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

特許第6204439号
(P6204439)

(45)発行日　平成29年9月27日(2017.9.27)　(24)登録日　平成29年9月8日(2017.9.8)

(51)Int.Cl.			F I		
H04L	9/10	(2006.01)	H04L	9/00	621A
H04L	9/32	(2006.01)	H04L	9/00	621Z
G06F	21/79	(2013.01)	H04L	9/00	673A
			G06F	21/79	

請求項の数 14　(全 13 頁)

(21)出願番号　特願2015-223639(P2015-223639)
(22)出願日　平成27年11月16日(2015.11.16)
(62)分割の表示　特願2014-523825(P2014-523825)の分割
原出願日　平成23年8月10日(2011.8.10)
(65)公開番号　特開2016-48951(P2016-48951A)
(43)公開日　平成28年4月7日(2016.4.7)
審査請求日　平成27年12月16日(2015.12.16)
(31)優先権主張番号　10-2011-0077271
(32)優先日　平成23年8月3日(2011.8.3)
(33)優先権主張国　韓国(KR)

前置審査

(73)特許権者　513146181
アイシーティーケー　カンパニー　リミテッド
大韓民国　１３５－９９７　ソウル市　カンナム区　テチドン　ジャウォン　ビルディング　９１２－３１　２、３階　フロア
(74)代理人　100079049
弁理士　中島　淳
(74)代理人　100084995
弁理士　加藤　和詳
(72)発明者　キム　ドン　ケ
大韓民国　１３０－１０３　ソウル市　トンデムン区　チャンアン　３－ドン　レミアン　チャンアン　１－チャ　アパート　ナンバー　１０５－２１０３

最終頁に続く

(54)【発明の名称】識別キー漏れを防止するＩＣチップ及びこの認証方法

(57)【特許請求の範囲】
【請求項１】
金融機能を行うＩＣチップにおいて、
前記ＩＣチップを用いた金融機能を行うとき認証に用いられるＰＩＮを提供するＰＩＮ提供部と、
前記ＰＩＮを前記ＩＣチップの外部に送信する入出力インタフェースと、
前記ＩＣチップに対する最初の活性化時における前記ＩＣチップへの最初アクセスで前記ＰＩＮが前記入出力インタフェースを介して外部に提供されると、前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断する遮断部と、
を備える、ＩＣチップ。
【請求項２】
前記遮断部は、
少なくとも１つのフューズ及び前記少なくとも１つのフューズそれぞれに、前記少なくとも１つのフューズをメルティングされるように臨界電流以上の電流である過電流を印加できる少なくとも１つのスイッチを含み、
前記少なくとも１つのスイッチは、前記ＩＣチップに対する前記最初アクセスで前記ＰＩＮが前記入出力インタフェースを介して外部に提供されると、前記少なくとも１つのフューズに前記過電流を印加して前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断する、請求項１に記載のＩＣチップ。
【請求項３】

前記ＰＩＮ提供部は、半導体製造工程偏差を用いて前記ＰＩＮを提供するＰＵＦ（Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ）を含む、請求項１に記載のＩＣチップ。

【請求項４】

前記ＰＩＮ提供部が提供したＰＩＮとユーザから受信されたＰＩＮとを比較し、前記ユーザから受信されたＰＩＮが前記ＰＩＮ提供部が提供したＰＩＮと一致する場合に前記ＩＣチップの使用を認証する認証部をさらに備える、請求項１に記載のＩＣチップ。

【請求項５】

前記認証部は、

前記ＰＩＮ提供部に提供されたＰＩＮを暗号化して格納し、前記ユーザから受信されたＰＩＮを暗号化し、前記暗号化されて格納されたＰＩＮと比較することによって一致する場合に前記ＩＣチップの使用を認証する、請求項４に記載のＩＣチップ。

【請求項６】

前記ＰＩＮ提供部で提供されたＰＩＮと前記ＩＣチップに含まれてユーザから受信されたＰＩＮの認証のための別途のＰＩＮに基づいて前記ＩＣチップの使用を認証する認証部をさらに備える、請求項１に記載のＩＣチップ。

【請求項７】

前記ＰＩＮ提供部は、予め入力されたＰＩＮを格納して前記格納されたＰＩＮを前記ＩＣチップを用いた金融機能実行の認証に用いられるＰＩＮとして提供する、請求項１に記載のＩＣチップ。

【請求項８】

金融機能を行うＩＣチップにおいて、

前記ＩＣチップを用いた金融機能実行の認証に用いられるＰＩＮを格納するＰＩＮ提供部と、

外部端末が、前記ＩＣチップに対する最初の活性化時に、前記ＩＣチップに最初にアクセスする場合、前記ＰＩＮ提供部に格納されたＰＩＮを前記外部端末に送信する入出力インタフェースと、

前記外部端末から制御信号を受信する場合、前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断する遮断部と、

を備える、ＩＣチップ。

【請求項９】

前記遮断部は、

少なくとも１つのフューズ及び前記少なくとも１つのフューズに電流を印加できるスイッチを含み、前記制御信号を受信する場合に前記スイッチを介して前記少なくとも１つのフューズに前記少なくとも１つのフューズそれぞれをメルティングするように臨界電流以上の過電流を印加して前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断する、請求項８に記載のＩＣチップ。

【請求項１０】

前記ＰＩＮ提供部が提供したＰＩＮとユーザから受信されたＰＩＮとを比較し、前記ユーザから受信されたＰＩＮが前記ＰＩＮ提供部が提供したＰＩＮと一致する場合に前記ＩＣチップの使用を認証する認証部をさらに備える、請求項８に記載のＩＣチップ。

【請求項１１】

金融機能を行うＩＣチップの活性化を行う端末装置において、

前記ＩＣチップに対する最初の活性化時に、前記ＩＣチップに最初に前記ＩＣチップの入出力インタフェースを介して前記ＩＣチップのＰＩＮ提供部にアクセスし、前記ＰＩＮ提供部が提供する前記ＩＣチップのＰＩＮを判読して出力し、

前記ＩＣチップのＰＩＮ提供部と前記ＩＣチップの入出力インタフェースとの間の遮断部に制御信号及び電流を印加し、前記ＩＣチップのＰＩＮ提供部と前記ＩＣチップの入出力インタフェースとの間の電気的な接続を遮断する、端末装置。

【請求項１２】

金融機能を行うＩＣチップにおいて、
前記ＩＣチップを用いた金融機能実行の認証に用いられるＰＩＮを提供するＰＩＮ提供部と、
前記ＩＣチップに対する最初の活性化時に、外部端末が前記ＩＣチップに最初にアクセスする場合、前記ＰＩＮ提供部に提供されるＰＩＮを前記外部端末に送信する入出力インタフェースと、
前記ＩＣチップを用いた金融機能実行のためにＰＩＮが入力されると、前記ＰＩＮ提供部に提供されたＰＩＮと前記入力されたＰＩＮとを比較して前記入力されたＰＩＮを認証し、前記入力されたＰＩＮが予め指定された回数以上エラーが入力されると前記ＩＣチップのアクセスを遮断する認証部と、
前記ＩＣチップに対する最初アクセスで前記ＰＩＮが前記入出力インタフェースを介して外部に提供されると、前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断する遮断部と、
を備える、ＩＣチップ。
【請求項１３】
前記遮断部は、
少なくとも１つのフューズ及び前記少なくとも１つのフューズそれぞれに、前記少なくとも１つのフューズをメルティングされるように臨界電流以上の電流である過電流を印加できる少なくとも１つのスイッチを含み、
前記少なくとも１つのスイッチは、前記ＩＣチップに対する前記最初アクセスで前記ＰＩＮが前記入出力インタフェースを介して外部に提供されると、前記少なくとも１つのフューズに前記過電流を印加して前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断する、請求項１２に記載のＩＣチップ。
【請求項１４】
金融機能を行うＩＣチップを認証する方法において、前記ＩＣチップが行うステップは、
金融機能を行うとき認証のためのＰＩＮを提供するステップと、
前記提供されたＰＩＮを、前記ＩＣチップに対する最初の活性化時に、前記ＩＣチップに最初にアクセスする時に前記ＩＣチップの外部に送信するステップと、
前記ＰＩＮの抽出を物理的に遮断するステップと、
前記提供されたＰＩＮとユーザから受信されたＰＩＮとを比較し、前記ユーザから受信されたＰＩＮが前記提供されたＰＩＮと一致する場合、前記ＩＣチップの使用を認証するステップと、　を含む、ＩＣチップ認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）チップの使用において、認証手段となる識別キー、例えば、ＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）の露出を根本的に遮断することのできるＩＣチップと前記ＩＣチップを認証する方法に関する。
【０００２】
より特定的に、本発明の実施形態は、スマートカードを活性化させる過程及び／又は金融決済を行う過程における認証に関し、カードを活性化した後には外部でのカード内にある識別情報、例えば、ＰＩＮにアクセスすることを不可能にする技術に関する。
【背景技術】
【０００３】
最近、クレジットカードのスマートカードなどの金融機能を有するＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）チップはその使用が便利であり、次第に現金を代替する手段として用いられている。
【０００４】

しかし、使用の便利性にもかかわらず、このような金融機能を有するＩＣチップは、物理的なカード複製やカード番号のハッキングなどによる事故が頻繁に報告されており、本人確認の過程を信頼性高く行うことが求められている。

【０００５】

このような本人確認の過程は、頻繁に、時点にユーザ個人の固有情報であるＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を確認するもので行われるが、このＰＩＮは、特定ユーザの本人確認のためのほぼ唯一の認証道具であるにもかかわらず、金融機関サーバのハッキングなどによるＰＩＮ自体の露出によって無力化される危険があった。

【０００６】

一方、韓国公開番号１０－２００７－００８４３５１「セキュリティセンサチップ」には、物理的パラメータに関するデジタル情報を記録するためにセンサチップにＣＰＵＦ（Ｃｏｎｔｒｏｌｌｅｄ　Ｐｈｙｓｉｃａｌ　Ｒａｎｄｏｍ　Ｆｕｎｃｔｉｏｎ）コーディング形態にＣＰＵＦが提供されることが記載されているが、これをクレジットカードに適用するとしても、金融機関サーバのハッキングなどによるＰＩＮ自体の露出危険から自由になれない。

【０００７】

例えば、従来のようにクレジットカード会社などの金融機関がＰＩＮを特定ユーザに発給し、金融機関が保管した後ユーザの時点にユーザが金融機関から発給されたＰＩＮを正確に入力する場合に認証を行えば、セキュリティ攻撃によって露出したＰＩＮによる不正使用に対して、金融機関は責任の免除を受けられなかった。

【０００８】

このように、従来のＰＩＮ発給及び管理方式によると、金融機関によるハッキング攻撃などのセキュリティ事故によるＰＩＮの露出危険があった。

【発明の概要】

【発明が解決しようとする課題】

【０００９】

金融機能のあるＩＣチップに対して使用されるＰＩＮがユーザ以外の他人に流出されることを基本的に防止できるＩＣチップ及びこれを用いた認証方法が提供される。

【００１０】

金融機関がユーザにＰＩＮを発給せず、ＰＩＮはＩＣチップ、すなわち、スマートカードそのものに保管され、ＰＩＮ露出に対して金融機関が責任を負わないように管理されるＩＣチップ及びこれを用いた認証方法が提供される。

【００１１】

ＰＩＮがＩＣチップ内に保管されて外部に流出されないことによって、ＩＣチップの金融時にＰＩＮをオンラインに送信する必要がないＩＣチップ及びこれを用いた認証方法が提供される。

【課題を解決するための手段】

【００１２】

金融機能を行うＩＣチップは、前記ＩＣチップを用いた金融機能を行うとき認証に用いられるＰＩＮを提供するＰＩＮ提供部と、前記ＰＩＮを前記ＩＣチップの外部に送信する入出力インタフェースと、前記ＩＣチップに対する最初アクセスで前記ＰＩＮが前記入出力インタフェースを介して外部に提供されると、前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断する遮断部とを備える。

【００１３】

一実施形態によると、前記遮断部は、少なくとも１つのフューズ及び前記少なくとも１つのフューズそれぞれに過電流（前記過電流は、前記少なくとも１つのフューズをメルティングされるように臨界電流以上の電流である）を印加できる少なくとも１つのスイッチを含み、前記少なくとも１つのスイッチは、前記ＩＣチップに対する前記最初アクセスで前記ＰＩＮが前記入出力インタフェースを介して外部に提供されると、前記少なくとも１

つのフューズに前記過電流を印加して前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断してもよい。

【００１４】

他の実施形態によると、前記ＰＩＮ提供部は、半導体製造工程偏差を用いて前記ＰＩＮを提供するＰＵＦ（Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ）を含んでもよい。

【００１５】

更なる実施形態によると、前記ＰＩＮ提供部が提供したＰＩＮとユーザから受信されたＰＩＮとを比較し、前記ユーザから受信されたＰＩＮが前記ＰＩＮ提供部が提供したＰＩＮと一致する場合に前記ＩＣチップの使用を認証する認証部をさらに備えてもよい。

【００１６】

更なる実施形態によると、前記認証部は、前記ＰＩＮ提供部に提供されたＰＩＮを暗号化して格納し、前記ユーザから受信されたＰＩＮを暗号化し、前記暗号化されて格納されたＰＩＮと比較することによって一致する場合に前記ＩＣチップの使用を認証してもよい。

【００１７】

更なる実施形態によると、前記ＰＩＮ提供部で提供されたＰＩＮと前記ＩＣチップに含まれてユーザから受信されたＰＩＮの認証のための別途のＰＩＮに基づいて前記ＩＣチップの使用を認証する認証部をさらに備えてもよい。

【００１８】

更なる実施形態によると、前記ＰＩＮ提供部は、予め入力されたＰＩＮを格納して前記格納されたＰＩＮを前記ＩＣチップを用いた金融機能実行の認証に用いられるＰＩＮとして提供してもよい。

【００１９】

金融機能を行うＩＣチップは、前記ＩＣチップを用いた金融機能実行の認証に用いられるＰＩＮを格納するＰＩＮ提供部と、外部端末が前記ＩＣチップにアクセスする場合、前記ＰＩＮ提供部に格納されたＰＩＮを前記外部端末に送信する入出力インタフェースと、前記外部端末から制御信号を受信する場合、前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断する遮断部とを備える。

【００２０】

金融機能を行うＩＣチップの活性化を行う端末装置は、前記ＩＣチップの入出力インタフェースを介して前記ＩＣチップのＰＩＮ提供部にアクセスし、前記ＰＩＮ提供部が提供する前記ＩＣチップのＰＩＮを判読して出力し、前記ＩＣチップのＰＩＮ提供部と前記ＩＣチップの入出力インタフェースとの間の遮断部に制御信号及び電流を印加し、前記ＩＣチップのＰＩＮ提供部と前記ＩＣチップの入出力インタフェースとの間の電気的な接続を遮断する。

【００２１】

ただし、前記電気的な接続遮断を行う物理的な主体は前記端末装置であってもよく、前記ＩＣチップ内または共に配置される周辺機器（ｐｅｒｉｐｈｅｒａｌ）回路のうち少なくとも一部であってもよく、以下はこのような電気的な接続遮断を行う主体に対して別の言及がなくても前記端末によって行われるものとしてのみ限定的に解釈されることはない。

【００２２】

金融機能を行うＩＣチップは、前記ＩＣチップを用いた金融機能実行の認証に用いられるＰＩＮを提供するＰＩＮ提供部と、外部端末が前記ＩＣチップにアクセスする場合、前記ＰＩＮ提供部に提供されるＰＩＮを前記外部端末に送信する入出力インタフェースと、前記ＩＣチップを用いた金融機能実行のためにＰＩＮが入力されると、前記ＰＩＮ提供部に提供されたＰＩＮと前記入力されたＰＩＮとを比較して前記入力されたＰＩＮを認証し、前記入力されたＰＩＮが予め指定された回数以上エラーが入力されると前記ＩＣチップのアクセスを遮断する認証部と、前記ＩＣチップに対する最初アクセスで前記ＰＩＮが前

記入出力インタフェースを介して外部に提供されると、前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断する遮断部とを備える。

【００２３】

金融機能を行うＩＣチップを認証する方法において、前記ＩＣチップが行うステップは、金融機能を行うとき認証のためのＰＩＮを提供するステップと、前記提供されたＰＩＮを前記ＩＣチップに対する最初アクセス時に前記ＩＣチップの外部に送信するステップと、前記ＰＩＮの抽出を物理的に遮断するステップと、前記提供されたＰＩＮとユーザから受信されたＰＩＮとを比較し、前記ユーザから受信されたＰＩＮが前記提供されたＰＩＮと一致する場合、前記ＩＣチップの使用を認証するステップとを含む。

【発明の効果】

【００２４】

金融機能ＩＣチップを用いて実行することにおいて、本人確認のためのＰＩＮをクレジットカード会社などの金融機関が保管しないため、金融機関に対するハッキングなどのセキュリティ攻撃にユーザのＰＩＮ露出を根本的に遮断することができる。

【００２５】

したがって、金融機関は、ＰＩＮの露出によるカードの不正使用に対して免責主張することができる。

【図面の簡単な説明】

【００２６】

【図１】本発明の一実施形態において識別キー漏れを防止するＩＣチップを説明するための概念図である。

【図２】本発明の一実施形態においてＩＣチップの構成を示すブロック図である。

【図３】本発明の一実施形態においてＩＣチップに含まれる遮断部の動作を説明するための回路図である。

【図４】本発明の一実施形態においてＩＣチップに含まれる遮断部の動作を説明するための回路図である。

【図５】本発明の一実施形態においてＩＣチップに含まれる遮断部の動作を説明するための回路図である。

【図６】本発明の一実施形態においてＩＣチップに含まれる遮断部の動作を説明するための回路図である。

【図７】本発明の一実施形態においてＩＣ認証方法を説明するためのフローチャートである。

【発明を実施するための形態】

【００２７】

以下、本発明の実施形態について添付の図面を参照しながら詳細に説明する。

【００２８】

図１は、本発明の一実施形態において、識別キー漏れを防止するＩＣチップを説明するための概念図である。

【００２９】

図面を参照すると、本発明に係るＩＣチップは、信用などの金融機能を行うスマートカード１００などに含まれてもよい。前記ＩＣチップは、信用決済に使用するために値が変わらない乱数（ｔｉｍｅ　ｉｎｖａｒｉａｎｔ　ｒａｎｄｏｍ　ｎｕｍｂｅｒ）形態の識別キー（Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｋｅｙ）例えば、ＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を提供することができるが、そのために一例として、前記ＩＣチップは回路構成によって前記ＰＩＮを提供するＰＵＦ（Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ）を含んでもよい。

【００３０】

ＰＵＦは、半導体工程の工程偏差を用いたデジタル機器の複製防止技術のうちの１つとして、同一の回路であっても回路を実現する工程によって線路遅延（ｗｉｒｅ　ｄｅｌａｙ）、ゲート遅延（ｇａｔｅ　ｄｅｌａｙ）などが異なるという点を用いて固有のデジタ

ル値を取得する技術である。このようなＰＵＦを用いてＰＩＮを提供する場合、ＰＵＦは同一の半導体素子の配列に過ぎないため、他人がスマートカード１００を所持又は習得するとしても、ＩＣチップからＰＩＮを識別することができないためＰＩＮの流出を未然に防止することができる。

【００３１】

一方、前記ＩＣチップはユーザが金融機関ＡＴＭ１１０などのような端末装置で活性化する場合、最初の活性化時にのみＰＩＮを前記端末装置に伝達する。端末装置に送信されたＰＩＮは、例えば、前記端末装置のディスプレイ部を通したディスプレイ、別途のプリントアウトなどの方法によってユーザに出力されてもよい。この場合、前記端末装置は前記ＰＩＮの提供や保管にいずれの役割を行わず、単に前記活性化過程の後に前記ＩＣチップが使用可能な状態（Ａｃｔｉｖａｔｅｄ）になるようにし、前記提供されたＰＩＮを単にユーザへ伝達（Ｂｙｐａｓｓ）する役割のみを行う。

【００３２】

このようにユーザに伝えられたＰＩＮは前記ユーザのみが記憶したり保管し、本発明の一側に係る前記ＩＣチップは、前記最初のアクセス後のいかなる外部アクセスにもＰＩＮを提供しないようにＰＩＮを提供するパス（Ｐａｔｈ）を物理的及び／又は論理的に完全遮断（ｃｕｔ　ｏｒ　ｉｓｏｌａｔｅ）する。

【００３３】

そのためにＩＣチップは、例えば、少なくとも１つのフューズ及び少なくとも１つのスイッチを含んでもよいが、この場合、前記ＰＩＮに対する最初のアクセス後には前記少なくとも１つのスイッチによって前記フューズに過電流を印加して前記少なくとも１つのフューズを切ることによって、物理的に前記ＰＩＮに対する外部のアクセスを遮断することができる。

【００３４】

一方、他の実施形態として、前記ＰＩＮに対する外部のアクセス遮断を金融機関ＡＴＭ１１０などの端末装置が行ってもよい。すなわち、前記端末装置は、前記ＩＣチップの入出力インタフェースを介して前記ＩＣチップにアクセスして前記ＩＣチップのＰＩＮを読み出して出力すると、前記ＩＣチップのＰＩＮ提供部と前記ＩＣチップの入出力インタフェースとの間の遮断部に制御信号及び電流を印加し、前記ＩＣチップのＰＩＮ提供部と前記ＩＣチップの入出力インタフェースとの間の電気的な接続を遮断してもよい。

【００３５】

その後、前記端末装置は、ネットワーク１０１を用いて前記ＩＣチップが含まれたスマートカード１００の発給を金融機関サーバ１２０に通知することによって、前記発給されたスマートカード１００が加盟店端末１３０を通して一般的なカード機能を行うことができるようにする。

【００３６】

この場合、前記金融機関サーバ１２０は、前記ＩＣチップで提供されるＰＩＮを別途のサーバに格納したり、前記ユーザ以外のいかなる第３者にも提供しない。したがって、金融機関サーバに対するハッキングなどのセキュリティ攻撃にユーザＰＩＮの露出が根本的に遮断されるため、金融機関はＰＩＮの露出によるカードの不正使用に対して免責を主張することができる。

【００３７】

一方、本発明の一実施形態によると、前記ＩＣチップは前記スマートカード１００の使用を認証するために前記活性化後にユーザが前記ＩＣチップを用いるために入力するＰＩＮが前記ＩＣチップに対して提供されたＰＩＮと一致するか否かを判断する。この場合、前記ＩＣチップに対して提供されたＰＩＮは暗号化されて保管されているため、前記ユーザが入力するＰＩＮが一致するか否かを認証する過程は、前記入力されたＰＩＮを暗号化した後に行われてもよい。

【００３８】

図２は、本発明の一実施形態においてＩＣチップの構成を示すブロック図である。以下

、図２を参照して本発明のＩＣチップの構成及び機能を詳細に説明する。
【００３９】
スマートカード１００のＩＣチップは、ＰＩＮ提供部２１０、入出力インタフェース２２０、遮断部２３０及び認証部２４０を備える。
【００４０】
ＰＩＮ提供部２１０はＰＩＮを提供する役割を行うものとして、上述したようにＰＵＦを用いて前記ＩＣチップを用いた金融機能を行うとき認証に用いられるＰＩＮを提供する。しかし、前記ＰＩＮ提供部２１０はこれに限定されることなく、当業者の要求に応じて予め入力されたＰＩＮを格納してから前記格納されたＰＩＮを前記ＩＣチップを用いた金融機能実行の認証に用いられるＰＩＮとして提供するものとして実現されてもよい。例えば、前記ＰＩＮ提供部２１０は、ＥＥＰＲＯＭなどのような不揮発性メモリとして実現されてもよい。この場合、前記スマートカード１００は、ＥＥＰＲＯＭなどに乱数として提供されたＰＩＮを格納してから外部入力ＰＩＮとしてユーザに提供し、ユーザから入力されたＰＩＮと前記ＥＥＰＲＯＭなどに格納されたＰＩＮとを比較してユーザを認証してもよい。
【００４１】
入出力インタフェース２２０は、前記ＰＩＮ提供部２１０で提供されるＰＩＮをＩＣチップに対する最初のアクセス時に前記ＩＣチップの外部へ送信する。
【００４２】
本発明の一実施形態に係る遮断部２３０は、前記ＰＩＮ提供部２１０と前記入出力インタフェース２２０との間に位置し、前記ＩＣチップに対する最初アクセスで前記ＰＩＮが前記入出力インタフェース２２０を介して外部端末に提供されると、前記ＰＩＮ提供部２１０と前記入出力インタフェース２２０との間を物理的に遮断する。
【００４３】
したがって、ＰＩＮ提供部２１０がＰＵＦを含んでＰＩＮを提供する場合、スマートカード１００内にはＰＩＮがハードウェア的にのみ存在し、その後は永久的にＰＩＮの抽出が不可能になる。
【００４４】
一方、一実施形態に係る前記遮断部２３０は、少なくとも１つのフューズ及び前記少なくとも１つのフューズそれぞれに過電流を印加できる少なくとも１つのスイッチを含んでもよい。ここで、前記過電流は、少なくとも１つのフューズをメルティングすることのできる臨界電流以上の電流であってもよい。
【００４５】
この場合、少なくとも１つのスイッチは、前記ＩＣチップに対する最初アクセスで前記ＰＩＮが前記入出力インタフェース２２０を介して外部に提供されると、少なくとも１つのフューズに前記過電流を印加して前記ＰＩＮ提供部と前記入出力インタフェースとの間を物理的に遮断する。このような遮断部２３０の具体的な構成について、後述する図３～図６を参照して詳細に説明することにする。
【００４６】
認証部２４０は、金融機関ＡＴＭのような外部端末装置から入出力インタフェース２２０を介してユーザが入力したＰＩＮを受信すると、前記ＰＩＮ提供部２１０が提供したＰＩＮとユーザから受信されたＰＩＮとを比較し、前記ユーザから受信されたＰＩＮが、前記ＰＩＮ提供部２１０が提供したＰＩＮと一致する場合に前記ＩＣチップの使用を認証する。
【００４７】
ここで、一実施形態として前記認証部２４０は、ＰＩＮ提供部２１０で提供されたＰＩＮを暗号化して格納し、ユーザから受信されたＰＩＮを暗号化して前記暗号化して格納されたＰＩＮと比較することで、一致する場合に前記ＩＣチップの使用を認証する。
【００４８】
この場合、認証部２４０に格納されるＰＩＮは暗号化アルゴリズムを介して暗号化され

るため、ユーザが入力したＰＩＮが前記暗号化して格納されたＰＩＮと同じＰＩＮであることを認証できるものの、暗号化されたＰＩＮに基づいて本来の、すなわち、暗号化される前のＰＩＮを把握することは基本的に不可能である。したがって、スマートカード１００を習得又は所持した者が認証部２４０に格納された暗号化されたＰＩＮを抽出するとしても、暗号化されたＰＩＮを用いてスマートカード１００を使用することは不可能である。

【００４９】

一方、他の実施形態として前記認証部２４０は、前記ＰＩＮ提供部２１０で提供されたＰＩＮと前記ＩＣチップに含まれてユーザから受信されたＰＩＮの認証のための別途のＰＩＮに基づいて前記ＩＣの使用を認証してもよい。例えば、ＰＩＮ提供部２１０は、第１ＰＵＦ及び第２ＰＵＦを含んでもよい。この場合、第１ＰＵＦで提供されるＰＩＮを金融機能の実行時に外部入力ＰＩＮとして使用し、前記第１ＰＵＦで提供されるＰＩＮと第２ＰＵＦで提供されるＰＩＮを連動させた値を前記ＩＣチップを認証するための最終ＰＩＮとして使用してもよい。この場合、前記第２ＰＵＦで提供されるＰＩＮはどのような方法でも外部から抽出できず、前記第１ＰＵＦで提供されるＰＩＮとの排他的論理和（ＸＯＲ；Ｅｘｃｌｕｓｉｖｅ　ＯＲ）ゲートによって前記ＩＣチップの使用を認証するよう実現される。したがって、ユーザの不注意などにより第１ＰＵＦで提供されるＰＩＮが漏れても最終ＰＩＮを複製することは不可能である。

【００５０】

その後、認証部２４０はユーザから入力されたＰＩＮが認証されると、ユーザから入力されたスマートカード１１０に含まれる一般的なカードの機能を行うことができるようにする。しかし、前記ＰＩＮが予め指定された回数以上エラーが入力されると、認証部２４０は、前記ＩＣチップのアクセスを遮断することによってスマートカード１１０を使用できないようにする。

【００５１】

以下、図３～図６を参照して本発明の一実施形態においてＩＣチップに含まれる遮断部の動作をより具体的に説明する。

【００５２】

まず、図３を参照すると、遮断部２３０は、ＰＩＮ提供部２１０と入出力インタフェース２２０との間に位置し、少なくとも１つのフューズ及び少なくとも１つのスイッチを含んでもよい。図３では、一実施形態で１つのフューズ及び４個のスイッチで遮断部２３０を構成するものと図示されているが、前記フューズ及びスイッチの数又は位置は当業者の要求に応じて変形実施されてもよい。

【００５３】

遮断部２３０は、ＩＣチップに対する最初アクセス（例えば、スマートカードの発給など）時に各スイッチを制御することによって、ＰＩＮ提供部２１０で提供されるＰＩＮが入出力インタフェース２２０を介して外部に送信されるようにする。そして、前記ＰＩＮが外部に送信されると、前記それぞれのスイッチを制御することによって電源（ｖｄｄ）により回路に過電流が流れるようにし、前記フューズをメルティングすることによって前記ＰＩＮ提供部２１０と前記入出力インタフェース２２０との間を物理的に遮断してもよい。

【００５４】

一方、前記遮断部２３０は、外部端末から制御信号を受信される場合、前記制御信号に基づいて前記それぞれのスイッチを制御することによって前記フューズに過電流が流れるようにし、前記ＰＩＮ提供部２１０と前記入出力インタフェース２２０との間を物理的に遮断してもよい。

【００５５】

図４は、第１スイッチ及び第２スイッチを閉鎖することによってＰＩＮ提供部２１０で提供されるＰＩＮが入出力インタフェース２２０に送信されることを示し、図５は、第３スイッチ及び第４スイッチを閉鎖閉することによってフューズに過電流が流れることを示

す。
【００５６】
遮断部２３０は、制御信号を生成したり外部端末から受信して前記制御信号に基づいてＰＩＮ提供部２１０のＰＩＮを外部に提供したり前記ＰＩＮが外部に提供されることを遮断してもよい。一例として、図４に示すように、前記制御信号として「１」が印加されると、第１スイッチ及び第２スイッチは閉鎖されてもよく、第３スイッチ及び第４スイッチは開放されてもよい。したがって、ＰＩＮ提供部２１０で提供されるＰＩＮが入出力インタフェース２２０を介して外部端末に送信されてもよい。
【００５７】
しかし、これに対して図５に示すように、前記制御信号として「０」が印加されると前記第１スイッチ及び第２スイッチは開放されてもよく、第３スイッチ及び第４スイッチは閉鎖されてもよい。したがって、前記フューズには過電流が流れ、図６に示すように、再び第１スイッチ及び第２スイッチが閉鎖されてもメルティングされたフューズによって前記ＰＩＮ提供部２１０と前記入出力インタフェース２２０との間が途切れることによって、外部にＰＩＮが送信されることを物理的に完全に遮断することができる。
【００５８】
以下、図７を参照して本発明の一実施形態においてＩＣ認証方法を説明する。
【００５９】
ユーザが外部端末装置を用いてＩＣチップが含まれたスマートカードを発給する場合、前記ＩＣチップに対する最初アクセス時に、ＰＩＮ提供部で生成又は格納（本明細書ではこのような「生成」及び／又は「格納」を「提供」のように表現したりもする）されたＰＩＮが入出力インタフェースを介して外部端末装置に送信されると（Ｓ７１０）、前記外部端末装置は、受信したＰＩＮをディスプレイ部を介してディスプレイしたり別途のプリントアウトなどの方法によってユーザに出力する。
【００６０】
そして、前記ＩＣチップの遮断部は、ＰＩＮ提供部と入出力インタフェースとの間を遮断することによって前記ＰＩＮの抽出を物理的に遮断する（Ｓ７２０）。
【００６１】
このような方法で登録されたスマートカードをユーザが用いる場合、ユーザが加盟店端末などを用いてＰＩＮを入力すると（Ｓ７３０）、ＩＣチップの認証部は、ユーザから受信したＰＩＮと前記認証部に格納されたＰＩＮとが一致するか否かを判断してＰＩＮを認証する（Ｓ７４０）。ここで、前記認証部に格納されたＰＩＮが暗号化して格納されている場合には、ユーザから入力されたＰＩＮを暗号化した後、前記暗号化して格納されたＰＩＮと比較することによって一致するか否かを判断する。
【００６２】
その後、認証部はＰＩＮが一致すると判断される場合、スマートカードと外部インタフェースを接続し（Ｓ７５０）、ユーザが前記スマートカードを用いて金融機能を行うことができるようにする。
【００６３】
しかし、ユーザが入力したＰＩＮが予め指定された回数、例えば、３回以上エラーが入力されると（Ｓ７６０）、認証部はＩＣチップのアクセスを遮断することによってＩＣチップを非活性化させる。
【００６４】
上述したような識別キー漏れを防止するＩＣチップ及びこの認証方法はスマートカードの認証に使用されるものとして限定されることなく、Ｍｉｃｒｏ　ＳＤ、ＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）カード、クレジットカードなどの認証にも用いられてもよく、さらに、ユーザ識別及び認証に必要な様々な形態のデジタル技術分野で用いられてもよい。
【００６５】
また、識別キー漏れを防止するＩＣチップ及びこの認証方法は、従来のクレジットカー

ドや現金カードなどのためのスマートカードチップを活性化させるゲートとして活用されてもよい。この場合、従来の金融決済システムの使用方法を全く修正することなく、本発明に係る識別キー漏れを防止するＩＣチップの認証方法を用いてもよい。例えば、本発明に係る識別キー漏れを防止するＩＣチップがスマートカードの使用時に優先的にユーザ認証手続を行い、ユーザ認証に失敗するとエラーメッセージを出力し、ユーザ認証が成功するとスマートカードを活性化させることでインタフェース信号をバイパスできる。

【００６６】

また、本発明に係る識別キー漏れを防止するＩＣチップ及びこの認証方法は、ユーザ認証をＩＣチップが行うことによってＰＩＮをクレジットカード会社などの金融機関が保管しないため、金融機関に対するハッキングなどのセキュリティ攻撃にもユーザのＰＩＮの露出が根本的に遮断される効果があるだけではなく、金融機関はＰＩＮの露出によるカードの不正使用に対して免責主張することができる。

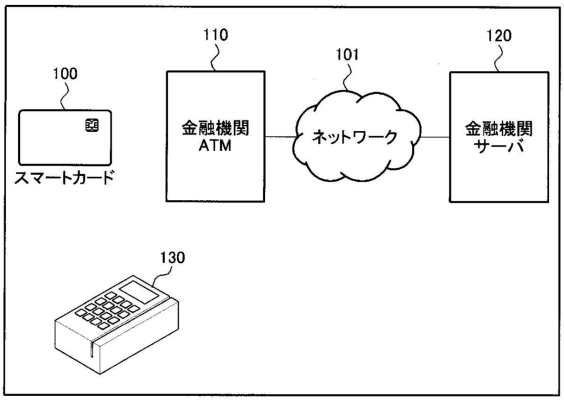
【００６７】

上述したように本発明を限定された実施形態と図面によって説明したが、本発明は、上記の実施形態に限定されることなく、本発明が属する分野における通常の知識を有する者であれば、このような実施形態から多様な修正及び変形が可能である。

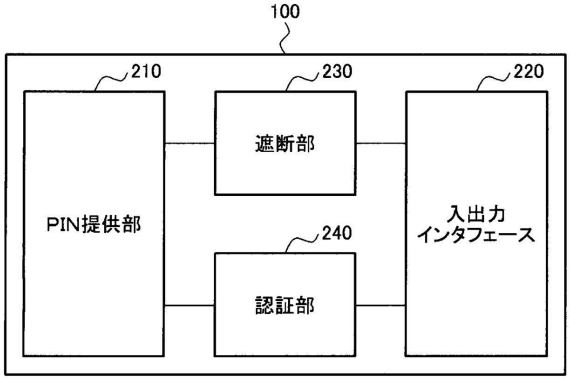
【００６８】

したがって、本発明の範囲は、開示された実施形態に限定されて定められるものではなく、特許請求の範囲だけではなく特許請求の範囲と均等なものなどによって定められるものである。

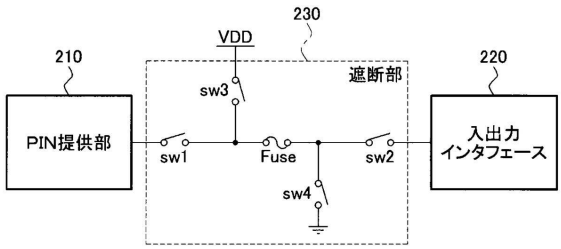
【図１】



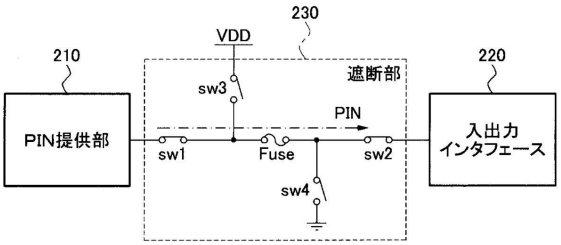
【図２】



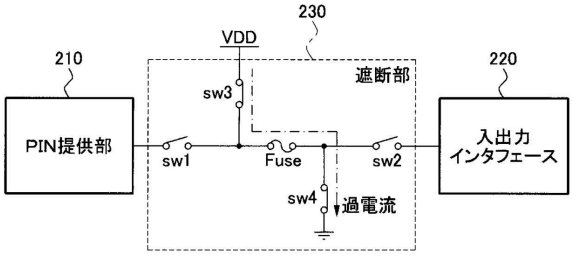
【図３】



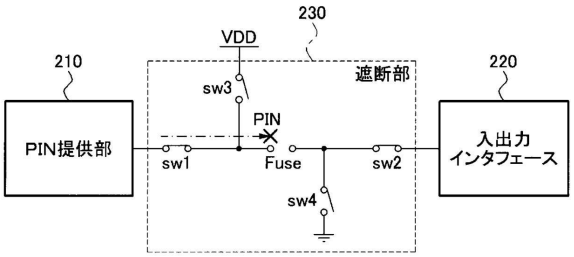
【図４】



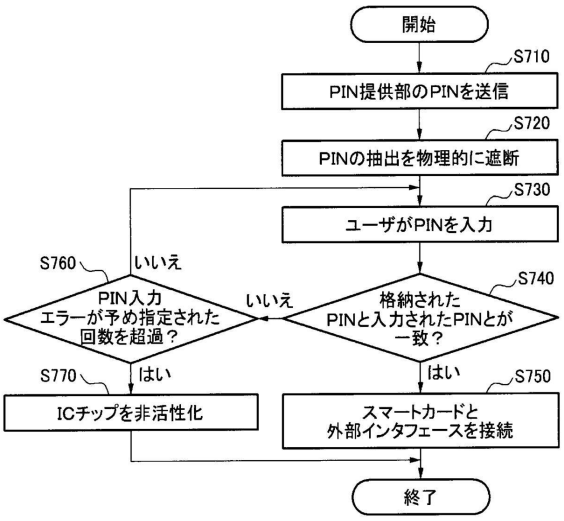
【図５】


230
VDD
210
遮断部
sw3
220
PIN提供部
sw1
Fuse
sw2
入出力
インタフェース
sw4
過電流

【図６】


230
VDD
210
遮断部
sw3
220
PIN
PIN提供部
sw1
Fuse
sw2
入出力
インタフェース
sw4

【図７】


開始
S710
PIN提供部のPINを送信
S720
PINの抽出を物理的に遮断
S730
ユーザがPINを入力
S740
格納された
PINと入力されたPINとが
一致？
いいえ
はい
S760
PIN入力
エラーが予め指定された
回数を超過？
いいえ
はい
S770
ICチップを非活性化
S750
スマートカードと
外部インタフェースを接続
終了

フロントページの続き

(72)発明者 チョイ ビョン デク
大韓民国 １３４－８４０ ソウル市 カントン区 ソンネ ２－ドン ７７－５
(72)発明者 キム ドン ヒュン
大韓民国 ４４８－１３０ キョンギ道 ヨンイン市 スジ区 サンヒョン－ドン ８２４－１２ サンギョン マウル サンギョン アパート ナンバー １７６－１２０１
(72)発明者 パク サン セン
大韓民国 ４６３－７５１ キョンギ道 ソンナム市 ブンダン区 チョンジャン－ドン チョンジャン マウル ドンガ アパート ナンバー ２０８－１０２
(72)発明者 ジ クァン ヒュン
大韓民国 ４７１－７１６ キョンギ道 クリ市 キョムン ２－ドン ハナ アパート ナンバー ２０５－１６０３

審査官 青木 重徳

(56)参考文献 特開平０４－２５８８９８（ＪＰ，Ａ）
特開２００３－３０３３０９（ＪＰ，Ａ）
特開２００６－０３１５７６（ＪＰ，Ａ）
国際公開第２０１０／０３５２０２（WO，Ａ１）
登録実用新案第３１６０５５４（ＪＰ，Ｕ）
中国特許出願公開第１０１８５４３５７（ＣＮ，Ａ）
楫 勇一 ほか，パスワード事前宣言による個人認証法－磁気カードを用いた安全な個人認証法，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会［オンライン］，１９９５年１２月１５日，Ｖｏｌ．９５，Ｎｏ．４２３，ｐ．２１－２８，［平成２６年 2月２４日検索］，インターネット，ＵＲＬ，<http://ci.nii.ac.jp/els/110003297047.pdf?id=ART0003723813&type=pdf&lang=jp&host=cinii&order_no=&ppv_type=0&lang_sw=&no=1393216512&cp=>
D. W. Davies and W. L. Price 著／上園 忠弘 監訳，ネットワーク・セキュリティ，日本，日経マグロウヒル社，１９８５年１２月 5日，1版1刷，ｐ．２６６－２７０

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／１０
Ｇ０６Ｆ ２１／７９
Ｈ０４Ｌ ９／３２