※同じ内容のリリースを、総務省記者クラブ、テレコム記者会、情報通信記者会等へ配信しております。

【報道発表資料】

KDDI R&D LABS　九州大学

株式会社 KDDI 研究所
国立大学法人　九州大学

2013 年 7 月 19 日

次世代暗号を対象とした解読コンテストで世界記録を達成

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）と国立大学法人九州大学（本部：福岡市東区　総長 有川節夫）は、暗号解読コンテスト「Thechnische Universitat Darmstadt Ideal Lattice Challenge[*1]」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、世界記録を達成いたしました。

次世代公開鍵暗号は、現在使われている公開鍵暗号[*2]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[*3]はその有力な候補の 1 つです。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す。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りますが、次元が高すぎると計算速度が遅くなります。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ます。

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ます。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ります。今回、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 週間で解読いたしました。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、5 月 26 日～30 日にギリシャで開催された国際暗号学会主催の国際会議 Eurocrypt 2013 のランプセッションにて報告しました。

以　上

【用語解説】

*1Technische Universität Darmstadt, Ideal Lattice Challenge,

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、世界の暗号研究者が熾烈な戦いを繰り広げる。

http://www.latticechallenge.org/ideallattice-challenge/

*2 公開鍵暗号

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、まったく関係のない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。

*3 格子暗号

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。

【補足資料】

図１：世界記録が掲載された Web ページ
（http://www.latticechallenge.org/ideallattice-challenge/）

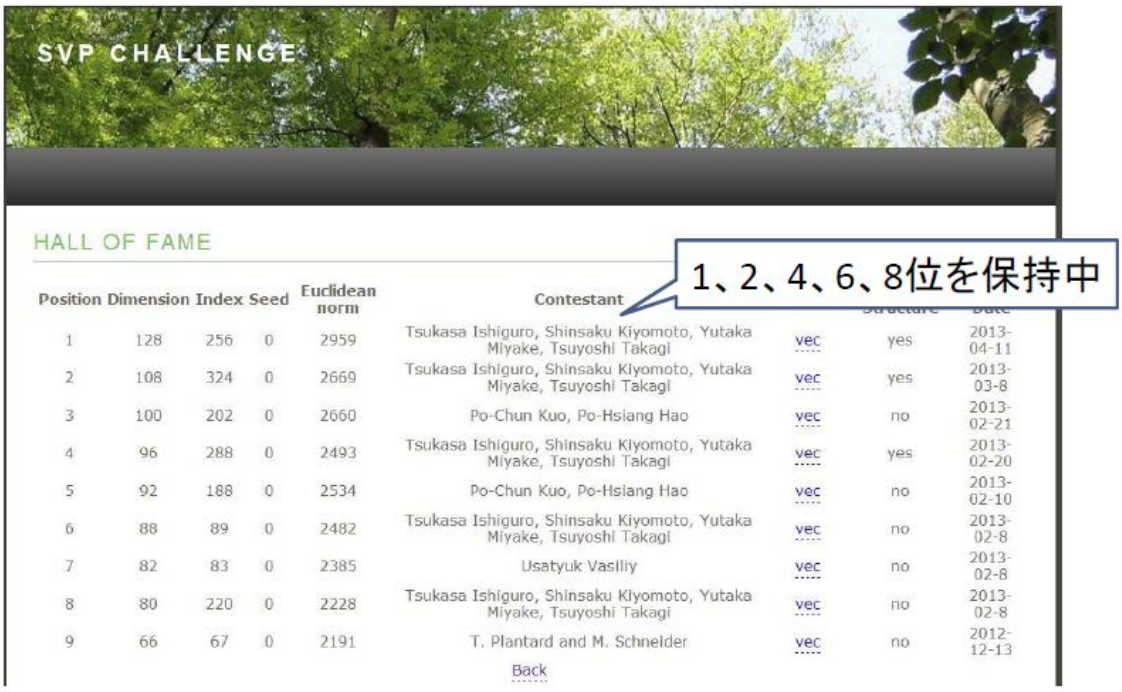


図２　２次元格子の例と最短ベクトル問題

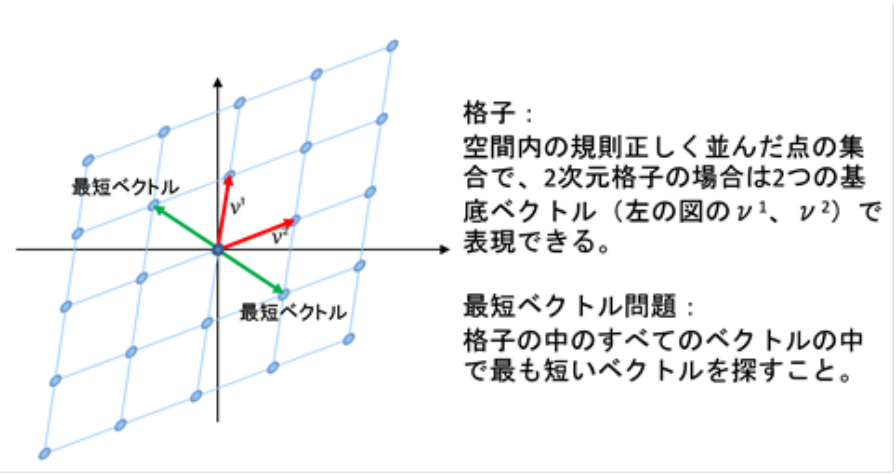
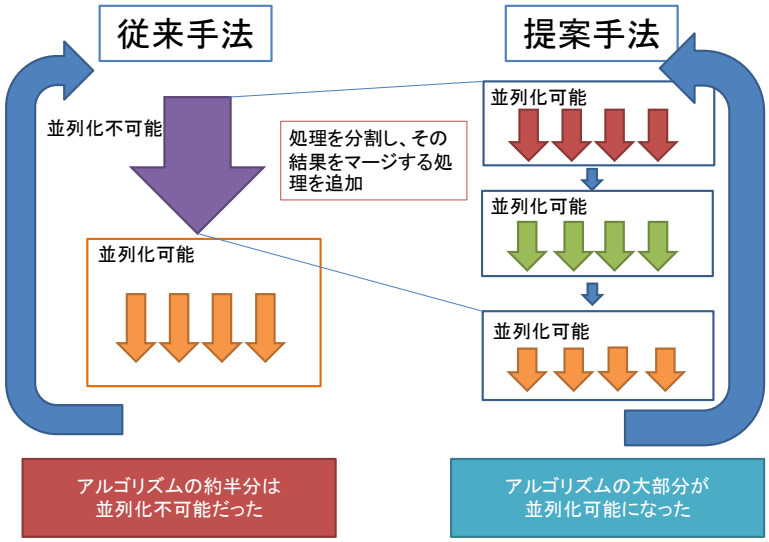


図３　計算アルゴリズムの並列化



（最短ベクトルを探すために事前の計算結果を利用しながら何度も同じ処理を行う必要があるが、従来手法ではその処理を並列化することができず、計算に時間を要していた。提案手法では、並列化可能な部分のみを切り出して並列処理を行うことにより、計算の高速化が実現した。）

【研究に関するお問い合わせ先】
国立大学法人九州大学　マス・フォア・インダストリ研究所　教授　高木剛
Tel: 092-802-4456　　E-mail:takagi@imi.kyushu-u.ac.jp
092-802-4402　　（事務室：上記電話番号不在時にはご用件をお預かりいたします）
【広報に関するお問合せ先】
国立大学法人　九州大学　　広報室
TEL:092-642-2106　　E-mail：koho@jimu.kyushu-u.ac.jp