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

特許第4755862号
(P4755862)

(45)発行日　平成23年8月24日(2011.8.24)　(24)登録日　平成23年6月3日(2011.6.3)

(51)Int.Cl.　　F I
H04N 7/167 (2011.01)　　H04N 7/167 Z
H04N 7/173 (2011.01)　　H04N 7/173 630

請求項の数 2　(全 12 頁)

(21)出願番号　特願2005-233504(P2005-233504)
(22)出願日　平成17年8月11日(2005.8.11)
(65)公開番号　特開2006-54895(P2006-54895A)
(43)公開日　平成18年2月23日(2006.2.23)
審査請求日　平成20年7月14日(2008.7.14)
(31)優先権主張番号　04300532.1
(32)優先日　平成16年8月11日(2004.8.11)
(33)優先権主張国　欧州特許庁(EP)

(73)特許権者　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　Ｆｒａｎｃｅ
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】デバイスペアリング

(57)【特許請求の範囲】
【請求項１】
第２のデバイスとペアにされる第１のデバイスにおいて使用するセキュリティモジュールであって、前記セキュリティモジュールはプロセッサとメモリとを有し、前記メモリは前記第１のデバイスがマスターデバイスであるかスレーブデバイスであるかを示す可変のデバイス状態を記憶し、
前記セキュリティモジュールは、
専用の個別情報を受信し処理する手段と、
前記セキュリティモジュールが前記第１のデバイスと接続されているとき、前記専用の個別情報に含まれる指示に応じて、前記メモリに記憶した前記デバイス状態を変更する手段と
を有することを特徴とするセキュリティモジュール。
【請求項２】
第２のデバイスとペアにされる第１のデバイスにおいて使用するセキュリティモジュールであって、前記セキュリティモジュールはプロセッサとメモリとを有し、前記メモリは前記第１のデバイスがマスターデバイスであるかスレーブデバイスであるかを示す可変のデバイス状態を記憶し、
前記セキュリティモジュールは、
専用の個別情報を受信し処理する手段と、
前記セキュリティモジュールが前記第１のデバイスと接続されているとき、所定の使用

時間経過後、それまでに前記専用の個別情報を受信しなければ、前記メモリに記憶した前記デバイス状態を変更する手段と
を有することを特徴とするセキュリティモジュール。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明はデバイスのペアリングに関し、特に端末にコンテントへの限定的アクセスをさせるシステムにおけるデバイスのペアリングに関する。また、本発明はペイテレビシステムにおけるデコーダのペアリングに有利に適用することができる。
【背景技術】
【０００２】
ここで、「デコーダ」という用語は、端末の実施例として使用するが、レシーバから物理的に分離したデコーダでもよいし、セットトップボックス（デコーダ）のようにレシーバとデコーダが一体になったものでもよいし、レコーディングデバイス・ディスプレイ・ウェブブラウザのように付加的機能を有するものでもよい。限定受信方式の概念は一般に周知であり、ここで詳しく説明しなくとも、本発明の理解には差し支えない。
【０００３】
限定受信方式は、例えば本明細書を通して使用するペイテレビ等であり、多数の国で広く受け入れられている。多数の家庭がデコーダを有しており、家庭の大半はテレビを１台以上持っている。現在、加入者は１台のデコーダを用いて１台のテレビセットだけでペイテレビの番組にアクセスできるという場合が多い。この問題を解決するために大きく分けて２つの解決策が提案されている。
【０００４】
第１の解決策は、受信したコンテントを家庭内で配信するという方法である。現在の技術水準ではワイヤレスのアナログ再送信を用いる。残念ながら、ビデオ品質はよくなく、接続されたテレビセットすべてで１つの同一の番組を見ることができるだけである。
【０００５】
第２の解決策は、家庭により多くのデコーダを備えることである。多数の放送事業者は、既加入の家庭に第２の加入権（subscription）をより安い価格で提供している。しかし、放送事業者は、加入者が隣近所や親類と共謀して２つの加入権を「共有」して、平均で安い価格で加入してしまうことをおそれて、２つのデコーダをペアとすることを要求する。図１は、従来からの基本的なコンセプトを示す図である。２つのデコーダ１１、１２は双方向のデジタル接続１３を介してリンクされている。一方のデコーダ１１はマスターとして動作し、他方のデコーダ１２はスレーブとして動作する。マスター１１は加入権により認められた放送に常にアクセスすることができるが、スレーブ１２はマスター１１に接続されているときのみ加入権により認められた放送にアクセスすることができる。
【０００６】
２つのデコーダがいっしょに使用されていることを検証する方法には、いくつかの方法がある。
【０００７】
１つの方法として限定受信方式のプロバイダーにより提案されているものは、専用の個別情報（Entitlement Management Message, EMM）を使用する方法である。マスターデコーダ１１は、それ自身宛のEMMとは別に、スレーブデコーダ１２宛のEMMも受信し、デジタル接続１３を介してスレーブ１２に後者のEMMを送る。より複雑な別の方法もあるが、当然のことながら、この比較的簡単な方法でも限定受信方式を大きく変更しなければならず、放送事業者のバックオフィスとの強いリンクが必要となる。それゆえ、この方法は、使用不可能ではなくても、水平的市場においては現実的ではない。
【０００８】
ネットワークで接続されたデバイス間のペアリングを保証する方法が提案されている（

例えば特許文献１参照）。デバイスが完全な動作をするためには、初期化フェーズで組み込まれたセキュリティデバイスがあることが必要である。この方法でデコーダをペアとすることはできるが、マスターデコーダとスレーブデコーダとを区別する必要があり、製造者、小売業者、アフターサービススタッフにとって問題となる。

【０００９】

ネットワークで接続されたデバイス間のペアリングを保証する他の方法が提案されている（例えば特許文献２参照）。第２のデバイス（すなわちスレーブデバイス）は、それが最初にペアとされた所定の第１の端末（すなわちマスター）とペアとなっていて、通信可能なときにのみ、コンテントにアクセスすることができる。この方法も、フレキシビリティを一部欠く状況に限定される。というのは、スレーブデコーダはマスターとペアとなっていなければ動作することができないからである。すでに述べたように、製造者、小売業者、アフターサービススタッフにとって問題となる。

【特許文献１】PCT国際出願第WO2004/019296号「Secure Electric Anti-Theft Device, Anti-Theft System Comprising One Such Device and Method of Matching Electric Devices」

【特許文献２】PCT国際出願第WO03/105437号「Method, System and Terminal for Receiving Content with Authorized Access」

【発明の開示】

【発明が解決しようとする課題】

【００１０】

以上から明らかなように、制御され信頼性の高いやり方でデコーダをマスターデコーダまたはスレーブデコーダにすることができるフレキシブルなソリューションが必要とされている。その変換は加入者の家（または同等な場所）で行われることが好ましい。さらに、そのソリューションは、マスターデコーダとスレーブデコーダ間のペアリングができるものでなければならない。本発明は、このようなソリューションを提供することを課題とする。

【課題を解決するための手段】

【００１１】

第１の態様において、本発明は他のデバイスとペアにされるデバイスで使用するセキュリティモジュールに関する。該セキュリティモジュールは、プロセッサとメモリとを有し、前記メモリは前記第１のデコーダがマスターであるかスレーブであるかを示すデバイス状態を記憶する。

【００１２】

該セキュリティモジュールはこのようにデバイス状態を提供することができ、そのデバイス状態は可変なので、より柔軟に使用することができる。

【００１３】

好ましい一実施形態において、前記デバイス状態は可変であり、専用の個別情報（EMM）を受信し処理した時に変化させられる。

【００１４】

デバイス状態は放送ネットワークを通して可変であり、これはデバイス状態が遠隔操作で変更できることを意味する。

【００１５】

別の好ましい一実施形態において、新しいセキュリティモジュールのデバイス状態は可変であり、前記セキュリティモジュールが専用の個別情報（EMM）を受信しなければ、所定時間使用された後に変化する。

【００１６】

このように、放送ネットワークを通して変更することはできなくても、デバイス状態は自動的に変更できる。これは、デバイス状態を自動的に、または遠隔操作で変更することができることを意味する。

【００１７】

第２の態様において、本発明は、限定受信システムにおいてデバイスにデバイス状態を提供する方法であって、前記デバイス状態はセキュリティモジュールに記憶され、前記デバイスにマスターデバイスとスレーブデバイスのいずれとして動作すべきかを知らせる方法に関する。前記セキュリティモジュールが前記デバイスと接続されていることが検出され、前記セキュリティモジュールから前記デバイスに前記デバイス情報が転送される。

【００１８】

該方法は、デバイスにデバイス状態を備える簡単な方法を提供する。

【００１９】

好ましい一実施形態において、デバイス状態を転送するために、前記デバイスが識別データと乱数を前記セキュリティモジュールに送る。前記セキュリティモジュールが、前記識別データと記憶されたマスター鍵を用いて生成鍵を計算し、前記生成鍵と、前記乱数と、前記デバイス状態とからハッシュを計算し、前記セキュリティモジュールから前記デバイスへ前記デバイス状態と前記ハッシュとを送る。前記デバイスは、前記ハッシュ、前記生成鍵、および前記乱数を用いて前記デバイス状態を検証する。

【００２０】

デバイス状態はこのようにセキュリティモジュールからデバイスに安全に転送される。

【００２１】

好ましい一実施形態において、デバイスもデバイス状態を記憶する。

【００２２】

第３の態様において、本発明はスレーブデバイスをマスターデバイスとペアリングする方法に関する。スレーブデバイスが前記マスターデバイスに自分の識別情報を返すように要求するコマンドを送り、マスターデバイスが自分を識別するメッセージを前記スレーブデバイスに送る。前記スレーブデバイスがマスターデバイスとまだペアになっていないとき、前記スレーブデバイスが前記受信したメッセージを用いて前記マスターデバイスのアイデンティティをチェックする。アイデンティティが検証されたとき、前記スレーブデバイスは前記マスターデバイスとペアとなる。

【００２３】

該方法の実行が成功すると、スレーブデバイスはマスターデバイスとペアになる。

【００２４】

他の好ましい一実施形態において、前記スレーブデバイスがマスターデバイスとペアとなっているとき、前記マスターデバイスのアイデンティティが前に記憶されたマスターデバイスのアイデンティティと同じかどうかを確認し、前記確認が成功したとき、前記スレーブデバイスを前記マスターデバイスとペアにする。

【００２５】

さらに別の好ましい一実施形態において、少なくとも１回チャレンジ－レスポンスプロトコルを実行し、前記デバイスをペアリングする前にすべてのプロトコルが成功することを要求すれば、セキュリティをさらに強化することができる。

【００２６】

第４の態様において、本発明は、第２のデバイスとペアリングする第１のデバイスに関する。前記第１のデバイスはスレーブデバイスとして動作し、前記第２のデバイスはマスターデバイスとして動作する。前記第１のデバイスは、前記第２のデバイスに自分の識別情報を返すように要求するコマンドを送り、前記第２のデバイスを識別するメッセージを前記第２のデバイスから受け取るインターフェイスを有する。また、第１のデバイスは、第１のデバイスがマスターデバイスとまだペアになっていないとき、第２のデバイスのアイデンティティをチェックし、そのアイデンティティが検証されたとき、第１のデバイスを第２のデバイスとペアリングさせるプロセッサも有する。

【００２７】

本発明による方法を用いて、他のデバイスとペアになるデバイスが提供される。

【発明を実施するための最良の形態】

【００２８】

図２は、本発明の好ましい実施形態によるデコーダ２０のアーキテクチャを示す概略図である。デコーダ２０は、中央演算装置（CPU）２４、ビデオ部２３、ISO-7816準拠のスマートカードインターフェイスであるセキュリティモジュールインターフェイス２６、シリアルインターフェイス２７、メモリ２５を有する。メモリ２５は、セキュアな不揮発メモリ２５ａ、不揮発メモリ２５ｂ、ランダムアクセスメモリ（RAM）２５ｃである。ビデオ部２３は、着信接続２１を介してビデオストリームを受信し、共通情報（Entitlement Control Message、ECM）と個別情報（EMM）とを抽出し、抽出したECM・EMMをCPU２４に送る。ECM・EMMはセキュリティモジュールインターフェイス２６を介してセキュリティモジュール（図示せず）に転送される。ビデオ部２３は、セキュリティモジュールにより権限を与えられると、ビデオストリームをデスクランブルし、接続２２に出力する。この接続２２は、通常、ディスプレイ（図示せず）に接続されている。セキュリティモジュールインターフェイス２６は、セキュリティモジュールとの物理的かつ電気的なインターフェイスを実現する。RS232シリアルインターフェイス２７は、図１を参照して上で説明したように、特に、デジタル接続１３を介して他のデコーダとの接続を可能とする。そのデジタル接続は、例えば有線接続でもブルートゥース（登録商標）による接続でもよい。

【００２９】

図３は、本発明によるセキュリティモジュール３０を示す概略図である。このセキュリティモジュール３０は、以下で説明する図４のセキュリティモジュール４３、４４等になる。セキュリティモジュール３０は、中央演算装置（CPU）３１、メモリ３２、通信部３３を有する。通信部３３はISO-7816に準拠し、ホストデコーダ（図２の参照数字２０）のセキュリティモジュールインターフェイス（図２の参照数字２６）と通信する。メモリ３２とCPU３１のRAM（図示せず）はセキュアであると仮定する。すなわち、攻撃者によるアクセスは困難であり、不可能な場合もあるものと仮定する。セキュリティモジュール３０は、例えば、本発明の技術分野で周知であるスマートカードやPCカードであってもよい。

【００３０】

以下に説明する本発明によるペアリング方法を実行するために、好ましい一実施形態において、セキュリティモジュールとデコーダはデータを格納し、一定の機能を実行できる。

【００３１】

セキュリティモジュール３０のメモリ３２は、同時に次の情報を格納していることが好ましい：

・マスター対称鍵MK、
・「マスター」または「スレーブ」の２つの論理値を取る状態CAM_STATE34、および
・計算と検証用の一時変数。

【００３２】

セキュリティモジュール３０のCPU３１は、以下を実行するように構成されている：

・鍵生成アルゴリズムKeyDevAlgo。これは、例えばアドバンストエンクリプションスタンダード（AES）アルゴリズムであり、例えばマスター鍵MKと識別値とから鍵を生成する（FIPSパブリケーション１９７：「アドバンストエンクリプションスタンダード」、米商務省標準技術局、2001年参照）。
・メッセージ確認コード（MAC）生成アルゴリズムMACGenerate。これは例えばハッシュ値を計算するHMAC-SHA1である（FIPSパブリケーション１９８：「鍵ハッシュメッセージ確認コード（HMAC）」、米国商務省標準技術局、2001年参照）。

【００３３】

デコーダ２０は、好ましくは括弧内の参照数字（セキュア不揮発メモリ２５ａ、不揮発メモリ２５ｂ、RAM２５ｃ）により示されたメモリに、必ずしも同時にではなく、次のものを格納する：

・識別データID（２５ｂ）、
・等式DK=KeyDevAlgo{MK}(ID)を満たす生成対称鍵（DK）（２５ｃ）、
・２つの論理値「マスター」または「スレーブ」を取ることができる状態decoder_STATE

（２５ａ）、
・各デコーダでユニークな非常に大きな数S（２５ａ）、
・モデル、生産者、システムの各デコーダで等しい公開数n。nは秘密の２つの非常に大きな素数の積である（２５ｂ）、
・
【００３４】
【数１】

$$S = \sqrt{V} \bmod n$$

を満たす数V（２５ｂ）、
・放送事業者によりサインされたVのシグネチャSigV（２５ｂ）、
・シグネチャのチェックに使用する放送事業者の公開鍵K_{pub_sig}（２５ａ）、
・３つの論理値「バージン」、「ペア」、「ブロック」を取ることができる状態PAIRING_STATE２８（２５ａ）、
・乱数R（２５ｃ）、
・計算と検証に用いる一時変数（２５ｃ）、および
・数V’（２５ｃ）。これについては以下で説明する。
【００３５】
デコーダ２０のCPU２４は次を実行することができる：
・メッセージ認証コード（MAC）検証アルゴリズムMACVerify、および
・乱数の生成。この乱数は実際には疑似乱数（PRNG）である。
【００３６】
図４は、本発明の好ましい一実施形態によるペアになったデコーダを示す図である。限定受信システム４０において、デコーダ４１、４２にはリムーバブルのセキュリティモジュール４３、４４（CAモジュールとも呼ぶ）が備えられている。これらはスマートカードやPCMCIA（Personal Computer Memory Card International Association）フォームファクターのモジュール（PCカードとも呼ぶ）のいずれかである。セキュリティモジュール４３、４４は個別情報（EMM）と共通情報（ECM）とを処理し、その中の情報を用いてデコーダがスクランブルされた送信データを復号する。
【００３７】
本発明によると、新しく生産された同一モデルのデコーダは多くの面で同一であり、特にマスターでもスレーブでもないが、マスターかスレーブのいずれか（以下に説明するように、少なくとも単一のデコーダペアの中ではなく、同時にではないが、マスターとスレーブの両方になることもある）になることができるという点で同一である。
【００３８】
デコーダ４１、４２が最初にインストールされたとき、デコーダはマスターとして動作するかスレーブとして動作するかをセキュリティモジュール４３、４４に問い合わせ、セキュリティモジュール４３、４４は記憶しているCAM_STATE４５、４６を返す。セキュリティモジュール４３、４４がマスターと答えると、デコーダ４１、４２はマスターデコーダ４１として動作する。逆に、セキュリティモジュール４３、４４がスレーブと答えると、デコーダ４１、４２はスレーブデコーダ４２として動作する。マスターデコーダ４１は、そのセキュリティモジュール４３が適当なデスクランブル（復号）鍵を返すと、コンテントをデスクランブル（解読ともいう）する。このデスクランブルは、エラーが無ければ、加入に対応するサービス（番組を含む）のためのものである。スレーブデコーダ４２は、２つのデコーダ４１、４２がデジタル接続１３を介して接続されていて、正しくペアになっているときにのみ、そのセキュリティモジュール４４から提供されたデスクランブル鍵を用いてコンテントをデスクランブルする。
【００３９】
デコーダは、動作についてそのセキュリティモジュールにインストール時に問い合わせ

るのに加えて、セキュリティモジュールが挿入（または接続）されたことを検出するたびに同じ問い合わせを行う。また、好ましくは図５に示した以下の方法を用いて、ランダムな時間または間隔をあけて同じ問い合わせを行ってもよい。しかし、注意すべきことは、セキュリティモジュールは動作情報を直接デコーダに送ることもできるということである。

【００４０】

本発明によると、デコーダがそのセキュリティモジュールに動作について問い合わせた時に、２つの方法を用いることができる。最も簡単な方法は、簡単なコマンドを使って要求することである。しかし、この方法には、例えばハッカーが応答を容易に再生できてしまうという欠点がある。好ましい、よりセキュアな方法は、デコーダとセキュリティモジュールの間にセッション鍵に基づきセキュアチャンネルを設けることである。セキュアチャンネルに必要な情報について、すべてのデコーダが同一のグローバルな秘密鍵を持っていてもよい。ただし、この場合、システムはリバースエンジニアリングされ易くなる。各デコーダが個別に秘密鍵を有することが好ましく、リバースエンジニアリングを困難にする。

【００４１】

ステップ５１において、デコーダはPRNGを用いて乱数R（現実には疑似乱数）を決める。自分のIDとともにこの乱数Rをメッセージ５２としてセキュアチャンネルを介してセキュリティモジュールに送る。セキュリティモジュールは、ステップ５３においてKeyDevAlgoを用いて受信したIDとMKからDKを計算し、ステップ５４においてMACGenerateを用いて状態CAM_STATE、生成鍵DK、乱数Rからハッシュを計算する。そして、状態CAM_STATEとハッシュHをメッセージ５５としてデコーダに送る。最後に、ステップ５６において、デコーダはMACVerifyを用いてデータH、R、DKを用いてCAM_STATEを検証する。CAM_STATEが検証されると、decoder_STATEはCAM_STATEの値をとり、さもなければdecoder_STATEの値は変化しない。このようにデコーダはマスターになったり、スレーブになったりする。しかし、セキュリティモジュールから応答がない場合、またはセキュリティモジュールに接続されていないと検知した場合、マスターデコーダは自動的に「スレーブ」に変わることが好ましい。直ちに変わることが好ましいが、セキュリティモジュールへの接続を何度か試してみた後や、一定の時間が経過した後でもよい。

【００４２】

セキュリティモジュールは異なる方法で応答に関わる情報を受信したものであってもよい。

【００４３】

１つのソリューションは、CAプロバイダーが、マスターカードとスレーブカードの２種類のセキュリティモジュールを配布することである。マスターカードは常に「マスター」と応答し、スレーブカードは常に「スレーブ」と応答する。

【００４４】

他の好ましいソリューションは、CAプロバイダーが、デフォルトで１種類の応答（すなわち「マスター」か「スレーブ」かいずれか）を返す１つのユニークなセキュリティモジュールを配布することである。そして、放送事業者は専用のEMMを送信することにより、この応答を変更することができる。より複雑な仕組みも可能である。例えば、セキュリティモジュールに最初は「マスター」と応答させ、所定の使用時間（例えば２週間）が経過した後、「マスター」にとどまることを指示するEMMを受信しない限り、応答を変更して「スレーブ」と応答してもよい。

【００４５】

図６は、スレーブデコーダがペアとなっているマスターデコーダがあるかを検証する方法を示すフローチャートである。この方法は、デコーダがスレーブデコーダになった時はいつも、および／またはランダムな時間に実行することができる。スレーブデコーダ４２は、ステップ６０１において、他のデコーダに自分の識別情報を返すように要求するコマンドを、リンク１３を通して送る。他のデコーダが存在し、そのdecoder_STATEがマスタ

ーであるとき、そのデコーダはVとSigVを返す。さもなければ、何も返さない。ステップ６０２において、応答があったか否か検証する。何も応答が無いとき、スレーブデコーダのPAIRING_STATEは「ブロック」に設定され、本方法は終了する。応答があったとき、スレーブのPAIRING_STATEをチェックする。３つの可能性がある。

【００４６】

・スレーブデコーダのPAIRING_STATEが「バージン」である（すなわち、まだペアになったことがない）とき

スレーブデコーダのCPUは、公開鍵K_{pub_sig}を用いて、シグネチャSigVを用いてVをチェックする。ステップ６０４でシグネチャを検証することができると、スレーブデコーダは、ステップ６０５においてマスターデコーダとL回連続してチャレンジ－レスポンスプロトコルを開始する。このプロトコルは、有利にも、本技術分野において周知のゼロ知識タイプのもの（例えば、Fiat-Shamir）である。実施例を図７に示す。ここで、Lの典型的な値は１０と２０の間（両端を含む）の範囲である。すべてのチャレンジ－レスポンスプロトコルが成功したとき、ステップ６０７において、CPUはVをV’として格納し、PAIRING_STATEを「ペア」に変更する。デコーダはスレーブデコーダとして完全に動作できるようになる。ステップ６１３において、本方法は終了する。しかし、チャレンジ－レスポンスプロトコルが失敗するとすぐに、デコーダはそのPAIRING_STATEを変更せず、コンテントをデスクランブルできない状態にとどまる。その後すぐに、または所定時間経過後、またはランダム時間経過後に、デコーダは図６に示した方法を再スタートし、チャレンジ－レスポンスプロトコルのシーケンスを再スタートする。

【００４７】

・スレーブデコーダのPAIRING_STATEが「ペア」（すなわち成功裏にペアとなっている）または「ブロック」（すなわちデコーダの機能の一部が抑制されている）のとき

CPUはステップ６０８において、受信したVは記憶されたV’と等しいかどうか検証する。等しくない場合（例えば、ユーザがデコーダをそれがペアになっているデコーダ以外のデコーダにリンクさせようとした場合）、ステップ６０９においてPAIRING_STATEは「ブロック」に設定され、デコーダはコンテントをデスクランブルできなくなる（または、場合に応じて、デスクランブルできない状態に留まる）。しかし、VとV’が一致したとき、CPUはステップ６１０においてチャレンジ－レスポンスプロトコルのシーケンスをスタートし、すべてのプロトコルが成功したとき、スレーブデコーダのPAIRING_STATEは「ペア」となる。スレーブデコーダはステップ６１２でスレーブデコーダとして完全に動作可能となり、本方法はステップ６１３で終了する。一方、プロトコルが失敗すると、スレーブデコーダのPAIRING_STATEは「ブロック」となり（または、「ブロック」に留まり）、デコーダはステップ６０９においてコンテントをデスクランブルできなくなる（または、できない状態に留まる）。その後、本方法はステップ６１３において終了する。

【００４８】

マスターデコーダは常にコンテントをデスクランブルできるが、スレーブデコーダは正式にペアとなっているときだけ、コンテントをデスクランブルできる。マスターデコーダに接続されていない場合、デスクランブルすることはできない。また、注意すべきことは、デコーダはそのdecoder_STATEが「マスター」のときにのみ、スレーブデコーダから送られたチャレンジ、その他のメッセージ、要求に応答するということである。スレーブデコーダは応答しない。

【００４９】

図７は、先行技術による２つのデコーダ（図４の４１と４２）間のチャレンジ－レスポンスプロトコルを示す図である。以下の説明では、マスターデコーダおよびスレーブデコーダという用語を例として使用するが、これが通常の状況だからである。スレーブデコーダはステップ７１においてプロトコルを開始し、接続１３を通してマスターデコーダにコミットメントを要求するメッセージ７２を送る。ステップ７３において、マスターデコーダは一時的な値rを選択し、コミットメント$G=r^2$を計算し、メッセージ７４でスレーブに送る。スレーブデコーダはステップ７５においてPNRGを用いてランダムチャレンジbを選

択し、それをメッセージ７６でマスターに送る。マスターはステップ７７においてレスポンスA=rS^bを計算し、メッセージ７８としてスレーブに返す。ステップ７９において、スレーブはA^2が本当にGV^bと等しいことをチェックすることにより、レスポンスを検証する。検証が成功すると、チャレンジ－レスポンスプロトコルは成功である。さもなければ、失敗である。

【００５０】

以上の説明から明らかなように、本発明はここで説明したように２つのデコーダを強制的にペアリングする方法を提供するものであり、以下の長所を有する。

・製造の段階ではデコーダ間に違いはない。デコーダはマスターデコーダまたはスレーブデコーダのいずれかになり、違いはデコーダをインストールした後に生じるだけである。

・本発明を実施するために必要な限定受信システムの変更は少しである。CAプロバイダーがカードを個人化の際に異ならせれば、既存のメッセージで本方法を実行することができる。

・デコーダの状態は専用個別情報EMMの送信により無線で交信することができる。

・バックオフィスはエンタイトルメントとデコーダの組み合わせをトレースし、リスト化する必要が無く、販売後のメンテナンスが簡単になる。

【００５１】

当然のことながら、本発明を純粋に実施例により説明し、本発明の範囲を逸脱することなく細部を変更することができる。特に、本発明は携帯電話その他のデバイスや、端末が限定的に接続される他のタイプのシステム（音楽やコンピュータファイルにアクセスするシステム等）のペアリングに適用することができる。

【００５２】

明細書、特許請求の範囲（適当な場合）、図面に開示した各特徴は、個別に提供してもよいし、適当に組み合わせて提供してもよい。ハードウェアで実施すると説明した特徴をソフトウェアで実施してもよいし、その逆でもよい。

【００５３】

言うまでもなく、「マスターデコーダ」という用語は少なくとも一時的にマスターデコーダとして動作するデコーダとして解釈すべきであり、反対に、「スレーブデコーダ」という用語は少なくとも一時的にスレーブデコーダとして動作するデコーダとして解釈しなければならない。

【図面の簡単な説明】

【００５４】

【図１】従来技術によるデコーダのペアリングの基本的コンセプトを示す概略図である。

【図２】本発明によるデコーダのアーキテクチャを示す図である。

【図３】セキュリティモジュールを示すブロック図である。

【図４】本発明によるペア状態のデコーダを示すブロック図である。

【図５】本発明による、デコーダと関連セキュリティモジュールによる状態検証の方法を示す図である。

【図６】本発明による２つのデコーダ間のペアリング方法を示すフローチャートである。

【図７】従来技術によるチャレンジ－レスポンスプロトコルを示す図である。

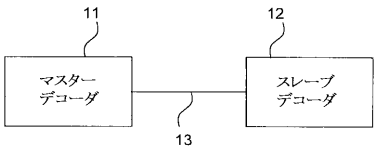
【符号の説明】

【００５５】

１１　マスターデコーダ
１２　スレーブデコーダ
２３　ビデオユニット
２６　セキュリティモジュールインターフェイス
２５ａ　セキュリティメモリ
２５ｂ　不揮発メモリ
２７　シリアルインターフェイス
３３　通信ユニット

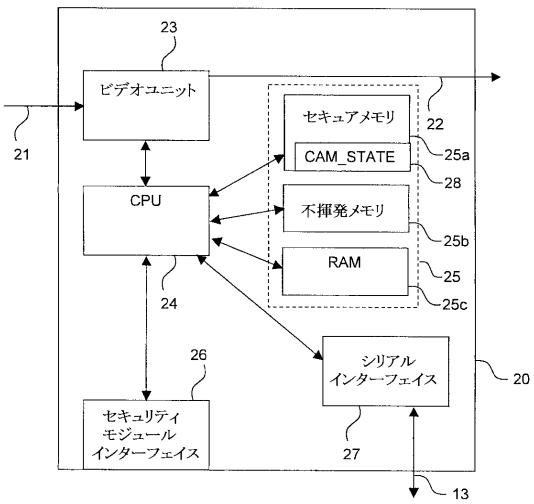
３２　　セキュリティメモリ
４１　　マスターデコーダ
４２　　スレーブデコーダ
４３　　セキュリティモジュール
４４　　セキュリティモジュール

【図１】

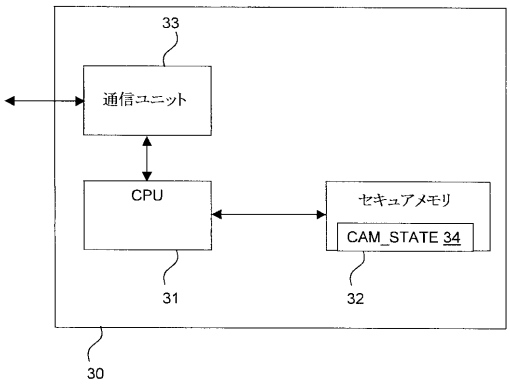


（従来技術）

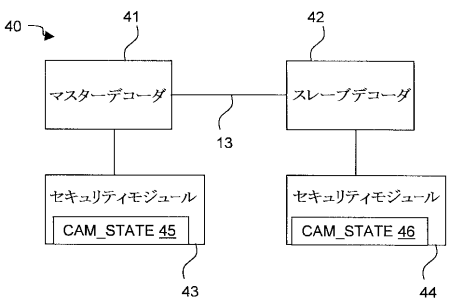
【図２】



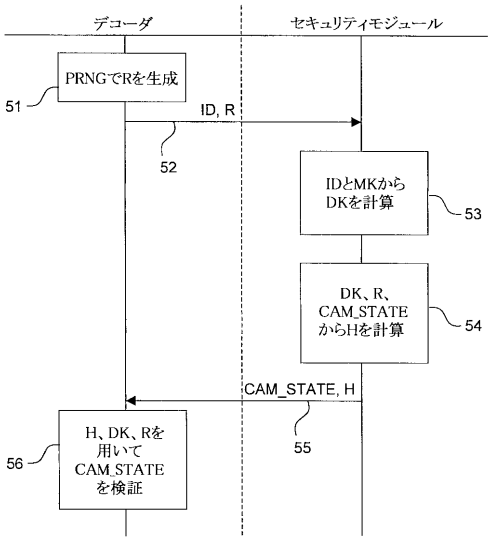
【図３】



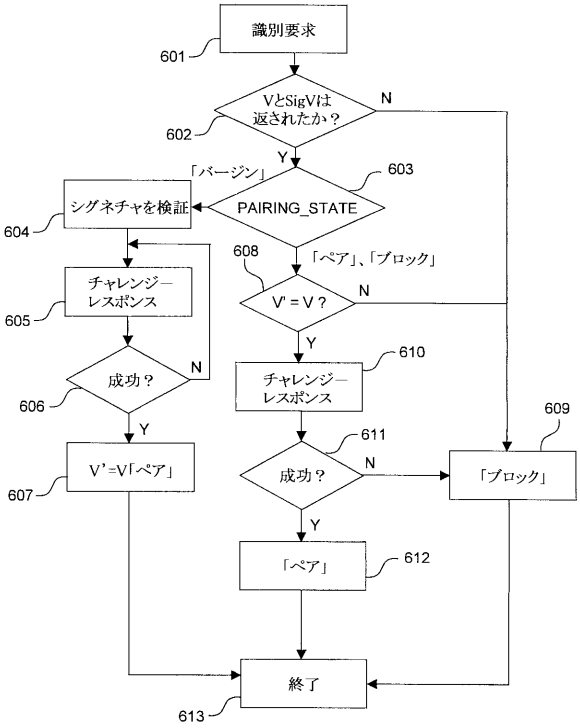
【図４】



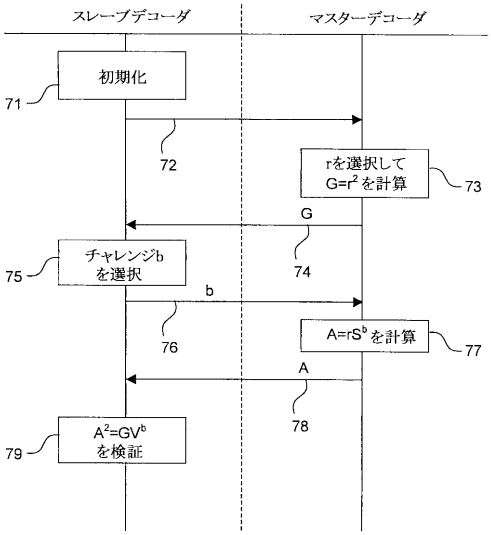
【図５】


デコーダ
セキュリティモジュール
PRNGでRを生成
51
ID, R
52
IDとMKから
DKを計算
53
DK、R、
CAM_STATE
からHを計算
54
CAM_STATE, H
55
H、DK、Rを
用いて
CAM_STATE
を検証
56

【図６】


識別要求
601
VとSigVは
返されたか？
602
N
Y
「バージン」
603
PAIRING_STATE
シグネチャを検証
604
「ペア」、「ブロック」
608
チャレンジ－
レスポンス
605
V' = V ?
N
Y
成功？
606
N
Y
610
チャレンジ－
レスポンス
611
V'=V「ペア」
607
成功？
N
609
「ブロック」
Y
「ペア」
612
終了
613

【図７】


スレーブデコーダ
マスターデコーダ
初期化
71
72
rを選択して
G=r² を計算
73
G
74
チャレンジb
を選択
75
b
76
A=rS^b を計算
77
A
78
A²=GV^b
を検証
79

（従来技術）

フロントページの続き

(74)代理人 100135079
弁理士 宮崎 修
(72)発明者 エリク ディエル
フランス国, ３５３４０ リフレ, ラ・ビュザルディエール（番地なし）
(72)発明者 ジャン－ピエール アンドロー
オランダ国, １０１２ エスペー アムステルダム, スパイストラート 3エフ2
(72)発明者 ルイ－グザヴィエ カルボネル
フランス国, ３５７４０ パセ, リュ・デ・ブルー ２５
(72)発明者 アラン デュラン
フランス国, ３５０００ レンヌ, リュ・ド・ディナン ７９

審査官 矢野 光治

(56)参考文献 特開２０００－３４１２２７（ＪＰ，Ａ）
特開２００１－２９８７２２（ＪＰ，Ａ）
特開２０００－０５９４０８（ＪＰ，Ａ）
特開２０００－００４４３１（ＪＰ，Ａ）
特開２００４－１４７３４４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｎ ７／１６－７／１７３