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

(11) EP 2 180 488 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.04.2010 Bulletin 2010/17

(51) Int Cl.:
H01H 13/702 *(2006.01)* ***H01H 13/704*** *(2006.01)*

(21) Application number: **09172841.0**

(22) Date of filing: **13.10.2009**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Designated Extension States:
AL BA RS

(30) Priority: **21.10.2008 BR MU8802356 U**

(71) Applicant: **Tecvan Informática LTDA.**
Município de Ilhéus - Estado da Bahia (BR)

(72) Inventor: **Dias Rodrigues, Wagner**
Município de São Bernardo do Campo - Estado de São Paulo (BR)

(74) Representative: **Robba, Pierpaolo**
Interpatent S.R.L.
Via Caboto 35
10129 Torino (IT)

(54) Constructive device introduced into a security keyboard for information and secret processes stored by electronic means

(57) Device characterized by including a protective mechanism for the keyboard system which makes attacks impossible by mechanical manipulation, mechanical perforation, part separation, chemical short circuits or the insertion of intrusive devices.

One of the objectives of this invention is to provide a constructive device for a keyboard in order to impede the insertion of unauthorized access devices into their internal circuits, guaranteeing the internal inviolability of installed equipment at the point of sale and providing a significant increase in security of the keyboard system.

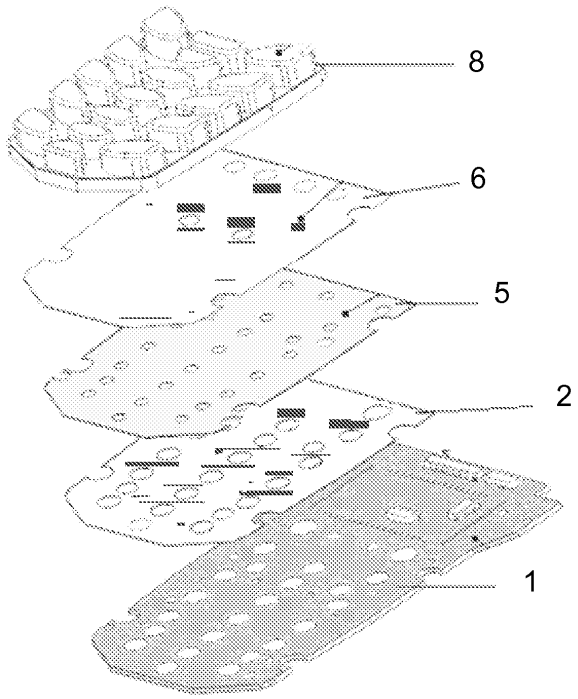

Fig. 1

EP 2 180 488 A1

Description

[0001] Referring to the present descriptive report of the Utility Model of a security keyboard, as the opportunity for its designation, in order to protect information and secret processes stored by electronic means against unauthorized access.

[0002] The point of sale terminals (POS, PDV, Pinpad, encrypted keyboard) allow the clients to pay their bills using several payment methods, such as credit cards, debit cards, smart cards and others.

[0003] To guarantee that the payment information is not intercepted from one of the sales point terminals until the center of payments, such information is normally encrypted and protected during transmission, using, for example, digital authentication technology. Therefore, the confidential payment information, keyed in by the user at a Point of Sale, could be intercepted by a physical violation of the Point of Sale

[0004] To impede any violation and consequent digital information interception, the keyboard in question, the object of this report, is assembled in a way as to guarantee the inviolability of its internal content, setting off an intruder alarm at any attempt at front, rear or side manipulation or mechanical perforation of any internal part of the keyboard or of the circuits activated by its keys.

[0005] The referred intrusion alarm sets off a security mechanism, which destroys stored information, going back to the security concept of the former cryptex.

[0006] The major part of the solutions found currently do not have a security mechanism for the detection of intrusion circuits inserted in the keyboard, based on circuits mounted externally to the printed circuit board where the keyboard buttons to be operated, close the exposed terminals.

[0007] The standard activating mechanism of a keyboard system consists of a rigid printed circuit board containing a demarcated area, two open exposed terminals, connected to an electronic circuit which, for its turn, detects the closing of these contacts. Each keyboard is connected to a conducting element in the face around the contacts, in such a way, when pressing the key, the conducting element touches the two contacts closing them in a circuit, allowing the keyboard processor to decode any key operated.

[0008] An observed disadvantage in the conventional solutions is that they allow the occurrence of frauds by the means of the introduction of a device between the circuit board and the keyboard button, detecting the keys and the pressing sequence of them, allowing the capture of personal identity numbers (PIN) and other secret information of the user.

[0009] One of the objectives of this Utility Model is to provide a constructive device for a keyboard in order to impede the insertion of unauthorized access devices into their internal circuits, guaranteeing the internal inviolability of installed equipment at the point of sale and providing a significant increase in security of the keyboard system.

[0010] Therefore, in order to allow a better clarification of the object in question, let's proceed to its detailed description with reference to the drawings below where:

Figure 1 illustrates in exploded perspective view the keyboard circuit layers;
figure 2 illustrates a front view of the upper face of the malleable security circuit;
figure 3 illustrates a front view of the lower face of the malleable security circuit;
figure 4 illustrates a front view of the lower face above the malleable contacts circuit;
figure 5 illustrates a front view of the upper face of the malleable contacts circuit;
figure 6 illustrates a front view of the lower face of the spacer.

[0011] In conformity with the illustrated figures mentioned above, the security keyboard, objective of this Utility Model, is made up of a rigid printed circuit (1), having an insulating flexible membrane (2), of a determined thickness, with holes (3) located over the position of the two exposed contacts (4), with the function of a spacer over which the malleable electronic circuit is placed (5) with some conductive material, in the lower face, aligned with the exposed contacts (4) of the rigid printed circuit (1), being the keyboard (8) separated from the rest of the assembly by a malleable electronic protection board (6), which indicates any break in its circuit.

[0012] Due to the presence of the flexible membrane (2) between the malleable electronic circuit (5) and the rigid printed circuit (1), the conducting material does not close the contacts, in spite of the hole present in that position. The mechanical key, in this case, does not have the capability of closing the contact, but presses the conducting material of the malleable electronic circuit on the membrane spacer, deforming it until the conducting material enters into contact with the two exposed contacts (4) and closes the circuit, signaling to the processor element that the contact was closed.

[0013] The first mechanism additional to the traditional system refers to the insertion of a malleable electronic protection circuit (6), between the keyboard (8) and the malleable electronic circuit of the contacts (5), as illustrated in figure 1, in a way so as to create a physical barrier against mechanical attacks of the perforating, obliteration, cutting or short circuiting chemicals types.

[0014] The said malleable electronic protection circuit (6) has on both faces, multiple electronic circuits in a coil form, with a random design, running through the circuit surface in a dense physical mesh. On each face of the malleable circuit, there are two independent circuits, positioned near each other, whose terminals are linked in a security circuit which when detecting any anomaly sets off a security alarm which will generate the protection and security procedures of the Point of Sale terminal.

[0015] From each of these circuits is transmitted a dig-

ital electronic signal in a waveform and univocal frequency, generated by the security circuit which is monitored by the security circuit receiver. In other words, each circuit has a signature permanently monitored by the security circuit.

[0016] If there is a perforating type violation attempt which breaks any segment of this circuit, it is immediately detected by the security circuit.

[0017] If there is a chemical violation attempt by short circuiting the mesh, seeking to make it possible to subsequently break the protection circuit, the alarm will be set off, because there are two circuits with different signatures and the security circuit is not capable of distinguishing the signatures of each circuit in the case of a short circuit in the mesh.

[0018] The protection circuits have very complex random designs, in order to make it difficult for a violator to check the circuit visually and find its respective terminals.

[0019] The malleable protection circuit has a larger size than the keyboard activating circuits, seeking to completely cover physically the lower keyboard circuits, in a way to impede side attacks to the keyboard system.

[0020] To impede the attempt at separating the many keyboard system components, usually seeking to insert electronic devices, independent monitoring circuits are positioned, starting at the lower rigid printed circuit and connecting to the upper invasion monitoring circuit, at the ends of this circuit, returning to the lower rigid circuit, in a position diametrically opposite the input.

[0021] Again, each circuit has a digital signature with its own frequency and waveform, impeding a crossover short circuit. The mechanical contact between the upper and lower circuits occurs through projections in the keyboard or the lid of the device, which exert enough mechanical pressure to maintain the circuits closed. In an attempt to separate the diverse elements in the keyboard system, these contacts are opened, activating security sensors in the point of sale terminal.

[0022] Preferably, the separation detection circuits between the keyboard system components can be provided with an intermediate conductor circuit, which stays closed by mechanical pressure between the mechanical keyboard and the device lid. If an invasion occurs in this secure area, the sensor activating communicates to the processor which then destroys all the secret information stored in the electronic memory.

[0023] Without this information, it is impossible to recuperate the secret information stored in the memory as well as carry out secret processes turning the equipment inoperable.

[0024] Regarding the signatures generated by each monitoring mesh circuit, inside the microprocessor there is a true random number generator. The random numbers of this generator are used to create signal forms of amplitude, frequency and phase parameters for the sensor. These signals pass through the sensor group and return to the microprocessor, whose comparing circuits check the referred parameters of the original signals.

[0025] Detecting differences in the parameters, the invasion alarm circuit is activated and immediately secret information is destroyed turning the equipment inoperable and making it impossible to recuperate the information.

[0026] The constructive disposition presented here is not limited to any specific format or to its constructive sequence, presuming there are numerous variations in the present constructive of a security keyboard for information and secret processes stored by electronic means without impairing the objective of this Utility Model.

Claims

1. "CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS" **characterized by** a rigid printed circuit (1), having an insulating flexible membrane (2), of a determined thickness, with holes (3) located over the position of the two exposed contacts (4), with the function of a spacer over which the malleable electronic circuit is placed (5) with some conductive material, in the lower face, aligned with the exposed contacts (4) of the rigid printed circuit (1), being the keyboard (8) separated from the rest of the assembly by a malleable electronic protection board (6), which indicates any break in its circuit.

2. "CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS", in agreement with Claim 1, **characterized by** including a protective mechanism for a keyboard system which makes attacks impossible by mechanical manipulation, mechanical perforation, part separation, chemical short circuits or the insertion of intrusive devices.

3. "CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS", in agreement with Claim 1, **characterized by** the insertion of a malleable electronic protective circuit (6), between the keyboard and malleable electronic circuit with contacts (5) in a way as to create a physical barrier against attacks of the perforating mechanical type, obliteration, cutting or chemical short circuits

4. "CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS", in agreement with Claim 3, **characterized by** the input and output of monitoring points of a same circuit to be positioned diametrically opposite, in a cross form or passed between the circuits,

making it impossible to insert intrusive devices in various angles of attack.

5. "CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS", in agreement with Claim 3 **characterized by** the fact said malleable electronic protection circuit (6) has on both faces, a double electronic circuit in a coil form, with a complex random design, running through the circuit surface in a dense physical mesh, there are each face of the malleable circuit, two independent circuits, positioned near each other, whose terminals are linked in a security circuit which when detecting any anomaly sets off a security alarm responsible for generating the protection and security procedures of the Point of Sale terminal.

6. "CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS", in agreement with Claim 1, **characterized by** the use of a multiple monitoring circuit with a complex random design pattern which makes it difficult to follow the circuit logic, making it impossible to visually identify the input and output terminals of each circuit by possible fraudsters.

7. "CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS", in agreement with Claim 1, **characterized by** the use of a monitoring circuit of larger dimensions than the lower circuits, forming a protective area, impeding side attacks on the keyboard system.

8. ""CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS", in agreement with Claim 1, **characterized by** the use of a printed circuit below the keyboard, which has an internal layer with electric circuits in a coil form, responsible for the detection of invasion or attack attempts on the lower part of the keyboard.

9. ""CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS", **characterized by** the insertion of a flexible security circuit consisting of diverse traces that delineate circuits whose contacts are maintained closed by projections located in the terminal cabinet of the point of sale and in the mechanical keyboard, in a way so that any attempt to separate mechanically any component of the keyboard system causes these circuits to open, setting off a security system.

10. "CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS", in agreement with Claim 9, **characterized by** the fact that the said monitoring traces are proof against chemical or mechanical attack that causes a short circuit in the monitoring mesh.

11. "CONSTRUCTIVE DEVICE INTRODUCED INTO A SECURITY KEYBOARD FOR INFORMATION AND SECRET PROCESSES STORED BY ELECTRONIC MEANS", in agreement with Claim 9, **characterized by** the fact that each circuit has a digital signature with its own frequency and waveform, impeding a crossover short circuit.

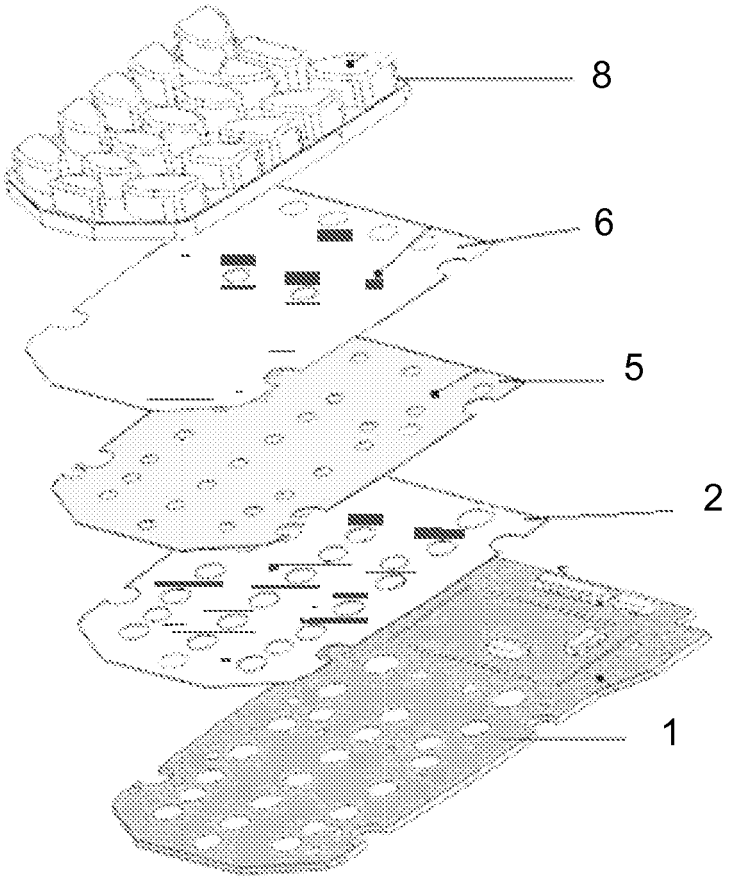

Fig. 1

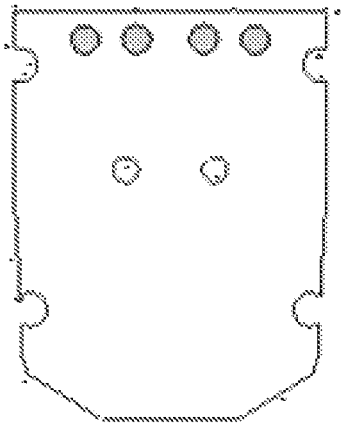

Fig. 2

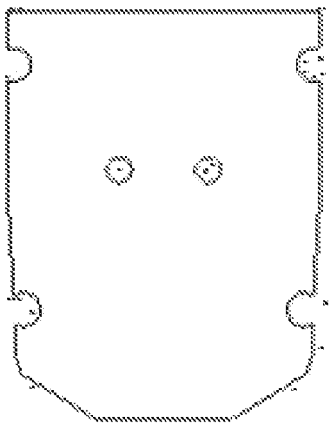

Fig. 3

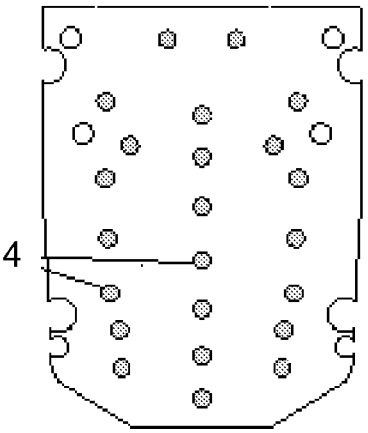

Fig. 4

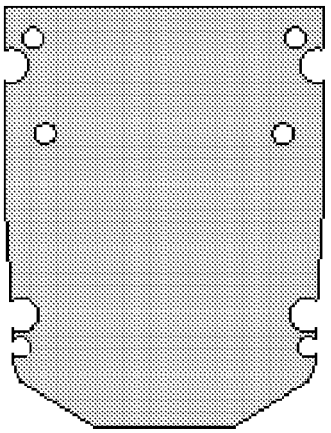

Fig. 5

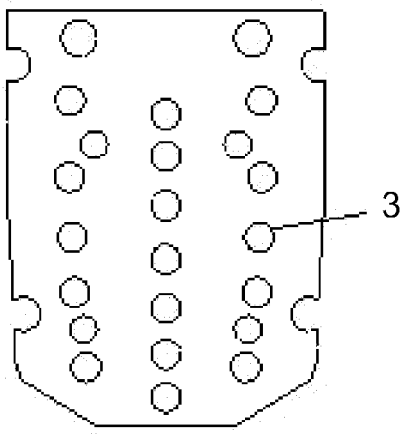

Fig. 6

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 09 17 2841

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X Y	DE 43 12 905 A1 (KRONE AG [DE]) 20 October 1994 (1994-10-20) * column 2, line 40 - column 4, line 17; figures * -----	1-3,5-11 4	INV. H01H13/702 H01H13/704
Y	US 7 270 275 B1 (MORELAND FLYNT [US] ET AL) 18 September 2007 (2007-09-18) * column 6, lines 8-17; figures * -----	4	
X A	WO 2005/086546 A2 (LIPMAN ELECTRONICS ENGINEERING [IL]; WARD RICHARD [GB]; RICHARDS GARET) 15 September 2005 (2005-09-15) * abstract; figures 2-4 * -----	9 1	

TECHNICAL FIELDS SEARCHED (IPC)

H01H

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	14 January 2010	Findeli, Luc

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 09 17 2841

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

14-01-2010

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4312905 A1	20-10-1994	NONE	
US 7270275 B1	18-09-2007	NONE	
WO 2005086546 A2	15-09-2005	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82