(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2006-340407
(P2006-340407A)
(43)公開日　平成18年12月14日(2006.12.14)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/14	(2006.01)	H04L	9/00	641	5J104

審査請求 有　請求項の数 18　OL　（全 29 頁）

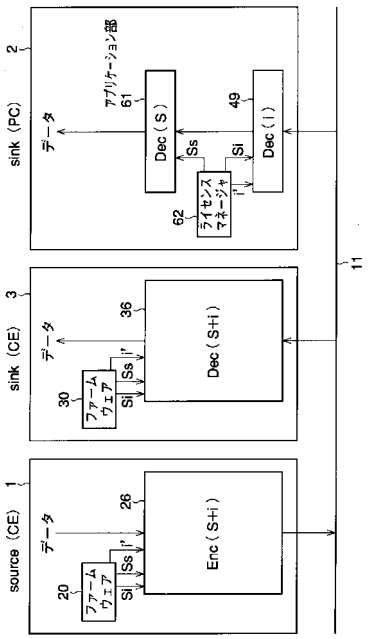
(21)出願番号　特願2006-258760 (P2006-258760)
(22)出願日　平成18年9月25日 (2006.9.25)
(62)分割の表示　特願平9-106136の分割
原出願日　平成9年4月23日 (1997.4.23)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　刑部　義雄
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】暗号化装置および方法、並びに復号装置および方法

(57)【要約】
【課題】不正なコピーを確実に防止する。
【解決手段】DVDプレーヤ１の１３９４インタフェース２６で暗号化されたデータを、１３９４バス１１を介して、パーソナルコンピュータ２と光磁気ディスク装置３に伝送する。機能を変更することがユーザに開放されていない光磁気ディスク装置３においては、受信したデータを１３９４インタフェース３６で復号する。これに対して、機能の変更がユーザに開放されているパーソナルコンピュータ２においては、１３９４インタフェース４９で時変キーｉを用いて暗号化データを復号し、その復号結果をアプリケーション部６１でセッションキーＳを用いてさらに復号する。
【選択図】図１０



【特許請求の範囲】
【請求項１】
暗号鍵を用いてデータを暗号化する暗号化装置において、
第１の鍵情報を供給する第１の供給手段と、
セッション中に変更される第２の鍵情報を供給する第２の供給手段と、
前記第２の鍵情報の変更に応じて前記セッション中に所定のタイミングで変更される前記暗号鍵を、前記第１の鍵情報と前記第２の鍵情報とに基づいて生成する生成手段と、
前記暗号鍵を用いてデータを暗号化する暗号化手段と
を備えることを特徴とする暗号化装置。
【請求項２】
前記暗号鍵で暗号化されたデータを、他の装置に送信する送信手段
をさらに備える
ことを特徴とする請求項1に記載の暗号化装置。
【請求項３】
暗号鍵を用いてデータを暗号化する暗号化装置の暗号化方法において、
第１の鍵情報を供給し、
セッション中に変更される第２の鍵情報を供給し、
前記第２の鍵情報の変更に応じて前記セッション中に所定のタイミングで変更される前記暗号鍵を、前記第１の鍵情報と前記第２の鍵情報とに基づいて生成し、
前記暗号鍵を用いてデータを暗号化する
ことを特徴とする暗号化方法。
【請求項４】
前記暗号鍵で暗号化されたデータを、他の装置に送信する
ことを特徴とする請求項３に記載の暗号化方法。
【請求項５】
暗号鍵を用いてデータを復号する復号装置において、
暗号化されたデータを受信する受信手段と、
第１の鍵情報を供給する第１の供給手段と、
セッション中に変更される第２の鍵情報を供給する第２の供給手段と、
前記第２の鍵情報の変更に応じて前記セッション中に所定のタイミングで変更される前記暗号鍵を、前記第１の鍵情報と前記第２の鍵情報とに基づいて生成する生成手段と、
前記暗号鍵を用いて、前記受信手段で受信された暗号化されたデータを復号する復号手段と
を備えることを特徴とする復号装置。
【請求項６】
暗号鍵を用いてデータを復号する復号装置の復号方法において、
暗号化されたデータを受信し、
第１の鍵情報を供給し、
セッション中に変更される第２の鍵情報を供給し、
前記第２の鍵情報の変更に応じて前記セッション中に所定のタイミングで変更される前記暗号鍵を、前記第１の鍵情報と前記第２の鍵情報とに基づいて生成し、
前記暗号鍵を用いて、受信した暗号化されたデータを復号する
ことを特徴とする復号方法。
【請求項７】
暗号鍵を用いてデータを暗号化する暗号化装置において、
暗号化部と、
前記暗号化部に接続された暗号鍵生成部と、
前記暗号鍵生成部に接続された第１の鍵情報供給部と、
前記暗号鍵生成部に接続された第２の鍵情報供給部と
を備え、

前記暗号化部は、前記第１の鍵情報供給部から供給される第1の鍵情報と、前記第２の鍵情報供給部から供給される、セッション中に所定のタイミングで変更される第２の鍵情報とに基づいて前記暗号鍵生成部によって生成された前記暗号鍵を用いて、前記データを暗号化する

ことを特徴とする暗号化装置。

【請求項８】

前記暗号鍵で暗号化されたデータを、他の装置に送信する送信部

をさらに備える

ことを特徴とする請求項７に記載の暗号化装置。

【請求項９】

暗号鍵を用いてデータを復号する復号装置において、

受信部と、

前記受信部に接続された復号部と、

前記復号部に接続された暗号鍵生成部と、

前記暗号鍵生成部に接続された第１の鍵情報供給部と、

前記暗号鍵生成部に接続された第２の鍵情報供給部と

を備え、

前記復号部は、前記第１の鍵情報供給部から供給される第１の鍵情報と、前記第２の鍵情報供給部から供給される、セッション中に所定のタイミングで変更される第２の鍵情報とに基づいて前記暗号鍵生成部によって生成された前記暗号鍵を用いて、前記受信部で受信された暗号化されたデータを復号する

ことを特徴とする復号装置。

【請求項１０】

暗号鍵を用いてデータを暗号化する暗号化装置において、

他の装置との通信によって、前記暗号化装置と前記他の装置との間で共通に保持されている第１の鍵情報を供給する第１供給手段と、

所定のタイミングで変更される第２の鍵情報を供給する第２供給手段と、

前記第２の鍵情報の変更に応じて前記所定のタイミングで変更される前記暗号鍵を、前記他の装置と共通に保持する前記第１の鍵情報と前記所定のタイミングで変更される前記第２の鍵情報とに基づいて生成する生成手段と、

前記暗号鍵を用いてデータを暗号化する暗号化手段と

を備えることを特徴とする暗号化装置。

【請求項１１】

前記暗号鍵で暗号化されたデータを、前記他の装置に送信する送信手段

をさらに備える

ことを特徴とする請求項１０に記載の暗号化装置。

【請求項１２】

暗号鍵を用いてデータを暗号化する暗号化装置の暗号化方法において、

他の装置との通信によって、前記暗号化装置と前記他の装置との間で共通に保持されている第１の鍵情報を供給し、

所定のタイミングで変更される第２の鍵情報を供給し、

前記第２の鍵情報の変更に応じて前記所定のタイミングで変更される前記暗号鍵を、前記他の装置と共通に保持する前記第１の鍵情報と前記所定のタイミングで変更される前記第２の鍵情報とに基づいて生成し、

前記暗号鍵を用いてデータを暗号化する

ことを特徴とする暗号化方法。

【請求項１３】

前記暗号鍵で暗号化されたデータを、前記他の装置に送信する

ことを特徴とする請求項１２に記載の暗号化方法。

【請求項１４】

暗号鍵を用いてデータを復号する復号装置において、
暗号化されたデータを受信する受信手段と、
他の装置との通信によって、前記復号装置と前記他の装置との間で共通に保持されている第１の鍵情報を供給する第１の供給手段と、
所定のタイミングで変更される第２の鍵情報を供給する第２の供給手段と、
前記第２の鍵情報の変更に応じて前記所定のタイミングで変更される前記暗号鍵を、前記他の装置と共通に保持する前記第１の鍵情報と前記所定のタイミングで変更される前記第２の鍵情報とに基づいて生成する生成手段と、
前記暗号鍵を用いて、前記受信手段で受信された暗号化されたデータを復号する復号手段と
を備えることを特徴とする復号装置。
【請求項１５】
暗号鍵を用いてデータを復号する復号装置の復号方法において、
暗号化されたデータを受信し、
他の装置との通信によって、前記復号装置と前記他の装置との間で共通に保持されている第１の鍵情報を供給し、
所定のタイミングで変更される第２の鍵情報を供給し、
前記第２の鍵情報の変更に応じて前記所定のタイミングで変更される前記暗号鍵を、前記他の装置と共通に保持する前記第１の鍵情報と前記所定のタイミングで変更される前記第２の鍵情報とに基づいて生成し、
前記暗号鍵を用いて、受信した暗号化されたデータを復号する
ことを特徴とする復号方法。
【請求項１６】
暗号鍵を用いてデータを暗号化する暗号化装置において、
暗号化部と、
前記暗号化部に接続された暗号鍵生成部と、
前記暗号鍵生成部に接続された第1の鍵情報供給部と、
前記暗号鍵生成部に接続された第２の鍵情報供給部と
を備え、
前記暗号化部は、前記第1の鍵情報供給部から供給される、他の装置との通信によって前記他の装置との間で共通に保持されている第1の鍵情報と、前記第２の鍵情報供給部から供給される、所定のタイミングで変更される第２の鍵情報とに基づいて前記暗号鍵生成部によって生成された前記暗号鍵を用いて、前記データを暗号化する
ことを特徴とする暗号化装置。
【請求項１７】
前記暗号鍵で暗号化されたデータを、前記他の装置に送信する送信部
をさらに備える
ことを特徴とする請求項１６に記載の暗号化装置。
【請求項１８】
暗号鍵を用いてデータを復号する復号装置において、
受信部と、
前記受信部に接続された復号部と、
前記復号部に接続された暗号鍵生成部と、
前記暗号鍵生成部に接続された第1の鍵情報供給部と、
前記暗号鍵生成部に接続された第２の鍵情報供給部と
を備え、
前記復号部は、前記第1の鍵情報供給部から供給される、他の装置との通信によって前記他の装置との間で共通に保持されている第1の鍵情報と、前記第２の鍵情報供給部から供給される、所定のタイミングで変更される第２の鍵情報とに基づいて前記暗号鍵生成部によって生成された前記暗号鍵を用いて、前記受信部で受信された暗号化されたデータを

復号する
ことを特徴とする復号装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号化装置および方法、並びに復号装置および方法に関し、特に、より安全性を高めるようにした暗号化装置および方法、並びに復号装置および方法に関する。
【背景技術】
【０００２】
最近、ＡＶ機器、コンピュータなどに代表される複数の電子機器を、バスで相互に接続し、ネットワークを構成して、ネットワーク内で各種のデータを相互に授受することができるようになってきた。
【０００３】
その結果、例えば、ネットワークに接続されているDVDプレーヤにより、DVDから再生した映画のデータを、バスを介して、テレビジョン受像機、モニタなどの表示装置に転送し、表示することができる。通常、DVDより再生された映画を表示装置に表示して視聴することは、DVDを購入した時点において、著作権者から許容されるところである。
【０００４】
しかしながら、DVDから再生されたデータを、他の記録媒体にコピーし、利用することは、一般的には著作権者から許容されていない。そこで、バス（ネットワーク）を介して送出するデータが、不法にコピーされるのを防止するために、送出する側において、データを暗号化するようにし、受信側において、これを復号することが考えられる。
【０００５】
しかしながら、DVDプレーヤ、テレビジョン受像機などのコンシューマエレクトロニクス機器（CE機器）は、通常、所定の目的のために設計、製造されているものであり、ユーザがこれを改造したり、他の部品を組み込んだりして、装置の内部のデータを取得したり、改ざんしたりすること（機能の変更）はできないように製造されている。これに対して、例えばパーソナルコンピュータは、多くの場合、アーキテクチャや回路が公開されており、ボードなどを追加したり、各種のアプリケーションソフトウエアをインストールすることにより、様々な機能を追加、変更することができるようになされている。
【０００６】
従って、パーソナルコンピュータにおいては、その内部バス上のデータを、所定のハードウェアを付加したり、ソフトウェアプログラムを作成することで、パーソナルコンピュータ内部のバス上のデータを直接見たり、改ざんすることが、比較的容易に行うことができる。このことは、例えば、DVDプレーヤからテレビジョン受像機に暗号化して伝送したデータを、パーソナルコンピュータで受け取り、これを復号して、コピーしたりすることが、アプリケーションソフトウエアを作成することで、容易に行えることを意味する。
【０００７】
換言すれば、パーソナルコンピュータは、バスを介して、通信を行うリンク部と、送受信するデータを用意したり、受信したデータを利用するアプリケーション部とのつながりが希薄であり、物理的にも、論理的にも、そこにユーザが手を加えることができる部分が多い。これに対して、CE機器においては、両者のつながりが密接で、ユーザが介在できる部分が殆どない。
【発明の開示】
【発明が解決しようとする課題】
【０００８】
本発明はこのような状況に鑑みてなされたものであり、データの不正なコピーを、より確実に防止することができるようにするものである。
【課題を解決するための手段】
【０００９】

本発明の第１の側面の暗号化装置は、暗号鍵を用いてデータを暗号化する暗号化装置において、第１の鍵情報を供給する第１の供給手段と、セッション中に変更される第２の鍵情報を供給する第２の供給手段と、前記第２の鍵情報の変更に応じて前記セッション中に所定のタイミングで変更される前記暗号鍵を、前記第１の鍵情報と前記第２の鍵情報とに基づいて生成する生成手段と、前記暗号鍵を用いてデータを暗号化する暗号化手段とを備えることを特徴とする。

【００１０】

本発明の第１の側面の暗号化装置は、前記暗号鍵で暗号化されたデータを、他の装置に送信する送信手段をさらに備えることができる。

【００１１】

本発明の第１の側面の暗号化方法は、暗号鍵を用いてデータを暗号化する暗号化装置の暗号化方法において、第１の鍵情報を供給し、セッション中に変更される第２の鍵情報を供給し、前記第２の鍵情報の変更に応じて前記セッション中に所定のタイミングで変更される前記暗号鍵を、前記第１の鍵情報と前記第２の鍵情報とに基づいて生成し、前記暗号鍵を用いてデータを暗号化することを特徴とする。

【００１２】

本発明の第１の側面の暗号化方法は、前記暗号鍵で暗号化されたデータを、他の装置に送信することができる。

【００１３】

本発明の第２の側面の復号装置は、暗号鍵を用いてデータを復号する復号装置において、暗号化されたデータを受信する受信手段と、第１の鍵情報を供給する第１の供給手段と、セッション中に変更される第２の鍵情報を供給する第２の供給手段と、前記第２の鍵情報の変更に応じて前記セッション中に所定のタイミングで変更される前記暗号鍵を、前記第１の鍵情報と前記第２の鍵情報とに基づいて生成する生成手段と、前記暗号鍵を用いて、前記受信手段で受信された暗号化されたデータを復号する復号手段とを備えることを特徴とする。

【００１４】

本発明の第２の側面の復号方法は、暗号鍵を用いてデータを復号する復号装置の復号方法において、暗号化されたデータを受信し、第１の鍵情報を供給し、セッション中に変更される第２の鍵情報を供給し、前記第２の鍵情報の変更に応じて前記セッション中に所定のタイミングで変更される前記暗号鍵を、前記第１の鍵情報と前記第２の鍵情報とに基づいて生成し、前記暗号鍵を用いて、受信した暗号化されたデータを復号することを特徴とする。

【００１５】

本発明の第３の側面の暗号化装置は、暗号鍵を用いてデータを暗号化する暗号化装置において、暗号化部と、前記暗号化部に接続された暗号鍵生成部と、前記暗号鍵生成部に接続された第１の鍵情報供給部と、前記暗号鍵生成部に接続された第２の鍵情報供給部とを備え、前記暗号化部は、前記第１の鍵情報供給部から供給される第1の鍵情報と、前記第２の鍵情報供給部から供給される、セッション中に所定のタイミングで変更される第２の鍵情報とに基づいて前記暗号鍵生成部によって生成された前記暗号鍵を用いて、前記データを暗号化することを特徴とする。

【００１６】

本発明の第３の側面の暗号化装置は、前記暗号鍵で暗号化されたデータを、他の装置に送信する送信部をさらに備えることができる。

【００１７】

本発明の第４の側面の復号装置は、暗号鍵を用いてデータを復号する復号装置において、受信部と、前記受信部に接続された復号部と、前記復号部に接続された暗号鍵生成部と、前記暗号鍵生成部に接続された第１の鍵情報供給部と、前記暗号鍵生成部に接続された第２の鍵情報供給部とを備え、前記復号部は、前記第１の鍵情報供給部から供給される第１の鍵情報と、前記第２の鍵情報供給部から供給される、セッション中に所定のタイミン

グで変更される第２の鍵情報とに基づいて前記暗号鍵生成部によって生成された前記暗号鍵を用いて、前記受信部で受信された暗号化されたデータを復号することを特徴とする。

【００１８】

本発明の第５の側面の暗号化装置は、暗号鍵を用いてデータを暗号化する暗号化装置において、他の装置との通信によって、前記暗号化装置と前記他の装置との間で共通に保持されている第１の鍵情報を供給する第１供給手段と、所定のタイミングで変更される第２の鍵情報を供給する第２供給手段と、前記第２の鍵情報の変更に応じて前記所定のタイミングで変更される前記暗号鍵を、前記他の装置と共通に保持する前記第１の鍵情報と前記所定のタイミングで変更される前記第２の鍵情報とに基づいて生成する生成手段と、前記暗号鍵を用いてデータを暗号化する暗号化手段とを備えることを特徴とする。

【００１９】

本発明の第５の側面の暗号化装置は、前記暗号鍵で暗号化されたデータを、前記他の装置に送信する送信手段をさらに備えることができる。

【００２０】

本発明の第５の側面の暗号化方法は、暗号鍵を用いてデータを暗号化する暗号化装置の暗号化方法において、他の装置との通信によって、前記暗号化装置と前記他の装置との間で共通に保持されている第１の鍵情報を供給し、所定のタイミングで変更される第２の鍵情報を供給し、前記第２の鍵情報の変更に応じて前記所定のタイミングで変更される前記暗号鍵を、前記他の装置と共通に保持する前記第１の鍵情報と前記所定のタイミングで変更される前記第２の鍵情報とに基づいて生成し、前記暗号鍵を用いてデータを暗号化することを特徴とする。

【００２１】

本発明の第５の側面の暗号化方法は、前記暗号鍵で暗号化されたデータを、前記他の装置に送信することができる。

【００２２】

本発明の第６の側面の復号装置は、暗号鍵を用いてデータを復号する復号装置において、暗号化されたデータを受信する受信手段と、他の装置との通信によって、前記復号装置と前記他の装置との間で共通に保持されている第１の鍵情報を供給する第１の供給手段と、所定のタイミングで変更される第２の鍵情報を供給する第２の供給手段と、前記第２の鍵情報の変更に応じて前記所定のタイミングで変更される前記暗号鍵を、前記他の装置と共通に保持する前記第１の鍵情報と前記所定のタイミングで変更される前記第２の鍵情報とに基づいて生成する生成手段と、前記暗号鍵を用いて、前記受信手段で受信された暗号化されたデータを復号する復号手段とを備えることを特徴とする。

【００２３】

本発明の第６の側面の復号方法は、暗号鍵を用いてデータを復号する復号装置の復号方法において、暗号化されたデータを受信し、他の装置との通信によって、前記復号装置と前記他の装置との間で共通に保持されている第１の鍵情報を供給し、所定のタイミングで変更される第２の鍵情報を供給し、前記第２の鍵情報の変更に応じて前記所定のタイミングで変更される前記暗号鍵を、前記他の装置と共通に保持する前記第１の鍵情報と前記所定のタイミングで変更される前記第２の鍵情報とに基づいて生成し、前記暗号鍵を用いて、受信した暗号化されたデータを復号することを特徴とする。

【００２４】

本発明の第７の側面の暗号化装置は、暗号鍵を用いてデータを暗号化する暗号化装置において、暗号化部と、前記暗号化部に接続された暗号鍵生成部と、前記暗号鍵生成部に接続された第1の鍵情報供給部と、前記暗号鍵生成部に接続された第２の鍵情報供給部とを備え、前記暗号化部は、前記第1の鍵情報供給部から供給される、他の装置との通信によって前記他の装置との間で共通に保持されている第1の鍵情報と、前記第２の鍵情報供給部から供給される、所定のタイミングで変更される第２の鍵情報とに基づいて前記暗号鍵生成部によって生成された前記暗号鍵を用いて、前記データを暗号化することを特徴とする。

【００２５】
本発明の第７の側面の暗号化装置は、前記暗号鍵で暗号化されたデータを、前記他の装置に送信する送信部をさらに備えることができる。
【００２６】
本発明の第８の側面の復号装置は、暗号鍵を用いてデータを復号する復号装置において、受信部と、前記受信部に接続された復号部と、前記復号部に接続された暗号鍵生成部と、前記暗号鍵生成部に接続された第1の鍵情報供給部と、前記暗号鍵生成部に接続された第２の鍵情報供給部とを備え、前記復号部は、前記第1の鍵情報供給部から供給される、他の装置との通信によって前記他の装置との間で共通に保持されている第1の鍵情報と、前記第２の鍵情報供給部から供給される、所定のタイミングで変更される第２の鍵情報とに基づいて前記暗号鍵生成部によって生成された前記暗号鍵を用いて、前記受信部で受信された暗号化されたデータを復号することを特徴とする。
【００２７】
本発明の第１の側面においては、セッション中に変更される第２の鍵情報の変更に応じて前記セッション中に所定のタイミングで変更される暗号鍵が、第１の鍵情報と前記第２の鍵情報とに基づいて生成され、前記暗号鍵を用いてデータが暗号化される。
【００２８】
本発明の第２の側面においては、暗号化されたデータが受信され、セッション中に変更される第２の鍵情報の変更に応じて前記セッション中に所定のタイミングで変更される暗号鍵が、第１の鍵情報と前記第２の鍵情報とに基づいて生成され、前記暗号鍵を用いて、暗号化されたデータが復号される。
【００２９】
本発明の第３の側面においては、第1の鍵情報と、セッション中に所定のタイミングで変更される第２の鍵情報とに基づいて生成された暗号鍵を用いて、データが暗号化される。
【００３０】
本発明の第４の側面においては、第１の鍵情報と、セッション中に所定のタイミングで変更される第２の鍵情報とに基づいて生成された暗号鍵を用いて、暗号化されたデータが復号される。
【００３１】
本発明の第５の側面においては、所定のタイミングで変更される第２の鍵情報の変更に応じて前記所定のタイミングで変更される暗号鍵が、他の装置と共通に保持する第１の鍵情報と前記所定のタイミングで変更される前記第２の鍵情報とに基づいて生成され、前記暗号鍵を用いてデータが暗号化される。
【００３２】
本発明の第６の側面においては、所定のタイミングで変更される第２の鍵情報の変更に応じて前記所定のタイミングで変更される暗号鍵が、他の装置と共通に保持する第１の鍵情報と前記所定のタイミングで変更される前記第２の鍵情報とに基づいて生成され、前記暗号鍵を用いて、暗号化されたデータが復号される。
【００３３】
本発明の第７の側面においては、他の装置との通信によって前記他の装置との間で共通に保持されている第1の鍵情報と、所定のタイミングで変更される第２の鍵情報とに基づいて生成された前記暗号鍵を用いて、データが暗号化される。
【００３４】
本発明の第８の側面においては、他の装置との通信によって前記他の装置との間で共通に保持されている第1の鍵情報と、所定のタイミングで変更される第２の鍵情報とに基づいて生成された暗号鍵を用いて、暗号化されたデータが復号される。
【発明の効果】
【００３５】
以上の如く、本発明の第１の側面、第３の側面、第５の側面、および第７の側面によれ

ば、より安全に暗号化を行うことが可能となる。

【００３６】

また、本発明の第２の側面、第４の側面、第６の側面、および第８の側面によれば、より安全に暗号化されているデータを復号することが可能となる。

【発明を実施するための最良の形態】

【００３７】

図１は、本発明を適用した情報処理システムの構成例を表している。この構成例においては、IEEE１３９４シリアルバス１１を介してDVDプレーヤ１、パーソナルコンピュータ２、光磁気ディスク装置３、データ放送受信装置４、モニタ５、テレビジョン受像機６が相互に接続されている。

【００３８】

図２は、この内のDVDプレーヤ１、パーソナルコンピュータ２、および光磁気ディスク装置３の内部のより詳細な構成例を表している。DVDプレーヤ１は、１３９４インタフェース２６を介して、１３９４バス１１に接続されている。CPU２１は、ROM２２に記憶されているプログラムに従って各種の処理を実行し、RAM２３は、CPU２１が各種の処理を実行する上において必要なデータやプログラムなどを適宜記憶する。操作部２４は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより操作されたとき、その操作に対応する信号を出力する。ドライブ２５は、図示せぬDVD（ディスク）を駆動し、そこに記録されているデータを再生するようになされている。EEPROM２７は、装置の電源オフ後も記憶する必要のある情報（この実施の形態の場合、鍵情報）を記憶するようになされている。内部バス２８は、これらの各部を相互に接続している。

【００３９】

光磁気ディスク装置３は、CPU３１乃至内部バス３８を有している。これらは、上述したDVDプレーヤ１におけるCPU２１乃至内部バス２８と同様の機能を有するものであり、その説明は省略する。ただし、ドライブ３５は、図示せぬ光磁気ディスクを駆動し、そこにデータを記録または再生するようになされている。

【００４０】

パーソナルコンピュータ２は、１３９４インタフェース４９を介して１３９４バス１１に接続されている。CPU４１は、ROM４２に記憶されているプログラムに従って各種の処理を実行する。RAM４３には、CPU４１が各種の処理を実行する上において必要なデータやプログラムなどが適宜記憶される。入出力インタフェース４４には、キーボード４５とマウス４６が接続されており、それらから入力された信号をCPU４１に出力するようになされている。また、入出力インタフェース４４には、ハードディスク（HDD）４７が接続されており、そこにデータ、プログラムなどを記録再生することができるようになされている。入出力インタフェース４４にはまた、拡張ボード４８を適宜装着し、必要な機能を付加することができるようになされている。EEPROM５０には、電源オフ後も保持する必要のある情報（この実施の形態の場合、各種の鍵情報）が記憶されるようになされている。例えば、PCI(Peripheral Component Interconnect)、ローカルバスなどにより構成される内部バス５１は、これらの各部を相互に接続するようになされている。

【００４１】

なお、この内部バス５１は、ユーザに対して解放されており、ユーザは、拡張ボード４８に所定のボードを適宜接続したり、所定のソフトウェアプログラムを作成して、CPU４１にインストールすることで、内部バス５１により伝送されるデータを適宜受信することができるようになされている。

【００４２】

これに対して、DVDプレーヤ１や光磁気ディスク装置３などのコンシューマエレクトロニクス（CE）装置においては、内部バス２８や内部バス３８は、ユーザに解放されておらず、特殊な改造などを行わない限り、そこに伝送されるデータを取得することができないようになされている。

【００４３】

次に、所定のソースとシンクとの間で行われる認証の処理について説明する。この認証の処理は、図３に示すように、ソースとしての、例えばDVDプレーヤ１のROM２２に予め記憶されているソフトウェアプログラムの１つとしてのファームウェア２０と、シンクとしての、例えばパーソナルコンピュータ２のROM４２に記憶されており、CPU４１が処理するソフトウェアプログラムの１つとしてのライセンスマネージャ６２との間において行われる。

【００４４】

図４は、ソース（DVDプレーヤ１）と、シンク（パーソナルコンピュータ２）との間において行われる認証の手順を示している。DVDプレーヤ１のEEPROM２７には、サービスキー（service_key）と関数（hash）が予め記憶されている。これらはいずれも著作権者から、このDVDプレーヤ１のユーザに与えられたものであり、各ユーザは、EEPROM２７に、これを秘密裡に保管しておくものである。

【００４５】

サービスキーは、著作権者が提供する情報毎に与えられるものであり、この１３９４バス１１で構成されるシステムにおいて、共通のものである。なお、本明細書において、システムとは、複数の装置で構成される全体的な装置を示すものとする。

【００４６】

hash関数は、任意長の入力に対して、６４ビットまたは１２８ビットなどの固定長のデータを出力する関数であり、ｙ（＝hash（ｘ））を与えられたとき、ｘを求めることが困難であり、かつ、hash（ｘ１）＝hash（ｘ２）となるｘ１と、ｘ２の組を求めることも困難となる関数である。１方向hash関数の代表的なものとして、MD５やSHAなどが知られている。この１方向hash関数については、Bruce Schneier著の「Applied Cryptography(Second Edition),Wiley」に詳しく解説されている。

【００４７】

一方、シンクとしての例えばパーソナルコンピュータ２は、著作権者から与えられた、自分自身に固有の識別番号（ID）とライセンスキー（license_key）をEEPROM５０に秘密裡に保持している。このライセンスキーは、ｎビットのIDとｍビットのサービスキーを連結して得たｎ＋ｍビットのデータ（ID ｜｜ service_key）に対して、hash関数を適用して得られる値である。すなわち、ライセンスキーは次式で表される。

license_key=hash(ID ｜｜ service_key)

【００４８】

IDとしては、例えば１３９４バス１１の規格に定められているnode_unique_IDを用いることができる。このnode_unique_IDは、図５に示すように、８バイト（６４ビット）で構成され、最初の３バイトは、IEEEで管理され、電子機器の各メーカーにIEEEから付与される。また、下位５バイトは、各メーカーが、自分自身がユーザに提供する各装置に対して付与することができるものである。各メーカーは、例えば下位５バイトに対してシリアルに、１台に１個の番号を割り当てるようにし、５バイト分を全部使用した場合には、上位３バイトがさらに別の番号となっているnode_unique_IDの付与を受け、そして、その下位５バイトについて１台に１個の番号を割り当てるようにする。従って、このnode_unique_IDは、メーカーに拘らず、１台毎に異なるものとなり、各装置に固有のものとなる。

【００４９】

ステップＳ１において、DVDプレーヤ１のファームウェア２０は、１３９４インタフェース２６を制御し、１３９４バス１１を介してパーソナルコンピュータ２に対してIDを要求する。パーソナルコンピュータ２のライセンスマネージャ６２は、ステップＳ２において、このIDの要求を受信する。すなわち、１３９４インタフェース４９は、１３９４バス１１を介してDVDプレーヤ１から伝送されてきたID要求の信号を受信すると、これをCPU４１に出力する。CPU４１のライセンスマネージャ６２は、このID要求を受けたとき、ステップＳ３においてEEPROM５０に記憶されているIDを読み出し、これを１３９４インタフェース４９を介して１３９４バス１１からDVDプレーヤ１に伝送する。

【００５０】

DVDプレーヤ１においては、ステップＳ４で１３９４インタフェース２６が、このIDを受け取ると、このIDがCPU２１で動作しているファームウェア２０に供給される。

【００５１】

ファームウェア２０は、ステップＳ５において、パーソナルコンピュータ２から伝送を受けたIDと、EEPROM２７に記憶されているサービスキーを結合して、データ（ID ｜｜ service_key）を生成し、このデータに対して、次式に示すようにhash関数を適用して、キーlkを生成する。

lk＝hash（ID ｜｜ service_key）

【００５２】

次に、ステップＳ６において、ファームウェア２０は、暗号鍵skを生成する。この暗号鍵skの詳細については後述するが、この暗号鍵skは、セッションキーとしてDVDプレーヤ１とパーソナルコンピュータ２のそれぞれにおいて利用される。

【００５３】

次に、ステップＳ７において、ファームウェア２０は、ステップＳ５で生成した鍵lkを鍵として、ステップＳ６で生成した暗号鍵skを暗号化して、暗号化データ（暗号化鍵）ｅを得る。すなわち、次式を演算する。　ｅ＝Enc（lk,　sk）

【００５４】

なお、Enc（Ａ，Ｂ）は、共通鍵暗号方式で、鍵Ａを用いて、データＢを暗号化することを意味する。

【００５５】

次に、ステップＳ８で、ファームウェア２０は、ステップＳ７で生成した暗号化データｅをパーソナルコンピュータ２に伝送する。すなわち、この暗号化データｅは、DVDプレーヤ１の１３９４インタフェース２６から１３９４バス１１を介してパーソナルコンピュータ２に伝送される。パーソナルコンピュータ２においては、ステップＳ９で、この暗号化データｅを１３９４インタフェース４９を介して受信する。ライセンスマネージャ６２は、このようにして受信した暗号化データｅをEEPROM５０に記憶されているライセンスキーを鍵として、次式に示すように復号し、復号鍵sk'を生成する。　sk'＝Dec（license_key，ｅ）

【００５６】

なお、ここで、Dec（Ａ，Ｂ）は、共通鍵暗号方式で鍵Ａを用いて、データＢを復号することを意味する。

【００５７】

なお、この共通鍵暗号方式における暗号化のアルゴリズムとしては、ＤＥＳが知られている。共通鍵暗号化方式についても、上述した、Applied Cryptography(Second Edition)に詳しく解説されている。

【００５８】

DVDプレーヤ１において、ステップＳ５で生成するキーlkは、パーソナルコンピュータ２のEEPROM５０に記憶されている（license_key）と同一の値となる。すなわち、次式が成立する。　lk＝license_key

【００５９】

従って、パーソナルコンピュータ２において、ステップＳ１０で復号して得たキーsk'は、DVDプレーヤ１において、ステップＳ６で生成した暗号鍵skと同一の値となる。すなわち、次式が成立する。　sk'＝sk

【００６０】

このように、DVDプレーヤ１（ソース）とパーソナルコンピュータ２（シンク）の両方において、同一の鍵sk，sk'を共有することができる。そこで、この鍵skをそのまま暗号鍵として用いるか、あるいは、これを基にして、それぞれが疑似乱数を作り出し、それを暗号鍵として用いることができる。

【００６１】

ライセンスキーは、上述したように、各装置に固有のIDと、提供する情報に対応するサ

ービスキーに基づいて生成されているので、他の装置がskまたはsk'を生成することはできない。また、著作権者から認められていない装置は、ライセンスキーを有していないので、skあるいはsk'を生成することができない。従って、その後DVDプレーヤ１が暗号鍵skを用いて再生データを暗号化してパーソナルコンピュータ２に伝送した場合、パーソナルコンピュータ２が適正にライセンスキーを得たものである場合には、暗号鍵sk'を有しているので、DVDプレーヤ１より伝送されてきた、暗号化されている再生データを復号することができる。しかしながら、パーソナルコンピュータ２が適正なものでない場合、暗号鍵sk'を有していないので、伝送されてきた暗号化されている再生データを復号することができない。換言すれば、適正な装置だけが共通の暗号鍵sk，sk'を生成することができるので、結果的に、認証が行われることになる。

【００６２】

仮に１台のパーソナルコンピュータ２のライセンスキーが盗まれたとしても、IDが１台１台異なるので、そのライセンスキーを用いて、他の装置がDVDプレーヤ１から伝送されてきた暗号化されているデータを復号することはできない。従って、安全性が向上する。

【００６３】

図６は、ソース（DVDプレーヤ１）に対して、パーソナルコンピュータ２だけでなく、光磁気ディスク装置３もシンクとして機能する場合の処理例を表している。

【００６４】

この場合、シンク１としてのパーソナルコンピュータ２のEEPROM５０には、IDとしてID１が、また、ライセンスキーとしてlicense_key１が記憶されており、シンク２としての光磁気ディスク装置３においては、EEPROM３７に、IDとしてID２が、また、ライセンスキーとしてlicense_key２が記憶されている。

【００６５】

DVDプレーヤ１（ソース）とパーソナルコンピュータ２（シンク１）の間において行われるステップＳ１１乃至ステップＳ２０の処理は、図４におけるステップＳ１乃至ステップＳ１０の処理と実質的に同様の処理であるので、その説明は省略する。

【００６６】

すなわち、上述したようにして、DVDプレーヤ１は、パーソナルコンピュータ２に対して認証処理を行う。そして次に、ステップＳ２１において、DVDプレーヤ１は、光磁気ディスク装置３に対して、IDを要求する。光磁気ディスク装置３においては、ステップＳ２２で１３９４インタフェース３６を介して、このID要求信号が受信されると、そのファームウェア３０（図１０）は、ステップＳ２３でEEPROM３７に記憶されているID（ID２）を読み出し、これを１３９４インタフェース３６から、１３９４バス１１を介してDVDプレーヤ１に伝送する。DVDプレーヤ１のファームウェア２０は、ステップＳ２４で、１３９４インタフェース２６を介して、このID２を受け取ると、ステップＳ２５で、次式から鍵lk２を生成する。

lk２＝hash（ID２ ｜｜ service_key）

【００６７】

さらに、ファームウェア２０は、ステップＳ２６で次式を演算し、ステップＳ１６で生成した鍵skを、ステップＳ２５で生成した鍵lk２を用いて暗号化し、暗号化したデータｅ２を生成する。

【００６８】

そして、ステップＳ２７で、ファームウェア２０は、この暗号化データｅ２を１３９４インタフェース２６から１３９４バス１１を介して光磁気ディスク装置３に伝送する。

【００６９】

光磁気ディスク装置３においては、ステップＳ２８で１３９４インタフェース３６を介して、この暗号化データｅ２を受信し、ステップＳ２９で次式を演算して、暗号鍵sk２’を生成する。

sk２’＝Dec（license_key２，ｅ２）

【００７０】

以上のようにして、パーソナルコンピュータ２と光磁気ディスク装置３のそれぞれにおいて、暗号鍵sk１’，sk２’が得られたことになる。これらの値は、DVDプレーヤ１における暗号鍵skと同一の値となっている。

【００７１】

図６の処理例においては、DVDプレーヤ１が、パーソナルコンピュータ２と、光磁気ディスク装置３に対して、それぞれ個別にIDを要求し、処理するようにしているのであるが、同報通信によりIDを要求することができる場合は、図７に示すような処理を行うことができる。

【００７２】

すなわち、図７の処理例においては、ステップＳ４１で、ソースとしてのDVDプレーヤ１が、全てのシンク（この例の場合、パーソナルコンピュータ２と光磁気ディスク装置３）に対して同報通信でIDを要求する。パーソナルコンピュータ２と光磁気ディスク装置３は、それぞれステップＳ４２とステップＳ４３で、このID転送要求の信号を受け取ると、それぞれステップＳ４４またはステップＳ４５で、EEPROM５０またはEEPROM３７に記憶されているID１またはID２を読み出し、これをDVDプレーヤ１に転送する。DVDプレーヤ１は、ステップＳ４６とステップＳ４７で、これらのIDをそれぞれ受信する。

【００７３】

DVDプレーヤ１においては、さらにステップＳ４８で、次式から暗号鍵lk１を生成する。

lk１＝hash（ID１ ｜｜ service_key）

【００７４】

さらに、ステップＳ４９において、次式から暗号鍵lk２が生成される。

lk２＝hash（ID２ ｜｜ service_key）

【００７５】

DVDプレーヤ１においては、さらにステップＳ５０で、暗号鍵skが生成され、ステップＳ５１で、次式で示すように、暗号鍵skが、鍵lk１を鍵として暗号化される。

ｅ１＝Enc（lk１，sk）

【００７６】

さらに、ステップＳ５２においては、暗号鍵skが、鍵lk２を鍵として、次式に従って暗号化される。

ｅ２＝Enc（lk２，sk）

【００７７】

さらに、ステップＳ５３においては、ID１，ｅ１，ID２，ｅ２が、それぞれ次式で示すように結合されて、暗号化データｅが生成される。

ｅ＝ID１ ｜｜ ｅ１ ｜｜ ID２ ｜｜ ｅ２

【００７８】

DVDプレーヤ１においては、さらにステップＳ５４で、以上のようにして生成された暗号化データｅが同報通信で、パーソナルコンピュータ２と光磁気ディスク装置３に伝送される。

【００７９】

パーソナルコンピュータ２と光磁気ディスク装置３においては、それぞれステップＳ５５またはステップＳ５６で、これらの暗号化データｅが受信される。そして、パーソナルコンピュータ２と光磁気ディスク装置３においては、それぞれステップＳ５７またはステップＳ５８において、次式で示す演算が行われ、暗号鍵sk１’，sk２’が生成される。

sk１’＝Dec（license_key１，ｅ１）　sk２’＝Dec（license_key２，ｅ２）

【００８０】

図８は、１つのシンクが複数のサービスを受けること（複数の種類の情報の復号）ができるようになされている場合の処理例を表している。すなわち、この場合においては、例えば、シンクとしてのパーソナルコンピュータ２は、複数のライセンスキー（license_key１，license_key２，license_key３など）をEEPROM５０に記憶している。ソースとして

のDVDプレーヤ１は、そのEEPROM２７に複数のサービスキー（service_key１，service_key２，service_key３など）を記憶している。この場合、DVDプレーヤ１は、ステップＳ８１でシンクとしてのパーソナルコンピュータ２に対してIDを要求するとき、DVDプレーヤ１が、これから転送しようとする情報（サービス）を識別するservice_IDを転送する。パーソナルコンピュータ２においては、ステップＳ８２で、これを受信したとき、EEPROM５０に記憶されている複数のライセンスキーの中から、このservice_IDに対応するものを選択し、これを用いて、ステップＳ９０で復号処理を行う。その他の動作は、図４における場合と同様である。

【００８１】

図９は、さらに他の処理例を表している。この例においては、ソースとしてのDVDプレーヤ１が、そのEEPROM２７に、service_key、hash関数、および疑似乱数発生関数pRNGを記憶している。これらは、著作権者から与えられたものであり、秘密裡に保管される。また、シンクとしてのパーソナルコンピュータ２のEEPROM５０には、著作権者から与えられたID、LK，LK'、関数Ｇ、および疑似乱数数発生関数pRNGを有している。

【００８２】

LKは、著作権者が作成したユニークな乱数であり、LK'は、次式を満足するように生成されている。

LK'＝Ｇ＾－１（Ｒ）　Ｒ＝pRNG（Ｈ）（＋）pRNG（LK）　Ｈ＝hash（ID ｜｜ service_key)

【００８３】

なお、Ｇ＾－１は、Ｇの逆関数を意味する。Ｇ＾－１は、所定の規則を知っていれば、簡単に計算することができるが、知らない場合には、計算することが難しいような特徴を有している。このような関数としては、公開鍵暗号に用いられている関数を利用することができる。

【００８４】

また、疑似乱数発生関数は、ハードウェアとして設けるようにすることも可能である。

【００８５】

DVDプレーヤ１のファームウェア２０は、最初にステップＳ１０１において、パーソナルコンピュータ２のライセンスマネージャ６２に対してIDを要求する。パーソナルコンピュータ２のライセンスマネージャ６２は、ステップＳ１０２でID要求信号を受け取ると、EEPROM５０に記憶されているIDを読み出し、ステップＳ１０３で、これをDVDプレーヤ１に伝送する。DVDプレーヤ１のファームウェア２０は、ステップＳ１０４でこのIDを受け取ると、ステップＳ１０５で次式を演算する。

Ｈ＝hash（ID ｜｜ service_key)

【００８６】

さらに、ファームウェア２０は、ステップＳ１０６で鍵skを生成し、ステップＳ１０７で次式を演算する。

ｅ＝sk（＋）pRNG（Ｈ）

【００８７】

なお、Ａ（＋）Ｂは、ＡとＢの排他的論理和の演算を意味する。

【００８８】

すなわち、疑似ランダム発生キーpRNGにステップＳ１０５で求めたＨを入力することで得られた結果、pRNG（Ｈ）と、ステップＳ１０６で生成した鍵skのビット毎の排他的論理和を演算することで、鍵SKを暗号化する。

【００８９】

次に、ステップＳ１０８で、ファームウェア２０は、ｅをパーソナルコンピュータ２に伝送する。

【００９０】

パーソナルコンピュータ２においては、ステップＳ１０９でこれを受信し、ステップＳ１１０で、次式を演算する。

sk'＝ｅ （＋） Ｇ（LK'） （＋） pRNG（LK）

【００９１】

すなわち、DVDプレーヤ１から伝送されてきたｅ、EEPROM５０に記憶されている関数Ｇに、やはりEEPROM５０に記憶されているLK'を適用して得られる値Ｇ（LK'）、並びに、EEPROM５０に記憶されているLK'を、やはりEEPROM５０に記憶されている疑似乱数発生関数pRNGに適用して得られる結果pRNG（LK）の排他的論理和を演算し、鍵sk'を得る。

【００９２】

ここで、次式に示すように、sk＝sk'となる。

sk'＝ｅ （＋） Ｇ（LK'） （＋） pRNG（LK）

＝sk （＋） pRNG（Ｈ） （＋） Ｒ （＋） pRNG（LK）

＝sk （＋） pRNG（Ｈ） （＋） pRNG（Ｈ） （＋） pRNG（LK） （＋） pRNG（LK）

＝sk

【００９３】

このようにして、ソースとしてのDVDプレーヤ１とシンクとしてのパーソナルコンピュータ２は、同一の鍵sk, sk'を共有することができる。LK, LK'を作ることができるのは、著作権者だけであるので、ソースが不正に、LK, LK'を作ろうとしても作ることができないので、より安全性を高めることができる。

【００９４】

以上においては、ソースとシンクにおいて認証を行うようにしたが、例えばパーソナルコンピュータ２には、通常、任意のアプリケーションプログラムをロードして用いることができる。そして、このアプリケーションプログラムとしては、不正に作成したものが使用される場合もある。従って、各アプリケーションプログラム毎に、著作権者から許可を得たものであるか否かを判定する必要がある。そこで、図３に示すように、各アプリケーション部６１とライセンスマネージャ６２との間においても、上述したように、認証処理を行うようにすることができる。この場合、ライセンスマネージャ６２がソースとなり、アプリケーション部６１がシンクとなる。

【００９５】

次に、以上のようにして、認証が行われた後（暗号鍵の共有が行われた後）、暗号鍵を用いて、ソースから暗号化したデータをシンクに転送し、シンクにおいて、この暗号化したデータを復号する場合の動作について説明する。

【００９６】

図１０に示すように、DVDプレーヤ１、あるいは光磁気ディスク装置３のように、内部の機能が一般ユーザに解放されていない装置においては、１３９４バス１１を介して授受されるデータの暗号化と復号の処理は、それぞれ１３９４インタフェース２６または１３９４インタフェース３６で行われる。この暗号化と復号化には、セッションキーＳと時変キーｉが用いられるが、このセッションキーＳと時変キーｉ（正確には、時変キーｉを生成するためのキーｉ’）は、それぞれファームウェア２０またはファームウェア３０から、１３９４インタフェース２６または１３９４インタフェース３６に供給される。セッションキーＳは、初期値として用いられる初期値キーSsと時変キーｉを攪乱するために用いられる攪乱キーSiとにより構成されている。この初期値キーSsと攪乱キーSiは、上述した認証において生成された暗号鍵sk（＝sk'）の所定のビット数の上位ビットと下位ビットにより、それぞれ構成するようにすることができる。このセッションキーＳは、セッション毎に（例えば、１つの映画情報毎に、あるいは、１回の再生毎に）、適宜、更新される。これに対して、攪乱キーSiとキーｉ’から生成される時変キーｉは、１つのセッション内において、頻繁に更新されるキーであり、例えば、所定のタイミングにおける時刻情報などを用いることができる。

【００９７】

いま、ソースとしてのDVDプレーヤ１から再生出力した映像データを１３９４バス１１を介して光磁気ディスク装置３とパーソナルコンピュータ２に伝送し、それぞれにおいて

復号するものとする。この場合、DVDプレーヤ１においては、１３９４インタフェース２６において、セッションキーＳと時変キーｉを用いて暗号化処理が行われる。光磁気ディスク装置３においては、１３９４インタフェース３６において、セッションキーＳと時変キーｉを用いて復号処理が行われる。

【００９８】

これに対して、パーソナルコンピュータ２においては、ライセンスマネージャ６２が、セッションキーＳのうち、初期値キーSsをアプリケーション部６１に供給し、攪乱キーSiと時変キーｉ（正確には、時変キーｉを生成するためのキーｉ’）を１３９４インタフェース４９（リンク部分）に供給する。そして、１３９４インタフェース４９において、攪乱キーSiとキーｉ’から時変キーｉが生成され、時変キーｉを用いて復号が行われ、その復号されたデータをアプリケーション部６１において、さらにセッションキーＳ（正確には、初期値キーSs）を用いて復号が行われる。

【００９９】

このように、パーソナルコンピュータ２においては、内部バス５１が、ユーザに解放されているので、１３９４インタフェース４９により第１段階の復号だけを行い、まだ暗号の状態としておく。そして、アプリケーション部６１において、さらに第２段階の復号を行い、平文にする。これにより、パーソナルコンピュータ２に対して、適宜、機能を付加して、内部バス５１において授受されるデータ（平文）をハードディスク４７や他の装置にコピーすることを禁止させる。

【０１００】

このように、この発明の実施の形態においては、内部バスが解放されていないCE装置においては、暗号化、または復号処理は、セッションキーＳと時変キーｉを用いて１度に行われるが、内部バスが解放されている装置（パーソナルコンピュータ２など）においては、復号処理が、時変キーｉを用いた復号処理と、セッションキーＳを用いた復号処理に分けて行われる。このように、１段階の復号処理と、２段階に分けた復号処理の両方ができるようにするには、次式を成立させることが必要となる。

Dec（Ｓ，Dec（ｉ， Enc（algo（Ｓ＋ｉ），Data））＝Data

【０１０１】

なお、上記式において、algo（Ｓ＋ｉ）は、所定のアルゴリズムにセッションキーＳと時変キーｉを入力して得られた結果を表している。

【０１０２】

図１１は、上記式を満足する１３９４インタフェース２６の構成例を表している。この構成例においては、アディティブジェネレータ７１により生成したｍビットのデータが、シュリンクジェネレータ７３に供給されている。また、LFSR(Linear Feedback Sift Register)７２が１ビットのデータを出力し、シュリンクジェネレータ７３に供給している。シュリンクジェネレータ７３は、LFSR７２の出力に対応して、アディティブジェネレータ７１の出力を選択し、選択したデータを暗号鍵として加算器７４に出力している。加算器７４は、入力された平文（１３９４バス１１に伝送するｍビットのデータ）と、シュリンクジェネレータ７３より供給されるｍビットのデータ（暗号鍵）とを加算し、加算した結果を暗号文（暗号化されたデータ）として、１３９４バス１１に出力するようになされている。

【０１０３】

加算器７４の加算処理は、mod ２＾ｍ（＾はべき乗を意味する）で、シュリンクジェネレータ７３の出力と平文を加算することを意味する。換言すれば、ｍビットのデータ同志が加算され、キャリオーバを無視した加算値が出力される。

【０１０４】

図１２は、図１１に示した１３９４インタフェース２６のさらにより詳細な構成例を表している。ファームウェア２０から出力されたセッションキーＳのうち、初期値キーSsは、加算器８１を介してレジスタ８２に転送され、保持される。この初期値キーSsは、例えば、５５ワード（１ワードは８ビット乃至３２ビットの幅を有する）により構成される。

また、ファームウェア２０から供給されたセッションキーＳのうちの、例えばLSB側の３２ビットで構成される攪乱キーSiは、レジスタ８５に保持される。

【０１０５】

レジスタ８４には、キーｉ’が保持される。このキーｉ’は、例えば１３９４バス１１を介して１個のパケットが伝送される毎に、２ビットのキーｉ’がレジスタ８４に供給され、１６パケット分の（３２ビット分の）キーｉ’がレジスタ８４に保持されたとき、加算器８６により、レジスタ８５に保持されている３２ビットの攪乱キーSiと加算され、最終的な時変キーｉとして加算器８１に供給される。加算器８１は、そのときレジスタ８２に保持されている値と加算器８６より供給された時変キーｉを加算し、その加算結果をレジスタ８２に供給し、保持させる。

【０１０６】

レジスタ８２のワードのビット数が、例えば８ビットである場合、加算器８６より出力される時変キーｉが３２ビットであるので、時変キーｉを４分割して、各８ビットをレジスタ８２の所定のアドレス（０乃至５４）のワードに加算するようにする。

【０１０７】

このようにして、レジスタ８２には、最初に初期値キーSsが保持されるが、その後、この値は、１６パケット分の暗号文を伝送する毎に、時変キーｉで更新される。

【０１０８】

加算器８３は、レジスタ８２に保持されている５５ワードのうちの所定の２ワード（図１２に示されているタイミングの場合、アドレス２３とアドレス５４のワード）を選択し、その選択した２ワードを加算して、シュリンクジェネレータ７３に出力する。また、この加算器７３の出力は、図１２に示すタイミングでは、レジスタ８２のアドレス０に転送され、前の保持値に代えて保持される。

【０１０９】

そして、次のタイミングにおいては、加算器８３に供給されるレジスタ８２の２ワードのアドレスは、アドレス５４とアドレス２３から、それぞれアドレス５３とアドレス２２に、１ワード分だけ、図中上方に移動され、加算器８３の出力で更新されるアドレスも、図中、より上方のアドレスに移動される。ただし、アドレス０より上方のアドレスは存在しないので、この場合には、アドレス５４に移動する。

【０１１０】

なお、加算器８１，８３，８６では、排他的論理和を演算させるようにすることも可能である。

【０１１１】

LFSR７２は、例えば、図１３に示すように、ｎビットのシフトレジスタ１０１と、シフトレジスタ１０１のｎビットのうちの所定のビット（レジスタ）の値を加算する加算器１０２により構成されている。シフトレジスタ１０１は、加算器１０２より供給されるビットを、図中最も左側のレジスタb_nに保持すると、それまでそこに保持されていたデータを右側のレジスタb_{n-1}にシフトする。レジスタb_{n-1}，b_{n-2}，・・・も、同様の処理を行う。そして、さらに次のタイミングでは、各ビットの値を加算器１０２で加算した値を再び、図中最も左側のビットb_nに保持させる。以上の動作が順次繰り返されて、図中最も右側のレジスタb_1から出力が１ビットずつ順次出力される。

【０１１２】

図１３は、一般的な構成例であるが、例えば、より具体的には、LFSR７２を図１４に示すように構成することができる。この構成例においては、シフトレジスタ１０１が３１ビットにより構成され、その図中右端のレジスタb_1の値と左端のレジスタb_{31}の値が、加算器１０２で加算され、加算された結果がレジスタb_{31}に帰還されるようになされている。

【０１１３】

LFSR７２より出力された１ビットのデータが論理１であるとき、条件判定部９１は、アディティブジェネレータ７１の加算器８３より供給されたｍビットのデータをそのままF

ＦＩＦＯ９２に転送し、保持させる。これに対して、LFSR７２より供給された１ビットのデータが論理０であるとき、条件判定部９１は、加算器８３より供給されたｍビットのデータを受け付けず、暗号化処理を中断させる。このようにして、シュリンクジェネレータ７３のＦＩＦＯ９２には、アディティブジェネレータ７１で生成したｍビットのデータのうち、LFSR７２が論理１を出力したタイミングのもののみが選択され、保持される。

【０１１４】

ＦＩＦＯ９２により保持したｍビットのデータが、暗号鍵として、加算器７４に供給され、伝送されるべき平文のデータ（DVDからの再生データ）に加算されて、暗号文が生成される。

【０１１５】

暗号化されたデータは、DVDプレーヤ１から１３９４バス１１を介して光磁気ディスク装置３とパーソナルコンピュータ２に供給される。

【０１１６】

光磁気ディスク装置３は、１３９４インタフェース３６において、１３９４バス１１から受信したデータを復号するために、図１５に示すような構成を有している。この構成例においては、シュリンクジェネレータ１７３にアディティブジェネレータ１７１の出力するｍビットのデータと、LFSR１７２が出力する１ビットのデータが供給されている。そして、シュリンクジェネレータ１７３の出力するｍビットの鍵が、減算器１７４に供給されている。減算器１７４は、暗号文からシュリンクジェネレータ１７３より供給される鍵を減算して、平文を復号する。

【０１１７】

すなわち、図１５に示す構成は、図１１に示す構成と基本的に同様の構成とされており、図１１における加算器７４が、減算器１７４に変更されている点だけが異なっている。

【０１１８】

図１６は、図１５に示す構成のより詳細な構成例を表している。この構成も、基本的に図１２に示した構成と同様の構成とされているが、図１２における加算器７４が、減算器１７４に変更されている。その他のアディティブジェネレータ１７１、LFSR１７２、シュリンクジェネレータ１７３、加算器１８１、レジスタ１８２、加算器１８３、レジスタ１８４，１８５、加算器１８６、条件判定部１９１、ＦＩＦＯ１９２は、図１２におけるアディティブジェネレータ７１、LFSR７２、シュリンクジェネレータ７３、加算器８１、レジスタ８２、加算器８３、レジスタ８４，８５、加算器８６、条件判定部９１、およびＦＩＦＯ９２に対応している。

【０１１９】

従って、その動作は、基本的に図１２に示した場合と同様であるので、その説明は省略するが、図１６の例においては、シュリンクジェネレータ１７３のＦＩＦＯ１９２より出力されたｍビットの鍵が、減算器１７４において、暗号文から減算されて平文が復号される。

【０１２０】

以上のように、１３９４インタフェース３６においては、セッションキーＳ（初期値キーSsと攪乱キーSi）と時変キーｉを用いて、暗号化データが１度に復号される。

【０１２１】

これに対して、上述したように、パーソナルコンピュータ２においては、１３９４インタフェース４９とアプリケーション部６１において、それぞれ個別に、２段階に分けて復号が行われる。

【０１２２】

図１７は、１３９４インタフェース４９において、ハード的に復号を行う場合の構成例を表しており、その基本的構成は、図１５に示した場合と同様である。すなわち、この場合においても、アディティブジェネレータ２７１、LFSR２７２、シュリンクジェネレータ２７３、および減算器２７４により１３９４インタフェース４９が構成されており、これらは、図１５におけるアディティブジェネレータ１７１、LFSR１７２、シュリンクジェネ

レータ１７３、および減算器１７４と基本的に同様の構成とされている。ただし、図１７の構成例においては、アディティブジェネレータ２７１に対して、ライセンスマネージャ６２から、時変キーｉを生成するためのキーｉ’と、セッションキーＳのうち、時変キーｉを攪乱するための攪乱キーSiとしては、図１５における場合と同様のキーが供給されるが、初期値キーSsとしては、全てのビットが０である単位元が供給される。

【０１２３】

すなわち、図１８に示すように、初期値キーSsの全てのビットが０とされるので、実質的に、初期値キーSsが存在しない場合と同様に、時変キーｉだけに基づいて暗号鍵が生成される。その結果、減算器２７４においては、暗号文の時変キーｉに基づく復号だけが行われる。まだ初期値キーSsに基づく復号が行われていないので、この復号の結果得られるデータは、完全な平文とはなっておらず、暗号文の状態になっている。従って、このデータを内部バス５１から取り込み、ハードディスク４７や、その他の記録媒体に記録したとしても、それをそのまま利用することができない。

【０１２４】

そして、以上のようにして、１３９４インタフェース４９において、ハード的に時変キーｉに基づいて復号されたデータをソフト的に復号するアプリケーション部６１の構成は、図１９に示すように、アディティブジェネレータ３７１、LFSR３７２、シュリンクジェネレータ３７３および減算器３７４により構成される。その基本的構成は、図１５に示したアディティブジェネレータ１７１、LFSR１７２、シュリンクジェネレータ１７３、および減算器１７４と同様の構成となっている。

【０１２５】

ただし、セッションキーＳのうち、初期値キーSsは、図１５における場合と同様に、通常の初期値キーが供給されるが、時変キーｉを生成するための攪乱キーSiとキーｉ’は、それぞれ全てのビットが０である単位元のデータとされる。

【０１２６】

その結果、図２０にその詳細を示すように（そのアディティブジェネレータ３７１乃至FIFO３９２は、図１６におけるアディティブジェネレータ１７１乃至FIFO１９２に対応している）、レジスタ３８４に保持されるキーｉ’とレジスタ３８５に保持される攪乱キーSiは、全てのビットが０であるため、加算器３８６の出力する時変キーｉも全てのビットが０となり、実質的に時変キーｉが存在しない場合と同様の動作が行われる。すなわち、初期値キーSsだけに基づく暗号鍵が生成される。そして、減算器３７４においては、このようにして生成された暗号鍵に基づいて暗号文が平文に復号される。上述したように、この暗号文は、１３９４インタフェース４９において、時変キーｉに基づいて第１段階の復号が行われているものであるので、ここで、初期値キーSsに基づいて第２段階の復号を行うことで、完全な平文を得ることができる。

【０１２７】

光磁気ディスク装置３においては、以上のようにして暗号文が復号されると、CPU３１が、復号されたデータをドライブ３５に供給し、光磁気ディスクに記録させる。

【０１２８】

一方、パーソナルコンピュータ２においては、CPU４１（アプリケーション部６１）が、以上のようにして復号されたデータを、例えばハードディスク４７に供給し、記録させる。パーソナルコンピュータ２においては、拡張ボード４８として所定のボードを接続して、内部バス５１で授受されるデータをモニタすることができるが、内部バス５１に伝送されるデータを最終的に復号することができるのは、アプリケーション部６１であるので、拡張ボード４８は、１３９４インタフェース４９で、時変キーｉに基づく復号が行われたデータ（まだ、セッションキーＳに基づく復号が行われていないデータ）をモニタすることができたとしても、完全に平文に戻されたデータをモニタすることはできない。そこで、不正なコピーが防止される。

【０１２９】

なお、セッションキーの共有は、例えば、Diffie-Hellman法などを用いて行うようにす

ることも可能である。

【０１３０】

なお、この他、例えばパーソナルコンピュータ２における１３９４インタフェース４９またはアプリケーション部６１の処理能力が比較的低く、復号処理を行うことができない場合には、セッションキーと時変キーのいずれか、あるいは両方をソース側において、単位元で構成するようにし、シンク側においても、これらを単位元で用いるようにすれば、実施的にセッションキーと時変キーを使用しないで、データの授受が可能となる。ただし、そのようにすれば、データが不正にコピーされるおそれが高くなる。

【０１３１】

アプリケーション部６１そのものが、不正にコピーしたものである場合、復号したデータが不正にコピーされてしまう恐れがあるが、上述したようにアプリケーション部６１をライセンスマネージャ６２で認証するようにすれば、これを防止することが可能である。

【０１３２】

この場合の認証方法としては、共通鍵暗号方式の他、公開鍵暗号方式を用いたデジタル署名を利用することができる。

【０１３３】

以上の図１１、図１２、図１５乃至図２０に示す構成は、準同形(homomorphism)の関係を満足するものとなっている。すなわち、キーK_1，K_2がガロアフィールドＧの要素であるとき、両者の群演算の結果、K_1・K_2もガロアフィールドＧの要素となる。そして、さらに、所定の関数Ｈについて次式が成立する。

$H(K_1 \cdot K_2) = H(K_1) \cdot H(K_2)$

【０１３４】

図２１は、さらに１３９４インタフェース２６の他の構成例を表している。この構成例においては、セッションキーＳがLFSR５０１乃至５０３に供給され、初期設定されるようになされている。LFSR５０１乃至５０３の幅n_1乃至n_3は、それぞれ２０ビット程度で、それぞれの幅n_1乃至n_3は、相互に素になるように構成される。従って、例えば、セッションキーＳのうち、例えば、上位ｎ１ビットがLFSR５０１に初期設定され、次の上位n_2ビットがLFSR５０２に初期設定され、さらに次の上位n_3ビットがLFSR５０３に初期設定される。

【０１３５】

LFSR５０１乃至５０３は、クロッキングファンクション５０６より、例えば論理１のイネーブル信号が入力されたとき、ｍビットだけシフト動作を行い、ｍビットのデータを出力する。ｍの値は、例えば、８，１６，３２，４０などとすることができる。

【０１３６】

LFSR５０１とLFSR５０２の出力は、加算器５０４に入力され、加算される。加算器５０４の加算値のうち、キャリー成分は、クロッキングファンクション５０６に供給され、sum成分は、加算器５０５に供給され、LFSR５０３の出力と加算される。加算器５０５のキャリー成分は、クロッキングファンクション５０６に供給され、sum成分は、排他的論理和回路５０８に供給される。

【０１３７】

クロッキングファンクション５０６は、加算器５０４と加算器５０５より供給されるデータの組み合わせが、００，０１，１０，１１のいずれかであるので、これらに対応して、LFSR５０１乃至５０３に対して、０００乃至１１１のいずれか１つの組み合わせのデータを出力する。LFSR５０１乃至５０３は、論理１が入力されたとき、ｍビットのシフト動作を行い、新たなｍビットのデータを出力し、論理０が入力されたとき、前回出力した場合と同一のｍビットのデータを出力する。

【０１３８】

排他的論理和回路５０８は、加算器５０５の出力するsum成分とレジスタ５０７に保持された時変キーｉの排他的論理和を演算し、その演算結果を排他的論理和回路５０９に出力する。排他的論理和回路５０９は、入力された平文と、排他的論理和回路５０８より入

力された暗号鍵の排他的論理和を演算し、演算結果を暗号文として出力する。

【０１３９】

図２２は、光磁気ディスク装置３における１３９４インタフェース３６の構成例を表している。この構成例におけるLFSR６０１乃至排他的論理和回路６０９は、図２１におけるLFSR５０１乃至排他的論理和回路５０９と同様の構成とされている。従って、その動作も、基本的に同様となるので、その説明は省略する。ただし、図２１の構成例においては、暗号化処理が行われるのに対して、図２２の構成例においては、復号処理が行われる。

【０１４０】

図２３は、パーソナルコンピュータ２の１３９４インタフェース４９の構成例を表している。この構成例におけるLFSR７０１乃至排他的論理和回路７０９も、図２２における、LFSR６０１乃至排他的論理和回路６０９と同様の構成とされている。ただし、LFSR７０１乃至７０３に初期設定されるセッションキーＳは、全てのビットが０の単位元とされている。従って、この場合、実質的にレジスタ７０７に保持された時変キーｉだけに対応して復号化処理が行われる。

【０１４１】

図２４は、パーソナルコンピュータ２のアプリケーション部６１の構成例を表している。この構成例におけるLFSR８０１乃至排他的論理和回路８０９は、図２２における、LFSR６０１乃至排他的論理和回路６０９と基本的に同様の構成とされている。ただし、レジスタ８０７に入力される時変キーｉが、全てのビットが０である単位元とされている点のみが異なっている。従って、この構成例の場合、セッションキーＳだけに基づいて暗号鍵が生成され、復号処理が行われる。

【０１４２】

なお、図１９、図２０、および図２４に示す処理は、アプリケーション部６１において行われるので、ソフト的に処理されるものである。

【０１４３】

以上においては、DVDプレーヤ１をソースとし、パーソナルコンピュータ２と光磁気ディスク装置３をシンクとしたが、いずれの装置をソースとするかシンクとするかは任意である。

【０１４４】

また、各電子機器を接続する外部バスも、１３９４バスに限らず、種々のバスを利用することができ、それに接続する電子機器も、上述した例に限らず、任意の装置とすることができる。

【０１４５】

以上のように、機能の変更がユーザに開放されていない第１の情報処理装置においては、第１の鍵と、データを復号しているとき、所定のタイミングで変更される第２の鍵を用いて、暗号鍵を生成するようにし、機能の変更がユーザに開放されている第２の情報処理装置においては、第１の鍵と、第２の鍵の一方を用いて生成した第１の暗号鍵で、暗号化されているデータを復号し、第１の鍵と第２の鍵の他方を用いて生成した第２の暗号鍵を用いて、その復号されたデータをさらに復号するようにする場合、より安全な情報処理システムを実現することが可能となる。

【０１４６】

また、第１の暗号鍵と、データを復号しているとき、所定のタイミングで変更される第２の暗号鍵を、ソフトウェアプログラムで生成するようにする場合、アプリケーションプログラム毎に復号を行うことが可能となり、不正なコピーをより確実に防止することが可能となる。

【図面の簡単な説明】

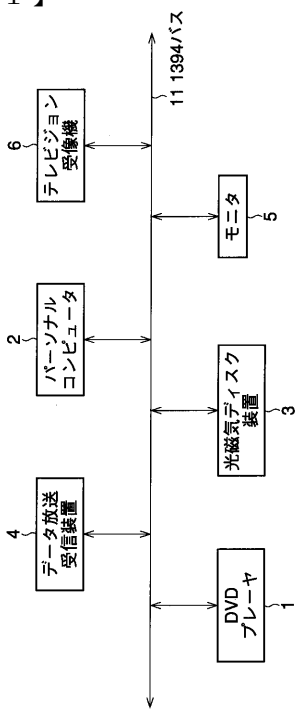
【０１４７】

【図１】本発明を適用した情報処理システムの構成例を示すブロック図である。

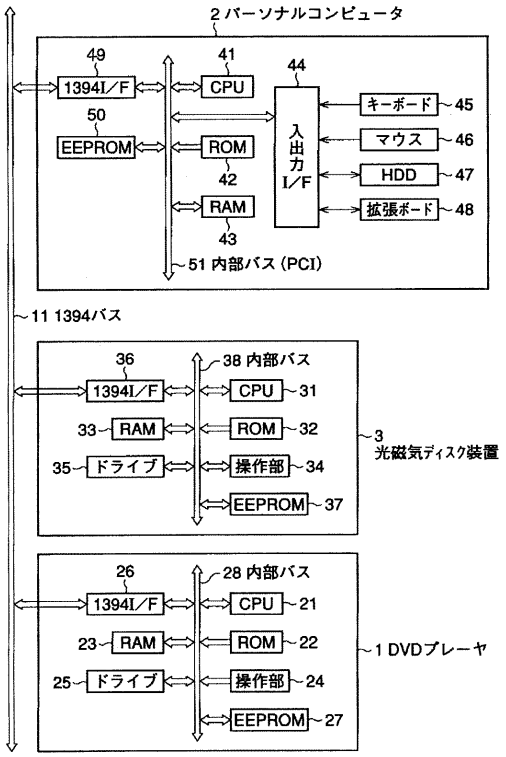
【図２】図１のDVDプレーヤ１、パーソナルコンピュータ２、および光磁気ディスク装置３の内部の構成例を示すブロック図である。

【図３】認証処理を説明する図である。
【図４】認証処理を説明するタイミングチャートである。
【図５】node_unique_IDのフォーマットを示す図である。
【図６】他の認証処理を説明するタイミングチャートである。
【図７】さらに他の認証処理を説明するタイミングチャートである。
【図８】他の認証処理を説明するタイミングチャートである。
【図９】他の認証処理を説明するタイミングチャートである。
【図１０】暗号化処理を説明するブロック図である。
【図１１】図１０の１３９４インタフェース２６の構成例を示すブロック図である。
【図１２】図１１の１３９４インタフェース２６のより詳細な構成例を示すブロック図である。
【図１３】図１２のLFSR７２のより詳細な構成例を示すブロック図である。
【図１４】図１３のLFSR７２のより具体的な構成例を示すブロック図である。
【図１５】図１０の１３９４インタフェース３６の構成例を示すブロック図である。
【図１６】図１５の１３９４インタフェース３６のより詳細な構成例を示すブロック図である。
【図１７】図１０の１３９４インタフェース４９の構成例を示すブロック図である。
【図１８】図１７の１３９４インタフェース４９のより詳細な構成例を示すブロック図である。
【図１９】図１０のアプリケーション部６１の構成例を示すブロック図である。
【図２０】図１９のアプリケーション部６１のより詳細な構成例を示すブロック図である。
【図２１】図１０の１３９４インタフェース２６の他の構成例を示すブロック図である。
【図２２】図１０の１３９４インタフェース３６の他の構成例を示すブロック図である。
【図２３】図１０の１３９４インタフェース４９の他の構成例を示すブロック図である。
【図２４】図１０のアプリケーション部６１の他の構成例を示すブロック図である。
【符号の説明】
【０１４８】
１ DVDプレーヤ，２ パーソナルコンピュータ，３ 光磁気ディスク装置，１１ １３９４バス，２０ ファームウェア，２１ CPU，２５ ドライブ，２６ １３９４インタフェース，２７ EEPROM，３１ CPU，３５ ドライブ，３６ １３９４インタフェース，３７ EEPROM，４１ CPU，４７ ハードディスク，４８ 拡張ボード，４９ １３９４インタフェース，５０ EEPROM，５１ 内部バス，６１ アプリケーション部，６２ ライセンスマネージャ

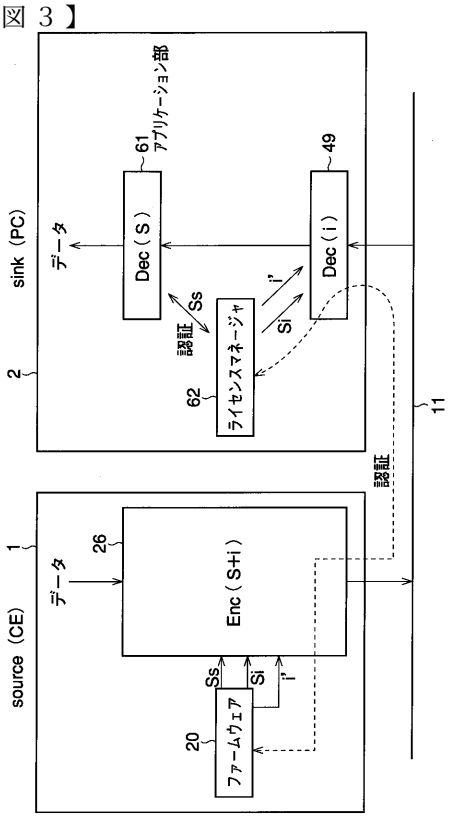
【図１】


11 1394バス
6 テレビジョン受像機
モニタ 5
2 パーソナルコンピュータ
光磁気ディスク装置 3
4 データ放送受信装置
DVDプレーヤ 1

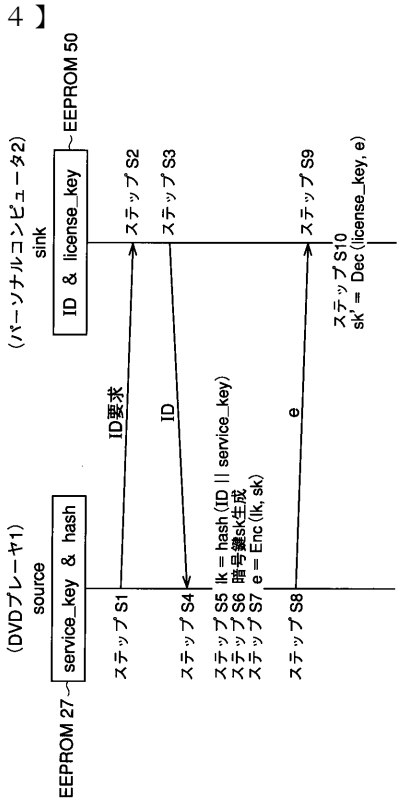
【図２】


2 パーソナルコンピュータ
49 1394I/F
41 CPU
44 入出力I/F
キーボード 45
マウス 46
HDD 47
拡張ボード 48
50 EEPROM
ROM 42
RAM 43
51 内部バス (PCI)
11 1394バス
36 1394I/F
38 内部バス
CPU 31
33 RAM
ROM 32
35 ドライブ
操作部 34
EEPROM 37
3 光磁気ディスク装置
26 1394I/F
28 内部バス
CPU 21
23 RAM
ROM 22
25 ドライブ
操作部 24
EEPROM 27
1 DVDプレーヤ

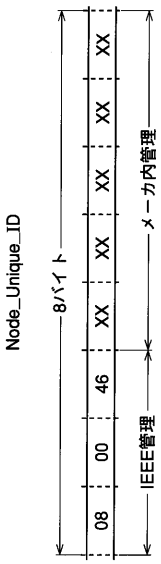
【図３】


sink (PC)
2
データ
61 アプリケーション部
Dec (S)
Dec (i) 49
認証
Ss
Si
i'
62 ライセンスマネージャ
11
認証
source (CE)
1
データ
26
Enc (S+i)
Ss
Si
i'
20 ファームウェア

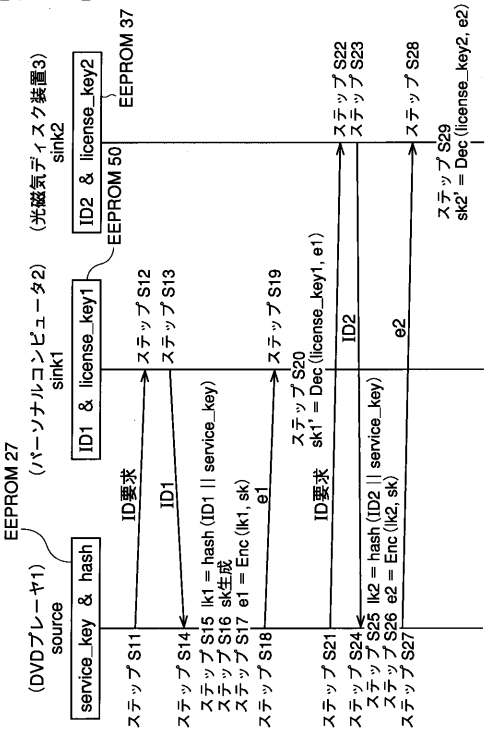
【図４】


(パーソナルコンピュータ2)
sink
ID & license_key
EEPROM 50
ステップ S2
ステップ S3
ステップ S9
ステップ S10
sk' = Dec (license_key, e)
ID要求
ID
e
(DVDプレーヤ1)
source
service_key & hash
EEPROM 27
ステップ S1
ステップ S4
ステップ S5 Ik = hash (ID || service_key)
ステップ S6 暗号鍵sk生成
ステップ S7 e = Enc (Ik, sk)
ステップ S8

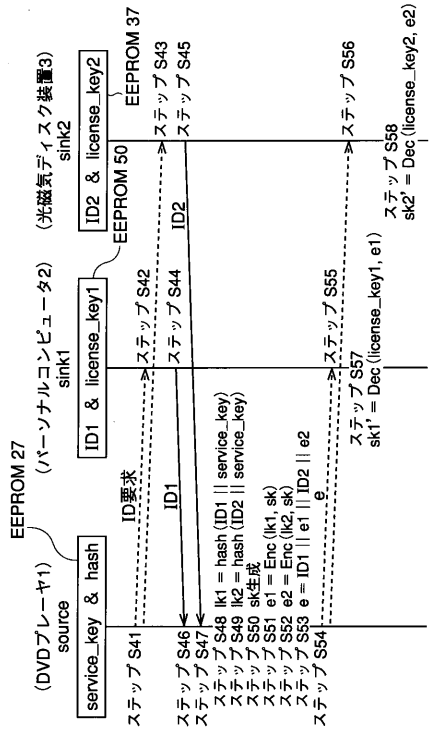
【図５】


Node_Unique_ID
8バイト
08
00
46
XX
XX
XX
XX
XX
IEEE管理
メーカ内管理

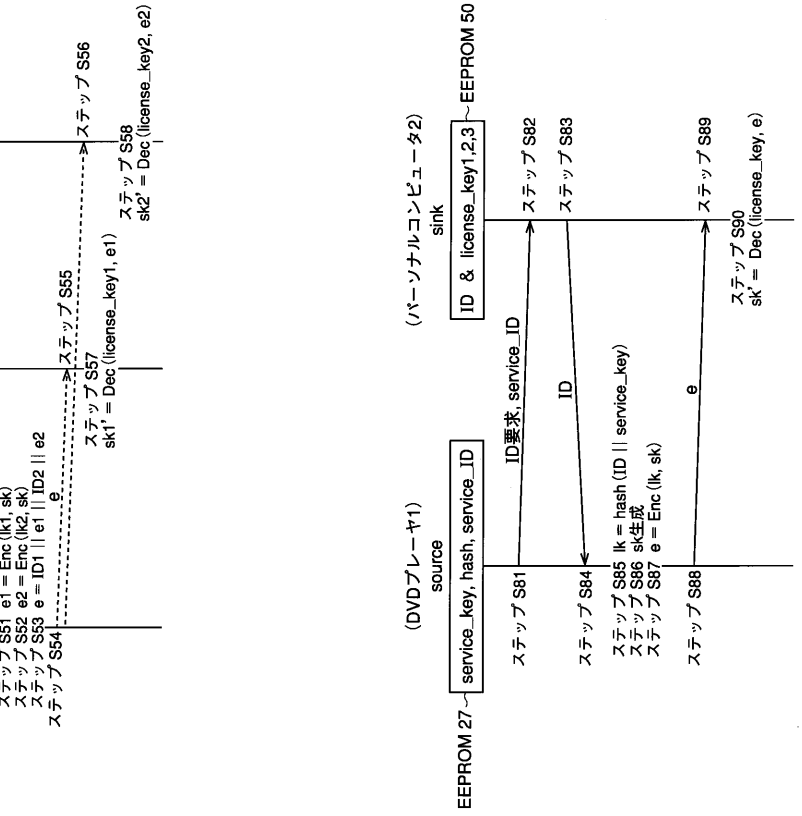
【図６】


EEPROM 27
(DVDプレーヤ1)
source
service_key & hash
(パーソナルコンピュータ2)
sink1
ID1 & license_key1
EEPROM 50
(光磁気ディスク装置3)
sink2
ID2 & license_key2
EEPROM 37
ステップ S11
ID要求
ステップ S12
ID1
ステップ S13
ステップ S14
ステップ S15 lk1 = hash (ID1 || service_key)
ステップ S16 sk生成
ステップ S17 e1 = Enc (lk1, sk)
e1
ステップ S18
ステップ S19
ステップ S20
sk1' = Dec (license_key1, e1)
ID要求
ステップ S21
ID2
ステップ S22
ステップ S24 lk2 = hash (ID2 || service_key)
ステップ S23
ステップ S25
ステップ S26 e2 = Enc (lk2, sk)
e2
ステップ S27
ステップ S28
ステップ S29
sk2' = Dec (license_key2, e2)

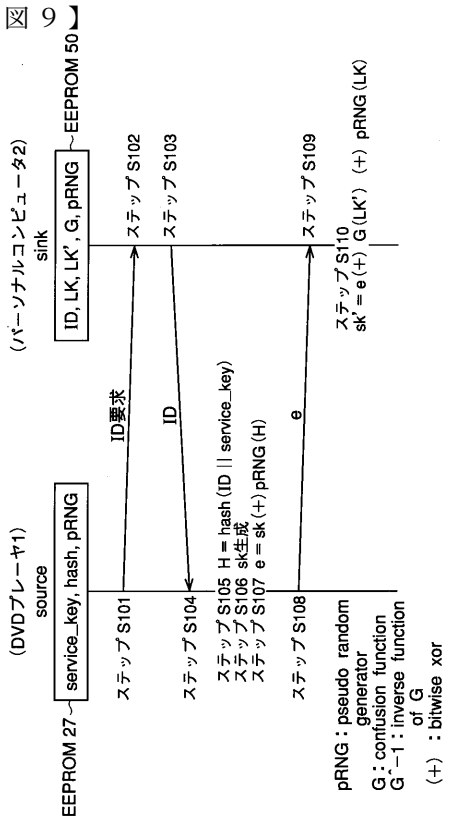
【図７】


EEPROM 27
(DVDプレーヤ1)
source
service_key & hash
(パーソナルコンピュータ2)
sink1
ID1 & license_key1
EEPROM 50
(光磁気ディスク装置3)
sink2
ID2 & license_key2
EEPROM 37
ステップ S41
ID要求
ステップ S42
ID1
ステップ S43
ステップ S44
ID2
ステップ S45
ステップ S46
ステップ S47
ステップ S48 lk1 = hash (ID1 || service_key)
ステップ S49 lk2 = hash (ID2 || service_key)
ステップ S50 sk生成
ステップ S51 e1 = Enc (lk1, sk)
ステップ S52 e2 = Enc (lk2, sk)
ステップ S53 e = ID1 || e1 || ID2 || e2
e
ステップ S54
ステップ S55
ステップ S56
ステップ S57
sk1' = Dec (license_key1, e1)
ステップ S58
sk2' = Dec (license_key2, e2)

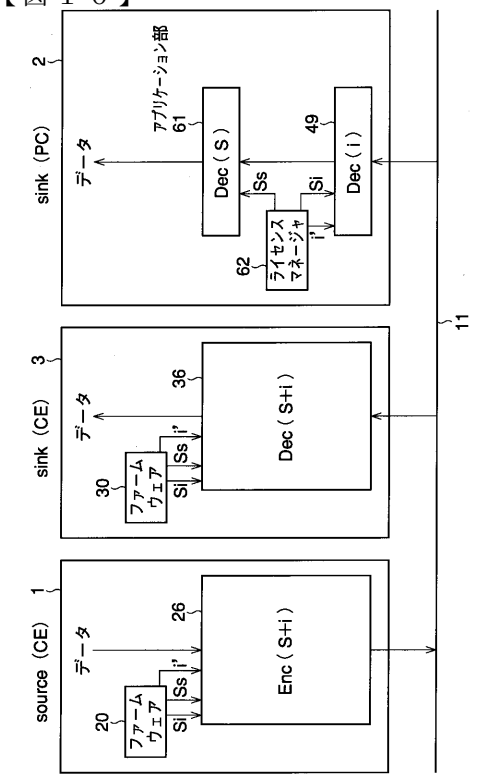
【図８】


EEPROM 27
(DVDプレーヤ1)
source
service_key, hash, service_ID
(パーソナルコンピュータ2)
sink
ID & license_key1,2,3
EEPROM 50
ステップ S81
ID要求, service_ID
ステップ S82
ステップ S83
ID
ステップ S84
ステップ S85 lk = hash (ID || service_key)
ステップ S86 sk生成
ステップ S87 e = Enc (lk, sk)
e
ステップ S88
ステップ S89
ステップ S90
sk' = Dec (license_key, e)

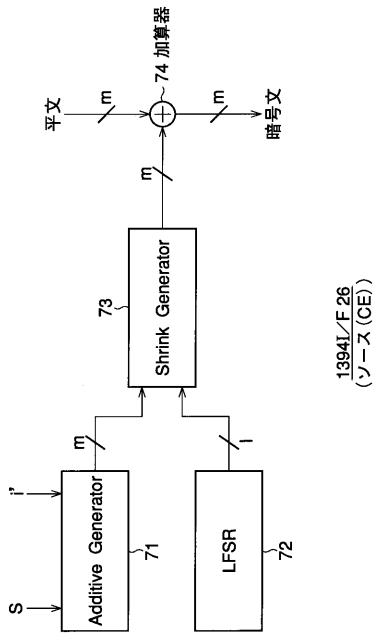
【図９】



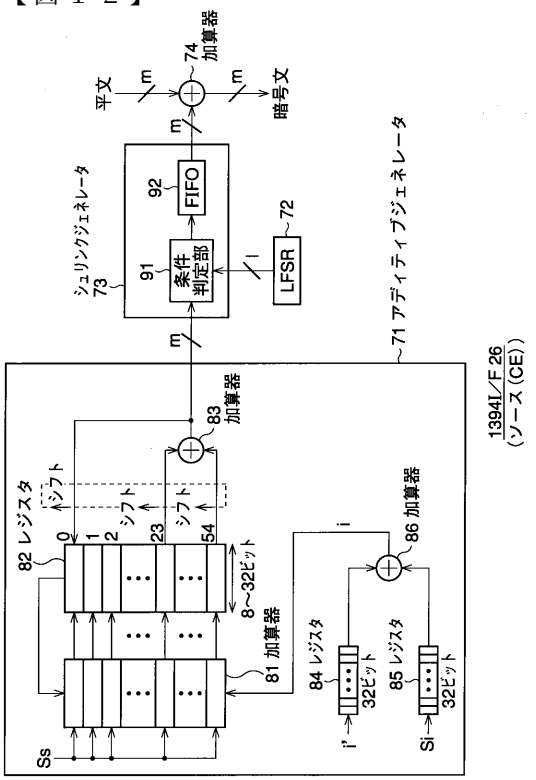
【図１０】



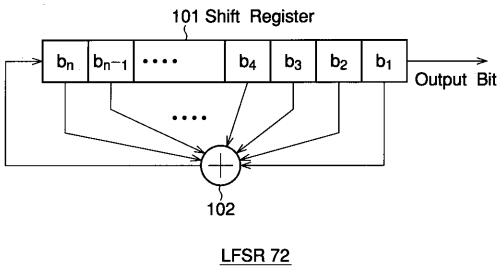
【図１１】



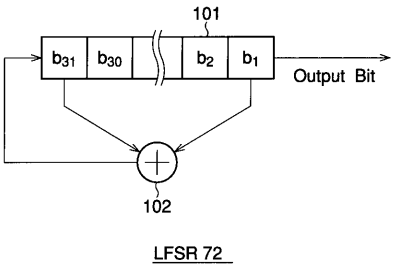
【図１２】



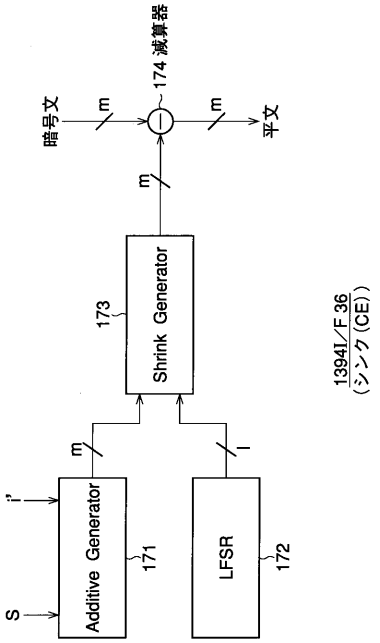
【図１３】



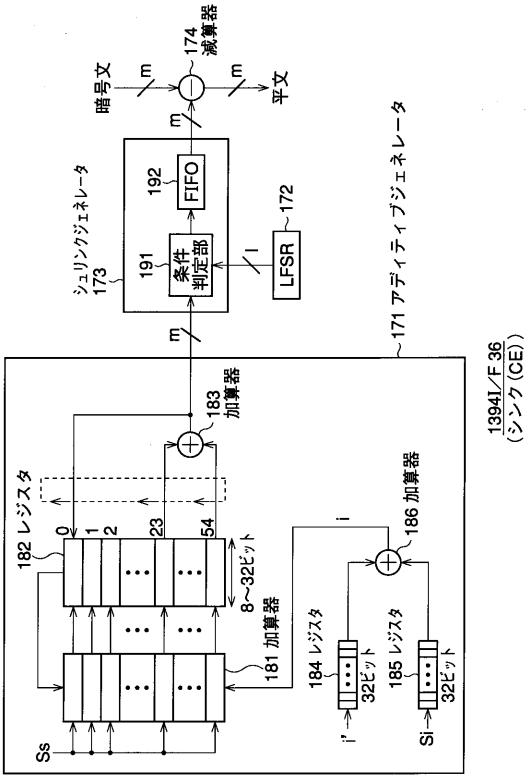
【図１４】



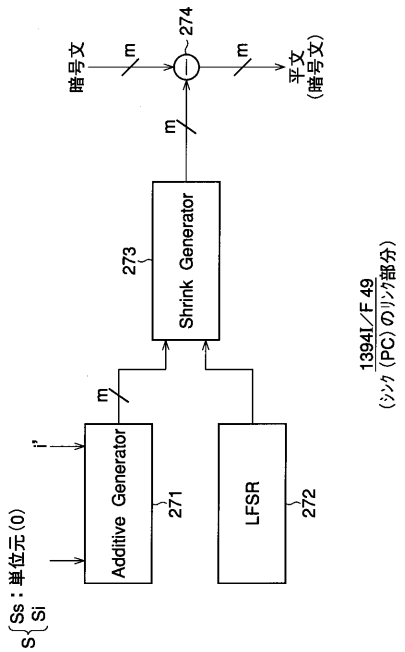
【図１５】



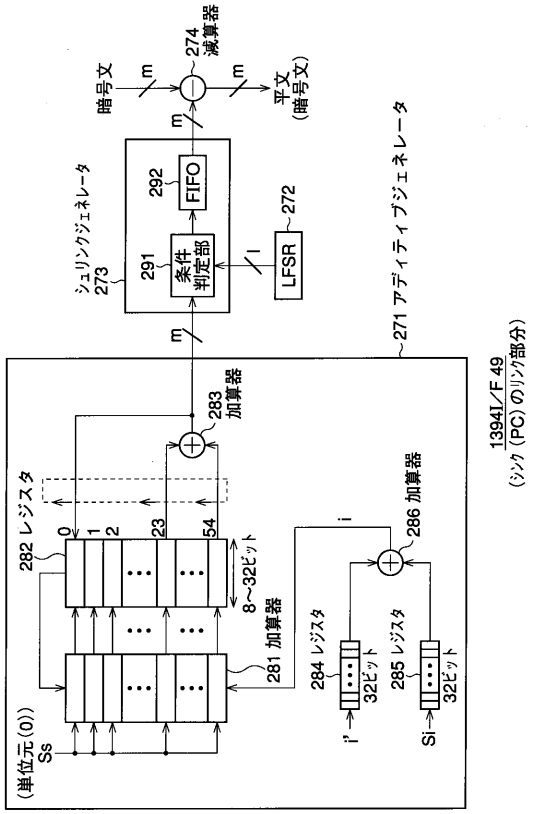
【図１６】



【図１７】

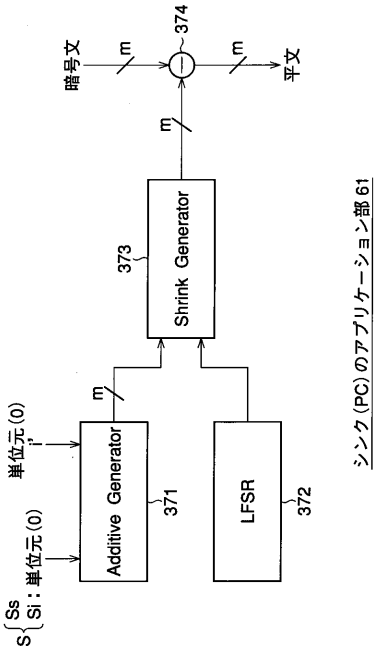


【図１８】



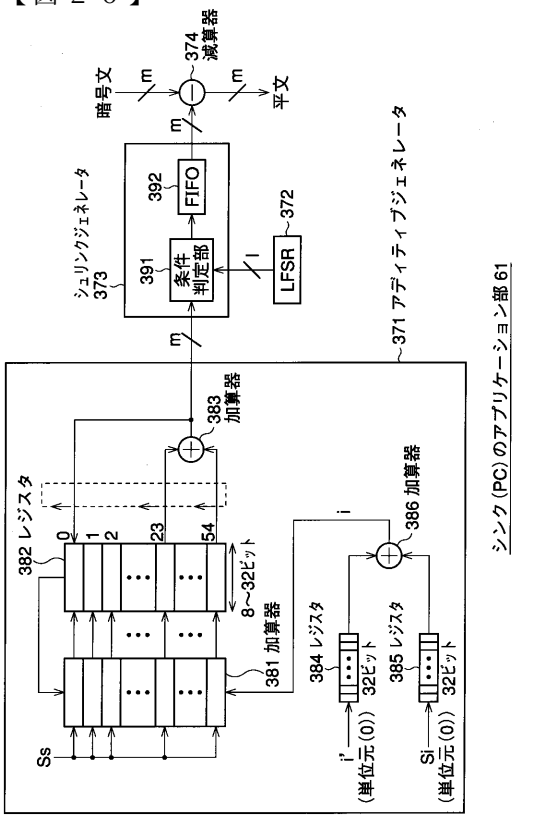
1394I/F 49
(シンク(PC)のリンク部分)

【図１９】



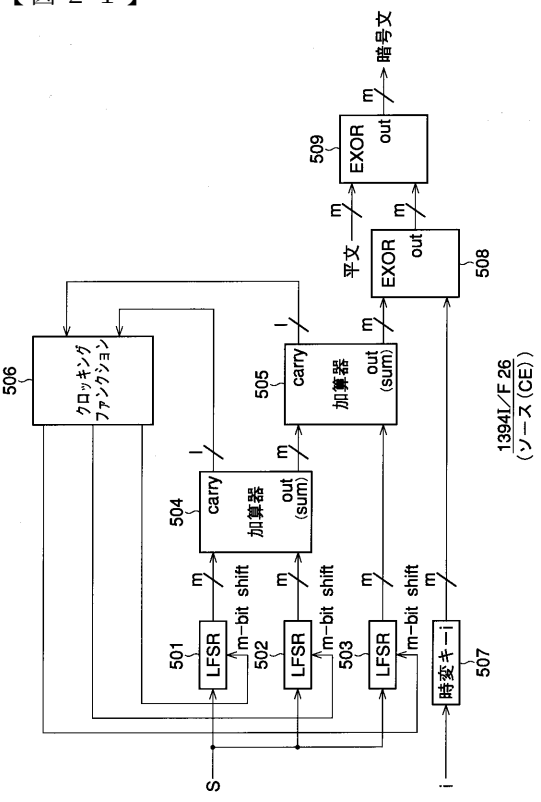
シンク(PC)のアプリケーション部 61

【図２０】



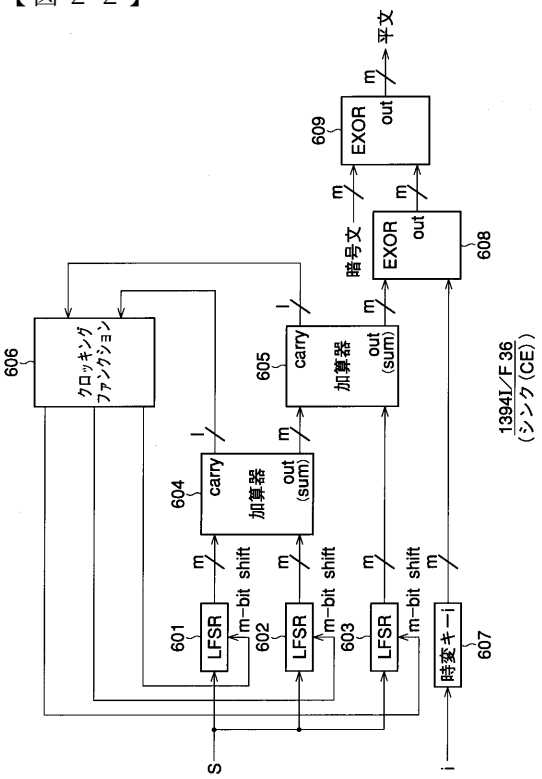
シンク(PC)のアプリケーション部 61

【図２１】

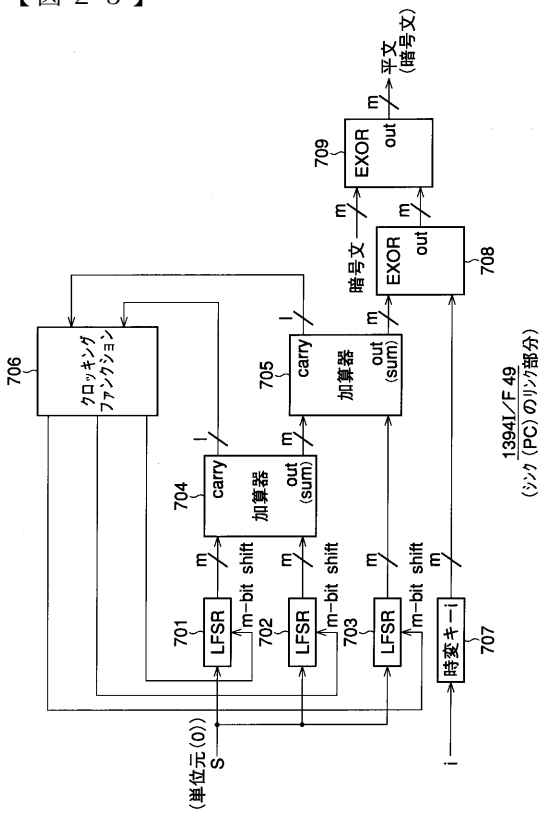


1394I/F 26
(ソース(CE))

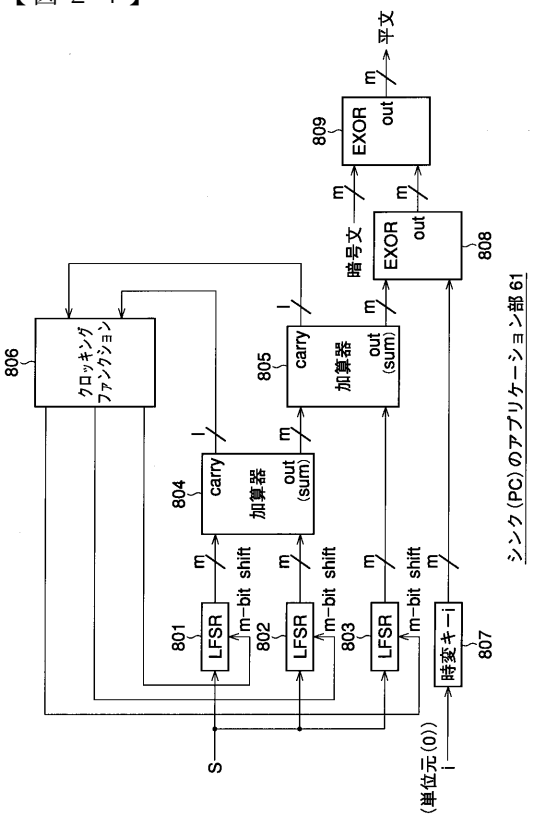
【図２２】


606
クロッキング
ファンクション
601
602
603
LFSR
m-bit shift
604
605
carry
加算器
out
(sum)
607
時変キーi
608
609
EXOR
暗号文
平文
S
i
1394I/F 36
(シンク(CE))

【図２３】


706
クロッキング
ファンクション
701
702
703
LFSR
m-bit shift
704
705
carry
加算器
out
(sum)
707
時変キーi
708
709
EXOR
暗号文
平文
(暗号文)
(単位元(0))
S
i
1394I/F 49
(シンク(PC)のリンク部分)

【図２４】


806
クロッキング
ファンクション
801
802
803
LFSR
m-bit shift
804
805
carry
加算器
out
(sum)
807
時変キーi
808
809
EXOR
暗号文
平文
S
(単位元(0))
i
シンク(PC)のアプリケーション部61

フロントページの続き

(72)発明者　佐藤　真
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　嶋　久登
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

Ｆターム(参考) 5J104 AA12　AA16　AA32　EA04　EA15　EA16　JA03　MA05　NA02　NA27
NA37　PA14