3　量子情報通信
3 Quantum Info-Communications

3-1　量子情報通信の概要とNICTにおける取組
3-1 Overview of Quantum Info-Communications and Research Activities in NICT

佐々木雅英
SASAKI Masahide

要旨

現在の光通信は光の強度のみを制御しているが、波としての性質を生かすと更に多機能で大容量の伝送を実現できる。しかし、その性能もいずれはショット雑音限界で頭打ちとなる。これに対して量子情報通信では、光子の量子状態を直接制御することで、物理原理に基づく情報安全性の確保やショット雑音限界を超えた大容量通信が可能となる。量子情報通信の全体像と戦略課題について概観し、情報通信研究機構（NICT）における取組について報告する。

Present optical communication relies on the intensity control of light. By exploiting the wave nature of light, transmission with higher capacity and multi-functions must be possible. Its performance, however, will be bounded at the shot noise limit in the near future. In quantum info-communications, where one directly controls quantum states of photons, information security based on physical principle and ultra-high capacity beyond the shot noise limit could be realized. In this article, we present an overview of quantum info-communications, and review the research activities in NICT.

[キーワード]
量子通信，量子暗号，スクィーズド光，量子状態，光子数識別器
Quantum communications, Quantum cryptography, Squeezed light, Quantum state, Photon-number resolving detector

1　まえがき

現在の光通信は、レーザー光の強度変調とその直接検波で成り立っており、光の波としての性質すら使っていない。波としてのポテンシャルを生かすコヒーレント光通信では、ホモダイン検波を使うことで従来方式に比べ、最大 20 dB 程度の受信感度の改善が可能といわれる。実際、ホモダイン検波の検出性能は、既に光自身が持つ量子的な揺らぎ、いわゆるショット雑音限界まで達している。パワー当たりの伝送情報量をどんどん増やしていくと、最終的にはこの量子揺らぎが通信性能を規定するようになる。

この量子的な揺らぎは、不確定性原理に起因するもので完全に消し去ることは不可能である。しかし、ある位相の領域で揺らぎを抑圧することは可能である。そのかわり、別の位相の揺らぎは逆に大きくなってしまう。

このように量子的揺らぎを人為的に制御した状態がスクィーズド状態である[1]。スクィーズド光を使って揺らぎが抑圧された位相のポイントにロックして、情報処理を行えば、ショット雑音に制

限されない高度な情報処理が可能になる。

1980 年代半ばにはスクィーズド光の生成が可能になり、1990 年代にかけて量子光学が大いに進展した[2]－[4]。また、1980 年代半ばには量子鍵配送の提案[5][6]と量子計算機の定式化[7]がなされた。1994 年には、量子計算機が素因数分解など膨大な計算量を要する問題を簡単に解くことができ、したがって、実現すれば現代暗号も簡単に破られてしまうことが理論的に示された[8]。これを契機として、量子情報技術の意義が広く認識され、これまでの研究が合流して爆発的に進展することとなった。

その中でも光を基礎とした量子情報通信は、0 でもありながら同時に 1 でもあるような情報、巨視的スケールに広がった量子状態が引き起こす直感を超えた相関現象など、量子力学の最もパラドキシカルな側面を情報通信と融合させるという大きな革新を迫るものである。

2 量子力学の原理と量子情報通信の概要

量子力学には二つの基本原理がある。一つは重ね合わせの原理で、これを情報技術の世界に持ち込むと、0 でもあり同時に 1 でもある状態、いわゆる量子ビット（Qubit，キュービット）という概念を構成することができる。これを拡張すると、複数の可能性を同時並行で処理できる超並列性処理が可能になる。これが量子計算で、現代のセキュリティを揺るがす大きな脅威となっている。

しかし、幸運にももう一つの原理、不確定性原理がこの危機を救ってくれる。これは二つの正準共役な物理量（例えば、粒子の位置と運動量）に関する状態を、外乱を与えずに同時に正確に測定することは不可能という原理である。この原理を拡張することで、盗聴の完全な検知が可能になり、量子計算でも破ることができない無条件安全な量子暗号という技術が可能になる。

一方、測定に原理的限界があるとする不確定性原理は、大容量化に最終的な伝送限界を課すことになる。そして、その量子限界まで通信性能を高めるためには、実は量子計算に基づく新しい符号化技術、量子符号化が必須の手段になるということが分ってきた。量子情報通信の研究は、重ね合わせの原理と不確定性原理を基礎にして、大容量化を目指す研究とセキュリティの確立を目指す研究の二つの大きな柱からなる（図 1 を参照）。量子暗号については実用化が視野に入ってきたが、量子計算や量子符号化はまだ長期的課題である。

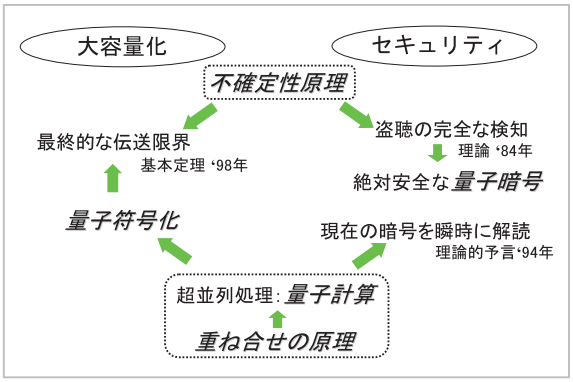

図 1 量子力学の原理と量子情報通信の概要

3 量子情報通信研究開発プロジェクト

これらの課題を総合的かつ戦略的に進めるため、総務省の下で産学官連携による量子情報通信研究開発プロジェクトが 2001 年から開始されている。その推進体制を図 2 に示す。実用化が視野に入ってきた量子暗号については、NICT 委託研究によりテストベッド構築を進めてきた。また、実用化に向けて早急に装置化が必要な基盤技術についても NICT 委託研究により推進している。

一方、理論の実証や実験でのブレークスルーが必要でリスクが高い量子計算や量子符号化の研究については、NICT 総合研究系における自主研究として推進している。また、新原理の開拓や萌芽的基礎研究については、総務省の戦略的情報通信研究開発推進制度の公募研究で大学などが中心となって推進している。

推進に当たっては全参加チームの主要メンバーが年一、二度一堂に会して、研究成果報告、最新動向の紹介・分析、今後の研究戦略の検討など行う研究代表者会議が核となり、NICT と他の産学官の機関及び総務省政策担当者の密接な連携の下で、国家的・戦略的な運営がなされてきた。

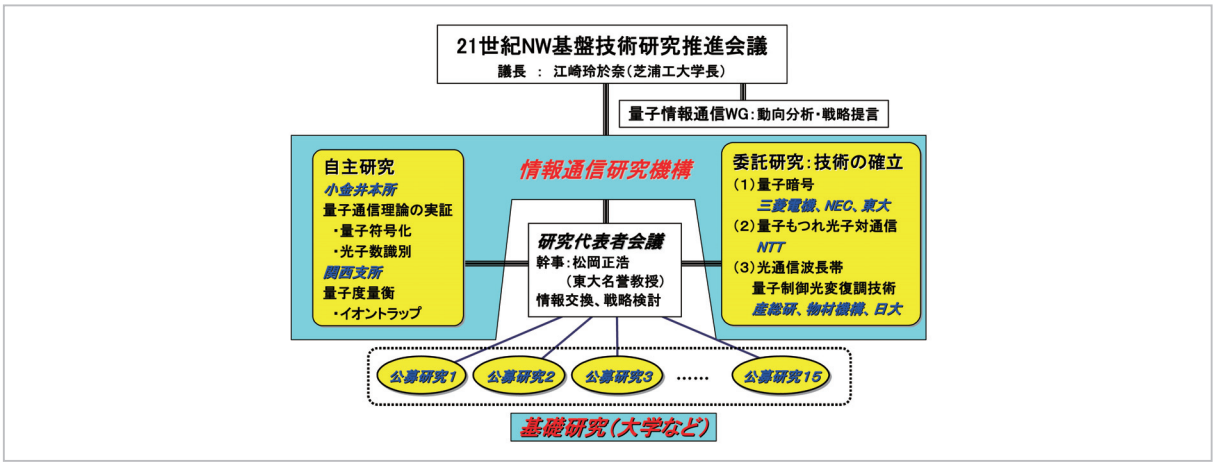

図2 量子情報通信研究開発プロジェクトの推進体制

4 研究開発の現状

重ね合わせの原理と不確定性原理という二つの基本原理のうち、技術応用が比較的容易なのは後者である。しかも 1 キュービットレベルの量子効果の制御で実現できるのが BB84 プロトコルに代表される量子暗号であり、実用化が近い理由となっている。

(1) 量子暗号

現在のインターネットでは、公開鍵暗号と呼ばれる方式が主流となっているが、現在、無条件安全性が証明されている量子暗号は、より原始的な秘密鍵暗号に基づいている。秘密鍵とは送受信者間のみで共有されたランダムなビット列のことである。これでメッセージを暗号化し、秘密鍵の使用は一度きり（One time pad）とすれば盗聴は完全に不可能となる。この秘密鍵を安全に共有する方法が量子鍵配送である。技術的には、受信者に届いた単一光子事象の中から安全な鍵を抽出して使う。安全性確保のためには高品質の単一光子源が望まれるが、当面はレーザー光を減衰させた、ポアッソン光源でもよい。システム性能はむしろ光子検出器の性能に大きく依存する。幸い、市販の雪崩増幅型光子検出器で対応が可能で、フィールド試験や製品化が始まっている。NICT 委託研究の成果として、世界最長となる既設ファイバ 96km でのフィールド試験に成功したほか、商用ファイバを用いた実環境下で 14 日間連続での最終鍵生成に成功した（**3-2** 長谷川ほか）。

(2) 量子もつれ状態

技術応用が始まった不確定性原理に対して、重ね合わせの原理の応用はまだ基礎研究の段階である。重ね合わせ状態は日常の世界ではすぐに壊れてしまうためにその制御は容易ではない。特に、巨視的スケールにわたって広がった複数本の光ビームで形成される重ね合わせ状態は、一方のビームへの測定結果によって他のビームの量子状態が影響を受ける特殊な相関を有しており、「量子もつれ（あるいは量子エンタングルメント）状態」と呼ばれる。これを自在に生成し、制御することが量子情報通信の重要課題の一つである。特に、光ファイバ帯での量子もつれ光子対発生技術は、現在の通信インフラ上に、量子鍵配送、量子テレポーテーション、量子秘密共有等の高度な量子通信を実現するための重要な要素技術である。NICT 委託研究の成果として、光ファイバ中の四光波混合を用いた量子もつれ光子対生成技術を開発して、明瞭度 99.3%の良好な二光子干渉波形を取得し、20 km 隔てられた状態でも、量子相関の証拠となる Bell 不等式の破れ $S=2.65\pm0.09>2$ を得ることに成功した（**3-3** 武居）。

(3) 量子テレポーテーション

この量子もつれ状態を使った魔法ともいえるような新しい情報伝達法が量子テレポーテーションである。量子計算機のメモリには、複雑な重ね合わせ状態が格納される。量子メモリを結ぶネットワーク上では、複雑な重ね合わせ状態がやり取りされる。送りたい量子状態の素性が分かれば、それを従来のビット情報に符号化して送れるが、重ね合わせ状態は実は観測すると

壊れてしまうので、この方法は使えない。重ね合わせ状態の伝送手段となるのが量子テレポーテーションである[9][10]。

さらに、量子テレポーテーションそのものを使って量子計算を実現できることも分かってきた。大容量化を目指す量子符号化では、光に対する量子計算が必要になるが、量子テレポーテーションは、まさにそのための構成要素になるのである。

(4) 量子計算

多項式時間による素因数分解など古典的対応を持たない機能の実現には、数 100 量子ビット以上の大規模な量子計算が必要であるが、従来の通信や計測技術と組み合わせて総合的な性能改善に使う場合には、小規模の量子計算でも十分意義がある。その場合、光を使う量子計算を考えることになるが、一般に光子と光子の相互作用は非常に弱く、基本ゲートの実現が容易ではない。しかし、単一光子状態やスクィーズド状態などの非古典光と光子数識別器があれば、小規模な光量子計算を現有技術の延長線上に実現できることが分かってきた。

補助的な非古典光を用意して信号光と干渉させ量子もつれ状態を形成し、その一部だけ光子数測定を行う。もう一方の光は測定結果に応じて状態変化を受ける。所望の非線形変化に対応する測定結果のときのみ、信号処理を進めることで実効的に信号光子に対する量子ゲートを実現できる。この操作は確率的にしか作れないが、各ゲート操作を事前に別の場所(オフライン)で成功するまで繰り返しておき、成功したらゲート操作を量子テレポーテーションによって信号のあるオンラインに乗せることで量子計算の成功確率を原理的に 1 にできる[11]-[13]。

(5) 量子符号化

大容量化の鍵は受信技術にある。最新の量子情報理論の成果によれば、与えられたパワーと帯域制限の下で線形損失通信路を通して最適に通信を行う方法とは次のようなものである[14]。究極の通信路容量を実現する送信側での最適解は、通常のレーザー光の振幅をガウス分布に従う連続変数で変調し、そのパルス列でメッセージを符号化するというものである。パルス間で量子もつれ状態を形成して送っても、通信路容量を上げる上では何の効果もない。その代わり、受信側では入ってきたコヒーレント光のパルス列に量子力学が許す最高の復号操作を行う。量子制御は受信側でこそ求められる。

最高の復号操作とは、光の量子計算を組み込んだ復号操作でこれが量子符号化の本質である。つまり、パルスごとに個別に測定して光電変換を行う代わりに、受信したパルス列のブロック全体にいったん何らかの量子計算を施して適切な重ね合わせ状態生成してからパルスごとの測定を行うことで、正味取り出せる情報量を増やすことができる。このような測定法のことを量子一括測定と呼ぶ。その効果を象徴的に示したのが図 3 である。量子雑音を伴う信号(非直交量子状態)で伝送を行う場合、量子一括測定を行うことで通信資源を 2 倍に増やしたときに 2 倍以上の情報量を取り出すことが可能となる。これを超加法的量子符号化利得と呼ぶ。その原理は最近実証されたが[15]、擬似的単一光子状態の偏光と経路の自由度を使ったモデルを用いており、まだ実用には程遠い。実用的な光信号への適用はこれからの課題である。

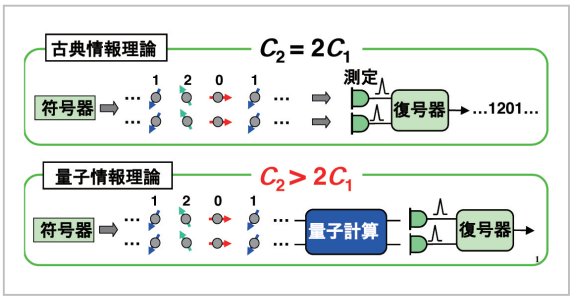

図3 二つのパルスに対する量子一括測定(下)と従来の復号方式(上)との比較

量子一括測定を従来の復号回路に組み込めば、復号計算量を大幅に削減でき、実効的な通信性能を改善できる[16]。超長距離通信では、非常に長い符号化を行って通信の精度を確保するが、復号に要する手間や装置コストも同時に増えていく。量子一括測定を組み込んだ量子-古典ハイブリッド符号化では、この復号コストを低減でき、量子一括測定の規模が増えるごとに通信性能は一歩一歩着実に向上していく。そして、量子一括測定を十分大きな規模で行えるようになったとき、究極の通信路容量を達成することが可能になるのである。現在の光通信から量子通信へと発展する最も自然なルートである。

5　今後の戦略課題

(1) 量子暗号

量子暗号の研究開発はいよいよ実用化に向けて最終段階を迎える。今後、2010 年までの戦略目標として NICT 委託研究では、50 km 圏内のメトロ系 IP ネットワークで実用可能な量子鍵配送システムの開発と 100 km 超の中長距離における世界トップクラスの性能のテストベッド実現を挙げている。

メトロ対応量子鍵配送システムでは、実用的な安全性を重視した上で、鍵生成速度は最低限、電話・ファックス対応可能な 1 Mbps 以上を目標としている。さらにシステム機能として、波長多重やスイッチング機能の併用により、8 程度のノード間での自在な接続切替え、最適迂回経路の設定技術の確立が目標となる。また、光集積回路による装置の小型化・携帯化も合わせて進める予定である。

中長距離対応量子鍵配送テストベッドでは、鍵生成速度は 10 kbps 以上を実現し、鍵生成レート対伝送距離のトレードオフ曲線における世界トップクラスの性能を実証することが目標となる。

(2) 光子検出器

上記の目標を実現するための鍵を握るのは単一光子検出技術の高性能化である。APD のアフターパルス現象は鍵生成速度を制限し、暗計数は安全性を劣化させ鍵配送距離を限定してしまう。これらを抑えて実効的な光子検出速度を向上させることが、量子鍵配送の性能を向上させるための抜本策といっても過言ではない。

1 Mbps 級のメトロ対応量子鍵配送システム実現のためには実効的な光子検出レートを 10 MHz まで上げられる単一光子検出技術が必要である。技術候補としては、化合物半導体の APD、通信波長帯から近赤外帯への波長変換と Si APD の組合せ、超伝導素子の大きく三つの方式が上げられる。

通信波長帯での直接検出が可能で、集積化や量産対応が可能な化合物半導体 APD で抜本的改善が実現できればこれが最終方式となろう。しかし、良質の結晶成長の実現などまだ基礎的でチャレンジングな課題を地道に解決していく必要がある。

波長変換＋Si APD 方式では、10 MHz 弱での動作速度や最終検出効率 50 %弱といった現有技術としては優れた性能が実現できており、中長距離対応量子鍵配送テストベッドの実現に有望と期待される。ただし、波長変換素子の帯域制限から将来の波長多重への対応などで制限要因が残る可能性がある。

超伝導素子は、低雑音・高速性から性能自体に関しては最も有望な候補であるが、極低音環境を要することや広い波長感度を有することから、来る背景光遮蔽対策が実用化への制限要因になる可能性がある。これらの候補の開発を平行で進め、最終候補を絞っていくことになろう。

(3) 量子中継

量子暗号で使われる信号セットは、信号の量子状態を壊すことなく複製を作るのが不可能なように設計されている。このような信号セットは実は増幅することもできない。このため減衰が避けられない現実の光ファイバネットワーク上で直接的に暗号鍵を配送できる距離には限界があり、200 km あたりが限界だろうと考えられている。

これを超える距離で量子暗号ネットワークを形成するためには、量子中継という高度な技術が必要になる。その根底にある原理は量子状態を壊すことなく遠隔地に再生する量子テレポーテーションである。つまり、減衰に耐えられる距離の 2 地点 A，B 間で量子もつれ状態を共有し、さらに 2 地点 B，C 間でも量子もつれ状態を共有する。中継点 B で特殊な測定を行うことで、A，C 間にわたる量子もつれ状態を形成することができる。いわゆるエンタングルメントスワッピングであるが、このようにして形成された量子もつれ状態を使って光子の状態を A から遠隔地の C へ転送する。

実際には、量子もつれ状態も減衰や緩和に極めて弱いので、多くの量子もつれ状態の対を生成して共有し、劣化した多くの対の中から純度の高いものを生成する。これを制御されたタイミングで行うためには、量子状態をある時間安定に保持するための量子メモリが必要になる。

そのための基盤技術を整備するため、NICT 委託研究を核にした産学官の連携で、2010 年までに量子中継に必要となる量子メモリの物理モデルの実証及び量子中継の最も簡単なシステム実証を目標に研究開発を行う。

(4) 光の万能量子ゲート

現在の光通信は、どんなに波長多重や多値変調を行っても、いずれショット雑音限界によって毎秒 10^{18} (エクサ) ビットの伝送レートの手前で限界がくるだろうと予想される。エクサビット／秒の壁を越えていくためには量子符号化の利用を真剣に考える必要がある。その鍵は受信側における量子計算で、信号状態はコヒーレント状態である。

コヒーレント状態は光子がボーズ凝縮した状態で、減衰があっても量子的揺らぎの最小不確定状態を保持できるので、伝送には最も適した巨視的なガウス状態である。究極の通信ではこのような巨視的状態で重ね合わせの原理を制御して、光子当たり最大の情報を取り出す必要がある。これは、1 キュービットレベルの量子制御で実現できる量子暗号に比べると、格段に難しい技術である。光子レベルで高い非線形効果を実現する必要がある。

現在ではそのために必要な基本要素が理論的に分かっている。つまり、3 次の位相ゲートと呼ばれる変換さえ実現できれば、これを従来の技術 (厳密には線形光学素子、2 次非線形素子とホモダイン検波からなるガウス型操作) と組み合わせることで、原理的に任意の光非線形効果を実現できることが知られている。つまり、任意の光量子回路を構成することができるわけで光の万能ゲートセットが手に入ることになる [12][13]。その 3 次の位相ゲートは、図 4 のような光回路で実現できることが知られている。この 3 次の位相ゲートを従来の光通信システムに組み込めば、一気に従来のショット雑音限界を超えることができるわけである。

この回路で鍵となるのは、二つのスクィーズド光を干渉させて作る量子もつれ状態と、高精度の光子数識別器である。この二つの要素技術は、3 次の位相ゲートのみならず、広い技術領域での応用が可能である。図中、初段の量子もつれ状態に変調操作を施す部分は、既に実現されており、ショット雑音限界を超える精密計測に応用可能である [17]。これに対して光子数識別技術はまだ世界的にも満足の行くレベルにはなく、現在でも挑戦的課題である。NICT では、低雑音の半導体受光素子と高利得・低雑音の積分型読出回路を組み合わせた光子数識別器 (英語の略称として CIPD) の開発を進めており、感度、雑音特性で世界トップクラスの性能を実現している ([18]－[20] 及び **3-4** 藤原ほか)。

量子もつれ状態や光子数識別器を組み合わせて、従来のショット雑音限界を超えるための回路設計とその性能評価に関する理論はまだ完成しておらず、NICT ではその理論の構築にも取り組んでいる。最新成果については **3-5** で北川と武岡が報告している。

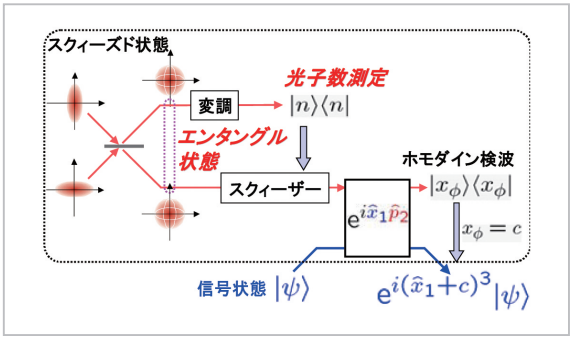

図4 3 次の位相ゲート回路構成

(5) 量子ネットワーク

量子計算や量子テレポーテーション及び量子中継の技術が発展すれば、純粋に量子的なネットワークが形成される。いわば量子 LAN、量子 WEB である。そこでは小規模の量子計算機をつないだ量子分散処理や、量子もつれ状態を使った秘密証拠供託、個人情報を保護しながら投票や決済を行う量子認証などが可能となる。そのための基盤技術については、**3-6** で早坂が報告している。

6 まとめ

通信の大容量化や安全性確保への要求が高まるなかで、電子デバイスの微細化や光信号の高密度化が進み、情報通信技術は光子や電子レベルの信号を取り扱う時代に入った。そして、これまでの集積化・高密度化に原理的限界が見え始めるなかで、情報通信技術が究極の物理法則である量子力学に行き着くのは時代の必然である。量子情報通信はこれまでのどんな方法よりも、はるかに多くの夢を与えてくれる。これからの情報通信技術の進むべき道標になろうとしている。光波通信がその性能限界を向かえたあと、ペタビット/秒という伝送レートの限界を超えて、更にその先のエク

サビット、ゼッタビット/秒という世界を頑健な情報安全性の下に支える技術の種として、量子情報通信は現在、我々が手にしている唯一の可能性である。

量子暗号のように実用化が視野に入ったテーマもあるが、量子情報通信の研究は、全般にまだ基礎科学としての研究フェーズにある。必要な要素技術の開発に取り組む過程で新現象を発見する可能性も高い。基礎科学の意義を尊重しながら、戦略的に実用化研究に取り組めば、その過程で様々な分野へ大きな波及効果をもたらすものと期待される。

参考文献

1 H. P. Yuen, Phys. Rev. A13, 2226, 1976.
2 松岡正浩, “量子光学”, 東京大学出版会, 1996.
3 山本喜久, 渡部仁貴, “量子光学の基礎”, 培風館, 1994.
4 D.F.Walls, G.J.Milburn (霜田光一, 張　吉夫訳), “量子光学”, シュプリンガー・フェアラーク東京, 2000.
5 S.Wiesner, SIGACT News 15, 78, 1983.
6 C.H.Bennett and G.Brassard, Proc. of IEEE Intern. Conf. on Computers, Systems, and Signal Processing, Bangalore, India IEEE, New York, pp.175-179, 1984.
7 D.Deutsch, Proc. R. Soc. Lond. A 400, 97, 1985.
8 P.Shor, Proc. of 35th Annual Symp. on the theory of Computer Science, p124, 1994.
9 古沢　明, “現代物理最前線５”, 共立出版, 2001.
10 竹内繁樹, “光学33”, 284, 2004.
11 K.Knill, et al., Nature 409, 46, 2001.
12 D.Gottesman, A.Kitaev, and J.Preskill, Phys. Rev. A64, 012310, 2001.
13 S.D.Bartlett and B.C.Sanders, Phys. Rev. A65, 042304, 2002.
14 V.Giovannetti, et al., Phys. Rev. Lett. 92, 027902, 2004.
15 M.Fujiwara, et al., Phys. Rev. Lett., 90, 167906, 2003.
16 M.Takeoka, et al., Phys. Rev. A 69, 052329, 2004.
17 J.Mizuno, et al.,Phys. Rev. A 71, 012304, 2005.
18 M.Akiba, M.Fujiwara, and M.Sasaki, Opt. Lett. 30, 123, 2005.
19 M.Fujiwara and M.Sasaki, Appl. Phys. Lett. 86, 111119, 2005.
20 M.Fujiwara and M.Sasaki, Optics Lett., 31, 691, 2006.

佐々木雅英（ささきまさひで）
新世代ネットワーク研究センター光波量子・ミリ波 ICT グループ研究マネージャー（旧基礎先端部門量子情報技術グループリーダー）　博士（理学）
量子情報通信