平成２３年度 新規委託研究課題
「セキュアフォトニックネットワーク技術の研究開発」
研究計画書

独立行政法人
情報通信研究機構

１．研究開発課題

『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

課題イ　量子暗号安全性評価理論

課題ウ　連続量量子鍵配送技術とその応用

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

２．研究開発の目的

様々な社会活動が情報通信ネットワークへの依存性を高めている中で、情報漏洩や盗聴への対策は喫緊の課題である。情報データの中には、国家機密や個人の生命にかかわるデータなどコストをかけてでも守るべきものがあり、その範囲は科学技術の進展とともに年々増加している。また、ネットワークの急速な光化やクラウド化に伴い、光ファイバへの盗聴攻撃や制御系の撹乱など新たな安全性脅威が現れている。

量子鍵配送技術は、光通信路に対するどんな盗聴でも検知でき、配送された暗号鍵をワンタイムパッドで用いることで、理論上完全な秘匿通信を実現できる。量子鍵配送技術は、これまでの研究開発によって、敷設ファイバ 50 ㎞圏で 100kbps 程度の鍵生成速度を実現できる段階に達したが、現実的な環境下での運用実績がまだ乏しく、装置の不完全性に起因する安全性の抜け穴、いわゆるサイドチャネルやその対策も十分明らかにはなっていない。また、ネットワーク上で効率的に鍵を管理・運用する手法や、認証や署名などへのアプリケーションの拡大も今後の課題である。最終的には、量子鍵配送技術を他の光秘匿通信技術（光符号分割多重通信や量子雑音秘匿通信など）や現代暗号技術とともに、新しい光通信インフラであるフォトニックネットワーク上で統合的に運用し、種々の攻撃や脅威からネットワークを守りつつ、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ようにする必要がある。

そこで、本研究開発課題では、このような、いわゆるセキュアフォトニックネットワークの構築を目指して、量子鍵配送ネットワークの信頼性試験を進めるとともに、新しいネットワーク制御技術や安全性評価技術の研究開発を行う。また、光通信と親和性の高い連続量制御に基づく新しい実装技術の研究開発を行うとともに、セキュアフォトニックネットワークアーキテクチャの研究開発を行う。

３．採択件数、研究開発期間及び予算

研究開発期間：契約締結日から平成 27 年度までの５年間。

予算：　平成２３年度は総額３２０百万円を上限とする。

提案の予算額の調整を行った上で採択する場合がある。なお、平成２４年度以降は対前年比で６％削減した金額を上限として提案を行うこと。

本研究開発課題は、個別研究開発課題毎に公募する。

個別研究開発課題

課題ア　量子鍵配送ネットワーク制御技術

採択件数：最大３件。

予算　：平成２３年度は、総額２２０百万円を上限とする（１件当たり上限１００百万円。）

課題イ　量子暗号安全性評価理論

採択件数：１件。

予算　：平成２３年度は、総額１５百万円を上限とする。

課題ウ　連続量量子鍵配送技術とその応用

採択件数：１件。

予算　：平成２３年度は、総額５５百万円を上限とする。

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

採択件数：１件。

予算　：平成２３年度は、総額３０百万円を上限とする。

４．提案に当たっての留意点

課題ア、イ、ウ、エのそれぞれに対して、同一の法人から同時に提案することができる。なお、提案書は、課題ごとに独立に作成すること。

５．研究開発の到達目標

課題ア　量子鍵配送ネットワーク制御技術

以下で述べるアー１、 アー２、アー３、アー４について取り組む。この中から一つ以上（数は任意）を選択した上で、適正な研究計画を作成し応募すること。

アー１ 安定化技術

鍵配送装置や伝送路の周辺環境に特性変動があった場合でも、量子ビット誤り率を 3%以下に保持し安定に安全鍵を生成できるような能動的安定化技術を開発する。都内敷設ファイバ網の典型的な動作環境として、伝送損失 0.4dB/km 程度、敷設の地下率が 50%程度、敷設ファイバ長 50km にわたる 1 昼夜間でのパルス到着時間揺らぎが 1 ナノ秒程度、偏光回転は 10 分間で 90 度程度が想定される。以上を考慮して、目標となる量子鍵配送性能を提案書に明記すること。

アー２ アプリケーションプラットフォームの拡張

種々の方式の携帯端末へ安全鍵をダウンロードできるインターフェースの開発や、信頼できる中継サーバを介して任意の携帯端末間で秘匿通話を実現する有無線統合型鍵交換システムの研究開発を行い、フィールド環境下で動作実証を行う。なお、受託者が有する量子鍵配送装置の台数が限られる場合には、他の課題の受託者と連携の上で可能な限り多くの端末間でフィールド実証を行うのが望ましい。

アー３ 次世代量子鍵配送システム技術

上記アー１、アー２や以下で述べる課題イの研究開発成果を活用しながら、主要なサイドチャネル攻撃対策及び能動的安定化技術、及びより高効率な鍵蒸留処理技術を実装した次世代の量子鍵配送システム技術を開発する。特に、ユーザ数の増加に伴う鍵消費量の増加に十分対応できるような性能目標とその根拠を盛り込んで提案すること。情報通信研究機構（以下、「機構」という。）の光ネットワークテストベッド JGNX の敷設ファイバ網で適宜フィールド試験を行いながら、試験結果を踏まえたうえで装置の最適化を進めること。装置サイズはより小型のものが望ましい。光子検出器の方式は問わない。試験運用に適用する際には、機構の研究グループが有する超伝導光子検出器を利用することも可能である。

アー４ 長期運用試験

機構の光ネットワークテストベッド JGNX の敷設ファイバ網に量子鍵配送装置を設置して、長期間の連続運転による試験を行い、通信路、装置等の短期・長期的変動の観測と鍵配送性能への影響の解析を行う。鍵生成速度や量子ビット誤り率など典型的な性能指標のデータを随時公開できる運用システムも併せての開発すること。試験運用に用いる装置は、すでに応募者が開発済みのものでもよいし、上記のアー３で新たに開発するものでもよいが、数カ月から年単位の連続運転を繰り返し行える装置とする。

課題イ　量子暗号安全性評価理論

課題アの試験運用によって得られたデータをもとに、量子鍵配送システムのモデル化を行い、実際の装置の安全性を定量的に解析できるような安全性評価理論を構築する。特に、有限サイズの生鍵から安全な鍵を蒸留するための基準の検討や、より効率的な計算コストで安全鍵を蒸留する方式の開発に取り組む。さらに、量子鍵配送特有のサイドチャネルの同定とそこを突く攻撃に対する対策の検討も合わせて行う。これらの成果を課題ア及び以下で述べる課題ウの受託者へ提示するとともに、最終的には、標準化を目指した定量的な安全性評価基準を策定して報告書としてまとめる。

課題ウ　連続量量子鍵配送技術とその応用

コヒーレント状態とホモダイン検出器を用いて情報理論的に安全な量子鍵配送を実現するための連続量量子鍵配送技術の研究開発を行い、都市圏のフィールド環境で動作実証を行う。また、課題イの研究開発成果を活用しながら、当該方式特有のサイドチャネル攻撃対策の検討と安全性評価技術の開発を行う。さらに、情報理論的に安全な連続量量子鍵配送以外にも、計算量的安全性だが光ネットワーク上での実装性や長距離・大容量性に優れた光秘匿通信技術を同一装置内で実装するためのシステム設計を行い、両者を適宜選択できる光暗号装置の開発と動作実証を行う。連続量量子鍵配送技術と光秘匿通信技術の両方について、安全性と通信性能に関する目標とその根拠を盛り込んで提案すること。【参考値として、連続量量子鍵配送に関しては数 10km の伝送距離で１～１０kbps の安全鍵生成、光秘匿通信技術に関しては、伝送距離 300km で、40Gbps 級の秘匿通信などが挙げられる。】

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

効率的な安全鍵の管理・運用に向けて新しい鍵管理アーキテクチャの実装技術を開発するとともに、課題ア、イ、ウで開発される技術と上位レイヤの現代暗号方式を相補的に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行う。機構の研究グループが進める、最新のネットワーク理論に基づく鍵管理方式やセキュリティプロトコルの研究開発成果も適宜試作実装し連携して動作試験を行う。

なお、受託者は量子鍵配送技術の潜在的なニーズや要求条件を把握しているとともに、現代暗号の知識も有し、さらに次段落で述べるような課題ア、イ、ウの成果のシステム統合に関するノウハウを有している必要がある。

課題ア、イ、ウ、エに共通する推進体制について

課題エの受託者は、研究開発の方針や進め方について広い観点から助言を頂くため、学識経験者、有識者を含んだ研究開発運営委員会を組織し、年 1～2 回開催するとともに、課題ア、イ、ウの受託者は、本研究開発運営委員会に参画する。本研究開発運営委員会には、機構の関連する研究室（量子 ICT 研究室やセキュリティ基盤研究室、ナノ ICT 研究室）も参画する。また、課題エの受託者は、ア、イ、ウ、エの全課題を通した研究開発全体の取りまとめを行い、最終年度では、全受託者の協力の下にフィールド環境で開発成果の動作検証を行うものとする。

課題イの受託者は、自らと課題ア、ウの受託者及び機構の量子 ICT 研究室、セキュリティ基盤研究室が参画する研究開発検討会を年に３～４回主催する。本研究開発検討会では、それぞれのチーム、研究者が直面している問題点を共有し、それらの解決に向けた検討を行う。

６．研究開発の運営管理及び評価について

研究開発に当たっては、機構の自主研究との連携を図ること。

また、全課題について、平成２５年度に中間評価、平成２７年度に事後評価を行う。

７．参考

研究課題の背景及びその必要性

様々な社会活動が情報通信ネットワークへの依存性を高めている中で、情報漏洩や盗聴への対策は喫緊の課題である。現在、インターネットの情報安全性は、ネットワーク階層構造の上位レイヤにおいて現代暗号技術によって守られている。この方法は汎用的で現状十分に機能しているものの、解読に膨大な計算を要する数学アルゴリズムに基づいており、科学技術の進展によって危殆化する危険性を常に伴う。このような計算量的安全性に基づく暗号技術では、定期的な仕様の更新が避けられず、その作業コストは膨大なものである。情報データの中には、国家機密や医療データなど長期間秘匿性を保持したいものも存在し、その範囲は科学技術の進展とともに年々増加している。そのため、より強力な暗号技術の開発や、計算量的安全性ではなく、どんな将来技術でも解読できない無条件の安全性、いわゆる情報理論的安全性に基づく暗号技術の開発が望まれている。

一方、ネットワークの急速な光化やクラウド化に伴い、光ファイバへの盗聴攻撃や制御系の撹乱など新たな安全性脅威が現れている。実際、あと 5 年内には高性能の光子検出技術（検出効率 50%、暗計数 100 毎秒個、時間分解能 30 ピコ秒）が市販される可能性が高く、これらを利用してファイバタッピングによる盗聴が現実に行われる可能性も高い。特に、ネットワークの物理レイヤに対する攻撃や撹乱は、従来の暗号ソフトウェアの不備を突く攻撃に比べ、ハードウェアのトラブルに繋がる場合が多く、いったん起こってしまうとその解決には長い時間がかかりサービス停止を引き起こしかねない。このように従来の技術のみでは、物理レイヤに対する高度な攻撃の検知が難しく、多様化する脅威に対して光インフラの安全性を守りきることができない。

量子鍵配送技術は、物理原理を用いることで理論上、光通信路に対するどんな盗聴行為も検知可能で、その結果、盗聴の可能性を排除した安全な暗号鍵を配送できる。このようにして配送された安全鍵を平文と同じサイズだけ用意してワンタイムパッド暗号化することで情報理論的に安全な秘匿通信が可能になる。現在、最新の量子鍵配送技術は、敷設ファイバ 50 ㎞圏で 100kbps 程度の安全鍵生成速度を実現できる段階に達している。物理的に守られた中継ノードを介せば鍵のカプセルリレーによって鍵配送距離を延ばすことができる。しかし、100kbps の鍵生成速度は依然としてボトルネックであり、まだ大容量通信に適用できるレベルではない。一方、特定の専用線において限られた時間だけでも高度な秘匿通信を行いたい用途などには適用できる性

能である。

実利用に向けては、まず、実際の実装環境において安全性を定量的に保証できなければならない。量子鍵配送のプロトコル自体は情報理論的安全性を保証するものであるが、実際の装置化においては、証明の根拠となっている仮定からのずれなど、必ず不完全性が生じる。このような不完全性やシステムを取り巻く周辺環境からのアクセスルートは、一般にサイドチャネルと呼ばれ、安全性への抜け穴となる。サイドチャネルはどの暗号にも共通の課題であるが、量子鍵配送特有のサイドチャネルの同定とそれを塞ぐ対策の開発、また新しい安全性評価理論の構築は今後の重要な課題である。これには、有限サイズのデータから安全性を大きく損なわずに効率的に鍵蒸留処理を行う手法の開発も含まれる。

その上で、常に変動する環境下でも、システムを許容範囲の条件下で安定に動作させるための能動的安定化技術を開発する必要がある。量子鍵配送技術は、他の暗号技術と比べまだ利用実績が乏しく、システムの信頼性を保証するためには、今後長期の試験運用を行いながら安定化技術の開発を進め、問題点を発掘しその解決策を提示・検証しながらシステム稼働実績を積む必要がある。これはサイドチャネルの同定にとっても重要な作業である。

一方、量子鍵配送技術自体の性能改善も引き続き望まれる。しかし、現存技術の改善で４～５年内に実現できる性能は、鍵生成速度にして現状比１～２桁程度と予想される。一方で、限られた鍵配送性能の下で、如何に効率良くネットワーク上で安全鍵をリレー、もしくはルーティングし運用するかついてはまだまだ研究の余地がある。新しいルーティング機能の実装や、最新のネットワーク情報理論の成果を活かした鍵管理アーキテクチャの研究とその実証は今後の重要課題である。また、データ秘匿化のためのワンタイムパッド暗号化に止まらず、安全鍵を上位レイヤで認証や証明などの新機能に利用するための研究開発も、今後のアプリケーション拡大にとって有用である。

このような研究開発によって生み出される新しい安定化技術、鍵蒸留処理技術やルーティング機能、鍵管理アーキテクチャ、及び必要なインターフェースを搭載した最新の量子鍵配送システムをシンプルかつコンパクトに実装するのが向こう 5 年間の目標になる。

量子鍵配送は、現在、単一光子伝送を使う方式が主流であるが、光子検出器がコストを上げる大きな要因になっている。一方、量子鍵配送には、通常の光通信で使われるレーザ光（コヒーレント状態）と、フォトダイオードからなるホモダイン検出器を用いる方式もあり、連続量方式と呼ばれている。この連続量量子鍵配送方式でも、情報理論的に安全なプロトコルが示されている。しかし、過剰雑音があると安全性の許容範囲が急速に狭まることから、性能としてはフィールド 10km で 10kbps 程度の鍵配送が限界となっている。低雑音ホモダイン検出器を開発し、我が国が有する優れたコヒーレント多値伝送技術と組み合わせ鍵配送性能を向上させることができれば、光

通信の部品類を使った低コストの量子鍵配送システムを実現できる。この技術は、光通信技術との親和性から、光符号分割多重通信や量子雑音秘匿通信など光インフラで利用可能な種々の秘匿通信技術へ展開することが可能である。

今後の光インフラとして間もなく登場するフォトニックネットワークでは、従来の電気を介したノード処理ではなく、すべてを光でシームレスに処理するフォトニックノードによって、広域にわたって光のトランスペアレントなリンクを構築することが可能になる。そこでは、物理レイヤにおいて量子鍵配送や光秘匿通信技術を利用して秘匿通信や鍵配送を行い、上位レイヤの暗号方式と相補的に連動させ、ユーザの要求に応じて適応的に暗号化方式を選択することで、今後現れうる種々の攻撃や脅威からネットワークを守りつつ、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ようになる。このようなフォトニックネットワーク技術の研究開発を実施することで、安心・安全で利便性の高い情報通信サービスの提供が可能になると期待される。

他の関連する研究課題

本課題においては、安全性が保証された「古典的な」中継ノードを用意し、秘密鍵を別の秘密鍵でカプセル中継することで、専用線での量子鍵配送を都市間秘匿通信路の実用化に発展させる。それに対し、H23 年度から開始する委託研究開発課題「量子もつれ中継技術の研究開発」では、量子もつれ相関を全量子的手法により直接共有し、量子もつれ鍵配送ネットワークを構築するための基盤研究を行う。

また、本課題と密接に関連するこれまでの研究課題としては、機構の委託研究として、量子暗号ネットワークとその基盤技術に関する研究開発がある。H13 年度～H17 年度に実施した「量子暗号技術の研究開発」で量子暗号基盤技術を開発し、H18 年度～H22 年度に実施した「量子暗号の実用化のための研究開発　課題イ：量子暗号ネットワーク」で 50km 圏の専用線を用いた量子暗号ネットワークの試験運用システムを構築したところである。本課題は、これらの成果に基づき、極めて高い安全性が要求されるハイエンド用途で、高い信頼性を持っての実利用できる量子暗号ネットワークを開発するとともに、将来、さらに広い用途に展開するための新しいセキュアフォトニックネットワークの基盤技術を開発するためのものである。