株式会社 KDDI 研究所
国立大学法人　九州大学
2016 年 7 月 19 日

世界で誰にも解読されていない暗号問題を初めて解読！

～スーパーコンピューターでも一万年以上かかる問題を、約 16 日間で解読に成功！～

株式会社 KDDI 研究所（本社：埼玉県ふじみ野市、代表取締役所長：中島康之、以下「KDDI 研究所」）と国立大学法人九州大学（本部：福岡市西区、総長 久保千春、以下「九州大学」）は、暗号解読コンテスト「TU Darmstadt Learning with Errors Challenge （注 1）」において、これま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（注 2）解読しました。

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す。この問題を解くことは、多くの研究機関で研究が進められている格子暗号（注 3）が解読できることに相当します。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ります。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します。
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法の研究が進められています。

KDDI 研究所と九州大学は、この度、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 1 万年以上かかる（注 4）60 次元の LWE 問題を、約 16 日間で解読しました。また、55 次元以下の問題についても、KDDI 研究所、九州大学により解読できました。

本研究成果は、次世代公開鍵暗号（注 5）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ります。

KDDI 研究所と九州大学マス・フォア・インダストリ研究所は、引き続き解読アルゴリズムの高速化検討を進めるとともに、より高速で安全な次世代公開鍵暗号実現に向けた研究開発を推進していきます。また、本研究成果は、2016 年 10 月 11 日～13 日に秋田で開催されるコンピュータセキュリティシンポジウム 2016 にて報告予定です。

【本件に関するお問合せ先】
株式会社KDDI研究所 営業･広報部
TEL:049-278-7464
E-mail：inquiry@kddilabs.jp
国立大学法人九州大学　マス・フォア・インダストリ研究所　数理 IMI 秘書室
TEL:092-802-4401

（注 1） TU Darmstadt Learning with Errors Challenge はドイツのダルムシュタッド工科大学が主催するコンテスト。暗号解読をめぐって、世界中の暗号研究者の参加が見込まれる。
https://www.latticechallenge.org/lwe_challenge/challenge.php

（注 2） 2016 年 7 月 19 日時点。

（注 3）格子暗号とは、LWE 問題や格子の最短ベクトル問題などを安全性の根拠とする公開鍵暗号方式。次世代公開鍵暗号の有力な候補の一つで、現在使われている RSA 暗号や楕円曲線暗号よりも安全かつ高速な方式として期待されている。格子暗号を用いると、暗号文の状態で様々な演算が可能になる完全準同型暗号など実用的な暗号システムを構成することができるため、多くの研究機関で研究が進められている。

（注 4）解読アルゴリズムを利用せず、解となりうる全ての可能性を、2016 年時点における世界最高性能のスーパーコンピューターで試した場合。

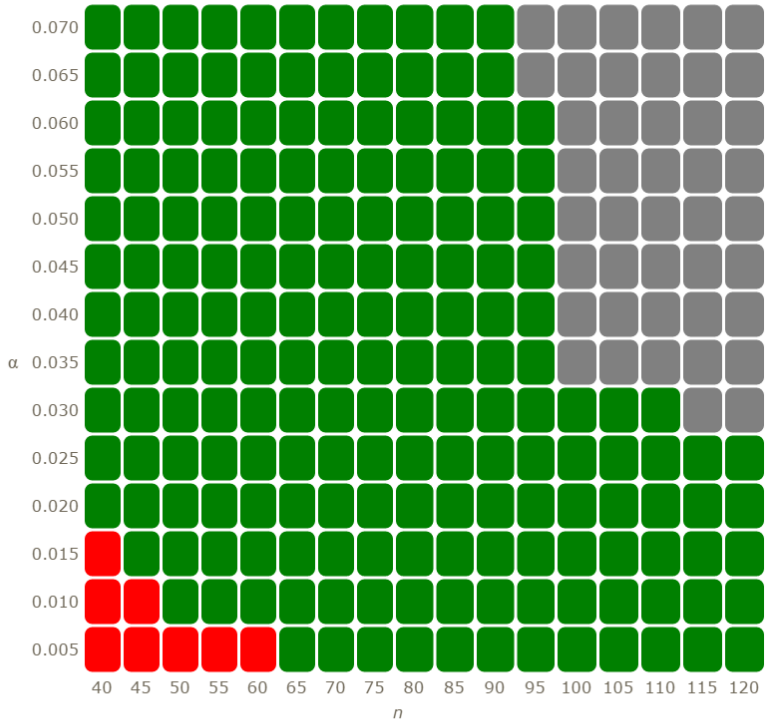
（注 5）公開鍵暗号とは二つの鍵（A と A’）を作成し、どちらか一方の鍵で暗号化し、もう一方で復号するという仕組み。自分あてに情報を送るための暗号化用の鍵（A）は世間に広く公開しておき（公開鍵）、 その鍵（A）を使って暗号化して送ってもらう。復号するためには、公開してある鍵ではないもう一方の鍵（A’）で復号する。この復号するための鍵（秘密鍵）は復号する本人しか知らないので、復号できるのは本人のみとなる。この二つの鍵は、数学的な関係があるので、関係のない他の鍵で復号することはできない。RSA 暗号や楕円曲線暗号等が主流となっており、オンライン決済や SSL の暗号化通信といった、個人情報のやり取りなどに使われている。

別紙

図 1: 世界記録が掲載された Web サイト（2016 年 7 月 4 日現在）
（https://www.latticechallenge.org/lwe_challenge/challenge.php）
赤は解読済みの問題（すべて KDDI 研究所、九州大学による解読）、緑は未解読の問題。灰色は作成中の問題。

CHALLENGE TABLE

Here is an overview of all challenges. By clicking on an a **green** cell (representing an unsolved challenge), you can either *download* the instance or go directly to the submission page to *submit a solution*. Clicking on a **red** cell (representing a solved instance), on the other hand, allows to either *download* the instance or *see details* of the submission. Cells in **grey** are still under generation and will be updated, once they are generated by the participating parties.



LATEST SUBMISSIONS

Date	Dimension	Relative error	Contestant	Error norm	Submission
2016-07-01	60	0.005	Rui Xu Kazuhide Fukushima Shinsaku Kiyomoto Tsuyoshi Takagi	1089.84	Details
2016-06-15	50	0.005	Rui Xu Kazuhide Fukushima Shinsaku Kiyomoto Tsuyoshi Takagi	634.66	Details
2016-06-15	55	0.005	Rui Xu Kazuhide Fukushima Shinsaku Kiyomoto Tsuyoshi Takagi	835.17	Details
2016-06-15	45	0.005	Rui Xu Kazuhide Fukushima Shinsaku Kiyomoto Tsuyoshi Takagi	463.09	Details
2016-06-15	40	0.005	Rui Xu Kazuhide Fukushima Shinsaku Kiyomoto Tsuyoshi Takagi	327.13	Details

Only the five latest successful submissions are shown here. The full hall of fame can be found here. Toy challenges are excluded from both lists.

図 2: LWE 問題の概要

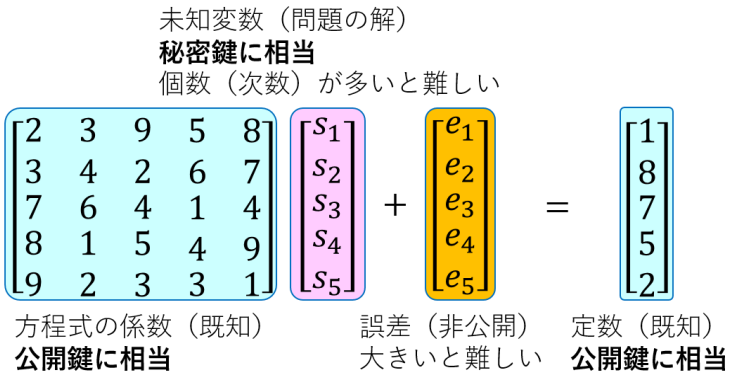


図 3:解読処理の概要