV会議、電子カルテシステムを取り込んだ。（課題ア、エ－２の成果取込）
  - ③ キーマネージメントレイヤーに、①で新たに取り込んだ各量子鍵配送装置の鍵生成状況を公開サイトに反映するようにした。

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
量子暗号技術を活用した安全な通信網の構築技術の研究	1 （1）	0 （0）	0 （0）	15 （9）	1 （1）	0 （0）	0 （0）

5. 研究成果発表会等の開催について

（1）学会発表

・課題エ－３
2014年2月5日　Photonics West 2014” High-speed bridge circuit for InGaAs avalanche photodiode single-photon detector”
高速光子検出器の開発に関する口頭発表

・課題エ－４
2013年9月17日　2013年電子情報通信学会ソサイエティ大会「波長多重による高速量子鍵配送システムの長期間フィールド試験」を発表

（2）情報誌掲載

・課題エ－４
2013年4月21日　日経ヴェリタス【4/21（月）発売号】「サイバー攻撃と戦う「光の鍵」」掲載

6. 今後の研究開発計画

課題エ-1　ベースラインモデルの開発

効率的な安全鍵の管理・運用に向けて、課題ア、ウで開発される量子鍵配送装置と鍵管理システム間のインターフェイスに機能を追加することにより、量子鍵配送装置の盗聴検出、状態を把握できるセキュアフォトニックネットワークの運用面での機能向上を図る。また、セキュアフォトニックネットワークで利用されるアプリケーションとして現代暗号を利用した回線暗号装置、及びスマートフォンとの融合を図るために必要となるインターフェイスの開発及び評価を行う。

課題エ-2　周辺関連技術の適用研究

典型的なベースラインモデルで、認証、鍵の複数拠点間における効率的な伝送、共有、鍵の有効性管理を評価するために、スマートフォンによる秘匿通信及び、現代暗号を利用した回線暗号装置と量子鍵配送との融合したアプリケーションを開発及び評価を実施する。

課題エ-3　量子暗号技術の適用研究

課題アと協力して量子暗号鍵配付装置をネットワークに適合させるための装置監視方法を検討する。

課題エ-4　環境構築／動作検証

最終目標である量子暗号配送と現代暗号を融合したセキュアネットワークアーキテクチャを策定・実装して安全情報伝送の実証を行うために、課題エ－１及び課題エ－２で開発・評価を用いた適用例を開発し（情報通信研究機構所有の）ネットワークで運用しながら、課題解決方式を抽出する。