

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2016-90884
(P2016-90884A)

(43) 公開日 平成28年5月23日 (2016.5.23)

(51) Int.Cl. F I テーマコード (参考)
G09C 1/00 (2006.01) G09C 1/00 620Z 5J104

審査請求 未請求 請求項の数 9 O L (全 18 頁)

(21) 出願番号	特願2014-226964 (P2014-226964)	(71) 出願人	504133110 国立大学法人電気通信大学 東京都調布市調布ヶ丘一丁目5番地1
(22) 出願日	平成26年11月7日 (2014.11.7)	(74) 代理人	100121131 弁理士 西川 孝
		(74) 代理人	100082131 弁理士 稲本 義雄
		(72) 発明者	小木曾 公尚 東京都調布市調布ヶ丘一丁目5番地1 国立大学法人電気通信大学内
		(72) 発明者	藤田 貴大 東京都調布市調布ヶ丘一丁目5番地1 国立大学法人電気通信大学内
		Fターム(参考)	5J104 JA21 NA02 NA37

(54) 【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

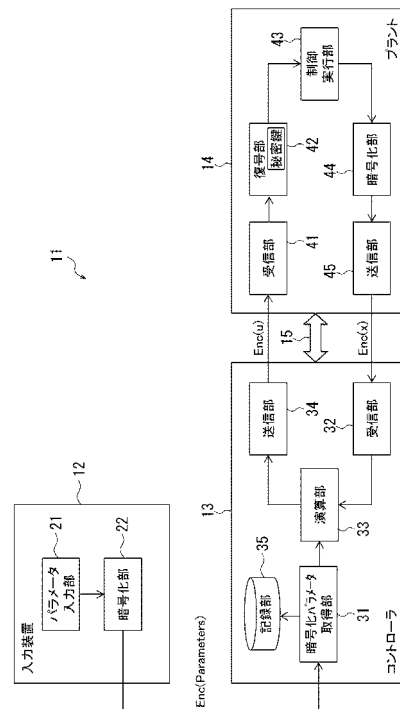
(57) 【要約】 (修正有)

【課題】 よりセキュリティ強化が図られた暗号化制御システムを提供する。

【解決手段】 暗号化制御システム11は、プラント14側で、制御実行部43における制御結果として出力される制御出力を暗号化して、暗号化制御出力を求める暗号化部44と、コントローラ13側で、暗号化制御出力を暗号化するのに使用した公開鍵と同一の公開鍵を使用してプラントの制御に用いられるパラメータが予め暗号化された暗号化パラメータと、制御系バスを介して受信される暗号化制御出力とを暗号化したまま用いて、プラントを制御するための制御入力に暗号化されている暗号化制御入力を算出する演算部33と、プラント14側で、制御系バスを介して受信される暗号化制御入力を、公開鍵に対応する秘密鍵を使用して復号し制御入力を取得する復号部42とを備える。

【選択図】 図1

図1



【特許請求の範囲】**【請求項 1】**

制御装置およびプラントが制御系バスを介して接続された暗号化制御システムにおいて

、
前記プラント側で、制御結果として出力される制御出力を暗号化して、暗号化制御出力を求める制御出力暗号化部と、

前記制御装置側で、前記制御出力暗号化部が前記暗号化制御出力を暗号化するのに使用した公開鍵と同一の公開鍵を使用して前記プラントの制御に用いられるパラメータが予め暗号化された暗号化パラメータと、前記制御系バスを介して取得される前記暗号化制御出力とを暗号化したまま用いて、前記プラントを制御するための制御入力に暗号化されている暗号化制御入力を算出する演算部と、

前記プラント側で、前記制御系バスを介して取得される前記暗号化制御入力を、前記公開鍵に対応する秘密鍵を使用して復号する復号部と

を備える暗号化制御システム。

【請求項 2】

オペレータによる操作に応じて前記パラメータが入力されるパラメータ入力部と、

前記パラメータ入力部に入力された前記パラメータを、前記公開鍵を使用して暗号化して、前記暗号化パラメータを求めるパラメータ暗号化部と

をさらに備える請求項 1 に記載の制御システム。

【請求項 3】

前記暗号化パラメータ、前記暗号化制御出力、および前記暗号化制御入力のうち、少なくともいずれか 1 つを記録する記録部

をさらに備える請求項 1 または 2 に記載の制御システム。

【請求項 4】

前記暗号化パラメータは、準同型性を持つ暗号により暗号化されたものである

請求項 1 乃至 3 のいずれかに記載の制御システム。

【請求項 5】

前記暗号化パラメータは、乗法に関して準同型性を持つ暗号により暗号化されたものであり、

前記演算部は、比例制御のゲインとして入力された前記パラメータが暗号化された前記暗号化パラメータを用いて、前記プラントに対して比例制御を実行するための演算を行う請求項 1 乃至 4 のいずれかに記載の制御システム。

【請求項 6】

前記暗号化パラメータは、乗法および加法に関して準同型性を持つ暗号により暗号化されたものであり、

前記演算部は、P I D (Proportional Integral Derivative) 制御の目標値として入力された前記パラメータが暗号化された前記暗号化パラメータを用いて、前記プラントに対して前記 P I D 制御を実行するための演算を行う

請求項 1 乃至 4 のいずれかに記載の制御システム。

【請求項 7】

前記演算部は、前記 P I D 制御において加算を行う対象となる一部分ごとに所定数に分割して乗算を行うことで、その一部分ごとの前記暗号化制御入力を算出し、

前記復号部は、一部分ごとの前記暗号化制御入力を復号して、加算を行う対象となる所定数の一部分ごとの制御入力を求め、

前記プラント側で、所定数の一部分ごとの前記制御入力を加算する処理を行って前記制御入力を求める加算処理部をさらに備える

請求項 6 に記載の制御システム。

【請求項 8】

制御装置およびプラントが制御系バスを介して接続された暗号化制御システムの暗号化制御方法において、

10

20

30

40

50

前記プラント側で、制御結果として出力される制御出力を暗号化して、暗号化制御出力を求め、

前記制御装置側で、前記暗号化制御出力を暗号化するのに使用した公開鍵と同一の公開鍵を使用して前記プラントの制御に用いられるパラメータが予め暗号化された暗号化パラメータと、前記制御系バスを介して取得される前記暗号化制御出力とを暗号化したまま用いて、前記プラントを制御するための制御入力に暗号化されている暗号化制御入力を算出し、

前記プラント側で、前記制御系バスを介して取得される前記暗号化制御入力を、前記公開鍵に対応する秘密鍵を使用して復号する

を含む暗号化制御方法。

10

【請求項 9】

制御装置およびプラントが制御系バスを介して接続された暗号化制御システムを制御するコンピュータに実行させるプログラムにおいて、

前記プラント側で、制御結果として出力される制御出力を暗号化して、暗号化制御出力を求め、

前記制御装置側で、前記暗号化制御出力を暗号化するのに使用した公開鍵と同一の公開鍵を使用して前記プラントの制御に用いられるパラメータが予め暗号化された暗号化パラメータと、前記制御系バスを介して取得される前記暗号化制御出力とを暗号化したまま用いて、前記プラントを制御するための制御入力に暗号化されている暗号化制御入力を算出し、

20

前記プラント側で、前記制御系バスを介して取得される前記暗号化制御入力を、前記公開鍵に対応する秘密鍵を使用して復号する

ステップを含む処理をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、暗号化制御システムおよび暗号化制御方法、並びにプログラムに関し、特に、よりセキュリティ強化を図ることができるようにした暗号化制御システムおよび暗号化制御方法、並びにプログラムに関する。

【背景技術】

30

【0002】

近年、電気やガス、水道などの生活を支えるインフラを制御する制御システム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やICT (Information and Communication Technology) の進化により、制御システムに多大な恩恵が与えられる一方、サイバー攻撃という新たな脅威を呼び込むことが懸念されている。実際に、発電所や工場などのプラント動作を監視または制御する制御システムに対するサイバー攻撃が出現しており、社会的に重要な問題として注目されている。

【0003】

そのため、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が急務とされており、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などに関する研究が進められている。

40

【0004】

例えば、特許文献 1 には、ネットワークを介して PLC (Programmable Logic Controller) に暗号化された制御プログラムを送信し、その制御プログラムを PLC が復号して設備機器を制御する制御システムが開示されている。

【0005】

また、特許文献 2 には、産業用コントローラが認証済みネットワークを介してのみ命令を受信することによって、特許文献 3 には、セキュリティサーバへのセキュリティ通知を集約することによって、セキュリティ性を高めた産業用制御システムが開示されている。

【先行技術文献】

50

【特許文献】

【0006】

【特許文献1】特開2008-67162号公報

【特許文献2】特開2013-232190号公報

【特許文献3】特開2013-232191号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

ところで、従来の産業ネットワークにおいて、暗号化された情報を、コントローラおよびプラントの間を接続する制御系バスを介して送受信する構成を採用することによって、セキュリティ性を高めることが行われている。このような構成では、コントローラ側で制御入力を決定する際に一旦復号を行うため、コントローラおよびプラントの双方が秘密鍵を保持する必要があった。

10

【0008】

このため、例えば、コントローラがハッキングされて秘密鍵が漏洩した場合には、コントローラおよびプラントの間で送受信される情報が漏洩することが懸念されており、セキュリティを強化することが求められている。

【0009】

本開示は、このような状況に鑑みてなされたものであり、よりセキュリティ強化を図ることができるようにするものである。

20

【課題を解決するための手段】

【0010】

本開示の一側面の暗号化制御システムは、制御装置およびプラントが制御系バスを介して接続された暗号化制御システムにおいて、プラント側で、制御結果として出力される制御出力を暗号化して、暗号化制御出力を求める制御出力暗号化部と、制御装置側で、制御出力暗号化部が暗号化制御出力を暗号化するのに使用した公開鍵と同一の公開鍵を使用してプラントの制御に用いられるパラメータが予め暗号化された暗号化パラメータと、制御系バスを介して取得される暗号化制御出力とを暗号化したまま用いて、プラントを制御するための制御入力が暗号化されている暗号化制御入力を算出する演算部と、プラント側で、制御系バスを介して取得される暗号化制御入力を、公開鍵に対応する秘密鍵を使用して復号する復号部とを備える。

30

【0011】

本開示の一側面の暗号化制御方法またはプログラムは、制御装置およびプラントが制御系バスを介して接続された暗号化制御システムの暗号化制御方法、または、この暗号化制御システムを制御するコンピュータに実行させるプログラムにおいて、プラント側で、制御結果として出力される制御出力を暗号化して、暗号化制御出力を求め、制御装置側で、暗号化制御出力を暗号化するのに使用した公開鍵と同一の公開鍵を使用してプラントの制御に用いられるパラメータが予め暗号化された暗号化パラメータと、制御系バスを介して取得される暗号化制御出力とを暗号化したまま用いて、プラントを制御するための制御入力が暗号化されている暗号化制御入力を算出し、プラント側で、制御系バスを介して取得される暗号化制御入力を、公開鍵に対応する秘密鍵を使用して復号するステップを含む。

40

【0012】

本開示の一側面においては、プラント側で、制御結果として出力される制御出力が暗号化されて、暗号化制御出力が求められ、制御装置側で、暗号化制御出力を暗号化するのに使用した公開鍵と同一の公開鍵を使用してプラントの制御に用いられるパラメータが予め暗号化された暗号化パラメータと、制御系バスを介して取得される暗号化制御出力とが暗号化したまま用いられ、プラントを制御するための制御入力が暗号化されている暗号化制御入力が算出され、プラント側で、制御系バスを介して取得される暗号化制御入力が、公開鍵に対応する秘密鍵を使用して復号される。

【発明の効果】

50

【 0 0 1 3 】

本開示の一側面によれば、よりセキュリティ強化を図ることができる。

【 図面の簡単な説明 】

【 0 0 1 4 】

【 図 1 】 本技術を適用した F A システムの一実施の形態の構成例を示すブロック図である。

【 図 2 】 F A システムにおける制御処理について説明するフローチャートである。

【 図 3 】 シミュレーション結果を示す図である。

【 図 4 】 暗号化された信号について説明する図である。

【 図 5 】 本技術を適用した F A システムの変形例を示すブロック図である。

10

【 図 6 】 本技術を適用したコンピュータの一実施の形態の構成例を示すブロック図である。

【 発明を実施するための形態 】

【 0 0 1 5 】

< 暗号について >

まず、本技術を適用した具体的な実施の形態について説明する前に、本技術において用いられる暗号について説明する。

【 0 0 1 6 】

一般的に、整数の集合 Z に含まれる平文 M を、整数の集合 Z に含まれる暗号文 C に変換する暗号は、次の式 (1) で表される。

20

【 0 0 1 7 】

【 数 1 】

$$C = \text{Enc}(M) \quad \dots(1)$$

【 0 0 1 8 】

また、平文 M_1 と平文 M_2 との二項演算 $M_1 \oplus M_2$ を暗号化した暗号文 $\text{Enc}(M_1 \oplus M_2)$ を、平文 M_1 を暗号化した暗号文 $\text{Enc}(M_1)$ と、平文 M_2 を暗号化した暗号文 $\text{Enc}(M_2)$ とを用いて計算することができる暗号は、準同型暗号と称される。このような準同型暗号は、クラウドコンピューティングや金融機関の暗証システムなどに応用されている。

【 0 0 1 9 】

30

例えば、乗法に関して準同型性を持つ RSA (Rivest Shamir Adleman) 暗号は、多桁の素因数分解問題の困難性を利用した公開鍵暗号であり、デジタル署名などに応用されている。以下では、RSA暗号の暗号化および復号のアルゴリズム、および、RSA暗号の乗法に関する準同型性について説明する。

【 0 0 2 0 】

RSA暗号により暗号化を行う際には、まず、公開鍵 e 、公開鍵 n 、および秘密鍵 d が生成され、公開鍵 e および公開鍵 n のみを用いて平文が暗号化される。一方、RSA暗号により復号を行う際には、秘密鍵 d を知る必要がある。

【 0 0 2 1 】

公開鍵 n は、2つの大きな値の素数 p および素数 q を決定し、素数 p および素数 q の積 ($n = p \times q$) を演算することにより生成される。一方、公開鍵 e は、公開鍵 n のオイラーの関数 $\phi(n) = (p - 1) \times (q - 1)$ と互いに素 ($\text{gcd}(e, \phi(n)) = 1$) となる任意の正整数となるように生成される。また、秘密鍵 d は、法を $\phi(n)$ とした公開鍵 e の逆数として生成され、次の式 (2) のように定められる。

40

【 0 0 2 2 】

【 数 2 】

$$ed \equiv 1 \pmod{\phi(n)} \quad \dots(2)$$

【 0 0 2 3 】

また、剰余の定義より、秘密鍵 d は、次の式 (3) に示すような、未知定数 Q を用いた不定方程式を解くことにより求められる。なお、次の式 (4) に示すような形をとる不定

50

方程式は、拡張ユークリッド互除法により効率的に解くことができる。

【 0 0 2 4 】

【 数 3 】

$$\begin{aligned} ed &= \phi(n)Q + 1 \\ &= \phi(n)Q + \gcd(e, \phi(n)) \end{aligned} \quad \dots(3)$$

【 数 4 】

$$aX + bY = \gcd(a, b) \quad \dots(4)$$

【 0 0 2 5 】

このように、公開鍵 n および秘密鍵 d は共に、事前に決定される素数 p および素数 q から生成される。このとき、素数 p および素数 q の桁数が十分に大きければ、公開鍵 $n (= p \times q)$ を公開しても素因数分解により素数 p および素数 q を復元することは困難であることより、素数 p および素数 q が漏洩しない限り、秘密鍵 d を知ることは困難である。

10

【 0 0 2 6 】

次に、整数の集合 Z に含まれる平文 M は、次の式 (5) に示すように暗号文 C へと変換 (暗号化) される。

【 0 0 2 7 】

【 数 5 】

$$\begin{aligned} C &= \text{Enc}(M) \\ &= M^e \bmod n \end{aligned} \quad \dots(5)$$

20

【 0 0 2 8 】

但し、式 (5) において、平文 M の桁数は公開鍵 n の桁数未満 ($M < n$) でなければならず、平文 M の桁数が公開鍵 n の桁数以上 ($M \geq n$) の場合には、公開鍵 n の桁数ごとに平文 M を分割して暗号化する必要がある。また、この暗号化には、大きな整数のべき乗計算が含まれており、その計算を行うための効率的なアルゴリズムが存在する。

【 0 0 2 9 】

一方、暗号文 C は、次の式 (6) に示すように平文 M に変換 (復号) される。

【 0 0 3 0 】

【 数 6 】

$$\begin{aligned} M &= \text{Dec}(C) \\ &= C^d \bmod n \end{aligned} \quad \dots(6)$$

30

【 0 0 3 1 】

ここで、式 (6) について証明を行う。まず、次の式 (7) に示すような補題を導入する。

【 0 0 3 2 】

【 数 7 】

$$(X \bmod n)^d \bmod n = X^d \bmod n \quad \dots(7)$$

40

【 0 0 3 3 】

また、暗号文 C を、次の式 (8) のように定義すると、剰余の定義より定数 Q を介して $X = Q \times n + C$ と置くことができ、上述の式 (7) の左辺は、次の式 (9) に示すように置き換えられる。

【 0 0 3 4 】

【 数 8 】

$$C := X \bmod n \quad \dots(8)$$

【数 9】

$$(X \bmod n)^d \bmod n = C^d \bmod n \quad \dots(9)$$

【0035】

一方、この式(9)の右辺を二項定理により展開すると、次の式(10)のように、右辺 = 左辺となる。

【0036】

【数 10】

$$\begin{aligned} X^d \bmod n &= (Qn + C)^d \bmod n && 10 \\ &= \sum_{k=0}^d \binom{d}{k} (Qn)^k C^{d-k} \bmod n \\ &= \left(C^d + \left(\sum_{k=1}^d \binom{d}{k} Q^k n^{k-1} C^{d-k} \right) n \right) \bmod n && \dots(10) \\ &= C^d \bmod n \end{aligned}$$

【0037】

そして、復号の演算に、上述した式(7)を用いると、次の式(11)のようになり、この式(11)に上述した式(3)を代入すると、次の式(12)が求められる。 && 20

【0038】

【数 11】

$$\begin{aligned} \text{Dec}(C) &= C^d \bmod n \\ &= (M^e \bmod n)^d \bmod n && \dots(11) \\ &= M^{ed} \bmod n \end{aligned}$$

【数 12】

$$\begin{aligned} \text{Dec}(C) &= M^{ed} \bmod n && 30 \\ &= M^{\phi(n)Q+1} \bmod n \\ &= \left(M^{\phi(n)} \right)^Q M \bmod n && \dots(12) \\ &= \left(M^{\phi(n)} \bmod n \right)^Q (M \bmod n) \bmod n \end{aligned}$$

【0039】

ここで、次の式(13)に示すオイラーの定理より、式(12)は、次の式(14)のようになる。

【0040】

【数 13】

$$M^{\phi(n)} \bmod n = 1 \quad \dots(13) \quad 40$$

【数 14】

$$\begin{aligned} \text{Dec}(C) &= 1^Q (M \bmod n) \bmod n \\ &= M \bmod n && \dots(14) \end{aligned}$$

【0041】

従って、暗号化時の仮定より、平文 M の桁数は公開鍵 n の桁数未満 ($M < n$) であるならば $M \bmod n = M$ であることより、復号が達成されることが証明された。

【0042】

次に、準同型性について説明する。RSA暗号は、乗法に関する準同型性を持ち、次の式(15)に示す関係が成立する。

【0043】

【数15】

$$\text{Enc}(M_1M_2) = \text{Enc}(M_1)\text{Enc}(M_2) \pmod n \quad \dots(15)$$

【0044】

ここで、式(15)について証明を行う。被除数が負の場合を含むとき、剰余の定義は複数あるが、一例として、次の式(16)に示す定義を用いる。

【0045】

【数16】

$$X \pmod Y := X - \text{fix}(X/Y)Y$$

$$\text{fix}(\bullet) := \begin{cases} \lfloor \bullet \rfloor & (\bullet \geq 0) \\ \lceil \bullet \rceil & (\bullet < 0) \end{cases} \quad \dots(16)$$

【0046】

このとき、次の式(17)に示すような2つの暗号文について考えると、次の式(18)に示すようになる。

【0047】

【数17】

$$C_1 = \text{Enc}(M_1) = M_1^e \pmod n \quad \dots(17)$$

$$C_2 = \text{Enc}(M_2) = M_2^e \pmod n$$

【数18】

$$M_1^e = q_1n + C_1, \quad M_2^e = q_2n + C_2 \quad \dots(18)$$

$$q_1 := \text{fix}(M_1^e/n), \quad q_2 := \text{fix}(M_2^e/n)$$

【0048】

従って、上述した式(15)の左辺は、次の式(19)に示すように右辺に一致することより、式(15)に示すような関係が成立することが証明された。

【0049】

【数19】

$$\begin{aligned} \text{Enc}(M_1M_2) &= (M_1M_2)^e \pmod n \\ &= (q_1n + C_1)(q_2n + C_2) \pmod n \\ &= ((q_1q_2n + q_1C_2 + q_2nC_1)n + C_1C_2) \pmod n \quad \dots(19) \\ &= C_1C_2 \pmod n \\ &= \text{Enc}(M_1)\text{Enc}(M_2) \pmod n \end{aligned}$$

【0050】

本技術では、以上のような準同型性を持つRSA暗号が利用される。

【0051】

以下、本技術を適用した具体的な実施の形態について、図面を参照しながら詳細に説明する。

【0052】

<FAシステムの構成例>

図1は、本技術を適用したFA(Factory Automation)システムの一実施の形態の構成例を示すブロック図である。なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0053】

10

20

30

40

50

図 1 において、F A システム 1 1 は、準同型暗号を用いた制御系として構成され、入力装置 1 2、コントローラ 1 3、プラント 1 4、および制御系バス 1 5 を備え、コントローラ 1 3 およびプラント 1 4 が制御系バス 1 5 を介して接続されて構成される。

【 0 0 5 4 】

F A システム 1 1 においては、オペレータが入力装置 1 2 を操作して、コントローラ 1 3 がプラント 1 4 を制御するためのパラメータを入力する。そのパラメータは、入力装置 1 2 において暗号化された後にコントローラ 1 3 に送信され、コントローラ 1 3 がパラメータを暗号化したまま処理を行い、制御系バス 1 5 を介してプラント 1 4 に対する制御が実行される。

【 0 0 5 5 】

入力装置 1 2 は、パラメータ入力部 2 1 および暗号化部 2 2 を備えて構成される。

【 0 0 5 6 】

パラメータ入力部 2 1 は、例えば、キーボードやタッチパネルなどの操作手段を有しており、オペレータによる操作に応じて入力されるパラメータを暗号化部 2 2 に供給する。暗号化部 2 2 は、パラメータ入力部 2 1 から供給されるパラメータを、公開鍵を用いて暗号化し、暗号化されたパラメータ $Enc(Parameters)$ をコントローラ 1 3 に送信する。

【 0 0 5 7 】

コントローラ 1 3 は、暗号化パラメータ取得部 3 1、受信部 3 2、演算部 3 3、送信部 3 4、および記録部 3 5 を備えて構成される。

【 0 0 5 8 】

暗号化パラメータ取得部 3 1 は、入力装置 1 2 と通信を行って、暗号化部 2 2 から送信される暗号化されたパラメータ $Enc(Parameters)$ を取得し、演算部 3 3 に供給する。受信部 3 2 は、プラント 1 4 から送信される暗号化された制御出力 $Enc(x)$ を受信し、演算部 3 3 に供給する。

【 0 0 5 9 】

演算部 3 3 は、暗号化パラメータ取得部 3 1 から供給される暗号化されたパラメータ $Enc(Parameters)$ と、受信部 3 2 から供給される暗号化された制御出力 $Enc(x)$ とを用いて、プラント 1 4 に対する制御を実行するための演算を行う。このとき、演算部 3 3 は、パラメータおよび制御出力を暗号化したまま演算 $\{Enc(u[k]) = g'(Enc(x), Enc(u))\}$ して、復号および暗号化を行わずに、プラント 1 4 を制御するために入力される制御入力 u が暗号化された状態の制御入力 $Enc(u)$ を算出する。

【 0 0 6 0 】

そして、演算部 3 3 は、演算により求めた暗号化された制御入力 $Enc(u)$ を送信部 3 4 に供給し、送信部 3 4 は、制御系バス 1 5 を介して、暗号化された制御入力 $Enc(u)$ をプラント 1 4 に送信する。

【 0 0 6 1 】

記録部 3 5 は、暗号化パラメータ取得部 3 1 が取得した暗号化されたパラメータ $Enc(Parameters)$ を記録する。さらに、記録部 3 5 は、暗号化されたパラメータ $Enc(Parameters)$ とともに、その暗号化されたパラメータ $Enc(Parameters)$ を用いた演算部 3 3 の演算において用いられた暗号化された制御出力 $Enc(x)$ と、その演算により求められた暗号化された制御入力 $Enc(u)$ を記録する。なお、記録部 3 5 は、暗号化されたパラメータ $Enc(Parameters)$ 、暗号化された制御出力 $Enc(x)$ 、および暗号化された制御入力 $Enc(u)$ のうち、少なくともいずれか 1 つを記録するように構成されていればよい。

【 0 0 6 2 】

プラント 1 4 は、受信部 4 1、復号部 4 2、制御実行部 4 3、暗号化部 4 4、および送信部 4 5 を備えて構成される。

【 0 0 6 3 】

受信部 4 1 は、コントローラ 1 3 の送信部 3 4 から制御系バス 1 5 を介して送信されてくる暗号化された制御入力 $Enc(u)$ を受信し、復号部 4 2 に供給する。復号部 4 2 は、暗号化部 2 2 が暗号化に用いた公開鍵に対応する秘密鍵を有しており、受信部 4 1 から供

10

20

30

40

50

給される暗号化された制御入力 $Enc(u)$ を復号して得られる平文の制御入力 u を、制御実行部43に供給する。

【0064】

制御実行部43は、復号部42から供給される制御入力 u に従って、例えば、図示しないアクチュエータに対する制御を実行する。また、制御実行部43は、例えば、アクチュエータの駆動を測定するセンサを有しており、そのセンサによって測定された追従偏差を、制御入力 u に従った制御に対する制御出力 x として暗号化部44に供給する。または、制御実行部43は、制御入力 u に従った制御に対する制御出力 x を求めるための演算 $\{x[k]=f(x, u)\}$ を行ってもよい。

【0065】

暗号化部44は、制御実行部43から供給される制御出力 x を暗号化し、暗号化された制御出力 $Enc(x)$ を送信部45に供給する。送信部45は、暗号化部44から供給される暗号化された制御出力 $Enc(x)$ を、制御系バス15を介してコントローラ13に送信する。

【0066】

以上のように、FAシステム11は構成されており、コントローラ13およびプラント14を接続する制御系バス15を介して送受信される情報の暗号化に、準同型暗号が採用される。これにより、コントローラ13の演算部33は、制御出力 $Enc(x)$ を復号することなく、プラント14に対する制御を実行するための演算を行うことができる。従って、FAシステム11は、プラント14の復号部42のみが秘密鍵を保持する構成とすることができる。

【0067】

上述したような従来の産業ネットワークでは、コントローラおよびプラントの双方が秘密鍵を保持する構成であり、このような構成と比較して、FAシステム11は、秘密鍵を保持する箇所を削減することができる。従って、FAシステム11は、仮に、コントローラ13がハッキングされたとしても秘密鍵が漏洩することを回避することができ、また、コントローラ13の記録部35に記録されたパラメータ、制御出力および制御入力のそれぞれが暗号化されているため、たとえこれらが漏洩したとしても、コントローラ13およびプラント14の情報が漏洩することがなく、よりセキュリティ強化を図ることができる。即ち、FAシステム11においては、コントローラ13およびプラント14が離れた位置に配置され、制御系バス15を介して制御入力および制御出力を送受信するような構成であっても、コントローラ13およびプラント14の間で情報が漏洩してしまう危険性を低減することができる。

【0068】

このように、FAシステム11は、従来の産業ネットワークよりも、被攻撃箇所を削減することができる。なお、準同型暗号の性質上、各種のゲインなどのようにコントローラ13が演算を行うためのパラメータは暗号化しておく必要があるが、これらのパラメータの暗号化は公開鍵のみで行うことができ、脆弱性は増加することはない。

【0069】

また、FAシステム11において、上述したようなRSA暗号を使用した場合、RSA暗号は、加法に関して準同型性を持たないため、コントローラ13は、加法の必要ない比例制御(P制御)を用いてプラント14に対する制御を行う。同様に、フィードバック誤差の演算を暗号文に対して行うことができないため、制御実行部43は、例えば、レギュレーション問題またはセンサにより偏差を直接的に測定可能となるように構成される。

【0070】

次に、FAシステム11において、コントローラ13に比例制御を実装した例について説明する。

【0071】

例えば、オペレータは、比例制御で用いられるPゲイン K_p をパラメータとして、パラメータ入力部21に入力する。そして、暗号化部22は、次の式(20)に示すように、

10

20

30

40

50

公開鍵 e および公開鍵 n を用いて P ゲイン K_p を暗号化して、暗号化された P ゲイン $Enc(K_p)$ をコントローラ 13 に送信する。

【0072】

【数20】

$$\begin{aligned} K_{pe} &= Enc(K_p) \\ &= K_p^e \pmod n \end{aligned} \quad \dots(20)$$

【0073】

一方、プラント 14 では、制御実行部 43 が、センサにより測定した追従偏差 ε を、制御出力として暗号化部 44 に供給する。そして、暗号化部 44 は、次の式 (21) に示すように、公開鍵 e および公開鍵 n を用いて追従偏差 ε を暗号化して、暗号化された追従偏差 $Enc(\varepsilon)$ をコントローラ 13 に送信する。この際、暗号化部 44 は、観測信号が実数である場合には、暗号化のために整数値に変換した後に暗号化を行う。

10

【0074】

【数21】

$$\begin{aligned} \varepsilon_e &= Enc(\varepsilon) \\ &= \varepsilon^e \pmod n \end{aligned} \quad \dots(21)$$

【0075】

そして、コントローラ 13 では、演算部 33 が、RSA暗号の準同型性を利用し、暗号化された P ゲイン $Enc(K_p)$ および追従偏差 $Enc(\varepsilon)$ を用いて、次の式 (22) に示す演算を行うことで、暗号化された制御入力 $Enc(u)$ を求める。

20

【0076】

【数22】

$$\begin{aligned} u_e &= Enc(K_p \varepsilon) \\ &= K_{pe} \varepsilon_e \pmod n \end{aligned} \quad \dots(22)$$

【0077】

そして、演算部 33 が求めた暗号化された制御入力 $Enc(u)$ は、送信部 34 を介してプラント 14 に送信される。

30

【0078】

その後、プラント 14 では、復号部 42 が、次の式 (23) に示すように、秘密鍵 d を用いて暗号化された制御入力 $Enc(u)$ を復号して、平文の制御入力 u を制御実行部 43 に供給する。

【0079】

【数23】

$$\begin{aligned} u &= Dec(u_e) \\ &= u_e^d \pmod n \end{aligned} \quad \dots(23)$$

【0080】

これにより、制御実行部 43 は、制御入力 u に従って、図示しないアクチュエータを動作させる。

40

【0081】

このように、FAシステム 11 は、RSA暗号の準同型性を利用して、演算部 33 が、暗号化された P ゲイン $Enc(K_p)$ および追従偏差 $Enc(\varepsilon)$ を復号することなく、暗号化された制御入力 $Enc(u)$ を求めることができるように構成されている。従って、FAシステム 11 は、プラント 14 の復号部 42 が復号を行うときのみ秘密鍵 d が必要となる構成であることより、よりセキュリティ強化を図ることができる。

【0082】

次に、図 2 のフローチャートを参照して、FAシステム 11 における制御処理について

50

説明する。

【0083】

制御処理が開始され、ステップS11において、オペレータがパラメータとしてPゲイン K_p を入力すると、入力装置12では、パラメータ入力部21がPゲイン K_p を取得して、暗号化部22に供給する。

【0084】

ステップS12において、入力装置12では、暗号化部22が、ステップS11でパラメータ入力部21から供給されたPゲイン K_p を、公開鍵eおよび公開鍵nを用いて暗号化する。そして、暗号化部22は、コントローラ13の暗号化パラメータ取得部31と通信を行い、暗号化されたPゲイン K_p をコントローラ13に送信する。

10

【0085】

ステップS13において、プラント14では、制御実行部43が、センサにより追従偏差を測定し、制御出力として暗号化部44に供給する。そして、暗号化部44は、その追従偏差を公開鍵eおよび公開鍵nを用いて暗号化し、送信部45は、暗号化された追従偏差 $Enc(\quad)$ を、制御系バス15を介してコントローラ13に送信する。

【0086】

ステップS14において、コントローラ13では、暗号化パラメータ取得部31が、暗号化部22により暗号化されたPゲイン $Enc(K_p)$ を取得して演算部33に供給し、受信部32が、暗号化部44により暗号化された追従偏差 $Enc(\quad)$ を受信して演算部33に供給する。そして、演算部33は、暗号化されたPゲイン $Enc(K_p)$ および追従偏差 $Enc(\quad)$ から、上述した式(22)に示す演算を行うことで、暗号化された制御入力 $Enc(u)$ を求める。送信部34は、演算部33が求めた暗号化された制御入力 $Enc(u)$ を、制御系バス15を介してプラント14に送信する。

20

【0087】

ステップS15において、プラント14では、受信部41が、コントローラ13から送信されてくる暗号化された制御入力 $Enc(u)$ を受信する。復号部42は、秘密鍵dを用いて制御入力 $Enc(u)$ を復号して、平文の制御入力uを制御実行部43に供給する。

【0088】

ステップS16において、プラント14では、制御実行部43が、制御入力uに従った駆動するようにアクチュエータを制御し、制御処理は終了される。

30

【0089】

以上のように、FAシステム11では、予め暗号化されたPゲイン $Enc(K_p)$ を暗号化パラメータ取得部31が取得し、演算部33は、暗号化されたPゲイン $Enc(K_p)$ および追従偏差 $Enc(\quad)$ を暗号化したまま用いて、暗号化された状態の制御入力 $Enc(u)$ を直接的に算出することができる。従って、コントローラ13において暗号鍵を保持する必要がなく、従来よりもセキュリティ強化を図ることができる。

【0090】

<シミュレーション結果について>

このようなFAシステム11における制御処理の動作について、数値例を用いたシミュレーションを行うことにより確認する。

40

【0091】

例えば、RSA暗号の初期設定において、RSA暗号に必要なパラメータとして、公開鍵eに23を設定し、素数pに1009を設定し、素数qに2003を設定する。これらのパラメータを用いることで、公開鍵nとして2021027が生成され、秘密鍵dとして526439が生成される。

【0092】

また、シミュレーション条件として、プラント14の制御実行部43は、次の式(24)に示す演算に従い動作する。なお、制御実行部43による処理は、10msで離散化して行われる。

【0093】

【数 2 4】

$$\dot{x}(t) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & -3 & -5 \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} u(t) \quad \dots(24)$$

$$y(t) = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} x(t)$$

【0 0 9 4】

そして、シミュレーション条件として、パラメータ入力部 2 1 に入力するパラメータとして P ゲイン K_p に 3 を設定すると、暗号化部 2 2 により、次の式 (2 5) に示す値が、暗号化された P ゲイン $Enc(K_p)$ として求められる。

【0 0 9 5】

【数 2 5】

$$K_p = 3 \quad \dots(25)$$

$$K_{pe} = Enc(K_p) = 1720140$$

【0 0 9 6】

このようなシミュレーション条件に基づいてシミュレーションを行った。なお、暗号化部 4 4 による暗号化時における整数化は、例えば、12bit AD/DAコンバータの使用を想定し、次の式 (2 6) に示すように行った。但し、式 (2 6) において、 ε は、暗号化部 4 4 へ与える追従偏差の整数値であり、 ε_{raw} は、制御実行部 4 3 が有するセンサから得られた追従偏差の実数値である。

【0 0 9 7】

【数 2 6】

$$\varepsilon = \text{round}(\varepsilon_{raw} \times 2^{12}) \quad \dots(26)$$

【0 0 9 8】

図 3 には、上述したシミュレーション条件におけるシミュレーション結果が示されている。

【0 0 9 9】

図 3 において、横軸は、時刻 (Time[s]) を示しており、縦軸は、制御実行部 4 3 からの制御出力 (Output) を示している。また、図 3 では、制御の追従目標 (tracking target) が破線で表され、暗号化したままで制御の演算を行ったシミュレーション結果 (With encoding) が実線で表され、従来のように復号して演算を行ったシミュレーション結果 (Without encoding) が丸印で表されている。

【0 1 0 0】

図 3 に示すように、FA システム 1 1 において、演算部 3 3 が暗号化したままで制御の演算を行った応答は、微細な誤差はあるものの、復号して演算を行った応答とほぼ同一であるというシミュレーション結果を得ることができた。なお、この誤差は、暗号化時における整数化での打ち切りによるものであると考えられる。

【0 1 0 1】

このように、FA システム 1 1 は、乗法に関して準同型性を持つ RSA 暗号を利用して比例制御を行うとき、演算部 3 3 が暗号化したままで制御の演算を行っても、応答が劣化することを回避することができる。

【0 1 0 2】

また、FA システム 1 1 では、プラント 1 4 およびコントローラ 1 3 を接続する制御系バス 1 5 において、暗号化された信号 (制御出力および制御入力) が伝達される。このため、FA システム 1 1 は、コントローラ 1 3 およびプラント 1 4 が離れた位置に配置され、制御系バス 1 5 を介して制御入力および制御出力を送受信するような構成であっても、制御系バス 1 5 において情報が漏洩することを防止することができる。

10

20

30

40

50

【 0 1 0 3 】

ここで、図 4 を参照して、暗号化された信号について説明する。図 4 には、シミュレーション条件として、 $y[0] = 1$ および $r[k] = 0$ を設定した場合におけるシミュレーション結果が示されている。

【 0 1 0 4 】

図 4 A には、図 3 と同様のシミュレーション結果が示されており、図 4 B には、暗号化された制御出力 (Encoded Output) が示されており、図 4 C には、暗号化された制御入力 (Encoded Control Input) が示されている。

【 0 1 0 5 】

例えば、図 4 A に示すように、 $y[k]$ が $r[k] = 0$ を追従するようにシミュレーションを行ったときに、プラント 1 4 からコントローラ 1 3 に制御系バス 1 5 を介して送信される信号が図 4 B に示されている。同様に、コントローラ 1 3 からプラント 1 4 に制御系バス 1 5 を介して送信される信号が図 4 C に示されている。

10

【 0 1 0 6 】

図 4 に示すように、制御系バス 1 5 を介して伝送される信号 (制御出力および制御入力) は暗号化されており、セキュリティ性を高めることができる。

【 0 1 0 7 】

このように、FA システム 1 1 では、コントローラ 1 3 およびプラント 1 4 の間でやり取りされる測定量や操作量などの信号を秘匿することができ、例えば、制御システムにおけるリプレイアタック対策を実現することができる。また、FA システム 1 1 では、入力装置 1 2 からコントローラ 1 3 に伝送される目標信号 (パラメータ) を秘匿することができるので、例えば、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などのレシピ情報を秘匿することができる。さらに、FA システム 1 1 は、コントローラ 1 3 およびプラント 1 4 の内部における制御アルゴリズムも秘匿することができる。

20

【 0 1 0 8 】

以上のように、FA システム 1 1 では、制御システムにおける 3 つの秘密情報を秘匿したままの演算を可能としており、従来よりも、より強固なセキュリティを実現することができる。

【 0 1 0 9 】

なお、FA システム 1 1 は、制御系に暗号化処理を応用しており、制御のリアルタイム性に影響を与えることが懸念される。そこで、プラント 1 4 において、暗号化部 4 4 が追従偏差を暗号化して、復号部 4 2 が制御入力 u を復号するまでの制御周期ごとの所要時間をシミュレーションにより求めたところ、0.5ms 以下であるというシミュレーション結果が得られた。例えば、一般的な制御周期は数秒以上であることより、FA システム 1 1 は、暗号化処理のリアルタイム性を十分に確保できることが確認された。

30

【 0 1 1 0 】

ところで、上述したように、FA システム 1 1 では、乗法に関して準同型性を持つ RSA 暗号を利用して、演算部 3 3 が、暗号化された P ゲイン $Enc(K_p)$ および追従偏差 $Enc(\quad)$ から、暗号化された制御入力 $Enc(u)$ を求める演算を行うことができる。この構成では、FA システム 1 1 において、演算に乗法のみを用いる制御の実装に限定されることになる。

40

【 0 1 1 1 】

これに対し、例えば、FA システム 1 1 は、乗法および加法に関して準同型性を持つ暗号 (Gentry が提案した完全準同型暗号) を利用する構成を採用することができる。この構成により、例えば、乗法および加法の必要な PID (Proportional Integral Derivative) 制御を FA システム 1 1 に実装することが可能となり、より実用性を高めることができる。

【 0 1 1 2 】

次に、図 5 は、本技術を適用した FA システムの変形例を示すブロック図である。

【 0 1 1 3 】

50

図5に示すFAシステム11Aにおいて、図1のFAシステム11と共通する構成については同一の符号を付し、その詳細な説明は省略する。即ち、FAシステム11Aは、入力装置12およびコントローラ13は、図1のFAシステム11と共通の構成とされる。但し、FAシステム11Aは、プラント14Aにおいて、復号部42と制御実行部43との間に加算処理部46が設けられている点で、図1のFAシステム11と異なる構成となっている。

【0114】

例えば、FAシステム11Aでは、演算部33は、PID制御において加算を行う対象となる一部分ごとに所定数Nに分割して乗算を行い、それらの乗算により求められる一部分ごとの暗号化された制御入力 $Enc(u_i)$ ($i = 1 \sim N$)を算出する。そして、演算部33は、このようにして求めた所定数Nの一部分ごとの制御入力 $Enc(u_i)$ を、送信部34を介してプラント14に送信する。

10

【0115】

プラント14では、復号部42は、所定数Nの一部分ごとの制御入力 $Enc(u_i)$ をそれぞれ復号し、加算を行う対象となる所定数Nの制御入力 u_i を加算処理部46に供給する。そして、加算処理部46は、所定数Nの制御入力 u_i を全て加算する処理を行って、PID制御における制御入力 u を求め、制御実行部43に供給する。

【0116】

また、制御実行部43は、所定数Nの制御出力 x_i を求めて暗号化部44に供給し、暗号化部44は、暗号化された制御出力 $Enc(x_i)$ を、送信部45を介して暗号化パラメータ取得部31に送信する。

20

【0117】

このような構成とすることで、FAシステム11Aは、乗法および加法に準同型性を持つ暗号を利用することができ、PID制御を実行することができる。

【0118】

なお、本実施の形態では、暗号化パラメータ取得部31が暗号化パラメータを取得するたびに演算部33が演算を行うように構成されている。これに対し、例えば、暗号化パラメータ取得部31は、取得した暗号化パラメータが既に記録部35に記録されている場合、その暗号化パラメータに対応付けられて記録されている暗号化された制御出力および制御入力を読み出して演算部33に供給するようにしてもよい。この場合、演算部33は、暗号化された制御出力も一致していれば、暗号化された制御入力を求める演算をすることなく、暗号化パラメータ取得部31から供給される暗号化された制御入力を、そのまま送信部34を介してプラント14に送信する。これにより、FAシステム11では、処理の高速化を図ることができる。

30

【0119】

また、FAシステム11は、上述したような比例制御またはPID制御を行う他、例えば、モデル予測制御を行ってもよい。即ち、FAシステム11は、制御方法により限定されることはない。

【0120】

なお、上述のフローチャートを参照して説明した各処理は、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって処理されるものであっても良い。

40

【0121】

また、上述した一連の処理（情報処理方法）は、ハードウェアにより実行することもできるし、ソフトウェアにより実行することもできる。一連の処理をソフトウェアにより実行する場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラ

50

ムが記録されたプログラム記録媒体からインストールされる。

【0122】

図6は、上述した一連の処理をプログラムにより実行するコンピュータのハードウェアの構成例を示すブロック図である。

【0123】

コンピュータにおいて、CPU (Central Processing Unit) 101, ROM (Read Only Memory) 102, RAM (Random Access Memory) 103は、バス104により相互に接続されている。

【0124】

バス104には、さらに、入出力インタフェース105が接続されている。入出力インタフェース105には、キーボード、マウス、マイクロホンなどよりなる入力部106、ディスプレイ、スピーカなどよりなる出力部107、ハードディスクや不揮発性のメモリなどよりなる記憶部108、ネットワークインタフェースなどよりなる通信部109、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどのリムーバブルメディア111を駆動するドライブ110が接続されている。

10

【0125】

以上のように構成されるコンピュータでは、CPU101が、例えば、記憶部108に記憶されているプログラムを、入出力インタフェース105及びバス104を介して、RAM103にロードして実行することにより、上述した一連の処理が行われる。

【0126】

コンピュータ (CPU101) が実行するプログラムは、例えば、磁気ディスク (フレキシブルディスクを含む)、光ディスク (CD-ROM (Compact Disc-Read Only Memory), DVD (Digital Versatile Disc) 等)、光磁気ディスク、もしくは半導体メモリなどよりなるパッケージメディアであるリムーバブルメディア111に記録して、あるいは、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の伝送媒体を介して提供される。

20

【0127】

そして、プログラムは、リムーバブルメディア111をドライブ110に装着することにより、入出力インタフェース105を介して、記憶部108にインストールすることができる。また、プログラムは、有線または無線の伝送媒体を介して、通信部109で受信し、記憶部108にインストールすることができる。その他、プログラムは、ROM102や記憶部108に、あらかじめインストールしておくことができる。

30

【0128】

なお、本実施の形態は、上述した実施の形態に限定されるものではなく、本開示の要旨を逸脱しない範囲において種々の変更が可能である。

【符号の説明】

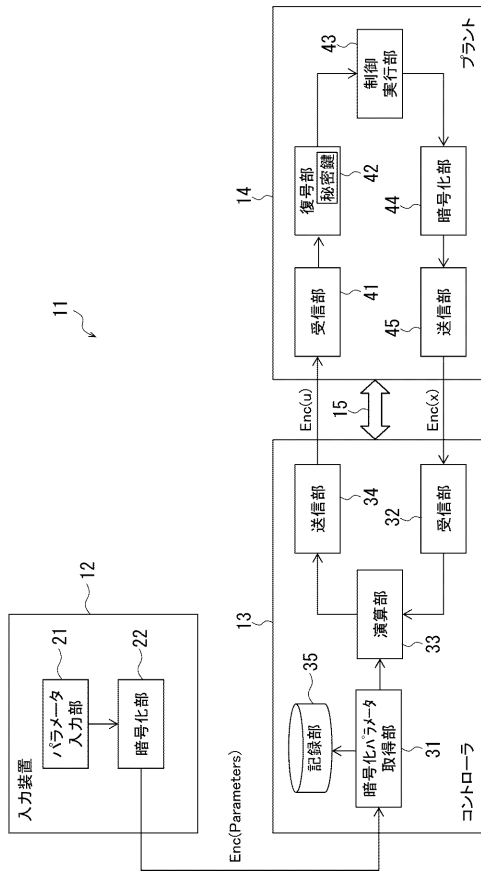
【0129】

11 FAシステム, 12 入力装置, 13 コントローラ, 14 プラント,
15 制御系バス, 21 パラメータ入力部, 22 暗号化部, 31 暗号化パラ
メータ取得部, 32 受信部, 33 演算部, 34 送信部, 35 記録部,
41 受信部, 42 復号部, 43 制御実行部, 44 暗号化部, 45 送信
部, 46 加算処理部

40

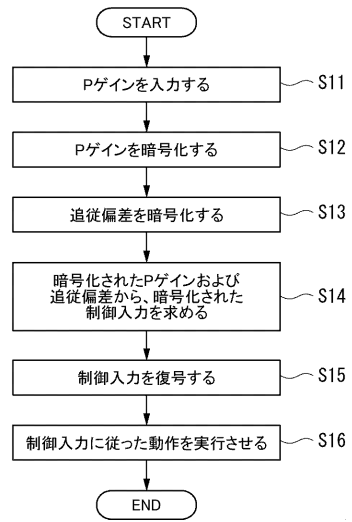
【図1】

図1



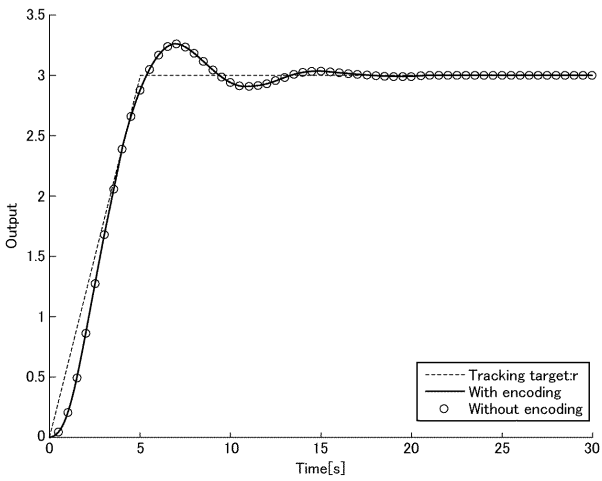
【図2】

図2



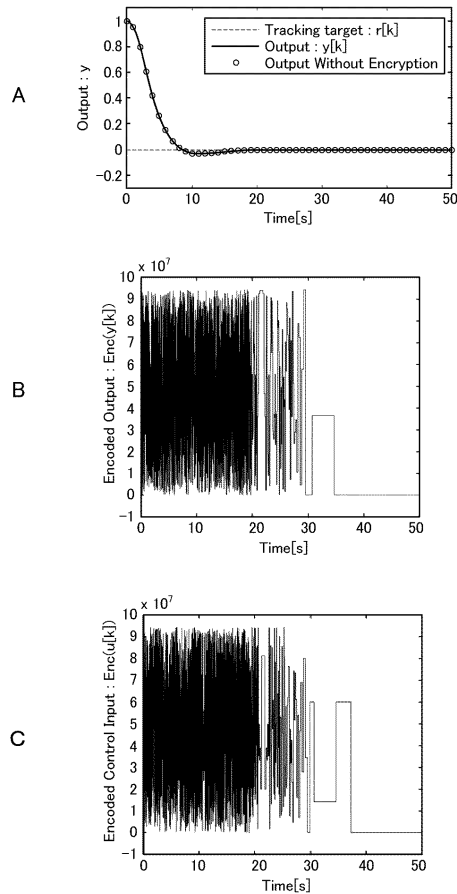
【図3】

図3

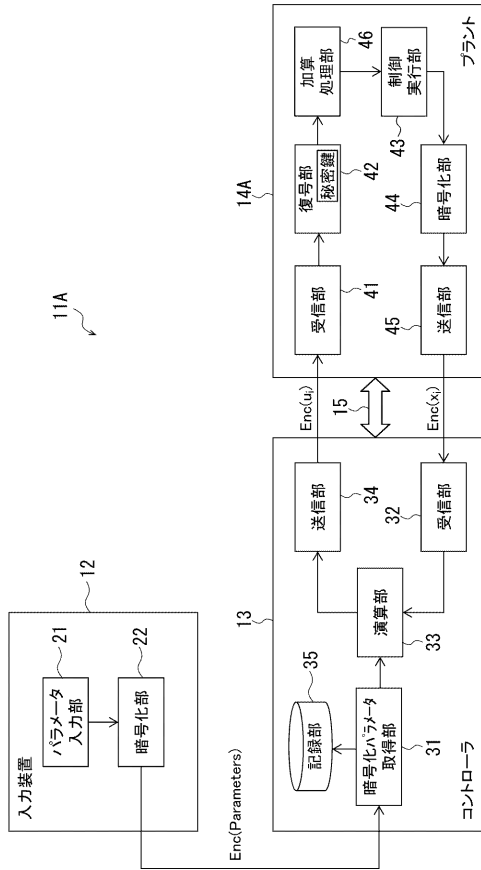


【図4】

図4



【図5】
図5



【図6】
図6

