URL https://journal.ntt.co.jp/article/32648
DOI https://doi.org/10.60249/25031301

NTT社会情報研究所
特別研究員

佐々木 悠 Yu Sasaki

IoT向け軽量共通鍵暗号の標準化と実装保護技術の研究

人間どうしのコミュニケーション用途だけではなく，さまざまなデバイスもインターネットにつながる時代になりました．その反面，インターネット上で流通する情報は，多岐にわたり個人情報や機密情報だけでなく，デバイスが発する情報が傍受され，犯罪などに悪用されるリスクも高まっています．通信の第三者の傍受を防ぐ「共通鍵暗号」の分野で，IoT（Internet of Things）デバイスの通信を想定した「軽量暗号」を研究されている佐々木悠特別研究員にお話を伺いました．

◆PROFILE：2007年電気通信大学電気通信学研究科情報通信工学専攻博士前期課程修了．同年，日本電信電話株式会社入社．2010年電気通信大学電気通信学研究科情報通信工学専攻博士後期課程修了．博士（工学）．2015～2016年Nanyang Technological University（NTU）にシニアリサーチフェローとして赴任．2022年から現在までアメリカ国立標準技術研究所（NIST）に海外客員研究員として赴任中．世界中の通信が暗号で保護される世界の実現のために安全性共通鍵暗号方式の設計・安全性解析研究に従事．2023年 International Association for Cryptologic Research（IACR）テストオブタイムアワード，2019年 第75回（平成30年度）電子情報通信学会 論文賞．

IoTで活用するような末端の通信まですべて暗号化し，あらゆる機器が暗号により守られる世界をめざす

■どのような研究をされているのでしょうか．

私の研究テーマは入社してからずっと同じで，共通鍵暗号について研究しています．暗号には公開鍵暗号と共通鍵暗号の分野があり，共通鍵暗号はその演算の速さや実装コストの低さから日常生活で利用するデータ通信の暗号化に使われています．共通鍵暗号の中にはデファクトとして国際的に標準化された暗号もあるのですが，設計の妥当性が不透明であるという問題もあるため，最先端の理論を取り入れ，安全と利便性がうまく両立されたことが誰から見ても分かるような暗号の設計をめざしています．

さらに，安全性評価が不十分な共通鍵暗号は，弱点をついて攻撃されると通信の情報を盗聴されるおそれもあります．それを防ぐ堅牢な要塞をつくるためには，敵の攻撃を事前に想定する必要があり，入社してからしばらくは「アタック」という暗号の解読技術の習得をしていました．アタックは公開された暗号に対し，さまざまな攻撃アプローチを試すことにより脆弱性を見つけ出し，安全ではないことを示します．もちろんアタック自体が目的ではなく弱点を克服し，すべての通信が守られている世界をめざしています．

公開鍵暗号の世界ではその安全性を「数学的に解読困難と証明されている問題」に帰着することで証明することができるのですが，私が研究している共通鍵暗号は職人の手により性能をチューニングしてセキュリティを担保するという，絶妙なバランスを取らなければいけない分野です．想定される攻撃や，過去の攻撃パターンなどを網羅して対策し，新たなアプローチでの攻撃も予測して対策するなど，職人気質な専門性が求められます．

■この研究がもたらす影響について教えてください．

共通鍵暗号の活用例として，IoTのような末端の通信に使われる「軽量暗号」があります．近年ではスマートシティプロジェクトなどが流行っている中で，スマートセンサなどが注目されています．もしすべてのガスメータにセンサが搭載されIP通信が可能になり，使用者のデータをガス会社がセンサから集め，月ごとの使用量と金額を算出して人を介在せず自動的に請求できるとします．では，そのガスメータの情報を暗号化せずに生のまま送るとどうなるでしょうか．

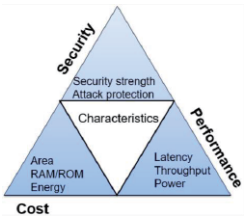
生のまま通信した電波を傍受する悪い人に情報が漏れてしまう可能性があります．それがどれぐらい問題になるかというと，「ここしばらくガス代が0円のため，この人は今留守なのだろう」ということが泥棒に知られてしまいます．ほかにも，ジョギングするときにGPSと連動して走行距離やタイム，ルートを地図上に表示するようなチップの通信が暗号化されていなければ，利用者の

軽量暗号に関するNISTの見解

- 汎用PCから限られたリソースを持つデバイス（RFIDタグ, センサー, IoT）への遷移に対応した暗号が必要.
- 暗号アルゴリズムの重量とは，ターゲットとなるデバイス・実装環境に依存した評価方法で計測される実装性能を指す.
  - ハード：回路規模，レイテンシ，処理速度，消費電力等
  - ソフト：RAMサイズ，コードサイズ，処理速度等
- さまざまな利用用途があるため，全性能で優れた暗号を1つ選ぶことは難しい．最適なトレードオフが重要.

汎用暗号では対応できない例

- AESの暗号化・複合を実装するだけのメモリがない16-bit マイコンが存在.
- ハッシュ関数SHA-3はもっと大きなメモリが必要．軽量版のSHA-3も存在するがまだ標準化されていない.



以下の資料から要点抽出
https://csrc.nist.gov/CSRC/media/Presentations/nist-lwc-standardization/images-media/session1-turan-update-on-nist-lwc-standardization.pdf

図　軽量暗号に関するNISTの見解

住所や生活パターンが漏洩します．それを防ぐため，末端のユーザに至るすべての情報を暗号で守ることが私の目標です.

最近では，その職人が悪い人で自分たちだけが簡単に暗号化された通信を解読できるようなバックドアを仕込む可能性もあるため，自分の設計した暗号の安全性を第三者に評価してもらう傾向があります．公の場で暗号の仕様を全部公開し透明性を高め，アカデミック等，公平な第三者から評価を受け安全性を認めてもらうことで信頼性を高め，「これは良い暗号だ」というコンセンサスがコミュニティにできたら，それを標準化して世界中の人にも私たちの技術を使ってもらえます．私はそこをめざして研究しており，暗号の標準化を見据えた設計を心掛けています.

NISTのコンペティションでは複数チームに所属し，暗号設計の選択肢を広げる

■研究環境について教えてください.

基礎的な研究は計算機科学に近く，例えば量子コンピュータが完成した際に今の暗号はどれぐらいのコストで解読されてしまうのかという未来について議論をする場合，想定する量子コンピュータはまだ存在しないので，紙と鉛筆でシミュレートするしかありません．このようなケースは頻繁に発生します.

私の研究テーマの１つは公開されている暗号への「アタック」ですが，アタックを考える際も誰かがつくった暗号を理解することから始めますので，まずは公開されているマニュアルやスペックを読み込みます．複数人でアタックを検討する場合は大学の研究室のような小部屋に皆で集まり資料を読みあさって議論しています.

その後，実際にこの暗号の脆弱性はどこなのか，過去に知られた攻撃が適用できないか，などの検証段階になると，最近では自動評価ツールをつくり，計算機サーバで実際に攻撃できるかを検討していきます.

現在私は米国のワシントンD.C.からすぐ近くにあるアメリカ国立標準技術研究所（NIST）に赴任しています．NISTは米国政府が使う標準技術を決める機関で，以前までは世界中からコンペティション形式で良い暗号を募集しており，私も複数チームに所属して応募していました.

チーム内の役割は安全性評価や各暗号のコンポーネント設計，速度計測など複数のタスクがあり，各専門家が集まり分業作業で暗号をつくり上げます．その中で私が専門としている軽量暗号の場合は使用する機器の問題も考えなければなりません[(1)]（**図**）.

対象がPCであれば電源から電気が供給されますが，IoTの場合はチップに電池が組み込まれていて，電池が切れたらもうその機械は使えなくなります．メモリもなく，そこまで高速に実装できるCPUもなく，使える電池は限られている，そういう状況で何を求めるのかを考え選択する必要があります.

しかし，高速演算と低消費電力は相反した目標ですので，両方を同時に達成することはできません．そのため特定のアプリケー

ションを考慮してそれに最適なバランスを実現するものを選ばなければいけないと考えています．

複数チームに参加している理由はそこにあり，このアプローチが得意なのはこのチーム，というようにチームにより特性が異なるため，より多くの選択肢を見つけるために複数のチームに参加していました．

つくり上げた暗号の安全性を示して「標準化」させ，多くの方に利用していただく未来をめざす

■現時点での研究の成果や，これからの展望について教えてください．

暗号研究は数学の研究に似た部分があり，理論的研究の側面があります．その点で現実利用を進めるというより，数学のように暗号理論を突き詰めるという作業をしています．この側面での成果といえば，多くの論文が採録されたり，私たちの活動の場でありコミュニティである国際暗号学会（IACR）から少しずつ重要な仕事を任されることが増えてきました．個人としても，NISTのコンペで最終選考に残るなど，少しずつ認められてきたと感じています．

研究所として「共通鍵暗号の研究の権威になる」ことを目標にしており，NTTの名前とともに「共通鍵暗号だったらNTTの佐々木に聞け」と言われるように努力していきます．

また，自分がつくった暗号を多くの方に利用していただきたいとも考えています．暗号を使ってもらう方法は2つあり，標準化して皆さんが自由に使っていただく方法と，実際にそのプロダクトをつくる中で自分たちの暗号の使用を提案する方法があります．

具体的にはSKINNYという軽量暗号を設計したのですが，2022年にISOで標準化されており，自分のつくった暗号も少しずつ使われる機会が出てきたと感じています．そのSKINNYの利用についていうとプリミティブとモードの2つのキーワードがあります．プリミティブとはエンジン設計，モードとはエンジンをどのように使ってどのような機能を実現するのかという使い方に該当し，SKINNYはそのエンジン部分にあたります．

数カ月前からは，私たちが提案していた「SKINNYを使ってどんな機能を実現するかというモード部分の標準化」についてもISOから国際標準化を開始する合意が取れたため，モードの標準化を進めているところです．

■NISTに赴任された経緯を教えてください．

1年の留学ではなく複数年にわたる長期の海外赴任は研究所の中でもかなり例外的かもしれません．NISTは，サイバーセキュリティの研究がとても盛んな場所にあります．従来，NTTとNISTには直接パイプはなかったのですが，5～6年前からNISTのコンピュータセキュリティ部門をとおして，NTTの研究者を受け入れてもらえることになりました．

前任者が3年ほどNISTに赴任し，任期が終わるころに誰か後任はいないかという話があったときに，当時のNISTの暗号研究者が私のスキルを知っていたこともあり，私を後任に選んでいただきました．

米国の標準技術は実質的な世界標準なので，米国の政府の組織で標準化の仕組みを学ぶことや，標準化の裏側で何が走っているかをみて今後の活動に活かしたいというモチベーションでしたので，3年間でとても貴重な経験をさせてもらいました．

近年，NISTのコンペティションは透明性の確保はできてもNISTの負荷が大きいため，NISTが主になって標準技術を決めていくという流れになってきました．そうなると，パブリックコメントとして世界中誰でも意見はできても，最終的に判断するのがNISTのため，標準化を決めるにあたってその内部にいることは非常に重要です．そのため，任期を延長してあと2年NISTに滞留し，標準を決める流れを直近でみていきたいと思っています．

■この研究における課題や困難だったことをお伺いできますでしょうか．

先ほど研究チームの分業体制について話をしましたが，やはり自分1人では専門性が不足するため，その各業務を各タスクの専門家にお願いをしなければいけません．そうなると，人脈などヒューマンネットワークもとても重要ですし，自分と同じ熱意と感覚の人を見極めるのは難しく苦労することが多いのですが，暗号研究者は仲が良い傾向があります．

まだ人脈がなく知識も不足していた時期，少しビクビクしながらも海外の研究会などに参加していましたが，急に参加者全員でグループディスカッションが始まったりします．そうしていくうちに少しずつ参加者の得意分野が分かり，自分のことも知ってもらうことで人脈が広がっていきました．今では国際的な研究会などに積極的に参加し，その世界でもっとも技術が優れている人を見つけています．

また，サイバーセキュリティと同様，暗号の研究も相当トレンドの流れが速く，アンテナを張り続けていないとあっという間に流行り廃りが変わります．2015年ぐらいまでは量子コンピュータを共通鍵暗号に応用する話はほとんど聞きませんでしたが，数年後にはとてもアクティブに研究が始まりましたし，今は当然AI（人工知能）を暗号に応用することも研究されています．暗号の設計でも多くの人がトライをしていますが，暗号の設計や暗号解読を全部AIに任せることできていません．しかし，AI関連の論文や研究はすごく流行っており，そういうところでも流行り廃りを感じます．

■この研究の魅力はどういうところにありますか．

共通鍵暗号は知恵比べのようなものだと思っています．公開鍵

暗号はすべてを数学で議論できる分野ですが，共通鍵暗号は職人気質な分野であり，やはり職人の腕を競うのは楽しいものです．カジュアルな話をすると，私は昔からパズル作家をしており，ひねりが効いた数独やクロスワードの問題をつくって知恵比べをするのがもともと好きだったので，同じようにアイデア１つで良いものもできるし，逆に悪いものにするところに魅力を感じています．

例えばアタックにおいて，皆が安全だと思っても自分がその弱点を見つけられ，しかるべき機関に報告できたときには，達成感があります．

ほかにも，暗号設計が完成して，その設計が良いものだと認められた瞬間というのはやはり嬉しいものです．ISOで標準化された瞬間や，NISTのコンペティションで第１ラウンド，第２ラウンド，ファイナリストと勝ち進んだところは少しゲーム感覚を彷彿させるような楽しみがありました．

■若き研究者の方や学生，ビジネスパートナーへのメッセージをお願いします．

日本にいたときは学生の方と共同研究する機会があり，そういうときには研究者の道も楽しいよという話をしていました．

その楽しさはいろいろありますが，私自身は国を越えて活動できるのが楽しいと感じるので，今NISTにいるのもそうですが価値観も違えば生活も違うのに，数式なり計算式の話で語り合えることも面白く思います．出張に行くだけでもいいと思いますし，そういう異文化の体験はとても楽しく学びがありますので，国際的な研究をすることはお薦めです．

基礎研究をやりたい方に関しては，研究のアイデアで生きていくしかありません．私が研究している共通鍵暗号の世界は知恵比べのようなものなのですが，知恵が出なくて辛いこともあります．しかし，何にも思いつかないということも経験上あまりなくて，苦しめば苦しんだ分，何かの役に立つアイデアや成果は出てくるものです．

また，研究する機関としてNTTはとてもいい機関だと感じています．大学などで研究されている方も多いと思うのですが，どうしても大学の業務や資金面でも苦しまれているのを見ています．NTTは，少なくとも今は暗号の研究に関して価値を認めてくれて，自分のやりたいことを後押ししてくれます．もちろん会社と意識を合わせ，会社にとっても必要なことをするのですが，やりたいことを思い切ってやらせてくれる会社です．

さらに私がいるグループは，基礎研究の重要性を認めていて，自分が選ぶ大学で共同研究留学をして，技術を学ぶなり経験を積めるようにしてくれます．2015年にシンガポールのNanyang Technological Universityに１年間留学させてもらいました．

人間関係でいえば，各個人がプロフェッショナルで実績も多いので，お互いにリスペクトし合っています．逆にいえば，同じグループの同僚と研究テーマが離れているということでもありますが，阻害要因ではなく，ある程度距離を保ってお互いにリスペクトを持って，良い雰囲気でやっています．NTTの研究者の特徴として，科学や技術に向き合って楽しみながら真摯に取り組んでいる方ばかりなので，研究をしたい人には，NTTなら良い環境で研究ができるのでお薦めです．

また，私は現在NISTで客員研究員というポジションにいますが，２年後には日本に戻ります．すでに具体的な話もみえてきていますが，今後は日本のプロダクトやプロトコルに実際に私が設計した暗号の活用を提案していきたいと考えています．

ビジネスパートナーの方にはぜひ実際にお話をお伺いして，需要に合ったできる限り良いものを設計したいと考えていますので，アイデア交流をどんどん行っていきたいと思っています．

■参考文献

(1) https://csrc.nist.gov/CSRC/media/Presentations/nist-lwc-standardization/images-media/session1-turan-update-on-nist-lwc-standardization.pdf

（今回はリモートにてインタビューを実施しました）