国立研究開発法人
情報通信研究機構

NICT NEWS

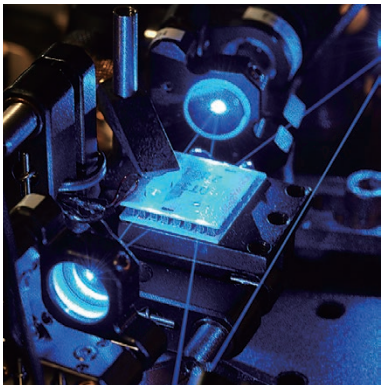
No.459 AUG 2016

FEATURE

量子で拓く情報通信の新しい地平

NICT NEWS No.459 AUG 2016
国立研究開発法人情報通信研究機構

CONTENTS



FEATURE

TOPICS

INFORMATION

表紙写真
レーザー光を鏡の間で往復させて蓄えるための光共振器とその中心に配置された非線形光学結晶。蓄えられて高強度となったレーザー光による非線形効果を用いて「量子もつれ光子対」が生成されます。

INTERVIEW

量子が導く情報通信の広大な沃野

佐々木 雅英（ささき まさひで）
未来ICT研究所 主管研究員
NICTフェロー
大学院博士課程修了後、NKK（現JFEホールディングス）勤務を経て1996年に郵政省通信総合研究所（現NICT）入所、量子情報通信技術の研究開発に従事。博士（理学）。

従来のコンピュータの1億倍高速な演算能力を持つという量子コンピュータ。決して破られることがないという量子暗号。情報通信に革新をもたらす可能性がある存在として、「量子」の考え方が大きな注目を集めている。従来の技術との違いはどこにあるのか。また、どのようなところから実用化されていくと考えられるのか。未来ICT研究所の佐々木雅英主管研究員にお話を伺った。

■「量子」とは、「量子ICT」とは何か

――近年、新しい技術のキーワードとして耳にすることが増えた「量子」という言葉ですが、そもそも、「量子ICT」とはどういうものなのでしょうか。

佐々木　「量子」とは、「ものを計る最小単位」という意味です。例えば、我々が普段日常生活で接する電気は、電流が何アンペアであるとか、電圧が何ボルトであるとか、といった測り方をします。しかし、極微細なデバイスを作って、そこで電流や電圧を測ろうと思うと、ちょっと様子が変わってきます。それまでは「ツマミを回すと連続的に変化する」量であったものが、どんどん小さくしていくと、ある段階から急に離散的な振る舞い、飛び飛びの値が出てくるのです。これはその段階で、電子というそれ以上は分割できない「つぶ」の動きを見ているために、そうなるのです。

あるいは、レーザーポインターから出ている光もそうです。これもどんどん減衰させていくと、最終的には雨だれのように途切れ始め、飛び飛びの振る舞いをする1個1個の「つぶ」、光子になる。

こんなふうに、我々が普段使っている量というのは、必ず、それ以上は分割できないつぶになる。面白いことに、この「つぶ」は、我々が普段接している物とはまったく違う振る舞いをします。例えば、とある経路にパチンコ玉を転がした場合、分岐があれば、パチンコ玉は必ずどちらか一方に行くはずです。しかし量子の世界では、「つぶ」が1つであるにもかかわらず、その分岐の両方に「存在する」状態を示すのです。そうなると、もうパチンコというゲームは成り立ちません。根本的なルール自体が変わってしまっているからです。

しかし、こうした現象をうまく工夫して使えば、古典的なルールに従って構築されていた計算や通信とはまったく違う、革新的なものができる。それが、量子コンピュータや量子暗号に代表される、量子ICTなのです。

■量子ICTの研究が目指すもの

――これまでの体系を、新しいルールにのっとってすっかり塗り替えていく可能性がある研究というわけですね。そうしたなかで、特にテーマと言えるものは何でしょうか。

佐々木　情報通信には、大きな2つの課題があります。

まず1つは大容量化です。通信量は増加の一途をたどっており、どうやってその増えてくる情報を処理するのか。いかに少ないエネルギーでより多くの情報を伝送するかという、伝送効率の問題ですね。特に量子ICTの分野からこの問題に応えるのが、量子通信という分野です。

もう1つはセキュリティの問題です。大量の重要情報がネットワークでやり取りされる今日、情報の漏洩は致命的な事態を招

INTERVIEW

量子が導く情報通信の広大な沃野

きかねません。漏洩を防ぐ具体的な方策は情報の暗号化ですが、これを量子の概念を使って行うのが量子暗号です。特に実用化という点では、量子暗号は目前の段階まで来ており、企業によるユーザ環境での試験運用も始まっています。

量子暗号のキーワードは「絶対に傍受できない」ことです。「不確定性原理」という法則に従う光子1個1個に情報を載せることで、測ろうとすること自体が光子の状態を変えてしまう、つまり盗聴しようとすると必ずそれが判ってしまうという機能を実現できます。これが、従来の暗号にはありえない革新的な違いと言えます。

一方の量子通信は、先に述べた、「つぶ」が2つの状態に同時に存在する、いわゆる「重ね合わせ」の現象を利用したものです。しかし、これは極めてデリケートな現象で、外乱がまったくない状況下でしかその効果を得られないため、現在は、まだ実験室の中でようやく扱うことができるという段階です。しかし今後10年、20年経って、この技術を受信機に組み込んで使えるようになれば、伝送効率が今よりも千倍や1万倍、場合によっては100万倍にもなるという、非常に有望なものでもあります。さらに、計測標準技術にも革新をもたらします。

というわけで、我々の研究は、まだ実験室のレベルですが、遠い将来を見据えてやっている量子通信と、半ば実用化の域に達している量子暗号の両方があります。

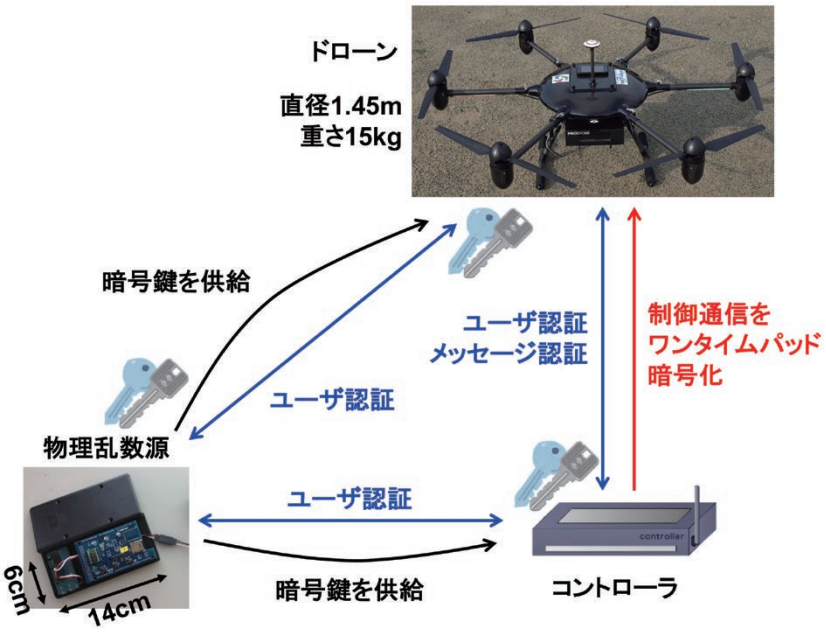


図1　秘匿ドローン通信技術。物理乱数源で生成した真性乱数を暗号鍵としてドローンとコントローラに供給し、制御信号のパケットを毎回暗号化します。一度使った暗号鍵は2度と使いません（ワンタイムパッド暗号化）。また、ユーザ認証やメッセージ認証にも真性乱数を用いて最強の安全性を確保しています。

■既存分野にも大きな広がりをもたらす

――研究そのものも、既存の技術からどんどん離れていく感じなのでしょうか。

佐々木　いいえ。それはまったく違います。

一つひとつの「つぶ」を制御できるようにすれば新たなルールで動くけれども、その手前、つまり多くの「つぶ」の集まりであれば、古典的なルールに従います。この分野の研究者は、その両方を見ています。それだけに、我々は今までのICTという体系を最も広い視点から見ているという自負があります。もっと言えば、これまでのICTをすべて包含しているとさえ言えると思っているのです。

実際に、量子ICTに取り組む中で、そこから翻って、従来の暗号技術や従来のネットワーク技術の分野でも、きちんと独創的な論文や特許が書けるような広がりが出てきています。

最近の例では、量子暗号で開発した乱数生成技術を応用して秘匿ドローン通信技術の実証実験に成功しています。ドローンは様々な用途で利用が始まっていますが、その制御通信やデータ通信のセキュリティ対策は十分ではなく、安全性の確立は大きな課題となっています。我々の技術は、乱数によるワンタイムパッド暗号化を用いることで、理論上、最高強度の暗号を最軽量でドローンに実装することができます（図1参照）。報道発表をしても、まさか我々のチームだとは思われず、例えばワイヤレスネットワーク分野の方に問い合わせが行ってしまったりするのですが（笑）。

量子ICTの研究は、情報通信の根幹の原理を追求していくので、その過程で、従来の暗号技術やネットワーク技術にとっても

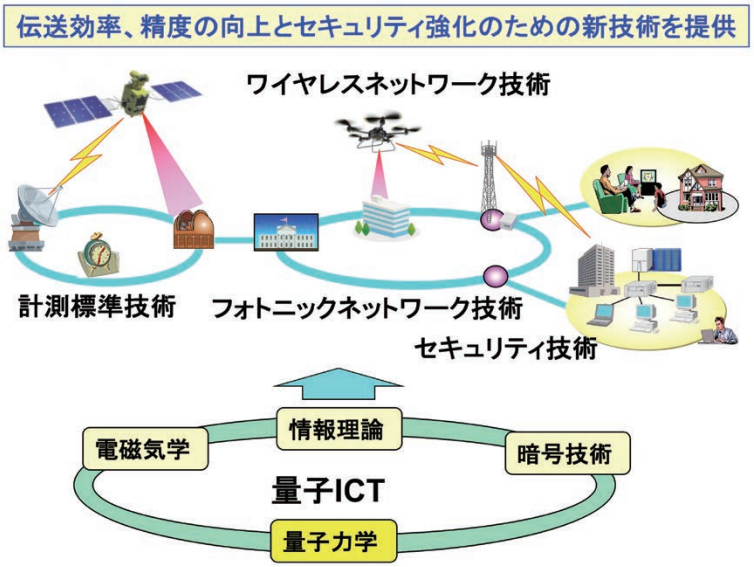


図2　量子ICTとは、電磁気学、情報理論、暗号技術に更に量子力学まで取り入れて突き詰めた情報通信技術であり、セキュリティ技術、ネットワーク技術、計測標準技術に新たな地平を切り拓くものと期待されています。

新知見や発見がもたらされるわけです。これらの成果は、電磁気学や情報理論、暗号技術の言語で書かれていて、まだ量子の性質を使ったものではありませんが、これまでのネットワークの接続性や安全性を向上させる新しい技術になっています。我々はいずれ、それを一段掘り下げて、さらに量子の言葉に拡張したいと思っています。その先に情報通信の沃野が広がっており、これまで見たことのない新しい地平が拓かれると思います（図2参照）。それが量子ICTをやっていて、最近とてもエキサイティングだと思える部分です。

――量子ICTそのものの研究もあり、一方で既存分野への展開もある。非常に幅広く、やりがいもある研究ですね。

佐々木　ものによっては「これのどこが量子なの」などと言われることもありますが、我々にとっては、対象が量子ICTであれ、従来のICTであれ、フロンティアであることには変わりがない。実際、既存技術と量子通信の概念をハイブリッドすることで、「物理レイヤ暗号」といった今後のネットワークに革新をもたらし、そして量子通信よりずっと早く実用化の域に達しそうな新たな技術も誕生してきています。

「量子の視点」から取り組む情報通信の研究は、非常にダイナミックかつ、エキサイティングな手ごたえのある分野です。近年、衛星やドローンを使った新しいネットワークの構築に向けて、ネットの巨人といわれる企業が総力を挙げて研究開発に取り組み始めています。まだ、ネットの接続性や利便性の追及が優先されているように見えますが、セキュリティも決して後回しにはできません。この点に関しては、我々がトップランナーであるという自負もあり、その面から、学術的にも実用上も有用な成果を出して貢献していきたいと思います。

COLUMN

グローバルセキュアネットワーク構築に向けた物理レイヤ暗号の研究開発

究極の伝送効率を目指す量子通信と、究極の秘匿化を目指す量子暗号は、これまで独立に研究開発が行われてきました。秘匿性の実現には、暗号化のために余分な帯域や符号化が必要なので、高い秘匿性を要求すると伝送効率はどうしても犠牲になります。その意味で量子通信と量子暗号は、情報通信の両極限にある技術ですが、両者の利点をうまく組み合わせたものが物理レイヤ暗号という技術です。これは、通信路の特性に応じて伝送効率と秘匿性のバランスを最適化する方式で、光はもちろん他の電磁波帯でも使える汎用的な技術体系です。特に、衛星やドローンを用いた新しいグローバルセキュアネットワークを構築する際のコアとなる技術です。我々は2014年に東京光空間テストベッドを構築し、物理レイヤ暗号の実証的な研究開発に取り組んでいます。

東京光空間テストベッドのNICTターミナル（本部3号館屋上）と研究開発チームの主要メンバー。通信のほかセンシングにも使える全天候型スキャナを搭載したコンテナシステムです。電気通信大学に設置された光ターミナルと地上8kmの光空間リンクを構成し、物理レイヤ暗号や新しいセンシング技術の開発を行っています。

量子情報通信

通信・計測の極限技術を追求する

武岡 正裕（たけおか まさひろ）
未来ICT研究所
量子ICT先端開発センター
センター長
大学院博士課程修了後、2001年に独立行政法人通信総合研究所（現NICT）入所、量子光学、量子情報理論、量子暗号の研究に従事。博士（工学）。

現在の情報通信技術は19世紀に確立された物理法則に基づいて設計されていますが、通信容量の限界や暗号解読の危機など、将来的に性能限界を迎えることが危惧されています。その限界を打破するため、NICTでは究極の物理法則である量子力学に基づく新しい情報通信技術「量子情報通信技術」や、その応用技術の研究開発を進めています。ここではその概要を紹介します。

■量子情報通信

現代の情報通信技術の発展は目覚ましいものがあり、今も日々進歩し続けています。一方で、現在の技術体系の延長上では、将来性能限界を迎える可能性も指摘されています。例えば、光ファイバーに入力できるレーザーの電力には物理的限界があり、また宇宙での通信が超長距離化すれば、信号が弱すぎて正確に受信できなくなってきます。一方、通信のセキュリティについても、現在の一般的な暗号方式は、将来のコンピュータ技術等の発展により解読されてしまう危険性が指摘されています。

これに対して近年、量子力学という原子や電子、光子などミクロな世界を扱う最新の物理学を駆使した情報技術が実現できれば、従来技術では不可能な安全性を実現する「量子暗号」や、現在のコンピュータでは何万年もかかる計算を短時間で実行する「量子コンピュータ」など、抜本的な技術革新が可能になることが次々に予言されました。こうした量子情報技術の研究開発は、21世紀に入り世界各地で本格的に開始されています。

NICTでは、この中で特に通信に関わる技術から2つの研究テーマを設定し「量子光ネットワーク技術」、「量子ノード技術」と名付けて研究開発を進めています。図1、2に、その概要を示します。

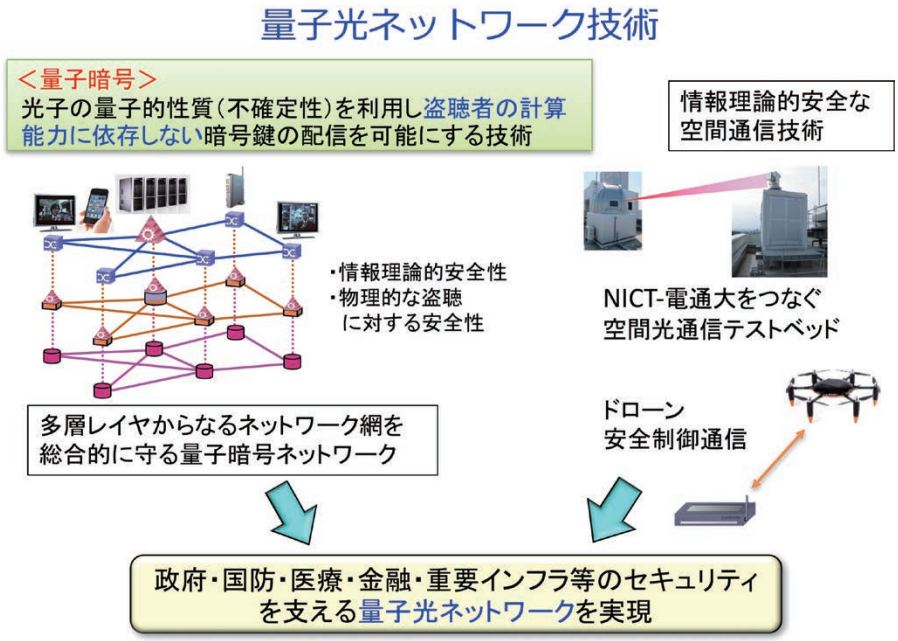


図1　量子光ネットワーク技術の概要

■量子光ネットワーク技術

現在、社会の様々な場面で暗号が用いられていますが、将来的な計算技術の革新によって解読されてしまう危険性があります。これは、国家情報や医療情報など、機密情報の通信では重大な問題となってきます。この問題を抜本的に解決するため、NICTでは究極の暗号通信と呼ばれる「量子暗号」を中心に研究開発を進めています。量子暗号は、どれほど強力な計算能力を使っても解読不可能な安全性を保証する情報理論的安全性と、どのような物理的な盗聴攻撃（例えば光ファイバーから一部の信号を抜き取ってしまうなど）に対しても安全性を保証する物理的な盗聴に対する安全性という、現在の暗号方式にはない大きな特長があります。これらを、光の量子力学的な性質を使うことで実現できるのが量子暗号ネットワークです。具体的な内容は、本号の記事を参照ください。また、NICTでは量子暗号に限らず、物理的な雑音を利用した情報理論的に安全な通信を、ドローンや衛星のような無人の移動体、空間光通信など、社会の様々な場面に実装するための研究開発も進めています。

■量子ノード技術

こちらはより長期的な基礎研究開発です。光通信の極限的な性能を引き出すためには、光子1個レベルの微弱信号に情報を載せ、それを正確に計測し取り出す必要があります。そのためには、量子力学特有の現象を壊さずに計測・制御できることが不可欠です。しかし現実には、量子力学的性質は非常に壊れやすく、実現にはまだいくつかの技術革新が必要です。

ノードとは、通信ネットワークの中継点の事です。本テーマでは、ノードの意味を広くとらえて、中継点で微弱な光信号を量子的に受信、処理するために必要な種々の極限技術を研究しています。特に、光の量子状態を制御する「光量子制御技術」、原子やイオンを1つずつ制御して量子通信や周波数標準技術に応用する「量子計測標準技術」、マクロサイズの人工原子である超伝導回路を使い、光と物質の相互作用を光子1個レベルで精密制御する「超伝導量子回路技術」の3つが中心的な研究課題です。詳細は本号の記事で紹介されていますが、いずれも量子物理学そのものを開拓する未来技術であり、まだ誰も完全には実現していない挑戦的な課題です。

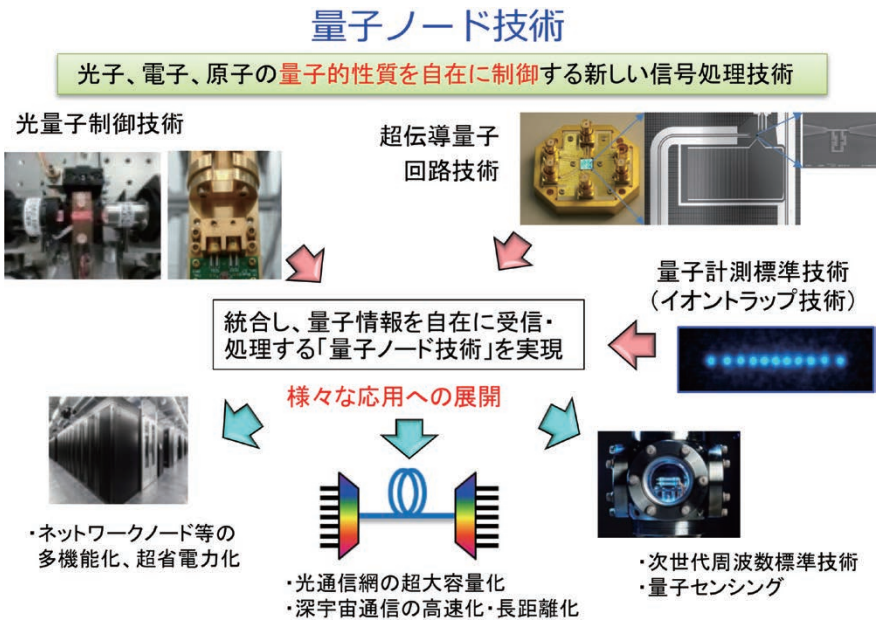


図2　量子ノード技術の概要

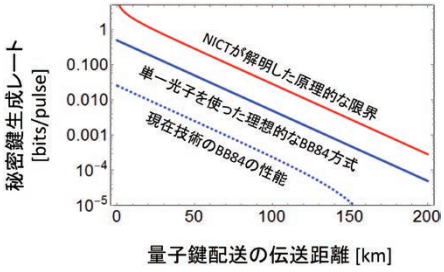


図3　量子鍵配送の鍵生成レートの限界と伝送距離。BB84は現在最もスタンダードな量子鍵配送方式。我々の示した原理限界は、今後どのような優れた新方式を考案したとしても超えられない限界があることを示している。

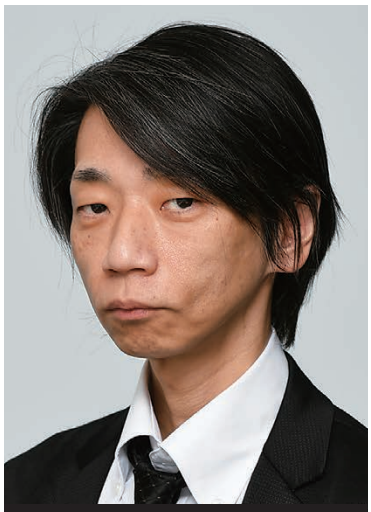
■おわりに

量子情報の研究開発を進めるには、理論研究も重要です。現在のデジタル通信技術は、1948年にシャノンがその原理限界と可能性を理論的に明らかにしたことで、今日の発展を迎えています。量子情報通信は、シャノンの情報理論に量子力学を取り入れた新しい理論で体系化されるべきですが、その確立はまだ道半ばです。逆に言えば、技術と基礎理論が同時進行で発展している非常に面白い研究分野といえます。最近我々は、情報理論と量子力学を適切に用いて、量子暗号通信の根幹である量子鍵配送の原理的な性能限界を明らかにする新しい理論を確立しました（図3）。こうした基礎理論は、科学として重要なだけでなく、量子鍵配送の新しいプロトコルの探索や具体的な装置の設計を行う際、どこまでの性能を追求すべきか、またどこからは元々追求してはいけない領域なのか、といったベンチマークを与えるもので、今後の技術開発における重要な指針となります。本研究成果は、Nature Communications誌*に掲載されています。

量子情報通信技術は、物理学やデバイス工学、通信工学、セキュリティ技術、情報理論など様々な分野の境界にある新しい技術であり、NICT内の様々なバックグラウンドを持つ研究グループが共同して研究開発を進めています。また、国内外の様々な研究機関・企業とも積極的に連携しています。光や原子、超伝導人工原子、そして情報を操る極限的な技術は、量子情報通信以外にも時間・周波数標準、センシングなどの諸分野への展開も期待されます。

＊タイトル：Fundamental rate-loss tradeoff for optical quantum key distribution
著　　者：Masahiro Takeoka, Saikat Guha, and Mark M.Wilde
文献番号：Nature Communications 5:5235 (2014)
DOI: 10.1038/ncomms6235

絶対安全な通信を目指して
量子鍵配送ネットワークの研究開発



藤原 幹生（ふじわら みきお）
未来ICT研究所
量子ICT先端開発センター
研究マネージャー
大学院修士課程修了後 1992 年郵政省通信総合研究所（現 NICT）に入所。衛星搭載用遠赤外検出器、光子数識別器、極低温エレクトロニクス、量子鍵配送の研究に従事。博士（理学）。

NICTでは絶対安全な通信を可能とする量子鍵配送(quantum key distribution: QKD)リンクと、それらをネットワーク化する研究を進めています。QKDでの安全性は物理法則が担保しており、将来どれほど計算機が発達しても解読できない暗号通信を行うことが可能です。また、それらをネットワーク化して運用することによりサービスエリアの拡大のみならず、応用用途の拡大が期待されています。今回、その原理とネットワークアーキテクチャをご紹介します。

■背景

元NSA・CIA職員のスノーデン氏によるリーク情報*でも喧伝されていますが、インターネットで使用されている暗号の一部は、既に破られている可能性があります。また、海外では、現在一般的に使用されている公開鍵暗号を瞬時に解読できる量子コンピュータ開発に多額の資金が投入されています。我々の社会生活でも既に高度に秘匿すべき情報もインターネット上を行き来する時代ですが、情報漏洩への危機意識はいまだ希薄である感があります。ゲノムデータなど個人の生涯を超えて安全を担保しなければならない個人情報は過去に取り扱ったことがなく、長期に秘匿しなければならない情報をいかに伝送すべきかを真剣に考えなければいけません。国家機密やゲノム情報など30年後に解読されても大きな問題となる情報を安全に伝送させるには、利便性が高く、計算機能力向上に左右されない安全な暗号方式を開発する必要があります。

■量子鍵配送の概要

NICTでは第2期中期目標期間（2006-2010）から絶対安全な通信を目指し、二者間で絶対安全に乱数（暗号鍵）を共有できる技術としてQKDの研究を進めてきました。1984年にBennett博士、Brassard教授によって提案されたQKDプロトコルはBB84と呼ばれ、誕生から30年以上経っていますが、QKDの実験が盛んになったのは今世紀に入ってからです。QKDは、情報媒体に光子を利用し、2つの非直交な基底（図1）を用いて光子1つに1ビットの情報を乗せ、送受信者間で乱数を共有する技術です。光子1個という“量子状態”は非常に壊れやすく、盗聴者がこの光子を測定・再送すると有限の確率で量子状態が変化し

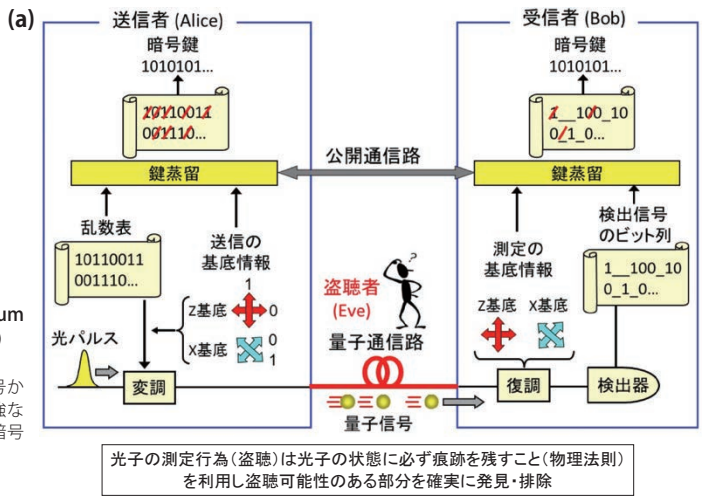


図1 (a) 量子鍵配送（quantum key distribution: QKD）の原理
受信者に届いた光子信号から誤り訂正、秘匿性増強などの鍵蒸留処理を経て暗号鍵を生成
(b) QKD装置写真

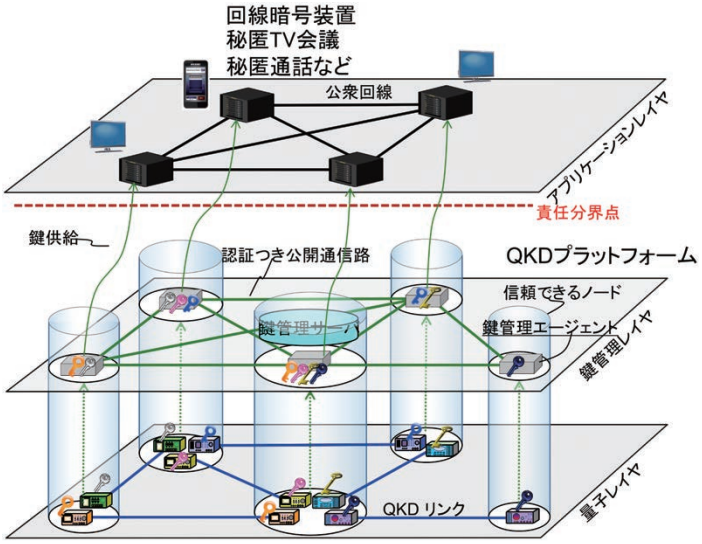


図2　QKDプラットフォームの概要
量子レイヤ　様々なベンダーのQKDリンクで構成
鍵管理レイヤ　鍵管理サーバ：ネットワーク全体の状態を常に監視しリルーティングなどの管理
鍵管理エージェント：暗号鍵のフォーマットを整え記録しユーザからのリクエストに応じて提供

ます。その変化をとらえるため正規送受信者の間で共有した乱数の一部を公開し答え合わせをします。答えに誤りが発見された場合、何らかの盗聴行為があったと判断でき、盗聴行為がなかった乱数を送受信者は暗号用の鍵として使用できます。物理状態の変化は量子力学（詳しくはno-cloning定理）が正しい限り絶対であるため、物理法則が安全性を担保しているプロトコルといえます。このようにして共有した暗号鍵で、1948年に情報理論の巨人であるシャノン博士が情報理論的（無限大の計算能力をもってしても解読できない）に安全な暗号方式であると証明した、one time pad暗号（送受信双方で共有した暗号鍵で排他的論理和演算を行う：毎回異なる乱数を使用）を適用することにより、将来計算機がどれほど性能向上しても解読不可能な通信（絶対安全な通信）を実現することが可能になります。現在、我が国で開発されているQKDリンクは、産学官の連携により世界最高レベルの性能・安全性を誇っています。

■QKDネットワーク技術 利便性向上を目指して

QKDは非常に高い安全性を保証することが可能ですが、情報の伝送媒体が光子1つ1つであるがゆえに伝送時にその多くが消失してしまいます。鍵生成は到達した光子を利用すれば良いので光子の消失があっても可能ですが、伝送可能距離が延びるに従い鍵生成率が急激に劣化します。世界最高レベルのQKDリンクでもファイバ伝送距離50kmにおいて鍵生成レートは数百k～1Mbps程度です。伝送レートは波長多重技術を用いることにより改善が可能であることが検証されていますが、伝送距離の伸長を可能とする技術の開発には克服すべき技術課題が多く、いわゆる量子中継技術の実現には、まだまだ研究を重ねる必要があります。現実解としてQKDリンクを数珠つなぎに配置し、中間地点で一旦古典情報として保存し、鍵情報をリレーする手法が取られています。例えばA-B間のQKDリンクで生成した鍵をK1、B-C間QKD装置で生成した鍵をK2とします。A-C間で鍵を共有するにはBから排他的論理和（K1⊕K2）を古典情報としてCに送ります。CではK2を知っていますのでK1⊕K2⊕K2= K1となり、A-C間で鍵共有できます。この場合、古典情報で保存している場所（ノード）では鍵情報が盗まれる危険性があり、厳重かつ安全に鍵情報を管理する必要があります。このようなノードを“信頼できるノード”と呼び、QKDをネットワーク化する上で重要な役割を果たします。QKDリンクのネットワーク化は利用エリア・利用用途の拡大や機能の可用性を担保するためには必須技術です。ネットワーク接続時において重要な技術は異なるベンダーのQKDリンクで生成される鍵のフォーマットの調整、鍵リレーの正確な実施、正確な鍵の提供などが挙げられます。NICTではQKDネットワークのアーキテクチャとして、レイヤ構造の定義と中央監視型ネットワークを提案しています。QKDリンク群で形成される量子レイヤ、鍵を古典情報として保存管理する鍵管理レイヤと定義しています。鍵管理レイヤは様々なユーザやアプリケーションに安全・確実に手渡すインターフェースを有しています。この2つのレイヤを合わせてQKD プラットフォームと命名し、JGN-Xと情報通信システム室の協力を得て、敷設ファイバを用いたQKDネットワーク（Tokyo QKD Network）を運用しています（図2）。このテストベッドを用いてQKDリンクの長期安定性やインシデント発生時のリルーティング等の試験を繰り返し、QKD プラットフォームの信頼性を高める研究を進めています。さらに、OSIモデルのレイヤ2～4の通信機器に暗号鍵を供給し、様々なアプリケーションへの展開を可能としています。特に携帯電話への鍵供給は秘匿通話だけではなく個人認証デバイスとしての応用も可能としています。さらに、ドローンなどこれからのIoT社会への展開が期待されている機器への鍵供給も視野に研究を進めています。

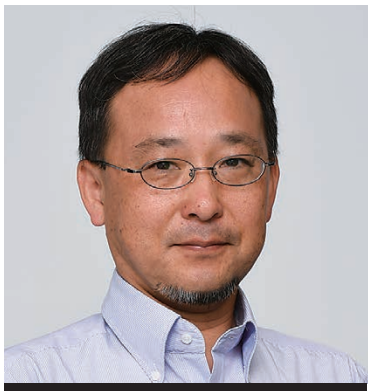
■今後の展望

我々は絶対安全な通信の実現を目指してQKD装置とそのネットワーク化について研究開発を進めています。伝送だけではなく分散ストレージなどへ応用し、安全にデータを保存できる機能の研究も進めています。細菌学者パスツールの言葉に“偶然は準備のできていない人を助けない”というものがあります。我々は将来、現在の暗号への脅威が突如発見され、絶対に破られない暗号が緊急に必要とされたとき、即座にソリューションを提供できるよう研究を進めています。

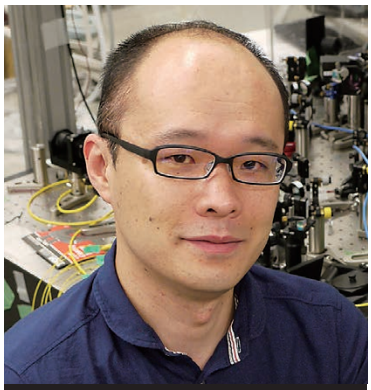
＊ http://www.fortinet.co.jp/security_blog/130906-NSAs-and-GCHQ-Decryption-Capabilities.html
https://agilecatcloud.com/2015/10/20/researchers-claim-to-have-solved-nsa-crypto-breaking-mystery/

従来の限界を打破する量子通信の実現を目指して

光子・原子の極限制御技術の開発



早坂 和弘（はやさか かずひろ）
未来ICT研究所
量子ICT先端開発センター
研究マネージャー
大学院修士課程修了後、1990 年に郵政省電波研究所（現 NICT）入所。イオントラップを用いた量子光学の研究に従事。大阪大学大学院基礎工学研究科招へい准教授。博士（理学）。



和久井 健太郎（わくい けんたろう）
未来ICT研究所
量子ICT先端開発センター
主任研究員
大学院修了後、株式会社富士通研究所を経て、2009 年 NICT 入所。量子光学、非線形光学の研究に従事。博士（工学）。

将来の情報ネットワークの主要なノードでは、基幹回線を行きかう光信号に最適な量子制御を施せる、いわゆる「量子ノード技術」が必要になります。その実現には光子や原子のような量子物理系の極限制御技術が不可欠です。このような極限技術は量子ノード技術以外にも様々な応用が期待されます。本稿では量子ICT先端開発センターで行っている量子ノード技術開発の一端として、光子とレーザ冷却イオンの量子状態極限計測について紹介します。

■背景

いかに正確に多くの情報を効率よく伝送するかという問題は、スマートフォンやインターネットの普及とともに、我々にとってもますます身近で切迫した課題となっています。量子情報理論の最新の成果によると、基幹回線で究極の伝送容量を実現するためには、受信側で信号パルス間に量子計算を施しながら復号を行う必要があります。これは復号回路の中に「シュレディンガーの猫」と称される巨視的な量子重ね合わせ状態を自在に生成し、制御しながら測定を行うことを意味します。量子重ね合わせ状態とは、いわば「猫が生きながらも死んでいる」という、日常とは異なる量子力学的な性質のひとつです。その制御のためには外乱や損失を光子や原子レベルで制御できる極限環境を情報ネットワークの主要なノードに配置し、基幹回線を行きかう光信号に最適な量子制御を施せる量子ノード技術が必要になります。量子ノード技術を実現するためには、光子や原子のような量子物理系を測定し、制御できる技術が欠かせません。

■光子の量子もつれ交換

量子力学では無限に離れた2つの粒子が、一見、瞬時に情報をやり取りするかのような不可思議な相関を持つことが許されます。このような量子力学的な相関を持つ光子のペアは量子もつれ光子対と呼ばれます。量子もつれ光子対はレーザ光では実現できない安全な通信（量子暗号）や高速の計算（量子計算）、さらには、高精度の光計測へと応用できます。しかし、量子もつれ光源には特殊な結晶や駆動用レーザを開発する必要があり、量子もつれ光子対の生成・検出を高速化することは容易ではありません。そのため、現在も世界中で研究開発が進んでいます。

量子もつれ光源を用いた通信プロトコルの中でも、量子暗号の長距離化や量子計算機のネットワーク化で基本となるのが、量子もつれ交換と呼ばれるプロトコルです。

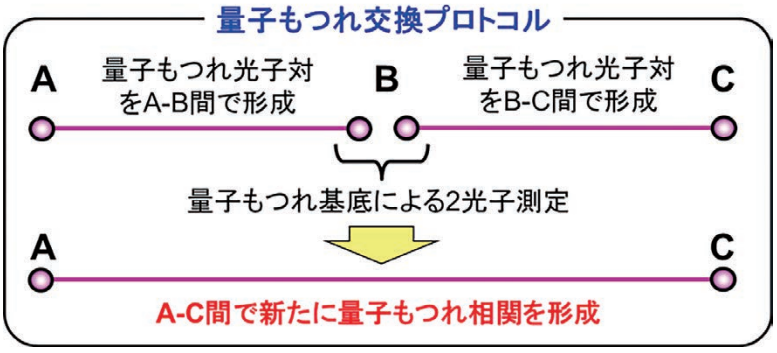


図1　量子もつれ交換の手順

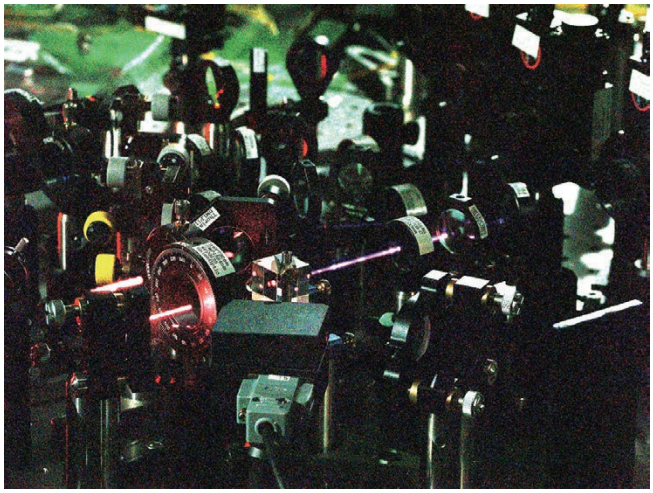


図2　量子もつれ交換に使用した実験装置

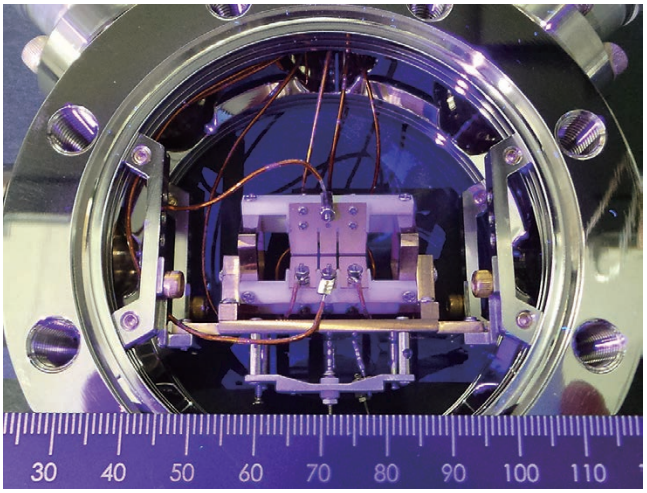


図3　イオントラップ装置

量子もつれ交換の方式を図1に示します。まず、地点AとB、地点BとCでは、それぞれが別々の量子もつれ光子のペアを共有します。最初、A-B間とB-C間で共有される光子のペアには何も相関がありません。次に、地点Bにおいて特殊な測定を行い、光子が来たかどうかを判別します。これは目隠しで光子をつかむような測定ですが、AとCのどちらから光子が来たか、あえて分からないようにすることで、AとCの間に新たな量子もつれが形成できます。実際の実験系は図2に示すようなもので、特殊な光学素子（特定の波長で高反射率を持つ鏡など）や様々な色のレーザ、さらには、高効率の光子検出器を用います。

NICTでは、光ファイバ通信に重要な波長帯（波長1,550 nm近辺）において、量子もつれ光子対の生成効率を高める技術を独自開発しました。また、この高効率の量子もつれ光子を複数用いることで、量子もつれ交換を従来よりも大幅に高性能化することに成功しました。量子もつれ交換は様々な研究機関で研究が進められてきましたが、我々は特殊な光学結晶の探索や、光子検出器を高効率化するといった技術的な改善を積み重ねることにより、つい先ごろ、先行研究と比較して1,000倍以上多い成功回数の量子もつれ交換を実証することに成功しています。

■イオンの量子状態計測

光子が量子状態の伝送に適していると考えられる一方、原子は量子計算や量子状態のメモリに適しているとされています。原子が電子を失ってイオンになると、電場による運動の制御が可能になり、レーザ冷却という手法で空間中に孤立して静止させることができます。図3はイオンを閉じ込めるイオントラップという装置で、図4はその中でレーザ冷却されたカルシウムイオン（Ca^+）とインジウムイオン（In^+）を示したものです。このようなイオンを用いて数個レベルでの量子計算の実証が報告されています。

原子は内部構造によって決まる固有遷移周波数の光しか吸収できないことが量子力学で明らかにされています。レーザ周波数をこの周波数と一致するように制御すると、世界のどの場所でいつ動作させても正確に同一周波数の光を発生する光周波数標準を作ることが可能です。イオントラップ中でレーザ冷却されたイオンは、運動や衝突による光周波数の変動がないために優れた光周波数標準として期待されており、幾つかのイオン種で研究開発が行われています。我々は従来型より2桁以上の精度向上が期待されるIn^+を光周波数標準に応用するための新しい極限計測技術の研究開発を行ってきました。

In^+はレーザ冷却と量子状態測定に波長159nmの光を必要としますが、このような短波長の光は生成が困難であるため、新たな手法の開発が必要となります。そこでレーザ冷却可能な2個のCa^+を用いてIn^+を間接的に冷却する共同冷却法を開発し、量子力学の許す最低のエネルギー状態である振動基底状態までの冷却を実現しました。図4は生成したCa^+とIn^+の配列を超高感度カメラで撮影したものです。このようにして静止させたIn^+の量子状態測定法として、In^+の弱い遷移を用いた方法、In^+の量子状態をCa^+に移して測定する量子論理分光法を開発することができました。これらの技術のいくつかを時空標準研究室に移転し、In^+の光周波数標準動作を実証することができました。

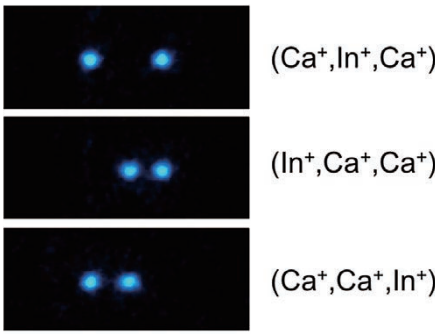


図4　超高感度カメラで観測したカルシウムイオン（Ca^+）とインジウムイオン（In^+）の配列。In^+は直接観測することができません。

■今後の展望

量子もつれ交換の高速化が光ファイバ通信に適した波長帯で実現したことにより、安価で高性能の光通信部品との組み合わせが可能となり、量子暗号など他の量子通信方式の高性能化が期待できます。今後は、量子もつれ交換装置の動作スピードをギガヘルツ帯まで向上させることにより、量子もつれを用いた量子計算や、高精度の光計測など、量子ノード技術に向けた様々な技術の実現が期待されます。

現在のイオントラップシステムは総重量が100kg以上となるため、情報ネットワークのノードに配置する用途には適しません。新たに研究開発を開始した集積型イオントラップでは計測器用汎用ラックに収納するサイズを目指しており、量子ノード技術実現に一歩近づくことが期待されます。また、光通信用レーザの光周波数安定化に応用することで通信容量の大幅な改善が期待されています。

超伝導回路で探る量子物理の世界

物質と光の相互作用を光子１個レベルで解き明かす

仙場 浩一（せんば こういち）
未来ICT研究所
フロンティア創造総合研究室
上席研究員
NTT 物性科学基礎研究所及び国立情報学研究所量子情報国際研究センターにて量子情報、超伝導量子エレクトロニクスの研究に従事。2013 年に NICT 入所。巨視的量子物理プロジェクト 主幹。博士（工学）。

巨視的量子物理プロジェクトでは、物質と光の相互作用を光子1個レベルで精密に測定・制御する研究を進めています。物質の代表としては、半導体微細加工技術を使って作られた、原子とよく似た性質をもつ超伝導回路（人工原子）や、半導体結晶中の電子スピンの集団などの巨視的量子系を使います。その理由は、原子を使った場合と比べて、相互作用が何桁も強い状況を作れるので、光子1個レベルで物質と光の相互作用を観測・制御しやすくなるからです。このような巨視的量子系で初めて現われる物理現象の解明を通じて、未来の情報通信に役立つ量子技術の開拓を目指します。

■「シュレディンガーの猫」と超伝導人工原子

今からおよそ100年前、20世紀の初め頃、原子など微視的な世界の物理法則は、誰もが直感的に体得している物理法則と比べて、とても奇妙であることが徐々に明らかになっていました。日常生活では、朝、通学・通勤するのに、電車で行くか、バスに乗るか、歩いていくか、どれかひとつしかできませんが、原子の世界では任意の割合で全て同時進行可能です。つまり、「ほぼ歩いていて、少しだけ電車に乗り、ひょっとするとバスに乗っている」という状態も可能です（「重ね合わせ」）。また、1本しかない傘を私が使い弟はレインコートを使うことと、その反対に、私がレインコートで弟が傘をさすことの2つの組み合わせも同時に進行可能なのです（「量子もつれ」）。ただし、誰かに見つけられる（観測される）と、そのうちのどれかひとつの状態になってしまいます。「重ね合わせ」や「量子もつれ」のような量子状態のとても不思議な性質は、まとめて「量子リソース」とも呼ばれます。

ヤングの2重スリットという実験があります（図1）。この実験では、光源から2重スリットを介してスクリーン上で観測される光の干渉縞は、光の最小単位である光子1粒に、どちらのスリットを通過してきたかという自分自身の“別の歴史”と干渉する不思議な性質が備わっているために、この場所では干渉で弱め合い、ほとんど観測されず、少し離れたところでは、強め合って観測されやすいというように、おびただしい数の単一の光子があちこちで観測されたことの集大成として縞模様が現れます。

ところで、私達を含めて身の周りのあらゆるものは、原子から構成されているのに、状態の「重ね合わせ」や「量子もつれ」が観測されないのは、なぜだろう？あるいは、どの大きさまで状態の重ね合わせができるのだろうか？ という問いかけは、誰もが抱く疑問です。いまだに完全には解かれていないこの疑問を、「猫の思考実験」を使って、最初に指摘したのがシュレディンガーでした。1935年のことです。シュレディンガーが提示した思考実験は次のようなものでした。「平均して1時間に1回の頻度で生じる原子核の放射性崩壊に連動して、猛毒の入った瓶が割れ

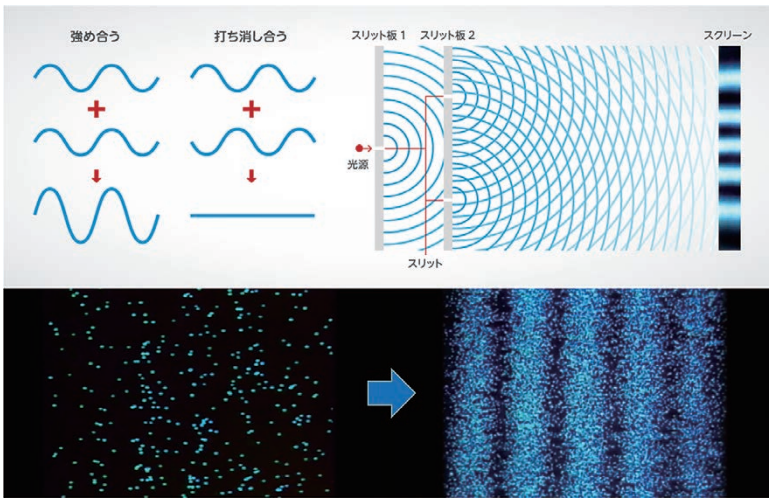


図1　極微弱光極限でのヤングの2重スリット実験（出典：浜松ホトニクス「Photonてらす」）

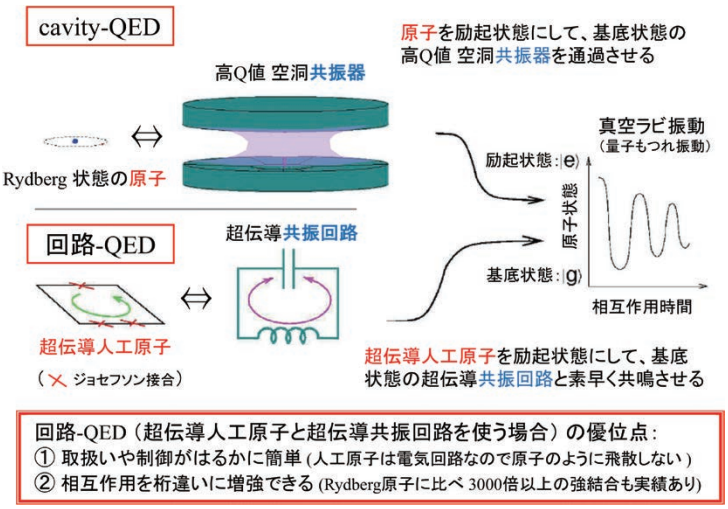
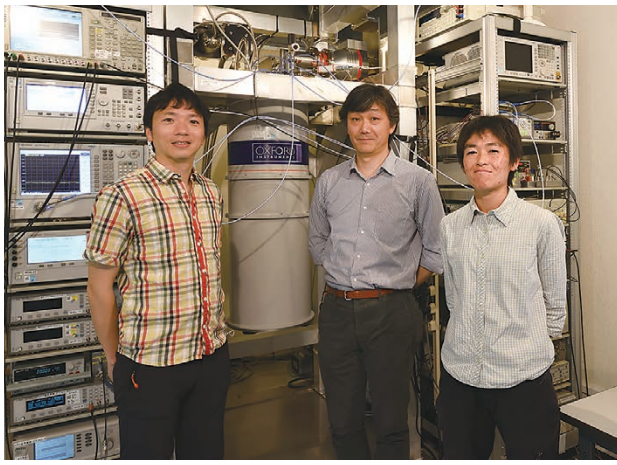


図2　原子と空洞共振器を使う cavity-QED とチップ上の超伝導回路を使う回路-QED の比較



回路-QED実験装置と巨視的量子物理プロジェクトメンバー
左から吉原文樹主任研究員、仙場、布施智子主任研究員

巨視的量子物理プロジェクト の研究紹介ページ
https://www.nict.go.jp/frontier/mqp/index.html

る装置があるとする。この装置に猫を入れて1時間そっとしておき、1時間後に観測するとどうなるか？ 生きた猫と死んだ猫の重ね合わせ状態を観測することになるのだろうか？」というものです。このように、ミクロな世界の物理法則がマクロ（巨視的）なものにまで影響が及ぶと仮定すると、典型的な不可逆現象である生命現象と矛盾し、大変困った状況となることを鋭く指摘した思考実験です。これは、巨視的量子現象の分野に関する当時の認識の限界と100年後の将来への課題をも示した偉大な思考実験だったのです。

それから80年以上経過した今日では、まだ猫よりはずっと小さいものの、超伝導人工原子と呼ばれる、顕微鏡で見える大きさの電気回路を低温に冷却することにより、巨視的量子現象の分野を実験的に探索・研究することが可能になりました。我々の研究では、超伝導体（アルミニウム）で形成された電気回路を巡回する数百ナノアンペア程度の超伝導電流が時計回りに流れている状態と反時計回りに流れている2状態の任意の重ね合わせを実験室で作り出すことができ、制御・測定することが可能です。

■物質と光の相互作用の増強手段 ― 回路-QED

物質と光の基本的な相互作用を光子1個のレベルで取り扱う共振器量子電磁力学、いわゆる cavity-QED は、従来Q値の大きなシングルモード空洞共振器中の光子及びその光子とエネルギー的に共鳴条件にある一対の準位を有する原子という組み合わせを用いて行われてきました。2001年頃には、この原子を超伝導人工原子に、空洞共振器を超伝導共振回路にそれぞれ置き換えて同様な実験が可能であると理論的には予想されていました（図2参照）。それが2004年以降、次々と実験で実証されました。しかも、超伝導人工原子とマイクロ波光子の相互作用は、従来知られている原子とマイクロ波光子の相互作用に比べて数千倍に増強できるため、マイクロ波光子1個の有無が、人工原子のエネルギー準位の変化やプローブマイクロ波の位相のシフトなど測定可能な変化量となって現れます。このように、シリコン基板上に作製した超伝導量子回路を用いた回路-QED の実験は、量子状態の制御に関する限り、従来の原子・分子を使った手法で可能であったことを基本的に再現できます。また、はるかに制御性が良いことから、量子シミュレーターや 量子コンピュータに代表されるような量子的リソースが秩序正しく制御されて動く機械の研究開発が世界中で進んでいます。それが完成した時、「シュレディンガーの猫」も現われるでしょう。

さらに、従来の原子・分子を使った手法よりはるかに強い結合が可能なため、従来は実現困難であった超強結合状態や、超放射量子相転移などの新たな物理の領域を開拓できる可能性があります。我々の研究では、アルミニウム製の超伝導人工原子とLC共振回路の間に、非常に強い相互作用を実現しました（図3）。透過波スペクトルの精密測定から結合系の状態は、今まで誰も実現できなかった未踏領域にあることを示すデータが得られ始めています。

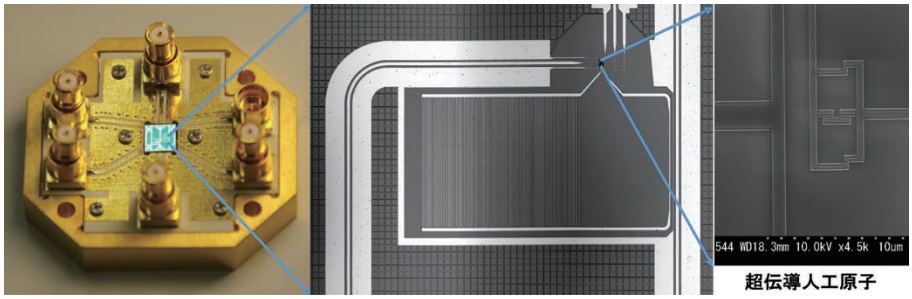


図3　超伝導人工原子を使った回路-QED 実験用試料（写真白色部分はアルミニウム製の超伝導薄膜回路）
左：回路-QED 実験に使う3mm角の試料チップをサンプルホルダにマウントしたところ
中央：超伝導人工原子・LC回路結合系　右：超伝導人工原子（寸法は 約4μm×8μm）

■今後の展望

我々は、巨視的量子系（超伝導人工原子）を光子や電子スピンと相互作用させ、未踏領域の物理を探索し、そこで発現する現象を光子1個のレベルで解明し、精密制御する研究を通じて、未来のICTに役立つ新原理・新現象の開拓を目指しています。量子情報通信以外にも 時間・周波数標準 の高精度化、高感度センシング、量子シミュレーター、量子コンピュータなどの諸分野への展開が期待されます。

ビジネスシーンで、産業で、社会インフラとして、その利用が進むワイヤレスネットワークの展示会＆セミナー

ワイヤレス・テクノロジー・パーク2016開催報告

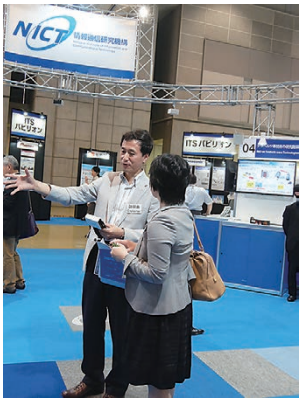
ワイヤレスネットワーク総合研究センター 企画室

NICTは、YRP研究開発推進協会及びYRPアカデミア交流ネットワークと共同で、「ワイヤレス・テクノロジー・パーク（以下、WTP）2016」（2016年5月25～27日、東京ビッグサイト）を開催しました。

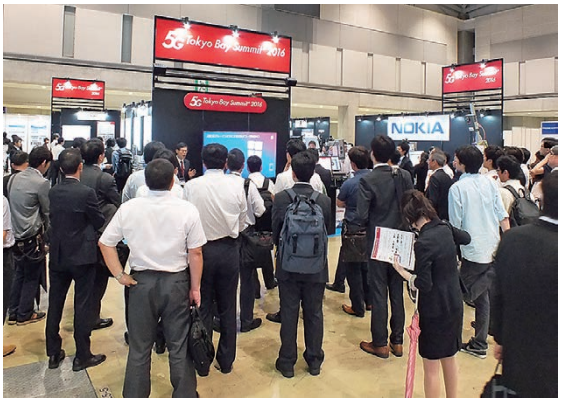
展示会では116機関の出展、セミナーは25コースで計124件の講演があり、来場者数は同時開催イベントと合わせて約47,000人、WTPは前回の約1割増となる約11,000人で、過去最多となりました。特に5G（第5世代移動体通信システム）のパビリオン・セミナーは注目を集めました。

NICTは、当センターを中心に最新成果17項目の出展と10件の講演を行い、来場者から技術の実用化に向けて様々な質問やコメントを頂きました。

WTP2016にご協力いただいた企業・団体の皆様には、この場をお借りして厚く御礼申し上げます。次回（2017年5月24～26日予定）は更に魅力的で充実した内容となるよう一層努めます。



UWB技術を利用した高精度の屋内測位システムを紹介する李統括研究員



最新の5G研究成果が集結した5G Tokyo Bay Summit® パビリオン

Interop Tokyo 2016 出展報告

NICTは、6月8～10日に、幕張メッセで開催された、インターネットとデジタルメディアの専門イベントである「Interop Tokyo 2016」に出展いたしました。会場には、昨年度を上回る140,945人が訪れました。

NICT では、IoT時代に対応したネットワーク技術とセキュリティ技術及び起業家万博の最終選抜者の事業紹介の展示をしました。また、“NICTERファミリーによる次世代のサイバー攻撃対策”の講演は、大変盛況であったため追加講演を行い150名以上の方にご聴講いただきました。NICTのブースにお越しいただきましてありがとうございました。

NICTブースの様子

Awards

文部科学大臣表彰は、科学技術に関する研究開発、理解増進等において顕著な成果を収めた者に授与されます。市村学術賞は、大学及び研究機関で行われた研究のうち、学術分野の進展に貢献し、実用化の可能性のある研究に功績のあった技術研究者またはグループに贈呈されます。

文部科学大臣　科学技術分野の文部科学大臣表彰
平成28年度 科学技術賞開発部門
Development Category, Prizes for Science and Technology

浦塚 清峰（うらつか せいほ）
電磁波研究所
統括

受賞の言葉

地震や火山噴火など広域で深刻な災害時に、天候や昼夜にかかわらず、いち早く被害の状況把握することを目的として、航空機搭載合成開口レーダー（Pi-SAR2）の開発を進めて参りました。

受賞は、この技術が災害時に役立つことが社会に広く認められたことによるものであり、一緒に開発に努力した多くの関係者と、この栄誉を共有したいと思います。

災害に強靭な社会の実現を祈念し、それにこの技術が広く活用されることを期待してやみません。

data

●受賞日：2016年4月20日
●受賞内容：災害被害を迅速に把握するためのPi-SAR2の研究開発により、安心、安全な国民生活の向上に寄与した

公益財団法人 新技術開発財団
第48回 市村学術賞功績賞
48th The Ichimura Prize in Science for Excellent Achievement

大久保 美也子（おおくぼ みやこ）
サイバーセキュリティ研究所
セキュリティ基盤研究室 主任研究員

大久保美也子（中央）

受賞の言葉

受賞内容は、簡単かつ安全にセキュリティシステムを開発できることを目指した「群構造維持暗号系（Structure-Preserving Cryptography: SP暗号系）」による新たな設計コンセプトの提唱と、それを具体化するSPデジタル署名等の暗号技術です。本研究の共著者の皆様に、深く感謝いたします。また、これまでご支援・ご指導下さりました皆様方に心よりお礼申し上げます。これを励みに、本分野へのより一層の貢献を目指します。

data

●共同受賞者：阿部 正幸（日本電信電話株式会社）
●受賞日：2016年4月25日
●受賞内容：相互接続を実現する群構造維持暗号系に関する先駆的研究

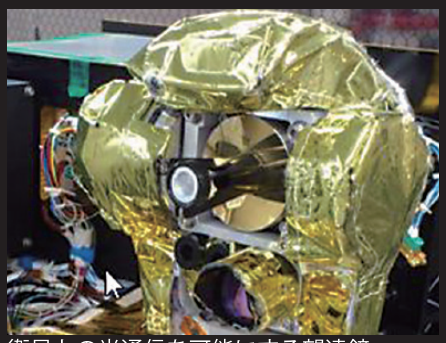
第5回 NICT オープンハウス 2016

10月27日(木)・28日(金)9:30〜17:00

※28日は16:30まで。無料・事前申込不要（一部除く）

ラボツアー（予定）

最先端光半導体デバイス作製環境（クリーンルーム）



衛星との光通信を可能にする望遠鏡

オープニングセレモニー【10月27日（木）10:00〜】

特別講演

「デジタルが経済・産業・社会・地方を変える」

森川　博之氏

東京大学　先端科学技術研究センター　教授

講演会【10月28日（金）午前・午後】

NICTの研究者が最新の研究成果について講演します。

ラボツアー【10月28日（金）午前・午後　※事前申込制】

研究施設見学（ラボツアー）にて、最新の研究活動をご紹介します。

技術展示【10月27日（木）・28日（金）】

最新の研究成果について、多数のデモ・パネル展示を行います。

NICT は、最新の研究成果を講演、ラボツアー、デモンストレーション、パネル展示でご紹介する「NICT オープンハウス 2016」を本部において開催します。

※詳細は後日公開する専用 Web サイトでご確認ください。

会場：情報通信研究機構 本部

〒184-8795 東京都小金井市貫井北町4-2-1

お問い合わせ 国立研究開発法人情報通信研究機構 広報部 NICTオープンハウス2016事務局

TEL：042-327-5322　E-mail：open-house-2016@ml.nict.go.jp

NICT NEWS No.459 AUG 2016

編集発行

国立研究開発法人情報通信研究機構 広報部

NICT NEWS 掲載URL http://www.nict.go.jp/data/nict-news/

〒184-8795 東京都小金井市貫井北町4-2-1

TEL: 042-327-5392　FAX: 042-327-7587

E-mail: publicity@nict.go.jp

URL: http://www.nict.go.jp/

Twitter: @NICT_Publicity

ISSN 1349-3531 (Print)

ISSN 2187-4042 (Online)

〈再生紙を使用〉