東北大学
TOHOKU UNIVERSITY

Orchestrating a brighter world
NEC

JST

Press Release

2023 年 12 月 5 日

国立大学法人東北大学
日本電気株式会社
国立研究開発法人科学技術振興機構（JST）

新概念の鍵変換で暗号の物理安全性が飛躍的に向上

様々な暗号ソフトウェア・ハードウェアに革新

【発表のポイント】

- 新しい概念の「鍵変換」により暗号化した情報を物理的な攻撃(注 1)から守る手法を開発しました。
- 開発した鍵変換手法の安全性を数学的に証明しました。
- 様々な暗号ソフトウェア・ハードウェアを低コストで実装可能とする成果です。
- 今後の暗号搭載製品の長期的な安全性と性能の向上に大きく貢献すると期待されます。

【概要】

近年、個人情報や金融情報などの重要な情報を IC（集積回路）カードをはじめとする情報通信機器を通してインターネット上でやりとりすることが一般的となっています。そのような情報を守るため、機器内部には暗号化処理を実行するソフトウェアやハードウェア（暗号モジュール）が搭載されています。しかしサイドチャネル攻撃(注 2)と呼ばれる、暗号モジュールの動作時に副次的に発生する電力消費や電磁波などを利用して秘密情報を盗み出す攻撃が指摘されています。

東北大学電気通信研究所および日本電気株式会社(NEC)は、新しい概念の「暗号鍵変換」によりサイドチャネル攻撃から暗号モジュールを長期にわたって強固に保護する技術を開発しました。開発した技術は、これまでの 10 分の 1 以下の対策コストで長期間の安全性を維持できます。また、その安全性を数学的にも証明しており、様々な用途の暗号モジュールの長期的な安全性を低コストで実現できます。今後、開発した技術により、IC カード、スマートフォンや車載機器をはじめとする暗号機能を搭載した機器全体の安全性と性能向上に貢献することが期待されます。

本成果は、2023 年 12 月 4 日に国際暗号学会の国際学術雑誌 IACR Transactions on Cryptographic Hardware and Embedded Systems に先行掲載されました。さらに、2024 年 9 月に開催される同雑誌の採択論文による国際会議において発表を行う予定です。

研究

【詳細な説明】

研究の背景

現在、個人情報や金融情報といった大切な情報が情報通信機器を通してインターネット上でやりとりされることが一般的となっており、そのような情報をサイバー攻撃から守る上で機器内部には暗号化処理を実行するソフトウェアやハードウェア（暗号モジュール）が搭載されています。一方、暗号モジュールの物理的な挙動から秘密情報を盗み出す物理攻撃(注 1)による現実的な脅威が指摘されています。特に、暗号モジュール動作中の消費電力や放射電磁波（サイドチャネル情報）を観測するサイドチャネル攻撃(注 2)は、非接触・非破壊に攻撃が可能で痕跡が残らないため、最も強力な物理攻撃の一つとされています（図 1）。暗号モジュールの普及が進む欧米では、サイドチャネル攻撃による脅威の報告が多くなされています。こうしたサイドチャネル攻撃は、数学的に安全性が保証された最新の国際標準暗号を用いた場合であっても脅威となり得ます。そのため、いかに同攻撃への耐性を備えた暗号モジュールを設計・実装するかについて世界的に研究開発が進められています。

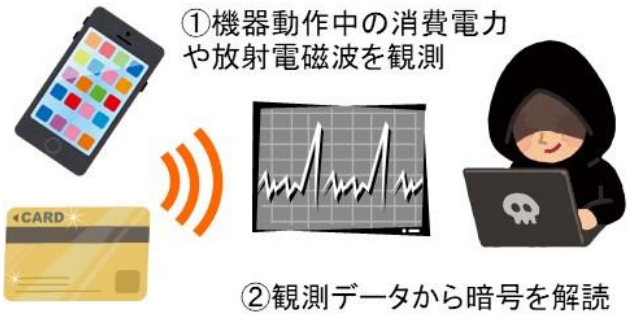

図 1. サイドチャネル攻撃の概要：暗号モジュールの動作から暗号が解読される恐れ

東北大学電気通信研究所環境調和型セキュア情報システム研究室（本間尚文教授、上野嶺助教）および NEC・セキュアシステムプラットフォーム研究所（峯松一彦主席研究員、井上明子主任）の研究グループは、今後のスマート社会で期待される新たなサービスを安心・安全に利用できるシステムの構築を目指し、暗号処理ソフトウェアやハードウェアを数学的にも物理的にも安全に実現するための技術開発を行ってきました。

今回の取り組み

今回開発した技術は、暗号鍵(注 3)の再生成および切り替えを行う「リキーイング（鍵変換）」と呼ばれる技術の新手法で、攻撃に対して 100%安全な構成要素が無い状況であっても、安全のかなめである暗号鍵を適切に交換すれば現実的に十分な安全性を有する暗号モジュールを実現できることを明らかにしています。適用範囲が広く、様々な暗号モジュールの物理攻撃耐性（物理安全性）を高めることができます。

これまでサイドチャネル攻撃への対策は、特殊な回路技術を付加するなど非

常に大きなコスト（速度低下や消費電力増加）を伴うものが大半でした。これに対して今回の手法は、軽量な対策を施した暗号モジュールであっても、そのサイドチャネル攻撃への耐用期間を現実的な条件・環境下で指数関数的に延長できるため、性能と物理安全性の両立をこれまでより数万倍以上効率的に実現する可能性を有します。例として、従来の主要対策で比較を行った結果、開発手法により対策コストを 10 分の 1 以下に抑えても十分に長期的な安全性を達成できることを確認しました（図 2）。

図 2. 安全性実証実験の様子：サイドチャネル攻撃に晒されても現実的な時間で秘密が漏えいしないことを確認

さらに、その安全性（耐用期間を指数関数的に延長できるという特長）を、最も強力なサイドチャネル攻撃者を想定した条件下において数学的にも証明しました。すなわち、本成果を適用した暗号モジュールの物理安全性の耐用期間は数学的に保証されたと言えます。本共同研究チームは、現在世界中で広く利用されている国際標準暗号 AES[注 4]に開発した手法を適用し、安全な暗号モジュールを構成する具体的な方法を明らかにしています。

今後の展開

今回開発した技術は、特別な回路技術などを必要とせずに暗号モジュールを長期にわたって強固に保護する汎用的な手法です。今後のスマート社会では、様々な機器がネットワークに接続されると想定されており、そこでやり取りされるデータを様々な攻撃から守る暗号モジュールの重要性はますます高まると予想されています。今後は、開発手法を様々な機器やシステム向けの暗号モジュールに適用して実証実験をさらに進めます。特に、これまでコストの面から搭載困難だった小型の機器に本技術を適用し、その有効性を明らかにしていきます。これにより、様々な機器の安全性確保が可能となり、スマート社会における新たな応用やサービスの開拓につながることが期待されます。将来的には、本技術を活用して、暗号を利用する様々な情報通信機器およびそれらを用いたシステム全体の安全性と性能向上に貢献することを目指しています。

【謝辞】
今回の研究成果は、科学技術振興機構（JST）戦略的創造研究推進事業 CREST「Society5.0 を支える革新的コンピューティング技術」研究領域（研究総括：坂井修一）「耐量子計算機性秘匿計算に基づくセキュア情報処理基盤」（研究代表者：本間尚文、グラント番号：JPMJCR19K5）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. 暗号モジュールへの物理攻撃

物理的な弱点（脆弱性）を突いて解読を行う攻撃を物理攻撃と呼ぶ。標準規格に採用されている暗号のアルゴリズムは、一般に公開されて専門家による安全性評価を十分に受けており、数学的には解読できないとされている。しかし、暗号アルゴリズムは通常ソフトウェアやハードウェアといった暗号モジュールとして実装されて利用されるため、その実装方式の物理攻撃耐性も考慮する必要がある。物理攻撃は、暗号モジュールの破壊を伴う攻撃と、サイドチャネル攻撃のように破壊を伴わない攻撃に大別される。

注2. サイドチャネル攻撃

暗号アルゴリズムを実行するハードウェアもしくはソフトウェア（暗号モジュール）では、その動作中に様々な物理量（処理時間や消費電力、放射電磁波など）が生じる。そのような正規の入出力以外に副次的に生じる物理的な情報（サイドチャネル情報）を観測して暗号を解読する物理攻撃の総称をサイドチャネル攻撃と呼ぶ。

注3. 暗号鍵

暗号では、一般に、入力データから暗号文を生成する、また、暗号文から元のデータを復元する際に「鍵」と呼ばれる秘密のパラメータが用いる。攻撃者から鍵を守ることで暗号の安全性が保たれる。

注4. AES

Advanced Encryption Standard の略。2001 年に米国国立標準技術研究所が連邦標準（FIPS PUB 197）として制定した暗号アルゴリズムで、2005 年に国際標準規格（ISO/IEC18033-3）として採用された。世界で最も広く利用されている暗号アルゴリズムの一つ。Wi-Fi の暗号化方式としても知られる。

【論文情報】
タイトル：Fallen Sanctuary: A Higher-Order and Leakage-Resilient Rekeying Scheme
著者：Rei Ueno, Naofumi Homma, Akiko Inoue, Kazuhiko Minematsu
*責任著者：東北大学電気通信研究所　助教　上野嶺
掲載誌：IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2024, No. 1, pp. 264-308, December 2023
URL：https://tches.iacr.org/index.php/TCHES/issue/view/341

【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
助教　上野嶺
TEL: 022-217-5506
Email: contact.ecsislab[at]grp.tohoku.ac.jp

（報道に関すること）
東北大学電気通信研究所　総務係
TEL: 022-217-5420
Email: riec-somu[at]grp.tohoku.ac.jp

NEC　コーポレートコミュニケーション部　山梨
TEL: 080-2024-6148
Email: press[at]news.jp.nec.com

科学技術振興機構　広報課
TEL: 03-5214-8404
Email: jstkoho[at]jst.go.jp

（JST 事業に関すること）
科学技術振興機構　戦略研究推進部　ICT グループ
前田さち子
TEL: 03-3512-3526
Email: crest[at]jst.go.jp