COVID-19禍で 最先端数理暗号の現場が選んだ 「VELUGA 3000シリーズ」

社会の根幹技術となった暗号の最新事情

「暗号」と聞くと、前世紀なら軍事利用を思い浮かべていたが、現代では、ごく普通の日常で多くの人が利用するようになっている。今やオンラインで「買い物したり予約したり契約したり」というのはごく当たり前の行為だが、そのいずれにおいても「暗号」が重要な役割を果たしている。オンラインでの"経済活動"では、サービス利用を始めるとき契約や登録などで利用者の個人情報をやり取りするのはもちろんのこと、支払いにおいてはオンラインバンキングの口座番号やクレジットカード番号、そして、利用者のアカウントとパスワードなど、個人の財産や安全に大きく影響する情報がインターネットを流れていくことになる。

インターネットを流れていくということは、誰もが情報を取得することが可能ということで、これらの情報が第三者に利用されないように、暗号化することが必須となっている。加えて、企業におけるデジタルトランスフォーメーションの広がり、IoT導入によるデータ通信の広がりによって、インターネットを流れる情報の安全確保とそのために必要な暗号の重要性は急速に増している。もちろん、以前から情報漏えいの大きな理由の1つとなっているPCやスマートフォンの盗難や紛失への対策としてデバイスが搭載するストレージに保存しているデータに対しても暗号化の重要性が訴求されている。

このように、現代では、身の回りにある情報に対して暗号が利用されており、個人や企業、そして社会全体の機密情報保護を担うほどにその影響は大きくなっている。ただ一方で、「解読できない暗号はない」という言葉があるように、暗号を解読する試みも「いい意味でも悪い意味でも」絶えることなく進んでいる。ここでいう「悪い意味でも」は、いうまでもなく犯罪行為における暗号解読だ。一方、いい意味での暗号解読の挑戦は、暗号の強度を検証するために必要不可欠なものでもある。暗号研究において、暗号の強度を高めるとともに、利用されている暗号が現在、そして将来予想される技術水準に対してどのぐらいの強度を確保できるのかの検証が重要なテーマとなっている。

今回は、現代、そして将来における暗号技術について、「数学」の観点から最先端の暗号技術の研究に取り組んでいる立教大学理学部数学科の安田雅哉准教授に聞いた。

安田准教授は、2002年3月に京都大学理学部数学科卒業後、2004年には東京大学大学院数理科学研究科修士課程修了、2007年に同博士課程修了（数理科学博士号）した。ただ、その後大学に残らず、富士通研究所に所属して暗号技術の安全評価とプライバシー保護情報利活用の研究に7年間携わっている。
2015年からは九州大学マスフォアインダストリの准教授として、暗号技術の安全性を数学的視点から解析する研究に取り組み、最新の数理暗号技術として「格子暗号」「同種写像暗号」の研究を進めている。2020年4月からは立教大学理学部の准教授として数理暗号の安全性解析の研究に携わっている。

最先端の数理暗号

まずは暗号と数学の関係について簡単に説明しておこう。

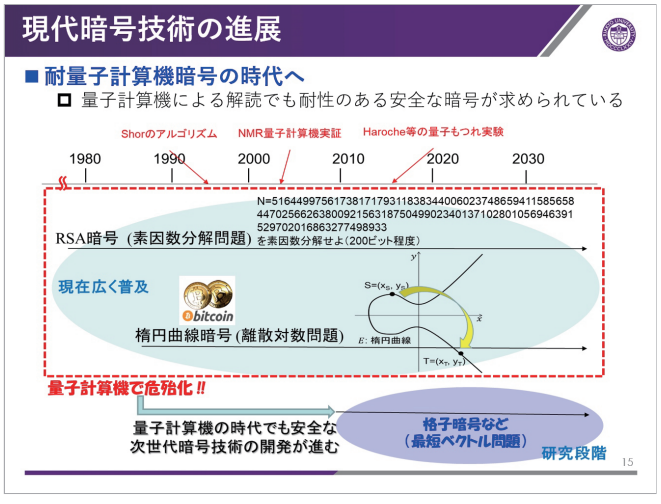
暗号の基本は「意味のある記号の並び」を「意味のない記号の並び」に「並び替える」ことにある。意味のない記号の並びを「元の意味のある記号の並び」に並べなおす場合は、事前に用意している「並びなおすことができるカギ」を使えば短時間で可能だ。ただし、カギがなくても、「並びなおすためのあらゆる方法」を試すことで、いつかは元の並びに戻すことができる。ただ、そのために要する時間は、多くの場合「天文学的時間」となる。できたとしてもあまり得なことはないので、普通は誰もやろうとはしない。

「並び替えたもの」を「元通りに並びなおす」ためにはルールが必要になる。ルールに従って「元の並び」という正解を導き出す。そのため、ルールとして「数学」を用いることが暗号技術では一般的だ。暗号をいかにして解読しにくくするか。暗号をいかにして解読するか。そのどちらにおいても根幹となるのが数学だ。

暗号で「並び変える＝暗号化」「並びなおす＝復号」するとき、重要になるのは、先に述べた「手がかりがあっても可能な限り正解（＝元の並びから）にたどり着けないこと」だ。そのため、暗号関連技術者は、正解にたどり着くのが難しい＝解くのが難しい複雑な数式を考案し続けてきた。その意味では、暗号技術の進化は解くために必要な計算がより必要になる数式の複雑化ともいえる。
その進化した数式を取り入れた暗号技術の中に、安田准教授の研究テーマである「楕円曲線暗号」「格子暗号」がある。

楕円曲線暗号は、1985年に考案された暗号技術で、Blu-rayにおける著作権保護とコピー防止の暗号技術として採用されている。暗号を解読するために必要な計算量は、データサイズが160ビットの全数検索法では2の160乗回の計算が必要といわれている。また、楕円曲線暗号の安全性を検証する実証実験「Certicom ECC Challenge」で出題された問題では、「ECCp」の109ビットサイズデータを解くのに1万台の分散処理で549日（2002年）、「ECC2」の109ビットサイズデータを解くのに2600台の分散処理で17カ月（2004年）を要している。ただし、半導体による演算処理能力の向上と演算に用いるアルゴリズムの進化によって、2009年には「ECC-P112」（データサイズ112ビット）を200台のPlayStationによる分散処理と「ρ法アルゴリズム」の組み合わせによって半年間で解いている。

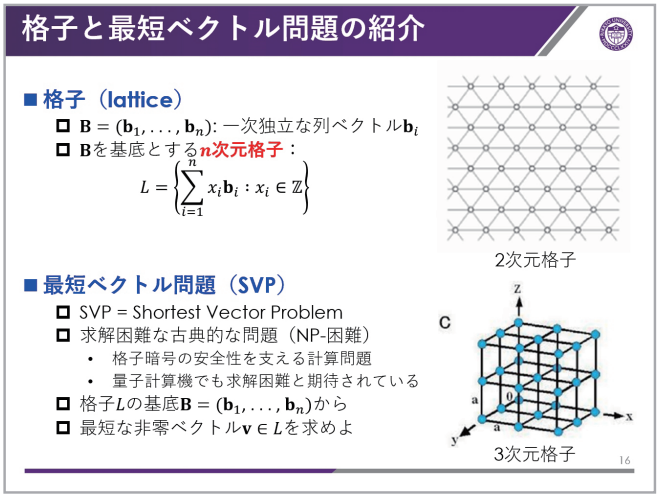
このように、数理暗号技術は演算能力の向上とアルゴリズムの進化で強度が徐々に低下していく"宿命"を持つ。特に最近では量子コンピューターの膨大な演算能力を想定した強度を確保することが数理暗号技術における最先端の研究テーマとなっている。安田准教授によると、現在普及のRSA暗号と楕円曲線暗号は量子コンピューターで想定されている演算能力では強度が不十分とされており、現在「耐量子コンピューター暗号」時代に備えて、格子暗号などの研究が進んでいるという。



長らく暗号技術の主流だったRSAは登場から40年が経とうとしている。楕円曲線暗号も量子コンピューターの登場で安全でなくなる。そのため、格子暗号など耐量子レベルの次世代暗号の研究が進んでいる

量子コンピューターにも耐えられる格子暗号

安田准教授もその格子暗号に九州大学時代から取り組んでおり、日本の格子暗号研究の第一人者だ。数学でいう「格子」とは、独立した列ベクトルを表す。
列ベクトルは次元を持ち、1次元列ベクトルをグラフにすると直線に、同様に2次元列ベクトルは平面に、3次元列ベクトルは立体になる。このように格子は数式で「n次元格子」と表すことができる。



格子演算問題の基本的な解説。SVPは解くのが困難で耐量子コンピュータークラスの強度を持つとされている

格子を用いた演算問題に「最短ベクトル問題」（以下、SVP＝Shortest Vector Problem）がある。安田准教授によるとSVPは量子コンピューターでも解くのが難しいとされており、格子暗号の安全性を確保する根幹的な数理問題という。
SVPがいかに解くのが難しいかを実証する「SVPチャレンジ」が2010年から実施されており、世界中の数理暗号研究者が挑んでいる。

SVPチャレンジでは現在までに東京大学と産総研のグループが150次元の問題を800コアの演算エンジンを搭載したコンピューターで1年半以上かけて解いた他、安田准教授が九州大学に在職していた当時の研究室で127次元の演算を解いている。東大と産総研のグループが800コアの演算エンジンで1年半かけていたのに対して、安田准教授の研究室では汎用PC1台をつかってわずか2カ月で解いている。安田准教授によると、アルゴリズムの改良によって少ない演算処理能力でも高い効率で問題を解くことが可能になるという。

COVID-19禍でも研究が止まらない理由

安田准教授は2020年4月から立教大学理学部の数学科の准教授に就任してからもそれまでの数理暗号の研究を継続して進めている。
SVPチャレンジのように膨大な演算処理を実施するときは、スーパーコンピュータで期限を決めて使用するが、通常の研究活動では立教大学の研究室に個人で購入したタワー型ワークステーションを用いている。このワークステーションでは、SVPチャレンジのような膨大な演算処理を実施する前の段階となる、アルゴリズムの単体処理実験やプロトタイプの演算処理実験を実施するという。

本来ならば、学生や院生など研究室のスタッフとともに研究を進めるはずだったが、COVID-19の影響で、まだ学生にあっていない状況にある。現在、研究室のスタッフとして院生が1人所属しているが、その1人もCOVID-19の感染防止のため研究室に来ることができず、自宅でリモート作業をしている。そのスタッフがリモート作業用として購入を希望したのがエルザ ジャパンのモバイルワークステーション「ELSA VELUGA 3000 for Windows」（以下、VELUGA 3000）だ。CPUにCore i7-9750H（6コア / 12スレッド、2.6GHz / 最大4.5GHz、キャッシュ12MB）を搭載し、GPUにNVIDIA Quadro RTX 3000を採用する一方で、重さ約1.94Kg、サイズ358（幅）×248（奥行き）×17.9（厚さ）mmと薄くて軽い携帯利用も重視したモデルだ。
なお、ELSA VELUGA 3000 for Windowsには、現在後継モデルとなる「ELSA VELUGA3000 G2」が登場している。こちらのCPUは「Core i9-10980HK」を採用して物理コア8基、同時16スレッド対応と強化された。加えて、ディスプレイもサイズは同じ15.6型ながら、解像度は従来モデルの1920×1080ドットから3840×2160ドットと向上している（従来モデルでも3840×2160ドット構成モデルは存在する）。

VELUGA 3000を使っているスタッフは、COVID-19感染防止のため立教大学の研究室に行けない状況にあって、自宅でもプロトタイプアルゴリズムの開発を継続するため、汎用のモバイルノートPCではなく、Quadro RTX 3000を載せて研究室と同等の開発環境を構築できるVELUGA 3000を選んだという。

このVELUGA 3000はスタッフのリモートワーク用として安田准教授が承認して購入しているが、安田准教授自身も「（予算があれば）あれば購入したい」という。その用途は、研究室において使うというより、スタッフと同様に自宅作業用だ。研究室で使っている研究開発用のアプリケーションがほぼ同じように使えるだけでなく、モバイルワークステーションとしては軽量薄型なので、研究室と自宅の間を持ち歩けることも期待している。
その他、GeForceシリーズを載せたコンシューマー向けハイパフォーマンスノートPCと比べたVELUGA 3000の優位性として「信頼性」も安田准教授は挙げている。
膨大な演算処理を必要とする数理暗号の研究現場では、SVPチャレンジのような大掛かりな演算を開始すると1年間程度連続して処理を実行することになる。プロトタイプであっても1週間連続で演算処理を実行することは珍しくない。そのため、内部の温度は常に高い状況が長時間続くため、クーラーファンからの騒音が大きくなるだけでなく、コンシューマー向けノートPCでは、処理の途中でPCが落ちてしまう可能性もある。対して、モバイルワークステーションでは、長時間処理も想定しているので最後まで安定して動作するという。

また、安田准教授は増員する予定の研究室スタッフ全員がモバイルワークステーションを所有する優位性にも期待する。スタッフ全員が1台のワークステーションにアクセスしてプロトタイプの開発やテストを実施するより、モバイルワークステーションを1人1台で所有して、各個人のモバイルワークステーションでそれぞれがプロトタイプの開発とテストを実施するほうが、研究室トータルとしての演算能力は高いと説明する。
「このとき、演算能力が高くてディスプレイがある程度大きくて解像度も高く、かつ、価格が50万円以下のVELUGAは研究室にとってとても選びやすいモバイルワークステーションです」（安田准教授）

数理暗号研究の将来はどこに向かうのだろうか。「暗号って生モノなんですよね」と語る。「RSAが登場して30年ないし40年経ちます。そろそろ交代の時期です。楕円曲線暗号が主流となりつつありますが、それも量子コンピューターが登場したら交代することになるでしょう。このように、暗号技術は時代に合わせながら変化していきます。古い時代からある理論だけでなく、計算と古い時代からある理論を組み合わせながら進化している分野です。時代の変化にマッチした研究開発を進めていく、というのが私の考えです」（安田准教授）

製品仕様 Technical Specifications

ELSA VELUGA 3000

高性能プロ向けQuadro RTX 3000グラフィックスと第9世代インテル Core i9-9880H またはi7-9750Hプロセッサを搭載した薄型・軽量ボディに15.6インチの4K（3840×2160）UHD またはフルHD（1920×1080）広視野角ディスプレイを組み合わせた実力派のモバイルワークステーションです。

オフィス/リモートを問わずいつでもどこでも高い性能を発揮し、みなさまへこれまでにない高い生産性をお届けします。

詳しくはこちらから▶

お問い合わせ先
株式会社 エルザ ジャパン
〒105-0014 東京都港区芝3丁目42番10号 三田UTビル
TEL：03-5765-7391 FAX：03-5765-7235

2020.12