

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4302189号
(P4302189)

(45) 発行日 平成21年7月22日(2009.7.22)

(24) 登録日 平成21年5月1日(2009.5.1)

(51) Int.Cl.	F I
HO 4 L 9/18 (2006.01)	HO 4 L 9/00 6 5 1
HO 4 N 7/167 (2006.01)	HO 4 N 7/167 Z

請求項の数 13 (全 12 頁)

(21) 出願番号	特願平10-527493	(73) 特許権者	590000248
(86) (22) 出願日	平成9年12月11日(1997.12.11)		コーニンクレッカ フィリップス エレク
(65) 公表番号	特表2000-507072(P2000-507072A)		トロニクス エヌ ヴィ
(43) 公表日	平成12年6月6日(2000.6.6)		オランダ国 5 6 2 1 ベーアー アイン
(86) 国際出願番号	PCT/IB1997/001558		ドーフェン フルーネヴァウツウェッハ
(87) 国際公開番号	W01998/027687		1
(87) 国際公開日	平成10年6月25日(1998.6.25)	(74) 代理人	100070150
審査請求日	平成16年12月8日(2004.12.8)		弁理士 伊東 忠彦
(31) 優先権主張番号	08/768,489	(72) 発明者	クッシア デヴィッド
(32) 優先日	平成8年12月18日(1996.12.18)		オランダ国 5 6 5 6 アーアー アイン
(33) 優先権主張国	米国(US)		ドーフェン プロフ ホルストラーン 6
		審査官	青木 重徳
		最終頁に続く	

(54) 【発明の名称】 デジタルテレビジョン受信機の復号機関とシステムデコーダとの間のインタフェースを暗号によって保障する方法及び装置

(57) 【特許請求の範囲】

【請求項 1】

デジタル受信機の暗号解読機関及びシステムデコーダの間の保障インタフェースを提供する方法であって、

前記システムデコーダは、暗号化されるビットストリームを受信し、暗号文ビットストリームを生成するものであり、該暗号文ビットストリームは、複数個であるN個の並列ビットラインを含む第1の並列データバスを介して前記暗号解読機関に供給され、前記N個の並列ビットラインは、前記暗号文ビットストリームを表すNビットの各々に対応するものであり、

前記暗号解読機関は、前記暗号文ビットストリームを解読し、平文ビットストリームを生成するものであり、該平文ビットストリームは、複数個であるN個の並列ビットラインを含む第2の並列データバスを介して前記システムデコーダに供給され、前記N個の並列ビットラインは、前記平文ビットストリームを表すNビットの各々に対応するものであり、当該方法は、

前記第1の並列データバスのN個のビットライン各々におけるNビットの暗号文ビットストリームのビットオーダをスクランブルし、Nビットのスクランブルされた暗号文ビットストリームを生成する工程と、

前記Nビットのスクランブルされた暗号文ビットストリームのビットオーダをスクランブル解除し、元の暗号文ビットストリームと同じスクランブル解除された暗号文ビットストリームを生成する工程と、

10

20

前記暗号解読機関を用いて、前記スクランブル解除された暗号文ビットストリームを解読し、前記平文ビットストリームを生成する工程と、

前記第2の並列データバスのN個のビットライン各々におけるNビットの平文ビットストリームのビットオーダをスクランブルし、Nビットのスクランブルされた平文ビットストリームを生成する工程と、

前記Nビットのスクランブルされた平文ビットストリームのビットオーダをスクランブル解除し、元の平文ビットストリームと同じスクランブル解除された平文ビットストリームを生成する工程と

を有し、前記第1の並列データバスのN個のビットライン各々におけるNビットの暗号文ビットストリームのビットオーダをスクランブルする前記工程及び前記Nビットのスクランブルされた暗号文ビットストリームのビットオーダをスクランブル解除する前記工程は、

10

相補的な状態マシンの対によって実行され、前記第2の並列データバスのN個のビットライン各々におけるNビットの平文ビットストリームのビットオーダをスクランブルする前記工程及び前記Nビットのスクランブルされた平文ビットストリームのビットオーダをスクランブル解除する前記工程は、

相補的な状態マシンの対の各々は、デジタル受信機の個々のパワーアップサイクルにおいて、異なる複数の相補的な状態を循環的に使用する方法。

【請求項2】

前記デジタル受信機はデジタルテレビジョン受信機に備わる請求項1記載の方法。

20

【請求項3】

Nビットの暗号文ビットストリームのビットオーダをスクランブルする前記工程は、第1のビットスクランブルアルゴリズムに従って実行され、及び

Nビットの平文ビットストリームのビットオーダをスクランブルする前記工程は、第2のビットスクランブルアルゴリズムに従って実行される請求項1記載の方法。

【請求項4】

前記第1及び第2のビットスクランブルアルゴリズムが同じである請求項3記載の方法。

【請求項5】

前記第1及び第2のビットスクランブルアルゴリズムが異なる請求項3記載の方法。

【請求項6】

30

前記デジタル受信機の複数のパワーアップサイクルの各々について、可能な複数の第1のビットスクランブルアルゴリズムの内、異なるものが使用される請求項3記載の方法。

【請求項7】

前記デジタル受信機の複数のパワーアップサイクルの各々について、可能な複数の第2のビットスクランブルアルゴリズムの内、異なるものが使用される請求項3記載の方法。

【請求項8】

暗号化されるビットストリームを受信し、暗号文ビットストリームを生成するシステムデコーダと、

前記暗号文ビットストリームを解読し、平文ビットストリームを生成する暗号解読機関と、

40

複数個であるN個の並列ビットラインを含み、前記システムデコーダの並列出力ポート及び前記暗号解読機関の並列入力ポートの間に結合された第1の並列データバスと、

複数個であるN個の並列ビットラインを含み、前記暗号解読機関の並列出力ポート及び前記システムデコーダの並列入力ポートの間に結合された第2の並列データバスと、

前記第1の並列データバスのN個のビットライン各々におけるNビットの暗号文ビットストリームのビットオーダをスクランブルし、Nビットのスクランブルされた暗号文ビットストリームを生成する手段であって、該暗号文ビットストリームは、前記第1の並列データバスを介して前記暗号解読機関の前記並列入力ポートに供給される手段と、

前記Nビットのスクランブルされた暗号文ビットストリームのビットオーダをスクランブル解除し、元の暗号文ビットストリームと同じスクランブル解除された暗号文ビットスト

50

リームを生成する手段と、
前記第2の並列データバスのN個のビットライン各々におけるNビットの平文ビットストリームを生成する手段と、
前記Nビットのスクランブルされた平文ビットストリームのビットオーダをスクランブル解除し、元の平文ビットストリームと同じスクランブル解除された平文ビットストリームを生成する手段と、
を有し、前記Nビットの暗号文ビットストリームのビットオーダをスクランブルすること及び前記Nビットのスクランブルされた暗号文ビットストリームのビットオーダをスクランブル解除することは、相補的な状態マシンの対によって実行され、
前記Nビットの平文ビットストリームのビットオーダをスクランブルすること及び前記Nビットのスクランブルされた平文ビットストリームのビットオーダをスクランブル解除することは、相補的な状態マシンの対によって実行され、
相補的な状態マシンの対の各々は、当該デジタル受信機の個々のパワーアップサイクルにおいて、異なる複数の相補的な状態を循環的に使用するデジタル受信機。

10

【請求項9】

当該デジタル受信機はデジタルテレビジョン受信機に備わる請求項8記載のデジタル受信機。

【請求項10】

20

前記Nビットの暗号文ビットストリームのビットオーダをスクランブルする前記手段は、前記システムデコーダ内に組み込まれた暗号文スクランブルモジュールを備え、
前記Nビットのスクランブルされた暗号文ビットストリームのビットオーダをスクランブル解除する前記手段は、前記暗号解読機関内に組み込まれた暗号文スクランブル解除モジュールを備え、

前記Nビットの平文ビットストリームのビットオーダをスクランブルする前記手段は、前記暗号解読機関内に組み込まれた平文スクランブルモジュールを備え、

前記Nビットのスクランブルされた平文ビットストリームのビットオーダをスクランブル解除する前記手段は、前記システムデコーダ内に組み込まれた平文スクランブル解除モジュールを備える

30

ようにした請求項8記載のデジタル受信機。

【請求項11】

前記第1及び第2の並列データバスは、少なくとも部分的に外部に曝される、請求項10記載のデジタル受信機。

【請求項12】

前記システムデコーダ及び前記暗号解読機関は、第1及び第2の個々のチップにおいて実現される、請求項11記載のデジタル受信機。

【請求項13】

前記第1及び第2の個々のチップを含む第1及び第2のボールグリッドアレイパッケージを具える、請求項12記載のデジタル受信機。

40

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、一般にデジタル受信機用の保障手段に関するものであり、より詳しくは、デジタルテレビジョン受信機の復号機関とシステムデコーダとの間の暗号によって保障するインタフェースを設けた方法及び装置に関するものである。

【背景技術】

【0002】

現在又は将来のケーブル又は衛星予約デジタルテレビジョンシステム（例えば、ATSCデジタルテレビジョン基準のようにISO/IEC 13818文書に記載されたMPE

50

G-2 デジタルビデオ圧縮基準に基づくデジタルテレビジョンシステム) のデジタルテレビジョン信号の侵害を防止するための種々の装置が開発されている。一般に、デジタルテレビジョン信号は、送信前にサービスプロバイダによって暗号化され、その後受信側で復号される。典型的には、システム加入者には、ケーブルフィーダ又は衛星受信機と加入者のテレビジョン受像機との間に接続した (個別のセットアップボックスに含まれた又はデジタルテレビジョン受像機それ自体の中に統合された) 復号機関を有するデジタルテレビジョン受信機が与えられる。Diffie-Hellman暗号アルゴリズム、R S A (Rivest-Shamir-Adleman) 暗号アルゴリズム及びD E S (Data Encryption Standard) 暗号アルゴリズムを含む、利用できる周知の暗号アルゴリズムが複数存在する。

【0003】

デジタルテレビジョンシステム (及び他のタイプのデジタルデータ伝送システム) において、復号機関は、用いられる特定の暗号アルゴリズムに依存する公開キー及び未知で復号機関で秘密にされた個人キーを用いるとともに対応する復号アルゴリズムに従って、デジタルテレビジョン受信機によって受信した暗号化されたテレビジョン信号を復号する。このようなシステムによって与えられた保障の完全性は、個人キーの秘密の保持状態に依存する。侵害者 (アタッカ) が個人キーを発見できる場合、熟練した侵害者 (セットアップボックスのデコーダ及び復号チップを悪用することができる個人又は会社) が他の「密造」復号チップを製造し、それを「ブラックボックス」に組み込み、非加入者 (すなわち、サービスプロバイダに加入料を支払わない者) によるプログラミングの受信を可能にすることが当たり前になる。

【0004】

デジタルテレビジョンシステム (及び他のタイプのデジタルデータ伝送システム) 用の暗号システムにおいて、2 レベルの暗号、すなわち、公開キー暗号及び個人キー暗号が用いられる。データの大部分は、個人キー暗号の速度に起因するために、個人キー暗号 (すなわち、D E S のようなブロック暗号) を用いて暗号化される。データ伝送のセッション (典型的には、セッションは数ミリ秒の伝送データとなる。) は、セッションキーと呼ばれる相違する個人キーを用いることによって、ブロック暗号で暗号化される。各セッションはそれ自体の個人キーを有する。セッションキーそれ自体は、典型的には公開キー暗号システムを用いて暗号化され、公開キーシステムのユーザの個人キーを保持するユーザのみが復号することができ、これによって復元が行われ、セッションキーは、伝送されたデータのセッションの復号に用いられる。このようなシステムによって与えられた保障の完全性は、ユーザ個人キーの秘密の保持に主に依存し、任意のセッションキーの秘密にある程度依存する。侵害者 (アタッカ) が個人キーを発見できる場合、熟練した侵害者 (セットアップボックスのデコーダ及び復号チップを悪用することができる個人又は会社) が他の「密造」復号チップを製造し、それを「ブラックボックス」に組み込み、非加入者 (すなわち、サービスプロバイダに加入料を支払わない者) によるプログラミングの受信を可能にすることが当たり前になる。

【0005】

復号機関を実現する最も保障された方法は、復号機関をシステムデコーダと同一のダイに集積して集積回路 (I C) を設けることである。例えば、M P E G-2 移送ストリームを処理する受信機に対して、システムデコーダは、移送ストリームからパケット化基本ストリーム (P E S) にデマルチプレクサ処理する。M P E G-2 タイプのストリームにおいて、P E S パケットを取り出すとともにそれから移送パケットを形成することができる (a)。この際、移送パケットを暗号化することができる。P E S パケットを暗号化し、暗号化された P E S パケットから移送パケットを形成し、そのまま伝送することができる (b)。最後に、P E S パケットのデータを暗号化し、信号化された P E S データから移送パケットを形成することができ、各々が暗号化された移送パケットペイロードを有する。方法 (a) を用いる場合、デジタル受信機は、移送パケットペイロードを最初に復号し、その後 P E S パケットを復元するのに要求されるデマルチプレクサ処理を実行する必要がある (デマルチプレクサ処理前の復号)。方法 (b) を用いる場合、デジタル受信機は移

送パケットをデマルチプレクサ処理して暗号化された P E S パケットを形成し、その後 P E S パケットを復号する必要がある（デマルチプレクサ処理後の復号）。方法（c）を用いる場合、マルチプレクサ前後の復号が要求される。復号機関をシステムデコーダと同一のダイに統合すると、復号機関の悪用が非常に困難になる特殊なマスク及び設計を用いて I C 内部に有線接続することによってシステムデコーダ及び復号機関が接続される。しかしながら、このような有線 I C は、変形できないのでシステム設計者にとって柔軟性がなく、他の全てを排除するために単一の暗号形態のみをサポートする。したがって、互いに相違する暗号アルゴリズムをサポートするように特別に設計した個別の I C を、相違する暗号アルゴリズムを用いるサービスに対して用いる必要がある。

【0006】

復号機関を実現する最も柔軟性のある方法は、相違する暗号アルゴリズムをサポートするソフトウェアによって再構成することができる一般的な目的のデジタル信号処理装置（例えば、フィールドプログラマブルゲート／論理アレイ（F P G A 又は F P L A）又は A S I C コア）を用いることである。しかしながら、この技術によって、システムの保障は著しく低下される。その理由は、システムが、ソフトウェア及びハードウェアアタックに対して攻撃を受けやすいからである。

【0007】

復号機関を実現する他の方法は、復号機関及びシステムデコーダを個別のチップ上に実現することであり、その結果、復号機関がシステムデコーダからオフチップされる。このようにして、相違する復号機関を、単にチップを代用することによって利用することができる。しかしながら、これが暗号機関を実現する特に柔軟性のある方法であるが、外界に対してシステムデコーダと復号機関との間の相互接続部が露出されるためにシステムの保障が危うくなり、その結果、以下のタイプのアタックに対して露出した相互接続部が攻撃を受けやすくなる。すなわち、アタッカが、相互接続部（例えば、第 1 の並列又は直列データバス）から暗号文（すなわち、暗号化されたビットストリーム）を読み出されるとともに、相互接続部（例えば、第 2 の並列又は直列データバス）から対応する平文（すなわち、復号されたビットストリーム）から読み出されるおそれがある。暗号文及び平文に対してアクセスすることによって、アタッカは既知の平文を実行することができ、選択した暗号文は、個人キーの全て又は一部の復元を試みる際に復号機関にアタックする。一般に、復号形態の個人キー又は権利キーを復元しようとするアタックは解読として既知である。解読の特別のサブセットは、差分（differential）解読と呼ばれ、D E S 暗号化／復号形態において有効である。露出したインタフェースを用いると、アタッカは選択した暗号文アタックを用いることができ、その結果、差分解読を復号機関で実行することができ、これによって権利キーを復元する。さらに、露出したインタフェースによって、アタッカは、困難なく平文に対応する暗号文及び手段を発生させるラボラトリー装置を用いることができる。このような状況下で、アタッカは、用いられる暗号化形態と、サービスプロバイダ及び／又はクライアント（加入者）の公開キーを知るだけでよい。

【0008】

さらに、データ伝送サービスが対話式である場合、すなわち、双方向通信リンクを通じて加入者がフィードバックできる場合、個別の加入者のセットトップボックスに復号機関及び送信機が設けられ、その結果、加入者は、伝送前に個人キーを用いて認証に対する暗号化及び「符号化」を行うデータを（例えば、キーボードを通じて）入力することができる。したがって、個人キーをあばくアタッカは、個人キーを用いて本当の加入者のまねをすることもできる。

【0009】

これまで説明したことに基づいて、現在利用できる技術を用いて最も強固なデジタルテレビジョン受信機の復号機関とシステムデコーダとの間の暗号によって保障されたインタフェースを設けた方法及び装置が従来から必要であることが理解することができ、これによって、システムに入り込もうとする任意のアタッカに対して非常に高いコスト対報酬比となる。

10

20

30

40

50

【発明が解決しようとする課題】

【0010】

これに関して、デジタルテレビジョン受信機又は他の任意のタイプのデジタルデータ受信機（すなわち、より広く言えばデジタル受信機）の復号機関とシステムデコーダとの間に露出した相互接続部からアタッカが十分な情報を得ることが非常に困難（又は不可能）となる方法及び装置が従来必要であった。本発明は、従来のこの要求を満足する。

【課題を解決するための手段】

【0011】

本発明は、デジタル受信機、例えば、MPEG-2 デジタルテレビジョン受信機の復号機関とシステムデコーダとの間を保障するインタフェースを設けた方法を含む。システムデコーダは、暗号化されたビットストリームを受信するとともに、Nビットの暗号文ビットストリームにそれぞれ対応するN（Nは複数）並列ビットラインを有する第1並列データベースを通じて復号機関に供給される暗号文ビットストリームを発生させる。復号機関は、暗号文ビットストリームを復号するとともに、Nビットの平文ビットストリームにそれぞれ対応するN（Nは複数）並列ビットラインを有する第2並列データベースを通じてシステムデコーダに供給される平文ビットストリームを発生させる。

10

【0012】

この方法は、第1データベースのN並列ビットラインの各々のNビットの暗号文ビットストリームのビットオーダをスクランブルして、Nビット幅のスクランブルされた暗号文ビットストリームを発生させるステップと、スクランブルされたNビットの暗号文ビットストリームのビットオーダをスクランブル解除して、元の暗号文ビットストリームと同一のスクランブル解除された暗号文ビットストリームを発生させるステップと、復号機関を用いて前記スクランブル解除された暗号文ビットストリームを復号して、平文ビットストリームを発生させるステップと、第2データベースのNビットラインの各々のNビットの平文ビットストリームのビットオーダをスクランブルして、Nビット幅のスクランブルされた平文ビットストリームのビットオーダをスクランブル解除して、元の平文ビットストリームと同一のスクランブル解除された平文ビットストリームを発生させるステップとを有する。

20

【0013】

前記Nビットの暗号文ビットストリームのビットオーダをスクランブルするステップを、第1ビットスクランブルアルゴリズムに従って実行し、前記Nビットの平文ビットストリームのビットオーダをスクランブルするステップを、第2ビットスクランブルアルゴリズムに従って実行する。第1及び第2ビットスクランブルアルゴリズムを同一しても互いに相違するようにしてもよい。

30

【0014】

本発明の好適例において、前記第1ビットスクランブルアルゴリズムを、前記デジタル受信機の複数の連続的なパワーアップサイクルの各々に対する互いに相違する複数のあり得る第1ビットスクランブルアルゴリズムのうちの一つとし、前記第2ビットスクランブルアルゴリズムを、前記デジタル受信機の複数の連続的なパワーアップサイクルの各々に対する互いに相違する複数のあり得る第2ビットスクランブルアルゴリズムのうちの一つとする。

40

【0015】

Nビットのスクランブルされた暗号文ビットストリームのビットオーダのスクランブル解除ステップを、第1ビットスクランブルアルゴリズムとは逆の第1ビットスクランブル解除アルゴリズムに従って実行し、Nビットのスクランブルされた平文ビットストリームのビットオーダのスクランブル解除ステップを、第2ビットスクランブルアルゴリズムの逆である第2ビットスクランブル解除アルゴリズムに従って実行する。

【0016】

さらに、Nビットの暗号文ビットストリームのビットオーダをスクランブルするステップは、Nビットのスクランブルされた暗号文ビットストリームのビットオーダをスクランブル

50

ル解除するステップと同期をとり、Nビットの平文ビットストリームのビットオーダをスクランブルするステップは、Nビットのスクランブルされた平文ビットストリームのビットオーダをスクランブル解除するステップと同期をとる。

【0017】

本発明は、暗号化されたビットストリームを受信するとともに暗号文ビットストリームを発生させるシステムデコーダと、暗号文ビットストリームを復号するとともに平文ビットストリームを発生させる復号機関と、システムデコーダの並列出力ポートと復号機関の並列入力ポートとの間に結合したN（Nは複数）並列ビットラインを有する第1並列データベースと、復号機関の並列出力ポートとシステムデコーダの並列入力ポートとの間に結合したN（Nは複数）並列ビットラインを有する第2並列データベースとを有するデジタル受信機も含む。

10

【0018】

システムデコーダは、第1データベースのNビットライン上でNビットの平文ビットストリームのビットオーダをスクランブルして、第1並列データベースを通じて復号機関の並列入力ポートに供給されるNビット幅のスクランブルされた暗号文ビットストリームを発生させる暗号文スクランブルモジュールを有する。

【0019】

復号機関は、Nビットのスクランブルされた暗号文ビットストリームのビットオーダをスクランブル解除して、元の暗号文ビットストリームと同一のスクランブル解除された平文ビットストリームを発生させる平文スクランブル解除モジュールを有する。復号機関は、第2データベースのNビットライン上でNビットの平文ビットストリームのビットオーダをスクランブルして、第2並列データベースを通じてシステムデコーダの並列入力ポートに供給されるNビット幅のスクランブルされた平文ビットストリームを発生させる平文スクランブルモジュールを更に有する。システムデコーダは、Nビットのスクランブルされた平文ビットストリームのビットオーダをスクランブル解除して、元の平文ビットストリームと同一のスクランブル解除された平文ビットストリームを発生させる平文スクランブル解除モジュールを更に有する。

20

【0020】

好適例において、第1及び第2並列データベースは、少なくとも部分的に外界に露出され、システムデコーダ及び復号機関を個別の第1及び第2チップ上で実現する。さらに、暗号文スクランブルモジュール及び暗号文スクランブル解除モジュールを、好適には相補的な第1及び第2状態マシン（例えば、線形フィードバックシフトレジスタの組合せ）として実現し、平文スクランブルモジュール及び平文スクランブル解除モジュールを、好適には相補的な第3及び第4状態マシンとして実現する。

30

【0021】

さらに、システムデコーダ及び復号機関を、好適には共通電源に結合するとともに、互いにパワーサイクルして、第1及び第2状態マシンは、複数の連続的なパワーアップサイクルに亘って相補的な第1及び第2状態のシーケンスをそれぞれ同期をとって繰り返し、第3及び第4状態マシンは、複数の連続的なパワーアップサイクルに亘って相補的な第3及び第4状態のシーケンスをそれぞれ同期をとって繰り返す。

40

【0022】

本発明は、後に詳細に説明する情報デジタル受信機及び方法の他の変形例も含む。

【0023】

本発明のこれら及び他の種々の形態及び態様を、添付図面に関連して以下詳細に説明する。

【発明の実施の形態】

【0024】

ここで図1を参照すると、本発明の好適な実施の形態によるデジタルテレビジョン受信機の復号機関とシステムデコーダとの間を暗号によって保障するインタフェースを設けた方法及び装置を示す。より詳細には、デジタル受信機、例えば、MPEG-2 デジタルテレ

50

ビジョン受信機は、データバス16, 18、例えば、16ビット幅の並列データバスを通じて互いに通信する復号機関12及びシステムデコーダ14を有し、これらは共に復号機関12とシステムデコーダ14との間の相互接続部を有する。本発明によれば、システムデコーダ14は、通常のデコーダ回路に加えて、暗号文スクランブル回路又はモジュール20と、平文スクランブル回路又はモジュール22とを有し、復号機関12は、通常の復号回路に加えて、暗号文スクランブル解除回路又はモジュール24と、平文スクランブル回路又はモジュール26とを有する。システムデコーダの暗号文スクランブルモジュール20及び復号機関12の暗号文スクランブル解除モジュール24は、16ビット幅の並列バス16を通じて通信し、復号機関12の平文スクランブルモジュール26及びシステムデコーダ14の平文スクランブルモジュール22は、16ビット幅の並列バス18を通じて通信する。

10

【0025】

本発明によれば、暗号文ビットストリームを具えるビットのビットオーダ（ビット位置）（すなわち、デジタルテレビジョン受信機10によって受信した暗号化されたデジタルテレビジョン信号）は、任意の適切なビットスクランブルアルゴリズムによって、システムデコーダ14の暗号文スクランブルモジュール20によってスクランブルされる。例えば、暗号文ビットストリームの奇数ビットを、並列データバス16の偶数ビットライン上に配置することができ、暗号文ビットストリームを、並列データバス16の奇数ビットライン上に配置することができる。当然、暗号文ビットストリームのビットオーダをスクランブルするのに用いられる特定のビットストリームアルゴリズムは、本発明を制限するものではない。

20

【0026】

復号機関12の暗号文スクランブル解除モジュール24は、ビットスクランブル解除アルゴリズムによって、並列データバス16上で受信したスクランブルされた暗号文ビットストリームのビットオーダのスクランブル解除を行うように機能し、このアルゴリズムは、システムデコーダ14の暗号文スクランブルモジュール20によって実行されるビットスクランブルアルゴリズムの逆である。スクランブル解除された暗号文ビットストリームは、復号機関12によって通常の方法で復号され、これによって平文ビットストリームを発生させる。

【0027】

本発明の他の態様によれば、復号機関12によって発生した平文ビットストリームを具えるビットのビットオーダは、任意の適切なビットスクランブル形態に応じて、復号機関12の平文スクランブルモジュール26によってスクランブルされる。例えば、平文ビットストリームの奇数ビットを、並列データバス18の偶数ビットライン上に配置することができ、平文ビットストリームの偶数ビットを、並列データバス18の奇数ビットライン上に配置することができる。当然、平文ビットストリームのビットオーダをスクランブルするのに用いられる特定のビットスクランブルアルゴリズムも、本発明を制限するものではない。これに関連して、暗号文ビットストリーム及び平文ビットストリームのビットオーダをスクランブルするのに用いられるビットスクランブルアルゴリズムは、同一でも互いに相違してもよい。

30

40

【0028】

システムデコーダ14の平文スクランブル解除モジュール22は、ビットスクランブル解除アルゴリズムを実行することによって並列データバス18上で受信したスクランブルされた平文ビットストリームのビットオーダをスクランブル解除するように機能し、このアルゴリズムは、復号機関12の平文スクランブルモジュール26によって実行されるビットスクランブルアルゴリズムの逆であり、これによってスクランブル解除された平文ビットストリームを発生させ、これは、通常の方法で十分処理される。

【0029】

復号機関12とシステムデコーダ14との間の相互接続の暗号の保障を増大させる本発明の他の態様によれば、デジタルテレビジョン受信機10の各パワーアップの際に、以前の

50

パワーアップで用いられたものと異なるビットスクランブル形態を、データバス16上の暗号文ビットストリームのビットオーダとデータバス18上の平文ビットストリームのビットオーダの両方をスクランブルするのに用いることができる。例えば、複数の互いに相違するビットスクランブル形態の任意の又は予め決定されたものを、デジタルテレビジョン受信機10の各パワーアップの際にシステムデコーダ14の暗号文スクランブルモジュール20及び暗号機関12の平文スクランブルモジュール26によって選択することができる。

【0030】

本発明のこの実施の形態に対する要求は、常に同時に相補的なビットスクランブル／スクランブル解除アルゴリズムを実行するようにシステムデコーダ12の暗号文スクランブルモジュール20及び復号機関12の暗号文スクランブル解除モジュール24の同期をとることと、常に同時に相補的なビットスクランブル／スクランブル解除アルゴリズムを実行するように復号機関12の平文スクランブルモジュール26及びシステムデコーダ14の平文スクランブル解除モジュール22の同期をとることだけである。

【0031】

本実施の形態において、これを、相補的な状態マシンのような暗号文スクランブルモジュール20及び暗号文スクランブル解除モジュール24を実現することによって、並びに相補的な状態マシンのような平文スクランブルモジュール26及び平文スクランブル解除モジュール22を実現することによって達成される。相補的な状態マシンの対の各々は、例えば、デジタルテレビジョン受信機10の連続的なパワーアップサイクル上の複数の相違するビットスクランブル／スクランブル解除アルゴリズムに対応する複数の互いに相違する相補的な状態を繰り返す。例えば、状態マシンを、多数の状態を有するように形成し、その結果、これらは、連続的なパワーアップサイクルの短い期間中に「重なり合わず」に同一パターンの状態を繰り返す。この理由は、一度アタッカがパターンを決定すると、状態マシンをパワーアップして、状態マシンを必要なx回特定の状態にして繰り返すことはアタッカにとって通常のこととなるからである。暗号機関12とシステムデコーダ14との間の相互接続部を1対の16ビット幅の並列データバス16、18で構成した図1に図示した実施の形態において、理論的には、16ビット幅の並列データバス16、18によって実行される2バイトワードのビットのオーダ（位置）をスクランブルするために発生させる216の相違するあり得るビットパターン（したがって、各状態マシンの216のあり得る状態）が存在する。

【0032】

動作中、状態マシンは同一である。各状態マシンは、同一の初期化ベクトルを有する。パワーが繰り返されると、状態マシンの次の状態が実現される。復号機関12及びシステムデコーダ14を共通電源に結合するので、これらは共に給電され、その結果、復号機関12及びシステムデコーダ14の各々の状態マシンは、本来同期がとられる。（所定の入力に対する）各状態マシンの出力は、その状態マシンの現在の状態に依存する。したがって、各状態マシンによって実行されるビットスクランブル／スクランブル解除アルゴリズムは、その現在の状態（又はシード状態）に依存する。

【0033】

したがって、常に同時に相補的にビットスクランブル／スクランブル解除アルゴリズムを実行するように、システムデコーダ14の暗号文スクランブルモジュール20及び復号機関12の暗号文スクランブル解除モジュール24の同期をとるとともに、常に同時に相補的なビットスクランブル／スクランブル解除アルゴリズムを実行するように、復号機関12の平文スクランブルモジュール26及びシステムデコーダ14の平文スクランブル解除モジュール22の同期をとるという要求を、連続的なパワーアップサイクル中に同一回数 of 相補的な状態を繰り返すように暗号文スクランブルモジュール20の状態マシン及び暗号文スクランブル解除モジュール24の状態マシンを形成し、かつ、連続的なパワーアップサイクル中に同一回数 of 相補的な状態を繰り返すように平文スクランブルモジュール26及び平文スクランブル解除モジュール22を形成することによって、容易に満足させる

ことができる。

【0034】

いかなる理由であっても、復号機関 1 2 がパワーアップするとともにシステムデコーダ 1 4 がパワーアップせず、又は復号機関 1 2 がパワーアップしないとともシステムデコーダ 1 4 がパワーアップしない場合、これらの間のインタフェースは同期をとらず、これによってこれらの間の任意の通信は防止される。このようなことが発生する場合、システム内の任意の手段（ハードウェア又はソフトウェア）によってこのような「同期をとらない」状態が訂正可能でないことが好ましい。その理由は、これは、システムを暗号によって保障するからである。

【0035】

さらに本発明によれば、以下の四つの追加の侵害防止手段を採用して、システムへのアタックの困難さ及びコスト対報酬を増大させる。

【0036】

(1) 復号機関 1 2 及びシステムデコーダ 1 4 のパッケージ化に対するボールグリッドアレイ (BGA) パッケージの使用。この理由は、BGA パッケージが IC ピンへのアクセスを制限するからであり、また、BGA パッケージは、一度システムボードの表面に装着するとシステムボードから取り除くのが困難となるからである。したがって、BGA パッケージを使用することによって、アタッカになろうとする者がピンにアクセスするためにボードから IC を取り除くとともにこれらをソケットに配置するのが困難になる。これによって、装置を悪用するのが著しく困難になる。

【0037】

(2) 基板経路をパッケージに接続する埋め込み経路の使用。これによって、バスデータ信号へのアクセスが制限される。

【0038】

(3) 内側層上にトレースが見えるのを防止するための復号機関 1 2 及びシステムデコーダ 1 4 の下の少なくとも一つのパワープレーン (power plane) (例えば、多層基板中の全ての銅層) の使用。多層基板の内側層上のトレースを見ることを試みるために、アタッカとなる者は、パワープレーン層にドリルで孔を開ける必要がある。これによって短絡が生じ、全装置が不作動状態となり、アタックを無効にする。

【0039】

(4) 復号機関 1 2 とシステムデコーダ 1 4 の両方の BGA パッケージを包むエポキシの使用。

【0040】

(5) 回路の悪用を困難にするためにスクランブルモジュール回路配置を曖昧にする ASI C 技術のマスク技術と、走査電子顕微鏡を用いた ASI C 設計の検査からの「シード状態」との利用。

【0041】

本発明の好適な実施の形態をこれまで詳細に説明したが、当業者には明らかなここで教示した基本的な発明の概念の多数の変形及び変更は、添付した請求の範囲で規定したように本発明の精神及び範囲内にある。

【0042】

例えば、本発明を、並列データバス 1 6 及び 1 8 で構成した相互接続部に関連して説明したが、本発明は、直列データバスで構成した相互接続部を有するデジタル受信機にも同様に適用することができる。さらに、本発明を、デジタルテレビジョン受信機 1 0 に関連して説明したが、本発明を任意のタイプのデジタル受信機に同様に適用することができる。さらに、MPEG-2 仕様、例えば、ATSC 基準を満足する圧縮デジタルビデオビットストリームは、ビデオ、音響、テキスト、音声、データ、図形、画像及び他のタイプのマルチメディアデータを含む多様なデータを含むが、これらに制限されるものではない。

【0043】

システムの暗号保障を更に増強させるためにビットスクランブル／スクランブル解除形態

10

20

30

40

50

を増強させることができる。例えば、並列データバス16, 18上のビットの位置に加えて又はその代わりに、ビットの各々を、可変時間によって（例えば、可変クロックサイクルによって）遅延させることができる。このタイプのビットスクランブルは、一時ビットスクランブル（temporal bit-scrambling）として教示される。

【0044】

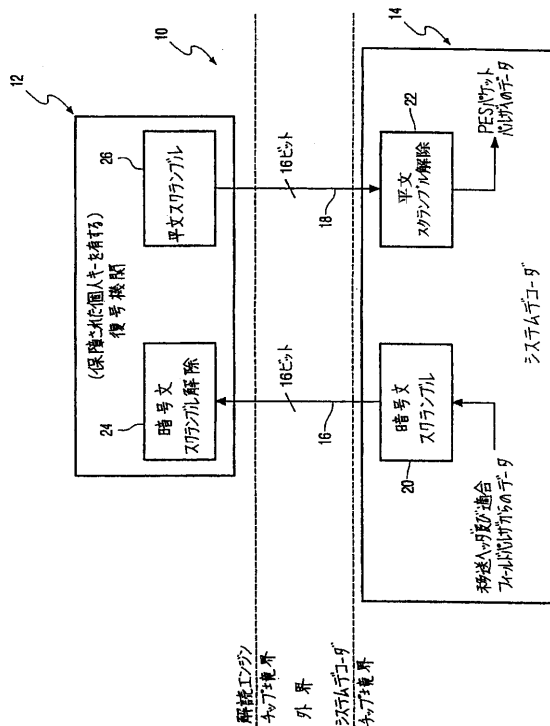
さらに、データバス16及び18の並列データラインの各々に対して存在するビットストリームの連続的なビットの順次のオーダを同様にスクランブルすることかできる。暗号文スクランブルモジュール20、暗号文スクランブル解除モジュール24、平文スクランブルモジュール26及び平文スクランブル解除モジュール22を状態マシンとして実現するのではなく、これらモジュールを、状態マシンの出力を制御信号として利用できる各状態マシンの制御の下での信号処理回路として実現することができる。例えば、状態マシンの出力を、読出し専用メモリ（ROM）に記憶された相違するビットパターン（ビット位置結合）をルックアップするアドレス又はビットパターンを発生させる線形フードバックシフトレジスタ（LFSR）に対するシード状態として用いることができる。また、状態マシンの出力を、各信号処理回路によって変換して、最終ビットストリームを発生させることができる。

【図面の簡単な説明】

【0045】

【図1】 デジタルテレビジョン受信機の復号機関とシステムデコーダとの間で暗号による保障された相互接続部を提供する本発明の好適な実施の形態による装置を有するデジタルテレビジョン受信機の一部のブロック図である。

【図1】



フロントページの続き

- (56)参考文献 特開平06-303611 (JP, A)
特開平02-031290 (JP, A)
特開平02-172340 (JP, A)
特開平08-125651 (JP, A)
実開昭60-085485 (JP, U)

(58)調査した分野(Int.Cl., DB名)

H04L 9/18

H04N 7/167