明日のトップランナー

NTT社会情報研究所

藤堂洋介 特別研究員

次世代基礎理論の構築と目的特化型暗号が切り拓く「共通鍵暗号」の未来

情報通信のセキュリティを考えるうえで必要不可欠な技術である「暗号」．暗号の方式には「公開鍵暗号」と「共通鍵暗号」がありますが，今回は共通鍵暗号における基礎理論の構築と目的特化型暗号の研究に従事する藤堂洋介特別研究員にお話を伺いました．

◆PROFILE：2012年日本電信電話株式会社入社（修士卒），NTTセキュアプラットフォーム研究所所属．2015年CRYPTO Best Paper Award受賞，2017年博士号取得（神戸大学），2019年７月～2020年10月ルール大学ボーフム客員研究員，2020年CRYPTO Best Paper Award受賞．2021年４月～NTTセキュアプラットフォーム研究所 特別研究員．現在，NTT社会情報研究所 特別研究員．

暗号化と復号に共通の鍵を使用する「共通鍵暗号」

◆「共通鍵暗号」とはどのようなものなのでしょうか．

情報通信において，何かを隠す，守るといったようなことを考えたとき，最終的なよりどころとなるものが「暗号」です．そして暗号はセキュリティという大きなシステムを構成する最小単位のパーツ，いわば歯車であるといえます．この歯車が欠けたり，歪んだりしているとシステム全体に影響を与え，安全性の問題に直結します．そのため「いかに安全性の高い，高性能な歯車をつくり上げるか」を追求するのが暗号研究といえるでしょう．

暗号には，暗号化と復号に別々の鍵を使用し，そのうち暗号化の鍵を公開する「公開鍵暗号」と，暗号化と復号に同一の鍵を使用する「共通鍵暗号」とがあります（**図**）．

公開鍵暗号は庭の物置などに掛ける「南京錠」に例えることができます．南京錠は誰でもロックすることができますが，開けるときには専用の鍵が必要となります．南京錠をたくさん配布しておき，対応する鍵を持っている人だけが開けられるという仕組みが「公開鍵暗号」です．これをデジタル的に再現するには，素因数分解や離散対数問題，格子問題など，解くことが難しいような数学の問題を仕組みとして利用します．そのため，そうした難しい数学の問題を解くとき同様に，暗号化・復号にはコンピュータを使った複雑な計算が必要となります．

一方，共通鍵暗号は，旅館などにある「セキュリティボックス」に例えることができます．ロックを掛けるときにはある番号を入力し，解除するときには同じ番号を入力する仕組みです．共通鍵暗号は公開鍵暗号とは違い，使う環境に応じて効率的な計算を

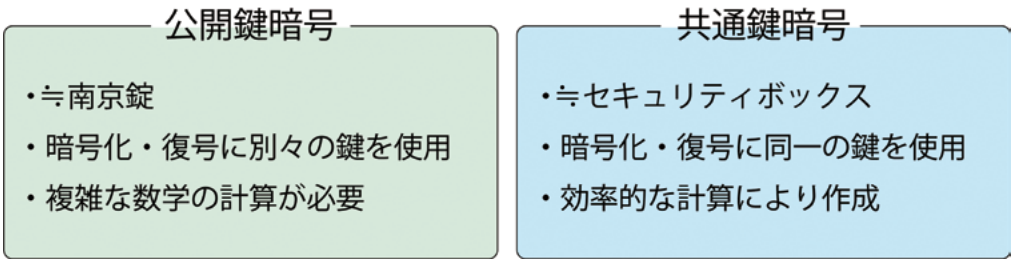

図　公開鍵暗号と共通鍵暗号

行ってつくり上げるという考え方が基本になっています．そのため，共通鍵暗号は公開鍵暗号に比べて100倍～1000倍の処理速度を持ち，大量の情報を扱う場合に適しています．

私はこのうち共通鍵暗号を扱っており，現在は中長期的には「次世代の共通鍵暗号基礎理論」，短中長期的には「目的特化型暗号とソリューション」を研究テーマとしています．

◆「次世代の共通鍵暗号基礎理論」はどのような研究なのでしょうか．

共通鍵暗号は公開鍵暗号と違い，解くことが難しい数学問題のようなバックグラウンドを持たないため，暗号自体が本当に安全なのかどうか，どうやって安全性を保証するのか，が非常に重要な課題となっています．

例えば古代ローマの政治家ガイウス・ユリウス・カエサルが使用したとされる「シーザー暗号」は暗号化前の文（平文）の各文字を決まった数だけシフトする共通鍵暗号とみなすこともできますが，いとも簡単に解読されてしまいます．一般的に，共通鍵暗号は誰でもつくることができますが，素人の設計では，すぐに解読されてしまうという欠点があります．共通鍵暗号を専門とする暗号学者の登場から半世紀近くが経ち，今では解読が難しいとされる暗号がいくつも開発されています．しかし，ある暗号にさまざまな攻撃を行いテストして安全性を保証できても，将来，暗号解読の天才が現れたときの安全性までは保証することはできません．

そこで，新たな解読方法・解析方法を発見したり，既存の解読方法・解析方法に対して絶対的に安全を保証するにはどうしたら良いかという方策を探索したりする研究が共通鍵暗号の基礎理論です．もちろん，本当の意味で「絶対に安全な暗号」を作成することは困難ですが，「特定の攻撃に対しては絶対に安全」のように少しずつ安全性を保証していくような取り組みです．

これは暗号学者としてはある意味ライフワークにあたるもので，私は入社以来「Integral Cryptanalysis」という解読方法に着目し，暗号の複雑度合い，専門用語でいうと「“代数次数”を正確に見積もることによる攻撃法の脆弱性」について研究しています．簡単にいうと「暗号が攻撃を受ける際，少なくともこのレベルよりは安全性は低いという，暗号の安全性を“上から押さえる”」研究です．その結果，暗号分野の最高峰国際会議といわれるCryptoにおいて，2015年に日本人として初となるBest Paper Awardを受賞し，さらに2020年には世界歴代3人目となる2回目の受賞を果たしました．また，最近は，少なくともこのレベルよりは安全性が高いという，安全性を“下から押さえる”研究にも取り組んでいます．

◆「目的特化型暗号とソリューション」はどのような研究なのでしょうか．

先ほど暗号を歯車に例えましたが，歯車は基本的にどこに使われるか分からない状態で製造されます．そのため，可能な限り安全性の高い，高性能な歯車をつくろうとするわけですが，世の中には当然「この製品にしか使わない」という特殊な歯車も存在するでしょう．

そこで，この歯車と同様に用途に合わせてオーダーメイドの暗号をつくろう，というアプローチが「目的特化型暗号とソリューション」の研究です．最近ではIoTデバイスやスマートカードでも個人情報など重要なデータを扱う機会が増加し，暗号化が求められるデバイスは多様化しています．それに対するソリューションとして，パソコンよりも計算能力が限られているようなデバイスにも実装可能な「軽量暗号」の研究を進めています．

目的に特化したオーダーメイド暗号の設計

◆共通鍵暗号の研究はどのような分野に活用が可能でしょうか．

「次世代の共通鍵暗号基礎理論」の研究は，攻撃者サイドに立った暗号の安全性を“上から押さえる”研究に，設計サイドに立った「少なくともこのレベルよりは安全性は高い」という暗号の安全性を“下から押さえる”研究も合わせ，汎用的な「標準暗号」を構築することが考えられます．現在の暗号の土台は40年前に構築されたものですから，新たな汎用的標準暗号が構築されれば，それが次世代の土台となって安全性を高めることができ，あらゆる分野で活用されるのではないでしょうか．

そして，目的特化型暗号の1つに「超低消費電力暗号」がありますが，これは医療分野での活用が期待されます．例えば，ある体内埋め込み型の医療機器が，人体に関するさまざまなデータを収集し，医療機関に送信することを想定してみましょう．そうし

た人命にかかわるセンシティブなデータは，剽窃や改ざんを防ぐため当然暗号化されるべきです．しかし，機器のバッテリーが切れるたびに再手術するのでは大変です．そこで，小さなバッテリーで長時間稼働するような機器が必要となり，暗号も消費電力を極力抑えることが求められるわけです．

これまでの暗号に対するアプローチは，ある意味汎用的で，すべての要素についてバランスを取り，全体のパフォーマンスを向上していくようなものでしたが，シチュエーションに合わせてある部分を犠牲にしても他のある部分の性能を振り切る，というものが私のめざす目的特化型暗号です．このほかにも小さなセンサなどでは回路規模を可能な限り小さくする，CPU～メモリ間の通信では遅延を可能な限り小さくするなど，用途に応じたさまざまな暗号が考えられます．

守秘義務のあるデータや個人情報を扱うような組織の方に情報の用途を伺って，それぞれの用途に特化した新しい暗号を作成するような活動ができれば面白いのではないかな，と考えています．

◆今後の研究の方向性について教えてください．

まずは究極の「耐タンパー性」をめざすことです．現在の暗号の安全性に関する研究では，平文と暗号文を第三者に見られることは想定していますが，その途中段階，つまり暗号化処理の工程を見られることまでは想定していません．しかし，すでにハードウェアの消費電力やそこから漏れ出てくる電磁波などの情報から暗号鍵を推測する「サイドチャネル攻撃」と呼ばれる攻撃が登場しています．ソフトウェアの場合はさらに深刻で，例えばスマートフォンにダウンロードしたアプリからリバースエンジニアリングにより暗号化部分のアルゴリズムを取り出すといったケースも出てきています．こうした暗号化処理の工程への攻撃に耐える強さを耐ダンパー性と言います．

こうした暗号化処理の工程を見られてしまうという状況の中，現在は100%安全とはいえなくても，万が一暗号化のアルゴリズムが流出した場合にも安全なものをつくる，「ホワイトボックスクリプトグラフィ」あるいは「グレーボックスクリプトグラフィ」といった研究分野にも注力しています．

◆現在の研究環境の特徴について教えてください．

NTTの強みは「優秀な人材が多い」ことです．私が10年前に入社したときには，まだ共通鍵暗号のことも，論文の書き方も，研究の進め方も知りませんでしたが，先輩方からたくさん指導していただいて今に至ります．新しい研究分野というものは自分で生み出さなければいけませんが，研究の基本を理解する過程においては，1人で勉強するよりも先輩方が切り拓き巧みに敷いたレールを辿るほうが，理解の質と速さの面でかなり有利でしょう．

また，現在同じ研究所に「暗号」という共通のカテゴリで複数の特別研究員がいるということも貴重ではないかと思います．1つのカテゴリに複数の特別研究員がいると研究に多様性が生まれますし，それが新しい技術の創造につながるのではないかと考えています．何より，特別研究員の指導を受ける若手研究者にとっても大きな成果を出せば任用されるという実績ですので，励みになるのではないかと思います．

（今回はリモートにてインタビューを実施しました）