平成１８年度　新規委託研究

「量子暗号の実用化のための研究開発」

研究計画書

概要

物理層において無条件安全性を保証できる量子鍵配送技術や量子テレポーテーションに基づく新しいネットワーク技術、さらには従来限界を超えて超大容量通信を可能とする量子符号化技術などを組み込んだ量子情報通信ネットワークを早期に構築することを目指して、そのための基盤技術、システム技術の研究開発を委託研究「量子暗号の実用化のための研究開発」として総合的に進める。特に、量子情報通信の基盤となる高性能光子検出技術、都市圏や光ファイバ基幹回線での実用的量子暗号ネットワーク技術及び将来、量子鍵配送ネットワークを超長距離化するための量子中継技術を課題の柱として進める。

１．研究テーマ

「量子暗号の実用化のための研究開発」

２．研究開発の目的

安全で安心なネットワーク社会を実現する上で、物理原理に基づく無条件安全性が保証された量子鍵配送技術に対する期待は高い。量子鍵配送が鍵配送システムとして実用的であるためには、それが、メトロ系ネットワークと長距離あるいは超長距基幹回線ネットワークによって構成されるネットワーク上において、無条件安全性を保証しつつ十分な通信速度で以って実現されることが必要である。

単一光子を用いた量子鍵配送システムは数 10km の近距離においては一定の通信速度を達成し、実用化が可能なことが実証できるレベルにまで発展を遂げている。しかしながら、拡大を続ける通信需要に見合う速度を得るには更なる高速化が必須である。その鍵を握るのは、単一光子検出技術の高性能化である。これは量子鍵配送システムの長距離化、更にはネットワーク化にとってもボトルネックとなる重要課題である。また、各種の量子情報通信ネットワークプロトコルを実証するためにも共通の基幹技術となる。そこで、本研究ではまず、光ファイバ通信波長帯用の高性能単一光子検出技術の研究開発を行うことを目的とする。

次に、この高性能単一光子検出技術を利用して、無条件安全性が理論的に保証された高速な量子鍵配送プロトコルをメトロ系ネットワークで実現するためのシステム技術の開発及び量子鍵配送を基幹回線ネットワークへ適用して行くための基盤技術の開発を行い、メトロ系ネットワークと基幹回線ネットワークが接続したネットワーク上における量子鍵配送システムを開発して、その性能を実証することを目的とする。

さらに、量子暗号網が 1000km 程度にまで超長距離化されるためには、通信網の送受信者間で量子もつれ状態にある光子対を共有する必要がある。量子もつれ光子は、原理的には単一光子など他の量子鍵配送用量子光源よりも長距離の伝送が可能であるとされているが、そのためには、損失により破壊されていくもつれ光子対の量子コヒーレンスを伝送の中継点において回復する、量子中継技術が必要不可欠となる。量子中継技術の開発には、伝送路中の各中継点で必要なデバイスの要素技術開発と、多数の中継点を全てつないだネットワーク全体の構成方法、性能評価に関する理論的研究の双方が必要となる。そこで、本研究ではさらに、量子中継システムについて、構成に関する理論的研究と、要素技術の開発を含むプロトタイプの開発及び実証実験を行い、将来の大規模量子中継システムの実現性や量子鍵配布の超長距離化への適用可能性を理論的に明らかにすることを目的とする。

３．研究開発期間及び予算

研究開発期間：平成１８年度から平成２２年度末までの５年間。

予算：平成 18 年度は総額３０５百万円程度を上限とする。また、課題毎の内訳は以下のとおりとする。

課題ア：年間 45 百万円程度
課題イ：年間 180 百万円程度
課題ウ：年間 80 百万円程度

なお､平成 19 年度以降の予算については未定ではあるが､提案を行う前提として、平成 19 年度以降の総額及び課題毎の予算については、平成 18 年度提案額と同額或いは未満の金額で提案を行うこと。

４．研究開発課題

以下のとおり。なお、応募にあたっては、以下の 3 つの課題ア、イ、ウのそれぞれに対して、理論・実験双方が互いに連携した研究提案を行うこと。

課題ア　化合物半導体型単一光子検出器の研究開発

量子鍵配送システムの高性能化を実現するために不可欠な、光ファイバ通信波長帯において、高速で高い検出効率と低アフターパルス確率、低ダークカウントを有する単一光子検出技術を確立するための研究開発を行う。InGaAs など現在使われている化合物半導体、あるいは化合物半導体とシリコン半導体の張り合わせ構造など小型化・量産化へのポテンシャルを持ち、光ファイバ通信波長帯の信号の直接検出が可能な単一光子検出技術の高性能化に関する研究開発を行う。そして、本課題と平行して進められる「課題イ-1　都市圏対応型量子鍵配送システム技術」において開発する都市圏対応型量子鍵配送システムに実際に組み込んで実証実験を行う。

＜備考＞

備考１：入射方式（面入射、導波路入射など）は問わない。

備考２：公的資金の性質上、単に既存製品の組み合わせでパッケージ化するレベルの提案ではなく、独自技術開発を主眼とした単一光子検出技術のポテンシャルアップに繋がる提案を優先する。

課題イ　量子暗号ネットワーク技術の研究開発

物理的安全性が理論的に保証された量子鍵配送プロトコル[備考３]に基づき、高度な量子暗号ネットワークの実現を目指して以下のような課題の研究開発を行う。

課題イ-１　都市圏対応型量子鍵配送システム技術の研究開発

物理的安全性が理論的に保証された量子鍵配送プロトコル[備考３]に基づき、５０km 圏内のメトロ系 IP ネットワークで実用可能な量子鍵配送システムを、課題アの成果である単一光子検出技術を組み込んで開発する。実用的な安全性を重視することとし、その上で鍵生成速度は 1 対１の通信において最低限、電話・ファックス対応可能な 1Mbps 以上とする。さらにシステム機能として、波長多重機能やスイッチング機能を組み込み、複数ノード間で接続を自在に切り替え、トラフィックや盗聴状況に応じて最適迂回経路を設定できるネットワーク制御技術も開発する。ノード数は８程度を目標とする。また、光集積回路による装置の小型化も合せて進める。光源については、これらのシステム性能に結びつくものであれば、減衰させたポアソン光でも単一光子光源でも良く、特に限定しない。以上の開発成果をまとめつつ量子鍵配送システムを開発し、メトロ系ネットワークにおいて実証実験を行う。提案書には、想定される盗聴者の能力とシステムの不完全性を定量化し、それに対するセキュリティ保証の評価基準も合せて記述すること。

課題イ-２　基幹回線対応型量子鍵配送技術の研究開発

物理的安全性が理論的に保証された量子鍵配送プロトコル[備考３]に基づき、１００km～２００km の中長距離で可能な限り高速の鍵生成レートを実現するための技術を開発する。都市間フィールド試験によって性能を評価できることが理想であるが、実験室レベルでの実証も可とする。終了年度までには、課題イ-1 のメトロ系 IP ネットワーク対応の量子鍵配送システムとの接続の実証実験まで行う。セキュリティ保証に関しては課題イ-1 に順ずる。光源についても、同様に特に限定しない。中長距離の量子鍵配送を実現するための単一光子検出技術に関しては、例えば波長変換とシリコン半導体を用いる方式による検出技術など、必要な技術の開発を行うものとする。

＜備考＞

備考３：少なくとも個別攻撃に対する安全性が理論的に証明されているプロトコルであること。

課題ウ　量子中継システムの研究開発

量子もつれ状態を長距離伝送するための量子中継技術の確立を目指して以下のような課題の研究開発を行う。

課題ウ-1 量子中継システム設計の理論的研究開発

大規模システム化可能な量子中継プロトコルの提案とシステム設計・評価に関して理論面から研究開発を行う。これまでいくつかの方式が提案されているが、全ての方式において、必ずしも将来の実用的なシステム構成が可能であると保証されているとは言えない状況である。

本研究課題では、具体的なデバイスの特性を基にした量子中継プロトコルを提案し、実現可能なシステムの性能を数値的に明確にするための理論的な研究開発を行う。量子中継システムを構成するデバイスには、中継の媒質として原子系や固体系の量子ビット、また中継点をつなぐバスに単一光子、コヒーレント光などを用いる様々な方式が考えられる。提案するプロトコルはこれらのどのようなものを用いたものでも構わないが、通信波長と量子ビットのプロセッシングを行う波長の整合性、必要となる量子プロセッサ、量子メモリ等の性能等が明確化でき、システム全体がスケーラブルに構成できるような将来性があるものに限る。具体的には、後述の到達目標が達成可能であるようなシステムの理論的な構成を行う。

課題ウ-2 量子中継のための量子メモリ、量子プロセッサの基盤技術開発

課題ウ-1 を満たす量子中継プロトコルでは、量子計算機などに比べ極めて小規模ではあるが、量子ビットを保持する量子メモリ、量子ビットに対する量子ゲート操作を行う量子プロセッサの技術が必要となる。量子ビットを保持、処理できる時間は系のコヒーレンス時間で決まるが、量子中継を実現させるためには、量子メモリでは一連の中継プロトコル全体にかかる総時間よりも長いコヒーレンス時間、量子プロセッサでは量子ビットのプロセッシングやメモリへの転写時間等よりも長いコヒーレンス時間を持つデバイスが必要となる。

本研究課題では、課題ウ-1 において提案される方式を実現するための要素技術としての量子メモリ、量子プロセッサの研究開発を行う。具体的な物理系、動作温度などはどのようなものでも構わないが、課題ウ-1 の提案で必要となる量子メモリ、量子プロセッシングのコヒーレンス時間を実証できるものに限り、その原理実証実験を行う。

課題ウ-3 量子中継システムの実証実験

課題ウ-1 の提案、課題ウ-2 の技術を用いて量子中継プロトコルを行うため、まずは隣接する 2 中継点間での量子もつれ状態配信を行うための基本システムを構成し、実験室レベルでの動作原理実証実験を行う。中継点間の距離は最低 10km 以上を達成することとし、またその実験結果から、将来的に中継点を増やして大規模量子中継システムを構成した際に、必要となる量子状態のスワッピング、純粋化等が実現可能であり、最終的に遠隔地で純粋化された量子

もつれ状態の保持が可能になること及び量子鍵配送の超長距離化への適用可能性を理論的に明らかにする。

５．研究テーマ選定の背景，研究開発の必要性及び他で実施されている類似研究との切り分け

１）当該研究テーマを取り巻く現状

単一光子検出技術

現在、実用を目指した検出器として、大きく分けて半導体に基づく方式と超伝導体に基づく方式の研究開発が進められている。特に GHz レベルの高速動作が期待される超伝導体検出器は、先行する米国に追いつくために集中した開発体制を早急に整える必要があるが、これについては情報通信研究機構が自ら実施する研究として進める。以下、当該 2 方式の現状を述べる。

半導体に基づく光子検出については、2004 年には NEC での単一光子検出器の動作速度で 62.5MHz が達成されたとの報道がなされている。これは一旦光検出を行った場合、不感時間を 10μsec 程度設ける設計となっており、実効 100kHz の繰り返しとみなされる。この結果は市販品を流用したにも関わらず高速化が実現されており、最適化を行ったサンプルでは更なる性能の向上が期待できる。同様に C. Elliott(BBN Technology) 等による quant-ph/0412029 The DARPA Quantum Network(2004) 及び quantph/0503058 Current status of the DARPA Quantum Network (2005) というレポートにおいて、BBN Technology 社、ハーバード大学、ボストン大学の３拠点間を結ぶ量子鍵配送ネットワークの実証実験に成功している。その際使用した検出器としては Epitaxx 社製品の APD を用いている。動作速度としては 5 MHz となっているが、不感時間を数μsec 設けており、量子効率も 10～20%程度である。その他の機関において同様に Epitaxx 社製品を用いて量子効率が 30%に迫る値での使用例が報告されているが、(M. Fiorentino 等 Northwestern University 米国、IEEE Photonics Tech. Lett. Vol. 14, No. 7, 983 (2002))ダークカウントが 10^{-3}/pulse 以上であり、量子鍵配送用途での動作条件下で運用されてはいない。化合物半導体 APD については、材料や構造の最適化は成されておらず、この材質での限界を見極める状況にない。一方非線形結晶を用いて長波長の光子を短波長に波長変換して Si-APD で検出するという試みが米国スタンフォード大学と NTT のグループにより報告されている(New J. Phys. 7 (Nov.2005) 232.)。ここで使用されている Si-APD の動作速度は 20 MHz の同期信号を必要としない単一光子検出器である。また量子効率も 60～70%と高く、ほぼ 100%の確率で波長変換できる技術と組み合わせ、量子鍵配送のデモンストレーションが行われているが、ダークカウントが 1M c/sec 程度あり、安全な鍵配送距離を限定している要因となっている。

超伝導体に基づく光子検出については、現時点において量子効率は 1%程度ではあるが、1～2GHz 動作が可能であるとの示唆が論文で報告されている（A.Korneev et al. Appl. Phys.

Lett., Vol. 84, No. 26, 2004)。量子効率と動作速度は二律背反しており、性能改善にはキャビティー構造等の工夫を必要とする。上の動作速度は NbN 材料から決定される動作限界に近い目標値であるため、更に臨界温度の高い材料での試行が必要となる。

量子鍵配送システム

2002 年 6 月、スイス id Quantique 社が世界で初めて量子暗号装置を商用化して以来、欧米ベンチャーによる製品化が相次ぎ、現在では、100km 程度の鍵配送ができるようになっている（但し、生鍵であって、必ずしも安全性が確保されたものではない)。

近年、欧米では、多額の国家予算を投入して研究開発を加速している。特に、米国においては DoD(The Department of Defense)が総額 20.6 百万ドル（約 22 億円）出資して量子暗号など量子情報関連のプロジェクトを推進中で、全体的には 50 百万ドル（約 55 億円）がここ数年のうちに量子暗号に対して投資されると予想される。最近では国家機密に属する研究開発課題に移行しつつある。欧州においては、ＦＰ６において量子暗号のネットワーク化を目指し、４１研究機関、１２カ国(Austria, Belgium, Canada, the Czech Republic, Denmark, France, Germany, Italy, Russia, Sweden , Switzerland, United Kingdom)が参加する SECOQC (Development of a Global Network for Secure Communication based on Quantum Cryptography)なるプロジェクトが 2004 年 4 月に開始されている。出資額 11.4 百万ユーロ(約 16 億円)で、4 年間で量子暗号ネットワークを構築することを目的とし、コヒーレント光－ホモダイン検波型量子暗号（ジュネーブ大にて 20 光子/パルスの信号で、14km 伝送で秘密鍵 1.2kbps の生成に成功：Legre et al. quant-ph/0511113）や量子ワイヤレス通信も含む研究開発が進められている。

アジア圏では、シンガポールにおいて、政府の研究開発プロジェクトの一環で、シンガポール大学等が実用規模の量子暗号網の実証システム構築を 2002 年から進めている。

国内でも 2001 年から情報通信研究機構の委託研究「量子暗号技術の研究開発」として量子暗号システムの研究開発を実施し、その成果として既設ファイバを用いた 96km フィールド試験や商用ファイバ（16km）による平均最終鍵生成レート 16kbps での 14 日間連続運転などに成功している。また、Stanford 大学－NTT により、105km にわたって約 200bps の秘密鍵の生成に成功している。このように 1 対 1 の量子暗号については短距離で実用段階に入ってきたと言える。

一方、こうした１対１のリンクとしての利用からネットワークでの利用実現へ向けた動きが欧米で始まっている。米国では、BBN Technologies 社、ハーバード大学、ボストン大学が３地点を結ぶ量子暗号ネットワークの屋外実証実験に成功し（C. Elliott(BBN Technology)らによる quant-ph/0412029 The DARPA Quantum Network(2004)及び quantph/0503058 Current status of the DARPA Quantum Network(2005)でのレポート)、最近ではノード数を 10 まで増やし、光ファイバベースの位相変調方式から量子もつれ光子を

用いたもの、自由空間量子暗号までカバーするようになっている。スイスでは、id Quantique 社とデックポイント社が共同で、量子暗号を使ったネットワークサービスのデモを行っている（2004 年 9 月）。さらに、NIST(National Institute of Standards and Technology)のチームが Acadia Optronics と共同で、自由空間 730m の距離で最大 1Mbit の鍵を共有（2004 年 7 月）するなど、光ファイバを用いない自由空間量子暗号への取り組みも始まっている。このような国内外の動向を踏まえ、量子暗号システムの市場は、ここ数年で 200 百万ドル(約 220 億円)に達するとの予想もある(MagiQ VICE PRESIDENT, Andrew Hammond 氏)。

量子中継

量子暗号の長距離化や、その他の量子情報プロトコルのネットワーク化を進めていくにあたって、量子中継はその重要な基幹技術の一つである。その将来的な重要性は世界各国で強く認識されており、欧米の主要研究グループでは国家や EU のプロジェクトによるサポートの元、各機関の連携により、基礎理論、基礎デバイスの探索からシステム技術開発までの系統的な研究が近年急速に進められている。一方、我が国では、基礎的、萌芽的な内容を中心とした研究では優れた成果があるものの、これらの研究はそれぞれの研究室で個別に行われるにとどまっており、量子中継のシステム構成からデバイス開発まで一貫した研究開発体制の確立が急務となっている状況である。

２）研究開発の必要性

単一光子検出技術に関しては、半導体での単一光子検出器は結晶品質や積層構造の最適化を集中して行った研究例がほとんどなく、現有結晶成長技術における限界を見極めることが火急の課題である。また更なる結晶や層構造の高精度化へむけた基礎技術の確立が、将来のより高度な量子情報通信技術の基盤となる。

量子鍵配送システムについては、これまで情報通信研究機構の委託研究「量子暗号技術の研究開発」の成果を、メトロネットワーク、さらには基幹回線ネットワークへ適用して行くために、光ネットワーク技術を駆使して多機能かつ製品レベルの量子鍵配送システムを早急に開発する必要がある。これは依然、基礎的・先端的で研究リスクが大きく、産学官のポテンシャルを結集して国家戦略的に推進する必要がある。

量子中継技術の基本的な存在意義について述べる。現在開発が進められている主な量子暗号では、１つの光子、または弱いコヒーレント光パルスに秘密鍵の元となる乱数を載せて送受信する方式を用いているが、これらの方法では伝送路の損失により安全性と伝送容量が著しく制限されるため、1000km 圏程度の超長距離通信網で実用的な量子暗号を実現することは非常に困難であると考えられている。これに対して、まず純粋化された完全な量子もつれ状態にある光子対を送受信者の間で共有し、その後の状態の測定によって秘密鍵を生成する方法では、原理的には超長距離においても無条件に安全な量子暗号が可能であると言われている。これは、

伝送時は量子もつれ光子対自体は秘密鍵に関する特定の情報を含んでいないので、伝送路の損失で量子もつれ光子の量子状態が破壊されたとしても、途中の中継点で盗聴者へ秘密鍵の情報が漏洩されることなくその量子状態を回復することが可能だからである。このようにして 10～100km 程度で繋がれた各中継点での量子状態の回復を経て、最終的に純粋量子もつれ状態の光子を超長距離伝送し受信者へと届ける伝送技術が、量子中継技術である。量子暗号以外でも、量子もつれ状態は様々な量子プロトコルに必要な資源であるから、これらのネットワーク化を進める上では必須の技術になるものと予想される。

本研究テーマにおける量子中継技術の研究開発の必要性及び本研究テーマで想定している典型的量子中継手法とその用語について述べる。量子中継の典型的な手法では、隣接する中継点からそれぞれ、中継点と量子もつれ状態にある光子を発生し、それらの光子に量子スワッピングと呼ばれる操作を行うことにより、隣接中継点の間に量子もつれ状態を形成する。形成された中継点間の量子もつれは量子メモリにより保持しつつ、同様にして次々と連なる中継点間の量子もつれを形成していくことにより、最終的に送受信者の間でもつれ状態が形成される。また、各中継点では量子もつれ抽出等の方法による破壊された量子状態の回復の機構も組み込み、量子もつれの純粋性を保つ。従って、各中継点では小規模な（通常は単体で 1～2 ビットレベルの）量子メモリや、量子もつれ抽出に必要な小型量子プロセッサを組み込む必要がある。各中継点ではこのような量子メモリ、プロセッシングデバイスが必要な数、配置される（本計画書ではこの配置する数を「各中継点で用いる量子ビット数」と呼び、後述のようにそれが 100 個以下となるようなシステムの設計を目標とする）。現在の量子暗号技術を凌駕する伝送距離を量子中継で達成するには、ファイバ系において実装可能な量子中継プロトコルの新規開発、システム全体の設計などの理論的研究と、量子メモリ、量子プロセッサ等の各要素技術開発の双方の進展が必要とされている。

３）他で実施されている類似研究との切り分け

単一光子検出技術に関しては、これまでの委託研究課題においてはシステムとしての性能を最終目標としていたため、要素技術の高度化に必ずしも充分な予算が執行されていなかった。またその他基礎研究課題では通信波長帯に特化したデバイス技術開発は技術的困難さから敬遠されてきている。本研究テーマは予算的技術的問題から敬遠されてきた課題に相当し、国家戦略的に推進する必要がある。

量子鍵配送システムについては、科学技術振興機構や学術振興会の公募研究制度において量子鍵配送への応用をうたった基礎研究課題が数件実施されており、この中では、量子鍵配送ネットワークへ向けての量子もつれの制御技術研究や新しい量子鍵配送プロトコルの理論的研究が行われている。また、産業技術総合研究所では、量子鍵配送を戦略的な研究課題に挙げ、情報セキュリティ研究の一環として研究を拡大させる動きがある。しかし、フィールド試験まで入れた量子鍵配送ネットワークのシステム開発を総合的に推進することを目的としている

ものは本研究テーマのみである。

量子中継技術についても、既に、科学技術振興機構や総務省の公募研究制度において基礎研究に関する研究課題が数件実施されている。しかしながら、これらの課題はいずれもアカデミックな側面が強く、要素技術開発に向けた原子物理・固体物理の基礎研究や、学問としての体系化を目指した理論研究などが個別に進められているものである。一方、本研究テーマは、将来的に技術としての量子中継の確立を目指したものであり、そのため量子中継のシステム設計から要素技術開発まで一貫した研究体制で進める課題構成となっている。

６．研究開発の到達目標

課題ア　化合物半導体型単一光子検出器の研究開発

本課題と平行して進められる「課題イ-１　都市圏対応型量子鍵配送システム技術」の波長多重機能が対象とする波長帯において光子検出が可能であること。そして、課題イ-１ において開発予定の都市圏対応型量子鍵配送システムに実際に組み込んで、５０km 圏内で １ 対１の鍵生成速度 1Mbps をフィールド実証するのに十分な性能を実現すること。また、汎用化に向けたモジュール化も実施し、量産化の可能性と根拠も明示すること。そのための検出器単体の性能として下記の性能目標をひとつの目安とする。

実効的な光子検出レート	左記レートにおけるアフターパルス確率
１０ MHz	1E-5 以下

- Gated Geiger mode による動作を可
- 動作温度 ７７ K 以上

＜備考＞

上記数値目標は、現在の技術レベルに理想的な研究開発進捗を見込んで策定されたものである。その確度には、結晶や薄膜の高品質化という読みきれない技術要素による不確定さが含まれる。そこで、第一回中間評価の時点で一度、プロジェクトの成果及び国内外の研究開発の状況、技術レベルを精査し、再度適切な性能目標を検討し、必要に応じて修正する。

課題イ　量子暗号ネットワーク技術の研究開発

課題イ-1　都市圏対応型量子鍵配送システム技術の研究開発

50km 圏内のメトロ系 IP ネットワーク上において、1 対１の鍵生成速度 1Mbps 以上、８程度のノード間で自在な接続切り替えが可能で、小型化に対応した実用的量子鍵配送システムを構築し、フィールド実証を行うこと。また、標準化や CRYPTREC 登録を目指して、安全性の評価基準をまとめること。

課題イ-2　基幹回線対応型量子鍵配送技術の研究開発

鍵生成レート対伝送距離のトレードオフ曲線における世界トップクラスの性能を 100km 超の距離において実証すること。さらに終了年度までに、上記のメトロ系 IP ネットワーク対応の量子鍵配送システムとの接続試験を行い、実用化への可能性を立証すること。安全性の評価基準については課題イ-1 と同様とする。

課題ウ　量子中継システムの研究開発

課題ウ-1 量子中継システム設計の理論的研究開発

回線の長さ 1,000km 程度を想定した量子中継としては、通信・処理時間 1 秒程度で量子もつれ状態 1 つを 95%以上の忠実度で配送できるようなシステム、回線の長さ 10,000km 程度を想定した量子中継では、通信・処理時間 10 秒程度で量子もつれ状態 1 つを 95%以上の忠実度で配送できるようなシステムを提案すること。

なお、このような量子もつれ状態 1 つを配送する際に、中継点において量子もつれの抽出等の処理に用いる原子系や固体系の量子ビット数は、各中継点で各々100 個程度以下となるようにすること。

課題ウ-2 量子中継のための量子メモリ、量子プロセッサの基盤技術開発

量子メモリについては課題ウ-1 の目標に対応して 1 秒～10 秒より十分長いコヒーレンス時間、量子プロセッサについては具体的な操作（隣接中継点での量子もつれ状態の配信、プロセッサ／メモリ間の情報転写等）に必要な時間の合計よりも十分長いコヒーレンス時間を実証すること。

課題ウ-3 量子中継システムの実証実験

量子もつれ状態配送では、隣接中継点の間での動作原理実証として、10km 以上離れた 2 中継点間で、忠実度 75%以上の量子もつれ状態の配信を実験的に達成すること。また、その実証実験結果から、将来的に大規模量子中継システムが実現可能になることの理論的な証明を

示すこと。

７．期待される波及効果

量子暗号鍵配送システムの高速化、長距離化を実現でき、量子情報技術のもたらす恩恵を情報セキュリティという形で早期に広く国民に提供できる。開発する要素技術は、量子情報通信の新たな可能性の探求と各種の計測技術への強力な手段となり得、我が国の技術レベルの高度化を促進できる。また、高性能な量子もつれ光源、量子中継技術は、量子暗号のみならず様々な量子情報処理プロトコルにおいて必要とされ、量子情報通信・量子計算技術全般の発展に大きく寄与する。

８．研究開発スケジュール

本研究テーマの研究開発期間は、平成１８年度から平成２２年度までの５年間であり、スケジュールは概ね以下のとおりである。