令和２年度新規研究開発課題に係る基本計画書概要　【研究推進室】
グローバル量子暗号通信網構築のための研究開発

別紙1参考

背景・目標

背景

将来、実用的な量子コンピュータが実現されることで、現代暗号で守られていたデータが全て解読されてしまう事態が懸念されている。従って、量子コンピュータ時代においても、国家間や国内重要機関間で機密情報を安全にやりとり可能とするため、広域的な量子暗号通信ネットワーク技術を確立し、極めて堅牢性の高い安全なサイバー空間を実現する必要がある。

政策目標（アウトカム目標）

量子通信・暗号リンク技術、トラステッドノード技術、量子中継技術、及び広域量子暗号通信ネットワーク構築・運用技術を確立することによって、グローバルな量子暗号通信網の実現に寄与する。また、開発成果の国際標準化や市場展開を推進し、我が国の量子暗号通信技術の国際的な競争力を強化する。

研究開発目標（アウトプット目標）

地上系の数百km圏において、ノード数が2桁以上で万単位のユーザ端末の収容及び鍵供給を可能とし、100kbps以上の暗号鍵生成スループット、及び高い安全性と可用性を同時に可能とする技術を実現する。また、都市圏距離において、1Mbps程度の暗号鍵生成速度を達成する量子暗号装置を実現する。

技術課題

○課題（1）　量子通信・暗号リンク技術

ア）量子暗号通信の高性能化技術
2地点間通信の高速化や長距離化に資する技術確立及び装置開発。

イ）光子検出技術

a）低雑音光子検出技術
単一光子検出の高精度化。

b）広帯域ホモダイン検出技術
安価な量子暗号通信の実現。

○課題（2）　トラステッドノード技術

ア）鍵管理サーバ技術の高信頼化
鍵管理システム全体の堅牢化、及び耐タンパー性の保証。

イ）高度分散化技術
可用性の高い鍵配送・供給の実現、及び安全かつ高効率な暗号鍵・データのリレー配送等の実現。

○課題（3）　量子中継技術

ア）量子メモリの光リンク技術
量子メモリ間での量子もつれ実現。

イ）量子中継基盤技術
量子メモリ間のリンクの長距離化のための新たな基盤技術の実現。

○課題（4）　広域ネットワーク構築・運用技術

ア）ネットワーク制御管理技術
多地点間量子暗号通信の実現、複数方式の連携動作、及び複数方式のネットワークに跨がる鍵管理等。

到達目標

○課題（1）　量子通信・暗号リンク技術

現在敷設環境で動作中の量子暗号装置と比較し、3倍程度の高速化及び当該装置の限界を超える長距離化等を実現可能な新たな装置等を作製する。

○課題（2）　トラステッドノード技術

高信頼鍵管理サーバのハードウェアモジュールの作製、および3パーティ以上の秘匿計算を1Mbps以上の速度で実行する技術等の開発及び実証を行う。

○課題（3）　量子中継技術

独立して動作する2個以上の量子メモリ間を10km以上の光ファイバーで接続し、量子ビットの中継（転送）操作（量子もつれ等）を1秒に10回以上の頻度で生成するための技術や、さらなる長距離化に資する新たな量子中継方式等を確立する。

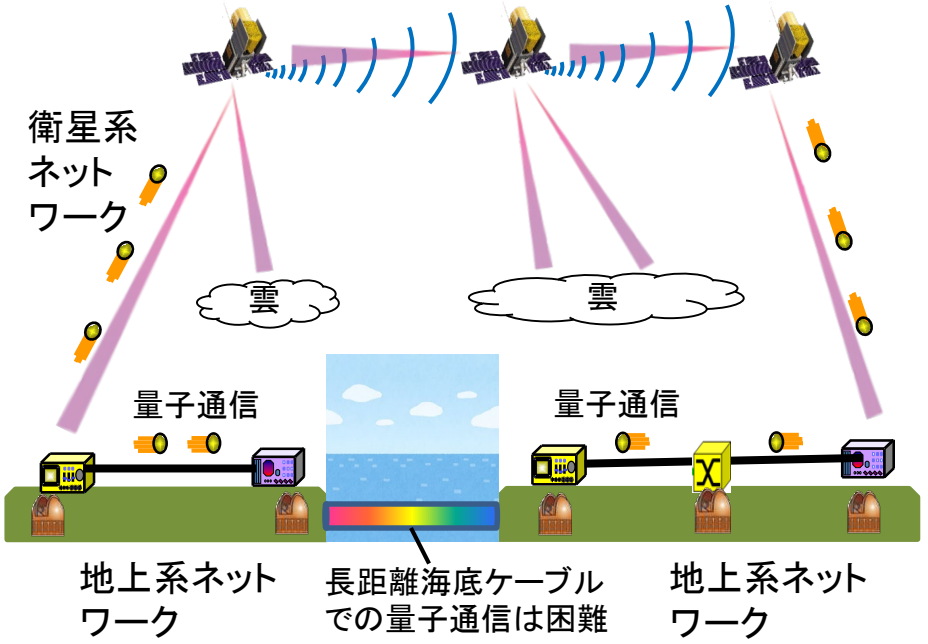
○課題（4）　広域ネットワーク構築・運用技術

ノード数が2桁以上で、万単位のユーザ端末の収容及び鍵供給を可能とする量子暗号通信網を構築可能な技術を開発する。ネットワーク内で、3種類以上の方式の量子暗号装置の連携動作を可能とし、かつ複数方式のネットワークにまたがる安全な広域鍵管理の技術等を確立する。また、QKDネットワークを効率的に運用するための新たな制御管理技術等を確立する。

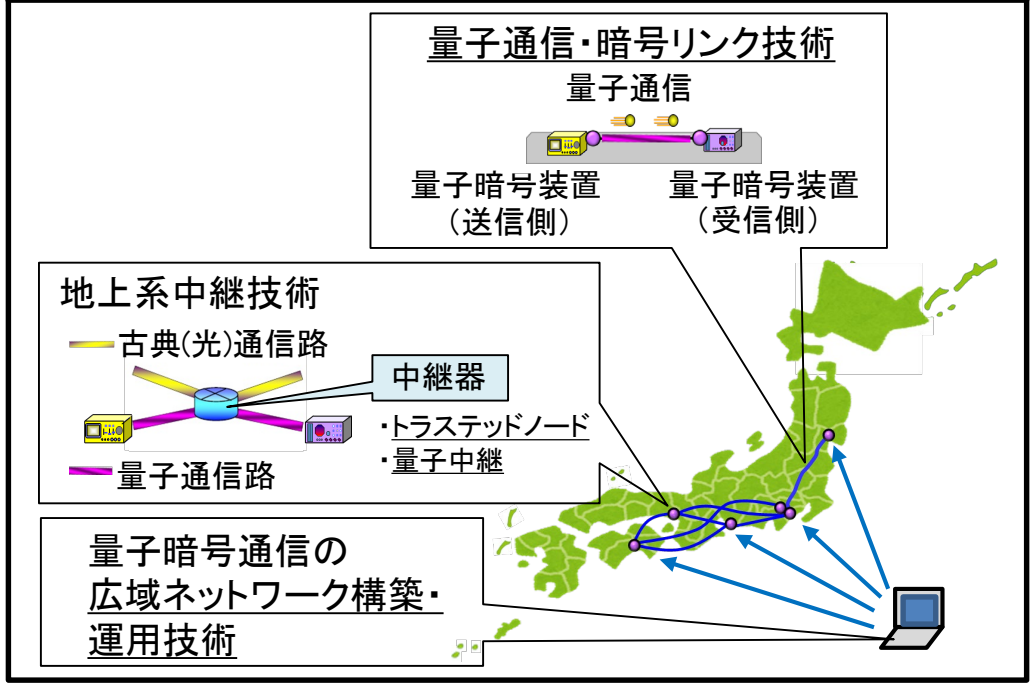
（参考）グローバル量子暗号通信網構築のための研究開発

【事業概要】
○ 量子コンピュータ時代においても、国家間や国内重要機関間で機密情報を安全にやりとり可能とするため、距離に依らない堅牢な量子暗号通信網の技術を確立する。
○ 具体的には、
・地上系2地点間通信において、通信速度を維持しつつ、長距離化と高可用性を両立できる「量子通信・暗号リンク技術」
・地上系中継点において、電気処理の鍵リレーによる更なる長距離化や鍵管理・鍵配送の堅牢化等に資する「トラステッドノード技術」
・地上系中継点において、長距離化と絶対安全な鍵管理・鍵配送を両立できる「量子中継技術」
・量子暗号通信の広域ネットワーク化に向けた「広域ネットワーク構築・運用技術」
の研究開発を実施する。

グローバル量子暗号通信網の簡易イメージ



研究開発内容の概略



所要経費　14.4億円（令和2年度）　　**研究開発期間**　令和2年度～令和6年度

（参考） 課題（1）： 量子通信・暗号リンク技術

研究開発内容

地上系量子通信チャネルにおける通信の高速化・長距離化に向けて、新たな量子鍵配送方式や、高効率な単一光子検出器及び広帯域検出器を開発し、それら開発技術を組み込んだ量子暗号装置を作製する。

見込まれる技術的な効果

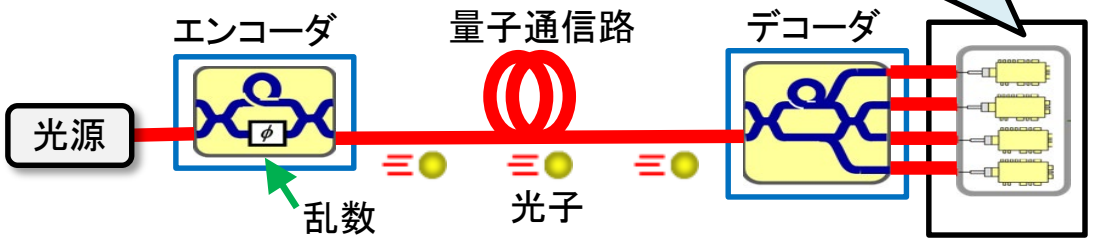
○雑音耐性の高い光子検出器等の実現により、地上系量子暗号通信の高速化・長距離化
○小型かつ安価な量子暗号装置の開発
○鍵生成量/コストでの装置の国際競争力強化
等

本研究開発の技術的ポイント

ア）：量子暗号通信の高性能化技術

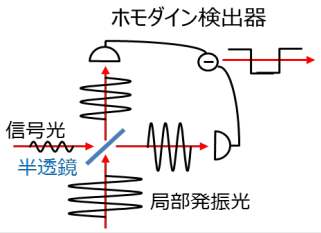
量子通信チャネル
より長距離、高速

イ）-a：低雑音光子検出技術



イ）-b：広帯域ホモダイン検出技術

非量子通信チャネルとの並存
より安価、小型



ホモダイン検出器の高い波長選択性により雑音耐性を向上、多重化を実現等

課題

ア）：量子暗号通信の高性能化、メンテナンス容易化
イ）-a：受信側における光子検出精度の向上
イ）-b：既設の光ファイバー等の非量子暗号通信チャネルとの並存（低コスト化、早期実現）

本研究開発における取り組み

ア）：量子鍵配送の高性能化や量子暗号装置作製
イ）-a：実用に適した低雑音単一光子検出器の開発
イ）-b：非量子暗号通信チャネルと並存可能な広帯域ホモダイン検出器の開発

（参考） 課題（2）： トラステッドノード技術

研究開発内容

中継点における電気処理により長距離化を実現する
トラステッドノードにおいて、鍵管理システム全体の堅牢化及び耐タンパー性の保証、さらには秘密分散等を活用した機密性・完全性・可用性等の向上が可能な技術を確立する。

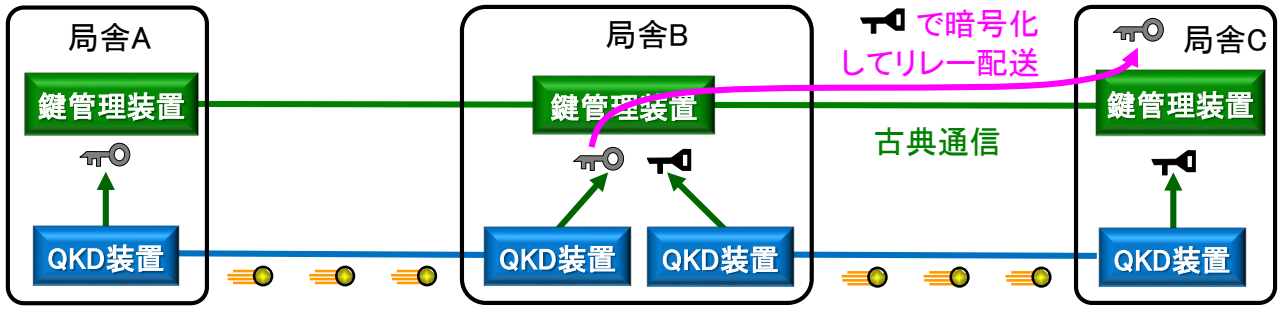
見込まれる技術的な効果

○ 地上系量子暗号通信の長距離化
○ サービス停止攻撃等への脆弱性を解消
○ 各中継点における鍵管理・鍵配送の機密性・完全性・可用性を向上
等

本研究開発の技術的ポイント

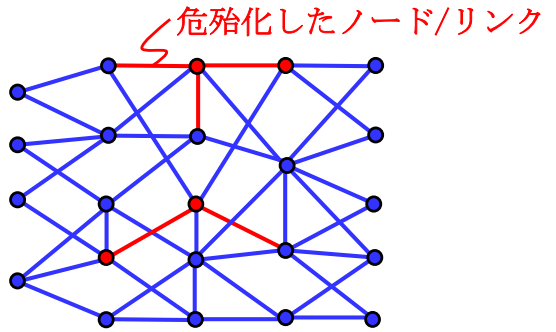
ア）：鍵管理サーバ技術の高信頼化

ネットワーク化は、局舎（電気処理）を介した鍵のバケツリレーで実現。



イ）：高度分散化技術

複数のノード及びリンクで分散的に符号化・暗号通信



課題

ア）：サイバー攻撃や災害等によって局舎が機能不全状態に陥っても、安全に鍵の管理・処理・保管等を実行
イ）：可用性の高い鍵配送・供給の実現、及び安全かつ高効率な暗号鍵・データのリレー配送等の実現

本研究開発における取り組み

ア）：鍵管理サーバシステム全体を堅牢化し、さらに耐タンパー性を保証する技術等の開発
イ）：秘密分散やマルチパーティ計算等を活用した機密性・完全性・可用性の高い技術や、ネットワークコーディング等を導入した新たな技術の開発

（参考） 課題（3）： 量子中継技術

研究開発内容

地上系量子暗号通信の更なる長距離化及び安全性向上のため、中継点において、量子状態を一定時間保持できる量子メモリ技術や、その周辺技術の開発、また、波長多重量子中継や全光量子中継等の新方式の基盤技術等に関する研究開発を行う。

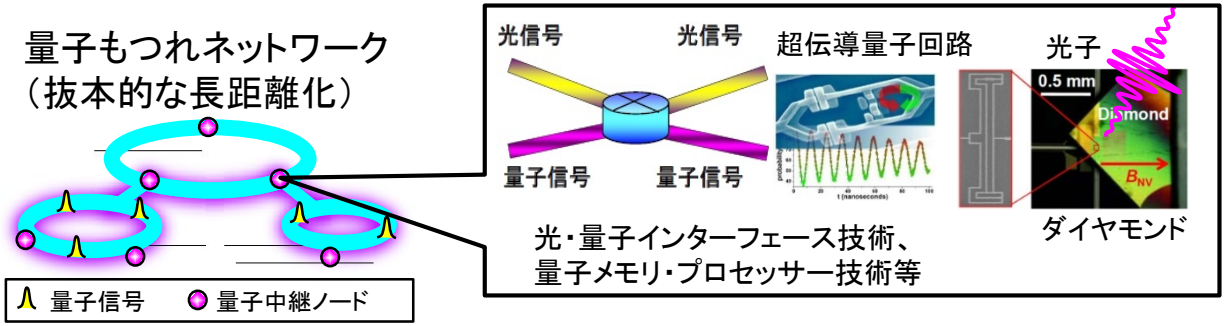
見込まれる技術的な効果

〇地上系量子暗号通信の長距離化
〇トラステッドノードと比較し、
・安全性向上
・送受信間の鍵共有の簡易化
等

本研究開発の技術的ポイント

ア）：量子メモリの光リンク技術

イ）：量子中継基盤技術



※ 量子もつれ：物理的に離れた複数の光子同士が特有の相関を持っている状態
※ 量子テレポーテーション： 一方の光子を観測すると、未知だった量子状態が未知のまま他方の光子に再生される

課題

ア）：離れた中継点に置かれた量子メモリの間を光でリンクする必要
イ）：量子メモリ間のリンクの大規模化するための基盤技術の実現

本研究開発における取り組み

ア）：複数の量子メモリを光で接続し、量子メモリ間での量子ビットの中継（転送）操作（量子もつれ等）を実現する技術の設計及び開発
イ）：波長多重量子中継や全光量子中継等の新方式の基盤技術の設計及び開発

（参考） 課題(4)： 広域ネットワーク構築・運用技術

研究開発内容

・量子通信・暗号リンク技術やトラステッドノード技術、量子中継技術等を組み合わせて多地点間通信を可能とするため、量子暗号通信ネットワークの広域化に資するネットワーク制御管理技術の研究開発を行う。

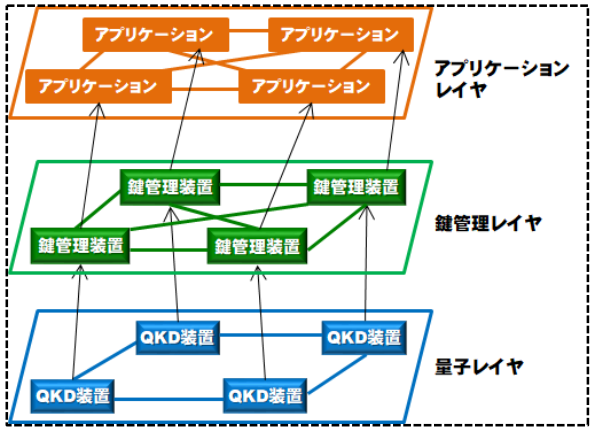
見込まれる技術的な効果

○ 複数方式の量子暗号通信ネットワークが混在された環境において、多地点間通信や安全な広域鍵管理・配送が可能なメッシュ型ネットワークの実現
○ 量子暗号通信の長距離化
等

本研究開発の技術的ポイント

ア)：ネットワーク制御管理技術

アーキテクチャ(例)



課題

ア)：量子暗号通信の広域ネットワーク化、
複数方式の量子暗号通信の連係動作、及び
複数方式のネットワークに跨がる安全な広域鍵管理、
効率的なネットワーク運用。

本研究開発における取り組み

ア)：異なるQKD方式の暗号装置及び異なるベンダ装置の相互接続技術の開発。
複数方式通信の連携動作のための制御技術、及び
複数方式網に跨がる広域鍵管理技術の開発。
QKDネットワークの効率運用のための新技術の開発。

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ネットワーク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。