東北大学
TOHOKU UNIVERSITY

Press Release

2026 年 8 月 18 日

報道機関　各位

国立大学法人東北大学

暗号機器の物理セキュリティの数学的証明に成功
― 安全な暗号機器の設計方法を確立 ―

【発表のポイント】

- 暗号デバイスから漏えいする物理的情報（消費電力や電磁波など）を悪用するサイドチャネル攻撃に対し、代表的な対策技術「マスキング」の安全性を数学的に保証する必要十分条件を世界で初めて明らかにしました。
- 上記の条件を応用し、従来技術と比べて半分以下のコストで、物理的漏えいに対して安全な暗号デバイスを実現する新たな設計手法を開発しました。
- サイドチャネル攻撃とマスキングの発見から 25 年以上にわたり未解決だった、マスキングの有効性に関する原理的な問いに答えるものであり、暗号・情報セキュリティ分野の基礎理論に貢献します。
- 本成果は、スマートフォンや IC カード、IoT 機器などに搭載される暗号デバイスの安全性向上への貢献が期待されます。

【概要】

電子メールやメッセージングアプリ、電子商取引等、多くのデジタルサービスの安全な情報通信に暗号技術が広く用いられていますが、暗号処理を実行する機器の消費電力や漏えい電磁波などを観測・悪用して秘密情報を奪取する攻撃の脅威が知られており、対策技術の確立が強く求められていました。

東北大学電気通信研究所の本間尚文教授、伊東燦助教、京都大学大学院情報学研究科の上野嶺准教授、日本電気株式会社の峯松一彦主席研究員、井上明子主任からなる研究グループは、暗号デバイスから生じる物理的漏えい（消費電力や放射電磁波など）を解析して、安全性の保証に必要な条件を明らかにし、さらにその条件を利用して物理的安全性が保証された暗号デバイスを従来よりも大幅に少ないコストで実現する技術を開発しました。

本成果は、数学的にも物理的にも安全な暗号機器を効率的に実現する新たなアプローチとして、今後の安心・安全な情報通信社会の構築に資することが期待されます。

本成果は、2026 年 8 月 13 日に Proceedings of Annual International Cryptology Conference（CRYPTO 2026）に公開されました。また、8 月 17 日（現地時間）より米国カリフォルニア州サンタバーバラ市で開催される 2026 年国際暗号学会議 (CRYPTO 2026) にて発表されます。

【詳細な説明】

研究の背景

電子メールやメッセージングアプリ、電子商取引を始めとする多くのデジタルシステムにおいて、安全な情報通信を実現するために暗号技術が広く用いられています。暗号は秘密の暗号鍵を用いて平文などの秘密情報を、攻撃者に見られても安全な暗号文に変換する方法などを指す技術であり、現在使用される暗号の数学的安全性は十分に評価されています。一方で、暗号演算を実行する機器（デバイス）から放射される物理的情報（消費電力や漏えい電磁波など）を観測・悪用して秘密鍵を推定するサイドチャネル攻撃（図 1）の脅威が知られており、対策技術の確立が強く求められていました。暗号・情報セキュリティ分野において、物理的漏えいやサイドチャネル攻撃への対策技術の確立や、その効果の原理究明は重要課題の一つとして位置付けられています。

最も有望なサイドチャネル攻撃対策技術として、マスキングが長年研究されてきました。マスキングとは、秘密情報に関する物理的漏えいが一つ観測されても、秘密鍵が分からないようにデバイス上で秘密情報を複数の値にランダムに分散する（マスクする）技術です。暗号デバイスにマスキングを適用することによりサイドチャネル攻撃が難しくなることが、これまで実験的に確認されてきました。しかしながら、原理的には、攻撃者は一つでなく複数の物理的漏えいを観測すればサイドチャネル攻撃により秘密鍵を推測することが可能です。マスキングの適用がサイドチャネル攻撃をどの程度難しくするのか、そして、どのような条件下でマスキングがサイドチャネル攻撃への防御として有効なのか、という原理究明は、サイドチャネル攻撃とマスキングが発見されてから 25 年以上にわたり未解決であり、その解決は暗号分野における重要な課題でした。マスキングの数学的解析を行うことでこれを解決しようという試みも複数ありますが、これまでの解析や証明は特定の条件下でしか成立しないもので、どこまでその適用範囲を広げられるかは不明でした。

今回の取り組み

本研究グループは、これまで、物理的に安全な暗号デバイスの実現に向けてサイドチャネル攻撃やマスキング、暗号設計などに関する研究を推進してきました。今回の研究成果では、暗号デバイスから生じる物理的漏えいを数学的に解析することで、こうした漏えいに対する暗号デバイスの物理セキュリティを定量的に評価する技術を開発し、漏えい対策技術の安全性を評価・証明するための理論を構築しました。さらに、本成果を応用して、従来の漏えい対策技術と比べて半分以下のコストで、物理的漏えいに対して安全に暗号デバイスを実現する手法を開発しました。本研究は、サイドチャネル攻撃対策として広く用いられているマスキングの安全性を一般的な形で説明するものです。

今回の研究では、サイドチャネル攻撃者が物理的漏えいから得る情報を確率

論や情報理論などの数学的形式モデルを使って表すことで、サイドチャネル攻撃者の優位さ（アドバンテージ）(注 1) を攻撃成功確率として定量化しました。その上で、漏えいを解析してこの値の上限値を与える方法を導出しました。これにより、秘密情報を分散する数を増やすことで攻撃者のアドバンテージを大幅に小さくできることを、現実的なサイドチャネル攻撃の状況下で示すことに成功しました（図 2）。さらに、本研究成果では、そのような安全な暗号デバイスを実現するための必要十分条件を漏えいの強度 (注 2) の観点から明らかにし、マスキングが有効に機能する範囲（すなわち、どの程度の漏えいならマスキングが有効で、それ以上の漏えいならマスキングが安全でなくなるかの境界）を数学的に示しました。マスキングにより暗号デバイスが安全に動作する条件が明らかになったことから、従来よりも大幅に少ない漏えい対策コスト (注 3) で安全な暗号デバイスを実現できるようになります。本研究で提案する対策では、実用的な安全性を、従来の半分から五分の一以下の実コストで対策を達成できます。

本研究成果は、安全な暗号デバイスの実現に向けた大きな進歩であり、安心・安全な情報通信社会における基礎技術としてその実現に貢献します。

今後の展開

本成果は、安全な暗号デバイスの実現のための理論的基礎となるものであり、これまでのマスキングに基づく方法論を用いた対策に確固たる裏付けを与えるとともに、安全な暗号デバイスの実現に向けた研究開発の新たな方向性を示しました。本成果は、スマートフォンや IC カード、IoT 機器など、身近な情報通信機器に搭載される暗号デバイスの安全性向上に貢献することが期待されます。

研究グループは今後、今回開発した技術を現実世界で実装・評価することで、第三者評価を含めたさらなる検証を実施するとともに、本成果が広く利用されるように社会実装に取り組む予定です。

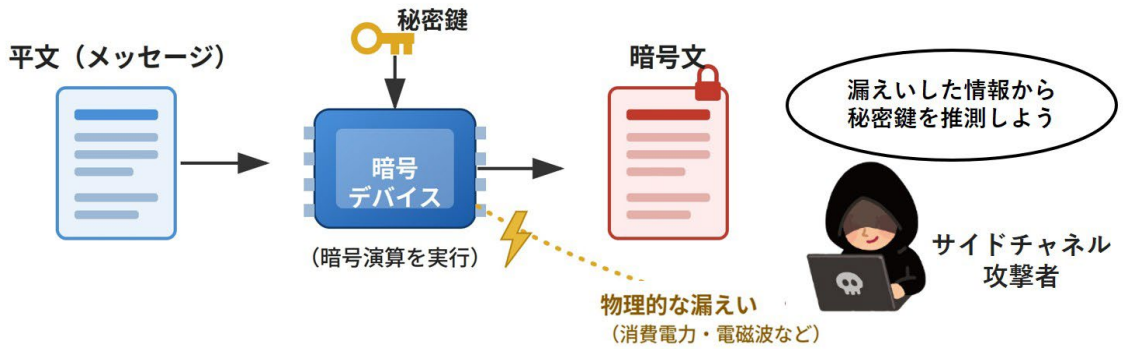

図 1. サイドチャネル攻撃の概要
攻撃者は暗号デバイスが暗号演算中に生じる物理的な漏えい（サイドチャネル情報）から秘密鍵を奪取する。

図 2. サイドチャネル攻撃実験の様子
対象となる暗号デバイスの消費電力を測定し、PC を用いた解析により秘密鍵推測の可否を評価する。

【謝辞】
今回の研究成果の一部は、科学技術振興機構（JST）経済安全保障重要技術育成プログラム「人工知能（AI）が浸透するデータ駆動型の経済社会に必要な AI セキュリティ技術の確立」（プログラム・オフィサー：松本勉）「AI ハードウェアセキュリティ基盤技術の開発」（研究代表者：本間尚文、グラント番号：JPMJKP24C1）の事業・研究課題の助成により得られました。

【用語説明】
注1. 攻撃者のアドバンテージ：攻撃者が漏えい情報から秘密情報を推測する力のこと。正しく秘密鍵を推測できる確率と、ランダムに推測したときの正解確率の差を示す。

注2. 漏えいの強度：秘密情報がどの程度漏えいしているかを表現する特徴量。暗号デバイスの種類と測定環境によって決まる。数学的には、相互情報量や確率分布の全変動距離などの情報理論と確率統計理論で利用される特徴量などを用いて定義される。

注3. 漏えい対策コスト：マスキング対策を施すことで増加する計算量や回路面積のこと。

【論文情報】

タイトル：A Formal Security Proof of Masking: Reduction from Strong Noisy Leakage to Probing Model without Random Probing and Application to LR Primitive

マスキングの形式的安全性証明：強雑音漏えいからプロービングモデルへの乱択プロービングを用いない帰着と漏えい耐性プリミティブへの応用

著者：Rei Ueno*,**, Akiko Inoue**, Kazuhiko Minematsu**, Akira Ito**, and Naofumi Homma**

*筆頭著者

京都大学大学院情報学研究科・准教授・上野嶺

**共同責任著者

日本電気株式会社・主任・井上明子

日本電気株式会社・主席研究員・峯松一彦

東北大学電気通信研究所・助教・伊東燦

東北大学電気通信研究所・教授・本間尚文

掲載誌：Proceedings of Annual International Cryptology Conference (CRYPTO 2026)

URL：https://link.springer.com/chapter/10.1007/978-3-032-35415-0_11

【問い合わせ先】

（研究に関すること）

東北大学電気通信研究所

教授　本間尚文

TEL: 022-217-5506

Email: contact.ecsislab@grp.tohoku.ac.jp

（報道に関すること）

東北大学電気通信研究所　広報室

TEL: 022-217-5427

Email: riec-kohoshitsu@grp.tohoku.ac.jp