2018 年講演会

「デジタルトランスフォーメーションとブロックチェーン」について

NEC セキュリティ研究所　特別技術主幹
日本学術会議連携会員
佐古和恵（旧姓 田中）
1986 年学部卒

昨年の京都大学理学研究科・理学部数学教室同窓会において、標記題目で講演させていただいた。

企業研究の歩み

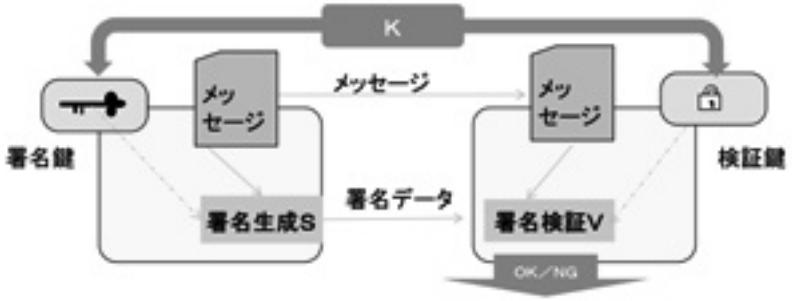
学部生の時代は、平井武先生にご指導をいただき、数学の本を一行一行証明を追いながら読むのは好きであったが、数学の才能のなさを痛感し、学部卒業とともに NEC に就職した。配属されるやいなや、上司に渡されたのが RSA 公開鍵暗号に関する解説論文であった。素因数分解の難しさに基づく鍵生成と、フェルマーの小定理を用いた復号メカニズムの他、素数判定アルゴリズムの効率性など、数学が具体的にデータの暗号化に適用できることに衝撃を受け、以来 30 年以上、この研究に携わっている。ちょうど、暗号化と復号に同じ鍵を用いる共通鍵暗号ではなく、一方の鍵を公開しても安全性が保たれる公開鍵暗号が提案されて 10 年がたち、知識を漏らさずに証明することができるゼロ知識証明など、新しい研究が立ち上がった時期であり、わくわくしながら研究をすすめた。具体的には、単なるデータの暗号化にとどまらず、不正投票も不正集計も防止する無記名電子投票方式や、公平にランダムに当選者が選ばれていることを検証できる電子抽選方式、組織に所属していることは認証できるが、組織の中の誰かは秘匿できる匿名認証方式などの研究開発に従事した。また、これらの新しい技術が実際の社会で活用されるように標準化をすすめたり、海外 NPO 法人の理事になって普及を推進したりしている。現在、一番興味をもって研究しているのは、コンピュータやサーバの中のアルゴリズムが見えない「ブラックボックス」のサービスがあふれる現状を打破してくれる「ブロックチェーン」技術である。当日はこの話を中心にご紹介した。

デジタライゼーションと数学

私がかかわった電子投票、電子抽選、ブロックチェーン（暗号通貨）などはそれぞれ、投票、抽選、お金をデジタライゼーションしたものとみなすことができる。このデジタライゼーションを、そして究極的には社会がデジタルトランスフォーメーションを正しく実施するためには、数学の力が肝要になる。具体的には数学的思考を用いて以下のプロセスを行う。まず、デジタライゼーションする対象が「ど

のようなシステムであるか」を再定義してモデル化し、そのシステムがどのような性質をもつべきかを定式化する。そして、実際に暗号学的要素技術を活用して設計し、そのシステムが目的とする性質を満たしていることを数学的に証明するのである。

署名をデジタライゼーションしたデジタル署名を例にとって、このプロセスを紹介しよう。デジタル署名は、下記の図のようにモデル化できる。



すなわち、署名鍵とメッセージから署名データを生成する署名アルゴリズムＳと、メッセージと署名データと検証鍵から、これらの三つ組が正しいかどうかを判定する署名検証アルゴリズムＶ、さらには、署名鍵と検証鍵の対を生成する鍵生成アルゴリズムＫからなる、とモデル化する。そして、このシステムがどのような性質を持つべきかというと、

> 「正しい鍵生成アルゴリズムＫから生成された署名鍵と検証鍵を用いれば、定義域内のどのようなメッセージに対しても、正しい署名アルゴリズムＳの出力結果である署名データは、上記検証鍵、上記メッセージとともに署名検証アルゴリズムＶに入力すると、三つ組みは正しいと判定する」

がまず挙げられる。すなわち、署名検証アルゴリズムは、正しいときに正しいといってくれるものである、という性質を満たさなくてはならない。さらに、間違っているときに間違っているといってもらうための性質が必要になる。

> 「正しい鍵生成アルゴリズムＫから生成された検証鍵に対して、署名検証アルゴリズムＶに入力して「正しい」と判定される「メッセージ」と「署名データ」の対は、検証鍵に対応する署名鍵を知らなければつくることができない。」

さらには、検証鍵から署名鍵が容易に推測されないような鍵生成アルゴリズムＫの性質が必要である。

このように定式化してから、実際にアルゴリズムK,S,Vを構築して、デジタル署名システムを構成し、その安全性を証明する。具体的には、検証鍵から署名鍵が

容易に推測されないために、素因数分解の困難さや、離散対数問題の難しさに依存するアルゴリズム K が開発されている。

お金のデジタライゼーション

次に、「お金」のデジタライゼーションを考えてみる。お金を、どの口座にいくらあるかを台帳で管理するものとする。そして、ある口座の持ち主から別の口座へお金の移動要求（送金要求）を実現する機能があるもの、とシンプルに見る。送金要求があるときは、要求元が本人であることを確認し、指定された額をその口座から減額し、同じ額を指定された口座に増額するものである。電子マネーなどはその台帳を管理する企業があり、ビジネスモデルとして移動されたお金の一部を手数料として振込先の口座から徴収して自分の口座に入れることが多い。

現状の電子マネーなどで課題になるのは、この口座残高が記載されている台帳がひとつの企業で管理されていることである。もちろん、国内では国の法律に従って企業が厳密に管理しているが、国を超えてインターネット上で信頼できる送金をするためには、この台帳が正しく管理される必要がある。

そこで、ビットコインでは、この台帳を複数の管理者で管理する方式として「ブロックチェーン技術」を考案した。そのしくみを紹介する。

ブロックチェーン技術の概要

上述したように、ある口座の持ち主から、別の口座の持ち主への送金要求（トランザクションと呼ぶ）があり、それが台帳に書き込まれると、自動的にそれらの口座の残高が読み替えられる。トランザクションが台帳に書き込まれる際には、それが正しい持ち主からの要求であるか、ということと、その持ち主が同額の残高を口座に持っているか、という確認が行われる。

単独権限者による台帳管理を回避するために、このトランザクションを、複数の台帳管理者で共有し、同じチェックルーチンを走らせ、結果的に同じ台帳を管理できることを目指す。

課題は、複数多数のトランザクションが存在したときに、また、ネットワークの遅延や不達問題がある中で、すべての管理者がすべてのトランザクションを同じ順番で管理できるか、ということである。

実はブロックチェーンには大きく分けて２種類ある。台帳管理者が特定有数である場合と、不特定多数である場合である。前者は台帳管理者になるために許可が必要であるため Permissioned blockchain と呼ばれている。このような「許可」与えるような権限を持つような構造がないものが、Permissionless blockchain と呼ばれるもので、不特定多数の管理者が存在することになる。台帳管理者が特定有数であれば、同期問題は既存の「ビザンチン問題」として研究が存在する。ビットコインが注目されたのは、不特定多数の管理者であっても台帳の同期がとれる方式を画期的な方式を編み出したことである。

それは、同期のための時間稼ぎを目的とした「暗号パズル」を解くというアイディアに基づく。各トランザクションをパズルのピースとみたて、複数のピースを使って暗号パズルを時間をかけて最初に解いた管理者が、そのトランザクションを台帳に組む込むことを、その順番とともに決定する、ということにするのである。パズルのよいところは、解くのに時間がかかっても、パズルが解けていることを確認するのは瞬時であることである。暗号パズルの解を受信する都度、その正しさを確認し、それが規定する内容を順に台帳に組み込むことにすれば、それぞれの管理者で同期がとれることになる。この暗号パズルが解けたトランザクションの集合を「ブロック」といい、これをつなげるところから「ブロックチェーン」という名がつけられた。

暗号パズルは暗号学的に安全なハッシュ関数をつかって定義されている。ハッシュ関数は、任意の長さの入力から有限の値域の数字（ハッシュ値と呼ぶ）を出力する決定的な関数であり、出力のハッシュ値からもとの入力を逆算することは難しいとされている。ランダムな入力に対して、ランダムな数字を出力する関数と見なすことができる。すなわち、出力のハッシュ値をコントロールすることができない。そこで、暗号パズルは、トランザクションの列を入力とみなし、そこにどういう「数字」を追加すれば、小さなハッシュ値を出力できるか、その「数字」を求めることにある。様々な「数字」を試行し、偶然小さなハッシュ値になるように、現在も世界中のコンピュータがフル回転で暗号パズルを解いているのである。

なぜ、電力の無駄遣いにも見える暗号パズルを解いているのであろうか。それは、暗号パズルを解き、台帳更新に貢献した管理者は、後に「ビットコイン」で報酬が与えられるからである。その報酬めあてに、必死に暗号パズルを解いているのである。しかも、報酬が与えられるためには、自分が作成したブロック（暗号パズル）の次にたくさんのブロックが、フォロワーのように続いてくれる必要がある。そのためには、暗号パズルを不正なく解く必要があるし、自分の前のブロックも正しいものにつなげられるように、確認する必要がある。このような報酬欲しさから、相互に確認する活動が結び付き、ブロックチェーンの正しさが継続するのである。

最後に

講演では、アニメーションを用いてブロックがつながる様子を紹介し、また会場からいただいた多くの疑問点を解消しながら、説明を行った。最後は、残り時間が少ない中で、当初サトシナカモトが想定した理想とは異なる、欲にかられたビジネスが登場する中で、新聞を騒がせる事件の背景も紹介した。

最後に、当時、私が会長を務めていた日本応用数理学会(http://www2.jsiam.org)の紹介をさせていただいた。ブロックチェーンをはじめ、安全性や正当性を数学的に評価するような研究を、日本応用数理学会ではコミュニティとして推進していく

所存である。また、国際応用数理学会の 4 年に一度の大会も初めての日本招致に成功したことを報告した。2023 年の開催に向けて、企業とのつながりを太くしながら活発に活動する抱負をつたえるとともに、企業にお勤めの同窓生の皆様に、年間一口 5 万円の法人賛助会員になっていただけるようお願いをさせていただき、講演をしめくくった。

編集部からの注

佐古氏がビットコインを解説する講演は、数学アドバンストイノベーションプラットフォーム (AIMAP) の企画の一環として、東京で開催されるサイエンスアゴラ 2019(11/15-17) でも予定されているそうです。アニメーションを使った解説をご覧になりたい方は是非。