量子コンピュータと暗号化手法

量子コンピュータは暗号解読が可能？

「量子ビット」で大規模な並列演算が可能
可能性のある組み合わせを調べる高速化アルゴリズム
整数の素因数を見つけるのを高速化するアルゴリズム

エニグマ
DES
RSA
量子暗号
格子暗号
⋮

量子コンピュータの登場により、悪意を持ったハッカーがこれを利用し始めれば、SSL や暗号化されたファイル、仮想通貨などの暗号を解読されてしまうのでは？という心配が高まっています。
量子コンピュータは、「量子ビット」を活用してこれまで難しかった大規模な並列演算を可能にし、性能はスーパーコンピュータの 9000 兆倍にもなるともいわれています。本格的な実用化にはコストや技術的な問題でまだまだ先だと思われていますが、最近のハッカーはお金を大量に持っているため、大きな脅威になっています。
ハッカーは、量子コンピュータが持つ、組み合わせを高速に計算するアルゴリズムや、整数の素因数を見つけるのを格段に速くするアルゴリズム等を使って、可能性のある全ての暗号鍵の組み合わせを短時間で試すことができるため、ブルートフォース攻撃を仕掛けてくる可能性があります。
それまで、非常に大きな素数の掛け合わせの逆算は困難であることを防御の拠り所としていた RSA などの公開鍵暗号システムに対し、2000 万キュービットの量子コンピュータでは、2048 ビットの RSA 鍵を 8 時間足らずで解読できると可能性があるとのことです。
暗号の過去の歴史を振り返れば、第二次世界大戦のドイツの使用で有名になった機械式暗号機の「エニグマ」の暗号解読のエピソードは映画にもなりました。それ以降、暗号解読は機械からコンピュータに移り、軍事用途だけでなく、企業間の商取引などの用途でも攻防が繰り広げられるようになりました。暗号方式を公開した 56 ビットの鍵を使った共通鍵暗号を基盤としている「DES 暗号」も、鍵の組み合わせは 2 の 56 乗で約 7 京もあるため解読不可能と思われていたのですが、1994 年に解読されてしまいました。その後、共通鍵暗号の問題点を解決するため、公開鍵暗号方式が登場し、それを実装した「RSA 暗号」は、素因数分解を用いる方式です。この公開鍵暗号方式の RSA 暗号と共通鍵暗号方式を併用したのが SSL です。
暗号方式の中で史上最強と言われてきた「量子暗号」でさえ、「量子もつれ」に脆弱性が見つかったともいわれています。量子コンピュータを使用した暗号解読の脅威に対抗するためには、「格子暗号」など耐量子コンピュータソリューションを提供する企業も増えてきました。歴史は繰り返され、暗号化の攻防は、まだまだ続くと思われます。