NICT NEWS

国立研究開発法人
情報通信研究機構

No.5
2026
通巻 519

FEATURE

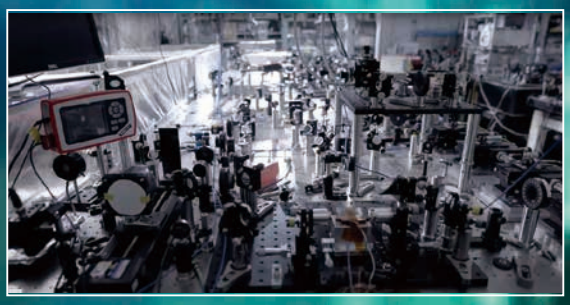
「量子の世界を操る」未来の情報通信技術

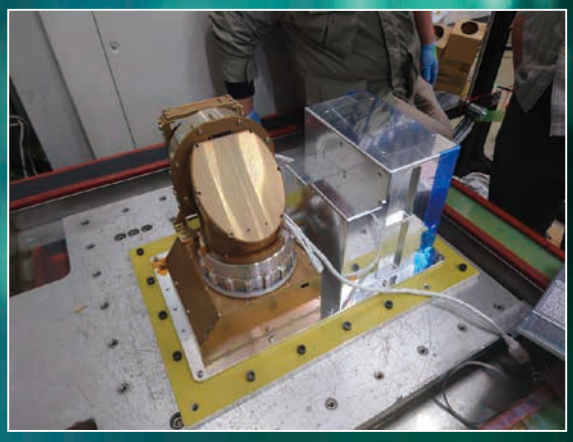
対談

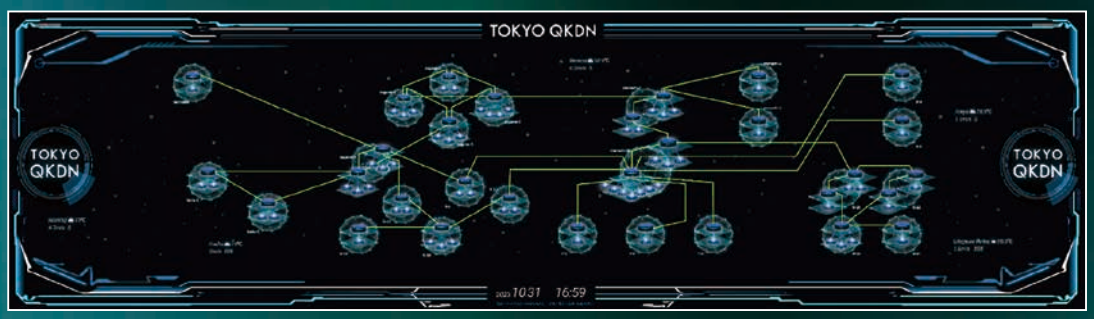
量子暗号通信の未来とは？

人類のフロンティアを拓く 2 人の研究者に聞く！

富田 章久×加藤 豪

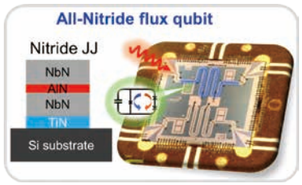






CONTENTS

NICT NEWS 2026 No.5 通巻519
国立研究開発法人情報通信研究機構



表紙写真
量子光学実験を支える光学定盤上の機器群（上）、衛星量子暗号の実現可能性検証のためISSに設置された小型光送信機（中央）、そしてNICTが構築した東京QKDネットワークの現在の構成（下）。光子の生成・制御から、宇宙空間を介した通信、都市圏光ファイバ網での長期運用まで、研究室内の実験成果を実環境での量子暗号通信へつなげ、社会実装へ近づける多面的な研究開発の広がりを示しています。

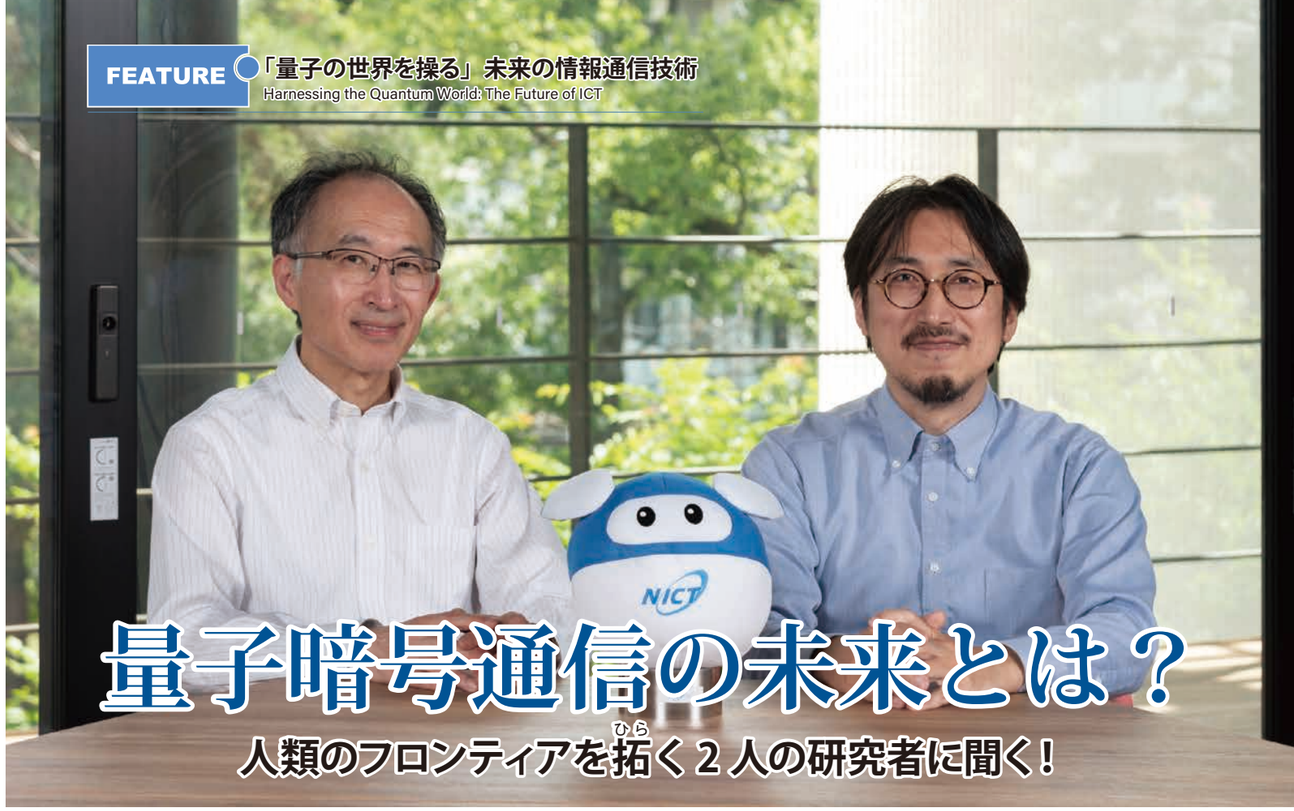
左上の写真
窒化ニオブ（NbN）を用いた超伝導量子ビットと調和振動子を結合したチップ（右）と、ジョセフソンジャンクション部の積層構造（左）。微細加工技術により、量子状態を精密に制御する基盤デバイスです。

FEATURE

「量子の世界を操る」未来の情報通信技術

TOPICS

INFORMATION



富田 章久（とみた あきひさ）
量子 ICT 協創センター
研究センター長

大学院修了後、企業研究所、大学教員を経て、2025 年に NICT に入所。量子情報技術、光量子情報処理、量子暗号などに関する研究に従事。博士（工学）

加藤 豪（かとう ごう）
未来 ICT 研究所
小金井フロンティア研究センター　研究統括／
量子 ICT 研究室　室長

大学院修了後、企業研究所を経て、2022 年に NICT に入所。量子制御、量子暗号などに関する理論研究に従事。博士（理学）

量子暗号通信は、情報セキュリティの概念そのものを変えてしまう新しい技術。量子力学の原理を基盤とするこの革新的な手法は、安全保障からビジネス、個人情報保護まで幅広い分野で実用化が期待されます。今回は、世界各国が開発にしのぎを削る通信技術の最前線で活躍する 2 人の研究者、量子 ICT 協創センターの富田章久センター長と、未来 ICT 研究所 量子 ICT 研究室の加藤豪室長の対談をお届けします。

――まず初めに、お二人のご経歴をお願いします。

富田　私は、企業で 14 年ほど、半導体を使った光通信用の光デバイスの研究をしたあと、1999 年から量子情報の研究を始めました。2010 年に北海道大学に移り、量子情報の実験的な研究、光を使った量子情報処理の研究をしていました。昨年の 4 月に NICT に入所し、引き続き量子暗号関係、特に最近では標準化に関する仕事をしています。今年の 4 月からは、量子 ICT 協創センターのセンター長として、量子 ICT の社会実装の全般も含めてみています。

加藤　私は、大学の頃は物理現象を解析的に解明する数理物理の研究をしていました。2004 年に博士課程修了後企業に移り、将来形になるのが見える理論研究として量子情報に興味を持ち、量子暗号を含めた量子情報研究を継続してきました。その後、2022 年に NICT に入所し、研究の軸足が量子暗号を含めた量子通信に移ってきています。最初の頃は、教科書に載る仕事がしたいなっていうのがあったんですけど、それと世の中に残すっていうのは、ある種両立もできるし、どっちを追いかけてもいいかなと。現在は、量子 ICT 研究室の室長として、量子暗号の理論的なところをフォローしつつ、量子情報処理の研究に対して目配りをするという役割をやらせていただいています。

■現代のインターネット社会とは？

富田　現代は、通信がないと日常生活が成り立たなくなっている、というのがありますね。もともと人間は、目の届く範囲、あるいは声が聞こえる範囲、自分で走っていける範囲、そういったところとの付き合いだけでした。それが、通信を使うことによって、広がりを持つようになりました。そして、さらに、相手の数が増えるようになりました。通信によって、人がつながる環境になり、それが当たり前のものになりました。

加藤　例えば、海外に出張して、インターネットがつながっていれば、何も心配ないというか。でも、インターネットが切れると、一瞬ですべてが止まってしまう。これが全てなんじゃないかなって。それはつまり必要不可欠というか。切り離せない存在ですよね。

富田　みんながつながっているということは、誰がつながっているか分からないし、どのような意図を持っている人がいるか分からないわけですね。そうすると、中には良くない考えを持っている人もいたりして。その良くない人たちを、どのように遮断するか。そのための様々な技術が出てきていますけど、完璧ではないですね。

加藤　そこで、そのようなことを研究するのは良いかなと思っています。普通の通信ではできないことが、量子通信ならできることが理論的に保証されているんですよ。人類として、そういうものを使ってどこまでできるのか突き詰めるというのは価値があると思っています。その新しい地平を見せる対象として、量子通信というものにチャレンジすることは大事だと思いますね。

■情報漏えいのリスクは今後どのようになっていきますか？

富田　情報漏えいが減ることはあり得ないですよね。新しい生成AIモデルは、ソフトウェアの実装の穴を探すことに、非常に長けたものです。実際ネットワークソフトウェアを作っている人たちが試したら、1日に何千、何万と、自分たちのプログラムの欠陥が見つかったんです。正しい使い方で間違い探しをするというのならば良いわけですが、弱点を利用しようとする人は必ずいるわけです。防ぐ技術も進歩していきますが、それをかいくぐって、抜け穴を探して利益を得ようとする人も必ずいます。いたちごっこは永遠に続いて、それがどんどん高度化していくんですよね。

加藤　みんなが使うシステムである以上、悪意がある人がいるというのは避けられない。その上で、どのようにリカバリーしていくかっていうのは、生物の進化に似ていると思っています。欠点を克服して、システムとしてうまく機能するようなものを作っていこうというたゆまない努力が、人間としての成熟度を上げていくんですね。「悪意を持った人が我々を成長させてくれるのだ」くらいの気持ちで、改善していくのが大事かなと思います。

■量子通信のおもしろい点は？

加藤　通信が排他的になるっていうのが、凄く独特なところですね。普通は、送りたかったら、同じ情報を送れるわけですよね。量子通信は、同じ情報を送れないんですよ。実はそれが、量子暗号の安全の起源にもなっているわけです。Aさんに送ろうと思うと、Bさんに送れなくなる。Bさんに送ろうと思うと、Aさんに送れなくなる。こういう状況が生じるのが、量子通信なんです。

富田　量子の世界というのは、“一夫一婦制”です。他の人が割り込めない固いきずなができるということですね。

加藤　他者が割り込もうとするとバレるから、量子暗号通信が成り立つんです。量子情報というのは、情が深いですよね（笑）。

■量子ICT分野でのNICTの強みは何ですか？

加藤　NICTは研究開発から社会実装まで一気通貫でやっています。大学などではある部分に特化したものを研究することが多いですが、NICTはいろんな研究をしている研究者が集まっているので、たくさんの視点を持った研究者とディスカッションできるところが、いちばんの強みだと思います。

■実証実験や社会実装で、印象に残っていることはありますか？

富田　2010年10月の東京QKDネットワーク実験ですね。QKDというのは、量子通信で暗号鍵を共有する仕組みなんですが、これを使った日本で最初の量子暗号のネットワークです。東芝やNEC、海外の研究機関が作った量子暗号装置などもつなげて、都市圏でのネットワークを作って、高速な量子暗号の共有をして、テレビ電話のデモンストレーションを行ったんです。あれが記念碑であり、始まりだったと思いますね。本当に社会のインフラとして、使えるものになっていることを示したというのは良かったです。

加藤　東京QKDネットワークを作った当時は、QKDをフィールド導入できたこと自体すごいことと思われましたし、このコミュニティ内であれば、誰でも知っている状況でした。

富田　その一方で、世界中で開発競争が激しくなってきてますよね。

加藤　そうですね。今では状況も変わってきていて、世界中で量子暗号通信の開発競争が激化しています。自分たちの存在意義をどうやってアピールしていくか、ちゃんと真剣に考える必要があるのかなと思います。

富田　どこに強みがあって、どういうところをちゃんとやっていくか…。

加藤　真摯にコミュニケーションを取ることが重要だと思っていて、「弱みがあるんだけれど、ここを頑張らなくちゃいけないんです」っていう、本音のトークがもっとできるようになるのがすごく大事なんじゃないかな。それが、少なくとも量子暗号においては、物量で圧倒しているカウンターパートがいるので、すぐにやらなきゃいけないんだろうと思います。

■研究段階から実用化に進む上で、どのような壁がありますか？

富田　私の身近なところで言いますと、量子暗号装置の商用化を目指しているんですけれど、それが本当に使えるものである、ということを示す認証制度です。実際使いたいと思っていても、安全かどうか分からないものは使えないと言われているので、認証は大事なところですね。社会の中で量子ICTを使っていってもらう機運をどのように盛り上げていくか、いろんな段階で、やはり必要なことっていうのはたくさんあるかなと。制度的な問題というのは、近い問題としてあると思うし、先を見た時には、技術開発というか、本当に社会で使っていける技術っていうのを考えて作っていくことが必要だと思っています。

加藤　最近思ったことは、例えば、量子暗号装置が、1個100円で売っていたら、みんな買って遊ぶと思うんですよ。その中で、「あ、なんかこうやって使えるじゃん」って気づいたりするんじゃないかなと。だから、世の中に浸透する1つの方法として、安くする。そのためには、量を作らないと安くはできないので、卵が先かニワトリが先かになっちゃうんですけれど、価格を追求するのも、社会実装において良い戦略なのかなって思うことはありますね。

■量子ICTの未来は？

富田　キーワードとしては、「量子通信の安全性」ですね。数十年以上、数億年以上と言ってもいいんですけれど、安全性を超長期的に担保できる通信ができますっていうのは、我々が今やっている量子暗号の仕事の非常に大きな特徴です。

さらに夢としては、人間の知のフロンティアを広げるっていうのがあって、量子ICTを持ったことによって、新たに広がっていく世界があると思っています。現世的なご利益も必ずあると思っていますし、それが、量子ICTを進めていくモチベーションにもなります。一方、そういった技術を進めていくことによって、更に量子を扱う技術が進んで、まだ見えてない新しい地平が見えてくるという期待もありますね。

加藤　量子ICTの研究が世の中に何を与えるかという観点になると思います。量子ICTは、現代の錬金術だと思うんです。錬金術は当初の目的である「黄金を産み出す」ということには失敗しましたが、その研究は科学の発展には多大な貢献をしました。例えば、量子ICTは量子暗号で役に立つと言われています。しかし、距離の問題や現実的な問題もあり、越えなくていけない課題がある。もしかしたら、それが私たちにとってアンハッピーなことに、役に立たないかもしれない。それでも、やる意味があると思っています。量子ICTや量子暗号の研究は、人々が扱っていなかったものをどのように扱えばいいのかということをみんなが必死になってやっているわけですよね。これは、「人類のフロンティア」なのです。その知識によって、後に築かれる世界が来る。つまり、未来の人類にとってのレガシーを与えるものになると思うんです。それを作れる環境にあるのだから、ちゃんと作っているのか振り返りながら研究するということが大事なのかなと思いますね。

――本日はありがとうございました。

単一光子間の和周波発生を用いた量子もつれ交換

単一光子間の非線形相互作用を利用した光量子情報処理に向けて

逢本 吉朗
（つじもと よしあき）
未来ICT研究所
小金井フロンティア研究センター
量子ICT研究室
研究マネージャー

大学院修了後、2017年にNICT入所。量子もつれ光子対源の開発と、それを用いた量子プロトコルの提案及び実証に関する研究に従事。博士（理学）。

量子ICTの実現には、光子同士の相互作用を自在に制御し、「量子もつれ」状態を高度に操作する技術が不可欠です。量子もつれとは、古典物理学では説明できない量子力学特有の相関を指します。これまで、光子同士の相互作用に基づく量子操作は、量子干渉を利用することで間接的に実現されてきました。一方で、複数の光が相互作用して新たな周波数の光を生み出す「非線形光学効果」を単一光子レベルで実現できれば、光子同士を直接相互作用させることが可能になります。これにより、量子情報処理システムの高機能化や小型化につながると期待されています。本記事では、私たちが世界で初めて単一光子間の非線形光学効果を量子操作に応用した研究成果について紹介します。

■背景

量子ICTでは、単一量子ビットに対する操作だけでなく、複数の量子ビットにまたがった量子操作を実行することが重要な基盤技術となります。光子を用いた量子ICTでは、これまで2つの光子間の量子干渉（二光子干渉）を利用してこのような操作を実現してきました。この二光子干渉では、図1(a)に示すように、半透鏡（透過率＝反射率＝1/2）の2つの入力ポートにそれぞれ1光子を入射させます。入力された2つの光子が互いに識別できる場合は、一方の出力ポートに2光子が出力される確率と、両方の出力ポートに1光子ずつが出力される確率は、それぞれ1/2となります。一方、2つの光子が全く識別できない場合には、光子同士の量子干渉によって後者の事象が起こらなくなります。二光子干渉を利用した代表的な量子通信プロトコルとして挙げられるのが量子もつれ交換です。このプロトコルでは2組の量子もつれ光子対を連結することで、元々相関のなかった2つの光子間に量子もつれを生成することが可能です。具体的には、それぞれの量子もつれ光子対から1光子ずつを取り出し、二光子干渉を利用した「ベル測定」と呼ばれる2量子ビットの測定を行います。この測定によって、元々は別々の光子対に属していた残りの2光子の間に、新たな量子もつれが生成されます。しかし、量子もつれ光子対の生成は一般に確率的であり、ここに大きな課題が生じます。すなわち、図1(b)でA1-A2とB1-B2にそれぞれ1ペアずつ量子もつれ光子対が生成される成功の事象だけでなく、A1-A2に2ペアが生成されB1-B2には光子のペアが生成されないといった失敗の事象も同じ確率で発生します。ところが、二光子干渉に基づくベル測定ではこれらの成功と失敗を区別することができません。そこで、量子もつれ交換が成功したことを確かめるため、A1とB2でそれぞれ1光子が来たことを検出する必要がありますが、検出と同時に光子が壊れてしまうため量子もつれ交換後の光子を有効活用できませんでした。

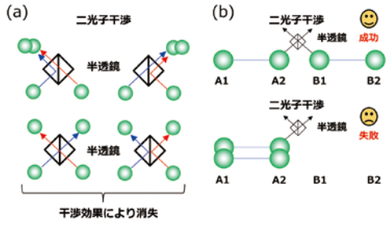


図1　(a)二光子干渉の概念図
(b)従来型の二光子干渉による量子もつれ交換

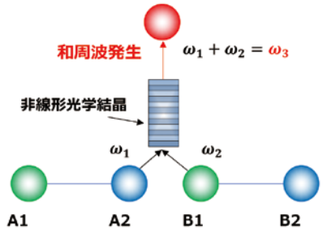


図2　単一光子間の和周波発生による量子もつれ交換

■単一光子の非線形光学効果

この問題を回避する方法として、二光子干渉ではなく、非線形光学効果の1つである和周波発生を単一光子レベルで利用することでベル測定を行う方法が理論的に提案されています（図2）。ここで、和周波発生とは、異なる周波数を持つ2本のレーザー光を非線形光学結晶に入力すると、それらの和の周波数を持つ新たな光が生成される現象です。本手法では、図2に示すように、光子A2とB1を互いに異なる周波数で準備し、両者を非線形光学結晶に入力します。すると、両方の光子が存在する場合に限り、それらの和の周波数を持つ光子が生成されます。この和周波光子を検出することでベル測定が行えます。この方法の利点は、A1-A2に2ペアが生成され、B1-B2には光子のペアが生成されないような望ましくない事象では和周波光子が発生しません。したがって、従来手法で区別できなかった失敗の事象を、ベル測定の段階で除去することができます。その結果、ベル測定が成功した時には必ず量子もつれ光子対が得られることになり、光子対を破壊する必要がなくなります。この特長は、ループホールのないベル不等式破れの検証*や、装置無依存量子鍵配送の長距離化に向けて大きな利点となります。しかし、このような単一光子間の和周波発生は2014年に初めて実験例が報告されたものの、観測された和周波光子の信号は極めて微弱であり、ほぼノイズに埋もれていました。以上の背景から、量子もつれ交換への応用を実現するには和周波光子の信号SN比（信号対雑音比）を大幅に向上させる必要がありました。

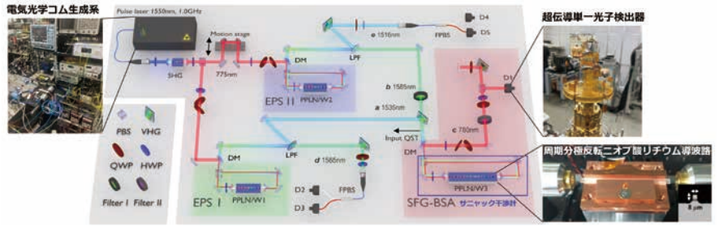


図3　単一光子間の和周波発生による量子もつれ交換の実験。EPS IとEPS IIで量子もつれ光子対を1対ずつ生成し、SFG-BSAで単一光子間の和周波発生を用いた量子ゲート操作を行う。

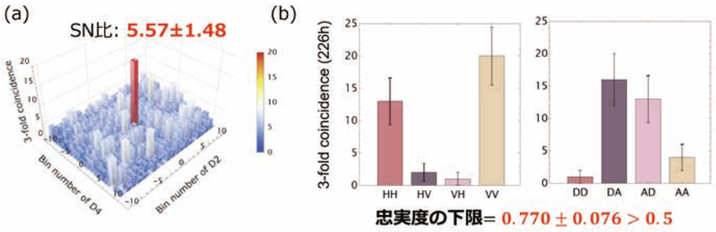


図4　(a)和周波光子の検出信号。(b)量子もつれ交換完了後の二光子の偏光相関。H、V、D、Aはそれぞれ横、縦、右斜め45度、左斜め45度偏光を表す。

■SN比改善と量子もつれ交換への応用

本研究では、NICTの持つ最先端技術を組み合わせて実験系を構築し（図3）、世界で初めて単一光子間の和周波発生を用いた量子もつれ交換に成功しました。本実験では、まず量子もつれ光子対を2ペア生成し、次に各光子対の片方を周期分極反転ニオブ酸リチウム（Periodically Poled $LiNbO_3$: PPLN）導波路へ入力して和周波光子を発生させます。最後に和周波光子を超伝導単一光子検出器（SSPD）で検出すると、残された光子の間に量子もつれが形成されて量子もつれ交換が完了します。この実験では次の独自技術を開発しました。まず、非線形光学効率を最大化するため、結晶長63 mmの長尺PPLN導波路を製作し、それをサニャック干渉計内に配置することで2量子ビット操作を実現しました。生成された和周波光子は暗計数0.15 Hzという低ノイズのSSPDで検出します。さらに、電気光学コムという装置を用いて、今回の実験に最適化した1 GHzの高速クロックで量子もつれ光子対の励起（れいき）光を発生させました。以上の技術により、先行研究と比較して約1桁近く高い和周波検出の信号SN比を達成しました（図4(a)）。図4(b)に、量子もつれ交換で得られた光子対の偏光相関を示します。この実験データのコントラストの平均値から最大量子もつれ状態との忠実度の下限を推定すると0.770±0.076となりました。この値から、単一光子間の非線形効果を用いた量子ゲート操作が初めて実現したことを確認できました。今回得られた結果は光量子情報処理における大きな一歩であり、将来的にはオンデマンドに量子もつれ光子対を生成するための鍵になる技術となることが期待されます。

■今後の展望

本手法を量子もつれ交換よりもさらに高度な量子情報プロトコルへ応用するには、更なるSN比の改善が必要であると予想しています。例えば、本研究で行ったシミュレーションによれば、ループホールのないベル不等式破れの検証では少なくとも更に3倍程度、また装置無依存量子鍵配送では50倍程度の非線形効果の改善が必要であると見込まれます。

今後は、非線形光学効果の増強を実現させ、光量子計算回路の小型・効率化や次世代量子鍵配送の長距離化につなげていきたいと考えています。

＊　量子もつれ光子対の相関を測定すると局所性・実在性を仮定して成立するベル不等式が破れる。しかし、生成された量子もつれ光子対のごく一部分しか検出されない場合には、「検出されなかった光子対も考慮するとベル不等式が破れていない」という可能性を排除できなくなる（検出効率のループホール）。和周波光子を検出した下では、このループホールを塞いだ検証実験が可能となる。

衛星量子暗号実現に向けて

国際宇宙ステーション(ISS)と地上局とでの暗号鍵共有実験

藤原 幹生
（ふじわら みきお）
量子ICT協創センター
主管研究員
1992年、通信総合研究所（現NICT）入所。遠赤外検出器、量子鍵配送、量子セキュアクラウドの研究開発に従事。博士（理学）。

小澤 俊介
（おざわ しゅんすけ）
未来ICT研究所
小金井フロンティア研究センター
量子ICT研究室
主任研究員
博士号取得後、東京大学、早稲田大学にて高エネルギー宇宙線の観測研究に従事。2019年 NICT着任後は衛星量子鍵配送の研究開発に従事。博士（工学）。

量子コンピュータの開発が世界各国で精力的に進められています。量子コンピュータには従来のスーパーコンピュータで数千年かかるような極めて複雑な計算を短時間で処理できる可能性があります。この演算能力により、新薬開発の加速、物流・発電の最適化、高度な金融リスク分析など幅広い分野での革新的な効用が期待されています。その一方で、我々がインターネットで利用している暗号が量子コンピュータによって瞬時に解読されることが懸念され、それ故量子コンピュータが完成した後も安全な通信を実現できる技術が求められています。量子暗号は有力な技術の1つであり、グローバル展開できるよう衛星搭載化に向けた研究開発を進めています。

■量子コンピュータと量子暗号

量子技術とは光子、電子、原子など極めて小さな物質が示す特有の性質（重ね合わせや量子もつれなど）を利用し、従来の技術を遥かに超える超高速計算、超高感度計測、完全秘匿通信などを実現するための技術です。近年、複数の状態を同時に重ね合わせて表現できる量子の特性を利用し、膨大な組み合わせの中から最適な解を瞬時に計算する量子コンピュータの開発が世界各国で行われています。量子コンピュータの開発には国家プロジェクトのほか、巨大な資本をもつ企業もしのぎを削っており、将来、創薬・材料開発・物流最適化などへ応用されることが期待されます。

しかし、量子コンピュータのインパクトはこれらだけではありません。我々が日々利用しているインターネットの通信の秘匿化に使われている暗号も瞬時に解読できるようになります。仮に今解読できなくてもそのデータを蓄積しておき、量子コンピュータが完成した後で解読するというシナリオが考えられます。現在のインターネットではゲノムデータのような超長期に秘匿性を必要とするデータの伝送も行われており、量子コンピュータの出現にともなう情報漏えいに対抗する方法が今まさに必要とされています。今データをためておいて、後から解読する攻撃方法はハーベスト攻撃と呼ばれており、世界各国でその対策が急がれています。ハーベスト攻撃の特効薬として、盗聴を必ず検知でき、離れた2者間で盗聴されることのない安全な暗号鍵の共有を可能とする量子鍵配送(Quantum Key Distribution: QKD)と送りたい情報1ビットごとに暗号鍵をかけるVernam's one time pad暗号(OTP)を組み合わせることで、将来どんなコンピュータが出現しても解読することができない、量子暗号が挙げられます。現在、様々な国でQKD装置の研究やインフラ導入に向けた社会実装が進んでいます。

■NICTが先導した東京QKDネットワーク

我が国でも量子暗号の研究をNICTが中心となって2000年代前半から開始してい

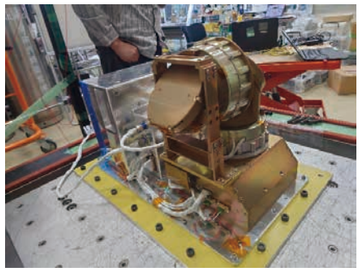


図1　ISSに搭載した物理レイヤ暗号用光源と潜望鏡式望遠鏡（SeCRETS）

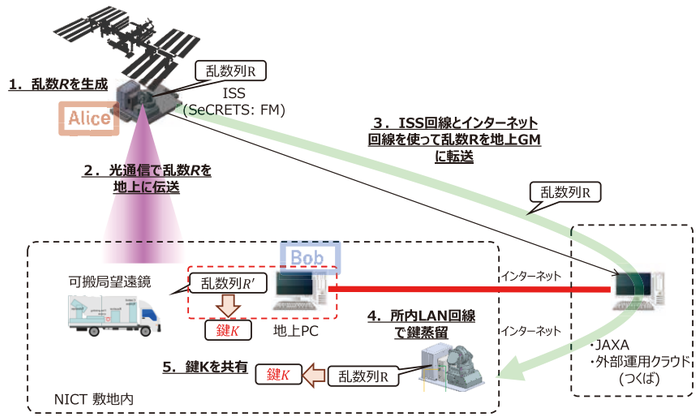


図2　ISS-可搬型光地上局間の物理レイヤ暗号通信実験の全体構成図

図3　可搬型光地上局

ます。2010年には、NICTはQKDリンクをネットワーク化した東京QKDネットワークの運用を開始し、現在に至るまで運用を続けています。我々が知る限り世界で最も運用の長いネットワークとなっており、様々な企業・官庁との社会実装実験を進め、先端的なアプリケーションの開発に成功しています。

また、QKD装置を衛星に載せることで、安全な鍵共有をグローバルスケールで実現することが可能になります。

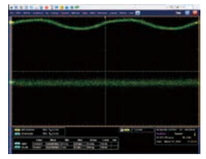
■世界の衛星量子暗号開発状況

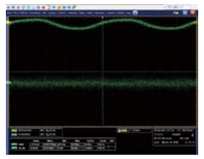
世界でも開発が進められている衛星量子暗号ですが、当初は中国が先行しました。2017年に世界初の量子暗号衛星（Micius）を打上げ、12,000 kmを超える距離での安全な鍵共有に成功しています。

一方、日本では、2018年より衛星搭載用QKD装置の開発を開始し、小型衛星搭載を想定したQKD送信機の開発と8トントラックに搭載可能な可搬型光地上局の開発を進めました。開発費の制限から独自の衛星の打ち上げは不可能でしたが、国際宇宙ステーション(ISS)と地上局との間での光伝送に向けた開発を進めました。この装置では通常のQKDのほか、衛星–地上間での通信のように、見通しのきく通信路を用いた通信であることを活かし、QKDよりもより効率的に安全な鍵生成が可能となる物理レイヤ暗号の実装も進めました。QKDでは光子の伝送路に量子メモリや量子コンピュータなどあらゆる物理操作を許したとしても安全な暗号鍵の共有を可能です。また、衛星–地上間などの通信では伝送路内に強力な盗聴者がいないことを他の方法で確認することが可能です。例えば北アメリカ航空宇宙防衛司令部（NORAD）は、24時間365日レーダーや人工衛星を用いて北米周辺の宇宙空間や空域を監視しています。その能力は10 cm以上の物体を見つけることが可能といわれています。また衛星との通信路を望遠鏡などで監視することも可能です。こういった“通信路には強力な盗聴者はいない”を受け入れられる場合、盗聴としては衛星–地上間での光ビームも漏れ光を受信することを想定することになります。漏れ光からの漏えい情報量の上限を見積もり、その分の情報を捨てることで安全な暗号鍵を得ることができます。NICTではこの物理レイヤ暗号をISSと地上局との間で実施するため、SONY CSL、スカパーJSAT、次世代宇宙技術研究組合と共に物理レイヤ暗号用光源や暗号鍵生成用の処理装置及び可搬型地上局の開発を行いました。図1はISSに搭載した光源（SeCuReIasEr communicaTionS terminal for LEO, SeCRETS）の写真です。潜望鏡型望遠鏡は半球のどこでも光軸を向けることが可能です。この装置をISSの中型曝露実験アダプタ(i-SEEP)に取り付け、宇宙空間で動作させました。図2には実験全体のコンセプトを示しています。10 GHzクロックの

可搬局望遠鏡ガイドカメラによる撮像

精追尾光学系カメラによる撮像とQDによるビーコン検知





10GHzクロックの微弱信号をキャッチ → 誤り訂正・秘匿性増強を経て安全な鍵共有に成功

図4　ISSからの受信信号

作動DPSK（差動位相偏移変調）信号が送信機から射出され、8トントラックに搭載された直径35 cmの反射型望遠鏡で受信します。図3に地上局の写真、図4に受信した信号波形を示します。この受信信号に対し、誤り訂正や秘匿性増強（安全な暗号鍵を抽出するプロセス）を行い、2024年に1回の上空通過で100万ビット以上の安全な暗号鍵の生成に成功し、ISSとのOTP暗号通信にも成功しました。

■将来の展望

この経験を基に宇宙戦略基金に応募し、NICTが代表機関となって『情報理論的安全な鍵共有を可能とする小型・低軌道衛星の研究開発』を推進しています。N-QUADISと命名した我が国初の量子鍵配送衛星は2029年打ち上げ予定です。この衛星を用いて安全な鍵共有をグローバルスケールで実現するための技術実証を成功させるため、日々研究開発に勤しんでいます。

外部からの磁場がいらない、新型「超伝導磁束量子ビット」の実証

ゼロ磁場で動く！未来の量子コンピュータを小さくする新技術

金 鮮美
（きむ そんみ）

未来ICT研究所
小金井フロンティア研究センター
量子ICT研究室
主任研究員

大学院修了後、物質材料研究機構と大阪大学の博士研究員、東京大学生産技術研究所特任助教を経て、2018年にNICTに入所。超伝導量子ビットに関する研究に従事。博士（理学）。

現在のコンピュータでは何年もかかるような複雑な計算を、一瞬で解くことができると期待されているのが「量子コンピュータ」です。新しい薬の開発や、これまでにない便利な材料の設計など、未来の科学技術に欠かせないものとして世界中で研究が進んでいます。その心臓部として情報のやり取りを行うのが「量子ビット」という素子です。NICTをはじめとする共同研究チームは、これまで動かすために磁力が必要だった「超伝導磁束量子ビット」を、磁力を全く加えない「ゼロ磁場」で最適に動かすことに世界で初めて成功しました。量子コンピュータの小型化や大規模化へ向けた、大きな一歩をご紹介します。

■背景

量子コンピュータという「未来の計算システム」を動かすために、絶対になくてはならない「情報を処理する最小の部品（単位）」が量子ビットです。量子ビットの素子としては、これまで、極低温に冷やすことで電気抵抗がゼロになる「超伝導」という現象を利用した「超伝導量子ビット」が主流でした。しかし、現在広く使われているタイプは「エネルギー準位の間隔の差（非調和性という）」が小さいため、たくさんの量子ビットを並べると、お互いの周波数がぶつかり合って誤動作してしまうという懸念（周波数衝突）がありました。

一方、超伝導電流の回る向きで情報を表す「超伝導磁束量子ビット」では、周波数衝突の問題を緩和することができます。しかし、超伝導磁束量子ビットを正しく動かすためには、外部のコイルを使って、常に「半磁束量子」と呼ばれる特定の強さの磁場をかけ続けなければならないという別の課題がありました。磁場を作るための部品やかさばるコントロール配線が必要なため、たくさんの量子ビットを詰め込んでコンピュータを大規模化していく上での高い壁になっていたのです。

■磁場がいらない秘密は「強磁性体」のミクロな仕掛け

そこでNICTの研究チームが注目したのが、超伝導回路に電流を生じさせる量子状態の位相差をπ（180度）反転させることができる特殊な接合（π接合）を組み込む方法です（図1(a)）。この接合には、磁石の性質を持つ強磁性体「PdNi（パラジウムニッケル）」の薄い膜を、超伝導体で挟み込んだ構造が使われています。

本来、磁束量子ビットで「右回り電流（0状態）」と「左回り電流（1状態）」がきれいに重なり合った最適動作点（ノイズに強い理想的な状態）を作るためには、外部磁場による調整が不可欠でした。従来の磁束量子ビットでは、外側の大きなコイルから正確に半磁束量子に該当する磁場を加えることでこの状態を実現していましたが、今回開発した新型ビットでは、薄い強磁性体が超伝導体接合の量子状態にπの位相差を生じさせることで、半磁束量子の磁場と同じ役割を果たします。そのため、外からの磁場がゼロの状態でも、自発的に最適動作点に達する回路が実現し、かさばるコイルや複雑な配線を一切なくすことに成功したのです。

■窒化物の技術を組み合わせて「寿命」を伸ばす

実は、回路に磁石の性質を組み込んで磁場を不要にする試みは、これまでにも海外で行われていました。しかし、これはπ接合を持つ位相量子ビットでその寿命がわずか4ナノ秒（ナノ秒は1秒の10億分の1）程度と極めて短く、計算を行う前に状態が壊れてしまうため実用的な動作には至っていませんでした。これはπ接合の影響よりも、位相量子ビット自体のコヒーレンス時間がナノ秒オーダーで短いからでした。

今回の研究では、NICTが長年培ってきた「窒化ニオブ（NbN）」という特別な超伝導体を用いてシリコン基板上にきれいな結晶を作る技術と、NTTが持つ長寿命な量子ビットの設計・測定技術、そして東北大学や名古屋大学が持つ強磁性体薄膜π接合の技術を融合しました。特に、NICTが結晶成長技術によって開発したNbNベースの超伝導接合（図1(b)）は、未来の量子コンピュータ実現に向けた高い潜在能力を秘めています。この接合は、一般的な量子ビット材料であるアルミニウムに比べて超伝導転移温度が一桁高いという特徴があります。さらに、超伝導エネルギーギャップが大きいため、熱的なノイズ（熱揺らぎ）の影響を受けにくく、量子ビットの寿命を飛躍的に向上させることが期待されています。なお、実際に作製された磁束量子ビットは非常に微細であり、光学顕微鏡等を用いてその構造が観察できます（図1(c)）。

ノイズを徹底的に抑えるために強磁性体の材料を一から見直して最適な回路デザインを構築した結果、ゼロ磁場で磁束量子ビットが最適動作点を表すマイクロ波分光スペクトラムを観測し（図2(a)）、従来のπ接合をもつ位相量子ビットと比べて寿命を約360倍（1.45マイクロ秒（マイクロ秒は1秒の100万分の1））も伸ばすことに成功しました（図2(b)）。これにより、ゼロ磁場で動作する磁束量子ビットを世界で初めて実証したのです。

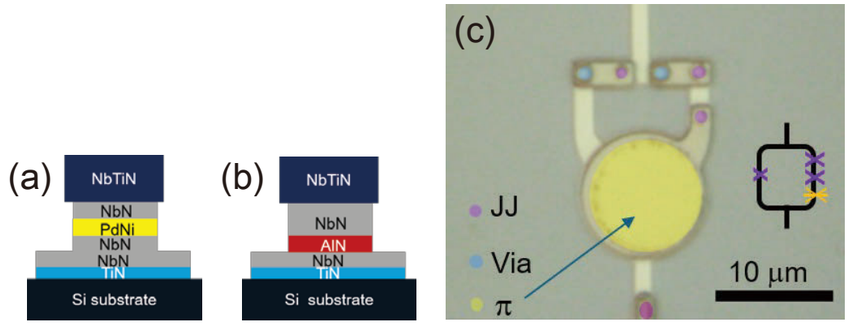


図1 （a）強磁性体（PdNi）の厚みを最適化した、全窒化物超伝導π接合（NbN/PdNi/NbN）の断面概略図。（b）磁束量子ビットの基本接合として用いられる、全窒化物接合（NbN/AlN/Nb）の断面概略図。（c）実際に作製したπ接合（π）を有する窒化物磁束量子ビットの光学顕微鏡写真。

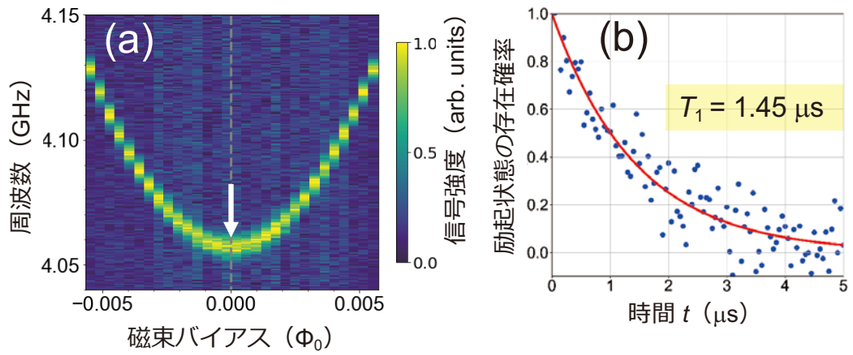


図2 （a）π接合を持つ窒化物で作製した磁束量子ビットにおける、基底状態から励起状態への遷移周波数の磁場依存性を表すマイクロ波分光スペクトラム。矢印は最適動作点を表している。(b) エネルギー緩和時間T_1＝1.45 μsを示すコヒーレンス時間の測定結果。T_1の値は励起状態存在確率Pの指数関数的な減衰関係式（$P=e^{-t/T1}$）を用いてフィッティングにより算出された。これは従来のπ接合を用いた位相量子ビットの研究報告と比較して、約360倍も長いコヒーレンス時間に相当する。

今後は、更に量子ビットの寿命を伸ばすためのプロセス最適化を進めるとともに、将来的な大量生産を見据えて、素子の性能を均一に揃える製造技術の向上に取り組みます。従来のアルミニウムをベースとした量子ビットの性能を凌駕（りょうが）する、新しい量子ハードウェアのプラットフォームを構築することで、将来的には私たちの生活を陰で支える量子コンピュータが、より身近なものとして社会へ普及していくことが期待されます。

■将来の展望

今回の成果は、外部磁場を必要としない新型の磁束量子ビットを世界で初めて実現したものです。これにより、量子コンピュータの心臓部にあたる回路の大幅な簡素化や微細化・省エネ化が可能となり、将来のチップ大規模集積化へ向けた強固な基盤が整いました。

量子暗号ネットワークの社会実装実験

将来にわたって安全な通信を実現する

富田 章久
（とみた あきひさ）
量子ICT協創センター
研究センター長
大学院修了後、企業研究所、大学教員を経て、2025年にNICTに入所。量子情報技術、光量子情報処理、量子暗号などに関する研究に従事。博士（工学）。

技術の進歩により現在の暗号は将来解読される恐れがあり、長期的に安全が保証できる暗号が必要です。そこで、量子力学に基づく量子鍵配送（QKD）が注目されています。NICTはQKDプラットフォームや量子セキュアクラウドを開発し、実用性を検証してきました。今後は耐量子暗号とのハイブリッド化や衛星QKD、量子中継を含む量子インターネットの実現が期待されます。

■背景

現代の社会では離れた人々の間でも様々な情報がやり取りされます。情報のやり取りへの信頼を支えているのが暗号です。暗号では情報を取り出すための鍵が「カギ」となります。鍵は予測不能な乱数列であり、他人に知られないようにします。現在広く使われている暗号では、鍵は強力なコンピュータでも解くのが難しい計算問題の答えで与えられます。このような意味での解読不可能な暗号を計算量的安全といいます。ところが、効率的な解法の発見や、コンピュータの性能向上があると問題が解かれてしまいます。このため、暗号は20から30年を寿命として、世代交代します。現在安全な暗号でも、数十年後には解かれる恐れがあり、暗号化された情報を傍受して保管しておき、後になって解読する盗聴戦略であるHarvest Now, Decrypt Later（HDNL）攻撃を受ける可能性があります。

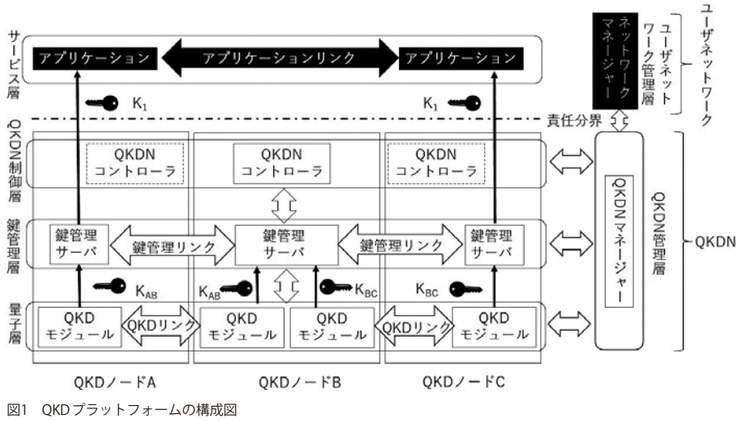


図1　QKDプラットフォームの構成図

■長期安全な暗号を求めて

今から30年ほど前に現在の暗号で使われている計算問題は量子コンピュータで容易に解けることが発見されました。量子コンピュータ開発は最近急速に進展し、2030年には暗号が破られるという予想すらされています。そこで、量子コンピュータにも効率的に解けない問題を使った暗号（耐量子暗号）の研究開発が進められ、アメリカでは政府が推奨するアルゴリズムの選定が進んでいます。ところが、耐量子暗号にも寿命があるのでHNDL攻撃のため、長期間の安全性を保証することはできません。

盗聴者が得る情報量を原理的に制限することで安全性を確保することも可能で、これを情報理論的安全といいます。この方法によれば、技術が進歩しても長期間の安全性が保証されます。しかし、情報理論的安全な暗号は、送受信者の間で共通の鍵を大量に使うため、鍵を効率的かつ安全に共有する方法が必要です。量子鍵配送(QKD)はその1つで、情報理論的安全な暗号とQKDを組み合わせた暗号を総称して量子暗号と呼んでいます。

QKDの安全性は量子力学の法則に基づいています。盗聴者は鍵の情報を得るために量子状態の測定を行いますが、特定の正しい方法で測定を行わない限り状態が変化します。そのため、盗聴すると受信した結果に誤りが現れ、その数から盗聴された情報量がわかります。元の測定結果から盗聴された分を差し引いたものを鍵とすると、盗聴者が情報を持たない鍵を共有できます。

■量子鍵配送プラットフォーム

QKDでは送受信者2人の間で秘密鍵の共有ができるだけなので、鍵共有量の制御、鍵の管理、アプリケーションへの鍵の配分といった機能が必要です。このため、NICTではQKDプラットフォームを開発しました。図1のようにQKDで鍵を共有する量子層、秘密鍵を必要なところに分配する鍵管理層、量子層と鍵管理層にあるノードに指令する制御層の3層からなり、さらにアプリケーション層にあるデバイス群で鍵を受け取って利用します。QKDを使った鍵の生成と分配は下の3層で行われるので、最上層では量子を使っていることを意識せずにアプリケーションの開発や実行をすることができます。2010年に作られた東京QKDネットワークは都市圏でのQKDプラットフォームとして世界で最も長い期間の運用実績があり、ドローン、スマートフォン、ネットワークスイッチなど様々なIT機器に鍵を供給して秘匿通信を行うことに成功しています。

さらに、データの保管や計算処理を行うために秘密分散が使われます。秘密分散は情報をいくつかのデータサーバに分けて保管します。サーバが攻撃されても他の大多数のサーバが無事であれば秘密が保たれます。また、一部のサーバが災害などでダウンしてもデータを復元することができます。秘密分散は情報理論的安全ですが、データをユーザやサーバの間でやり取りするときの秘匿性はありません。量子暗号と組み合わせることで情報理論的安全なデータ伝送・保管・処理ができるようになります。NICTはこのようなシステムを量子セキュアクラウドとして世界に先駆けて提案・実証しました。国内各社と協力して、ゲノムデータを保管し、ゲノム解析センターと病院の間でデータを量子暗号で伝送するシステムや、顔認証に使う特徴データを秘匿化して伝送するシステム、電子カルテのデータをQKD鍵で暗号化し、分散化したバックアップシステムからネットワーク経由で安全な伝送を行うシステムなどの実証実験が行われています。また、量子コンピュータと量子セキュアクラウドを結合する試みにも成功しています。ユーザは量子セキュアクラウドに保管されているデータを量子コンピュータに送り、そこで解析された結果を受け取ります。やり取りされる貴重なデータは量子暗号を使うことで保護することができます。このように、量子セキュアクラウドはHNDL攻撃に対抗して数十年以上の間秘密を保持することが必要な情報を扱う医療・防衛・金融・行政や産業基盤への応用が期待されています（図2）。

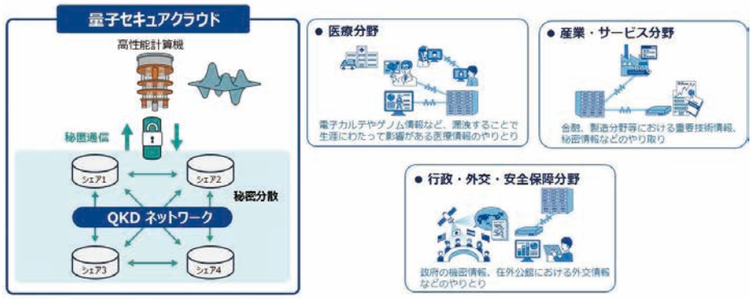


図2　量子セキュアクラウドと応用分野

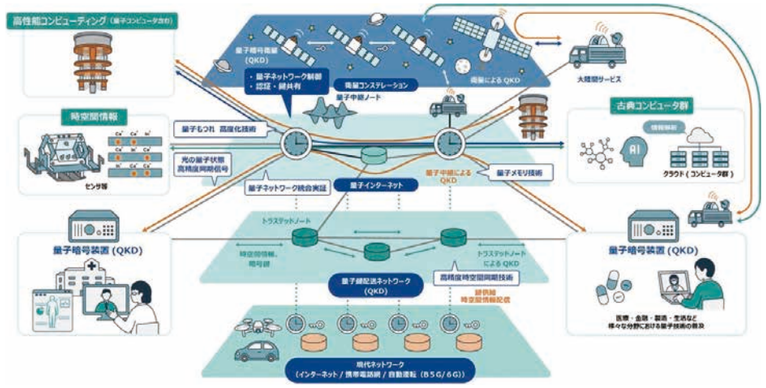


図3　量子インターネットの将来図

■将来の展望

量子暗号は耐量子暗号に比べるとコストが高く、応用範囲も限られています。耐量子暗号と量子暗号の長所を生かしたハイブリッド暗号システムを開発し、社会インフラとして整備していくことが必要です。また，グローバルなネットワークに向けて人工衛星を用いた量子鍵配送との統合や将来に向けた量子中継技術の研究開発も重要となります。量子暗号技術と現代暗号技術、量子コンピュータ、量子センサ、光や無線の通信ネットワークなどが融合された量子インターネットの実現が期待されます（図3）。

超わかりやすい!!

「アニメで学ぼう！量子の世界」を公開中！

量子 ICT 協創センター 総合企画室 主任　安井 由莉

NICT では、量子を分かりやすく説明したアニメーション動画「アニメで学ぼう！量子の世界」を、公式 YouTube チャンネルで公開しています。

近年、量子コンピューターや量子暗号通信といった言葉をニュースで目にする機会が増えています。これらの技術は、次世代の情報処理や通信技術を支えるものとして世界中で研究開発が進められています。しかし、「そもそも量子って何だろう？」と疑問に感じている方も多いのではないでしょうか。

この動画は、量子 ICT 協創センターと量子 ICT 研究室が共同で制作したもので、「量子とは何か」を直感的に理解していただくことを目的としています。舞台は近未来の理科室や研究室。研究者の陽子先生と高校生のそら、ナミが会話を交わしながら、量子の基本的な考え方や、NICT が取り組む量子の分野の研究について分かりやすく紹介しています。

アニメーションならではの表現手法によって、目に見えない量子の不思議な性質を楽しく学ぶことができます。量子に興味がある方はもちろん、量子について初めて学ぶ方にも親しみやすい内容となっています。

また、アニメーションに登場する陽子先生の声は、人気声優の茅野 愛衣（かやの あい）さんが担当しています。キャラクターたちによる会話を通して、量子の世界を身近に感じていただけます。

量子力学が誕生して今年で 101 年、量子の世界はまだまだ始まったばかりです。

この動画が、未来を支える量子への興味や理解を深めるきっかけとなれば幸いです。

ぜひ NICT 公式 YouTube チャンネルで、「アニメで学ぼう！量子の世界」を観て、ちょっと不思議な量子の世界をのぞいてみてください。

NICT 公式 YouTube チャンネルで、「アニメで学ぼう！量子の世界」
URL: https://www.youtube.com/watch?v=2dJyYo2H9Pw

衛星量子鍵配送の高信頼化・高効率化に向けた基盤技術の研究開発

川島 輝能
（かわしま てるよし）

未来 ICT 研究所
小金井フロンティア研究センター
量子 ICT 研究室
テニュアトラック研究員
博士（理学）

●経歴
1998 年　千葉県にて誕生
2021 年　慶應義塾大学理工学部物理学科卒業
2026 年　東京大学大学院博士課程修了後、NICT 入所、現職

●受賞歴等
2022 年　日本物理学会 2022年秋季大会 学生優秀発表賞

一問一答

Q 研究者になってよかったことは？
A 幼い頃から研究者に憧れていたため、これから研究に従事できることを率直に嬉しく思います。特に NICT では、自分の関心を深めつつ、その成果を社会に還元できる点にやりがいを感じています。

Q 最近はまっていること
A 昼食後に量子 ICT 研究室のメンバーと NICT の敷地内を散歩し、植物や昆虫を観察しています。写真は、土中の菌や樹木との関係で育つ、移植が難しい希少なキンランという植物です。

Q 休日の過ごし方は？
A 休日はジムで体を動かしたり、ラーメンなど近場のグルメを開拓したりしています。旅行や音楽ライブに行くこともあります。写真は家族と back number のライブに行った時のものです。

私は大学院で、高エネルギー宇宙線を観測する空気シャワー実験に参加し、光検出器の開発とデータ解析に携わりました。検出器開発では、光電子増倍管の読み出し回路を改良し、広い強度範囲の信号を測定できる検出器システムを開発しました。また、観測データから宇宙線の到来方向分布を解析し、その異方性を調べる研究にも取り組みました。

今後は、検出器開発の経験や宇宙線研究で得た知見を活かし、衛星を用いた量子鍵配送（QKD）の実用化に向けた研究に取り組みます。

量子 ICT 研究室では、衛星－地上間の光通信技術により、QKD の地上ファイバー網をグローバルに拡張する取組を進めています。衛星搭載機器には、宇宙環境への耐性に加え、小型・軽量・低消費電力化が求められます。QKD には偏光変調を軸とした伝送プロトコルを用いるため、衛星搭載用の暗号装置は、特殊な干渉器や LN 変調器などで構成されます。

そこで私は、それらを機能統合し、小型・省電力で、衛星軌道上でも安定動作する QKD 送信機を開発したいと考えています。

一方で、衛星搭載機器が量子通信として安全性を持つかは、社会実装に向けた重要な課題です。QKD の送信系機器には、送信する光子の「独立同一分布性」が求められますが、ビット列や光信号の偏り、相関、時間的揺らぎを測定・解析する標準的手法は確立されていません。そのため、衛星搭載機器のみならず、地上 QKD にも係る安全性検証が求められています。この課題は送信機開発にも密接に関わるため、同時に推進したいと考えています。これにより、QKD 機器の信頼性・安全性を高め、実用的な衛星量子通信システムの実現に貢献することを目指します。

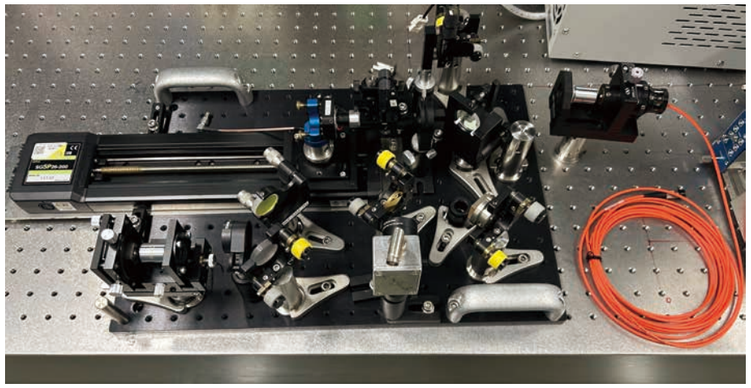


図　QKD の安全性検証に向けて、ビット間の相関の有無を評価するための光学系（1ビット遅延干渉計）を構築中

CEATEC Innovation for All 2026

会　期
2026年10月13日(火)－16日(金)　10:00～17:00

入場無料（登録入場制）

会場：幕張メッセ

https://ceatec.com/ja/

X（Transformation）パーク　ホール6

- NICTが描く2030年代の未来社会 ――「強靭な社会」「デジタル安全社会」「持続可能で活力のある社会」「人間中心のAI社会」の実現に向けたAI・コミュニケーション、Beyond 5G、量子情報通信、サイバーセキュリティなどの研究成果を紹介し、新たな協創と社会実装の促進を目指します。
- 革新的情報通信技術（Beyond 5G（6G））基金事業の研究成果や活用事例を紹介します。

ネクストジェネレーションパーク　ホール4

- 地域発ICTスタートアップの発掘・育成・事業拡大のサポートを行う「NICTアクセラレータ・プログラム」や、その最終成果発表会である「起業家甲子園」「起業家万博」に出場したスタートアップ等を紹介します。

総務大臣賞受賞

ICT mentor platform

NICT ICT Mentor Platform

長年にわたるICTスタートアップ支援活動が評価されました

6月1日「電波の日・情報通信月間記念中央式典」において、「NICT ICT Mentor Platform」として、
令和8年度「情報通信月間」総務大臣表彰をいただきました。
ICTメンターを代表して、田島聡一氏（JVCA代表）が登壇し、林 芳正総務大臣より表彰状を授与されました。
NICTは今後も全国のICTスタートアップを支援してまいります。


6/1「電波の日・情報通信月間記念中央式典」（ホテルニューオータニ）にて

令和8年度

NICTアクセラレータ・プログラム絶賛稼働中！

総務省・NICTでは、地域発ICTスタートアップの創出による地域課題の解決や経済の活性化を目的に、ICT人材の発掘・育成及び地域発ICTスタートアップの事業拡大等のサポートを行っています。
連携大会におけるNICT賞受賞者は、起業家甲子園・万博出場を目指します！

STEP 01 発掘フェーズ　各地域で連携大会を開催

STEP 02 育成フェーズ　ICTメンターによるブラッシュアップ

STEP 03 事業化支援・拡大フェーズ　全国大会「起業家甲子園」「起業家万博」の開催

連携大会一覧はコチラ▼

公式SNSはコチラ▼

NICT NEWS 2026 No.5 通巻519
編集発行：国立研究開発法人情報通信研究機構 広報部
発行日：令和8年（2026年）9月（隔月刊）

〒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: https://www.nict.go.jp/
@NICT_Publicity
#NICT

ISSN 1349-3531 (Print)
ISSN 2187-4042 (Online)

〈再生紙を使用〉