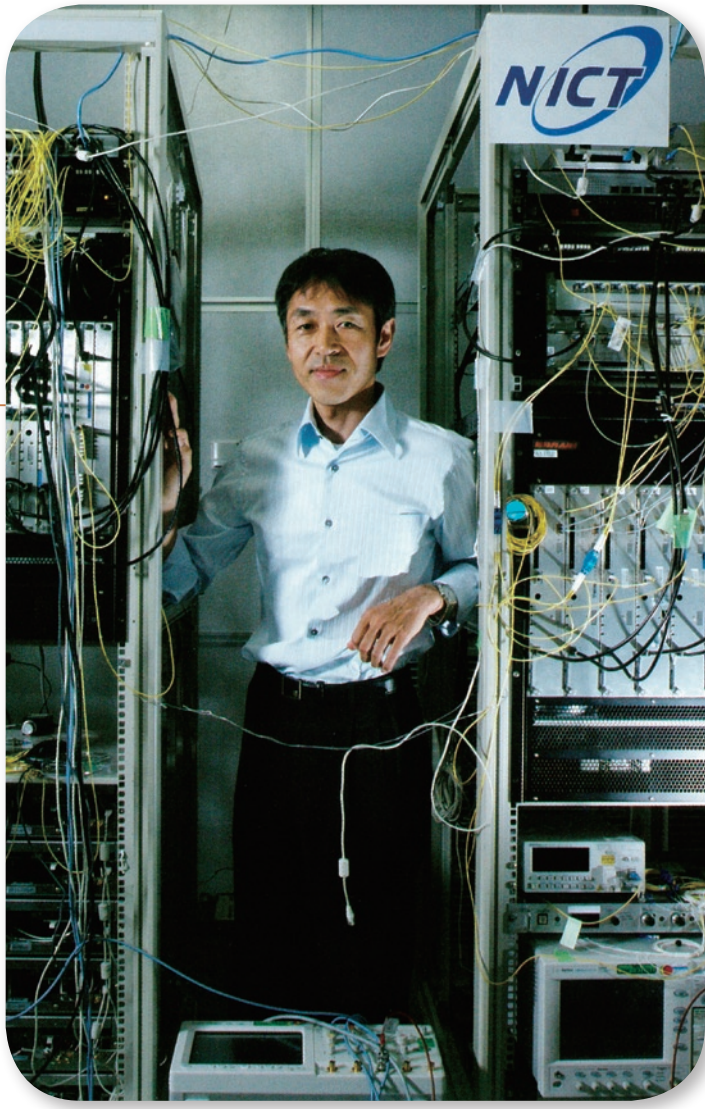
限りなく速く、そして絶対安全な通信に向けて

佐々木 雅英（ささき まさひで）
未来 ICT 研究所
量子 ICT 研究室 室長

1992 年、大学院博士課程修了後、日本鋼管株式会社（現在の JFE ホールディングス）入社。1996 年、郵政省通信総合研究所（現 NICT）入所。それ以来、量子情報通信の研究開発に従事し、2011 年量子 ICT 研究室室長に。6 階にある私たちの研究室では、窓から見える景色の半分以上が空です。遠くまで広がる大きな空を臨みながら、はるか未来を見据えた研究に日々励んでいます。



「量子情報通信は、盗聴不可能な暗号通信（量子暗号）や、低電力・大容量通信（量子通信）を実現する技術として期待されています。長期に亘り情報通信社会を支えるための必須の技術となるでしょう。」

量子通信の源流

量子通信の源流は 1960 年のレーザーの発明まで遡ります。それまで通信は電波を利用して行われていましたが、レーザーに使う光の粒子のエネルギーは、周波数が電波に比べ 10 万倍あり、温度に換算すると光子 1 つで 1 万度くらいに相当します。光が粒子であるという量子効果が顕在化するとともに、電波よりももっと大きな情報量を伝送できるだろうというアイデアがあって、そこから少しずつ量子通信は発展しました。ただ、当時はまだ光ファイバが実用化の段階にはなく、物理学の理論的な学問でしかありませんでした。

しかし、1980 年代に入って、量子通信は非常に大きな転換点を迎えます。完全に盗聴を見破る量子暗号が発明されたり、光子だけでなく原子や分子を操る技術が実現されたことで、量子計算などあらゆる情報通信に量子効果を利用するという量子情報技術のアイデアがどんどん生まれるようになりました。量子暗号の発明は偶然で、1982 年に IBM の物理学者のチャールズ・ベネットとモントリオール大学の暗号学者ジル・ブラサールがプエルトリコのプールで偶然出会って、何気ない会話から量子暗号が生まれたと言われています。1984 年の国際会議で彼らが発表した最初の量子暗号プロトコルは、BB84 と名付けられました。しかし、しばらくは大して注目されていませんでした。ところが、1994 年に米ベル研究所のピーター・ショアが「量子コンピュータが実現すれば、現在の暗号はすべて破られてしまう」という理論を発表したことで、量子情報技術研究が一気に広がりました。量子暗号は量子コンピュータでも破れない究極の暗号として一気に注目されるようになりました。ちょうど冷戦が終結した頃で、核による抑止力から、情報通信技術でいかに優位に立つかということが国家の存亡を左右する時代になっていたため、現代暗号を解読する量子コンピュータをどの国よりも先に持とう、あるいはより安全性の高い量子暗号技術を獲得しようという話になり、学術研究というより国家戦略として研究開発が行われるようになりました。

我が国でも、2000 年に科学技術振興事業団（現在の（独）科学技術振興機構）が、量子暗号のプロジェクトを採択し、当時の郵政省でも量子暗号や大容量化に向けた量子通信の研究開発をプロジェクト化して、2001 年に通信総合研究所（現在の NICT）で量子情報通信の本格的な研究開発が始まりました。

量子暗号の暗号化技術

量子暗号は、量子鍵配送とワンタイムパッド（鍵を毎回使い捨てで一度きり使って暗号化する）という 2 つのステップがあり、量子鍵配送では「0」と「1」のランダムな数列を使った鍵を作り、送受信者以外には絶対傍受されない状況で共有します（図 1）。データに鍵を足し算して送信し、受信したデータにもう一度鍵を足せば元のデータに

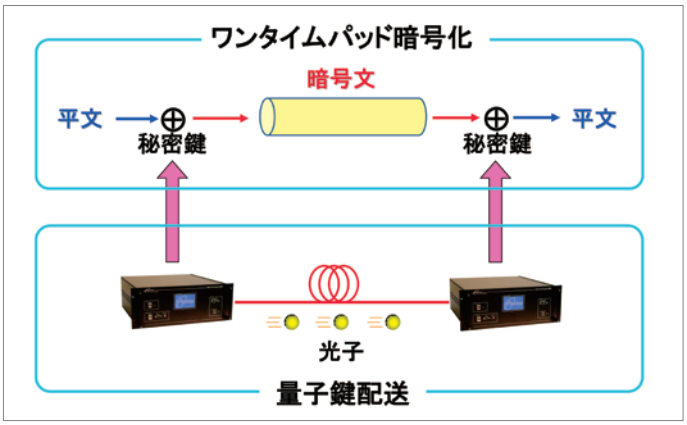


図1　量子暗号における操作の概要図
量子鍵を共有していなければ、たとえデータを傍受できたとしても元のデータに戻すことはできない。

戻るという、極めて単純な方式です。量子暗号では傍受されれば必ず分かり、更に同じ状態での複製が不可能という特性を持っているので、安全な暗号が可能となります。

現在の暗号化技術でも鍵は使われていますが、単純な足し算ではなく素因数分解を使った複雑な仕組みを使っており、めったに解けるものではありませんが、コンピュータの能力が上がれば解けるようになります。1つの暗号化方式が破られるまでの平均寿命は、約13年と言われています。量子暗号は、理論上こうした問題はありません。

量子暗号の利用用途

量子暗号は原理的に盗聴できない究極的暗号ですが、性能はまだ低く、敷設ファイバ50kmで秘密鍵の生成速度が数100kbpsでMPEG4の動画データをワンタイムパッド暗号化できるレベルです。1対1でこの程度の距離で厳格に管理した秘匿通信をしたいという用途に特化されます。国家機密や個人の生命にかかわる医療情報の安全な通信などが用途として想定されます。欧米ではすでに製品も市販されています。購入しているのは研究機関がほとんどですが、一部は銀行などにも納入されています。

日本では、2001年から日本電気株式会社(NEC)と三菱電機株式会社(三菱電機)、日本電信電話株式会社(NTT)が、また、2011年からは新たに株式会社東芝(東芝)も加わってNICTからの委託や共同研究で量子暗号技術の開発を行っています。特に、NICTが有する光テストベッドJGN-Xを用いて、都市圏敷設ファイバで量子暗号ネットワークを構築し長期運用試験を行っています。図2は2010年末時点でのネットワーク構成を示したものです。図3は実際の量子暗号装置の一部です。2010年10月に公開した実験では、6カ所の拠点を結んで量子暗号ネットワークを構築し、途中に高度な

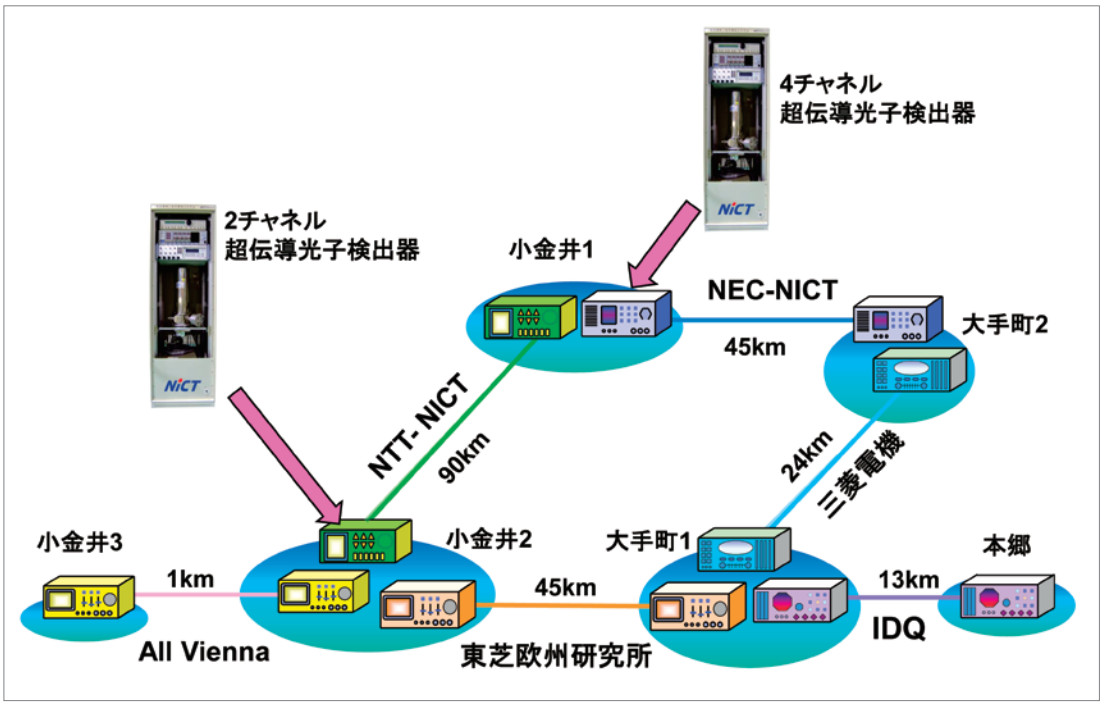


図2　2010年10月に行われた実験。各ノードに配置された量子暗号装置は、既存の光回線で繋がれている。

傍受装置を配置し、「実際に傍受されたことが分かるか」、「傍受されたら別の経路に迂回させられるか」、「その間データは途切れることはないか」、といった試験を行いました。2015 年頃には、実際のネットワーク環境で利用する計画で技術のブラッシュアップが進んでいます。ただし、一般のユーザーが量子暗号を利用するようになるためには、伝送距離や伝送速度の課題があるため、まだ 10 年以上はかかるだろうと思われます。

大容量化に向けた量子通信の必要性

実利用に近づいた量子暗号に比べ、大容量化に向けた量子通信はまだ基礎研究の段階です。今の光通信は、光パルスの有無で「0」と「1」の信号を表し光をエネルギーの塊としてしか制御していません。しかし、光を波と考えた場合、波と波がぶつかると波が強くなったり弱くなったりと相互に作用し、このような性質まで使うと、今の光通信よりもはるかに多くの情報量を伝えることができるようになります。さらに、光は波であると同時に粒子でもあり、光子としての性質を制御することで、与えられた送信エネルギーを最も効率よく使い、今よりも遙かに多くの情報を伝送する量子通信が可能になります。実現には受信側で光子を制御し、光子 1 個 1 個から最大の情報を取り出せる量子受信器の開発が必要です。まだ実験室での原理実証の段階であり、今後多くの未踏技術の開発が必要ですが、実現の暁には通信のほか計測技術にも革命をもたらすと期待されています。

現在、誰もが使っている携帯電話も、元々の理論は 1948 年にクロード・シャノンが発表した、「0」と「1」で画像や音声などの情報を送るための「情報理論」が最初で、当時はどうやって実現すればいいのかは全く分からない状態でありました。シャノンが予言した通信性能に到達したのは、最近のことです。現実が理論に追いつくためには、約半世紀ほどかかったことになります。量子通信が実際の我々の生活に使われ世の中を変えていくのにも半世紀はかかるでしょう。半世紀後の社会はおそらく現在想像もできないような新機能を自在に使いこなしているかも知れません。その夢を 1 つひとつ見つけ出していこうと思い、今日も産学官連携で研究開発に取り組んでいます。

図3　量子暗号ネットワーク監視装置
一般に普及するためには、小型化する必要がある。