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

特許第4512372号
(P4512372)

(45)発行日　平成22年7月28日(2010.7.28)　(24)登録日　平成22年5月14日(2010.5.14)

(51)Int.Cl.　　F I
G06F 21/24 (2006.01)　　G06F 12/14 540A
H04L 9/10 (2006.01)　　G06F 12/14 540P
　　H04L 9/00 621A

請求項の数 12　(全 8 頁)

(21)出願番号　特願2003-582615 (P2003-582615)
(86)(22)出願日　平成15年4月2日 (2003.4.2)
(65)公表番号　特表2005-527896 (P2005-527896A)
(43)公表日　平成17年9月15日 (2005.9.15)
(86)国際出願番号　PCT/FR2003/001024
(87)国際公開番号　WO2003/085496
(87)国際公開日　平成15年10月16日 (2003.10.16)
審査請求日　平成18年3月8日 (2006.3.8)
(31)優先権主張番号　02/04321
(32)優先日　平成14年4月8日 (2002.4.8)
(33)優先権主張国　フランス(FR)

(73)特許権者　505295499
ナグラ　トムソン　ライセンシング
フランス国　９２１００　ブローニュ－ビヤンクール　ケ　アルフォンス　ル　ガロ　４６
(74)代理人　100074332
弁理士　藤本　昇
(74)代理人　100114421
弁理士　薬丸　誠一
(74)代理人　100114432
弁理士　中谷　寛昭
(72)発明者　ダウボイス，ジャン－ルック
フランス国　Ｆ－７５１１６　パリ　ルー　エウジェン　マニュール　１９

最終頁に続く

(54)【発明の名称】メモリーに格納されたデジタルデータを保護するための方法および装置。

(57)【特許請求の範囲】
【請求項１】
チップカードのメモリー（４）に格納されたデジタルデータを暗号化キーを用いて保護する方法であって、前記暗号化キーが、少なくともチップカードに本質的に備えられたオペレーティング・パラメータによる関数として動的に定められており、以下のステップ、
・前記メモリー（４）への書き込み段階において、
ａ）前記チップカードに本質的に備えられた前記パラメータに相当するアナログ信号を、前記チップカードにおいて発生され、前記メモリー（４）にデータを書き込むためのアナログ電圧（１８）から予め定められた時間において抽出するステップ、
ｂ）この信号をアナログ／デジタル変換器（１４）によってデジタルシーケンスＳに変換するステップ、
ｃ）暗号化キーを形成している前記デジタルシーケンスＳによって、記憶させるデータを暗号化するステップ、
ｄ）前記メモリー（４）に暗号化されたデータを格納するステップ、
・そして、それに続く、格納されたデータを読み取る段階において、
－　書き込み段階でのステップａ）およびステップｂ）において定められた暗号化キーを再計算するステップ、
－　再計算されたキーによるデータを解読するステップ、
を有していることを特徴とするデジタルデータの保護方法。
【請求項２】

前記暗号化されたデジタルデータは、ＥＭＭメッセージとＥＣＭメッセージとを暗号化コードするためのデジタルキーである請求項１記載のデジタルデータの保護方法。
【請求項３】
前記チップカードに本質的に備えられている前記オペレーティング・パラメータは、メモリーにデータを書き込むためのチャージポンプ（１２）により提供されたものである請求項１記載のデジタルデータの保護方法。
【請求項４】
チップカードのメモリー（４）に格納され暗号化キーを用いて事前に暗号化されたデジタルデータを保護するための装置であって、前記チップカードに本質的に備えられた少なくとも一つのオペレーティング・パラメータに従って前記データを暗号化するキーを定義可能な計算モジュール（１０）が備えられているとともにアナログ電圧（１８）を発生させるジェネレーターが備えられており、前記計算モジュール（１０）は、予め定められた時間（ｔ）において前記アナログ電圧（１８）から前記本質的に備えられたオペレーティング・パラメータに相当するアナログ信号を抽出する手段を有し、さらに、前記暗号化キーを形成させるために前記アナログ信号を、前記暗号化キーを形成するデジタルシーケンスに変換する手段を有しており、前記チップカードに本質的に備えられている前記オペレーティング・パラメータは、メモリーにデータを書き込むためのチャージポンプ（１２）により提供されることを特徴とするデジタルデータの保護装置。
【請求項５】
前記デジタルデータがＥＭＭメッセージとＥＣＭメッセージとを暗号化コードするためのデジタルキーである請求項４記載のデジタルデータの保護装置。
【請求項６】
前記計算モジュール（１０）には、アナログ／デジタル変換器（１４）が備えられている請求項４記載のデジタルデータの保護装置。
【請求項７】
請求項４乃至６のいずれか１項に記載のデジタルデータの保護装置を有し、中央処理ユニット（２）を有することを特徴とするチップカード。
【請求項８】
前記計算モジュール（１０）が、前記中央処理ユニット（２）によって監督されることなく暗号化キーを計算するために、中央処理ユニット（２）から機能的に独立している請求項７に記載のチップカード。
【請求項９】
前記暗号化キーを形成するデジタルシーケンス（Ｓ）を生成するためのデジタル回路を中央処理ユニット（２）から独立した状態で備えている請求項７に記載のチップカード。
【請求項１０】
ロジック回路である暗号化モジュール（６）を有する請求項７に記載のチップカード。
【請求項１１】
前記メモリー（４）がＥＥＰＲＯＭタイプである請求項７乃至１０のいずれか１項に記載のチップカード。
【請求項１２】
前記メモリー（４）がフラッシュタイプである、請求項１１に記載のチップカード。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データの格納のためのメモリーの内容が侵害されることに対する対策に関し、特に、チップカードのメモリーに蓄積され、事前に暗号キーにより暗号化されたデジタルデータを保護する方法に関する。さらに、本発明は、さらにこのようなチップカードのメモリーを保護する、チップカード及び装置に関する。
【背景技術】
【０００２】

チップカードの内容の侵害は、一般には、ＲＯＭコードおよびカードのメモリーに含まれる秘密データの抽出によってなされる。そのようなことを回避する既知の技術としては、これらの不正な解読により使用可能となる重要データを、カードのメモリーに格納する前に秘密のキーを使用して、それらを暗号化することである。この暗号のキーも、メモリーに格納されることから、格納されたデータを使用可能とされるように、不正に解読される危険に曝される。したがって、このような技術は、侵害に対する対抗措置として有効とならないおそれを有している。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

本発明の目的はメモリー中に暗号化された形式で格納されたデータの最適なる安全性を確立することにある。

【０００４】

また、本発明のさらなる目的は、暗号キーを、カードの構成要素の少なくとも一つに本来備えられる１つ以上のオペレーティング・パラメータと緊密にリンクさせることである。このようなオペレーティング・パラメータとしては、メモリーやこのメモリーと関連するマイクロコントローラーなどの物理的構造に起因する物理的数値とすることができ、さらに、このメモリーやマイクロコントローラーの特定の操作状況における定められた挙動を反映する数値としてもよい。

【課題を解決するための手段】

【０００５】

より詳しくは、本発明は、例えばＥＥＰＲＯＭタイプあるいはフラッシュタイプのメモリーに暗号化された形式で格納されたデジタルデータを保護するための方法及び装置に関するものである。

本発明による方法は、前記暗号化キーが、少なくとも前記チップカードに本来備わっているオペレーティング・パラメータの関数として動的に定められることをもって特徴付けられる。

【０００６】

本発明によれば、チップカードに本来備えられたオペレーティング・パラメータは、チップカードの中で統合された関数ジェネレーターによって生成される。本発明によれば、前記オペレーティング・パラメータは、チップカードのメモリーに本来備わったものである。

【０００７】

本発明の一実施形態においては、方法は次のステップを含む：

メモリーにデータを書き込む過程において、

ａ－メモリー中の書き込みのためにアナログ電圧からアナログ信号を抽出すること、

ｂ－この信号をデジタルシーケンスに変換すること、

ｃ－前記デジタルシーケンスによって、格納されるデータを暗号化すること、

ｄ－暗号化されたデータをメモリーに格納すること、

そして、メモリーへ格納されたデータの読み取りの後の過程中においては、

－　書き込み過程のａ、ｂステップにおいて定義された暗号キーを再計算し、

－　再計算されたキーによってデータを解読すること。

【０００８】

この実施形態において、書き込み用のアナログ電圧はチャージポンプによって提供される。

【０００９】

本発明の装置は、少なくとも前記チップカードに本来備えられたオペレーティング・パラメータによる関数として格納されるデジタルデータの暗号化のためのキーを定義し得る計算モジュールを備えていることを特徴としている。

【００１０】

本発明の一実施形態によれば、計算モジュールは、チャージポンプによって提供されるアナログ書き込み電圧からアナログ信号を抽出し、暗号キーを形成するためにこのアナログ信号をデジタルシーケンスに変換する。

【００１１】

本発明は、また、データ処理のための中央ユニット（中央処理ユニット）、少なくとも一つのデータ格納メモリー、前記デジタルデータを暗号化するための暗号化モジュール、及び、少なくとも前記データを暗号化するためのキーについての計算を行う計算モジュールを備えるアクセスコントロールカードに関する。

【００１２】

本発明におけるアクセス制御カードによれば、少なくとも前記カードのメモリーに本来備えられたオペレーティング・パラメータの関数として暗号化キーが定義付けられる手段と、格納されたデータの各読み取りにおいて予め定義された暗号キーを動的に再計算する手段とが備えられている。

【００１３】

発明の特徴としては、計算モジュールは、中央処理ユニットから機能的に独立しており、そのため、暗号化キーの計算は単純に初期化され、中央処理ユニットに監督されないことである。

【００１４】

本発明の一実施形態においては、計算モジュールは、チップカードにデータを書き込むためのアナログ電圧を生じるチャージポンプと、前記アナログ電圧からアナログ信号を抽出し暗号化キーを形成するデジタルシーケンスに交換させるアナログ／デジタル変換器とを有している。

【発明を実施するための最良の形態】

【００１５】

本発明のその他の特徴および利点は、添付された図を参照しつつ、限定的でない例示によって、以下の詳述より明白になる。

本発明の、チップカードのメモリーに格納されたデータを保護する構造について詳しく述べる。

チップカードは、例えば暗号化された視聴覚プログラムなどのサービスやデータへのアクセス認証のコントロールパラメータを格納するような用途に広く使用されている。

このような応用において、スクランブル解除のために求められる情報は、ＥＣＭ（認証制御メッセージ）と呼ばれるアクセスコントロールメッセージ中で伝達され、以下の入力データから生成されている。

・スクランブル解除シーケンス初期化のための制御単語
・一人あるいは複数利用者のグループのために、制御単語にスクランブルを掛けるのに用いられるサービスキー
・サービスキーにスクランブルを掛けるために使用される利用者キー。

【００１６】

サービスキーは、前もって、個人またはグループの利用者キーから生成されたＥＭＭと呼ばれるメッセージ中で伝達されている。

【００１７】

ＥＣＭは、特に、制御単語によって構成され、サービスキーによって処理され、規則的な間隔で加入者に伝達されている。

【００１８】

ＥＭＭは、特に、サービスキーにより構成され、一つ以上の利用者キーを処理し、規則的な間隔で加入者に伝達されている。

【００１９】

受理においては、解読の原理は、チップカードのメモリー（ＥＭＭ）に含まれる一つ以上の利用者キーを使用しているサービスキーを見出すことに基づいている。

【００２０】

その後、このサービスキーは、それ自身が、スクランブル解除のシステム初期化を許す制御単語を見出すべく、ＥＣＭの解読に用いられる。

【００２１】

それは、前述したように、チップカードのメモリーの内容が抽出され、スクランブル化システムの初期化を許す制御単語を計算することを直接あるいは間接的に可能にするＥＭＭおよびＥＣＭを処理するためのキーを見つけるための不正な処理において再利用されるおそれがある。

【００２２】

図１は、メモリー装置の一般的なブロック図を示し、暗号化モジュール（暗号化／解読モジュール）６を通じてメモリー４と接続された中央処理ユニット２を備えている。中央処理ユニット２の外部に配された、計算モジュール１０も、暗号化／解読モジュール６に接続されている。

【００２３】

メモリー４に中央ユニット２にて処理されたデータを格納しなければならない時には、処理ユニット２は計算モジュール１０に活性化信号を送る。この信号を受け取ると、計算モジュール１０は、格納されるデータの暗号化のためのキーを設定し、暗号化／解読モジュール６にこのキーを送信する。

【００２４】

発明の本質的な特徴によれば、メモリー４に本質的に備えられたオペレーティング・パラメータの少なくとも一つの関数としてデータをメモリー４に格納する瞬間に、暗号化キーが計算される。この方法で計算された暗号化キーは、メモリー４に格納されない。しかしながら、チップカードの侵害においては、通常、中央ユニット２にインプリメントされた計算プログラム、および、中央ユニット２に関連したメモリー４に含まれている重大なデータの抽出が行われる。従って、これらのプログラム、およびメモリー４の内容の不正な抽出が行われる場合には、抽出されたデータは、前記データの書き込み時及びこれらのデータの読み込み時に動的に計算された暗号化キーなしでは利用することができない。

【００２５】

好ましくは、このキーは、前記メモリー４に本質的に備えられたオペレーティング・パラメータの一つ、あるいは複数を組み合わせた関数として計算される。

【００２６】

計算モジュール１０が中央ユニット２から独立しているため、定義された暗号化キーは外部からアクセス可能ではない。

【００２７】

操作において、中央ユニット２から計算モジュール１０までのデータの転送の時に、後者は、中央ユニット２から暗号化キーの計算を開始することができる最初の活性化信号を受け取る。この方法で計算されたキーは、メモリー４に格納される前にデータを暗号化するのに用いるべく暗号化／解読モジュール６に伝達される。

【００２８】

暗号化されたデータが読まれる場合、処理ユニット２は計算モジュール１０に暗号化キーを動的再計算させるための第二の活性化信号を送る。そして、その後、前記データの解読を行うために暗号化／解読モジュール６に用いられそれらを中央ユニットに伝達する。

【００２９】

暗号化キーの計算の例示として、図２を参照しつつ、発明の実施例を詳述すると、モジュール１０には、メモリー４にデータを書き込むためのアナログ電圧を用意するチャージポンプ１２、アナログ電圧から抽出されるアナログ信号を、暗号化キーを含有するデジタルシーケンスに変換するアナログ／デジタル変換器（ＣＡＮ）１４、書き込み電圧から抽出されるアナログ信号の期間を定めるためにチャージポンプ１２にリンクされたクロック１６を含んでいる。

【００３０】

アナログ電圧は、チャージポンプから独立したアナログ電圧ジェネレーターによって提

供されていてもよい。

【００３１】

ここには、示されないが他の実施形態として、チップカードは、デジタルシーケンスＳを直接提供する中央ユニット２から独立したデジタル回路を含んでもよい。

【００３２】

図３は、中央ユニット２からアウトプットされたデジタルデータをメモリー４に書き込むための電圧１８の印加と時間とを示すものである。電圧１８の値Ａは、クロック１６により期間ｔにプログラミングされ定められている。その後、この値ＡはＣＡＮ１４によって、デジタルデータを暗号化／解読するための暗号化／解読モジュール６に用いるデジタルシーケンスＳに変換される。

【００３３】

各リセットにおいては、計算モジュール１０が、クロック１６を使用してプログラムされた期間ｔを考慮して、暗号化キーの計算を行う。従って、たとえ侵害者がデジタルデータを抽出しても、彼／彼女は、本物のカードに本質的に備えられた値Ａに基づく暗号化キーを再計算することができない。暗号化キーは、初めてチップカードのカスタム化において初めて計算される。

【００３４】

発明の別の実施形態では、複数の値Ａに対応する複数の期間ｔが、各キーが前もって定められた期間に使用可能とされた複数の異なる暗号化キーを計算するのに有用とすべくあらかじめプログラムされていても良い。

【００３５】

また、別の実施形態においては、期間ｔを間接的に変更させるようにしてもよい。

【図面の簡単な説明】

【００３６】

【図１】図１には、本発明による装置の一般的な略図を表わす。

【図２】図２には、図１の装置の特定の実施形態を概略的に表わす。

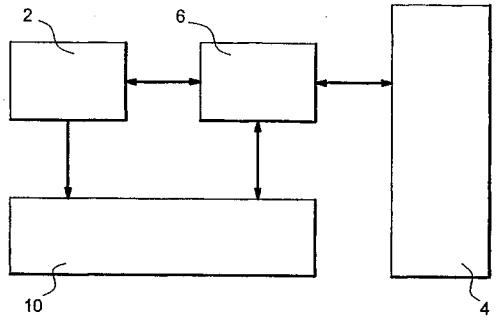
【図３】図３には、図２に例示された発明の利用を示すグラフを表す。

【符号の説明】

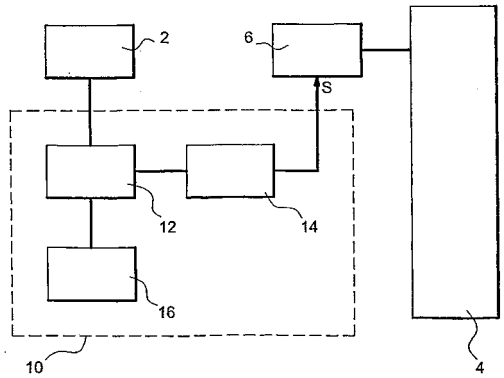
【００３７】

２　中央処理ユニット
４　メモリー
６　暗号化モジュール
１０　計算モジュール
１２　チャージポンプ
１４　アナログ／デジタル変換器
１６　クロック
Ｓ　デジタルシーケンス

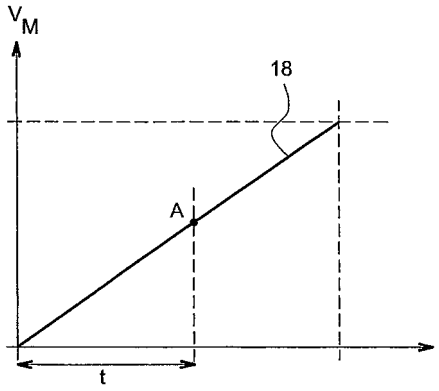
【図１】



【図２】



【図３】



フロントページの続き

審査官　高橋　克

(56)参考文献　特開平１０－１８７５４６（ＪＰ，Ａ）
特開２００２－０７７１４１（ＪＰ，Ａ）
米国特許第０５８１８７３８（ＵＳ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21
H04L 9