

本号の耐量子計算機暗号（以下、PQC）論文からも分かる通り、量子計算の恩恵と脅威が実生活へ与える影響を、真剣に考えなければならない時代がやってきた。筆者が物理学を志していた頃は、量子計算を専門とする研究室はまだ珍しかったことを思うと隔世の感がある。

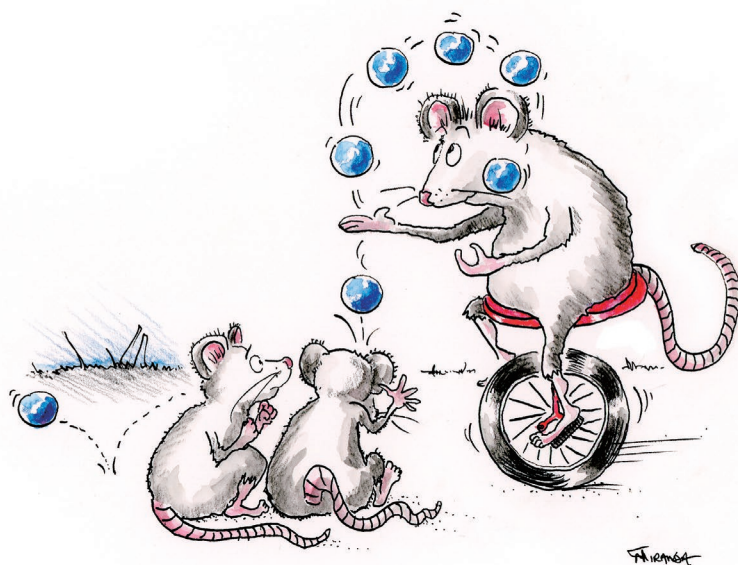
最近では、学術的な領域を超えて「量子力学」や「量子論」といった言葉がちょっとしたブームとなり、あたかも万能なもののように語られている節もあるが、量子コンピュータにも「できないこと」は存在する。PQCもまた、量子コンピュータでは解くことが「できない」

よりもずっと長い平行に近いベクトルの組を与えると、短いベクトルを取り出す手順が不明であるうえ、非常に煩瑣になると気づくだろう。また、短いベクトルを見つけても、そのベクトルが「最短」である保証はない。そして、格子の次元が大きくなるほど、最短ベクトルの探索はより困難なものとなる。

格子問題の歴史は古い。最短ベクトル問題は2次元の場合には厳密に解くことができるのだが、それを最初に示したのは1773年のLagrangeだった。その頃の日本は江戸中期。今年（2025年）放送されている大河ドラ

数 | 理 | の | 窓

暗号技術に使われる昔ながらの数学問題



数学の問題をもとにして実現されるものである。

ここでは、PQCの背景にある数学問題である格子問題（最短ベクトル問題）について紹介しよう。格子とは、碁盤目状の規則的な点の並びのことである。格子上に、次元と同じ数のベクトル（2次元の場合は2本）を与え、元々あった格子を隠す。このとき、これらのベクトルを使って、隠された格子上の2点を結ぶ最も短いベクトルを見つけよ、という問題である。直感的には、すぐ隣にある2点間を結んだものが最短ベクトルだが、意地悪なベクトルの組からこれを見つけるのは容易ではない。

格子上の各点は、与えられたベクトルの先またはその逆向きに移動した先にあり、順々に辿って見つけていくことができる。しかし、例えば、隠されている点の間隔

マで、薦谷重三郎が活躍しているのと同時期である。

この問題は、高次元の格子においては現在でも厳密に解くことは困難だが、ただ、「近似解」を構成するアルゴリズムが20世紀後半に発見された。このアルゴリズムの処理時間は、格子問題に基づく暗号（格子暗号）技術の安全性評価の根拠となっている。

暗号技術に応用されている数学問題の源流が、江戸時代まで遡るとするのは感慨深い。AIをはじめとした先進的な技術が次々と出てくる現在では、なにかと新しいものに関心が向き、世の中がテクノロジーの進化とともに変わり続けていくのは避けられない。ただ、そんな中でも、長い歴史の中で変わらぬものに目を向けていくこともまた、大切なことのように思われる。（上杉 信孝）