[計測自動制御学会論文集
Vol.51, No.9, 661/666（2015）]

ElGamal暗号を用いた制御器の暗号化

藤　田　貴　大*・小木曽　公　尚**

Encryption of Controllers Using ElGamal Cryptosystem

Takahiro Fujita* and Kiminao Kogiso**

This study proposes how to encrypt controllers using ElGamal encryption system. Based on a homomorphism of the ElGamal encryption, the proposed method enables to conceal not only signals over communication links in the control systems, but also parameters of controllers used in calculating a control input. A numerical example confirms that the proposed method correctly works for the cyber-security enhancement.

Key Words: ElGamal encryption system, homomorphic encryption, 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社会基盤設備，化学プラントなどの大規模工場において，制御系のネットワーク化が進んでいる．このようなネットワーク化された制御系では，系内の各種デバイスが相互接続されるため，通信路を介した遠隔地からの監視や制御，制御系内の情報収集とその利用，そして，制御の高度化・高性能化が可能となるなど，多大な恩恵がもたらされる．

その一方で，ネットワーク化によるアクセス性の向上と規格の共通化に伴い，サイバー攻撃の脅威が増加している[1)]．重要インフラの監視制御系への攻撃は，1990年代から顕在化し，2010年にはイランの核関連施設がウィルス (Stuxnet) に感染するなど，サイバー攻撃による損害が重大化している．そのため，産業界や情報セキュリティ分野のみならず，制御工学分野においても活発な議論が行なわれている[2)]．ネットワーク化制御系に対するサイバー攻撃の例として，制御系内の情報の盗聴が挙げられる．これは，オペレータの与える指令値，制御対象の入出力などの信号や，制御器の設計パラメータを盗聴することにより，製品の生産情報，制御器の設計ノウハウ，制御系の特性などを奪取する行為である[3)]．また，攻撃者が制御系の運転妨害を目的としたとき，制御系に関する情報を盗聴されると，効果的な妨害が可能になる．たとえば，制御系内の信号，制御器および制御対象の特性を攻撃者が把握している場合，より発覚しにくく，かつ，甚大な損害を与えることができる[4)]．したがって，制御系の盗聴対策は，情報保護の観点だけでなく，運転妨害対策としても重要である．

従来技術による盗聴対策としては，暗号理論が古くから応用されている．すでに各制御機器メーカーが，デバイス間の通信仕様として整備を進めており，主に処理時間や計算コストといった，実装性に関する議論が盛んである[5),6)]．また，文献7)では，デバイス間の通信路中の信号を暗号化することが，運転妨害の対策になることが示されている．しかしながら，これらの先行研究における暗号の利用形態では，通信路においてのみ暗号化を行なうため，攻撃者が制御装置の認証を突破し，不正アクセスを達成した場合には，信号や制御系情報だけでなく，暗号文復号用の鍵 (秘密鍵) も盗まれる可能性がある．

著者らは，公開鍵暗号方式のRSA暗号が有する準同型性を用いることで，制御器内部で取り扱われる各種信号やパラメータを暗号化し，信号とパラメータを秘匿したまま，暗号化された制御入力を直接計算する，暗号化制御則を提案した[8)]．また，この暗号化制御則は，暗号文復号用の秘密鍵を用いない演算方法であるため，制御器内部に秘密鍵を実装する必要がない．よって，暗号化制御則を用いることで，攻撃者が制御器へ侵入を果たした場合でも，制御系の情報を保護することができる．しかし，RSA暗号に基づく暗号化制御則では，運転状態を推察される可能性があった．さらに，RSA暗号に不確定性を付与する方法としてパディング[9),10)]が知られているが，準同型性が失われるため，暗号化制御則への適用は，困難である．

そこで本稿では，異なる暗号方式として，ElGamal暗号を用い，制御系の運転状態の推定が困難な暗号化制御則の実現

* 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 26, 2015）
（Revised July 6, 2015）

法を提案する．ElGamal 暗号は，離散対数問題の求解に係る計算の複雑さに着目した公開鍵暗号方式であり，さらに，乱数を用いた暗号化方式であるため，定数の秘密鍵に基づく RSA 暗号方式より安全で，実装が容易であることが知られている [11]．最後に，数値例による検証結果を示す．

2. ElGamal 暗号

ElGamal 暗号 [12]は，1984 年に ElGamal により提案された公開鍵暗号方式である．本章では，この暗号方式のアルゴリズムと準同型性について説明する．以下，本稿で使用する数学的記法を列挙する．$\mathbb{R}$, $\mathbb{Z}$ は，それぞれ実数と整数の全体を表わす．$\mathbb{Z}$ の部分集合として，$\mathbb{Z}^+$ は，非負整数の全体を，$\mathbb{Z}_n$ は，自然数 n を法とした剰余系 $\mathbb{Z}_n = \{0,\ 1,\ \cdots,n-1\}$, $\mathbb{Z}_n^\times$ は，$\mathbb{Z}_n$ の元のうち，n と互いに素なものの集合である．$\mathcal{M}$ は，平文の全体，$\mathcal{C}$ は，暗号文の全体をそれぞれ表わす．

2.1 ElGamal 暗号のアルゴリズム

ElGamal 暗号を含む，任意の公開鍵暗号方式 $\mathcal{E}$ は，鍵生成 (Gen)，暗号化 (Enc)，復号 (Dec) の三つのアルゴリズムにより定義され，$\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ と記述される．鍵生成は，暗号の強度を指定するセキュリティパラメータ k に従い，暗号化および復号に用いる公開鍵 k_p と秘密鍵 k_s を生成する．このとき，$\mathcal{E}$ により暗号化可能な数値の集合，すなわち平文空間 $\mathcal{M}$ が決定される．暗号化は，公開鍵 k_p を用いて平文空間 $\mathcal{M}$ の元を暗号化し，復号は，逆に暗号文空間 $\mathcal{C}$ の元を平文へと変換する．

ElGamal 暗号のアルゴリズム $\mathcal{E}$ を以下に記述する．

- $\mathsf{Gen}(1^k) = (k_p, k_s)$ は，入力された k bit のビット列を元に，公開鍵 $k_p = (\mathbb{G}, g, h, q)$ と秘密鍵 $k_s = s$ を生成する．ここで，q は，k bit の素数で，$p = 2q+1$ も素数となるものを選ぶ (Sophie Germain 素数)．$g \in [2,\ p-2]$ は，$g^q \mod p = 1$ を満足する整数値，s は，$\mathbb{Z}_q$ から無作為に抽出される乱数，そして，$h = g^s \mod p$ である．$\mathbb{G}$ は，集合 $\mathbb{G} = \left\{ g^i \mod p,\ \forall i \in \mathbb{Z}_q \right\} \in \mathbb{Z}_p^\times$ であり，生成元を g とする位数 q の巡回群 $\mathbb{G} = \langle g \rangle$ を成す．また，平文空間は $\mathcal{M} = \mathbb{G}$ である．
- $\mathsf{Enc}(k_p, m) : \mathcal{M} \to \mathcal{C}$ は，公開鍵 k_p を用い，平文 $m \in \mathcal{M}$ を暗号化する．

$$C = (c_1, c_2) = \mathsf{Enc}(k_p, m) = (g^r \mod p, mh^r \mod p) \quad (1)$$

ただし，r は，暗号化のたびに $\mathbb{Z}_q$ から一様に抽出される乱数である．なお，比較的計算資源の乏しい制御システムでは，擬似乱数の生成にある種の制約が生じる可能性がある．本稿では，その生成器に関する議論を今後の課題とし，理想的な乱数が暗号化部で生成できるものとする．

- $\mathsf{Dec}(k_s, C) : \mathcal{C} \to \mathcal{M}$ は，公開鍵 k_p および秘密鍵 k_s を用い，暗号文 $C \in \mathcal{C}$ を復号する．

$$m' = \mathsf{Dec}(k_s, C) = c_2 \left(c_1^s\right)^{-1} \mod p$$

このとき，暗号文 C が(1)式により生成されたものであれば，

$$m' = \mathsf{Dec}(k_s, C) = c_2 \left(c_1^s\right)^{-1} \mod p = mh^r (g^{rs})^{-1} = mg^{rs}g^{-rs} = m$$

が成立し，正しく復号される．

これらの演算に起因し，ElGamal 暗号は，二つの特徴をもつ．一つ目は，暗号化アルゴリズム Enc は，乱数 r の影響により不確定である．すなわち

$$m_1 = m_2 \not\Rightarrow \mathsf{Enc}(k_p, m_1) = \mathsf{Enc}(k_p, m_2)$$

が成立する．これは，平文が同一であれば暗号文も必ず一致する RSA 暗号とは異なる性質である．二つ目は，平文空間 $\mathcal{M} = \mathbb{G}$ は $\mathbb{Z}_p^\times$ の真部分群である．たとえば $\mathcal{M} = \{1, 2, 5, 6, 8, \cdots\}$ のように，間欠値が存在し，$\mathbb{Z}_p^\times$ のすべての元を網羅しない．

2.2 ElGamal 暗号の準同型性

ElGamal 暗号は，準同型暗号の一つであり，その定義を示す．

定義 1. [13] 公開鍵暗号方式 $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が以下の 3 条件を満足するとき，$\mathcal{E}$ は準同型暗号である．

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

（2） 平文空間の任意の元は暗号文空間に写像される．すなわち $\mathsf{Enc}(k_p, m) \in \mathcal{C},\ \forall m \in \mathcal{M}$ が成立する．

（3） 任意の二つの平文 $m_1, m_2 \in \mathcal{M}$ に対し，その暗号文を C_1，C_2 とするとき，次式が成立する．

$$\mathsf{Enc}(k_p, m_1 \bullet m_2) = C_1 * C_2 \quad (2)$$

この定義より，準同型暗号においては，平文同士の演算結果に対応した暗号文 $\mathsf{Enc}(m_1 \bullet m_2)$ を，復号を行なうことなくおのおのの平文に対応した暗号文 C_1，C_2 から計算できる．この特性から，準同型暗号は電子投票システムや生体認証への応用が期待されており，加算や乗算，ビットの和などに対する準同型な暗号方式が開発されている．

ElGamal 暗号は，乗算に関して準同型であり，平文 $m_1, m_2 \in \mathcal{M}$ と，それに対応した暗号文 $C_1 = (c_{11}, c_{12}), C_2 = (c_{21}, c_{22})$ について，下式が成立する．

$$\mathsf{Enc}(k_p, m_1 m_2) = C_1 \times_e C_2 \mod p \quad (3)$$

ここで，$\times_e$ は Hadamard 積を表わし，$C_1 \times_e C_2 \mod p = (c_{11}c_{12} \mod p, c_{21}c_{22} \mod p)$ である．すなわち，(2)において，平文同士の演算 $\bullet$ が乗算，暗号文同士の演算 $*$ が p を法とする Hadamard 積に対応しており，ElGamal 暗号では，平文同士の乗算を復号を行なわずに暗号文から計算できる．

注意 1. ElGama 暗号は，組み込み機器などの計算機資源の乏しい環境で用いる場合には，楕円曲線を用いたアルゴリズムで実装されること (楕円曲線 ElGamal 暗号) が一般的である．本稿では，暗号化制御則に着目するため，実装を考慮した手法については今後の課題とする．

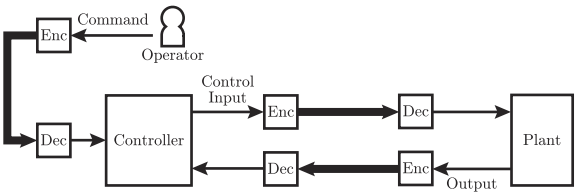

Fig. 1 Conventional cryptography-based protection for the cyber-security of the networked control systems

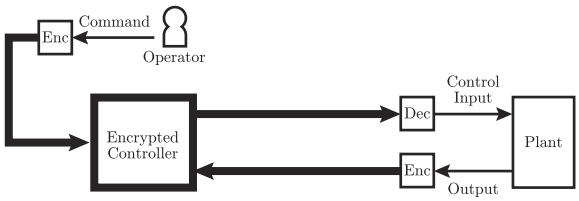

Fig. 2 Proposed cryptography-based protection for the cyber-security of the networked control systems, which is the encryption of the controller having no decryption processes inside

3. 暗号化制御則

本章では，暗号化制御則の概念を紹介し，ElGamal 暗号を用いた実現法を述べる．

3.1 平文空間への変換

まず準備として，ElGamal 暗号を制御系へ適用するための注意点を述べる．一般に，制御系において扱われる変数やパラメータは，実数であるが，前章のとおり，ElGamal 暗号により暗号化できるのは，平文空間 $\mathcal{M} = \mathbb{G} \subset \mathbb{Z}_p^{\times} \subset \mathbb{Z}^+$ の元のみである．そこで，この変換 $\mathbb{R} \to \mathbb{G}$ を考える．

実数から非負実数への変換 $\mathbb{R} \to \mathbb{R}^+$ を考える．ElGamal 暗号のアルゴリズムでは，すべての演算が p を法として行なわれる．したがって，ある実数値 $w \in \mathbb{R}$ の加法逆元を，$-w \to p - w$ とすることで，$w - w \mod p = w + (p - w) \mod p = 0$ と正しい結果が得られる．このため，非負値への変換は，下式により実現できる．

$$w^+ = \begin{cases} w & (w \geq 0) \\ p + w & (w < 0) \end{cases}, \ w \in \mathbb{R}, \ w^+ \in \mathbb{R}^+$$

つぎに，実数から平文空間への変換 $\mathbb{R} \to \mathcal{M}$ として，固定小数点法を元にした，次式の変換を考える．

$$\overline{m} = \lceil \gamma m \rfloor_{\mathcal{M}}, m \in \mathbb{R}, \ \overline{m} \in \mathcal{M}$$

ここで，$\gamma \in \mathbb{Z}$ は，適当な変換ゲイン，$\lceil \cdot \rfloor_{\mathcal{M}}$ は，平文空間 $\mathcal{M}$ 中の最近傍の元への丸めを表わす．このとき，通常の固定小数点法と同様，変換ゲイン γ を十分大きく取ることで，高精度な変換が可能である．

本稿では，これら二つの変換をあわせ，関数 $\Gamma_{\mathcal{M}} : \mathbb{R} \to \mathcal{M}$ で表わす．

$$\Gamma_{\mathcal{M}}(m, \gamma) = \left\lceil (\gamma m)^+ \right\rfloor_{\mathcal{M}} \tag{4}$$

3.2 暗号化制御則の概念と定義

制御系セキュリティにおける暗号理論の利用は，**Fig. 1** に示すように，各制御機器を接続する通信路を暗号化し，攻撃者による通信路の盗聴を防ぐ方法が一般的である．一方，著者らは，制御器に対する不正アクセス対策として，暗号化制御則の概念を提案した[8]．暗号化制御則とは，**Fig. 2** に示すように，暗号化された情報のみを用いて制御入力を決定できる制御則であり，攻撃者が制御器内部の情報を盗聴しても，暗号により保護が行なえるという特徴がある．

定義 2. 対象とするネットワーク化制御系に，パラメータ K と制御器への入力信号 $y(t)$ により制御入力 $u(t)$ を決定する離散時間制御則

$$u(t) = f(K, y(t)), \ \forall t \in \mathbb{Z}$$

が実装されており，ネットワーク上の通信路が暗号方式 $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ により暗号化されているとする．このとき，ある関数 $f_{\mathcal{E}}$ が，すべての時刻 $t \in \mathbb{Z}$ に対して，

$$f_{\mathcal{E}}(\mathsf{Enc}(k_p, \overline{K}), \mathsf{Enc}(k_p, \overline{y}(t))) = \mathsf{Enc}\left(\overline{f}(K, y(t))\right) \tag{5}$$

を満足し，かつ秘密鍵 k_s を使用しないとき，$f_{\mathcal{E}}$ を f に対する暗号化制御則と呼ぶ．

この定義より，暗号化制御則とは，暗号化されたパラメータおよび入力信号 $\mathsf{Enc}(k_p, K), \mathsf{Enc}(k_p, y(t))$ を用いて，復号を行なわずに暗号化された制御入力 $\mathsf{Enc}(k_p, u)$ を計算する関数である．したがって，暗号化制御則の導入は，制御器 (制御装置) への不正侵入に対する安全性の向上に貢献できる．

3.3 ElGamal 暗号に基づく暗号化制御則の実現

本節では，ElGamal 暗号に基づいて，運転状態を秘匿しつつ制御器の暗号化を達成する暗号化制御則の実現法を提案する．

まず，制御則 f が比例制御，つまり，パラメータである比例ゲイン K_P および制御器への入力 y を用いて，制御入力が

$$u(t) = f(K_P, y(t)) = K_P y(t) \tag{6}$$

と決定されるとする．このとき，ElGamal 暗号の準同型性を利用することで，暗号化制御則の定義(5)を満足する $f_{\mathcal{E}}$ を実現できる．

定理 1. 制御則 f が(6)式に示す比例制御であるとする．このとき，f に対する暗号化制御則は，つぎのとおりである．

$$\begin{aligned} &f_{\mathcal{E}}\left(\mathsf{Enc}(k_p, \overline{K}_P), \mathsf{Enc}(k_p, \overline{y}(t))\right) \\ &= \mathsf{Enc}(k_p, \overline{K}_P) \times_e \mathsf{Enc}(k_p, \overline{y}(t)) \mod p \end{aligned} \tag{7}$$

証明. ElGamal 暗号の準同型性(3)より，(7)式の右辺は

$$\begin{aligned} &\mathsf{Enc}\left(k_p, \overline{K}_P\right) \times_e \mathsf{Enc}\left(k_p, \overline{y}(t)\right) \mod p \\ &= \mathsf{Enc}\left(k_p, \overline{K}_P \overline{y}(t)\right) \\ &= \mathsf{Enc}\left(k_p, \overline{f}(K_P, y(t))\right) \end{aligned}$$

であり，暗号化制御則の定義式(5)を満足する． □

つぎに，制御則が一般的な線形制御の場合を考える．

$$\begin{cases} x_c(t+1) &= A_c x_c(t) + B_c v(t) \\ u(t) &= C_c x_c(t) + D_c v(t) \end{cases}$$

ここで，x_c は，制御器の状態変数，v は，制御器への入力である．行列 A_c, B_c, C_c, D_c を制御器のパラメータ，$x_c(t), v(t)$ を入力信号とすることで，線形制御則 f は，

$$\begin{bmatrix} x_c(t+1) \\ u(t) \end{bmatrix} = \begin{bmatrix} A_c & B_c \\ C_c & D_c \end{bmatrix} \begin{bmatrix} x_c(t) \\ v(t) \end{bmatrix} = \Phi\xi = f(\Phi, \xi)$$

と記述できる．ここで，この制御則 f では，$\Phi\xi$ の演算には和と積の双方が現れることに注意する．乗法に関してのみ準同型な ElGamal 暗号を適用しても暗号化制御則は実現できないため，f を乗算のみで実行可能な乗算部分 $f^{\times}$，および，加算のみで実行できる加算部分 f^{+} とに分割して考える．

$$f^{\times}(\Phi, \xi) = [\Phi_1\xi_1 \ \Phi_2\xi_2 \cdots \Phi_L\xi_L] = \Psi$$
$$f^{+}(\Psi) = \sum_{i=1}^{L} \Psi_i$$

ここで，$f = f^{+} \circ f^{\times}$ を満たし，行列 Φ，Ψ の添字は，それぞれの列ベクトル，ベクトル ξ の添字は，要素を表わす．$f^{\times}$ は，制御器のパラメータ Φ を必要とし，また，ElGamal 暗号の乗法準同型性を利用できる．一方，f^{+} は，入力された行列の列ベクトルを加算するだけで，制御器のパラメータを必要としないが，乗法準同型性を利用できない．したがって，本稿では，$f^{\times}$ のみを制御器において実行し，f^{+} は，復号後にて制御対象側で実行する．このとき，ElGamal 暗号の Dec アルゴリズムは，$\mathsf{Dec}^{+}(k_s, \overline{\Psi}) := f^{+} \circ \mathsf{Dec}(k_s, \overline{\Psi})$ と修正され，線形制御則の乗算部分 $f^{\times}$ に対する暗号化制御則は，つぎのように実現される．

定理 2. 線形制御則の乗算部分が次式で与えられるとする．

$$f^{\times}(\Phi, \xi) = [\Phi_1\xi_1 \ \Phi_2\xi_2 \cdots \Phi_L\xi_L]$$

このとき，$f^{\times}$ に対する暗号化制御則は，

$$f_{\mathcal{E}}^{\times}\left(\mathsf{Enc}\left(k_p, \overline{\Phi}\right), \mathsf{Enc}\left(k_p, \overline{\xi}\right)\right) = \Psi_{\mathcal{E}}$$
$$\Psi_{\mathcal{E}ij} = \mathsf{Enc}\left(k_p, \overline{\Phi}_{ij}\right) \times_e \mathsf{Enc}\left(k_p, \overline{\xi}_j\right) \mod p \quad (8)$$

である．ただし，$\Psi_{\mathcal{E}ij}$ は，行列 $\Psi_{\mathcal{E}}$ の i 行 j 列要素を表わす．

証明. ElGamal 暗号の準同型性(3)より，(8)式において，

$$\begin{aligned} \Psi_{\mathcal{E}ij} &= \mathsf{Enc}\left(k_p, \overline{\Phi}_{ij}\right) \times_e \mathsf{Enc}\left(k_p, \overline{\xi}_j\right) \mod p \\ &= \mathsf{Enc}\left(k_p, \overline{\Phi}_{ij}\overline{\xi}_j\right) = \mathsf{Enc}\left(k_p, \overline{\Psi}_{ij}\right) \end{aligned}$$

が成立する．よって，

$$\begin{aligned} f_{\mathcal{E}}^{\times}\left(\mathsf{Enc}\left(k_p, \overline{\Phi}\right), \mathsf{Enc}\left(k_p, \overline{\xi}\right)\right) &= \Psi_{\mathcal{E}} \\ &= \mathsf{Enc}\left(k_p, \overline{f}^{\times}(\Phi, \xi)\right) \end{aligned}$$

より，暗号化制御則の定義(2)を満足する． □

同様に，多項式型の非線形制御則

$$\begin{bmatrix} x_c(t+1) \\ u(t) \end{bmatrix} = f(K, x_c(t), v(t))$$
$$f(K, x_c(t), v(t)) = \sum_{l=1}^{L} \left(K_l \prod_{i=1}^{I_a} x_{ci}^{a_{li}}(t) \prod_{i=1}^{I_b} v_j^{b_{lj}}(t) \right)$$

に関しても，乗算部分

$$f^{\times}(K, x_c(t), v(t)) = [\psi_1 \ \psi_2 \ \cdots \ \psi_L] = \Psi$$
$$\psi_l = K_l \prod_{i=1}^{I_a} x_{ci}^{a_{li}}(t) \prod_{i=1}^{I_b} v_j^{b_{lj}}(t) \quad (9)$$

を定義することにより，$f^{\times}$ のみを対象とした暗号化制御則を実現することができる．

系 1. 多項式型の非線形制御則の乗算部分が(9)で与えられるとする．このとき，$f^{\times}$ に対応する暗号化制御則は，

$$f_{\mathcal{E}}^{\times}\left(\mathsf{Enc}(k_p, \overline{K}), \mathsf{Enc}\left(k_p, \overline{x}_c(t)\right), \mathsf{Enc}\left(k_p, \overline{v}(t)\right)\right) = \Psi_{\mathcal{E}}$$
$$\Psi_{\mathcal{E}jl} = \mathsf{Enc}\left(k_p, \overline{K}_{jl}\right) \times_e \prod_{i=1}^{I_a} \mathsf{Enc}\left(k_p, \overline{x}_{ci}^{a_{lj}}(t)\right) \times_e \prod_{i=1}^{I_b} \mathsf{Enc}\left(k_p, \overline{v}_i^{b_{lj}}(t)\right)$$

で実現できる．ただし，総乗およびべき乗記号は，便宜上，演算 $\times_e$ による平文の乗算を表わすものとする．

4. 数 値 例

提案法の暗号化制御則の効果を検証するため，数値シミュレーションを行なう．ここでは，Matlab 2014b を用い，モジュラ逆元の計算には拡張ユークリッドアルゴリズムを用いた．

4.1 制御系の設定

Fig. 3 に示すフィードバック系を考える．この系において，制御対象は，つぎの連続時間状態方程式を離散化周期 10 ms で離散化した系であるとし，

$$\begin{cases} \dot{x}_p(\tau) &= \begin{bmatrix} 0 & 2 \\ -2 & -3 \end{bmatrix} x_p(\tau) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u(\tau) \\ y(\tau) &= \begin{bmatrix} 1 & 0 \end{bmatrix} x_p(\tau) \end{cases}$$

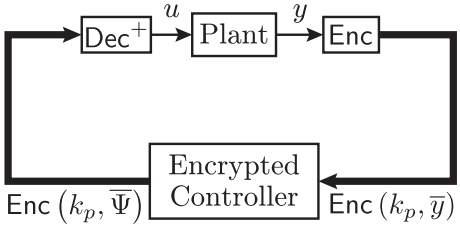

Fig. 3 A networked control system using the encrypted controller

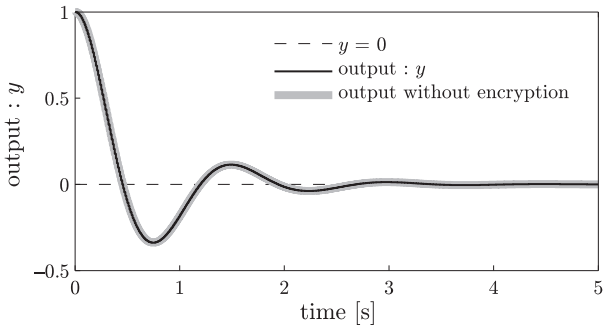

Fig. 4 Time-responses of the output $y(t)$ with and without the encrypted proportional controller

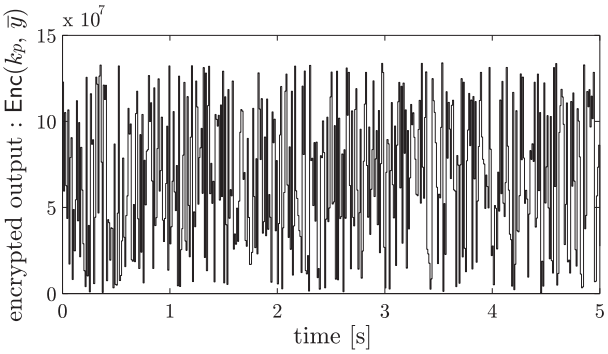

Fig. 5 A time-response of the scrambled output by the encrypted proportional controller

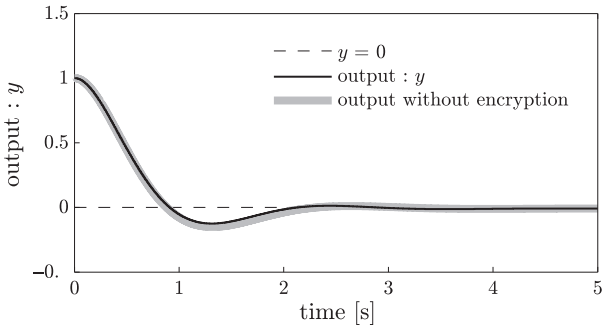

Fig. 6 Time-responses of the output $y(t)$ with and without the encrypted PID controller

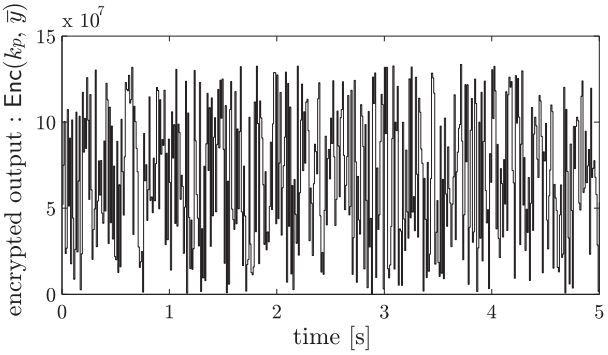

Fig. 7 A time-response of the scrambled output by the encrypted PID controller

制御器には，比例ゲインを $K_P = -8$ とした比例制御器，および，比例ゲイン $K_P = 2$，積分ゲイン $K_I = 0.1$，微分ゲイン $K_D = 0.01$ の連続時間 PID 制御器を同周期で離散化した

$$\begin{bmatrix} x_c(t+1) \\ u(t) \end{bmatrix} = \begin{bmatrix} 1 & 0.0063 & 0 \\ 0 & 0.3678 & 0.0063 \\ 10 & -99.9 & 3 \end{bmatrix} \begin{bmatrix} x_c(t) \\ -y(t) \end{bmatrix} = \Phi\xi$$

を用いる．

4.2 ElGamal 暗号の設定

本例題で用いた鍵は，つぎのとおりである．まず，Sophie Germain 素数 $q = 67108913$ を生成すると，$p = 2q + 1 = 134217827$ も素数となる．このとき，$g = 3$ とすることで，$g^q \mod p = 1$ が満足され，$\mathbb{G} = \langle g \rangle$ は，位数 q の巡回群を成す．したがって，秘密鍵の乱数 $k_s = s$ の任意性を残し，公開鍵 $k_p = (\mathbb{G}, 67108913, 3, g^s)$ が生成される．

4.3 比例制御

比例制御に関して，暗号化制御則の導入による結果を示す．比例ゲイン $K_P = 8$ は整数であるが，$8 \notin \mathcal{M}$ であるため，$\gamma = 100$ とし，(4)による変換を行なう．また，制御器への入力信号 y の変換には，$\gamma = 2^8$ を用いた．この設定のもと，得られる制御系の応答 y を **Fig. 4** に示す．細い実線が暗号化制御則を実装した系の応答，太い実線が暗号化しない場合の応答である．両者はよく一致している．一方，制御器内部で取り扱われる暗号化入力信号 $\mathsf{Enc}(k_p, \overline{y})$ は，**Fig. 5** に示すように暗号化されている．また，ElGamal 暗号の不確定性により，制御系が定常状態に達した後も暗号文は複雑さを保ち，運転状態の秘匿が行なえている．

4.4 PID 制御

同様の検証を PID 制御について行なう．制御器のパラメータの平文への変換は，$\gamma = 5 \times 10^3$，信号の変換は $\gamma = 2^{11}$ とした．この設定のもと，得られる制御系の応答 y を **Fig. 6** に示す．P 制御の場合と同じく，暗号化制御則を適用しても，制御性能はほぼ変化していない．また，制御器内部の暗号化された信号に関しても，**Fig. 7** に示すとおり，一見したところでは過渡状態と定常状態との特定は難しい．

4.5 秘匿性の確認

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の P 制御における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，部分空間法による同定を行なうものとする．**Fig. 8** に部分空間同定法の適用結果を示す．同図から，破線が真の閉ループ系の動特性，細い実線が暗号化則を用いない場合の同定結果，太い実線が提案した暗号化制御則を用いた場合の同定結果である．これらの結果から，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．

ほかにも，制御システムへの中間者攻撃やサイドチャネル攻撃 (タイミング攻撃や電力解析攻撃など) を想定することも重要であるが，これらの攻撃への対策法については今後の課題としたい．たとえば，サイドチャネル攻撃への対策は，文

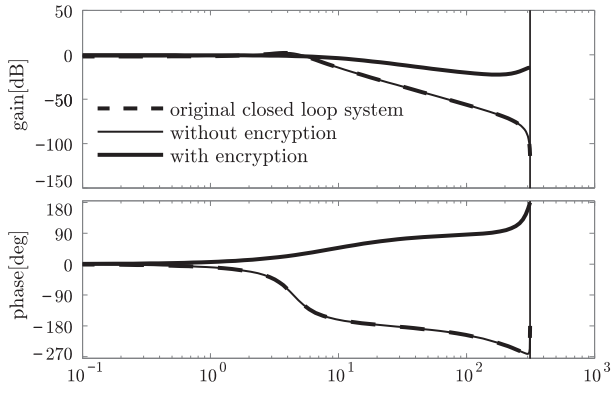

Fig. 8 Demonstration results of the subspace identification method (`n4sid` of Matlab) for the networked control system including the normal or encrypted controller

献 14), 15) を参照のこと.

5. おわりに

本稿では，ネットワーク化制御系のセキュリティ強化のため，ElGamal 暗号に基づく暗号化制御則の実現法を示した．数値例では，比例制御と PID 制御に関して，暗号化制御則の導入により，制御性能に大きな影響を与えることなく，制御器内部の情報を秘匿できることを示した．特に，ElGamal 暗号の不確定性から，過渡状態と定常状態との特定が困難になることを確認した．

今後の課題は，本提案法の実装可能性を，計算時間，計算資源の面から検討することである．また，モデル予測制御を始めとするほかの制御則に関しても，拡張可能であるかを検討する．

謝辞 本稿の査読プロセスにおきまして，査読者から非常に建設的かつ貴重なご意見，および，今後の研究に繋がる有益なアドバイスをいただくことができました．紙面を借りて，査読をご担当していただきました方々に感謝の意を申し上げたいと思います．どうもありがとうございました．

参考文献

1）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)
2）新 誠一：特集 制御システムセキュリティの現状と課題：[総論] コントローラ，それはネットワーク機器，計測と制御，**53**-10, 885/948 (2014)
3）情報処理振興事業協会：研究報告書 高信頼/高セキュリティ制御システムの研究，情報処理振興事業協会 (2000)
4）A. Teixeira, D. Perez, H. Sandberg and K.H. Johansson: Attack models and scenarios for networked control systems, *Proceedings of the 13th ACM International Conference on Hybrid systems: Computation and control*, 55/64 (2010)
5）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)
6）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)
7）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)
8）藤田，澤田，小木曽，新：RSA 暗号を用いたネットワーク制御系のセキュリティ強化，計測自動制御学会論文集，**51**-9, 655/660 (2015)
9）B. Mihir and R. Phillip: Optimal asymmetric encryption – how to encrypt with RSA, *Proceedings of EUROCRYPT 1994*, **950**, 92/111 (1995)
10）藤崎英一郎：暗号アルゴリズム評価報告書 RSA-OAEP，Technical report, 0006, 日本電信電話株式会社 (2001)
11）J. Katz and Y. Lindell: *Introduction to Modern Cryptography*, Second Edition, CRC Press Talyor & Francis Group (2015)
12）T. El Gamal: A public key cryptosystem and a signature scheme based on discrete logarithms, *Proceedings of CRYPTO '84*, **196**, 10/18 (1984)
13）森山，西巻，岡本：公開鍵暗号の数理，共立出版 (2011)
14）P. Kocher: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, *Proceedings of CRYPTO '96*, 104/113 (1996)
15）K. Itoh, T. Izu and M. Takenaka: Address-bit differential power analysis of cryptographic schemes OK-ECDH and OK-ECDSA, *Proceedings of Cryptographic Hardware and Embedded Systems*, 129/143 (2003)

[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．

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．