(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6360781号
(P6360781)
(45)発行日　平成30年7月18日(2018.7.18)　(24)登録日　平成30年6月29日(2018.6.29)

(51)Int.Cl.　F I
G09C 1/00 (2006.01)　G09C 1/00 620Z

請求項の数 9 (全 18 頁)

(21)出願番号　特願2014-226964(P2014-226964)
(22)出願日　平成26年11月7日(2014.11.7)
(65)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)
審査請求日　平成29年10月25日(2017.10.25)

(73)特許権者　504133110
国立大学法人電気通信大学
東京都調布市調布ケ丘一丁目５番地１
(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　小木曽　公尚
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内
(72)発明者　藤田　貴大
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内

審査官　金沢　史明

最終頁に続く

(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)【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、
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、ＰＩＤ（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ＰＩＤ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、
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が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。
【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が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
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】
【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。
【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】
【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。
【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。

【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。
【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。
【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】
【００１３】
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】
【００１４】
【図１】本技術を適用したＦＡ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】ＦＡ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ＦＡシステムの変形例を示すブロック図である。
【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】
【００１５】
＜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。
【００１６】
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。

【００１７】
【数１】

$$C = Enc(M) \quad \cdots(1)$$

【００１８】
また、平文M_1と平文M_2との二項演算$M_1 \bigcirc M_2$を暗号化した暗号文Enc（$M_1 \bigcirc M_2$）を、平文M_1を暗号化した暗号文Enc（M_1）と、平文M_2を暗号化した暗号文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。
【００１９】
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。
【００２０】
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。
【００２１】
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×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φ（ｎ）＝（ｐ－１）×（ｑ－１）と互いに素（$gcd(e,\phi(n))=1$）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φ（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。
【００２２】
【数２】

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

【００２３】
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。
【００２４】
【数３】

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

【数４】

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

【００２５】
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×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。
【００２６】
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。
【００２７】

【数５】

$$C = Enc(M) = M^{e} \bmod n \quad \cdots(5)$$

【００２８】

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≧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。

【００２９】

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。

【００３０】

【数６】

$$M = Dec(C) = C^{d} \bmod n \quad \cdots(6)$$

【００３１】

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。

【００３２】

【数７】

$$(X \bmod n)^{d} \bmod n = X^{d} \bmod n \quad \cdots(7)$$

【００３３】

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×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。

【００３４】

【数８】

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

【数９】

$$(X \bmod n)^{d} \bmod n = C^{d} \bmod n \quad \cdots(9)$$

【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】

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

【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。

【００３８】

【数１１】

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

【数１２】

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

【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】

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

【数１４】

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

【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 mod 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】

$$Enc(M_1M_2) = Enc(M_1)Enc(M_2) \bmod n \quad \cdots(15)$$

【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】

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

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

【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】

$$C_1 = Enc(M_1) = M_1^e \mod n$$
$$C_2 = Enc(M_2) = M_2^e \mod n \quad \cdots(17)$$

【数１８】

$$M_1^e = q_1 n + C_1, \quad M_2^e = q_2 n + C_2$$
$$q_1 := fix(M_1^e/n), \quad q_2 := fix(M_2^e/n) \quad \cdots(18)$$

【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】

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

【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】

図１において、ＦＡシステム１１は、準同型暗号を用いた制御系として構成され、入力装置１２、コントローラ１３、プラント１４、および制御系バス１５を備え、コントローラ１３およびプラント１４が制御系バス１５を介して接続されて構成される。

【００５４】

ＦＡシステム１１においては、オペレータが入力装置１２を操作して、コントローラ１３がプラント１４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１２において暗号化された後にコントローラ１３に送信され、コントローラ１３がパラメータを暗号化したまま処理を行い、制御系バス１５を介してプラント１４に対する制御が実行される。

【００５５】

入力装置１２は、パラメータ入力部２１および暗号化部２２を備えて構成される。

【００５６】

パラメータ入力部２１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２２に供給する。暗号化部２２は、パラメータ入力部２１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１３に送信する。

【００５７】

コントローラ１３は、暗号化パラメータ取得部３１、受信部３２、演算部３３、送信部

３４、および記録部３５を備えて構成される。

【００５８】

暗号化パラメータ取得部３１は、入力装置１２と通信を行って、暗号化部２２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３３に供給する。受信部３２は、プラント１４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３３に供給する。

【００５９】

演算部３３は、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パラメータEnc（Parameters）と、受信部３２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１４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３３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１４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。

【００６０】

そして、演算部３３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３４に供給し、送信部３４は、制御系バス１５を介して、暗号化された制御入力Enc（ｕ）をプラント１４に送信する。

【００６１】

記録部３５は、暗号化パラメータ取得部３１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３５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３３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３５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。

【００６２】

プラント１４は、受信部４１、復号部４２、制御実行部４３、暗号化部４４、および送信部４５を備えて構成される。

【００６３】

受信部４１は、コントローラ１３の送信部３４から制御系バス１５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４２に供給する。復号部４２は、暗号化部２２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４１から供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、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】

$$K_{pe} = \mathrm{Enc}(K_p) = K_p^e \bmod n \quad \cdots(20)$$

【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（ε）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。

【００７４】

【数２１】

$$\varepsilon_e = \mathrm{Enc}(\varepsilon) = \varepsilon^e \bmod n \quad \cdots(21)$$

【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（ε）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。
【００７６】
【数２２】

$$u_e = Enc(K_p\varepsilon) = K_{pe}\varepsilon_e \mod n \quad \cdots(22)$$

【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。
【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】

$$u = Dec(u_e) = u_e^d \mod n \quad \cdots(23)$$

【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。
【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（ε）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。
【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ε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ε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（ε）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（ε）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（ε）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。

【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。

【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（ε）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。

【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２４】

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

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

【００９４】

そして、シミュレーション条件として、パラメータ入力部２１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２２により、次の式（２５）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。

【００９５】

【数２５】

$$K_p = 3$$

$$\cdots(25)$$

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

【００９６】

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４４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（２６）に示すように行った。但し、式（２６）において、εは、暗号化部４４へ与える追従偏差の整数値であり、ε_{raw}は、制御実行部４３が有するセンサから得られた追従偏差の実数値である。

【００９７】

【数２６】

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

【００９８】

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。

【００９９】

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４３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。

【０１００】

図３に示すように、ＦＡシステム１１において、演算部３３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。

【０１０１】

このように、ＦＡシステム１１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３３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。

【０１０２】

また、ＦＡシステム１１では、プラント１４およびコントローラ１３を接続する制御系バス１５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１１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、制御系バス１５において情報が漏洩することを防止することができる。

【０１０３】

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。

【０１０４】

図４Ａ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４Ｂには、暗号化された制御出力（Encoded Output）が示されており、図４Ｃには、暗号化された制御入力（Encoded Control Input）が示されている。

【０１０５】

例えば、図４Ａ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１４からコントローラ１３に制御系バス１５を介して送信される信号が図４Ｂに示されている。同様に、コントローラ１３からプラント１４に制御系バス１５を介して送信される信号が図４Ｃに示されている。

【０１０６】

図４に示すように、制御系バス１５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。

【０１０７】

このように、ＦＡシステム１１では、コントローラ１３およびプラント１４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１１では、入力装置１２からコントローラ１３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１１は、コントローラ１３およびプラント１４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。

【０１０８】

以上のように、ＦＡシステム１１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で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。

【０１０９】

なお、ＦＡシステム１１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１４において、暗号化部４４が追従偏差εを暗号化して、復号部４２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１１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。

【０１１０】

ところで、上述したように、ＦＡシステム１１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３３が、暗号化されたＰゲインEnc（K_p）および追従偏差Enc（ε）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１１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。

【０１１１】

これに対し、例えば、ＦＡシステム１１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１１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。

【０１１２】

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。

【０１１３】

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～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。

【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。

【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。

【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。

【０１２１】

また、上述した一連の処理（情報処理方法）は、ハードウエアにより実行することもできるし、ソフトウエアにより実行することもできる。一連の処理をソフトウエアにより実行する場合には、そのソフトウエアを構成するプログラムが、専用のハードウエ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エ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】

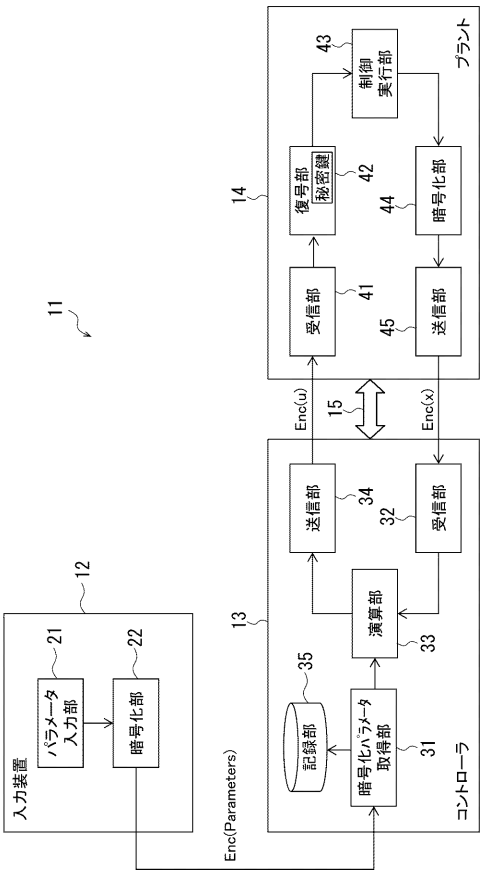
バス１０４には、さらに、入出力インタフェース１０５が接続されている。入出力インタフェース１０５には、キーボード、マウス、マイクロホンなどよりなる入力部１０６、ディスプレイ、スピーカなどよりなる出力部１０７、ハードディスクや不揮発性のメモリなどよりなる記憶部１０８、ネットワークインタフェースなどよりなる通信部１０９、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどのリムーバブルメディア１１１を駆動するドライブ１１０が接続されている。

【０１２５】

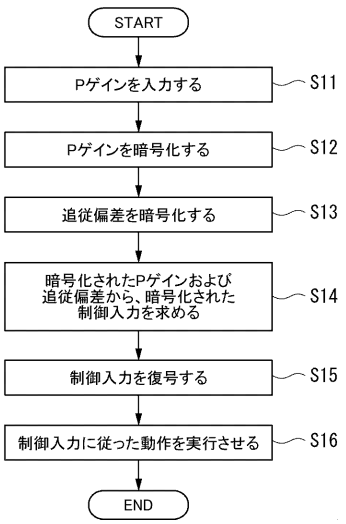
以上のように構成されるコンピュータでは、CPU１０１が、例えば、記憶部１０８に記憶されているプログラムを、入出力インタフェース１０５及びバス１０４を介して、RAM１０３にロードして実行することにより、上述した一連の処理が行われる。

【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。
【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。
【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

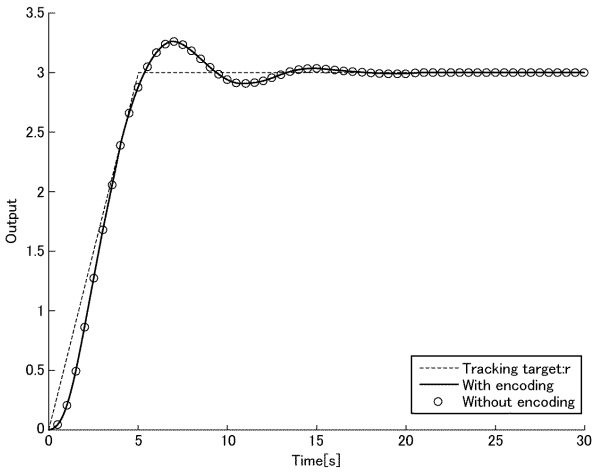
【図１】
図1



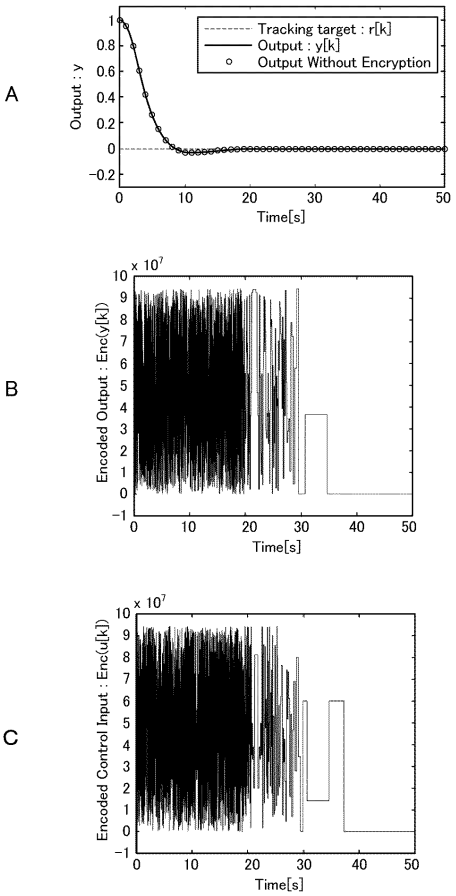
【図２】
図2



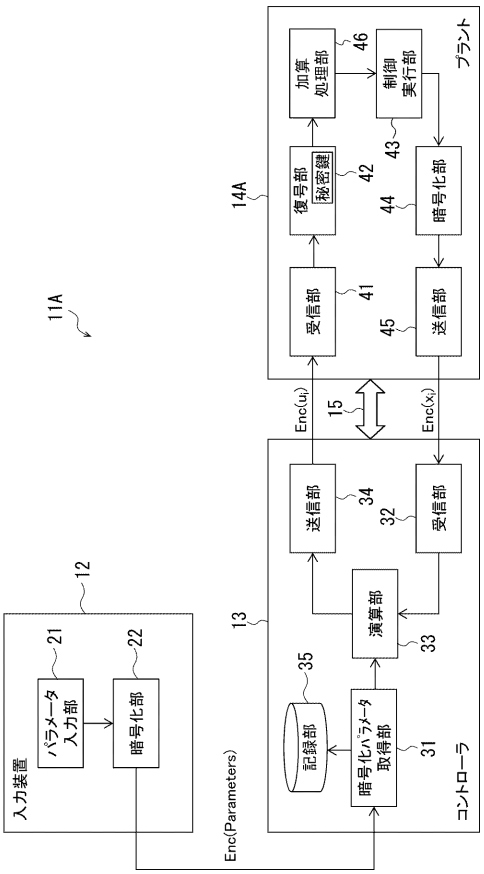
【図３】
図3



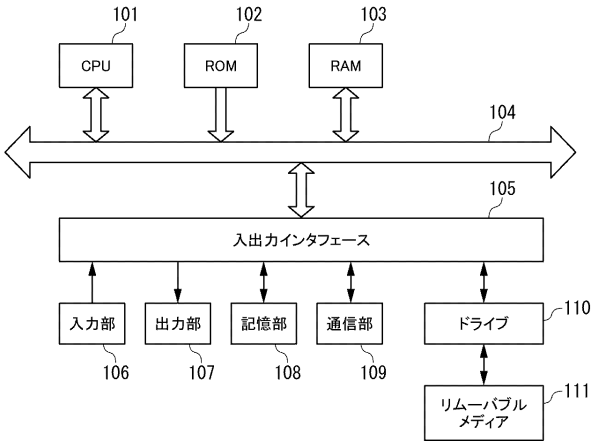
【図４】
図4



【図５】
図5



【図６】
図6



フロントページの続き

(56)参考文献 特開２００８－０６７１６２（ＪＰ，Ａ）
特開２００２－２７６８４９（ＪＰ，Ａ）
特開２０１４－１２６８６５（ＪＰ，Ａ）
特表２０１６－５０８３２３（ＪＰ，Ａ）
伯田恵輔，他，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，計測自動制御学会，２０１４年１０月１０日，第５３巻，第１０号，ｐｐ．９３６－９４２
南裕樹，PID制御，システム情報制御学会誌 システム／制御／情報，システム情報制御学会，２０１２年 4月１５日，第５６巻，第４号，ｐｐ．３４－３７

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ 1／００
Ｈ０４Ｌ 9／００－ 9／３８
Ｇ０５Ｂ １３／０２
Ｇ０６Ｆ ２１／３２