オープンイノベーション推進ポータル
株式会社キャンパスクリエイト

テーマ名	制御器の処理をリアルタイムに暗号化／復号化する セキュリティ技術と IoT への応用
組織名	国立大学法人電気通信大学 情報理工学研究科 小木曽 公尚 准教授
技術分野	IT、ものづくり

概要

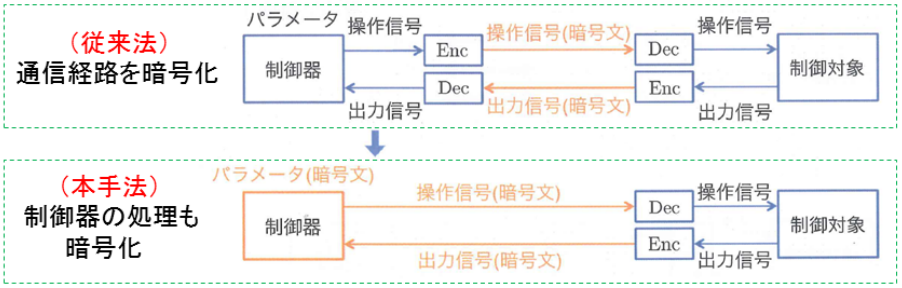
工場やプラントなどモノづくり産業における IoT インフラの整備や自動車の電子制御など、制御系のネットワーク化が進んでおり、それに伴ってセキュリティ強化も重要視されています。本研究では従来のセキュリティ技術の概念のように通信経路を暗号化するだけでなく、制御器（コントローラ）での処理までもリアルタイムに暗号化することで、セキュリティ性をより高める技術を研究しています。本技術の活用に意欲がある企業様を歓迎します。

簡略図

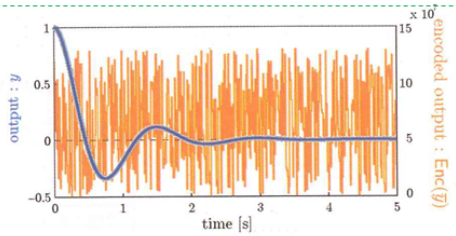
制御器の処理をリアルタイムに暗号化／複合化する
セキュリティ技術とIoTへの応用

【原理】

制御器の演算に用いる情報を秘匿したまま処理する手法を提案



（暗号化結果）
定常状態後も
高セキュリティ性を実現



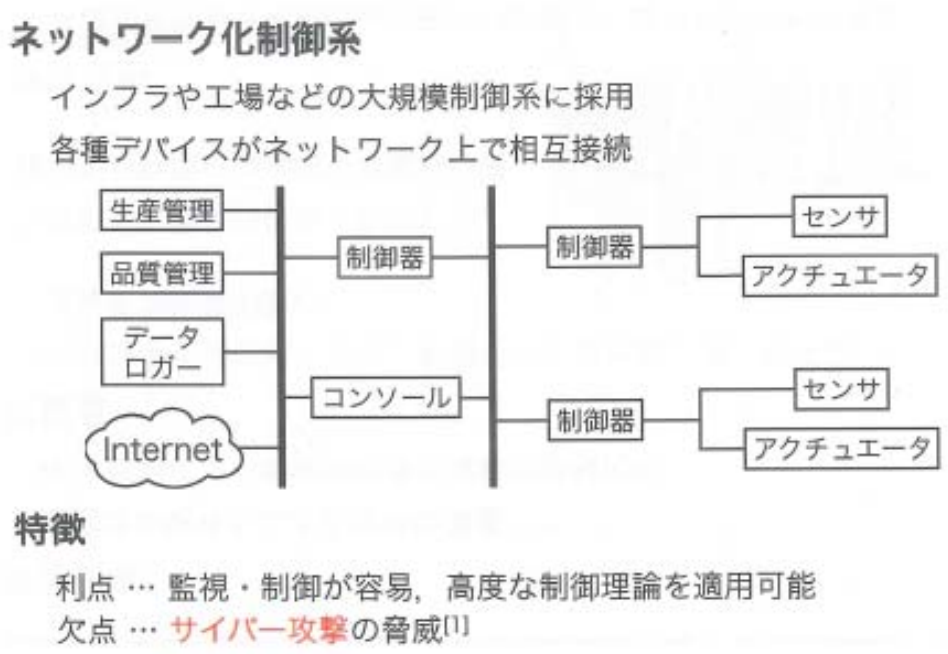
※青線：制御信号。 オレンジ線：暗号処理結果

製造業・インフラ・自動車など
制御系システムの新セキュリティ技術として活用可能

背景

現在、電気・ガス・水道など生活を支える重要インフラの制御システムは、ネットワーク化が進んでいます。特にモノづくり産業の IoT や自動車の電子制御が進むにつれてその傾向は顕著になっています。

しかしながら、ネットワーク化の進展に伴い、サイバー攻撃の危険性が注目されつつあります。実際に発電所や工場などのプラント動作を監視・制御する制御システムに対するサイバー攻撃が出現し、大きな社会的問題になっています。海外では 1990 年後半の米国重要インフラから始まり、2010 年のイランにおける核燃料施設のウラン濃縮用遠心分離を標的としたサイバー攻撃など重大な国際問題に繋がりかねない状況です。日本でも制御システムに対して USB メモリを介したウィルス感染、操作端末の入れ替え時やリモートメンテナンス回線による不正アクセス・マルウェア混入などによる危険性が指摘されています。



上記背景に伴い、セキュリティ技術の活用が期待されていますが、従来のセキュリティの概念は、制御器と制御対象間の通信経路を暗号化する手法がほとんどであり、制御器そのものがハッキングを受けた場合には脆弱です。

そこで本研究では、通信経路だけでなく、制御器内の処理そのものも暗号化／復号化することで、セキュリティ性をより高める技術を開発しています。

本技術の活用に関心がある企業様のご相談をお待ちしております。

※特許出願済み。

技術内容

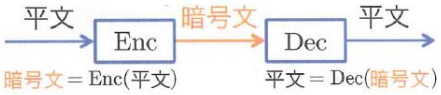
従来のセキュリティ技術は、下記の通り、制御器からの信号をエンコーダ・デコーダを通じた通信経路により制御対象へ伝えています。通信経路内を暗号化することでセキュリティ性を確保しますが、制御器の内部の情報は暗号化されていません。

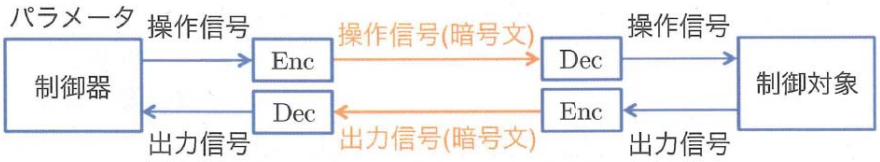
そのため、制御器内部に侵入された場合に信号や設計値を流出させてしまいます。

先行研究

ネットワークの暗号化・通信プロトコルの整備[2]

- 暗号による通信路の秘匿化
- 制御性能に影響しない

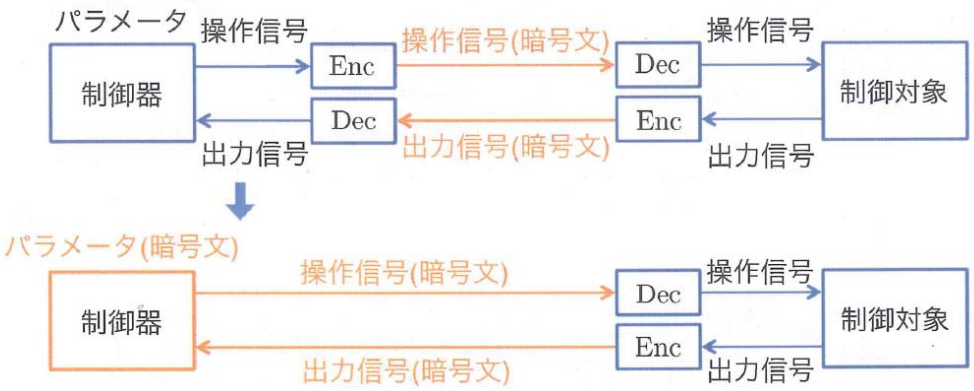




それに対し、本技術では制御器そのものを暗号化することで、制御器の内部処理を盗聴されても暗号文しか奪取されないようセキュリティ性を高めています。

暗号化された制御器はリアルタイムに処理できるため、制御性能はほとんど変化しません。

制御器の演算に用いる情報を秘匿したまま処理する手法を提案



暗号化／復号化は Elgamal 暗号あるいは RSA 暗号と呼ばれる手法を利用します。Elgamal 暗号は元の情報に対して乱数を用いて暗号化するため、仮に暗号文をハッキングされても、元の情報のおもかげがないため容易に解読できません。

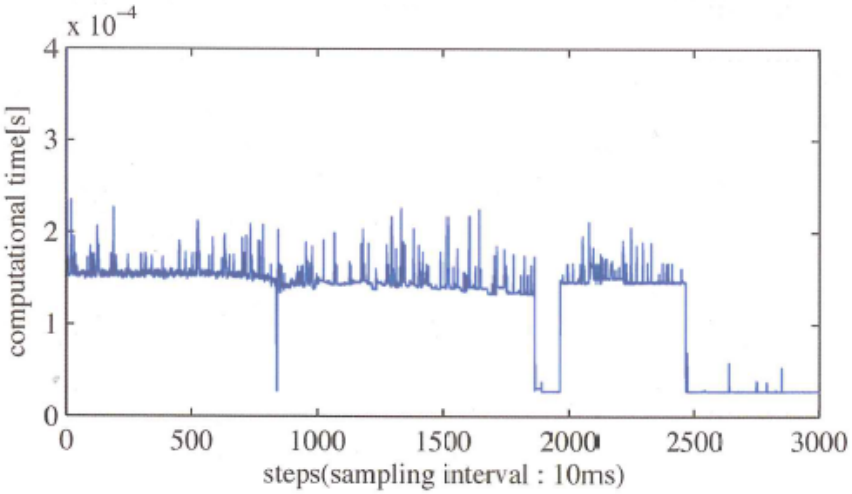
技術・ノウハウの強み（新規性、優位性、有用性）

・制御器の処理そのものを暗号化・復号化します。そのため、制御系がハッキングを受けても高いセキュリティ性を実現します。

・暗号化／復号化をリアルタイムに処理できるため、制御系の処理と並列して行うことができ、制御システムへの影響もほとんど発生しません。

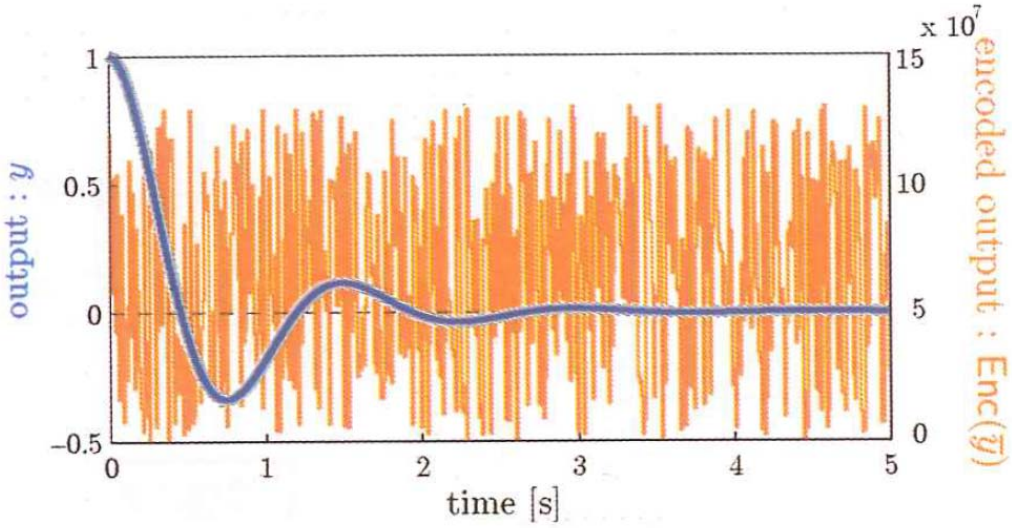
例えば下記は実験的に RSA 暗号という手法でシミュレーションした結果ですが、数十 msec オーダーで処理可能です。このシミュレーションは Matlab 上で行った結果のため、C 系言語でコーディングすることにより数 msec オーダーも十分に達成可能と想定できます。Elgamal 暗号の場合も同様です。

実行時間 (鍵長27bit)



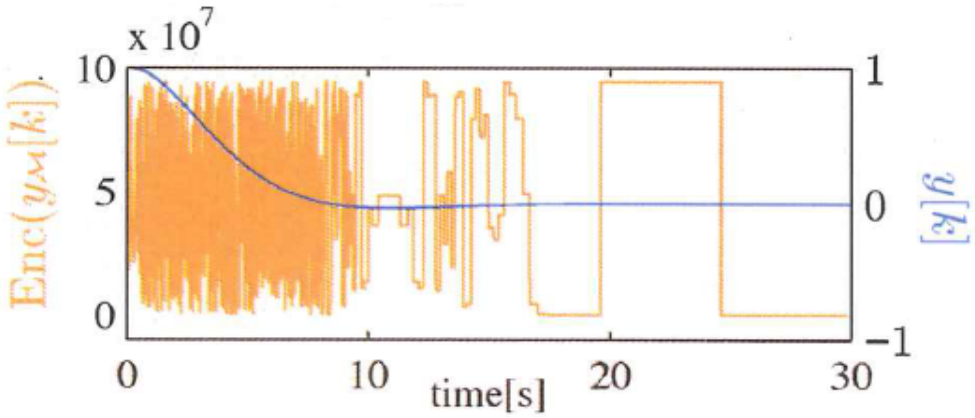
MATLAB R2014a　Intel Core i5 3.2GHz　RAM16GB

・Elgamal 暗号では、制御系が定常状態となってもセキュリティ性が保たれます。
下記は青線が制御信号であり、約 2.5 秒後に定常状態となっています。オレンジ線は制御信号を暗号化した結果ですが、定常状態後も変化がありません。



比較のため、RSA 暗号のシミュレーション結果を記載します。定常状態後はオレンジ線に規則性が出るため、セキュリティ性能が落ちてしまいます。Elgamal 暗号の利

用の背景は、RSA 暗号の定常状態後におけるセキュリティ脆弱性を解決するために開発しました。



連携企業のイメージ

本技術の活用に興味がある企業を歓迎いたします。
例えば、下記の企業と連携できる可能性があります。

1）制御用システム・製品を開発・事業としている企業。
2）セキュリティ分野の事業を展開している企業
3）製造業分野向けシステムソリューションを提供している企業。
4）カーエレクトロニクス向けシステムソリューションを提供している企業。
5）インフラ分野向けシステムソリューションを提供している企業。
6）その他本技術の活用に意欲がある企業。

技術・ノウハウの活用シーン（イメージ）

制御用の機器あるいはソフトウェア製品に本技術をパッケージ化して利用することを想定しています。制御用の機器は、製造業では PLC、自動車分野では ECU などが例として挙げられます。

即ち、PLC あるいは ECU にハッキングがあった場合、あるいは制御用ソフトウェアを処理している PC にハッキングがあった場合も高いセキュリティ性を確保できます。

技術・ノウハウの活用の流れ

本技術の活用にご関心があればお気軽にお問合せください。
詳細の技術内容をご紹介させていただきます。

暗号について詳しく無い場合も分かりやすくご紹介させていただきます。

専門用語の解説

【IoT】
IoT とは、コンピュータなどの情報・通信機器だけでなく、世の中に存在する様々な物体（モノ）に通信機能を持たせ、インターネットに接続したり相互に通信することにより、自動認識や自動制御、遠隔計測などを行う概念です。最近はドイツの Industry4.0 のようにモノづくり分野において IoT を活用する手法や、自動車などの自立制御の期待が高まり、普及が進んでいます。

【ElGamal 暗号】
位数が大きな群の離散対数問題が困難であることを安全性の根拠とした公開鍵暗号の一つです。乱数を用いることで高いセキュリティ性を実現できます。

【RSA 暗号】
桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つです。 暗号とデジタル署名を実現できる方式として最初に公開されたものであり、一般に普及しています。

お問合せ先

下記からお問合せください。
http://www.open-innovation-portal.com/open/it/iot.html