次世代暗号を対象とした解読コンテストでの世界記録達成

2013 年に KDDI 研究所と国立大学法人九州大学は、暗号解読コンテスト「Thechnische Universitat Darmstadt Ideal Lattice Challenge」において、総当たり方式による計算では数万年かかるといわれている 128 次元のイデアル格子最短ベクトル問題を解読し、世界記録を達成した。次世代公開鍵暗号は、現在使われている公開鍵暗号と比べて、より高速で安全性高い方式が実現できる技術として期待されており、最短ベクトル問題の難解さを根拠とする格子暗号はその有力な候補のひとつである。最短ベクトル問題は、あるベクトルの集合（基底）に対して、ベクトルを組み合わせて長さが最小になるベクトルを発見する問題である。この問題を解くことは、格子暗号が解読できることを意味するため、次元を高くして解読を困難にする必要があるが、次元が高すぎると計算速度が遅くなる。そのため、安全性が確保される最適な次元数（鍵の長さ）を求めるために、多くの研究機関で高速な解法の研究が進められている。

イデアル格子とは、格子暗号に利用される格子の種類の 1 つであり、暗号化処理を高速化し鍵長を削減できる方式として、特に注目を集めている。イデアル格子最短ベクトル問題は、このイデアル格子を対象としており、次元が増えるにしたがって難しくなる。KDDI 研究所は、効率的な並列処理が困難とされていた解読アルゴリズムの高速化並びに並列化の開発に成功し、128 次元のイデアル格子最短ベクトル問題を、商用クラウドの 84 台の仮想 PC を利用して、約 2 週間で解読した。本研究成果は、次世代公開鍵暗号として格子暗号を利用する際に、安全な鍵の長さを決めるための重要な情報となる。

本研究成果に関しては、暗号に関する最高峰国際会議 Eurocrypt 2013 のランプセッションにて速報するとともに、公開鍵暗号に関する権威ある国際会議 PKC 2014 にて発表を行った。