(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5113630号
(P5113630)

(45)発行日　平成25年1月9日(2013.1.9)　(24)登録日　平成24年10月19日(2012.10.19)

(51)Int.Cl.			F I		
G09C	1/00	(2006.01)	G09C	1/00	650Z
H04L	9/08	(2006.01)	G09C	1/00	660D
			H04L	9/00	601Z

請求項の数 13　(全 17 頁)

(21)出願番号　特願2008-142332 (P2008-142332)
(22)出願日　平成20年5月30日 (2008.5.30)
(65)公開番号　特開2009-288616 (P2009-288616A)
(43)公開日　平成21年12月10日 (2009.12.10)
審査請求日　平成22年9月10日 (2010.9.10)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000350
ポレール特許業務法人
(72)発明者　大和田　徹
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内
(72)発明者　伯田　恵輔
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】秘密分散方法、プログラム、及び装置

(57)【特許請求の範囲】
【請求項１】
情報処理装置において、秘密分散処理を行う秘密分散処理部が、データを二分割し、前記二分割された一方のデータを基にして第１の乱数の種を生成し、第１の乱数発生器が、前記第１の乱数の種を用いて第１の複数の異なる擬似乱数列を生成し、第１の暗号器が、前記第１の複数の異なる擬似乱数列を用いて、前記二分割された他方のデータを多重に暗号化し、前記秘密分散処理部が、前記他方のデータを基にして第２の乱数の種を生成し、第２の乱数発生器が、前記第２の乱数の種を用いて第２の複数の異なる擬似乱数列を生成し、第２の暗号器が、前記第２の複数の異なる擬似乱数列を用いて、前記一方のデータを多重に暗号化することを特徴とする秘密分散方法。
【請求項２】
前記他方のデータの暗号化は、前記第１の暗号器が、前記他方のデータと前記第１の複数の異なる擬似乱数列とを順にビット毎の排他的論理和を求め、前記一方のデータの暗号化は、前記第２の暗号器が、前記一方のデータと前記第２の複数の異なる擬似乱数列とを順にビット毎の排他的論理和を求めることを特徴とする請求項１記載の秘密分散方法。
【請求項３】
前記秘密分散処理部は、前記データをシャッフルし、前記二分割することを特徴とする請求項２記載の秘密分散方法。
【請求項４】
前記秘密分散処理部は、前記暗号化した一方及び他方のデータを、互いに異なる記憶装置

に格納することを特徴とする請求項２記載の秘密分散方法。
【請求項５】
データを二分割した一方のデータを基にした第１の乱数の種と任意の数値とを入力し、第１の複数の異なる擬似乱数列を生成する第１の乱数発生器、前記データを二分割した他方のデータを、前記第１の乱数発生器により生成された前記第１の複数の異なる擬似乱数列を用いて多重に暗号化する第１の暗号器、前記一方のデータを基にした第２の乱数の種と任意の数値とを入力し、第２の複数の異なる擬似乱数列を生成する第２の乱数発生器、および、前記他方のデータを、前記第２の乱数発生器により生成された前記第２の複数の異なる擬似乱数列を用いて多重に暗号化する第２の暗号器を有することを特徴とする秘密分散装置。
【請求項６】
前記第１の暗号器は、前記他方のデータと前記第１の複数の異なる擬似乱数列とを順にビット毎の排他的論理和を出力する第１の排他論理回路群であり、前記第２の暗号器は、前記一方のデータと前記第２の複数の異なる擬似乱数列とを順にビット毎の排他的論理和を出力する第２の排他論理回路群であることを特徴とする請求項５記載の秘密分散装置。
【請求項７】
前記第１の暗号器により暗号化された前記他方のデータを格納する第１の記憶装置と前記第２の暗号器により暗号化された前記一方のデータを格納する第２の記憶装置とをさらに有することを特徴とする請求項６記載の秘密分散装置。
【請求項８】
前記一方のデータの長さを入力する入力装置をさらに有することを特徴とする請求項６記載の秘密分散装置。
【請求項９】
前記第１の暗号器は、前記他方のデータを、前記第１の複数の異なる擬似乱数列を順次用いて多重に暗号化するブロック暗号器群であることを特徴とする請求項５記載の秘密分散装置。
【請求項１０】
秘密分散処理を行う秘密分散処理部が、データを二分割し、前記二分割された一方のデータを基にして第１の乱数の種を生成し、第１の乱数発生器が、前記第１の乱数の種を用いて第１の複数の異なる擬似乱数列を生成し、第１の暗号器が、前記第１の複数の異なる擬似乱数列を用いて、前記二分割された他方のデータを多重に暗号化し、前記秘密分散処理部が、前記他方のデータを基にして第２の乱数の種を生成し、第２の乱数発生器が、前記第２の乱数の種を用いて第２の複数の異なる擬似乱数列を生成し、第２の暗号器が、前記第２の複数の異なる擬似乱数列を用いて、前記一方のデータを多重に暗号化する手順をコンピュータに実行させることを特徴とする秘密分散プログラム。
【請求項１１】
前記他方のデータの暗号化は、前記第１の暗号器が、前記他方のデータと前記第１の複数の異なる擬似乱数列とを順にビット毎の排他的論理和を求め、前記一方のデータの暗号化は、前記第２の暗号器が、前記一方のデータと前記第２の複数の異なる擬似乱数列とを順にビット毎の排他的論理和を求める手順をコンピュータに実行させることを特徴とする請求項10記載の秘密分散プログラム。
【請求項１２】
前記秘密分散処理部は、前記データをシャッフルし、前記二分割する手順をコンピュータに実行させることを特徴とする請求項11記載の秘密分散プログラム。
【請求項１３】
前記秘密分散処理部は、前記暗号化した一方及び他方のデータを、互いに異なる記憶装置に格納する手順をコンピュータに実行させることを特徴とする請求項11記載の秘密分散プログラム。
【発明の詳細な説明】
【技術分野】

【０００１】
本発明は、電子情報を守秘すると共に不正な利用を防止するための秘密分散方法、プログラム、及び装置に関する。
【背景技術】
【０００２】
昨今、デジタルデータ利用における情報セキュリティ技術の重要性が指摘されており、その基盤技術の一つとして暗号技術がある。暗号技術は、守秘対象となるデータ（平文）に、秘密裏に保管される暗号鍵に基づく変換（暗号化）を施して暗号文を得、この暗号文からは、暗号鍵なしに平文を再現することが困難であることを安全性の根拠としている。暗号方式の安全性は、暗号鍵なしに暗号文から平文を得ることの困難性を評価尺度とすることが多く、具体的には暗号方式が用いる暗号鍵のビット長（鍵長）を用いている。例として、鍵長が１２８ビットであれば、暗号文から暗号鍵なしに平文を再現するには、２の１２８乗（2^{128}）通りの暗号鍵を候補とした総当り試行での暗号演算が必要となり、この試行に要する演算時間が、その時点で入手可能な演算器の能力をもってしても現実的でない場合に、その暗号方式は計算量的に安全であるとされる。
【０００３】
ここで、もう一つの情報セキュリティ基盤と目される技術として秘密分散技術がある。秘密分散技術とは、守秘対象となるデータを複数に分割すると共に暗号化などの処理を施すものであり、分割されたデータ片を定められた数以上集めると容易に元データを復元可能であるが、定められた数以下では元データの復元は困難であるという性質を持つものである。
【０００４】
このような秘密分散技術の一つとして、特許文献１に開示される分散データ生成技術がある。
【０００５】
【特許文献１】特開平２００６－３１１３８３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
特許文献１によれば、二分割されたデータ片の一片から元データ全体を得ることが不可能という、単なる暗号方式では得られない付加的な安全の向上が実現されている。しかし、分割されたデータ片の一片から得られる情報が部分的であるという利点はあるものの、安全性の根拠は暗号処理であることから、データの不正な解読に対する耐性を示す尺度である計算量的な安全強度は従来の暗号方式と同様である。又、特許文献１においては、分割されたデータ片の一片から元データ全体を得ることは不可能であるとするが、データ分割位置が単純な等分割から著しく偏った場合が考慮されていない。分割サイズの比が９対１であった場合には、大きなデータ片の暗号解読が成功した際に、元データの９０％が得られることになる。データのフォーマットによっては、例えば、単純なテキストデータであれば得られる文脈から、この９０％の部分から全体データの推測が可能となる。ここで、データの秘密分散保管においては、データ片の等分割が、望ましい分割サイズであるとは限らない。例えば、ハードディスクなどを用いた大容量記憶装置と、フラッシュメモリなどを用いた小容量記憶装置の二者間で秘密分散する場合には、データを大小の大きく偏ったサイズに不等分割し、大片を大容量記憶装置に、小片を小容量記憶装置に、保管する必要がある。この場合には、データを不等サイズに分割した際にも安全性の劣化を防止することが課題となる。
【０００７】
以上より、本発明の課題は、データを不等サイズに分割した際にも安全性の劣化を防止する秘密分散方法、プログラム、及び装置を提供することにある。
【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、本発明は、データを二分割して二つのデータ片を得、二分割されたデータの各々他方を由来とするデータを擬似乱数生成器の乱数生成元として用いた複数の異なる擬似乱数列によって、それぞれのデータを多重に暗号化する秘密分散方法、プログラム、及び装置である。ここで、他方を由来とするデータを乱数生成元とするということは、一方のデータの暗号化のために他方のデータを基にしたデータを乱数生成元として互いに（タスキがけの関係で）使用することである。

【０００９】

本発明の具体的な態様は次のような秘密分散方法、装置及びプログラムである。

【００１０】

データを二分割し、二分割した一方のデータを基にして第１の乱数の種を生成し、第１の乱数の種を用いて第１の複数の異なる擬似乱数列を生成し、第１の複数の異なる擬似乱数列を用いて、二分割した他方のデータを多重に暗号化し、他方のデータを基にして第２の乱数の種を生成し、第２の乱数の種を用いて第２の複数の異なる擬似乱数列を生成し、第２の複数の異なる擬似乱数列を用いて、一方のデータを多重に暗号化する秘密分散方法、装置及びプログラムである。

【００１１】

本発明の望ましい他の態様は、他方のデータの暗号化は、他方のデータと第１の複数の異なる擬似乱数列とを順にビット毎の排他的論理和を求め、一方のデータの暗号化は、一方のデータと第２の複数の異なる擬似乱数列とを順にビット毎の排他的論理和を求める。

【００１２】

本発明の望ましいさらに他の態様は、情報処理装置は、暗号化した一方及び他方のデータを、互いに異なる記憶装置に格納する。

【００１３】

本発明のさらに他の態様は、暗号化にブロック暗号器を用いる。

【発明の効果】

【００１４】

本発明によれば、データを不等サイズに分割した際にも安全性の劣化を防止可能な秘密分散が実現できる。

【発明を実施するための最良の形態】

【００１５】

本発明を実施するための最良の形態を実施例１～実施例３により以下に説明する。

【実施例１】

【００１６】

本実施例について、図１～図１１を用いて説明する。図１に、本実施例に係る情報処理装置(コンピュータ)の概略構成を示す。情報処理装置１０１は、バス１０７で接続したＣＰＵ１０２、揮発性記憶装置１０３、不揮発性記憶装置１０４、及び外部不揮発性記憶媒体制御装置１０６と、外部不揮発性記憶媒体制御装置１０６に接続し、その入出力を制御される外部不揮発性記憶媒体１０５とを有する。

【００１７】

１０２は、中央演算処理装置（以下、ＣＰＵとする）である。ＣＰＵ１０２は、ソフトウェアコードを読み込み、定められた処理を実行する。１０３は、ＣＰＵ１０２が演算処理を行なう際にワーク領域として用いる、ＳＲＡＭ、ＳＤＲＡＭなどの揮発性記憶装置である。１０４は、ＣＰＵ１０２が行なうべき処理が記述されたソフトウェアコード、例えば、ＯＳやアプリケーション、データを保管するための、フラッシュメモリ、ハードディスクなどの不揮発性記憶装置である。１０５は、例えばフラッシュメモリ、ハードディスクなどの不揮発性記憶媒体を用いた、情報装置１０１と接続、分離が可能な外部不揮発性記憶媒体である。１０６は、情報装置１０１、外部不揮発性記憶媒体１０５間を接続し、データのやり取りを制御する外部不揮発性記憶媒体制御装置である。１０７は、ＣＰＵ１０２、揮発性記憶装置１０３、不揮発性記憶装置１０４、外部不揮発性記憶媒体制御装置１０６などの情報処理装置１０１を構成する各機能ブロック間で命令、データをやり取り

するための命令、データバス線(以下、データバス)である。各装置の本実施例における動作は、以下、必要に応じて説明する。

【００１８】

尚、構成要素１０２から１０７は論理的構成を示し、必ずしも物理的に図と同一構成である必要はない。又、情報処理装置１０１で実行される秘密分散処理は、必ずしもＣＰＵ１０２と揮発性記憶装置１０３、不揮発性記憶装置１０４に保管されるプログラムによる実装とするする必要はなく、例えば、不揮発性記憶装置１０４や外部不揮発性記憶媒体制御装置１０６内に設ける、図示されていない専用のハードウェア、又は、図示されていない独立したＣＰＵと、メモリに保管されるプログラムによる実装としてもよく、物理的な構成方法は問わない。さらに本実施形態では、具体例の一つとして情報処理装置１０１を示したが、後述する乱数発生器や暗号器、暗号器を構成する排他論理和回路などの装置や回路による構成でも良いことは以下の説明から理解される。

【００１９】

図２は、本実施例に係る秘密分散方法のデータ分割動作の概要フローチャートであり、図３は、本実施例に係る秘密分散方法のデータ分割動作のデータ構造概要図である。図３中、ステップ２０１から２０５は、図２のフローチャートに示した処理ステップを示す。図２及び図３を参照して、以下説明する。

【００２０】

情報処理装置１０１は、秘密分散処理開始指示に従い、小片サイズによる調整を行なう（ステップ２０１）。元データをメッセージＭとし、このメッセージＭの長さをｍＬｅｎバイトとする。メッセージＭを大小２片に分割し、その分割サイズを大片ＢＬｅｎバイト、小片ＳＬｅｎバイトとする。ここで、小片サイズの最大値Ｄ、例えばＤ＝｛６４，１２８，２５６｝を予め定めておき、ＳＬｅｎが、小片サイズの最大値Ｄ以下か否かを確認する。ＳＬｅｎが小片サイズの最大値Ｄ以下であれば、ｍＬｅｎ－ＳＬｅｎによりＢＬｅｎの値を求める。又、ｎ＝ＳＬｅｎ／１６を求める。

【００２１】

次に、メッセージＭの先頭ＢＬｅｎバイト（大片）をＳＬｅｎバイト毎に分割し、その余りをαバイトとするように、ブロックに分割する（ステップ２０２）。剰余値によるバイトシャッフル又はビットシャッフルによって、乱数Ｓｅｅｄ（乱数の種）の偏り対策を行なう（ステップ２０３）。擬似乱数生成器Ｅを多段に使用し，データを攪拌(暗号化)したデータ大片の生成する（ステップ２０４）。元データを復元するために必要な暗号化したデータ小片の生成を行なう（２０５）。

【００２２】

図４～図７は、図３に示す概要のデータ構造詳細図である。図中、ステップ２０１～ステップ２０５は、図２のフローチャートに示した処理ステップを示す。

【００２３】

図４を用いて、図２のステップ２０１～ステップ２０３の処理詳細を説明する。処理対象の元データであるメッセージＭ、小片サイズＳＬｅｎ値を所与とする。ＳＬｅｎ値は１６の倍数とし、ＳＬｅｎ＝１６ｎで表す。ｎは自然数とする。すなわち、ＳＬｅｎバイトのデータは１６バイト単位にｎ分割が可能である。メッセージＭの長さをｍＬｅｎとする。大片サイズＢＬｅｎ＝ｍＬｅｎ－ＳＬｅｎを算出する（ステップ２０１）。

【００２４】

以下の手順でメッセージＭの分割を行なう（ステップ２０２）。メッセージＭの先頭からＳＬｅｎバイトずつ、データを分割していき、各々をメッセージＭ０、Ｍ１、・・・、としていく。メッセージＭがＳＬｅｎバイトの倍数でない場合、順に分割していくと、最後にデータ長がＳＬｅｎバイトに満たない分割データが生じる。ここで、メッセージＭをｍ分割した際に、最後の分割メッセージＭｍ－１をＳＬｅｎバイトとし、最後から２番目の分割メッセージＭｍ－２をＳＬｅｎバイトに満たない分割データとするように分割する。分割メッセージＭｍ－２の長さをαバイトとする。図４においては、メッセージＭを５分割（ｍ＝5）する場合を示しており、分割メッセージはＭ０～Ｍ４であり、Ｍ３の長さ

がαバイトである。

【００２５】

分割メッセージＭ０～Ｍｍ－１から、予め定めた間隔及び順序で、剰余値として定めた数バイト又は数ビットのデータを抜き取っていき（抜き取ったデータを図中にハッチングで示す。）、残ったデータに対し、データを抜いた隙間を詰める形で新しいデータ列を生成する（ステップ２０３）。抜き取ったデータは、先に生成した新しいデータ列の後ろに、抜き取った順に並べていく。生成された新しいデータ列をＭ’とし、データ列Ｍ’を、先のステップ２０２と同様の手順で分割し、分割メッセージＭ０’～Ｍｍ－１’を得る。図４においては、分割メッセージはＭ０’～Ｍ４’である。図４には、Ｍ４’が抜き取ったデータによる分割データのように図示しているが、データを抜き取る所定間隔によって抜き取ったデータを並べた先頭位置は異なる。

【００２６】

図５を用いて、図２のステップ２０４の処理詳細を説明する。図中、Ｅ（５０１，５０２）は、１２８ビット鍵、１２８ビット初期値を入力とする擬似乱数生成器を示す。ＳＬｅｎバイトの最後の分割メッセージＭｍ－１を１６バイト毎に分割し、ｎ個の１６バイト単位メッセージＭｍ－１１’～Ｍｍ－１ｎ’を得る。ｎ個の１６バイト単位メッセージＭｍ－１１’～Ｍｍ－１ｎ’の各々を鍵入力、任意のｎ個の数値Ｔ１～Ｔｎの各々を初期値入力として、ｎ個の擬似乱数生成器Ｅ(５０１)を動作させ、図示するように、これらｎ個の擬似乱数生成器Ｅ(５０１)から出力される、ｎ個の擬似乱数の各々の先頭ＳＬｅｎバイトを各々Ｓ１～Ｓｎとする。

【００２７】

これらのＳ１～Ｓｎに対し、順にビット毎の排他的論理和を求め、得られる結果をＳとする。このＳはＳＬｅｎバイトの長さのデータである。このＳを先頭から、１６バイト毎にｎ分割し、Ｓ１’～Ｓｎ’を得る。これらのＳ１’～Ｓｎ’を鍵入力、任意の数値ＩＶを初期値入力として、ｎ個の擬似乱数生成器Ｅ（５０２）を動作させ、図示するように、これらｎ個の擬似乱数生成器Ｅ（５０２）から出力される、ｎ個の擬似乱数の先頭ＢＬｅｎバイトを各々Ｒ１～Ｒｎとする。次に、分割メッセージＭ０’～Ｍｍ－２’及びＲ１～Ｒｎに対し、順にビット毎の排他的論理和を求め、得られる結果をＣ１１とする。このＣ１１は、ＢＬｅｎバイトの暗号化されたデータとなる。

【００２８】

図６及び図７を用いて、ステップ２０５の処理詳細を説明する。図６において、分割メッセージＭｍ－２’に対し、ＳＬｅｎ－αバイト分のデータパディングを行ない、端数であった分割メッセージＭｍ－２’の長さをＳＬｅｎバイトにする。図６では、αバイトのＭ３’にゼロパディングしているがパディングする内容は任意である。分割メッセージＭｍ－２’が端数ではなく、その長さがＳＬｅｎバイトであれば、データパディングは不要である。また、データパディングした後の分割メッセージを改めてＭｍ－２’とする。

【００２９】

次に、分割メッセージＭ０’～Ｍｍ－２’に対し、順にビット毎の排他的論理和を求め、得られる結果をＮ０とする。Ｎ０はＳＬｅｎバイトのデータである。更に、Ｎ０を１６バイト毎にｎ分割し、ｎ個の１６バイト単位メッセージＮ０１～Ｎ０ｎを得る。

【００３０】

次に、図７において、ｎ個の１６バイト単位メッセージＮ０１～Ｎ０ｎの各々を鍵入力、任意のｎ個の数値Ｔｎ＋１～Ｔ２ｎの各々を初期値入力として、ｎ個の擬似乱数生成器Ｅ（７０１）を動作させ、図示するように、これらｎ個の擬似乱数生成器Ｅ（７０１）から出力される、ｎ個の擬似乱数の、先頭ＳＬｅｎバイトを各々Ｎ１～Ｎｎとする。次に、これらのＮ１～Ｎｎに対し、順にビット毎の排他的論理和を求め、得られる結果をＮとする。又、分割メッセージＭｍ－１’（図示はＭ４）及びＮに対し、ビット毎の排他的論理和を求め、得られる結果をＣ２１とする。このＣ２１はＳＬｅｎバイトの長さの暗号化されたデータとなる。次に、任意の数値Ｔ２ｎ＋１を鍵入力、任意の数値ＩＶを初期値入力として、擬似乱数生成器Ｅ（７０２）を動作させ、擬似乱数生成器Ｅ（７０２）から出力

される擬似乱数の先頭４バイトをｒとする。ステップ２０３において用いられる、分割メッセージＭ０～Ｍｍ－２からデータを抜き取っていく単位となる、数バイト毎、数ビット毎などの数値を剰余値と呼ぶ。この剰余値を２バイトで表現し、ＢＬｅｎ値、ＳＬｅｎ値を各々１バイトで表現し、剰余値、ＢＬｅｎ値、及びＳＬｅｎ値を結合した４バイトデータと、ｒに対し、ビット毎の排他的論理和を求め、得られる結果をｒ’とする。上記で得られた、Ｃ１１、Ｎ、ｒを順に結合したものを分割データ大片Ｗ１とする。又、Ｃ２１、Ｓ、ｒ’を順に結合したものを分割データ小片Ｗ２とする。

【００３１】

暗号化された分割データ大片Ｗ１は不揮発性記憶装置１０４に保管され、暗号化された分割データ小片Ｗ２は外部不揮発性記憶媒体１０５に保管される。

【００３２】

メッセージＭを分割する際に、Ｍｍ－２をデータ長がＳＬｅｎバイトに満たない分割データとするよう最後の分割を行なうとしたが、データ長がＳＬｅｎバイトに満たない分割データとするのは、Ｍ０～Ｍｍ－１のいずれであっても構わない。Ｍ０～Ｍｍ－１のどのデータが、図６に示した端数としてパディングの対象となるか、事前に決めておくか、又は、分割データに、Ｍ０～Ｍｍ－１のどのデータがパディング対象なのかを示すデータを含めることで任意の位置を端数として処理すればよい。

【００３３】

以上のデータ分割動作を以下に処理アルゴリズムとして纏めて示す。

元データから分割片を得るアルゴリズム：
入力：秘密情報(メッセージ)Ｍ，Ｍのバイト長ｍＬｅｎ，小片サイズＳＬｅｎバイト
出力：分散情報Ｗ１，Ｗ２
１．　ＳＬｅｎが予め定められた小片サイズの最大値Ｄ（例えば，Ｄ＝｛６４，１２８，２５６｝など）以下か否かを確認し，もし以下でなければその旨を表示して終了する．
２．　ＢＬｅｎ＝ｍＬｅｎ－ＳＬｅｎ，ｎ＝ＳＬｅｎ／１６を計算する．
３．　ＭをＢＬｅｎバイト，ＳＬｅｎバイトに分割する（ＢＬｅｎ／１６の余りをαとする．）．
４．　Ｍの先頭ＢＬｅｎバイトデータ，最後尾のＳＬｅｎバイトデータをそれぞれ１６ｎバイト毎に分割する（Ｍの先頭ＢＬｅｎバイトデータの最後尾はαバイトとなる）
５．　ｍＬｅｎ／ＳＬｅｎより大の整数のうち，最小の整数を計算し、その値をｍｏｄｕｌｕｓとする．
６．　最上位バイトからｍｏｄｕｌｕｓバイトずつ区切り，上記区切った各ブロックに対して，上位（ｍｏｄｕｌｕｓ－１）バイトを最上位側に，下位１バイトを最下位側に振り分ける（振り分け後のデータをＭ’とする．）．
（図４を用いて説明したデータの抜き取りに関する処理（バイトシャッフル又はビットシャッフル）の具体例の一つとしてのバイトシャッフルである．）
７．　Ｍ’＝Ｍ０’｜｜Ｍ１’｜｜…｜｜Ｍｍｏｄｕｌｕｓ－１’とし，Ｍｍｏｄｕｌｕｓ－１’＝Ｍｍｏｄｕｌｕｓ－１，１’｜｜Ｍｍｏｄｕｌｕｓ－１，２’｜｜…｜｜Ｍｍｏｄｕｌｕｓ－１，ｎ’と１６バイトずつ区切る．
８．　ｆｏｒ　ｉ　ｆｒｏｍ　１　ｔｏ　ｎ　ｂｙ　＋１　ｄｏ
　　８．１．　１６バイト乱数Ｔｉを生成する．
　　８．２．　擬似乱数生成器ＥＭｍｏｄｕｌｕｓ－１，ｉ’，Ｔｉ）により１６ｎバイトの擬似乱数ｓｉを生成する．
９．　Ｓ＝（ｓ１（ＥＯＲ）ｓ２（ＥＯＲ）…（ＥＯＲ）ｓｎ）を計算する．ここで（ＥＯＲ）はビット毎の排他論理和を示す．
１０．　Ｓ＝ｓ１’｜｜ｓ２’｜｜…｜｜ｓｎ’と区切る．
１１．　ｆｏｒ　ｉ　ｆｒｏｍ　１　ｔｏ　ｎ　ｂｙ　＋１　ｄｏ
　　１１．１．　Ｅ（ｓｉ’，ＩＶ）によりＢＬｅｎバイトの擬似乱数Ｒｉを生成する．
１２．　Ｃ１１＝（（Ｍ０’｜｜Ｍ１’｜｜…｜｜Ｍｍｏｄｕｌｕｓ－２’）（ＥＯＲ）

Ｒ１（ＥＯＲ）Ｒ２（ＥＯＲ）…（ＥＯＲ）Ｒｎ）を計算する．
１３．　Ｎ０＝Ｍ０’（ＥＯＲ）Ｍ１’（ＥＯＲ）…（ＥＯＲ）（Ｍｍｏｄｕｌｕｓ－２’｜｜（００…０））＝Ｎ０１｜｜Ｎ０２｜｜…｜｜Ｎ０ｎと区切る．
１４．　ｆｏｒ　ｉ　ｆｒｏｍ　１　ｔｏ　ｎ　ｂｙ　＋１　ｄｏ
　　１４．１．　１６バイト乱数Ｔ２ｎ＋ｉを生成する．
　　１４．２．　Ｅ（Ｎ０ｉ，Ｔ２ｎ＋ｉ）により１６ｎバイトの擬似乱数Ｎｉを生成する．
１５．　Ｎ＝（Ｎ１（ＥＯＲ）Ｎ２（ＥＯＲ）…（ＥＯＲ）Ｎｎ），Ｃ２１＝Ｎ（ＥＯＲ）Ｍ４’を計算する．
１６．　１６バイト乱数Ｔ２ｎ＋１を生成する．
１７．　Ｅ（Ｔ２ｎ＋１，ＩＶ）により４バイトの擬似乱数ｒを生成する．
１８．　剰余値と各割符片のバイト長｜Ｃ１１｜，｜Ｃ２１｜を４バイトデータに格納し，上記格納した４バイトデータと擬似乱数ｒとの排他的論理和をとった値をｒ’とする．
１９．　Ｗ１＝（Ｃ１１｜｜Ｎ｜｜ｒ），Ｗ２＝（Ｃ２１｜｜Ｓ｜｜ｒ’）とし，Ｗ１，Ｗ２を出力する。

【００３４】

次に、図８及び図９を用いて、本実施例に係る秘密分散方法のデータ復元の動作概要を説明する。図８は、本実施例に係る秘密分散方法のデータ復元動作の概要フローチャートであり、図９は、本実施例に係る秘密分散方法のデータ復元動作のデータ構造詳細図である。図９中、ステップ８０１～８０４は、図８のフローチャートに示した処理ステップを示す。以下、図８及び図９を用いて説明する。

【００３５】

情報処理装置１０１は、秘密分散処理開始指示に従い、分割データ大片Ｗ１、及び、分割データ小片Ｗ２を入力し、分割データ大片Ｗ１、及び、分割データ小片Ｗ２に含まれるデータを順に取り出す。先ず、Ｗ１、及び、Ｗ２の各々最後尾４バイトに当たるｒ及びｒ’を取り出し、ｒ及びｒ’を対象として、ビット毎の排他的論理和を求めることで、剰余値、及びＢＬｅｎ値、及び、ＳＬｅｎ値を得る。ＳＬｅｎ値を認識することで、ｒ’を取り出したＷ２の残りから、Ｃ２１、及びＳを取り出す。同様に、ｒを取り出したＷ１の残りから、Ｃ１１、及びＮを取り出す（ステップ８０１）。

【００３６】

取り出したＮ、及びＣ２１を対象として、ビット毎の排他的論理和を求めることで、Ｍｎ－１’を得る（ステップ８０２）。

【００３７】

取り出したＳを１６バイト毎に分割することで、１６バイト単位メッセージＳ１’～Ｓｎ’が得られ、これらｎ個の１６バイト単位メッセージＳ１’～Ｓｎ’を鍵入力、データ分割に用いたのと同一の数値ＩＶを初期値入力として、ｎ個の擬似乱数生成器Ｅを動作させ、これらｎ個の擬似乱数生成器Ｅから出力されるｎ個の擬似乱数の先頭ＢＬｅｎバイトから各々Ｒ１～Ｒｎが得られる。次に、取り出したＣ１１、及び、Ｒ１～Ｒｎに対し、順にビット毎の排他的論理和を求めることで、Ｍ１’～Ｍｎ－２’が得られる（ステップ８０３）。

【００３８】

ステップ８０３で得られたＭ１’～Ｍｎ－１’に対し、取り出した剰余値に従い、バイト、ビット毎の順序を入替えることでメッセージＭが得られる（ステップ８０４）。

【００３９】

上記手順により、不揮発性記憶装置１０４、及び外部不揮発性記憶媒体１０５に各々分割保管されていた、分割データ大片Ｗ１、及び、分割データ小片Ｗ２から、メッセージＭを復元する。

【００４０】

以上のデータ復元動作を以下に処理アルゴリズムとして纏めて示す。

分割片から元データを復元するアルゴリズム：

入力：分散情報Ｗ１，Ｗ２
出力：秘密情報(メッセージ)Ｍ，Ｍのバイト長ｍＬｅｎ，小片サイズＳＬｅｎバイト
１．　Ｗ１＝（Ｃ１１｜｜Ｎ｜｜ｒ），Ｗ２＝（Ｃ２１｜｜Ｓ｜｜ｒ’）と区切る（ここで，Ｃ１１はＢＬｅｎバイト，Ｃ２１，Ｎ，ＳはＳＬｅｎバイト，ｒ，ｒ’は４バイト）．
２．　ｒ（ＥＯＲ）ｒ’を計算し，剰余値と各割符片のバイト長｜Ｃ１１｜，｜Ｃ２１｜を復元する．
３．　Ｍｍｏｄｕｌｕｓ－１’＝Ｃ２１（ＥＯＲ）Ｎを計算する．
４．　Ｓ＝ｓ１’｜｜ｓ２’｜｜…｜｜ｓｎ’と区切る（ここで，ｓｉは１６バイト）．
５．　ｆｏｒ　ｉ　ｆｒｏｍ　１　ｔｏ　ｎ　ｂｙ　＋１　ｄｏ
　　５．１．　Ｅ（ｓｉ’，ＩＶ）によりＢＬｅｎバイトの擬似乱数Ｒｉを生成する．
６．　（Ｍ０’｜｜Ｍ１’｜｜…｜｜Ｍｍｏｄｕｌｕｓ－２’）＝Ｃ１１（ＥＯＲ）Ｒ１（ＥＯＲ）Ｒ２（ＥＯＲ）…（ＥＯＲ）Ｒｎを計算する．
７．　Ｍ　’＝Ｍ０’｜｜Ｍ１’｜｜…｜｜Ｍｍｏｄｕｌｕｓ－１’とし，ステップ２で求めた剰余値を用いて分散処理ステップ６の逆変換を行い，逆変換の結果Ｍを出力する。

【００４１】

図１０は、本実施例に係る情報処理装置１０１のソフトウェア構成の概略図である。図中、APLは、不揮発性記憶装置１０４及び外部不揮発性記憶媒体１０５に保管される何らかのデータを取り扱うユーザアプリケーション１００１である。アプリケーション１００１の仕様は任意であり、例えば、図１に図示しない、キーボードやマウスの類の入力装置、表示装置などの出力装置を介して、本実施例に係る情報処理装置１０１のユーザとのやり取りを行なうものであってもよいし、図１に図示しない、何らかのセンサ装置の類の入力装置、ネットワークやシリアル通信などの何らかの通信装置を介して、他の機器類とのやり取りをおこなうものであってもよい。本実施例に係る秘密分散処理を行なう秘密分散処理部１００２は、アプリケーション１００１から見た場合に、ファイルシステムとして振舞うインタフェースを備えたファイルシステムインタフェース部１００３と、ファイルシステムインタフェース部１００３を介して、ユーザアプリケーション１００１から入力するユーザデータ１００９に対してデータ分割して下位層に出力する、又、下位層から入力する分割データから本来のユーザデータを復元し、ファイルシステムインタフェース部１００３に対して出力する、データ分割、復元処理部１００４とを有する。

【００４２】

秘密分散処理部１００２の下層に、物理的な記憶装置を仮想化し、データの取り扱いを容易化する、所謂ファイルシステム１００５を設ける。ファイルシステム１００５の下層には、ファイルシステム１００５の仮想化されたデータを、物理的な記憶装置が取り扱える形に変換するシステムソフトウェアであるデバイスドライバ層１００６を設ける。デバイスドライバ層１００６には、不揮発性記憶装置１０４に相当する物理記憶デバイス１００７および外部不揮発性記憶媒体１０５に相当する物理記憶デバイス１００８を接続する。データとして、ユーザアプリケーション１００１が、物理的な記憶装置へ保管されていると認識するユーザデータ１００９、物理記憶デバイス１００７に保管される分割データ大片Ｗ１（１０１０）及び物理記憶デバイス１００８に保管される分割データ小片Ｗ２（１０１１）を図示してある。

【００４３】

秘密分散を用いない、従来の情報処理装置は、秘密分散処理部１００２を有せず、ユーザアプリケーション１００１が取り扱うユーザデータ１００９は、ファイルシステム１００５、及びデバイスドライバ層１００６を介し、物理記憶デバイス１００７の１０１０の位置に直接保管される。これに対し、秘密分散処理部１００２は、上位層に対しては、ファイルシステムとして振舞い、データ分割、復元処理部１６０４が、メッセージＭと、分割データ大片Ｗ１、及び分割データ小片Ｗ２との関係を把握し、ファイルシステム１００５に対しては、分割データ大片Ｗ１、分割データ小片Ｗ２を独立した２つのデータ(ファイル)として取り扱う。以上により、ユーザアプリケーション１００１に、秘密分散を利

用していることを意識させない運用が可能である。

【００４４】

以上から明らかなように、図１０のＡＰＬ１００１の階層からデバイスドライバ層１００６は、一部分を図１に図示しないファームウエアによるが、揮発性記憶装置１０３及び／又は不揮発性記憶装置１０４に格納されるソフトウェアにより実現される。そのソフトウェアをＣＰＵ１０２が実行することにより、本実施例の動作を実現する。なお、情報処理装置は、本実施例の動作を実行する専用のハードウェアで実現しても良い。

【００４５】

図６及び図７に示したように、分割データ大片Ｗ１、分割データ小片Ｗ２に含まれる、メッセージＭに対応する暗号文であるＣ１１及びＣ２１は、ある特定の鍵長の擬似乱数生成器による暗号化をｎ回繰り返し行なっている。これにより、鍵長をｎ倍化した効果が得られ、安全性が改善されている。これにより、メッセージＭを単純な等分割ではなく、著しく偏って分割したとしても、データ大片から多くの情報が漏洩する危険性に対して、安全性を確保している。

【００４６】

一般に、安全性の根拠として独立した真性乱数データの生成を必要とする。生成される乱数値は擬似乱数生成器への「種」入力として用いられることから、安全性に大きな影響を与えることになる。一般的に、外部的な悪意による制御が困難、且つ性質のよい乱数生成源を安価に得るのは困難であり、例えば半導体素子の熱雑音に基づく乱数生成器を専用に具備する半導体装置を用いるなどコスト要因となる場合がある。したがって、低コストでの秘密分散利用に際して、独立した乱数データの生成を不要とすることも課題である。この課題に対して、本実施例では、擬似乱数生成器Ｅの「種（Ｓｅｅｄ）」入力である鍵及び初期値として、メッセージＭに由来するデータ、及び、任意の固定値を組み合わせて用いることで多様性を確保し、独立した真性乱数生成源を不要としており、装置実現の低コスト化に寄与している。

【００４７】

図５、図７において、擬似乱数生成器Ｅを、１２８ビット鍵、１２８ビット初期値を入力としたが、必ずしも、この鍵長に限定するものではなく、例えば、２５６ビット鍵を用いる乱数生成器を用いてもよい。詳細な説明は省略するが、その際には、小片サイズＳＬｅｎを３２の倍数とし、且つ、１６バイト単位メッセージに代わって、３２バイト単位メッセージを使うことでデータ分割及び復元が可能である。

【００４８】

図５、図７における擬似乱数生成器Ｅを、１２８ビット鍵、１２８ビット初期値を入力としつつ、小片サイズＳＬｅｎを３２の倍数とし、且つ、３２バイト単位メッセージを使う構成としてもよい。この場合には、各々の３２バイト単位メッセージを１６バイトデータに二分割し、一方を１２８ビット鍵、１２８ビット初期値の擬似乱数生成器Ｅの鍵入力、他方を、任意の定数であるＴ１～Ｔｎ、Ｔｎ＋１～Ｔ２ｎ、ＩＶの代わりの初期値入力として用いることが可能である。

【００４９】

図５、図７において、Ｅを擬似乱数生成器としたが、このＥをブロック暗号器としてもよい。図５におけるＥ５０１、５０２、及び図7におけるＥ７０１、７０２は、所謂カウンタモードのブロック暗号器を用いても構成できる。又、図５に示す構成は、図１１のようにしてもよい。図１１は、図５に示した本実施例に係る秘密分散方法のデータ分割動作のデータ構造詳細図の別形態である。図１１において、Ｅ（１１０１）はＣＢＣモードのブロック暗号器である。メッセージＭ’に対し、ＣＢＣモードのブロック暗号を施してＣ１を得、同様にＣ１に対し、ＣＢＣモードのブロック暗号を施してＣ２を得、以下繰り返して、最終的にＣ１１を得る。図中、他の構成は図５と同一であり、説明は省略する。又、データ復元については図８及び図９を用いた説明と同様であるので、説明は省略する。

【００５０】

以上、本実施例によれば、メッセージＭを単純な等分割ではなく、著しく偏って分割し

たとしても、データ大片から多くの情報が漏洩する危険性を避けることができる。
【００５１】
また本実施例によれば、専用の真性乱数生成器を具備することなく、安全な秘密分散が可能となることを特徴とする情報処理装置を実現可能である。
【実施例２】
【００５２】
本実施例を、実施例１と異なる部分を中心に説明する。
【００５３】
図１２は、本実施例に係る秘密分散方法のデータ分割動作の概要フローチャートである。
【００５４】
情報処理装置１０１は、キーボードやマウスの類の入力装置を介して行なわれるユーザの指示に従い、小片サイズＳＬｅｎを指定する（ステップ１２０１）。以下、ステップ２０１以下に従い、データ分割処理を実行する。ステップ２０１以下のデータ分割手順、及び、データ復元手順は、図３～図９に示した実施例１と同様であり、説明は省略する。又、本実施例に係る情報処理装置のソフトウェア構成の概略についても図１０に示した実施例１と同様であり、説明は省略する。
【００５５】
図１３は、本実施例に係る秘密分散方法におけるユーザ操作画面の概略図である。例えば、プルダウンメニューのような形式１３０１で、小片サイズＳＬｅｎを具体的に選択指定してもよいし、スクロールバーのような形式１３０２で、小片サイズＳＬｅｎを大小直感的に指定してもよい。又、実施例１の説明で示したように、小片サイズは暗号化の繰り返し数と比例関係にある。したがって、小片サイズを直接指定する代わりに、暗号強度、ここでは暗号鍵長を指定１３０３することで、間接的に小片サイズを指定してもよい。
【００５６】
このような構成により、本実施例に掛かる情報処理装置の不揮発性記憶媒体１０４、外部不揮発性記憶媒体１０５に記憶するデータの分割サイズをユーザが任意に決定することが可能となる。これにより、不揮発性記憶媒体１０４、外部不揮発性記憶媒体１０５の容量に応じて効率的なデータ分割が可能となると共に、任意のデータ毎にユーザが暗号化に用いる鍵長を任意に設定可能となることから、データの重要度に応じて、安全性の強弱を設定可能となる効果が得られる。
【００５７】
以上、本実施例によれば、記憶媒体の容量に応じた効率的なデータ分割、及びデータ毎の安全性強度設定が可能である。
【実施例３】
【００５８】
本実施例を、実施例１と異なる部分を中心に説明する。
【００５９】
図１４は、本実施例に係る秘密分散方法のデータ分割動作の概要フローチャートである。情報処理装置１０１は、ステップ２０１～２０５に従い、データ分割処理を行なう。ステップ２０１～２０５のデータ分割手順は、図３～図７に示した実施例１と同様であり、説明は省略する。
【００６０】
次に、Ｃ１１及びＣ２１を対象にデータのランダム化を行ない、Ｃ１１’及びＣ２１’を得る。分割データ大片Ｗ１、分割データ小片Ｗ２の、Ｃ１１及びＣ２１をそれぞれＣ１１’及びＣ２１’で置き換えることで、最終的な分割データ大片Ｗ１、分割データ小片Ｗ２を得る（ステップ１４０１）。
【００６１】
図１５は、本実施例に係る秘密分散方法のデータ分割動作のデータ構造詳細図である。図中に、図１４のフローチャートに示した処理ステップ１４０１を示す。ＢＬｅｎバイト

の暗号化データＣ１１，ＳＬｅｎバイトの暗号化データＣ２１に対して、ステップ２０３に示したのと同様の手順により、データの抜き取り、及び、並べ替えを施し、Ｃ１１’及びＣ２１’を得る。データ抜き取りのバイト数又はビット数は、図７に示した剰余値に格納する。Ｃ１１は、擬似乱数生成器Ｅから出力される乱数列のビット毎排他的論理和を繰り返すことで得られているが、Ｃ１１’は、途中のデータを抜き取っていることから、剰余値を元にして正しいＣ１１を復元することなしに擬似乱数生成器Ｅから出力される乱数列をそのままビット毎排他的論理和処理を行なっても、途中でデータと対応する適切な乱数値との位相ずれが生じ、正しい復号が行なわれない。これにより、暗号の攻撃耐性が向上する効果が得られる。

【００６２】

尚、データ復元手順は、図８、及び図９に示した手順と概略同様であるが、図８のステップ８０２に先立ち、Ｃ１１’及びＣ２１’からＣ１１及びＣ２１を得る処理が必要である点が異なっている。

【００６３】

以上、本実施例によれば、暗号の攻撃耐性が向上する。。

【００６４】

本実施形態によれば、情報処理装置において、専用の真性乱数生成器を具備することなく、情報漏洩を防止し、安全にデータを保管する秘密分散が可能となる。

【図面の簡単な説明】

【００６５】

【図１】実施例１に係る情報処理装置の概略構成図である。
【図２】実施例１に係る秘密分散方法のデータ分割動作の概要フローチャートである。
【図３】実施例１に係る秘密分散方法のデータ分割動作のデータ構造概要図である。
【図４】実施例１に係る秘密分散方法のデータ分割動作のデータ構造詳細図である。
【図５】実施例１に係る秘密分散方法のデータ分割動作のデータ構造詳細図である。
【図６】実施例１に係る情報処理装置のデータ分割動作のデータ構造詳細図である。
【図７】実施例１に係る情報処理装置のデータ分割動作のデータ構造詳細図である。
【図８】実施例１に係る秘密分散方法のデータ復元動作の概要フローチャートである。
【図９】実施例１に係る秘密分散方法のデータ復元動作のデータ構造概要図である。
【図１０】実施例１に係る情報処理装置のソフトウェア構成の概略図である。
【図１１】実施例１に係る秘密分散方法のデータ分割動作のデータ構造詳細図の別形態である。
【図１２】実施例２に係る秘密分散方法のデータ分割動作の概要フローチャートである。
【図１３】実施例２に係る秘密分散方法におけるユーザ操作画面の概略図である。第
【図１４】実施例３に係る秘密分散方法のデータ分割動作の概要フローチャートである。
【図１５】実施例３に係る情報処理装置のデータ分割動作のデータ構造詳細図である。

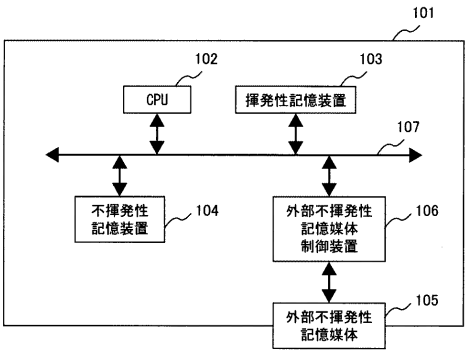
【符号の説明】

【００６６】

１０１：情報処理装置、１０２：ＣＰＵ、１０３：揮発性記憶装置、１０４：不揮発性記憶装置、１０５：外部不揮発性記憶媒、１０６：外部不揮発性記憶媒体制御装置、１０７：データバス、１００１：ユーザアプリケーション、１００２：秘密分散処理部、１００３：ファイルシステムインタフェース部、１００４：データ分割、復元処理部、１００５：ファイルシステム、１００６：デバイスドライバ層、１００７：物理記憶デバイス、１００８：物理記憶デバイス、１００９：ユーザデータ、１０１０：分割データ大片、１０１１：分割データ小片。

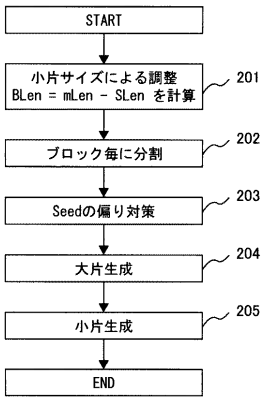
【図１】

図 1



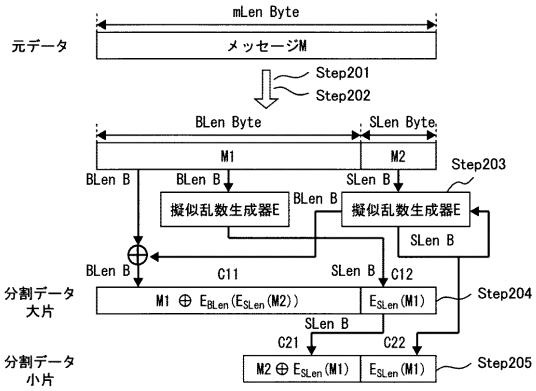
【図２】

図 2



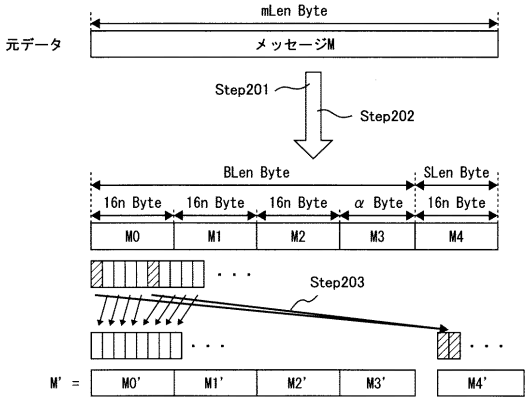
【図３】

図 3



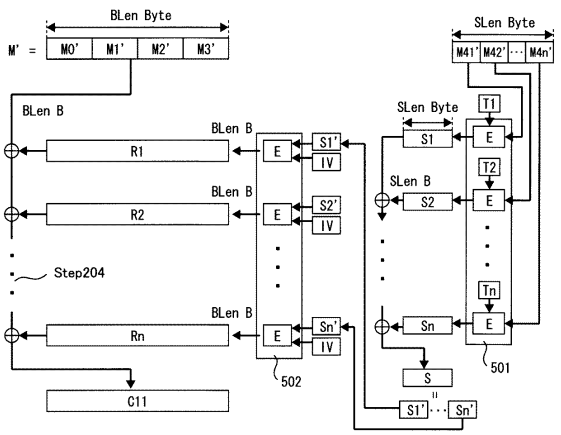
【図４】

図 4



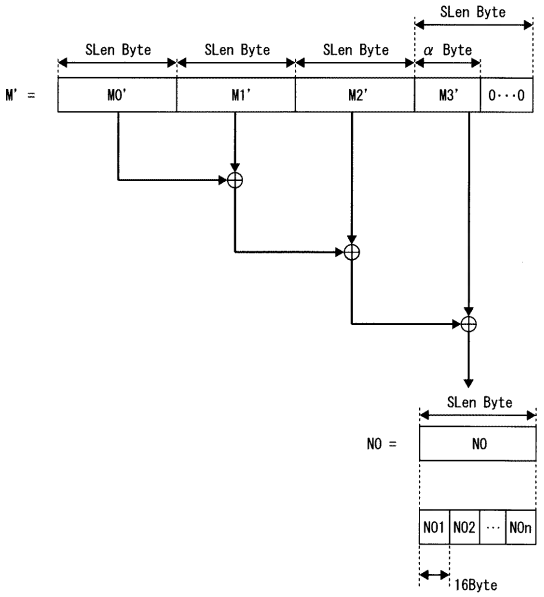
【図５】

図 5



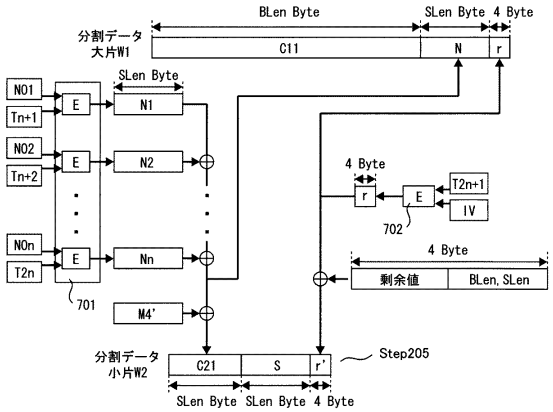
【図６】

図 6



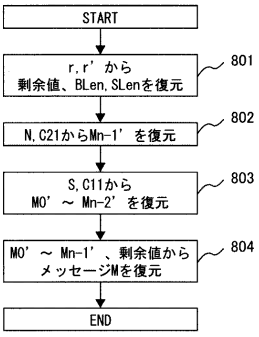
【図７】

図 7



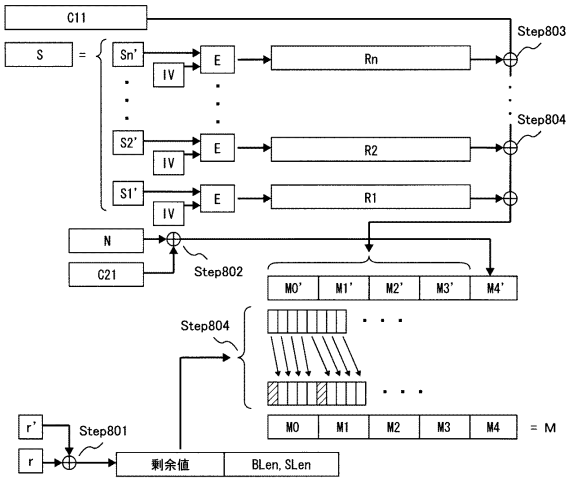
【図８】

図 8



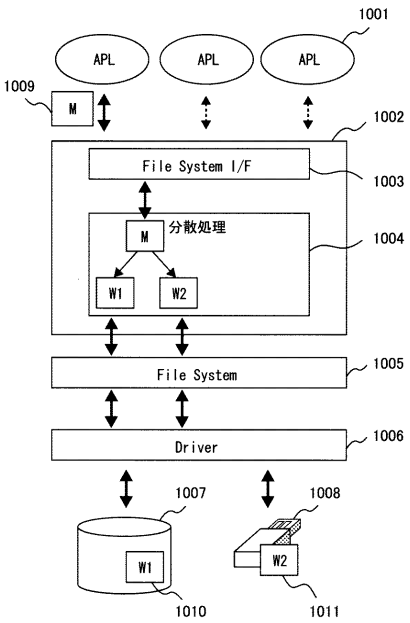
【図９】

図 9



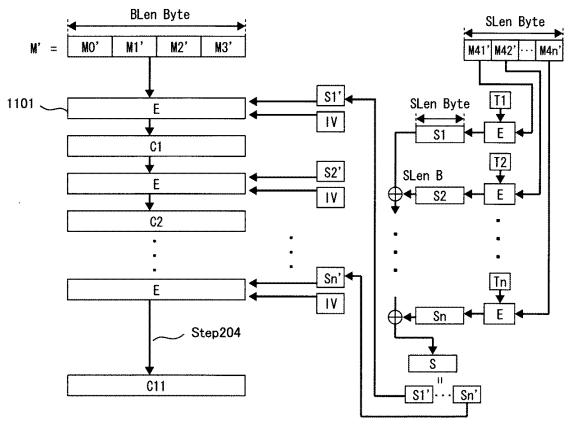
【図１０】

図 10



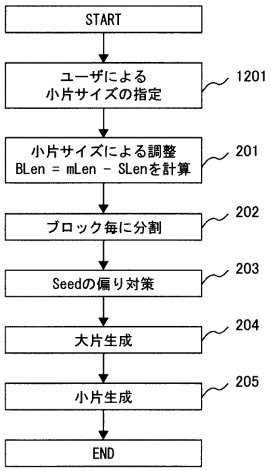
【図１１】

図 11



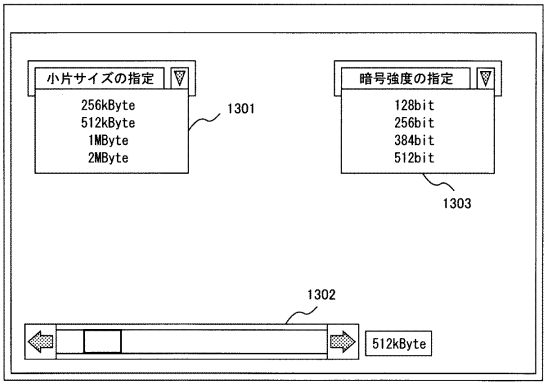
【図１２】

図 12



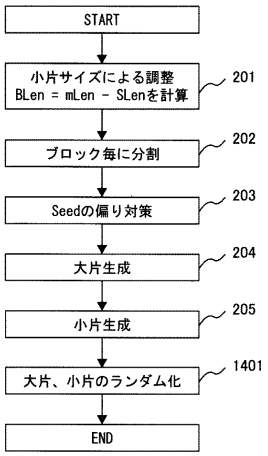
【図１３】

図 13



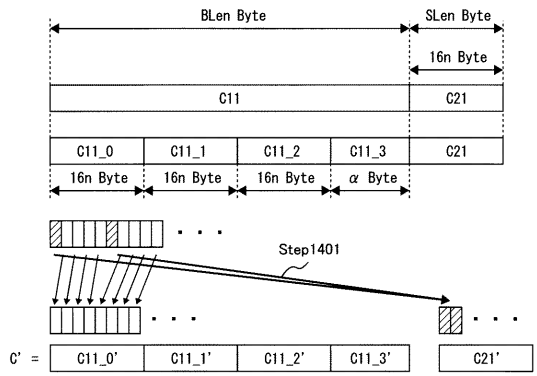
【図１４】

図 14



【図１５】

図 15



フロントページの続き

(72)発明者　坂崎　尚生
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

審査官　石田　信行

(56)参考文献　特開２００７－１２２３３６（ＪＰ，Ａ）
特開２００７－２４３３２９（ＪＰ，Ａ）
特開２００４－２１３６５０（ＪＰ，Ａ）
特開２００４－１４７２１８（ＪＰ，Ａ）
特開２００３－３４５２４３（ＪＰ，Ａ）
特開平１１－０９５９８４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／２４