(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 646 972 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
09.11.2011 Bulletin 2011/45

(21) Application number: **04743941.9**

(22) Date of filing: **12.07.2004**

(51) Int Cl.:
G06K 19/073 *(2006.01)*

(86) International application number:
PCT/IB2004/002279

(87) International publication number:
WO 2005/006247 (20.01.2005 Gazette 2005/03)

(54) **CHIP CARD INCLUDING TAMPER-PROOF SECURITY FEATURES**

CHIPKARTE MIT MANIPULATIONSSICHEREN SICHERHEITS-MERKMALEN

CARTE A PUCE COMPRENANT DES ELEMENTS DE SECURITE INVIOLABLES

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR

(30) Priority: **15.07.2003 EP 03291741**

(43) Date of publication of application:
19.04.2006 Bulletin 2006/16

(73) Proprietor: **Gemalto SA**
92190 Meudon (FR)

(72) Inventors:
- **SALIB, Rami**
  F-45000 Orléans (FR)
- **DELOCHE, Manuel**
  F-45100 Orléans (FR)

(74) Representative: **Cassagne, Philippe M.J. et al**
Gemalto SA
Intellectual Property Department
6, rue de la Verrerie
92197 Meudon Cedex (FR)

(56) References cited:
WO-A-97/22086 **FR-A- 2 740 887**

EP 1 646 972 B1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION

Field of the invention

[0001] The present invention generally relates to the protection against tampering of security features incorporated in chip cards.

Background art

[0002] A chip card comprises a card body and a chip module which is embedded in the card body and incorporates an integrated circuit (IC).

[0003] In addition to the embedded IC, so-called "security features" are often present on the surface of the card body. As a matter of fact, since smart cards are often used for authorising certain operations or to personally identify the holder of the card, it is necessary to include in the card some physical features that may be characterised on visual inspection, in contrast to authentication algorithms which rely on the exchange of signals with the microprocessor of the IC.

[0004] There has been proposed a number of security features, such as a photograph of the holder of the card, holograms, hologram-like features such as multiple laser images (MLI), laser engraving of individual data such as name and card number, etc. These features are created directly on the card body at the manufacturing stage, or maybe added at a later stage in the course of the personalization step of the blank card.

[0005] A problem nevertheless remains in ensuring integrity and security of the card. Though it is generally difficult to modify features as holograms, laser engraving, etc. without blatant alteration of the card, there exists some simple frauds consisting e.g. in peeling as a whole a layer of the card to replace printed or engraved information, still keeping unchanged the other layers of the cards and the chip module. Photographs printed on a card, like on driving licenses, passport, etc. are usually the first targets of such physical attacks.

[0006] Another attack consists in keeping the card body with all its security features as such, but removing the chip module and replacing it by a counter-felted module or a module taken from another card.

[0007] In order to make such physical attacks more difficult or render them more apparent in case of alteration of the card, multiple, different security features are incorporated in a single card and/or more and more sophisticated security features are used.

[0008] However, this makes the manufacturing process more complex and more expensive, while remaining vulnerable to some kinds of physical attacks such as exchanging the IC or peeling as a whole the layer incorporating the different security features. Thus the security features proposed so far, despite their sophistication, are not really tamper-proof and are still open to some kind of physical attacks.

[0009] WO-A-2004/012228 is a prior art document according to Article 54(3) EPC. It describes a security document comprising at least one security characteristic, and means to check the integrity of the security characteristic. In an embodiment, the checking of the integrity is made on an electrically pattern as follows: a reader read a number stored in the chip and retrieve data corresponding to electrical properties of a security thread by questioning a data base with this number; the reader then communicates this data to the chip for comparing it to a value directly measured on the security thread by applying a voltage to it.

SUMMARY OF THE INVENTION

[0010] It is therefore an object of the invention to provide a chip card protected against any physical attacks applied to a card containing security features, which can work as a tamper-proof feature making the card irreversibly non-functional in case of any attempt of such kind of fraud.

[0011] Another object of the invention is to provide such a tamper-proof chip card which may be manufactured through conventional manufacturing processes, and in a way cheaper than most security features like holograms or laser engraving.

[0012] A further object of the invention is to provide such a chip card enabling a reduction of the number of different security features needed to protect the card and the IC, hence with a lower manufacturing cost.

[0013] A still further object of the invention is to provide such a chip card which may be protected at once against both physical attacks like layer peeling and IC exchange.

[0014] A still further object of the invention is to provide a chip card in which the protection is obtained through incorporation of features which are invisible or near invisible to human eye in daylight, making it difficult to detect when the card is visually inspected in daylight.

[0015] The invention is set forth in claim 1.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] The foregoing and other objects, aspects and advantages of the invention will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the appended drawings, in which the same numerals refer to identical or functionally similar features over the different figures.

Figure 1 is a schematic, exploded view of a card incorporating the security feature according to the invention.

Figure 2 is a plan view of the specific security layer of the card of Figure 1.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT OF THE INVENTION

[0017] Referring now to the drawings, Figure 1 illustrates an exemplary embodiment of a card incorporating the security features of the invention.

[0018] This card comprises a card body 10 and a chip module 12 including an IC, typically an IC with a microprocessor-based chip allowing *inter alia* execution of suitable authentication, decryption, etc. algorithms for the preliminary identification of the user of the card.

[0019] The most common process for manufacturing a chip body is by lamination of a plurality of layers each made from a plastic foil. Card body 10 at least includes a base layer 14 and an upper layer 16 with a hole 18 punched or milled in order to form a recess for receiving the chip module 12.

[0020] The upper layer 16 includes one or several so-called "security features" such as a photograph 20 of the authorized user of the card, or personal identification data written by laser engraving 22. There exist a number of other security features, which are all well-known from the man skilled in the art such as holograms, multiple laser image, patterns or characters which are not visible under normal daylight but become apparent under UV or IR light, magnetically-readable encoding, etc. All such "security features" are features which are only of a physical nature, as opposed to identification, authentication and like functionalities involving processing of data by the IC incorporated in chip module 12.

[0021] The invention essentially lies in the incorporation in the card body of an additional layer 26, hereafter called "security layer", enabling detection of any alteration of the security features present on upper layer 16, attempts of peeling upper layer 16, or removal of the chip module 12 from the card in the case of fraud by IC exchange.

[0022] As better shown on Figure 2, security layer 26 includes a conductive pattern 28 forming a pathway running on the surface of layer 26 and having regions such as 30 and 32 which are located beneath security features 20 and 22 (shown in broken lines) of upper layer 16.

[0023] Conductive pattern 28 forms an electrical loop between end pads 34, 36 which are connected by suitable means to terminals of the IC embedded in module 12.

[0024] Basically, conductive pattern 28 acts as a switch that permanently and irreversibly deactivates the IC in case the circuit is broken due to fraudulent peeling of upper layer 16 or removal of chip module 12.

[0025] Alternatively, conductive pattern 28 is devised with specific electrical properties such as a given impedance or resistance, the IC being adapted to check whether said impedance or resistance matches a predetermined value stored in a memory of the IC.

[0026] For instance, peeling off the upper layer 16 will alter these electrical properties, which will not longer match the value stored within the IC, blocking any proper operation of the latter.

[0027] It is in particular possible to customize conductive pattern 28 in order to modify the electrical properties from one batch to the other and load the corresponding value in the IC memory during personalisation of the card, so that any attempt to exchange the module will result in a mismatch making IC operation impossible.

[0028] In case of contactless systems, or hybrid contact/contactless systems, conductive pattern 28 may constitute an antenna being part of a tuned circuit involved in contactless operation.

[0029] Many variants of the invention may be considered, and the above description is just given by way of example.

[0030] For instance, security layer 26 is not necessary located below layer 16 bearing security features to be protected. In other embodiments, the security layer may as well overlay the security features, the conductive pattern being in this case preferably made from a transparent or near transparent material.

[0031] Conductive pattern 28 may be formed from any known material. Preferably, it is made from conductive ink, which makes it easy to form by conventional techniques such as screen printing. There exist a number of conductive materials such as conductive polymer resins. The material and arrangement of pattern 28 may be chosen so as to be invisible or nearly invisible to human eye in daylight, making it difficult to detect thereof. Transparent or clear conductive material may be used, or may be devised in order to make it hardly visible, for instance a grey pattern applied on grey layer background.

[0032] Security layer 26 may be provided for as a layer added in the course of the lamination process, whenever the card is manufactured this way. However, this is not restrictive and the security layer may be used in conjunction with cards made by other manufacturing processes, for instance the security layer may be added onto a moulded card body before, or during, the personalization stage.

Claims

1. A chip card system, comprising

- a card body (10) and
- a chip module (12) embedded in said card body, said chip module comprising an integrated circuit,

said card body including at least one security feature (20, 22) incorporated in the card body, or applied on a surface of the card body, wherein said card body comprises a a tamper detection layer including a conductive pattern (28) connected to the integrated circuit, said conductive pattern having at least one region (30, 36) beneath or above said security feature (20, 22)
wherein said integrated circuit is adapted :

- to perform an integrity check of said conductive pattern by checking whether electrical properties of the pattern match a predetermined value stored in the integrated circuit for conditionally performing further operations only in case said integrity is recognized,
- or to be deactivated in case the pattern is broken

2. The system as in claim 1, wherein said conductive pattern (28) has given impedance or resistance and said integrated circuit is adapted to check whether said impedance or resistance matches a predetermined value stored in a memory of the integrated circuit.

3. The system as in cairn 1, wherein said at least one security feature is a feature from the group including photograph (20) hologram multiple laser image, laser engraving, UVIIR-readable pattern and magnetically-readable encoding.

4. The system as in claim 1, wherein said conductive pattern is made from a conductive ink material.

5. The system as in claim 1, wherein said conductive pattern is made from a transparent or near transparent material.

6. The system as in claim 1, wherein said conductive pattern (28) is connected to said terminals (34, 36) of the integrated circuit through permanent bonds.

Patentansprüche

1. Ein Chipkartensystem, bestehend aus

- einem Kartenkörper (10) und
- einem im Kartenkörper eingebauten Chipmodul (12), das über einen integrierten Schaltkreis verfügt,

der Kartenkörper enthält mindestens ein Sicherheitsmerkmal (20, 22), das in den Kartenkörper eingebaut oder auf der Oberfläche des Kartenkörpers angebracht ist, wobei der Kartenkörper eine Beschichtung zur Manipulationserkennung mit Leiterbild (28) aufweist, das an den integrierten Schaltkreis angeschlossen ist. Das Leiterbild verfügt über mindestens eine Region (30, 36) unterhalb oder oberhalb des Sicherheitsmerkmals (20, 22)

wobei der integrierte Schaltkreis angepasst wird:

- um eine Integritätsprüfung des Leiterbildes durchzuführen, wobei geprüft wird, ob elektrische Eigenschaften des Bildes einem vorgegebenen, im integrierten Schaltkreis hinterlegten Wert entsprechen, um weitere Operationen nur bedingt durchzuführen, für den Fall dass die Integrität erkannt wird,
- oder um deaktiviert zu werden, falls das Bild defekt ist

2. Das System nach Anspruch 1, wobei das Leiterbild (28) gegebenen Scheinwiderstand oder Wirkwiderstand aufweist und der integrierte Schaltkreis angepasst wird, um zu prüfen, ob der Schein- oder Wirkwiderstand einem vorgegebenen, in einem Speicher des integrierten Schaltkreises gespeicherten Wert entspricht.

3. Das System nach Anspruch 1, wobei das Sicherheitsmerkmal ein Merkmal der Gruppe darstellt, einschließlich Foto (20), Hologramm, Multiple Laser Image, Lasergravur, UV/IR-lesbarem Bild und magnetisch lesbarer Codierung.

4. Das System nach Anspruch 1, wobei das Leiterbild aus leitfähiger Tinte besteht.

5. Das System nach Anspruch 1, wobei das Leiterbild aus transparentem oder fast transparentem Material besteht.

6. Das System nach Anspruch 1, wobei das Leiterbild (28) dauerhaft mit den Klemmen (34, 36) des integrierten Schaltkreises verbunden ist.

Revendications

1. Système de carte à puce, comprenant

- un corps de carte (10) et
- un module de puce (12) intégré dans ledit corps de carte, ledit module de puce comprenant un circuit intégré,

ledit corps de carte comprenant au moins une caractéristique de sécurité (20, 22) incorporée dans le corps de carte, ou appliquée sur une surface du corps de carte, dans lequel ledit corps de carte comprend une couche de détection de violation comprenant un motif conducteur (28) connecté au circuit intégré, ledit motif conducteur ayant au moins une région (30, 36) au-dessous ou au-dessus de ladite caractéristique de sécurité (20, 22)

dans lequel ledit circuit intégré est conçu :

- pour effectuer un contrôle d'intégrité dudit motif conducteur en contrôlant si les propriétés électriques du motif correspondent à une valeur prédéterminé mémorisée dans le circuit intégré pour effectuer de manière conditionnelle d'autres opérations uniquement dans le cas où ladite intégrité est reconnue,

- ou pour être désactivé dans le cas où le motif est rompu.

2. Système selon la revendication 1, dans lequel ledit motif conducteur (28) a une impédance ou une résistance donnée et ledit circuit intégré est conçu pour contrôler si ladite impédance ou résistance correspond à une valeur prédéterminée mémorisée dans une mémoire du circuit intégré.

3. Système selon la revendication 1, dans lequel ladite au moins une caractéristique de sécurité est une caractéristique du groupe comprenant une photographie (20), un hologramme, une image laser multiple, une gravure au laser, un motif pouvant être lu sous UV/IR et un encodage pouvant être lu magnétiquement.

4. Système selon la revendication 1, dans lequel ledit motif conducteur est réalisé à partir d'une encre conductrice.

5. Système selon la revendication 1, dans lequel ledit motif conducteur est réalisé à partir d'un matériau transparent ou presque transparent.

6. Système selon la revendication 1, dans lequel ledit motif conducteur (28) est connecté auxdites bornes (34, 36) du circuit intégré par l'intermédiaire de liaisons permanentes.

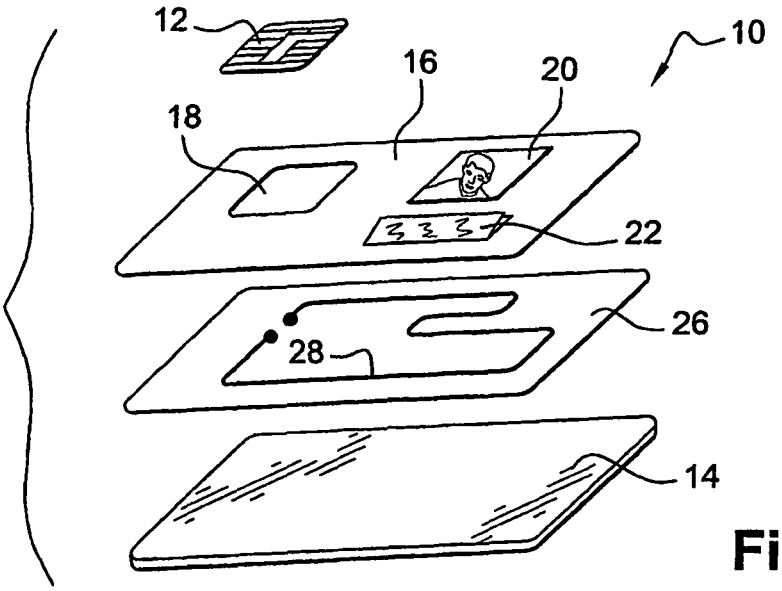

Fig. 1

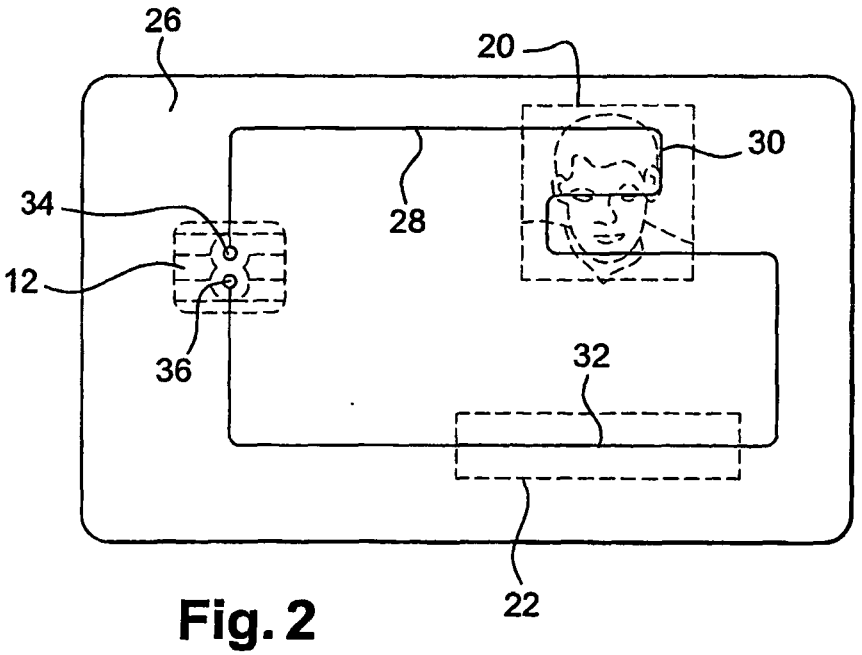

Fig. 2

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 2004012228 A **[0009]**