より高度で安全な暗号を目指して

物理情報システム専攻
藤﨑 英一郎 研究室

藤﨑 英一郎 連携教授　1966年東京都生まれ。1991年東京工業大学理学部数学科卒。同年NTT入社。1998年カリフォルニア大学デービス校客員研究員。1999年スタンフォード大学客員研究員。博士（理学）。2013年より東京工業大学総合理工学研究科物理情報システム専攻連携教授。現在、NTTセキュアプラットフォーム研究所特別研究員。

藤﨑研究室では暗号理論の研究を行なっている。単純な機能しかもたない暗号に比べてより高度な機能をもつ暗号は安全性を満たすのが大変である。先生はどのような手段によってより高度な機能をもつ暗号を作ろうとしているのだろうか。私たちの身近な事例を取り上げながら藤﨑研究室の暗号理論の研究について紹介していく。

暗号とは

私たちの身近なところには多くの暗号が使われている。私たちが暗号という言葉で思い浮かべるものは、縦読みといった言葉遊びやモールス信号といった文字を特定の記号で表す方法だろう。数ある暗号の中に、カエサル暗号というものがある（**図1**）。カエサル暗号とは、平文のアルファベットを何文字かだけずらして作る暗号である。例えば、平文のAは暗号文のDに、OはRに対応するというかたちである。カエサル暗号は文字をずらすためシフト暗号とも呼ばれる。

カエサル暗号を例にとると、現代暗号の流儀ではアルファベットをX文字ずらすことをアルゴリズムといい、代入された具体的な値X＝3を暗号の鍵という。アルゴリズムとは計算手順のことである。現代暗号ではアルゴリズムと鍵を区別して扱い、アルゴリズムは公開する。ゆえに、カエサル暗号のように単純な暗号はアルゴリズムを公開してしまえば、Xの値を探索することで簡単に解読されてしまう。アルゴリズムを公開するのは、学術的な研究対象として暗号を取り扱えるようにするためである。カエサル暗号のように、送信者と受信者が事前に同じ鍵を秘密裏に共有する暗号を共通鍵暗号と呼ぶ。

共通鍵暗号では送信者と受信者があらかじめ秘密を共有していなければ秘密通信ができない。公開鍵暗号はこれを解決する手段として、1976年に概念が提唱され、1978年には素因数分解の困難性

平文	A	B	C	D	E	……	X	Y	Z
暗号文	D	E	F	G	H	……	A	B	C

平文　I LOVE YOU

暗号文　L ORYH BRX

図1　カエサル暗号

この場合のカエサル暗号は、平文から暗号文に暗号化するときには3文字シフトさせる。

を利用した現在RSA暗号と呼ばれる公開鍵暗号が提案された。公開鍵暗号は、封じ手や封印入札などを電子的に行うときにも応用できる。

封じ手とは、囲碁、将棋のルールの一つで、試合が日をまたぐとき、次の一手を考える時間に対戦者間で不公平がないように事前に次の一手を紙などに記入し、立会人に渡しておくことである。封印入札とは、入札者がお互いに提示価格を知ることができないオークションのことだ。

共通鍵暗号や公開鍵暗号のような暗号通信に限定したものを狭義の暗号と呼ぶ。それ以外の安全性を考慮するプロトコルを広義の暗号という。封じ手や封印入札も広義の暗号である。プロトコルとは、一定の目的のための対話の手続きである。

多くの公開鍵暗号は数論の考え方によって作られている。数論とは数、特に整数およびそれから派生する数の集まりの性質について研究する数学の一分野である。数論によって、一見矛盾するような機能をもった暗号を作ることができる。

また、暗号ではP≠NP予想というものが前提となっている。P=NPが示されると多くの暗号の理論は成り立たなくなる。Pとは多項式時間で解ける問題の集合であり、NPとは答えを与えられれば多項式時間で答えを検証できる問題の集合である。P=NPとは、答えを与えられれば多項式時間で答えを検証できる問題は、答えを与えられなくても必ず多項式時間で解く方法があることを意味している。P≠NP予想 の証明には100万ドルの懸賞金がかかっている。P≠NP予想は暗号の中では重要な役割を担っている。

2つの暗号プロトコル

次に、2つの暗号プロトコルを見ていこう。まずは公開鍵暗号の具体的な説明をする。公開鍵暗号は2つの鍵を使う。1つは公開鍵である。これは誰でも入手できる公開されている鍵である。もう1つは秘密鍵である。こちらは誰にも知られないように保管しておく秘密の鍵である。この公開鍵と秘密鍵はペアの鍵で、お互いに関係はあるが公開鍵から秘密鍵を求めることはできない。そして公開鍵で暗号化した平文は秘密鍵でなければ復号

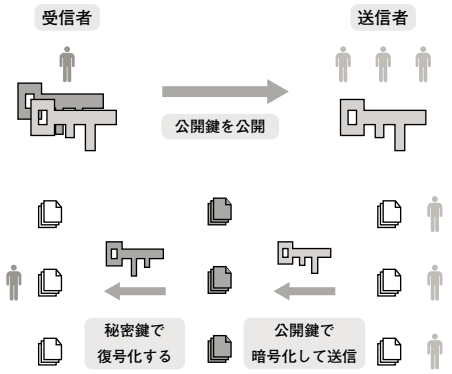

図2　公開鍵暗号

できない。復号とは暗号化された平文を元の平文に戻すことである。AがBに暗号通信をしたいときは、Bの公開鍵で暗号化する。公開鍵は公開されているので、誰でもB宛の暗号文を送信することができる。これを元に戻せるのは秘密鍵を持っているBだけである（**図2**）。

広義の暗号の例としてゼロ知識証明と呼ばれるものがある。ゼロ知識証明とは、ある人が他の人に自分の命題が真であることを伝えるのに、真であること以外何の知識も伝えることなく証明するプロトコルである。

ゼロ知識証明を詳しく説明するには、知識とは何か、知識を何も伝えないとは何かを定義する必要がある。しかし、ここではゼロ知識証明を理解してもらうために、洞窟にある魔法の扉の問題という比喩を用いて非技術的説明にとどめる。

魔法の呪文で開く扉で区切られた洞窟があったとする（**図3**）。Pさんが、魔法の扉を開くための合言葉をもっているとする。洞窟は途中で分かれているが奥ではつながっていて、そこは魔法の扉で仕切られている。扉を開かない限り、入った方と反対側からは出られない。Vさんは、お金を払って合言葉を手に入れたい。しかし、Pさんが本当に合言葉を知っているのか事前に確認したい。一方、Pさんはお金を受け取るまでは、合言葉を教えたくない。これを解決するために次のようなプロトコルを考える。Pさんは右、または左の好きな方から洞窟に入る。Vさんは洞窟の外で待っているので、左右のどちらから入ったかわからない。しばらくした後、Vさんはランダムに、右または

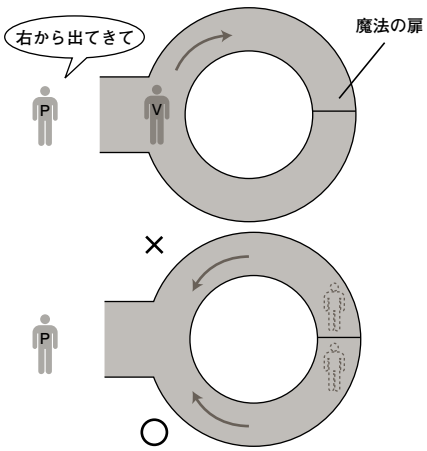

図3　洞窟の例
PさんはVさんが左右どちらかから入ったのかわからない。

左の出口から出るようにPさんに言う。ここでPさんが合言葉を知っているならば、左右どちらの出口を指定されても、秘密の扉を開けることで、指定された出口から必ず出ることができるはずだ。

しかし、もしPさんが合言葉を知らない場合は、入った入口からしか出られないため、指定された出口から出ることのできる確率は50%となる。以上の試行を数回繰り返すと、全ての回に指定された出口から出ることのできる確率はとても小さく、仮に10回も繰り返すと確率は0.1%未満となる。よってVさんは、Pさんが合言葉を知っているかどうか判別することが可能である。こうして、Pさんは合言葉自体を教えることなく、合言葉を知っている事実を証明するのだ。

より高度で安全な暗号を目指して

暗号は、安全性が満たされなければ意味をなさない。暗号はプロトコルに応じてそれぞれ必要な安全性が定義される。例えば、公開鍵暗号の安全性の概念には、秘匿性や頑強性などがある。秘匿性とは、暗号文から平文の情報が何も漏れない、つまりもともとのメッセージの情報が何も漏れないことである。ここでいう情報が何も漏れないというのは、暗号文から平文のどの一部分も知ることができず、平文が数字の場合にはある別な数との大小関係がわからないということだ。

例えば、秘匿性は先ほどの封じ手でも必要とされる。公開鍵暗号を使って封じ手は次のように作れる。まず、立会人Cが公開鍵を作る。対戦者Aは、日をまたぐ最後の一手を立会人の公開鍵で暗号化し対戦者Bにその暗号文を渡す。次の日、対戦者Aは前日に封じた一手とその一手を暗号化するときに利用した乱数を対戦者Bに渡す。暗号化手順はアルゴリズムなので、対戦者Aが正しい一手と乱数を公開していれば、前日得たのと同じ暗号文を作ることができ、対戦者Bは対戦者Aが前日にどんな手を封じたか確認できる。

ここで、対戦者Bは対戦者Aから前日に暗号文をあらかじめもらっているため、封じた手が何であるかわかってはならない。おそらく対戦者Bにとっては、試合展開から対戦者Aの一手をもともとある程度絞り込むことができるであろう。もしかしたら2つに絞り込めるかもしれない。暗号文からわずかでも平文の情報が漏れていれば、対戦者Bの読みと合わせて対戦者Aの手を特定できるかもしれない。暗号文が秘匿性をもつとは、言い換えれば対戦者Bに暗号文を与える前と与えた後で平文に関する知識が増えないということである。

一方、頑強性という安全性の概念がある。頑強性は、秘匿性を包含するより強い安全性の概念だ。例えば、封印入札を考える。オークションの出展者は公開鍵と秘密鍵を作り公開鍵を公開する。入札者は各自の希望する金額を書いた平文を出展者の公開鍵で暗号化し、その暗号文を出展者に送信する。出展者は暗号文を自らの秘密鍵で復号できるので、最終的な入札の最高額がわかる。一方、入札者は暗号文を見ても秘匿性から誰がいくらで入札したか出展者から発表があるまでわからない。よってオークションのプロトコルは秘匿性を満たす暗号を利用すれば構成できるようにみえる。しかし、奇妙なことにオークションのようなプロトコルでは暗号により強い安全性を求める。

今、Aさんは10万円と書かれた平文を暗号化して出展者に送信したとしよう。Aさんの暗号文は他の入札者も見ることができるとする。暗号文の秘匿性より、暗号文を見た後の平文、つまり入札額に関する知識は、暗号文を見る前の知識より増えないことが保証されているので一見問題ないは

ずである。しかしながら、次のような攻撃を防げるであろうか。BさんはAさんの暗号文を見た後、Aさんの入札額より常に1万円多い入札額を暗号化する。秘匿性より、BがAさんの入札額Xを知ることは無い。しかし、それはBがX＋1万円の暗号文を作れる可能性を否定するものではない。そして、そのような暗号文を作ることができるのであれば、Bは常にAさんに入札で勝つことができるわけである。頑強な暗号とは、与えられた暗号文から、その暗号文の平文と関係する平文の暗号文を作ることができないような暗号のことである。頑強性を満たせば秘匿性も満たすことは過去の研究の結果により知られている。

前述のとおり、公開鍵暗号は1970年代後半に、ゼロ知識証明は1980年代に発明されたものである。もちろん、これらの暗号が作られたあとも暗号の研究は続けられ、新たな暗号も作られている。それにもかかわらず、約30年前の暗号を利用し続けているのは、暗号として問題がないからである。では、先生は何のために研究しているのであろうか。単体では単純な機能しかもたないプロトコルも組み合わせることで、より高度なプロトコルとなる。ときには、公開鍵暗号やゼロ知識証明などのいろいろなプロトコルを組み合わせることが必要となる。プロトコルの安全性というのは、プロトコルが単独で動いているときを考えているため、プロトコルを組み合わせたときには安全性の証明が難しくなっている。つまり、既存のプロトコルを組み合わせて新たなプロトコルを作ると、また一からこのプロトコルの安全性を証明しなければならない。ここで先生は、他のプロトコルを組み合わせても安全性が自動的に保証されるプロトコルの作成を考えている。このようなプロトコルを汎用結合安全性のあるプロトコルという。

この汎用結合安全性をもつプロトコルというのは、理論的で、実用的でない場合も多い。その理由は効率が悪いからである。単独で安全なプロトコルより、汎用結合安全性をもつプロトコルの方が複雑になり、現代のコンピュータでは処理が追いつかないのである。現在は運用するには大変かもしれないが、これをどう効率良く作っていくか、ということを藤崎先生は研究している。

先生の暗号への思い

先生は、大学の数学科で学び、就職先の会社で暗号のグループに所属することになり、それをきっかけに暗号を研究しようと思い始めた。暗号というものは理論的な議論が多い。しかし、それに加えて実用的な側面ももつのが暗号の特徴である。実際に自分が作ったプロトコルが使用されたとき、意義を実感できると先生は言う。

公開鍵暗号やゼロ知識証明にみられるように暗号はトリッキーだ。一見不可能に思える仕組みを実現させてしまうおもしろさが暗号にはあるのだ。

暗号は10年前と比べ、純粋な学問に変化していると先生は感じている。現在、実際に使用されているのは原始的な公開鍵暗号やデジタル署名、共通鍵暗号といった30年前の暗号である。より高度な機能を備えた暗号が存在するがあまり利用されていない。このように、現段階における実用化をあまり考えず、現在のコンピュータの性能では利用が難しいような暗号を作るという方向に研究が進んでいる。先生が効率の良いプロトコルの作成を進め、また、コンピュータの性能の進歩が著しいので、10年後には実用の可能性もある。

現在使用されている暗号よりも導入が難しいが、複数の汎用結合性のあるプロトコルを利用することができれば、高度な機能をもつ暗号の安全性が高まる。先生は、この汎用結合性のあるプロトコルの利用によって、選挙などの高度な安全の保証が必要とされるプロトコルをデジタル化することができると考える。これには、汎用結合性のあるプロトコルが必要不可欠である。先生の研究によって、暗号におけるより高度な安全が保証されることとなるだろう。

執筆者より

取材では丁寧に説明をいただき、暗号についての理解を深めることができました。私自身、藤崎研究室を取材できたことを光栄に思います。お忙しい中、取材を引き受けていただいた藤崎先生に心より御礼申し上げます。

（松岡 雄己）