新技術説明会
New Technology Presentation Meetings!

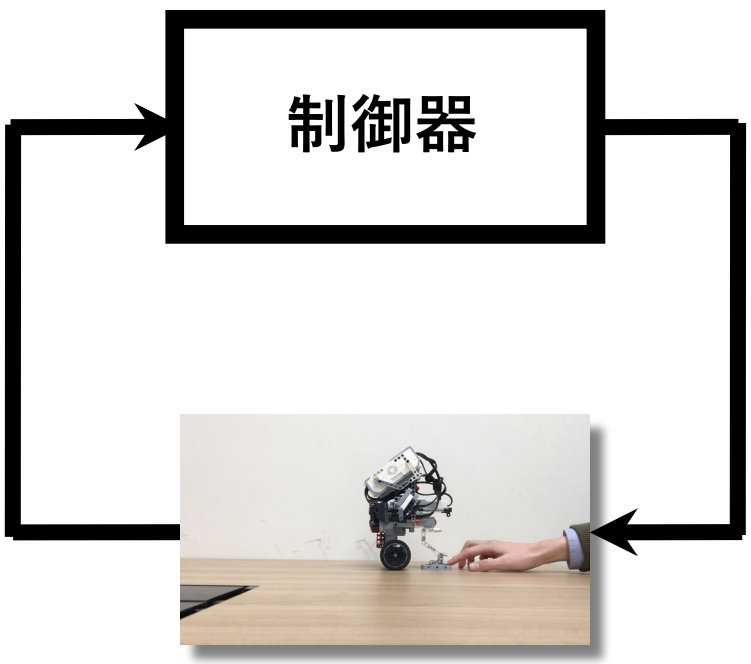
リアルタイム鍵更新と秘密計算によるセキュアな自動制御技術

電気通信大学 情報理工学研究科
機械知能システム学専攻
教授 小木曽公尚

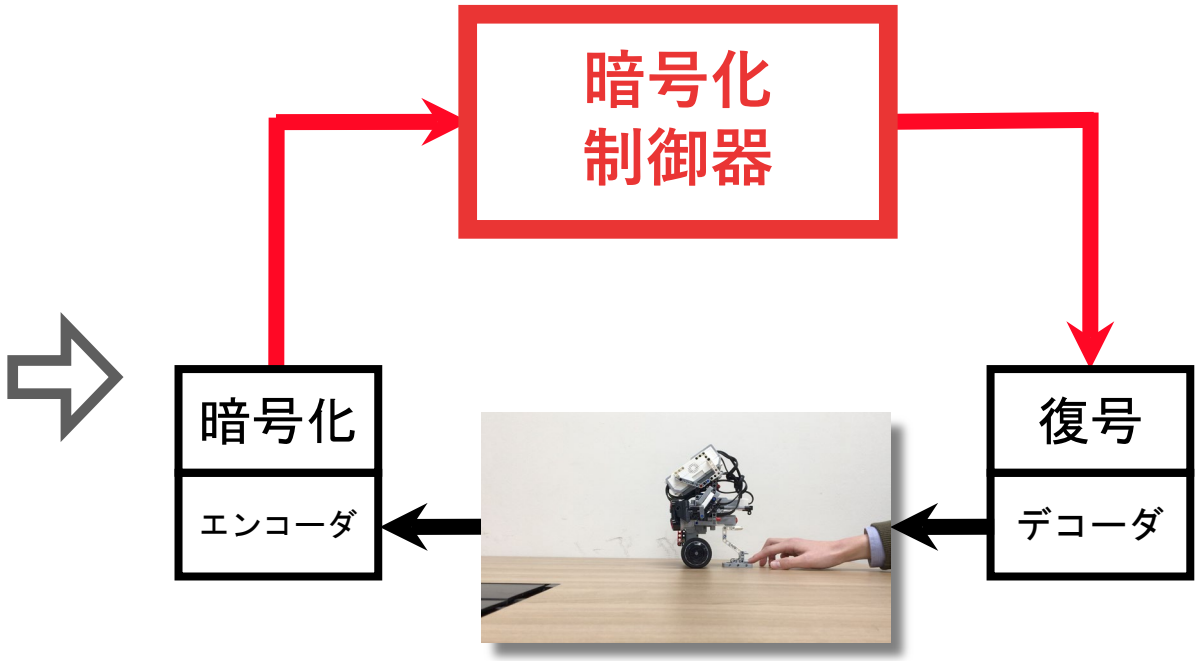
2024年5月14日

暗号化制御システムとは[1]

制御レイヤーの処理を秘密計算(準同型暗号)で再構成した制御技術



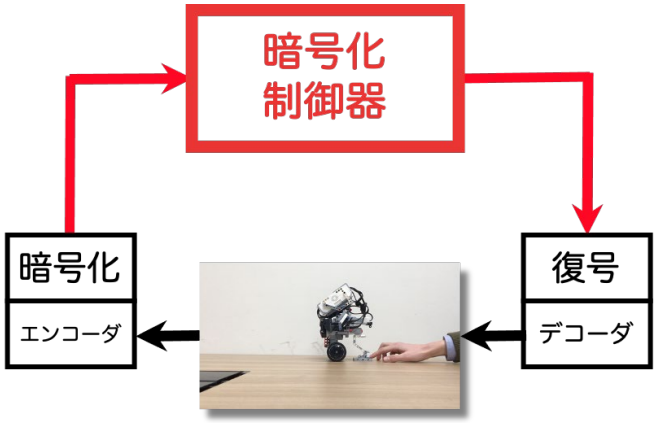
従来の制御システム



暗号化制御システム

[1] Kogiso, Fujita, “Cyber-security enhancement of networked control systems using homomorphic encryption,” *IEEE Conference on Decision and Control*, pp. 6836-6843, 2015.

従来技術とその問題点



多くの製造現場では、安全な通信プロトコルが採用される一方、自動制御システムにおける制御装置内部の信号データやパラメータ等を安全に保存・処理するまでには至っていない。


特許第6360781号

特許証
特許第６３６０７８１号
発明の名称 暗号化制御システムおよび暗号化制御方法、並びにプログラム
特許権者 東京都調布市調布ケ丘一丁目５番地１
国立大学法人電気通信大学
発明者 小木曽 公尚
藤田 貴大
出願番号 特願２０１４－２２６９６４
出願日 平成２６年１１月 ７日
登録日 平成３０年 ６月２９日
平成３０年 ６月２９日
特許庁長官
宗像直子

従来の暗号化制御技術（特許第6360781号）では、

・通信と制御の暗号化
・通信プロトコルと併用可能

を実現したものの、**暗号鍵を更新する仕組みが無く**、計算コストやセキュリティ強度の観点から広く利用されるまでには至っていない。

新技術の特徴・従来技術との比較

- 従来技術の問題点であった、**リアルタイム計算コスト**と**セキュリティ強度**を改良することに成功した。

リアルタイム計算コストの改良：

- 従来は、秒単位の時間を要する鍵生成アルゴリズムを鍵更新のタイミングで実行する必要があったが、新技術により、ミリ秒単位の制御周期と同期させられるまで鍵生成の時間を抑制させることができ、リアルタイムの暗号鍵更新が可能になった。
- たとえば，新技術では，1091 bit の従来技術を 641 bit の鍵長で実現でき、計算資源およびコストの抑制につながる[2]。

[2] Teranishi, Sadamoto, Chakrabortty, Kogiso, “Designing optimal key lengths and control laws for encrypted control systems based on sample identifying complexity and deciphering time,” *IEEE Transactions on Automatic Control*, 68-4, pp. 2183-2198, 2023.

新技術の特徴・従来技術との比較

- 従来技術の問題点であった、**リアルタイム計算コスト**と**セキュリティ強度**を改良することに成功した。

セキュリティの強化：

- 従来は、制御システムの運用中は同じ暗号鍵を使い続ける必要があったが、新技術により、制御周期ごとに新しい暗号鍵が生成される。さらに、数値改ざんなどによる正当性の崩れを用いた攻撃検知が容易になる。
  - セキュリティ強度の向上：より長い鍵長の設定が可能に。
  - 再生攻撃の検知：データ記録時の鍵と注入時の鍵が異なるため。
  - 制御装置の乗っ取り対策：制御周期で鍵の解読が必要に。

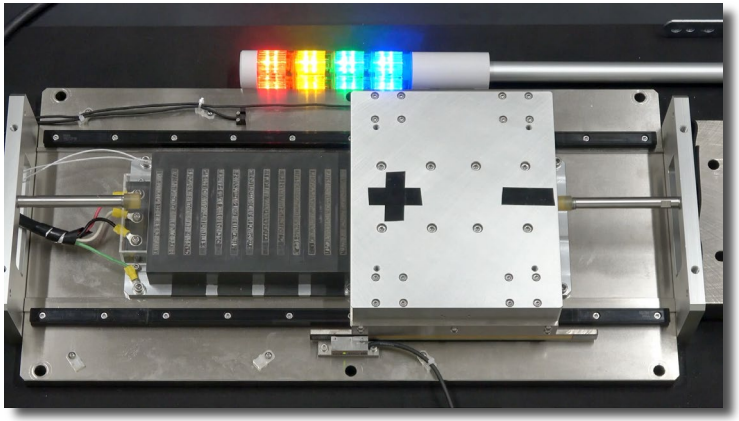
新技術の特徴・従来技術との比較

- バイラテラル制御への応用（KISTECにて展示中）

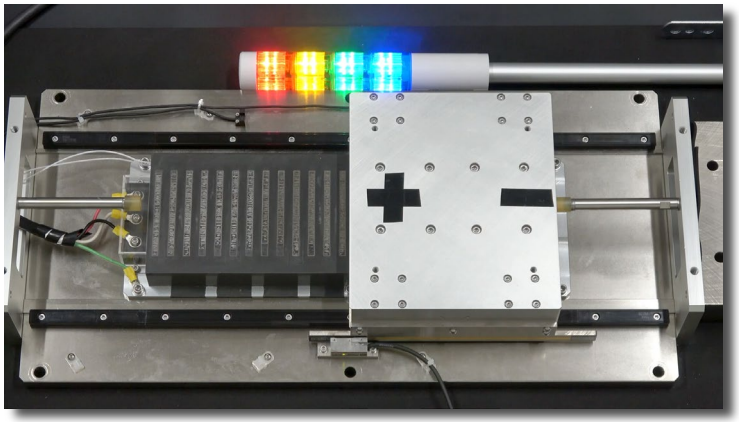
新技術の特徴・従来技術との比較

- ステージ制御への応用

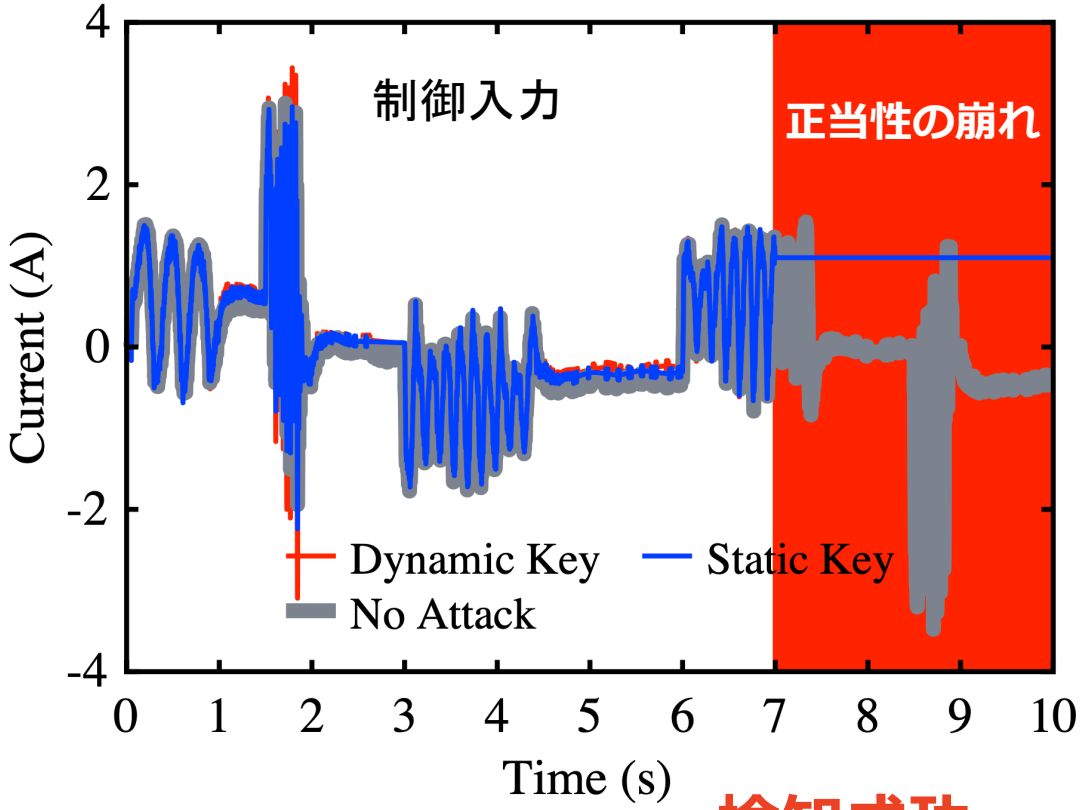
従来技術



新技術



検知失敗



検知成功
(3ミリ秒以内)

想定される用途

- 本技術の特徴を生かすためには、自動化プロセスの産業用計算機や産業用ロボットコントローラなどに適用することで、工場のサイバーセキュリティ強化のメリットが大きいと考えられる。
- 上記以外に、異常検知やプライバシーデータの秘匿化技術が欠かせない自動車・建設機械・船舶・UAVなどの自動運転に効果が得られることも期待される。
- また、セキュアなロボット制御技術が確立することで、遠隔診断・手術、放射性医薬品創薬などの分野に展開することも可能と思われる。

実用化に向けた課題

- 現在、汎用計算機(OS上)で動作する暗号化制御ソフトウェアを開発し、リアルタイム処理・攻撃検知が可能であることを確認済み。
  - **C/C++**：様々な暗号方式や暗号化制御の関数など，鍵長制限なし
  - **Python**：同上、公開・教育用途[3]
    ECLib v1.5.4 https://github.com/KaoruTeranishi/EncryptedControl
  - **MATLAB/Simulink**：暗号化PID制御ブロックなど[4]，鍵長制限あり
- 今後、FPGAを含む産業用制御装置に実装して処理データの収集および評価を行い、制御対象に応じた各種パラメータのチューニング方法や計算資源の限界を明らかにする。
- 実用化に向けて、制御周期内に一連の処理が完了するよう、ソフトウェアおよびハードウェアの技術を確立する必要もあり。

[3] 寺西，小木曽：ECLib：暗号化制御のためのPythonライブラリ，特集号 制御工学の発展・応用を支えるソフトウェア・ベンチマーク問題，**計測と制御**，Vol. 62, No. 9, pp. 523-526, 2023.
[4] 山田，小木曽：暗号化制御による通信と制御の秘匿化およびサイバーセキュリティ対策, 2024年度自動車技術会春季大会.

企業への期待

- 制御機器の仕様に応じた本技術の実装・チューニングが必要になるため、PoCから検討を進められることが好ましい。
- 共同研究について
  - 自動制御（制御レイヤー）にサイバーセキュリティ対策の導入を検討の企業
  - 制御機器のリバースエンジニアリング対策にご興味のある企業
  - 制御技術者の育成やサポートが必要な企業など
  - 社会人博士課程・共同研究員の活用

企業への貢献、PRポイント

- 本技術により制御システムのセキュア化が可能なため、製品やサービスに付加価値を与え、企業に貢献できると考えている。
- 本格導入にあたって、技術指導やサポートの実施。
- 知財の共同出願対応、論文化による公開

本技術に関する知的財産権

- 発明の名称：　暗号化制御システム、暗号化制御方法および暗号化制御プログラム
- 出願番号：　特願2021-504051
- 出願人：　電気通信大学
- 発明者：　小木曽公尚、日下雅博

産学官連携の経歴

- 2013年以降、建設系、自動車系、電子部品系など民間企業との共同研究を10件以上実施した実績あり

お問い合わせ先

国立大学法人電気通信大学
産学官連携センター
産学官連携ワンストップサービス

TEL:　042-443-5871
FAX:　042-443-5725
E-mail:　onestop@sangaku.uec.ac.jp