暗号デバイスの物理セキュリティの数学的証明に成功

―安全な暗号デバイスの設計方法を確立―

概要

大学院情報学研究科 上野嶺 准教授、東北大学 本間尚文 教授、同 伊東燦 助教、日本電気株式会社 峯松一彦 主席研究員、同 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。

暗号技術が安全な情報通信のために広く用いられている一方、暗号デバイスの物理的漏えいを観測・悪用して秘密の暗号鍵を詐取するサイドチャネル攻撃の脅威が知られていました。暗号・情報セキュリティ研究分野において、サイドチャネル攻撃に対する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した。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、将来的にスマートフォンや 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に貢献することが期待されます。

本成果は、2026 年 8 月 17 日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）にて発表されました。

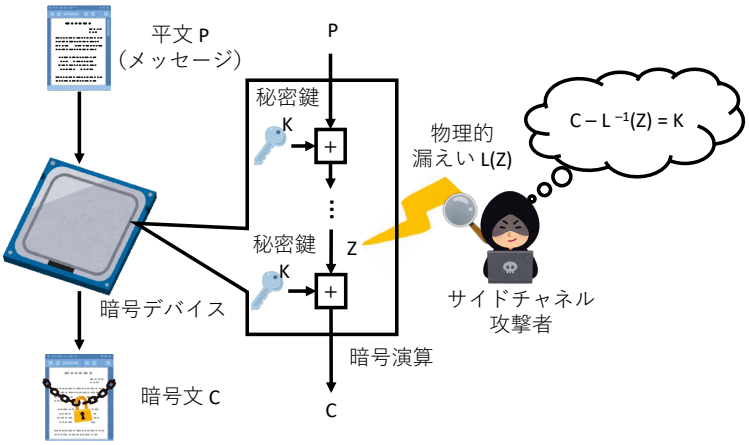

図 2：サイドチャネル攻撃の概要。攻撃者は暗号デバイスの物理的漏えい L(Z) から暗号演算内部の秘密情報 Z を推測して、秘密鍵 K を詐取する。（この図では国際標準暗号 AES のような暗号を想定している。）

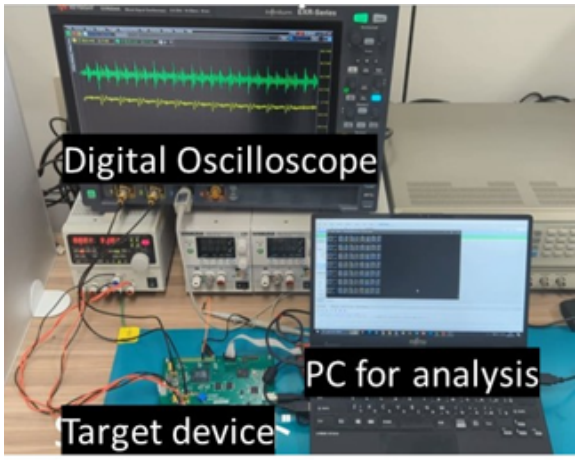

図 1：サイドチャネル攻撃実験の様子。ターゲットの暗号デバイスの消費電力をデジタルオシロスコープで測定し、測定結果を PC に送って秘密鍵を解析している。（東北大学本間研究室にて撮影）

１．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、秘匿通信や認証、電子署名に基づく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、現在実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。マスキングでは、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（図３）。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。

２．研究手法・成果

大学院情報学研究科 上野嶺 准教授、東北大学 本間尚文 教授、同 伊東燦 助教、日本電気株式会社 峯松一彦 主席研究員、同 井上明子 主任からなる研究グループは、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いました。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（消費電力や放射電磁波など）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が漏えい情報から秘密情報を推測する力を、攻撃成功確率を用いて定量化しました（注1）。その上で、漏えいを解析してこの値の上界を与えることによって、攻撃者が秘密情報を正しく推測する力を、設計のパラメータ（秘密情報の分散数）に対して指数関数的かつ任意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。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、どのような漏えいならマスキングが安全でなくなるのかの境界）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なる条件が明らかになったことから、その条件を満たす新たな暗号技術を開発し、従来よりも大幅に少ないコスト（注3）で漏えい対策が可能になることを示しました。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。

３．波及効果、今後の予定

本成果は、安全な暗号デバイスの実現における理論的基礎を確立するものであり、これまでのマスキングに基づく方法論を用いた研究開発に確固たる理論的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。今後は、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。

４．研究プロジェクトについて

本研究は、JSPS 科研費課題番号 25K03117、JST CRONOS 課題番号 JPMJCS25N1、そして JST K プログラム課題番号 JPMJKP24C1 の支援を受けたものです。

＜用語解説＞

注１：攻撃者が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絶対差分のことを攻撃者の力と呼んでいます。専門的には攻撃者のアドバンテージと呼ばれます。

注２：漏えいの強度は、秘密情報がどの程度漏えいしているかを定量的に表現する特徴量です。暗号デバイスの種類と測定環境によって決まります。具体的には、相互情報量や確率分布の全変動距離などの情報理論や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ます。

注３：従来手法では、対策技術の実装コストが安全性パラメータに対して二乗で増加するのに対し、提案手法では同等以上の安全性を線形のコストで達成可能です。実用的なパラメータでは、提案手法は、従来手法の半分から五分の一以下の実装コストで漏えい対策を実現できます。

＜論文タイトルと著者＞

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

掲 載 誌：Proceedings of Annual International Cryptology Conference (CRYPTO 2026)

DOI：10.1007/978-3-032-35415-0_11

URL： https://doi.org/10.1007/978-3-032-35415-0_11

＜参考図表＞

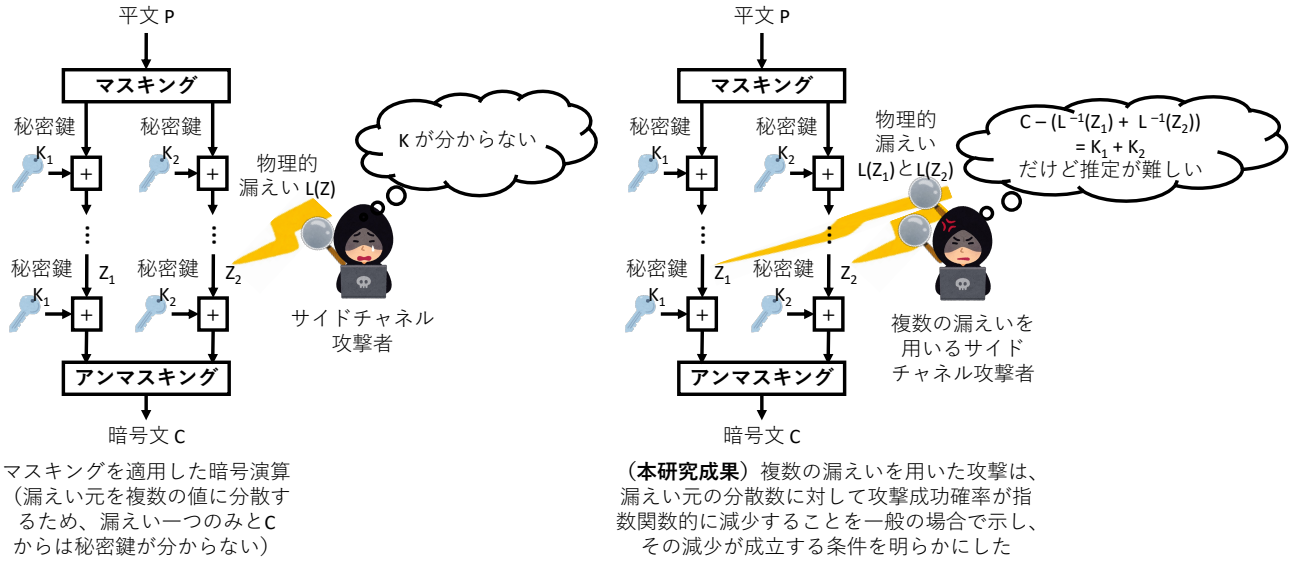

図 3：マスキングの概要と本研究成果。マスキングでは漏えい元の秘密情報を複数の情報にランダムに分散するため、漏えいを一つ観測しても秘密鍵が復元できない。原理的には複数の漏えいを用いれば秘密鍵の推定が可能だが、本研究では複数の漏えいを用いて攻撃は情報の分散数に対して指数的に難しくなることと、マスキングがそのように有効に機能するための必要十分条件（マスキングが機能するための漏えいの強度の境界）を明らかにした。