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

特許第4146934号
(P4146934)

(45)発行日　平成20年9月10日(2008.9.10)　(24)登録日　平成20年6月27日(2008.6.27)

(51)Int.Cl.			F I		
H04L	1/00	(2006.01)	H04L	1/00	B
G09C	1/00	(2006.01)	G09C	1/00	610A
H04K	1/00	(2006.01)	H04K	1/00	
H04L	9/20	(2006.01)	H04L	9/00	653

請求項の数 9　(全 12 頁)

(21)出願番号　特願平10-196416
(22)出願日　平成10年7月13日(1998.7.13)
(65)公開番号　特開平11-112479
(43)公開日　平成11年4月23日(1999.4.23)
審査請求日　平成17年7月13日(2005.7.13)
(31)優先権主張番号　896,002
(32)優先日　平成9年7月17日(1997.7.17)
(33)優先権主張国　米国(US)

(73)特許権者　398038580
ヒューレット・パッカード・カンパニー
HEWLETT-PACKARD COMPANY
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000
(74)代理人　100075513
弁理士　後藤　政喜
(74)代理人　100084537
弁理士　松田　嘉夫
(72)発明者　ジョシュ・ホガン
アメリカ合衆国カリフォルニア州ロス・アルトス　キングスウッド・ウエイ　620

審査官　谷岡　佳彦

最終頁に続く

(54)【発明の名称】暗号化装置および暗号化方法

(57)【特許請求の範囲】

【請求項１】

ランダムデータ列を生成し、誤り訂正のための冗長列を作成する疑似乱数生成器を備え、誤り訂正能力を維持しながらデータを暗号化する装置であって、

前記ランダムデータ列は、前記冗長列と組み合わされたとき、暗号化されるデータのサイズと等しく、

前記冗長列は、前記暗号化されるデータに適用されるのと同じ誤り訂正符号生成方式を用いて作成される、

ことを特徴とする装置。

【請求項２】

前記疑似乱数生成器は、前記ランダムデータ列を生成する前記乱数生成器を初期化するための乱数シードを生成するモジュールをさらに備え、

前記乱数シードの長さは要求される暗号強度を確実に得るのに十分な長さであることを特徴とする請求項１に記載の装置。

【請求項３】

前記疑似乱数生成器は、前記暗号化されるデータと前記ランダムデータ列との排他的論理和を取ることによって暗号化されたデータ列を作成するモジュールをさらに含むことを特徴とする請求項１または２に記載の装置。

【請求項４】

ホストプロセッサに配置された誤り訂正モジュールをさらに備え、

前記誤り訂正モジュールはホストプロセッサあるいは他の実体上で前記暗号化された列の誤り訂正を実行することを特徴とする請求項１から３までのいずれか１項に記載の装置。

【請求項５】

信頼できる実体に配置された誤り訂正モジュールをさらに備え、

前記誤り訂正モジュールはホストプロセッサ上で前記暗号化されたデータ列の誤り訂正を実行することを特徴とする請求項１から４までのいずれか１項に記載の装置。

【請求項６】

前記疑似乱数生成器は前記乱数シードを信頼できる実体に転送するモジュールをさらに備えることを特徴とする請求項１から５までのいずれか１項に記載の装置。

【請求項７】

前記信頼できる実体に配置され、前記所定の疑似乱数生成器を用いて第２のデータ列を生成するモジュールをさらに含み、

前記第２のデータ列の長さは前記データ列の長さと等しいことを特徴とする請求項１から６までのいずれか１項に記載の装置。

【請求項８】

前記第２のデータ列を生成するモジュールは、前記暗号化された列と前記第２のデータ列との排他的論理和を取ることによって複合化されたデータ列を作成するモジュールをさらに備えることを特徴とする請求項７に記載の装置。

【請求項９】

誤り訂正能力を維持しながらデータを暗号化する方法であって、

ランダムデータ列生成器を設けることと、

誤り訂正のための冗長列を作成することとを含み、

前記ランダムデータ列は、前記冗長列と組み合わされたとき、暗号化されるデータのサイズと等しく、

前記冗長列は前記暗号化されるデータに適用されるのと同じ誤り訂正符号生成方式を用いて作成される、

ことを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は計算機環境におけるデータの暗号化に関する。特に、本発明は他の実体により受信および平化すべきデータ符号語を元のデータの誤り訂正能力を維持しながら暗号化する方法に関する。

なお、本明細書では暗号化：encryptionに対し暗号分を平文にもどす復号：decryptionを平化と称し、符号化：encoding、復号（化）：decodingと区別しやすくした。

【０００２】

【従来の技術】

誤り訂正法はデータ伝送チャネルおよびコンパクトディスク（CD）、デジタルビデオディスク（DVD）、デジタルデータ記憶装置（DDS）およびデジタルビデオカセット（DVC）等のデータ記憶装置においてデータの完全性の維持に一般的に用いられている。かかる誤り訂正方法は媒体の欠陥やノイズ等の異常に起因する誤りを訂正するものである。通常の記憶装置のアプリケーションでは、データをホストプロセッサに伝送する前にドライブ上のプロセッサを用いて誤り訂正を実行する。

【０００３】

記憶装置ドライブのコストを低減する方法の１つに、ドライブ自体から誤り訂正アルゴリズムを削除し、その機能をホストコンピュータで実行するという方法がある。近年の記憶システムでは、ドライブ上での誤り訂正の実行に要する回路は高コストである。この回路は高価なスタティックランダムアクセスメモリ（RAM）および多大な処理力を必要とする。記憶されたデータの誤り訂正をドライブにおいてではなくホストプロセッサにおいてソ

フトウエアを用いて実行することが可能である。
【０００４】
この方法は途切れのない連続データストリームが必要ではない用途では特に有益である。誤り訂正に要する処理力は与えられたブロック内における訂正すべき誤りの数とともに劇的に変化する。しかし、１つのブロックで多数の誤りが発生する確率は非常に低い。したがって、処理力の低いホストプロセッサでも少数の誤りについては即応して訂正することができ、多数の誤りが発生してもその発生頻度の低い場合には、データフローを止めて反復的に誤り訂正を実行することができる。
【０００５】
【発明が解決しようとする課題】
当業界において、特に財産的データの無許可複製を防止するためにデータの暗号化すなわちスクランブルの必要性が増大しつつある。説明の目的上、暗号化およびスクランブルという用語は互換的に用いられる。データをコンピュータバス上に解放する前にそのすべてあるいは一部を暗号化することを提案する方式もある。これは、ドライブとカラー動画符号標準化作業グループ（MPEG）復号器等の有権実体:trusted entityとの間で取り決められる暗号化鍵を用いて実行される。この種の暗号化すなわちスクランブリング方式は通常誤り訂正符号語の完全性が維持されず、誤り訂正を暗号化すなわちスクランブリングの前にドライブ内で実行しなければならず、したがってホストプロセッサでは誤り訂正タスクは実行されない。
【０００６】
誤り訂正符号語の完全性を維持しながらデータを暗号化する暗号化方式を提供することが有益である。すなわち、この方式によってたとえば秘密データへのアクセスを許さずホストコンピュータによって秘密データの誤り訂正を実行することが可能になる。さらに、記憶装置ドライブあるいは該ドライブへのアクセス権を有する有権実体（たとえば、平化の実行を要求される実体）に重い負担を課すことなく容易に実行可能な暗号化方式を提供することが有益である。
【０００７】
【課題を解決するための手段】
本発明は元データの誤り訂正能力を維持しながらデータおよびそれに付随する冗長バイトを暗号化するデータ暗号化/平化システムを提供するものである。その結果、本発明は記憶装置ドライブのコスト低減を可能にする。本発明は伝送チャネルあるいは記憶装置ドライブさらに他の装置上で容易に実施することができる。
【０００８】
ここで説明するシステムにおいては、誤り訂正機能は記憶装置ドライブからは除去され、ホストプロセッサあるいは有権実体によって実行される。記憶装置ドライブは媒体から誤り訂正符号を含む生データを読み出し、このデータを次のように暗号化する。生データと同じ大きさの乱数を含むデータブロックが作成される。このランダムデータブロックに生データと同じ誤り訂正符号生成方式を用いて誤り訂正符号が追加される。生データとランダムデータブロックの排他的論理和が取られ、暗号化されたデータブロックが形成される。得られた誤り訂正符号は有効であり、したがってこの新たなデータブロックは暗号化された形式のままで訂正することができる。
【０００９】
新たなデータブロックの誤り訂正は秘密データを無許可のアクセスにさらすことなくホストプロセッサあるいは他の処理実体において実行することができる。その後、誤り訂正されたデータブロックは有権実体によって平化することができる。
【００１０】
平化を実行するために、有権実体は記憶装置ドライブ内で作成されたランダムデータブロックと同等なランダムデータブロックを作成する。誤り訂正されたデータブロックはランダムデータブロックと排他的論理和され、それによって元の誤り訂正された状態に戻る。
【００１１】

【発明の実施の形態】
説明の目的上、以下の説明においては記憶装置ドライブの例を用いる。しかし、本発明はデータが誤り訂正符号によって保護されたチャネルを介したデータ伝送にも同様にあてはまるものである。この方式は受信者が最初に誤り訂正を実行することなく受信したデータの暗号化を行なうことを可能にする。
【００１２】
図１において、典型的なコンピュータシステムアーキテクチャはデータバス105を含む。図１に示すデータバス105には通常バスマスターであるホストマイクロプロセッサ101が接続されている。このデータバスにはいくつかの装置、装置１ 102、装置２ 104、装置３ 103、・・・装置N 106を接続する場合がある。データはホストプロセッサ105から装置１ 102にたとえばデータバス105を介して送られる。データバス105に接続された装置はデータバス105上を転送されるあらゆるデータを監視することができる。また、かかる装置は蓄積スコープやデータ解析装置といったバス測定装置を含み、これらはデータバス105に直接接続することができる。このため、データバス105はこのコンピュータシステムの侵襲されやすく危険な領域となる。
【００１３】
かかる侵襲性のために、記憶装置ドライブのコスト低減の試みを妨げる問題が生じる。コンパクトディスク（CD）、デジタルビデオディスク（DVD）、DDSおよびDVC等の規格を用いる記憶装置ドライブはデータの完全性を維持するためにかかるドライブ上で誤り訂正法を実行する。誤り訂正機能をホストプロセッサで実行することによってドライブからこの機能を除去することによって記憶装置ドライブのコストを低減することが望ましい。ドライブのコスト低減はドライブ上で誤り訂正を実行するのに要する、高価なスタティックランダムアクセスメモリ（RAM）を含む回路を低減し、さらに必要処理力を低減することによって達成される。
【００１４】
図２に示すように、記憶装置ドライブあるいは伝送チャネル206からデータバス205を介してたとえばカラー動画符号標準化作業グループ（MPEG）復号器に転送される任意のデータは装置X 202あるいは装置Y 203によって監視することができる。したがって、このデータストリーム中のあらゆる財産的情報を発見することができる。その結果、当業界においてデータを暗号化すなわちスクランブルして財産的データの無許可の複製を防止すべしとの圧力が高まりつつある。
【００１５】
１つの方法として、データをコンピュータバス上に解放するまえにそのすべてあるいは一部を暗号化する方法がある。これはドライブとMPEG復号器等の有権実体との間で取り決められる暗号化鍵を用いて達成される。図３において、ドライブ206は、まず有権実体であるMPEG復号器204との間で暗号化鍵を取り決める。ドライブ206は媒体からデータを読み出し、そのデータに誤り訂正を実行する。続いて、ドライブ206は暗号化鍵を用いてこのデータを暗号化し、その結果得られたデータをデータバス205を介してMPEG復号器204に送る。MPEG復号器204はこのデータを受け取り、暗号化鍵を用いてそれを平化し、そのデータを処理する。この種の暗号化すなわちスクランブリング方式は通常誤り訂正符号語の完全性が維持されず、誤り訂正を暗号化すなわちスクランブリングの前にドライブ内で実行しなければならず、したがってホストプロセッサでは誤り訂正タスクは実行されない。
【００１６】
誤り訂正方式は多数存在し、本発明はそのいずれとも実施可能である。典型的な誤り訂正方式ではリードソロモン（RS）積符号が用いられ、この場合N×Mのデータブロックには冗長バイトが付加され（N+p）×（M+q）の誤り訂正符号語（ECC）ブロックが形成される。このデータブロックのN列それぞれにq個のRS冗長バイトが付加されてM+q RS符号語が形成される。この新たなブロックのM+q行のそれぞれにはp個のRS符号語が付加されN+pの長さのRS符号語が形成される。この説明の目的上、データのN×Mブロックをデータブロックと称し、この（N+p）×（M+q）ブロックをECCブロックと称する。

【００１７】
データがテープやディスクといった記憶媒体から読み出されるとき、たとえば欠陥やノイズに起因する誤りが存在する場合がある。しかし、データはRS符号語に含まれているため、かかる誤りを訂正することができる。
【００１８】
図４には例示のみを目的として簡略化したDVDフォーマットを示しており、ユーザーデータは32K バイト405に分割されている。２次元配列の各行および各列には誤り訂正符号が関係付けられている。データブロック全体のサイズは208バイト×182バイトである。このデータブロックの長さは182バイトであり、そのうち172バイトはユーザーデータ、残りの10バイトは誤り回復のために追加された誤り訂正符号（ECC）403である。同様に、行の数は208であり、16行は他のECC符号群404からなる。このデータの致命的部分は複製阻止に関する情報特に暗号化鍵を含むヘッダ情報401にある。通常の状態では、ユーザーはこのデータを受け取り、ヘッダ領域401あるいはECC符号403、404に何があるかを知る必要は全くない。この情報はデータがドライブ内にある間に抽出され、チェックされる。また、リードイン領域（図示せず）にもデータブロックがあり、機密度の高いデータを保持している。
【００１９】
誤り訂正機能がドライブから除去されホストコンピュータ内で実行されるとき問題が生じる。ホストコンピュータはこの制限されたヘッダ情報401（さらにリードイン領域の秘密データブロック）を含めてこのデータに関するすべてを知っていなければならない。このデータは開放型データバス上をドライブからホストコンピュータに転送されなければならない。データがスクランブルされるとECCの誤り訂正能力がなくなる。本発明は、なんらかの装置を用いてバスを聞いている人間にとって理解できずしかも誤り訂正を行なうことはできるようにデータを暗号化することによって、開放型コンピュータバス上での情報の転送の問題を解決するものである。
【００２０】
図５に示すように、ユーザーデータの172バイトを取り、このデータバイトについて計算された10バイトのECCを加えることによってECC符号語501が作成される。これによって、この符号語のどこかで誤りが発生した場合、ある特定の数まではかかる誤りを検出し訂正しうる一定した符号語が形成される。第２の符号語502が同様に作成されるが、これはそれに関係付けられた10バイトのECCを有するランダムデータである。これら２つの符号語の排他的論理和を取ると、別の符号語504が得られ、これもまた有効である。得られた10バイトのECCはこの新たなデータ集合にとって適切な誤り訂正符号となる。この方法は他の任意の誤り訂正単位のための符号をも生成しうるように拡張可能であることを指摘しておく。
【００２１】
本発明の一実施例においては、この方法によってデータブロック全体がカバーされる。記憶装置ドライブ内で新たなデータブロックが作成される。このデータはたとえば同じく記憶装置ドライブに配置された明確に定義された疑似乱数発生器を用いて生成される。この乱数発生器のシード（seed：種）の長さは要求される暗号強度を確実に得ることができるだけの長さである。32Kバイトのデータ領域が作成されると、それに関係するECCバイトが計算され、新たなECCブロックが完成する。
【００２２】
疑似乱数発生器によって生成された新たなデータを含むデータブロックとユーザデータの排他的論理和が取られ、第３のデータブロックが生成され、これがランダム化、すなわち暗号化あるいはスクランブルされたデータブロックである。この第３のデータブロックのデータすなわち暗号化データは保護されている。それはこのランダムデータブロックの知識がなければ元データを抽出することができないことによる。
【００２３】
上記の動作の結果、ECCの誤り訂正能力が維持される。図６に示すように、ノイズおよび/

または媒体の欠陥に起因する問題によって誤りが発生し、この誤りは元のユーザーデータブロック602全体に分散される。乱数601を含む新たなデータブロックには誤りはない。これは、このブロックが媒体に記憶されておらず、伝送されてもおらず、すなわちなんの危険もなかったためである。かかるデータブロックに誤りがあったとしても、かかる誤りもまた訂正可能であり、ここに説明した方式は満足に動作する。したがって、これら２つのブロックの排他的論理和を取ったとき、ECCの忠実性は維持される。よって、得られるデータブロック603はユーザーデータブロックと同じ位置に誤りを含み、符号語はすべて一致し、したがって誤り訂正によって誤りを十分に訂正することができる。

【００２４】

図７に示すように、得られたデータブロックは保護されており、誤り訂正を行なうためにデータバス704上を記憶装置ドライブ703からホストプロセッサ701に送られる（707）。ホスト701はこのデータブロック中の暗号化されない形式の実際の情報に対するアクセス権を有しないが、このデータブロックに対して誤り訂正を有効に実行することができる。誤り訂正タスクが完了すると、訂正されたデータが有権実体たとえばMPEG復号器702に送られる（705）。

【００２５】

有権実体たとえばMPEG復号器702は記憶装置703がユーザーデータブロックの暗号化のために作成したものと同じ乱数データ領域を作成しなければならない。たとえば、記憶装置703と有権実体702はいずれも同じシード706を有する同じ乱数発生器712、713を用いることができる。両装置が同じシードを用いる同じ乱数発生器を含むため、それらが作成するデータブロックは同一である。復号器702はいかなるECC部分も平化する必要がない。暗号化ユーザーデータはこの乱数データと再度排他的論理和され、元の状態に戻される。続いて、このデータが復号器702によって処理され、利用可能となる。たとえば、ビデオの日付の場合には、このデータを復号し、表示装置708あるいはディスプレイメモリに直接送ることができる。この非暗号化データはデータバス704には送出されない。

【００２６】

他の同様に好適な実施形態では以下のステップが実行される。

１）ドライブが乱数を生成する。乱数シードの長さは要求される暗号強度を確実に得ることができるだけの長さである。

２）ドライブが乱数シードをシードとするすなわちそれによって初期設定される所定の疑似乱数発生器を用いてデータ列を生成する。

３）ドライブが元データに用いられたものと同じ誤り訂正符号生成方式を用いた冗長性を生成する。これによって、ドライブは一連の符号語を生成し、これらの符号語は乱数シードによって決まり、また元のECCブロックと一致する。

４）ドライブがディスクあるいはテープから読み出した元の訂正されていない符号語とドライブの生成した符号語とのビット単位の排他的論理和を取る。

【００２７】

５）得られたデータストリームによってやはり有効な符号語が構成され、かかる符号語はテープあるいはディスクから読み出された符号語に含まれるあらゆる誤りを含む。ドライブによって生成された符号語は誤りを含まないため、この技術によって誤りがさらに導入されることはない。こうして得られたデータストリームは有効に暗号化され、元データの無許可の複製のリスクが生じることなく、誤り訂正のためにホストプロセッサあるいは他の処理実体に送ることができる。

６）平化はMPEG復号器等の有権実体によって実行される。これを行なうに、ドライブは標準的技術を用いて取り決められる鍵を用いてシード数NRを安全な方法で有権実体に転送する。

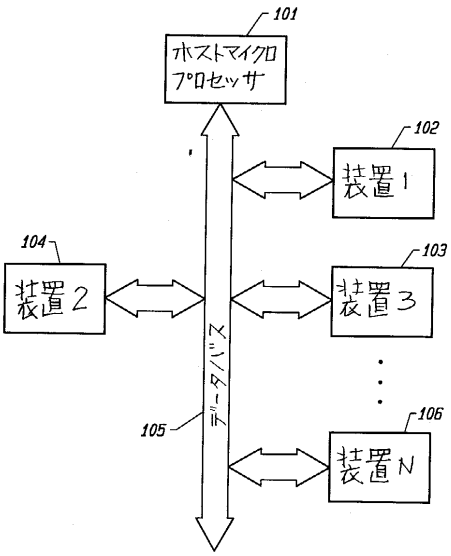
７）有権実体はドライブが生成したものと同じ疑似ランダムデータ列を生成し、この列を用いて、再度このランダムデータ列と暗号化されたデータのビット単位の排他的論理和を取ることによって、誤り訂正されているが依然として暗号化すなわちスクランブルされたデータを平化する。

【００２８】
本発明を好適な実施形態を参照して説明したが、当業者には本発明の精神と範囲から逸脱することなくここに述べたものに代わる他の用途が可能であることが容易に理解されよう。たとえば、ランダムデータ列を後続のデータの処理に再使用するか、あるいは処理すべき各データ量ごとに新たなランダムデータ列を生成することもできる。したがって、本発明は特許請求の範囲によってのみ限定されるものであるが、本発明の広範な実施の参考のために本発明の実施態様を例示する。
【００２９】
（実施態様１）
ランダムデータ列を生成し、誤り訂正のための冗長列を作成する疑似乱数発生器（713）を備え、誤り訂正能力を維持しながらデータを暗号化し暗号化されたデータ列を発生する装置であって、
前記ランダムデータ列は前記冗長列を結合したとき暗号化すべきデータのサイズとほぼ等しいかそれより大きく、
前記暗号化すべきデータに適用される誤り訂正符号生成方式を用いて前記冗長列が作成されることを特徴とする暗号化装置。
（実施態様２）
前記疑似乱数発生器は、前記ランダムデータ列の生成を開始させるための乱数シードを生成するモジュール（703）を含み、
前記乱数シードの長さは要求される暗号強度を確実に得るのに十分な長さであることを特徴とする実施態様１に記載の装置。
【００３０】
（実施態様３）
前記疑似乱数発生器はさらに、
前記暗号化すべきデータと前記ランダムデータ列の排他的論理和を取ることによって前記暗号化されたデータ列を作成するモジュールを含むことを特徴とする実施態様１または実施態様２のいずれかに記載の装置。
（実施態様４）
ホストプロセッサ（701）に配置された誤り訂正モジュールをさらに含み、
前記誤り訂正モジュールはホストプロセッサあるいは他の実体上で前記暗号化された列の誤り訂正を実行することを特徴とする実施態様１から実施態様３のいずれかに記載の装置。
【００３１】
（実施態様５）
有権実体（702）に配置された誤り訂正モジュールをさらに含み、
前記誤り訂正モジュールはホストプロセッサ上で前記暗号化されたデータ列の誤り訂正を実行することを特徴とする実施態様１から実施態様４のいずれかに記載の装置。
（実施態様６）
前記疑似乱数発生器（713）はさらに、
前記疑似乱数シードを有権実体（702）に転送するモジュールを含むことを特徴とする実施態様１から実施態様５のいずれかに記載の装置。
【００３２】
（実施態様７）
前記有権実体に配置され、前記所定の疑似乱数発生器を用いて第２のデータ列を生成するモジュール（712）をさらに含み、
前記第２のデータ列の長さは前記データ列と同じであることを特徴とする実施態様１から実施態様６のいずれかに記載の装置。
（実施態様８）
前記第２のデータ列を生成するモジュールはさらに、
前記暗号化された列と前記第２のデータ列の排他的論理和を取ることによって平化された

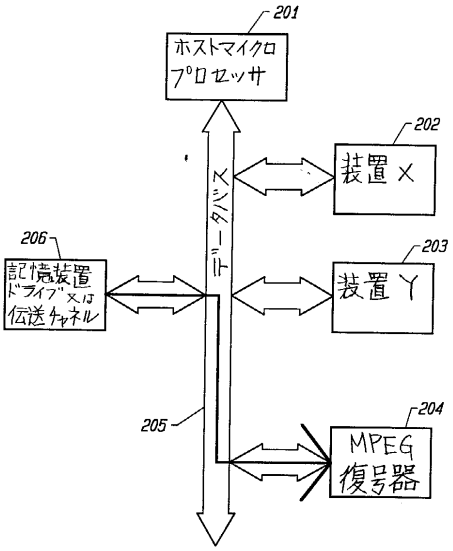
データ列を作成するモジュール（702）を含むことを特徴とする実施態様７記載の装置。
【００３３】
（実施態様９）
誤り訂正能力を維持しながらデータを暗号化する方法であって、
ランダムデータ列発生器を設けるステップ、および
誤り訂正のための冗長列を作成するステップとからなり、
前記ランダムデータ列は前記冗長列と組み合わせると暗号化すべきデータのサイズとほぼ等しいかそれより大きく、
前記冗長列は前記暗号化すべきデータに適用されたものと同じ誤り訂正符号生成方式を用いて作成されることを特徴とする暗号化方法。
【００３４】
【発明の効果】
本発明の実施により次のような利点が得られる。
-有権実体に安全な方法で送る必要のある追加情報は乱数発生器のシードのみである。
-乱数シードはセッションの始めに一度だけ生成し、暗号化し、有権実体に転送するだけでよい。この動作は長時間を要しないためソフトウエアで実行することができる。
-疑似乱数列および誤り訂正符号の生成に必要な処理力は誤り訂正に要する処理力に比べて大きなものではない。
－したがって、本発明はドライブにわずかな負担しかかけず、誤り訂正の大きな負担を除去する。有権実体もまた疑似乱数列の発生を要するが、誤り訂正符号の発生は要しない。
【図面の簡単な説明】
【図１】コンピュータシステムデータバスアーキテクチャのブロック図である。
【図２】コンピュータシステムデータバスアーキテクチャのブロック図である。
【図３】コンピュータシステムデータバスアーキテクチャにおける従来の暗号化法のブロック図である。
【図４】デジタルビデオディスクのデータブロックのデータ配置を示すブロック図である。
【図５】本発明の一実施形態において実行されるデータ符号語演算を説明するためのブロック図である。
【図６】本発明に係る誤りを含まない乱数データブロックと誤りを含むユーザーデータブロックを示すブロック図である。
【図７】本発明の一実施例おいて実施されるコンピュータシステムデータバスアーキテクチャ上のデータ経路を示すブロック図である。
【符号の説明】
101　ホストマイクロプロセッサ、
102，103，104，106　装置、
105，205　データバス、
206　記憶装置ドライブあるいは伝送チャネル、
202　装置X、
203　装置Y、　MPEG204　復号器、
206　ドライブ、
401　ヘッダ情報、
403　行、
404　列、
405　32K バイト、
501，502，504　ECC符号語、
601　乱数、
602　ユーザーデータブロック、
603　データブロック、
701　ホストプロセッサ、

702　MPEG復号器、
703　記憶装置ドライブ、
704　データバス、
705　707　データブロック、
706　シード、
708　表示装置、
712，713　乱数発生器、

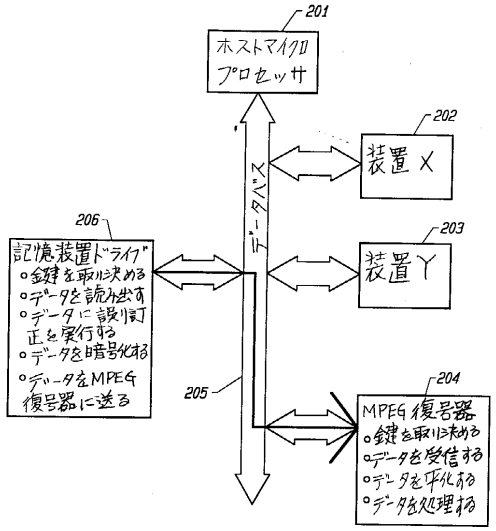
【図１】



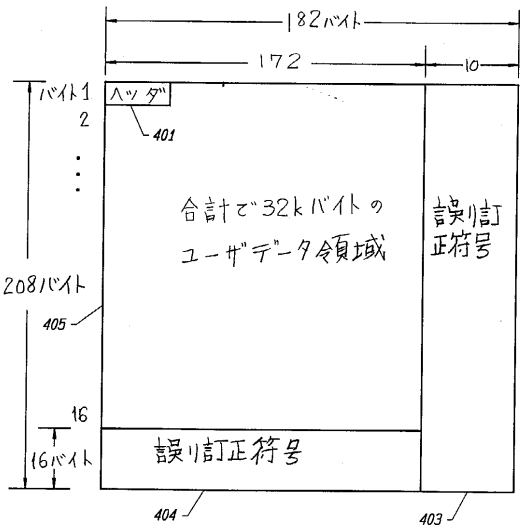
【図２】



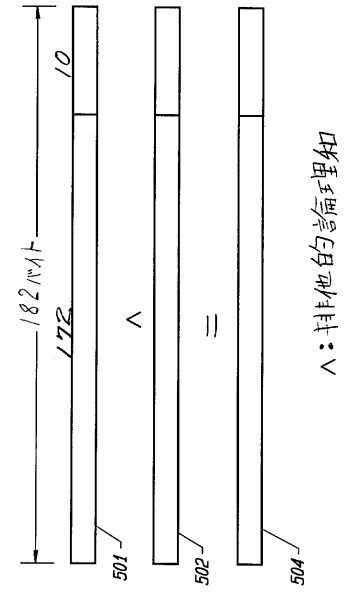
【図３】


201
ホストマイクロプロセッサ
202
装置 X
203
装置 Y
204
MPEG 復号器
・鍵を取り決める
・データを受信する
・データを平化する
・データを処理する
205
データバス
206
記憶装置ドライブ
・鍵を取り決める
・データを読み出す
・データに誤り訂正を実行する
・データを暗号化する
・データをMPEG復号器に送る

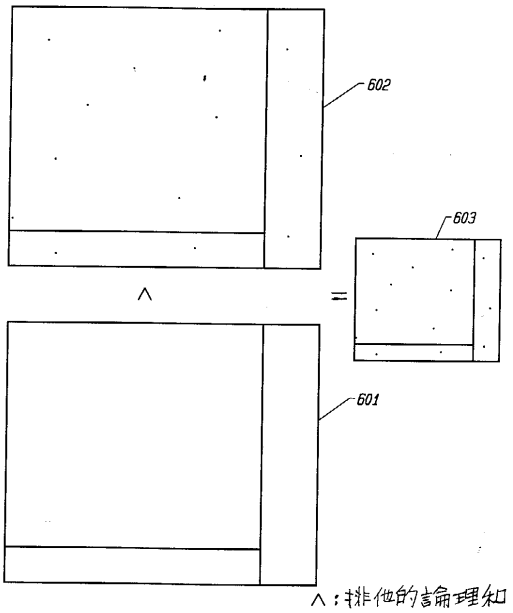
【図４】


182バイト
172
10
バイト1
2
ヘッダ
401
合計で32kバイトのユーザデータ領域
誤り訂正符号
208バイト
405
16
16バイト
誤り訂正符号
404
403

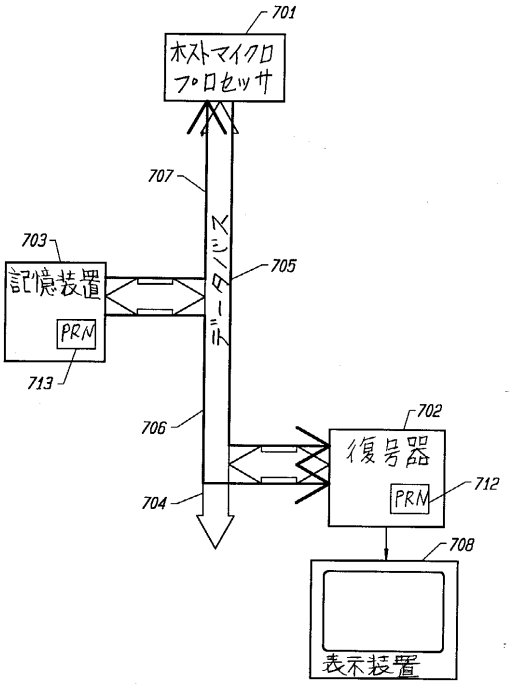
【図５】


10
182バイト
172
501
502
504
＝：排他的論理和

【図６】


602
603
601
＝：排他的論理和

【図７】


701
ホストマイクロプロセッサ
707
データバス
703
記憶装置
PRM
705
713
706
702
復号器
PRM
712
704
708
表示装置

フロントページの続き

(56)参考文献 特開平０５－０５６４３１（ＪＰ，Ａ）
特開平０４－３６０４３８（ＪＰ，Ａ）
特開平０９－０１８４６８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 1/00
G09C 1/00
H04K 1/00
H04L 9/20