

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4532476号
(P4532476)

(45) 発行日 平成22年8月25日 (2010. 8. 25)

(24) 登録日 平成22年6月18日 (2010. 6. 18)

(51) Int. Cl.	F I
G06K 17/00 (2006.01)	G06K 17/00 E
G06F 3/02 (2006.01)	G06F 3/02 320A

請求項の数 12 (全 9 頁)

(21) 出願番号	特願2006-508474 (P2006-508474)	(73) 特許権者	507219491
(86) (22) 出願日	平成16年5月28日 (2004. 5. 28)		エヌエックスピー ビー ヴィ
(65) 公表番号	特表2006-526836 (P2006-526836A)		NXP B. V.
(43) 公表日	平成18年11月24日 (2006. 11. 24)		オランダ国 5656エイジー アインド
(86) 国際出願番号	PCT/IB2004/050804		ーフエン ハイ テク キャンパス 60
(87) 国際公開番号	W02004/107255		High Tech Campus 60
(87) 国際公開日	平成16年12月9日 (2004. 12. 9)		, NL-5656 AG Eindhoven,
審査請求日	平成19年5月25日 (2007. 5. 25)		Netherlands
(31) 優先権主張番号	03101610.8	(74) 代理人	100147485
(32) 優先日	平成15年6月3日 (2003. 6. 3)		弁理士 杉村 憲司
(33) 優先権主張国	欧州特許庁 (EP)	(74) 代理人	100134005
			弁理士 澤田 達也

最終頁に続く

(54) 【発明の名称】 セキュアカード端末

(57) 【特許請求の範囲】

【請求項 1】

英数字データを入力するためのキーパッドと、キー信号を生成するための関連キーパッドマトリックスとを有する端末であって、スマートカードと通信することができる当該端末を使用して、前記スマートカードに前記英数字データを供給する方法において、

前記キー信号を生成するために、走査シーケンスを使用していかなるプレスされたキーに対しても前記キーパッドマトリックスを走査するステップを含み、前記走査シーケンスが前記スマートカードによって決定され、新たなセットのデータが前記キーパッドに入力されるたびに、前記スマートカードが前記走査シーケンスを変更する方法。

【請求項 2】

前記スマートカードが、乱数発生器を使用して各走査シーケンスを決定する、請求項 1 に記載の方法。

【請求項 3】

いかなるキー信号も前記スマートカードのみを通される、請求項 1 又は 2 の何れか一項に記載の方法。

【請求項 4】

いかなるキー信号も前記端末のセキュア記憶素子に記憶される、請求項 1 又は 2 の何れか一項に記載の方法。

【請求項 5】

前記端末がユーザ制御及び／又はスマートカード制御の下で入力されるプロテクトモー

10

20

ドにある場合、前記走査シーケンスが前記スマートカードによってのみ決定される、請求項1乃至4の何れか一項に記載の方法。

【請求項6】

スマートカードを入れるための端末であって、

前記スマートカードと通信するためのスマートカードポートと、英数字コードを入力するためのキーボードと、前記英数字コードの文字を入力するとキー信号を生成する前記キーボードに関連するキーボードマトリックスと、を有し、

前記スマートカードによって決定される走査シーケンスを使用して、いかなるプレスされるキーに対しても前記キーボードを走査する手段を更に有し、

新たなセットのデータが前記キーパッドに入力されるたびに、前記スマートカードにより前記走査シーケンスが変更される端末。

10

【請求項7】

任意のキー信号を前記スマートカードに直接送る手段を更に有する、請求項6に記載の端末。

【請求項8】

テレビジョンセット、セットトップボックス、パーソナルデジタルアシスタント、ゲームコンソール、遠隔制御装置、モバイル電話若しくは固定電話又はDVDプレーヤで用いられる、請求項6又は7に記載の端末。

【請求項9】

スマートカード及び請求項6乃至8の何れか一項に記載の端末を有する、加入者サービス用のシステム。

20

【請求項10】

有料エンターテイメントサービス、好ましくは、有料テレビジョンサービスのためのシステムである、請求項9に記載のシステム。

【請求項11】

銀行サービスのためのシステムである、請求項9に記載のシステム。

【請求項12】

英数字データを入力するためのキーパッドと、キー信号を生成するための関連キーパッドマトリックスとを有する端末と通信するスマートカードにおいて、

当該スマートカードが、前記キー信号を生成するために、いかなるプレスされたキーに対して前記キーパッドマトリックスを走査するための走査シーケンスを決定し、且つ新たなセットのデータが前記キーパッドに入力されるたびに、前記走査シーケンスを変更するスマートカード。

30

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、セキュア（secure、暗号化）カード端末及びこのカード端末の使用に関する。より具体的には、本発明は、カード端末を使用してスマートカードに英数字データを供給する方法と、このような端末が使用される加入者サービス用のシステムと、に関する。

【背景技術】

40

【0002】

或るサービスへのアクセスを得るためにコードが入力されなければならないキーパッドを備える端末を使用することは、よく知られている。一般に、このようなコードは、ユーザを識別すべきPIN（Personal Identification Number、個人識別番号）として使用される4桁コードである。このPINコードは、更に、端末に挿入されているスマートカードへのアクセスを得るために使用され得る。このアクセスは認定ユーザのみに制限されなければならないので、このコードは秘密に保たれなければならない。しかしながら、端末へのソフトウェア攻撃により、ユーザによって入力されたコードを検出し、記憶することができることが分かっている。これが極めて望ましくないことは明らかである。なぜならば、これは攻撃者が、可能性として銀行サービスを含む制限されたサービスへのアクセ

50

スを不正に得ることを可能にするからである。

【0003】

端末のキーパッド（又はキーボード）は、通常、一つの導体が各行に対応する行導体のセットと、一つの導体が各列に対応する列導体のセットと、から構成される関連キーパッドマトリックスをもつ。個別のキーがプレスされる場合、電氣的接続がそのキーの行導体と列導体との間に形成され、このキーパッドマトリックスが「キープレス（"keypressed"）」信号を生成する。その場合、このプレスされた個別のキーは、キーパッドマトリックスの行及び列を走査し、どの行及び列に特定の信号が存在するのかを決定することによって、識別される。このような特定の信号は、キーをプレスすることにより行導体と列導体との間に作られた電氣的接触によって、もたらされる。

10

【0004】

行及び列のこの走査は、通常、キーボードコントローラによって実施され、このコントローラは、この目的のために、走査プロセス中に行番号及び列番号を生成するカウンタを備えていてもよい。キーボードコントローラが端末の一部であり、端末上でランするアプリケーションによってアクセスされるので、疑わしい（compromised）端末は、キーシーケンス及び関連入力データを決定し、これらを第三者に伝送するか、又は端末の所有者によって承認されない使用に関するデータを保持する（retain, 留めておく）ことができる。

【0005】

米国特許第6, 056, 193号明細書は、一体的なスマートカードリーダを備えるコンピュータキーボードを開示する。このキーボードは、パーソナルコンピュータに接続される。PIN入力モードにおいて、スイッチは、キーボードコントローラからキーを切断し、これらのキーをセキュリティモジュール、即ち、専用プロセッサに接続する。このセキュリティモジュールが、キーボードマトリックスを制御するので、いかなるキープレスもキーボードコントローラによって検出されない。その代わりに、このマトリックスの走査ラインが、セキュリティモジュールの制御の下でこのセキュリティモジュールにリダイレクトされる（redirect, 出力先を変更される）。

20

【発明の開示】

【発明が解決しようとする課題】

【0006】

この既知の装置は、そのセキュリティ機能のために追加の専用プロセッサ、即ち、セキュリティモジュールを必要とするという欠点をもつ。この追加のプロセッサがキーボードのコスト及びサイズの双方を増すことは明らかである。それに加えて、更なる追加の構成部品であるスイッチも必要とされる。

30

【0007】

本発明の目的は、従来技術のこれら及び他の問題を克服し、端末がデータを傍受するリスクを大幅に排除する、スマートカードと関連付けられた端末にデータを入力する方法を提供することにある。

【課題を解決するための手段】

【0008】

従って、本発明は、英数字データを入力するためのキーパッドと、キー信号を生成するための関連キーパッドマトリックスとを有する端末であって、スマートカードと通信することができる当該端末を使用して、スマートカードに英数字データを供給する方法において、キー信号を生成するために、走査シーケンスを使用していかなるプレスされるキーに対してもキーパッドマトリックスを走査するステップを含み、この走査シーケンスがスマートカードによって決定される方法を提供する。

40

【0009】

キーパッドマトリックスの走査シーケンスが、端末によってではなくスマートカードによって決定されるので、この端末は走査シーケンスの情報をもっておらず、従って、どのキーがプレスされているのかを決定することはできない。

50

【0010】

好ましい実施形態において、走査シーケンスは、新たなセットのデータがキーパッドに
入力されるたびに変更される。単一のセットのデータは、例えば、一般に4桁から成るP
I Nコードによって構成されるが、3、5、6又は任意の他の適切な桁数から成って
いてもよい。新たな走査シーケンスが、各々のユーザセッションに対して、即ち、新たなユー
ザがキーパッドを使用するたびに、更に利用されることもできる。

【0011】

スマートカードによって決定される走査シーケンスが、端末によって決定される走査シ
ーケンスとは異なることが好ましいが、このことは必ずしも必要ではないことが理解され
るであろう。走査シーケンスが繰り返し変更され、端末が走査シーケンスの情報をもっ
ていない限り、その場合には、上記シーケンスは、端末によって使用されるシーケンスと同
じでもよい。

10

【0012】

好ましくは、スマートカードが、乱数発生器を使用して各々の走査シーケンスを決定す
る。これにより、疑わしい端末が、走査シーケンスをモニタし、スマートカードによって
生成された任意の過去の走査シーケンス又は今後生成されるであろう任意の将来の走査シ
ーケンスを予測するために用いられることができないことを確実にする。

【0013】

好ましくは、いかなるキー信号もスマートカードのみを通される。即ち、キー信号は端
末の回路には伝えられない。このことは、セキュリティの追加のレベルを提供する。但し
、代替の実施形態では、任意のキー信号が端末のセキュア記憶素子に記憶されてもよい。
このセキュア記憶素子は、例えば、暗号キーによりプロテクトされている制限されるアク
セスをもつレジスタであり得る。このような実施形態では、スマートカードがセキュア記
憶素子のキー信号を記憶し、この秘密（secret，シークレット）キーを端末の或る信頼で
きるソフトウェアアプリケーションにのみ供給することができる。更にセキュリティを高
めるために、キー信号は、暗号化された形態でセキュア記憶素子に記憶され得る。

20

【0014】

上記の説明から、本発明の方法では、端末自体（の制御回路）を排除するために、スマ
ートカードがキーパッドへの直接アクセスをもつことが明らかである。キーパッドマトリ
ックスは、端末がキーパッドアクションを観察するのを防止するために、端末がプロテクト
モード又は「P I Nモード」に置かれる場合、端末の回路からシールド（shield，遮蔽）
される。このシールドは、キーパッドマトリックスから端末回路を電氣的に切断するこ
とによって達成されてもよい。

30

【0015】

プロテクトモード又は「P I Nモード」は、例えば、スマートカードの存在の検出時に
、又は特定のキー、例えば、専用の「プロテクトモードキー」をプレスする場合に、アク
ティブな状態にされ得る。特定のキーをプレスすることは、P I N入力ルーチン又はデー
タをキーパッドに入力することを含んだ何らかの他のシーケンスのアクションを始動する
ことを要求する可能性がある。端末の回路は、セキュリティの理由のためハードウェアス
イッチの方が好ましいが、電子的若しくは機械的ハードウェアスイッチ又はソフトウェア
スイッチを使用して、キーパッドマトリックスから切断されることができる。

40

【0016】

従って、走査シーケンスは、端末がユーザ制御及び／又はスマートカード制御の下で入
力されるプロテクトモードにある場合、前記スマートカードによってのみ決定されることが
好ましい。

【0017】

更に、本発明は、スマートカードを入れるための端末であって、スマートカードと通信
するためのスマートカードポートと、英数字コードを入力するためのキーボードと、英数
字コードの文字を入力する際にキー信号を生成するキーボードに関連付けられるキーボ
ードマトリックスと、を有し、スマートカードによって決定される走査シーケンスを使用し

50

て、いかなるプレスされたキーに対してもキーボードを走査する手段を更に有する端末を供給する。この端末は、あらゆるキー信号をスマートカードに直接送る手段を更に有する。このようにして、端末がキー信号の情報を得ることが避けられる。

【0018】

本発明は、更に、加入者サービス用のシステムであって、少なくとも一つの端末及び少なくとも一つのスマートカードを有し、上記に規定された方法を利用するために配されるシステムを提供する。このようなシステムは、有料テレビジョンサービスのような有料エンターテイメントサービス、又は銀行サービスを提供してもよい。本発明は、更に、上記に規定された方法及びシステムに使用するためのスマートカードを供給する。

【0019】

本発明は、更に、添付の図面に示される例示的な実施形態を参照して、以下に説明される。

【発明を実施するための最良の形態】

【0020】

図1に限定されない実施例として単に示される端末1は、キーボード（キーパッド）4、スクリーン6及びカードスロット3を有している。このタイプの端末は、例えば、銀行トランザクション（transaction, 取り引き）用の預け払い機（teller machine, テラーマシン）として使用されてもよい。代替例として、この端末は、テレビジョンセット、セットトップボックス、パーソナルデジタルアシスタント（PDA）、ゲームコンソール、遠隔制御装置、モバイル（携帯）電話、ランドライン（固定）電話、DVDプレーヤ又はディスプレイ（スクリーン）及びキーボードをもつ任意の類似装置から構成されるか、又はこのような装置の一部であり得る。ディスプレイ及び／又はキーボードは、端末ハウジングに収容されなくてもよく、ワイヤードインタフェース又はワイヤレスインタフェースによって端末に接続されてもよい。

【0021】

CRTスクリーン、LCDスクリーン又は類似のディスプレイ装置であり得るスクリーン6は、ユーザにインストラクションを与え、キーパッド4の使用に関するフィードバックを供給するように役立つ。スマートカードは、スマートカードトランザクションのためにカードスロット3に挿入され得る。この目的のために、端末1はスマートカードリーダー（図3の参照符号7）を備えている。このスマートカードリーダー7は、スロット3に挿入されるカードを受け付ける（accept, アクセプトする）ことができるように、端末ハウジング内部に置かれ得る。後でより詳細に説明されるが、本発明によれば、端末1は、キーパッドマトリックスの走査が、端末1自体の制御の下ではなく、スマートカードの制御の下で実施されるように構成されている。

【0022】

例示的なスマートカードが、図2に示される。一般に、スマートカード2は、集積回路21が埋め込まれる基板を有している。印刷された又はエンボス加工されたしるし（indicia, 証印）22は、カード所有者及び／又はカード発行者を識別することができる。集積回路21は、端末1のスマートカードリーダーとの通信を可能にする接触（部）を備えている。この集積回路は、順に、プログラム及びアプリケーションデータを記憶するためのメモリ及びプロセッサを含むマイクロコンピュータを有していてもよい。

【0023】

集積回路21を有する図2のスマートカード2は、更に、内蔵キーボードコントローラを備えている。このキーボードコントローラは、別個の集積回路によって構成されてもよいが、好ましくは、集積回路21に収容される。キーボードコントローラの機能は、より詳細に図1の端末1の一部を示す図3を参照して、より詳細に説明される。

【0024】

図3において限定されない実施例によって単に示されるキーパッド4は、3個ずつのキーから成る4行に配された12個のキーを有している。キーパッドマトリックス5は、キーパッド4のどのキーをプレスしても、行の一つが、マトリックスの列の一つと電氣的に

接触するように配されている。この電氣的接触は、「キープレス」信号が生成される原因となる。このキープレス信号は、キーパッド回路51及び52によって検出され、スマートカードリーダー7によって（可能性として図3に示されない適切なスマートカードリーダーインタフェースを介して）スマートカード2にわたされる。このキープレス信号は、単にあるキーがプレスされていることを示すだけであり、どのキーがプレスされているかを示してはいないので、キーパッドマトリックス5は、その後、どの列及びどの行が、キープレス信号をもたらした電氣的な接触に関わっているのかを決定するために走査される。電氣的接触に関わり、その結果、特別な信号値を生成する、行及び列の組み合わせによって、キーが識別される。

【0025】

10

通常の端末では、端末回路は、一般に固定される走査シーケンスを決定する。キーパッド回路51及び52は、例えば、通常の端末のカウンタによって具現化されてもよく、各カウンタが、固定走査シーケンス1-2-3（列回路51）及び1-2-3-4（行回路52）をそれぞれステップスルー（step through）する。これらの走査シーケンスが固定され、端末によって決定されるので、プレスされる実際のキーは、端末回路に知られている。端末への不正なセキュリティ攻撃、例えば、ソフトウェア攻撃の場合、攻撃者は、どのキーがプレスされているのかを分かっている可能性がある。このことは、特に、上記のキープレスが、PINコードのようなシークレットコード（secret code, 暗号）を同時に形成する場合、極めて望ましくないことは明らかである。

【0026】

20

しかし、本発明によれば、キーパッドマトリックスの行及び列は、スマートカード2によって決定される走査シーケンスを使用して走査される。即ち、スマートカード2は、上記の回路51及び回路52を介してキーボードマトリックスにわたされる走査シーケンスを生成する。これらの走査シーケンスは、好ましくは、ランダムであり、暗号の目的のためにほとんどのスマートカードにある乱数発生器（random number generator）を使用して発生されてもよい。それゆえ、列走査シーケンス1-2-3, 3-2-1, 1-3-2, 2-3-1などが、スマートカードによって決定されるのにつれて交互に起こり得る。

【0027】

スマートカードによって生成される走査シーケンスは、端末回路に伝えられないので、端末はプレスされる実際のキーの情報をもっていない。この目的のために、端末回路は、好ましくは、2つの異なった動作モードをもつ。一方の動作モードは、キーボードマトリックスが端末回路によって読み取られることができないプロテクトモードであり、他方の動作モードは、キーボードマトリックスが読み取られることができる非プロテクトモードである。端末は、スマートカードの制御の下で又はユーザ制御の下で、各モード間を切り換えることができる。有利な実施形態では、端末が、例えば、スイッチ又は図1のスマートカードスロットに設けられる他のセンサを使用して、スマートカードの存在を検出し、他方の端末回路からキーパッド回路51及び52を切断する。特殊目的のLED又は専用スクリーン部のようなインジケータが、電流モードをユーザに示すために使用されてもよい。

30

【0028】

40

有利な実施形態では、キーパッド回路51及び52は、単一の論理「1」がその中に挿入されるシフトレジスタによって構成される。「1」が挿入される箇所は、スマートカードによって決定される上述のプロテクトモードにある。シフトレジスタが、キーボードマトリックスに対するものを除いて出力（部）をもっていないので、他方の端末回路は、シフトレジスタのコンテンツを決定することができず、それゆえ、キーシーケンスを決定することもできない。

【0029】

上記の用語「スマートカードリーダー」は、一般に、スマートカードにより双方向通信を可能にする装置に対して用いられ、従って、スマートカードから情報を読み取ることに制限されず、情報をスマートカードに書き込むこともできるということに留意されたい。更

50

に、この明細書では、上記の用語「キーパッド及びキーボード」が互いに交換可能なものとして用いられていることにも留意されたい。一般に、キーボードはキーパッドより多くのキーを含むが、キーの実際の数本発明にとって重要ではない。

【0030】

上記の実施例では、端末1が銀行の預け払い機として使用されていたけれども、本発明はそれに限定されるものではなく、更に、有料テレビ用のセットトップボックス、スマートカードを用いるパーソナルコンピュータ、PDA（パーソナルデジタルアシスタント）及び他の装置に適用されてもよい。更に、本発明は、キーパッドの画像を生成するディスプレイ及びこのキーパッド画像のアイテムを示すことができるポインタを使用するPDAのためのインタフェース及びセキュア画像に適用されてもよい。このような実施形態では、ポインタの位置に関する走査は、図3を参照して上記に説明されたキーボードマトリックスの走査と同じように実施され得る。更に、キーパッド画像は、好ましくは、スマートカードによって又はスマートカードの制御の下で生成される。これは、キーボードのレイアウトに変化をつけることを可能にし、それゆえ、キーボードに入力されるデータが、適切な観察装置を使用することによって、又は視覚的にユーザアクションを観察している第三者によって認識されるリスクを減らす。

10

【0031】

上記の用語「スマートカード」は、集積回路が埋め込まれる実質的にカード形状の基板に限定されるものではなく、集積回路又は類似の装置を含み、電気的接触を介して又はワイヤレスに端末と通信することができる、任意の形状又はサイズのトークンのような機能的な同等物を包含することをも意味することに留意されたい。従って、上記の用語「スマートカード」は、更に、GSMモバイル電話機のSIM（Subscriber Identification Module：加入者識別モジュール）カードを包含してもよい。

20

【0032】

本発明は、スマートカード端末がキーパッドに入力されるデータの情報を、たとえこれらのデータがスマートカードに前もって仕向けられている場合でさえ、得ることができるという洞察に基づく。本発明は、キーパッドに入力されるデータが、端末によってではなくスマートカードによって決定される標準的でない走査シーケンスを使用することによって、端末から「隠される（hidden）」ことができるという他の洞察にも基づく。

【0033】

本明細書に使用されるいかなる用語も、本発明の適用範囲を制限するものとして解釈されるべきではないことに留意されたい。特に、動詞「有する（comprise(s)及びcomprising）」は、具体的に述べられていないどんな構成要素でも除外されることを意味するものではない。単一の（回路）素子は、複数の（回路）素子又はそれらの同等物と置き換えられてもよい。

30

【0034】

当業者であれば、本発明は、上記に例証される実施形態に制限されるものではなく、多くの変更形態及び追加部が、添付の請求項に規定される本発明の適用範囲から逸脱することなく作られてもよいことを理解するであろう。

【図面の簡単な説明】

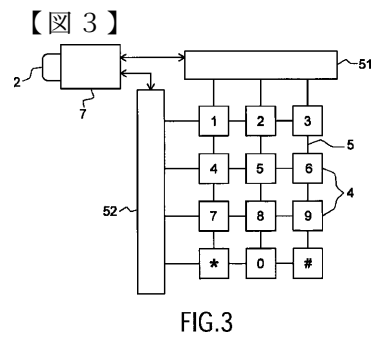
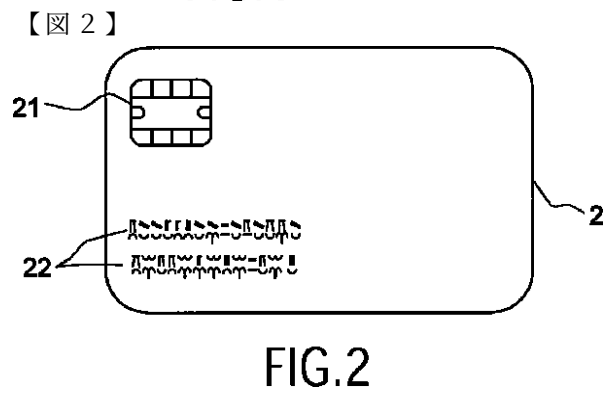
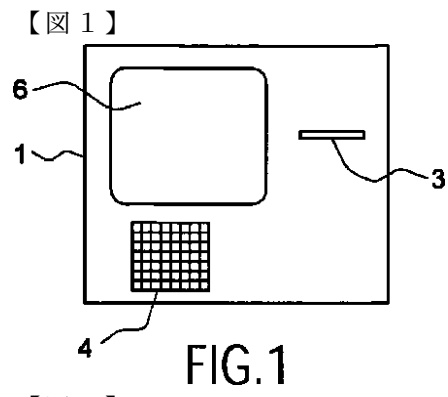
40

【0035】

【図1】本発明によるスマートカード端末を概略的に示す図である。

【図2】本発明に利用され得るスマートカードを概略的に示す図である。

【図3】本発明によるキーパッド装置を概略的に示す図である。



フロントページの続き

(72)発明者 バイカー キース

オーストリア共和国 エイー１１０１ ヴィエンナ トリエステル ストラッセ ６４ フィリッ
プス インテレクチュアル プロパティ アンド スタンダーズ

(72)発明者 プレウーニス ヨハネス マリア

オーストリア共和国 エイー１１０１ ヴィエンナ トリエステル ストラッセ ６４ フィリッ
プス インテレクチュアル プロパティ アンド スタンダーズ

審査官 高瀬 勤

(56)参考文献 国際公開第０２／０９１１４３ (WO, A1)

特表２００４－５２９４３４ (JP, A)

特開平０２－１６５３１２ (JP, A)

特開平０２－０３１２９０ (JP, A)

特開平１１－０３９０８２ (JP, A)

特開昭６２－２３９２７０ (JP, A)

特開２００１－０８４０８１ (JP, A)

柳川亮二, 暗証入力変換機能付ピンパッド決済端末, 東芝技術公開集, 日本, 株式会社東芝, 2
000年12月11日, 第18-65巻, p.104-108

(58)調査した分野(Int.Cl., DB名)

G06K 17/00

G06F 3/02