(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 774 492**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **98 01305**

(51) Int Cl^6 : **G 06 K 19/073**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 04.02.98.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 06.08.99 Bulletin 99/31.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *SCHLUMBERGER INDUSTRIES SA Societe anonyme* — FR.

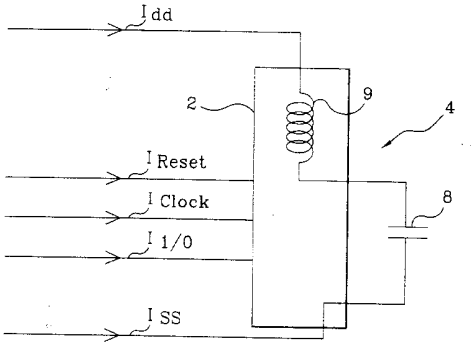
(72) **Inventeur(s) :** BONVALOT BEATRICE, SERVEL ERIC et LEYDIER ROBERT.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** SCHLUMBERGER INDUSTRIES.

(54) DISPOSITIF A CIRCUIT INTEGRE SECURISE PAR ATTENUATION DES SIGNATURES ELECTRIQUES.

(57) L'invention concerne un dispositif à circuit intégré destiné à être incorporé dans un objet portable à mémoire, notamment au format carte. L'invention se caractérise en ce que le dispositif à circuit intégré comporte au moins une capacité (8) apte à atténuer l'amplitude de pics du courant consommé par le circuit intégré dudit dispositif. L'invention s'applique en particulier, à l'atténuation des signatures électriques de cartes à puce.



FR 2 774 492 - A1

DISPOSITIF A CIRCUIT INTEGRE SECURISE PAR ATTENUATION DES SIGNATURES ELECTRIQUES

L'invention concerne des dispositifs à circuit intégré destinés à être incorporés dans des objets portables à mémoire et, en particulier, dans des objets portables à mémoire au format carte.

Les cartes à mémoire sont en général utilisées dans des applications dans lesquelles la sécurité du stockage et du traitement d'informations confidentielles sont essentielles. Ces cartes sont notamment destinées à des applications du domaine de la santé, à des applications de la télévision à péage, ou encore, à des applications dites de porte-monnaie électronique.

Elles se composent d'un corps de carte plastique dans lequel est incorporé un dispositif à circuit intégré. Il s'agit d'un module électronique comportant une puce à circuit intégré, ou alors, de la puce à circuit intégré elle-même.

Le suivi de l'intensité Idd du courant consommé par un dispositif à circuit intégré en fonction du temps constitue une signature de l'ensemble des tâches accomplies par ledit dispositif. L'analyse de cette signature électrique et, plus exactement, de sa forme, est révélatrice de l'activité du dispositif et permet d'avoir accès à des informations confidentielles contenues dans ledit dispositif.

De manière à éviter une telle analyse de signature, certains procédés de l'état de la technique proposent, dans un premier exemple, d'utiliser des algorithmes de programmation qui font notamment intervenir un déclenchement d'opérations à des moments pseudo-aléatoires ou proposent, dans un second exemple, de générer un bruit riche en informations aléatoires, ou alors, en opérations erronées.

Ces procédés de l'état de la technique comportent de multiples inconvénients. Ils monopolisent certaines ressources du dispositif, ressources qui pourraient être utilisées dans la réalisation d'autres

opérations, et ne résistent pas à une analyse approfondie des signatures.

Considérant ce qui précède, un problème technique posé est : de sécuriser l'accès à des données confidentielles en rendant l'analyse des signatures électriques de dispositifs à circuit intégré plus complexe.

La solution à ce problème objet de l'invention est : un dispositif à circuit intégré destiné à être incorporé dans un objet portable à mémoire, notamment au format carte, caractérisé en ce qu'il comporte au moins une capacité apte à atténuer l'amplitude de pics du courant consommé par le circuit intégré dudit dispositif.

De manière avantageuse, la capacité a une valeur supérieure à environ 0,1 nanofarad, notamment de l'ordre du nanofarad ; le dispositif comporte en outre au moins une résistance électrique ; la résistance électrique se caractérise par une valeur supérieure à environ 1 ohm, notamment de l'ordre de 10 ohms ; la résistance est une self inductance ; la self inductance se caractérise par une valeur supérieure à environ 50 nanohenry, notamment 500 nanohenry ; la capacité est connectée électriquement, d'une part, à un premier plot ou à une première plage du dispositif à circuit intégré et, d'autre part, à un second plot ou à une seconde plage du dispositif à circuit intégré, les premier et second plots ou les première et seconde plages étant susceptibles d'être traversés par un courant d'alimentation du circuit intégré ; le premier plot est le plot de contact Vss ou la première plage est la plage de contact Vss et le second plot est le plot de contact Vdd ou la seconde plage est la plage de contact Vdd ; la self-inductance est connectée électriquement au second plot ou à la seconde plage du dispositif à circuit intégré et mise en série avec la capacité ; la capacité est intégrée dans une couche supplémentaire d'une puce ; des sous-couches formant électrodes de la capacité sont raccordées électriquement à des plots du dispositif à circuit intégré ; la self

inductance se présente sous la forme d'une spirale, intégrée à une face active d'une couche de base du dispositif à circuit intégré.

L'invention sera mieux comprise à la lecture de l'exposé non limitatif qui suit, rédigé au regard des dessins annexés, dans lesquels :

- la figure 1 montre, en vue de dessus, une partie d'une carte équipée d'un dispositif à circuit intégré selon l'invention ;

- la figure 2 montre, de manière schématique, un dispositif à circuit intégré selon l'invention ;

. - la figure 3 est une représentation électrique schématique d'un dispositif à circuit intégré selon l'invention ;

- la figure 4 illustre, en vue de dessus, un dispositif à circuit intégré selon l'invention ;

- la figure 5 illustre, en coupe transversale, un circuit intégré selon l'invention ;

- la figure 6 est une vue de dessus d'une face active d'un dispositif à circuit intégré selon l'invention ;

- la figure 7 représente une cellule logique élémentaire CMOS d'un dispositif à circuit intégré selon l'invention ;

- la figure 8 présente des signaux caractéristiques Vin et i_{dd} de la cellule logique élémentaire CMOS de la figure 7 ; et

- la figure 9 montre des chronogrammes de trois signaux.

Le présent exposé de l'invention a trait à l'exemple des cartes à puce. Néanmoins, il est bien entendu que l'invention s'applique de manière générale à tout dispositif à circuit intégré destiné à être incorporé dans un objet portable à mémoire tel qu'un module d'identification abonné (SIM) au format jeton ou une étiquette électronique.

Les cartes à puce sont des objets portables standards fonctionnant avec et/ou sans contact et qui sont définis notamment dans les normes

ISO 78-10 et 78-16 dont le contenu est incorporé dans le présent exposé de l'invention, par citation de référence.

Ainsi que cela est plus particulièrement montré aux figures 1 et 2, les cartes 1 ayant un mode de fonctionnement à contacts comprennent une puce 2 à circuit intégré dont cinq plots de contact au moins 100, 101, 102, 103 et 104 sont connectés électriquement, par des fils conducteurs non représentés, à, respectivement, cinq plages de contact 200, 201, 202, 203 et 204 affleurantes à la surface du corps 3 de carte. Un plot de contact Reset 100 est connecté à une plage de contact Reset 200, un plot de contact Clock 101 est connecté à une plage de contact Clock 201, un plot de contact Vss 102 est connecté à une plage de contact Vss 202, un plot de contact I/O 103 est connecté à une plage de contact I/O 203 et un plot de contact Idd 104 est connecté à une plage de contact Vdd 204.

Les plots de contact 100, 101, 102, 103 et 104, de même que les plages de contact 200, 201, 202, 203 et 204, sont susceptibles d'être traversés par des courants respectifs d'intensité I_{Reset}, I_{Clock}, I_{ss}, $I_{I/O}$ et I_{dd}.

L'ensemble, puce 2, fils conducteurs et plages de contact 200, 201, 202, 203 et 204 est en général compris dans un module électronique 4 incorporé dans le corps 3 de carte.

Le dispositif à circuit intégré selon l'invention est notamment le module électronique 4 portant les plages 200, 201, 202, 203 et 204 et comportant une puce, ou alors, la puce 2 elle-même.

Ainsi que cela est plus particulièrement montré à la figure 3, il apparaît que, selon l'invention, le dispositif à circuit intégré comporte une capacité 8. Cette capacité 8 se caractérise par une valeur supérieure à environ 0,1 nanofarad, notamment de l'ordre du nanofarad. Elle est apte à atténuer l'amplitude des pics du courant consommé par le circuit intégré du dispositif selon l'invention.

En outre, le dispositif à circuit intégré selon l'invention comporte avantageusement une résistance électrique. Cette résistance électrique se caractérise par une valeur supérieure à environ 1 Ohm, notamment de l'ordre de 10 Ohms. Elle est préférentiellement constituée par une self inductance 9. Cette self inductance 9 se caractérise elle-même par une valeur supérieure à environ 50 nanohenry, notamment 500 nanohenry.

La capacité 8 est connectée électriquement, d'une part, au plot 102 de la puce 2 ou à la plage 202 du module électronique comportant ladite puce 2 et, d'autre part, au plot 104 de la puce 2 ou à la plage 204 du module électronique 4. Dans le cas avantageux où le dispositif comporte en outre une résistance électrique préférentiellement constituée par la self inductance 9, cette self inductance 9 est connectée électriquement au plot 104 de la puce 2 ou à la plage 204 du module électronique 4 comportant ladite puce 2 et mise en série avec la capacité 8.

En définitive, l'ensemble capacité 8 et self inductance 9 constitue une cellule de filtrage passe-bas, cette cellule de filtrage étant au moins constituée d'une capacité 8, préférentiellement d'une capacité 8 et d'une résistance, la résistance étant plus préférentiellement une self inductance 9, ladite cellule de filtrage se trouvant dans le module électronique 4, avantageusement au voisinage immédiat du circuit intégré.

Dans le mode de réalisation présenté ci-dessous au regard des figures 4, 5 et 6, la puce 2 comporte la capacité 8 et la self inductance 9.

Si l'on se rapporte tout d'abord à la figure 5, il apparaît que la puce 2 comporte trois couches principales. Il s'agit d'une première couche de base 105, d'une couche supplémentaire 106, lesdites première et

seconde couches étant liées par une couche intermédiaire 107 de scellement.

La couche 105 se compose de trois sous-couches, une sous-couche 108 de silicium, une sous-couche 109 d'intégration du circuit, lesdites sous-couches 108 et 109 étant recouvertes d'une sous-couche 110 de passivation.

La couche 106 se compose de six sous-couches, une sous-couche 111 isolante, une sous-couche 112 conductrice, par exemple à base de Tantale, formant une première électrode de la capacité 8, une sous-couche 113 isolante et diélectrique, par exemple d'oxyde de Tantale, une sous-couche 114 conductrice, par exemple à base de Tantale, formant une seconde électrode de la capacité 8, une sous-couche 115 isolante et une sous-couche 116 de silicium ou d'un autre matériau.

La couche 107 de scellement ne se subdivise pas en sous-couches. Elle se compose d'un agent de scellement par exemple polymérique. Il s'agit en particulier d'un polyimide.

Dans un exemple, l'épaisseur des sous-couches 110, 111, 112, 113, 114 et 115 est de l'ordre de quelques milliers d'angström, l'épaisseur de la sous-couche 109 et de la couche 107 est de l'ordre de 5 µm, l'épaisseur de la sous-couche 108 est de l'ordre de 50 µm et l'épaisseur de la couche 116 est de l'ordre de 150 µm.

La capacité 8 est ainsi intégrée dans la couche 106 supplémentaire. Les sous-couches 112 et 114 formant électrodes sont raccordées électriquement à des plots d'inter-connexion 117, 118 du circuit intégré, par des vias ou des bossages conducteurs 119.

Ainsi que cela est plus particulièrement montré à la figure 6, la self inductance 9 se présente sous la forme d'une spirale intégrée à la face active de la couche 105 de base. Ses deux bornes de connexion sont connectées, l'une au plot de contact Idd 104, l'autre au plot d'inter-connexion 118.

Le plot d'interconnexion 117 est connecté au plot de contact Vss 102 par un circuit de connexion 120 qui est avantageusement le moins résistif possible.

Ainsi que cela apparaît clairement à la figure 4, les couches 106 et 107 sont percées de trous à l'aide de techniques de micro-usinage. Ces trous permettent d'établir des liaisons par câblage thermosonique entre les plots 100, 101, 102, 103 et 104 affleurant à la face active de la couche 105 de base et les plages de contact 200, 201, 202, 203 et 204 du module électronique 4.

Dans un dispositif à circuit intégré, le circuit intégré forme une structure d'assemblage complexe de cellules logiques dans lesquelles une unité centrale de traitement (CPU) distribue et gère, par l'intermédiaire d'un bus de données et d'un bus d'adresses, des informations stockées dans des mémoires RAM, ROM ou EEPROM dudit circuit. Eventuellement, le circuit intégré forme en outre un micro-contrôleur associé à la CPU, ledit micro-contrôleur étant plus particulièrement destiné au codage cryptographique de données nécessitant des structures de calcul spécialisées. Ce micro-contrôleur est alors appelé cryptoprocesseur.

A la figure 7, on a représenté une cellule logique 5 élémentaire d'un dispositif à circuit intégré selon l'invention. Cette cellule 5 est du type CMOS. Elle est constituée d'un premier transistor MOS 6 de type P et d'un second transistor MOS 7 de type N, lesdits transistors 6, 7 étant montés en série. Chaque cellule 5 est commandée par un signal logique de commande Vin commun aux deux transistors 6, 7.

Soit idd, l'intensité du courant consommé par la cellule 5.

Aux deux états stables, c'est-à-dire aux états logiques 0 et 1, seul un 6 ou 7 des deux transistors est conducteur ou passant, l'autre transistor 7 ou 6 étant bloqué ou non-passant. L'intensité du courant i_{dd} consommé par la cellule 5 est alors égale à une valeur i_{fuite} de

courant de fuite, cette valeur étant sensiblement constante au cours du temps et dépendant en particulier de la température. En pratique, i_{fuite} est de l'ordre du nanoampère.

Par contre, lorsqu'on applique une tension de commande V_{in} aux bornes d'entrée de la cellule 5, et que V_{in} est supérieure à une valeur de seuil permettant la commutation des transistors 6, 7 de ladite cellule 5 d'un état stable à un autre état stable, cette cellule 5 est, pendant un intervalle de temps t_c, dans un état transitoire non-stable, intermédiaire entre les états logiques 0 et 1. Les transistors 6 et 7 sont alors conducteurs et i_{dd} est égal à i_{comm} bien supérieur à i_{fuite} et qui culmine à une valeur d'intensité i_{pic} dont la valeur est, dans l'invention, de quelques dizaines de microampères.

En analysant les variations de l'intensité du courant Idd, il serait possible, d'une part, d'en déduire les changements d'états de cellules logiques élémentaires 5 qui participent aux flux d'informations entre les divers sous-ensembles du circuit intégré RAM, EEPROM, ROM et cryptoprocesseur puis, d'autre part, d'interpréter le fonctionnement du circuit intégré.

A la figure 9, une courbe 300 représente l'intensité du courant Idd consommé dans un dispositif à circuit intégré selon l'invention en fonction du temps, une courbe 302 représente l'intensité du courant Idd consommé dans un dispositif selon l'état de la technique en fonction du temps, les courbes 300 et 301 étant rapprochées d'une courbe 300 représentative du signal d'horloge qui pilote ledit dispositif à circuit intégré.

Les dispositifs à circuit intégré selon l'invention et selon l'état de la technique à l'origine respectivement, des courbes 300 et 301 consomment à la fois sur le front montant et sur le front descendant de l'horloge. On notera que cela n'est cependant pas toujours le cas. En effet, certains dispositifs à circuits intégrés consomment sur un seul

des deux fronts de l'horloge et d'autres possèdent des moyens multiplicateurs de fréquence et le nombre de pics de courant par période d'horloge est alors supérieur à deux.

La courbe 301 montre des pics d'intensité du courant Idd consommé dont la hauteur ou amplitude est de l'ordre de 27 mA. Ces pics constituent une signature de l'ensemble des tâches accomplies par le circuit intégré. En analysant finement la courbe 301 en association avec une transaction, il est alors possible de comprendre le fonctionnement du circuit intégré et d'extraire des informations confidentielles. C'est une méthode d'investigation non destructive qui porte atteinte à la sécurité des données et des transactions.

La courbe 300 montre par contre des pics d'intensité du courant Idd consommé dont la hauteur est de l'ordre de 8 mA. Aussi, grâce à la présence de la capacité 8, et de la self inductance 9, la hauteur des pics a été réduite de plus de 50 %. L'analyse fine de la courbe 300 en association avec une transaction se révèle ainsi particulièrement complexe. Il n'est plus possible d'extraire simplement des informations confidentielles par une méthode d'investigation non destructive.

Par ailleurs, compte tenu du fait que des chutes de tension brutales dues à des variations importantes de l'intensité du courant d'alimentation Idd sont susceptibles d'entraîner, au cours du fonctionnement d'un dispositif à circuit intégré selon l'état de la technique et dans le cas où lesdites chutes amènent la tension au-dessous d'un seuil dit de détection nominale de fonctionnement, une nouvelle initialisation voire une perte de données et des erreurs d'écriture à l'origine de défaut d'intégrités des données, l'atténuation des signatures électriques et par suite l'absence de chutes de tension dans un dispositif selon l'invention apporte donc un avantage supplémentaire.

On notera que la structure des circuits intégrés CMOS est telle qu'un dispositif à circuit intégré peut être alimenté, de manière dégradée, par ses plots de contact Reset 100, I/O 103 voire Clock 101. Ces plots autres que les plots d'alimentation Vss et Vdd sont protégés contre des décharges électrostatiques, par des dispositifs non linéaires. Ces dispositifs sont principalement constitués de deux diodes reliées aux bus d'alimentations du circuit intégré. Ainsi, toute alimentation, en mode dégradé, du circuit intégré par les plots Reset, I/O et Clock, s'effectue au travers d'une diode vers l'alimentation Vdd. Ce dispositif non linéaire, associé à la capacité présente sur le Vdd, filtre le courant d'alimentation du circuit intégré. Cependant, on peut imaginer que le mode de réalisation exposé dans la présente description au regard des plots Vss et Vdd peut être appliqué aux plots 100, 101 ou 103 pour l'atténuation de signatures de la consommation électrique du circuit intégré sur ces plots.

On notera d'autre part que les puces à circuit intégré selon l'invention peuvent être réalisées par lots, sous la forme de tranches de silicium appelées wafer. En ce qui concerne les fabrications de puces par lots, on se reportera à la demande de brevet enregistrée en France sous le numéro 97/10764, qui n'a pas été rendue accessible au public, et dont le contenu est incorporé à la présente demande, par citation de référence.

Bien entendu, la présente invention est susceptible de venir compléter l'efficacité des routines de programmation en filtrant à l'aide d'une cellule analogique les transitoires de courant qui accompagnent l'ensemble des tâches d'un circuit intégré pour carte à puce.

REVENDICATIONS

1 - Dispositif à circuit intégré destiné à être incorporé dans un objet portable à mémoire, notamment au format carte, caractérisé en ce qu'il comporte au moins une capacité (8) apte à atténuer l'amplitude de pics du courant consommé par le circuit intégré dudit dispositif.

2 - Dispositif selon la revendication 1, caractérisé en ce que la capacité (8) a une valeur supérieure à environ 0,1 nanofarad, notamment de l'ordre du nanofarad.

3 - Dispositif selon l'une des revendications 1 ou 2, caractérisé en ce qu'il comporte en outre au moins une résistance électrique.

4 - Dispositif selon la revendication 3, caractérisé en ce que la résistance électrique se caractérise par une valeur supérieure à environ 1 ohm, notamment de l'ordre de 10 ohms.

5 - Dispositif selon l'une des revendications 3 ou 4, caractérisé en ce que la résistance est une self inductance (9).

6 - Dispositif selon la revendication 5, caractérisé en ce que la self inductance (9) se caractérise par une valeur supérieure à environ 50 nanohenry, notamment 500 nanohenry.

7 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que la capacité (8) est connectée électriquement, d'une part, à un premier plot ou à une première plage du dispositif à circuit intégré et, d'autre part, à un second plot ou à une seconde plage du dispositif à circuit intégré, les premier et second plots ou les première et seconde plages étant susceptibles d'être traversés par un courant d'alimentation du circuit intégré.

8 - Dispositif selon la revendication 7, caractérisé en ce que le premier plot est le plot de contact Vss (102) ou la première plage est la plage de contact Vss (202) et en ce que le second plot est le plot de contact Vdd (104) ou la seconde plage est la plage de contact Vdd (204).

9 - Dispositif selon l'une des revendications 7 ou 8, caractérisé en ce que la self-inductance (9) est connectée électriquement au second plot ou à la seconde plage du dispositif à circuit intégré et mise en série avec la capacité (8).

10 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que la capacité (8) est intégrée dans une couche supplémentaire (106) d'une puce (2).

11 - Dispositif selon la revendication 10, caractérisé en ce que des sous-couches (112) et (114) formant électrodes de la capacité (8) sont raccordées électriquement à des plots (117, 118) du dispositif à circuit intégré.

12 - Dispositif selon l'une des revendications 5 à 110, caractérisé en ce que la self-inductance (9) se présente sous la forme d'une spirale intégrée à une face active d'une couche (105) de base du dispositif à circuit intégré.

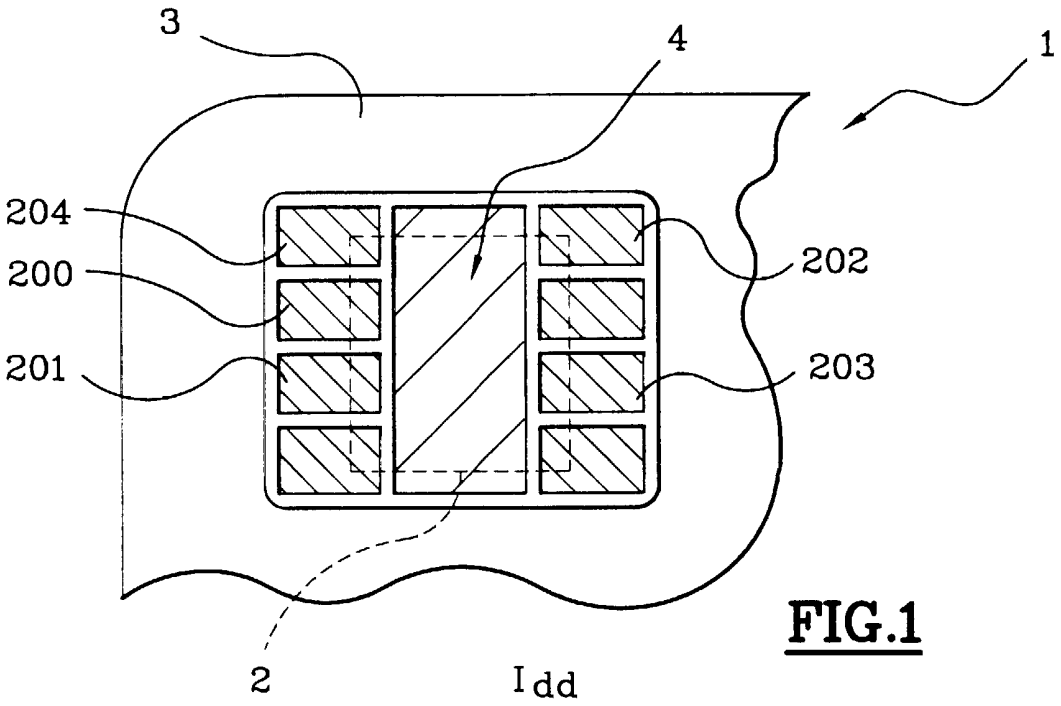

3
4
1
204
200
201
202
203
2

FIG.1

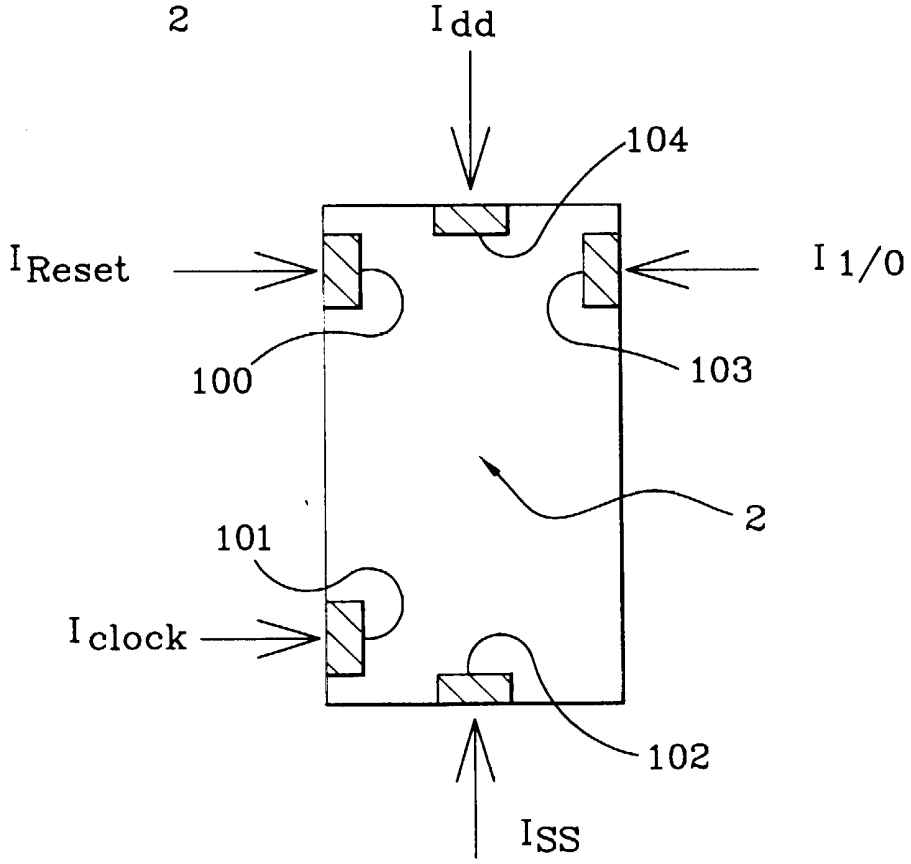

Idd
104
IReset
I 1/0
100
103
2
101
Iclock
102
ISS

FIG.2

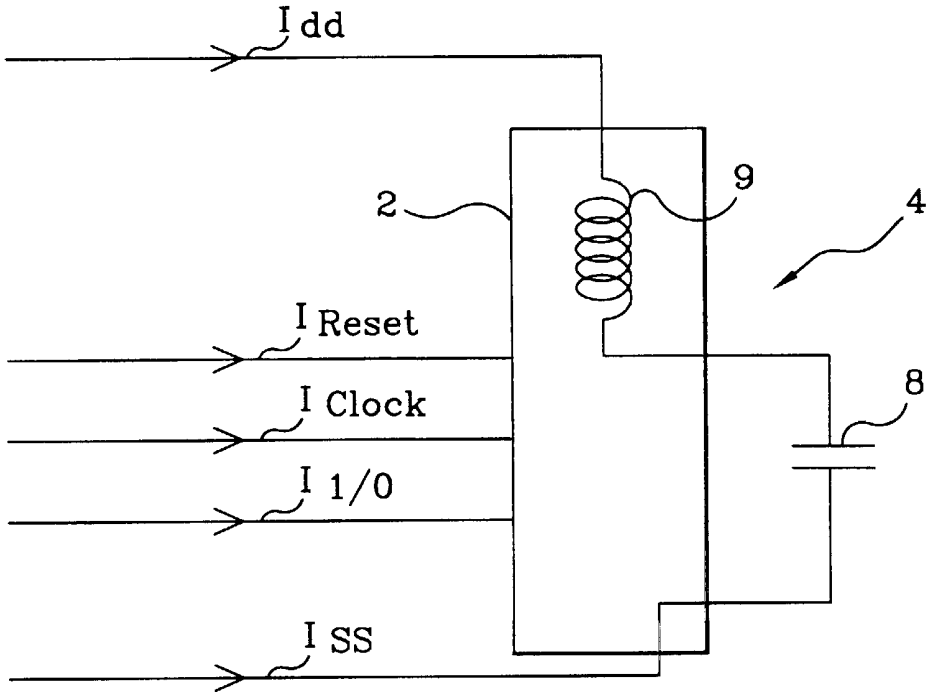

I dd
2
9
4
I Reset
I Clock
I 1/0
8
I SS

FIG.3

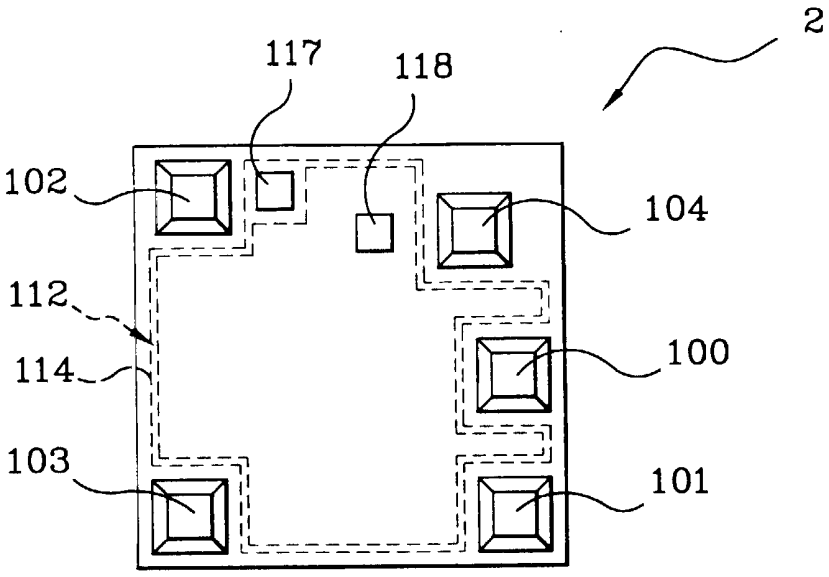

2
117
118
102
104
112
114
100
103
101

FIG.4

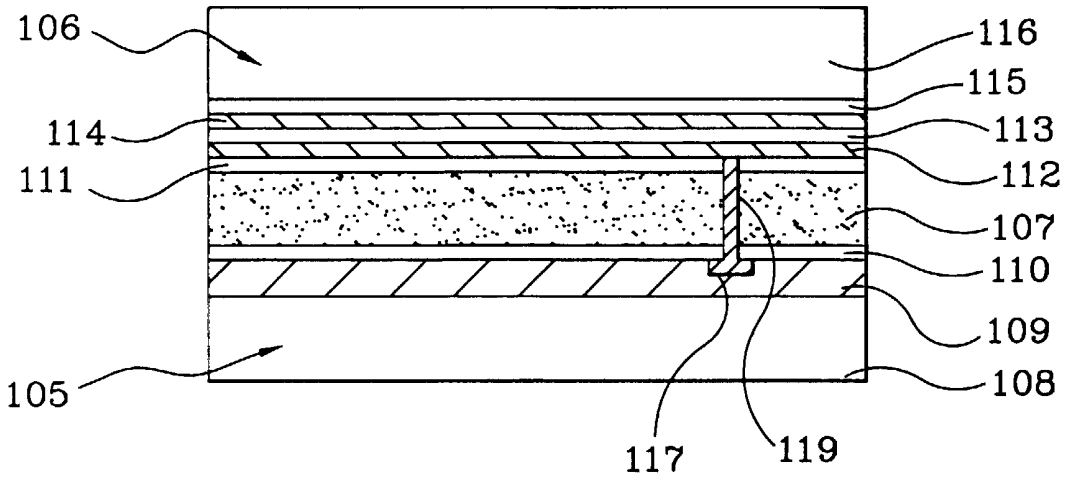

106
116
115
114
113
111
112
107
110
109
105
108
117
119

FIG.5

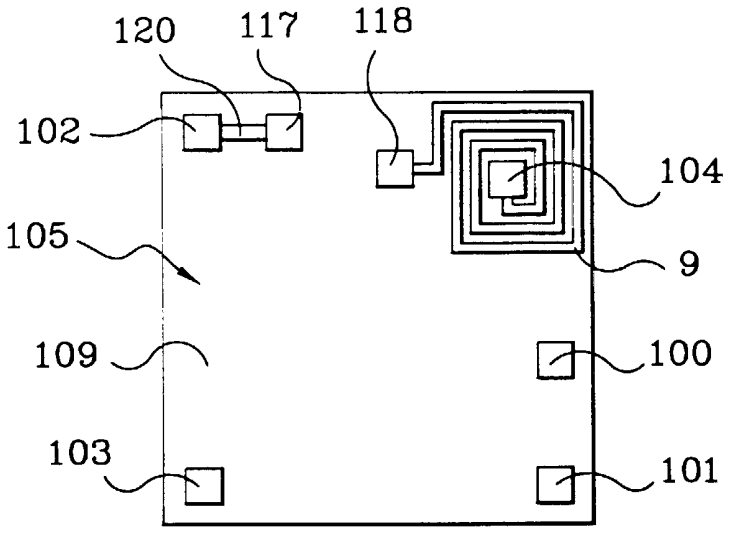

120
117
118
102
104
105
9
109
100
103
101

FIG.6

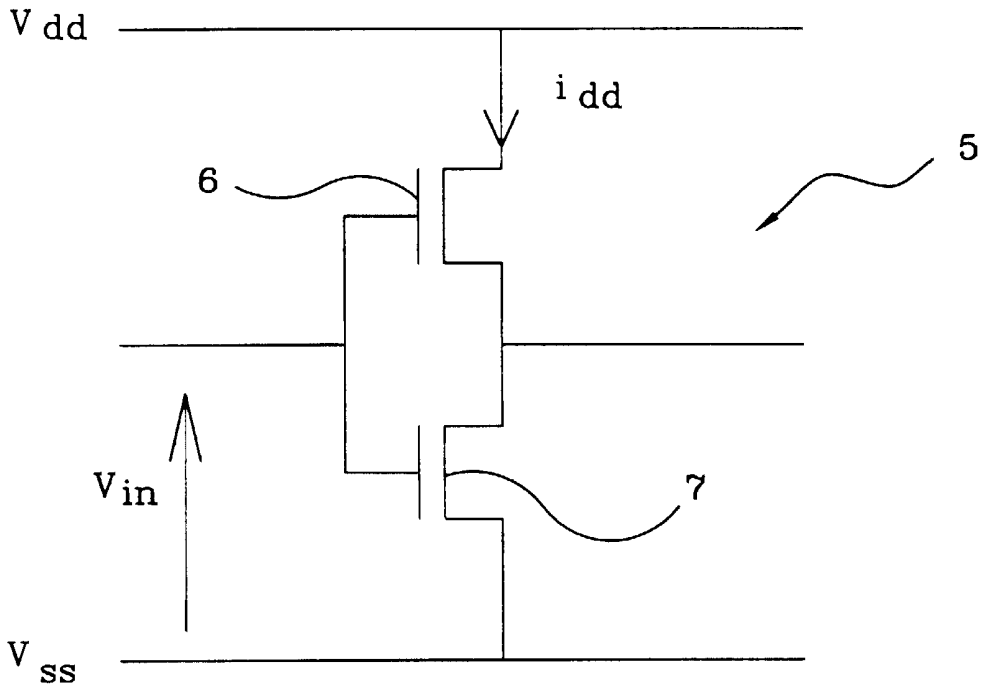


FIG.7

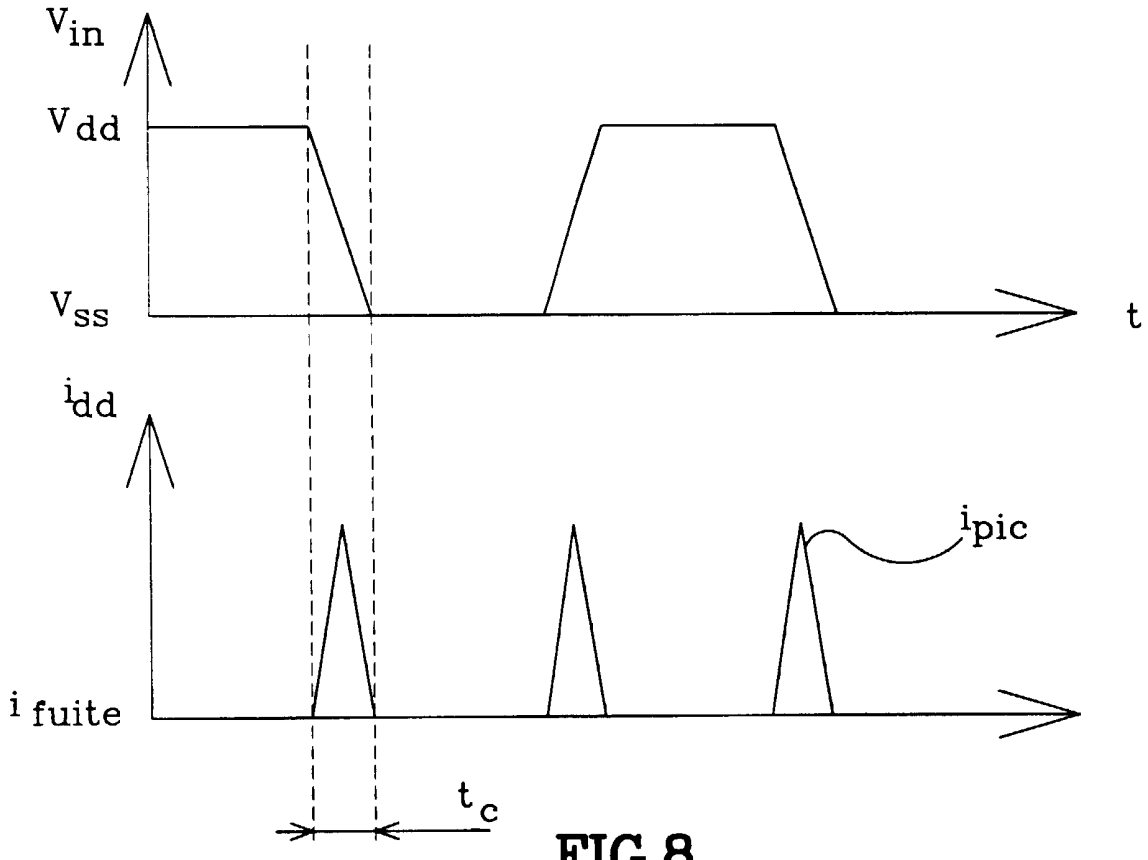


FIG.8

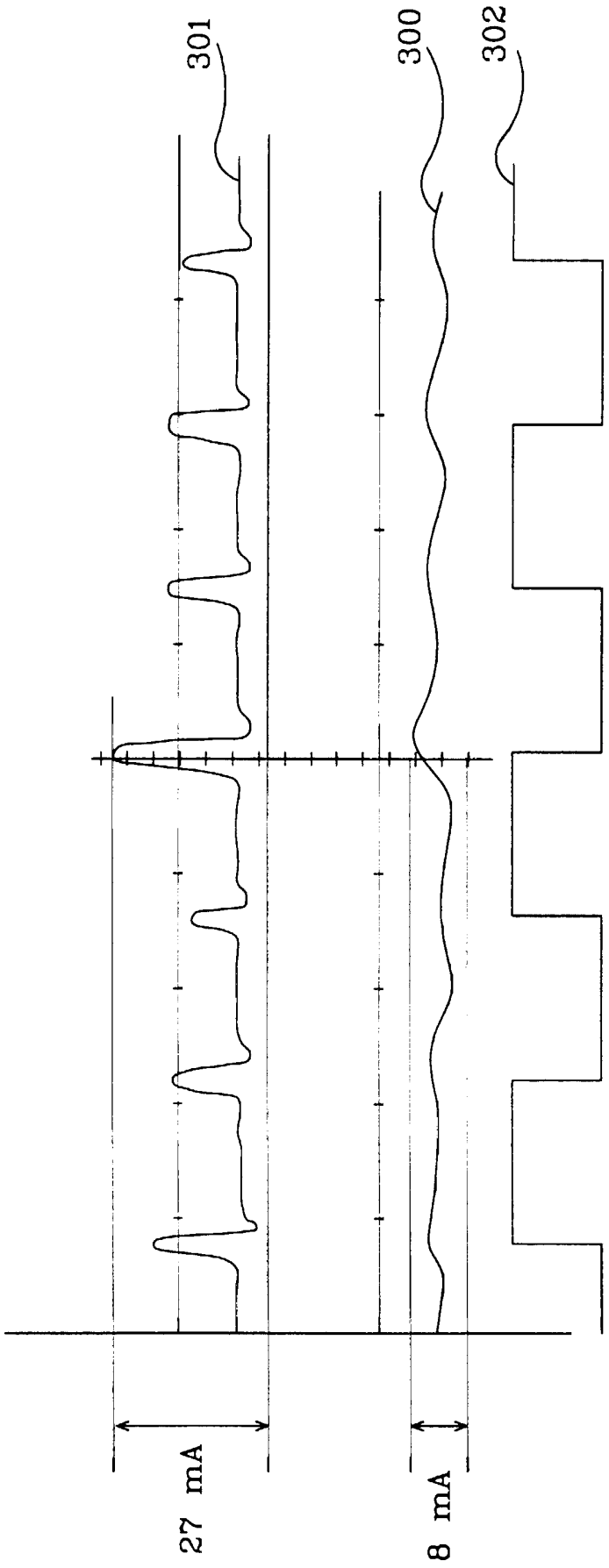


FIG.9

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 552624
FR 9801305

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X Y	US 5 687 109 A (PROTIGAL STANLEY N ET AL) 11 novembre 1997 * colonne 4, ligne 25 - colonne 5, ligne 19 * * figures 2-8 *	1-11 12
Y	US 4 864 292 A (NIEUWKOOP EVERT) 5 septembre 1989 * colonne 4, ligne 11 - ligne 23 * * figure 7 *	12
A	US 4 810 864 A (TAKAHASHI KAORU) 7 mars 1989 * colonne 2, ligne 59 - colonne 3, ligne 42 * * figures 1,2 *	1-12

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G06K

Date d'achèvement de la recherche	Examinateur
5 novembre 1998	Goossens, A

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)