埼玉新聞

(5) 経済 2014年（平成26年）4月9日（水曜日） 埼

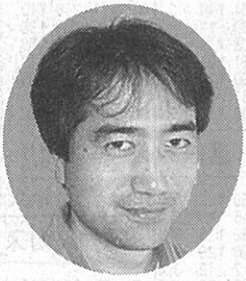
サイ・テクこらむ

知と技の発信 【161】

埼玉大学・理工学研究の現場

未来の情報化社会を守る

小柴健史 大学院理工学研究科 准教授



こしば・たけし
1967年生まれ。東京工業大学大学院修了。博士（理学）。2005年から現職。専門は、暗号理論、量子計算、擬似乱数生成・乱数抽出などの理論計算機科学。

今やインターネットは電力網や道路網のような社会基盤の一つとなっています。インターネットショッピングでクレジットカード番号を送信するなど、個人情報を送信する場面は数多くあります。

インターネットを介した通信の安全性を保証する技術に暗号認証技術があります。そして、現在の暗号認証技術は、素因数分解を計算することが非常に難しいということを前提としています。

■暗号認証技術

二つの大きな素数の積として表現される整数を素因数分解するのには、スパコンのような高性能コンピュータをもってしても天文学的な時間が必要であると考えられています。

また、新しい動作原理に基づくコンピュータの可能性も研究されており、量子力学的な効果を利用した量子コンピュータもその一つです。日常生活では体験することができないので想像しにくいと思いますが、ミクロの世界では複数の状態が同時に起こることがあり、これを量子重ね合わせ状態と呼びます。量子重ね合わせ状態を維持したまま制御することができ、超並列的な同時処理が可能です。

一方で短所もあり、量子重ね合わせ状態からは一つの可能性だけしか取り出すことができません。量子コンピュータの特長を生かして、素因数分解を効率的に計算する量子アルゴリズムが知られているのです。

■潜在的脅威

汎用的な量子コンピュータを実現するには克服すべき技術的課題が多いのですが、量子コンピュータは現在の暗号認証技術に対して潜在的脅威であることには変わりありません。

■量子ブラインド計算

私の研究室では、将来の情報セキュリティ技術を確保するために、量子コンピュータが実現したとしても安全性が担保される技術の研究を行っています。

敵対者としての量子コンピュータに対する防御だけでなく、量子力学的な効果を積極的に活用することで新たな情報セキュリティ技術を創成することにも挑戦しています。一例として量子ブラインド計算という技術を紹介しましょう。

一般ユーザが負荷の大きい計算タスクを抱えているとき、それをサーバ計算機に代理で計算してもらいたいとします。量子ブラインド計算では、ユーザの持つ入出力情報だけでなくユーザが実行したいプログラムさえもサーバ計算機に秘匿にすることができるのです。サーバ計算機にとっては何をさせられているのかまったく分からないことになります。

量子力学的効果はすでに実験的に検証されています。量子コンピュータの実現には至らなくても、現在実装できる量子力学的効果を利用した情報セキュリティ技術が次々と見出されています。量子情報セキュリティ技術は決して夢物語という訳ではありません。