(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-171222
(P2014-171222A)
(43)公開日　平成26年9月18日(2014.9.18)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 7　OL　外国語出願　（全 10 頁）

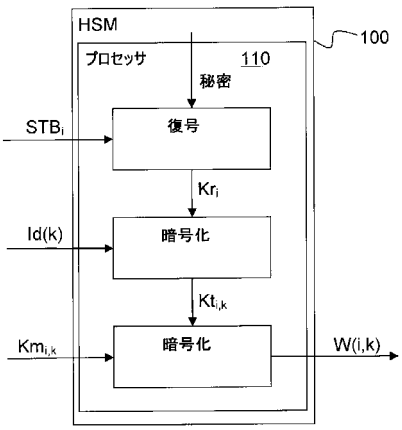
(21)出願番号　特願2014-40648(P2014-40648)
(22)出願日　平成26年3月3日(2014.3.3)
(31)優先権主張番号　13305245.6
(32)優先日　平成25年3月4日(2013.3.4)
(33)優先権主張国　欧州特許庁(EP)

(71)出願人　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　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】暗号化された鍵を生成する装置および暗号化された鍵を受信機に提供する方法

(57)【要約】
【課題】暗号化されたマスター鍵を生成する装置。
【解決手段】装置（１００）は、受信機識別子（STB_i）、サービス・プロバイダー識別子（Id(k)）およびサービス・プロバイダーのためのマスター鍵（$Km_{j,k}$）を受領するよう構成された少なくとも一つの入力インターフェースと；当該装置の秘密を記憶するよう構成されたメモリと；前記秘密を使って前記受信機識別子を処理してルート鍵（Kr_i）を得て、前記ルート鍵を使って前記サービス・プロバイダー識別子を処理してトップ鍵（$Kt_{i,k}$）を得て、前記トップ鍵を使って前記マスター鍵を処理して暗号化されたマスター鍵（W(i,k)）を得るよう構成されたプロセッサと；暗号化されたマスター鍵を出力するよう構成された出力インターフェースとを有する。暗号化されたマスター鍵を受信機に提供する方法も提供される。本装置は、新たなサービス・プロバイダーが、すでに展開済みのスマートカードを使って受信機にサービスを提供できるようにするという利点がある。
【選択図】図５



【特許請求の範囲】
【請求項１】
暗号化されたマスター鍵を生成する装置であって：
受信機識別子（STB_i）、サービス・プロバイダー識別子（Id(k)）およびサービス・プロバイダーのためのマスター鍵（$Km_{j,k}$）を受領するよう構成された少なくとも一つの入力インターフェースと；
当該装置の秘密を記憶するよう構成されたメモリと；
・前記秘密を使って前記受信機識別子を処理してルート鍵（Kr_i）を得て、
・前記ルート鍵を使って前記サービス・プロバイダー識別子を処理してトップ鍵（$Kt_{i,k}$）を得て、
・前記トップ鍵を使って前記マスター鍵を処理して暗号化されたマスター鍵（W(i,k)）を得るよう構成されたプロセッサと；
暗号化されたマスター鍵を出力するよう構成された出力インターフェースとを有する、装置。
【請求項２】
当該装置がハードウェア・セキュア・モジュールにおいて実装される、請求項１記載の装置。
【請求項３】
当該装置がスマートカードにおいて実装される、請求項１記載の装置。
【請求項４】
前記プロセッサが、前記秘密を復号鍵として使って前記受信機識別子を復号するよう構成されている、請求項１記載の装置。
【請求項５】
前記プロセッサが、前記ルート鍵を暗号化鍵として使って、前記サービス・プロバイダー識別子を暗号化するよう構成されている、請求項１記載の装置。
【請求項６】
前記プロセッサが、前記トップ鍵を暗号化鍵として使って前記マスター鍵を暗号化するよう構成されている、請求項１記載の装置。
【請求項７】
暗号化されたマスター鍵を受信機に提供する方法であって：
請求項１記載の、暗号化されたマスター鍵を生成する装置が、第一の装置から、前記暗号化されたマスター鍵を生成する、受信機識別子（STB_i）、サービス・プロバイダー識別子（Id(k)）およびサービス・プロバイダーのためのマスター鍵（$Km_{j,k}$）を受領する段階と；
暗号化されたマスター鍵を生成する前記装置が、前記暗号化されたマスター鍵を生成する段階と；
暗号化されたマスター鍵を生成する前記装置が、生成された暗号化されたマスター鍵を出力する段階と；
第三の装置が前記暗号化されたマスター鍵を前記受信機に送る段階とを含む、
方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概括的には暗号システムに関し、詳細には、安全な仕方で、新たなサービス・プロバイダーによって提供される暗号鍵を必要とするサービスの展開を可能にすることに関する。
【背景技術】
【０００２】
この節は、以下で記述および／または特許請求される本発明のさまざまな側面に関係しうる技術のさまざまな側面を読者に紹介することを意図したものである。この議論は、本

発明のそうしたさまざまな側面のよりよい理解を助けるための背景情報を読者に提供する助けとなると思われる。よって、これらの陳述は、従来技術の自認としてではなく、この観点で読まれるべきであることは理解しておくべきである。

【０００３】

テレビジョン（および他のメディア）のための条件付きアクセス・システム（これは限定しない例として使う）は、種々のコンテンツを保護するために以前から存在していた。簡単に言うと、そのようなシステムでは、サービス・プロバイダーがコンテンツ・プロバイダーからコンテンツを取得し、顧客への送達前に、条件付きアクセス・システム（CAS: conditional access system）を使って、特に暗号化を使って、該コンテンツを保護する。顧客は一般に何らかのデコーダを有しており、該デコーダは、条件付きアクセス・システムの一部を実装し、それによりユーザーがそのコンテンツにアクセスする権利を有しているかどうかを検証し、有していれば、そのコンテンツを復号してレンダリングする。

【０００４】

よく知られているように、ユーザー側では、CASの上記一部はしばしば、デコーダに除去可能な形で挿入されるスマートカード（これはセキュリティ・モジュールの限定しない例として本稿で使われる）において実装される。スマートカードは少なくとも間接的には、システムのセキュリティを保証するCASプロバイダーによって提供される。デコーダ・マスター鍵Km_iも、その使用を通じて得られる鍵も、スマートカードから抽出できるべきではない。

【０００５】

図１は、サービスにアクセスするための第一の従来技術の方式を示している。識別子STBiをもつスマートカードを備えたデコーダに、サービス鍵K_j（有利にはシステムにおける全デコーダに共通）を使って暗号化されたサービスjへのアクセスを許容するために、サービス・プロバイダーは対称暗号化アルゴリズム（たとえば先進暗号化標準（AED: Advanced Encryption Standard）など）およびサービス鍵K_jを使って、送信前にサービスjを暗号化する。サービス・プロバイダーは、全デコーダに共通であってもよいサービス鍵K_jをも、マスター鍵Km_iおよび好ましくは前記対称暗号化アルゴリズムに対応する鍵を使って暗号化し、暗号化されたサービス$E\{K_j\}(j)$と、暗号化されたサービス鍵をもつメッセージM(i,j)とをデコーダに送信する。

【０００６】

デコーダはまず対称暗号化アルゴリズムおよびそのマスター鍵Km_iを使ってメッセージM(i,j)を復号してサービス鍵K_jを得る。このサービス鍵K_jは、暗号化されたサービス$E\{K_j\}(j)$の復号のために前記対称暗号化アルゴリズムと一緒に使われて、サービスjが得られる。マスター鍵Km_iはデコーダに固有なので、それはメッセージM(i,j)を使ってサービスを復号できる唯一の鍵である。

【０００７】

図２は、サービスにアクセスするための第二の従来技術の方式を示している。システムにおけるさらなる柔軟性およびさらなる安全性を可能にするために、サービスjおよび典型的には時間期間tについてのセッション鍵$Ks_{j,t}$を使うことがしばしば好ましい。この場合、サービス・プロバイダーは、セッション鍵$Ks_{j,t}$を使ってサービスjを暗号化して、暗号化されたサービス$E\{Ks_{j,t}\}(j)$を得て、サービス鍵K_jを使ってセッション鍵Ks(j,t)を暗号化して第一のメッセージT(j,t)を得て、デコーダ・マスター鍵Km_iを使ってサービス鍵K_jを暗号化して第二のメッセージM(i,j)を得る。暗号化されたサービス$E\{K_{j,t}\}(j)$、第一のメッセージT(j,t)および第二のメッセージM(i,j)がデコーダに送られる。これは必ずしも同時ではない。

【０００８】

図１と同様に、デコーダはこれらの動作を逆に行なう。デコーダはデコーダ・マスター鍵Km_iを使って第二のメッセージM(i,j)を復号してサービス鍵K_jを得て、サービス鍵K_jを使って第一のメッセージT(j,t)を復号してセッション鍵を得て、そのセッション鍵が、暗

号化されたサービスE{$Ks_{j,t}$}(j)を復号するために使われて、サービスjが得られる。

【０００９】

図１および図２に示した方式は、単一のサービス・プロバイダーをもつシステムではよく機能する。しかしながら、最近では、デコーダは、「単に」コンテンツの復号を提供することから進化して新たなアプリケーションを含めるようになってきた。そのような新たなアプリケーションは次のようなものを含む。

・ユーザーの家庭ネットワークにおける他の装置、たとえば第二のデコーダ、スマートフォンまたはタブレット・コンピュータに宛てた、圧縮されたフォーマットでの付加価値サービスの送信。

・アプリケーション・ストア（たとえば、アップルストア、フリーボックス・レボリューション）からのゲームのようなアプリケーションのダウンロードおよび実行。

・コンテンツ・プロバイダーは、付加価値サービスをデコーダを介してユーザーに提供することができ、該付加価値サービスは、サービス・プロバイダーやCASプロバイダーの制御下にはない。

【００１０】

これは、CASの責任が発達しつつあることを意味している。以前にはシステム全体のセキュリティの保証者だったものが、サービス・プロバイダーの付加価値サービスのセキュリティに責任を負うようになっており、その一方、同時に、デコーダを他の「二次」サービス・プロバイダーと「共有」する。

【００１１】

二次サービス・プロバイダーはデコーダにおいて自分たちのサービスを保護するために独自のセキュリティ機能を要求し、この機能がCASと少なくとも同等のセキュリティ・レベルを提供する可能性が高い。

【００１２】

たとえば、図１および図２に示したものの上にさらに階層を加えることによって、さらなるサービス・プロバイダーを追加することができる。そのような方式は、図１に示した方式を拡張する図３に示されている。

【００１３】

さらなるサービス・プロバイダーは独自のマスター鍵$Km_{i,k}$を有している。そうしたマスター鍵はSTBiについてのルート鍵Kr_iを使って暗号化されて、暗号化されたマスター鍵W(i,k)が得られる。ここで、iはSTBiのインデックスであり、kはサービス・プロバイダーのインデックスである。この暗号化されたマスター鍵W(i,k)は、マスター鍵$Km_{i,k}$をスマートカードに提供することによって、スマートカードを使って得ることができる。スマートカードは、特定のヒューズが溶断されない限り、ルート鍵Kr_iを使ってマスター鍵$Km_{i,k}$を暗号化して、暗号化されたマスター鍵W(i,k)を出力する。暗号化されたマスター鍵W(i,k)は次いでスマートカード外に、たとえばフラッシュメモリに記憶されてもよい。しかしながら、ひとたびヒューズが溶断されたら、スマートカードは鍵を暗号化せず、暗号化された鍵を復号するのみとなる。

【発明の概要】

【発明が解決しようとする課題】

【００１４】

ルート鍵を知ることは必要ないが、スマートカードの寿命の間はサービス・プロバイダーを追加することが不可能であることを注意しておくべきである。というのも、ヒューズは、セキュリティ上の理由により、エンドユーザーへの送達前に溶断されるからである。対称暗号では暗号化は復号と同じとはいえ、「復号」のための鍵を提供して、「復号された」――暗号化されたのと同じ――鍵を得ることを期待することはできない。スマートカードからは復号されたサービスのみが出力され、中間的な鍵は内部に保持されるからである。

【００１５】

デコーダiは暗号化されたマスター鍵W(i,k)を受領し、ルート鍵Kr_iを使ってそれを復号

し、マスター鍵$Km_{i,k}$を出力する。このマスター鍵が第二のメッセージ(M,i,j,k)を復号してサービス・プロバイダーkについてのサービス鍵$K_{j,k}$を得るために使われる。サービス鍵$K_{j,k}$は次いで暗号化されたサービス$E\{Ks_{j,k}\}$(j,k)を復号してサービスj,kを平文で得るために使われる。

【００１６】

見て取れるように、いくつかの役者が関わっている：スマートカード製造業者、デコーダを製造する統合者（integrator）、一または複数のサービス・プロバイダーおよびデコーダをエンドユーザーに提供するクライアントである。従来技術の解決策は、いくつかのサービス・プロバイダーと協働するよう、その鍵を追加することによってスマートカードをカスタマイズすることを許容するものの、そのようなサービス・プロバイダーの数はスマートカード中の一回プログラム可能型（One Time Programmable）フラッシュメモリにおけるヒューズの数に限られる（追加される鍵毎に一つのヒューズが溶断される）。さらに、鍵は工場において特殊な機械を使って追加されねばならないので、こうしたサービス・プロバイダーは、カスタマイズされたスマートカードが送達される前に知られていなければならない。

【００１７】

このように、エンドユーザーに、最初に考えられていなかったサービス・プロバイダーにアクセスすることを許容するシステムが必要とされていることは理解されるであろう。セキュリティ上の理由により、デコーダ製造業者は、サービス・プロバイダーの追加を制御すべきではなく、サービス・プロバイダーの秘密鍵は他の役者に、特に他のサービス・プロバイダーに知られるべきではない。

【００１８】

本発明は、そのような可能性を提供する。

【課題を解決するための手段】

【００１９】

第一の側面では、本発明は、暗号化されたマスター鍵を生成する装置に向けられる。本装置は、受信機識別子、サービス・プロバイダー識別子およびサービス・プロバイダーのためのマスター鍵を受領するよう構成された少なくとも一つの入力インターフェースと；当該装置の秘密を記憶するよう構成されたメモリと；前記秘密を使って前記受信機識別子を処理してルート鍵を得て、前記ルート鍵を使って前記サービス・プロバイダー識別子を処理してトップ鍵を得て、前記トップ鍵を使って前記マスター鍵を処理して暗号化されたマスター鍵を得るよう構成されたプロセッサと；暗号化されたマスター鍵を出力するよう構成された出力インターフェースとを有する。

【００２０】

第一の実施形態では、本装置は、ハードウェア・セキュア・モジュール（Hardware Secure Module）において実装される。

【００２１】

第二の実施形態では、本装置は、スマートカードにおいて実装される。

【００２２】

第三の実施形態では、前記プロセッサは、前記秘密を復号鍵として使って前記受信機識別子を復号するよう構成されている。

【００２３】

第四の実施形態では、前記プロセッサは、前記ルート鍵を暗号化鍵として使って、前記サービス・プロバイダー識別子を暗号化するよう構成されている。

【００２４】

第五の実施形態では、前記プロセッサは、前記トップ鍵を暗号化鍵として使って前記マスター鍵を暗号化するよう構成されている。

【００２５】

第二の側面では、本発明は、暗号化されたマスター鍵を受信機に提供する方法に向けられる。上記第一の側面に基づく暗号化されたマスター鍵を生成する装置が、第一の装置か

ら、前記暗号化されたマスター鍵を生成する、受信機識別子（STB_i）、サービス・プロバイダー識別子（Id(k)）および該サービス・プロバイダーのためのマスター鍵（$Km_{j,k}$）を受領し；前記暗号化されたマスター鍵を生成し；第三の装置によって前記受信機に送られる、生成された暗号化されたマスター鍵を出力する。

【図面の簡単な説明】

【００２６】

ここで、本発明の好ましい特徴について、付属の図面を参照しつつ、限定しない例として記述する。

【図１】サービスにアクセスする第一の従来技術の方式を示す図である。

【図２】サービスにアクセスする第二の従来技術の方式を示す図である。

【図３】サービスにアクセスする第三の従来技術の方式を示す図である。

【図４】本発明のある好ましい実施形態に基づく、サービスへのアクセスを示す図である。

【図５】本発明のある好ましい実施形態に基づくハードウェア・セキュリティ・モジュールを示す図である。

【発明を実施するための形態】

【００２７】

従来技術の解決策は、デコーダが製造される前に、デコーダ製造業者がサービス・プロバイダーを知っていることを要求する。

【００２８】

さらなる鍵階層を追加することは、この問題を回避することを可能にする。さらに、各サービス・プロバイダーは、秘密である必要のない一意的な識別子Id(k)と、暗号化されたマスター鍵を生成する装置を有する。これについて以下でさらに述べる。

【００２９】

図４は、本発明のある好ましい実施形態に基づく、サービスへのアクセスを示している。これは図３に示した方式の拡張である。デコーダiのスマートカードまたは（システム・オン・チップ内の）暗号プロセッサのようなプロセッサは、少なくとも二つの方法の一つにおいてそのルート鍵Kr_iへのアクセスをもつ：ルート鍵はそのメモリに書き込まれてもよいし、あるいは暗号化されたルート鍵を復号するためにプロセッサの秘密を使うことによって生成されてもよい――後者のオプションは破線の四角内で図示されている。プロセッサはサービス・プロバイダーkの識別子Id(k)を受領し、そのルート鍵Kr_iを使ってこれを復号して、当該プロセッサおよびサービス・プロバイダーのためのトップ鍵$Kt_{i,k}$を得る。暗号化されたマスター鍵W(i,k)はトップ鍵$Kt_{i,k}$を使って復号され、マスター鍵$Km_{i,k}$が得られ、このマスター鍵が第二のメッセージ(M,i,j,k)を復号して、サービス・プロバイダーkのためのサービス鍵$K_{j,k}$を得るために使われる。次いでサービス鍵$K_{j,k}$は暗号化されたサービス$E\{Ks_{j,k}\}(j,k)$を復号してサービスj,kを平文で得るために使われる。

【００３０】

サービス・プロバイダーは、図５に示されるような、デコーダ製造業者によって提供されるいわゆるハードウェア・セキュリティ・モジュール（HSM: Hardware Security Module）１００を使って、安全な仕方でユーザーiのための暗号化されたマスター鍵W(i,k)を得る。HSM　１００はその秘密情報を外部には秘匿されたままにするよう実装される。HSM　１００は少なくとも一つのプロセッサ１１０ならびに出力インターフェース、メモリ、内部接続および電源（そのエネルギーは外部から提供されてもよい）のような、他の必要だが明確のために図示しない特徴を有する。

【００３１】

HSM　１００は装置から受信機の識別子STBi、サービス・プロバイダー識別子Id(k)およびそのサービス・プロバイダーおよび受信機のためのマスター鍵$Km_{i,k}$を受領する。プロセッサ１１０は内部メモリからHSMの秘密を取得し、それを使って識別子STBiを復号してルート鍵Kr_iを得る。プロセッサは次いでルート鍵Kr_iを使ってサービス・プロバイダー識別子Id(k)を暗号化してトップ鍵$Kt_{i,k}$を得る。次いでこのトップ鍵がマスター鍵$Km_{i,k}$を

暗号化して暗号化されたマスター鍵W(i,k)を得るのに使われる。この暗号化されたマスター鍵が、次いで、HSM　１００によって出力されて、デコーダiに送られ、デコーダiにおいて、サービスにアクセスするために使用されることができる。暗号化されたマスター鍵W(i,k)はすでに暗号化されているので、（電子メールまたはインバンド送信のような任意の好適な送信装置および方法を使っての）デコーダへの送信のためにそれをさらに暗号化する必要はない。対称暗号では、暗号化および復号は本質的には同一であることを注意しておくべきである。

【００３２】

トップ鍵$Kt_{i,k}$はHSM　１００によって出力されないので、サービス・プロバイダーによって変更されることはできないことが理解されるであろう。つまり、サービス・プロバイダーは、セキュリティの観点からは、互いに隔離されているということである。

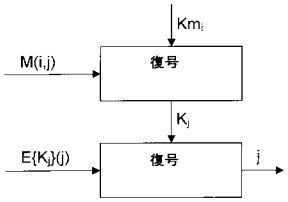
【００３３】

当業者は、本発明が、安全な仕方で新しいサービス・プロバイダーにアクセスすることをスマートカードに許する解決策を提供できることを認識するであろう。

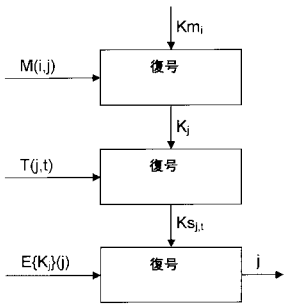
【００３４】

本稿および（適切な場合には）請求項および図面において開示される各特徴は、独立して提供されても、あるいは任意の適切な組み合わせにおいて提供されてもよい。ハードウェアにおいて実装されると記述されている特徴がソフトウェアで実装されてもよく、逆にソフトウェアにおいて実装されると記述されている特徴がハードウェアで実装されてもよい。請求項に参照符号があったとしても、単に例解のためであり、請求項の範囲に対する限定効果をもつものではない。

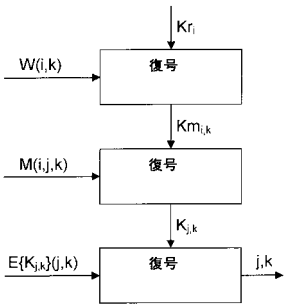
【図１】



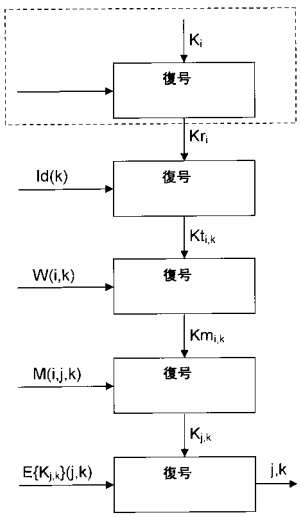
【図２】



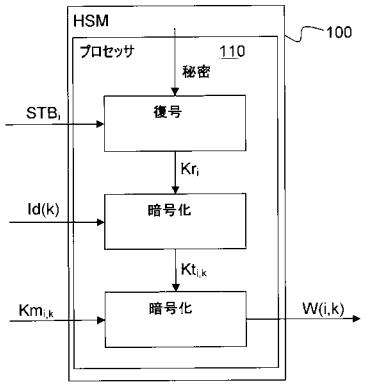
【図３】



【図４】



【図５】



フロントページの続き

(72)発明者 エリック デスミット
フランス国, ３５２３５ トリニエーフイヤール, リュ・ドゥ・シャン・メロアン １６
(72)発明者 オリヴィエ クルテ
フランス国, ３５０００ レンヌ, ルート・デ・ヴザン ６８
(72)発明者 ルノー リガル
フランス国 ３５ ５７６ セソン・セヴィニェ シー・エス １７６ １６ ザック・ド・シャン・ブラン アヴェニュ・ド・シャン・ブラン ９７５ テクニカラー・アールアンドディー・フランス

Ｆターム(参考) 5J104 AA16 EA17 JA03 MA05 NA02 PA07

【外国語明細書】
2014171222000001.pdf