東北大学
TOHOKU UNIVERSITY

Press Release

令和 4 年 2 月 2 日

報道機関　各位

東北大学　電気通信研究所

量子コンピュータにも耐性を持つ次世代暗号を安全に実現する技術を開発・実証

【発表のポイント】

- 量子コンピュータでも解読できない次世代暗号方式（PQC: Post Quantum Cryptography）をソフトウェアやハードウェアで安全に実現する方法を開発.
- PQC の国際標準候補のソフトウェア・ハードウェア化に伴う実装安全性を調査し，同候補に共通する攻撃の脅威を払拭する対策を初めて考案・実証.
- 今後の PQC 搭載製品の安全性向上と国際標準化活動に大きく貢献.

【概要】

将来的に大規模な量子コンピュータが実現された場合でも安全に利用できる次世代型暗号方式として、耐量子計算機暗号（PQC）が世界的に期待されています. 東北大学電気通信研究所は，日本電信電話株式会社と共同で，量子コンピュータでも解読が困難な次世代型暗号方式 PQC をソフトウェアやハードウェアで安全に実現する技術を開発しました. 現在 PQC の研究開発は世界的に活発化しており，国際標準方式の選定が進められています. 今回開発した技術は，国際標準候補（9 種類中 8 種類）をソフトウェアやハードウェアで実現した際に生じる物理的な攻撃への懸念を払拭するものであり，来るべき PQC 製品の安全性向上と国際標準化活動に大きく貢献することが期待されます.

この成果は，2021 年 12 月 6-10 日にオンラインで開催された国際暗号学会主催の国際会議「International Conference on the Theory and Application of Cryptology and Information Security（ASIACRYPT 2021）」にて発表されました. また，国際暗号学会の国際学術雑誌「IACR Transactions on Cryptographic Hardware and Embedded Systems」の 2022 年版に電子版が先行掲載されました.

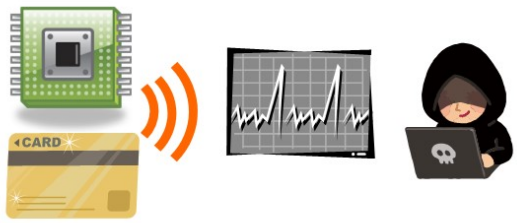
【問い合わせ先】
東北大学　電気通信研究所
担当　教授　本間尚文，助教　上野嶺
電話　022-217-5506
E-mail: contact.ecsislab@grp.tohoku.ac.jp

【開発の社会的背景】

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暗号技術の搭載が不可欠となっています．特に，将来的に大規模な量子コンピュータが実現された場合でも安全に利用できる耐量子計算機暗号（PQC: Post Quantum Cryptography）は，次世代型の暗号方式として世界的に期待されています．現在，米国標準技術研究所（NIST: National Institute of Standards and Technology）の主導によりPQCの国際標準化が進められており，2024年までに標準暗号方式が選定される予定です．国際標準の選定においては，数学的な安全性に加えて，物理的な安全性（PQC を搭載したシステム・製品の動作を物理的に観測・操作して暗号を解読する攻撃への耐性）が求められています． あらかじめ物理的な攻撃を把握することで，PQC をソフトウェアやハードウェアとして安全に実現することができます．

【開発の経緯】

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）および日本電信電話株式会社社会情報研究所（草川恵太主任研究員、高橋順子主任研究員）の研究グループは共同で， 今後の情報通信ネットワークにおけ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，PQC 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．



物理的な観測を使った攻撃（消費電力や計算時間の変化から暗号を解読する攻撃）

物理的な操作を使った攻撃（故意に出力誤りを起こさせて暗号を解読する攻撃）

図１：対策が必要な物理的攻撃の概要：PQC を実行するシステムの動作を物理的に観測・操作する攻撃により暗号が解読される恐れ

【発見・開発した内容】

今回開発した対策技術は，PQC の数学的安全性を高めるために不可欠な構成に係る攻撃を防ぐものであり，PQC をソフトウェアやハードウェアとして実装・搭載する際に適用される技術です．現在 NIST の PQC 国際標準化プロジェクトの最終候補９種類中８ 種類にこの対策が有効であることが分かりました． この対策がない場合，PQC を実行するシステムの動作を攻撃者に物

理的に観測・操作されることで暗号が解読されてしまう恐れがあります（図 1）．本共同研究チームは，そうした攻撃を防ぎつつ PQC を実行するシステムを安全に実現する対策を開発し，実機を用いた実験によりその有効性を実証しました（図 2）．今回の成果は，今後 PQC を搭載・実行するシステムを実現する場合の基盤技術になると期待されます．

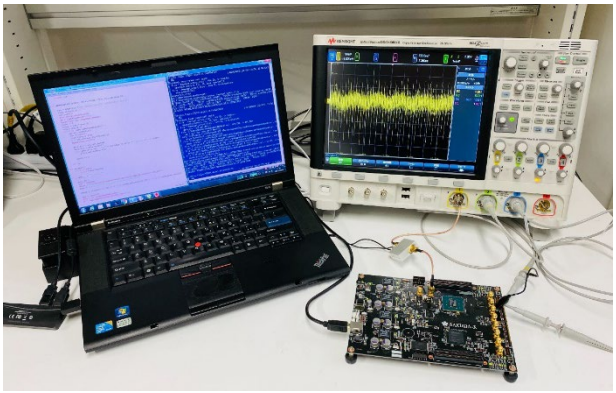


図 2：開発した対策技術による安全性実証実験の様子：物理的に観測されても PQC の動作中に秘密が漏えいしないことを実証

なお，本成果のうち物理的な操作を使った攻撃とその対策は，令和 3 年 12 月にオンラインで開催された国際暗号学会の国際会議 ASIACRYPT で発表されました．また，物理的な観測を使った攻撃とその対策は，国際暗号学会の国際学術雑誌 IACR Transactions on Cryptographic Hardware and Embedded Systems の 2022 年版に電子版が先行掲載されました（学会発表は令和 4 年 9 月の予定です）．

【今後の予定】

世界的に開発がすすむ量子コンピュータに先駆けて安全性を確保する PQC 技術は，今後重要性がますます高まると予想されています．今回開発した対策技術は，PQC をソフトウェアやハードウェアで搭載するシステムを安全に実現する上で必要となるものであり，NIST で選定される PQC の国際標準暗号の実現方法にも影響を与えると予想されます．今後は PQC を様々なシステムに搭載して実証実験をさらにすすめます．当該技術を通して，将来 PQC を利用するさまざま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向上に貢献することを目指しています．

【研究支援】

今回の研究成果は，以下の事業・研究課題の助成により得られました．

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」
科学技術振興機構（JST）戦略的創造研究推進事業
さきがけ「革新的コンピューティング技術の開拓」研究領域（研究総括：井上弘士）「バッテリレス無線センサネットワークのためのポスト量子暗号計算技術」

【発表論文】

著者：Rei Ueno, Keita Xagawa, Yutaro Tanaka, Akira Ito, Junko Takahashi, Naofumi Homma

論文タイトル：Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs
発表論文誌：IACR Transactions on Cryptographic Hardware and Embedded Systems

著者：Keita Xagawa, Akira Ito, Rei Ueno, Junko Takahashi, Naofumi Homma
論文タイトル：Fault-Injection Attacks against NIST's Post-Quantum Cryptography Round 3 KEM Candidates
発表学会：International Conference on the Theory and Application of Cryptology and Information Security（ASIACRYPT 2021）

【用語解説】
*PQC：Post Quantum Cryptography（耐量子計算機暗号）の略．将来的に大規模な量子コンピュータが開発された場合でも解読されることなく安全に利用できるとされる暗号．格子問題や多変数多項式問題の難しさなどを安全性の根拠とします．

**物理的な観測・操作を使った攻撃：サイドチャネル攻撃や故障注入攻撃などと呼ばれる物理的な脆弱性をつく攻撃．比較的安価な装置で実行可能であり，痕跡も残らないことから現実的な脅威として近年はその耐性が特に重要視されています．