



- (51) **International Patent Classification:**
G06F 21/86 (2013.01) *G06F 21/83* (2013.01)
- (21) **International Application Number:**
PCT/US2019/055774
- (22) **International Filing Date:**
11 October 2019 (11.10.2019)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
201910188334.9 13 March 2019 (13.03.2019) CN
16/575,710 19 September 2019 (19.09.2019) US
- (71) **Applicant: MICROCHIP TECHNOLOGY INCORPORATED** [US/US]; 2355 West Chandler Blvd., Chandler, Arizona 85224-6199 (US).
- (72) **Inventor: HUANG, Eric**; Unit 1610, Enjoy Center, Xiaomen, Fujian 361000 (CN).
- (74) **Agent: SLAYDEN, Bruce W., II**; Slayden Grubert Beard PLLC, 401 Congress Ave., Suite 1650, Austin, Texas 78701 (US).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

(54) **Title:** KEYBOARD FOR SECURE DATA ENTRY

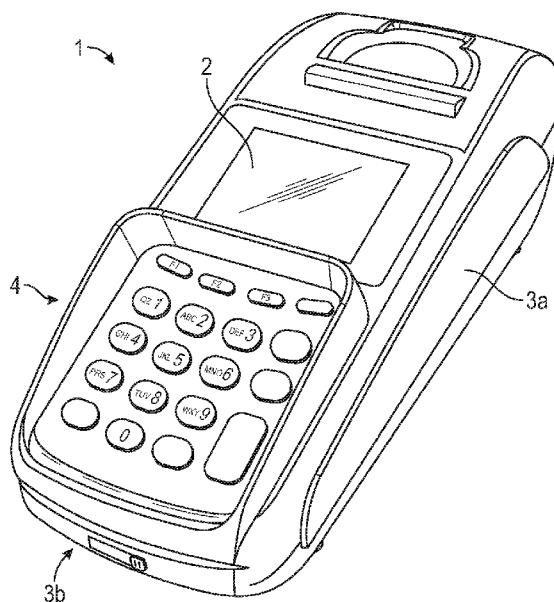


FIG. 1

(57) **Abstract:** A keyboard for secure data entry is provided. The keyboard comprises at least one or more of data entry buttons that can be depressed by a user. For each of the data entry buttons, a button actuator is provided that is movable upon the user depressing the respective data entry button and a primary capacitive sensor is provided that is arranged to determine movement of the button actuator of the respective data entry button by capacitance sampling. The button actuator is at least partly made from a conductive material. The button actuator is coupled to a defined electric potential at least during the capacitance sampling to shield the primary capacitive sensor from eavesdropping.



EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

- *with international search report (Art. 21(3))*

KEYBOARD FOR SECURE DATA ENTRY

RELATED APPLICATIONS

The present application claims priority to CN Patent Application No. 201910188334.9 filed March 13, 2019, the contents of which are hereby incorporated in their entirety.

5 TECHNICAL FIELD

The present invention relates to the field of keyboards for secure data entry.

BACKGROUND

This background section is provided for the purpose of generally describing the context of the disclosure. Work of the presently named inventor(s), to the extent the work is described
10 in this background section, as well as aspects of the description that may not otherwise qualify as prior art at the time of filing, are neither expressly nor impliedly admitted as prior art against the present disclosure.

In the field of computer technology, a possibility for secure and reliable entry of data is a necessity for a multitude of applications, such as in particular for authentication purposes to
15 gain access to an electronic or a physical resource.

For example, in Point-of-Sale (POS) or building access systems, a user is often required to enter a passcode or PIN. This passcode entry needs on the one hand to be reliable to allow the user to gain access conveniently, on the other hand, security of the entry needs to be maintained. In both of the preceding examples, the respective passcode entry may be conducted
20 in a public place. Due to that, corresponding passcode entry systems may be tampered with by a malicious third party to obtain the passcode and to gain access to the respective resource.

For example, it may be possible for a third party to try scanning the PIN entry using a so-called “side-channel attack”. This traditional key array scan method allows to scan for signal changes, e.g., high/low level changes on a keypad's column and row circuit. It is
25 relatively easy to monitor such changes using a side-channel attack that is widely available.

To solve the problem of side-channel scanning, a known solution is to protect the keypad input from being monitored by using a flexible mask with printed silver paste conductors, placed on top of a typical button dome array of the keypad. The silver paste mask is connected to internal anti-tamper pins to form an active shield mask. This solution however
30 provides frequent bending of the silver paste mask during the assembly process and during use,

which may lead to reliability problems. In addition, the cost of this kind of arrangement is quite high.

SUMMARY

The following summary of the present invention is provided to facilitate an understanding of some of the innovative features unique to the present invention and is not intended to be a full description. A full appreciation of the various aspects of the invention can be gained by taking the entire specification, claims, drawings, and abstract as a whole.

In light of the preceding discussion, a need exists to provide an improved keyboard that allows reliable, secure data entry and prevents eavesdropping by a malicious third party.

The invention, as defined in the independent claims, provides an improved keyboard for secure data entry, a point-of-sale device, and a method of secure data entry. Embodiments of the invention are discussed in the dependent claims and the following description.

According to one aspect of the present invention, a keyboard for secure data entry is provided. The keyboard comprises at least one or more of data entry buttons that can be depressed by a user, and for each of the data entry buttons, a button actuator, movable upon the user depressing the respective data entry button, and a primary capacitive sensor, arranged to determine movement of the button actuator of the respective data entry button by capacitance sampling. According to the present aspect, the button actuator is at least partly made from a conductive material, and the button actuator is coupled to a defined electric potential at least during the capacitance sampling to shield the primary capacitive sensor from eavesdropping.

According to another aspect of the present invention, a point-of-sale (POS) device is provided, comprising at least a POS transaction processor, one or more of data entry buttons that can be depressed by a user, and for each of the data entry buttons, a button actuator, movable upon the user depressing the respective data entry button, and a primary capacitive sensor, arranged to determine movement of the button actuator of the respective data entry button by capacitance sampling. The button actuator is at least partly made from a conductive material, and the button actuator is coupled to a defined electric potential at least during the capacitance sampling to shield the primary capacitive sensor from eavesdropping.

According to yet another aspect of the present invention, a method of secure data entry with a keyboard having one or more of data entry buttons that can be depressed by a user is provided. In the present aspect, for each of the data entry buttons, a button actuator, and a primary capacitive sensor is provided. The method comprises a) sampling of the primary

capacitive sensor to determine movement of the button actuator, and b) at least during the sampling, coupling the button actuator to a defined electric potential to shield the primary capacitive sensor from eavesdropping.

The basic idea of the aforementioned aspects of the present invention is to provide a keyboard for secure data entry having capacitive sensors to determine if a data entry button of the keyboard is depressed by a user, which keyboard uses a button actuator of each data entry button to at least temporarily provide a shield against eavesdropping by malicious third parties. Thus, a secure data entry is possible with a highly reliable and cost-efficient setup.

The above aspects and other aspects of the invention will be apparent from and elucidated with reference to the embodiments described hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings,

FIG. 1 shows a first embodiment of a point-of-sale (POS) device;

FIG. 2 shows a schematic block diagram of the POS device according to the embodiment of FIG. 1;

FIG. 3 shows a partial, exploded view of an embodiment of a keyboard;

FIG. 4 shows a schematic top-view of an intermediate PCB layer of the keyboard of the embodiment of FIG. 3;

FIG. 5 shows a schematic top-view of a top PCB layer of the keyboard of the embodiment of FIG. 3;

FIG. 6 shows a schematic top-view of a bottom PCB layer of the keyboard of the embodiment of FIG. 3;

FIG. 7 shows a flow chart of the operation when tampering is detected; and

FIG. 8 shows embodiments of a button actuator for the keyboard of FIG. 3.

DETAILED DESCRIPTION

Technical features described in this application can be used to construct various embodiments of keyboards for secure data entry, point-of-sale devices, and methods of secure data entry. Some embodiments of the invention are discussed so as to enable one skilled in the art to make and use the invention.

In a first exemplary aspect, a keyboard for secure data entry is provided. The keyboard comprises at least one or more data entry buttons that can be depressed by a user. For each of the data entry buttons, a button actuator is provided, which button actuator is movable upon

the user depressing the respective data entry button. In addition, for each of the data entry buttons, a primary capacitive sensor is provided, arranged to determine movement of the button actuator of the respective data entry button by capacitance sampling. According to the present aspect, the button actuator is at least partly made from a conductive material, and the button actuator is coupled to a defined electric potential at least during the capacitance sampling to shield the primary capacitive sensor from eavesdropping.

The keyboard according to the present aspect may be of any suitable type. In some embodiments, the keyboard is a computer keyboard, for example a QWERTY-type keyboard. In some embodiments, the keyboard is configured as a numeric keyboard, also referred to as a numeric keypad or number pad. In some embodiments, the data entry buttons are arranged in a matrix, for example a 3x3 matrix.

As discussed in the preceding, the keyboard according to the present aspect comprises one or more data entry buttons that can be depressed by the user, i.e., that are user-operable. The data entry buttons may be of any suitable type and material, depending on the application, such as for example plastic or metal in a square or round shape. The keyboard further comprises for each data entry button, an associated button actuator that is movable upon a user operating/depressing the respective data entry button. The button actuator is at least in part made from conductive material, but otherwise may of any suitable type. In some embodiments, the button actuator is made from a metal, plastic, or a combination thereof. In some embodiments, the button actuator is dome-shaped, which allows deforming of the button actuator when a user depresses the respective button.

The keyboard according to the present aspect further comprises for each data entry button, a primary capacitive sensor. The primary capacitive sensor serves to determine movement of the button actuator of the respective data entry button by capacitance sampling, i.e., by determining a change of the capacitance of the primary capacitive sensor. It is noted that in the present context, the term “movement” with respect to the button actuator is understood broadly and includes position changes of the button actuator, but also deforming of the button actuator.

The primary capacitive sensor may be of any suitable type, various of which are known in the art. In some embodiments, the primary capacitive sensor is a mutual-capacitance sensor, as for example described in US 9543948 or US 9430107, the entire contents of which are

incorporated herein by reference. In some embodiments, the primary capacitive sensor is a self-capacitance sensor.

According to the present aspect, the button actuator is coupled to a defined electric potential at least during the capacitance sampling of the primary capacitive sensor. This way, the button actuator, or more precisely the conductive parts of the button actuator, serve as an active shield to the primary capacitive sensor, so that eavesdropping or monitoring on the electric changes in the primary capacitive sensor in a typical side-channel attack is much more difficult.

For example, and in some embodiments, the button actuator is coupled or connected to ground potential at least during the capacitive sampling. In other embodiments, the button actuator is coupled to a potential, different from ground potential at least during capacitive sampling. In some embodiments, the button actuator is not only coupled to the defined electric potential during the capacitance sampling, but for longer periods. In some embodiments, the button actuator is coupled to the defined electric potential permanently when the keyboard is operational, i.e., powered-up.

In some embodiments, the button actuator of the respective button is coupled to the defined electric potential at least during the capacitance sampling. In some embodiments, the button actuators of all data entry buttons are coupled to the defined electric potential at least during the capacitance sampling. The latter embodiments provide a further improved shielding functionality.

In some embodiments, the keyboard may comprise additional components, such as, for example, one or more of a housing, a processor, a suitable power supply, a display, memory, credit card reader, printer, and an interface to a communications network. It is noted that in some embodiments, the keyboard, in addition to the one or more data entry buttons, may comprise one or more additional buttons, which do not comprise the button actuator and/or primary capacitive sensor as discussed in the preceding. For example, in a typical Point-of-Sale (POS) credit card terminal application, the keyboard may comprise a 3x3 matrix of (secure) data entry buttons as discussed, but also a power on/off button and a 'print' button, which may be of a typical, non-secure type.

In some embodiments, the keyboard comprises a keyboard controller, configured to control at least the capacitance sampling of the primary capacitive sensor and to couple the button actuator to the defined electric potential at least during the capacitance sampling. The

keyboard controller may be of any suitable type, comprising a microcontroller or a microprocessor without limitation.

5 In some embodiments, each data entry button comprises a button cap that can be depressed by the user, which button cap is arranged on a first side of the respectively associated button actuator. In some embodiments, the primary capacitive sensor is arranged on a second side of the button actuator, opposite to the first side thereof.

10 In some embodiments, the keyboard further comprises a shield removal detection circuit to determine tampering with one or more of the button actuators. The determination of tampering in this context may comprise, without limitation, removal of one or more of the button actuators and/or the buttons. In some embodiments where the keyboard comprises button caps, the determination of tampering may further comprise a detection of a direct contact of one of the button actuators by a human or by a conductive probe, since this would be indicative of the removal of the respective plastic button cap of the button. The preceding embodiments further increase the security of the keyboard.

15 In some embodiments, the shield removal detection circuit is configured to erase data and/or suspend operation of the keyboard when tampering is detected. In some embodiments, a tampering indicator, such as a corresponding LED, is activated. In some embodiments, a tampering indicator message is provided to a remote server in case tampering is detected. In some embodiments, the keyboard controller is connected to the shield removal detection circuit and is configured to control the operation of the shield removal detection circuit.

20 The shield removal detection circuit may be of any suitable type. In some embodiments, the shield removal detection circuit comprises, for each of the data entry buttons, a secondary capacitive sensor. The secondary capacitive sensor may be of any suitable type, for example, a mutual-capacitance sensor or a self-capacitance sensor. It is noted that in some embodiments, the secondary capacitive sensor may not be configured to determine, whether a button was pressed by the user, but only to determine tampering with one of the button actuators.

In some embodiments, the secondary capacitive sensor is arranged between the button actuator and the primary capacitive sensor. The present embodiments result in a very compact setup.

30 In some embodiments, the keyboard comprises at least one printed circuit board, which printed circuit board comprises one or more of the primary capacitive sensor and the secondary capacitive sensor. In particular and in some embodiments, the primary capacitive sensor is

arranged in an intermediate layer of the printed circuit board. The latter setup further increases the reliability of the keyboard, as dust or other environmental influences do not interfere with the detection of the user's button press.

According to another aspect, a point-of-sale (POS) device is provided that comprises at least a POS transaction processor and one or more of data entry buttons that can be depressed by a user. The POS device further comprises for each of the data entry buttons a button actuator, movable upon the user depressing the respective button; and a primary capacitive sensor, arranged to determine movement of the button actuator of the respective data entry button by capacitance sampling. According to this aspect, the button actuator is at least partly made from a conductive material; and the button actuator is coupled to a defined electric potential at least during the capacitance sampling to shield the primary capacitive sensor from eavesdropping.

The POS device according to the present aspect and in further embodiments may be configured according to one or more of the embodiments, discussed in the preceding with reference to the preceding aspect. With respect to the terms used for the description of the present aspect and their definitions, reference is made to the discussion of the preceding aspect.

In some embodiments, the POS transaction processor is configured to process credit card transactions of a connected credit card reader.

According to another aspect, a method of secure data entry with a keyboard is provided. The keyboard comprises one or more of data entry buttons that can be depressed by a user; and for each of the data entry buttons, a button actuator, movable upon the user depressing the respective data entry button and being at least partly made from a conductive material; and a primary capacitive sensor. The method of this aspect comprises sampling of the primary capacitive sensor to determine movement of the button actuator; and at least during the sampling, coupling or connecting the button actuator to a defined electric potential to shield the primary capacitive sensor from eavesdropping.

The method according to the present aspect and in further embodiments may be configured according to one or more of the embodiments, discussed in the preceding with reference to the preceding aspects. With respect to the terms used for the description of the present aspect and their definitions, reference is made to the discussion of the preceding aspects. In some embodiments, the preceding method steps of sampling of the primary capacitive sensor to determine movement of the button actuator; and at least during the

sampling, coupling the button actuator to a defined electric potential to shield the primary capacitive sensor from eavesdropping, are repeated during the operation of the keyboard.

Reference will now be made to the drawings in which the various elements of embodiments will be given numerical designations and in which further embodiments will be discussed.

Specific references to components, sections, parts, process steps, and other elements are not intended to be limiting. Further, it is understood that like parts bear the same reference numerals, when referring to alternate figures. It is further noted that the figures are schematic and provided for guidance to the skilled reader and are not necessarily drawn to scale. Rather, the various drawing scales, aspect ratios, and numbers of components shown in the figures may be purposely distorted to make certain features or relationships easier to understand.

As one of skill in the art will readily recognize, in the field of access control, such as for electronic payments or access to an electronic (e.g., computer access) or physical (e.g., building) resource and in particular when entering a password, it is important that the password stays secure and is only known to the authorized user(s) thereof. In the recent past, malicious third parties have tried to obtain personal identification numbers (PINs) from point-of-sale (POS) credit card terminals by placing a “scanner” close to the terminal, which scanner traces low/high signal changes of a keypad’s column and row circuits. In the following, an exemplary POS device 1 will be described in more detail that comprises a keyboard for secure data entry and that reduces the chance of a successful scanning attack by a malicious third party.

FIG. 1 shows a first embodiment of a point-of-sale (POS) device / system 1, i.e., a POS credit card / debit card processing terminal. The POS device 1 comprises a display 2, a magnetic card reader 3a, a chip reader 3b, and in particular, a keyboard 4 for secure data entry. FIG. 2 shows a schematic block diagram of the POS device 1, which shows further components, namely a communication interface 5, POS processor 6, and power supply 7. The POS processor 6 controls the operation of the POS device 1 and comprises a microprocessor and memory, the latter comprising firmware, i.e., software to provide transaction processing functionality of the POS device 1. The communication interface 5 is a wired/wireless LAN Ethernet interface for connection to a private or public network and serves, corresponding to typical POS device 1, to transmit transaction data to and to obtain an authorization for the respective transaction from a remote transaction processing server. The POS device 1 further comprises a power supply 7

for providing operating power to all other components of the device 1. So as not to obscure the drawing, connections from and to the power supply 7 have been omitted in FIG. 2.

In the following, the setup of keyboard 4 is discussed in detail. A partial, exploded view of the keyboard 4 is shown in FIG. 3. As shown in the drawing, the keyboard 4 comprises a plurality of data entry buttons 30, each comprising a plastic button cap 31 and a button actuator 32. Button actuator 32 in the present embodiment is dome-shaped and made of metal. The button actuator 32 is deformable when a user exerts force on it, i.e., upon depressing the respective data entry button 30 and is used to indicate that the respective button has been depressed. Button actuator 32 also acts as a spring so that the data entry button 30 returns to its original position when the user's force is removed.

The keyboard 4 further comprises a multi-layer printed circuit board (PCB) 33. An intermediate layer 35 of the PCB comprises a plurality of primary capacitive sensors 40, i.e., one sensor 40 per button 30. The primary capacitive sensors 40 are used to detect whether the user has depressed the respective data entry button 30 by capacitive sampling. The primary capacitive sensors 40 are mutual-capacitance sensors.

FIG. 4 shows a schematic top-view of the intermediate PCB layer 35. Each primary capacitive sensor 40 comprises a transmission (TX) node 41 and a reception (RX) node 42, which are connected with a keyboard controller 43 in a row/column setup. It is noted that the keyboard controller 43 is placed on the lowest PCB layer 37, which will be discussed in detail in the following with reference to FIG. 6.

The keyboard controller 43 during capacitive sampling generates a pulsed electric field between the transmission node 41 and the reception node 42 of each primary capacitive sensor 40 and determines over multiple pulses, whether the electric field has changed. The electric field between the TX node 41 and RX node 42 in the present embodiment is influenced by the metallic button actuator 32. If the actuator 32 is deformed by a user depressing the respective data entry button 30, the electric field in the associated primary capacitive sensor 40 will change, indicating that the button 30 was pressed by the user to the keyboard controller, which in turn provides corresponding information to POS processor 6.

The signal change of mutual-capacitive sensors 40 upon a user pressing a button 30 is relatively small, compared to prior art keyboards using electric contacts. Thus, the possibility to monitor the signal change by a malicious third party is reduced. In addition, the present setup provides a key depression detection that does not rely on an electrical contact to be closed and

opened, which provides a highly reliable setup, irrespective of environmental conditions, such as the presence of dust, moisture, etc., which may be problematic in a keyboard using electric contacts.

To further reduce the possibility of eavesdropping on the internal signals of the keyboard 4, the keyboard controller 34 couples the metallic button actuators 32 to ground potential during the capacitive sampling of the primary capacitive sensors 40. The metallic button actuators 32 thus form an active shield for the primary capacitive sensors 40.

A further active shielding function is provided by top PCB layer 34, which is shown in a schematic top view in FIG. 5. PCB layer 34 comprises secondary capacitive sensors 50, which in the present embodiment are formed as self-capacitive sensors 50. The purpose of the secondary capacitive sensors 50 is two-fold. On one hand, the secondary capacitive sensors 50 provide additional shielding for the primary capacitive sensors 40. On the other hand, the secondary capacitive sensors 50 together with button actuators 32 form part of a shield removal detection circuit 51 to allow a determination, whether the device 1 has been tampered with, e.g., whether the metallic button actuators 32 that shield the primary capacitive sensors 40 have been touched or removed.

The secondary capacitive sensors 50 are arranged on the top of the primary capacitive sensors 40 and are connected to keyboard controller 43 in five rows for cost-saving reasons. This is possible, since, as discussed in the preceding, the secondary capacitive sensors 50 are not designed to determine which button 30 is depressed by the user, but to monitor if any button 30 has been tampered with, such as by removing button actuator 32 or top PCB layer 34 by a malicious person. The secondary capacitive sensors 50 also determine if the button actuators 32 have been touched directly by a human or by a conductive probe, both of which are indicative that the button caps 31 have been removed.

The secondary capacitive sensors 50 and the primary capacitive sensors 40 are sampled in turn by the keyboard controller 43. During the capacitive sampling of the primary capacitive sensors 40, the button actuators 30, via the secondary capacitive sensors 50 are controlled to ground potential. During the capacitive sampling of the secondary capacitive sensors 50, i.e., in normal operation, it is determined, whether a button actuator 32 is removed. It is noted, that the secondary capacitive sensors 50 are not used to determine if the user presses on the button cap 31. Instead, a signal change is determined, when the button actuator 32 is removed, or as mentioned, when the button actuator 32 is touched directly. In these cases, the keyboard

controller 43 will stop capacitive sampling and send an alert to POS processor 6 to remove secure data in the POS processor 6 and inform the remote transaction processing server of the evident tampering, as can be seen from the flow chart of FIG. 7.

As shown in FIG. 5, the top PCB layer 34, i.e., the area outside of the secondary capacitive sensors 50, is connected to ground 52. PCB layer 34 may comprise a continuous metallization or, e.g., a “hash-type” metallization, for a further improved shielding of the primary capacitive sensors 50. A corresponding metallization is present on the bottom intermediate PCB layer 36 for additional shielding.

FIG. 6 shows a schematic top view of the bottom PCB layer 37. As discussed in the preceding, layer 37 comprises the keyboard controller 43 and comprises various connections to PCB layers 34 and 35 as well as to POS processor 6 using bus connection 60. Not shown in FIG. 6 are power and miscellaneous connections.

FIG. 8 shows alternate embodiments for button actuator 32, marked with reference numerals 32a and 32b. The setup of button actuator 32b will prevent the flat part of the actuator to approach the surface of the PCB 34, resulting in less field change when the button actuator is depressed. This setup provides a further improved resistance to eavesdropping.

The benefits of the described embodiment include a) an increased security against eavesdropping by using mutual-capacitance sensors, resulting in a relatively small signal change when a button is depressed by a user, b) insensitivity of the arrangement to environmental conditions, in particular to dust, c) improved reliability as no electric contacts are used for determining if a button is depressed, d) reduced cost compared to prior art designs using a silver paste mask, and e) employment of button actuators, acting as a spring to provide haptic feedback to the user.

While the invention has been illustrated and described in detail in the drawings and foregoing description, such illustration and description are to be considered illustrative or exemplary and not restrictive; the invention is not limited to the disclosed embodiments. For example, it is possible to operate the invention in an embodiment in which:

(1) mutual-touch and self-touch sensors are combined to form a secure keypad for a POS, resource (electronic or physical) access application;

(2) mutual-touch sensors are embedded in an intermediate PCB layer, arranged under every individual plastic button and the mutual-touch sensors are designed to sample the minor mutual capacitor change between a TX and a RX line;

(3) metal dome button actuators are coupled to GND when sampling the mutual capacitor sensors and when a user presses the plastic part of a button, this leads to the distortion of the metal dome, and the distortion of the metal dome will lead to a change of distance between the center part of the metal dome and the PCB surface, which in turn causes a mutual capacitor change that is sampled in this embodiment;

(4) self-touch sensors cover the top of every individual mutual touch sensor and the self-touch sensors are divided into several groups;

(5) the self-touch sensors are not designed to determine which button is pressed by the user, but to monitor if any keypad had been uncovered or touched by a person;

(6) self-touch sensors and mutual sensors are sampled in turn and in normal operation, the self-touch sensor will not lead to self-signal change when user presses on the top of the plastic part of the button;

(7) when the self-sensor detects a signal change (i.e., touch or anti-touch signal), the touch controller will stop the mutual touch sample timing, and send an alert to a main controller to remove secure data in the POS; and/or

(8) a self-sensor pad is in contact with the metal dome to form a self-sensor when in self sampling and/or coupled to GND when in mutual sampling.

Other variations to the disclosed embodiments can be understood and effected by those skilled in the art in practicing the claimed invention, from a study of the drawings, the disclosure, and the appended claims. In the claims, the word "comprising" does not exclude other elements or steps, and the indefinite article "a" or "an" does not exclude a plurality. A single processor, module or other unit may fulfill the functions of several items recited in the claims.

The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage. A computer program may be stored/distributed on a suitable medium, such as an optical storage medium or a solid-state medium supplied together with or as part of other hardware, but may also be distributed in other forms, such as via the Internet or other wired or wireless telecommunication systems. Any reference signs in the claims should not be construed as limiting the scope.

CLAIMS

1. A keyboard for secure data entry, comprising:
one or more of data entry buttons that can be depressed by a user; and
5 for each of the data entry buttons:
a button actuator, movable upon the user depressing the respective data entry
button; and
a primary capacitive sensor, arranged to determine movement of the button
actuator of the respective data entry button by capacitance sampling;
10 wherein:
the button actuator is at least partly made from a conductive material; and
the button actuator is coupled to a defined electric potential at least during the
capacitance sampling to shield the primary capacitive sensor from eavesdropping.
- 15 2. The keyboard of claim 1, wherein the primary capacitive sensor is a mutual-
capacitance sensor.
3. The keyboard of any claims 1-2, further comprising a shield removal detection circuit
to determine tampering with one or more of the button actuators.
- 20 4. The keyboard of claim 3, wherein the shield removal detection circuit is configured to
erase data and/or suspend operation of the keyboard when tampering with one or
more of the button actuators is determined.
- 25 5. The keyboard of any claims 3-4, wherein the shield removal detection circuit
comprises, for each of the data entry buttons, a secondary capacitive sensor.
6. The keyboard of claim 5, wherein the secondary capacitive sensor is arranged
between the button actuator and the primary capacitive sensor.
- 30 7. The keyboard of any of claims 5-6, wherein the secondary capacitive sensor is a self-
capacitive sensor.

8. The keyboard of any of claims 5-7, further comprising at least one printed circuit board, comprising one or more of the primary capacitive sensor and the secondary capacitive sensor.
9. The keyboard of claim 8, wherein the primary capacitive sensor is arranged in an intermediate layer of the printed circuit board.
10. The keyboard of any of claims 1-9, wherein the button actuator is dome-shaped.
11. The keyboard of any of claims 1-10, wherein the button actuator is made from metal.
12. The keyboard of any of claims 1-11, comprising multiple data entry buttons, arranged in a matrix.
13. The keyboard of claim 12, wherein the multiple data entry buttons are arranged to form a numeric keypad.
14. The keyboard of any of claims 1-13, further comprising a keyboard controller, configured to control at least the capacitance sampling of the primary capacitive sensor and to couple the button actuator to the defined electric potential at least during the capacitance sampling.
15. The keyboard of any of claims 1-15, wherein the defined electric potential is ground.

16. A point-of-sale device comprising:

a point-of-sale transaction processor;

one or more of data entry buttons that can be depressed by a user; and

for each of the data entry buttons:

5 a button actuator, movable upon the user depressing the respective button; and

a primary capacitive sensor, arranged to determine movement of the button actuator of the respective data entry button by capacitance sampling; wherein

10 the button actuator is at least partly made from a conductive material; and

the button actuator is coupled to a defined electric potential at least during the capacitance sampling to shield the primary capacitive sensor from eavesdropping.

15

17. A method of secure data entry with a keyboard, wherein the keyboard includes one or more data entry buttons that can be depressed by a user, wherein each of the data entry buttons includes a button actuator movable upon the user depressing the respective data entry button and being at least partly made from a conductive material, and the keyboard includes a primary capacitive sensor, wherein the method comprises:

20

sampling of the primary capacitive sensor to determine movement of the button actuator; and

25

at least during the sampling, coupling the button actuator to a defined electric potential to shield the primary capacitive sensor from eavesdropping.

18. The method of claim 17, wherein the keyboard is configured according to at least one of claims 1.

1/5

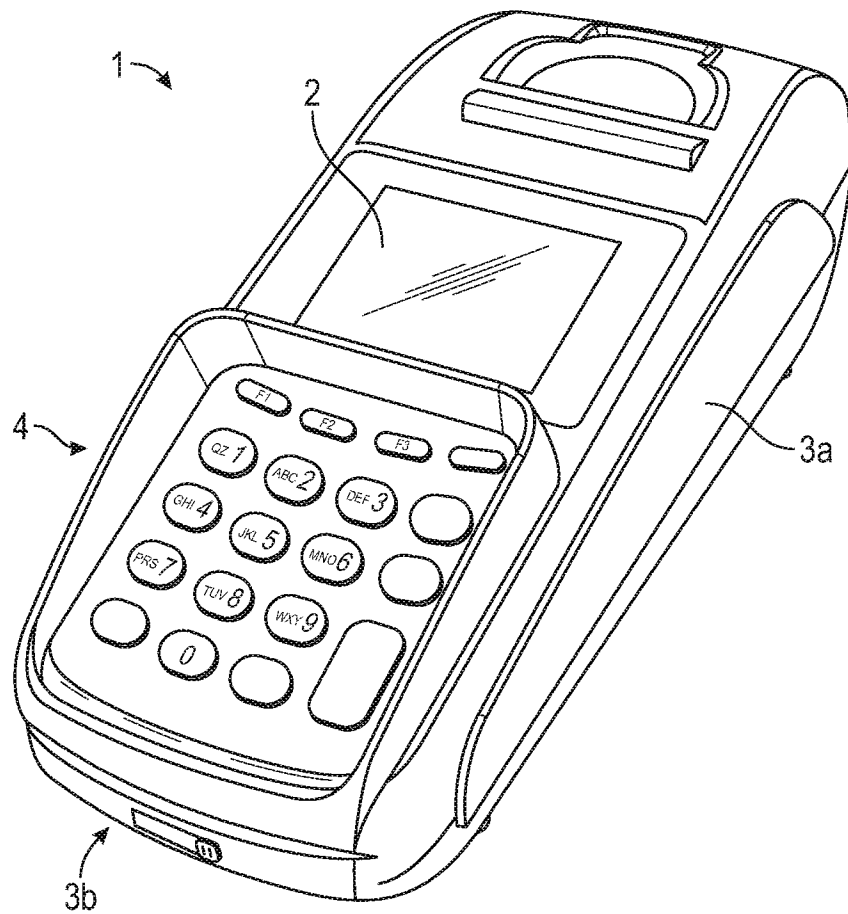


FIG. 1

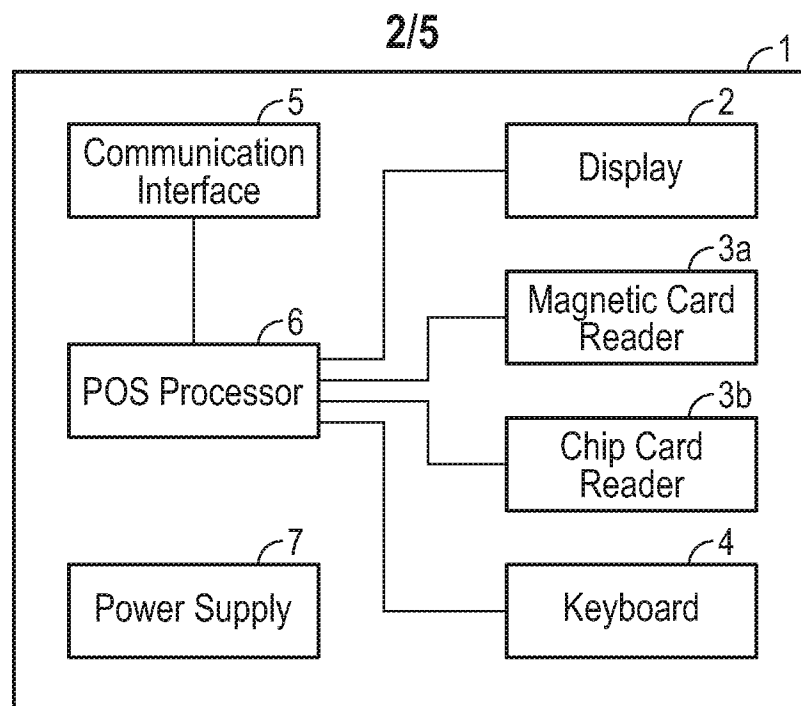


FIG. 2

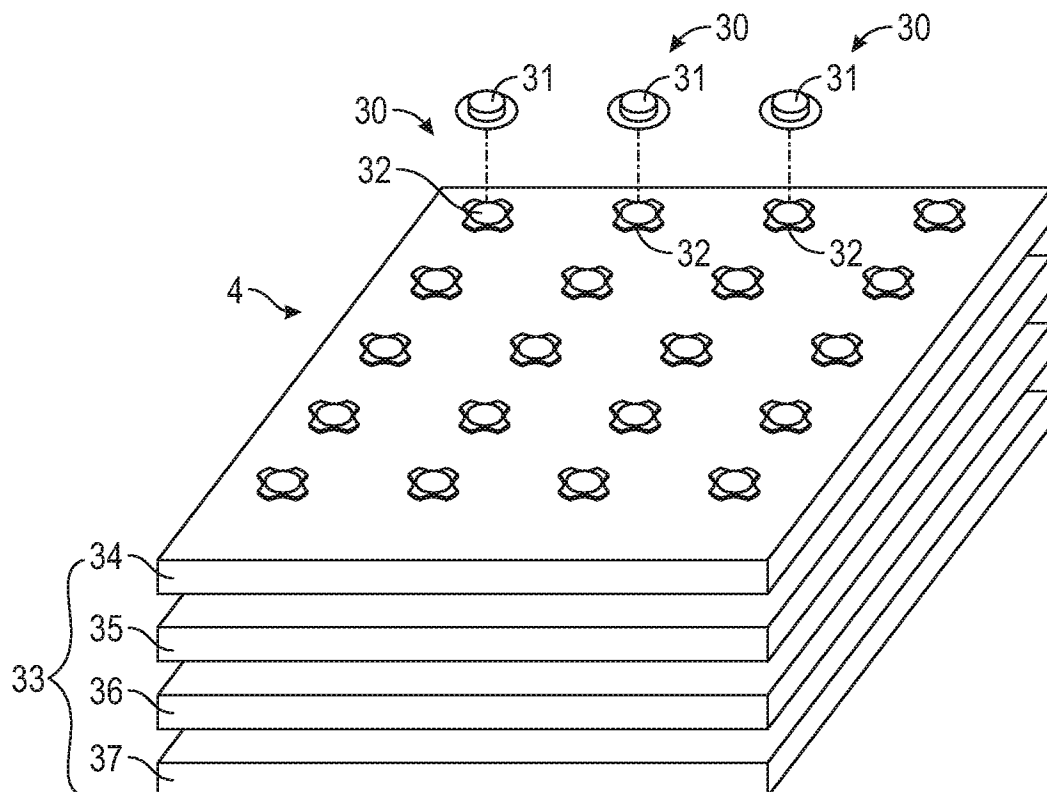


FIG. 3

3/5

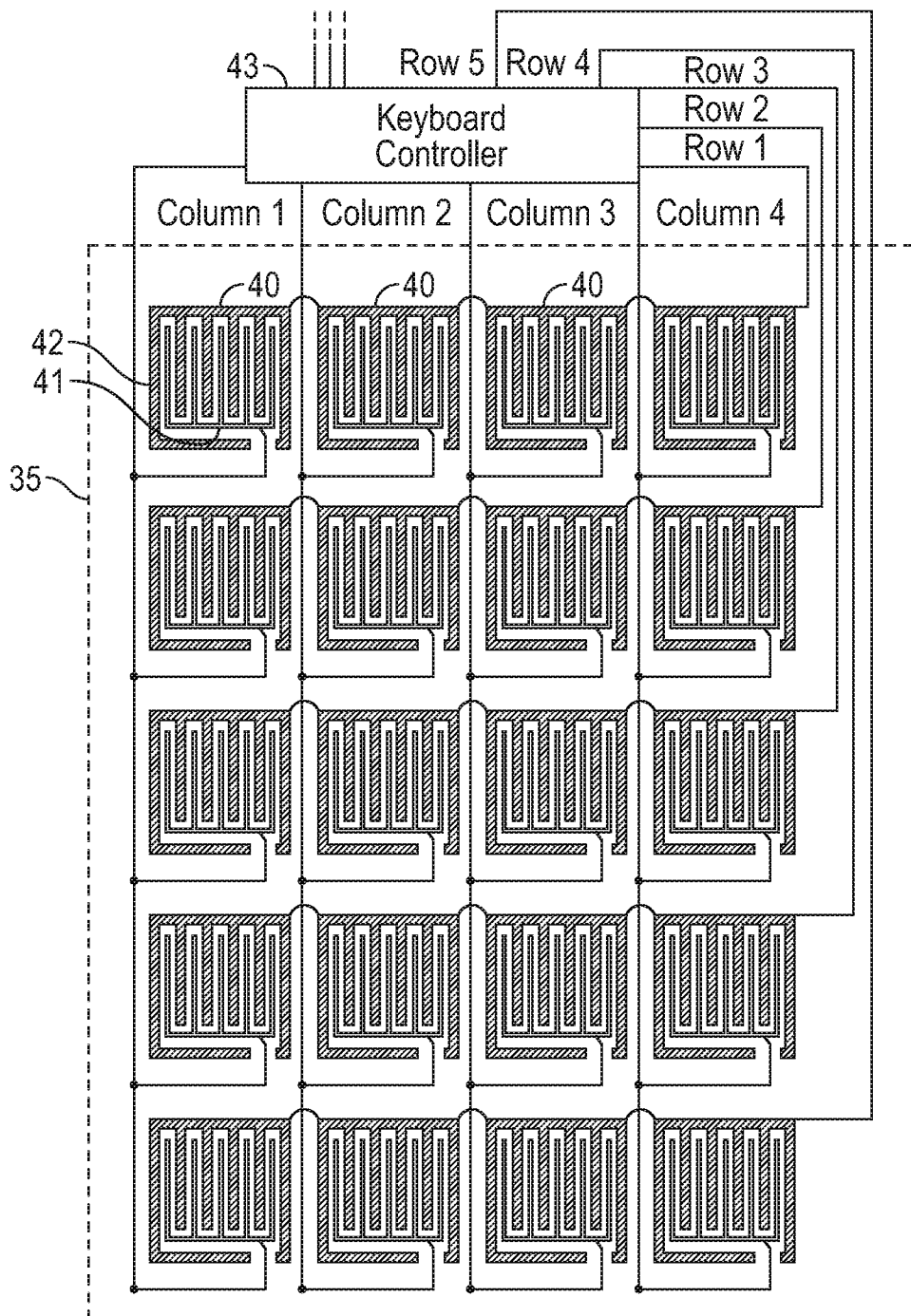


FIG. 4

4/5

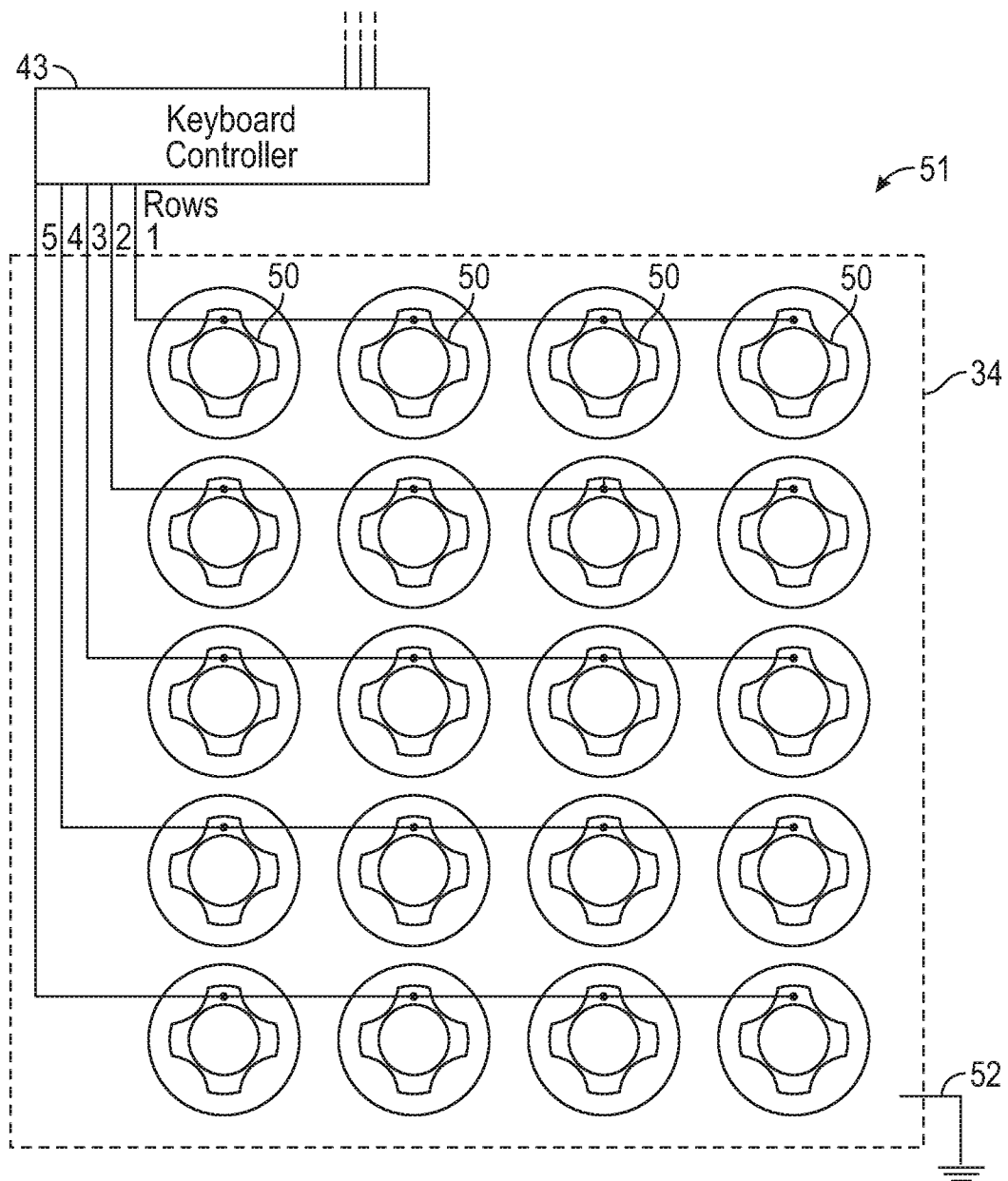


FIG. 5

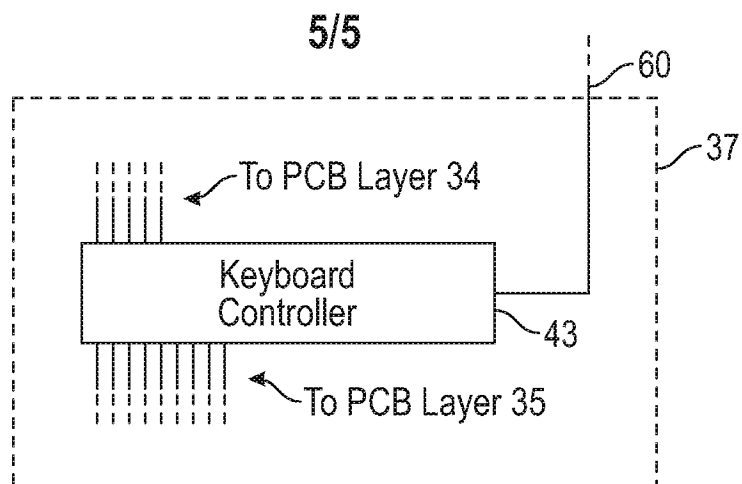


FIG. 6

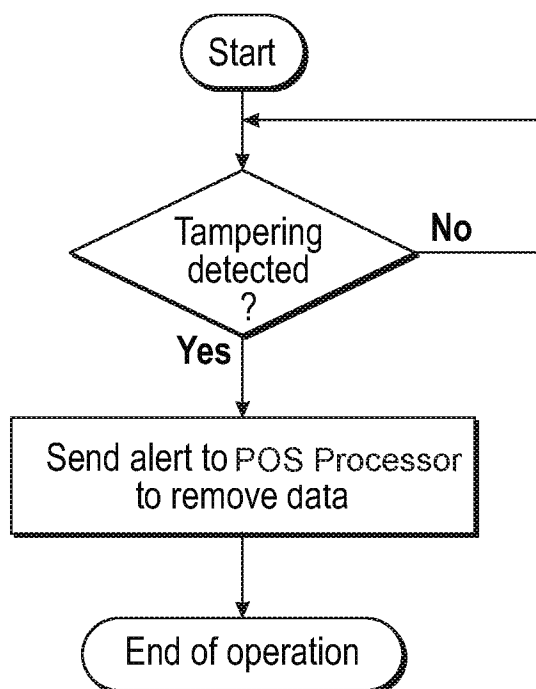


FIG. 7

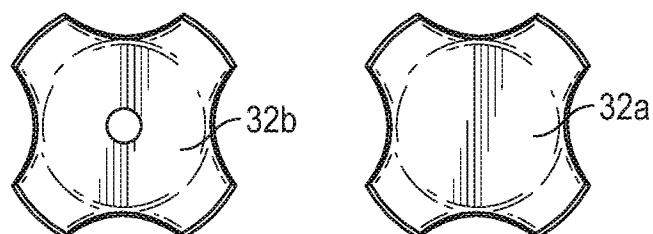


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2019/055774

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/86 G06F21/83
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/253505 A1 (VINCENT PAUL [US] ET AL) 11 September 2014 (2014-09-11) paragraph [0047] paragraph [0050] paragraph [0063] paragraph [0079] paragraph [0086]	1-18
A	----- MONACO JOHN: "SoK: Keylogging Side Channels", 2018 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP), IEEE, 20 May 2018 (2018-05-20), pages 211-228, XP033377735, DOI: 10.1109/SP.2018.00026 [retrieved on 2018-07-23] page 221, column 2, paragraph V ----- -/-	1-18



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

10 December 2019

Date of mailing of the international search report

19/12/2019

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Medvesan, Oana

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2019/055774

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014/375481 A1 (MCNICOLL GRANT A [GB]) 25 December 2014 (2014-12-25) paragraph [0056] -----	1-18
A	US 2011/095919 A1 (OSTERMOELLER MICHAEL [DE] ET AL) 28 April 2011 (2011-04-28) paragraph [0016] -----	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2019/055774

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014253505 A1	11-09-2014	CN 103503315 A	08-01-2014
		JP 2014512051 A	19-05-2014
		KR 20140012733 A	03-02-2014
		US 2012280923 A1	08-11-2012
		US 2014253505 A1	11-09-2014
		WO 2012139133 A1	11-10-2012

US 2014375481 A1	25-12-2014	BR 102014015621 A2	22-03-2016
		CN 104252608 A	31-12-2014
		EP 2819059 A1	31-12-2014
		US 2014375481 A1	25-12-2014

US 2011095919 A1	28-04-2011	DE 102008009936 A1	03-09-2009
		US 2011095919 A1	28-04-2011
		WO 2009103594 A1	27-08-2009
