新規研究開発課題に係る基本計画書概要
量子暗号通信網の早期社会実装に向けた研究開発

研究開発の背景・目標

量子コンピュータの実現に伴い、現在インターネット等で広く使われている暗号アルゴリズムが危殆化する可能性が指摘されている。攻撃者は、量子コンピュータの実現を見越して、既に通信の盗聴・保存（Harvest now, decrypt later攻撃）を始めていると考えられており、対策が急務となっている。そのため、世界各国で量子コンピュータでも解読できない情報理論的安全性を確保した通信の導入に向けた取り組みが加速している。本事業では、盗聴を確実に検知することが可能な「量子鍵配送（QKD）」を用いた高秘匿通信網「量子暗号通信網」の高機能化及び2030年頃までの社会実装に向けた研究開発を目的とする。

政策目標（アウトカム目標）

本事業により、実利用環境においても高機能な量子鍵配送装置の実現等、量子暗号通信網の早期の社会実装に必要な技術を確立し、量子コンピュータが実用化された際にも、重要データの安全な保管や秘匿通信等を実現するとともに、国際競争力強化・サイバー空間の安全性を確保する。

研究開発目標（アウトプット目標）

課題（1）～（3）の技術を確立する。また、本研究開発に係る特許の取得や国際標準の獲得、及び量子鍵配送装置の実装安全性を証明するための認証制度を確立し、本研究開発成果の製品化及び国際市場への更なる展開を実現する。

技術課題

〇課題（1） 量子鍵配送技術の高度化

ア）鍵生成速度の高速化技術
イ）伝送距離の長距離化・広域化技術
ウ）量子鍵配送とのオール光ネットワーク統合技術

〇課題（2） 量子鍵配送網における鍵管理技術の高度化

ア）大規模量子鍵配送網における鍵管理の最適制御・高信頼化技術
イ）高秘匿・高信頼鍵リレー技術

〇課題（3） 量子暗号通信網の高機能化と統合実証

ア）情報理論的安全な相手認証及びデータ完全性担保技術
イ）統合実証

到達目標

〇課題（1）
ア）BB84の小型化・集積化、波長多重による高速化（伝送損失10dBで4Mbps以上の鍵生成）、耐環境性能を有する装置の高速化（伝送損失10dB・架空線率50％以上で1Mbps以上の鍵生成）を実現。
イ）TF-QKDを敷設ファイバ区間を含む距離500 kmで鍵生成10bps以上を実現。スター型TF-QKDで3拠点以上を接続し、250km以上離れた任意の2拠点間で鍵共有を実現。CV-QKDのにより既存データ用チャネルとの波長多重伝送条件下で距離20kmで鍵生成50kbps以上を実現。空間CV-QKDを地上付近距離1kmで鍵生成10kbps以上を実現。
ウ）オール光ネットワーク上での波長多重伝送によりエンドーエンドで3ホップ以上の鍵リレーを専用ファイバ使用時と比較して50％未満の速度劣化で実現等。

〇課題（2）
ア）20ノード以上の実ネットワーク含む数百ノード程度の規模の計算環境において、ユーザ数10以上での鍵リレー管理手法・プロトコルを確立。
イ）50ノード程度の量子鍵配送網に対し、ノードディスジョイントの鍵リレールート選定を1分以内に実現。セキュアネットワーク符号化の処理速度を従来比3倍となる10 Mbps以上まで高速化等。

〇課題（3）
ア）任意のノード（2以上）で情報理論的安全な相互認証を1分以内に実現。
イ）オール光ネットワークとを連携・統合させ、鍵供給に伴う付加遅延を数百マイクロ秒以下を実現。課題（1）～（3）ア）の技術を適用した機能実証を行い社会実装に向けたユースケースを創出する。

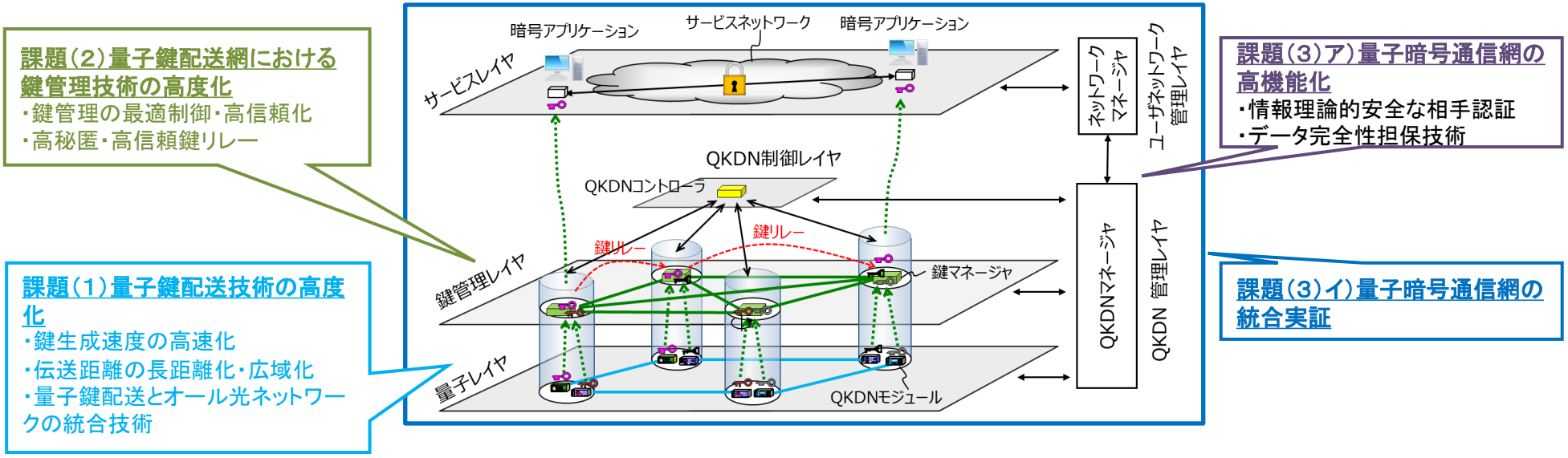
（参考）量子暗号通信網の早期社会実装に向けた研究開発

【事業概要】

「量子鍵配送（QKD）」を用いた高秘匿通信網「量子暗号通信網」の高機能化及び実用に向けた研究開発・実証実験を実施し、当該技術の早期の社会実装を目指す。具体的には、

- 鍵生成速度の高速化や伝送距離の長距離化・広域化等に向けた「量子鍵配送技術の高度化」
- 鍵管理 の最適制御・高信頼化を実現するための「量子鍵配送網における鍵管理技術の高度化」
- 高効率な相手認証・完全性保証技術や各技術課題の統合実証のための「量子暗号通信網の高機能化と統合実証」

の研究開発を実施する。



所要経費　17.0億円　　**研究開発期間**　R7年～R11年

（参考）課題（1） 量子鍵配送技術の高度化

研究開発内容

プロジェクト終了時に世界トップレベルの性能を有する実用性・信頼性の高い量子鍵配送(QKD)装置を実現するため、量子鍵配送における鍵生成速度の高速化、伝送距離の長距離化および広域化、オール光ネットワークとの統合技術の研究開発及び実用性検証を実施。

見込まれる技術的な効果

○鍵生成速度の更なる高速化（伝送損失10dBで4Mbps以上の鍵生成）達成による世界トップレベルの性能維持

○伝送距離の長距離化（500 km）・広域化（3拠点接続・空間伝送）技術の実現による、ユーザ数やサービスエリアの効率的拡大

○オール光ネットワークとの統合による量子鍵配送の効率的な広域展開

本研究の技術的ポイント

ア） 鍵生成速度の高速化技術

BB84型は我が国企業が300bps@10dBの装置を製品化し世界トップレベル。

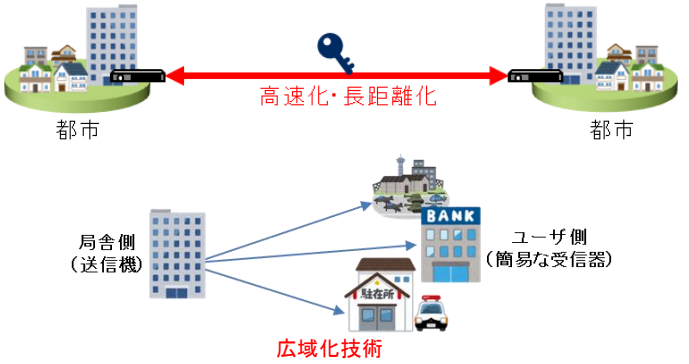
波長多重・光子検出器の性能向上等による更なる高速化等を実現。

イ） 伝送距離の長距離化・広域化技術

TF-QKDを長距離化を敷設ファイバ環境で実現。広域化のため

多拠点接続を可能とするスター型TF-QKD、メトロ・アクセス網への

の導入を想定したCV-QKDの小型化と空間伝送方式の実現。



ウ） 量子鍵配送とオール光ネットワークの統合技術

オール光ネットワークにオーバレイしたEnd-to-End量子鍵配送技術とその制御・管理系連携方式を確立。

（参考）課題（2） 量子鍵配送網における鍵管理技術の高度化

研究開発内容

大規模な量子鍵配送網の高信頼な運用・管理を実現するため、複数のユーザが利用することを想定した鍵管理システムの構築を行い、大規模量子鍵配送網における鍵管理の最適制御・高信頼化技術や、高秘匿・高信頼な鍵リレー技術の研究開発を実施。

見込まれる技術的な効果

○20ノード以上の実ネットワークを含む数百ノード規模のシミュレーション環境において、ユーザ数10以上で刻々と変化する鍵時需給状態やネットワーク状態の変化に応じた量子鍵配送を実現。

○ノードの危殆化に対する耐性の強化

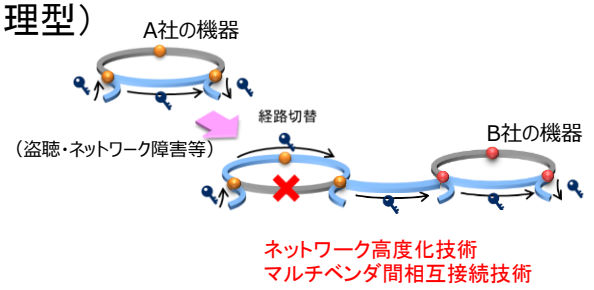
本研究の技術的ポイント

ア）大規模量子鍵配送網における鍵管理

現在我が国では20ノード規模の量子鍵配送網を構築。今後、さらに大規模な量子鍵配送網において最適な鍵供給サービスを実現するためプロアクティブ制御技術、異なる鍵管理システム（集中管理型・分散管理型）のインターワーキング技術を確立。

イ）高秘匿・高信頼鍵リレー技術

現在の鍵リレーは“信頼できる局舎”の安全性に依存している。そのため局舎内のデータ損失や情報漏洩対策として、ノード危殆化率やリンク誤り率・改竄率等を定量的に評価する手法等を確立。



（参考）課題（3） 量子暗号通信網の高機能化と統合実証

研究開発内容

量子鍵配送網が暗号インフラとして社会実装するために必要な認証、完全性保証等の機能の研究開発を実施。

量子鍵配送網とオール光ネットワークの連携によるセキュアオール光ネットワークの構築・実証、さらに、課題（１）から（３）ア）の技術を適用した機能実証を実施。

見込まれる技術的な効果

○情報理論的安全にマルチユーザに対応した相手認証やデータの完全性を担保する機能を実現

○セキュアオール光ネットワークの構築と具体的なユースケースに基づく各課題の成果の機能実証

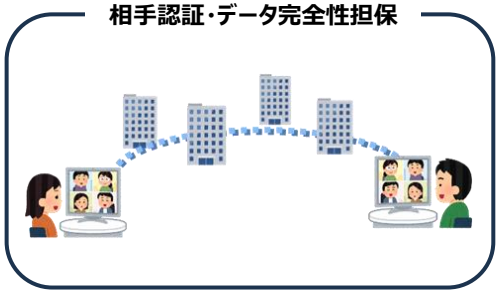
本研究の技術的ポイント

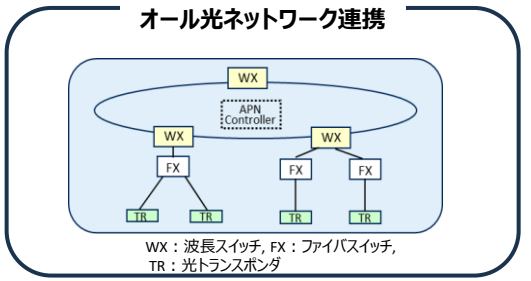
ア）情報理論的安全な相手認証及びデータ完全性担保技術

現代暗号技術に具備されている相手認証やデータの完全性保証を、量子暗号通信網に量子鍵配送の特徴である情報理論的安全性を備えた機能として具備するための技術開発を実施。

イ）統合実証

超高速・低遅延なオール光ネットワーク上での秘匿通信サービスの実現に向け、量子鍵配送網との統合に必要な要件の明確化を実施。さらに、課題（１）から（３）ア）について実用的な環境で信頼性試験等を行い社会実装に向けたフィージビリティを示す。





アウトカム目標の達成に向けた総務省の取組について

政策目標の達成に向けた取組方針

〇研究開発期間中

・受託者が設置する研究開発運営委員会において、政策意図を適切に反映させるとともに、学識経験者や有識者の助言をもとに研究開発全体の方針を調整する。

・研究開発推進のため、関連施策との連携を図るとともに、情報通信研究機構の実験機器や実験施設、テストベッド等のインフラを有効活用すべく、研究連携支援を行う。

・海外メーカーの開発動向、市場状況等を調査し、状況に応じた研究開発の加速化や、研究開発成果を基にした国際標準化活動を支援する。

・政策目標の早期実現や海外技術との差異化を図るため、各技術の高性能化や高機能化、高効率化の研究開発に必要となる予算の獲得を検討する。

・関連コンソーシアムと連携し、本研究開発をベースとした将来の量子暗号通信網を議論するとともに、要求される周辺技術の課題やその目標達成時期を明示する。

〇研究開発期間終了後

・成果報告を中心としたシンポジウムを開催し、オープンソース等の共有化を図るとともに、国際標準化に向け、国際会議、展示会等を通した海外へのアピールを促進させる。

・追跡調査・評価において、受託者等に製品化等の成果展開状況を確認するとともに、有識者等の助言を得ながら、標準化を推進すること等により国際競争力の強化を図る。

・本研究開発成果の応用展開のため、例えば量子インターネット技術等を後継研究開発として立案し、さらなる情報通信インフラの維持・発展に寄与する。