世界で誰にも解読されていない暗号問題の解読

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「TU Darmstadt Learning with Errors Challenge」において、2016 年 7 月 1 日時点で誰も解読に成功していなかった 60 次元の Learning with Errors（以下、LWE）問題を、世界で初めて解読した。LWE 問題は、故意に誤差を付加した多元連立一次方程式を解く問題である。この問題を解くことは、量子コンピュータによる解読に耐性を持つ耐量子計算暗号の最有力候補である格子暗号を解読することに相当する。安全な暗号を実現するためには、LWE 問題の次元（未知変数の個数）を高め、または誤差を大きくし、解読を困難にする必要がある。しかし次元が高すぎると計算時間が増大し、誤差が大きすぎると正しい暗号処理が行えない確率が増大する。このため、安全性が確保される最適な次元と誤差の大きさを求めるために、多くの研究機関で高速な解読アルゴリズムの研究が進められている。

KDDI 研究所と九州大学は、解読アルゴリズムの高速化並びに並列化に成功し、商用クラウドの 20 台の仮想 PC を利用することで、スーパーコンピューターを用いた総当たり方式による計算では一万年以上かかる 60 次元の LWE 問題を、約 16 日間で解読した。また、55 次元以下の問題についても、KDDI 研究所、九州大学が解読した。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次元や誤差の大きさを決めるための重要な情報となった。

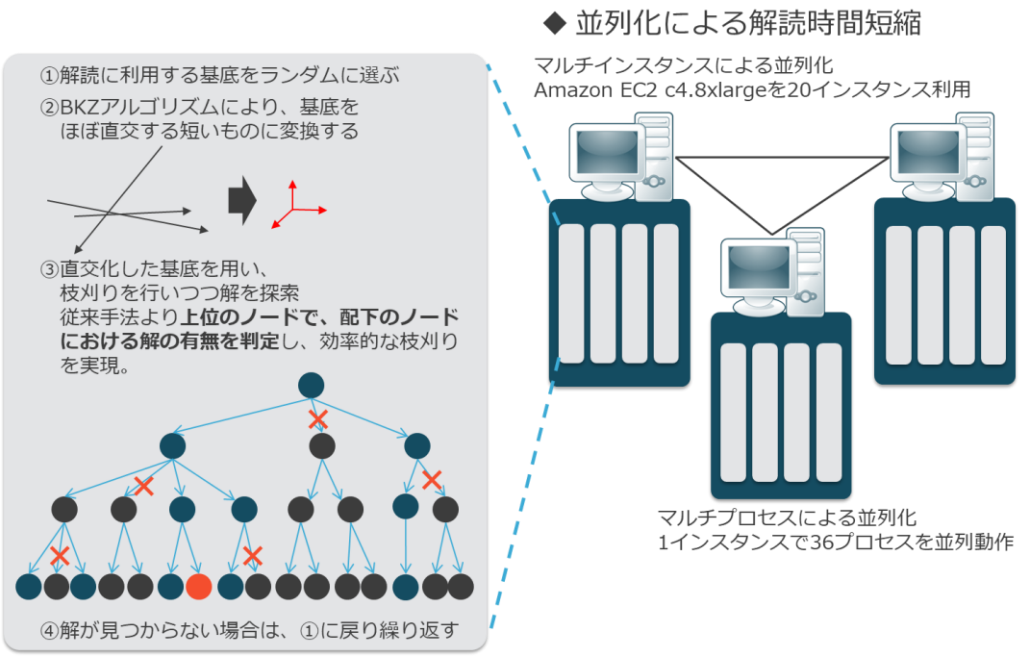

図　KDDI 研究所が開発した LWE 問題の解読アルゴリズム