量子コンピュータによる暗号解読への対策

近年、量子コンピュータの研究開発が急速に進んでいます。IBMは2019年1月から量子コンピュータの販売を開始。同年10月23日、Googleは、量子コンピュータの量子超越性を実証したと科学雑誌Natureで発表しました。2030年以降の無線通信システムが採用する暗号技術は、現行のコンピュータに加え、急速な進歩を遂げている量子コンピュータに対しても安全性を確保する必要があります。そこで本講演では、量子コンピュータとは何か、私たちが通信で使用している２種類の暗号、共通鍵暗号と公開鍵暗号について、どれくらい安全性が低下するリスクがあるのか、どのような対策が必要であるのかを説明します。その上で、ATRが取り組んでいる研究開発をご紹介します。
量子コンピュータとは、量子ビットを情報単位とし、量子版の論理演算を行う回路を組み合わせることで計算を実行する装置です。従来の電子計算機とは動作原理が違います。量子コンピュータは、あらゆる計算が速くなるわけではなく、速く解ける問題は、わずかしかわかっていないのですが、劇的に計算回数を減らせる問題の１つに「因数分解」があることが、暗号にとって極めて大きな脅威なのです。なぜなら、私たちが日常的に使っている暗号方式の１つである公開鍵暗号は、素因数分解の困難性を安全性の根拠としているからです。こうした背景から、量子コンピュータでも解読が困難な、耐量子計算機暗号が研究されています。さらに、有望なアルゴリズムを広く世界で使えるようにするための標準化が米国標準技術研究所において進行中であり、最終候補として７件、代替候補として８件のアルゴリズムが選考されています。ATRは、総務省のプロジェクト「安全な無線通信サービスのための新世代暗号技術に関する研究開発」において、無線通信環境における耐量子暗号の適切な管理運用を行う技術の研究を進めています。５Ｇから６Ｇへ通信技術が進歩すると共に、暗号技術も耐量子暗号へ移行します。皆さまが安心して通信ができるよう、ATRはこれからも基盤となる技術の研究開発に取り組んで参ります。