国立研究開発法人情報通信研究機構

NICT NEWS

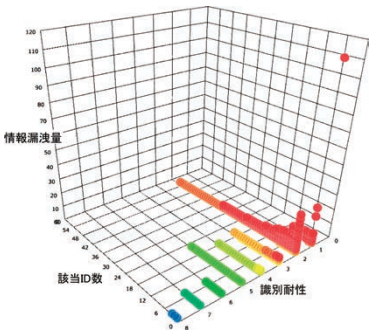
2019
No.2
通巻 474

FEATURE

暗号技術の最前線

NICT NEWS 2019 No.2 通巻474
国立研究開発法人情報通信研究機構

CONTENTS



FEATURE

TOPICS

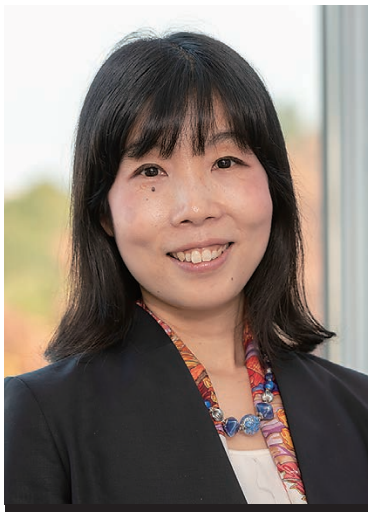
INFORMATION

表紙写真
議論するセキュリティ基盤研究室のメンバー。各メンバーは研究室で推進中の複数の研究プロジェクトに関わっており、和気あいあいと議論を重ね、有機的に連携しながら活動を行っています。
左上写真：安全なデータ加工を支援するプライバシーリスク評価システムURANUS（ウラヌス）。個人情報から名前等を削除するなど加工したデータに対して、個人特定のリスクを評価するツール。少ない情報で個人が特定され（識別耐性が小さく）、特定時の情報漏洩量が大きいケースを赤丸で示し、リスクの大きさを事前に注意喚起します。

INTERVIEW

安心・安全なデータ利活用を目指して

暗号研究の最前線を探る



盛合 志帆（もりあい しほ）
サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
大学卒業後、日本電信電話（株）、ソニー（株）を経て、2012年から現職。
暗号、情報セキュリティ、プライバシーに関する研究に従事。博士（工学）。

暗号技術は、インターネットが普及した現代社会に欠かせない重要な技術だ。この暗号が今、ある意味「危機」を迎えている。このところ急速に研究が進んでいる量子コンピュータが実現すると、現在広く使われている公開鍵暗号が簡単に破られてしまうためだ。

米国立標準技術研究所（NIST＊1）は、量子コンピュータに耐性のある「耐量子計算機暗号」（PQC＊2）の標準化に向けて準備を進めている。

これからの情報通信技術の激動の時代に、暗号技術はどのように変わり、社会に実装されていくのか。

暗号技術によるICTのセキュリティ基盤の研究をしているサイバーセキュリティ研究所セキュリティ基盤研究室室長の盛合志帆に話を聞いた。

■IoT時代にますます重要となる暗号技術

――暗号の歴史は古いですが、ネット社会になった今、暗号は不可欠な技術になっていると実感しています。暗号技術の変遷など基本的なところを教えてください。

盛合　暗号の歴史は古く、紀元前1世紀の古代ローマ時代にシーザーが使ったシーザー暗号がよく知られています。これは、アルファベットの文字を数文字ずらして伝達する素朴なものでした。暗号が大きく変わったのは、インターネットなどのネットが発達してからです。

ネットによる通信が盛んになるとともに、企業間の商取引に関わる通信、政府の調達や外交情報など、第三者に見られては困る情報がたくさん出てきました。そこで、ネットワークで安全に情報を送るため、暗号技術が急速に発達していきました。

最初は暗号のアルゴリズムを他者に隠すことでメッセージの内容を秘匿していたのですが、それでは不特定多数の人たちの間で利用することができません。そこで、アルゴリズムを公開しても、暗号を解く鍵さえ秘匿していれば安全性が保たれるような暗号が開発され、1977年にNISTの前身であるNBS＊3によって米国政府標準暗号DES＊4として制定され、これが世界標準となっていきました。

この頃から本格的にネットワークが普及し始め、暗号技術の研究が進んでいきました。このあと、DESはAES＊5というものに変わりましたが、どちらも共通鍵暗号です。また、DESが開発された頃、暗号技術に大革命をもたらした公開鍵暗号も登場してきました。

――公開鍵暗号とはどういうものですか。

盛合　暗号は、鍵（数字の列）を使って暗号化と復号を行います。共通鍵暗号は、暗号化も復号も同じ鍵を用います。特定の相手方と通信する場合は処理が早くて便利なのですが、事前に鍵を相手に渡して共有しておかなければなりません。この事前共有のコストが高いことと、第三者に漏れるリスクがあることが課題です。

これに対して、公開鍵暗号は、公開鍵と秘密鍵をペアで生成して、公開鍵を公開しておきます。通信したい人は相手の公開鍵でメッセージを暗号化して情報を送ると、相手方は自分の秘密鍵で復号できます。公開鍵暗号を用いて、共通鍵暗号で使う鍵を事前に共有することができるようになり、安全性が高まりました（次頁図参照）。

公開鍵暗号の代表的なものがRSA＊6暗号で、私たちがインターネットで使っているTLS＊7というセキュア通信プロトコル標準にも使われています。

――インターネットで暗号はどう変わってきたのでしょうか。

盛合　インターネットで様々な情報がやり

＊1 NIST: National Institute of Standards and Technology
＊2 PQC: Post-Quantum Cryptography
＊3 NBS: National Bureau of Standards
＊4 DES: Data Encryption Standard
＊5 AES: Advanced Encryption Standard
＊6 RSA: Rivest, Shamir, Adleman
＊7 TLS: Transport Layer Security

INTERVIEW

安心・安全なデータ利活用を目指して

暗号研究の最前線を探る

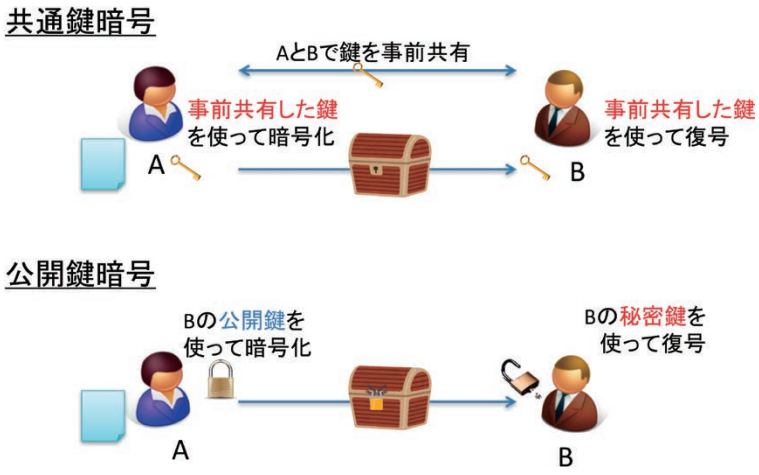


図　暗号技術の基本となる共通鍵暗号と公開鍵暗号

とりされるため、これを守るための暗号化技術も高度化してきています。電子メールでやりとりされるプライバシー情報や、電子マネーやクレジットカード情報などお金に関わる重要な情報もあります。これらの大切な情報を守るために暗号技術は欠かせないものとなっているのです。

今後は、IoTが普及していき、あらゆるものがインターネットにつながります。すなわち、あらゆるものがサイバー攻撃のターゲットになる可能性があるということです。このような中、暗号技術がますます重要になっていきます。

■ 3つの重点研究開発項目

―― NICTの暗号技術に関する取組を説明していただけますか。

盛合　NICTでは5年ごとに中長期計画を立てていまして、今年度は第4期中長期計画（2016～2020年）の3年目となっています。我々の研究室では、この中長期計画の課題として、機能性暗号技術、暗号技術の安全性評価、プライバシー保護技術の3つの研究開発に取り組んでいます。

――では、まず機能性暗号技術について聞かせてください。

盛合　これからはIoTの普及によって新しいニーズが生まれてきます。これにこたえることができるような新しい機能をもつ暗号技術を作ろうというのが本研究の目的です。例えば、IoTデバイスは小型で省電力、メモリサイズも小さいという特徴があり、従来よりも軽量な暗号が必要となります。

また、暗号化したままビッグデータ解析を行う技術も研究しています。ユーザがビッグデータ解析をしたい場合、しばしばデータをクラウドに保存したり、外部の機関に委託したりするケースが出てきます。このとき、個人情報が漏洩しては困ります。そこでデータを暗号化するのですが、暗号化してしまうと普通はそのままでは解析できません。現在、暗号化したままデータを解析できる「準同型暗号」の研究が世界的に進展しています。しかしながら、暗号化されているがゆえに、正しいデータに対して解析を行っているのか分からないという課題がありました。この課題に対して、誤データの混入を検知する機能をもった「まぜるな危険準同型暗号」という技術を提案しました（詳細はP4-5参照）。この技術によって、プライバシーを保護したまま安全にビッグデータ解析が行えるようになりました。昨年、筑波大学と共同で、個人の遺伝子情報と病気の罹患情報との統計的な関連性を、暗号化したまま安全に解析することに成功し、プレスリリース（プライバシーを保護したまま医療データを解析する暗号方式を実証（2018年7月18日） https://www.nict.go.jp/press/2018/07/18-1.html）を行っています。

――2つめの暗号技術の安全性評価についてもお願いします。

盛合　暗号技術の安全性評価に関する研究は、安心・安全なICTシステムの維持・構築に貢献することと、新たな暗号技術の普及・標準化に貢献することを目的としています。その一つの活動が、電子政府推奨暗号等の安全性を評価し、安全なICT社会の実現を目指すCRYPTREC（クリプトレック）*8というプロジェクトの運営です。本プロジェクトは、総務省、経済産業省及び独立行政法人情報処理推進機構と共同運営しています。例えば、量子コンピュータの実現のような大きな技術革新があると、実社会へのインパクトが計り知れません。実現すると、現在のインターネット上でのセキュア通信を支えている公開鍵暗号が破られてしまうため、今から対策を準備しておく必要があります。

――量子コンピュータはいつ頃実現するでしょうか。

盛合　予想は難しいですが、今使われている公開鍵暗号が量子コンピュータによって破られることは数学的に証明されているので、何もしないわけにはいきません。

公開鍵暗号の安全性に直接的なインパクトを与えるとされているのが、量子ゲート方式の量子コンピュータですが、現在使われている強度のRSA暗号を解読できる規模のものが実現するのはまだ先だと思います。一方、量子アニーリング方式のものは商用化が進んでいますが、これは最適化問題を解くのが得意なコンピュータで、RSA暗号の数学的根拠となっている素因数分解を解く手法の検討と評価を富士通研究所や東京大学と共に行っていますが、大きなパラメータの問題を解くのは難しいと考えています。

――3つめのプライバシー保護技術とはどういうものでしょうか。

盛合　パーソナルデータの利活用に貢献するための研究開発を様々な観点から進めており、P8-9で紹介する「プライバシー保護データ解析技術」のほか、匿名加工技術の評価技術についても取り組んでいます。2017年5月に、改正個人情報保護法が施行され、匿名加工情報というものが導入されました。特定の個人を識別することができないように個人情報を加工し、元の個人情報を復元することができないようにした「匿名加工情報」であれば、本人の同意を得ることなく、個人情報を第三者に提供できるというものです。

2019年から個人データを預かって管理する「情報銀行」等の事業が本格化したり、匿名加工医療情報を利活用したいと考えている企業もあります。社会実装に向けて、いかに再識別のリスクを低減して安全性を保ち、データの有用性を保ったまま加工するか。当研究室では、この匿名加工情報の安全性や有用性の評価も行っています。

このような取組は、NICTのみならず、2015年から情報処理学会コンピュータセキュリティシンポジウムにて、PWS CUP匿名加工・再識別コンテストを実施するなど、安全で有用性の高い匿名加工技術の開発を促進するために、業界全体で取り組んでいます。

――中長期計画最終年度である2020年の目標は何でしょうか。

盛合　耐量子計算機暗号の標準化を進めていかなくてはなりません。これまで新しい暗号技術の本格普及までには20年近い時間がかかってきたので、量子コンピュータがいつ完成したとしても間に合うよう、安全性を保つことができる耐量子計算機暗号の安全性評価と標準化が急務です。これを巡っては現在、国内外でいろいろな動きがありますが、特に米国のNISTが進めている標準化の影響は大きいです。

これまで多くの暗号技術について、NISTが主導して国際的デファクトスタンダードを作ってきた経緯があり、この標準化動向を世界各国や関係団体が注視しています。NISTは耐量子計算機暗号標準のドラフトを2022～23年頃を目標に発表することを表明しており、NICTとしても、耐量子計算機暗号の安全性評価や、国内のCRYPTRECにおける各府省の情報システム調達に参照される暗号技術に関する検討に貢献したいと考えています。

■目指す目標

――国立の研究開発機関としての役割は

国立研究開発法人として私たちが心掛けていることは、暗号技術の安全性評価について、公的な立場で中立公正で信頼性の高い情報を継続的に発信していくことです。

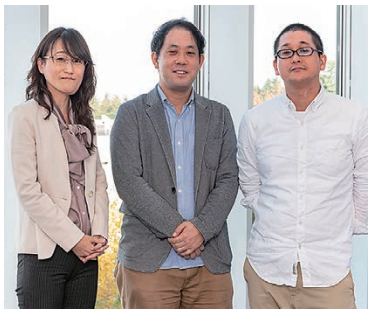
また、セキュリティだけでなく昨今関心の高まっているプライバシーをいかに守るかという課題にも取り組んでいきます。両者とも、今後ますます重要になっていますので、その研究拠点としての役割を果たせるよう尽力したいと考えています。

さらに、社会で実際に活用される研究成果を出し、世の中の役に立つ技術を目指すという気持ちで研究室一同頑張っていきたいと思います。

＊8 CRYPTREC: Cryptography Research and Evaluation Committees

準同型暗号の安全性向上について

個人情報を含んだビッグデータの安全な利活用に向けて



左から大久保美也子、江村恵太、林卓也

所属はすべて
サイバーセキュリティ研究所
セキュリティ基盤研究室

江村 恵太（えむら けいた）
主任研究員
2012年NICT入所。準同型暗号の安全性向上や匿名認証，安全な鍵失効技術等の研究に従事。博士（情報科学）。

大久保 美也子（おおくぼ みやこ）
主任研究員
前職NTTより2010年NICT入所。暗号アルゴリズム・暗号プロトコルの研究に従事。博士（工学）。

林 卓也（はやし たくや）
主任研究員
2018年NICT入所。暗号工学、暗号解析、プライバシー保護データマイニングに従事。博士（機能数理学）。

セキュリティというとニュース番組等でも頻繁に報道されるようになり、その重要性については世間的に認知されているものと思います。我々が研究している暗号理論はセキュリティの一分野ですが、暗号というとどのような印象を持たれるでしょうか。合言葉やパスワード、詳しい方でしたらネットショッピングで利用されていることもご存知かもしれません。暗号の基本的な機能・安全性として

［秘匿］　データを暗号化し、第三者に秘密にする
［改ざん検出］　データ書き換えの有無をチェックする
［相手認証］　通信相手が正しいかどうかチェックする

などを実現することができます。さらに、高い機能性を持った暗号方式が多く提案されており、今回はその中でも準同型暗号という方式とその安全性向上について紹介します。

■準同型暗号の仕組

準同型暗号というと難しい印象を持たれるかと思いますが、端的に言うと

暗号化したまま、暗号化されたデータに対して何らかの処理を行う

ことが可能な暗号方式です（具体的には、加算と乗算を行うことができます）。例えばある候補者の信任投票にて、賛成の場合は1を反対の場合は0を投票するというルールにすると、投票結果を足し算した結果が賛成票数に相当します。ここで自分が賛成したのか反対したのかという情報を漏らしたくない場合、暗号化することで上記の秘匿性により第三者には投票結果を知られないようにできます。しかしこの場合、どうやって集計するのでしょうか？一度暗号文から投票結果に戻し（暗号ではこの処理を復号と呼びます）、結果の足し算を行うと、どの暗号文が賛成を暗号化したのか反対を暗号化したのかという情報が漏れてしまいます。準同型暗号を用い、暗号化したまま足し算をすることで、賛成若しくは反対の暗号文から賛成票数の暗号文を復号することなしに計算することができます。暗号化したまま処理ができる準同型性を用いると、個人情報を含んだデータを扱う銀

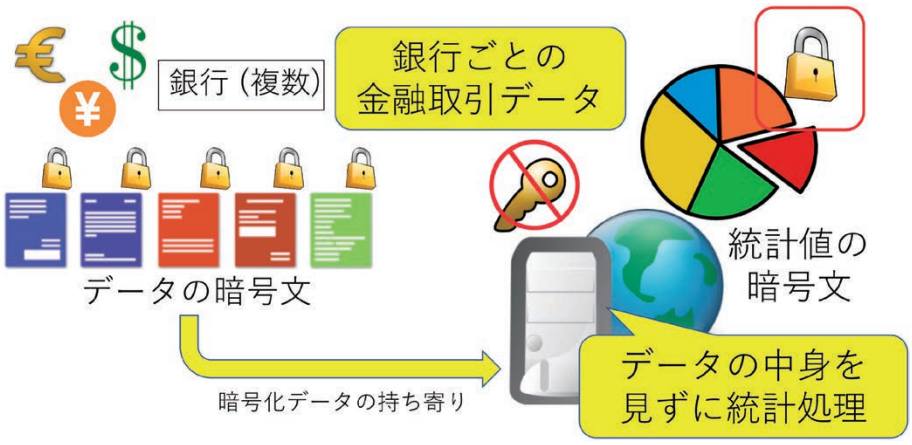


図1　複数組織データ利活用を促進するプライバシー保護データマイニング

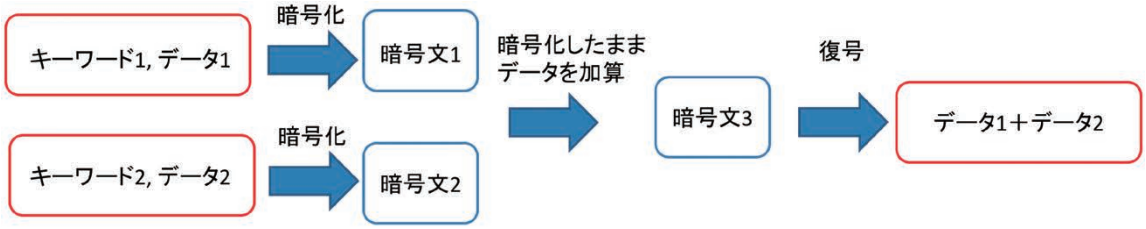


図2　同じキーワードに対する準同型演算（キーワード1=キーワード2）

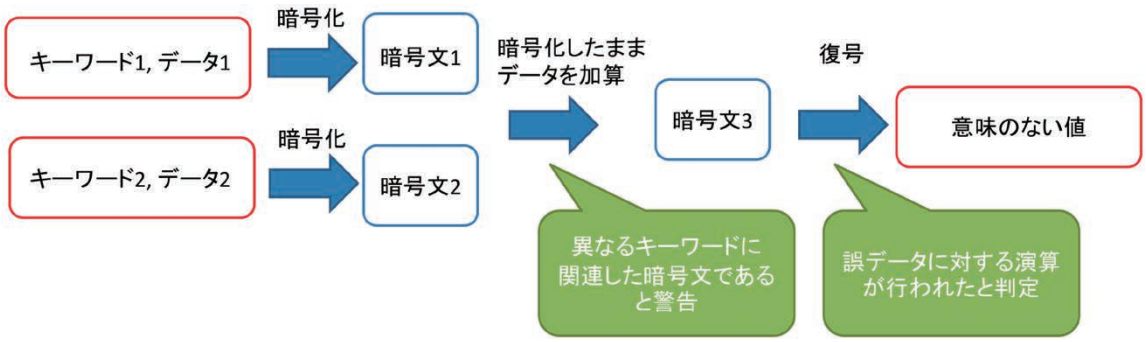


図3　異なるキーワードに対する準同型演算（キーワード1≠キーワード2）

行や病院などにおいて、データの解析を第三者に委託するなどの応用も考えられます（図1）。特に、通常は開示できないデータを暗号化し持ち寄ることで複数組織にまたがったデータを利用できるようになります。これを解析することで、1組織では知り得なかった新しい事実が発見できるかもしれません。個人情報を含んだビッグデータの利活用に向けて、準同型暗号は注目を浴びています。我々の研究室でもJST CRESTプロジェクト「複数組織データ利活用を促進するプライバシー保護データマイニング」を進めています。

■準同型暗号の安全性向上

暗号化したまま何が可能なのかというトピックは他研究者の稿に任せ（本誌P8-9、レ チュウ フォンほか、「プライバシー保護データ解析」を参照ください）、ここでは準同型暗号の安全性向上について本研究室の成果を紹介します。先ほど暗号の重要な機能・安全性の一つとして、改ざん検出を紹介しました。暗号化したまま処理が可能、すなわちあるデータの暗号文を別のデータの暗号文に変換可能という準同型暗号の機能を安全性面から見ると、実は暗号文が改ざん可能ということを示しています。秘匿と改ざん検出の両方を保証する安全性として、CCA安全性というものが定義されています。ここでは詳細には説明しませんが、例えばCRYPTREC電子政府推奨暗号リスト（https://www.cryptrec.go.jp/list.html）には、秘匿目的で使用される暗号方式としてCCA安全性が数学的に保証された方式が掲載されています。しかしながら準同型暗号は理論上CCA安全性を満たすことはできません。そこで我々は準同型演算用の鍵を新たに導入することで、準同型性とCCA安全性を同時に満たす方式「鍵付き準同型暗号」を提案しました。本成果は2012年 暗号と情報セキュリティシンポジウム（SCIS）にて最高賞に当たるイノベーション論文賞を受賞しました。

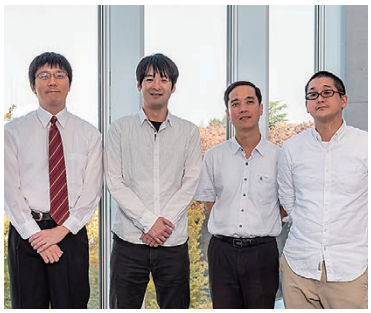
さらに、準同型演算時には暗号化されているがゆえに、正しいデータに対して処理を行っているのかわからないというジレンマがあります。例えば医療データの処理を行う際に、異なった病気のカルテが混在していたとしても、暗号化されているため検知できません。そこで我々は前述の鍵付き準同型暗号を改良し、誤データ混入防止機能を持つ「まぜるな危険準同型暗号」を提案しました。病名等をキーワードとして指定することで、異なるキーワードに関連付いた暗号文に対する準同型演算を防止することができます（図2、3参照）。なおキーワード自体も暗号化されるため、第三者に漏れることはありません。本方式を用いることで、解析中にデータの中身を見ることが許されない銀行や医療データ等に対して、解析対象外のデータが混在した場合でも高速に検出することができ、その解析結果が正当であることを暗号理論的に証明することができます。本成果は2016年コンピュータセキュリティシンポジウム（CSS）において、最優秀論文賞を受賞しました。現在、更なる効率改善として、暗号方式を動作させるうえで必要な数学的要素である楕円曲線上の双線形写像について、より効率的な演算が可能な曲線へ変換する技術を開発し、「まぜるな危険準同型暗号」に適用しています。

■今後の展望

準同型暗号は暗号化したまま計算ができるというユニークな機能を持ちますが、そのために普通の暗号方式で扱われた安全性をそのまま適用することが困難な場合があります。今後も、準同型暗号の安全性向上に向けて研究開発を行い、個人情報を含むビッグデータの利活用を安全に行える基盤技術を開発していきます。

耐量子計算機暗号の開発及び標準化

量子計算機によって暗号が高速に解読されてしまう脅威への対策



左から、青野良範、篠原直行、レ チュウ フォン、林卓也

所属はすべて
サイバーセキュリティ研究所
セキュリティ基盤研究室

篠原 直行（しのはら なおゆき）
主任研究員
2009年NICT入所。公開鍵暗号の安全性評価の研究に従事。博士（数理学）。

青野 良範（あおの よしのり）
主任研究員
2011年NICT入所。暗号の解読アルゴリズムの研究および安全性評価の仕事に従事。博士（理学）。

金森 祥子（かなもり さちこ）
研究技術員
2010年NICT入所。プライバシーに関する研究開発に従事。

黒川 貴司（くろかわ たかし）
研究技術員
2010年NICT入所。暗号技術の安全性評価に関する研究開発に従事。

林 卓也（はやし たくや）
主任研究員
2018年NICT入所。暗号工学、暗号解析、プライバシー保護データマイニングに従事。博士（機能数理学）。

レ チュウ フォン
主任研究員
2015年NICT入所。暗号アルゴリズムの設計、プライバシー保護データマイニングに従事。博士（学術）。

暗号技術は安全な通信や情報の保護のために欠かせない技術であり、携帯電話、電子パスポート、無線LAN、ネットショッピングやネットバンキングなど、身近なところで広く使用されています。近年、量子計算機の開発が進み、そのことによって現在利用されているいくつかの暗号技術の安全性が近い将来に大きく低下することが懸念されています。その対策として、量子計算機を用いた解読に対しても安全性を保つことが期待される暗号技術（耐量子計算機暗号：Post-quantum cryptography（PQC））の開発及び標準化が世界的に活発に進められています。本稿ではセキュリティ基盤研究室の成果を紹介します。

■耐量子計算機暗号が必要とされる理由

量子計算機による解読が懸念される暗号としてRSA暗号と楕円曲線暗号が挙げられます。これらは広く使用されている代表的な公開鍵暗号です。また、その懸念の理由は、これらの暗号で利用される数学的な構造及びShorのアルゴリズムと呼ばれる量子計算アルゴリズムに関係があります。

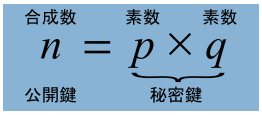
RSA暗号では、図1のように2つの素数が秘密鍵と呼ばれる秘匿すべき情報として利用され、それらの素数の積が公開鍵と呼ばれる誰でも取得可能な公開情報として利用されます。したがって、公開鍵である合成数を素因数分解することができれば秘密鍵を取得されてしまいます。そこで、現在使用されているRSA暗号では、現時点で素因数分解を最も効率よく計算するアルゴリズムである数体ふるい法を用いて、世界最速のスーパーコンピュータで十分な時間（1年など）計算しても解読できないように、公開鍵の大きさ（鍵長）を2048 bit（617桁）に設定しています。もし、数体ふるい法より計算効率が良いアルゴリズムが発見されても、またスーパーコンピュータの性能が向上しても、鍵長を十分大きくすることでRSA暗号の安全性を保つことができます。しかし、鍵長を大きくしすぎると、暗号処理にかかる時間も膨大になり、実用的ではなくなってしまいます。Shorのアルゴリズムは量子計算機を用いて整数の素因数分解を計算するアルゴリズムであり、数体ふるい法よりずっと計算効率が良いことが知られています。したがって、十分大きな素数の積に対してShorのアルゴリズムを適用できる大規模な量子計算機が開発されると、RSA暗号の実用性が大きく低下してしまいます。

同様のことが楕円曲線暗号についても生じることが知られています。楕円曲線暗号は楕円曲線上の離散対数問題を解く計算の困難性をその安全性の根拠としています。Shorのアルゴリズムは離散対数問題を解く計算にも適用でき、整数の素因数分解の場合と同様に、この場合の計算効率も良いことが知られています。

■耐量子計算機暗号の開発

素因数分解や離散対数問題とは異なる、量子計算機でも効率良く解くことができないと考えられている問題を安全性の根拠とした暗号は、耐量子計算機暗号と呼ばれています。現在、この暗号の研究開発及び標

整数を素数の積の形で表す
$23449 = 131 \times 179$
RSAにおける公開鍵と秘密鍵の関係



巨大な合成数の素因数分解は難しい ⇒ 素因数分解問題

図1　RSA暗号の安全性と素因数分解

準化が世界的に進められています。代表的な耐量子計算機暗号の一つとして、格子問題（図2）を利用した格子暗号が挙げられ、セキュリティ基盤研究室では新たな暗号方式であるLOTUS（ロータス）を開発しました。

近年の量子計算機の進化に伴い、米国NIST（国立標準技術研究所）は2016年に耐量子計算機暗号の標準化プロジェクトを開始し、2017年には方式の公募が行われました。NICTもそれに合わせて開発した格子暗号方式LOTUSを提案し、書類審査を通過した69件の中に含まれました（図3）。公募に提案された方式はNISTのWebページに全て掲載され、それに関する議論も専用のメーリングリストで公開されています。2018年12月までに、軽微なものも含めると約30件の方式に対して安全性の欠陥が指摘され、そのうち5件が既に取り下げられています。今のところLOTUSに対する重大な欠陥は発見されていません。しかし、NISTは提案されたPQCの候補を絞り込んだ結果を2019年1月30日に発表し、LOTUSはその候補として残りませんでした。LWE問題（図2）に基づく他の候補に比べてLOTUSの公開鍵のサイズは大きく、暗号文のサイズは小さいという特徴があります。この特徴は、公開鍵を頻繁に更新しない場合に適しています。

暗号方式の提案とは別に、実際に暗号を使うときにどの程度のパラメータを設定したらよいかという問題を議論するため、企業・大学及び公的機関が様々な暗号の安全性に関わる問題を公開し、問題のサイズと解読時間が評価されてきました。LOTUSの安全性の根拠となる格子問題では、ドイツのダルムシュタット工科大学が主催するLattice Challengeが有名であり、世界中の研究者が実験報告を行っています。セキュリティ基盤研究室では、このコンテストにおいて何度も世界記録を更新しており、格子暗号の安全性評価に長年貢献しています。

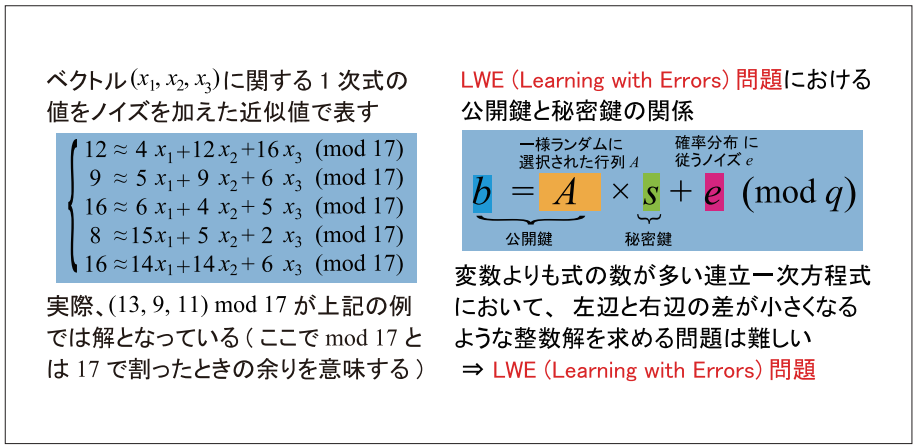


図2　格子問題の例（LWE 問題）

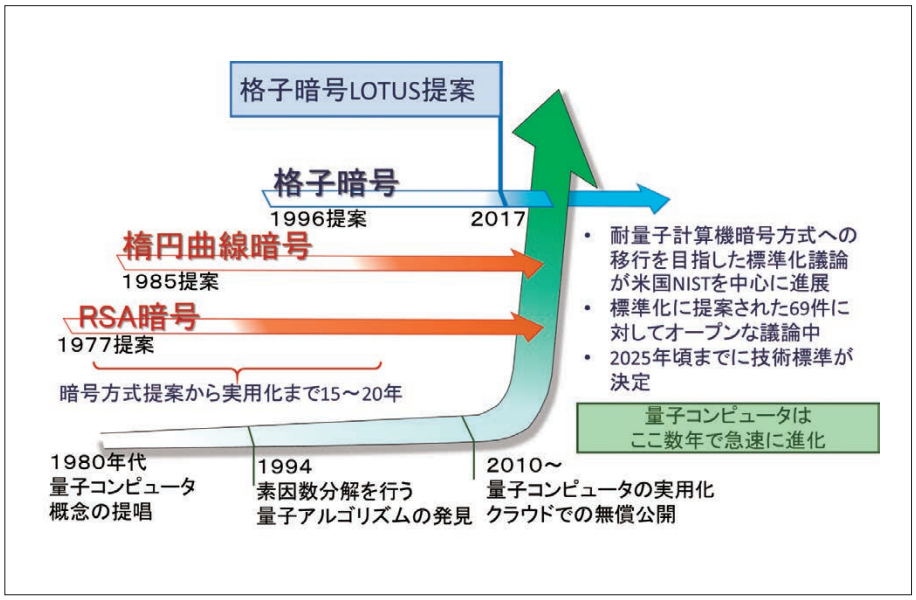


図3　格子暗号 LOTUS の開発

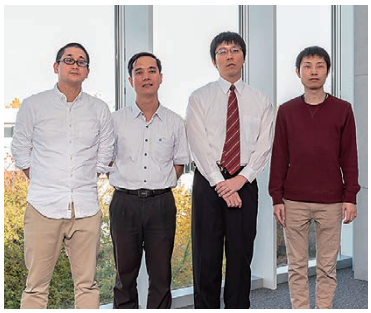
■日本国内における耐量子計算機暗号の標準化の準備

NICTは電子政府で使用する暗号技術の安全性評価等を行うプロジェクトであるCRYPTREC（クリプトレック）を総務省、経済産業省及び独立行政法人情報処理推進機構（IPA）と共同で運営しており、NICTではセキュリティ基盤研究室が実務を担当しています。このプロジェクトにおいて耐量子計算機暗号の有力な候補である格子暗号に関する調査を2014年に実施しています。さらに、他の有力な候補（符号暗号、多変数暗号、同種写像暗号等）についても2017年から調査を開始し、その技術報告書を2019年に公開する予定です。

■今後の展望

近年、NISTによる耐量子計算機暗号の公募等の実施により、多くの耐量子計算機暗号が提案されており、今後はそれらを含む新たな耐量子計算機暗号の安全性評価の研究が活発に進められることが予想されます。セキュリティ基盤研究室は研究開発及びCRYPTRECでの活動によって、格子暗号だけではなく他の耐量子計算機暗号の安全性評価及び開発にも貢献していきます。

プライバシー保護データ解析



左から、林卓也、レ チュウ フォン、青野良範、伊藤琢真

所属はすべて
サイバーセキュリティ研究所
セキュリティ基盤研究室

レ チュウ フォン
主任研究員
2015年NICT入所。暗号アルゴリズムの設計、プライバシー保護データマイニングに従事。博士（学術）。

林 卓也（はやし たくや）
主任研究員
2018年NICT入所。暗号工学、暗号解析、プライバシー保護データマイニングに従事。博士（機能数理学）。

青野 良範（あおの よしのり）
主任研究員
2011年NICT入所。暗号の解読アルゴリズムの研究および安全性評価の仕事に従事。博士（理学）。

伊藤 琢真（いとう たくま）
研究員
2018年NICT入所。暗号技術の安全性評価と実装に関する研究に従事。

近年のデータマイニング技術の進歩は、ビッグデータの中から利用価値の高い情報を引き出すことを可能とし、それらの情報を用いた様々なサービスが実現されています。例えば、商品販売サービスにおいて顧客の年齢・性別・購入履歴などを分析することで、その好みに合った商品を推薦するシステムが実用化されています。その一方で、利用価値の高い情報の中にはプライバシーに関わるものが少なからず含まれるため、その漏えいや際限のない利用に対してユーザ側の不安は日々強くなっています。このような問題を解決するための一手段として、プライバシー保護データ解析技術があります。

セキュリティ基盤研究室では、暗号技術を活用してプライバシーを保護した状態での高速なビッグデータ分析技術の研究開発を行っています。この技術により、機械学習・人工知能によるデータ分析を行う際に、データ提供者と無関係の機関[*1]がデータを盗み見ることを阻止できるため、提供者の不安を低減することができると期待しています。

本稿では、当研究室で開発した新たな準同型暗号技術であるSPHEREと深層学習を用いたDeepProtectについて紹介します。

SPHERE (Security-updatable Public-key Homomorphic Encryption with Rich Encodings)

データを暗号化した状態で処理することが可能な準同型暗号技術は、プライバシー保護データ解析に応用した際、データ処理を行うサーバが「どんな計算を行ったのか」を知ることはできますが、「どんなデータが含まれているのか」を知ることはできません。

このような、データの機密性を担保しているのは暗号の安全性ですが、暗号解読技術の進化によりそれが崩れてしまう危険性は常に存在します。今日暗号化したデータが数十年以上先の未来においても解読できないままであるかどうかは専門家の間でも意見が分かれており、安全側に倒した場合には長期間の使用をあきらめざるを得ないという問題が発生します。

セキュリティ基盤研究室ではこのような根本的課題の解決を目指し、2015年に、暗号化したデータのセキュリティレベルを上げる技術を組み込んだ準同型暗号SPHERE（スフィア）を開発しました。この技術を用いることで、暗号解読技術が進化した際にもそれに合わせ暗号強度を補強することが可能であり、保険・医療等の分野における、遺伝子情報などに対するデータマイニングへの応用が期待されます。

技術的には、耐量子計算機暗号の有力候補として知られる格子ベース準同型暗号を用いています。私たちは、データを暗号化する際に暗号文をデータ領域と暗号の強度を決める付加情報に分割するという特徴に注目し、暗号化したままの状態で付加情報を伸ばすことでセキュリティレベルを上げています（図1）。その際に、データ領域

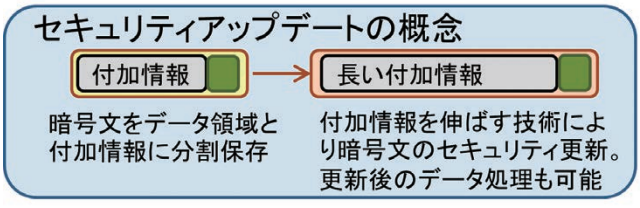


図1　セキュリティアップデートの概念

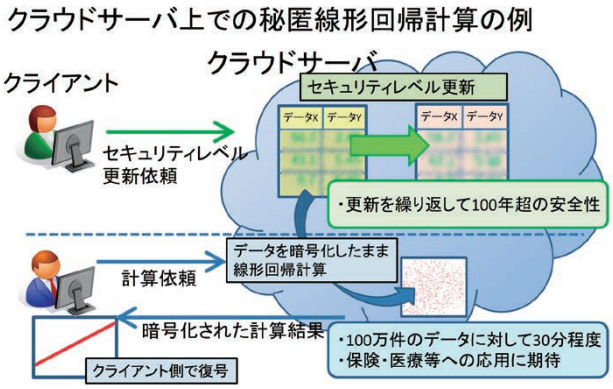


図2　SPHEREを用いた秘匿線形回帰計算

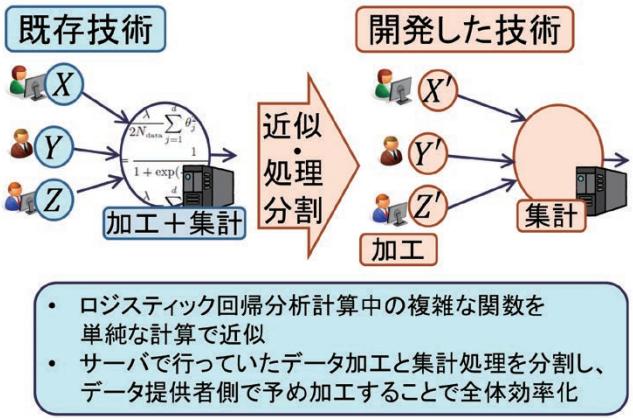


図3　開発したロジスティック回帰分析

には手を付けないため暗号の準同型性が保たれ、引き続き暗号化した状態でのデータ解析を行うことができます。

■SPHEREを使ったデータ解析実験

私たちは2015年に、開発した暗号方式SPHEREの実用性を確認するため、模擬データを使ったサーバ上での暗号化データ解析の実証実験で、100万件の暗号化データに対しての線形回帰計算を行い、標準的な計算サーバにより30分程度で解析可能であることを確認しました（図2）。

その後の1年間では、暗号化した状態でロジスティック回帰分析を行う方法を模索しました。高速化の決め手となったのは現実のデータ利活用でも用いられる以下の2つのテクニックです（図3参照）。

【近似計算】機械学習においては厳密な計算は必須ではなく、ある程度の近似計算でも実用上十分な分類性能を持つ。

【データの前処理】提供者のデータを適切な前処理を行ってからクラウドサーバにアップロードする。

これらを用いて、準同型暗号が苦手としていたロジスティック関数の計算を単純な2次関数で近似し、さらに、時間のかかる乗算処理を提供者側で行うことで大幅な高速化が実現しました。

2016年には模擬データを用いたシミュレーションにより、サーバ上で1億件のデータを30分以内で分析可能であることが確認できました。

■DeepProtect

現在、当研究室では、複数の異なる組織が個々のデータを開示せずに深層学習を行う技術の開発に取り組んでいます（図4）。一般的に、深層学習はデータ量が多いほど良い学習結果が得られるため、同業種他組織のデータを組み合わせることで、更に良い学習結果が得られることが期待できますが、機密保持の観点からこのような組織外へのデータ持ち出しはほぼ不可能でした。

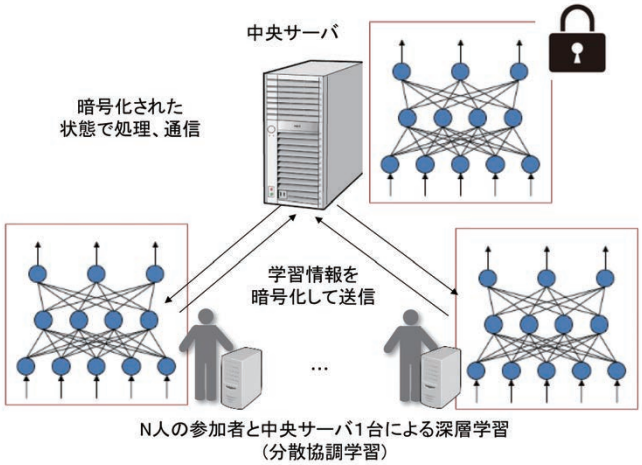


図4　データを開示せずに深層学習が可能となる技術

そこで私たちは、暗号技術と協調計算を組み合わせた深層学習技術DeepProtectを開発しました。深層学習では確率的勾配降下法という最適化アルゴリズムにより学習を行います。このアルゴリズムは、データ一つひとつに対して学習の計算を逐次行っていくという特徴があります。つまり、ある組織が保有するデータを用いて学習を行い、その学習結果のみを次の組織に渡し、これを全ての参加組織で行うことで、各組織が保有する全データについて学習を行うことと同等の学習が可能になります。この技術により、個々のデータの開示なしに全体の学習を行うことができます。

DeepProtectは実用性においても優れています。DeepProtectで実際に実験を行い、クレジットカードの不正取引に関する28万件のレコードについて学習時間が数分、不正取引か否かの判別が1ミリ秒程度で行うことができ、リアルタイムでの運用が可能であることが確認できました。

■まとめ

データマイニング技術の発達により、企業が持つビッグデータをいかに利活用するかが重要視される一方で、EU一般データ保護規則[*2]の制定など、プライバシーの保護が世界的に重要となっており、ビッグデータを解析できる高速性とプライバシー保護を実現する安全性の双方が求められています。セキュリティ基盤研究室では、これからも高速性と安全性を両立するプライバシー保護データ解析技術の研究開発を進めていきます。

＊1　例えば、データの保管や計算処理を行うクラウドサーバの管理者

＊2　EU域内の全ての個人に関するデータの保護規則。EU域外の事業者へも適用される。2018年5月25日に施行された。

情報理論的安全性に基づく小型人工衛星向けセキュア通信技術

吉田 真紀（よしだ まき）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
大学院博士課程修了後、大阪大学助教を経て2013年、NICT入所。以来、情報セキュリティの研究開発に従事。博士（工学）。

平成30年11月15日に人工衛星等の打上げ及び人工衛星の管理に関する法律が施行されました。同法律に関するガイドラインには、人工衛星の打上げ用ロケットとの通信に際してセキュリティ確保が必要である旨明記されています。民間事業者が宇宙ビジネスに参入する新たな時代に向け、私たちは、現在利用可能な低コスト電子デバイスを用いて、最高レベルのセキュリティである情報理論的安全性を達成できることを明らかにしました。本稿では私たちが提案したセキュア通信技術について紹介します。

■民間事業者による宇宙ビジネス時代の幕開け

小型人工衛星（以降、小型衛星と呼ぶ）が学術・商用目的で多数打ち上げられるようになり、今後も急激に数が増加していくことが見込まれています。さらに、民間事業者による小型衛星打上げ専用の低コスト小型ロケットが開発されるようになりました。このような背景の下、平成30年11月15日に人工衛星等の打上げ及び人工衛星の管理に関する法律（いわゆる宇宙活動法）が施行されました。

宇宙活動法に関するガイドラインには、人工衛星の打上げ用ロケットの型式認定や飛行許可にあたって、重要なシステム等に関する信号の送受信については、適切な暗号化等の措置が求められることが明記されています。実際、重要なシステム等に関する信号には飛行中断などクリティカルなコマンドが含まれており（図1下）、第三者による成りすましやコマンド改ざんがあれば、意図しない地点への落下など公共の安全を脅かす事態が発生します。それ以外の信号の送受信においても、例えば、人工衛星から地上局への伝送データ（図1右）は学術・商用的な価値をもつため、盗聴や改ざんは好ましくありません。

そこで本研究では、暗号技術を応用することで、地上局と小型人工衛星・小型ロケットとの信号送受信におけるセキュア通信の実現を目指します。

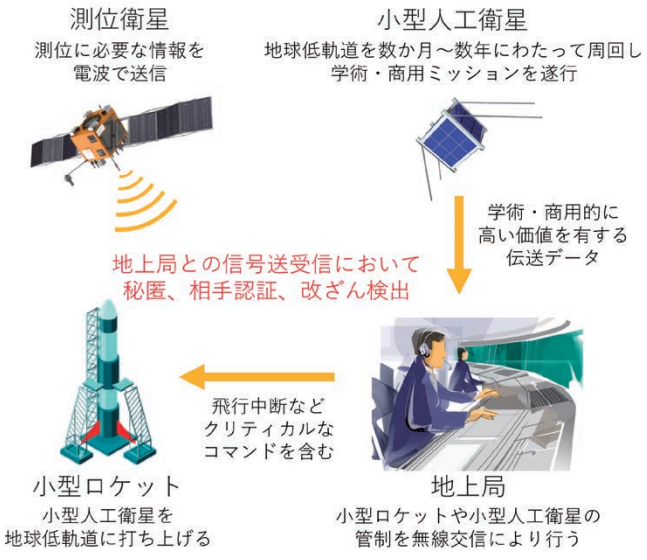


図1　地上局と小型人工衛星・小型ロケットのセキュア通信

■最高レベルのセキュリティ強度である情報理論的安全性

暗号技術の強度には様々なレベルがありますが、宇宙活動法に関するガイドラインには、どの程度の強度が適切かは具体的に規定されていません。公共の安全と伝送データの学術・商用的価値の保護を考えるならば、可能な限り高いレベルを達成することが理想的です。

暗号技術において最も高い強度レベルは情報理論的安全性です。情報理論的安全性とは、防御側が通信量に応じた大量の鍵を事前に用意することで、攻撃側が「無制限の計算リソース」を有するとしても解読できないことを意味します[*1]。ここで「無制限の計算リソース」とは、スパコンなどの現在の技術だけでなく量子コンピュータ

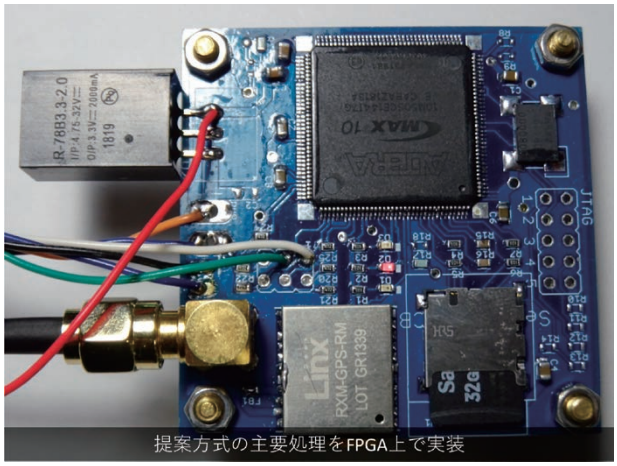


図2　プロトタイプボード

図3　無線伝送実験場所

を含めた将来のあらゆる技術、宇宙が終わるまでの時間、宇宙の全資源まで含みます。

■低コスト電子デバイスで情報理論的安全性を達成

本研究では、民間事業者による打上げにおける通信システムを想定し、現在利用可能な低コスト電子デバイスを用いて、情報理論的安全性が達成できることを初めて明らかにしました。具体的には、インターステラテクノロジズ株式会社の森岡澄夫博士と法政大学の尾花賢教授と連携し、通信システムの分析、セキュリティ要件の整理、安全性の定式化、方式の提案、基礎評価を実施しました。

情報理論的安全性の達成では、暗号技術を組み合わせ、鍵を用いてデータを加工し、通信する手順を定めます。暗号技術が単体で安全であっても、鍵が大量にあっても、組み合わせや使い方によってセキュリティ強度が変わります。設計を誤ると、鍵が無駄になるだけでなく、容易に解読できてしまいます。逆に、設計を工夫することで、鍵を最大限有効に使い、セキュリティ強度を下げることなく、コストを下げることができます。

提案した方式は、地上局・小型ロケット・小型衛星（以降、エンティティと呼ぶ）の通信におけるセキュリティ確立処理と、エンティティ間の同期維持処理からなります。まず、エンティティ間のやりとりの齟齬から管制を喪失しないよう、インタラクションを排除しました。次に、セキュリティ確立処理の「相手認証・改ざん検出機構」を同期維持処理にも活用し、セキュリティ強度を落とすことなく両処理を同時並行できるようにしました。また、想定する通信システムでは、打ち上げ前に地上局と小型ロケット・小型衛星が物理的に近接するため鍵共有が物理的に容易です。さらに、ライフタイムが比較的短く総通信量が抑えられます。これらにより、情報理論的安全性を低コストで達成できます。

提案方式の基礎評価として、その主要処理を、小型衛星や小型ロケットで現在利用できるデバイスと同水準の処理性能をもつローエンド FPGA で実装し（図2）、小型ロケットと地上局との通信（図3）を想定した無線伝送実験を実施しました。なお、制御信号や小量ミッションデータであれば、鍵のストレージとして数百Mバイト～数 Tバイト（メモリカードや SSD 程度）で十分です。ハードウェア実装では最大 16 Gbps の速度を達成し[*2]、無線伝送実験ではセキュリティ確立処理と同期維持処理の同時並行化が機能することを確認しました。

■今後の展望

本研究は、暗号技術の強度では最高レベルである情報理論的安全性に基づく宇宙機通信システムへの導入に向けた先駆的研究であり、半導体デバイスや通信機などの高密度化・低電力化によって、情報理論的安全性が実用段階に入ったことを示す貴重な成果です。

現在は小型ロケット・小型人工衛星・地上局との通信システムを想定していますが、今後は衛星光通信など大容量通信システムや、衛星によるコンステレーション構築におけるセキュア通信への適用も想定し、人類の新たな活動舞台である宇宙における安心・安全への貢献を目指します。

＊1　一般に広く使われている公開鍵暗号などの暗号技術は計算量的安全であり、防御側で必要になる鍵の量は極めて小さくできますが、攻撃側に「膨大な計算リソース」があれば解読できます。

＊2　提案方式において、一般的な地上通信システムと同様の暗号技術を使うことで計算量的安全な方式にできますが、情報理論的に安全な方式の方が、計算コストの点で軽量です。

汎用性の高いプロセスによる縦型酸化ガリウム(Ga_2O_3)トランジスタ開発に成功

～低コストGa_2O_3パワーデバイス量産への道筋～

現在、世界規模での革新的な省エネ技術開発が急務となっています。中でも、電力変換に用いるパワースイッチングデバイスは、その用途も多岐にわたることから、個々の機器における損失低減の積み重ねが、社会全体に大きな省エネ効果をもたらします。Ga_2O_3は、パワースイッチングデバイス材料として用いた場合、既存の半導体デバイスを上回る高耐圧・大電力・低損失特性が期待でき、また、簡便かつ安価に高品質・大口径単結晶ウェハーが製造可能であるため、Ga_2O_3パワートランジスタ、ダイオード開発が世界的に活発化しています。

NICT未来ICT研究所 グリーンICTデバイス先端開発センター 東脇正高 センター長らは、東京農工大学大学院工学研究院 熊谷義直教授、村上尚准教授らとの共同研究により、イオン注入ドーピング技術を用いた縦型酸化ガリウム（Ga_2O_3）トランジスタ*の開発に成功しました。イオン注入ドーピング技術は、不純物元素をイオン化した後、高速に加速し固体に直接打ち込む加工方法で、面内でのデバイス構造の作り込みが容易にでき、半導体デバイスの生産に多く使用されています。また、本開発によるトランジスタでは、ゲート電圧によるドレイン電流オン／オフ比8桁以上が得られ、これまでに報告されている同様の縦型Ga_2O_3トランジスタを上回るデバイス特性を実現しました。

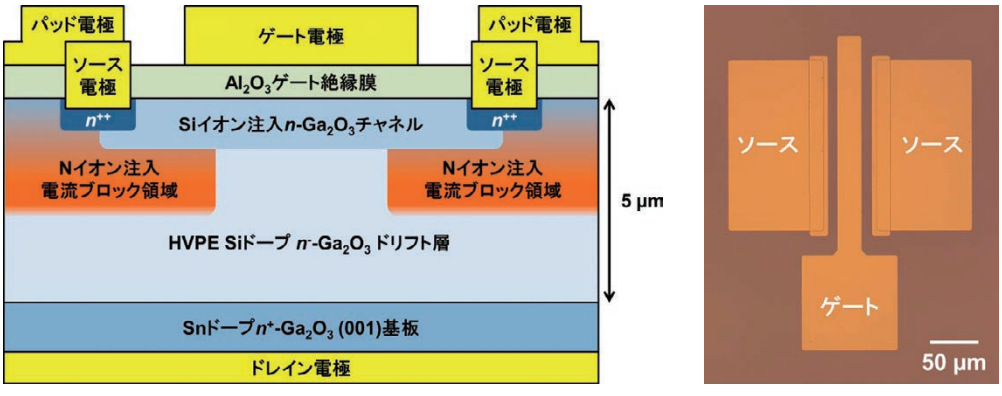
今後、本共同研究チームは、パワースイッチングデバイスとして求められるデバイス耐圧の向上などの残された課題を解決するための開発を継続します。近い将来、縦型Ga_2O_3トランジスタを実際の機器に応用した場合、既存の半導体トランジスタと比べて、スイッチング動作時の大幅な損失低減が期待されます。

今回採用したイオン注入ドーピングをベースとするデバイス作製技術は、量産に適し、汎用性も高く、低コスト製造が可能であるため、今後電機、自動車メーカー等民間企業におけるGa_2O_3パワーデバイス開発の本格化につながることが予想されます。高性能Ga_2O_3パワーデバイスは、グローバル課題である省エネ問題に対して直接貢献するとともに、日本発の新半導体産業の創出という経済面での貢献も併せて期待されます。

本研究の一部は、内閣府総合科学技術・イノベーション会議のSIP（戦略的イノベーション創造プログラム）「次世代パワーエレクトロニクス」［管理法人：国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）］によって実施されました。

Reference
Man Hoi Wong, Ken Goto, Hisashi Murakami, Yoshinao Kumagai, and Masataka Higashiwaki, "Current Aperture Vertical β-Ga_2O_3 MOSFETs Fabricated by N- and Si-Ion Implantation Doping," in IEEE Electron Device Letters.
https://ieeexplore.ieee.org/document/8556005
DOI: 10.1109/LED.2018.2884542

＊縦型トランジスタ
水平方向にドレイン電流を流す横型トランジスタ構造と比較して、垂直方向に流す縦型トランジスタ構造の場合、その電流通路の断面積を大きくすることで大電流動作が可能となる。また、オフ時、ドリフト層で印加電圧を吸収することが可能となるため、高電圧動作にも適している。



(a) (b)

図　作製した縦型Ga_2O_3トランジスタ構造の (a) 断面模式図、(b) 光学顕微鏡写真

■関連プレスリリース

- **世界初、イオン注入ドーピングを用いた縦型酸化ガリウム（Ga_2O_3）トランジスタ開発に成功**
  ～汎用性の高いデバイスプロセスを採用、低コストGa_2O_3パワーデバイス量産への道筋～
  （2018年12月12日付け　https://www.nict.go.jp/press/2018/12/12-1.html）

暗号技術の実装 ～高速性と安全性の両立を目指して～

林 卓也（はやし たくや）

サイバーセキュリティ研究所 セキュリティ基盤研究室
主任研究員　博士（機能数理学）

鍵交換や電子署名などの暗号技術は、例えばeコマースにおける安全な相互認証など、サービスに安全性や信頼性を付加することで価値を生みます。処理速度が遅いなどのために、暗号処理がサービスのボトルネックになるようなことがあってはならず、暗号処理の高速化が重要です。高速化には、暗号方式で扱う演算のアルゴリズムの選択や暗号パラメータなどの調整のほか、アセンブリ言語など低水準言語によるアーキテクチャ依存の最適化など、様々な手法があり、これらを適切に選択・組み合わせることで実装のパフォーマンスを改善していきます。

また、暗号を安全に実装するためには、攻撃者の視点も重要です。最近では、鍵などの秘密情報に起因する計算時間の差などを用いたサイドチャネル攻撃への対策のため、暗号処理の計算量が秘密情報と相関しないように実装することが求められています。対策をナイーブに実装すると低速になるため、計算アルゴリズムや実装の工夫によりできるだけ計算速度に影響しないよう対策を施す必要があります。

私は、学位取得まで特に暗号解読の研究に注力していて、攻撃者の視点で暗号技術を見てきました。暗号解読では、暗号方式や解読アルゴリズムの数理的理解だけでなく、実際に攻撃するための実装の高速化も重要です。前述のとおり、これらは暗号実装においても重要な知見です。最近は、暗号解読の研究もやりつつその知見を暗号実装の研究に活用しています。

最近注力しているのは、プライバシー保護データマイニング（本紙P4-5、8-9を参照ください）で用いる基盤技術の一つである準同型暗号の高速化です。準同型暗号は従来の暗号技術と比べて計算量が多く、高速化が特に重要です。世界的に高速化が進められているものの、様々なサービスへ展開するには更なる高速化が必須であると感じています。

暗号技術の実装では、高速性と安全性は天秤にかけるものではなく、いかにして両立するかが重要であり、面白いポイントです。両立を達成するには、実装高速化の知見だけでなく、攻撃者の視点も重要です。どのように方式を実装するか、その実装に穴は無いか、数式とプログラムを行き来しながらいつも思案しています。

■経歴

1985年　札幌市にて誕生
2008年　公立はこだて未来大学情報アーキテクチャ学科卒業
2010年　公立はこだて未来大学大学院システム情報科学研究科博士前期課程修了
2013年　九州大学大学院数理学府博士後期課程修了（機能数理学）。同年同大学研究員
2014年　NICTセキュリティ基盤研究室入所
2017年　神戸大学工学研究科特命助教
2018年　現職（2019年から主任研究員）

■受賞歴など

2012年度喜安記念業績賞
第12回ドコモ・モバイル・サイエンス賞 先端技術部門 優秀賞

■一問一答

Q：研究者になってよかったことは？

A：世界の最先端の知識に触れて、何らかの意味で最先端の更に先を行くという楽しみがある数少ない職だと思います。もちろん産みの苦しみもありますが…。

Q：最近はまっていること

A：寒くなってきたので家で鍋をつついています。料理下手ですが、鍋に野菜と肉や魚を入れれば美味しく仕上がるので重宝しています。

Q：研究者志望の学生さんにひとこと

A：学会等でできるだけいろんな人とネットワークを作っておくことをお勧めします。友人が増えるだけでなく、後々になって様々な形で助けになります。

「NICTのチャレンジャー」では、様々なことに挑むNICT職員の横顔をご紹介しています。

パーマネント研究職・総合職 採用 2020

NICT は、情報通信分野を専門とした我が国唯一の公的研究機関です。

研究者と総合職が一体になることで、高いパフォーマンスを発揮し、
情報通信の分野で『安心・安全で豊かな社会の実現』を目指して仕事をしています。
この NICT で、是非一緒に様々なことに挑戦していきませんか？

研究職・研究技術職・テニュアトラック研究員

■募集人数　パーマネント研究職、パーマネント研究技術職またはテニュアトラック研究員として十数名
■応募方法　当機構採用 web ページをご参照ください。
着任時期：2020 年 4 月 1 日(応相談)
応募締切：2019 年 4 月 12 日(金)必着

総合職

■仕事内容　経営企画、産学官連携、国際連携、広報、知的財産管理、法務・コンプライアンス、総務、財務など
■募集対象　大学・大学院を 2020 年 3 月卒業見込の方、あるいは既卒の 30 歳以下
(1989 年 4 月 1 日生まれまで）の方
■募集人数　1 ～ 5 名
■エントリー方法　マイナビ 2020 に登録後、エントリーをされた方へ順次ご案内いたします。

2019年3月1日エントリー スタート！

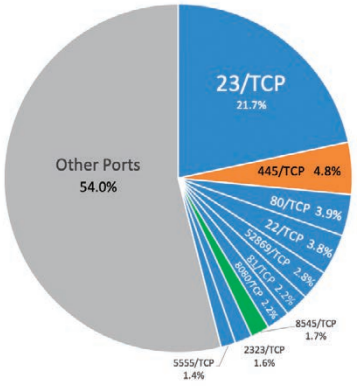
https://www.nict.go.jp/employment/

お問い合わせ先　パーマネント採用担当　jinji@ml.nict.go.jp　042-327-7304

NICTER観測レポート2018の公開

NICTは、2月5日、サイバーセキュリティ研究所において、NICTER観測レポート2018を公開しました*。NICTERプロジェクトの大規模サイバー攻撃観測網で2018年に観測されたサイバー攻撃関連通信は、2017年と比べて約1.4倍と昨年以上の増加傾向にあります。内訳としては海外組織からの調査目的とみられるスキャンの増加が著しく、総観測パケットの35%を占めました。IoT機器を狙った通信では、Telnet（23/TCP）を狙う攻撃が半減する一方、IoT機器に固有の脆弱性を狙う攻撃が増加し、全体としては2017年から2割程度の減少が見られました。詳細は以下をご覧ください。

「NICTER観測レポート2018」
https://www.nict.go.jp/cyber/report/NICTER_report_2018.pdf



ポート番号	攻撃対象
23/TCP	IoT機器（Webカメラ等）
445/TCP	Windows（サーバサービス）
80/TCP	Webサーバ（HTTP） IoT機器（Web管理画面）
22/TCP	IoT機器（ルータ等） 認証サーバ（SSH）
52869/TCP	IoT機器（ホームルータ等）
81/TCP	IoT機器（ホームルータ等）
8080/TCP	IoT機器（Webカメラ等）
8545/TCP	イーサリアム（仮想通貨）
2323/TCP	IoT機器（Webカメラ等）
5555/TCP	Android 機器 （セットトップボックス等）

宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

* NICTサイバーセキュリティ研究所では、NICTERプロジェクトにおいて大規模サイバー攻撃観測網（ダークネット観測網）を構築し、2005年からサイバー攻撃関連通信の観測を続けてきました。

NICTオープンハウス2019 in 小金井　6月21日(金)・22日(土)

オープンハウスは、内容を大幅にリニューアルして開催いたします。皆様のご来場をお待ちしています。（詳細は、確定次第ＨＰに掲載します。）

NICT NEWS 2019 No.2 通巻 474
編集発行：国立研究開発法人情報通信研究機構 広報部
発行日：平成31（2019）年3月（隔月刊）

〒184-8795 東京都小金井市貫井北町4-2-1
TEL: 042-327-5392　FAX: 042-327-7587
E-mail: publicity@nict.go.jp

URL: https://www.nict.go.jp/
@NICT_Publicity
#NICT

定期購読のお申込みは QR コード、Web または E-mail にて承っております。
ISSN 1349-3531 (Print)
ISSN 2187-4042 (Online)