[計測自動制御学会論文集
Vol.51, No.9, 655/660（2015）]

RSA 公開鍵暗号を用いたネットワーク制御系のセキュリティ強化

藤田貴大*・澤田賢治**
小木曽公尚**・新誠一**

Security Enhancement of Networked Control Systems with RSA Public-key Cryptosystem

Takahiro Fujita*, Kenji Sawada**,
Kiminao Kogiso** and Seiichi Shin**

This study aims at proposing a novel concept of a secured controller to achieve enhancement of cyber-security in networked control systems using RSA public-key encryption. With homomorphism of the RSA encryption, the proposed method enables to conceal not only signals over communication links in the control systems, but also parameters of controllers used in determining a control input. A numerical example is employed to confirm that the proposed method correctly functions for the cyber-security enhancement.

Key Words: RSA encryption, homomorphism, cyber-security, networked control system

1. はじめに

現在，電気・ガス・水道などわれわれの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る．ICT 技術やネットワーク化は，制御システムに多大な恩恵を与える一方，サイバー攻撃という新たな脅威を呼び込むことになった．実際，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る．海外では，1990 年後半の米国重要インフラに対する攻撃から始まり，2010 年のイランにある核燃料施設のウラン濃縮用遠心分離を標的とした Stuxnet による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ある [1]．わが国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る [2]．上記のように，重要インフラを支える制御システムをサイバー攻撃から守るための技術開発は，急務である．これを受けて，制御システムへの情報系セキュリティ技術の転用やサイバー攻撃の検知に関する研究 [3)~6)] が近年活発である．

ネットワーク制御系では，**Fig. 1** に示されるように，各デバイスがネットワークを介し相互に接続されていること，インターネット網を利用した外部からの遠隔監視・制御が行なわれていることから，企業内や大規模工場内のネットワーク情報が常に盗聴の危険に晒されている．本研究では，制御システムへの盗聴対策として，暗号に着目する．暗号は，秘密情報を攻撃者が理解できないように秘匿する技術である．制御システムにおける秘密情報には，三種類がある．一つは，制御対象と制御器間でやり取りされる測定量・操作量，そして，ログ収集サーバに保存される各種の信号である．この信号を秘匿することは，制御システムのシステム同定によるプラントモデルの盗取やリプレイアタック対策に繋がる．二つ目は，レシピ情報である．化学プラントにおいて，その企業独自のプラント運転手順であるレシピ情報は，第三者に対し秘匿されねばならない．この情報は，製造プロセスの状況監視オペレータから制御器へ伝達される目標信号に対応している．そ

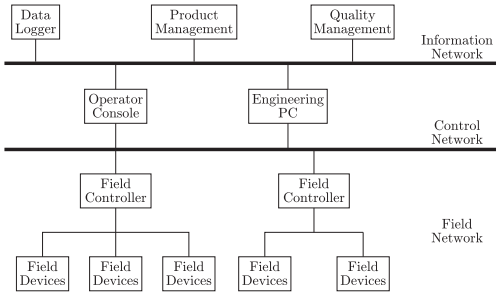

Fig. 1 Large-scale networked control system

* 奈良先端科学技術大学院大学情報科学研究科
生駒市高山町 8916–5
** 電気通信大学大学院情報理工学研究科　調布市調布ケ丘 1–5–1
* Graduate School of Information Science, Nara Institute of Science and Technology, 8916–5 Takayama-cho, Ikoma
** Graduate School of Information and Engineering, The University of Electro-Communications, 1–5–1 Choufu-gaoka, Chofu
（Received March 20, 2015）
（Revised July 6, 2015）

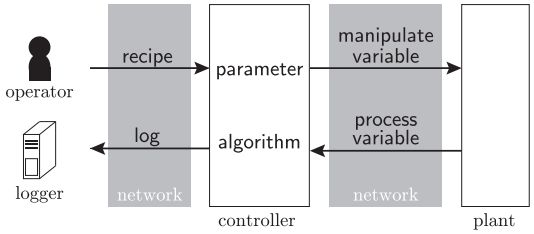

Fig. 2 Secret informations

して，三つ目は，制御器内のパラメータや制御アルゴリズムである．モデル予測制御など，内部にプラントの情報を含む補償器の場合，リバースエンジニアリングにより，制御アルゴリズムやプラントモデルの特定に繋がり，企業の重要技術の流出や漏洩を引き起こすかもしれない．**Fig. 2** は，ネットワーク制御系上の秘密情報を明示したものである．

このように，制御システムセキュリティにおける暗号化の利点は非常に大きく，ネットワーク上の通信路を対象とした暗号化の議論が従来より行なわれている [7)~9)]．しかし，これらの従来研究では，制御器において制御入力を決定するために，一度復号を行なっており，制御器の内部では暗号化されない情報が扱われる．このため，攻撃者が制御器への不正アクセスを行なった場合，情報流出の危険性がある．したがって，制御システム固有の秘密情報を保護するためには，制御システムの信号がすべて集まる補償器を暗号化することが重要であると考える．さらに，この補償器の暗号化は，新しい着想であり，制御システムのセキュリティ強化を実現する重要な要素技術になる可能性がある．

そこで本稿では，制御システムのセキュリティ強化を目的とし，前述の三種の情報をすべて暗号化したまま演算が可能な暗号化制御則の概念を提案する．そして，研究の端緒として，一般的な公開鍵暗号の一つである RSA 暗号を制御システムのセキュリティに応用することを考える．特に，RSA 暗号方式の場合にその準同型性から，比例制御に対する暗号化制御則が実現できることを示す．また，提案法の有用性を確認するため，RSA 暗号を制御システムに適用した際の動作と秘匿性を，数値シミュレーションにより検討する．なお，暗号化制御則の一般化，つまり，線形制御器や多項式で表わされる非線形補償器を対象とする暗号化制御則の実現は可能であるが，紙面の都合上，本稿では割愛する．文献 10) で示すアイデアと同様であるので，一般化についての詳細は，同文献を参照されたい．

2. RSA 暗号

暗号とは，第三者に知られたくない秘密情報を，意図した受信者のみが理解できるように加工する技術である．加工前の情報を平文，加工後の情報を暗号文と呼ぶ．平文から暗号文への変換を暗号化という．逆に，正当な受信者が暗号文から平文を復元する過程を復号と呼ぶ．暗号化と復号の際に用いられる定数を鍵という．

RSA 暗号は，1978 年に Rivest らにより発明された暗号方式であり，現在最も広く用いられている [11)]．以下に，RSA 暗号方式およびその準同型性について述べる．ここで，記号を定義しておく．$\mathbb{Z}$: 整数集合，$\mathbb{Z}^+$: 非負の整数集合，$\mathbb{Z}_n$: 0 以上 n 未満の整数集合 (n を法とする整数の集合 [12)]，$\mathbb{Z}_n \subset \mathbb{Z}$)，$\mathcal{M}$: 平文の集合 ($\mathcal{M} \subset \mathbb{Z}_n$)，$\mathcal{C}$: 暗号文の集合 ($\mathcal{C} \subset \mathbb{Z}_n$)．

2.1 RSA 暗号方式

任意の暗号方式 $\mathcal{E}$ は，鍵生成 (Gen)，平文の暗号化 (Enc)，暗号文の復号 (Dec) の 3 アルゴリズムにより構成され，$\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ と表わす．RSA 暗号の場合，各アルゴリズムは，つぎのように構成される．

鍵生成アルゴリズム (Gen)

平文の暗号化に用いる公開鍵 e，$n \in \mathbb{Z}^+$ と暗号文の復号に用いる秘密鍵 $d \in \mathbb{Z}^+$ を生成する．

（1） 二つの素数 p, q (パラメータ) を決定する．

（2） 一つ目の公開鍵 n を $n = pq$ とする．

（3） 二つ目の公開鍵 e を $\phi(n) = (p-1)(q-1)$ と互いに素な適当な正整数とする．

（4） 秘密鍵 d を次式を満足する正整数とする．

$$ed \mod \phi(n) = 1 \tag{1}$$

ここで，mod は，剰余を表わし，床関数 $\lfloor \bullet \rfloor$ を用いて $a \mod b = a - \lfloor a/b \rfloor b$ と定義される．(1) 式から，$d \mod \phi(n) = e^{-1} \mod \phi(n)$ は，モジュラ逆数となり，拡張ユークリッドアルゴリズムにより効率的に解くことができる [11)]．

暗号化アルゴリズム (Enc)

鍵生成により得られた公開鍵 n および e を用い，平文 $m \in \mathcal{M}$ を暗号化する．RSA 暗号の場合，平文は，写像 E により暗号文 $c \in \mathcal{C}$ へ変換される．

$$c = \mathrm{E}(m) := m^e \mod n \tag{2}$$

復号アルゴリズム (Dec)

鍵生成により得られた秘密鍵 d を用い，暗号文を復号する．RSA 暗号の場合，暗号文 $c \in \mathcal{C}$ は，写像 C により $m' \in \mathcal{M}$ へ変換される．

$$m' = \mathrm{D}(c) := c^d \mod n$$

ここで，$\mathrm{D}(\mathrm{E}(m)) = m$ である [11)]．

2.2 準同型性

定義 1. 公開鍵暗号 $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が準同型性をもつとは，Gen で生成される任意の鍵に対し，以下の三条件を満足することである [12)]．

（1） 平文空間 $\mathcal{M}$ とその上の演算 $\circ$，および暗号文空間 $\mathcal{C}$ とその上の演算 $*$ がそれぞれ群を成している．

（2） $\mathrm{E}(m) \in \mathcal{C},\ \forall m \in \mathcal{M}$

（3） $\mathrm{E}(m_1 \circ m_2) = \mathrm{E}(m_1) * \mathrm{E}(m_2),\ \forall m_1, m_2 \in \mathcal{M}$

また，準同型性を有する公開鍵暗号を準同型暗号という．

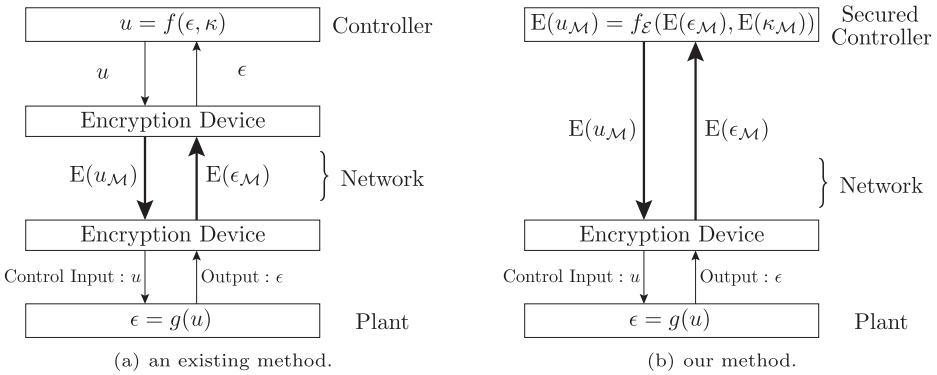

Fig. 3　Concept of secured controller for cybersecurity enhancement

この定義より，準同型暗号では，平文同士の演算結果に対応する暗号文 $\mathrm{E}(m_1 \circ m_2)$ を計算する際，$\mathrm{E}(m_1)$，$\mathrm{E}(m_2)$ を用いるため，復号が不要となり，比較的高い秘匿性が保証される．

RSA 暗号は，定義 1 条件 (3) での $\circ$ が乗算に，$*$ が乗算剰余に対応する準同型性を有しており，

$$\mathrm{E}(m_1 m_2) = \mathrm{E}(m_1)\mathrm{E}(m_2) \mod n \tag{3}$$

の成立が知られている [13]．以下に，(3)式の成立を確認する．各平文 m_1，m_2 に対応する暗号文 $\mathrm{E}(m_1)$，$\mathrm{E}(m_2)$ は，(2)式より，

$$\mathrm{E}(m_i) = m_i^e - Q_i n,\ i = 1, 2$$

となる．ここで，$Q_i \in \mathbb{Z}$ である．$\mathrm{E}(m_i)$ を(3)式の右辺に代入することで，同式左辺に一致する．

$$\begin{aligned}
&\mathrm{E}(m_1)\mathrm{E}(m_2) \mod n \\
&= (m_1^e - Q_1 n)(m_2^e - Q_2 n) \mod n \\
&= (Q_1 Q_2 n - (Q_1 + Q_2))\, n + m_1^e m_2^e \mod n \\
&= Q_3 n + m_1^e m_2^e \mod n \\
&= (m_1 m_2)^e \mod n
\end{aligned}$$

なお，RSA 暗号では，$\mathrm{E}(0) = 0$ で，E は単射である．

2.3　例題

RSA 暗号による暗号化・復号，および，準同型性を説明するため，二つの平文 $m_1 = 1234$，$m_2 = 4321$ を用いて，$m_1 m_2 = 5332114$ を計算する．

鍵生成

パラメータ $p = 9689$，$q = 9743$ とする．これより，$n = pq = 94399927$，および，$\phi(n) = (p-1)(q-1) = 94380496$ を得る．また，$\phi(n)$ と互いに素となる適当な正整数 $e = 587$ を選ぶ．このとき，$d \mod \phi(n) = e^{-1} \mod \phi(n)$ を満たすモジュラ逆数 d は，$d = 42929459$ と求まる．

暗号化

平文 $m_1 = 1234$，$m_2 = 4321$ を(2)式を用いて暗号化する．

$$\mathrm{E}(m_1) = 1234^{587} \mod 94399927 = 17816295$$

$$\mathrm{E}(m_2) = 4321^{587} \mod 94399927 = 61063136$$

準同型性

乗算 $E(m_1 m_2)$ を計算する．(3)式より，

$$\begin{aligned}
&\mathrm{E}(m_1 m_2) \\
&= \mathrm{E}(m_1)\mathrm{E}(m_2) \mod n \\
&= 17816295 \times 61063136 \mod 94399927 = 89094876
\end{aligned}$$

復号

暗号文 $\mathrm{E}(m_1)$，$\mathrm{E}(m_2)$ を復号せず，準同型性を用いて，乗算 $m_1 m_2 = D(89094876)$ を求める．

$$\begin{aligned}
\mathrm{D}(89094876) &= 89094876^{42929459} \mod 94399927 \\
&= 5332114
\end{aligned}$$

いま，$m_1 m_2 = 1234 \times 4321 = 5332114$ なので，演算結果は一致する．次章では，この演算の性質を制御系に応用することを考える．

3.　ネットワーク制御系の暗号化

従来より行なわれているネットワーク化制御系の暗号化は，**Fig. 3** (a) のように，デバイス間を接続する通信路のみを対象としている．制御対象や制御器内部の情報を攻撃者から秘匿するために，通信路を流れる信号だけでなく，制御則を暗号化するネットワーク制御系を構成する (Fig. 3 参照)．

3.1　実数と平文 (整数) の関係

制御系内を流れる信号は実数，平文は整数値である．そこで，準備として，実数 (信号) から整数 (平文) の対応を説明する．たとえば，$\psi = 3.56$ の場合，まず，356×10^{-2} と表現を変換し，整数 $a_1, a_2 \in \mathbb{Z}$ を用い，$a_1 \times 10^{a_2}$ と表わせる．a_2 が共通で固定とすれば，ψ の平文は，a_1 に対応する．一般に，ベクトル信号 $\psi \in \mathbb{R}^m$ からその平文 $\psi_{\mathcal{M}} \in \mathcal{M}^m \times \mathbb{Z}$ への写像 Γ は，$\Gamma : \mathbb{R}^m \to \mathcal{M}^m \times \mathbb{Z}$ と定義できる．また，その逆写像，平文 (ベクトル) から実数への写像も定義可能であり，Γ^{-1} と表記する．このとき，$\Gamma(\psi) = (\lfloor 10^{-a_2}\psi \rceil, a_2)$，$\Gamma^{-1}(\psi_{\mathcal{M}}, a_2) = \psi_{\mathcal{M}} \times 10^{a_2}$ と実現できる．ここで，$\lfloor \bullet \rceil$ は，小数点第一位での四捨五入を表わす．もし a_2 が無限大なら

ば，任意の $\psi \in \mathbb{R}^m$ に対し，$\Gamma^{-1}(\Gamma(\psi)) = \psi$ が成り立つ．無限大でない場合には，四捨五入による変換誤差が生じる．その変換誤差は，制御系の安定性や制御性能に影響を与えることが想像される．この点に関しては，今後の課題とする．本稿では，a_2 は，十分に大きな値として議論を進める．

暗号化と復号の定義を，実数を考慮したものに更新する．暗号化は，$\mathrm{E} : \mathcal{M}^m \times \mathbb{Z} \to \mathcal{C}^m \times \mathbb{Z}$ とし，復号は，$\mathrm{D} : \mathcal{C}^m \times \mathbb{Z} \to \mathcal{M}^m \times \mathbb{Z}$ と定義する．

3.2 信号と制御則の暗号化

本研究では，すでにネットワーク化制御系が設計されているとし，観測出力や目標値との偏差などの制御器への入力信号 $\epsilon \in \mathbb{R}^{m_1}$ および制御器のゲインをベクトルにまとめたパラメータ $\kappa \in \mathbb{R}^{m_2}$ を用い，制御入力 $u \in \mathbb{R}^{m_3}$ を決定する制御則 (の演算) $f : \mathbb{R}^{m_1} \times \mathbb{R}^{m_2} \to \mathbb{R}^{m_3}$,

$$u[k] = f(\epsilon[k], \kappa) \quad \forall k \in \mathbb{Z}_0^+ \tag{4}$$

を考える．ここで，k は，ステップを表わす．

定義 2. (4)式の制御則 $f(\epsilon, \kappa)$ に対し，ある暗号方式 $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を用いた写像 $f_{\mathcal{E}} : \mathcal{C}^{m_1} \times \mathcal{C}^{m_2} \times \mathbb{Z} \to \mathcal{C}^{m_3} \times \mathbb{Z}$ が存在し，$\mathcal{E}$ により暗号化された信号 $\mathrm{E}(\epsilon_{\mathcal{M}})$ および制御器のパラメータ $\mathrm{E}(\kappa_{\mathcal{M}})$ が次式

$$f_{\mathcal{E}}\left(\mathrm{E}(\epsilon_{\mathcal{M}}), \mathrm{E}(\kappa_{\mathcal{M}})\right) = E(\Gamma(f(\epsilon, \kappa))) \ \forall k \in \mathbb{Z}_0^+$$

を満たすとき，写像 $f_{\mathcal{E}}$ を f の暗号化制御則と呼ぶ．

暗号化制御則 $f_{\mathcal{E}}$ の特徴は，制御器内で秘密鍵 d を用いずに (暗号化された) 制御入力を直接計算できることである．本研究では，与えられた f と暗号方式に対して $f_{\mathcal{E}}$ を実現することにより，復号を行なわずに制御器内の演算を実行し，制御器内部処理の秘匿性を向上させる暗号化制御系の構成を目的とする．

3.3 RSA 暗号を用いた暗号化制御則

本稿では，RSA 暗号を用いた暗号化制御則を示す．

定理 1. 制御器パラメータ κ がゲイン $K \in \mathbb{R}$ の場合 $(m_1 = m_2 = m_3 = 1)$，制御則 $u[k] = f(\epsilon[k], K) = K\epsilon[k]$ に対し，RSA 公開鍵暗号方式を用いた暗号化制御則は，

$$\begin{aligned}\mathrm{E}(u_{\mathcal{M}}[k]) &= f_{\mathcal{E}}(\mathrm{E}(\epsilon_{\mathcal{M}}[k]), \mathrm{E}(K_{\mathcal{M}})) \\ &= \mathrm{E}(K_{\mathcal{M}})\mathrm{E}(\epsilon_{\mathcal{M}}[k]) \mod n\end{aligned}$$

である．ここで，$\epsilon_{\mathcal{M}} = \Gamma(\epsilon)$ は，誤差 $\epsilon \in \mathbb{R}$ の平文である．

証明. 準同型性(3)より，暗号化制御則の実現式

$$\begin{aligned}f_{\mathcal{E}}\left(\mathrm{E}(\epsilon_{\mathcal{M}}), \mathrm{E}(K_{\mathcal{M}})\right) &= \mathrm{E}(K_{\mathcal{M}})\mathrm{E}(\epsilon_{\mathcal{M}}) \mod n \\ &= \mathrm{E}(K_{\mathcal{M}}\epsilon_{\mathcal{M}}) = \mathrm{E}(u_{\mathcal{M}}) \\ &= \mathrm{E}(\Gamma(f(\epsilon, K)))\end{aligned}$$

が暗号化制御則の定義 2 を満たすことがわかる． □

この定理より，演算が乗算のみで閉じる制御則，たとえば，比例制御や 1 次系の状態フィードバック則に関しては，RSA 暗号を用いた暗号文上の制御則を定めることができる．一方，RSA 暗号は，加法に関して準同型ではないため，乗算のみで完結しない一般の線形な制御則 f に対し，RSA 暗号では，$f_{\mathcal{E}}$ を実現できない．

3.4 比例制御の場合

比例制御器 $u[k] = K\epsilon[k]$ を用い，Fig. 3 (b) における処理の流れを説明する．ここで，$u[k]$, $\epsilon[k]$ は，それぞれ，時刻 k での制御入力，追従偏差で，K は，比例ゲインである．なお，本手法では，追従偏差 ϵ は，センサなどで暗号化処理の前に計算可能であるとする．

(i) 比例ゲイン K を暗号化する：$\mathrm{E}(\Gamma(K)) = \mathrm{E}(K_{\mathcal{M}})$.

(ii) センサなど (制御対象側) で追従偏差 $\epsilon[k]$ を観測し，暗号化する：$\mathrm{E}(\Gamma(\epsilon[k])) = \mathrm{E}(\epsilon_{\mathcal{M}}[k])$.

(iii) 暗号化した追従偏差 $\mathrm{E}(\epsilon_{\mathcal{M}}[k])$ を通信路を介して制御器側へ送信する．

(iv) 制御器において，暗号化された制御入力 $\mathrm{E}(u_{\mathcal{M}}[k])$ を定理 1 より計算する．

$$\begin{aligned}\mathrm{E}(u_{\mathcal{M}}[k]) &= f_{\mathcal{E}}(\mathrm{E}(\epsilon_{\mathcal{M}}[k]), \mathrm{E}(K_{\mathcal{M}})) \\ &= \mathrm{E}(K_{\mathcal{M}})\mathrm{E}(\epsilon_{\mathcal{M}}[k]) \mod n\end{aligned}$$

(v) 制御器で求めた $\mathrm{E}(u_{\mathcal{M}}[k])$ を通信路を介して制御対象側へ送信する．

(vi) 制御対象側で秘密鍵を用い，制御入力を復号して駆動させる：$u[k] = \Gamma^{-1}(\mathrm{D}(\mathrm{E}(u_{\mathcal{M}}[k])))$.

以上より，通信路および制御器において，平文情報に対応する制御入力 u または $u_{\mathcal{M}}$ が存在せず，すべて暗号化された信号 $\mathrm{E}(u_{\mathcal{M}})$ で制御入力が決まる．このように，制御入力の決定過程 (制御則の演算過程) をすべて秘匿化するところが，本提案法の新規性である．

4. 数 値 例

定理 1 および暗号化制御系を検証するために，数値シミュレーションを行なう．パラメータおよび鍵は，2.3 節のものを用いた．

4.1 制御系

制御対象は，連続時間線形システム

$$\begin{aligned}\dot{x}(t) &= \begin{bmatrix}0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & -3 & -5\end{bmatrix} x(t) + \begin{bmatrix}0 \\ 0 \\ 1\end{bmatrix} u(t) \\ y(t) &= \begin{bmatrix}1 & 0 & 0\end{bmatrix} x(t)\end{aligned}$$

をサンプリング周期 10 ms で離散化して得られる離散時間線形系を対象とする．ここで，$x \in \mathbb{R}^3$ は，制御対象の状態変数，$y \in \mathbb{R}$ は，出力，$u \in \mathbb{R}$ は，制御入力である．また，制御則は，$K = 0.83$ の比例制御器 $u[k] = K\epsilon[k] = 0.83(r[k] - y[k])$ を用いる．ここで，$r[k]$ は，目標値である．K が実数値であるため，本数値例では，実数値を $a_2 = 100$ 倍して整数値へ変

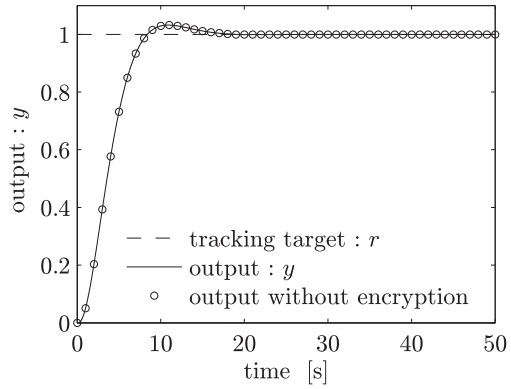

Fig. 4　Comparison of output responses

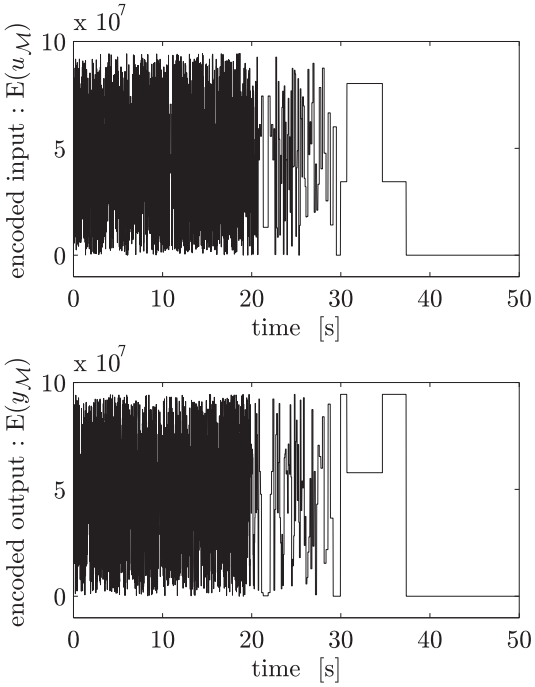

Fig. 5　Time response of encoded signals

換し，復号後に制御入力を a_2^{-1} 倍する．したがって，2.3 節で生成した鍵を用いるとき，比例ゲインは

$$\mathrm{E}(K_{\mathcal{M}}) = 83^{587} \mod 94399927 = 60036769$$

のように暗号化される．同様に，追従偏差 ϵ を暗号化する際には，a_2 に関しては 2^{16} を用いた．

4.2　応答の比較

Fig. 4 に $r[k] \equiv 1$ に対する制御対象の応答を示す．RSA 暗号の準同型性により，制御対象の応答 (実線) は，暗号化を行なわない場合の応答 (○) と一致する．

一方，制御器内部で処理される信号 $\mathrm{E}(\epsilon_{\mathcal{M}})$, $\mathrm{E}(u_{\mathcal{M}})$ の時系列は，**Fig. 5** に示すように暗号化されている．ただし，2.2 節であげた暗号文の一意性および原点が不変であるという RSA 暗号の特性により，応答が平衡点に近づくにつれ，暗号文の複雑性は，損なわれ，最終的に一定値へ収束してしまう．この結果は，RSA 暗号を用いて追従制御を行なう際，暗号化信号から制御系の運転状況が露呈する可能性を示唆している．原点での複雑性を考慮した暗号化方式の検討は今後の課題とする．

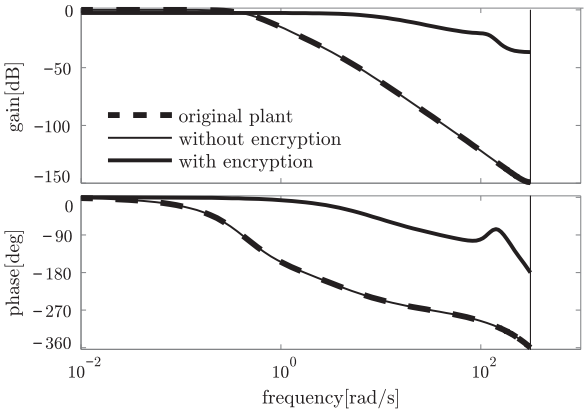

Fig. 6　System identification result with/without employing proposed method

4.3　秘匿性の確認

暗号化制御則の効果を確認する．ここでは，制御系の運転妨害や設計情報の奪取を狙った攻撃者が，制御器への侵入を果たし，制御系の入出力情報から上記閉ループ系の動特性を同定する状況を想定する．ただし，攻撃者は，閉ループ系の次数を知っており，暗号化後の入出力信号を平文の入出力信号と勘違いし，部分空間法による同定を行なうものとする．**Fig. 6** に，システム同定の結果を示す．同図において，太い破線は，元の閉ループ系の Bode 線図，細い実線は，制御器内部で扱われている信号が暗号化されていない場合の同定結果，太い実線は，暗号化制御則を用いた場合の同定結果である．この結果から，暗号化制御則の導入により，制御系の動特性を含め，情報を秘匿できていることがわかる．

5.　おわりに

本稿では，準同型暗号である RSA 暗号をネットワーク制御系のセキュリティ強化に応用し，制御器内部の演算を暗号化したまま実行する暗号化制御則の構成法を提案した．数値例では，比例制御によるフィードバック制御の実装方法を示し，暗号化制御系の応答と制御器内部の暗号化のようすを図示した．

一方で，提案法は，ある平文に対する暗号文が一意に定まるため，追従制御などでは，制御の状況 (過渡や定常の違い) が推測される可能性があるなどの問題点が明らかとなった．今後は，制御工学との親和性が高い暗号方式を新たに開発する必要がある．

参　考　文　献

1）A. Valenzano: Industrial cybersecurity, *IEEE Industrial Electronics Magazine*, **8**-2, 6/17 (2014)
2）新　誠一：社会インフラへのサイバー攻撃に対する課題と取組み，情報処理，**55**-7, 640/646 (2014)
3）Y. Mo, T.H.-H. Kim, K. Brancik, D. Dickinson, H. Lee,

A. Perrig and B. Sinopoli: Cyber-physical security of a smart grid infrastructure, *Proceedings of the IEEE*, **100**-1, 195/209 (2012)
4) O. Vukovic, K.C. Sou, G. Dan and H. Sandberg: Network-aware mitigation of data integrity attacks on power system state estimation, *IEEE Trans. Selected Areas in Communications*, **30**-6, 1108/1118 (2012)
5) T. Morita, S. Yogo, M. Koike, T. Hamaguchi, S. Jung, I. Koshijima and Y. Hashimoto: Detection of cyber-attacks with zone dividing and PCA, *Procedia Computer Science*, **22**, 727/736 (2013)
6) H. Sandberg: Cyberphysical security in networked control systems: An introduction to the issue, *IEEE Control Systems Magazine*, **35**-1, 20/23 (2015)
7) 伯田，内山，大和田，桶屋，鍛，萱島，吉田，渡辺：制御用コントローラ向け暗号通信機能の実現に向けて，計測と制御，**53**-10, 936/942 (2014)
8) 木内　舞：監視制御システムにおけるセキュリティ対策，Technical report, R07010, 電力中央研究所 (2008)
9) Z. Pang, G. Zheng, G. Liu and C. Luo: Secure transmission mechanism for networked control systems under deception attacks, *Proceedings of the 2011 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems*, 27/32 (2011)
10) 藤田，小木曽：ElGamal 暗号を用いた制御器の暗号化，計測自動制御学会論文集，**51**-9, 661/666 (2015)
11) R.L. Rivest, A. Shamir and L. Adleman: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystem*, 120/126, ACM (1978)
12) 森山，西巻，岡本：公開鍵暗号の数理，共立出版 (2011)
13) R.L. Rivest, L. Adleman and M.L. Dertouzos: On data banks and privacy homomorphism, *Foundations of Secure Computation*, Academia Press (1978)

［著　者　紹　介］

藤　田　貴　大（学生会員）

2011 年神戸市立工業高等専門学校電気電子工学専攻卒．2015 年奈良先端科学技術大学院大学情報科学研究科博士前期課程修了．同年横河電子機器（株）に入社，現在に至る．

澤　田　賢　治（正会員）

2009 年大阪大学大学院工学研究科機械工学専攻博士後期課程修了．同年電気通信大学システム工学科助教，2010 年同大学改組により知能機械工学科助教となり現在に至る．博士（工学）．飽和や量子化を有する制御系安定論，制御系セキュリティの研究に従事．システム制御情報学会，電気学会，IEEE の会員．

小木曽　公　尚（正会員）

2004 年大阪大学大学院工学研究科電子制御機械工学専攻博士後期課程修了．同年奈良先端科学技術大学院大学情報科学研究科 21 世紀 COE 研究員．2005 年同大学院助手，助教，2014 年電気通信大学大学院情報理工学研究科知能機械工学専攻准教授，現在に至る．2010～2011 年ジョージア工科大学客員研究員．拘束システムやハイブリッドシステムの解析と制御，ゲーム理論とその工学応用，制御セキュリティに関する研究に従事．博士 (工学)．システム制御情報学会，日本機械学会，IEEE の会員．

新　　誠　一（正会員）

1980 年東京大学大学院工学系研究科修士課程修了．同年，同大学工学部計数工学科助手．87 年工学博士（東京大学）．同大学講師を経て，88 年筑波大学電子・情報工学系助教授．92 年東京大学工学部助教授．2001 年，同大学情報理工学系研究科助教授．2006 年電気通信大学教授．同年，計測制御エンジニア．91，93，98 年計測自動制御学会論文賞，92 年同賞武田賞受賞．2006 年同技術賞受賞．計測自動制御学会元会長．制御理論を中心に広く工学全体に興味をもつ．（財）製造科学技術センター評議員．2012 年より制御システムセキュリティセンター理事長．