(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4986926号
(P4986926)
(45)発行日　平成24年7月25日(2012.7.25)　(24)登録日　平成24年5月11日(2012.5.11)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/00 601E

請求項の数 3　(全 10 頁)

(21)出願番号　特願2008-123948(P2008-123948)
(22)出願日　平成20年5月9日(2008.5.9)
(65)公開番号　特開2009-273054(P2009-273054A)
(43)公開日　平成21年11月19日(2009.11.19)
審査請求日　平成22年6月30日(2010.6.30)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　小原　栄
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　松平　英

最終頁に続く

(54)【発明の名称】暗号化通信システム

(57)【特許請求の範囲】
【請求項１】
少なくとも１つの拠点端末から１つの中央端末に内容を秘匿して情報データを送信する暗号化通信システムであって、
前記中央端末および夫々の前記拠点端末は、
同一の入力値から同一の出力値を出力する、全ての端末で同一に統一された擬似乱数発生アルゴリズムに入力値を入力して、出力乱数列を算出する擬似乱数発生手段と、
前記算出された出力乱数列から全ての端末で同一に統一されたルールに基づいて所定の桁数分の乱数列を切り出して該乱数列の各要素を夫々２値化して２値化数列を作成し、予め自端末に保持する２値化数列とパラメータ値との対応関係を示す全ての端末で同一に統一された管理テーブルに基づいて前記作成した２値化数列に対応するパラメータ値を算出する擬似乱数管理手段と、
を夫々備え、
前記拠点端末は、
拠点端末毎に異なる１つの入力値を予め保持する第一の記憶手段と、
前記中央端末に送信する情報データが入力されたとき、前記第一の記憶手段に保持されている入力値から自端末が備える前記擬似乱数発生手段および前記擬似乱数管理手段を用いて算出したパラメータ値を暗号化キーとして前記情報データを暗号化し、該暗号化した情報データを自端末の識別情報とともに前記中央端末に送信するデータ暗号化手段と、
を備え、

前記中央端末は、
拠点端末毎に異なる全ての入力値を前記拠点端末の識別情報と対応付けて格納する第二の記憶手段と、
前記拠点端末の識別情報とともに前記暗号化した情報データを受信したとき、前記第二の記憶手段に格納され前記受信した識別情報に対応付けられている入力値から自端末が備える前記擬似乱数発生手段および前記擬似乱数管理手段を用いて算出した前記暗号化キーとして使用されたパラメータ値と同一のパラメータ値を復号化キーとして、前記受信した暗号化した情報データを復号化するデータ復号化手段と、
を備えることを特徴とする暗号化通信システム。
【請求項２】
前記擬似乱数発生手段は、
前記擬似乱数発生アルゴリズムに入力値を入力して、出力乱数列と、切り出し開始層と、切り出し桁と、を算出し、
擬似乱数管理手段は、
前記算出された出力乱数列から、該出力乱数列の前記切り出し開始層の値が示す桁から前記切り出し桁の値が示す桁数分の乱数列を切り出す、
ことを特徴とする請求項１に記載の暗号化通信システム。
【請求項３】
前記中央端末は、所定の時間間隔で拠点端末毎に異なる入力値を生成して、該生成した入力値を夫々拠点端末の識別情報と対応付けて前記第二の記憶手段に格納するとともに、前記生成した入力値を夫々対応する拠点端末に送信する拠点端末別入力値生成手段をさらに備え、
前記拠点端末は、前記中央端末から入力値が送信されてきたとき、該送信されてきた入力値を自端末の第一の記憶手段に格納する、
ことを特徴とする請求項１または２に記載の暗号化通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、１つ以上の拠点端末から秘匿して送信される個体識別カードのカード情報を含む情報を１つの中央端末が受信する暗号化通信システムに関するするものである。
【背景技術】
【０００２】
現在、ＩＣカード、磁気カードなどの個体識別カードのカード情報を拠点端末から入力し、そのカード情報を中央端末に送信する通信システムは、銀行が発行するキャッシュカードの通信システム、クレジットカードの決済システムなど、幅広く適用されている。これらの一般的な個体識別カードのカード情報を送受信する通信システムにおいて送受信されるカード情報の秘匿性を確保する方法としては、磁気記録部位の多層化による保護策や、磁気カードの光学的処置によるセキュリティを測る方法など、物理的側面での対策が中心となっているのが現状である。
【０００３】
一方、近年の盗聴機器の技術水準が高いことを考慮すると、物理的な通信ネットワーク、例えば電話線（専用線）からの無線機器などを用いた情報漏洩への対策を行わなくてはならない。前述する物理的側面での対策は、スキミングなどによるカード偽造によるなりすましを防ぐのには効果的であるが、このような通信の盗聴による情報漏洩には対応できない。従って、すでに物理的側面での対策を行った通信システムにも簡単に導入できる情報漏洩対策技術が求められる。
【０００４】
物理的対策と情報漏洩対策とを兼ねた通信システムとしては、個体識別カードに取引ごとに更新されるｎ回目のカードナンバーＣｎと拠点端末の識別番号Ｔｎとを記録し、取引時に、拠点端末はＣｎとＴｎとをカード情報とともに暗号化して中央端末に送信し、中央

端末は、ＣｎとＴｎとを記録した履歴を照合して個体識別カードの正当性を確認する技術が特許文献１に開示されている。

【０００５】

また、通信システムの盗聴などによる情報漏洩対策技術としては、データ転送先は、データを暗号化するための転送鍵情報をデータ転送元に送信し、データ転送元は、この転送鍵情報を暗号鍵として転送データを暗号化してデータ転送先に送信する技術が、特許文献２に開示されている。

【０００６】

【特許文献１】特開２００３－１０８９０３号公報

【特許文献２】特開２００４－２６０３６７号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら、上記特許文献１の技術によれば、拠点端末や個体識別カードなどのハードウェアの変更が必要になるため、従来の通信システムに導入するときにコストや手間がかかりすぎるという問題があった。また、上記特許文献２の技術によれば、乱数発生装置により作成された乱数をそのままデータ暗号化用のキーに使用するので、自由度が低く、堅牢な暗号化方式とはいえないという問題があった。

【０００８】

本発明は、上記に鑑みてなされたものであって、個体識別カードのカード情報を含む情報を送受信する既存の通信システムに簡単に導入でき、自由度の高い暗号化方式によって送受信される情報の秘匿性を高める暗号化通信システムを得ることを目的とする。

【課題を解決するための手段】

【０００９】

上述した課題を解決し、目的を達成するために、本発明は、少なくとも１つの拠点端末から１つの中央端末に内容を秘匿して情報データを送信する暗号化通信システムであって、前記中央端末および夫々の前記拠点端末は、同一の入力値から同一の出力値を出力する、全ての端末で同一に統一された擬似乱数発生アルゴリズムに入力値を入力して、出力乱数列を算出する擬似乱数発生手段と、前記算出された出力乱数列から全ての端末で同一に統一されたルールに基づいて所定の桁数分の乱数列を切り出して該乱数列の各要素を夫々２値化して２値化数列を作成し、予め自端末に保持する２値化数列とパラメータ値との対応関係を示す全ての端末で同一に統一された管理テーブルに基づいて前記作成した２値化数列に対応するパラメータ値を算出する擬似乱数管理手段と、を夫々備え、前記拠点端末は、拠点端末毎に異なる１つの入力値を予め保持する第一の記憶手段と、前記中央端末に送信する情報データが入力されたとき、前記第一の記憶手段に保持されている入力値から自端末が備える前記擬似乱数発生手段および前記擬似乱数管理手段を用いて算出したパラメータ値を暗号化キーとして前記情報データを暗号化し、該暗号化した情報データを自端末の識別情報とともに前記中央端末に送信するデータ暗号化手段と、を備え、前記中央端末は、拠点端末毎に異なる全ての入力値を前記拠点端末の識別情報と対応付けて格納する第二の記憶手段と、前記拠点端末の識別情報とともに前記暗号化した情報データを受信したとき、前記第二の記憶手段に格納され前記受信した識別情報に対応付けられている入力値から自端末が備える前記擬似乱数発生手段および前記擬似乱数管理手段を用いて算出した前記暗号化キーとして使用されたパラメータ値と同一のパラメータ値を復号化キーとして、前記受信した暗号化した情報データを復号化するデータ復号化手段と、を備えることを特徴とする。

【発明の効果】

【００１０】

この発明によれば、個体識別カードのカード情報を含む情報を送受信する既存の通信システムに簡単に導入でき、自由度の高い暗号化方式によって送受信される情報の秘匿性を高める暗号化通信システムを得ることができる、という効果を奏する。

【発明を実施するための最良の形態】
【００１１】
以下に、本発明にかかる暗号化通信システムの実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。
【００１２】
実施の形態.
図１は、本発明にかかる実施の形態の暗号化通信システムの構成を示す図である。図１において、暗号化通信システム１００は、遠隔地などに設置された複数（ここでは２つ）の拠点端末２ａ、２ｂと、該拠点端末２ａ、２ｂがデータを送信する送信先の中央端末１とが、ネットワーク３を介して接続されている構成となっている。
【００１３】
拠点端末２ａ、２ｂは、ユーザが個体識別カードのカード情報を含む情報を入力して送信するための端末であり、中央端末１は、該カード情報を含む情報を受信して集中管理する端末である。例えば、本実施の形態の暗号化通信システム１００をクレジットカードの決済システムに適用する場合、中央端末１はクレジットカード会社のホストコンピュータ、拠点端末１ａ、１ｂは、各店舗にて購買者のクレジットカードが入力されるコンピュータ端末に相当する。
【００１４】
中央端末１、拠点端末２ａおよび拠点端末２ｂは、後述する各機能部を実現する構成であればどのようなハードウェア構成を有していてもかまわない。例えば、中央端末１および拠点端末２ａ、２ｂを、夫々中央演算装置（ＣＰＵ）と、ＲＯＭ、ＲＡＭ、およびハードディスクなどにより構成される記憶装置と、ネットワーク３に接続するための通信インターフェースと、を備えたコンピュータとし、夫々記憶装置に格納する所定のプログラムをＣＰＵに実行させることによって、各コンピュータに夫々中央端末１および拠点端末２ａ、２ｂの各機能部を実現させるようにしてもよい。また、ネットワーク３は、中央端末１と、遠隔地に設置された拠点端末１ａおよび１ｂとデータの送受信を行うためのネットワークであり、電話回線ネットワーク、電話回線の専用線ネットワーク、インターネット回線、イントラネット回線、各種規格の無線ネットワークなどネットワークの種類は特に限定しない。
【００１５】
中央端末１は、拠点端末別入力値生成部１１、擬似乱数発生部１２、擬似乱数管理部１３、データ復号化部１４、記憶部１５、および通信部１６の各機能部を有する。拠点端末別入力値生成部１１は、拠点端末１ａ、１ｂが中央端末１に送信するデータを暗号化するための暗号化キーであるパラメータ値を算出するための元となる入力値を、拠点端末１ａ、１ｂごとに生成して通信部１６を介して夫々拠点端末１ａ、１ｂに送信するとともに、各拠点端末１ａ、１ｂを識別する識別情報と対応付けて記憶部１５に格納する。
【００１６】
擬似乱数発生部１２は、作成された各拠点端末１ａ、１ｂごとの入力値から、擬似乱数発生アルゴリズムを使用して、擬似乱数である、出力乱数列と、該出力乱数列からパラメータ値を算出するために使用する部分を切り出す開始桁である切り出し開始層と、切り出す桁数である切り出し桁とを算出する。ここで、擬似乱数とは、一様分布でかつ過去の数から次の数が予測不能である乱数列のような数列であり、確定的な計算によって求められる。すなわち、この計算によれば、同一の入力値からは同一の擬似乱数が得られる。擬似乱数発生部１２は、このような計算を行う擬似乱数発生アルゴリズムを用い、同一の入力値から、同一の出力乱数列、切り出し開始層、および切り出し桁を算出するようにする。
【００１７】
なお、本発明の実施の形態における擬似乱数発生部１２が使用する擬似乱数発生アルゴリズムの種類は特に限定されるものではないが、上記説明したように、同一の入力値から、同一の出力乱数列、切り出し開始層、および切り出し桁を算出するものであればどのようなものであってもよい。すなわち、擬似乱数発生部１２は、出力乱数列、切り出し開始

層、および切り出し桁の３つの値を出力する１つの擬似乱数発生アルゴリズムを用いるようにしてもよいし、１つの入力値から１つの擬似乱数を出力し、出力された擬似乱数のうちの夫々異なる一部を出力乱数列、切り出し開始層、および切り出し桁とするようにしてもよいし、１つの入力値から別々の擬似乱数発生アルゴリズムを用いて夫々出力乱数列、切り出し開始層、および切り出し桁を算出するようにしてもよい。

【００１８】

擬似乱数管理部１３は、切り出し開始層が示す出力乱数列の桁から切り出し桁が示す桁数の乱数列を切り出し、切り出した乱数列の各要素を２値化して２値化数列を作成する。ここで、２値化の方法は特に限定されるものではないが、本実施の形態においては、要素が奇数の場合は１、偶数の場合は０とするようにする。そして、擬似乱数管理部１３は、予め記憶部１５に格納されている、２値化数列とパラメータ値とを対応付ける管理テーブルを参照し、パラメータ値を求める。求めたパラメータ値は、対応する拠点端末１ａ、１ｂの識別情報と対応付けて記憶部１５に格納する。

【００１９】

ここで、本実施の形態の中央端末１の記憶部１５に予め格納されている管理テーブルの詳細について説明する。図２は、管理テーブルの一例を説明する図である。図２に示す管理テーブルは、切り出し桁がｍの場合に参照される管理テーブルである。この管理テーブルにおいて、作成された２値化数列の１桁目からｍ桁目までの値とパラメータ値との対応関係が管理される。なお、管理テーブルは、切り出し桁がとりうる値のバリエーションの数だけ記憶部１５に格納されており、切り出し桁の値に応じた管理テーブルが使用されるものとする。

【００２０】

図１に戻り、データ復号化部１４は、通信部１６を介して拠点端末１ａ、１ｂのうちの何れかの端末から該端末の識別情報とともに暗号化データを受信したとき、該端末の識別情報に対応するパラメータ値を記憶部１５から読み出し、読み出したパラメータ値を復号化キーとして使用して復号化アルゴリズムを用いて暗号化データを復号化し、復号化されたデータを記憶部１５に格納する。

【００２１】

記憶部１５は、以上に説明した入力値、管理テーブル、パラメータ値、および復号化されたデータなどを格納する記憶装置である。通信部１６は、ネットワーク３を介した拠点端末１ａ、１ｂとの通信を制御する機能部である。

【００２２】

拠点端末１ａ、１ｂは、夫々同じ機能部を有する。すなわち、拠点端末１ａ、１ｂは、擬似乱数発生部２１、擬似乱数管理部２２、データ入力部２３、データ暗号化部２４、記憶部２５、および通信部２６を有する。

【００２３】

記憶部２５は、中央端末１の拠点端末別入力値生成部１１により作成され、送信されてきた入力値と、中央端末１の記憶部１５に格納されている管理テーブルと同一の管理テーブルと、自端末において作成したパラメータ値とを格納する。

【００２４】

擬似乱数発生部２１は、中央端末１が有する擬似乱数発生部１２と同一の擬似乱数発生アルゴリズムを使用し、自端末の記憶部２５に格納されている入力値に基づいて出力乱数列、切り出し開始層、および切り出し桁を算出する。擬似乱数管理部２２も同様に、中央端末１が有する擬似乱数発生部１２と同一の２値化の方法に基づき、擬似乱数発生部２１が算出した出力乱数列、切り出し開始層、および切り出し桁と自端末の記憶部２５に格納されている管理テーブルとを使用してパラメータ値を算出し、算出したパラメータ値を自端末の記憶部２５に格納する。

【００２５】

データ入力部２３は、自端末に入力される個体識別カードのカード情報を含む情報を受け付ける機能部である。該情報は、カード情報のみに限定するものではなく、例えば本実

施の形態の暗号化通信システム１００をクレジットカードの決済システムに適用する場合、購入金額やユーザにより別途入力される暗証番号など、取引ごとに送信されるデータを含ませるようにしても良い。

【００２６】

データ暗号化部２４は、受け付けたカード情報のデータを、自端末の記憶部２５に格納されているパラメータ値を暗号化キーとして使用して暗号化アルゴリズムを用いて暗号化し、暗号化したデータを通信部２６に指令して中央端末１に送信させる。ここで、データ暗号化部２４が使用する暗号化アルゴリズムおよび中央端末１のデータ復号化部１４が使用する復号化アルゴリズムの種類は特に限定しないが、復号化アルゴリズムは暗号化データを作成したときに暗号化アルゴリズムが使用した暗号化キーと同じキーを復号化キーとして該暗号化データを復号化できるものでなければならない。

【００２７】

通信部２６は、自端末と中央端末１との間でネットワーク３を介してデータの送受信を行う制御を行う機能部である。

【００２８】

このように、本実施の形態の暗号化通信システム１００においては、中央端末１が各拠点端末１ａ、１ｂに対して入力値を生成して送信するとともに、生成した入力値からパラメータ値を算出する。各拠点端末１ａ、１ｂは、夫々送信されてきた入力値からパラメータ値を算出する。各端末は同一のアルゴリズムを用いてパラメータ値を算出するので、中央端末１において記憶部１５に格納されている入力値から算出されたパラメータ値と、該入力値を受信した拠点端末１ａまたは１ｂが該入力値から算出したパラメータ値とは同一の値となる。中央端末１は、拠点端末１ａまたは１ｂが暗号化する際に暗号化キーとして使用したパラメータ値と同一のパラメータ値を使用して、暗号化されたデータを復号化する。

【００２９】

次に、以上のように構成される本実施の形態の暗号化通信システム１００の動作を説明する。まず、中央端末１が入力値を生成して各拠点端末１ａ、１ｂに送信し、各端末が入力値を格納する動作を説明する。図３は、該動作を説明するフローチャートである。

【００３０】

図３において、中央端末１の拠点端末別入力値生成部１１が、拠点端末１ａ、１ｂに送信する夫々異なる入力値を生成する（ステップＳ１）。そして、拠点端末別入力値生成部１１は、生成した各入力値を夫々拠点端末１ａ、１ｂの識別情報と対応付けて記憶部１５に格納する（ステップＳ２）。そして、拠点端末別入力値生成部１１は、生成した各入力値を、夫々対応する拠点端末１ａ、１ｂに送信する（ステップＳ３）。そして、拠点端末１ａ、１ｂは、受信した入力値を自端末の記憶部２５に格納する（ステップＳ４）。これにより、中央端末１によって生成されて保持される拠点端末別の入力値と同じ入力値が、対応する各拠点端末１ａ、１ｂにも夫々保持されるようになる。

【００３１】

続いて、各端末が入力値からパラメータ値を算出する動作を説明する。ここで、中央端末１と拠点端末１ａ、１ｂのパラメータ値を算出する動作とは等しいので、代表として拠点端末１ａを例にとって説明する。下記動作説明において、拠点端末１ａの擬似乱数発生部２１、擬似乱数管理部２２、および記憶部２５は、夫々、中央端末１の擬似乱数発生部１２、擬似乱数管理部１３、および記憶部１５に相当することはいうまでもない。図４は、パラメータ値を算出する動作を説明するフローチャートである。

【００３２】

まず、擬似乱数発生部２１は、記憶部２５に格納されている入力値に基づいて、出力乱数列、切り出し開始層、および切り出し桁を算出する（ステップＳ１１）。そして、擬似乱数管理部２２は、出力欄数列の切り出し開始層から切り出し桁分の乱数列を切り出す（ステップＳ１２）。そして、擬似乱数管理部２２は、切り出した乱数列の各要素を２値化する（ステップＳ１３）。すなわち、要素が奇数の場合、１とし、偶数の場合、０とする

。そして、擬似乱数管理部２２は、２値化した乱数列と記憶部１５に格納されている管理テーブルとからパラメータ値を算出し、記憶部１５に格納する（ステップＳ１４）。

【００３３】

例えば、ステップＳ１１にて、出力乱数列、切り出し開始層、および切り出し桁として、夫々「１３２４８」、「１」、「５」と算出されたとする。この場合、ステップＳ１２においては、切り出して算出される乱数列として、「１３２４８」が得られる。ステップＳ１３において、この乱数列を２値化され、「１１０００」が得られる。そして、ステップＳ１４において、図２に示す管理テーブルが参照され、例えば「１１０００」が図２における管理テーブルの上から３行目のエントリに該当する場合、パラメータ値として「０３」が得られる。

【００３４】

なお、中央端末１は、記憶部１５に格納されている全ての入力値についてパラメータ値を算出し、夫々拠点端末１ａ、１ｂの識別情報と対応付けて記憶部１５に格納する。

【００３５】

このようにして、各端末において、暗号化キーおよび復号化キーとして使用されるパラメータ値が算出される。そして、各拠点端末１ａ、１ｂが算出して自端末の記憶部２５に格納したパラメータ値と同じ値のパラメータ値が中央端末１においても算出され、中央端末１の記憶部２５に格納される。この動作を行うことにより、暗号化・復号化キーとして擬似乱数をそのまま使用する通信システムに比べてより堅牢な秘匿性が得られる。

【００３６】

次に、拠点端末１ａ、１ｂに入力された個体識別カードのカード情報を含む情報が暗号化されて中央端末１に送信され、中央端末１において復号化される動作を説明する。ここでは、拠点端末１ａから中央端末１に情報を送信するとして説明する。図５は、該動作を説明するフローチャートである。

【００３７】

図５において、拠点端末１ａのデータ入力部２３に個体識別カードのカード情報を含むデータが入力されると（ステップＳ２１）、拠点端末１ａのデータ暗号化部２４は、自端末の記憶部２５に格納されているパラメータ値を暗号化キーとして該データを暗号化する（ステップＳ２２）。そして、拠点端末１ａの通信部２６は、該暗号化されたデータを自端末の識別情報とともに中央端末１に送信する（ステップＳ２３）。そして、中央端末１の通信部１６が識別情報とともに該暗号化されたデータを受信すると（ステップＳ２４）、中央端末１のデータ復号化部１４は、受信した識別情報に対応付けられているパラメータ値を記憶部１５から読み出し、受信した暗号化データを、読み出したパラメータ値を復号化キーとして使用して復号化し、記憶部１５に格納する（ステップＳ２５）。

【００３８】

このようにして、拠点端末１ａ、１ｂにてユーザが個体識別カードを使用して入力したデータは、暗号化されて送信され、中央端末１の記憶部１５に格納される。

【００３９】

なお、以上の説明においては、管理テーブルは予め夫々の記憶部に格納されているものとしているが、定期的に一斉に変更されるようにしてもよい。すなわち、特許文献２に示される従来の技術に比べて、本実施の形態の暗号化通信システム１００は、より自由度の高い方法であるといえる。

【００４０】

また、各端末は、予め入力値からパラメータ値を算出して記憶部に格納しておくとして説明したが、拠点端末１ａ、１ｂは、データを暗号化する都度、パラメータ値の算出を行うようにしてもよい。また、中央端末１も同様に、暗号化データを受信する都度、パラメータ値の算出を行うようにしてもよい。

【００４１】

また、図３のステップＳ１～ステップＳ４に示す動作を、例えば一日毎など、所定の時間間隔で行うようにしてもよい。このようにすると、暗号化・復号化に用いられるパラメ

ータ値が定期的に更新されるので、より堅牢な秘匿性が得られる。

【００４２】

また、以上の説明において、度々クレジットカードの決済システムに適用する例を述べたが、本実施の形態の暗号化通信システムは、暗号化して送受信されるデータに個体識別カードのカード情報のほかに、物理的側面からの対策により入力されるあらゆるセキュリティ関連情報を含ませることができるので、少なくとも１つの拠点端末から１つの中央端末に内容を秘匿して個体識別カードを含む情報データを送信する通信システムであれば、クレジットカードの決済システム以外の通信システムにもハードウェアの変更を行うことなく簡単に導入することができる。

【００４３】

このように、本実施の形態によれば、ソフトウェアの変更のみで導入でき、かつ、暗号化および復号化アルゴリズムに使用されるキーに、元となる入力値から擬似乱数を求め、さらに擬似乱数を２値化し、予め設定される管理テーブルに基づいて該２値化した擬似乱数からパラメータ値を求め、該パラメータ値を使用するように構成したので、個体識別カードのカード情報を含む情報を送受信する既存の通信システムに簡単に導入でき、自由度の高い暗号化方式によって送受信される情報の秘匿性を高める暗号化通信システムを得ることができる。

【産業上の利用可能性】

【００４４】

以上のように、本発明にかかる暗号化通信システムは、１つ以上の拠点端末から秘匿して送信される個体識別カードのカード情報を含む情報を１つの中央端末が受信する暗号化通信システムに適用して好適である。

【図面の簡単な説明】

【００４５】

【図１】本実施の形態の暗号化通信システムの構成を示す図である。

【図２】管理テーブルの一例を示す図である。

【図３】入力値を生成する動作を説明するフローチャートである。

【図４】パラメータ値を算出する動作を説明するフローチャートである。

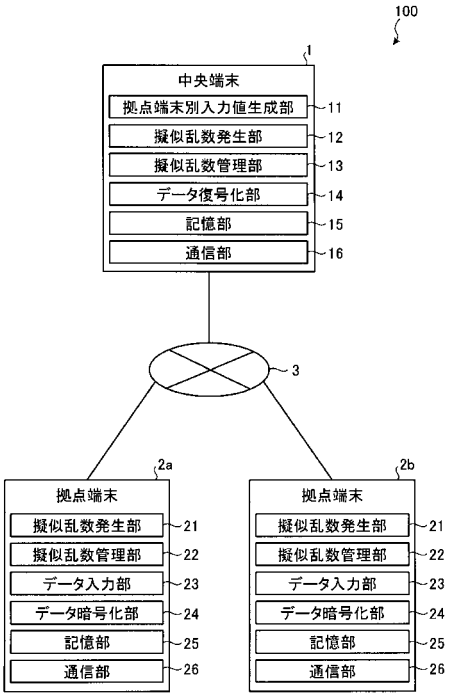
【図５】データを送受信する動作を説明するフローチャートである。

【符号の説明】

【００４６】

１　中央端末
２ａ、２ｂ　拠点端末
３　ネットワーク
１１　拠点端末別入力値生成部
１２　擬似乱数発生部
１３　擬似乱数管理部
１４　データ復号化部
１５　記憶部
１６　通信部
２１　擬似乱数発生部
２２　擬似乱数管理部
２３　データ入力部
２４　データ暗号化部
２５　記憶部
２６　通信部
１００　暗号化通信システム

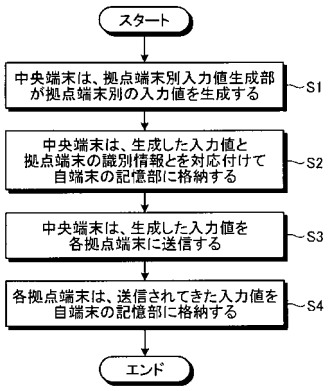
【図１】



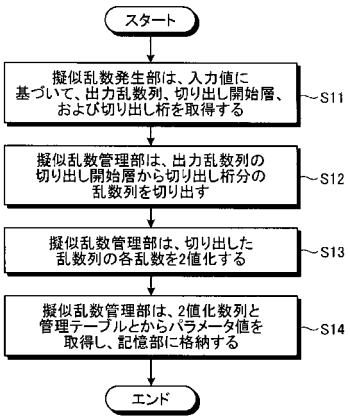
【図２】

1	2	・・・	m	パラメータ値
0	0		0	01
1	0		0	02
1	1	⋮	0	03
⋮	⋮		⋮	⋮
0	1		1	2^m

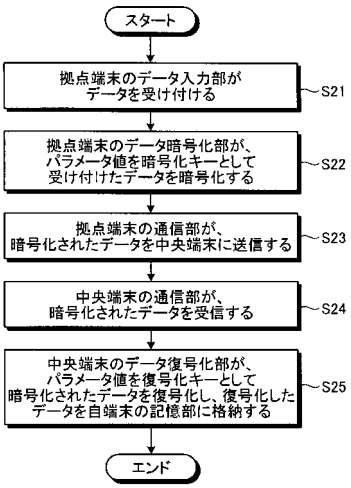
【図３】



【図４】



【図５】



フロントページの続き

(56)参考文献 特開平６－７５５２４（ＪＰ，Ａ）
特開２０００－１０４７６（ＪＰ，Ａ）
国際公開第２００４／０３２０９８（WO，Ａ１）
特表２００９－５３２９７５（ＪＰ，Ａ）
国際公開第２００７／１１３７４６（WO，Ａ１）
特開２００８－１２４９３５（ＪＰ，Ａ）
特表２０１０－５１５０８３（ＪＰ，Ａ）
特開２００８－１８５６０８（ＪＰ，Ａ）
特開２００９－５６２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００
Ｇ０９Ｃ　　１／００