戦略的創造研究推進事業　CREST
研究領域
「量子情報処理システムの実現を目指した新技術の創出」

研究課題
「通信波長帯量子もつれ光子とその応用システム」

研究終了報告書

研究期間　平成17年10月～平成23年3月

研究代表者：井上　恭
（大阪大学大学院工学研究科、教授）

§1 研究実施の概要

本チームは、ファイバー伝送系への展開を念頭に、通信波長帯の量子情報通信技術の確立を目指して研究を推進した。具体的には、ポイント-to-ポイント(P2P)量子鍵配送(QKD)に関する研究、量子もつれ光子発生技術及びそのシステム応用技術、単一光子検出をはじめとする周辺技術、などである。以下、各項目について、実施内容と得られた成果の概略を述べる。

本チームの研究テーマは「量子もつれとその応用システム」である。もつれ応用システムの大きな目標のひとつは量子もつれQKDによる暗号鍵配送距離の拡大であるが、その前段階としてP2Pシステムの性能を見極めることが重要と考え、これに関する実験的・理論的研究を行った。その中で特筆すべき成果は200kmファイバーQKD実験である。本チームが培ってきたオリジナルプロトコルである差動位相シフト(DPS)QKD の実験系に低雑音・高速動作特性を有する超伝導単一光子検出器を適用することにより、世界最長距離を達成した。本実験では、それまでの秘密鍵生成速度に関しても、それ以前の記録を大幅に更新した(2桁以上@100km)。またその他にも、実用性を意識した正弦波ゲート動作 InGaAs/InP-APD 光子検出器を用いた高速 QKD 実験や中短距離での高速鍵生成を目指した周波数上方変換型単一光子検出器を用いた1 Mbit/s鍵生成実験など、P2P－QKD 実験に関する最先端の成果を得た。実験の他にも、強い参照光を用いる B92 プロトコル及び単一光子DPS-QKDの無条件安全性証明や実際のデバイスに即したBB84プロトコルの無条件安全性証明など、QKD の安全性理論に関する成果を得た。さらには、DPS－QKD プロトコルのシステム性能向上を目的とする4値DPSやデコイDPS、実用性向上を目的とする巨視的DPS、B92の実用性を高めるプロトコル、などの新規または改良QKD方式の提案・システム性能評価や、暗号鍵を2者に分割して供給する量子秘密共有を DPS のアイデアにより実現するプロトコルの提案・実証実験、などを行った。

本チームの主要テーマである通信波長帯量子もつれ光子に関しては、まず発生技術の確立を図った。光ファイバー内の自然四光波混合(SFWM)による発生法、周期反転分極 $LiNbO_3$(PPLN)内のパラメトリック・ダウン・コンバージョンによる発生法、シリコン細線導波路内のSFWMによる発生法など、各種発生方法について、システム実験に適用可能な高品質かつ高安定な量子もつれ光源を開発した。前2者は原理確認レベルであったものをシステム実験可能なまでに性能アップした成果であり、最後の発生法は本チームが世の中に先駆けて行いその有効性を示した成果である。

次に、発生させた量子もつれ光子のファイバー伝送実験を試みた。冷却した光ファイバーから発生させた時間位置もつれ光子の 60km 伝送、連続ポンプ PPLN もつれ光源から発生させた時間位置もつれ光子の 100km 伝送、ファイバーループ PPLN 光源からの偏波もつれ光子の 82km 及び 132km 伝送、などを行い、長距離にわたってファイバー伝送させても良好に量子もつれ特性が保たれることを示した。これらは、量子もつれ光子のファイバー伝送距離のトップデータとなる成果である。そしてこれらの成果を基に、ファイバー伝送量子もつれQKD実験を行った。まず、PPLNもつれ光源と超伝導光子検出器を用いて、100kmファイバー伝送量子もつれQKD実験に成功した。さらには、シリコン細線導波路もつれ光源と正弦波ゲート InGaAs/InP-APD 光子検出器を用いた 100km ファイバー伝送量子もつれ QKD 実験にも成功した。これらは、ファイバー伝送量子もつれQKDの最長距離実験となった。

その他の量子もつれシステム実験として、独立したファイバーもつれ光源あるいは PPLN もつれ光源からの光子を用いて Hong-Ou-Mandel 型量子干渉実験を行い、これらの光源から識別不可能性を有する光子が得られることを実証した。さらにこれらを用いて量子もつれ交換実験を行い、異なる光源から発生する光子間に量子相関を形成することに成功した。これは、QKD の伝送距離拡張のための量子リレーあるいは量子中継システムにつながる成果である。

上記の他にも、フォトニック量子インターフェースに関する実験、広帯域量子もつれ光子発生実験、APD 光子検出器の性能向上に関する検討、周波数変換型光子検出器の偏波無依存化、量子/古典波長多重伝送に関する検討、光雑音を用いた乱数発生法の検討、などを行った。

§2. 研究構想

（1）当初の研究構想

「量子もつれ」は特異な性質を有する量子力学的状態として関心を集めているが、本プロジェクト開始当時は主に物理学的興味の対象であり、応用技術としての研究はあまりなされていなかった。そこで本プロジェクトは、量子もつれ光子のファイバー通信への応用技術を開拓することを目標として研究を開始した。具体的には、通信波長帯での量子もつれ光子発生技術の確立やその応用システムの検討並びに実験的検証、及びそれらの関連技術の開発、などである。以下、各項目について当初構想した研究計画・進め方の概要を述べる。

通信波長帯量子もつれ発生技術の確立：光ファイバー内の自然四光波混合または周期分極反転 $LiNbO_3$（PPLN）内のパラメトリック・ダウン・コンバージョンによる通信波長帯量子もつれ光子発生技術を開発する。もつれ状態としては、NTT グループは時間位置もつれ、産総研グループは偏波もつれ、を検討対象とする。これらの量子もつれ状態について、システム応用実験に適用可能な高効率/低雑音/均一/高安定なもつれ光子発生源の実現を目指す。具体的な手法は、光フィルタリングやポンプ光条件の最適化、光学系安定化技術の開発、など。

応用システムの提案・評価：応用システムとして、(i) 量子もつれ秘密鍵配送、(ii) 差動位相シフト量子秘密共有、(iii) 動的制御量子もつれ秘密共有、(iv) 偏波もつれ光子によるマルチパーティー量子鍵配送、などについて検討する。項目(i)は時間位置もつれを用いて量子鍵配送の伝送距離を拡大するシステムである。もつれ光子対のそれぞれを離れた2者（アリス、ボブ）に送信する鍵配送システムや、もつれ光子源を2つ用意し、それぞれからのもつれ光子対の片割れを{アリス、ボブ}へ送る一方、残りの光子同士を一括測定（ベル測定）する量子リレーシステム、などがある。項目(ii)は、チャーリーが送る暗号文を{アリス、ボブ}が協力したときのみ解読できるという機能を差動位相シフト（DPS）量子鍵配送（QKD）のアイデアで実現するシステム、項目(iii)は時間位置もつれを用いてその機能を実現するシステム、項目(iv)は複数の偏波もつれ光子対を用いて複数の受信者に同時に暗号鍵を配布するシステム、である。これらのシステムの性能（鍵生成効率、配布距離、など）について検討する。

光子検出技術の開発：量子情報通信システムの実現にあたっては、単一光子検出が基本要素技術である。光子検出技術として、通信波長帯光子を短波長帯に波長変換し、高性能な短波長用 Si-APD で光子検出する周波数変換型光子検出法、及びクエンチ動作 InGaP-APD 光子検出器について検討する。

システム実験の実施：上記の結果を踏まえ、量子もつれ鍵配送などのシステム実験を実施する。

（2）新たに追加・修正など変更した研究構想

上記は当初作成した研究計画書の内容を要約したものであるが、研究を進めていく中で、当初計画にはなかった研究項目も構想・実施した。

第一世代であるポイント-to-ポイント量子鍵配送（QKD）は当初計画には含まれていなかったが、量子もつれ QKD に移行する前段階としてそのシステム性能や実用性を見極めておくことが重要と考え、本プロジェクトの中で採り上げることとした。具体的な内容は、オリジナル QKD プロトコルである差動位相シフト QKD 方式の長距離ファイバー伝送実験や高速鍵生成実験、さらに改良プロトコルの検討、などである。また、プロジェクト遂行途中で NTT グループに QKD 安全性解析の専門家が加わったことから、これに関する項目も採り上げた。

量子もつれ発生技術に関しては、光ファイバーあるいはPPLNによる発生法の研究を進めていく中で、新たな発生法の検討も必要と考え、またNTTの他研究所において光通信応用を目的とするシリコン細線導波路の研究が進展したこともあり、シリコン細線導波路内の自然四光波混合による量子もつれ発生を構想・実施した。

また応用システム実験としても、当初計画では想定しなかった項目を構想・実施した。波長の異なる2光子の識別可能性消去や単一光子の周波数下方変換などである。

以上のように新たに加えた研究項目がある一方で、実施しなかった項目もある。動的制御量子もつれ秘密共有実験、偏波もつれ光子によるマルチパーティー量子鍵配送、クエンチ動作InGaP-APD光子検出器、などである。これらは、他の項目を優先して行ったため実施に至らなかった。

§３ 研究実施体制

(1)「阪大」グループ

① 研究参加者

氏名	所属	役職	参加時期
井上 恭	大阪大学・工学研究科	教授	H17.10～H23.3
森島 健太	同上	修士学生	H17.10～H18.3
渡辺 一弘	同上	修士学生	H17.10～H19.3
田代 隆義	同上	修士学生	H17.10～H19.3
玉尾 圭史	同上	修士学生	H17.10～H19.3
林 周作	同上	修士学生	H18.4～H20.3
野口 由比多	同上	修士学生	H18.4～H20.3
大橋 徹也	同上	修士学生	H19.4～H21.3
岩井 祐樹	同上	修士学生	H19.4～H21.3
久木田 達哉	同上	修士学生	H20.4～H22.3
武田 真	同上	修士学生	H20.4～H22.3
細川 圭吾	同上	修士学生	H20.3～H22.3
普照 伶	同上	修士学生	H20.4～H22.3
殿井 雄介	同上	学部生	H20.10～H21.3
河原 光貴	同上	修士学生	H20.10～H23.3
高田 博史	同上	修士学生	H21.4～H23.3
岡 徹	同上	修士学生	H22.4～H23.3
欅田 直也	同上	修士学生	H22.4～H23.3
清水 勝一郎	同上	修士学生	H22.4～H23.3
北之園 静香	同上	チーム事務員	H17.10～H23.3

② 研究項目

・ 全体取りまとめ及び応用システムの提案・性能評価

(2)「NTT」グループ

① 研究参加者

氏名	所属	役職	参加時期
武居 弘樹	NTT 物性科学基礎研究所	主任研究員	H17.10～H23.3
都倉 康弘	同上	部長	H17.10～H23.3
本庄 利守	同上	研究主任	H17.10～H23.3
清水 薫	同上	主幹研究員	H17.11～H23.3
玉木 潔	同上	社員	H18.4～H23.3
橋本 卓郎	芝浦工業大学	修士学生	H19.4～H20.3
原田 健一	NTT 物性科学基礎研究所	博士研究員	H20.4～H22.3
Myrtille Hunault	Ecole Superieure de Physique et Chimie Industrielles de Paris	修士学生	H21.10～H21.12

②研究項目

・ 時間位置もつれ光子対を用いた量子通信実験

(3)「産総研」グループ

①研究参加者

氏名	所属	役職	参加時期
吉澤　明男	(独)産業技術総合研究所	主任研究員	H17.10～H23.3
土田　英実	同上	上席研究員	H17.10～H23.3
大舘　暁	同上	CREST 研究員	H18.4～H19.8
薛　迎紅	同上	特別研究員	H21.4～H23.3

②研究項目

・　偏波に基づく多光子間量子もつれ合い技術の開発

§4 研究実施内容及び成果

4．1 量子通信システムの提案・評価（大阪大学 井上グループ）

(1)研究実施内容及び成果

阪大グループは、プロジェクト全体を取りまとめるとともに、量子鍵配送（QKD）の方式提案、特に代表研究者発案の差動位相シフト（DPS）QKD プロトコルを軸とした新方式・改良方式の提案及びそのシステム性能評価を行った。また、QKD システムの実現に向けた様々な周辺要素技術の検討・開発を行った。以下、項目ごとに具体的な実施内容を述べる。

量子秘密共有システム

チャーリーの暗号鍵をアリスとボブが分割して所有し、アリスまたはボブ単独ではチャーリーの暗号化データを解読できず両者が協力した場合にのみ解読可能、という機能を提供するシステムを秘密共有という。量子秘密共有は、この秘密共有を量子力学の原理により実現するシステムである。これに関し、量子秘密共有を微弱コヒーレントパルス列を用いるという DPS-QKD の発想に基づいて実装するプロトコルを考案した。

図 1-1 にその基本構成を示す。アリスは{0, π}でランダム位相変調された平均 1 光子／パルスの微弱コヒーレントパルス列をボブに送信し、ボブはこれにさらに{0, π}のランダム位相変調を加えてチャーリーに転送する。チャーリーは、受け取ったパルス列の位相差を1ビット遅延干渉計により測定する。すると、{0 + 0 = 0, 0 + π = π, π + π = 2π = 0}であるので、チャーリーの測定結果はアリスとボブの変調位相の排他的論理和 XOR となる。したがって、アリス・ボブ単独ではチャーリーの測定結果は分からず、両者が互いの変調位相を照合してのみ知ることになる。このことを利用して暗号鍵を生成すると、秘密共有機能が実現される。

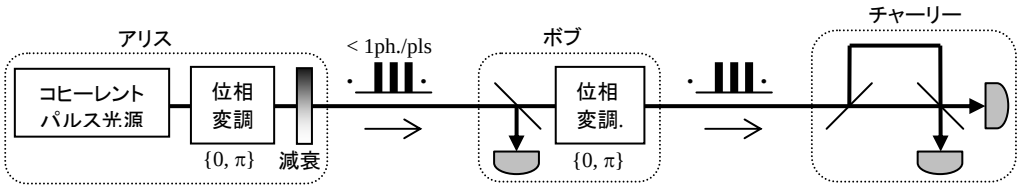


図 1-1.DPS 量子秘密共有の構成

生成した鍵の安全性は、DPS-QKD と同様にして、微弱コヒーレントパルス列の位相は完全には測定できないことより保証される。なお秘密共有では、通常の1対1鍵配送と異なり、3者のうちの誰かが裏切って一人で鍵情報を独占することができないように仕組まれていなくてはならない。図 1-1 の構成図において、ボブが入力光の一部を分岐して光子検出しているのは、アリスの裏切りを許さないためである。

本プロトコルについて、各種盗聴を考慮したシステム性能（鍵生成率、伝送距離）を評価し、さらに実証実験を行った。

これまでも、量子秘密共有としていくつかのプロトコルが提案されているが、それらは量子もつれ光子を用いていたり、BB84-QKD プロトコルに準拠して基底の一致/不一致を利用していたりした。これらに対し本提案方式は、微弱コヒーレントパルス列を用いておりまた基底選択のプロセスが不要であるため、構成が簡便で実用に適したシステムとなっている。

差動4値位相シフト（DQPS）量子鍵配送方式

DPS-QKD 方式には、無条件安全性が未証明という課題があり、また、連続クリック・インターセプト・リセンド攻撃と呼ばれる盗聴により伝送距離が制限されることが指摘されてい

た。これらに対処する方法として、差動4値位相シフト(Differential Quadrature Phase Shift: DQPS)量子鍵配送方式を考案した。

図 1-2 にその基本構成を示す。送信者は位相が{0, π}{π/2, 3π/2}のいずれかである微弱コヒーレントパルス列を送信し、受信者はこれを位相差 0 またはπ/2 の遅延マッハツェンダー干渉計(MZI)でランダムに選択受信する(図 1-2)。位相差{0, π}の信号を位相差 0 の MZI で受信または位相差{π/2, 3π/2}の信号を位相差π/2 の MZI で受信すると確定した測定結果となり、そうでない場合には不確定となる。そこで、確定的な測定事象より秘密鍵を生成する。

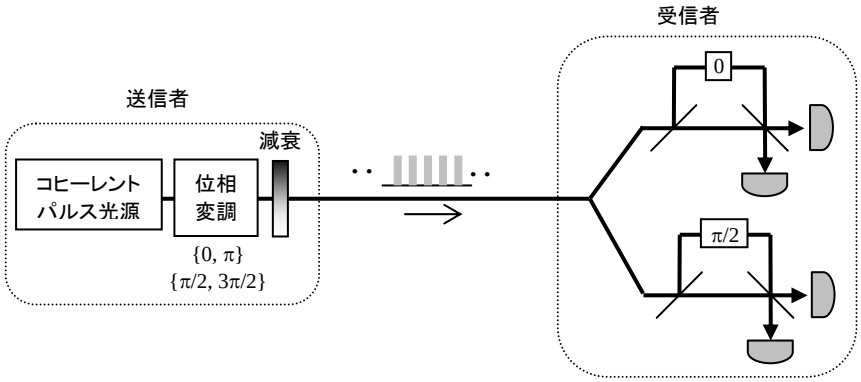


図 1-2. DQPS 量子鍵配送の構成

このプロトコルの基本構造は、代表的な QKD プロトコルである BB84 に類似している。すなわち、非直交関係にある4状態{0, π}{π/2, 3π/2}を使用し、基底の一致/不一致を利用して安全性を確保している。このため、従来の DPS-QKD において課題であった連続クリック・インターセプト・リセンド盗聴に対して強固なシステムとなっている。さらに、微弱コヒーレントパルス列を用いるという DPS プロトコルのアイデアを踏襲しており、これによりBB84 の難敵である光子数分岐攻撃に対する耐性も備えている。

本プロトコルについて、連続クリック・インターセプト・リセンド攻撃及び一般個別攻撃に対するシステム性能を解析し、従来の DPS 方式よりも伝送距離が拡大されることを示した(図 1-3)。また、実証実験も行った。

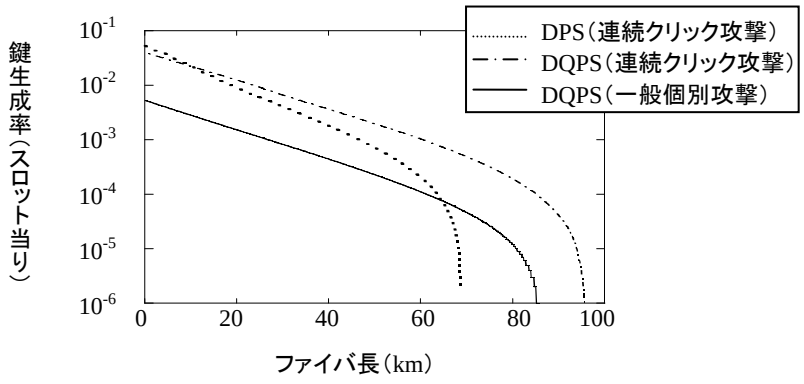


図 1-3. DQPS 量子暗号方式の秘密鍵生成率

本提案方式は、DPS－QKD のアイデアと直交・非直交を利用するという伝統的な BB84-QKD プロトコルの考え方を組み合わせたものである。そのため、BB84 の安全性レベルに準拠しつつ、光子数分岐攻撃に対して強いという DPS 方式の特長を併せ持った方式となっている。

デコイ DPS 量子鍵配送方式

DPS-QKD の安全性を高める方式として、デコイ(おとり)DPS－QKD 方式を考案した。

図 1-4 にその基本構成を示す。送信者は通常の DPS 信号光パルス列にそれより振幅の大きいパルス(デコイパルス)をランダムに挿入して送信する。盗聴者は信号パルスとデコイパルスを区別できないため、盗聴に際してデコイパルスも信号パルスと同様に処理する。すると、受信者は常に一定振幅のパルス列を受け取ることになる。一方、正常時であれば、デコイパルススロットでの光子検出確率は信号パルスよりも高いはずである。つまり、盗聴が行われると、デコイパルススロットでの光子検出率が正常時と盗聴時で異なることになる。この差より盗聴を発見する。

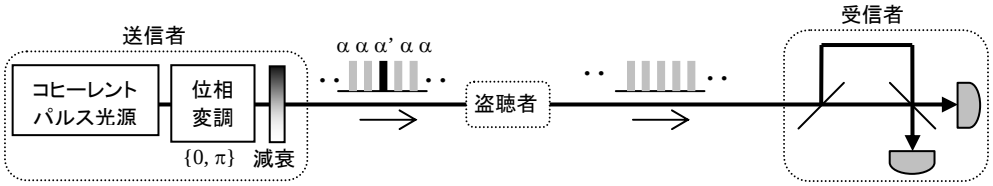


図 1-4. デコイ DPS 量子鍵配送方式の構成

本提案方式について、従来の DPS 方式に対するものと同じ盗聴攻撃を受けた場合のシステム性能を評価し、従来 DPS 方式より長距離化が可能であることを示した(図 1-5)。

本方式は、BB84-QKD で用いられているデコイ法を DPS-QKD に適用したものである。BB84 ではデコイ方式による無条件安全性が証明されている。今のところデコイ DPS の安全性については従来の具体的盗聴法に対しての検討のみであるが、デコイ BB84 と同等の安全度が期待される。

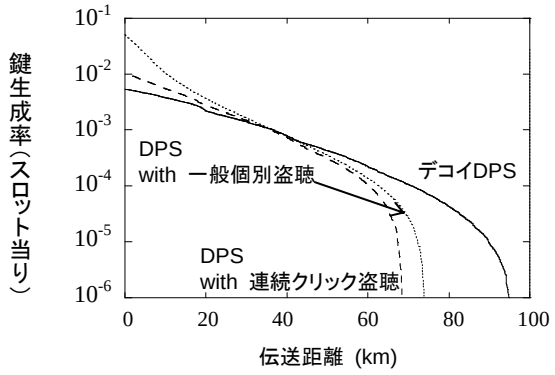


図 1-5. デコイ DPS－QKD の鍵生成率

フレーム化 DPS 量子鍵配送

連続クリック・インターセプト・リセンド盗聴に対する別の対処方法として、フレーム化 DPS 方式を発案した。送信者は、DPS 信号をフレーム化し、フレーム間には空パルスを挿入して送信する(図 1-6)。空パルスの位置は後で受信者に通知する。このような信号に連続クリック・インターセプト・リセンド盗聴が仕掛けられると、フレームの端スロットでの光子検出率が正常時と盗聴時で違ってくる。この違いから盗聴を検知する。まだ発案段階で詳細なシステム性能は未検討であるが、前述の対策法(DQPS、デコイ)より簡便な構成で連続クリック・インターセプト・リセンド盗聴を防御できることが期待される。

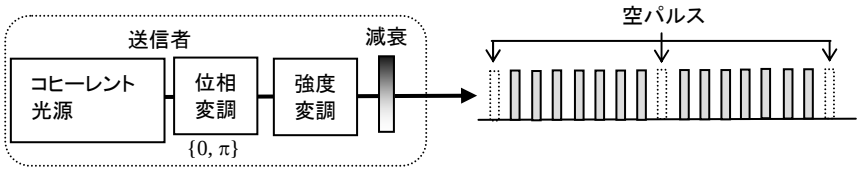


図 1-6. フレーム化 DPS-QKD の送信信号

巨視的 DPS 量子鍵配送方式

光子を用いる量子鍵配送では、単一光子検出が実装上の大きな課題となっている。これを回避すべく、コヒーレント光をホモダイン検出する量子暗号方式(連続変数 QKD)も最近盛んに研究されているが、そこでは微弱光に対する安定かつ過剰雑音の小さいホモダイン検出技術が必要となる。これらの課題に鑑み、通常の光通信システムと同じ送受信機構成で秘密鍵を配布する方式を考案した。

図 1-7 にその基本構成を示す。送信者は一定振幅のコヒーレント光を{δ, −δ}でランダムに位相変調して送信する。ここで、δ は2つのコヒーレント状態が量子雑音のため一部が重なり合う程度に小さいものとする(図 1-8(a))。また送信光パワーは、このコヒーレント状態がファイバー伝送後に通常の光検出器で直接検波可能なレベルとする。受信者は、伝送されてきた信号光を光増幅器により前置増幅し、1ビット遅延干渉計を通した後、直接差動検波する。これにより受信者は、位相差{−2δ, 0, 2δ}に対応する3値の復調信号を得る。ここで、各復調信号レベルは、前置増幅器雑音/量子雑音/熱雑音等のため変動しており、その確率分布は図 1-8(b)に示すように3値に対応するピークが重なり合った形となる。これに対し受信者は、高い方のピーク及び低く方のピークの外側に閾値{+d, −d}を設定する。

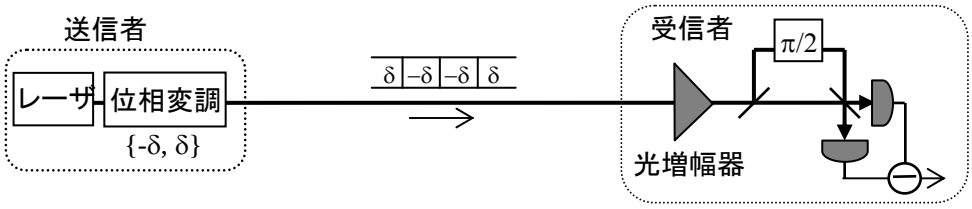
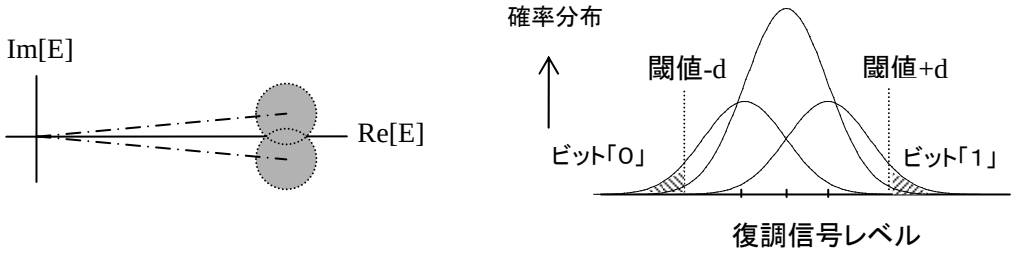


図 1-7. 巨視的 DPS-QKD(光前置増幅型)の構成



(a)送信光 (複素電場) の状態　　(b)復調信号の分布状態

図 1-8. 巨視的 DPS-QKD における送受信状態

以上の構成を用いて、送受信者は次の手順により秘密鍵を生成する。(i) 受信者は、+d より大きい復調信号よりビット「1」を、−d より小さい復調信号よりビット「0」を生成する。(ii) 受信者は、ビットを生成した信号スロットを送信者に知らせる。(iii) 送信者は受信者がビットを生成した信号スロットについて、自身の変調位相差が+2d ならビット「1」を、−2d ならビット「0」を生成する。(iv) 送信者は受信者に対して、変調位相差が 0 である信号スロットを受信者に知らせる。(v) 受信者は、送信位相差が0であるビットは廃棄する。以上の手順によ

り、送受信者は同一のランダムビット列すなわち秘密鍵を得る。

生成した秘密鍵の安全性は、伝送信号光が量子雑音のため一部が重なり合った2つのコヒーレント状態であることにより保証される。この2状態は非直交関係にあり、誤りなく識別することはできず、したがって正規の送受信者に気付かれずに盗聴することができない。代表的な盗聴を考慮してシステム性能評価を行い、数十 km の鍵配送が可能という結果を得た(図 1-9)。

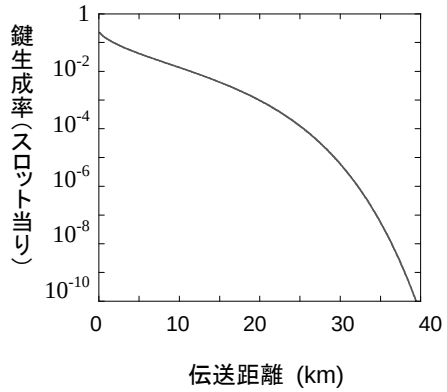


図 1-9. 巨視的 DPS－QKD の鍵生成率

本提案方式の特徴は、送受信系構成が従来の光通信分野で広く普及している DPSK システムと全く同じとなっていることである。これまでの QKD システムのように光子検出あるいは微弱ホモダイン検出の必要がなく、高い実用性が期待される。また、微弱光を用いていないので、従来型 QKD システムとは異なり、通常の光通信システムとの波長多重伝送の可能性がある。但し、鍵配送距離はあまり長くない。これは、実用性を意識して従来光通信で広く用いられている光前置増幅器を採用したためである。性能の高さよりも実用性を重視した中短距離向けの方式といえる。

巨視的 DQPS 量子鍵配送方式

前項の巨視的 DPS-QKD の改訂版として、送信状態を2状態から4状態に拡張した巨視的 DQPS(4値差動位相シフト)量子鍵配送方式を考案した。送信者は、{ δ ,- δ }{ π /2 + δ , π /2- δ }でランダムに位相変調した一定振幅のコヒーレント光を送信する。ここで、δ は対となる2つのコヒーレント状態が量子雑音のため一部が重なり合う程度に小さいものとする(図 1-10(a))。受信者はそれを位相差が 0 または π /2 の1ビット遅延干渉計で復調する(図 1-10(b))。

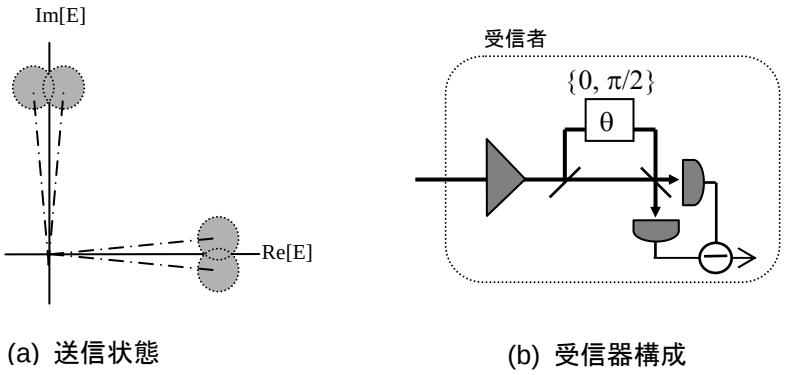


図 1-10. 巨視的 DQPS-QKD

本方式は、巨視的 DPS-QKD に BB84 の考え方を持ち込んだものとなっている。{ δ , −δ }の2状態を識別するには複素平面上の虚数軸への射影するのが最適測定系であるが(図 1-10(a)参照)、その場合には{ π /2 + δ , π /2 − δ }は識別不可能となる。一方、{ π /2 + δ , π /2 − δ }の最適識別測定系では、{ δ , − δ }は識別不可能となる。このように、BB84 における基底の一致/不一致に類似の仕組みを取り入れることにより盗聴されにくくして、安全性を高めている。2状態の場合と同一条件下でシミュレーションを行ったところ、鍵配送距離が10～20km程度長くなるという結果が得られた。前項の巨視的DPS-QKD のシステム性能向上を目論んだのであるが、残念ながら、受信器構成が複雑になるわりには飛躍的な性能向上は得られなかった。ひとつの検討結果というところである。

周波数変換型光子検出器を用いる DPS 量子鍵配送システムの偏波無依存化

本CRESTプロジェクトのNTTグループでは、実効的な光子検出率向上のため、連続動作が可能な周波数変換型単一光子検出器の開発を進めている。この光子検出器は、通信波長帯の光子を光パラメトリック過程により短波長光子に変換し、これを連続動作可能なSi-APD で検出するというものであるが、光パラメトリック過程に偏波依存性が存在するため、使用に際して偏波制御が必要という課題がある。この解決策として、交互直交偏波パルス列を用いる DPS－QKD システムを考案した。

図 1-11 にその基本構成を示す。送信者は、偏波状態がパルスごとに交互に直交している微弱コヒーレントパルス列を送信する。各パルスは、DPS プロトコルに従って{0, π }でランダム位相変調されている。受信者は、これを2ビット遅延干渉計に通した後、光子検出する。このようにすると、干渉計出力では同一偏波状態である1つおきのパルス同士が干渉することになる。この干渉結果を使い、DPS プロトコルの手順に従って秘密鍵を生成する。ここで、光子検出器には直交偏波光が交互に入力されている。そのため、検出器が特定の偏波成分の光子しか検出しなくても、ダイバーシティ効果により平均としては偏波無依存動作が得られる。但しその分、偏波が揃ったシステムに比べると検出効率は半分になる。

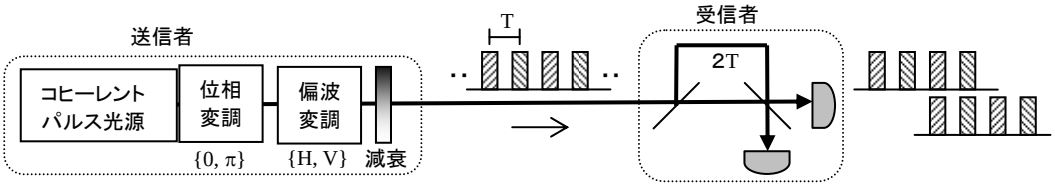


図 1-11. 偏波無依存 DPS-QKD システム

上記動作原理を確かめるため、実証実験を行った。図 1-12 に実験結果を示す。ここでは、受信系への入力偏波状態を様々に変えて秘密鍵を生成している。送信系において偏波変調を行わない場合には入力偏波状態に依存して鍵生成率が大きく変わるのに対し、偏波変調により交互直交偏波パルス列とするとほぼ一定の鍵生成率となることが確認された。

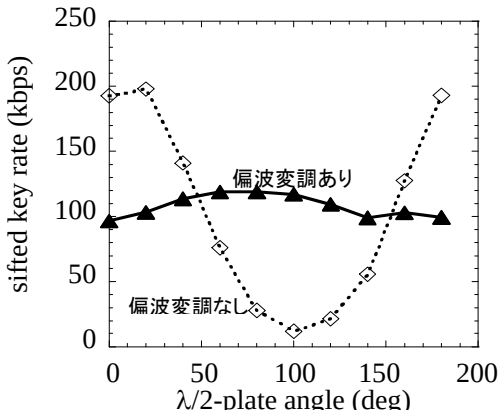


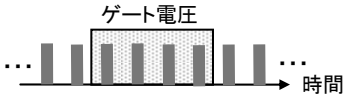
図 1-12. 偏波無依存動作の実験結果

周波数変換型単一光子検出器は、その高速動作性から量子通信用光子検出器の有力候補のひとつであるが、偏波依存性が実システム応用に際しての難点となっている。これまでも受信系をダイバーシティ構成にする偏波無依存化法が考えられていたが、それらに比べて本提案方式は、送信系に偏波変調器を入れるだけという簡便さが特徴的である。周波数変換型光子検出器の実システム応用に向けた重要技術といえる。

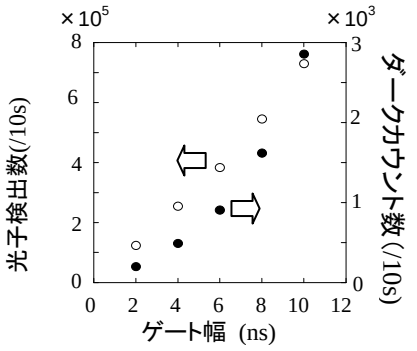
広ゲート幅 APD 光子検出器

単一光子検出器は量子情報通信システムにおけるキーデバイスである。通信波長帯の光子検出器としては、使い勝手の良さから、ゲート動作させた InGaAs-APD が広く用いられている。このゲート動作のゲート時間幅を拡げることにより、実効的な光子検出効率の向上を図った。

通常のゲート動作では、1ゲート内に1パルスが入るように設定する。これを、ゲート電圧パルスの時間幅を拡げて、1ゲート内に数パルスが入るようにする(図 1-13(a))。すると、光子を検出し得るパルス数が増え、実効的に光子検出効率が高くなる。この駆動方法は、DPS-QKD のようにクロックレートの高いパルス列を用いるシステムで特に有効である。また、時間位置もつれ光子の量子もつれ交換におけるベル測定では連続して光子を検出する必要があるが、そのようなシステムにも有効である。さらには、広ゲート幅とすることで、光パルスとゲートパルスとの精確な時刻同期が不要になるという利点もある。



(a) 広ゲート電圧印加



(b) 光子検出数とダークカウント

図 1-13. 広ゲート動作 APD 光子検出器

本検出方法の実証実験を行った。図 1-13(b)は、{パルス幅 125ps、繰り返し周波数

1GHz}の光パルス列をゲート幅{2, 4, 6, 8, 10}ns とした APD 光子検出器で受信したときの検出効率とダークカウントの測定結果である。ゲート幅を広げることにより検出数が比例して高くなることが確認された。但し一方、ダークカウントが比例関係以上に増加した。

得られた測定結果を基にして、この検出器を用いて DPS-QKD 伝送を行ったとしたときのシステム性能をシミュレートしたところ(図 1-14)、広ゲート化により鍵生成速度が向上する様子が示された。但し、ダークカウント増加を反映して、伝送距離は短くなっている。ダークカウント増加の理由は今のところ不明である。今後さらに検討を進めたい。

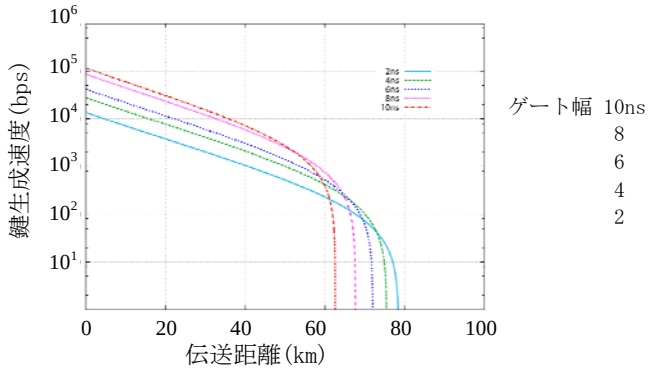


図 1-14. 広ゲート動作 APD 光子検出器を用いた DPS-QKD シミュレーション

本検出法によれば、特に回路構成を変更することなく実効的な検出効率の向上が図れる。また、自己差分検出法など他の高速動作技術と組み合わせも可能であり、さらなる性能向上が期待される。

DPS-QKD における光源コヒーレンス時間の影響

本プロジェクトは、通信波長帯すなわちファイバー伝送系の量子情報通信システムを研究対象としている。そこではファイバー伝送しても量子状態が安定に保たれることが必要であり、この観点から、隣接パルス間の位相差を情報の担い手として利用することが多い。DPS-QKD 方式はその代表例である。そのような場合、搬送波にはパルス列にわたってコヒーレントであることが要求される。では定量的にどの程度のコヒーレンス性が必要であるか。本プロジェクトの基本情報として、DPS-QKD に必要とされる光源のコヒーレンス性について定量的に検討した。

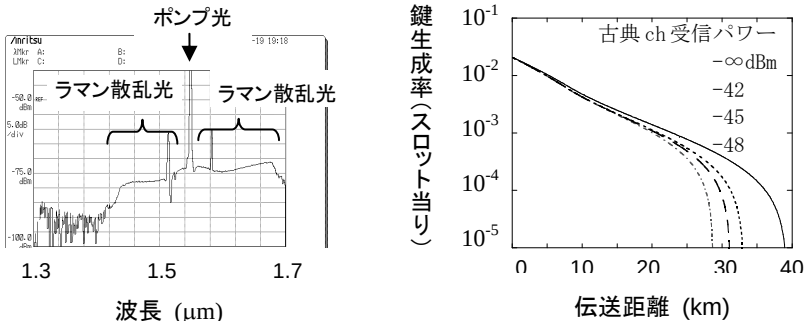
コヒーレンス性は光源のスペクトル線幅と対応関係にある。そこで、スペクトル線幅の異なる光源を用意して、DPS-QKD 実験を行った。また、1ビット遅延干渉計をマッハツェンダー型光フィルターと見立て、これに有限のスペクトル幅の光を透過させたとするモデルにより理論計算を行った。その結果、良好な秘密鍵生成を行うために要求されるスペクトル幅は、遅延干渉計を光フィルターと見做したときの FSR の 0.07%以下であることを明らかにした。

量子/古典波長多重伝送における自然ラマン散乱の影響

量子鍵配送では、量子状態を転送する量子チャンネルと基底情報などをやり取りする古典チャンネルとが用いられる。また、実際のシステムでは時刻同時信号も量子状態伝送に並行して送信される。通常、これらは別々の伝送媒体上にインストールされるが、実際の応用を考えると、同一媒体で多重伝送できればシステムとしての効率がよい。光通信において典型的な多重伝送方式は波長多重伝送である。そこで、量子/古典チャンネル波長多重伝送系について検討した。

古典チャンネルでは通常の光通信と同レベルのパワーの信号光が伝送される。一方、

量子チャンネルの伝送光パワーは1光子レベル以下である。このような状況では、ファイバー内で古典チャンネル光から発生する自然ラマン散乱光が雑音光として量子チャンネルの伝送特性を劣化させることが考えられる。そこで、ファイバーで発生する自然ラマン散乱光パワーの波長依存性/ファイバー長依存性/ポンプ光パワー依存性を系統的に測定し、その結果に基づいて量子/古典波長多重伝送系における量子チャンネルの伝送特性を評価した。図 1-15(a)にラマン散乱光発生の測定例、(b)に多重伝送時の DPS-QKD システム性能の計算例を示す。様々の状況を想定したシミュレーションの結果、APD 光子検出器を用いた QKD システムでは、量子チャンネルの劣化を軽微として 3.2Mbps 程度の古典チャンネルの多重伝送が可能である一方、超伝導光子検出器(SSPD)を用いるシステムでは、古典チャンネルを多重伝送すると量子チャンネル伝送特性が大きく劣化すること示した。これは、SSPD システムは検出器の低雑音性のため伝送距離が長く、また古典 ch 送信光パワーも大きいためである。



(a) ファイバー出力スペクトル　　(b) 鍵生成率

図 1-15. 自然ラマン散乱の影響

QKD 信号光と通常信号光との波長多重に関しては、従来の光通信システムと QKD システムとを同一ファイバー上に多重するという観点から研究がなされていたが、そこでは、ラマン散乱の影響により同一波長帯での多重伝送は無理、というのが大よその結論となっている。本検討は、QKD システムにおける量子チャンネルと古典チャンネルの波長多重という観点からラマン散乱の影響を系統立てて見直し、古典チャンネルが波長多重可能となる条件を明らかにしたものである。QKD の実システム適用に向けた基礎データとなる。

光雑音を用いた乱数発生

ポイント to ポイントの量子鍵配送システムでは、送信者はランダムに変調された量子状態を受信者に送信する。この際、完全な安全性を保証するためには乱数発生器が必須である。そこで、光雑音を用いる乱数発生を試みた。光増幅器あるいはスーパールミネッセントダイオードからの出力光を直接検波する。すると検波出力は、自然放出-自然放出ビート雑音のために変動する。これを閾値処理して「0」「1」のランダムビット列を得る。まだ初期検討の段階であるが、1～2Gbps の速度で乱数発生が可能な感触を得ている。

光を用いる乱数発生法は電気を用いる方法より高速なことが期待できる。これまで、光カオスを利用した 1Gbps 乱数発生が報告されているが、それに比べて本方法は簡便な構成となっている。

(2)研究成果の今後期待される効果

阪大グループ並びにNTTグループの成果により、ポイントtoポイントの量子暗号については、実用システムが視野に入る技術レベルまでになってきた。今後は、さらなる性能向上並びに実用化のためのシステム技術向上を図ることはもちろんであるが、それと同時に、実用システムとしてどう展開していくかの戦略的検討が必要であろう。そこでは、単なる技

術論だけでなく、既存通信ネットワークとの親和性、ニーズの見極め、サービス展開の仕方、などを考えることが重要となる。

昨年、総務省の諮問機関的組織である PNF（フォトニック・ネットワーク・フォーラム）において、フォトニックネットワークのセキュリティについて議論する会合が数回にわたって開催された。参加者は、光通信ネットワークの専門家、現代暗号の専門家、そして量子暗号関係者（本研究代表者を含む）と多岐に渡る。そこでは、これからは物理層でのセキュリティ確保も重要であることが認識された。量子暗号の出番がやってくる可能性は少なくないと思われる。

4．2 時間位置もつれ光子対を用いた量子通信実験（NTT 武居グループ）

(1)研究実施内容及び成果

NTT グループは、主に時間位置もつれ光子に関する実験的研究を行った。また、ポイント-to-ポイント（P2P）量子鍵配送（QKD）実験や安全性解析も行った。

DPS-QKD プロトコルによる長距離・高速 QKD 実験

量子もつれシステムの前段階として P2P-QKD の性能を見極めることが重要と考え、これに関する実験的研究を行った。具体的には、代表研究者（井上）らの提案による DPS-QKD プロトコルを実装し、長距離かつ高速な量子鍵配送実験を行った。

最も重要な成果は、超伝導単一光子検出器(SSPD)を用いて、200 km の光ファイバー上での量子暗号鍵配送に成功した 2007 年の実験である(H. Takesue et al., Nature Photonics 1, 343)。SSPD とは、バイアス電流を印加した超伝導状態の窒化ニオブ細線に光子を入射すると、超伝導状態が破れて巨視的な電圧の変動が生じることを利用して光子を検出するもので、低雑音かつ高時間分解能を有する単一光子検出器である。現在広く使われている InGaAs/InP-APD 光子検出器とは異なり連続動作が可能であり、高いクロックレートの連続パルス列を用いる DPS－QKD プロトコルの特徴を活かす検出器でもある。本検出器を 10-GHz クロックの DPS-QKD システムに適用し、長距離鍵生成実験を行った。得られた安全鍵配送率と光ファイバー長・伝送損失の関係を図 2-1 に示す。200 km ファイバー伝送時に 12 bit/s の安全鍵生成率を得ることに成功した。これは、QKD 実験の鍵配送距離の当時の世界記録である。また、安全鍵生成速度についても、105km において 17 kbit/s を実現した。これは、それ以前に我々が周波数上方変換型単一光子検出器を用いて達成した記録(166 bit/s@100km)を 2 桁上回るものである。このように、SSPD の低雑音性と高速性を活用して、鍵配送距離/生成率ともにそれまでの記録を大幅に上回る QKD システムを実現した。本成果は、発表後3年で既に 100 件以上引用され、長距離 QKD のベンチマーク的実験となっている。

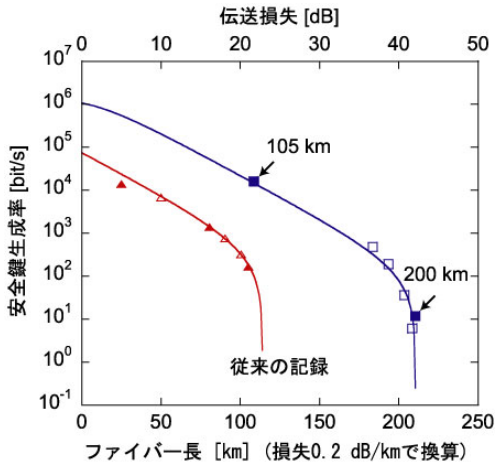


図 2-1. SSPD を用いた DPS-QKD 実験における伝送ファイバー長と安全鍵生成率

その他、高速動作が可能な正弦波ゲート動作InGaAs/InP-APD光子検出器による高速かつ実用的なQKD実験(N. Namekata et al., Appl. Phys. Lett. 91, 011112 (2007))や、連続動作可能な周波数上方変換型単一光子検出器を用いた1 Mbit/sを越える安全鍵配送速度のQKD実験(Q. Zhang et al., New J. Phys. 11, 045010 (2009))など、QKD実験において世界を牽引する成果を挙げた。

光ファイバーによる時間位置量子もつれ光子対発生及び識別不可能特性

本プロジェクト開始前に、NTT グループは分散シフトファイバー(DSF)内の自然四光波混合(SFWM)を用いる通信波長帯偏波もつれ光子発生の基本実験に成功していた。本プロジェクトでは、この発生方法を時間位置量子もつれに適用し、またさらなる高品質化を図った。

DSF内のSFWMによる量子もつれ光子対発生においては、ファイバー内でポンプ光から発生する自然放出ラマン散乱光が雑音光子として作用し、これによる量子相関度の低下が課題であった。この問題を解決するために、DSF を液体窒素温度まで冷却して量子もつれを発生させた。ファイバーを冷却するとガラス媒質の格子振動が抑圧され、ラマン散乱発生を抑えることができる。この手法により低雑音な時間位置もつれ光子対発生をさせ、その長距離ファイバー伝送(60 km)に成功した(H. Takesue, Opt. Express 14, 3453-3460 (2006))。

さらに、独立した２つの冷却した DSF により発生させた光子対を用いてHong-Ou-Mandel 型量子干渉実験を行い、Mandel ディップの観測に成功した(H. Takesue, Appl. Phys. Lett. 90, 204101 (2007))。この結果は、光ファイバーを用いた量子もつれ光子対源により識別不可能な光子を発生可能であることを示すものであり、後述の量子もつれ交換実験実現のための重要なステップとなった。

PPLN導波路による量子もつれ光子対

NTT グループは、本プロジェクト開始前に、周期分極反転 $LiNbO_3$(PPLN)導波路中の自然放出パラメトリック下方変換(SPDC)による時間位置もつれ光子対の発生に成功していた。PPLN を用いる方法は、光ファイバー発生法に比べて低雑音という利点を有する。本プロジェクトでは、PPLN により発生させた量子もつれ光子のファイバー伝送実験を行った。2007 年に、本方式により発生させた時間位置もつれ光子対を周波数上方変換型光子検出器で受信することにより、100 km 光ファイバー伝送を達成した(T. Honjo et al., Opt. Express 15, 13957-13964)。

さらに2010年には、PPLN導波路に1.5μm帯のポンプ光を入力し、PPLN中のカスケードχ_2過程を用いる 1.5μm 帯の量子もつれ光子対発生に世界で初めて成功した(M. Hunault et al., Opt. Lett. 35, 1239-1241)。通常、PPLNで通信波長帯のもつれ光子対を発生させるには短波長のポンプ光が必要であるが、本技術によればポンプ光波長が 1.5μm 帯でよく、従来より簡易な構成で高品質な量子もつれ光子対を発生することができる。

シリコン細線導波路による量子もつれ光子対発生

上記のように光ファイバー及びPPLNによる量子もつれ光子発生技術を進展させたが、光ファイバー法には自然ラマン散乱雑音光子の問題が解決し切れずに残り、また、PPLN法には群速度分散のため完全に識別不可能な光子を得ることに難点があった。そこで新たな試みとして、シリコン細線導波路を用いる量子もつれ光子対発生を行った。

シリコン細線導波路とは、コア径がナノスケールの単結晶シリコンの光導波路であり(図2-2)、光通信分野において、従来のシリカ系光導波路技術に比べて飛躍的に小さい光回路を実現する技術として現在盛んに研究されている。また、コア径が小さいことから光強度を高めることができるため、光非線形デバイス応用としても研究が進められている。この高い光非線形性は量子もつれ発生にも都合がよい。

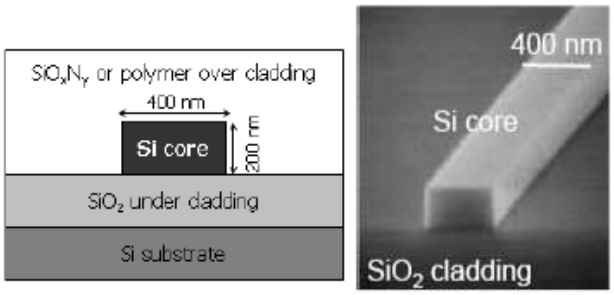


図 2-2. シリコン細線導波路

そこで、シリコン細線導波路内の自然四光波混合を利用して量子もつれ光子対を発生させた。まず 2007 年に、シリコン細線導波路に 1.5 μ m 帯のポンプ光パルスを入力し、世界で初めて通信波長帯時間位置もつれ光子対発生を観測した (H. Takesue et al., Appl. Phys. Lett. 91, 201108 (2007))。その後さらに実験を続け、現在では、本発生法によりほとんど雑音光子を含まない高品質量子もつれ光子対が発生可能であることを確認している (図 2-3, K. Harada et al., Opt. Express 16, 20368-20373 (2008))。 この成果はシリコンフォトニクス技術を用いた量子光学実験の先駆的研究として注目を集め、CLEO/QELS 2009 を含む5件の招待講演を依頼された。

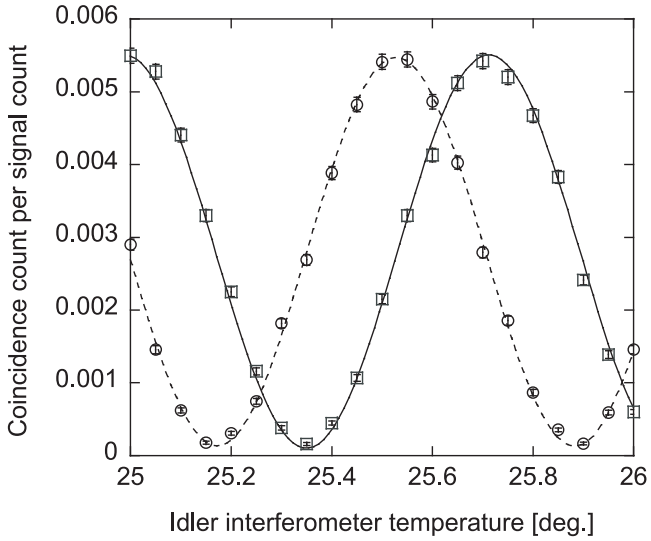


図 2-3. シリコン細線導波路により発生させた時間位置もつれ光子対の二光子干渉波形。明瞭度 95%以上を観測した。

通信波長帯量子もつれ光子対による量子鍵配送実験

上記の量子もつれ光子対源を用いて、本プロジェクトの最終目標のひとつである量子もつれシステム実験を行った。量子もつれ QKD 実験及び量子もつれ交換実験である。

まず、PPLN 導波路中の自然放出パラメトリック下方変換に基づく時間位置もつれ光子対源と、米国 NIST 及び情報通信研究機構(NICT)が開発した超伝導単一光子検出器(SSPD)を用いて、100 km (50 km×2)の光ファイバー上での量子鍵配送実験を行った(T.

Honjo et al., Opt. Express 16, 19118-19126 (2008), 図 2-4 参照)。6.9%の誤り率で、0.57 bit/s のシフト鍵を生成することに成功した。これは、量子もつれ QKD 実験における光ファイバー伝送鍵配送距離の世界記録である。

さらに、シリコン細線導波路中の SFWM に基づく時間位置もつれ光子対源と正弦波ゲーティング法による高速 InGaAs/InP APD 光子検出器を用いた 100 km ファイバー伝送量子もつれ QKD を行った(H. Takesue et al. Opt. Express 18, 16777-16787 (2010))。本実験では使い勝手のよい APD 光子検出器を使用しており、より実用的なシステム実験といえる。ここで達成した秘密鍵生成は現実的な閾値検出器に適用可能な安全性理論(T. Tsurumaru and K. Tamaki, Phys. Rev. A 78, 032302 (2008))に基づいており、無条件に安全な QKD 伝送を量子もつれ光子対を用いて実現した初めての実験ともなっている。

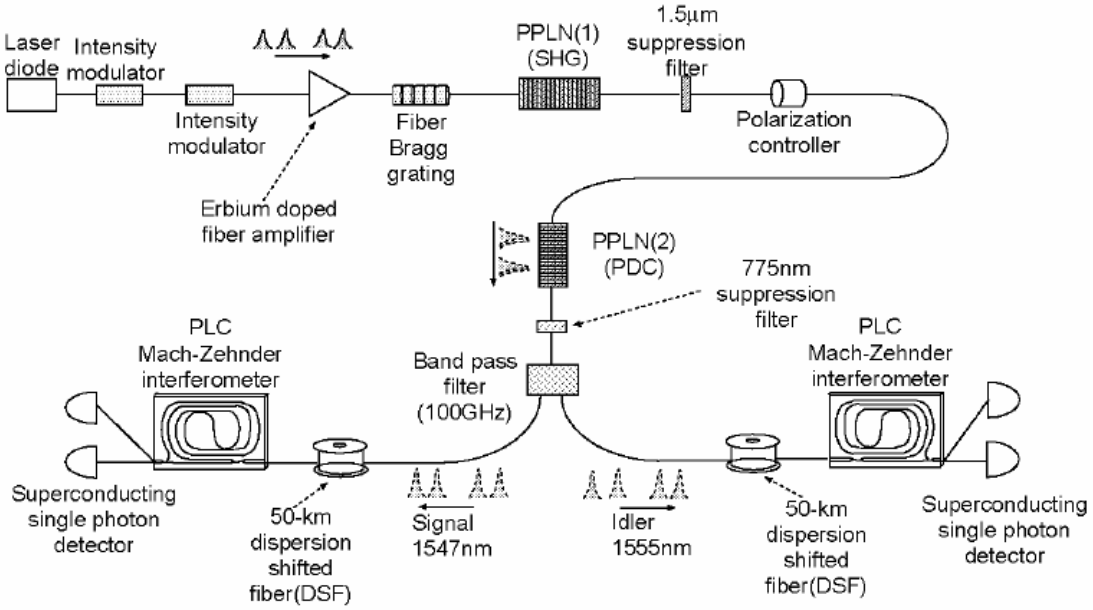


図 2-4. 量子もつれ光子対を用いた量子鍵配送実験系

通信波長帯量子もつれ光子対による量子もつれ交換実験

量子もつれ交換(entanglement swapping)は、量子リレーさらには量子中継により QKD の鍵配送距離を拡張するための基本技術であり、また量子コンピューター間を接続するような量子ネットワーク実現に向けた要素技術である。これに関する実験的検証は、1998 年の最初の実験以来、可視波長帯においては数多くの報告がなされているが、通信波長帯では十分な性能の光子対源や光子検出器が得られないために困難であった。特に 1.5μm 帯光子対を用いた実験としては、2007 年にジュネーブ大によるものが報告されていたのみであった。そこで、前述の光ファイバー内 SFWM に基づく時間位置もつれ光源を用いて、1.5μm 帯量子もつれ交換実験を行った。

実験系を図 2-5 に示す(H. Takesue and B. Miquel, Opt. Express 17, 10748-10756 (2009))。2つの独立なもつれ光源から識別不可能な光子対をそれぞれ発生させ、両光源の中間点に配置されたノードにおいて、光子対の片割れ同士に対してベル状態測定と呼ばれる量子測定を行う。すると、独立光源から出力された他の 2 光子が「もつれた」状態となる。これが量子もつれ交換である。この系において、もつれさせた 2 光子に対し同時計数測定を行ったところ、図 2-6 に示すような明瞭な二光子干渉波形が観測された。すなわち、量子もつれ交換が確認された。本実験においては、正弦波ゲーティング方式により 500 MHz ゲート周波数で駆動された InGaAs/InP APD 光子検出器を使用することにより、

上記ジュネーブ大の報告の約 20 倍の量子もつれ交換成功率を得た。

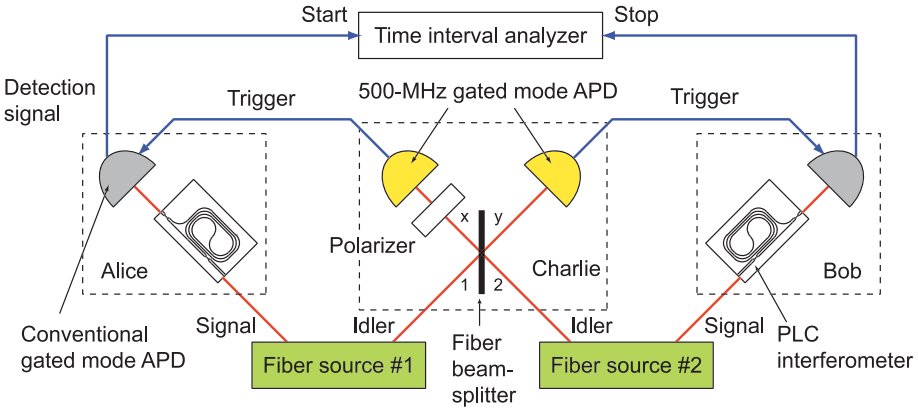


図 2-5. 量子もつれ交換実験系

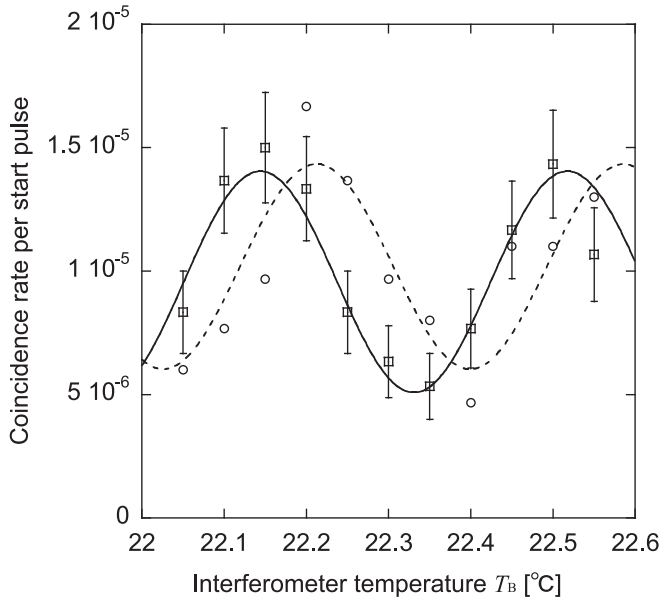


図 2-6. 量子もつれ交換実験における 2 光子干渉測定結果

<u>波長の異なる 2 光子の識別不可能性実験</u>

量子情報通信では、複数の光子の同一性(i.e.,識別不可能性)を利用することが多々ある。ここで、2光子の波長が異なっていると、両者が識別されるためシステムが構築できない。そこで、周波数上方変換技術を用いて、周波数の異なる 2 光子の識別可能性を消去することを試みた(H. Takesue, Phys. Rev. Lett. 101, 173901 (2008))。図 2-7 にその実験系を示す。まず、光ファイバー中の自然放出四光波混合により、光周波数の異なる 1.5 μm 帯の 2 つの光子をそれぞれ発生させた。但し、周波数以外の属性(パルスの時間形状やスペクトル形状など)は同一とした。これを、PPLN 導波路中の和周波発生過程により、同じ周波数にそれぞれ周波数上方変換した。そして、変換後の 2 光子に対して Hong-Ou-Mandel 型量子干渉実験を行ったところ、非古典的なディップが観測され、識別不可能性が確認された。この実験結果は、異なる波長の 2 光子に対してもベル状態測定などの量子干渉測定が行えることを示唆するものであり、量子ネットワークの柔軟性の飛躍的増大の可能性を示している。

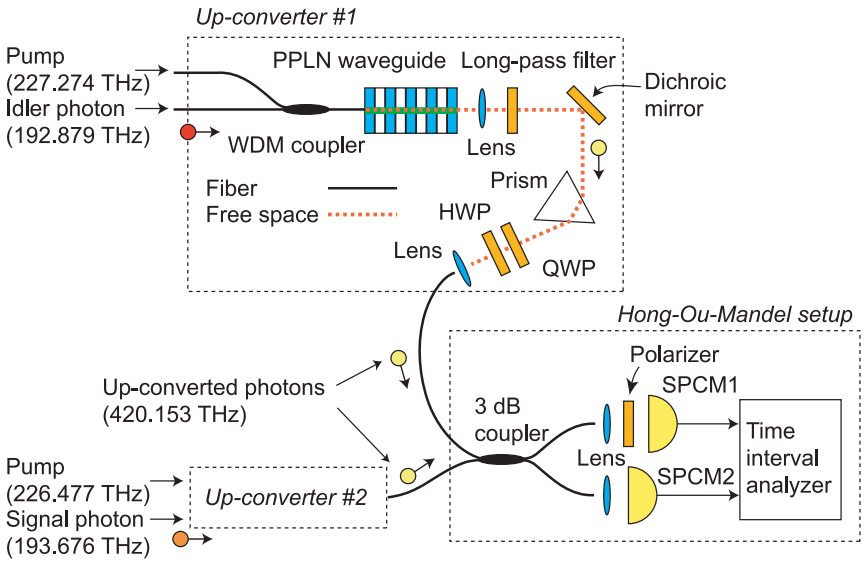


図 2-7. 周波数識別可能性消去実験系

単一光子の周波数下方変換

本プロジェクトでは、ファイバー伝送系を想定して、1.5 μm 帯での量子情報通信技術の研究を進めているが、一方で短波長帯においては、光子と物質系との相互作用を利用した量子情報処理技術の研究が行われている。将来的には、両者が統合された量子情報通信システムも考えられる。例えば、ファイバー伝送は通信波長帯/量子メモリ機能は短波長帯でそれぞれ実装し、それらを組み合わせる量子中継システムなどである。そのようなシステム実現のためには、通信波長帯と短波長帯を結びつける「フォトニック量子インターフェース」技術が必要となる。

通信波長帯から短波長帯へのインターフェース、すなわち単一光子の周波数上方変換は、通信波長帯光子を短波長用 Si-APD で高性能に検出するための技術として、NTT-Stanford を含め、これまで数多くの研究がなされてきた。しかし一方その逆、すなわち周波数「下方」変換については報告例がなかった。そこで、単一光子のコヒーレント周波数下方変換実験を行った(H. Takesue, Phys. Rev. A 82, 013833 (2010))。

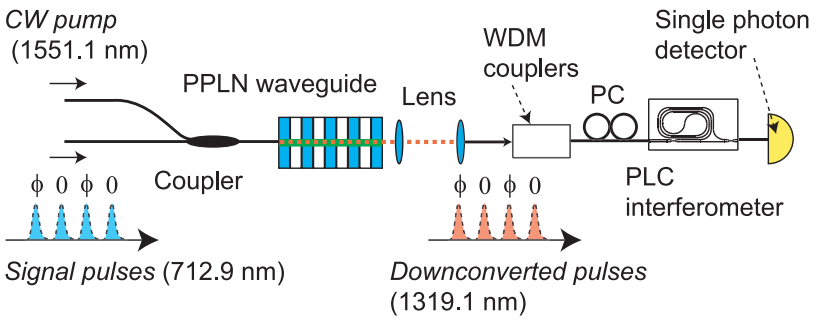


図 2-8. 単一光子の周波数下方変換実験系

図 2-8 にその実験系を示す。パルスあたりの平均光子数を 1 以下とした波長 0.7 μm の信号光パルス列に対しパルス毎に交互に{0, ϕ }位相変調を施し、1.5 μm の連続ポンプ

光と合波した後、PPLN 導波路に入力する。ここで、PPLN 導波路中の差周波発生過程により、0.7μm 信号パルス列を位相情報を保持したまま波長 1.3μm に周波数下方変換する。PPLN 導波路から出力された光子列は、ポンプ光除去のための光フィルターに通し、1ビット遅延干渉計により隣接パルス同士が干渉させられた後、単一光子検出器により受信される。得られた光子検出結果を図 2-9 に示す。0.7μm 信号光子の位相変調値 φ とともにカウントレートが変化する様子が示されている。すなわち、位相情報を保持したまま単一光子が周波数下方変換されたことが確認された。量子情報ネットワーク実現に向けた成果といえる。

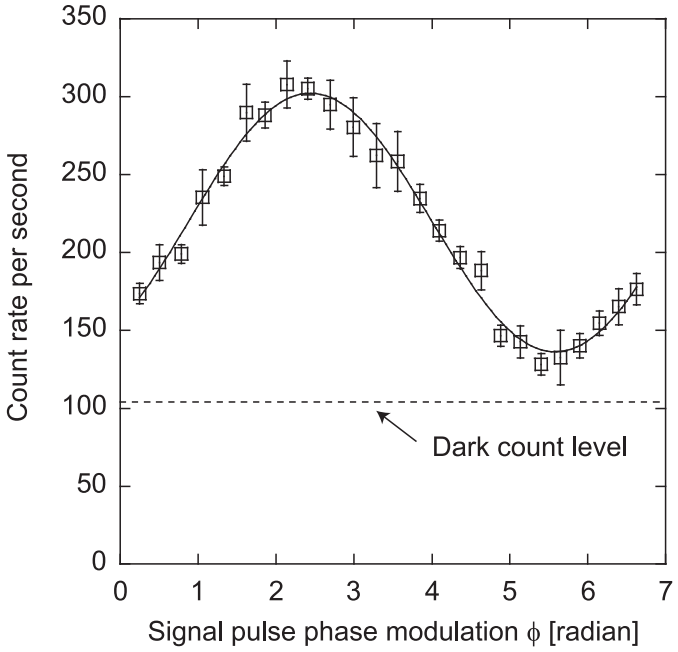


図 2-9. 単一光子周波数下方変換実験結果。縦軸は検出器のカウントレート、横軸が 0.7μm 光パルス列の位相変調値。

量子鍵配送の安全性理論

量子暗号は究極的な安全性を謳っている。その意味で、絶対的に安全であること(無条件安全性)の証明あるいは安全性理論の構築が求められる。具体的には、(i)安全性証明のための一般的なテクニックの構築、(ii)構築したテクニックを具体的なプロトコルに適用して安全性を解析する、(iii)安全性解析で得られた知見を基に新たなプロトコルを産み出す、(iv)安全性解析での仮定と実際のデバイスとのギャップを解消する、といった事柄である。NTT グループでは、これらに関する研究を行った。

項目(i)の安全性証明のテクニックに関しては、これまでいくつかの方法が提案されてきたが、中でも大阪大学・小芦が考案した相補性に基づく手法が最も簡潔なものとして知られている。これについて、既存の解析手法あるいは実際のプロトコルとの対応関係に関する研究を行った(K.Tamaki and G. Kato, Phys. Rev. A 81, 022316 (2010))。相補性による安全性証明では、実際のプロトコルと相補的な仮想プロトコルを想定して理論を展開する。そこで、仮想プロトコル用の量子回路を構築し、それを基に、相補性理論により従来の解析法あるいは実際のプロトコルが解釈可能であることを示した。安全性理論の体系化に寄与する成果である。

項目(ii)の具体的プロトコルの安全性証明に関しては、まず、強い参照光を用いる B92

プロトコルについて検討した。B92 は BB84 に次いで代表的な QKD プロトコルであるが、強い参照光を用いる B92 の無条件安全性は証明されていなかった。そこで、受信者ボブが真空/単一光子/多光子を見分ける検出器を使う場合と光子数がある範囲にあるか否かを見分ける検出器と使う場合とについて安全性解析を行い、その無条件安全性を証明した(K. Tamaki, N. Lütkenhaus, M. Koashi, J. Batuwantudawe, Phys. Rev. A 80, 032302 (2009)、図 2-10 参照)。

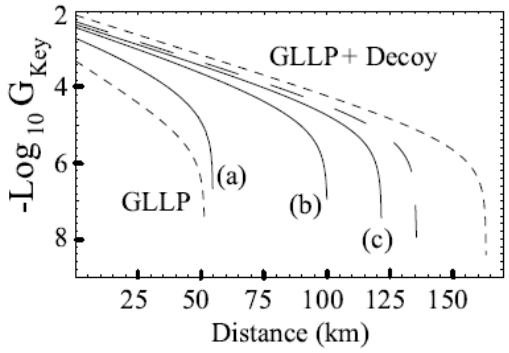


図 2-10. 構築した QKD 安全性理論に基づく秘密鍵生成率。GLLP:BB84 with coherent light、(a)-(c):B92 with various intensities of reference light。

また、本プロジェクトで実験を進めているDPS－QKDプロトコルの安全性解析も行った。DPS-QKD では連続パルス列を送受信する。これをいくつかのブロックに区切り、さらに真空/単一光子/多光子を見分けられる検出器を仮定すると、ボブの構造が単一光子を用いた B92 と類似であることが分かり、単一光子 B92 の安全性証明を参考にしつつ無条件安全性を証明した(K. Wen, K. Tamaki, Y. Yamamoto, Phys. Rev. Lett. 103, 170503 (2009))。本解析では1ブロック内は単一光子であることを仮定しており、連続コヒーレントパルス列を用いる実際のシステムと全く同じ状況ではないが、DPS－QKD の無条件安全性証明へ向けた大きな前進である。

項目(iii)については、B92 の改良プロトコルを考案し、その無条件安全性を証明した(K. Tamaki, Phys. Rev. A 77, 032341 (2008))。オリジナル B92 では強い参照光と微弱コヒーレント信号光を用いているところを、信号光と参照光の強度を同じとしても安全な鍵配送が可能となるように改良した。このようにすると、送信系の実装が容易になり、また強い参照光からの散乱光に影響されなくなる。

項目(iv)に関しては、光子検出器についての既存の安全性解析の仮定と実際のデバイスとのギャップを解消した。従来の無条件安全性証明では光子数を見分けることができる検出器を仮定しているが、実際の光子検出器では光子数を識別することはできない。そこで、BB84 プロトコル(T. Tsurumaru, and K. Tamaki, Phys. Rev. A 78, 032302 (2008))と6状態プロトコル(G. Kato and K. Tamaki, Arxiv:1008.4663)について、真空とそれ以外の光子状態しか見分けられない検出器を用いたシステムの無条件安全性を証明した。さらに、従来の安全性解析ではボブが用いる2つの光子検出器の検出効率は同一としているところを、検出効率が異なっている状況での無条件安全性を証明した(C-H. F. Fung, K. Tamaki, B. Qi, H-K. Lo, X. Ma, QIC, vol. 9, pp. 0131-0165 (2009))。

(2)研究成果の今後期待される効果

NTT グループが行った DPS-QKD 実験及び安全性解析により、QKD のシステム性能(鍵配送距離、鍵生成速度、安全性)が飛躍的に向上した。また、上記では述べなかった

が、総務省系プロジェクトの一環として QKD をベースとしたセキュア通信システム（量子チャンネル伝送以外の各種技術）の開発も並行して行っており、実用的な量子暗号システムを実現するための基本技術は確立できた。今後コストの低下が実現され、さらに量子暗号の適用先となる秘匿性の高い通信ニーズを確立することができれば、本プロジェクトの成果は量子暗号実用化のための基本技術として使用される可能性がある。

一方、本プロジェクトのメインテーマである量子もつれ光子対とその適用システムは、第一世代であるポイント to ポイント QKD システムの性能限界の打破，特に鍵配送の長距離化のための重要な要素技術である。本プロジェクトの成果として得られた通信波長帯の量子もつれ光子対源、単一光子周波数変換技術、量子通信システム技術は、将来の「量子中継」の概念に基づく大規模量子通信システムにおいて重要な要素技術として使用されることが期待される。今後は、これらの要素技術の更なる特性向上を図るとともに、量子中継実現に必須の技術である量子メモリ技術や、量子通信の構成要素の大規模集積化のために重要な光子量子回路技術などの基礎研究に取り組んでいく必要がある。特に、本プロジェクトの成果のひとつであるシリコン細線導波路を用いた量子もつれ光子対発生は、光子量子回路におけるアクティブ素子の集積化を実現するための技術として今後の展開が期待できる。

4．3 偏波に基づく多光子間量子もつれ合い技術の開発（産総研　吉澤グループ）

(1)研究実施内容及び成果

産総研グループは、偏波に基づく多光子間量子もつれ合いを対象として、通信波長帯での量子もつれによる多者間量子情報処理技術の開発及び実験的検証を行った。具体的には、高品質な多光子間量子もつれ合い生成技術の確立、もつれ光子を安定に発生させるための光ファイバー量子干渉計最適制御技術の確立、多者間量子情報処理の実験的検証、などを行った。また、量子通信システムの基盤技術として、単一光子検出器についても検討した。各項目の内容・成果は以下の通りである。

InGaAs-APD 光子検出器のゲート動作最適化

量子暗号をはじめとする量子情報通信システムにおいて、単一光子検出器は実装にあたってのキーデバイスである。通信波長帯の光子検出器としては、ゲート動作 InGaAs-APD が広く用いられているが、アフターパルスと呼ばれる誤計数（不純物準位に捕獲された増倍電子によって起こるダークカウント）のためゲート繰り返し周波数を高くできず（通常は数 MHz 程度が上限）、光子検出器の動作速度を制限する要因となっていた。そこで、APD 光子検出器の高速動作化を目指して、放電パルス計数動作 APD 光子検出器について検討した。

この光子検出方法は、本プロジェクト開始前に共同研究者（吉澤）により考案されていたものである。高速化のためにはアフターパルスを抑えればよく、そのためには不純物準位に捕獲される電子数を少なくすればよく、そのためには APD のなだれ増倍の規模を小さくすればよく、そのためには高感度で光子検出できればよい。そこで、光子入射による電子増倍を直接的に検出するのではなく、なだれ増倍が起きない時の放電パルス出力を利用して高感度で光子を検出することによりゲート繰り返し周波数を高速化するのが放電パルス計数動作法である。

この手法の基本動作は確認済みであったが、本プロジェルトでさらに詳細に検討した。具体的には、ゲートパルスに対する光子入射時刻と発生するなだれ増幅パルス波高との関係を調べ、最適条件下では高い量子効率を保ちつつなだれの規模が小さくなることを明らかにした。そして上記最適設定により、ゲート繰り返し周波数 10MHz での低アフターパルス特性を確認した（図 3-1）。

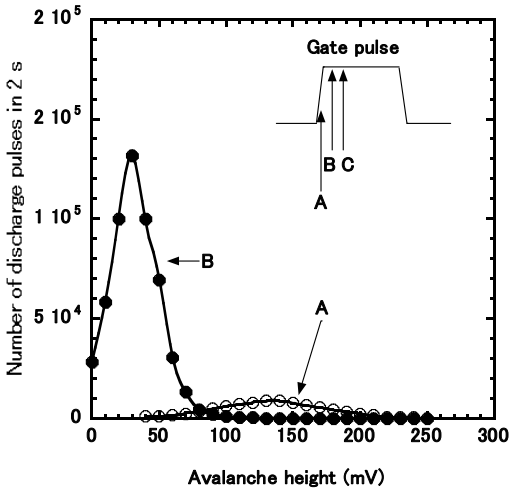


図 3-1. なだれ増幅パルスの波高分布。A、B、Cは光子入射時刻を示す。Bが最適条件。

InGaAs-APD 光子検出器の低雑音化

前項は InGaAs-APD 光子検出器の高速化についての研究であるが、低雑音化についても検討した。低雑音とするには APD をできるだけ低温に冷やせばよい。ところが冷却し過ぎると、不純物準位に捕獲された増倍電子の滞在時間が長くなり、アフターパルス確率が大きくなる。すなわち、アフターパルスと低雑音化はトレードオフの関係にあるため、冷却温度には限界がある。ここで、上記の放電パルス計数法によりアフターパルスが抑えられれば、より低い温度まで APD を冷却することができ、その結果、熱雑音を抑えることができる。

この低雑音化方法に関し、実証実験を行った。結果を表 3-1 にまとめる。放電パルス計数法を採用することで低温においてもアフターパルスが抑制される一方、冷却効果により熱雑音に起因する暗計数率は小さくなることが確認された。なお、この時のゲート周波数は 20MHz、光パルス周波数は 100kHz、ゲート幅は 1ns である。

表 3-1 放電パルス計数 APD の光子検出特性

動作温度	量子効率	暗計数率	アフターパルス雑音
130 K	10%	1.4×10^{-7}	6.3×10^{-4}
155 K	10%	3.4×10^{-7}	8.3×10^{-5}
180 K	10%	1.1×10^{-6}	7.8×10^{-5}

光子検出器評価方法の提案・実証

光子検出器の検出効率を正確に測定する技術は、量子情報通信システムの基盤である。今回、PPLN から発生させた相関光子対を用いて光子検出効率を測定する新しい方法を提案し、実証実験を行った。図 3-2 にその構成を示す。従来法の問題点であった測定系の損失と検出効率の切り分けが容易で、より精度の高い測定法となっている。

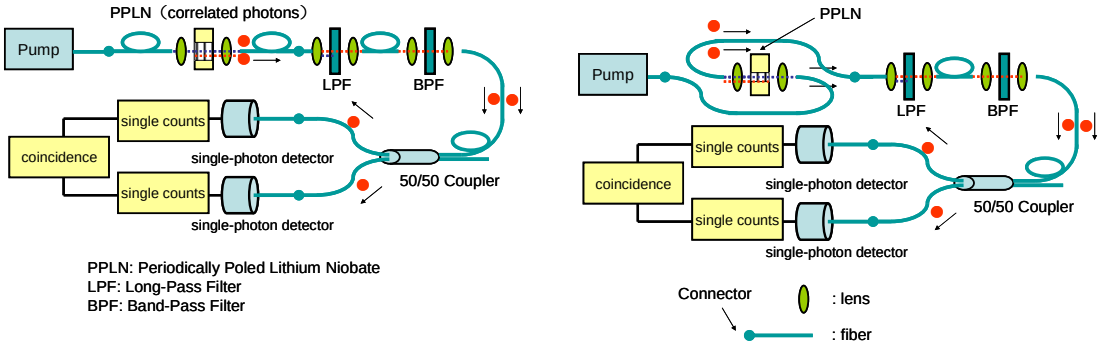


図 3-2. 励起光の双方向入射による量子効率測定法の概略図
双方向入射のため両者では励起光(Pump)と PPLN の位置関係が逆転している。

ファイバーループ構成による偏波もつれ光子の発生

偏波もつれ光子の発生法としては、短波長帯では、バルク非線形媒質におけるパラメトリックダウンコンバージョン(PDC)を利用する方法が広く用いられているが、通信波長帯かつファイバー系には適さない。通信波長帯偏波量子もつれ発生方法としては、研究代表者(井上)によりファイバーループ内の自然四光波混合を用いる手法が提案されている。しかしながら、ファイバー四光波混合による方法には自然ラマン散乱により雑音光子が発生するという難点がある。そこで、ファイバーループ内に周期分極反転 $LiNbO_3$(PPLN)導波路を配置し、PPLN 内の PDC による偏波もつれ光子対の発生を行った。

図 3-3 にその基本構成を示す。偏波ビームスプリッタ(PBS)に入力されたポンプ光は、縦偏波成分と横偏波成分に分けられ、縦成分は右回り/横成分は左回りでループ内を伝播する。ループ内の PPLN には両方向からポンプ光が入射される。ここで、ループは偏波保持ファイバー(PMF)で構成されており、PMF の軸を捻ることにより、PPLN へは双方向から同一偏波のポンプ光が入射され、PDC によりそれと同一偏波の量子相関光子対がそれぞれの方向に発生する。発生した双方向の相関光子対は PBS において直交偏波状態で合波される。ここで、ポンプ光パワーの調整により PPLN における光子対発生効率を適切に設定すると、PBS からは縦偏波光子対と横偏波光子対の重ね合わせ状態、すなわち偏波もつれ光子対が出力される。

本構成では、右回り光と左回り光が同一経路を逆向きに伝播するため、位相揺らぎが相殺され、相対位相が定まったもつれ光子対を得ることができる。発生させたもつれ光子対により二光子干渉測定を行ったところ(図 3-4)、図 3-5 に示すような干渉パターンが得られた。明瞭度は偶発的同時計数を含めて 85%であった。

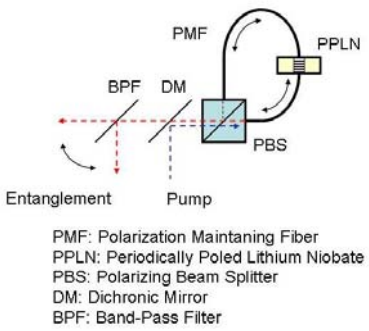


図 3-3. ファイバーループ構成

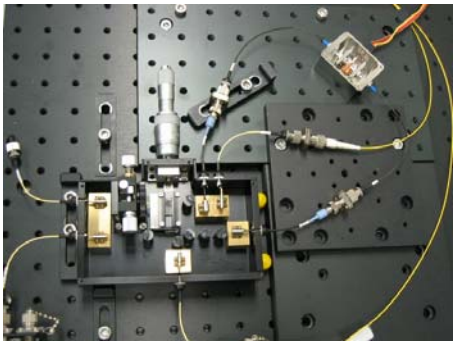


図 3-4. 実験系

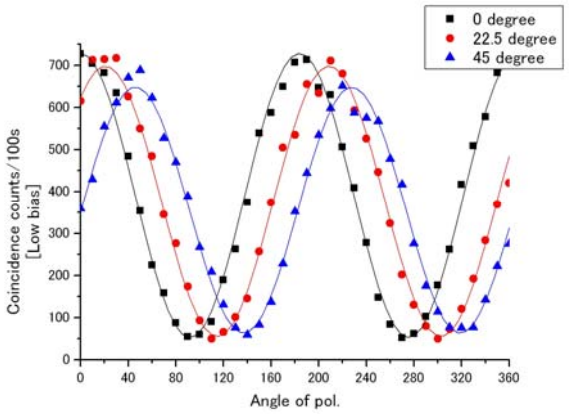


図 3-5. 二光子干渉結果

PPLN 内 PDC による偏波もつれ発生の高品質化

前項のもつれ発生構成において、ポンプ光を短パルス光とすることにより、安定的に偏波もつれ光子対を発生させた。これを量子トモグラフィー測定し、忠実度 96.8%と高品質なもつれ状態であることを確認した(図 3-6)。

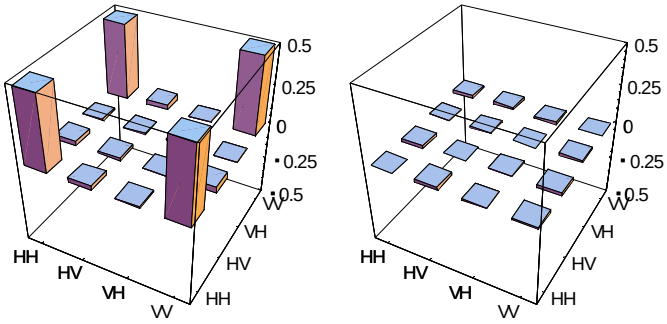


図 3-6. 量子トモグラフィー評価結果(忠実度 96.8%)

PPLN 内 PDC による偏波もつれ発生の広帯域化とファイバ伝送実験

上記偏波もつれ発生回路において、ファイバーループ内の PPLN を短尺導波路(1mm)とすることにより、1525-1580nm という広い波長範囲にわたって量子もつれ光子対を発生させた(図 3-7)。もつれ忠実度はパルス励起時で 85%、CW 励起時で 95%であった。さらに、長距離ファイバー伝送実験(全長 82km 及び 132km)を行い、伝送後のもつれ忠実度 86%及び 60%を確認した(図 3-8)。

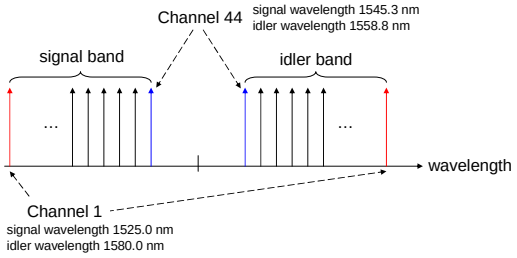


図 3-7. 広帯域偏波もつれ光子対発生

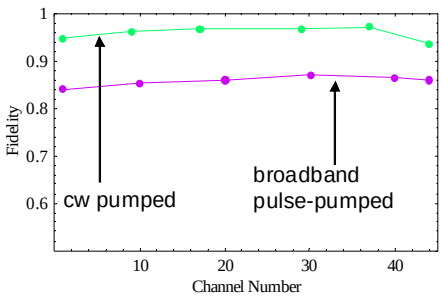


図 3-8. 忠実度測定結果

PPLN 内 PDC による四光子偏波もつれ発生と量子干渉実験

上記偏波もつれ光子源を2台作製し、四光子による量子干渉実験を行った。

まず、2台のもつれ光子源からそれぞれ独立に発生した光子対を用いて偏波量子干渉計を構成した。四光子同時計数によるMandel dipの観測実験を行い74.5%の良好な可干渉度を得た(図 3-9)。

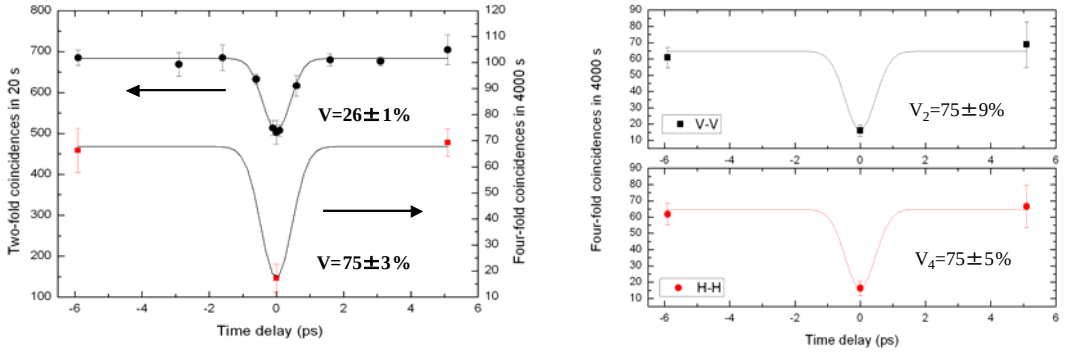


図 3-9. Mandel dip 観測結果
(右側:斜め45度偏光、左側上段:垂直偏光、下段:水平偏光)

また、2台の偏波もつれ光子源と無偏光ビームスプリッタによるベル測定による量子もつれ交換実験を実施した。得られた状態を量子トモグラフィーにより評価したところ、忠実度70.5%(偶発計数は除く)であった(図 3-10)。さらに、実験系を理論/実験両面から詳細に検討し、四光子同時計数時に発生する偶発計数が PPLN 内の自然パラメトリック下方変換により偶発的に発生する六光子に起因することを明らかにした。

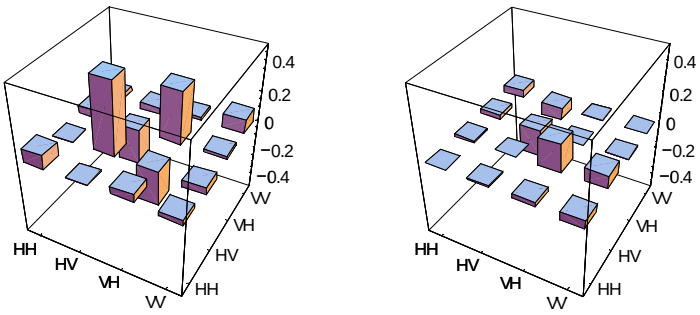


図 3-10. 量子トモグラフィー評価結果(忠実度 70.5%)

(2)研究成果の今後期待される効果

本グループでは偏波に基づく多光子間量子もつれ合い技術の開発を研究課題とし量子暗号ネットワーク/量子中継システムに関する基盤要素技術を開発し、最終的には四光子レベルでの量子干渉及び量子もつれ交換実験を通信波長帯で実施した。通信波長帯量子情報通信システムの実現へ向けて一定の成果が得られたといえるが、量子中継システムに求められる量子メモリや高効率ベル測定技術などの未解決の研究課題も多い。今後、本研究成果と超伝導光子検出器による量子効率の改善、量子メモリの候補となる可能性のある物質・メカニズムの探索等を結びつけることで次世代量子暗号通信技術の中核である量子中継技術における重要な要素技術である量子もつれ光子対発生、光子検出、中継システムの高度化が期待される。

§5 成果発表等

(1)原著論文発表　(国内(和文)誌 0 件、国際（欧文）誌 69 件)

1. T. Honjo, K. Inoue, "Differential-phase-shift QKD with an extended degree of freedom," *Opt. Lett.* **31**, 522 (Feb. 2006).
   DOI: 10.1364/OL.31.000522

2. K. Inoue, H. Takesue, "Quantum key distribution using entangled-photon trains with no basis selection," *Phys. Rev. A* **73**, 032332 (Mar. 2006).
   DOI: 10.1103/PhysRevA.73.032332

3. H. Takesue, "Long-distance distribution of time-bin entanglement generated in a cooled fiber," *Opt. Express* **14**, 3453 (Apr. 2006).
   DOI: 10.1364/OE.14.003453

4. T. Honjo, K. Inoue, A. Sahara, E. Yamazaki, H. Takahashi, "Quantum key distribution experiment through a PLC matrix switch," *Opt. Commun.* **263**, 120 (Jul. 2006).
   DOI: 10.1016/j.optcom.2006.01.018

5. H. Takesue, K. Inoue, "Quantum secret sharing based on modulated high-dimension time-bin entanglement," *Phys. Rev. A* **74**, 012315 (Jul. 2006).
   DOI: 10.1364/OE.16.015469

6. H. Takesue, T. Honjo, H. Kamada, "Differential phase shift quantum key distribution using 1.3-μm up-conversion detectors," *Jpn. J. Appl. Phys.* **45**, 5757 (Jul. 2006).
   DOI: 10.1143/JJAP.45.5757

7. K. Inoue, "Quantum key distribution technologies," *IEEE J. Sel. Top. Quantum Electron.* **12**, 888 (Aug. 2006).
   DOI: 10.1109/JSTQE.2006.876606

8. A. Yoshizawa, H. Tsuchida, "Timing adjustment of incoming photons in the gated-mode single-photon detection at 1550 nm," *Jpn. J. Appl. Phys. Pt.2.* **45**, L854 (Aug. 2006).
   DOI: 10.1143/JJAP.45.L854

9. X. Ma, C-H. F. Fred, F. Dupuis, K. Chen, K. Tamaki, H-K. Lo, "Decoy-state quantum key distribution with two-way classical postprocessing," *Phys. Rev. A.* **74**, 032330 (Sept. 2006).
   DOI: 10.1103/PhysRevA.74.032330

10. H. Takesue, E. Diamanti, C. Langrock, M. M. Fejer, Y. Yamamoto, "10-GHz clock differential phase shift quantum key distribution experiment," *Opt. Express* **14**, 9522 (Oct. 2006).
    DOI: 10.1364/OE.14.009522

11. H. Takesue, E. Diamanti, C. Langrock, M. M. Fejer, Y. Yamamoto, "1.5-μm single photon counting using polarization-independent up-conversion detector," *Opt. Express* **14**, 13067 (Dec. 2006).
    DOI: 10.1364/OE.14.013067

12. E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, Y. Yamamoto, "100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors," *Opt. Express* **14**, 13073 (Dec. 2006).
    DOI: 10.1364/OE.14.013073A.

13. Yoshizawa, S. Odate, H. Tsuchida, "Discharge pulse counting for low-noise single-photon detection at 1550 nm using an InGaAs avalanche photodiode cooled to 130 K," *Jpn. J. Appl. Phys. Pt.1.* **46**, 220 (Jan. 2007).
DOI: 10.1143/JJAP.46.220

14. T. Honjo, H. Takesue, K. Inoue, "Generation of energy-time entangled photon pairs in 1.5-μm band with periodically poled lithium niobate waveguide," *Opt. Express* **15**, 1679 (Feb. 2007).
DOI: 10.1364/OE.15.001679

15. C-H. F. Fung, B. Qi, K. Tamaki, H-K. Lo, "Phase-Remapping Attack in Practical Quantum Key Distribution Systems," *Phys. Rev. A* **75**, 032314 (Mar. 2007).
DOI: 10.1103/PhysRevA.75.032314

16. T. Honjo, H. Takesue, K. Inoue, "Differential-phase quantum key distribution experiment using a series of quantum entangled photon pairs," *Opt. Lett.* **32**, 1165 (May 2007).
DOI: 10.1364/OL.32.001165

17. H. Takesue, "1.5-μm band Hong-Ou-Mandel experiment using photon pairs generated in two independent dispersion shifted fibers," *Appl. Phys. Lett.* **90**, 204101 (May 2007).
DOI: 10.1063/1.2739077

18. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, Y. Yamamoto, "Quantum key distribution over 40 dB channel loss using superconducting single-photon detectors," *Nature Photonics* **1**, 343 (Jun. 2007).
DOI: 10.1038/nphoton.2007.75

19. N. Namekata, G. Fujii, S. Inoue, T. Honjo, H. Takesue, "Differential phase shift quantum key distribution using single-photon detectors based on a sinusoidally gated InGaAs/InP avalanche photodiode," *Appl. Phys. Lett.* **91**, 011112 (Jul. 2007).
DOI: 10.1063/1.2753767

20. Q. Zhang, X. Xie, H. Takesue, S. W. Nam, C. Langrock, M. M. Fejer, Y. Yamamoto, "Correlated photon-pair generation in reverse-proton-exchange PPLN waveguides with integrated mode demultiplexer at 10 GHz clock," *Opt. Express* **15**, 10288 (Jul. 2007).
DOI: 10.1364/OE.15.010288

21. T. Honjo, H. Takesue, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, K. Inoue, "Long-distance distribution of time-bin entangled photon pairs over 100 km using frequency up-conversion detectors," *Opt. Express* **15**, 13957 (Oct. 2007).
DOI: 10.1364/OE.15.013957

22. S. Odate, A. Yoshizawa, D. Fukuda, H. Tsuchida, "Quantum efficiency measurements by bidirectional coincidence counting of correlated photon pairs," *Opt. Lett.* **32**, 3176 (Oct. 2007).
DOI: 10.1364/OL.32.003176

23. H. Takesue, Y. Tokura, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, S. Itabashi, "Entanglement generation using silicon wire waveguide," *Appl. Phys. Lett.* **91**, 201108 (Nov. 2007).
DOI: 10.1063/1.2814040

24. T. Honjo, S. Yamamoto, T. Yamamoto, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, K. Inoue, "Field trial of differential-phase-shift quantum key distribution using polarization independent frequency up-conversion detectors," *Optics Express* **15**, 15920 (Nov. 2007).

DOI: 10.1364/OE.15.015920

25. S. Odate, A. Yoshizawa, H. Tsuchida, "Polarisation-entangled photon-pair source at 1550 nm using 1-mm-long PPLN waveguide in fiber-loop configuration," *Electron. Lett.* **43**, 1376 (Nov. 2007).
DOI: 10.1049/el:20071590

26. Q. Zhang, C. Langrock, H. Takesue, X. Xie, M. M. Fejer, Y. Yamamoto, "Generation of 10-GHz clock sequential time-bin entanglement," *Opt. Express* **16**, 3293 (Feb. 2008).
DOI: 10.1364/OE.16.003293

27. K. Tamaki, "Unconditionally secure quantum key-distribution with relatively strong signal pulse," *Phys. Rev. A* **77**, 032341 (Mar. 2008).
DOI: 10.1103/PhysRevA.77.032341

28. H. Takesue, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, Y. Tokura, S. Itabashi, "Generation of polarization entangled photon pairs using silicon wire waveguide," *Opt. Express* **16**, 5721 (Apr. 2008).
DOI: 10.1364/OE.16.005721

29. Q. Zhang, H. Takesue, S. W. Nam, C. Langrock, X. Xie, B. Baek, M. M. Fejer, Y. Yamamoto, "Distribution of time-energy entanglement over 100 km fiber using superconducting singlephoton detectors," *Opt. Express* **16**, 5776 (Apr. 2008).
DOI: 10.1364/OE.16.005776

30. M. Curty, K. Tamaki, T. Moroder, "Effect of detector dead times on the security evaluation of differential-phase-shift quantum key distribution against sequential attacks," *Phys. Rev. A* **77**, 052321 (May. 2008).
DOI: 10.1103/PhysRevA.77.052321

31. H. Lim, A. Yoshizawa, H. Tsuchida, K. Kikuchi, "Stable source of high quality telecom-band polarization-entangled photon-pairs based on a single, pulse-pumped, short PPLN waveguide," *Opt. Express* **16**, 12460 (Aug. 2008).
DOI: 10.1364/OE.16.012460

32. T. Tsurumaru, K. Tamaki, "Security proof for quantum-key-distribution systems with threshold detectors," *Phys. Rev. A* **78**, 032302 (Sept. 2008).
DOI: 10.1103/PhysRevA.78.032302

33. H. Lim, A. Yoshizawa, H. Tsuchida, K. Kikuchi, "Distribution of polarization-entangled photon-pairs produced via spontaneous parametric down-conversion within a local-area fiber network: Theoretical model and experiment," *Opt. Express* **16**, 14512 (Sept. 2008).
DOI: 10.1364/OE.16.014512

34. K. Inoue, T. Ohashi, T. Kukita, K. Watanabe, S. Hayashi, T. Honjo, H. Takesue, "Differential-phase-shift quantum secret sharing," *Opt. Express* **16**, 15469 (Sept. 2008).
DOI: 10.1364/OE.16.015469

35. H. Lim, A. Yoshizawa, H. Tsuchida, K. Kikuchi, "Broadband source of telecom-band polarization-entangled photon-pairs for wavelength-multiplexed entanglement distribution," *Opt. Express* **16**, 16052 (Sept. 2008).
DOI: 10.1364/OE.16.016052

36. H. Shibata, T. Maruyama, T. Akazaki, H. Takesue, T. Honjo, Y. Tokura, "Photon detection and fabrication of MgB2 nanowire," *Physica C* **468**, 1992 (Sept. 2008).
DOI: 10.1016/j.physc.2008.05.248

37. H. Takesue, “Erasing distinguishability using quantum frequency up-conversion,” *Phys. Rev. Lett.* **101**, 173901 (Oct. 2008).
DOI: 10.1103/PhysRevLett.101.173901

38. T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, Y. Yamamoto, “Long-distance entanglement-based quantum key distribution over optical fiber,” *Opt. Express* **16**, 19118 (Nov. 2008).
DOI: 10.1364/OE.16.019118

39. T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, Y. Yamamoto, “Long-distance entanglement-based quantum key distribution over optical fiber,” *Opt. Express* **16**, 19118 (Nov. 2008).
DOI: 10.1364/OE.16.019118

40. K. Harada, H. Takesue, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, Y. Tokura, S. Itabashi, “Generation of high-purity entangled photon pairs using silicon wire waveguide,” *Opt. Express* **16**, 20368 (Nov. 2008).
DOI: 10.1364/OE.16.020368

41. H. Lim, A. Yoshizawa, H. Tsuchid, K. Kikuchi, “Wavelength-multiplexed distribution of highly entangled photon-pairs over optical fiber,” *Opt. Express* **16**, 22099 (Dec. 2008).
DOI: 10.1364/OE.16.022099

42. K. Inoue, Y. Iwai, “Differential-quadrature-phase-shift quantum key distribution,” *Phys. Rev. A* **79**, 022319 (Feb. 2009).
DOI: 10.1103/PhysRevA.79.022319

43. B. Miquel, H. Takesue, “Observation of 1.5 μm band entanglement using single photon detectors based on sinusoidally gated InGaAs/InP avalanche photodiodes,” *New J. Phys.* **11**, 045006 (Apr. 2009).
DOI: 10.1088/1367-2630/11/4/045006

44. Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, Y. Yamamoto, “Megabits secure key rate quantum key distribution,” *New J. Phys.* **11**, 045010 (Apr. 2009).
DOI: 10.1088/1367-2630/11/4/045010

45. Y. Iwai, T. Honjo, K. Inoue, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, “Polarization-independent, differential-phase-shift, quantum-key distribution system using upconversion detectors,” *Opt. Lett.* **34**, 1606 (May 2009).
DOI: 10.1364/OL.34.001606

46. H. Takesue, B. Miquel, “Entanglement swapping using telecom-band photons generated in fibers,” *Opt. Express* **17**, 10748 (Jun. 2009).
DOI: 10.1364/OE.17.010748

47. H. Takesue, Y. Noguchi, “Implementation of quantum state tomography for time-bin entangled photon pairs,” *Opt. Express* **17**, 10976 (Jun. 2009).
DOI: 10.1364/OE.17.010976

48. J. F. Dynes, H. Takesue, Z. L. Yuan, A. W. Sharpe, K. Harada, T. Honjo, H. Kamada, O. Tadanaga, Y. Nishida, M. Asobe, A. J. Shields, “Efficient entanglement distribution over 200 kilometers,” *Opt. Express* **17**, 11440 (Jul. 2009).

DOI: 10.1364/OE.17.011440

49. H. Takesue, K. Shimizu, "Effects of multiple pairs on visibility measurements of entangled photons generated by spontaneous parametric processes," *Opt. Commun.* **283**, 276 (Jul. 2009).
DOI: 10.1016/j.optcom.2009.10.008

50. K. Tamaki, N. Lutkenhaus, M. Koashi, J. Batuwantudawe, "Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse," *Phys. Rev. A* **80**, 032302 (Sept. 2009).
DOI: 10.1103/PhysRevA.80.032302

51. M. Lucamarin, G. Di Giuseppe, K. Tamaki, "Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states," *Phys. Rev. A* **80**, 032327 (Sept. 2009).
DOI: 10.1103/PhysRevA.80.032327

52. K. Wen, K. Tamaki, Y. Yamamoto, "Unconditional security of single-photon differential phase shift quantum key distribution," *Phys. Rev. Lett.* **103**, 170503 (Oct. 2009).
DOI: 10.1103/PhysRevLett.103.170503

53. K. Harada, H. Takesue, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, Y. Tokura, S. Itabashi, "Frequency and polarization characteristics of correlated photon-pair generation using a silicon wire waveguide," *IEEE J. Sel. Top. Quantum Electron.* **16**, 325 (Jan. 2010).
DOI: 10.1109/JSTQE.2009.2023338

54. K. Tamaki, G. Kato, "Quantum circuit for the proof of the security of quantum key distribution without encryption of error syndrome and noisy processing," *Phys. Rev. A* **81**, 022316 (Feb. 2010).
DOI: 10.1103/PhysRevA.81.022316

55. H. Takesue, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, Y. Tokura, S. Itabashi, "Entanglement generation using silicon wire waveguide," *Opt. Spectrosc.* **108**, 160 (Feb. 2010).
DOI: 10.1134/S0030400X10020025

56. H. Takesue, K. Harada, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, Y. Tokura, S. Itabashi, "Entanglement generation using silicon photonic wire waveguide," *J. Nanosci. Nanotechnol.* **10**, 1814 (Mar. 2010).
DOI: 10.1166/jnn.2010.2048

57. Y. Xue, A. Yoshizawa, H. Tsuchida, "Hong-Ou-Mandel dip measurements of polarization-entangled photon pairs at 1550 nm," *Opt. Express* **18**, 8182 (Apr. 2010).
DOI: 10.1364/OE.18.008182

58. K. Tamaki, T. Tsurumaru, "Security Proof of Quantum Key Distribution," *IEICE Trans. Fund.* **E93-A**, 880 (May 2010).
DOI: 10.1587/transfun.E93.A.880

59. K. Inoue, "DPS Quantum Key Distribution System," *IEICE Trans. Fund.* **E93-A**, 897 (May 2010).
DOI: 10.1587/transfun.E93.A.897

60. H. Takesue, T. Honjo, K. Harada, B. Miquel, "Quantum communication experiments using telecom-band entangled photons," *IEICE Trans. Fund.* **E93-A**, 903 (May 2010).
DOI: 10.1587/transfun.E93.A.903

61. Q. Zhang, H. Takesue, C. Langrock, Xiuping Xie, M. M. Fejer, Y. Yamamoto, “Hong-Ou-Mandel dip using degenerate photon pairs from a single periodically poled lithium niobate waveguide with integrated mode demultiplexer,” *Jpn. J. Appl. Phys.* **49**, 064401 (Jun. 2010).
DOI: 10.1143/JJAP.49.064401

62. H. Takesue, K. Harada, K. Tamaki, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, S. Itabashi, “Long-distance entanglement-based quantum key distribution experiment using practical detectors,” *Opt. Express* **18**, 16777 (Jul. 2010).
DOI: 10.1364/OE.18.016777

63. H. Takesue, “Single-photon frequency down-conversion experiment,” *Phys. Rev. A* **82**, 013833 (Jul. 2010).
DOI: 10.1103/PhysRevA.82.013833

64. H. Lim, A. Yoshizawa, H. Tsuchida, K. Kikuchi, “Wavelength-multiplexed entanglement distribution,” *Opt. Fiber Technol.* **16**, 225 (Aug. 2010).
DOI: 10.1016/j.yofte.2010.05.001

65. M. Hunault, H. Takesue, O. Tadanaga, Y. Nishida, M. Asobe, “Generation of time-bin entangled photon pairs by cascaded second-order nonlinearity in a single periodically poled LiNbO3 waveguide,” *Opt. Lett.* **35**, 1239 (Aug. 2010).
DOI: 10.1364/OL.35.001239.

66. T. Seki, H. Shibata, H. Takesue, Y. Tokura, N. Imoto, “Comparison of timing jitter between NbN superconducting single-photon detector and avalanche photodiode,” *Physica C* **470**, 1534 (Nov. 2010).
DOI: 10.1016/j.physc.2010.05.156

67. T. Kukita, H. Takada, K. Inoue, “Macroscopic differential phase shift quantum key distribution using an optically pre-amplified receiver,” *Jpn. J. Appl. Phys.* **49**, 122801 (Dec. 2010).
DOI: 10.1143/JJAP.49.122801

68. A. Yoshizawa, Y. Xue, H. Tsuchida, “Accidental coincidence counts observed in Mandel dip measurement using independently produced photon pairs at 1550 nm,” *Jpn. J. Appl. Phys.* **49**, 122802 (Dec. 2010).
DOI: 10.1143/JJAP.49.122802

69. H. Kawahara, A. Medhipour, K. Inoue, “Effect of spontaneous Raman scattering on quantum channel wavelength-multiplexed with classical channel,” *Opt. Commun.*, **284**, 691 (Jan. 2011).
DOI: 10.1016/j.optcom.2010.09.051

(2)その他の著作物(総説、書籍など)

1. H. Takesue, T. Honjo, K. Tamaki, Y. Tokura, “Differential phase shift quantum key distribution,” *IEEE Commun. Magazine* **47**, 102 (May 2009).

2. 武居弘樹、「通信波長帯量子もつれ光子対の発生と量子鍵配送への応用」、『情報通信研究機構季報』、52巻3号63頁 (Sept. 2006). / *Journal of the National Institute of Information and Communications Technology* **52**(3), 69 (Sept. 2006) (English translation).

3. 井上恭、「量子暗号通信の最近の動向」、応用物理、75 巻 11 号 1317-1323 頁(Nov. 2006).
4. 武居弘樹、「光ファイバーを用いた光通信波長帯量子もつれ光子対の発生」、『応用物理』、75 巻 11 号 1354 頁 (Nov. 2006).
5. 都倉康弘、森田雅夫、「差動位相シフト方式と波長変換型光子検出器による高速化・長距離化」、『量子情報通信』、監修、佐々木・松岡、オプトロニクス社、第 2 部 第 4 章担当 (Nov. 2006).
6. 吉澤明男、「光ファイバ通信帯での単一光子検出器」、『量子情報通信』、監修、佐々木・松岡、オプトロニクス社、第4部 第1章担当 (Nov. 2006).
7. 井上恭、「量子鍵配送システム －量子もつれ光子対」、『光技術コンタクト』、44 巻、通巻 516、21 頁(Dec. 2006).
8. 武居弘樹、「ニュース解説:200km の光ファイバ上で量子暗号鍵の配送に成功」、『電子情報通信学会誌』、90 巻 10 号 906 頁 (Oct. 2007).
9. 井上恭、『工学系のための量子工学』、森北出版(Feb. 2008).
10. 吉澤明男、「光ファイバ通信波長帯で+の単一光子検出器」、『レーザー研究』、36 巻 8 号 476 頁 (Aug. 2008).
11. 鎌田英彦、俵毅彦、山口貴雄、本庄利守、武居弘樹、西田好毅、忠永修、遊部雅生、井上恭、「通信波長帯単一光子・エンタングル光子対の生成と伝送」、『光学』、 37 巻 8 号 447 頁 (Aug. 2008)
12. 武居弘樹、「量子暗号」、『まぐね』、4 巻、6 号、294 頁 (Jul. 2009)
13. 武居弘樹、「量子暗号通信技術の進展と今後の展望」、『応用物理』、78 巻 10 号 972 頁、(Oct. 2009).
14. 井上恭、「量子光学と量子情報通信 －光の量子的性質をシステム応用へ」、『光アライアンス』、20 巻 10 号 1 頁、(Oct. 2009).
15. 井上恭、「光通信ネットワークに登場する非線形光学効果」、『O plus E』、369 号(Aug. 2010).
16. 玉木潔、「量子鍵配布理論」、電子情報通信学会 知識ベースβ版「知識の森」、S2 群 5 編「量子通信と量子計算」、1 章 1-2、(中村泰信編、分担執筆)、(2010).
17. 井上恭、「離散鍵配布実験:離散量 QKD」、電子情報通信学会 知識ベースβ版「知識の森」、S2 群 5 編 「量子通信と量子計算」、1 章 1-3、(中村泰信編、分担執筆)、(2010).
18. 武居弘樹、「光子検出器技術」、電子情報通信学会 知識ベースβ版「知識の森」、S2 群 5 編 「量子通信と量子計算」、1 章 1-6、(中村泰信編、分担執筆)、(2010).

(3)国際学会発表及び主要な国内学会発表
① 招待講演　　(国内会議 12 件、国際会議 24 件)

1. K. Inoue (Osaka U.), "Differential-phase-shift quantum key distribution," 2006 IEEE/LEOS Summer Top. Meeting on Quantum Commun. in Telecom Networks, Quebec City, Canada, (18 Jul. 2006).
2. E. Diamanti (Stanford U.), C. Langrock (Stanford U.), E. Waks (Stanford U.), M. M. Fejer (Stanford U.), Y. Yamamoto (Stanford U.), H. Takesue (NTT), T. Honjo (NTT), K. Inoue (Osaka U.), "Differential-phase-shift quantum key distribution with up-conversion single-photon detectors," 2006 IEEE/LEOS Summer Top. Meeting on Quantum Commun. in Telecom Networks, Quebec City, Canada, (18 Jul. 2006).
3. Y. Yamamoto (Stanford U.), E. Diamanti (Stanford U.), H. Takesue (NTT), C. Langrock (Stanford U.), M. M. Fejer (Stanford U.), "Differential phase shift quantum key distribution," Conf. on Quantum Information and Quantum Control II, Toronto, Canada, (10 Aug. 2006).
4. K. Inoue (Osaka U.), H. Takesue (NTT), "Generation of entangled photon and their system applications," 2006 OSA Annual Meeting: Frontier in Opt., Rochester, NY., USA, (10 Oct. 2006).
5. K. Inoue (Osaka U.), H. Takesue (NTT), T. Honjo (NTT), "Differential-phase-shift quantum key distribution with single-photon detection," Opt. Fiber Commun. Conf. 2007, Anaheim, CA., USA, (28 Mar. 2007).
6. T. Honjo (NTT), H. Takesue (NTT), H. Kamada (NTT), Y. Nishida (NTT), O. Tadanaga (NTT), M. Asobe, (NTT), K. Inoue (Osaka U.), "Long-distance distribution of time-bin entangled photon pairs over 100 km using frequency up-conversion detectors," 16th Int'l Laser Physics Workshop (LPHYS'07), 7.7.2, Leon, Mexico, (23 Aug. 2007).
7. K. Inoue (Osaka U.), H. Takesue (NTT), T. Honjo (NTT), "Differential-phase-shift quantum key distribution," SPIE Opt. East, Boston, MA., USA, (12 Sept. 2007).
8. Y. Tokura (NTT), "Latest achievement in QKD experiments at NTT," Updating Quantum Cryptography 2007 (UQC 2007), Tokyo, Japan, (2 Oct. 2007).
9. H. Takesue (NTT), "R&D of quantum relay technology at NTT," Updating Quantum Cryptography 2007 (UQC 2007), Tokyo, Japan, (3 Oct. 2007).
10. A. Yoshizawa (AIST), "AIST's technologies for single-photon detection at 1550 nm," Updating Quantum Cryptography 2007 (UQC 2007), Tokyo, Japan, (3 Oct. 2007).
11. H. Takesue (NTT), "Quantum communication experiments using entangled photons generated in dispersion shifted fiber," IEEE/LEOS Winter Top., Sorrento, Italy, (15 Jan. 2008).
12. T. Honjo (NTT), S. W. Nam (NIST), H. Takesue (NTT), Q. Zhang (Stanford U.), H. Kamada (NTT), Y. Nishida (NTT), O. Tadanaga (NTT), M. Asobe (NTT), B. Baek (NIST), R. Hadfield (NIST), S. Miki (NICT), M. Fujiwara (NICT), M. Sasaki (NICT), Z. Wang (NICT), K. Inoue (Osaka U.), Y. Yamamoto (Stanford U.), "Entanglement-based BBM92 QKD experiment using superconducting single photon detectors," 17th Int'l Laser Phys. Workshop (LPHYS'08), 7.10.4, Trondheim, Norway, (3 Jul. 2008).
13. H. Lim (U. of Tokyo), A. Yoshizawa (AIST), H. Tsuchida(AIST), K. Kikuchi (U. of Tokyo), "Broad-band source of polarization-entangled photon-pairs suitable for multi-channel wavelength-multiplexed entanglement distribution," 34th Eur. Conf. and

Exhibition on Opt. Commun. (ECOC2008), Brussels, Belgium, (22 Sept. 2008).

14. H. Takesue (NTT), H. Fukuda (NTT), T. Tsuchizawa (NTT), T. Watanabe (NTT), K. Yamada (NTT), Y. Tokura (NTT), S. Itabashi (NTT), "Entanglement generation using silicon wire waveguide," 5th Int'l Conf. on Group IV Photonics (GFP 2008), FD1, Sorrento, Italy, (19 Sept. 2008).

15. H. Takesue (NTT), K. Harada (NTT), H. Fukuda (NTT), T. Tsuchizawa (NTT), T. Watanabe (NTT), K. Yamada (NTT), Y. Tokura (NTT), S. Itabashi (NTT), "Entanglement generation using silicon wire waveguide," XII Int'l Conf. on Quantum Opt. and Quantum Information (ICQO2008), Vilnius, Lithuania, (22 Sept. 2008).

16. H. Takesue (NTT), H. Fukuda (NTT), T. Tsuchizawa (NTT), T. Watanabe (NTT), K. Yamada (NTT), Y. Tokura (NTT), S. Itabashi (NTT), "Entanglement generation using silicon photonic wire waveguide," The 2nd IEEE Nanotechnology Materials and Devices Conf. (NMDC 2008), MoC II-3, Kyoto, Japan, (20 Oct. 2008).

17. K. Yamada (NTT), T. Tsuchizawa (NTT), T. Watanabe (NTT), H. Fukuda (NTT), H. Shinojima (NTT), H. Nishi (NTT), H. Takesue (NTT), T. Tanabe (NTT), A. Shinya (NTT), E. Kuramochi (NTT), M. Notomi (NTT), Y. Tokura (NTT), S. Itabashi (NTT), "Applications of nonlinear effects in silicon wire waveguides: all-optical modulation, wavelength conversion, and quantum entanglement," SPIE Asia-Pacific Opt. Commun. (APOC 2008), Paper 7134-64, Hangzhou, China, (28 Oct. 2008).

18. H. Takesue (NTT), T. Honjo (NTT), "Quantum communication experiments using telecom-band entangled photons," LEOS Annual Meeting 2008, ThG4, Newport Beach, CA., USA, (13 Nov. 2008).

19. K. Tamaki (NTT), "Unconditional security proof of QKD and imperfections of devises," Updating Quantum Cryptography 2008, Tokyo, Japan, (2 Dec. 2008).

20. H. Takesue (NTT), "Telecom-band entanglement swapping using high-speed single photon detectors based on sinusoidally gated InGaAs/InP avalanche photodiodes," SPIE Defense Security + Sensing 2009, Advanced Photon Counting Techniques III, (Proc. SPIE, Vol. 7320), Orlando, FL., USA, (14 Apr. 2009).

21. H. Takesue (NTT), K. Harada (NTT), H. Fukuda (NTT), T. Tsuchizawa (NTT), T. Watanabe (NTT), K. Yamada (NTT), Y. Tokura (NTT), S. Itabashi (NTT), "Silicon photonics in quantum communications," CLEO/IQEC 2009, CMAA1, Baltimore, MD., USA, (1 Jun. 2009).

22. H. Takesue (NTT), "Quantum communication experiments using telecom-band entangled photons," Int'l Conf. on Quantum Information and Technology (ICQIT), Tokyo, Japan, (3 Dec. 2009).

23. H. Lim (U.of Tokyo), A. Yoshizawa (AIST), H. Tsuchida (AIST), K. Kikuchi (U.of Tokyo), "Broadband source of polarization-entangled photon-pairs suitable for multi-channel wavelength-multiplexed entanglement distribution," 2nd Global COE Int'l Symposium - Electronic Device Innovation (EDIS 2009) - Frontier Workshop for Advanced Opt. Commun., Osaka, Japan, (11 Dec. 2009).

24. H. Takesue (NTT), "Single-Photon Frequency Downconversion Experiment," Photonics Global Conference 2010, Oral 3-4A-2, Suntec, Singapore, (16 Dec. 2010).

25. 井上恭(阪大)、「量子暗号通信 -暗号通信と量子力学の融合」、大阪大学情報通信技術シンポジウム、千里ライフサイエンスセンター(大阪)、(2006 年 2 月 17 日)

26. 井上恭(阪大)、「量子情報の話 −究極の暗号通信から超並列情報処理まで」、適塾の夕べ、洪庵忌(大阪)、(2006 年 6 月 5 日)

27. 武居弘樹(NTT)、「光ファイバ網を用いた量子通信」、第 2 回光産業創出フォーラム、慶応義塾大学(東京)、(2006 年 8 月 23 日)

28. 井上恭(阪大)、「量子暗号研究の動向」、日本光学会年次学術講演会、Opt. and Photonics Japan 2006・シンポジウム「量子情報通信技術の進展」、学術総合センター(東京)、(2006 年 11 月 8 日)

29. 武居弘樹(NTT)、「光ファイバを用いた量子もつれ光子対の発生」、日本光学会年次学術講演会、Optics and Photonics Japan 2006・シンポジウム「量子情報通信技術の進展」、学術総合センター(東京)、(2006 年 11 月 8 日)

30. 井上恭(阪大)、「量子鍵配送システム−量子もつれ光子対」、日本オプトメカトロニクス協会セミナー、機械振興会館(東京)、(2006 年 12 月 7 日)

31. 武居弘樹(NTT)、「分極反転デバイスを用いた単一光子検出器と量子暗号への応用」、第 54 回応用物理学関係連合講演会・シンポジウム「時代が求める分極反転光デバイス」、28p−ZS−10、青山学院大学(神奈川)、(2007 年 3 月 28 日)

32. 武居弘樹(NTT)、「光通信波長帯における量子情報通信」、未踏・ナノデバイステクノロジー第 151 委員会、浜松研修センター、(静岡)、(2007 年 4 月 20 日)

33. 武居弘樹(NTT)、「差動位相シフト量子鍵配送実験」、第3回量子情報未来テーマ開拓研究会、ホテルサンライズ知念(沖縄)、(2007 年 9 月 1 日)

34. 武居弘樹(NTT)、原田健一(NTT)、福田浩(NTT)、土澤泰(NTT)、渡辺俊文(NTT)、山田浩治(NTT)、都倉康弘(NTT)、板橋聖一(NTT)、「シリコン細線導波路を用いた量子もつれ発生」、2009 年春季応用物理学関係連合講演会、31p−ZT−8、筑波大学(茨城)、(2009 年 3 月 31 日)

35. 武居弘樹(NTT)、「光通信波長帯における量子通信実験」、応用物理学会・量子エレクトロニクス研究会 −量子情報の最前線と今後 10 年の展開、上智大学(長野)、(2010 年 1 月 9 日)

36. 武居弘樹(NTT)、「光通信波長帯量子もつれ光子対を用いた量子通信実験」、電子情報通信学会総合大会、エレクトロニクスソサイエティ・シンポジウム「量子エンタングルメントの展開(実験, 理論から応用まで)」、東北大学(宮城)、(2010 年 3 月 16 日)

②口頭講演　　(国内会議 79 件、国際会議 38 件)

1. H. Takesue (NTT), “Long-distance distribution of time-bin entangled photon pairs generated in optical fiber cooled by liquid nitrogen,” CLEO/QELS 2006, JTuA3, Longbeach, CA., USA, (23 May 2006).

2. T. Honjo (NTT), H. Takesue (NTT), K. Inoue (Osaka U.), “Generation of energy-time entangled photon pairs in 1.5 μ m band with periodically poled lithium niobate waveguide,” CLEO/QELS 2006, JTuA5, Longbeach, CA., USA, (23 May 2006).

3. E. Diamanti (Stanford U.), C. Langrock (Stanford U.), E. Waks (Stanford U.), M. M. Fejer (Stanford U.), Y. Yamamoto (Stanford U.), H. Takesue (NTT), T. Honjo (NTT), K. Inoue (Osaka U.), “Fast and long-distance differential-phase-shift quantum key distribution,” CLEO/QELS 2006 , JTuH2, Longbeach, CA., USA, (23 May 2006).

4. T. Honjo (NTT), H. Takesue (NTT), K. Inoue (Osaka U.), “Differential-phase quantum key distribution experiment using a series of quantum entangled photon pairs,” 15th Int’l Laser Physics Workshop (LPHYS’06), 7.7.5, Lausanne, Switzerland, (27 Jul. 2006).

5. K. Tamaki (NTT), N. Lutkenhaus (U. Waterloo), M. Koashi (Osaka U.), J. Batuwantudawe (U. Waterloo), “Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse,” Conf. on Quantum Information and Quantum Control II (CQIQC), Toronto, Canada, (8 Aug, 2006).

6. H. Takesue (NTT), E. Diamanti (Stanford U.), C. Langrock (Stanford U.), M. M. Fejer (Stanford U.), Y. Yamamoto (Stanford U.), “100 km secure key distribution using low-jitter up-conversion detectors,” The 8th Int’l Conf. on Quantum Commun., measurement and computing (QCMC ’06), SA4-2, Tsukuba, Ibaraki, Japan, (2 Dec. 2006).

7. K. Inoue (Osaka U.), S. Hayashi (Osaka U.), “Secret key distribution using differential-phase-shift keyed macroscopic coherent light,” CLEO/QELS2007, QML7, Baltimore, MD., USA, (7 May 2007).

8. X. Xie (Stanford U.), Q. Zhang (Stanford U.), C. Langrock (Stanford U.), Y. Yamamoto (Stanford U.), M. M. Fejer (Stanford U), H. Takesue (NTT), S. W. Nam (NIST), “Photon pair generation in reverse-proton-exchange lithium niobate waveguides with mode demultiplexing at a pump repetition rate of 10 GHz,” CLEO/QELS 2007, QWF4, Baltimore, MD., USA, (9 May 2007).

9. A. Yoshizawa (AIST), S. Odate (AIST), D. Fukuda (AIST), H. Tsuchida (AIST), “Bidirectional coincidence counting of correlated photons to determine the ditection efficiency of a single-photon detector without a reference standard,” CLEO/Pacific Rim2007, Soul, Korea, (28 Aug. 2007).

10. S. Odate (AIST), A. Yoshizawa (AIST), H. Tsuchida (AIST), “Polarization-entangled photon source based on the fiber loop configuration in the telecom wavelength band,” CLEO/Pacific Rim2007, Soul, Korea, (28 Aug. 2007).

11. N. Namekata (Nihon U.), G. Fujii (Nihon U.), T. Honjo (NTT), H. Takesue (NTT), S. Inoue (Nihon U.), “Quantum key distribution using single-photon detectors based on sinusoidally gated InGaAs/InP avalanche photodiodes,” CLEO/Pacific Rim 2007, Soul, Korea, (August 2007).

12. H. Takesue (NTT), H. Fukuda (NTT), T. Tsuchizawa (NTT), T. Watanabe (NTT), K. Yamada (NTT), Y. Tokura (NTT), S. Itabashi (NTT), “Entanglement generation using silicon wire waveguide,” Eur. Conf. Opt. Commun. (ECOC 2007), postdedline paper 2.3, Berlin, Germany, (20 September 2007).

13. Y. Iwai (Osaka U.), T. Honjo (NTT), K. Inoue (Osaka U.), H. Kamada (NTT), Y. Nishida (NTT), O. Tadanaga (NTT), M. Asobe (NTT), “Polarization independent DPS-QKD system using up-conversion detectors,” CLEO/QELS2008, QWB5, San Jose, CA., USA, (7 May 2008).

14. K. Inoue (Osaka U.), K. Hosokawa (Osaka U.), Y. Noguchi (Osaka U.), S. Hayashi (Osaka U.), “Differential-phase-shift quantum key distribution utilizing decoy pulses,” CLEO/QELS2008, QWB6, San Jose, CA., USA, (7 May 2008).

15. T. Honjo (NTT), S. W. Nam (NIST), H. Takesue (NTT), Q. Zhang, H. Kamada (NTT), Y. Nishida (NTT), O. Tadanaga (NTT), M. Asobe (NTT), B. Baek (NIST), R. H. Hadfield (NIST), S. Miki (NICT), M. Fujiwara (NICT), M. Sasaki (NICT), Z. Wang (NICT), K. Inoue (Osaka U.), Y. Yamamoto (Stanford U.), “Entanglement-based BBM92 QKD experiment using superconducting single photon detectors,” CLEO/QELS2008, QWB1, San Jose, CA., USA, (7 May 2008).

16. Q. Zhang (Stanford U.), H. Takesue (NTT), C. Langrock (Stanford U.), X. Xie (Stanford U.), M. M. Fejer (Stanford U.), Y. Yamamoto (Stanford U.), "Hong-Ou-Mandel dip using photon pairs from a PPLN waveguide," CLEO/QELS2008, QFE1, San Jose, CA., USA, (9 May 2008).

17. H. Lim (U. of Tokyo), A. Yoshizawa (AIST), H. Tsuchida (AIST), K. Kikuchi (U. of Tokyo), "High quality telecom-band polarization-entangled photon-pairs from a stable, pulse-pumped, short PPLN waveguide," CLEO/QELS 2008, QFE2, San Jose, CA., USA, (9 May 2008).

18. H. Takesue (NTT), H. Fukuda (NTT), T. Tsuchizawa (NTT), T. Watanabe (NTT), K. Yamada (NTT), Y. Tokura (NTT), S. Itabashi (NTT), "Generation of 1.5-μm band polarization entanglement using silicon wire waveguide," CLEO/QELS2008, QFE3, San Jose, CA., USA, (9 May 2008).

19. H. Takesue (NTT), T. Honjo (NTT), K. Tamaki (NTT), Y. Tokura (NTT), "Differential phase shift quantum key distribution," ITU-T Kaleidoscope Academic Conf., Innovations in NGN - Future Network and Services, S8.2, Geneva, Switzerland, (13 May 2008).

20. H. Lim (U. of Tokyo), A. Yoshizawa (AIST), H. Tsuchida (AIST), K. Kikuchi (U. of Tokyo), "Wavelength-multiplexed entanglement distribution over 10 km of fiber," ECOC2008, Brussels, Belgium, (25 Sept. 2008).

21. B. Baek (NIST), S. W. Nam (NIST), D. Rosenberg (NIST), J. E. Nordholt (NIST), H. Takesue (NTT), Y. Yamamoto (Standord U.), M. Sasaki (NICT), A. Tomita (NEC), "Application of superconducting single photon detector technology to practical quantum key distribution systems," 2008 Applied Superconductivity Conf. (ASC 2008), 2EY06, Chicago IL., USA, (19 Aug. 2008).

22. H. Shibata (NTT), M. Asahi (NTT), T. Maruyama (NTT), T. Akazaki (NTT), H. Takesue (NTT), T. Honjo (NTT), Y. Tokura (NTT), "Optical Response and Fabrication of MgB2 Nanowire Detectors," 2008 Applied Superconductivity Conf. (ASC 2008), 3EPD02, Chicago IL., USA, (20 Aug. 2008).

23. H. Takesue (NTT), "Swapping telecom-band entanglement generated in fibers," 8th Asian Conf. on Quantum Information Science (AQIS 2008), Seoul, Korea, (30 Aug. 2008).

24. K. Harada (NTT), H. Takesue (NTT), H. Fukuda (NTT), T. Tsuchizawa (NTT), T. Watanabe (NTT), K. Yamada (NTT), Y. Tokura (NTT), S. Itabashi (NTT), "High-purity entanglement generation using silicon wire waveguide," 8th Asian Conf. on Quantum Information Science (AQIS 2008), Seoul, Korea, (30 Aug. 2008).

25. T. Tsurumaru (Mitsubishi Electric Corp.), K. Tamaki (NTT), "Security proof for QKD system with threshold detectors", 8th Asian Conf. on Quantum Information Science (AQIS 2008), Seoul, Korea, (28 Aug. 2008).

26. Q. Zhang (Stanford U.), H. Takesue (NTT), T. Honjo (NTT), K. Wen (Stanford U.), T. Hirohata (Hamamatsu Photon.), M. Suyama (Hamamatsu Photon.), Y. Takiguch i(Hamamatsu Photon.), H. Kamada (NTT), Y. Tokura (NTT), O. Tadanaga (NTT), Y. Nishida (NTT), M. Asobe (NTT), Y. Yamamoto (Stanford U.), "Megabits secure key rate quantum key distribution," CLEO/IQEC 2009, ITul1, Baltimore, MD., USA, (2 Jun. 2009).

27. K. Inoue (Osaka U.), Y. Iwai (Osaka U.), T. Kukita (Osaka U.), T. Honjo (NTT), "Differential-Quadrature-Phase-Shift (DQPS) quantum key distribution," CLEO/IQEC 2009, ITuI4, Baltimore, MD., USA, (2 Jun. 2009).

28. K. Shimizu (NTT), H. Takesue (NTT), K. Tamaki (NTT), “Two-photon interference for quantum cryptography with a non-maximally entangled photon pair,” CLEO/IQEC 2009, IWC6, Baltimore. MD., USA, (3 Jun. 2009).

29. H. Takesue (NTT), “Erasing frequency distinguishability using single-photon up-conversion,” CLEO/IQEC 2009, IThJ7, Baltimore, MD., USA, (4 Jun. 2009).

30. J. F. Dynes (Toshiba), H. Takesue (NTT), Z. L. Yuan (Toshiba), A. W. Sharpe (Toshiba), K. Harada (NTT), T. Honjo (NTT), H. Kamada (NTT), O. Tadanaga (NTT), Y. Nishida (NTT), M. Asobe (NTT), A. J. Shields (Toshiba), “Ulta-long distance and efficient entanglement distribution over 200 kilometers,” CLEO/IQES 2009, postdeadline paper IPDA7, Baltimore, MD., USA, (4 Jun. 2009).

31. H. Takesue (NTT), K. Harada (NTT), K. Tamaki (NTT), H. Fukuda (NTT), T. Tsuchizawa (NTT), T. Watanabe (NTT), K. Yamada (NTT), S. Itabashi (NTT), “Unconditionally secure entanglement-based quantum key distribution experiment,” Conf. on Quantum Information & Quantum Control (CQIQC) III, Session 10, Toronto, Canada, (27 Aug. 2009).

32. K. Yamada (NTT), T. Tsuchizawa (NTT), T. Watanabe (NTT), H. Fukuda (NTT), H. Shinojima (NTT), H. Nishi (NTT), K. Harada (NTT), H. Takesue (NTT), Y. Tokura (NTT), S. Itabashi (NTT), “Nonlinear functions and quantum entanglement generation using silicon photonic wire waveguides,” ECOC 2009, Session 7.2, Vienna, Austria, (23 Sept. 2009).

33. J. F. Dynes (Toshiba), H. Takesue (NTT), Z. L. Yuan (Toshiba), A. W. Sharpe (Toshiba), K. Harada (NTT), T. Honjo (NTT), H. Kamada (NTT), O. Tadanaga (NTT), Y. Nishida (NTT), M. Asobe (NTT), A. J. Shields (Toshiba), “Efficient entanglement distribution over 200 kilometers fiber using self-differencing InGaAs avalanche photodiodes,” Frontiers in Opt. 2009, JWE2, San Jose, CA., USA, (14 Oct. 2009).

34. K. Inoue (Osaka U.), T. Kukita (Osaka U.), H. Takada (Osaka U.), “Macroscopic DPS-QKD using an optically amplified receiver,” CLEO/QELS 2010, QThI3, San Jose, CA., USA, (20 May 2010).

35. Y. Xue (AIST), A. Yoshizawa (AIST), H. Tsuchida (AIST), “Quantum interference measurement for realizing a polarization-based quantum relay at 1550 nm,” CLEO/QELS2010, QThI6, San Jose, CA., USA, (20 May 2010).

36. M. Hunault (ESPCI ParisTech & NTT), H. Takesue (NTT), O. Tadanaga (NTT), Y. Nishida (NTT), M. Asobe (NTT), “Generation of time-bin entangled photon pairs using cascaded second-order nonlinearity in single periodically-poled lithium niobate waveguide,” CLEO/QELS 2010, QThG4, San Jose, CA., USA, (20 May 2010).

37. H. Takesue (NTT), “Quantum frequency downconversion experiment,” QCMC 2010, P3-1, Brisbane, Australia, (22 Jul. 2010).

38. K. Tamaki (NTT), G. Kato (NTT), “Quantum circuit for security proof of quantum key distribution without encryption of error syndrome and noisy processing,” 10th Asian Conf. on Quantum Information Science (AQIS 2010), Tokyo, Japan, (29 Aug. 2010).

39. 吉澤明男(産総研)、土田英実(産総研)、「放電パルス測定による光子検出の最適化」、2006 年春季 第 53 回 応用物理関係連合講演会、24p-T-2、武蔵工業大学(東京)、(2006 年 3 月 24 日)

40. 井上恭(阪大)、武居弘樹(NTT)、「時間量子もつれ光パルス列による量子鍵配送の提案」、2006 年春季 第 53 回 応用物理関係連合講演会、24p-T-17、武蔵工業大学(東京)、(2006 年 3 月 24 日)

41. 武居弘樹(NTT)、E. Diamanti(スタンフォード大)、本庄利守(NTT)、C. Langrock(スタンフォード大)、M. M. Fejer(スタンフォード大)、井上恭(NTT)、山本喜久(スタンフォード大)、「周波数上方変換型単一光子検出器を用いた高速な差動位相シフト量子鍵配送実験」、2006 年春季 第 53 回 応用物理関係連合講演会、24p-T-18、武蔵工業大学(東京)、(2006 年 3 月 24 日)

42. 渡辺一弘(阪大)、本庄利守(NTT)、武居弘樹(NTT)、井上恭(阪大)、「差動位相シフト量子秘密共有」、2006 年春季 第 53 回応用物理関係連合講演会、24p-T-19、武蔵工業大学(東京)、(2006 年 3 月 24 日)

43. 本庄利守(NTT)、武居弘樹(NTT)、井上恭(阪大)、「導波路型PPLNを用いた 1.5μm 帯 energy-time entanglement の発生」、2006 年春季 第 53 回応用物理関係連合講演会、24p-T-20、武蔵工業大学(東京)、(2006 年 3 月 24 日)

44. 鎌田英彦(NTT)、武居弘樹(NTT)、本庄利守(NTT)、西田好殻(NTT)、遊部雅生(NTT)、「通信波長帯 PPLN 周波数上方変換検出器の非ゲートモード動作特性」、2006 年秋季 第 67 回応用物理学会学術講演会、29p-ZB-3、立命館大学(滋賀)、(2006 年 8 月 29 日)

45. 吉澤明男(産総研)、大舘暁(産総研)、土田英実(産総研)、「InGaAs APD の冷却と放電パルス測定による1550nm帯光子検出の低雑音化」、2006年秋季 第67回応用物理学会学術講演会、29p-ZB-4 立命館大学(滋賀)、(2006 年 8 月 29 日)

46. 大舘暁(産総研)、吉澤明男(産総研)、土田英実(産総研)、「ファイバ干渉計を用いた通信波長帯における量子もつれ光子対の生成とその評価」、2006年秋季 第67回応用物理学会学術講演会、29p-ZB-6 立命館大学(滋賀)、(2006 年 8 月 29 日)

47. 井上智博(阪大)、本庄利守(NTT)、井上恭(阪大)、「差動位相シフト量子鍵配送システムにおける光源線幅への要求条件」、2006 年秋季 第 67 回応用物理学会学術講演会、29p-ZB-8、立命館大学(滋賀)、(2006 年 8 月 29 日)

48. 林周作(阪大)、井上恭(阪大)、「2つの巨視的コヒーレント状態を利用した差動位相シフト秘密鍵配送」、2006 年秋季 第 67 回応用物理学会学術講演会、29p-ZB-9、立命館大学(滋賀)、(2006 年 8 月 29 日)

49. 武居弘樹(NTT)、E. Diamanti(スタンフォード大)、 C. Langrock(スタンフォード大)、 M. M. Fejer(スタンフォード大)、 山本喜久(スタンフォード大)、「10GHz クロック差動位相シフト量子鍵配送実験」、2006 年秋季 第 67 回応用物理学会学術講演会、29p-ZB-10、立命館大学(滋賀)、(2006 年 8 月 29 日)

50. 本庄利守(NTT)、武居弘樹(NTT)、井上恭(阪大)、「もつれ光子対列を用いた差動位相量子鍵配送実験」、2006 年秋季 第 67 回応用物理学会学術講演会、 29p-ZB-11、立命館大学(滋賀)、(2006 年 8 月 29 日)

51. 橋本卓郎(芝浦工大)、武居弘樹(NTT)、堀口常雄(芝浦工大)、「Faraday Rotator Mirror による量子相関光子対源の偏波安定化」、2007 年春季 第 54 回応用物理学関係連合講演会、27a-M-2、青山学院大学(神奈川)、(2007 年 3 月 27 日)

52. 大舘暁(産総研)、吉澤明男(産総研)、土田英実(産総研)、「パルス励起したパラメトリック下方変換による通信波長帯光子対の品質評価」、2007 年春季 第 54 回応用物理学関係連合講演会、27a-M-3、青山学院大学(神奈川)、(2007 年 3 月 27 日)

53. 野口由比多(阪大)、武居弘樹(NTT)、「時間位置もつれ光子対の量子トモグラフィ測定」、2007 年春季 第 54 回応用物理学関係連合講演会、27a-M-4、青山学院大学(神奈川)、(2007 年 3 月 27 日)

54. 武居弘樹(NTT)、「2 つの独立した光ファイバで発生した光子対による 1.5μm 帯

Houg-Ou-Mandel 実験」、2007 年春季 第 54 回応用物理学関係連合講演会、27a-M-5、青山学院大学(神奈川)、(2007 年 3 月 27 日)

55. 吉澤明男(産総研)、福田大治(産総研)、大舘暁(産総研)、土田英実(産総研)、「相関光子対によるゲート動作型単一光子検出器信頼性試験」、2007 年春季 第 54 回応用物理学関係連合講演会、27a-M-6、青山学院大学(神奈川)、(2007 年 3 月 27 日)

56. 林周作(阪大)、井上恭(阪大)、「デコイパルスを用いた差動位相シフト量子鍵配送」、2007 年春季 第 54 回応用物理学関係連合講演会、27a-M-8、青山学院大学(神奈川)、(2007 年 3 月 27 日)

57. 玉木潔(NTT)、N. Lutkenhaus(ウォータールー大)、小芦雅斗(阪大)、J. Batuwantudawe(ウォータールー大)、「強い参照光を用いたベネット 1992 量子鍵配送プロトコルの無条件安全性」、第 16 回量子情報技術研究会(QIT16)、NTT 厚木研究開発センタ講堂(神奈川)、(2007 年 5 月 18 日)

58. 柴田浩行(NTT)、丸山達朗(NTT)、赤崎達志(NTT)、武居弘樹(NTT)、本庄利守(NTT)、都倉康弘(NTT)、「MgB2 超伝導ナノワイヤの作成と光検出」、2007 年秋季 第 68 回応用物理学会学術講演会、5a-ZH-9、北海道工業大学(北海道)、(2007 年 9 月 5 日)

59. 本庄利守(NTT)、武居弘樹(NTT)、鎌田英彦(NTT)、西田好毅(NTT)、忠永修(NTT)、遊部雅生(NTT)、井上恭(阪大)、「Time-bin エンタングルメントの 100 km 光ファイバー伝送」、2007 年秋季、第 68 回応用物理学会学術講演会、7p-N-7、北海道工業大学(北海道)、(2007 年 9 月 7 日)

60. 武居弘樹(NTT)、S. W. Nam(NIST)、Q. Zhang(スタンフォード大)、R. H. Hadfield(スタンフォード大)、本庄利守(NTT)、玉木潔(NTT)、山本喜久(スタンフォード大)、「超伝導単一光子検出器を用いた 200 km 量子鍵配送」、2007 年秋季 第 68 回応用物理学会学術講演会、7p-N-9、北海道工業大学(北海道)、(2007 年 9 月 7 日)

61. 行方直人(日大)、藤井剛(日大)、本庄利守(NTT)、武居弘樹(NTT)、井上修一郎(日大)、「500 MHz 正弦電圧ゲート動作型 InGaAs/InP APD を用いた量子鍵配送実験」、2007 年秋季 第 68 回応用物理学会学術講演会、7p-N-10、北海道工業大学(北海道)、(2007 年 9 月 7 日)

62. 野口由比多(阪大)、林周作(阪大)、井上恭(阪大)、「高いレベルおとりパルスを用いた差動位相シフト量子鍵配送」、2007 年秋季 第 68 回応用物理学会学術講演会、7p-N-11、北海道工業大学(北海道)、(2007 年 9 月 7 日)

63. 大橋徹也(阪大)、玉尾圭史(阪大)、井上恭(阪大)、「分配型差動位相シフト量子鍵配送システムの研究」、2007 年秋季 第 68 回 応用物理学会学術講演会、7p-N-12、北海道工業大学(北海道)、(2007 年 9 月 7 日)

64. 林周作(阪大)、渡辺一弘(阪大)、井上恭(阪大)、「差動位相シフト量子秘密共有における誤り訂正・秘匿性増強」、2007 年秋季 第 68 回 応用物理学会学術講演会、7p-N-13、北海道工業大学(北海道)、(2007 年 9 月 7 日)

65. 山本秀人(NTT)、山本貴司(NTT)、本庄利守(NTT)、鎌田英彦(NTT)、西田好毅(NTT)、忠永修(NTT)、遊部雅生(NTT)、「偏波無依存化した周波数上方変換型光子検出器を用いた量子鍵配送フィールド伝送実験」、電子情報通信学会 2007 ソサイエティ大会、B-10-24、鳥取大学(鳥取)、(2007 年 9 月 11 日)

66. 玉木潔(NTT)、N. Lutkenhaus(ウォータールー大)、小芦雅斗(阪大)、J. Batuwantudawe(ウォータールー大)、「強い参照光を用いたベネット 1992 量子鍵配送プロトコルの無条件安全性」、日本物理学会 第 62 回年次大会、23pRG-13、北海道大学(北海道)、(2007 年 9 月 23 日)

67. 行方直人(日大)、藤井剛(日大)、本庄利守(NTT)、武居弘樹(NTT)、井上修一郎(日大)、「正弦電圧ゲート動作型 InGaAs/InP なだれフォトダイオードを用いた高速量子鍵配送」、第17回量子情報技術研究会(QIT17)、山陽新聞さん太ホール(岡山)、(2007年11月22日)

68. 大舘暁(産総研)、吉澤明男(産総研)、土田英実(産総研)、「ファイバーループ構成におけるパルス励起偏波量子もつれ光子対源」、日本光学会年次学術講演会 (Optics & Photonics Japan 2007)、28pA8、大阪大学(大阪)、 (2007年11月28日)

69. 岩井裕樹(阪大)、本庄利守(NTT)、井上恭(阪大)、鎌田英彦(NTT)、西田好毅(NTT)、忠永修(NTT)、遊部雅生(NTT)、「周波数上方変換光子検出器を用いた差動位相シフト量子鍵配送の偏波無依存化」、2008年春季 第55回応用物理学関係連合講演会、27p-ZE-5、日本大学(千葉)、(2008年3月27日)

70. 細川圭吾(阪大)、野口由比多(阪大)、林周作(阪大)、井上恭(阪大)、「連続クリック攻撃に対するおとりパルス付差動位相シフト量子鍵配送」、2008 年春季 第 55 回応用物理学関係連合講演会、27p-ZE-6、日本大学(千葉)、(2008年3月27日)

71. 本庄利守(NTT)、S. W. Nam(NIST)、武居弘樹(NTT)、Q. Zhang(スタンフォード大)、鎌田英彦(NTT)、西田好毅(NTT)、忠永修(NTT)、遊部雅生(NTT)、B. Baek(NIST)、R. Hadfield(NIST)、三木茂人(NICT)、藤原幹生(NICT)、佐々木雅英(NICT)、Z. Wang(NICT)、井上恭(阪大)、山本喜久(スタンフォード大)、「超電導単一光子検出器を用いた BBM92 量子鍵配送実験」、2008 年春季 第 55 回応用物理学会学関係連合講演会、27p-ZE-7、日本大学(千葉)、(2008年3月27日)

72. 橋本卓郎(芝浦工大)、武居弘樹(NTT)、堀口常雄(芝浦工大)、「高非線形ファイバを用いた量子もつれ光子対の発生」、2008 年春季 第 55 回応用物理学関係連合講演会、27p-ZE-13、日本大学(千葉)、(2008年3月27日)

73. Lim Han Chuen(東大)、吉澤明男(産総研)、土田英実(産総研)、菊池和朗(東大)、「高品質通信波長帯偏光もつれ光子対の発生および配送」、2008 年春季 第 55 回応用物理関係連合講演会、27p-ZE-14、日本大学(千葉)、(2008年3月27日)

74. 武居弘樹(NTT)、福田浩(NTT)、土澤泰(NTT)、渡辺俊文(NTT)、山田浩治(NTT)、都倉康弘(NTT)、板橋聖一(NTT)、「シリコン細線導波路を用いた量子もつれ発生」、2008 年春季 第55回応用物理学会学関係連合講演会、27p-ZE-15、日本大学(千葉)、(2008年3月27日)

75. Chi-Hang Fred Fung(香港大)、玉木 潔(NTT)、Bing Qi(トロント大)、Hoi-Kwong Lo(トロント大)、Xiongfeng Ma(トロント大)、「検出器の効率の差異を取り入れた BB84 の無条件安全性証明」、第 18 回量子情報技術研究会(QIT18)、東京大学(東京)、 (2008年5月22日)

76. Lim Han Chuen(東大)、吉澤明男(産総研)、土田英実(産総研)、菊池和朗(東大)、「Generation and distribution of high quality telecom-band polarization-entangled photon-pairs」、第 18 回量子情報技術研究会(QIT18)、東京大学(東京)、 (2008年5月22日)

77. 井上恭(阪大)、大橋徹也(阪大)、林周作(阪大)、「量子雑音を利用した DPSK 量子鍵配送」、電子情報通信学会 光通信システム研究会(OCS) 、千歳科学技術大学(北海道)、(2008年6月13日)

78. 岩井祐樹(阪大)、井上恭(阪大)、「差動4値位相シフト量子鍵配送方式」、2008 年秋季 第69回応用物理学会学術講演会、5a-ZD-1、中部大学(愛知)、(2008年9月5日)

79. 久木田達哉(阪大)、大橋徹也(阪大)、本庄利守(NTT)、井上恭(阪大)、「差動位相シフト量子秘密共有における最終鍵生成」、2008 年秋季 第 69 回応用物理学会学術講演会、5a-ZD-2、中部大学(愛知)、(2008年9月5日)

80. 大橋徹也(阪大)、林周作(阪大)、井上恭(阪大)、「量子雑音を利用したDPS量子鍵配送におけるIntercept-Resend Attackの影響」、2008年秋季 第69回応用物理学会学術講演会、5a-ZD-4、中部大学(愛知)、(2008年9月5日)

81. 原田健一(NTT)、武居弘樹(NTT)、福田浩(NTT)、土澤泰(NTT)、渡辺俊文(NTT)、山田浩治(NTT)、都倉康弘(NTT)、板橋聖一(NTT)、「シリコン細線導波路を用いた光子対発生の量子相関度向上」、2008年秋季 第69回応用物理学会学術講演会、5a-ZD-7、中部大学(愛知)、(2008年9月5日)

82. Lim Han Chuen(東大)、吉澤明男(産総研)、土田英実(産総研)、菊池和朗(東大)、「波長分割多重もつれ配送のための広帯域偏光もつれ光子対源」、2008年秋季 第69回応用物理学会学術講演会、5a-ZD-9、中部大学(愛知)、(2008年9月5日)

83. 武居弘樹(NTT)、「光ファイバ光子対源を用いた通信波長帯量子もつれ交換」、2008年秋季 第69回応用物理学会学術講演会、5a-ZD-10、中部大学(愛知)、(2008年9月5日)

84. 山田浩治(NTT)、土澤泰(NTT)、渡辺俊文(NTT)、福田浩(NTT)、篠島弘幸(NTT)、西英隆(NTT)、武居弘樹(NTT)、原田健一(NTT)、都倉康弘(NTT)、板橋聖一(NTT)、「シリコン細線光導波路における光非線形現象とその応用」、電子情報通信学会2009総合大会、CI-2-3、愛媛大学(愛媛)、(2009年3月18日)

85. 清水薫(NTT)、武居弘樹(NTT)、玉木潔(NTT)、「光子ペアの非最大エンタングルド状態を利用した量子鍵配送」、日本物理学会 2009年春季 第64回年次大会、30aSK-9、立教大学(東京)、(2009年3月30日)

86. 久木田達哉(阪大)、岩井裕樹(阪大)、本庄利守(NTT)、井上恭(阪大)、「差動 4 値位相シフト量子鍵配送(DQPS-QKD)の鍵生成実験」、 2009年春季第56回応用物理学関係連合講演会、1p-ZL-2、筑波大学(茨城)、(2009年4月1日)

87. Lim Han Chuen(東大)、吉澤明男(産総研)、土田英実(産総研)、菊池和朗(東大)、「波長分割多重もつれ配送システムにおける過剰雑音」、2009年春季第56回応用物理学関係連合講演会、1p-ZL-4、筑波大学(茨城)、(2009年4月1日)

88. 原田健一(NTT)、武居弘樹(NTT)、福田浩(NTT)、土澤泰(NTT)、渡辺俊文(NTT)、山田浩治(NTT)、都倉康弘(NTT)、板橋聖一(NTT)、「シリコン細線導波路を用いた光子対発生の周波数帯域と偏光特性」、2009年春季第56回応用物理学関係連合講演会、1p-ZL-5、筑波大学(茨城)、(2009年4月1日)

89. 武居弘樹(NTT)、「量子周波数上方変換を用いた識別可能性の消去」、2009年春季第56回応用物理学関係連合講演会、1p-ZL-6、筑波大学(茨城)、(2009年4月1日)

90. 関忠聖(NTT)、柴田浩行(NTT)、武居弘樹(NTT)、都倉康弘(NTT)、井元信之(阪大)、「NbN超伝導ナノワイヤ単一光子検出器の作成」、2009年秋季応用物理学会学術講演会、8p-R-6、富山大学(富山)、(2009年9月8日)

91. 原田健一(NTT)、武居弘樹(NTT)、福田浩(NTT)、土澤泰(NTT)、渡辺俊文(NTT)、山田浩治(NTT)、都倉康弘(NTT)、板橋聖一(NTT)、「独立した 2 つのシリコン細線導波路を用いた識別不可能光子対発生」、2009年秋季 第70回応用物理学会学術講演会、11a-T-8、富山大学(富山)、(2009年9月11日)

92. 吉澤明男(産総研)、薛迎紅(産総研)、福田大治(産総研)、土田英実(産総研)、「導波路型相関光子対利用による光子検出器量子効率測定時の誤差要因」、 2009年秋季 第70回応用物理学会学術講演会、11p-T-2、富山大学(富山)、(2009年9月11日)

93. 河原光貴(阪大)、A. Medhipour(阪大)、井上 恭(阪大)、「量子/古典波長多重伝送系におけるラマン散乱の影響」、2009年秋季 第70回応用物理学会学術講演会、11p-T-3、富

山大学(富山)、(2009 年 9 月 11 日)

94. 武田真(阪大)、井上恭(阪大)、「連続検出率モニターによる DPS-QKD への連続クリック攻撃検知方法」、2009 年秋季 第 70 回応用物理学会学術講演会、11p-T-5、富山大学(富山)、(2009 年 9 月 11 日)

95. 細川圭吾(阪大)、井上恭(阪大)、「おとりパルス付差動位相シフト量子鍵配送の各種盗聴法に対する性能評価」、2009 年秋季 第 70 回応用物理学会学術講演会、11p-T-6、富山大学(富山)、(2009 年 9 月 11 日)

96. 武居弘樹(NTT)、原田健一(NTT)、玉木潔(NTT)、福田浩(NTT)、土澤泰(NTT)、渡辺俊文(NTT)、山田浩治(NTT)、板橋聖一(NTT)、「無条件に安全な量子もつれ QKD 実験」、2009 年秋季 第 70 回応用物理学会学術講演会、11p-T-7、富山大学(富山)、(2009 年 9 月 11 日)

97. Kai Wen(スタンフォード大)、玉木潔(NTT)、山本喜久(スタンフォード大)、「単一光子を用いた差動位相シフト量子鍵配送の無条件安全性」、日本物理学会 2009 年秋季大会、27aZE-9、熊本大学(熊本)、(2009 年 9 月 27 日)

98. 吉澤明男(産総研)、薛迎紅(産総研)、土田英実(産総研)、「1550nm 帯偏光量子相関四光子による Mandel dip 測定」、2010 年春季第 57 回応用物理学関係連合講演会、18a-L-4、東海大学(神奈川)、(2010 年 3 月 18 日)

99. 薛迎紅(産総研)、吉澤明男(産総研)、土田英実(産総研)、「二組の 1550nm 帯偏光量子相関光子対による量子交換実験」、2010 年春季第 57 回応用物理学関係連合講演会、18a-L-5、東海大学(神奈川)、(2010 年 3 月 18 日)

100. Myrtille Hunault(ESPCI ParisTech & NTT)、武居弘樹(NTT)、忠永修(NTT)、西田好毅(NTT)、遊部雅生(NTT)、「2 PPLN 導波路中のカスケード 2 次非線形光学効果を用いた時間位置もつれ光子対の発生」、2010 年春季 第 57 回応用物理学関係連合講演会、18a-L-12、東海大学(神奈川)、(2010 年 3 月 18 日)

101. 高田博史(阪大)、久木田達哉(阪大)、井上恭(阪大)、「光プリアンプ受信機を用いた巨視的差動位相シフト量子鍵配送」、2010 年春季 第 57 回応用物理学関係連合講演会、18a-L-13、東海大学(神奈川)、(2010 年 3 月 18 日)

102. 河原光貴(阪大)、欅田直也(阪大)、井上恭(阪大)、「クロストーク光及び自然放出光雑音による信号劣化を低減するフィードフォーワード制御付 DPSK 受信機」、電子情報通信学会 2010 年総合大会、B-10-59、東北大学(宮城)、(2010 年 3 月 19 日)

103. 欅田直也(阪大)、河原光貴(阪大)、「フィードフォワード制御による光強度変調信号の改善」、井上恭(阪大)、電子情報通信学会 光通信システム研究会(OCS)、ニューウェルシティ湯河原(静岡)、(2010 年 7 月 29 日)

104. 吉澤明男(産総研)、薛迎紅(産総研)、土田英実(産総研)、「1550nm 帯偏光量子もつれ交換実験とMandel-dip 測定」、2010 年秋季 第 71 回応用物理学会学術講演会、14p-E-6、長崎大学(長崎)、(2010 年 9 月 14 日)

105. 薛迎紅(産総研)、吉澤明男(産総研)、土田英実(産総研)、「1550nm 帯偏光量子もつれ交換実験とトモグラフィ評価」、2010 年秋季 第 71 回応用物理学会学術講演会、14p-E-7、長崎大学(長崎)、(2010 年 9 月 14 日)

106. 武居弘樹(NTT)、「量子周波数下方変換」、2010 年秋季 第 71 回応用物理学会学術講演会、14p-E-8、長崎大学(長崎)、(2010 年 9 月 14 日)

107. 高田博史(阪大)、久木田達哉(阪大)、井上恭(阪大)、「巨視的 4 値差動位相シフト量子鍵配送」、2010 年秋季 第 71 回応用物理学会学術講演会、14p-E-11、長崎大学(長崎)、(2010

年 9 月 14 日）

108. 鎌田英彦(NTT)、遊部雅生(NTT)、忠永修(NTT)、武居弘樹(NTT)、本庄利守(NTT)、「光子周波数変換型光子検出器の低暗計数率での動作」、2010 年秋季 第 71 回応用物理学会学術講演会、14p-E-13、長崎大学（長崎）、（2010 年 9 月 14 日）

109. 岡徹(阪大)、井上恭(阪大)、「SLD 出力光による乱数発生」、2010 年秋季 第 71 回応用物理学会学術講演会、14p-E-17、長崎大学（長崎）、（2010 年 9 月 14 日）

110. 松田信幸(NTT)、武居弘樹(NTT)、倉持栄一(NTT)、納富雅也(NTT)、「シリコンフォトニック結晶結合共振器光導波路を用いた非線形パルス圧縮」、2010 年秋季 第 71 回応用物理学会学術講演会、15p-ZW-13、長崎大学（長崎）、（2010 年 9 月 15 日）

111. 柴田浩行(NTT)、武居弘樹(NTT)、本庄利守(NTT)、赤崎達志(NTT)、都倉康弘(NTT)、「MgB2 ナノ細線による単一光子検出」、2010 年秋季 第 71 回応用物理学会学術講演会、6a-T-4、長崎大学（長崎）、（2010 年 9 月 16 日）

112. 欅田直也（阪大）、河原光貴（阪大）、井上恭（阪大）、「フィードフォワード制御による光強度変調信号の波形劣化改善」、電子情報通信学会 2010 年ソサイエティ大会、B-10-61、大阪府立大学（大阪）、（2010 年 9 月 17 日）

113. 河原光貴（阪大）、欅田直也（阪大）、井上恭（阪大）、「フィードフォワード制御による光強度変調信号の消光比改善」、電子情報通信学会 2010 年ソサイエティ大会、B-10-62、大阪府立大学（大阪）、（2010 年 9 月 17 日）

114. 金田真也(阪大)、武田真(阪大)、清水勝一郎(阪大)、井上恭(阪大)、「ゲート幅拡張 APD 単一光子検出器」、2010 年秋季 第 71 回応用物理学会学術講演会、17p-H-5、長崎大学（長崎）、（2010 年 9 月 17 日）

115. 玉木潔(NTT)、加藤豪(NTT)、「シンドロームの暗号化がない QKD の安全性証明用の量子回路及びシフト鍵への雑音印加処理」、日本物理学会 2010 年秋季大会、23pRF-12、大阪府立大学（大阪）、（2010 年 9 月 23 日）

116. 薛迎紅（産総研）、吉澤明男（産総研）、土田英実（産総研）、「1550nm 帯偏光量子もつれ交換実験と偶発的計数評価」、2011 年春季第 58 回応用物理学関係連合講演会、神奈川工科大学（神奈川）、（投稿中）

117. 吉澤明男（産総研）、薛迎紅（産総研）、土田英実（産総研）、「偏光量子もつれ交換と偶発的四光子同時計数推定」、2011 年春季第 58 回応用物理学関係連合講演会、神奈川工科大学（神奈川）、（投稿中）

③ポスター発表 （国内会議 10 件、国際会議 17 件）

1. S. Odate (AIST), A. Yoshizawa (AIST), H. Tsuchida (AIST), “Tomographic evaluation of polarization-entangled photon pairs in the telecom wavelength band using a fiber interferometer,” QCMC2006, Ibaraki, Japan, (30 Nov. 2006).
2. K. Tamaki (NTT), N. Lutkenhaus (U. Waterloo), M. Koashi (Osaka U.), J. Batuwantudawe (U. Waterloo), “Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse,” QCMC2006, P2-5, Ibarki, Japan, (2 Dec. 2006).
3. A. Yoshizawa (AIST), S. Odate (AIST), H. Tsuchida (AIST), “Low-noise gated-mode single-photon detection at 1550 nm using a cooled InGaAs avalanche photodiode,” QCMC2006, P2-32, Ibaraki, Japan, (2 Dec. 2006).
4. H. Takesue (NTT), “1.5-μm band Hong-Ou-Mandel experiment using photon pairs

generated in two independent optical fibers," CLEO/QELS 2007, JTuA5, Baltimore, USA (8 May 2007)

5. S. Odate (AIST), A. Yoshizawa (AIST), H. Tsuchida (AIST), "Polarization-entangled photon source based on the fiber loop configuration in the telecom wavelength band," CLEO/Pacific Rim2007, Soul, Korea (29 Aug. 2007).

6. H. Lim (U. of Tokyo), A. Yoshizawa (AIST), H. Tsuchida (AIST), K. Kikuchi (U. of Tokyo), "Distribution of polarization-entangled photon-pairs produced via spontaneous parametric down-conversion over 82km and 132km of optical fiber," AQIS2008, Soul, Korea (28 Aug. 2008).

7. H. Lim (U. of Tokyo), A. Yoshizawa (AIST), H. Tsuchida (AIST), K. Kikuchi (U. of Tokyo), "Excess noise in bandwidth-resource-efficient entanglement distribution," CLEO/Europe-EQEC 2009, Munich, Germany (17 Jun. 2009).

8. Y. Xue (AIST), A. Yoshizawa (AIST), H. Tsuchida (AIST), "Four-fold coincidence measurement for demonstrating polarization-based quantum swapping at 1550 nm," Int'l Conf. on Quantum Information and Technol., Tokyo, Japan (3 Dec. 2009).

9. A. Yoshizawa (AIST), Y. Xue (AIST), H. Tsuchida (AIST), "Long-term Mandel-dip measurement for demonstrating polarization-based quantum swapping at 1550 nm," 2010 Int'l Symposium on Phys. of Quantum Technol. (ISPQT 2010), 8TH-05, Tokyo, Japan (8 Apr. 2010).

10. Y. Xue (AIST), A. Yoshizawa (AIST),H. Tsuchida (AIST), "Quantum swapping at 1550 nm using two polarization-entangled photon pairs created in two periodically poled lithium niobate waveguides," 2010 Int'l Symposium on Phys. of Quantum Technol. (ISPQT 2010), 8TH-06, Tokyo, Japan, (8 Apr. 2010).

11. H. Takesue (NTT), "Erasing frequency distinguishability using quantum frequency up-conversion" 2010 Int'l Symposium on Phys. of Quantum Technol. (ISPQT 2010), 8TH-8, Tokyo, Japan, (8 Apr. 2010).

12. J. F. Dynes (Toshiba), H. Takesue (NTT), Z. L. Yuan (Toshiba), A. W. Sharpe (Toshiba), K. Harada (NTT), T. Honjo (NTT), H. Kamada (NTT), O. Tadanaga (NTT), Y. Nishida (NTT), M. Asobe (NTT), A. J. Shields (Toshiba), "Entanglement distribution over 200 km," 2010 Int'l Symposium on Phys. of Quantum Technol. (ISPQT 2010), 8TH-54, Tokyo, Japan, (8 Apr. 2010).

13. H. Kawahara (Osaka U.), N. Kunigita (Osaka U.), K. Inoue (Osaka U.), "DPSK receiver with feedforward control to mitigate in-band crosstalk and ASE noise", CLEO/QELS 2010, JThE62, CA., USA, (20 May 2010).

14. A. Yoshizawa (AIST), Y. Xue (AIST), H. Tsuchida (AIST), "4-photon Mandel-dip measurement with a 77.6% visibility using two periodically poled lithium niobate waveguides operating at 1550 nm," QCMC2010, Brisbane, Australia, (20 Jul. 2010).

15. Y. Xue (AIST), A. Yoshizawa (AIST), H. Tsuchida (AIST), "Telecom-band entanglement swapping with polarization-entangled photon pairs generated in separated PPLN waveguides," QCMC2010, Brisbane, Australia, (22 Jul. 2010).

16. A. Yoshizawa (AIST), Y. Xue (AIST), H. Tsuchida (AIST), "Polarization-based entanglement swapping experiment at 1550 nm for fiber-optic quantum network system," AQIS2010, Tokyo, Japan, (28 Aug. 2010).

17. Y. Xue (AIST), A. Yoshizawa (AIST), Tsuchida (AIST), “Evaluation of polarization entanglement created by telecomband entanglement swapping,” UQCC2010, Tokyo, Japan, (19 Oct. 2010).

18. 武居弘樹(NTT)、井上恭(阪大)、「分散シフトファイバ中の自然放出四光波混合を用いた1.5μm帯量子相関光子対の発生:ファイバ冷却による雑音光子の抑圧」、第13回量子情報技術研究会(QIT13)、東北大学(宮城)、(25 Nov. 2005).

19. 吉澤明男(産総研)、土田英実(産総研)、「ゲート動作光子検出時の入射光子タイミング調整」、第14回量子情報技術研究会(QIT14)、東工大(東京)、(29 May 2006).

20. 大舘暁(産総研), 吉澤明男(産総研)、福田大治(産総研)、土田英実(産総研)、「相関光子対の双方向同時計数による単一光子検出器量子効率測定」、第16回量子情報技術研究会(QIT16)、NTT厚木研究開発センタ講堂(神奈川)、(18 May 2007).

21. 橋本卓郎(芝浦工大)、武居弘樹(NTT)、堀口常雄(芝浦工大)、「周波数上方変換型単一光子検出器を用いた時間位置もつれ光子対の観測」, 第 17 回量子情報技術研究会(QIT17)、山陽新聞本社さん太ホール(岡山)、(21 Nov. 2007).

22. 武居弘樹(NTT)、福田浩(NTT)、土澤泰(NTT)、渡辺俊文(NTT)、山田浩治(NTT)、都倉康弘(NTT)、板橋聖一(NTT)、「シリコン細線導波路を用いた量子もつれ発生」、第18回量子情報技術研究会、東京大学(東京)、(22 May 2008).

23. Lim Han Chuen(東大)、吉澤明男(産総研)、土田英実(産総研)、菊池和朗(東大)、「Wavelength-multiplexed entanglement distribution technology」、第19回量子情報技術研究会、大阪府立大学(大阪)、(20 Nov. 2008).

24. 薛迎紅(産総研)、吉澤明男(産総研)、土田英実(産総研)、「二組の1550 nm帯偏光量子もつれ光子対を用いたHong-Ou-Mandel干渉実験」、第21回量子情報技術研究会 QIT21、調布市、電気通信大学(東京)、(4 Nov. 2009).

25. 薛迎紅(産総研)、吉澤明男(産総研)、土田英実(産総研)、「二個のPPLN導波路による二組の光通信波長帯光子対発生と量子干渉実験」、日本光学会年次学術講演会 Optics & Photonics Japan 2009、24pP21、新潟コンベンションセンター(新潟)、(24 Nov. 2009).

26. 薛迎紅(産総研)、吉澤明男(産総研)、土田英実(産総研)、「光通信波長帯偏光量子もつれ光子対を用いた量子交換実験」、第 22 回量子情報技術研究会、大阪大学(大阪)、(14 Sept. 2010).

27. 吉澤明男(産総研)、薛迎紅(産総研)、土田英実(産総研)、「光通信波長帯四光子Mandel-dip測定における偶発計数評価」、第22回量子情報技術研究会、大阪大学(大阪)、(14 Sept. 2010).

(4)知財出願

① 国内出願 (28件)

1. “量子秘密共有システム及び量子秘密鍵生成方法”、本庄利守・井上恭、日本電信電話株式会社、2005.11.4、特願2005－321052
2. “量子暗号鍵配送装置及び鍵情報盗聴検出方法”、武居弘樹・井上恭、日本電信電話株式会社、2006.2.17、特願2006-041306
3. “量子鍵配送システムおよび盗聴検知方法”、武居弘樹・井上恭、日本電信電話株式会社、2006.4.18、特願2006-114804
4. “量子暗号通信装置及び量子暗号通信方法”、本庄利守・井上恭、日本電信電話株

式会社、2006.5.13、特願 2006-152720

5. “秘密鍵配送装置及び秘密鍵配送装置”、本庄利守・井上恭、日本電信電話株式会社、2006.9.6、特願 2006-241751

6. “量子通信システム”、武居弘樹・井上恭、日本電信電話株式会社、2006.9.26、特願 2006-261086

7. “量子効率測定方法および装置”、吉澤明男・福田大治・大舘暁、独立行政法人産業技術総合研究所、2007.4.20、特願 2007-112232

8. “量子暗号通信システムおよび方法”、本庄利守・井上恭、日本電信電話株式会社、2007.5.28、特願 2007-140669

9. “量子暗号通信システムおよび盗聴検知方法”、本庄利守・井上恭、日本電信電話株式会社、2007.5.29、特願 2007-140576

10. “量子暗号通信装置”、玉木潔・井上恭、日本電信電話株式会社、2007.6.7、特願 2007-151886

11. “量子暗号システム”、本庄利守・井上恭、日本電信電話株式会社、2007.8.27、特願 2007-220094

12. “量子鍵配送システム”、本庄利守・井上恭、日本電信電話株式会社、2007.8.27、特願 2007-220095

13. “量子もつれ光子対発生装置”、武居弘樹・都倉康弘・福田浩・山田浩治・板橋聖一、日本電信電話株式会社、2007.9.13、特願 2007-238313

14. “量子暗号装置”、本庄利守・井上恭、日本電信電話株式会社、2007.12.11、特願 2007-320029

15. “エンタングル光子対発生装置およびエンタングル光子対発生方法”、本庄利守・井上恭、日本電信電話株式会社、2007.12.27、特願 2007-337892

16. “量子暗号鍵配送システム”、本庄利守・井上恭、日本電信電話株式会社、2008.3.14、特願 2008- 066379

17. “量子干渉装置および量子通信システム”、武居弘樹、日本電信電話株式会社、2008.10.6、特願 2008-260012

18. “量子暗号通信データ処理方法及び量子暗号通信装置”、玉木潔・鶴丸豊広、日本電信電話株式会社・三菱電機株式会社、2009.4.14、特願 2009-98133

19. “量子暗号装置および量子暗号通信方法”、武居　弘樹・井上　恭、日本電信電話株式会社、2009.6.5、特願 2009-136674

20. “量子相関光子対発生装置および量子もつれ光子対発生装置”、武居弘樹、日本電信電話株式会社、2009.6.30、特願 2009-155838

21. “乱数を発生させる装置および方法”、井上恭、日本電信電話株式会社、2009.8.3、特願 2009-180711

22. “光受信器及び光ファイバ伝送システム”、福徳光師・井上恭、日本電信電話株式会社、2009.11.30、特願 2009-272549

23. “光受信器”、福徳光師・井上恭、2010/2/10、特願 2010-028071

24. “光雑音低減回路及び光雑音低減方法”、福徳光師・井上恭、日本電信電話株式会社、2010.3.1、特願 2010-04461

25. “光位相雑音抑圧回路及び位相揺らぎ検出回路及び位相揺らぎ検出方法”、福徳光師・井上恭、日本電信電話株式会社、2010.3.1、特願 2010-04462

26. “光子検出器”、本庄利守・井上恭、日本電信電話株式会社、2010.4.20 特願 2010-097053

27. “量子通信システム及び量子鍵配送システム”、武居弘樹、日本電信電話株式会社、2010.6.18、特願 2010-139591

28. “量子通信システム”、武居弘樹、日本電信電話株式会社、2010.6.18、特願 2010-139592

② 海外出願 (0 件)

③ その他の知的財産権

(5)受賞・報道等

① 受賞

・ H. Takesue, T. Honjo, K. Tamaki, Y. Tokura, ITU-T Kaleidoscope Academic Conference: Innovations in NGN - Future Network and Services, Best Paper Award, second place for presentation “Differential phase shift quantum key distribution,” (May 2008).

・ 武居弘樹、平成22年度科学技術分野の文部科学大臣表彰・若手科学者賞受賞、(業績名: 光通信波長帯における高速・長距離量子暗号通信の研究)、(Apr. 2010).

②マスコミ(新聞・TV等)報道

・「NTT、倍の 200km 伝送」、日本経済新聞、(2007 年 6 月 2 日朝刊)
・「量子暗号、実用化へ道」、朝日新聞、(2007 年 6 月 4 日朝刊)
・「世界最速 10 ギガヘルツの量子暗号 光ファイバーで 200km 配送」、日刊工業新聞、(2007 年 6 月 4 日朝刊)
・「量子暗号通信 伝送距離 200 キロ達成」、日経産業新聞、(2007 年 6 月 4 日朝刊)
・「量子暗号鍵 200 キロメートルの伝送に成功」、電気新聞、(2007 年 6 月 4 日朝刊)
・「長距離量子暗号システムへ前進」、電波新聞、(2007 年 6 月 4 日朝刊)
・「量子暗号鍵の伝送記録更新」、科学新聞、(2007 年 6 月 8 日)
・「正弦波ゲート方式 InGaAs/InP APD を用いた QKD 実験」、日経 NETWORK、「量子暗号技術」2007 年 8 月号 18 頁。
・「量子暗号通信 数十 km で実用化にめど」、日刊工業新聞(2007 年 8 月 17 日)

(6)成果展開事例

① 実用化に向けての展開

特になし

② 社会還元的な展開活動

・ 本研究成果をインターネットで公開し、一般に情報提供している。
阪大グループ URL: http://www1b.comm.eng.osaka-u.ac.jp/com02adm/project-inoue.htm
NTT グループ URL: http://www.brl.ntt.co.jp/people/htakesue/indexj.html
産総研グループ URL: http://staff.aist.go.jp/yoshizawa-akio/

§６ 研究期間中の主なワークショップ、シンポジウム、アウトリーチ等の活動

特になし

§７ 結び

研究内容としては概ね順調に遂行できたと考えている。特に NTT グループは、DPS-QKD 実験及び通信波長帯量子もつれ光子の発生/ファイバー伝送/もつれ QKD 実験/もつれ交換実験など、常に第一線の成果を出し続けた。これにより、本プロジェクト開始前は何とか（通信波長帯）量子もつれ光子が発生できるという程度であった技術レベルが、システム実験を行うまで達した。量子情報通信の発展に大きく貢献したと思っている。ただ欲を言えば、量子もつれ光子を使って第一世代であるポイント-to-ポイント（P2P）QKD システムを超える性能を達成できなかったことは残念である。量子もつれシステムは同時検出事象を利用するため効率が悪いこと、光パラメトリック過程によるもつれ発生方法では発生光子対数がポワソン分布に従うためマルチ光子対発生が避けられないこと、などが障害となっている。これらのため、単なる秘密鍵配送システムとしては P2P-QKD で十分、というのが実情である。量子もつれは物理としては興味深いが、システム応用にはまだまだ力不足というところであろうか。言い方を変えれば、量子もつれ通信システムはどこまでできるか、課題は何か、を明らかしたのが本プロジェクトの意義と言えるかもしれない。P2P－QKD を凌駕するシステム性能を実現するには、量子メモリ及びそれを用いた量子中継技術やポワソン分布ではない量子もつれ光子発生法（例えば半導体量子ドットの準位間遷移を利用する方法）の開発が望まれる。また、鍵配送以外の量子もつれならではのアプリケーションを模索していくことも必要であろう。

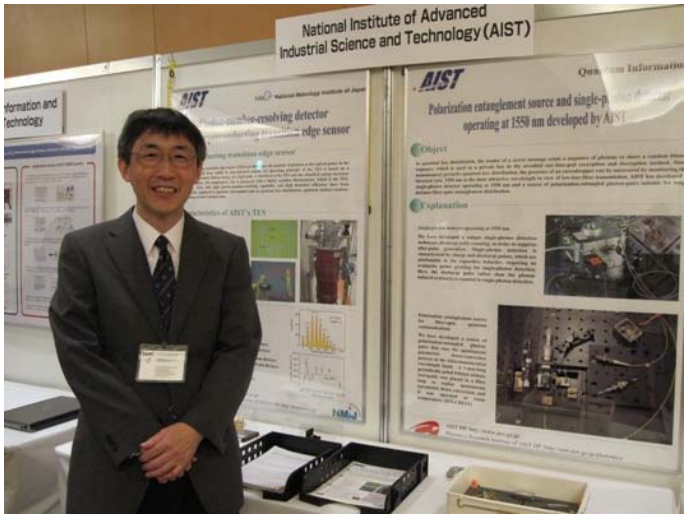
一方で、P2P－QKD に関してはやろうと思えば実用化可能な技術レベルに達しつつある。これには本プロジェクトの貢献も大きい。特に、NTT グループによる長距離 QKD 実験は大きなインパクトを与えた。また、阪大グループは足固め的な研究を行った。今後の課題は、実用にもっていくための戦略であろう。単なる技術論でなく、既存通信ネットワークとの親和性、ニーズの見極め、サービス展開の仕方、などが必要となる。

プロジェクト運営については、実際のところ、何をどうやるかは各グループにおまかせ状態であった。研究費の使い方も同様である。やはり別組織であるので、他グループのことに口は出しにくい。ただ、阪大グループとNTTグループとの間での議論/情報交換は、研究代表者が毎月2回NTTに出向いていたという状況もあり、密に行った。そのようなレベルでの連携は十分できたと思っている。産総研グループとは、学会・研究会等で議論/情報交換を行った。

自身のグループに関しては、大学で研究することの難しさを感じながらの5年間であった。特に代表研究者は企業の研究所から移った直後であり、全くゼロからのスタートであったためその感が強い。研究室のメンバーは修論生と卒論生のみで、ほとんど何も知らない学生を教育しながらの研究活動であった。ただそういった中でも、本プロジェクトのおかげで研究費に恵まれたことは幸いであった。ひと通りの実験装置を揃えることができ、事務補助員の雇用や各種出張など諸経費に不自由せずにすんだ。学生にとっても、充足した実験設備の元で第一線の研究活動に触れたことは貴重な経験となったはずである。残念ながら本研究室の学生は修士課程止まりであるが、研究とはどういうものか、そしてその面白さの一端を伝えることができたのではないかと思っている。

国立情報学研究所の山本教授を総括とするこの JST/CREST に参画できたことに感謝する次第である。

大阪大学 井上研究室



産総研　吉澤