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エ

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　：課題エ　セキュアフォトニックネットワークアーキテクチャ
◆副題　　：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
◆実施機関　　：日本電気株式会社（幹事者）、国立大学法人北海道大学
◆研究開発期間：平成２３年度から平成２７年度（５年間）
◆研究開発予算：総額　２１１百万円（平成２７年度６９百万円）

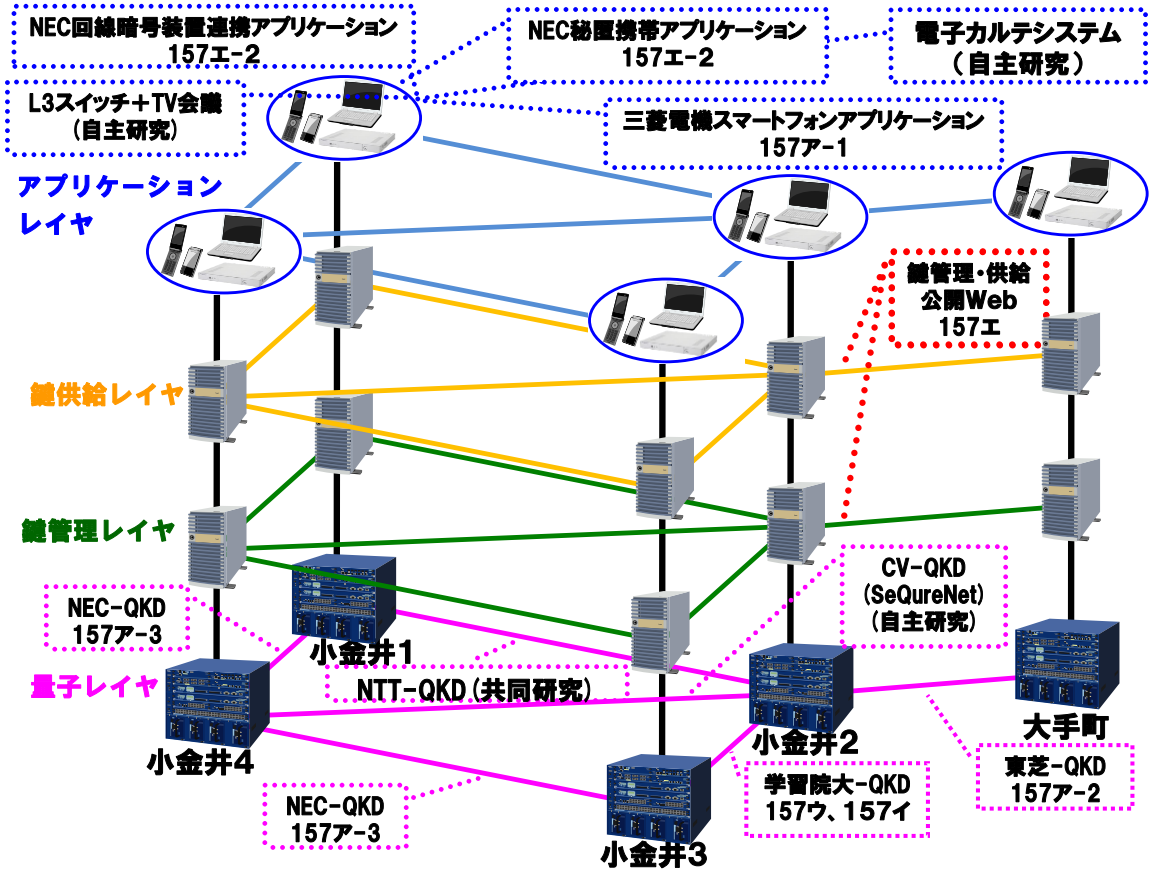
2. 研究開発の目標

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27年度の目標は、課題ア～ウで開発される技術と現代暗号方式を連動させ適応的に暗号化方式を選択することで、ニーズとコストに応じた柔軟なセキュリティサービスを提供できるセキュアフォトニックネットワークのアーキテクチャの研究開発を完了することである。

すなわち、要求条件を抽出するためのベースラインとなるネットワークモデルを研究・定義し、効率的な鍵運用のための鍵管理アーキテクチャ、現代暗号との融合方式、アプリケーションとそのインタフェース方式を開発・評価し、セキュアネットワークアーキテクチャを策定・実装して、課題ア、ウで開発する量子暗号鍵配送装置を用いて（NICT所有の）ネットワーク上での安全な情報伝送を実証する。

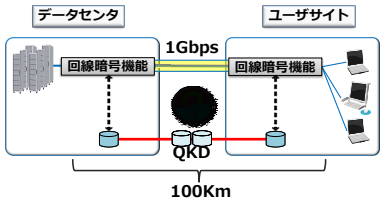


構築したセキュアフォトニックネットワーク実証環境（Tokyo QKD Network）

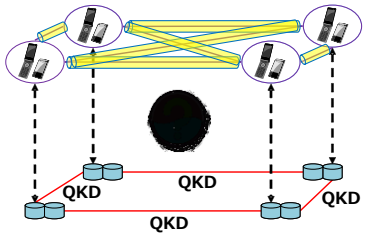
3. 研究開発の成果

課題エ-1　ベースラインモデルの研究　（日本電気株式会社）

ベースラインモデルの定義

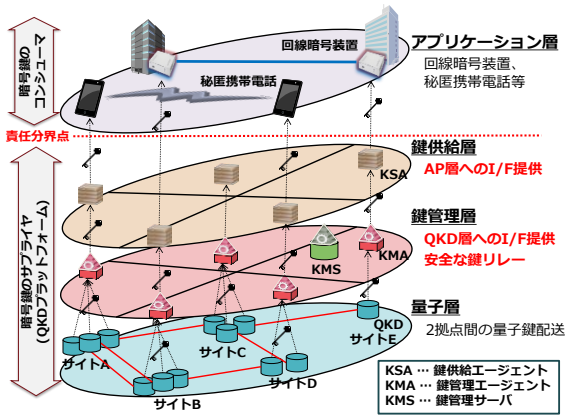


1対1の通信モデル



1対多の通信モデル

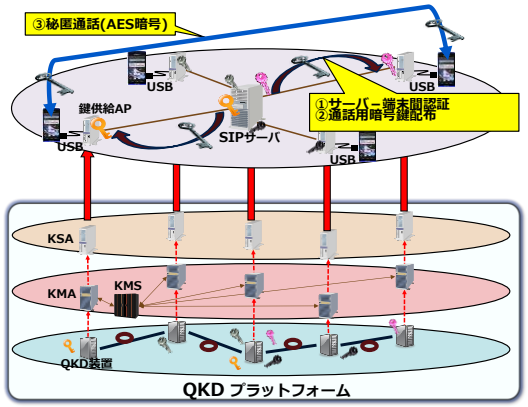
ベースラインモデルの改善



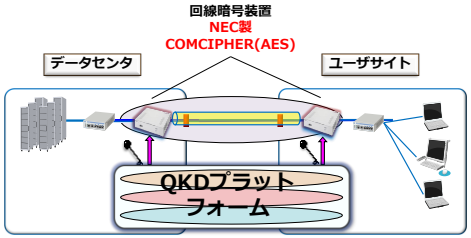
階層アーキテクチャによる
鍵配送の長距離/多拠点/冗長化対応と
多様なアプリケーション/QKD装置への対応

課題エ-2　周辺関連技術の適用研究　（日本電気株式会社）

ベースラインモデル実証のためのアプリケーション開発



スマートフォンによる秘匿通信AP



レイヤ2回線暗号装置連携AP

研究開発成果：ベースラインモデルの研究

【課題】

- 社会に資するセキュアフォトニックネットワークアーキテクチャの策定のためには、実現すべき具体的な通信モデル(ユースケース)を想定・定義し、そこから要求条件・技術課題を抽出して解決を図る必要がある(この通信モデルを「ベースラインモデル」と呼ぶ)。
- 抽出した要求条件・技術課題に対し、各種技術の適応研究(課題エ－2、3) も踏まえながら、ベースラインモデルの逐次改善によりネットワークアーキテクチャの策定を行う必要がある。

【成果】

ベースラインモデルの定義

- 社会インフラを構成する典型的通信環境として、次の2つのモデルを定義した。
  ①「1対1の通信モデル」…データバックアップセンタとの長距離大容量(100km/1Gbps)通信
  ②「1対多の通信モデル」…複数拠点(4拠点)からなる秘匿電話網

ベースラインモデルの改善

- (とくに1対1の通信モデルにおいて)暗号鍵の消費量を鑑み現代暗号の概念を導入した。
- 技術課題として、①one-time pad(以降「OTP」)暗号や現代暗号を利用する多様なアプリケーション(以降「AP」)への鍵供給、②実装方式の異なる多様なQKD装置で構成される任意拠点間の鍵共有、③ネットワーク冗長性の確保と光子伝送路での盗聴/障害への対応、を抽出した。
- 上記技術課題の解決のため、図に示す階層アーキテクチャと層間インタフェース(以下「I/F」)を定義した。量子層－鍵管理層間のI/Fには、鍵生成状況等の統計情報収集を加え、光子伝送路における盗聴/障害の検知と鍵リレー経路の切り替え(迂回)を可能とした。
- AP層より下位の層は、AP層にQKDを意識させずに安全な暗号鍵を供給するインフラとして、AP層と明確に区分し、「QKDプラットフォーム」と定義した。

研究開発成果：周辺関連技術の適用研究

【課題】

- セキュアフォトニックネットワークの課題として、認証、鍵の効率的な伝送と共有、鍵の管理が考えられ、これらを解決するための既存技術を周辺関連技術として抽出する必要がある。
- ベースラインモデルを実証するためのAPの開発が必要である。

【成果】

周辺関連技術の抽出

- QKDプラットフォーム内の鍵伝送におけるノード間の認証方式として、複数の認証方式を周辺関連技術として抽出し、Wegman-Carter認証方式を選択・実装した。
- AP層への鍵供給方式として、様々なAP端末に対応できるよう、物理I/F方式を周辺関連技術として複数抽出し、有線LAN、無線LAN、USB、FLAP(FeliCa)を選択・実装した。

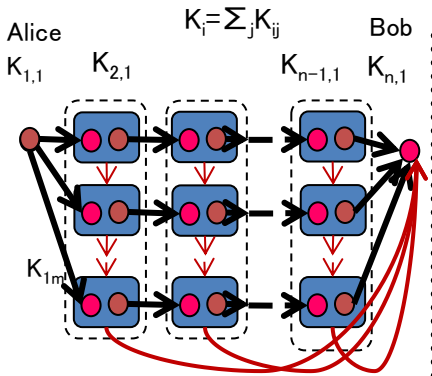
ベースラインモデル実証のためのアプリケーション開発

- 1対1の通信モデル実証のため、現代暗号を利用するレイヤ2回線暗号装置連携APを開発。
- 1対多の通信モデル実証のため、現代暗号とOTPを併用するスマートフォン秘匿通信APを開発。
- いずれも開発においては段階的なカスタマイズを行った。

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）

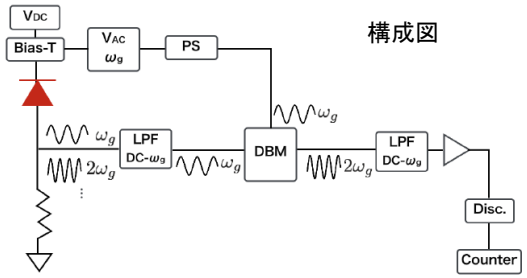
量子リレープロトコルを提案

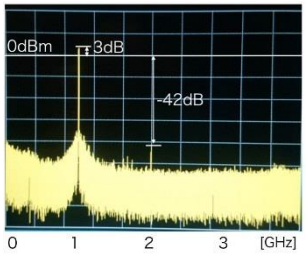


パリティを分散計算：$P_i=K_i \oplus K_{i+1}$

$\oplus_i P_i=K_1 \oplus K_n$

簡易型光子検出器を提案

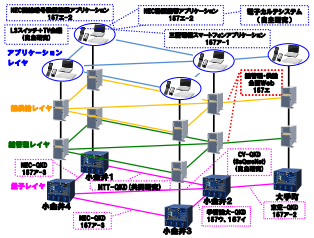




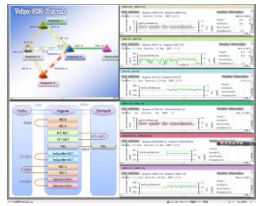
光子検出時のスペクトル

課題エ-4　環境構築／動作検証　（日本電気株式会社）

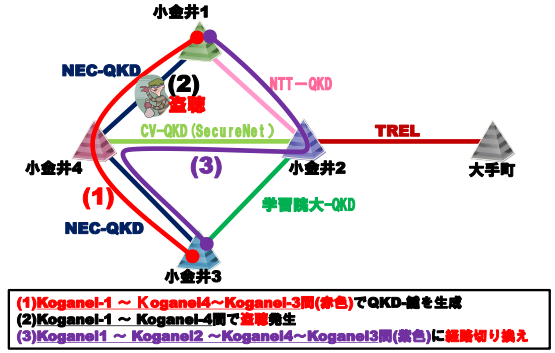
全課題の成果を融合した実証環境の構築と動作検証



実証環境(Tokyo QKD Network)



鍵生成状況監視システム



盗聴検知時の動作
（鍵リレー経路自動切換えと盗聴位置の推定）

研究開発成果：量子暗号技術の適用研究

【課題】

- セキュアフォトニックネットワークの課題として、認証、鍵の効率的な伝送と共有、鍵の管理が考えられ、これらを解決するための量子暗号技術・量子通信技術を抽出する必要がある。
- 安全情報伝送の実証を行うためには実環境での量子暗号装置の評価が必要である.

【成果】

量子情報技術の活用提案

- 量子リレーにおける課題を解決するために、量子グループ秘密分散技術と分散コンピューティング技術を用いた量子リレーのプロトコルを提案した。
- 初期鍵共有の問題を解決するために、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が低減できることが明らかにした。
- 束縛量子もつれのアクティベーションを利用したもつれ回復を検討した。また、束縛量子もつれ生成に必要な高次元量子もつれ光子対発生装置の設計製作した。
- ダブルバランスドミクサを用いた調整不要型の低価格APD光子検出回路の開発を行った。

量子暗号方式の適合化

- 実際の装置の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い、変動要因を解析した。さらに、変動の影響をおさえるソフト的な手法を提案した。
- 実機において必要な光子検出器の検出効率と暗計数の等化法を提案した。

研究開発成果：環境構築／動作検証

【課題】

- NICT所有のネットワーク上に、課題エ－１～3を通して策定したセキュアフォトニックネットワークアーキテクチャを実装し、課題エ－2で開発したアプリケーションの動作検証によりベースラインの実証を行う必要がある。
- 課題ア、ウで開発された(実装方式の異なる多様な)QKD装置を動作検証環境に組み込んで動作検証をすることで、研究開発全体として安全な情報伝達を実証する必要がある。
- 本研究開発の成果はその展開に向け、グローバルな量子暗号学術界に発信する必要がある。

【成果】

全課題の成果を融合した実証環境の構築と動作検証

- 5拠点から成る動作検証環境「Tokyo QKD Network」を構築。QKD層に、課題ア、ウで開発されたQKD装置を接続し、AP層に、エ－2で開発したAP、三菱電機(株)の成果であるスマートフォンAP、NICT自主研究の成果であるL3スイッチAP、TV会議AP、電子カルテシステムを接続し、各QKD装置、各APの動作を検証した。
- 鍵生成状況・気象・温度などをモニタするための鍵生成状況監視システム(公開Webサイト)を構築し、Tokyo QKD Networkの状態モニタとして、平成24年度から運用し続けた。
- エ－1で策定した盗聴検知機能を拡張し、盗聴/障害検知時に、鍵管理層において、鍵リレーの最適経路を自動選択して切換え、盗聴/障害の位置を推定する機能を実装・動作検証した。その中で、4拠点間(3スパン、距離合計約114km、伝送ロス合計約41dB)の鍵リレーを検証。

研究開発成果の発信

- 研究開発成果につき、2015年9月28日～10月2日に開催されたUQCC2015およびQCrypt2015において、口演発表およびデモンストレーションを実施した。

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・報道	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)	2 (0)	36 (14)	9 (7)	4 (3)	0 (0)

（1）その他研究発表

・2015年4月14日　某省庁向けに、量子暗号鍵配送技術の紹介を行った。
・2015年9月28～10月2日に開催されたUQCC/QCrypt2015において、回線暗号システムに関する発表を行い、また、盗聴検知のデモ、秘匿携帯のデモ、NICT自主研究の電子カルテシステムとの連携のデモを実施した。

（2）情報誌掲載

以下のメディアに掲載された。
・2015年7月2日：日経産業新聞「量子暗号通信、8月から実証実験　国内勢、実用化急ぐ」
・2015年9月28日：日本経済新聞「NEC、量子暗号システムの実用化に向けた評価実験をサイバーセキュリティ・ファクトリーで開始」
・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」

• 5. 研究開発成果の展開・普及等に向けた計画・展望

- 暗号鍵共有方式として現在主に使用されている公開鍵暗号方式については、量子コンピュータを用いて多項式時間で解くアルゴリズムが知られており、量子コンピュータの研究開発が進む中、米国家安全保障局は2015年8月、暗号の観点から見た量子コンピュータの脅威を述べる声明を発した。一方で、QKDは理論的に安全とされる暗号鍵共有方式であり、近年、世界各地で広域QKDネットワーク構築の計画が見られる。
- 上記状況を鑑み、将来にわたる安全な社会インフラの構築に資するべく、革新的研究開発推進プログラム(ImPACT)「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」にNICTとともに参画し、本研究開発の成果をベースとして、原理的に盗聴できない暗号鍵を様々な情報端末や制御機器に供給し、重要情報を安全に伝送する量子セキュアネットワークを都市圏に構築するための研究開発を行う(～H30年度予定)。
- また、本研究開発の成果の一部(鍵管理方式、インターフェースなど)をもとに、QKD関連技術の標準化への寄与がNICTにおいて検討されている。
- これまで実施してきた潜在ユーザ層へのヒヤリングなどについてはこれを継続し、啓蒙活動およびユーザニーズと市場の把握を図る。また、課題アと協力して開発した秘匿通信システムについて、実装の安全性などの評価を行い、本研究開発の成果である量子暗号技術と現代暗号技術の親和性向上によりユーザが必要とするセキュリティレベルに合わせたシステム提供を可能とし、実用化を図る。