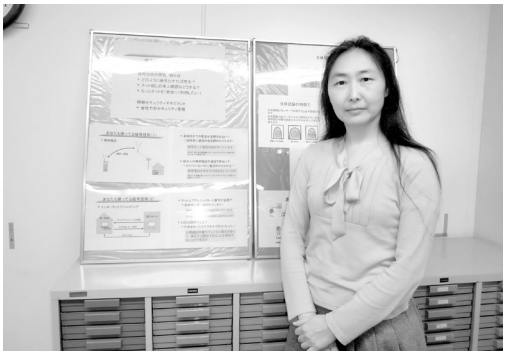
In Laboratory Now

研究室訪問 6

暗号プロトコルが創り出す未来

尾形 わかは 研究室～技術経営専攻



尾形 わかは 准教授

インターネットの普及で、コンピュータ間で通信を行う機会、特に個人情報や機密情報を送受信する機会が以前に比べ格段に増えている。その際に、情報が外部に漏れないようにするためには、情報を暗号化して送る技術が必要である。

尾形研究室では暗号プロトコルと呼ばれる、コンピュータ間での暗号を用いた通信のルールについての研究を行っている。本稿では、先生が主に行っている、暗号プロトコルの改良と、今注目のクラウドに応用できると期待されている検索可能暗号という暗号プロトコルについて取り上げる。

暗号プロトコルとは

インターネット上で個人情報を送信したり、メールで機密情報をやりとりしたりすることが増えている現代、暗号はなくてはならないものとなっている。尾形先生は、その中でも暗号プロトコルという分野に関する研究を主に行っている。

プロトコルとは、コンピュータ間で通信を行う際、事前に共有しなければならないルールのことで、どのような順序で、どのような内容の情報を送受信するかについて定めている。その中でも暗号プロトコルは、暗号を使った通信で用いられるプロトコルのことを指す。これは通常のプロトコルが定めていることに加え、どの段階で暗号化や復号をするのか、なども定めている。復号とは、暗号化された情報を元に戻すことである。

例として、信任投票における電子投票システムで使われている暗号プロトコルについて説明しよう。まず、投票所で一票一票に対してそれぞれの内容を決められた手順で暗号化する。次に、その暗号化されたデータを集計所に転送する。そして、集計所ですべてのデータを集め、復号すると投票結果が出る。この一連の流れを具体的に定めたものが暗号プロトコルだ。

先生は情報を安全に、かつ効率よく処理することができる暗号プロトコルを目指し、日々改良を行っている。続いて、どのようにして暗号プロトコルを改良していくのか紹介する。

暗号プロトコルの改良

暗号プロトコルの安全性

通信において情報が外部に漏れないようになっているとき、暗号プロトコルの安全性が保たれていると言う。安全性が保たれているかどうかは、いくつかの安全基準を満たしているかどうかで評価される。

今までに提案されてきた暗号プロトコルは、安全性が欠けているものが多かった。その原因は、大きく分けて二つある。一つは、現実に起こりう

る事象に見合った安全基準を定義できていないということである。

安全基準の定義の例として、安全基準の一つである秘匿性の定義について考えよう。秘匿性とは、限られた人間とシステム以外に対して、情報が漏洩しないように守られている状態のことである。秘匿性の定義を次のようにしたとする。まず、暗号を解読しようとする、攻撃者と呼ばれるプログラムを用意する。次に、任意の文章を暗号化し、その暗号文を攻撃者に渡す。そして、渡された暗号文を攻撃者に解読させる。解読結果が元の文章と完全に一致している確率が十分小さければ、秘匿性を満たしているとする。

この定義に従うと、仮に解読結果が元の文章とほとんど一致している場合でも、完全に一致しているわけではないため、秘匿性を満たしているとされる。しかし、現実的には元の文章のほとんどが解読されることは問題である。このように安全基準の定義が現実に見合っていない場合、必ずしも安全性が保たれているとは言えないのだ。

暗号プロトコルの安全性が欠けているもう一つの原因は、暗号プロトコルが安全基準を満たしていることの証明が完璧ではないということである。安全基準の定義はきちんとされていても、証明の途中で論理が破綻していたり、場合分けに漏れがあったりすれば、証明が完璧であるとは言えない。証明をきちんとしなければ、暗号プロトコルの安全性が保たれているとは言えないのだ。

多くの暗号プロトコルは、以上の二つの原因によって、安全性が欠けていた。しかしこれらの暗号プロトコルは、それぞれ優れた機能をもっている。そこで尾形先生は、これらを組み合わせることで、より安全性の高い暗号プロトコルを作り出している。

それでは、先生がどのようにして安全性が欠けている暗号プロトコルを改良しているのか説明しよう。初めに、現実に見合った安全基準の定義をし、その定義を既存の暗号プロトコル一つひとつに照らし合わせていく。こうすることで、ある場合においては安全基準が満たされているが、別の場合では満たされていないというように、暗号プロトコルがもつ特徴を知ることができる。次に、その特徴を参考にしながら、あらゆる場合で安全基準が満たされるように暗号プロトコルを組み合わせる。最後に、組み合わせた暗号プロトコルが安全性を保っていることを証明する。もし完璧な証明ができなければ、暗号プロトコルの組み合わせの一部を変えて証明し直す。

この手順の中で特に手間がかかるのが、暗号プロトコルを組み合わせていく作業である。それぞれの暗号プロトコルがもつ長所に注目して組み合わせていったとしても、その結果、今まで満たしていた安全基準が満たされなくなる場合があるからだ。このような試行錯誤を重ねながら、先生はより安全で、機能も充実した暗号プロトコルを作り出している。

Multi-secret sharing

尾形先生が改良した暗号プロトコルの一つに、秘密分散共有法という技術を用いたものがある。秘密分散共有法とは、情報の一部が漏洩してもその一部からは元の情報が推測できないように、情報を分散させる技術のことである。この技術によって分散された情報は、一定数集めなければ元の情報に戻すことができない。これによって安全に情報を共有することができる。

秘密分散共有法を用いた従来の暗号プロトコルはどのような仕組みになっているのだろうか。初めにデータの送り主は秘密分散共有法を用いて、データVをv_1, v_2, v_3というように分散させる。次に送り主は情報が漏洩しないように、分散した情報v_1, v_2, v_3をそれぞれ対応した受け手１，２，３に送る。そして受け手１，２，３は情報v_1, v_2, v_3を持ち寄って、データVを復元する。

従来の暗号プロトコルを用いると、送り主は新しくデータを共有するたびに、受け手の人数分の送信を行わなければならない。このため頻繁にデータを共有する場合には、送り主の負担が大きくなってしまうという欠点がこの方法にはある。

そこで最近、Multi-secret sharingと呼ばれる、掲示板システムを利用した暗号プロトコルが数多く提案されている。ここで言う掲示板システムとは、ある特定の人間が情報を書き込み、不特定多数の人間が閲覧できるシステムのことを指す。

Multi-secret sharingの一番の特長は、データを新たに共有するときに、掲示板システムに情報

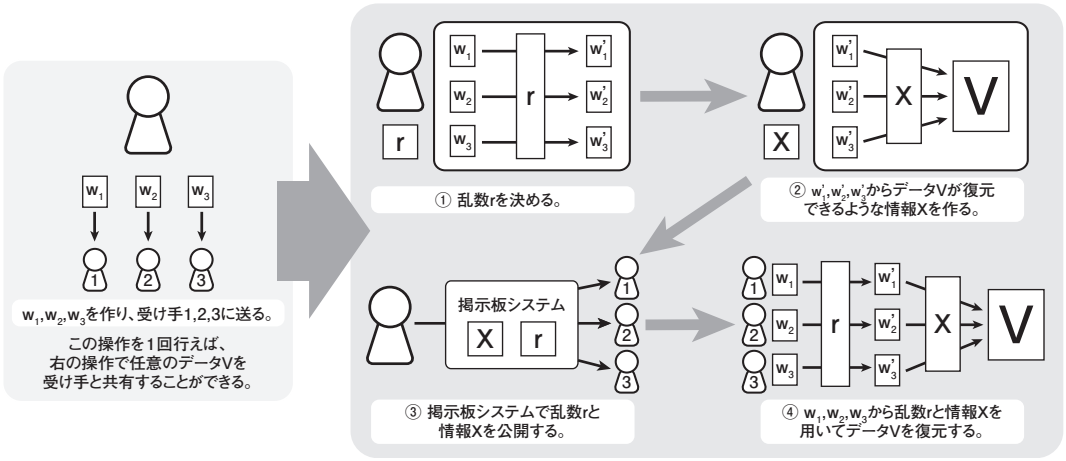


図1　一般的なMulti−secret sharingの仕組み

を一度書き込むだけで済むという点である。

それでは、Multi−secret sharingはどのような仕組みになっているのか説明しよう（**図1**）。あらかじめ、送り主は任意のデータw_1, w_2, w_3を対応する受け手1，2，3に送っておく。データVを共有する際は、送り主は乱数rと情報Xを決め、掲示板システム上に公開する。このとき、乱数rを用いてw_1, w_2, w_3をw'_1, w'_2, w'_3に変形し、それらと情報Xを合わせると、データVが復元できるようになっている。受け手1，2，3は乱数rを用いて得たw'_1, w'_2, w'_3を持ち寄り、情報Xと合わせてデータVを復元する。

Multi−secret sharingは、新たに違うデータを共有するときには乱数rと情報Xだけを変えればよい。そのため、送り主は毎回データを分散させて受け手一人ひとりに送るという作業をせずに済む。この方法によって、送り主の負担は従来に比べ軽減されるのだ。

しかし、過去に提案されてきたMulti−secret sharingの多くは二つの問題点を抱えていた。それは、安全であることの証明が完璧ではないため、必ずしも安全とは言えないという点と、送り主が掲示板システムに書き込まなければならない情報量が莫大であるという点である。

尾形先生は、Multi−secret sharingの暗号プロトコルを改良してこれらの問題点を解消した上、新たな機能をもつものにした。その新たな機能とは、データの復元の際に共有するデータが改ざんされることを防ぐというものだ。データVを復元する際、正しく復元できないことがある。この理由として、送り主が受け手に渡す情報を改ざんしている場合と、受け手の一人が送られてきた情報を改ざんしている場合が考えられる。そこで先生は、送り主が情報を改ざんしていないか、受け手がチェックできる機能と、受け手の一人が送られてきた情報を復号する段階で不正をしていないか、他の受け手がチェックすることができる機能の二つを加えた。この二つの機能によって、復号した結果が本当に正しいものかを確認することができるのだ。

先生は以上のように、既存のプロトコルを改良することで、より安全で機能も充実した暗号プロトコルへと進化させている。次に、現在先生が研究を進めている検索可能暗号について紹介する。

検索可能暗号

生体認証や電子投票などさまざまな技術が生まれている現在、従来にはなかった新たな機能を追加した暗号プロトコルが考えられている。その中でも先生が注目しているのが、検索可能暗号と呼ばれる暗号プロトコルである。

通常、文章を暗号化すると、その後は復号しない限りその文章から単語を検索することはできない。そこで、暗号化したまま検索ができるように改良した暗号プロトコルが検索可能暗号だ。

検索可能暗号は、クラウドと呼ばれる、インター

ネット上で提供されているさまざまなサービス全体に使えると考えられている。ここではクラウドのサービスの一つであるオンラインストレージを例に考えてみよう。

オンラインストレージとは、インターネット上でファイルなどのデータを保存するスペースを貸し出すサービスである。このサービスを使えば、利用者はハードディスクやUSBメモリなどを持たずに済む。しかしストレージを利用すると、データはストレージを管理している事業者の手元にすべて置かれることになるため、事業者はデータの中身を閲覧できてしまう。データの中身を暗号化すれば事業者がデータを閲覧することはできないが、ストレージ上でファイルを検索することもできない。つまり、単にファイルを暗号化して事業者に渡すだけでは、利用者は欲しいデータをすぐに手に入れることができない。そこで、検索できるようにうまく暗号化する必要がある。このように検索可能暗号は、オンラインストレージを始めとするクラウドのサービスを利用する上で、重要になってくるだろうと考えられている。

では暗号化された状態で検索できるようにするためには、どのような暗号プロトコルを作ればよいのだろうか。現在研究が進められている方法は大きく分けて方法αと方法βの二種類がある。

まず、二つの方法において検索を可能にするために、どのように暗号化しているのかについて説明しよう。どちらの方法においても、あらかじめ検索単語として考えられるものがすべて含まれている単語のリストを作る。そして、それを用いて、ファイル中にどの単語が含まれているのか、利用者は事前にすべてのファイルで調べておく。このとき検索単語の情報が漏洩しても問題がないように、リスト中の単語を暗号化し、その暗号化されたものをキーワード1、キーワード2、……というようにそれぞれ対応させる。また、その対応表を作っておく。

方法αと方法βでは表の作り方と暗号化する部分に違いがある(**図2**)。方法αでは縦列にファイル名、横列にキーワードをふった表を用意する。この表に、ファイルにキーワードが含まれているかいないかを一つひとつ書き込んでいく。そして、最後にキーワードごとに列全体を暗号化する。方法βではキーワードをすべて縦に並べ、その横にキーワードを含むファイル名をすべて書き上げていく。最後にファイル名が並んだ文章を暗号化していく。

次に、この二つの方法における実際の検索手順について説明しよう。方法αでは、まず利用者は検索する単語をサーバーに暗号化して送る(**図3**)。サーバーは対応表から検索単語に対応するキーワードを探し、それを利用者に送る。次に利用者はキーワードから暗号を解くための鍵を生成して、その鍵をサーバーに送る。そして、サーバーから検索結果を受け取る。

方法βでは次のような手順を取っている。まず利用者は検索する単語を暗号化したものと、その単語から生成された、暗号を解くための鍵をサー

方法α　　0:なし　1:あり

	key A	key B	key C	key D
File a	0	1	0	0
File b	1	1	0	1
File c	1	0	1	0

方法β

	どのファイルにあるか
key A	File a,File c,File d
key B	File b,File d
key C	File a,File b,File c

暗号化する部分

図2　方法αと方法βの暗号方式の違い

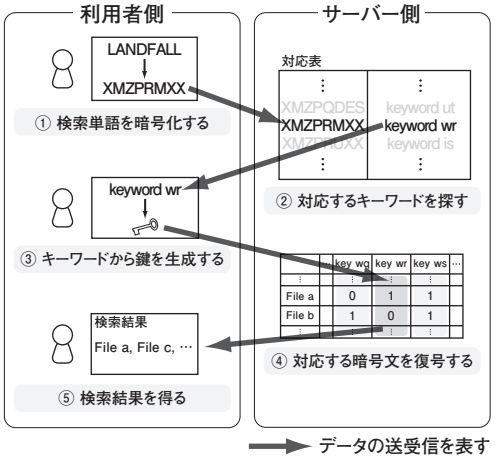


図3　方法αの検索手順

バーに送る。次にサーバーは対応表を用いて検索単語に対応するキーワードを探し、そこからさらにキーワードに対応する暗号文を探す。そして暗号文を鍵で復号し、検索結果を利用者に送る。

このように検索可能暗号の暗号プロトコルは方法αと方法βの二つがあるのだが、それぞれ欠点を抱えている。

方法αの欠点の一つは検索手順にある。検索において送受信される単語とそれを含むファイルがどのように関係しているのかは、暗号を解読する側にとって重要な情報である。これを隠すために、方法αでは通信を2往復しなければならない。一方、方法βでは通信を1往復するだけで済む。そこで先生は、方法αでも方法βのように通信が1往復で済むように改良を行っている。

一方、方法βは暗号を作る方法に欠点がある。方法βの暗号方式は、オンラインストレージにファイルが追加される場合を考えたとき、そのファイルに含まれる単語に対応する暗号文をすべて書き換える必要がある。また、ファイルが追加されたときにどの暗号文が変更されたのかがわかると、そこから追加されたファイルの中身が推測されてしまう可能性がある。

方法α、方法βの両方がもつ欠点も存在する。それは、あらかじめ単語のリストを作るため、新たに使われるようになった用語に対応できないという点である。オンラインストレージに追加されるファイルには、リストには含まれていない新たな用語が含まれている可能性がある。そのため、古いリストを使っていると正しい検索結果が得られない場合があるのだ。しかし、リストを更新するという作業は大変である。新たにリストに追加された単語がストレージ内のファイルに含まれているか、すべてのファイルで調べなければならないからだ。そこで先生は、どのようにしてリストを常に最新のものにすればいいのか考えている。

尾形先生は以上のような二つの方法がもつ欠点を解消し、実用化できるように改良を進めている。検索可能暗号という比較的新しい分野における先生の今後の研究に期待したい。

これからの暗号プロトコル

現在、検索可能暗号のように、暗号そのものに新たな機能をもたせた暗号プロトコルが考えられている。しかし高い安全性を保ったまま、このような暗号プロトコルを実際に利用することは難しい。なぜなら、安全性が高い暗号プロトコルは、暗号文の容量が無視できないほど大きくなってしまうなどの弊害があるからだ。

従来にない機能を兼ね備えた暗号プロトコルに最高レベルの安全性をもたせることは現在不可能である。仮にできたとしてもその暗号プロトコルは利便性がなく、実用的ではない。特にクラウドで使われる検索可能暗号において、利便性は必要不可欠であると先生は考えている。そこで先生はこれらの暗号プロトコルが実用化できるようにするために、実際に使用する際の影響があまり出ない程度に弊害が収まるように、安全性のレベルを下げることも考慮すべきだと考えている。

先生はさまざまな安全基準を定義し、それによってどの程度の安全性が保たれるのかを示すことが重要であると考えている。しかし、安全性の評価軸はさまざまなものがあり、絶対的なものはない。そのため、ある評価軸では最高レベルの安全性であっても、それが他の評価軸でも最高レベルであるとは限らない。そこで先生は、先生の考える評価軸を元に、安全性がどの程度保たれているのかという相対的な見方を提案している。

安全性のレベルの違う暗号プロトコルを用意することができれば、サービスを利用する人はその人のニーズによって安全性と利便性の兼ね合いを選ぶことができる。これによって、さまざまな機能をもつ暗号プロトコルが実用化されていけば、さらに便利な社会になっていくだろう。

今回は女性の方の研究室を紹介するということで、尾形先生にお話を伺いました。今回紹介した研究の他にも、先生はさまざまな研究を行っていますが、紹介できずとても残念です。お忙しい中、度重なる取材や質問に快く応じてくださった尾形先生に心からお礼申し上げます。　（伊藤 笙子）