

# 情報を守る暗号化制御

～”秘密のまま計算する”次世代制御技術～

工学研究科 機械工学専攻

◎M2 なかやましょうた 中山聖太、教授 さとうたかお 佐藤孝雄

## キーワード

暗号化制御, 準同型暗号, 暗号化, 復号化,  
サイバーセキュリティ, 産業 DX



## 研究概要

IoT やクラウド技術の発展により、工場設備やロボットをネットワーク経由で監視・制御する仕組みが普及している。今後は「機械を購入する」だけでなく、「制御サービスを利用する」形態も広がると考えられる。このような環境では、計測データや制御信号、制御器がクラウド上で扱われるため、情報漏洩やデータ改ざんなどのリスクが高まる。

そこで本研究では、データを暗号化したまま計算できる準同型暗号を用いた暗号化制御を研究している。これにより、第三者に制御情報を開示することなく制御計算を実行できる。しかし、暗号化制御は平文(非暗号)の制御で一般的に用いられる高度で複雑な計算(非線形)を実行することはできない。そのため、既存の制御理論を単純に暗号化するだけでは不十分であり、暗号文で計算可能な理論を作り直す必要がある。この課題に対して私は、計算の高速化、理論保証、サイバー攻撃対策の観点から研究を進めている。本稿では、その中でもデータ改ざん攻撃への対策を紹介する。暗号化制御ではデータが一見ランダムな数字になっているため、センサ値が改ざんされても異常を判定することが難しい。そこで本研究では、データを復号化せずに攻撃の影響を評価し、安全な制御入力へ切り替える仕組みを提案している。これにより、制御情報を秘匿したまま、サイバー攻撃による機械の誤動作を抑えることを目指している。

図 1 提案した暗号化制御システム

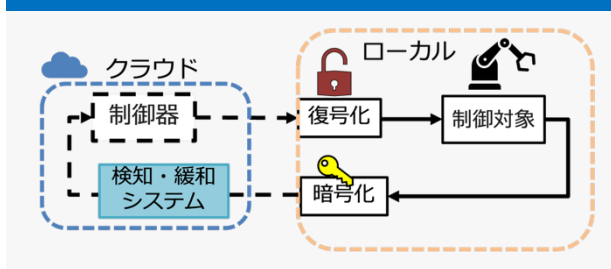
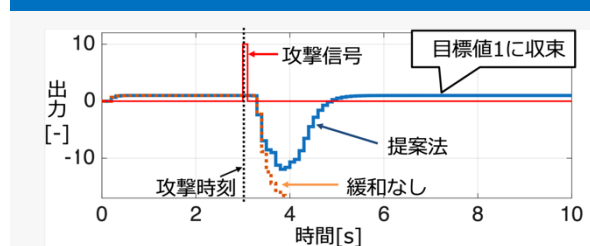


図 2 シミュレーション結果



## アピールポイント

・攻撃検知のためには大小比較や条件分岐が使用されるが、暗号データは、それらの複雑な(非線形の)処理はできないため、従来は攻撃の判定や対処を行うために、平文で処理する必要があった。そこで、暗号文のみで計算可能な攻撃緩和システムを構成することで、攻撃の影響評価から安全な制御入力への切り替えまでを暗号化したまま実現した。これは攻撃評価とその緩和を復号することなく暗号データで計算することのできる初めての暗号化制御手法である。

・これまでの暗号化制御に関する研究成果について、システム情報制御学会(ISCIE) 第 69 回研究発表講演会をはじめとした計 3 回の学会において発表しており、さらに国際会議での 1 件の発表を予定している。また、論文 1 件が ISCIE 論文誌に掲載されており、現在は本稿で紹介した攻撃緩和型暗号化制御および暗号化制御の安定性の解析に関する論文 2 件の投稿準備を進めている。