平成24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 132百万円（平成24年度28百万円）

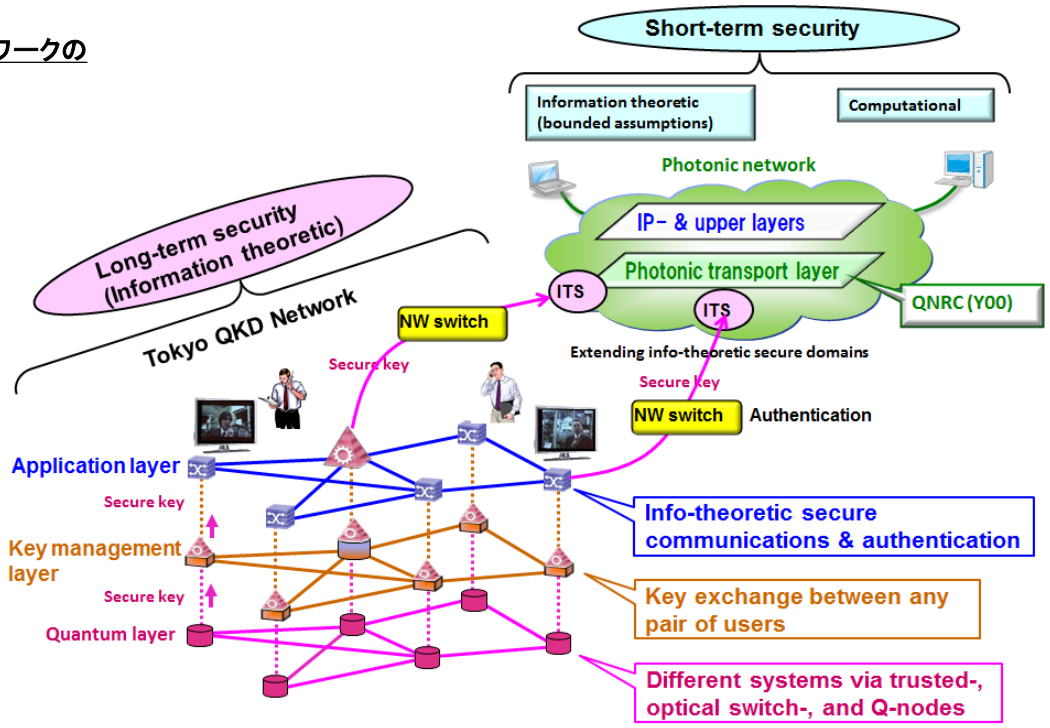
2．研究開発の目標

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。

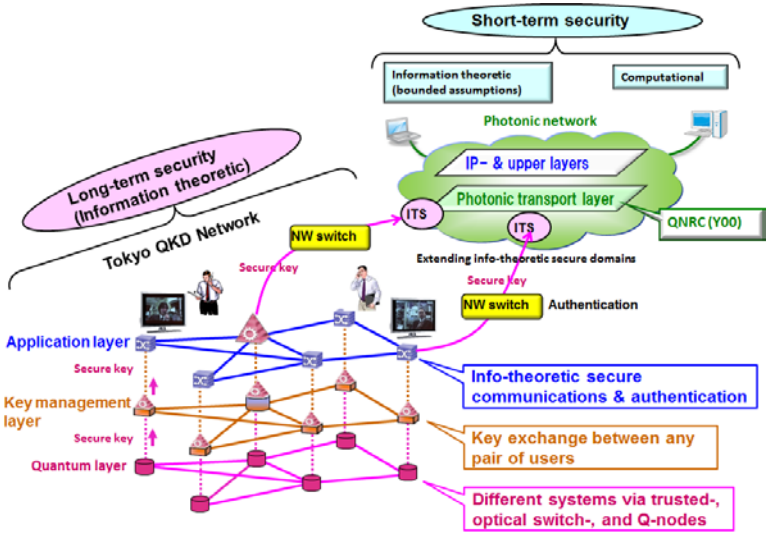
平成24年度の目標としては、前年度に定義した、社会インフラを構成する典型的な通信環境における暗号通信網の構成方式を基に、周辺関連技術の動向及び量子暗号技術の動向を反映した構成方式の改善案を提案し、各種技術の融合を考慮したモデルの定義まで完了する。

セキュアフォトニックネットワークの全体像



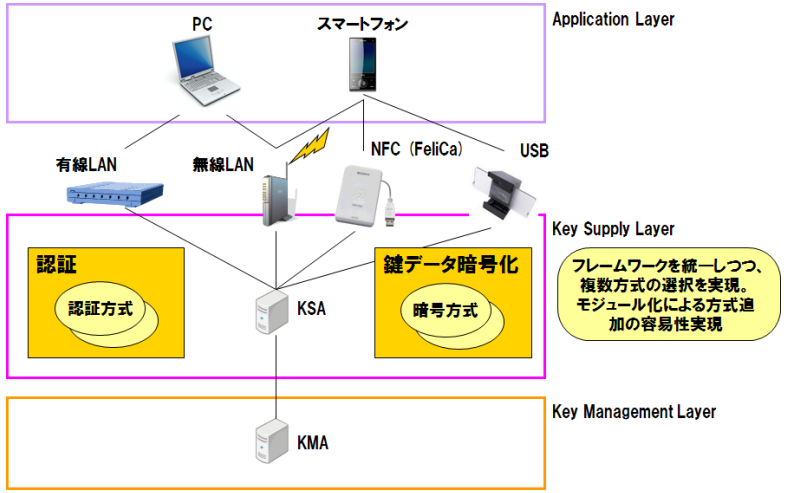
3. 研究開発の成果

課題エ-1 ベースラインモデルの研究 （日本電気株式会社）



セキュアフォトニックネットワークの全体像

課題エ-2 周辺関連技術の適用研究 （日本電気株式会社）



アプリケーションレイヤーへの鍵配送に関する方式の策定

研究開発成果：ベースラインモデルの研究

【課題】

H23年度、ベースラインモデルを策定したが、周辺関連技術の動向及び量子暗号技術の動向を反映したベースラインの改善案を策定し、全課題に提示する必要がある。

【成果】

ベースラインモデルの改善

・H23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。
・量子鍵配送装置が生成する鍵の数や生成速度には限りがあるため、アプリケーション側で鍵を使用する際は、鍵の残量を考慮した仕組みが必要であることが分かった。アプリケーションによっては生成した鍵を大量に消費することになるため、今後、鍵の消費量を局限する方策をユーザー毎に提案する必要があることが分かった。

研究開発成果：周辺関連技術の適用研究

【課題】

アプリケーションレイヤーへの鍵配送に関して、ユーザー目線の使用イメージや使い勝手を考慮した方式を策定する。また、安全な鍵配送を実現するために、鍵の配送先の正当性を確認する確実な認証方式と、鍵データの管理方式を策定する。

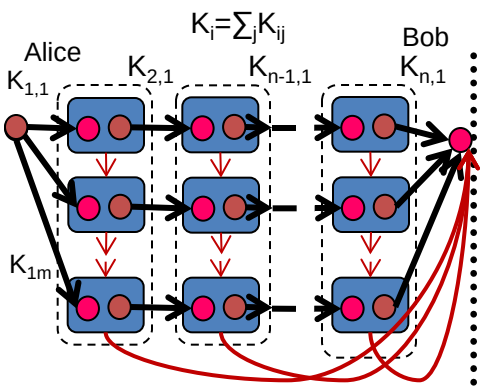
【成果】

周辺関連技術の適用研究

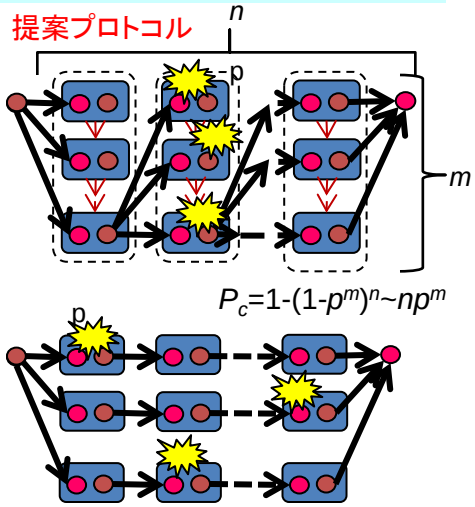
・アプリケーションレイヤーへの鍵配送に関して、汎用性の高いインタフェースの設計を実施した。具体的には、配送先の端末の機種に依らず、また、配送先の端末に鍵を吸い上げるための手段を自由に選択できるようなインタフェースの設計を実施した。
・量子暗号技術活用範囲外の経路におけるエンド-エンドの通信の安全性を匿名認証技術の適用を基準とした検討を実施した結果、匿名認証方式ではなくWegman-Carter認証方式を取り入れる方向になった。今後は、Wegman-Carter認証方式を取り入れた場合の、ネットワーク全体の安全性について検証する予定である。

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）

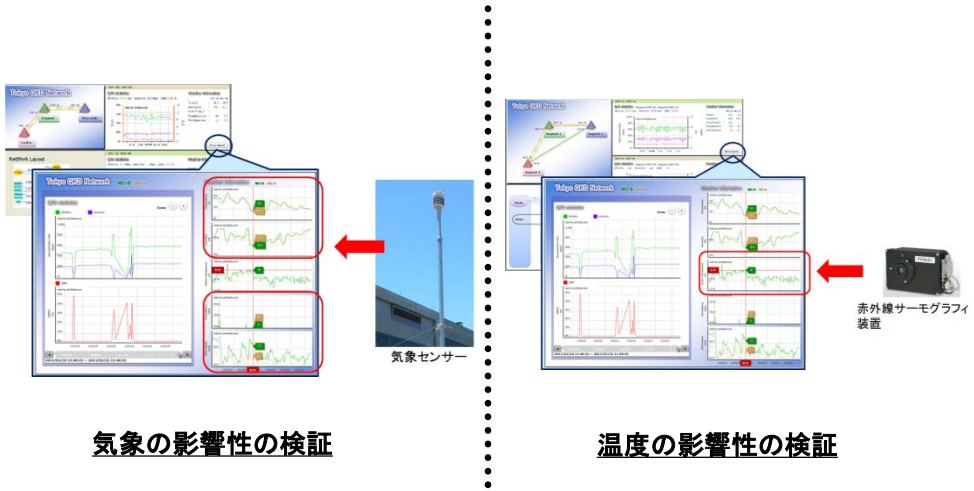


量子鍵配送ベースのプロトコル提案



類似プロトコルとの比較

課題エ-4　環境構築／動作検証　（日本電気株式会社）



気象の影響性の検証　　温度の影響性の検証

研究開発成果：量子暗号技術の適用研究

【課題】

・H23年度、量子リレーにおける課題を解決するために、抽出された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。しかし、上記提案を実施するためには他の類似した方法との優劣を明らかにする必要がある。

・H23年度提案したプロトコルは量子グループ秘密分散技術を仮定していた。この技術の安全性・実現可能性は不明確であるので、量子鍵配送を用いてそれに近いプロトコルが可能であれば、実施がより容易である。そのため、量子グループ秘密分散技術の役割を再検討し代替可能性を検討する必要がある。

【成果】

類似プロトコルとの比較

・本研究開発での提案プロトコルと、既に提案されている類似プロトコル及び単純に複数経路で得た鍵をXORするプロトコルとの比較を行った。比較は伝送損失がある場合の鍵生成効率とある確率で中継点が支配されたときに鍵が奪われる確率について行い、提案プロトコルは効率と安全性のいずれかの点で優位にあることが示された。

量子鍵配送ベースのプロトコル提案

・量子グループ秘密分散技術は中継点で分散した情報から鍵を生成する方法であるため複数の経路を用いた量子鍵配送で各中継点で共有された鍵情報を分散情報とみなすことでほぼ同等のプロトコルが実現可能であることを明らかにした。この場合、通信相手の中継点が持つ鍵情報を共有するため、量子グループ秘密分散技術を用いた場合より中継点が持つ情報が多いが、現在考えている安全性については同等と考えられる。

研究開発成果：周辺関連技術の適用研究

【課題】

全課題（ア、イ、ウ、エ）の課題解決方法の実証環境の継続的な改善を実施する必要がある。量子鍵配送装置の鍵生成に影響を与える要因として、気象変化や量子鍵配送装置表面の温度変化が想定されるため、これらの基礎データを収集する仕組みを構築し、影響を検証する必要がある。

【成果】

環境構築

全課題（ア、イ、ウ、エ）の課題解決方法の実証環境として、気象センサー及び赤外線サーモグラフィ装置を検証環境に追加した。また、気象センサー及び赤外線サーモグラフィ装置から収集した環境データを、公開サイトに反映させるソフトウェアを作成した。

動作検証

・気象センサーが収集した気象データはほぼリアルタイムで公開サイトに表示され、安定的に動作している。気象データの変化が量子鍵配送装置の鍵生成にどの程度影響しているかの検証では、現時点（H24年度3月）までは大きな影響は見られないことが分かった。

・赤外線サーモグラフィ装置が収集した温度データはほぼリアルタイムで公開サイトに表示され、安定的に動作している。赤外線サーモグラフィ装置は、NECの量子鍵配送装置（Bob側の背面）に向けて設置し、一定期間モニターした結果、装置表面の温度変化は鍵生成に大きな影響がないことが分かった。

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	0 (0)	0 (0)	0 (0)	5 (3)	0 (0)	0 (0)	0 (0)

5. 研究成果発表会等の開催について

（1）某省庁　セキュリティ製品提案

・課題エ（全般）
2012年10月19日　某省庁　セキュリティ製品報告：技術動向として、量子暗号鍵配送技術の研究についての概要を口頭説明

（2）学会発表

・課題エ-3
2012年9月4日　2nd Annual Conference on Quantum Cryptography “A Protocol of the Quantum Relay using Quantum Group Secret Sharing”を発表
2012年11月27日　第27回量子情報技術研究会 「量子グループ秘密分散を利用した量子リレープロトコル」を発表

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。

課題エ-1　ベースラインモデルの開発

1対1の通信モデルの検証において、制約事項等が発生した場合、その許容可能性を評価し、許容可能な変更をベースラインモデルに加え、ベースラインモデルを改定する。

課題エ-2　周辺関連技術の適用研究

定義された通信モデルにおいて、課題解決に必要な周辺関連技術の追加、活用方法の変更等を実施し、周辺関連技術部分の課題解決策を評価する。

課題エ-3　量子暗号技術の適用研究

定義された通信モデルにおいて、課題解決に必要な量子暗号方式の修正を提案し、妥当性を評価する。また、課題エの他分担課題と共に周辺関連技術との融合方法を検討してその結果を課題ア-ウに提案し、必要な設計変更や評価を共同で行う。さらに、量子情報技術の活用による課題解決法を提案し、想定された環境における有効性を評価する。

課題エ-4　環境構築／動作検証

課題エ-1で定義した1対1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。このため、課題ア、ウで開発する量子暗号鍵配付装置を用いた（情報通信研究機構殿所有の）ネットワークに必要な市販暗号装置等を付加した環境において、動作の検証を実施することにより、全体としての課題解決策を評価する。