資料２－２－２

量子情報通信分野の短中期的な研究開発戦略

～ 量子情報通信ＷＧ報告書概要 ～

２１世紀ネットワーク基盤技術研究推進会議
量子情報通信ワーキンググループ

量子情報通信技術の最近の動向

量子暗号が実用段階に

量子暗号システム（短距離、1対1）の商用化

○欧米ベンチャーによる量子暗号システムの製品化（伝送距離：数十km、鍵伝送レート：最大1kbps）【スイスid Quantique社（2002年6月）、米国MagiQ Technologies社（2003年2月）】

○国内では、100kbpsの量子暗号鍵配送（NEC）、96kmの屋外伝送実験（三菱）等の成果を踏まえ、2007年頃までに～100km、50kbps程度のシステム製品化を予定

量子暗号のネットワークでの利用実現へ

・米国DARPAの支援で、BBN Technologies社、ハーバード大学、ボストン大学が6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（2004年7月）

・id Quantique社とデックポイント社（スイス）が共同で、量子暗号を使ったネットワークサービスをデモ（2004年9月）

課題：量子暗号を伝送できる距離に限界　→　量子中継器が必要

量子もつれ制御、光子検出等、基礎技術が進展

○3者間量子テレポーテーションに成功（東大：2004年）

○半導体を用いた量子もつれ光子対の発生（東北大：2004年）

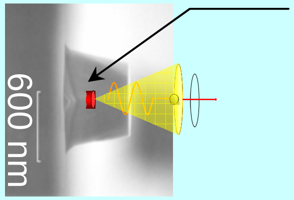
単一光子源等のデバイス開発が進展

最近の単一光子研究（2004年）

単一光子源まで至っていないが、通信波長帯（に近づいた）量子ドット研究が報告

グループ	国	デバイス	波長
東北大	日	CuCl単結晶薄膜を利用したエンタングルメント	390nm
国立科学技術センター	仏	Collidal CdSe/ZnS QD　室温	570nm
バーゼル大	スイス	窒素雰囲気, 10nmのポリメチルメタクリレート薄膜中20%のDiIC$_{18}$(3)分子を利用した単一光子発生。Si-APDを用いているため発光波長は1μm以下。	－
カナダ国立研究評議会	カナダ	サイト選択InAs/InP SQD成長。	1455nm
ローザンヌ工科大	スイス	InAs/GaAs SQD, 低温1.3μm帯発光	～1290nm
レッチェ大	伊	室温1.3μm動作の量子ドットLED, 低密度（1.6×10^{9}cm^{-2}）	1315nm@RT
レッチェ大	伊	InGaAs/GaAs QD-LED microcavity @RT.　MOCVD成長	1298nm@RT
ローザンヌ工科大	スイス	3D-microcavity型QD-LED @RT	～1170nm@RT

国内で、世界初の通信波長帯動作
（富士通/東大：2004年）



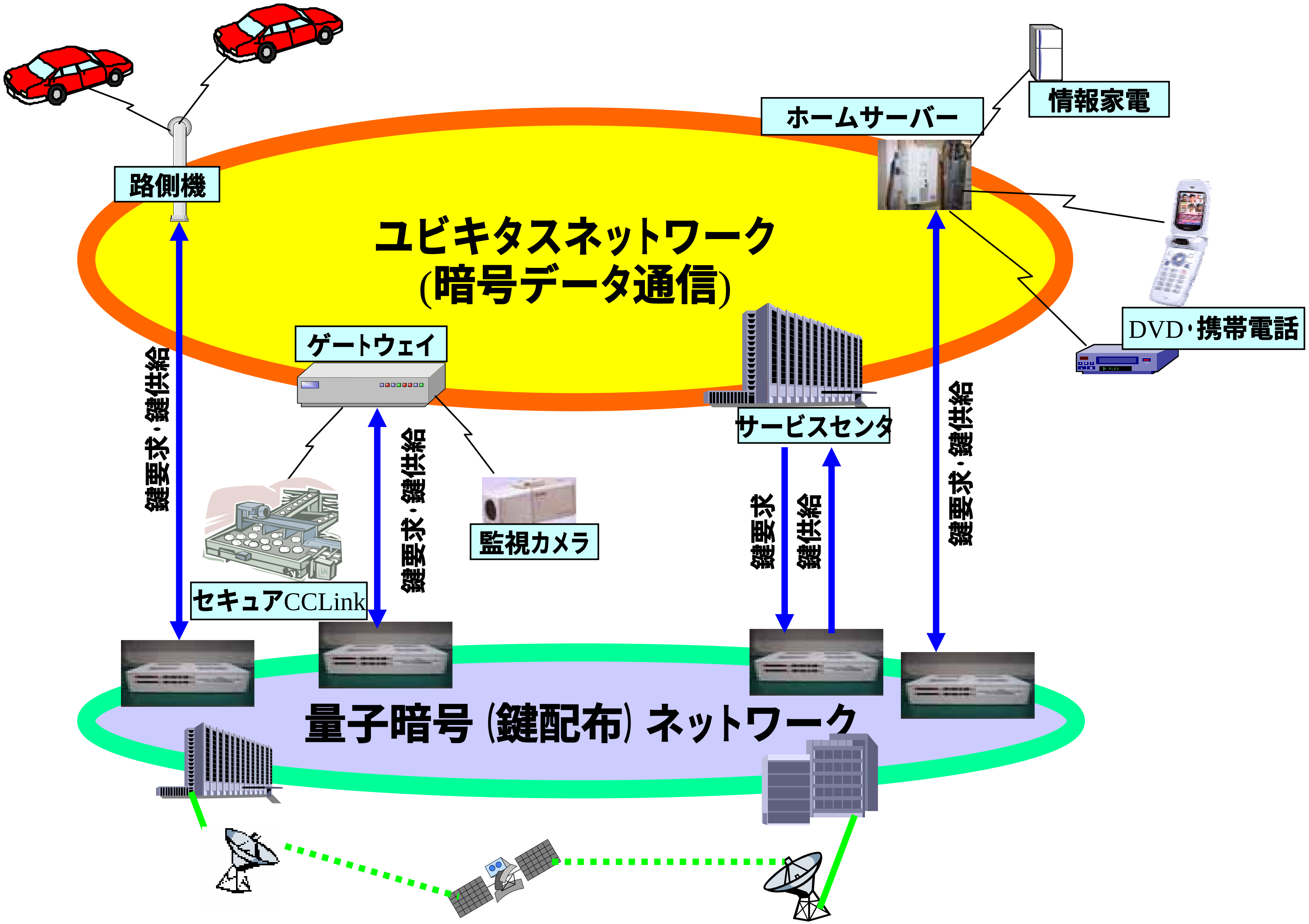
埋め込まれた量子ドットから放出される1.3μm単一光子

単一光子発生器

JJAP Express Letter, **43**, p. L993, 2004

○欧州で、量子テレポーテーションの屋外実験等、量子中継の原理実験が実施されるなど、量子もつれを用いたシステム研究が進展。
○また、FP6において、量子暗号のネットワーク化を目指す研究が2004年に開始（SECOQC; Development of a Global Network for Secure Communication based on Quantum Cryptography）。コヒーレント型量子暗号や量子ワイヤレスを含む研究開発が計画。

ユビキタスネット社会における量子情報通信の実現像



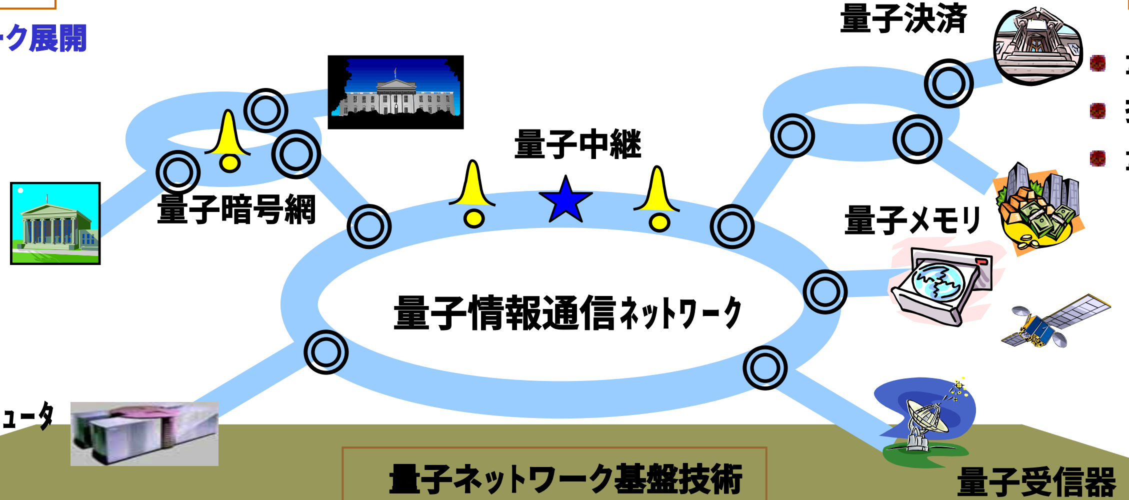
量子情報通信の研究開発課題

短期的課題 (2010年までに実現すべきもの)

中期的課題 (2015年までの実現に向け、2010年までに要素技術を確立すべきもの)

量子暗号テストベッド

- 量子暗号のメトロネットワーク展開
- 中距離量子暗号
- ワイヤレス量子暗号
- コヒーレント光型量子暗号
- 量子暗号プロトコルの評価



量子情報セキュリティ

- 量子中継による長距離量子暗号
- 携帯量子暗号
- 量子認証・決済

量子信号処理

- 量子通信路符号化技術
- 固体素子による光量子ゲート
- 原子系量子もつれ制御技術

量子ネットワーク基盤技術

- 量子波長変換技術
- 光-原子 /光-電子インターフェース技術
- 固体量子メモリ
- 量子もつれネットワーク/量子マルチパーティプロトコル

量子情報通信ネットワーキング

量子情報デバイス技術

- 量子制御光源技術 (単一光子/量子もつれ光源、スクィーズド光)
- 光子検出技術
- 光子数識別技術

量子情報理論

- 量子通信理論 / 量子情報基礎理論

共通要素・基礎技術

量子情報セキュリティ

- 安全性が物理学的に保証されている量子鍵配送（QKD）システムに関し、メトロネットワークへの展開を開始。複数のQKD装置間の接続を動的に切り替え、任意のQKD装置間で鍵配送を実現したり、盗聴検出があった場合でも、鍵配送レートを劣化させることなく最適迂回経路を設定可能とする制御技術を確立。
- 制御性の良い単一光子源の組み込みや単一光子/量子もつれあい 光子源に基づく量子暗号により、QKDシステムの小型・高性能化、長距離化を図る。
- 柔軟性に富む量子情報ネットワークを構築するために、量子ワイアレス通信技術の開発も必要。量子レベルのビームリンク技術、送受信技術を実現し、近接距離間用途（端末-端末間、地上短距離間通信など）への適用を目指す 。
- 他方、伝送損失への耐性を持ち、システム開発が比較的容易な、多光子状態を用いたQKDシステムの研究開発も重要であり、複数のアプローチにより現在の暗号システムと共存するセキュアなネットワークを構築。また、量子暗号の実用化のためには、長距離化と高伝送レート化に加え、セキュリティの保証に関する評価基準を示す必要。
- 中期的には、全国規模での量子暗号網の形成に不可欠な、量子中継による長距離量子暗号を実現するための研究開発の他、携帯量子暗号装置、量子クレジットカードによる量子認証等、QKD以外の量子セキュリティ技術の研究開発が重要。

2008年		2010年		2015年
・50km圏100kbps程度のメトロ対応量子暗号の実現 ・近距離（<1km）ワイヤレス量子暗号の実現 ・各種量子暗号方式の無条件安全性証明 ・セキュリティ保証の評価基準策定	▶	・100km圏1Mbps級のメトロ対応量子暗号の実現 ・単一光子源の組み込みによる量子暗号システムの高性能化 ・近距離（<1km）ワイヤレス量子暗号の実現 ・各種量子暗号プロトコルの評価	▶	・量子中継による長距離(>>100km)量子暗号の実現 ・カードサイズの量子暗号装置の実現 ・量子クレジットカードなどの携帯用認証の実現

＜要素技術＞
・波長多重システム技術、波長切り替え量子鍵配布、リコンフィギュアラブル量子鍵配送システム技術、超小型高性能量子鍵配布システム技術
・量子ビームリンク技術（光学系制御、検出等）、量子有無線シームレス接続技術
・量子もつれあい光子源、量子メディア変換技術、量子バッファ、認証プロトコル

量子ネットワーク基盤技術

- 量子中継に不可欠な、量子状態のメディア変換を可能とするため、光と原子/電子間での量子インターフェースに関し、固体素子と原子系という二つの方式で相補的に進めることが重要。
- また、フレキシブルな量子ネットワークシステム構成を可能にするため、伝送、信号処理、検出をそれぞれに適した波長帯で行い、その間を量子状態の非古典性を壊すことなく自在に波長変換する技術の開発が必要。
- これら量子波長変換技術や量子メディア変換技術を用いて、光の量子もつれをネットワークに展開し、量子情報の分散処理を行うことにより1対多、多対多の量子暗号プロトコル（量子マルチパーティープロトコル）を実現。

2008年

- 原子/イオン系の冷却、量子もつれ制御技術の開発
- 光と結合する安定な素励起の探索と制御技術の開発
- ナノ構造、フォトニック結晶作製技術の適用による光アクセス技術の開発

- 光パラメトリック過程の低損失化と高効率化

2010年

- 光子-イオン間、光ー原子集団間での量子状態転写の実証
- 光子-電子スピン-核スピン間での量子状態転写の実証
- 固体量子メモリの開発（核スピン、不純物束縛励起子等）

- 量子波長変換技術の原理検証とシステム実験

- 量子マルチパーティプロトコルの実装法
- 量子分散処理用デバイスの開発

2015年

- 少数ビットの演算による量子マルチパーティプロトコルの実現

＜要素技術＞
・量子ドット中の素励起の高速光制御技術、量子ドット構造・フォトニック結晶構造作製技術、冷却原子を用いた量子演算回路
・量子もつれの発生・制御、量子マルチパーティプロトコル、量子計算量・通信容量理論　等

量子信号処理

- 深宇宙通信や大容量光ネットワークにおける、減衰したコヒーレント信号から、最大の情報を取り出すための新しい符号化技術に関する研究開発に中期的に取り組む必要。特に、受信したコヒーレント信号のパルス間で最適な量子もつれ状態を生成しながら量子力学的な復号を行なう量子一括復号が重要。
- 光の量子信号処理の鍵となる光量子ゲートに関し、固体EIT、微小共振器、フォトニック結晶等の技術を利用して、固体素子による実現、デバイス化を目指す。
- また、冷却イオン系による量子計算に基づくハイゼンベルグ限界測定を行うことで、究極の測距技術や周波数・時間標準技術への応用を目指す。

2010年		2015年
・3～4モードの光量子計算システム構築	➤	・測定誘起型非線形過程による小規模量子符号化の実現
・少数(単一)光子での量子位相ゲート実現		・光量子ゲートの量子中継、量子通信への適用
・原子系量子もつれ制御技術による量子測距・時刻同期の物理スキーム探索		・原子系量子もつれ制御技術による量子測距・時刻同期の原理実証

＜要素技術＞
・非古典光の生成・制御技術、高感度の光子数識別技術
・小規模光量子信号処理技術
・量子最適受信技術　等

共通要素・基礎技術

- 量子情報デバイスとして、半導体量子ナノ構造に基づく通信波長帯単一光子源、通信波長帯量子もつれ光子対源、及び近赤外・通信波長帯におけるスクイーズド光源の研究開発と共に、高量子効率、低ダークカウントの通信波長帯光子検出器の開発が極めて重要。
- 中期的には、光領域での高度な量子信号処理へ向けて、近赤外、通信波長帯における光子数識別器の実現を目指す。
- また、量子通信路容量の解明等に寄与する量子通信理論や、量子もつれの基本的性質、定量化法の解明に関する量子情報基礎理論の研究により、量子情報ネットワークシステム高性能化への指針を構築。

2008年

- 通信波長帯単一光子源（繰り返しレート100MHz）
- 量子もつれ光子対源（100kc/s, ビジビリティ95%）
- 近赤外/通信波長帯パルス・スクイーズド光源（4～6dB）
- 量子効率40%、繰り返しレート10MHz以上の通信波長帯光子検出器

2010年

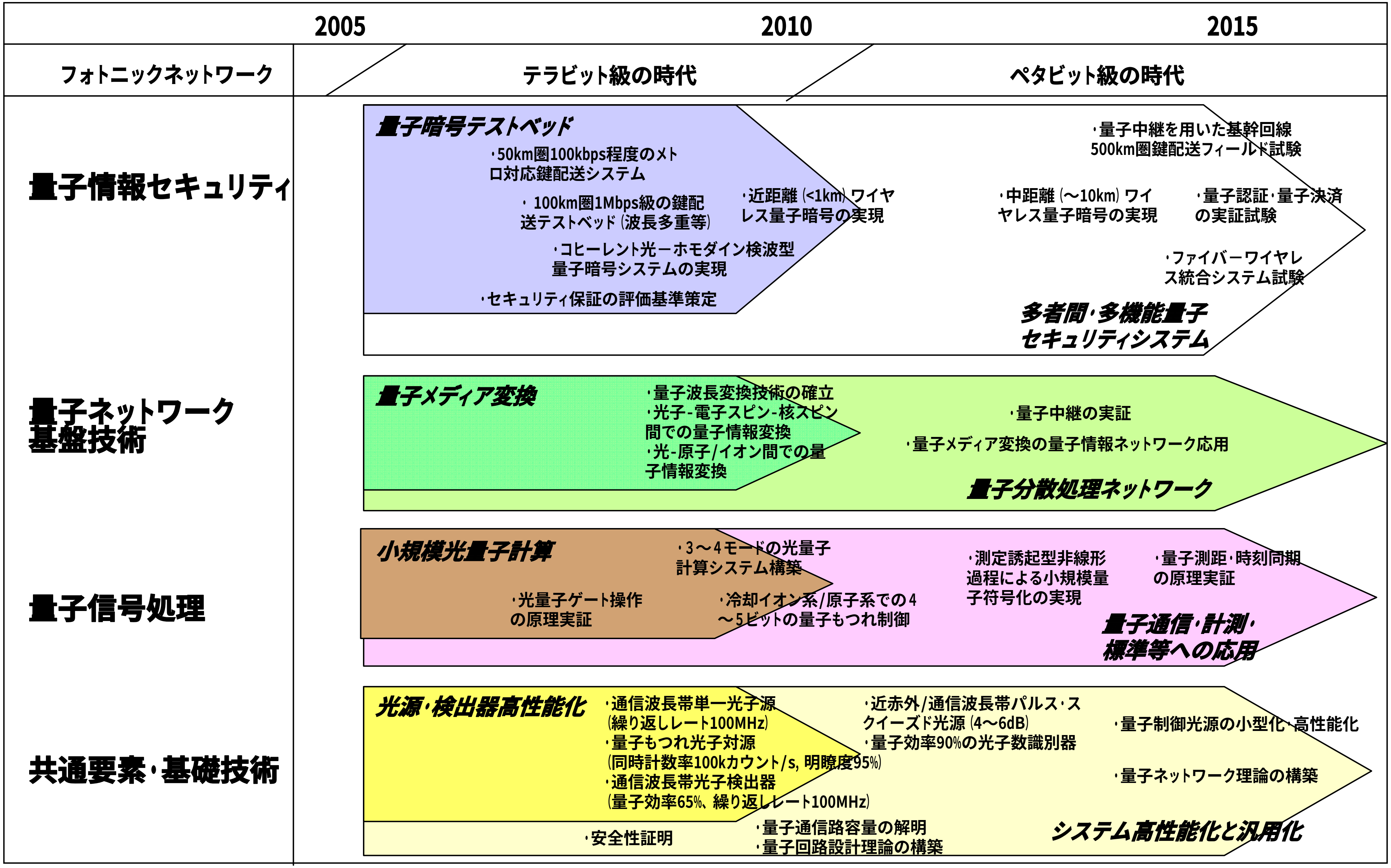
- 量子制御光源の小型化・高性能化
- 量子効率65%、繰り返しレート100MHz以上の通信波長帯光子検出器
- 近赤外帯で量子効率85%、繰返しレート10MHz程度、通信波長帯で量子効率90%、繰返しレート1MHz程度での光子数識別
- 量子回路設計理論の構築と実験への提供

2015年

- 光子数識別器（近赤外・通信波長帯）の量子効率、分解能の更なる向上（数値目標未確定）や新方式の検討（原子ガス、新規材料等）
- 量子ネットワーク理論の構築とネットワークシステム実験への提供

＜要素技術＞
・単一光子源、相関光子源、コヒーレント光制御技術
・単一光子検出器
・光子数識別技術　等

量子情報通信の技術開発ロードマップ（案）



量子情報通信研究開発の全体戦略について（案）

次世代フォトニックネットワーク

量子情報セキュリティプロジェクト

量子暗号通信を都市内ネットワークへ展開するためのシステム技術、柔軟性に富んだ量子暗号網を構築可能とする量子ワイヤレス通信技術等の研究開発を実施

2008年　1Mbps級のメトロ対応システム、
　　　　近距離（<1km）ワイヤレス量子暗号の実現
2010年　単一光子源の組み込みによる小型・高性能化等

安全性基準調査検討委員会

量子ネットワーク基盤技術プロジェクト

量子状態の転送による中継技術等、量子情報ネットワークを実現する上で鍵となる基盤技術に関し、ナノ技術を活用した研究開発を実施

2010年　量子メディア変換技術の実現
2015年　量子中継の実証等

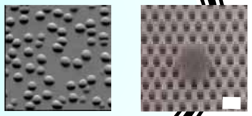
ナノITネットワーク

量子情報・ナノデバイス研究センター

量子ナノデバイスや量子情報理論等に関する総合的な開放型研究開発拠点

研究者ネットワーク

研究代表者会議等を通じた研究交流、情報交換等



基礎研究・理論研究

競争的研究資金等により、原理・フィージビリティの実証実験、量子情報理論等の基礎研究を実施

量子信号処理プロジェクト

光通信を超える超大容量通信や量子原子時計等を実現可能な、光量子による信号処理技術の研究開発 を実施

2010年　3～4モードの光量子計算システムの構築
2015年　量子通信路符号化装置の開発等