(19)日本国特許庁(JP)

再 公 表 特 許(A1)

(11)国際公開番号
WO2019/078343

発行日　令和2年11月12日(2020.11.12)

(43)国際公開日　平成31年4月25日(2019.4.25)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/14	(2006.01)	H04L	9/00	641	
G09C	1/00	(2006.01)	G09C	1/00	620Z	

審査請求 未請求　予備審査請求 未請求　（全 33 頁）

出願番号　特願2019-548817(P2019-548817)
(21)国際出願番号　PCT/JP2018/038954
(22)国際出願日　平成30年10月19日(2018.10.19)
(31)優先権主張番号　特願2017-203513(P2017-203513)
(32)優先日　平成29年10月20日(2017.10.20)
(33)優先権主張国・地域又は機関
日本国(JP)

(71)出願人　504133110
国立大学法人電気通信大学
東京都調布市調布ケ丘一丁目５番地１
(74)代理人　110000925
特許業務法人信友国際特許事務所
(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　鈴木　崇司
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

最終頁に続く

(54)【発明の名称】暗号化制御システム、暗号化制御方法及び暗号化制御プログラム

(57)【要約】
暗号鍵が漏洩するリスクをより低減させることができる、暗号化制御システム、暗号化制御方法及び暗号化制御プログラムを提供する。入力装置、プラント側制御装置及びコントローラには、共通の機能を有する擬似乱数算出部を装備して、時刻同期を行う。そして、同一時刻で同期運転を開始する。このように暗号化制御システムを構成することで、制御システム全体の制御周期に同期して、公開鍵と秘密鍵のペアを切り替えることが可能になる。よって、制御システムに対する、悪意ある第三者による介入を瞬時に且つ明確に検出することが可能になる。

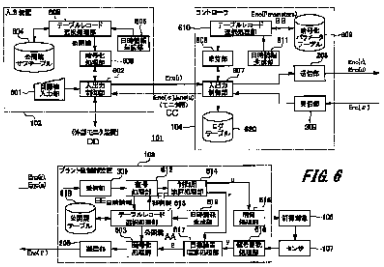


FIG. 6

102 Input device
103 Plant-side control device
104 Controller
106 Object to be controlled
107 Sensor
208 Transmission unit
309 Reception unit
601 Target value input unit
602, 607 Input/output control unit
603 Encryption processing unit
604 Public key sub-table
605, 610, 613 Table record selection processing unit
606, 611, 616 Date and time information generation unit
608 Multiplication unit
609 Encryption parameter table
612 Decryption processing unit
614 Control arithmetic processing unit
615 Control processing unit
616 Signal conversion processing unit
617 Target error arithmetic processing unit
618 Public key table
620 Log table
AAPublic key
BBEnc(Parameters)
CC For monitor
DD External monitor device
EEDate and time information
FF Private key

【特許請求の範囲】
【請求項１】
コントローラと、プラント側制御装置を有する暗号化制御システムであり、
前記コントローラは、
目標値を公開鍵で暗号化して暗号化目標値を出力する第一の暗号化処理部と、
前記第一の暗号化処理部に対し、公開鍵が複数個格納される公開鍵サブテーブルから所定のレコードを選択すると共に、制御システムのパラメータが前記公開鍵サブテーブルの公開鍵によって暗号化された暗号化パラメータが記録されたレコードよりなる暗号化パラメータテーブルから所定のレコードを選択する第一のテーブルレコード選択処理部と、
前記プラント側制御装置から暗号化目標誤差を受信して、前記第一のテーブルレコード選択処理部が選択した前記暗号化パラメータを乗算して暗号化制御入力を出力する乗算部と、
前記乗算部から出力される前記暗号化制御入力に付加する日時情報を提供すると共に、前記第一のテーブルレコード選択処理部に日時情報を提供すると共に起動タイミングを与える第一の日時情報生成部と
を具備し、
前記プラント側制御装置は、
前記コントローラから受信した前記暗号化目標値を復号して目標値を得ると共に、前記コントローラから受信した前記暗号化制御入力を復号して制御入力を得る復号処理部と、
前記制御入力に基づいて所定の制御対象を制御する制御処理部と、
前記制御対象を観測するセンサから観測値を取得する信号変換処理部と、
前記目標値から前記観測値を減算して目標誤差を算出する目標誤差演算処理部と、
前記目標誤差を暗号化して暗号化目標誤差を出力する第二の暗号化処理部と、
前記復号処理部に対し、公開鍵と前記公開鍵の対になる秘密鍵が複数個格納される公開鍵テーブルから所定のレコードを選択すると共に、前記第二の暗号化処理部に対し、前記公開鍵テーブルから所定のレコードを選択する第二のテーブルレコード選択処理部と、
前記第二の暗号化処理部から出力される前記暗号化目標誤差に付加する日時情報を提供すると共に、前記第二のテーブルレコード選択処理部に起動タイミングを与える第二の日時情報生成部と
を具備し、
前記第一の日時情報生成部と、前記第二の日時情報生成部は、相互に同時に起動タイミングを生成するものである、
暗号化制御システム。
【請求項２】
入力装置と、コントローラと、プラント側制御装置を有する暗号化制御システムであり、
前記入力装置は、
目標値を公開鍵で暗号化して暗号化目標値を出力する第一の暗号化処理部と、
前記第一の暗号化処理部に対し、公開鍵が複数個格納される公開鍵サブテーブルから所定のレコードを選択する第一のテーブルレコード選択処理部と、
前記第一のテーブルレコード選択処理部に日時情報を提供すると共に起動タイミングを与える第一の日時情報生成部と
を具備し、
前記コントローラは、
制御システムのパラメータが前記公開鍵サブテーブルの公開鍵によって暗号化された暗号化パラメータが記録されたレコードよりなる暗号化パラメータテーブルから所定のレコードを選択する第二のテーブルレコード選択処理部と、
前記プラント側制御装置から暗号化目標誤差を受信して、前記第二のテーブルレコード選択処理部が選択した前記暗号化パラメータを乗算して暗号化制御入力を出力する乗算部と、

前記乗算部から出力される前記暗号化制御入力に付加する日時情報を提供すると共に、前記第二のテーブルレコード選択処理部に起動タイミングを与える第二の日時情報生成部と
を具備し、
前記プラント側制御装置は、
前記入力装置から受信した前記暗号化目標値を復号して目標値を得ると共に、前記コントローラから受信した前記暗号化制御入力を復号して制御入力を得る復号処理部と、
前記制御入力に基づいて所定の制御対象を制御する制御処理部と、
前記制御対象を観測するセンサから観測値を取得する信号変換処理部と、
前記目標値から前記観測値を減算して目標誤差を算出する目標誤差演算処理部と、
前記目標誤差を暗号化して暗号化目標誤差を出力する第二の暗号化処理部と、
前記復号処理部に対し、公開鍵と前記公開鍵の対になる秘密鍵が複数個格納される公開鍵テーブルから所定のレコードを選択すると共に、前記第二の暗号化処理部に対し、前記公開鍵テーブルから所定のレコードを選択する第三のテーブルレコード選択処理部と、
前記第二の暗号化処理部から出力される前記暗号化目標誤差に付加する日時情報を提供すると共に、前記第三のテーブルレコード選択処理部に起動タイミングを与える第三の日時情報生成部と
を具備し、
前記第一の日時情報生成部と、前記第二の日時情報生成部と、前記第三の日時情報生成部は、相互に同時に起動タイミングを生成するものである、
暗号化制御システム。
【請求項３】
前記第一のテーブルレコード選択処理部と、前記第二のテーブルレコード選択処理部と、前記第三のテーブルレコード選択処理部は、同一の初期値を与えられ、所定の周期に同一の演算処理を行い、前記公開鍵サブテーブルと、前記暗号化パラメータテーブルと、前記公開鍵テーブルのレコード番号に相当する整数を出力する擬似乱数算出部を具備する、請求項２に記載の暗号化制御システム。
【請求項４】
入力装置から暗号化目標値を含む第一のデータフレームを受信する暗号化目標値受信ステップと、
前記第一のデータフレームに付されているエンコード日時フィールドから第一のエンコード日時情報を読み出し、前記第一のエンコード日時情報から始動日時情報を減算し、所定の周期で除算することで暗号化目標値ステップ数を算出する、暗号化目標値ステップ数算出ステップと、
前記暗号化目標値ステップ数に基づいて第一の擬似乱数を算出し、公開鍵と前記公開鍵の対になる秘密鍵が複数個格納される公開鍵テーブルのレコード番号を前記第一の擬似乱数に基づいて指定して、選択したレコードに格納されている前記秘密鍵を用いて前記暗号化目標値を復号する、暗号化目標値復号ステップと
を有する、暗号化制御方法。
【請求項５】
更に、
コントローラから暗号化パラメータを含む第二のデータフレームを受信する暗号化パラメータ受信ステップと、
前記第二のデータフレームに付されているエンコード日時フィールドから第二のエンコード日時情報を読み出し、前記第二のエンコード日時情報から始動日時情報を減算し、所定の周期で除算することで暗号化パラメータステップ数を算出する、暗号化パラメータステップ数算出ステップと、
前記暗号化パラメータステップ数に基づいて第二の擬似乱数を算出し、前記公開鍵テーブルのレコード番号を前記第二の擬似乱数に基づいて指定して、選択したレコードに格納されている前記秘密鍵を用いて前記暗号化パラメータを復号する、暗号化パラメータ復号

ステップと、
前記暗号化パラメータ復号ステップにおいて復号された前記暗号化パラメータの値に所定の演算処理を施して制御入力を得る制御用演算処理ステップと、
前記制御入力に基づいて制御対象が制御され、前記制御対象を観測したセンサから得られた観測値を前記目標値から減算して、目標誤差を得る目標誤差演算処理ステップと、
前記暗号化パラメータステップ数算出ステップにて算出した前記暗号化パラメータステップ数に１を加算した新たなステップ数に基づいて第三の擬似乱数を算出し、前記公開鍵テーブルのレコード番号を前記第三の擬似乱数に基づいて指定して、選択したレコードに格納されている前記公開鍵を用いて前記目標誤差を暗号化する、目標誤差暗号化処理ステップと、
前記目標誤差に、現在日時情報を格納するエンコード日時フィールドと、始動日時情報を格納する始動日時フィールドを付加して、第三のデータフレームを前記コントローラに送信する、暗号化目標誤差送信ステップと
を有する、請求項４に記載の暗号化制御方法。
【請求項６】
計算機に、
入力装置から暗号化目標値を含む第一のデータフレームを受信する暗号化目標値受信ステップと、
前記第一のデータフレームに付されているエンコード日時フィールドから第一のエンコード日時情報を読み出し、前記第一のエンコード日時情報から始動日時情報を減算し、所定の周期で除算することで暗号化目標値ステップ数を算出する、暗号化目標値ステップ数算出ステップと、
前記暗号化目標値ステップ数に基づいて第一の擬似乱数を算出し、公開鍵と前記公開鍵の対になる秘密鍵が複数個格納される公開鍵テーブルのレコード番号を前記第一の擬似乱数に基づいて指定して、選択したレコードに格納されている前記秘密鍵を用いて前記暗号化目標値を復号する、暗号化目標値復号ステップと
を実行させる、暗号化制御プログラム。
【請求項７】
更に、
コントローラから暗号化パラメータを含む第二のデータフレームを受信する暗号化パラメータ受信ステップと、
前記第二のデータフレームに付されているエンコード日時フィールドから第二のエンコード日時情報を読み出し、前記第二のエンコード日時情報から始動日時情報を減算し、所定の周期で除算することで暗号化パラメータステップ数を算出する、暗号化パラメータステップ数算出ステップと、
前記暗号化パラメータステップ数に基づいて第二の擬似乱数を算出し、前記公開鍵テーブルのレコード番号を前記第二の擬似乱数に基づいて指定して、選択したレコードに格納されている前記秘密鍵を用いて前記暗号化パラメータを復号する、暗号化パラメータ復号ステップと、
前記暗号化パラメータ復号ステップにおいて復号された前記暗号化パラメータの値に所定の演算処理を施して制御入力を得る制御用演算処理ステップと、
前記制御入力に基づいて制御対象が制御され、前記制御対象を観測したセンサから得られた観測値を前記目標値から減算して、目標誤差を得る目標誤差演算処理ステップと、
前記暗号化パラメータステップ数算出ステップにて算出した前記暗号化パラメータステップ数に１を加算した新たなステップ数に基づいて第三の擬似乱数を算出し、前記公開鍵テーブルのレコード番号を前記第三の擬似乱数に基づいて指定して、選択したレコードに格納されている前記公開鍵を用いて前記目標誤差を暗号化する、目標誤差暗号化処理ステップと、
前記目標誤差に、現在日時情報を格納するエンコード日時フィールドと、始動日時情報を格納する始動日時フィールドを付加して、第三のデータフレームを前記コントローラに

送信する、暗号化目標誤差送信ステップと
を実行させる、請求項６に記載の暗号化制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号化制御システム、暗号化制御方法及び暗号化制御プログラムに関する。
【背景技術】
【０００２】
近年、インターネット等の情報技術の発達に伴い、電気、ガス、水道等の、国民生活を支えるインフラストラクチャ（Infrastructure：社会基盤）、あるいは工場や発電所等の工業施設を制御する制御システムにおいて、情報技術を応用したネットワーク化が進んでいる。このような制御システムのネットワーク化やＩＣＴ（Information and Communication Technology）の進化により、制御システムには処理速度の向上、処理内容の高度化等の多大な恩恵がもたらされる。その一方で、制御システムのネットワーク化には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】
このような背景により、重要なインフラストラクチャ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、制御システムに対して情報系セキュリティ技術を転用する他、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】
特許文献１には、本発明の発明者を一部含む、暗号化制御システムの技術が開示されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１６－９０８８４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
発明者は、特許文献１において、制御システムの中核部分に当たるコントローラが暗号化された入力データ及び出力データに対して直接演算処理を施すことで、コントローラに公開鍵及び／または秘密鍵を不要にした制御システムの実現に成功した。この発明により、制御システムはプラントにのみ秘密鍵を装備すればよいこととなり、公開鍵及び／または秘密鍵が漏洩するリスクを低減させることを実現した。
しかしながら、特許文献１に使用される公開鍵と秘密鍵のペアは１組だけである。このため、クラウドコンピューティング等の膨大な計算機資源を用いると暗号を解読されてしまう虞がある。
【０００７】
本発明は係る課題を解決し、暗号鍵が漏洩するリスクをより低減させることができる、暗号化制御システム、暗号化制御方法及び暗号化制御プログラムを提供することを目的とする。
【課題を解決するための手段】
【０００８】
上記課題を解決するために、本発明の暗号化制御システムは、コントローラと、プラント側制御装置を有する。
コントローラは、目標値を公開鍵で暗号化して暗号化目標値を出力する第一の暗号化処理部と、目標値を公開鍵で暗号化して暗号化目標値を出力する第一の暗号化処理部と、
第一の暗号化処理部に対し、公開鍵が複数個格納される公開鍵サブテーブルから所定のレ

コードを選択すると共に、制御システムのパラメータが公開鍵サブテーブルの公開鍵によって暗号化された暗号化パラメータが記録されたレコードよりなる暗号化パラメータテーブルから所定のレコードを選択する第一のテーブルレコード選択処理部と、プラント側制御装置から暗号化目標誤差を受信して、第一のテーブルレコード選択処理部が選択した暗号化パラメータを乗算して暗号化制御入力を出力する乗算部と、乗算部から出力される暗号化制御入力に付加する日時情報を提供すると共に、第一のテーブルレコード選択処理部に起動タイミングを与える第二の日時情報生成部とを具備する。

プラント側制御装置は、コントローラから受信した暗号化目標値を復号して目標値を得ると共に、コントローラから受信した暗号化制御入力を復号して制御入力を得る復号処理部と、制御入力に基づいて所定の制御対象を制御する制御処理部とを具備する。更に、制御対象を観測するセンサから観測値を取得する信号変換処理部と、目標値から観測値を減算して目標誤差を算出する目標誤差演算処理部と、目標誤差を暗号化して暗号化目標誤差を出力する第二の暗号化処理部と、復号処理部に対し、公開鍵と公開鍵の対になる秘密鍵が複数個格納される公開鍵テーブルから所定のレコードを選択すると共に、第二の暗号化処理部に対し、公開鍵テーブルから所定のレコードを選択する第二のテーブルレコード選択処理部と、第二の暗号化処理部から出力される暗号化目標誤差に付加する日時情報を提供すると共に、第二のテーブルレコード選択処理部に起動タイミングを与える第二の日時情報生成部とを具備する。

そして、第一の日時情報生成部と、第二の日時情報生成部は、相互に同時に起動タイミングを生成するものである。

【発明の効果】

【０００９】

本発明によれば、暗号鍵が漏洩するリスクをより低減させることができる、暗号化制御システム、暗号化制御方法及び暗号化制御プログラムを提供することができる。

上記した以外の課題、構成及び効果は、以下の実施形態の説明により明らかにされる。

【図面の簡単な説明】

【００１０】

【図１】本発明の実施形態に係る、暗号化制御システムの全体構成を示す概略図である。

【図２】入力装置のハードウェア構成を示すブロック図である。

【図３】コントローラのハードウェア構成を示すブロック図である。

【図４】プラント側制御装置のハードウェア構成を示すブロック図である。

【図５】日時情報源装置のハードウェア構成を示すブロック図である。

【図６】暗号化制御システムの、制御ネットワークにおけるソフトウェア機能を示すブロック図である。

【図７】暗号化制御システムの、情報ネットワークにおけるソフトウェア機能を示すブロック図である。

【図８】公開鍵テーブル、公開鍵サブテーブル及び暗号化パラメータテーブルのフィールド構成を示す表である。

【図９】入力装置とコントローラのテーブルレコード選択処理部のソフトウェア機能と、プラント側制御装置の暗号化目標値におけるテーブルレコード選択処理部のソフトウェア機能を説明するブロック図である。

【図１０】プラント側制御装置の暗号化制御入力におけるテーブルレコード選択処理部のソフトウェア機能を説明するブロック図である。

【図１１】コントローラの日時情報生成部における、同期運転開始処理の流れを示すフローチャートである。

【図１２】コントローラの擬似乱数算出部の動作の流れを示すフローチャートである。

【図１３】暗号化制御システムの同期運転を説明するタイムチャートである。

【図１４】特許文献１に係る暗号化制御システムと、本発明の実施形態に係る暗号化制御システムにおける、制御入力uと目標誤差εのグラフである。

【図１５】特許文献１に係る暗号化制御システムと、本発明の実施形態に係る暗号化制御

システムにおける、攻撃検出器のグラフである。
【図１６】本発明の実施形態の変形例に係るコントローラの、制御ネットワークにおけるソフトウェア機能を示すブロック図である。
【発明を実施するための形態】
【００１１】
［暗号化制御システム１０１の実施形態］
図１は、本発明の実施形態に係る、暗号化制御システム１０１の全体構成を示す概略図である。なお、これ以降の説明において、暗号化された値をEnc()という関数で示す。
暗号化制御システム１０１は、入力装置１０２と、プラント側制御装置１０３と、コントローラ１０４と、日時情報源装置１０５を有する。
入力装置１０２は、コントローラ１０４を通じて、プラント側制御装置１０３に対し、目標値rを公開鍵暗号で暗号化した暗号化目標値Enc(r)を送信する。
プラント側制御装置１０３には、制御対象１０６とセンサ１０７が接続されている。プラント側制御装置１０３は、制御対象１０６に制御信号を与え、センサ１０７から制御対象１０６の状態情報である観測値yを取得する。そして、コントローラ１０４と第二制御ネットワークＬ１０９で接続され、暗号化制御情報の送受信を行う。
【００１２】
コントローラ１０４は、入力装置１０２と第一制御ネットワークＬ１０８で接続されると共に、プラント側制御装置１０３と第二制御ネットワークＬ１０９で接続される。コントローラ１０４は入力装置１０２から第一制御ネットワークＬ１０８を通じて暗号化目標値Enc(r)を受信し、プラント側制御装置１０３から第二制御ネットワークＬ１０９を通じて暗号化目標誤差Enc(ε)を受信する。そして、暗号化されたこれら情報を暗号化されたまま復号せずに所定の演算処理を行い、第二制御ネットワークＬ１０９を通じてプラント側制御装置１０３へ演算結果である暗号化制御入力Enc(u)を送信する。
【００１３】
本発明の実施形態に係る暗号化制御システム１０１において使用する公開鍵暗号は、特許文献１に開示されるものと同じく、例えばＲＳＡ暗号（Rivest Shamir Adleman）等の、準同型性を持つ公開鍵暗号を使用する。準同型性を持つ公開鍵暗号は、２つの暗号化した値同士を復号せずにそのまま乗算し、乗算した値を復号することで、暗号化される前の値を乗算した値と一致させることが可能である。
公開鍵暗号の準同型性に関する説明は特許文献１に記載されており、本発明の実施形態に係る暗号化制御システム１０１では公開鍵及び秘密鍵のペアを複数個使用する以外は、公開鍵暗号自体の演算処理には何も変更がないので、公開鍵暗号自体の詳細な説明は割愛する。
【００１４】
入力装置１０２、コントローラ１０４、プラント側制御装置１０３はそれぞれ情報ネットワークＬ１１０を通じて、日時情報源装置１０５に接続される。日時情報源装置１０５は、ネットワークＯＳとＮＴＰサーバ（Network Time Protocol）及びＮＴＰクライアントが稼働するパソコンやサーバである。
第一制御ネットワークＬ１０８及び第二制御ネットワークＬ１０９はデータ転送の確実性を重視したネットワークであり、様々な種類のネットワークインターフェースが利用可能である。
一方、情報ネットワークＬ１１０は制御ネットワーク程の確実性は要求されない。本発明の実施形態では、周知のＴＣＰ／ＩＰを使用するものとする。
【００１５】
入力装置１０２、コントローラ１０４及びプラント側制御装置１０３は、プログラマブルコントローラと呼ばれる装置である。スロットを多数有するケース状のマウントベース１１１に、スロットに収納される大きさのモジュールを、必要な機能に応じて収納する。マウントベース１１１にはモジュール同士を接続するインターフェースが内蔵されており、モジュールをスロットに挿入すると、モジュール間のデータの送受信や適切な電源の供

給が確立される。

【００１６】

入力装置１０２のマウントベース１１１ａには、ＣＰＵモジュール１１２と、情報ネットワークモジュール１１３と、第一制御ネットワークモジュール１１４ａが装着されている。

コントローラ１０４のマウントベース１１１ｂには、ＣＰＵモジュール１１２と、情報ネットワークモジュール１１３と、第一制御ネットワークモジュール１１４ｂと、第二制御ネットワークモジュール１１５が装着されている。

プラント側制御装置１０３のマウントベース１１１ｃには、ＣＰＵモジュール１１２と、情報ネットワークモジュール１１３と、第二制御ネットワークモジュール１１５と、入出力モジュール１１６が装着されている。

入力装置１０２の第一制御ネットワークモジュール１１４ａは送信側であり、コントローラ１０４の第一制御ネットワークモジュール１１４ｂは受信側である。

コントローラ１０４とプラント側制御装置１０３の第二制御ネットワークモジュール１１５は、相互の送信側端子と受信側端子が互いに接続されている。

【００１７】

［入力装置１０２のハードウェア構成］

図２は、入力装置１０２のハードウェア構成を示すブロック図である。

入力装置１０２は、マウントベース１１１に設けられているモジュールバス２０１に接続されているＣＰＵモジュール１１２、情報ネットワークモジュール１１３、第一制御ネットワークモジュール１１４ａを備える。

ＣＰＵモジュール１１２は、内部バス２０６に接続されているＣＰＵ２０２、ＲＯＭ２０３、ＲＡＭ２０４、及び日時情報を生成するＲＴＣ（RealTime Clock）２０５を備える。内部バス２０６はモジュールバス２０１に接続されている。

ＣＰＵモジュール１１２のＲＯＭ２０３には、暗号化制御システム１０１における制御演算処理及び暗号化処理等を遂行するためのプログラムが格納されている。

【００１８】

情報ネットワークモジュール１１３は、内部バス２０６に接続されているＣＰＵ２０２、ＲＯＭ２０３、ＲＡＭ２０４、及びＮＩＣ（Network Interface Card）２０７を備える。内部バス２０６はモジュールバス２０１に接続されている。情報ネットワークモジュール１１３のＲＯＭ２０３には、ネットワークＯＳと、ＮＴＰサーバプログラム及びＮＴＰクライアントプログラム等が格納されている。

第一制御ネットワークモジュール１１４ａは、送信部２０８がモジュールバス２０１に接続されている。

【００１９】

［コントローラ１０４のハードウェア構成］

図３は、コントローラ１０４のハードウェア構成を示すブロック図である。

コントローラ１０４は、マウントベース１１１に設けられているモジュールバス２０１に接続されている、ＣＰＵモジュール１１２、情報ネットワークモジュール１１３、第一制御ネットワークモジュール１１４ｂ、及び第二制御ネットワークモジュール１１５を備える。

ＣＰＵモジュール１１２と情報ネットワークモジュール１１３は、入力装置１０２のものと同じなので説明は割愛する。

第一制御ネットワークモジュール１１４ｂは、受信部３０９がモジュールバス２０１に接続されている。

第二制御ネットワークモジュール１１５は、送信部２０８と受信部３０９が内部バス２０６に接続されている。内部バス２０６はモジュールバス２０１に接続されている。

【００２０】

［プラント側制御装置１０３のハードウェア構成］

図４は、プラント側制御装置１０３のハードウェア構成を示すブロック図である。

プラント側制御装置１０３は、マウントベース１１１に設けられているモジュールバス２０１に接続されている、ＣＰＵモジュール１１２、情報ネットワークモジュール１１３、第二制御ネットワークモジュール１１５、及び入出力モジュール１１６を備える。

ＣＰＵモジュール１１２、情報ネットワークモジュール１１３、第二制御ネットワークモジュール１１５は、コントローラ１０４のものと同じなので説明は割愛する。

入出力モジュール１１６は、内部バス２０６に接続されている、センサ１０７が接続されるＡ／Ｄ変換器４１０と、制御対象１０６が接続されるＤ／Ａ変換器４１１を備える。内部バス２０６はモジュールバス２０１に接続されている。なお、この入出力モジュール１１６はあくまで一例であり、制御対象１０６やセンサ１０７等の接続される対象に応じて、Ａ／Ｄ変換器４１０及びＤ／Ａ変換器４１１に接続される信号処理回路等が必要になる場合がある。

【００２１】

［日時情報源装置１０５のハードウェア構成］

図５は、日時情報源装置１０５のハードウェア構成を示すブロック図である。

サーバ装置やパソコン等で構成される日時情報源装置１０５は、バス５０７に接続されているＣＰＵ５０１、ＲＯＭ５０２、ＲＡＭ５０３、不揮発性ストレージ５０４、ＲＴＣ５０５、及びＮＩＣ５０６を備える。パソコンを流用する場合は、表示部５０８、操作部５０９を備えることもある。

不揮発性ストレージ５０４には、ネットワークＯＳと、ＮＴＰサーバプログラム及びＮＴＰクライアントプログラムが格納されている。

【００２２】

［暗号化制御システム１０１の、制御ネットワークにおけるソフトウェア機能］

図６は、暗号化制御システム１０１の、制御ネットワークにおけるソフトウェア機能を示すブロック図である。図６では紙面の都合上、情報ネットワークＬ１１０の記述を割愛している。情報ネットワークＬ１１０については図７で説明する。

入力装置１０２は、プラント側制御装置１０３に対して、暗号化目標値Enc(r)を生成して、コントローラ１０４を介してプラント側制御装置１０３へ送信する。

目標値入力部６０１は、暗号化されない目標値rを入出力制御部６０２に与える。

入出力制御部６０２は、目標値入力部６０１から入力された目標値rを暗号化処理部６０３に引き渡す。そして、暗号化処理部６０３が生成した暗号化目標値Enc(r)を受け取り、コントローラ１０４へ送信する。

【００２３】

暗号化処理部６０３は、公開鍵サブテーブル６０４からテーブルレコード選択処理部６０５が選択した公開鍵レコードを用いて、入出力制御部６０２から引き取った目標値rに暗号化処理を施す。そして、生成した暗号化目標値Enc(r)を入出力制御部６０２に引き渡す。

テーブルレコード選択処理部６０５は、日時情報生成部６０６から受け取った現在日時情報に基づき、公開鍵サブテーブル６０４のレコード番号（ラベル）を生成する。そして、生成したラベルに相当する公開鍵サブテーブル６０４のレコードに記録されている公開鍵を読み取り、暗号化処理部６０３に引き渡す。

日時情報生成部６０６は、現在日時情報を出力すると共に、テーブルレコード選択処理部６０５に対する起動及び停止制御を行う。

【００２４】

入力装置１０２から第一制御ネットワークモジュール１１４ａのケーブルを通じてコントローラ１０４に送信される暗号化目標値Enc(r)は、コントローラ１０４の入出力制御部６０７に入力される。

入出力制御部６０７は、入力装置１０２から受信した暗号化目標値Enc(r)をそのまま第二制御ネットワークモジュール１１５の送信部２０８を通じて、プラント側制御装置１０３へ送信する。そして、プラント側制御装置１０３から第二制御ネットワークモジュール１１５の受信部３０９を通じて受信した暗号化目標誤差Enc(ε)を、乗算部６０８に引き

渡す。

【００２５】

乗算部６０８は、暗号化パラメータテーブル６０９からテーブルレコード選択処理部６１０が選択した暗号化パラメータEnc(Parameters)を用いて、暗号化目標誤差Enc(ε)と乗算処理を行うことで、暗号化制御入力Enc(u)を算出する。なお、この乗算部６０８における暗号化パラメータEnc(Parameters)と暗号化目標値Enc(r)との乗算処理は、単純な乗算ではなく、特許文献１に開示されている、部分的な乗算処理である。

乗算部６０８は、暗号化パラメータEnc(Parameters)と暗号化目標値Enc(r)との乗算処理によって算出した暗号化制御入力Enc(u)を、入出力制御部６０７に引き渡す。

【００２６】

テーブルレコード選択処理部６１０は、プラント側制御装置１０３から第二制御ネットワークモジュール１１５の受信部３０９を通じて受信したデータフレームに含まれている現在日時情報に基づき、暗号化パラメータテーブル６０９のレコード番号（ラベル）を生成する。そして、生成したラベルに相当する暗号化パラメータテーブル６０９のレコードに記録されている暗号化パラメータを読み取り、乗算部６０８に引き渡す。

日時情報生成部６１１は、現在日時情報を出力すると共に、コントローラ１０４の日時情報生成部６１１から指示された、同期運転開始時点の日時情報（以下「始動日時情報」）も出力する。また、テーブルレコード選択処理部６１０に対する起動及び停止制御を行う。しかし、コントローラ１０４の日時情報生成部６１１が生成する現在日時情報は、入力装置１０２の日時情報生成部６０６とは異なり、テーブルレコード選択処理部６１０が実行する、暗号化パラメータテーブル６０９のラベルの演算には使われない。その代わり、日時情報生成部６１１が生成する現在日時情報は、乗算部６０８から入出力制御部６０７及び送信部２０８を通じて送信される暗号化制御入力Enc(u)のデータフレームのエンコード日時フィールドに、エンコード日時情報として格納される。

【００２７】

コントローラ１０４から第二制御ネットワークモジュール１１５の送信部２０８を通じてプラント側制御装置１０３に送信される暗号化目標値Enc(r)及び暗号化制御入力Enc(u)は、プラント側制御装置１０３の第二制御ネットワークモジュール１１５の受信部３０９を通じて復号処理部６１２に入力される。

復号処理部６１２は、暗号化目標値Enc(r)及び暗号化制御入力Enc(u)を、テーブルレコード選択処理部６１３から取得した秘密鍵を用いて復号する。復号された目標値r及び制御入力uの基となる値は、制御用演算処理部６１４に引き渡される。

【００２８】

制御用演算処理部６１４は、目標値r及び制御入力uの基となる値を演算して、目標値r及び制御入力uを生成する。制御入力uは制御処理部６１５に引き渡される。

制御処理部６１５は、制御入力uから制御信号を生成し、制御対象１０６を制御する。例えば、制御対象１０６がモータであるならば、制御処理部６１５は、モータに与える電圧や位相等を制御する。制御対象１０６が制御処理部６１５によって制御されると、制御対象１０６の動作はセンサ１０７によって検出される。

センサ１０７が出力する観測信号は、信号変換処理部６１６によって観測値yに変換される。信号変換処理部６１６が出力する観測値yは、制御用演算処理部６１４が出力する目標値rと共に目標誤差演算処理部６１７に入力される。目標誤差演算処理部６１７は、目標値rから観測値yを減算して、目標誤差εを出力する。

目標誤差εは、暗号化処理部６０３によって暗号化され、暗号化目標誤差Enc(ε)に変換される。暗号化目標誤差Enc(ε)は、第二制御ネットワークモジュール１１５の送信部２０８を通じて、コントローラ１０４へ送信される。

【００２９】

テーブルレコード選択処理部６１３は、コントローラ１０４から第二制御ネットワークモジュール１１５の受信部３０９を通じて受信したデータフレームに含まれている現在日時情報及び始動日時情報に基づき、公開鍵テーブル６１８のレコード番号（ラベル）を生

成する。そして、生成したラベルに相当する公開鍵テーブル６１８のレコードに記録されている秘密鍵を読み取り、復号処理部６１２に引き渡す。また同様に、生成したラベルに相当する公開鍵テーブル６１８のレコードに記録されている公開鍵を読み取り、暗号化処理部６０３に引き渡す。

【００３０】

日時情報生成部６１９は、現在日時情報を出力すると共に、コントローラ１０４の日時情報生成部６１１から指示された、同期運転開始時点の日時情報（以下「始動日時情報」）も出力する。また、日時情報生成部６１９は、テーブルレコード選択処理部６１０に対する起動及び停止制御を行う。しかし、プラント側制御装置１０３の日時情報生成部６１９が生成する現在日時情報は、入力装置１０２の日時情報生成部６０６とは異なり、テーブルレコード選択処理部６１３が実行する、公開鍵テーブル６１８のラベルの演算には使われない。その代わり、日時情報生成部６１９が生成する現在日時情報は、暗号化処理部６０３から送信部２０８を通じて送信される暗号化目標誤差Enc(ε)のデータフレームのエンコード日時フィールドに、エンコード日時情報として格納される。

【００３１】

なお、入力装置１０２の入出力制御部６０２は、必要に応じて図示しない外部モニタ装置が接続されることがある。暗号化制御システム１０１の監視作業者は、外部モニタ装置を入力装置１０２に接続して、所定の監視業務等を遂行する。

コントローラ１０４の入出力制御部６０７には、暗号化目標値Enc(r)、暗号化制御入力Enc(u)、暗号化目標誤差Enc(ε)等を暗号化されたまま記録するログテーブル６２０が設けられ、監視業務に利用される。

【００３２】

［暗号化制御システム１０１の、情報ネットワークＬ１１０におけるソフトウェア機能］

図７は、暗号化制御システム１０１の、情報ネットワークＬ１１０におけるソフトウェア機能を示すブロック図である。

入力装置１０２の日時情報生成部６０６と、コントローラ１０４の日時情報生成部６１１と、プラント側制御装置１０３の日時情報生成部６１９は、情報ネットワークＬ１１０を通じて日時情報源装置１０５に接続される。

入力装置１０２の日時情報生成部６０６と、コントローラ１０４の日時情報生成部６１１と、プラント側制御装置１０３の日時情報生成部６１９は、日時情報源装置１０５と同様に、ネットワークＯＳと、ＮＴＰサーバプログラム及びＮＴＰクライアントプログラムの機能を有しており、各々の日時情報生成部６０６は日時情報源装置１０５の日時情報に同期する。

更に、入力装置１０２の日時情報生成部６０６と、コントローラ１０４の日時情報生成部６１１と、プラント側制御装置１０３の日時情報生成部６１９のうちのどれか一つは、同期運転の開始を指揮するマスター（master）の役割を担い、残り二つは、マスターの指示に従って同期運転を実行するスレーヴ（slave）の役割を担う。

【００３３】

［テーブルのフィールド構成］

図８は、公開鍵テーブル６１８、公開鍵サブテーブル６０４及び暗号化パラメータテーブル６０９のフィールド構成を示す表である。

公開鍵テーブル６１８は、レコード番号フィールドと、公開鍵フィールドと、秘密鍵フィールドを有する。

レコード番号フィールドは、１から始まる整数が格納される。このレコード番号は、公開鍵テーブル６１８のレコードを一意に識別する番号であり、ラベルとも呼ばれる。

公開鍵フィールドは、公開鍵暗号方式の、所望の値を暗号化するための公開鍵が格納される。

秘密鍵フィールドは、公開鍵暗号方式の、暗号化された所望の値を復号するための、公開鍵フィールドの公開鍵と対になる秘密鍵が格納される。

【００３４】

公開鍵サブテーブル６０４は、レコード番号フィールドと、公開鍵フィールドを有する。

すなわち、公開鍵サブテーブル６０４は、公開鍵テーブル６１８から秘密鍵フィールドを削除した、公開鍵テーブル６１８のサブセットである。

【００３５】

暗号化パラメータテーブル６０９は、レコード番号フィールドと、暗号化第一パラメータフィールドと、暗号化第二パラメータフィールドと、暗号化第三パラメータフィールドを有する。

暗号化第一パラメータフィールドには、制御システムのゲインとなる第一パラメータKpを暗号化した暗号化第一パラメータEnc(Kp)が格納される。

暗号化第二パラメータフィールドには、制御システムのゲインとなる第二パラメータKiを暗号化した暗号化第二パラメータEnc(Ki)が格納される。

暗号化第三パラメータフィールドには、制御システムのゲインとなる第三パラメータKdを暗号化した暗号化第三パラメータEnc(Kd)が格納される。

第一パラメータKp、第二パラメータKi及び第三パラメータKdは制御システムにおいて不変の値であり、制御システムの設計時に所定の計算にて決定される。

なお、上記の第一パラメータKp、第二パラメータKi及び第三パラメータKdは、ＰＩＤ制御を想定しているが、制御システムはＰＩＤ制御に限らない。暗号化パラメータテーブル６０９は、制御システムが要求するパラメータの数に応じて、暗号化パラメータのフィールドが設けられる。

【００３６】

暗号化パラメータテーブル６０９のレコード番号フィールドが「１」のレコードにおける暗号化第一パラメータフィールドには、第一パラメータKpを、公開鍵テーブル６１８のレコード番号フィールドが「１」のレコードにおける公開鍵フィールドに格納されている公開鍵を用いて暗号化された、暗号化第一パラメータEnc(Kp)が格納される。

同様に、暗号化パラメータテーブル６０９のレコード番号フィールドが「１」のレコードにおける暗号化第二パラメータフィールドには、第二パラメータKiを、公開鍵テーブル６１８のレコード番号フィールドが「１」のレコードにおける公開鍵フィールドに格納されている公開鍵を用いて暗号化された、暗号化第二パラメータEnc(Ki)が格納される。

同様に、暗号化パラメータテーブル６０９のレコード番号フィールドが「１」のレコードにおける暗号化第三パラメータフィールドには、第三パラメータKdを、公開鍵テーブル６１８のレコード番号フィールドが「１」のレコードにおける公開鍵フィールドに格納されている公開鍵を用いて暗号化された、暗号化第三パラメータEnc(Kd)が格納される。

【００３７】

暗号化パラメータテーブル６０９のレコード番号フィールドが「２」のレコードにおける暗号化第一パラメータフィールドには、第一パラメータKpを、公開鍵テーブル６１８のレコード番号フィールドが「２」のレコードにおける公開鍵フィールドに格納されている公開鍵を用いて暗号化された、暗号化第一パラメータEnc(Kp)が格納される。

以下同様に、暗号化パラメータテーブル６０９における各レコードの暗号化パラメータは、各レコードのレコード番号フィールドに紐付く公開鍵テーブル６１８の公開鍵フィールドに格納されている公開鍵で暗号化されている。

【００３８】

［テーブルレコード選択処理部６０５］

図９Ａは、入力装置１０２のテーブルレコード選択処理部６０５のソフトウェア機能を説明するブロック図である。

日時情報生成部６０６が出力する現在日時情報は、同期運転開始時点に記憶していた始動日時情報９０１と共に、ステップ数算出部９０２に入力される。ステップ数算出部９０２は、現在日時情報から始動日時情報９０１を減算し、ステップ時間で除算して、ステップ数を算出する。例えば、ステップ時間が１０ｍｓｅｃ、現在日時情報が２０１７年１１月１日０９時３０分０５．１００秒、始動日時情報９０１が２０１７年１１月１日０９時

３０分０５．０００秒である場合、ステップ数は１００÷１０＝１０である。なお、ステップ時間は、制御対象１０６の制御周期と一致する。

【００３９】

産業機器等では、ある制御周期で計測と制御に係る制御プログラムを実行する。そこで、本発明の実施形態に係る暗号化制御システムでは、制御プログラムの始動日時を０として、制御周期毎にステップ数を計数する。このステップ数は、後述する擬似乱数算出部９０３に利用される。また、図１３で詳述するが、プラント側制御装置１０３では、受信するデータと送信するデータとの間で、ステップ数が「１」だけ進む。

【００４０】

ステップ数算出部９０２が出力するステップ数は、擬似乱数算出部９０３に入力される。擬似乱数算出部９０３は、初期値９０４を与えられ、確定的な演算処理を入力されるステップ数だけ繰り返すことで、０以上の整数または自然数の擬似乱数を生成する。生成した擬似乱数は、公開鍵サブテーブル６０４のレコード数にて剰余演算が行われ、この剰余がラベル、すなわちレコード番号となる。擬似乱数算出部９０３はラベルを用いて公開鍵サブテーブル６０４の公開鍵フィールドを読み出し、公開鍵を暗号化処理部６０３へ出力する。なお、レコード番号を０から始めるか（０以上の整数）１から始めるか（自然数）は設計事項である。

入力装置１０２、コントローラ１０４、そしてプラント側制御装置１０３のテーブルレコード選択処理部６０５に同一の演算処理を行う擬似乱数算出部９０３を装備して、同一の初期値９０４を与える。これにより、同一のステップ数を与えられた各々の擬似乱数算出部９０３は、同一のラベルを出力する。

【００４１】

図９Ｂは、コントローラ１０４のテーブルレコード選択処理部６１０のソフトウェア機能を説明するブロック図である。

プラント側制御装置１０３から受信したデータフレームＤ９０５には、暗号化目標誤差Enc(ε)の他に、始動日時フィールドと、エンコード日時フィールドが付されている。

エンコード日時フィールドに含まれているエンコード日時情報と、始動日時フィールドに含まれている始動日時情報９０１は、ステップ数算出部９０２に入力される。ステップ数算出部９０２は、エンコード日時情報から始動日時情報９０１を減算し、ステップ時間で除算して、ステップ数を算出する。すなわち、コントローラ１０４におけるステップ数算出部９０２の処理は、入力装置１０２のステップ数算出部９０２と、入力されるデータが異なる以外は、演算処理自体は全く同じである。

【００４２】

ステップ数算出部９０２が出力するステップ数は、擬似乱数算出部９０３に入力される。擬似乱数算出部９０３は、初期値９０４を与えられ、確定的な演算処理を入力されるステップ数だけ繰り返すことで、０以上の整数または自然数の擬似乱数を生成する。生成した擬似乱数は、暗号化パラメータテーブル６０９のレコード数にて剰余演算が行われ、この剰余がラベル、すなわちレコード番号となる。擬似乱数算出部９０３はラベルを用いて暗号化パラメータテーブル６０９の暗号化第一パラメータフィールド、暗号化第二パラメータフィールド及び暗号化第三パラメータフィールドを読み出し、暗号化第一パラメータ、暗号化第二パラメータ及び暗号化第三パラメータを乗算部６０８へ出力する。

【００４３】

図９Ｃは、プラント側制御装置１０３の、暗号化目標値におけるテーブルレコード選択処理部６１３のソフトウェア機能を説明するブロック図である。

入力装置１０２からコントローラ１０４を通じて受信したデータフレームＤ９０６には、暗号化目標値Enc(r)の他に、エンコード日時フィールドが付されている。

エンコード日時フィールドに含まれているエンコード日時情報は、同期運転開始時点に記憶していた始動日時情報９０１と共に、ステップ数算出部９０２に入力される。ステップ数算出部９０２は、エンコード日時情報から始動日時情報９０１を減算し、ステップ時間で除算して、ステップ数を算出する。すなわち、プラント側制御装置１０３の、暗号化

目標値におけるステップ数算出部９０２の処理は、入力装置１０２のステップ数算出部９０２と、入力されるデータが異なる以外は、演算処理自体は全く同じである。

【００４４】

ステップ数算出部９０２が出力するステップ数は、擬似乱数算出部９０３に入力される。擬似乱数算出部９０３は、初期値９０４を与えられ、確定的な演算処理を入力されるステップ数だけ繰り返すことで、０以上の整数または自然数の擬似乱数を生成する。生成した擬似乱数は、公開鍵テーブル６１８のレコード数にて剰余演算が行われ、この剰余がラベル、すなわちレコード番号となる。擬似乱数算出部９０３はラベルを用いて公開鍵テーブル６１８の秘密鍵フィールドを読み出し、秘密鍵を復号処理部６１２へ出力する。

【００４５】

図１０は、プラント側制御装置１０３の、暗号化制御入力におけるテーブルレコード選択処理部６１３のソフトウェア機能を説明するブロック図である。

コントローラ１０４から受信したデータフレームＤ１００７には、暗号化制御入力Enc(u)の他に、始動日時フィールドと、エンコード日時フィールドが付されている。

エンコード日時フィールドに含まれているエンコード日時情報と、始動日時フィールドに含まれている始動日時情報９０１は、ステップ数算出部９０２に入力される。ステップ数算出部９０２は、エンコード日時情報から始動日時情報９０１を減算し、ステップ時間で除算して、ステップ数を算出する。

ここで、図１０に示すステップ数算出部９０２の、図９Ａ、図９Ｂ及び図９Ｃにおけるステップ数算出部９０２との相違点は、エンコード日時情報から始動日時情報９０１を減算し、ステップ時間で除算して、擬似乱数算出部９０３へステップ数を出力するだけでなく、ステップ数＋１も出力する点である。

【００４６】

ステップ数算出部９０２が出力するステップ数及びステップ数＋１の値は、擬似乱数算出部９０３に入力される。擬似乱数算出部９０３は、初期値９０４を与えられ、確定的な演算処理を入力されるステップ数だけ繰り返すことで、０以上の整数または自然数の擬似乱数を生成する。生成した擬似乱数は、公開鍵テーブル６１８のレコード数にて剰余演算が行われ、この剰余がラベル、すなわちレコード番号となる。

擬似乱数算出部９０３は、ステップ数に対応するラベルを用いて公開鍵テーブル６１８の秘密鍵フィールドを読み出し、秘密鍵を復号処理部６１２へ出力する。

次に擬似乱数算出部９０３は、ステップ数＋１の値に対応するラベルを用いて公開鍵テーブル６１８の公開鍵フィールドを読み出し、公開鍵を暗号化処理部６０３へ出力する。

【００４７】

図９Ａに示した入力装置１０２のテーブルレコード選択処理部６０５、図９Ｂに示したコントローラ１０４のテーブルレコード選択処理部６１０、図９Ｃ及び図１０に示したプラント側制御装置１０３のテーブルレコード選択処理部６１３の、それぞれに設けられている擬似乱数算出部９０３は、全て同一の確定的な演算処理が組み込まれている。したがって、同一の初期値９０４を与えると、同じステップ数であれば全て同一のラベルを出力する。

【００４８】

［同期運転開始処理］

図１１は、コントローラ１０４の日時情報生成部６１１における、同期運転開始処理の流れを示すフローチャートである。この図１１では、コントローラ１０４の日時情報生成部６１１がマスターであることを前提に説明するが、入力装置１０２やプラント側制御装置１０３がマスターであっても同様である。

処理を開始すると（Ｓ１１０１）、コントローラ１０４の日時情報生成部６１１は自身の日時情報が、日時情報源装置１０５が出力する日時情報と十分小さい誤差にて較正されているか否かを確認する（Ｓ１１０２）。

【００４９】

コントローラ１０４の日時情報生成部６１１自身の日時情報が、日時情報源装置１０５

が出力する日時情報と十分小さい誤差にて較正されているならば（Ｓ１１０２のＹＥＳ）、次にコントローラ１０４の日時情報生成部６１１は、入力装置１０２の日時情報生成部６０６に対し、入力装置１０２の日時情報生成部６０６が、日時情報源装置１０５が出力する日時情報と十分小さい誤差にて較正されているか否かを問い合わせる（Ｓ１１０３）。

【００５０】

入力装置１０２の日時情報生成部６０６の日時情報が、日時情報源装置１０５が出力する日時情報と十分小さい誤差にて較正されているならば（Ｓ１１０３のＹＥＳ）、次にコントローラ１０４の日時情報生成部６１１は、プラント側制御装置１０３の日時情報生成部６１９に対し、プラント側制御装置１０３の日時情報生成部６１９が、日時情報源装置１０５が出力する日時情報と十分小さい誤差にて較正されているか否かを問い合わせる（Ｓ１１０４）。

ステップＳ１１０２、Ｓ１１０３及びＳ１１０４の何れの条件分岐においても、日時情報の較正が正常に完了していなければ（Ｓ１１０２のＮＯ、Ｓ１１０３のＮＯ、Ｓ１１０４のＮＯ）、ステップＳ１１０２まで戻って確認作業が繰り返される。

【００５１】

ステップＳ１１０４で、プラント側制御装置１０３の日時情報生成部６１９の日時情報が、日時情報源装置１０５が出力する日時情報と十分小さい誤差にて較正されているならば（Ｓ１１０４のＹＥＳ）、この時点で入力装置１０２、コントローラ１０４及びプラント側制御装置１０３の全ての日時情報生成部６０６が較正されている。そこで、コントローラ１０４の日時情報生成部６１１は、同期運転の準備段階として、テーブルレコード選択処理部６１０の擬似乱数算出部９０３と協調して、同期運転を開始する時間、ステップ時間、入力装置１０２の擬似乱数算出部９０３及びプラント側制御装置１０３の擬似乱数算出部９０３に与える初期値９０４等のパラメータを決定し、入力装置１０２及びプラント側制御装置１０３の日時情報生成部６１９へ送信する（Ｓ１１０５）。

【００５２】

ステップＳ１１０５にて同期運転の準備が完了したら、コントローラ１０４の日時情報生成部６１１は設定した同期運転開始時間になるまで待ち（Ｓ１１０６のＮＯ）、同期運転開始時間になったら（Ｓ１１０６のＹＥＳ）、同期運転を開始して（Ｓ１１０７）、一連の処理を終了する（Ｓ１１０８）。

【００５３】

［擬似乱数算出部９０３の擬似乱数算出処理］

擬似乱数算出部９０３が使用する擬似乱数は、悪意ある第三者に対して容易に規則性が見出されないように工夫する必要がある。暗号理論に多用される楕円曲線関数の加法定理を応用した擬似乱数生成関数の一例を示す。

図１２は、コントローラ１０４の擬似乱数算出部９０３の動作の流れを示すフローチャートである。

処理を開始すると（Ｓ１２０１）、先ず、擬似乱数算出部９０３は楕円曲線関数$y^2 = x^3 + ax + b$の係数a,bを決定する（Ｓ１２０２）。

【００５４】

次に、擬似乱数算出部９０３はステップＳ１２０２で決定した楕円曲線上の点Pを決定する（Ｓ１２０３）。この点Pは、y座標が０でないことが必須条件である。以上の係数a,b及び点Pと、公開鍵サブテーブル６０４、暗号化パラメータテーブル６０９及び公開鍵テーブル６１８のレコード数pが、入力装置１０２の擬似乱数算出部９０３及びプラント側制御装置１０３の擬似乱数算出部９０３に与える初期値９０４である。

次に、擬似乱数算出部９０３は日時情報生成部６１１と協調して、同期運転を開始する時間、ステップ時間、そして初期値９０４である係数a,b及び点Pを、入力装置１０２の日時情報生成部６０６及びプラント側制御装置１０３の日時情報生成部６１９に送信する（Ｓ１２０４）。

以上の、ステップＳ１２０２、Ｓ１２０３及びＳ１２０４が、図１１のステップＳ１１

０５に相当する。

【００５５】

次に、擬似乱数算出部９０３はステップ数ｔを０に初期化し、点Qに点Pの座標情報を代入する（Ｓ１２０５）。そして、日時情報生成部６１１の制御の下、同期運転開始時間を待つ（Ｓ１２０６）。このステップＳ１２０６は、図１１のステップＳ１１０６に相当する。

同期運転開始時間になったら（Ｓ１２０６のＹＥＳ）、日時情報生成部６１１は起動トリガを擬似乱数算出部９０３に与える。擬似乱数算出部９０３はこれを受けて、これ以降の処理を継続する。

【００５６】

先ず、擬似乱数算出部９０３は点Pと点Qを結ぶ直線に交わる、楕円曲線上の第三の点Rの座標を求める（Ｓ１２０７）。点Pと点Qが同一座標である場合は、楕円曲線上の接線に交わる交点を点R'とする。

次に、擬似乱数算出部９０３は点R'のx座標の値を整数に変換する。点R'のx座標は有理数であるが、例えばＭＡＴＬＡＢ（登録商標）に実装されているnumden()関数は、有理数を分数に変換し、その分母と分子を出力する。このnumden()関数のような、有理数を分数に変換し、その分母を取り出すことで、点Rのx座標の値を整数に変換することが可能である。そして、得られた擬似乱数である整数から、レコード数pの剰余を求める（Ｓ１２０８）。この剰余が、ラベル、すなわち公開鍵サブテーブル６０４、暗号化パラメータテーブル６０９及び公開鍵テーブル６１８のレコードを指し示すレコード番号になる。

次に、擬似乱数算出部９０３はステップ数ｔを１インクリメントする（Ｓ１２０９）。そして、点R'のy軸の値の符号を反転させた値を点R'の写像であるRとする。この点Rの座標情報を点Qに代入する（Ｓ１２１０）。そして、ステップＳ１２０７から一連の処理を繰り返す。

【００５７】

図１２では、マスターであるコントローラ１０４の擬似乱数算出部９０３の動作の流れを示したが、スレーヴである入力装置１０２の入力装置１０２の擬似乱数算出部９０３及びプラント側制御装置１０３の擬似乱数算出部９０３は、ステップＳ１２０４の時点でコントローラ１０４の日時情報生成部６１１から初期値９０４を受信すると、ステップＳ１２０５以降の動作を実行する。すなわち、ステップＳ１２０５以降の擬似乱数算出部９０３の動作は、マスターもスレーヴも同じである。

【００５８】

［同期運転処理］

図１３は、暗号化制御システム１０１の同期運転を説明するタイムチャートである。図１３中、ステップ時間を１０ｍｓｅｃ、ステップ数をｔとする。同期運転始動時をｔ＝０とし、ｔ＝０以降、ｔが１ずつインクリメントする。

同期運転始動時（ｔ＝０）、入力装置１０２は目標値rをｔ＝０のラベルに相当する公開鍵で暗号化して、暗号化目標値Enc(r)を得る。そして、暗号化目標値Enc(r)をコントローラ１０４を経由してプラント側制御装置１０３へ送信する（Ｓ１３０１）。暗号化目標値Enc(r)のデータフレームＤ１３２１には、日時情報生成部６０６が生成したｔ＝０における現在日時情報が含まれている。

【００５９】

同期運転始動時（ｔ＝０）、コントローラ１０４は暗号化パラメータテーブル６０９からｔ＝０のラベルに相当する暗号化第一パラメータ、暗号化第二パラメータ及び暗号化第三パラメータを読み出し、初期値９０４としての制御入力uと乗算部６０８にて乗算処理を行い、暗号化制御入力Enc(u)を得る。そして、暗号化制御入力Enc(u)をプラント側制御装置１０３へ送信する（Ｓ１３０２）。暗号化制御入力Enc(u)のデータフレームＤ１３２２には、同期運転開始時における始動日時情報９０１と、ｔ＝０における現在日時情報が含まれている。この時点では、始動日時情報９０１と現在日時情報は同一である。

【００６０】

同期運転始動時（ｔ＝０）、プラント側制御装置１０３は入力装置１０２からコントローラ１０４を経由して暗号化目標値Enc(r)を、コントローラ１０４から暗号化制御入力Enc(u)を受信する（Ｓ１３０３）。

次にプラント側制御装置１０３の復号処理部６１２は各々のデータフレームに付されている現在日時情報、始動日時情報９０１を基にラベルを計算し、算出したラベルに対応する暗号鍵を用いて、目標値rと制御入力uをデコードする。制御用演算処理部６１４は、復号処理部６１２によってデコードされた目標値rと制御入力uの基となる値に演算処理を行い、目標値rと制御入力uを生成する。本発明の実施形態において使用する、準同型性を持つ公開鍵暗号は、暗号化したままのデータ同士を乗算（除算）することはできるが、加算（減算）ができない。そこで、コントローラ１０４の乗算部６０８は、与えられるデータに対し、制御用演算処理における乗算処理のみを行う。そして、暗号化したままではできない加算処理を制御用演算処理部６１４で遂行することで、制御用演算処理が完遂する。制御処理部６１５は、制御入力uから制御信号を生成し、制御対象１０６を制御する。制御対象１０６が制御処理部６１５によって制御されると、制御対象１０６の動作はセンサ１０７によって検出される。

【００６１】

センサ１０７が出力する観測信号は、信号変換処理部６１６によって観測値yに変換される。信号変換処理部６１６が出力する観測値yは、制御用演算処理部６１４が出力する目標値rと共に目標誤差演算処理部６１７に入力される。目標誤差演算処理部６１７は、目標値rから観測値yを減算して、目標誤差εを出力する（Ｓ１３０４）。

暗号化処理部６０３は、目標誤差εを、ｔ＋１のステップ数に相当するラベルに対応する公開鍵で暗号化する（Ｓ１３０５）。この時点ではｔ＝０なので、ｔ＋１＝１、すなわちステップ数１に相当するラベルに対応する公開鍵が、目標誤差εの暗号化に使われる。

【００６２】

同期運転始動からステップ数が１インクリメントして、ｔ＝１になった時点で、プラント側制御装置１０３は、第二制御ネットワークモジュール１１５の送信部２０８を通じて、暗号化目標誤差Enc(ε)をコントローラ１０４へ送信する（Ｓ１３０６）。暗号化目標誤差Enc(ε)のデータフレームＤ１３２３には、同期運転開始時における始動日時情報９０１と、ｔ＝１における現在日時情報が含まれている。

【００６３】

ｔ＝１の時点で、コントローラ１０４は、プラント側制御装置１０３から暗号化目標誤差Enc(ε)を受信する（Ｓ１３０７）。コントローラ１０４の第二制御ネットワークモジュール１１５の受信部３０９から受信した暗号化目標誤差Enc(ε)は、入出力制御部６０７を通じて乗算部６０８に引き渡される。乗算部６０８は、暗号化目標誤差Enc(ε)のデータフレームに付されている、始動日時情報９０１と、ｔ＝１における現在日時情報をテーブルレコード選択処理部６１０に引き渡す。テーブルレコード選択処理部６１０は、ｔ＝１のラベルに相当する暗号化第一パラメータ、暗号化第二パラメータ及び暗号化第三パラメータを読み出し、乗算部６０８に引き渡す。乗算部６０８は暗号化第一パラメータ、暗号化第二パラメータ及び暗号化第三パラメータと、暗号化目標誤差Enc(ε)を乗算処理して、暗号化制御入力Enc(u)を得る（Ｓ１３０８）。そして、暗号化制御入力Enc(u)をプラント側制御装置１０３へ送信する（Ｓ１３０９）。暗号化制御入力Enc(u)のデータフレームＤ１３２４には、同期運転開始時における始動日時情報９０１と、ｔ＝１における現在日時情報が含まれている。

【００６４】

ｔ＝１の時点で、入力装置１０２は目標値rをｔ＝１のラベルに相当する公開鍵で暗号化して、暗号化目標値Enc(r)を得る。そして、暗号化目標値Enc(r)をコントローラ１０４を経由してプラント側制御装置１０３へ送信する（Ｓ１３１０）。暗号化目標値Enc(r)のデータフレームＤ１３２５には、ｔ＝１における現在日時情報が含まれている。

【００６５】

ｔ＝１の時点で、プラント側制御装置１０３は入力装置１０２からコントローラ１０４

を経由して暗号化目標値Enc(r)を、コントローラ１０４から暗号化制御入力Enc(u)を受信する（Ｓ１３１１）。

次にプラント側制御装置１０３の復号処理部６１２は各々のデータフレームに付されている現在日時情報、始動日時情報９０１を基にラベルを計算し、算出したラベルに対応する暗号鍵を用いて、目標値rと制御入力uをデコードする。制御用演算処理部６１４は、復号処理部６１２によってデコードされた目標値rと制御入力uの基となる値に演算処理を行い、目標値rと制御入力uを生成する。制御処理部６１５は、制御入力uから制御信号を生成し、制御対象１０６を制御する。制御対象１０６が制御処理部６１５によって制御されると、制御対象１０６の動作はセンサ１０７によって検出される。

【００６６】

センサ１０７が出力する観測信号は、信号変換処理部６１６によって観測値yに変換される。信号変換処理部６１６が出力する観測値yは、制御用演算処理部６１４が出力する目標値rと共に目標誤差演算処理部６１７に入力される。目標誤差演算処理部６１７は、目標値rから観測値yを減算して、目標誤差εを出力する（Ｓ１３１２）。

暗号化処理部６０３は、目標誤差εを、ｔ＋１のステップ数に相当するラベルに対応する公開鍵で暗号化する（Ｓ１３１３）。この時点ではｔ＝１なので、ｔ＋１＝２、すなわちステップ数２に相当するラベルに対応する公開鍵が、目標誤差εの暗号化に使われる。

【００６７】

以下同様に、プラント側制御装置１０３は、入力装置１０２からステップ数ｔにおける暗号化目標値Enc(r)を、コントローラ１０４からステップ数ｔにおける暗号化制御入力Enc(u)を受信すると、目標値rと制御入力uに基づいて制御対象１０６を制御する。その結果、センサ１０７から得られた観測値yを目標値rから減算して目標誤差εを得る。暗号化処理部６０３は、目標誤差εをステップ数ｔ＋１における公開鍵で暗号化して、暗号化目標誤差Enc(ε)をコントローラ１０４へ出力する。

つまり、プラント側制御装置１０３のデータ受信、演算、データ送信のサイクルにおいて、ステップ数は１インクリメントする。

【００６８】

これに対し、コントローラ１０４は、プラント側制御装置１０３から受信した暗号化目標誤差Enc(ε)のデータフレームに付されている現在日時情報、始動日時情報９０１から得たステップ数ｔにおける暗号化第一パラメータ、暗号化第二パラメータ及び暗号化第三パラメータを、暗号化目標誤差Enc(ε)と乗算処理して、暗号化制御入力Enc(u)を得て、プラント側制御装置１０３へ送信する。

つまり、コントローラ１０４のデータ受信、演算、データ送信のサイクルにおいて、ステップ数はそのまま変化しない。

【００６９】

［数値シミュレーション］

以上説明した実施形態に係る暗号化制御システム１０１の理論的検証のため、計算機上で数値シミュレーションを実施した。

図１４Ａは、特許文献１に係る暗号化制御システム１０１における、制御入力uと目標誤差εのグラフである。

図１４Ｂは、本発明の実施形態に係る暗号化制御システム１０１における、制御入力uと目標誤差εのグラフである。

図１４Ａ及び図１４Ｂの何れのグラフも、ステップ時間を１０ｍｓｅｃとし、時刻１０ｓｅｃにおいて、暗号化目標誤差Enc(ε)に対して改竄攻撃を行ったと想定したシミュレーション結果である。

【００７０】

図１４Ａでは、使用する公開鍵及び秘密鍵の組が１組だけであるため、改竄攻撃による影響が目標誤差εに現れない。しかし、図１４Ｂでは、ステップ数毎に使用する公開鍵及び秘密鍵の組をランダムに切り替える仕組みを採用しているので、改竄攻撃によって目標誤差εが改竄攻撃される前とは明確に異なる、連続性のない変化を示す。

【００７１】
制御システムは制御対象１０６が安定した状態であることが望ましい。このため、目標誤差εが大幅に変動することはまずあり得ない。したがって、目標誤差εの変動幅は概ね小さく、連続性を有する。通常の状態において変動幅が小さく連続性を有する信号が、急に変動幅が大きくなり、連続性のない変化を示すようになれば、何らかの異常が発生したものと明確に認識することができる。
【００７２】
例えば、目標誤差εの変動幅を２乗して、所定の閾値と比較して、当該閾値を超えていれば、暗号化制御システム１０１に対する攻撃があったと判定することができる。この判定演算を攻撃検出器とする。
図１５Ａは、特許文献１に係る暗号化制御システム１０１における、攻撃検出器のグラフである。
図１５Ｂは、本発明の実施形態に係る暗号化制御システム１０１における、攻撃検出器のグラフである。
【００７３】
図１５Ａでは、使用する公開鍵及び秘密鍵の組が１組だけであるため、攻撃検出器は改竄攻撃を検出することができない。しかし、図１５Ｂでは、ステップ数毎に使用する公開鍵及び秘密鍵の組をランダムに切り替える仕組みを採用しているので、攻撃検出器は改竄攻撃によって目標誤差εが改竄攻撃されたことを明確に認識することができる。
【００７４】
以上に説明した実施形態には、以下のような変形例が考えられる。
（１）上記の実施形態では、擬似乱数算出部９０３が、計算の要求が発生した時点で動作するように構成されていたが、予め計算した結果をラベルテーブルに記憶しておいてもよい。
ラベルテーブルは、ステップ数フィールドとラベルフィールドを有する。
ステップ数フィールドにはステップ数が格納される。
ラベルフィールドにはステップ数に対応する、擬似乱数算出部９０３が算出したラベルが格納される。
このようなラベルテーブルを数千あるいは数万レコード程度記憶しておけば、ＣＰＵモジュール１１２の演算リソースを主たる制御演算に集中させることができる。
【００７５】
（２）上記の実施形態では、制御周期毎に公開鍵と秘密鍵のペアを切り替えるように構成されていたが、複数の制御周期毎に切り替えるように構成してもよい。但し、あまり切り替えの周期が長すぎると、悪意ある第三者に対する脆弱性が増大する虞がある。
（３）日時情報源装置１０５の機能を、入力装置１０２、プラント側制御装置１０３、コントローラ１０４の何れか１台が兼用してもよい。例えば、入力装置１０２にＧＰＳ（global positioning system）受信機を装備することで、正確な日時情報を得ることが可能になる。
【００７６】
（４）入力装置１０２とコントローラ１０４を一体化することができる。
図１６は、本発明の実施形態の変形例に係るコントローラ１６０１の、制御ネットワークにおけるソフトウェア機能を示すブロック図である。
図１６に示すコントローラ１６０１は、図６に示した入力装置１０２とコントローラ１０４を一体化した構成である。
先ず、テーブルレコード選択処理部１６０２は、入力装置１０２のテーブルレコード選択処理部６０５とコントローラ１０４のテーブルレコード選択処理部６１０の機能を有する。すなわちテーブルレコード選択処理部１６０２は、暗号化処理部６０３に対し、公開鍵サブテーブル６０４から所定のレコードを選択すると共に、暗号化パラメータテーブル６０９から所定のレコードを選択する機能を有する。
【００７７】

次に、入出力制御部１６０３は、入力装置１０２の入出力制御部６０２とコントローラ１０４の入出力制御部６０７の機能を有する。

そして、入力装置１０２の日時情報生成部６０６は省略される。すなわち日時情報生成部６１１は、乗算部６０３から出力される暗号化制御入力に付加する日時情報を提供すると共に、テーブルレコード選択処理部１６０２に日時情報を提供すると共に起動タイミングを与える機能を有する。

【００７８】

以上に説明したように、暗号化制御システム１０１において、入力装置１０２とコントローラ１０４に代えて、入力装置１０２とコントローラ１０４を一体化したコントローラ１６０１を用いても、同等の機能を実現することができる。

なお、図６の入力装置１０２は公開鍵サブテーブル６０４を有している。そこで、入力装置１０２とコントローラ１０４を一体化したコントローラ１６０１を実現する際、暗号化処理部６０３に目標値rだけでなく、第一パラメータKp、第二パラメータKi及び第三パラメータKdも一緒に暗号化させる構成にすれば、暗号化処理部６０３の演算量は増えるが、暗号化パラメータテーブル６０９を省略することができる。

【００７９】

本実施形態では、暗号化制御システム１０１を開示した。

入力装置１０２、プラント側制御装置１０３及びコントローラ１０４には、共通の機能を有する擬似乱数算出部９０３を装備して、時刻同期を行う。そして、同一時刻で同期運転を開始する。このように暗号化制御システム１０１を構成することで、制御システム全体の制御周期に同期して、公開鍵と秘密鍵のペアを切り替えることが可能になる。よって、制御システムに対する、悪意ある第三者による介入を瞬時に且つ明確に検出することが可能になる。

【００８０】

以上、本発明の実施形態について説明したが、本発明は上記実施形態に限定されるものではなく、請求の範囲に記載した本発明の要旨を逸脱しない限りにおいて、他の変形例、応用例を含む。

【符号の説明】

【００８１】

１０１…暗号化制御システム、１０２…入力装置、１０３…プラント側制御装置、１０４…コントローラ、１０５…日時情報源装置、１０６…制御対象、１０７…センサ、１１１…マウントベース、１１２…ＣＰＵモジュール、１１３…情報ネットワークモジュール、１１４ａ、１１４ｂ…第一制御ネットワークモジュール、１１５…第二制御ネットワークモジュール、１１６…入出力モジュール、２０１…モジュールバス、２０２…ＣＰＵ、２０３…ＲＯＭ、２０４…ＲＡＭ、２０５…ＲＴＣ、２０６…内部バス、２０７…ＮＩＣ、２０８…送信部、３０９…受信部、４１０…Ａ／Ｄ変換器、４１１…Ｄ／Ａ変換器、５０１…ＣＰＵ、５０２…ＲＯＭ、５０３…ＲＡＭ、５０４…不揮発性ストレージ、５０５…ＲＴＣ、５０６…ＮＩＣ、５０７…バス、５０８…表示部、５０９…操作部、６０１…目標値入力部、６０２…入出力制御部、６０３…暗号化処理部、６０４…公開鍵サブテーブル、６０５…テーブルレコード選択処理部、６０６…日時情報生成部、６０７…入出力制御部、６０８…乗算部、６０９…暗号化パラメータテーブル、６１０…テーブルレコード選択処理部、６１１…日時情報生成部、６１２…復号処理部、６１３…テーブルレコード選択処理部、６１４…制御用演算処理部、６１５…制御処理部、６１６…信号変換処理部、６１７…目標誤差演算処理部、６１８…公開鍵テーブル、６１９…日時情報生成部、６２０…ログテーブル、９０１…始動日時情報、９０２…ステップ数算出部、９０３…擬似乱数算出部、９０４…初期値、１６０１…コントローラ、１６０２…テーブルレコード選択処理部、１６０３…入出力制御部

【図１】

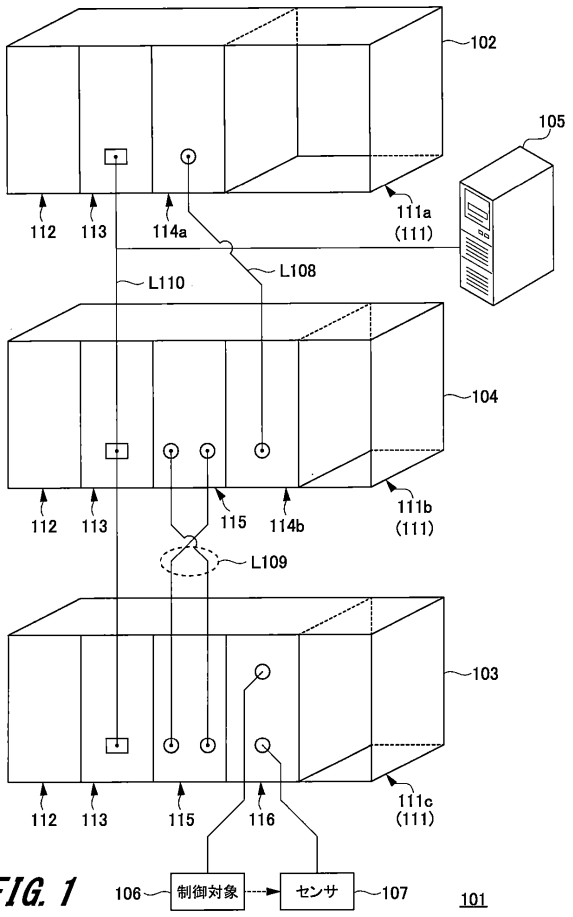
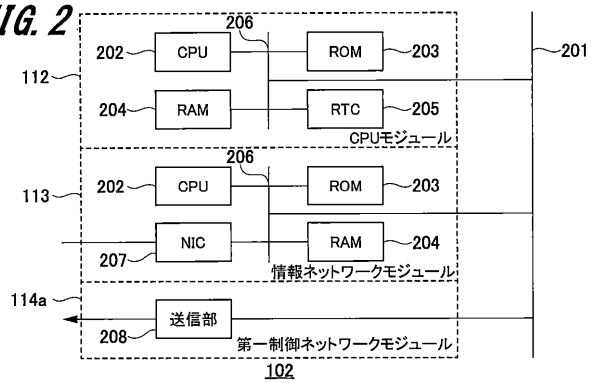


FIG. 1

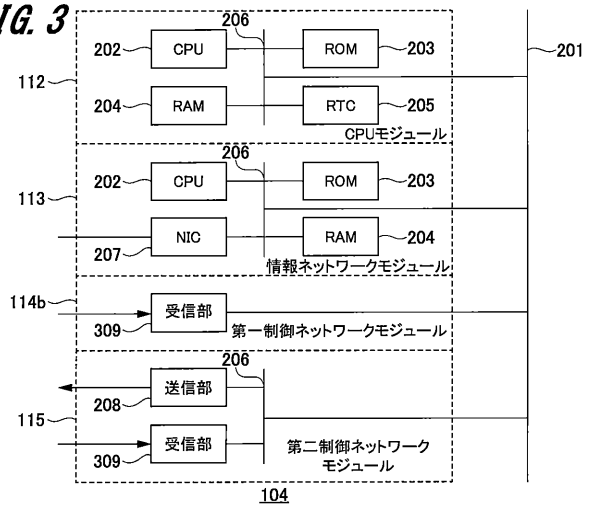
【図２】

FIG. 2



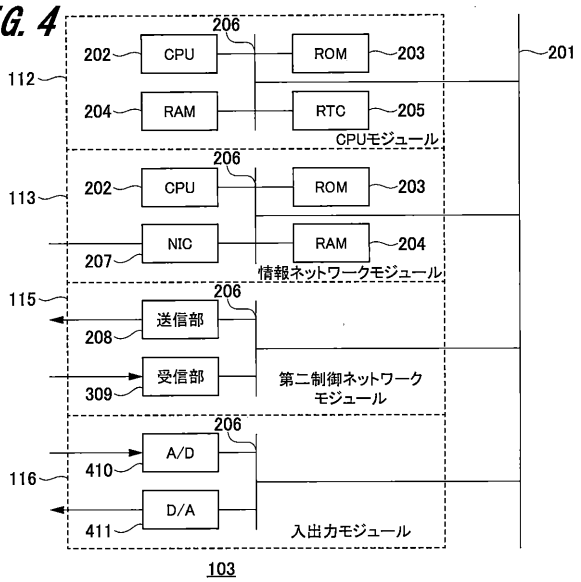
【図３】

FIG. 3



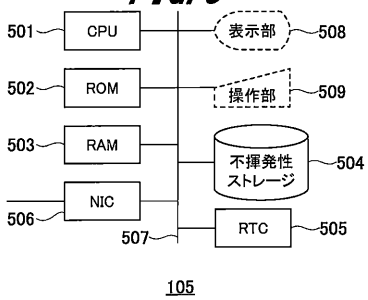
【図４】

FIG. 4



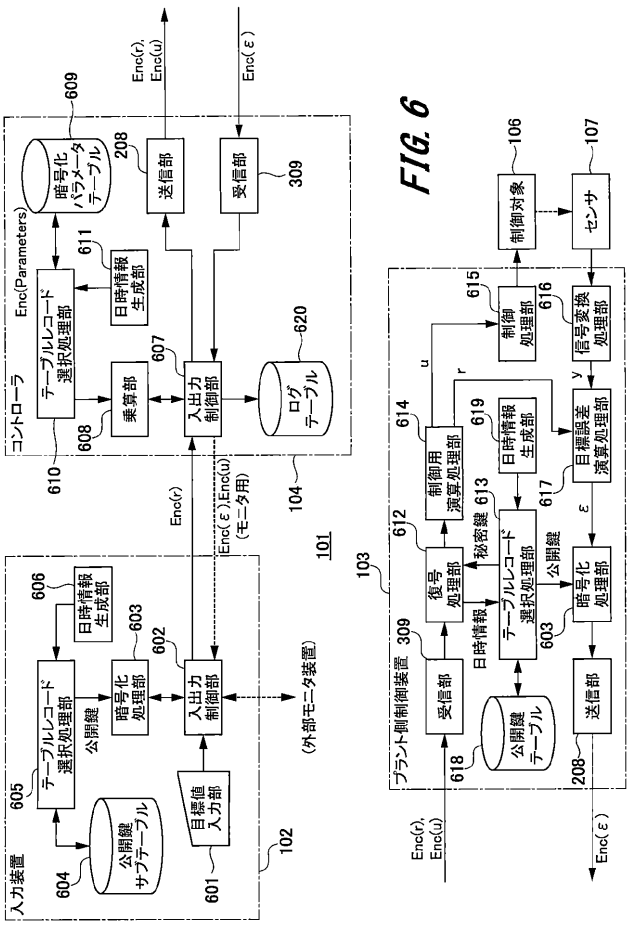
【図５】

FIG. 5



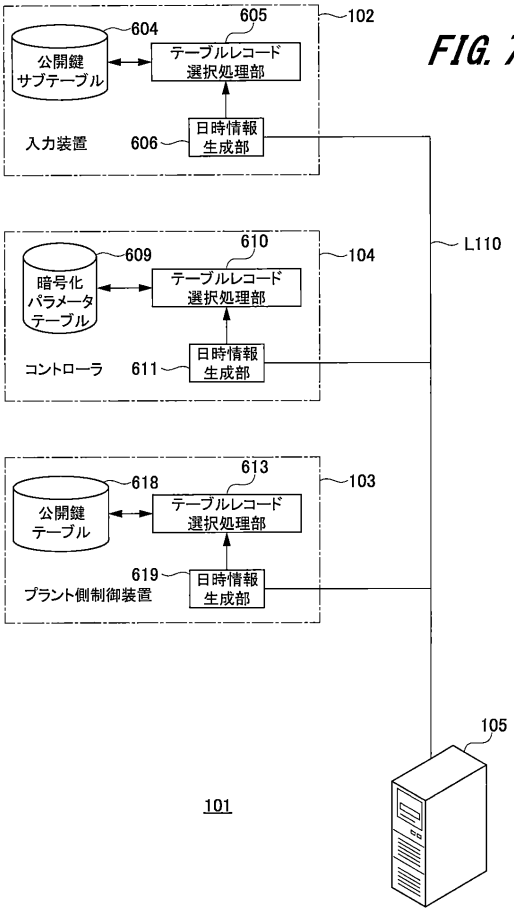
【図６】

FIG. 6



【図７】

FIG. 7



【図８】

618 公開鍵テーブル

レコード番号（ラベル）	公開鍵	秘密鍵
1		
2		
⋮		

604 公開鍵サブテーブル

レコード番号（ラベル）	公開鍵
1	
2	
⋮	

609 暗号化パラメータテーブル

レコード番号（ラベル）	暗号化第一パラメータ (Enc(Kp))	暗号化第二パラメータ (Enc(Ki))	暗号化第三パラメータ (Enc(Kd))
1			
2			
⋮			

FIG. 8

【図９】

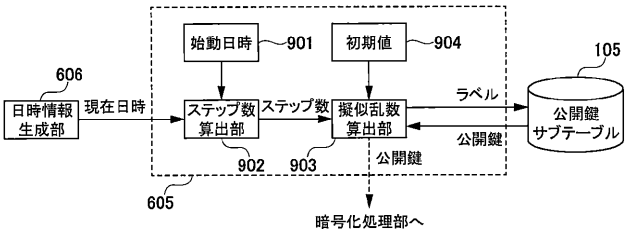


FIG. 9A

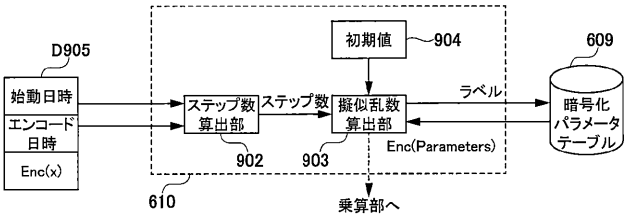


FIG. 9B

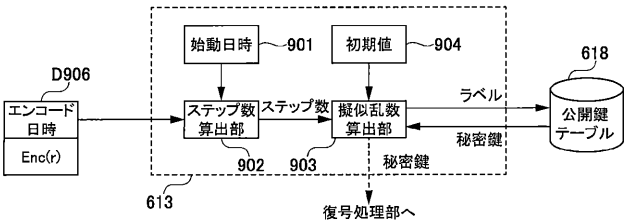


FIG. 9C

【図１０】

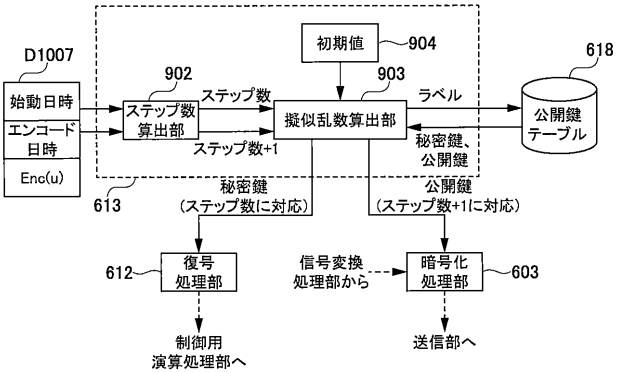


FIG. 10

【図１１】

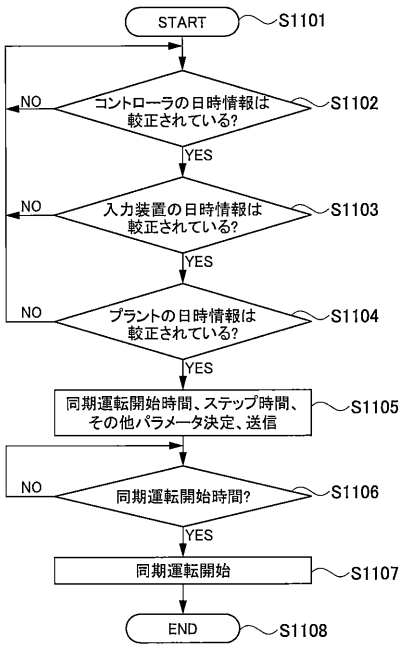


FIG. 11

【図１２】

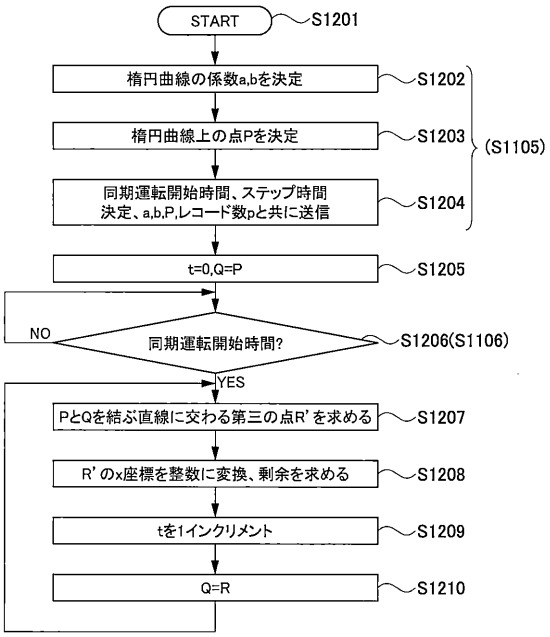


FIG. 12

【図１３】

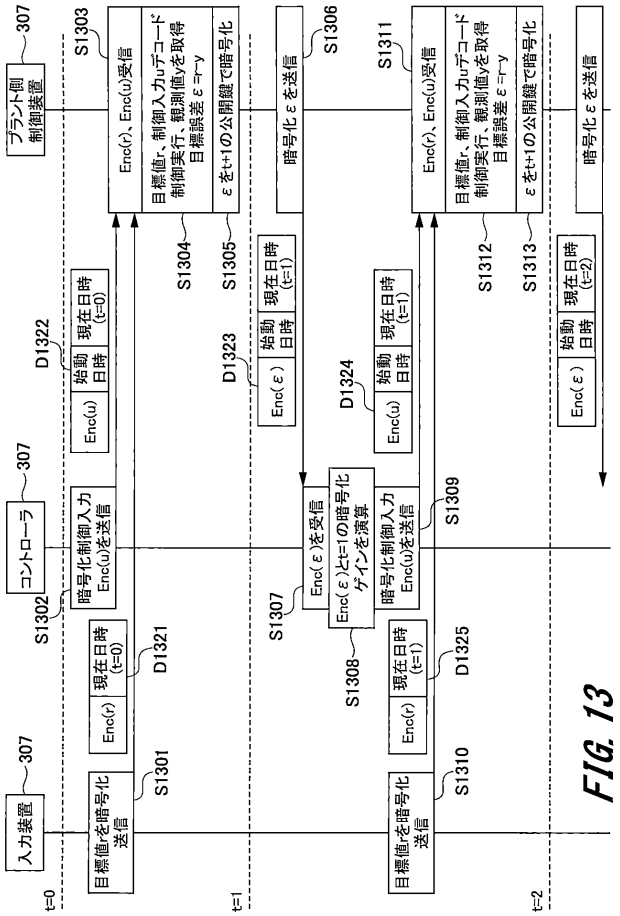


FIG. 13

【図１４】

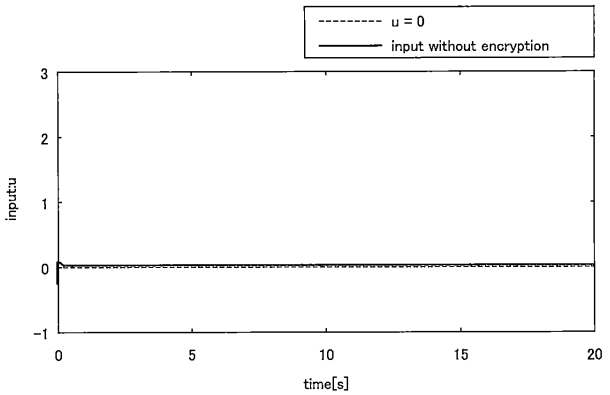


FIG. 14A

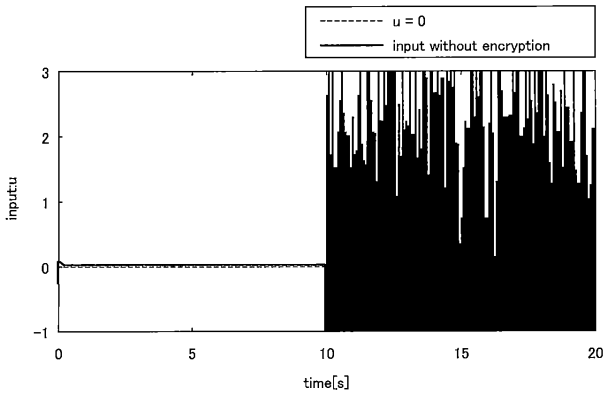


FIG. 14B

【図１５】

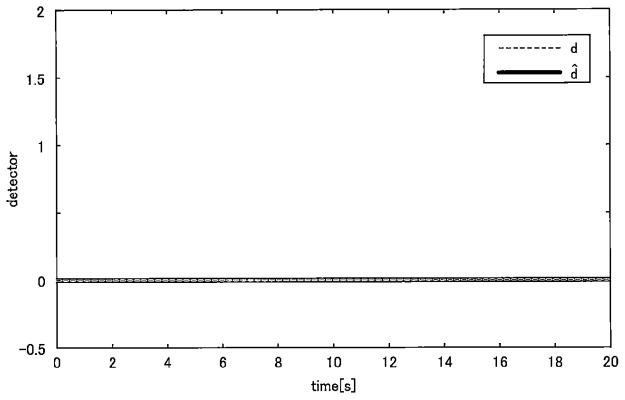


FIG. 15A

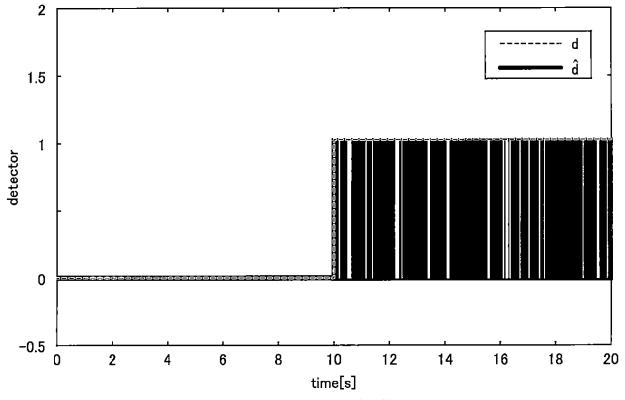


FIG. 15B

【図１６】

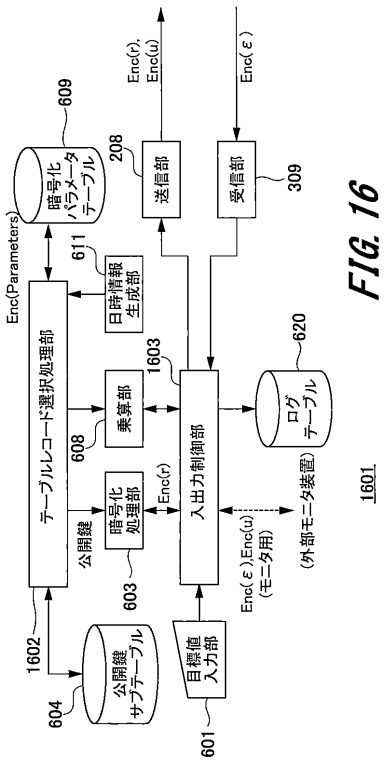


FIG. 16

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/038954

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04L9/14(2006.01)i, G09C1/00(2006.01)i
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl. H04L9/14, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922–1996
Published unexamined utility model applications of Japan	1971–2018
Registered utility model specifications of Japan	1996–2018
Published registered utility model applications of Japan	1994–2018

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore, THE ACM DIGITAL LIBRARY

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2013/189783 A1 (ABB RESEARCH LTD.) 27 December 2013, page 6, line 17 to page 10, line 9, fig. 1-4 & EP 2677680 A1	1-6
A	藤田 貴大 ほか, 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, 30 September 2015, vol. 51, no. 9, pp. 661-666, (FUJITA, Takahiro et al., "Encryption of Controllers Using ElGamal Cryptosystem", Transactions of the Society of Instrument and Control Engineers)	1-6

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 December 2018 (07.12.2018)	25 December 2018 (25.12.2018)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/038954

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 1-212041 A (HITACHI, LTD.) 25 August 1989, page 3, upper right column, line 2 to page 5, upper right column, line 18, page 5, lower right column, line 19 to page 6, upper left column, line 14, fig. 1-3 (Family: none)	1-6
A	JP 2016-527844 A (BEDROCK AUTOMATION PLATFORMS INC.) 08 September 2016, paragraphs [0032]-[0035], [0046], fig. 1-7 & US 2016/0078213 A1, paragraphs [0042]-[0045], [0057], fig. 1-7 & US 2018/0089416 A1 & WO 2015/020633 A1 & KR 10-2016-0040277 A & CN 105531635 A	1-6
T	鈴木崇司 ほか, 動的鍵管理による暗号化制御系, 第60回自動制御連合講演会講演論文集, 10 November 2017, SaC3-3, [retrieval date 06 December 2018], internet <URL:https://www.jstage.jst.go.jp/article/jacc/60/0/60_513/_article/-char/ja>, non-official translation (SUZUKI, Takashi et al., "Encrypted Control System with selective Keys", Proceedings of the 60th Japan Joint Automatic Control Conference)	1-6

Form PCT/ISA/210 (continuation of second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/038954

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
See extra sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/038954

<Continuation of Box III>

(Invention 1) Claims 1-3

Claim 1 has a special technical feature in which "the controller is provided with

:...

a multiplication unit, which receives an encryption target error from the plant-side control device, and multiplies the same by the encryption parameter selected by the first table record selection processing unit to output an encryption control input; and

a first date and time information generation unit, which provides date and time information to be added to the encryption control input output from the multiplication unit, provides the date and time information to the first table record selection processing unit, and assigns a start timing". Claims 2-3 have the same technical features as claim 1. Therefore, claims 1-3 are classified as invention 1.

(Invention 2) Claims 4-6

Claims 4-6 share, with claim 1 classified as invention 1, a common technical feature of receiving an encryption target value and decrypting the encryption target. However, it is obvious that this technical feature does not make a contribution over the prior art in light of the disclosure of document 1 (particularly see paragraph [0063]), etc.), and thus said technical feature is not considered to be a special technical feature. Furthermore, these inventions do not share other identical or corresponding special technical features.

Furthermore, claims 4-6 are not dependent on claim 1. Furthermore, claims 4-6 are not substantially identical or equivalent to any of the claims classified as invention 1.

Therefore, claims 4-6 cannot be classified as invention 1.

Claims 4-6 have a special technical feature of "an encryption target value step number calculation step in which first encoded date and time information is read from an encoded date and time field added to the first data frame, starting date and time information is subtracted from the first encoded date and time information to perform a division at a prescribed period, so as to calculate an encryption target value step number". Thus, claims 4-6 are classified as invention 2.

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２０１８／０３８９５４

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl. H04L9/14(2006.01)i, G09C1/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl. H04L9/14, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１８年
日本国実用新案登録公報	１９９６－２０１８年
日本国登録実用新案公報	１９９４－２０１８年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore, THE ACM DIGITAL LIBRARY

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	WO 2013/189783 A1 (ABB RESEARCH LTD) 2013.12.27, 第６頁第１７行－第１０頁第９行、Ｆｉｇ．１－４ & EP 2677680 A1	1-6
A	藤田 貴大 ほか, Ｅ１Ｇａｍａ１暗号を用いた制御器の暗号化, 計測自動制御学会論文集, 2015.09.30, 第５１巻 第９号, ｐｐ．６６１－６６６	1-6

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０７．１２．２０１８	２５．１２．２０１８

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	５Ｓ	４２２９
	青木 重徳	
	電話番号 ０３－３５８１－１１０１ 内線 ３５４６	

国際調査報告 国際出願番号 ＰＣＴ／ＪＰ２０１８／０３８９５４

Ｃ（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Ａ	JP 1-212041 A（株式会社日立製作所）1989.08.25，第３頁右上欄第２行－第５頁右上欄第１８行、第５頁右下欄第１９行－第６頁左上欄第１４行、第１－３図（ファミリーなし）	1-6
Ａ	JP 2016-527844 A（ペドロック・オートメーション・プラットフォームズ・インコーポレーテッド）2016.09.08，段落［００３２］－［００３５］、［００４６］、図１－７ & US 2016/0078213 A1，段落［００４２］－［００４５］、［００５７］、ＦＩＧ．１－７ & US 2018/0089416 A1 & WO 2015/020633 A1 & KR 10-2016-0040277 A & CN 105531635 A	1-6
Ｔ	鈴木 崇司 ほか，動的鍵管理による暗号化制御系，第６０回自動制御連合講演会講演論文集，2017.11.10，ＳａＣ３－３，［検索日2018.12.06］，インターネット：<ＵＲＬ：https://www.jstage.jst.go.jp/article/jacc/60/0/60_513/_article/-char/ja>	1-6

（発明１）請求項１－３
請求項１は、
[前記コントローラは、
…（中略）…
前記プラント側制御装置から暗号化目標誤差を受信して、前記第一のテーブルレコード選択処理部が選択した前記暗号化パラメータを乗算して暗号化制御入力を出力する乗算部と、
前記乗算部から出力される前記暗号化制御入力に付加する日時情報を提供すると共に、前記第一のテーブルレコード選択処理部に日時情報を提供すると共に起動タイミングを与える第一の日時情報生成部と
を具備]
という特別な技術的特徴を有しており、請求項２－３も、請求項１と同一の技術的特徴を有している。したがって、請求項１－３を発明１に区分する。

（発明２）請求項４－６
請求項４－６は、発明１に区分された請求項１と、暗号化目標値を受信し、前記暗号化目標を復号するという共通の技術的特徴を有している。しかしながら、当該技術的特徴は、文献１の開示内容（特に段落［００６３］などを参照）に照らして、先行技術に対する貢献をもたらすものではないから、当該技術的特徴は、特別な技術的特徴であるとはいえない。また、これらの発明の間には、他に同一の又は対応する特別な技術的特徴は存在しない。
さらに、請求項４－６は、請求項１の従属請求項ではない。また、請求項４－６は、発明１に区分されたいずれの請求項に対しても実質同一又はそれに準ずる関係にはない。
したがって、請求項４－６は発明１に区分できない。
そして、請求項４－６は、
[前記第一のデータフレームに付されているエンコード日時フィールドから第一のエンコード日時情報を読み出し、前記第一のエンコード日時情報から始動日時情報を減算し、所定の周期で除算することで暗号化目標値ステップ数を算出する、暗号化目標値ステップ数算出ステップ]
という特別な技術的特徴を有しているので、発明２に区分する。

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２０１８／０３８９５４

第Ⅱ欄 請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求項 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求項 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求項 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅲ欄 発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

特別ページ参照。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求項について作成した。

2．☑ 追加調査手数料を要求するまでもなく、すべての調査可能な請求項について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求項のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求項について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。

☐ 追加調査手数料の納付はあったが、異議申立てはなかった。

フロントページの続き

(81)指定国・地域 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。