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

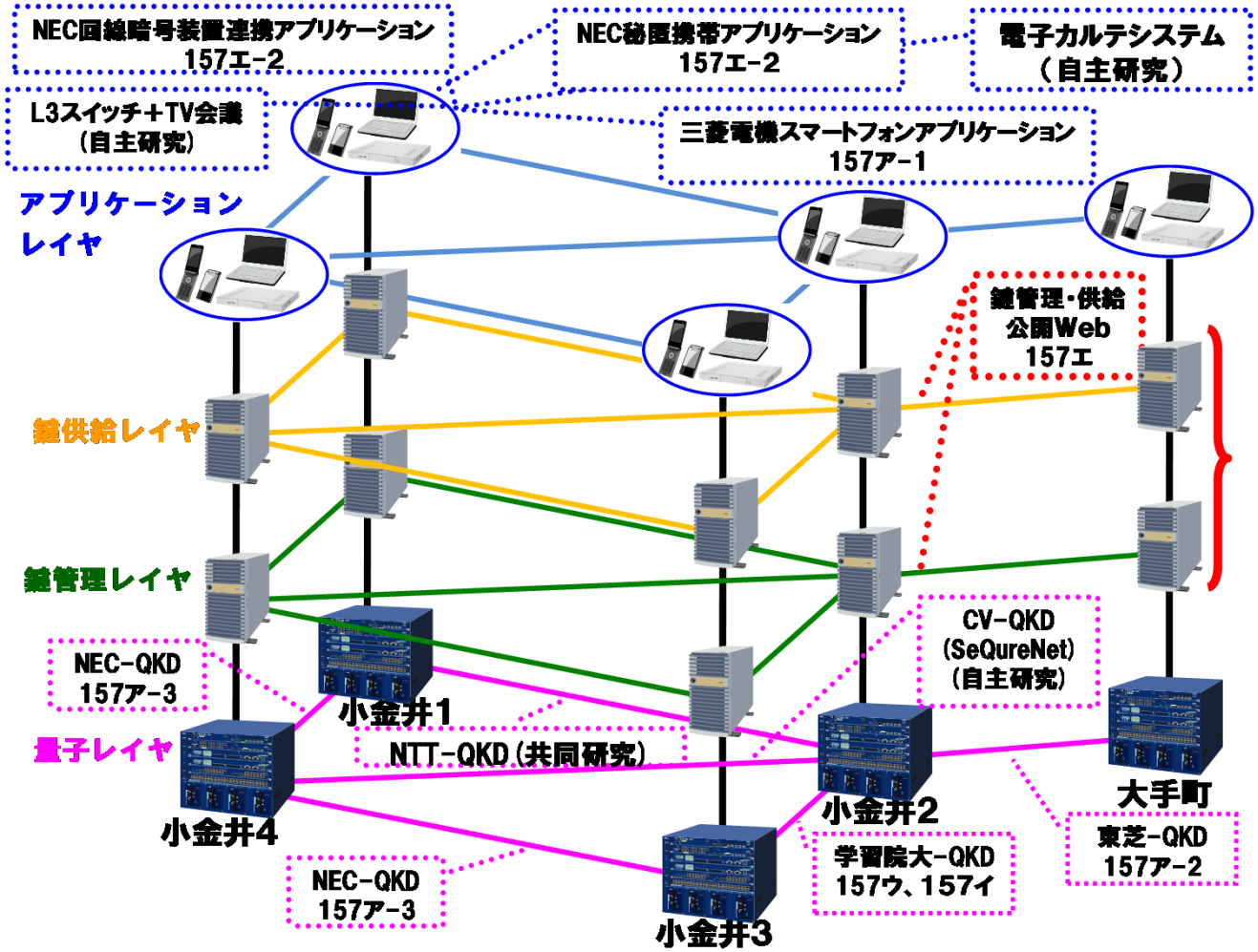
■実施機関　　日本電気株式会社（幹事者）、北海道大学
■研究開発期間　　平成23年度から平成27年度（5年間）
■研究開発費　　総額 211百万円（平成26年度58百万円）

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26年度の目標は、課題エ－1及びエ－2の成果を用いた適用例を開発し、NICT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ことである。

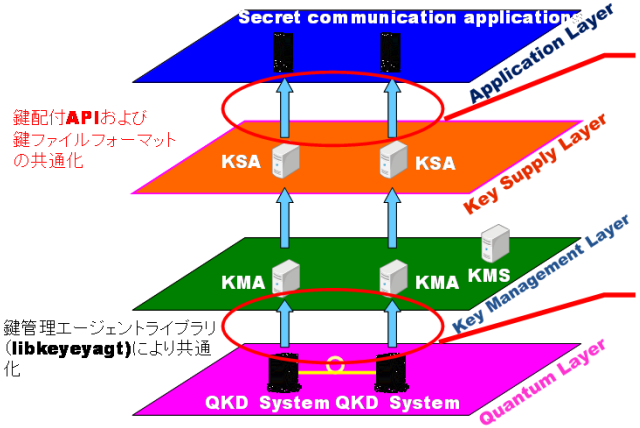


実証環境の構築（Tokyo QKD Network 2014）

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）

効率的な安全鍵の管理・運用のため、「量子鍵生成状況の把握」「盗聴検知」の機能を追加。現代暗号を利用したアプリケーション「回線暗号装置」「スマートフォン」のインタフェースを開発。



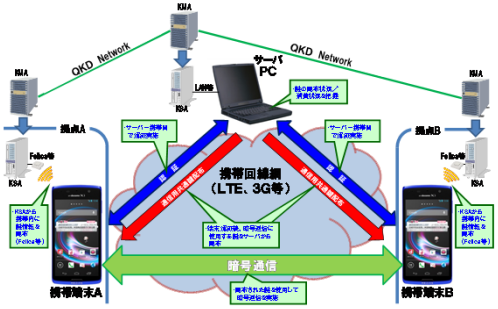
現代暗号を利用したアプリケーション
のインタフェースの開発
・回線暗号装置（エー2）
・スマートフォン（エー2）

効率的な安全鍵の管理・運用
・量子鍵生成状況の把握
・盗聴検知

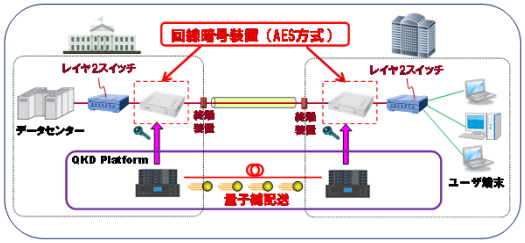
KSA: Key Supply Agent
KMA: Key Management Agent
KMS: Key Management Server

課題エ-2　周辺関連技術の適用研究　　（日本電気株式会社）

量子鍵配送と融合した現代暗号を利用したアプリケーションの開発：
・スマートフォンによる秘匿通信アプリケーション
・回線暗号装置連携アプリケーション



スマートフォンによる秘匿通信アプリケーション



回線暗号装置連携アプリケーション

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、H25年度に策定したベースラインモデルに、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、量子鍵の管理するレイヤーと量子鍵を供給するレイヤーに分離することで、量子鍵を管理・配送できる部分と量子鍵を共通鍵としてアプリケーションレイヤーに提供できる部分を個別に扱えるようになったが、効率的な安全鍵の管理・運用ができる仕組および現代暗号を利用したアプリケーションとの融合の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

QKDレイヤーで生成された量子鍵を受け取り、量子鍵を管理・配送するキーマネージメントレイヤーに、QKDレイヤーから鍵生成の情報、盗聴による鍵生成ができなくなる（盗聴検知）のインタフェースの機能を追加することにより効率的な安全鍵の管理・運用をできるようにした。また、エー2で開発する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、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フェースを開発し、課題エー4の実証環境を構築できるようにした。

研究開発成果：周辺関連技術の適用研究

【課題】

H25年度に、周辺関連技術の評価を実施するため、キーサプライレイヤーに汎用性の高いインタフェースとして、有線LAN、無線LAN（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。課題エー1で定義した典型的なベースラインモデルで、鍵の複数点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、量子鍵配送と融合した現代暗号を利用したアプリケーションを開発する必要がある。

【成果】

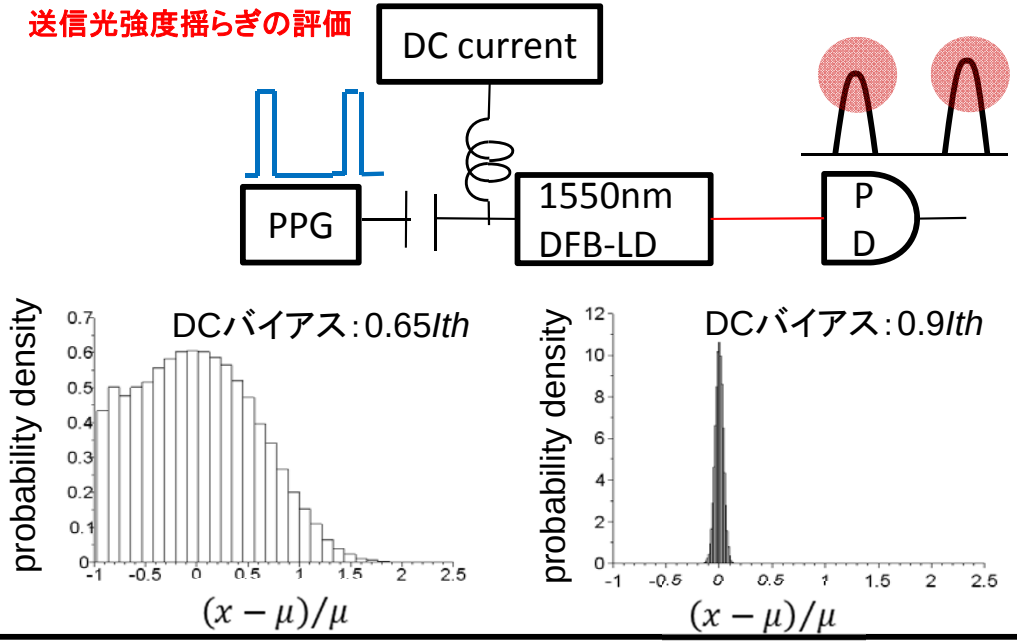
連携アプリケーションの開発

量子鍵配送との融合した現代暗号を利用したアプリケーションとして、スマートフォンによる秘匿通信アプリケーション（以下、「AP1」）、および回線暗号装置連携アプリケーション（以下、「AP2」）の2つを開発した。AP1は、キーサプライレイヤーからの鍵供給については、FALPインタフェースを実装しスマートフォンへ量子鍵を供給する。スマートフォンへ供給された量子鍵は、SIPサーバー～スマートフォン間の端末認証に用いる。量子鍵を用いた端末認証を行った上で、暗号通信で使用する暗号鍵をSIPサーバーからスマートフォンに配布する。AP2は、キーサプライレイヤーからの鍵供給については、有線LANインタフェースを実装し回線暗号装置へ量子鍵を供給する。回線暗号装置に供給された量子鍵をワークキーとして通信データをAES暗号する。この2つのアプリケーションをセキュアフォトニックネットワークに取り込んだ（成果は課題エー4の実証環境構築へ）。

3. 研究開発の成果

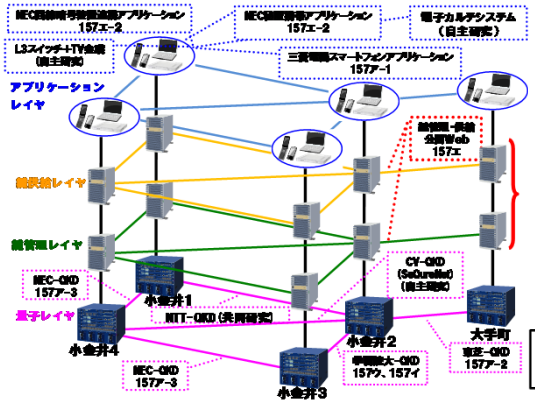
課題エ-3　量子暗号技術の適用研究　（北海道大学）

送信光強度揺らぎの評価

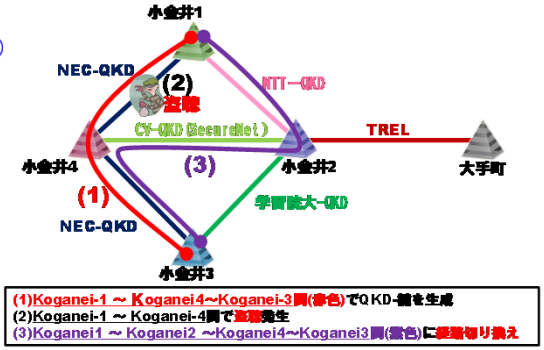


課題エ-4　環境構築／動作検証　（日本電気株式会社）

全課題との連携：実証環境の構築
（Tokyo QKD　Network 2014）



全課題との連携：動作検証
（盗聴と自動経路変更）



研究開発成果：量子暗号技術の適用研究

【課題】

・ デコイBB84プロトコルにおいては光源の強度の揺らぎがないことを仮定している。実際の装置では強度変動が起こりうるため、安全性の保証にあたっては、強度揺らぎが安全性に与える影響の解析、装置における揺らぎの大きさの評価、揺らぎの抑圧が必要である。

【成果】

量子暗号方式の適合化（半導体レーザの強度揺らぎ評価）

・ 半導体レーザの強度揺らぎを、注入電流を変えて評価した。注入するDCバイアス電流が小さい領域では発振が不安定になり、強度揺らぎが大きいことを見出した。DCバイアス、パルス電流ともに大きい方が強度揺らぎが小さくなるが、パルス間の位相相関を抑圧するためにはDCバイアスを閾値電流の90%程度に抑える必要がある。パルス電流を大きくすることで強度揺らぎを5%程度まで減少させることが可能である。

量子暗号方式の適合化（実際の装置における強度揺らぎ評価）

・ 実際の装置のテストポートを利用して、パルス毎の強度を記録するシステムを開発し、強度変動の評価を行った。強度変動の要因には上記の半導体レーザの強度変動の他に強度変調器に起因するものが考えられる。強度変調器における強度変動の要因分析を行い、変調信号波形の影響があることを見出した。

量子情報技術の活用提案

・ ダブルバランスドミクサを用いた調整不要型のAPD光子検出回路の開発を行い、フィルタによる参照信号の高純度化が信号対雑音比の向上に有効であるという知見を得た。

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、課題エ－２で開発したスマートフォンによる秘匿通信アプリケーションと回線暗号装置連携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／動作検証

・ セキュアフォトニックネットワークの安全情報伝送の実証を行うために、課題エ－１で実装した盗聴検知機能と鍵管理システムのカプセル化リレー機能を用いたセキュアフォトニックネットワークの自動切り替えを可能とする実証環境を構築した。

① 課題アで新たに開発したNECの量子鍵配送装置１式をQKDレイヤーに取り込み、トポロジーを変更した（Tokyo QKD　Network2014）（課題アの成果取込）。
② アプリケーションレイヤーに、課題エー２で開発したスマートフォンによる秘匿通信アプリケーションと回線暗号装置連携アプリケーションを取り込んだ（課題ア、エー２の成果取込）。
③ 平成２５年度に取り込んだ課題アで開発したNECの量子鍵配送装置に対し盗聴を仕掛けて検知させた際に、あらかじめ設定した迂回路に自動切り替えを行い、継続して量子鍵リレーできることを確認した。

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 （0）	0 （0）	1 （0）	22 （7）	2 （1）	1 （1）	0 （0）

5. 研究成果発表会等の開催について

（1）その他研究発表

・課題エ－３
2015年3月23日　UK-Japan Quantum Technology Workshopにて、日本における量子暗号装置開発の現状を報告、英国と日本の量子情報技術分野での協力の可能性を議論した。
・課題エ－４
2014年12月5日、2015年2月2日　某官庁向け量子暗号技術の最新動向に関する説明会の実施。
2015年3月25日　ImPACT第一回全体会議　ポスター展示　“Secure communication employing quantum key distribution ”。

（2）情報誌掲載

・課題エ－４
2014年11月21日　日経産業新聞掲載：「盗めば壊れる、究極の「量子暗号」 NEC、東芝など事業化に挑む」

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

平成26年度までの成果を踏まえ、セキュアフォトニックネットワークにおける1対1及び1対多の通信モデルを定義する。1対1の通信モデルは、100km/1Gbpsのデータバックアップセンターとの通信を想定し、1対多の通信モデルは、4点間の秘匿通信電話網を想定し、セキュアフォトニックネットワークを利用するためのベースラインを定義する。

課題エ-2　周辺関連技術の適用研究

平成26年度までの成果を踏まえ、典型的なベースラインモデルにおける課題（認証、（論理）鍵の複数拠点間における効率的な伝送と共有、鍵の有効性管理）について、これらを解決するために抽出した既存技術をネットワーク管理方式に提案し、その実効性を評価する。さらに、量子暗号技術・量子通信技術と融合してネットワーク全体として課題を解決するために必要となる周辺関連技術のカスタマイズを行う。

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の監視技術の実装を行う。また、平成25年度まで行ってきた量子もつれに関する実験をまとめ、量子もつれ光子対を用いた量子暗号プロトコルの原理実証を行う。

課題エ-4　環境構築／動作検証

昨年度までに構築してきた検証環境を活用し、課題エ-1で定義した1対1の通信モデル及び1対多の通信モデルにおいて、課題エ-2及び課題エ-3で特定した課題解決方式の妥当性を評価する。