岡山大学
担当部署連絡先：
研究協力課・外部資金獲得推進グループ
kaken@adm.okayama-u.ac.jp
作成日：2020年2月27日
更新日：—

科研費 KAKENHI

# IoT・AI時代を支える暗号技術とその攻撃安全性評価

研究者所属・職名：大学院自然科学研究科・教授

ふりがな　のがみ　やすゆき
氏名：野上　保之

主な採択課題：
- 挑戦的研究(開拓)「ICTおよび暗号技術を駆使した医療情報セキュア管理システムの構築」(2019-2022)
- 基盤研究(A)「IoT時代の遠隔操作型・自律型移動システムにおける安全かつ高信頼な通信の実現」(2016-2018)
- 基盤研究(B)「楕円ペアリング暗号に対する共役有理点ノルムを用いた分散並列攻撃法の開発と実証実験」(2013-2015)

分野：情報セキュリティ、暗号技術

キーワード：IoTセキュリティ、アクセス制御、攻撃安全性、情報漏洩対策、データベース保護

## 課題

●なぜこの研究をおこなったのか？（研究の背景・目的）

IoT時代を迎え、様々なデバイスが人の手を介することなく、自律的に情報を通信し、制御コントロールする時代になっている。そのような中、さらにそのデータをクラウド上に集積し、AIが人に代わって重要な操作を担うとなれば、そこには堅牢なセキュリティ対策を実施することが必須である。しかし、それを担うデバイスは必ずしも計算リソースが潤沢ではなく、まさにその隙を突くサイバーフィジカル攻撃が成立し得るため、自動運転をはじめとする最新のシステム・データベースに対して、強力な解読・改ざん攻撃をもって厳密な安全性の評価と、その対策検討が必要となる。

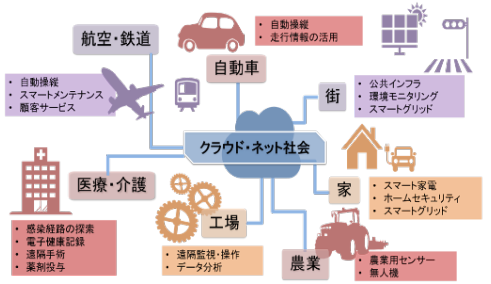

図1　Connected社会のイメージ

●研究するにあたっての苦労や工夫（研究の手法）

情報セキュリティの根幹を成す暗号技術は、複雑な数学をベースとしている。これを実社会において、とりわけ自動運転などの分野においてはリアルタイム処理性能を損なうことなく、またセキュアデータベースに対してはデータサイズのスケーラビリティを達成しながら、ソフト・ハードの両面から効率的に実装する必要がある。効率性と安全性は、とかくトレードオフの関係になりがちであり、その両立を目指すためには、これまでに積み重ねてきた暗号計算アルゴリズム技術およびセキュアな実装技術を緻密に融合させる必要がある。

岡山大学
担当部署連絡先：
研究協力課・外部資金獲得推進グループ
kaken@adm.okayama-u.ac.jp
作成日：2020年2月27日
更新日：—

# IoT・AI時代を支える暗号技術とその攻撃安全性評価

## 研究成果

●どんな成果がでたか？どんな発見があったか？

ターゲットとして、ロボット・自動運転などを実現する種々の技術に対するセキュリティを考えた。Connected Carなどのようにして繋がる社会、それをAIなど駆使しながら遠隔操作することを考えた場合、その末端を担うIoTデバイスには、制御・観測データの認証機能、接続するためのアクセス制御が必要になる。これらを実現するために、広く使われているAES暗号やMAC生成のためのハッシュ関数などを搭載し、これらがソフト・ハードの両面で安全となり得るか攻撃実験を行った。その結果、サイドチャネル攻撃と呼ばれるノイズ観測攻撃に対して、ある状況下においては対策がなければ脆弱であることが分かり、そのための対策を合わせて実装すれば問題を解消し得ることを実証し、またそのような解読・改ざん攻撃の結果として秘密鍵（パスワード）が漏洩する可能性もあるため、実時間での処理が可能な鍵更新機能も開発した。その鍵更新機能をより現実的なものとするために、安全な真性乱数・擬似乱数の生成に関する研究開発、また楕円曲線暗号・楕円ペアリング暗号と呼ばれるIoTデバイス実装に適しているとされる暗号技術を駆使したシステムを開発した。このように、対策を二重三重に施す必要性があることを攻撃実験なども経ながら痛感した。そのような研究開発の延長線上において、医療情報のような機微な個人情報のクラウド管理などを視野に入れた場合、如何にして巨大化するデータベースを漏洩・解読のような攻撃から安全安心に守れるか、またその攻撃の担い手がAIになり得ることも想定しながら、かつその活用性や利便性を損なわない対策を開発する必要があると考え、これまでの研究成果を組合せながら、次世代の独自データベースセキュリティシステムの構築に向けた研究にも着手しているところである。

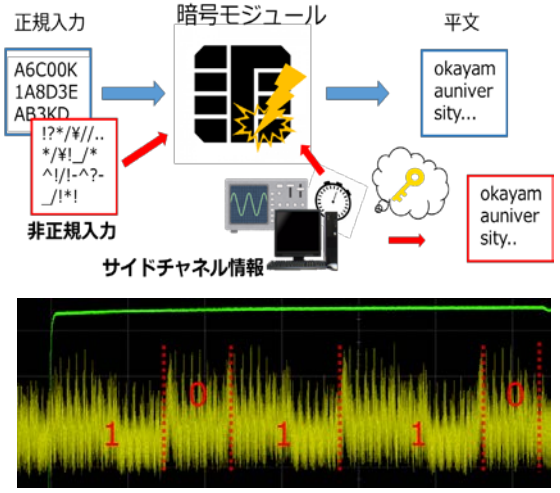


図2　サイドチャネル攻撃のイメージ図
（下図は観測されるノイズ波形）

## 今後の展望

●今後の展望・期待される効果

ユーザやシステムの安全安心を支えるIoT・AI時代のセキュリティ・暗号技術の実現には、既成概念を超える解読・改ざん攻撃を想定し、種々のデバイス・システムを高いレベルで連携させて、それを模擬した強力な攻撃の実証実験も経なければ成し得ない。そのような攻撃手と守り手の間で繰り広げられる攻防を、極めて高いレベルかつ現実的な実証の中で、しかも速い時代の流れに遅れることなくシミュレートする必要がある。攻防両者がAI技術に加え量子計算機を駆使する時代、安全安心なサイバーフィジカル環境の実現に、これまでの研究成果をさらに発展させる必要がある。

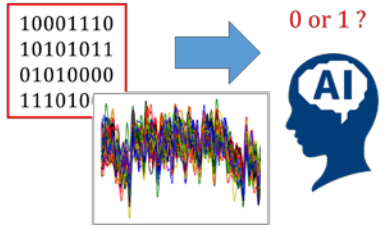


図3　AIによる解読攻撃の
イメージ図