(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 626 777**

(51) Int. CI.:

G06F 21/83 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.07.2014 E 14177204 (6)**

(97) Fecha y número de publicación de la concesión europea: **01.03.2017 EP 2829999**

(54) Título: **Dispositivo de refuerzo de la seguridad de un teclado capacitivo y terminal correspondiente**

(30) Prioridad:

26.07.2013 FR 1357422

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.07.2017

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

FLEURY, FABRICE y
LEMAIRE, JEAN-ERIC

(74) Agente/Representante:

ELZABURU SLP, .

DESCRIPCIÓN

Dispositivo de refuerzo de la seguridad de un teclado capacitivo y terminal correspondiente

1 CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo del refuerzo de la seguridad de terminales de pago y, más en particular, a la protección de los datos introducidos por un usuario por intermedio de tales terminales.

En efecto, tales datos, como por ejemplo el código secreto introducido por el usuario, se pueden considerar datos sensibles que tienen que ser protegidos de ocasionales “piratas”, con el fin de cumplir con unas normas de seguridad y aprobaciones para la explotación comercial de tales terminales.

En particular, la invención es de aplicación en los terminales de pago electrónicos que presentan un teclado capacitivo.

2 SOLUCIONES DE LA TÉCNICA ANTERIOR

Ciertos terminales de pago electrónicos actuales integran un teclado táctil, lo cual plantea nuevos problemas de seguridad relacionados con el espionaje de la utilización de tales teclados.

En efecto, existen sistemas “espías” encaminados a tratar de averiguar los datos introducidos por el usuario por intermedio del teclado táctil del terminal de pago electrónico, mediante observación de los “rastros” dejados por los dedos del usuario, o también mediante medida del nivel de señal en las teclas de un teclado capacitivo. Ahora bien, hasta la fecha no existen soluciones fiables que permitan paliar estos problemas de “pirateo” de teclado capacitivo.

Algunas soluciones conocidas tienen como finalidad detectar el deterioro de tal teclado, como por ejemplo un arrancamiento o una fractura del cristal del teclado, mediante la añadidura de un “anillo de guarda” alrededor del teclado, por ejemplo en forma de una línea conductora de cobre o según una tecnología llamada “ITO” (por “Indium Tin Oxide”).

En cambio, este tipo de soluciones de protección de los teclados táctiles contra la intrusión no permite solucionar los problemas de pirateo de los datos introducidos por intermedio de los teclados capacitivos.

El documento WO 2012/139133 A1 describe un dispositivo de refuerzo de la seguridad de un teclado capacitivo que comprende un circuito que permite la conexión de una capacidad entre el electrodo receptor y un electrodo emisor, con el fin de simular una pulsación de tecla sobre el teclado.

3 SUMARIO DE LA INVENCIÓN

La invención no presenta los inconvenientes del estado de la técnica. En efecto, la invención concierne a un dispositivo de refuerzo de la seguridad de un teclado capacitivo de un terminal de pago electrónico que comprende al menos un procesador de gestión de las teclas de dicho teclado capacitivo según la reivindicación 1.

De acuerdo con la invención, el dispositivo de refuerzo de la seguridad es apto para comunicarse con dicho procesador, y dicho dispositivo de refuerzo de la seguridad comprende un módulo de pilotaje (10) de al menos un elemento de simulación (S) de al menos una pulsación de tecla sobre dicho teclado capacitivo, comprendiendo dicho módulo de pilotaje unos medios de recepción (101) de al menos un comando de simulación (Cmd1) transmitido aleatoriamente por dicho procesador.

De este modo, la invención propone una solución novedosa e inventiva del refuerzo de la seguridad de un teclado capacitivo de un terminal de pago electrónico, especialmente frente a “piratas” que ponen en práctica sistemas de espionaje de la introducción de un código confidencial basados en una medida del nivel de señal de las teclas, por ejemplo.

La solución de la invención está basada en la simulación de pulsaciones de teclas aleatorias, por ejemplo durante una introducción de datos confidenciales por un usuario, para así perturbar un ocasional espionaje. Por otro lado, al estar pilotada esta simulación por el propio procesador de gestión de las teclas del teclado capacitivo del terminal de pago electrónico, este procesador no se ve perturbado por estas pulsaciones simuladas de teclas, pues no interpreta como pulsaciones reales de teclas las pulsaciones simuladas de teclas que motiva.

En cambio, un dispositivo espía, puesto en práctica en el teclado capacitivo del terminal de pago electrónico, se encuentra perturbado por estas pulsaciones aleatorias de teclas, a las que interpreta como pulsaciones reales de teclas, las cuales, por tanto, le impiden detectar los datos sensibles introducidos en el mismo momento por el usuario.

De acuerdo con una característica particular de la invención, el elemento de simulación (S) pone en práctica al menos una capacidad (CP1) de un valor predeterminado, llamada capacidad parásita, y el módulo de pilotaje dispara la actuación de dicha capacidad parásita (CP1) mediante cierre de al menos un interruptor, uniéndose dicha

capacidad parásita (CP1), cuando dicho interruptor está cerrado, a al menos un electrodo receptor (Y1) unido a al menos una tecla de dicho teclado capacitivo.

De este modo, de acuerdo con esta forma de realización, el dispositivo de refuerzo de la seguridad pone en práctica una simulación de una pulsación de tecla por intermedio de una capacidad llamada parásita, disparada, por ejemplo, mediante el cierre de un interruptor a la recepción de un comando de simulación con origen en el procesador del terminal de pago electrónico. De esta manera, cuando el interruptor está cerrado, la capacidad parásita se encuentra directamente unida a un electrodo receptor, unido a su vez a una o varias teclas del teclado táctil.

Dependiendo de las características del comando de simulación (duración, frecuencia, ...), se ven interesadas una o varias teclas unidas al electrodo receptor y, por tanto, se simulan una o varias pulsaciones de teclas.

De acuerdo con un aspecto particular de la invención, el elemento de simulación (S) pone en práctica al menos una capacidad (CP1) de un valor predeterminado, llamada capacidad parásita, y el módulo de pilotaje dispara la actuación de dicha capacidad parásita (CP1) por mediación de al menos un transistor, uniéndose dicha capacidad parásita (CP1), cuando es activado dicho transistor, a al menos un electrodo receptor (Y1) unido a al menos una tecla de dicho teclado capacitivo.

De este modo, de acuerdo con esta forma de realización, el dispositivo de refuerzo de la seguridad pone en práctica una simulación de una pulsación de tecla por intermedio de una capacidad, llamada parásita, disparada, por ejemplo, por mediación de un transistor a la recepción de un comando de simulación con origen en el procesador del terminal de pago electrónico. De esta manera, cuando es activado el transistor, la capacidad parásita se encuentra directamente unida a un electrodo receptor, unido a su vez a una o varias teclas del teclado táctil.

Dependiendo de las características del comando de simulación (duración, frecuencia, ...), se ven interesadas una o varias teclas unidas al electrodo receptor y, por tanto, se simulan una o varias pulsaciones de teclas.

En particular, el módulo de pilotaje es apto para pilotar al menos dos capacidades parásitas (CP1, CP2), a la recepción de al menos dos comandos de simulación distintos (Cmd1, Cmd2) con origen en dicho procesador, uniéndose cada una de dichas capacidades parásitas a un electrodo receptor distinto (Y1, Y2) que permite la simulación de al menos todas las teclas numéricas de dicho teclado capacitivo.

De este modo, de acuerdo con esta forma de realización, pueden ser simuladas al menos todas las teclas numéricas, correspondientes la mayoría de las veces a los datos sensibles tales como un código confidencial o un número de tarjeta bancaria, para engañar a un ocasional dispositivo espía puesto en práctica en el teclado capacitivo del terminal de pago electrónico.

Por ejemplo, el valor predeterminado de dicha capacidad parásita se corresponde sensiblemente con un valor de capacidad representativo de una pulsación sobre una tecla de dicho teclado capacitivo.

De acuerdo con un aspecto particular de la invención, el dispositivo se implementa en una zona de seguridad de dicho terminal de pago electrónico.

De este modo, de acuerdo con esta forma de realización de la invención, el propio dispositivo de refuerzo de la seguridad queda situado, en el seno del terminal de pago electrónico, en una zona protegida por medios puestos en práctica en el terminal de pago electrónico, al objeto de que el dispositivo de refuerzo de la seguridad no pueda ser inhibido o deteriorado. Por lo tanto, la seguridad de la introducción de datos sensibles en el teclado capacitivo del terminal de pago electrónico es óptima.

Asimismo, la invención concierne a un terminal de pago electrónico, que comprende un dispositivo de refuerzo de la seguridad tal y como se ha descrito anteriormente.

Asimismo, la invención concierne a un procedimiento de refuerzo de la seguridad según la reivindicación 7.

Asimismo, la invención concierne a un programa de ordenador descargable desde una red de comunicación y/o almacenado en un soporte legible por ordenador y/o ejecutable por un procesador, que comprende instrucciones de código de programa para la ejecución del procedimiento de refuerzo de la seguridad tal y como se descrito anteriormente, cuando es ejecutado por un procesador.

4 LISTA DE FIGURAS

Otras características y ventajas de la invención se pondrán más claramente de manifiesto con la lectura de la siguiente descripción de una forma particular de realización, dada a título de mero ejemplo ilustrativo y no limitativo, y de los dibujos que se acompañan, de los que:

- la figura 1 presenta un esquema de un dispositivo de refuerzo de la seguridad de un teclado táctil de un

terminal de pago electrónico según una forma de realización de la invención;
- las figuras 2 y 4 presentan dos ejemplos de puesta en práctica de un dispositivo de refuerzo de la seguridad de un teclado táctil de un terminal de pago electrónico, según una forma de realización de la invención; y
- la figura 3 presenta las principales etapas del procedimiento de refuerzo de la seguridad de un teclado táctil de un terminal de pago electrónico, según una forma de realización de la invención.

5 DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

5.1 Principio general

El principio de la invención consiste en poner en práctica, en un terminal de pago electrónico, un dispositivo de refuerzo de la seguridad del teclado capacitivo del terminal de pago electrónico, encaminado a engañar a un ocasional sistema de espionaje de las pulsaciones de teclas sobre el teclado, por ejemplo, en la introducción de datos, llamados sensibles, por un usuario.

En efecto, el principio de la invención reside en la simulación de pulsaciones de teclas para así perturbar un ocasional sistema de espionaje basado en la medida de la señal en las teclas del teclado capacitivo. De este modo, esta simulación se puede poner en práctica, por ejemplo, al mismo tiempo que la introducción real de datos por un usuario por intermedio del teclado capacitivo, momento en el que también es puesto en práctica el ocasional dispositivo espía.

En cambio, el dispositivo de refuerzo de la seguridad no debe perturbar, mediante estas simulaciones de pulsaciones de teclas, el propio procedimiento de gestión de las teclas del terminal de pago electrónico. Esta es la razón por la que la invención prevé que el dispositivo de refuerzo de la seguridad se comunique con el procedimiento de gestión de las teclas del teclado capacitivo del terminal de pago electrónico. Esta comunicación puede llevarse a cabo directamente, del procesador de gestión de las teclas al dispositivo de refuerzo de la seguridad según la invención, o por intermedio de uno o varios módulos / elementos intermedios, según las diferentes formas particulares de realización de la invención.

De este modo, la invención prevé, según sus diferentes formas de realización, que este procesador transmita, aleatoriamente, uno o varios comandos de simulación de simulación de pulsaciones de teclas al dispositivo de refuerzo de la seguridad, con el fin de engañar a un ocasional sistema de espionaje. Por ende, el procesador, puesto que es el que motiva (directa o indirectamente) comandos de simulación de pulsaciones de teclas, no se ve perturbado en su interpretación de las pulsaciones “reales” de teclas, efectuadas por un usuario sobre el teclado. En efecto, el procesador sabe en qué momento transmite un comando de simulación de pulsación de tecla y, por tanto, no interpreta esta pulsación simulada de tecla como una pulsación real de tecla.

Finalmente, el carácter aleatorio de esta simulación de pulsaciones de teclas permite evitar una detección del dispositivo de refuerzo de la seguridad de la invención, al objeto de que no se pueda modificar un ocasional dispositivo espía para tenerlo en cuenta. De este modo, aun si un ocasional sistema espía llegara a sospechar la existencia de la puesta en práctica de este dispositivo de refuerzo de la seguridad según la invención, no podría tratar de sortearlo, al no ser identificables ni previsibles las pulsaciones simuladas de teclas, debido a su carácter aleatorio.

Es de señalar que la invención es asimismo de aplicación en todo terminal de pago que tiene una superficie sensible al tacto o “touch screen” que utiliza la tecnología capacitiva, es decir, que pone en práctica electrodos emisores / receptores.

5.2 Descripción de una forma de realización

Se describe a continuación con mayor detalle una forma de realización de un dispositivo de refuerzo de la seguridad de un teclado capacitivo de un terminal de pago electrónico, con referencia a las figuras 1 a 4.

La figura 1 ilustra un ejemplo de tal dispositivo que comprende un módulo de pilotaje 10 de un elemento de simulación S de pulsación(-ones) de tecla(s).

De acuerdo con esta forma de realización de la invención, el módulo de pilotaje comprende asimismo unos medios de recepción 101 de comando(s) de simulación transmitido(s) aleatoriamente por un procesador (el procesador de gestión de las teclas del teclado capacitivo o bien un procesador en relación con este último) del terminal de pago electrónico.

De este modo, a la recepción de un comando de simulación Cmd1, transmitido aleatoriamente por el procesador del terminal de pago electrónico y recibido por los medios de recepción 101 del módulo de pilotaje 10, este dispara la actuación del elemento de simulación S de una pulsación de tecla.

Un ocasional sistema de espionaje de las pulsaciones de teclas sobre el teclado capacitivo del terminal de pago electrónico detecta entonces una pulsación de tecla, sin poder, con todo, identificarla como una pulsación simulada

de tecla. Entonces se encuentra perturbado el espionaje y, por tanto, ya no es posible la identificación de los datos introducidos realmente por el usuario sobre este teclado capacitivo del terminal de pago electrónico.

De manera idónea, el dispositivo de refuerzo de la seguridad del teclado tan solo se activa en la introducción real de datos por un usuario sobre este teclado. En efecto, no es necesario (ni económico, en cuanto a optimización de la utilización de los componentes del terminal de pago electrónico), simular pulsaciones de teclas durante toda la utilización del terminal de pago electrónico, sino únicamente durante fases en las que es utilizado el teclado, e incluso únicamente cuando son susceptibles de ser introducidos por un usuario datos identificados como sensibles. Además, si se limita la activación del dispositivo de refuerzo de la seguridad a instantes concretos, se hace más difícil la detección de este dispositivo y se hace más eficaz su acción.

La figura 3 ilustra las principales etapas puestas en práctica en un dispositivo de refuerzo de la seguridad tal y como está presentado en la figura 1, a saber, una primera etapa de recepción 30 de un comando de simulación, transmitido aleatoriamente por el procesador del terminal de pago electrónico, que desencadena una etapa de pilotaje 31 de un elemento de simulación de pulsación de tecla, que conlleva una etapa de simulación 32 de una pulsación de tecla.

La figura 2, por su parte, ilustra un primer ejemplo de puesta en práctica de un dispositivo de refuerzo de la seguridad de un teclado táctil tal y como se ha descrito anteriormente, en un terminal de pago electrónico.

De este modo, en esta forma particular de realización, se asume que el teclado capacitivo se constituye a partir de una “matriz” de cuatro columnas y cuatro filas que, como es convencional, presenta unas teclas numéricas (del 0 al 9), así como unas teclas de función tales como “Validación”, “Anulación”, “Corrección”, etc.

Cada una de estas teclas está unida a un electrodo receptor que permite la detección de una pulsación de tecla, siendo estos electrodos receptores, en este ejemplo, en número de tres y señalados con Y0, Y1 e Y2.

De acuerdo con esta forma de realización de la invención, el dispositivo de refuerzo de la seguridad comprende un módulo de pilotaje que permite simular al menos una pulsación de tecla para todas las teclas numéricas, susceptibles de ser utilizadas, por ejemplo, para la introducción de un código confidencial. De este modo, el módulo de pilotaje permite simular una pulsación sobre las teclas unidas a los electrodos receptores Y1 e Y2 del teclado capacitivo, no viéndose interesado el electrodo receptor Y0 según esta forma particular de realización de la invención. Para conseguir esto, se necesitan dos elementos de simulación, señalados con CP1 y CP2.

Es de señalar que, según diferentes formas de realización de la invención, pueden verse interesados los tres electrodos receptores, para poder simular una pulsación sobre todas las teclas del teclado, que potencialmente precisa de tres elementos de simulación.

En esta forma de realización, cada elemento de simulación pone en práctica una capacidad, llamada parásita, que, cuando es disparada su actuación, permite simular una o varias pulsaciones de teclas.

De este modo, la capacidad parásita CP1 se une, cuando es disparada su actuación, al electrodo receptor Y1, y la capacidad parásita CP2 se une, cuando es disparada su actuación, al electrodo receptor Y2.

Por otro lado, el módulo de pilotaje comprende dos interruptores Inter1 e Inter2, que se cierran a la recepción de un comando de simulación específico, recibido con origen en el procesador, respectivamente señalados con Cmd1 y Cmd2. Estos dos interruptores Inter1 e Inter2 permiten unir, respectivamente, la capacidad parásita CP1 al electrodo receptor Y1 y la capacidad parásita CP2 al electrodo receptor Y2.

De este modo, cuando es recibido por el dispositivo de refuerzo de la seguridad un comando de simulación Cmd1, por intermedio de los medios de recepción de su módulo de pilotaje, el interruptor Inter1 une la capacidad parásita CP1 al electrodo Y1, simulando así, según los parámetros del comando de simulación Cmd1, una pulsación sobre una o varias de las teclas 1, 4, 7, +, F, Ca, Cl y V.

Igualmente, cuando es recibido por el dispositivo de refuerzo de la seguridad un comando de simulación Cmd2, por intermedio de los medios de recepción de su módulo de pilotaje, el interruptor Inter2 une la capacidad parásita CP2 al electrodo Y2, simulando así, según los parámetros del comando de simulación Cmd2, una pulsación sobre una o varias de las teclas 2, 5, 8, 0, 3, 6, 9 y −.

En la práctica, no es necesario que se puedan simular todas las teclas, la simulación aleatoria de cuatro teclas numéricas, por ejemplo, permite engañar a un ocasional dispositivo espía, sin dejar de ser indetectable.

De acuerdo con una variante de realización, ilustrada en la figura 4, el módulo de pilotaje del dispositivo de refuerzo de la seguridad pone en práctica uno o varios transistores (T1, T2) que, ante la recepción de uno o varios comandos de simulación (Cmd1, Cmd2) del procesador del terminal de pago electrónico, permiten disparar la actuación de una

o varias capacidades parásitas (CP1, CP2), que a su vez permiten perturbar uno o varios electrodos receptores (Y1, Y2) del teclado capacitivo.

Por supuesto, se puede poner en práctica cualquier otro medio que permita suministrar una pequeña capacidad para la simulación de una pulsación de tecla sobre un teclado capacitivo, según otras formas particulares de realización de la invención, no descritas en el presente documento.

REIVINDICACIONES

1. Dispositivo de refuerzo de la seguridad de un teclado capacitivo de un terminal de pago electrónico que comprende al menos un procesador de gestión de las teclas de dicho teclado capacitivo,

- siendo apto dicho dispositivo de refuerzo de la seguridad para comunicarse con dicho procesador,
- comprendiendo dicho dispositivo de refuerzo de la seguridad un módulo de pilotaje (10) de al menos un elemento de simulación (S) de al menos una pulsación de tecla sobre dicho teclado capacitivo,
- comprendiendo dicho módulo de pilotaje unos medios de recepción (101) de al menos un comando de simulación (Cmd1) transmitido aleatoriamente por dicho procesador,
- poniendo en práctica dicho elemento de simulación (S) al menos una capacidad (CP1) de un valor predeterminado, llamada capacidad parásita,
- disparando dicho módulo de pilotaje la actuación de dicha capacidad parásita (CP1) mediante cierre de al menos un interruptor, uniéndose dicha capacidad parásita (CP1), cuando dicho interruptor está cerrado, a al menos un electrodo receptor (Y1) unido a al menos una tecla de dicho teclado capacitivo, y
- siendo apto dicho módulo de pilotaje para pilotar al menos dos capacidades parásitas (CP1, CP2), disparando la actuación de dichas al menos dos capacidades parásitas (CP1, CP2) mediante cierre de al menos un interruptor, a la recepción de al menos dos comandos de simulación distintos (Cmd1, Cmd2) con origen en dicho procesador, uniéndose cada una de dichas capacidades parásitas, cuando dicho al menos un interruptor está cerrado, a un electrodo receptor distinto (Y1, Y2) que permite la simulación de al menos todas las teclas numéricas de dicho teclado capacitivo.

2. Dispositivo de refuerzo de la seguridad según la reivindicación 1, **caracterizado por que** dicho interruptor es un transistor.

3. Dispositivo de refuerzo de la seguridad según la reivindicación 1, **caracterizado por que** dicho valor predeterminado de dicha capacidad parásita se corresponde sensiblemente con un valor de capacidad representativo de una pulsación sobre una tecla de dicho teclado capacitivo.

4. Dispositivo de refuerzo de la seguridad según la reivindicación 3, **caracterizado por que** se implementa en una zona de seguridad de dicho terminal de pago electrónico.

5. Terminal de pago electrónico, **caracterizado por que** comprende un dispositivo de refuerzo de la seguridad según una cualquiera de las reivindicaciones 1 a 4.

6. Procedimiento de refuerzo de la seguridad de un teclado capacitivo de un terminal de pago electrónico que comprende al menos un procesador de gestión de las teclas de dicho teclado capacitivo, comprendiendo el procedimiento las siguientes etapas, puestas en práctica en un dispositivo de refuerzo de la seguridad apto para comunicarse con dicho procesador:

- una etapa de recepción (30) de al menos un comando de simulación (Cmd1) transmitido aleatoriamente por dicho procesador;
- una etapa de pilotaje (31), desencadenada por dicha etapa de recepción, de al menos un elemento de simulación (S) que pone en práctica al menos una capacidad (CP1) de un valor predeterminado, llamada capacidad parásita, y que permite simular al menos todas las teclas de dicho teclado capacitivo;

una etapa de simulación (32) de al menos una pulsación de tecla sobre dicho teclado capacitivo mediante disparo de la actuación de al menos dos capacidades parásitas (CP1, CP2) mediante cierre de al menos un interruptor, uniéndose cada una de dichas capacidades parásitas, cuando dicho al menos un interruptor está cerrado, a un electrodo receptor distinto (Y1, Y2) que permite la simulación de al menos todas las teclas numéricas de dicho teclado capacitivo.

7. Programa de ordenador descargable desde una red de comunicación y/o almacenado en un soporte legible por ordenador y/o ejecutable por un procesador, comprendiendo el programa instrucciones de código de programa para la ejecución del procedimiento de refuerzo de la seguridad según la reivindicación 6, cuando es ejecutado por un procesador.

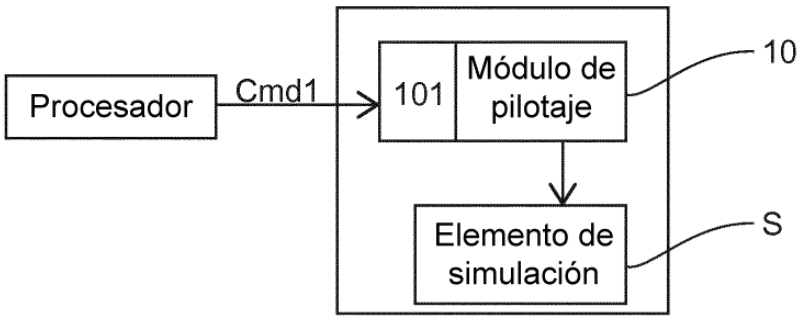
Procesador
Cmd1
101
Módulo de pilotaje
10
Elemento de simulación
S

Fig. 1

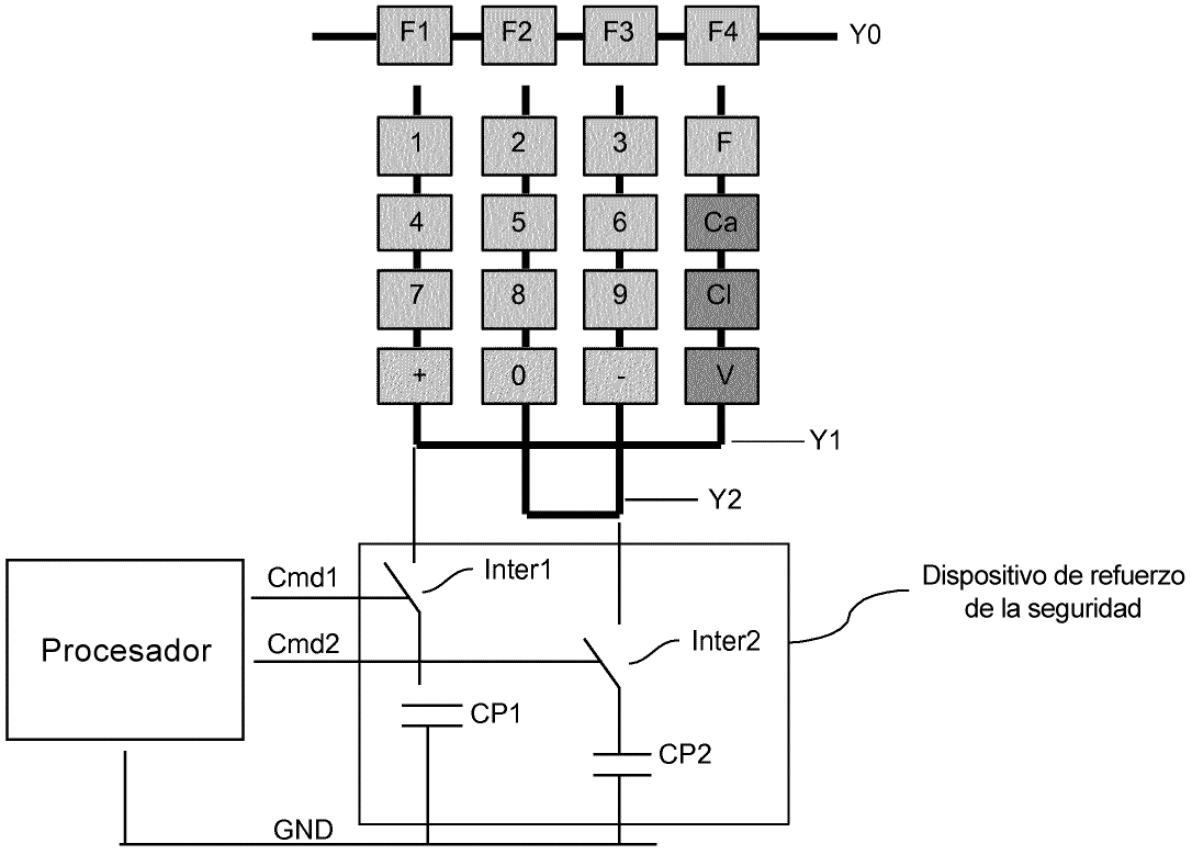
F1
F2
F3
F4
Y0
1
2
3
F
4
5
6
Ca
7
8
9
Cl
+
0
-
V
Y1
Y2
Procesador
Cmd1
Cmd2
Inter1
Inter2
CP1
CP2
GND
Dispositivo de refuerzo de la seguridad

Fig. 2

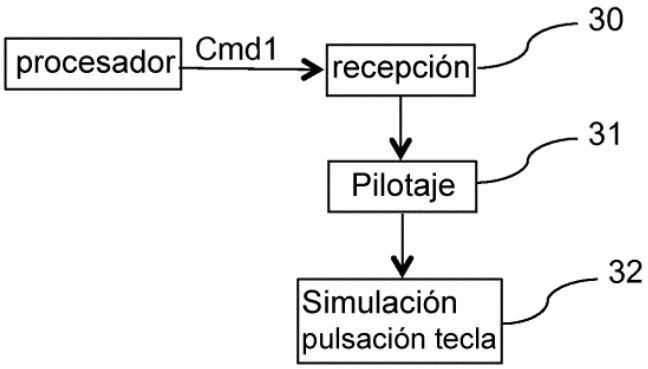
procesador
Cmd1
recepción
30
Pilotaje
31
Simulación
pulsación tecla
32

Fig. 3

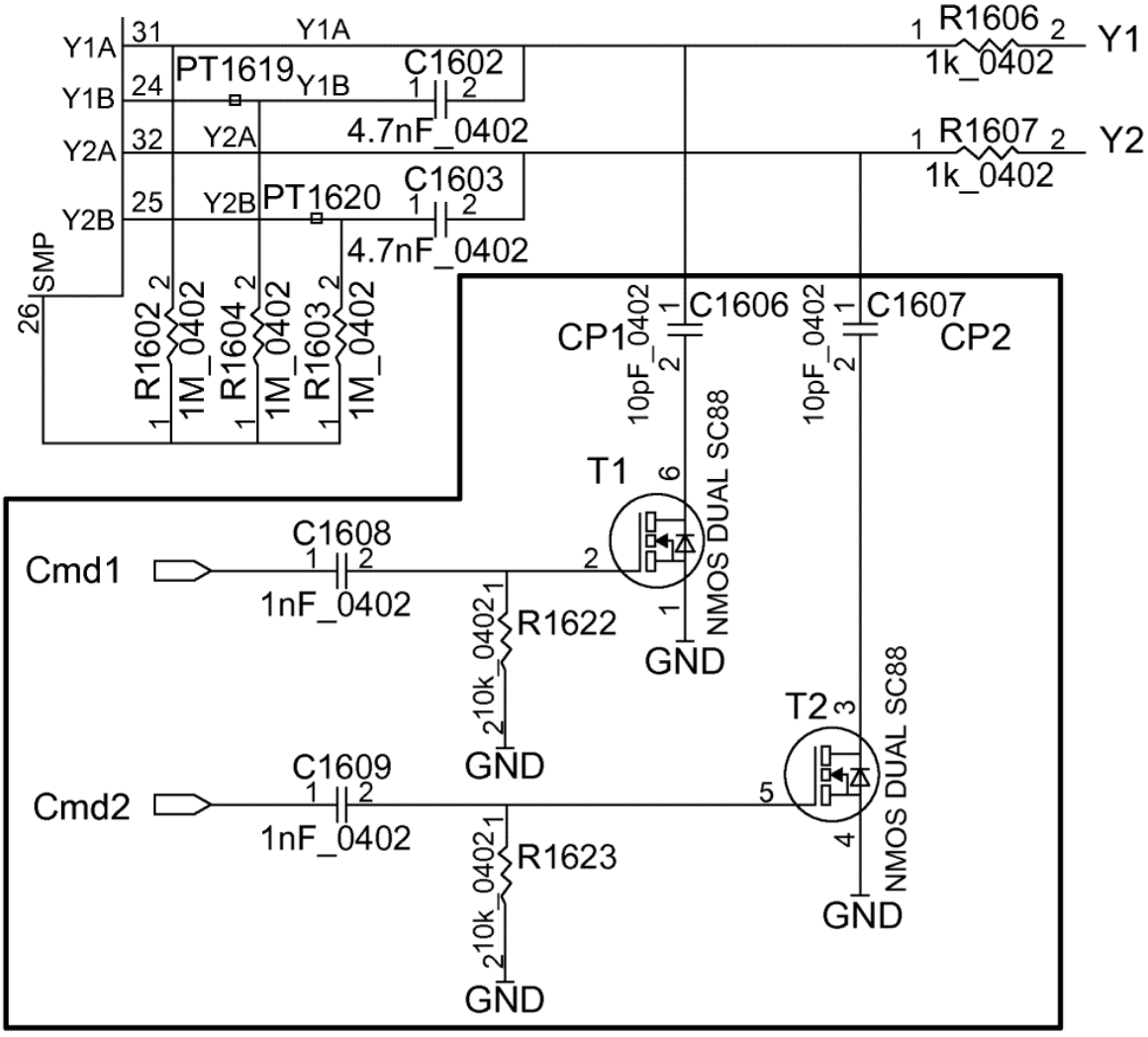
Y1A
31
Y1A
PT1619
C1602
4.7nF_0402
Y1B
24
Y1B
Y2A
32
Y2A
PT1620
C1603
4.7nF_0402
Y2B
25
Y2B
SMP
26
R1602
R1604
R1603
1M_0402
R1606
1k_0402
Y1
R1607
1k_0402
Y2
CP1
CP2
C1606
C1607
10pF_0402
T1
T2
NMOS DUAL SC88
Cmd1
C1608
1nF_0402
R1622
10k_0402
GND
Cmd2
C1609
1nF_0402
R1623
10k_0402
GND

Fig. 4