(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 823 398**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 04586**

(51) Int Cl[7] : **H 04 L 9/32,** G 06 K 19/07

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 04.04.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 11.10.02 Bulletin 02/41.

(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) :** *STMICROELECTRONICS SA* *Société anonyme* — FR.

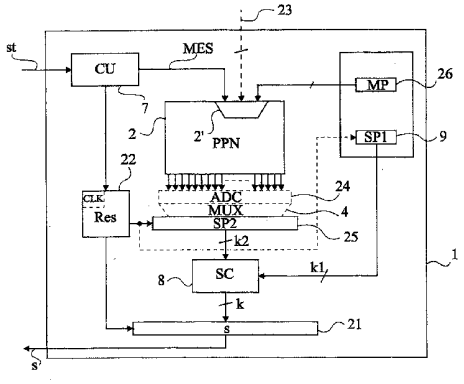
(72) **Inventeur(s) :** LIARDET PIERRE YVAN, WUIDART LUC et GUETTE FRANCOIS.

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

(74) **Mandataire(s) :** CABINET MICHEL DE BEAUMONT.

(54) EXTRACTION D'UNE DONNEE PRIVEE POUR AUTHENTIFICATION D'UN CIRCUIT INTEGRE.

(57) L'invention concerne un procédé et un circuit d'extraction d'une donnée secrète (s) dans un circuit intégré participant à une procédure d'authentification au moyen d'un dispositif externe tenant compte de cette donnée secrète, la donnée secrète étant générée sur demande et rendue éphémère.



FR 2 823 398 - A1

EXTRACTION D'UNE DONNÉE PRIVÉE POUR AUTHENTIFICATION D'UN CIRCUIT INTÉGRÉ

La présente invention concerne l'authentification d'un circuit intégré ou d'un élément ou sous-ensemble électronique contenant un tel circuit au moyen d'une procédure d'authentification ayant recours à une donnée secrète contenue dans le circuit intégré. L'invention concerne plus particulièrement les procédures d'authentification basées sur l'utilisation d'une donnée ou clé privée (dite aussi secrète) au moyen d'un dispositif externe. Un exemple d'application de la présente invention est le domaine des cartes à puce qu'elles soient à unités de compte prépayées ou non.

Les divers procédés d'authentification d'une carte à puce ou analogue ont pour but d'éviter le piratage ou la falsification d'une carte soit par utilisation d'un dispositif discret reproduisant la carte, soit par piratage d'un terminal de lecture ou encore par reproduction à grande échelle de cartes à puce falsifiées.

Les procédés d'authentification les plus performants ont recours à une donnée privée présente dans le circuit intégré à authentifier et à une donnée ou clé dite publique, dépendant de cette donnée privée et stockée dans un dispositif externe. La donnée privée est mise en jeu de façon indirecte à chaque besoin

d'authentification du circuit intégré, sans qu'il y ait "transfert de connaissance". Dans des procédés dits "sans transfert de connaissance" (ou "zero-knowledge"), l'authentification se déroule suivant un protocole qui, de façon prouvée, et sous des hypothèses reconnues comme parfaitement raisonnables par la communauté scientifique, ne révèle rien de la clé secrète de l'entité dont la signature est à authentifier. Des exemples de procédés d'authentification connus auxquels s'applique la présente invention sont décrits dans la demande de brevet français n° 2 716 058 et dans le brevet américain n° 4 995 082.

L'inconvénient du recours à une donnée privée par ailleurs indispensable pour distinguer ou différencier des ensembles ou sous-ensembles électroniques, par exemple des cartes à puce, les uns par rapport aux autres est que cette donnée constitue une donnée stockée dans le composant à identifier. Une telle donnée est par conséquent susceptible d'être piratée par examen de l'élément de stockage de cette donnée dans la carte à puce, ou par piratage des registres dans lesquels est stockée la donnée, etc. La donnée privée est de plus généralement immuable pour une carte à puce donnée afin de permettre une authentification répétitive de celle-ci. Il en découle une fragilité de la fonction d'authentification.

Dans une application à des cartes à puce prépayées (par exemple, des cartes d'unités téléphoniques), si la donnée privée est la même pour toute une famille de carte à puce, cela rend possible des piratages à grande échelle.

En pratique, on n'envoie pas la donnée privée elle-même, mais un résultat de calcul prenant en compte cette donnée privée, un nombre fonction d'un nombre aléatoire choisi par le circuit intégré et communiqué au dispositif externe, et un nombre aléatoire choisi par le dispositif externe et communiqué à la carte. Le résultat est alors vérifié par le dispositif externe pour authentifier la carte.

La présente invention vise à améliorer les procédures et systèmes d'authentification de circuits intégrés ayant recours à une donnée privée émanant du circuit intégré.

L'invention vise, plus particulièrement, à optimiser la sécurité anti-fraude des dispositifs électroniques ayant recours à un circuit intégré pourvu d'une donnée privée en empêchant l'extraction de cette donnée privée par diverses attaques du circuit intégré.

Pour atteindre ces objets, la présente invention prévoit un procédé d'extraction d'une donnée privée dans un circuit intégré participant à une procédure d'authentification au moyen d'un dispositif externe tenant compte de cette donnée privée, la donnée privée étant générée sur demande et rendue éphémère.

Selon un mode de réalisation de la présente invention, à chaque génération de la donnée privée, on initialise une durée de vie de cette donnée privée et on efface cette donnée d'au moins un premier élément de mémorisation la contenant, à l'issue de cette durée de vie.

Selon un mode de réalisation de la présente invention, la génération de la donnée privée et l'initialisation de sa durée de vie sont déclenchées par un même signal.

Selon un mode de réalisation de la présente invention, on réduit la durée de vie de la donnée privée au fur et à mesure de ses générations.

Selon un mode de réalisation de la présente invention, la durée de vie est variable.

Selon un mode de réalisation de la présente invention, la donnée privée est obtenue au moins partiellement à partir d'un réseau de paramètres physiques.

Selon un mode de réalisation de la présente invention, le réseau de paramètres physiques est programmable.

Selon un mode de réalisation de la présente invention, le réseau de paramètres physiques est programmé, au moins partiellement, par un mot fourni par un élément de mémorisation.

Selon un mode de réalisation de la présente invention, le réseau de paramètres physiques est programmé, au moins partiellement, par du bruit.

Selon un mode de réalisation de la présente invention, on commande le réseau de paramètres physiques également hors des périodes de génération de la donnée privée.

Selon un mode de réalisation de la présente invention, la donnée privée est obtenue au moins à partir d'une première donnée mémorisée dans le circuit intégré et d'une deuxième donnée générée sur demande par le réseau de paramètres physiques.

Selon un mode de réalisation de la présente invention, on rend éphémère la deuxième donnée.

Selon un mode de réalisation de la présente invention, les nombres de bits des première et deuxième données sont proches l'un de l'autre, de préférence égaux.

La présente invention prévoit également un circuit intégré, comportant des moyens pour la mise en oeuvre du procédé.

Selon un mode de réalisation de la présente invention, le circuit comporte un circuit de réinitialisation d'au moins un élément de mémorisation.

Selon un mode de réalisation de la présente invention, le circuit de réinitialisation est constitué d'un ou plusieurs éléments retardateurs initialisés par une commande de génération de la donnée privée.

Selon un mode de réalisation de la présente invention, le retard apporté par au moins un élément retardateur du circuit de réinitialisation est variable.

Ces objets, caractéristiques et avantages, ainsi que d'autres de la présente invention seront exposés en détail dans la description suivante de modes de réalisation particuliers faite à titre non-limitatif en relation avec les figures jointes parmi lesquelles :

la figure 1 illustre, sous forme d'organigramme, un procédé d'authentification d'un circuit intégré mettant en oeuvre une donnée privée auquel s'applique la présente invention ;

la figure 2 représente, sous forme de schéma-blocs et de façon très schématique, un circuit d'extraction d'une donnée privée selon un mode de réalisation de la présente invention ;

la figure 3 représente un mode de réalisation d'un réseau de paramètres physiques d'un circuit d'extraction selon la présente invention ;

les figures 4A et 4B illustrent, sous forme de chronogrammes, le fonctionnement du réseau de la figure 3 ; et

les figures 5, 6 et 7 représentent trois modes de réalisation d'un circuit de réinitialisation d'un circuit d'extraction selon la présente invention.

Les mêmes éléments ont été désignés par les mêmes références aux différentes figures. Pour des raisons de clarté, seules les étapes de procédés et les éléments du circuit d'extraction qui sont nécessaires à la compréhension de l'invention ont été représentés aux figures et seront décrits par la suite. En particulier, les procédés d'authentification et les algorithmes ayant recours à des données privées sont parfaitement connus et ne seront pas détaillés, sauf en ce qui concerne la fourniture de la donnée privée faisant l'objet de l'invention.

Une caractéristique de la présente invention est de ne pas stocker, de façon permanente, la donnée privée ou secrète sous forme binaire dans le circuit intégré mais de générer cette donnée privée sur demande, c'est-à-dire lors d'une procédure d'authentification. L'invention prévoit de plus que cette donnée privée soit éphémère, c'est-à-dire qu'elle ne soit plus détectable dans le circuit intégré au bout d'un temps prédéterminé qui suit sa génération.

La figure 1 représente, sous forme d'organigramme simplifié, un mode de mise en oeuvre d'une procédure d'authentification du type auquel s'applique la présente invention. Cet exemple concerne l'authentification d'une carte à puce par un dispositif externe. En figure 1, on a fait ressortir les étapes de la procédure d'authentification se déroulant côté carte C ou côté lecteur R.

Une phase d'authentification suit bien entendu l'introduction d'une carte dans le lecteur, l'envoi d'un identifiant par la carte au lecteur ou à un central, sa vérification par le central, puis l'extraction par le central d'une donnée ou clé publique v à partir de l'identifiant communiqué par la carte. Cette clé publique provient le plus souvent d'une table de clés.

Pour la phase d'authentification proprement dite, on commence par tirer aléatoirement, côté carte, un nombre r (bloc 10). Ce nombre r est mémorisé (bloc 11, MEM(r)) dans le circuit intégré de la carte. Puis, on applique (bloc 12) à ce nombre r un premier algorithme ALGO1 fournissant un résultat X. Le résultat X est transmis au lecteur R qui le mémorise (bloc 13, MEM(X)). Côté lecteur, on tire un nombre aléatoire e (bloc 14) que l'on mémorise (bloc 15, MEM(e)). Ce nombre e est envoyé à la carte C qui elle-même le mémorise (bloc 16, MEM(e)).

La carte extrait alors sa donnée privée s (bloc 17) selon le procédé de la présente invention. Cette donnée privée s est prise en compte dans un deuxième algorithme ALGO2 (bloc 18) avec les données r et e pour fournir un résultat Y. De préférence, le nombre r est effacé après avoir été utilisé pour le calcul du nombre Y et avant l'envoi de ce dernier. Le résultat Y est envoyé au lecteur R qui vérifie (bloc 19) au moyen d'un troisième algorithme ALGO3 que la grandeur X est bien égale à l'application de cet algorithme aux grandeurs Y, e et v. La clé publique v est bien entendu fonction de la donnée ou clé privée s de la carte. Selon le résultat du test de cohérence, le lecteur fournit un indicateur d'authentification (T) ou d'absence d'authentification (F) à la carte (bloc 20). La procédure d'authentification est alors terminée.

Un procédé d'authentification tel que décrit en figure 1 est connu. L'invention intervient uniquement pour fournir la donnée privée s de façon caractéristique.

Les tailles des différentes données sont généralement importantes pour améliorer la sécurité contre le piratage.

Selon un exemple particulier de réalisation, les différentes grandeurs sont liées entre elles par les algorithmes et relations suivantes :

les clés publiques v et privées s sont liées entre elles par la relation $v = g^{-s}$ modulo n, où g représente un générateur de groupe cyclique et n un nombre entier ;

le premier algorithme ALGO1 est $X = g^{r}$ modulo n ;

le deuxième algorithme ALGO2 est $Y = r + e.s$; et

le troisième algorithme ALGO3 est $X = g^{Y}.v^{e}$ modulo n.

Toujours selon cet exemple, les différentes données prises en compte peuvent avoir les tailles suivantes :

n, g et X représentent chacun environ 1000 bits ;

r, s et Y représentent chacun environ 220 bits ; et

e représente environ 30 bits.

On notera que divers algorithmes sont connus de la technique et pourront être mis en oeuvre en ayant recours au procédé de l'invention. Par exemple, la clé publique v pourra être calculée par le lecteur ou le central à partir de l'identifiant de la carte et d'une donnée émise par cette dernière.

La figure 2 représente un mode de réalisation d'une cellule 1 d'extraction de donnée privée dans un circuit intégré selon la présente invention. La cellule 1 comporte un réseau de paramètres physiques (PPN) liés à la fabrication de la puce de circuit intégré. Ce réseau de paramètres physiques 2 fournit un grand nombre de signaux et participe à la génération de la donnée privée s selon l'invention.

Un mode de réalisation préféré d'un réseau de paramètres physiques sera illustré par la suite en relation avec la figure 3. Toutefois, on pourra également recourir à un réseau classique de paramètres physiques consistant, par exemple à mesurer des paramètres électriques. Il peut s'agir, par exemple d'une mesure d'une tension seuil d'un transistor, d'une mesure d'une résistance ou d'une mesure de capacité parasite, d'une mesure de courant produit par une source de courant, d'une mesure

de constante de temps (par exemple, un circuit RC), d'une mesure d'une fréquence d'oscillation, etc. Comme ces caractéristiques sont sensibles aux dispersions technologiques et de procédé de fabrication, on peut considérer que le ou les paramètres électriques pris en compte sont propres à une fabrication et constituent une signature des circuits intégrés issus de cette fabrication.

Dans l'exemple d'une mesure de paramètres électriques, ces signaux sont convertis en signaux numériques au moyen d'un convertisseur analogique numérique 24 (ADC) et le cas échéant multiplexés par un multiplexeur 4 (MUX) pour constituer un mot binaire SP2, stocké dans un registre 25. Le mot SP2 est donc sensible aux dispersions technologiques et de procédé de fabrication. Le convertisseur 24 et le multiplexeur 4 ont été représentés en pointillés car il s'agit d'éléments optionnels. En particulier, le convertisseur 24 pourra être omis dans le mode de réalisation préféré du réseau de paramètres physiques décrit ultérieurement en relation avec la figure 3.

De préférence, les paramètres électriques mesurés au moyen du réseau 2 ne sont pas toujours les mêmes. Le réseau 2 est alors programmable. Il est paramétré ou configuré à chaque mesure à partir d'un mot binaire MP, stocké dans un registre 26. Le mot MP est propre à la puce de circuit intégré et peut être individualisé d'une carte à une autre. La mesure des paramètres physiques est déclenchée par un signal MES issu d'une unité de commande 7 de la cellule 1.

La cellule 1 reçoit de préférence un unique signal de commande St, déclencheur d'une extraction du paramètre s délivré sur une unique borne de sortie de la cellule 1.

Le mot SP2 est fourni à un combineur 8 recevant également un mot binaire SP1 stocké dans un registre 9. Le rôle du circuit 8 est de combiner les mots SP1 et SP2 pour fournir la donnée privée s stockée dans un registre 10.

A titre d'exemple particulier de réalisation, la combinaison opérée par le combineur 8 peut être du type :

$$s = ((SP1 - SP2)^2 + (SP1 + SP2)^2)^2 \text{ modulo } P,$$

où P est un nombre premier sur k bits. Le nombre s est alors un mot de k bits obtenu à partir des mots SP1 et SP2 respectivement sur k1 et k2 bits. De préférence, les nombres k1 et k2 de bits des mots SP1 et SP2 sont égaux. Cela permet de garder l'égalité de difficulté à un pirate éventuel pour le cas où une partie (SP1 ou SP2) du mot s viendrait à être découverte.

Comme le nombre MP, le nombre SP1 est différent d'une carte à l'autre. Le combineur 8 garantit la taille de la donnée s et une valeur non nulle. Le recours à une donnée SP1 propre à la carte garantit que la clé privée s soit unique quelle que soit la donnée MP fournie au réseau de paramètres physiques pour le configurer. Selon un mode de réalisation simplifié, par exemple pour un circuit de taille réduite, on pourra chercher, pour une taille de clé privée donnée, à limiter la taille du réseau de paramètres physiques en augmentant la taille de la donnée SP1.

Selon l'invention, la cellule 1 comporte également un circuit 22 de réinitialisation (remise à zéro ou à un) de certains de ses registres. Le circuit 22 a notamment pour rôle de rendre temporaire la présence de la donnée privée s dans le registre 21. Pour garantir une sécurité optimale, le circuit 22 (Res) commande la réinitialisation non seulement du registre 21 mais également du registre 25 contenant la donnée SP2 extraite du réseau 2. En d'autres termes, on fixe la durée de vie de la donnée privée et/ou de ses constituants à partir de sa génération.

Un avantage de la présente invention est qu'en combinant le recours à un réseau de paramètres physiques pour conditionner au moins une partie de la donnée privée et à une réinitialisation temporisée des éléments de mémorisation (par exemple, des registres) stockant cette donnée privée, on empêche à un pirate éventuel de découvrir la donnée privée de la carte par un examen par exemple visuel.

Les combinaisons des paramètres MP et SP1 conditionnant l'obtention de la donnée privée augmentent la difficulté de

piratage. On notera toutefois que le recours à une combinaison des mots SP1 et SP2 est optionnel. On pourra dans une première version se contenter de générer directement la donnée privée à partir du réseau de paramètres physiques et de rendre celle-ci éphémère grâce au circuit 22. Selon une autre variante simplifiée de réalisation, les données MP et SP1 sont confondues. Dans ce cas, un seul registre 9 ou 26 est utilisé. On pourra également détecter la cohérence de la réponse du réseau de paramètres physiques dans la mesure où les données SP1 et SP2 sont alors corrélées. Cela peut permettre, par exemple, de détecter une copie réalisée après piratage de la donnée SP1 et reproduction du réseau 2, si les dispersions technologiques ou de procédé de fabrication sont différentes pour le circuit d'origine et le circuit pirate.

Le circuit 22 est par exemple commandée par une horloge CLK déclenchée par l'unité de commande 7 à l'arrivée d'un signal St de déclenchement de l'extraction du paramètre s.

Selon un mode de réalisation de l'invention appliqué au cas ou un code est saisi par l'utilisateur de la carte, ce code peut être stocké de manière directe ou modifiée dans le registre 9 pour constituer le code SP1. Dans ce cas, le circuit 22 peut également remettre à zéro le registre 9 pour empêcher la présence permanente du code SP1 sur la carte. Cette fonction est illustrée par un pointillé en figure 2.

Selon une autre variante, on peut adjoindre à la commande du réseau de paramètres physiques une source de bruit (pointillés 23). Il s'agit de fournir au réseau de paramètres physiques des commandes aléatoires hors de périodes d'authentification. Cela rend alors plus difficile le piratage par observation de la consommation du circuit. En faisant fonctionner le réseau 2 en permanence, il sera plus difficile pour un pirate de repérer à quel moment celui-ci est utilisé pour générer une clé. De plus, un pirate pourra considérer le réseau 2 comme une simple source de bruit analogique utilisée pour brouiller la consommation, ce qui est connu en soi, et par suite

éliminer la contribution à la consommation dans son attaque, y compris au moment où le réseau est utilisé pour générer une clé. Le signal de mesure commande alors un multiplexeur chargé de sélectionner ou de combiner les signaux de configuration représentés par le mot MP et les bits M23 arrivant sur la liaison 23. Le signal MES est, par exemple, un bit de déclenchement d'un multiplexeur 2' des signaux MP et M23. La source de bruit 23 peut remplacer tout ou partie du mot MP dans le paramétrage ou la programmation du réseau 2.

Selon une autre variante, le mot MP est fourni en permanence au réseau 2 qui passe alors son temps à générer la donnée SP2. La clé privée s reste toutefois générée de façon éphémère lors de la combinaison avec la donnée SP1. Il y a alors encore plus de chances que le pirate filtre la réponse en consommation du réseau 2 lors d'une attaque consistant en examiner la consommation du circuit.

La réalisation d'un réseau de paramètres physiques consistant à mesurer des paramètres électriques présents dans le réseau sous la forme de résistances, de capacités parasites ou analogues ne fait pas l'objet de la présente invention. Une telle réalisation est parfaitement classique. Il pourra s'agir, par exemple, d'un réseau de résistances et/ou de capacités commutables associées en parallèle et/ou en série, les commutateurs étant commandés en fonction des signaux de configuration MP et éventuellement M23 arrivant sur le réseau 2.

En guise de réseaux de paramètres physiques, on pourra également recourir à des circuits faisant appel à une mesure temporelle. Par exemple, on mesure le temps de lecture/écriture d'une mémoire de type EEPROM. Un exemple de réseau de paramètres physiques de ce type est décrit dans le brevet américain N° 5818738.

La figure 3 représente le schéma électrique d'un mode de réalisation préféré d'un réseau de paramètres physiques selon la présente invention.

Dans cet exemple, le circuit 2 comporte une unique borne 42 d'entrée destinée à recevoir un signal numérique E de déclenchement d'une génération. Pour la mise en oeuvre de l'invention, le signal E doit comprendre, comme on le verra par la suite en relation avec les figures 4A et 4B, au moins un front par identification. Il pourra s'agir directement du signal St.

Le circuit 2 délivre directement un code binaire B_1, B_2, ..., B_{i-1}, B_i, ..., B_{n-1}, B_n sur un nombre de bits prédéterminé, ce code étant sensible aux dispersions technologiques et de procédé de fabrication du circuit. Chaque bit B_i est délivré sur une borne 3_1, 3_2, ..., 3_{i-1}, 3_i, ..., 3_{n-1}, 3_n du circuit 2 qui lui est propre. Le circuit 2 délivre donc le code d'identification sous forme parallèle.

A chaque bit B_i du code d'identification est associé un chemin électrique P_1, P_2, ..., P_i, ..., P_n reliant la borne d'entrée commune 42 à une borne 3_i de même rang. De préférence, les retards apportés par les différents chemins électriques P_i sont choisis pour être légèrement différents les uns des autres de façon à garantir une sensibilité aux dispersions technologiques du procédé de fabrication.

On voit donc déjà que, par les différents retards apportés par les chemins électriques, le front déclencheur du signal d'entrée E est reproduit sur les différentes sorties à des instants différents.

On prévoit d'effectuer la lecture de l'information présente aux sorties du circuit 2 de façon synchronisée et à un instant correspondant, de façon approximative, au retard moyen théorique entre les différents chemins électriques. Plus précisément, selon le mode de réalisation préféré de l'invention illustré par la figure 3, on prévoit un chemin électrique moyen 44 (C0) pour fixer l'instant de lecture à partir de l'apparition du front déclencheur du signal d'entrée E.

Par exemple, le chemin 44 relie l'entrée 42 du circuit 2 aux bornes Ck de bascules 5_1, 5_2, ..., 5_i, ..., 5_n faisant partie des chemins électriques respectifs P_1, P_2, ..., P_i, ...,

P_n et dont les sorties respectives Q constituent les bornes 3_1, 3_2, ..., 3_i, ..., 3_n de sortie du circuit 2. Selon ce mode de réalisation, chaque chemin électrique P_i comporte un élément retardateur 6_1 (C1), 6_2 (C2) ..., 6_i (Ci) ..., 6_n (Cn) reliant l'entrée 42 du circuit à l'entrée D de la bascule correspondante du chemin. Les éléments retardateurs 6_i sont les éléments qui présentent, selon la présente invention, des retards différents les uns par rapport aux autres. En effet, les bascules 5_i ont, de préférence, la même constitution. Elles participent toutefois au retard apporté au signal d'entrée jusqu'aux bornes de sortie respective du circuit 2 par rapport au retard moyen C0 apporté par l'élément 44.

Lorsqu'on applique un front sur le signal d'entrée E, ce front arrive sur les entrées D respectives des bascules à des instants différents. La lecture de l'état d'entrée des différentes bascules est synchronisée par le front du signal E retardé, cette fois, par l'élément 44. C'est notamment pour cette raison que l'on choisit préférentiellement un retard C0 correspondant approximativement au retard moyen des différents éléments 6_i.

Dans l'exemple de la figure 3, les différentes sorties 3_i du circuit 2 sont reliées individuellement en entrée d'un registre de mémorisation du code binaire obtenu, chaque bit B_i correspondant à l'une des sorties du circuit. En pratique, ce registre est le registre 25 de la figure 2.

Les figures 4A et 4B illustrent, sous forme de chronogrammes et sans respect d'échelle, le fonctionnement du réseau 2 de la figure 3. Les figures 4A et 4B représentent des exemples d'allures du signal E, et des signaux en sortie des différents éléments retardateurs. Dans l'exemple des figures 4A et 4B, on considère pour simplifier le cas d'un code binaire sur quatre bits. Les chronogrammes ont été désignés par les références C0, C1, C2, C3 et C4.

La différence entre les figures 4A et 4B représente la différence entre deux circuits 1 intégrés sur des puces issues de fabrications différentes.

En figure 4A, on suppose qu'à un instant t5, on déclenche un front montant sur le signal E. Ce front apparaît sur les différentes entrées des bascules D (correspondant aux sorties des éléments retardateurs C1, C2, C3 et C4) à des instants respectifs différents t1, t2, t3 et t4. Par ailleurs, l'élément 44 (C0) apporte un retard déclenchant la lecture des données en entrée des bascules à un instant t0. Tous les chemins qui génèrent un retard supérieur au retard C0 fournissent un bit à l'état 0 dans la mesure où le front du signal E ne leur est pas encore parvenu. Tous les chemins qui génèrent un délai inférieur au délai C0 produisent un bit à l'état 1 dans le mesure où le front du signal E arrive sur l'entrée de la bascule correspondante avant l'expiration du délai C0. Dans l'exemple de la figure 4A, à l'instant t0, on fournit le code 1010 comme code d'identification.

La figure 4B illustre le même circuit issu d'un procédé de fabrication différent donnant donc une puce différente. Le code obtenu y est différent. Par exemple, il s'agit du code 0010. En figure 4B, on a fait apparaître arbitrairement un instant t5 identique au cas de la figure 4A. Par contre, les instants t'0, t'1, t'2, t'3 et t'4 auxquels le front du signal E a terminé de parcourir les chemins respectifs C0, C1, C2, C3 et C4 sont différents du cas de la figure 4A.

On remarquera que l'élément retardateur C0 est lui-même sensible aux dispersions technologiques et de procédé de fabrication. Cela n'a cependant pas d'incidence pour la mise en oeuvre de l'invention dans la mesure où ce retard représente un retard moyen et où le code recherché est arbitraire. En effet, pour la génération d'une clé privée, ce qui est important, c'est que des circuits intégrés issus d'un même procédé de fabrication fournissent le même code. Comme les éléments retardateurs sont sensibles aux dispersions de procédé de fabrication, ce sera le

cas avec la mise en oeuvre du mode de réalisation préféré du réseau 2 de paramètres physiques.

Un avantage de ce mode de réalisation est que le réseau 2 est particulièrement sensible. En pratique, la différence détectable des retards apportés par les différents chemins est de l'ordre de la picoseconde. Or, les dispersions des procédés de fabrication ou technologiques apportent le plus souvent des différences de l'ordre d'au moins une dizaine de picosecondes.

Un autre avantage est qu'en cas de dérive dans le temps d'un des retards apportés par les éléments, cela n'affecte pas les résultats du circuit. En effet, tous les éléments de retard étant de préférence de constitution similaire, la dispersion sera dans le même sens pour tous les éléments (chemins).

Pour réaliser les éléments retardateurs des chemins électriques du réseau de la figure 3, on pourra utiliser n'importe quels éléments intégrés sensibles aux dispersions technologiques ou influencés par le procédé de fabrication. Il pourra s'agir, par exemple, de séries de résistances et/ou de condensateurs. Pour les résistances, on pourra recourir à des résistances dans l'épaisseur du circuit intégré, mais on préférera utiliser des résistances en silicium polycristallin dont la valeur est liée à la géométrie et qui présentent l'avantage d'être moins dépendante de la température. Bien entendu, les éléments retardateurs pourront prendre d'autres formes, pourvu d'être sensibles aux dispersions technologiques et/ou de procédés de fabrication. De plus, le choix de la plage de variation des retards apportés par les différents éléments dépendent de l'application et de la sensibilité souhaitée.

Un avantage du réseau de paramètres physiques illustré par la figure 3 est qu'il évite le recours à un convertisseur analogique/numérique 24 dans la mesure où le mot binaire est directement délivré par les sorties respectives des bascules.

Les figures 5 à 7 représentent, de façon schématique et partielle, différents modes de réalisation du circuit 22 de réinitialisation.

Selon un premier mode de réalisation illustré par la figure 5, le circuit 22 est constitué de plusieurs éléments retardateurs 71 (τ), 72 (τ'), 73 (τ'') pour différencier les instants de réinitialisation des registres 25, 9 et 21. Dans l'exemple de la figure 5, l'élément 71 apporte le retard τ de réinitialisation du registre 25. L'élément 72 et l'élément 71 avec lequel il est en série apportent le retard $\tau+\tau'$ de réinitialisation du registre 9. L'élément 73 et l'élément 71 avec lequel il est en série apportent le retard $\tau+\tau''$ de réinitialisation du registre 21. On voit que, de façon simplifiée, le signal appliqué à l'élément retardateur 71 constituant le premier élément du circuit 22 peut être directement le bit du signal St qui peut également constituer le bit MES de commande du réseau de paramètres physiques. Dans ce cas, il suffit que les entrées de réinitialisation des différents registres soient activables par l'état approprié du bit St.

Selon le deuxième mode de réalisation de la figure 6, on utilise le signal MES pour déclencher un élément retardateur 74 fournissant un retard minimal τm. Puis on ajoute à ce retard minimal, un retard variable τv fourni par un élément 75 configurable en fonction du signal MP et, s'il existe, du bruit 23. La figure 6 illustre également un exemple de commande du réseau de paramètres physiques plus détaillé qu'en figure 2. On y a fait figurer un multiplexeur 76 de combinaison des signaux MP et du bruit 23 ou de sélection du signal MP ou du bruit 23. La lecture de ce multiplexeur est commandée par le signal MES. La sortie du multiplexeur délivre un mot de configuration dans un registre 77 (REG). Ce mot de configuration sert au réseau de paramètres physiques 2" proprement dit et, selon ce mode de réalisation, à configurer le retard variable τv.

Selon un troisième mode de réalisation illustré par la figure 7, on utilise un retard τ fixe, fourni par un élément 71. Toutefois, au lieu d'être déclenché par l'apparition du signal St, le retard τ est déclenché par la mise en oeuvre du réseau de paramètres physiques, c'est-à-dire par le multiplexeur 76 ou par

le registre 77 (non représenté en figure 7), ou par un signal produit par le réseau lui-même. Dans l'exemple de la figure 7, l'élément retardateur 71 peut être bien entendu associé aux éléments 72 et 73 de la figure 5. Plus généralement, les différents exemples de réalisation ainsi que d'autres peuvent être prévus individuellement ou en combinaison.

Bien entendu, la présente invention est susceptible de diverses variantes et modifications qui apparaîtront à l'homme de l'art. En particulier, bien que l'invention ait été décrite en relation avec un procédé d'authentification particulier, celle-ci s'applique quelle que soit la procédure d'authentification envisagée, pourvu qu'elle ait recours à une donnée privée de la part du circuit à identifier.

De plus, on a fait référence à des registres de stockage qui pourront être remplacés par tout élément de mémorisation adapté, par exemple, des mémoires ou des parties de mémoire volatiles ou non selon le type de donnée stockée. En outre, l'écriture et la lecture des données dans ces éléments de mémorisation pourront être série ou parallèle.

Enfin, on pourra prévoir de réduire le temps de présence de la clé privée au fur et à mesure de ses générations lors d'une même authentification, par exemple lors de générations successives requises par des authentifications infructueuses. Cela améliore encore la fiabilité en réduisant la présence de la clé privée pour le cas où il s'agit d'une attaque visant à détecter cette clé.

REVENDICATIONS

1. Procédé d'extraction d'une donnée privée (s) dans un circuit intégré participant à une procédure d'authentification au moyen d'un dispositif externe tenant compte de cette donnée privée, caractérisé en ce qu'il consiste à générer la donnée privée sur demande et à la rendre éphémère.

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste, à chaque génération de la donnée privée (s), à initialiser une durée de vie de cette donnée privée et effacer cette donnée d'au moins un premier élément de mémorisation (21) la contenant, à l'issue de cette durée de vie.

3. Procédé selon la revendication 2, caractérisé en ce que la génération de la donnée privée et l'initialisation de sa durée de vie sont déclenchées par un même signal (St).

4. Procédé selon la revendication 2 ou 3, caractérisé en ce qu'il consiste à réduire la durée de vie de la donnée privée (s) au fur et à mesure de ses générations.

5. Procédé selon l'une quelconque des revendications 2 à 4, caractérisé en ce que la durée de vie est variable.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que la donnée privée (s) est obtenue au moins partiellement à partir d'un réseau de paramètres physiques (2).

7. Procédé selon la revendication 6, caractérisé en ce que le réseau de paramètres physiques (2) est programmable.

8. Procédé selon la revendication 7, caractérisé en ce que le réseau de paramètres physiques (2) est programmé, au moins partiellement, par un mot (MP) fourni par un élément de mémorisation.

9. Procédé selon la revendication 7 ou 8, caractérisé en ce que le réseau de paramètres physiques (2) est programmé, au moins partiellement, par du bruit (23).

10. Procédé selon l'une quelconque des revendications 6 à 9, caractérisé en ce qu'il consiste à commander le réseau de

paramètres physiques (2) également hors des périodes de génération de la donnée privée (s).

11. Procédé selon l'une quelconque des revendications 6 à 10, caractérisé en ce que la donnée privée (s) est obtenue au moins à partir :

d'une première donnée (SP1) mémorisée dans le circuit intégré ; et

d'une deuxième donnée (SP2) générée sur demande par le réseau de paramètres physiques (2).

12. Procédé selon la revendication 11, caractérisé en ce qu'il consiste à rendre éphémère la deuxième donnée (SP2).

13. Procédé selon la revendication 11 ou 12, caractérisé en ce que les nombres de bits des première (SP1) et deuxième (SP2) données sont proches l'un de l'autre, de préférence égaux.

14. Circuit intégré, caractérisé en ce qu'il comporte des moyens pour la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 13.

15. Circuit selon la revendication 14, caractérisé en ce qu'il comporte un circuit (22) de réinitialisation d'au moins un élément de mémorisation (21, 9, 25).

16. Circuit selon la revendication 15, caractérisé en ce que le circuit de réinitialisation est constitué d'un ou plusieurs éléments retardateurs (71, 72, 73, 74, 75) initialisés par une commande de génération de la donnée privée (s).

17. Circuit selon la revendication 16, caractérisé en ce que le retard apporté par au moins un élément retardateur (75) du circuit de réinitialisation est variable.

2823398

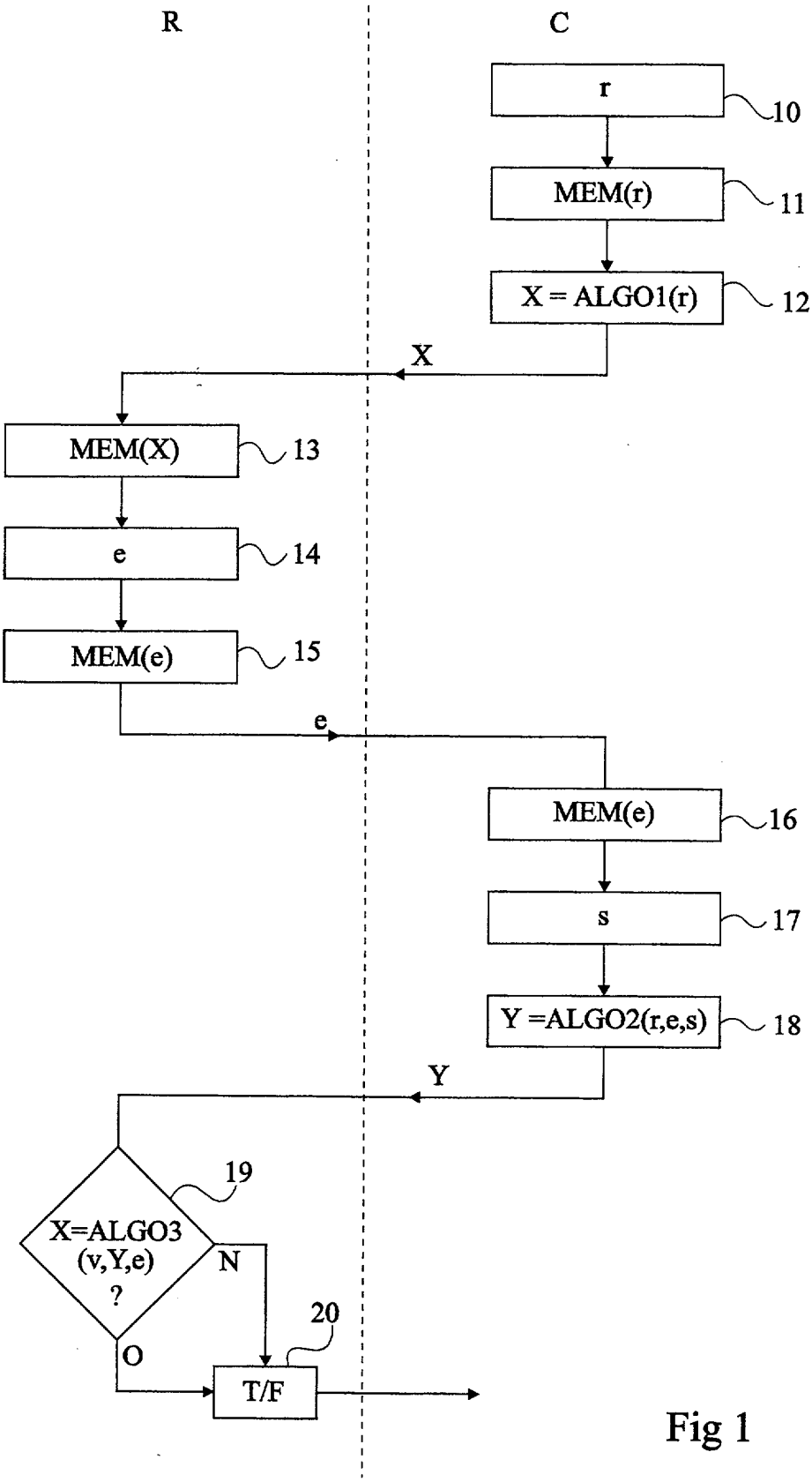


Fig 1

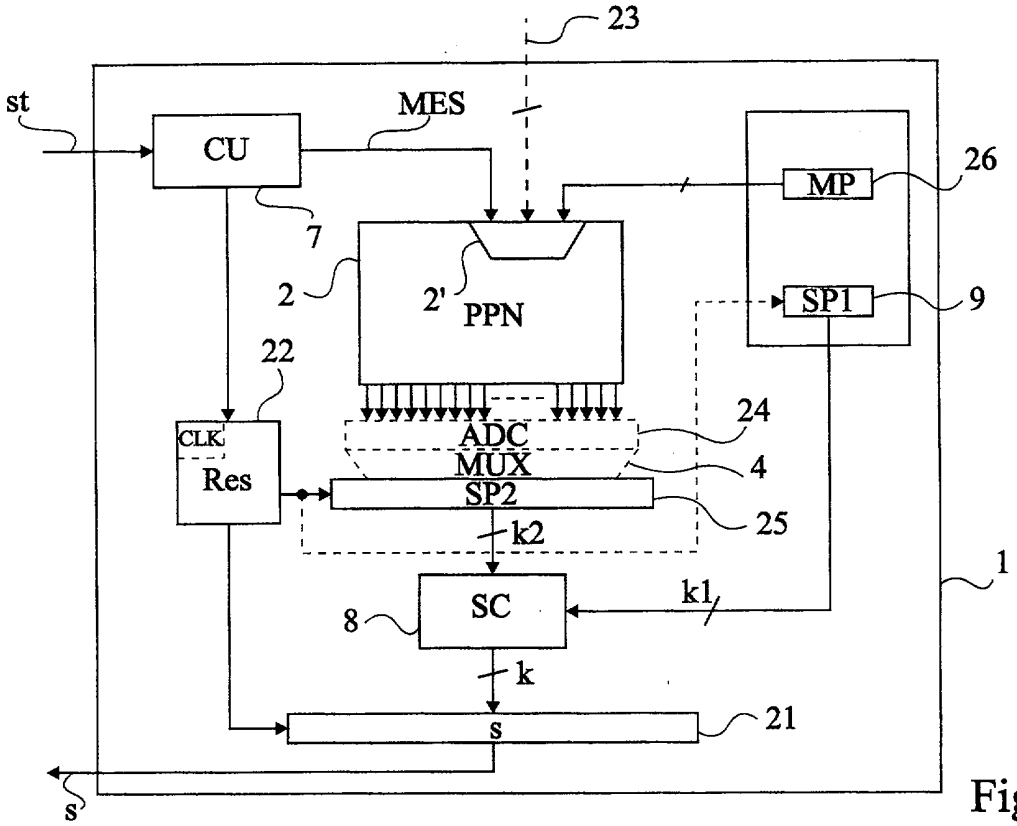


Fig 2

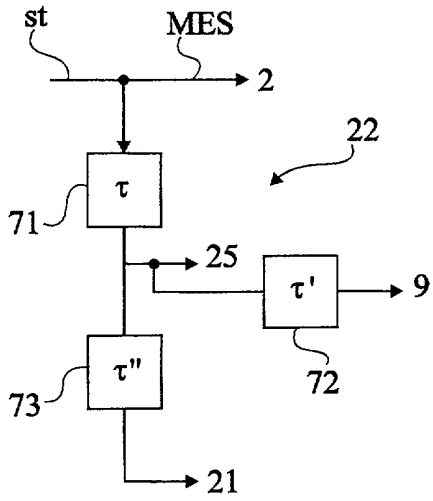


Fig 5

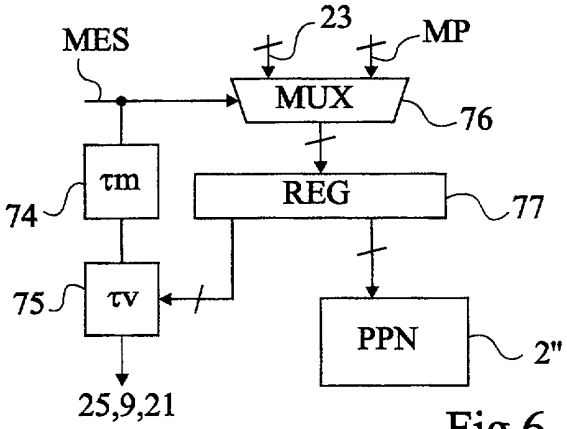


Fig 6

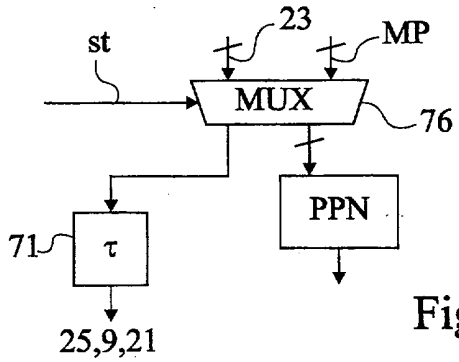


Fig 7

2823398

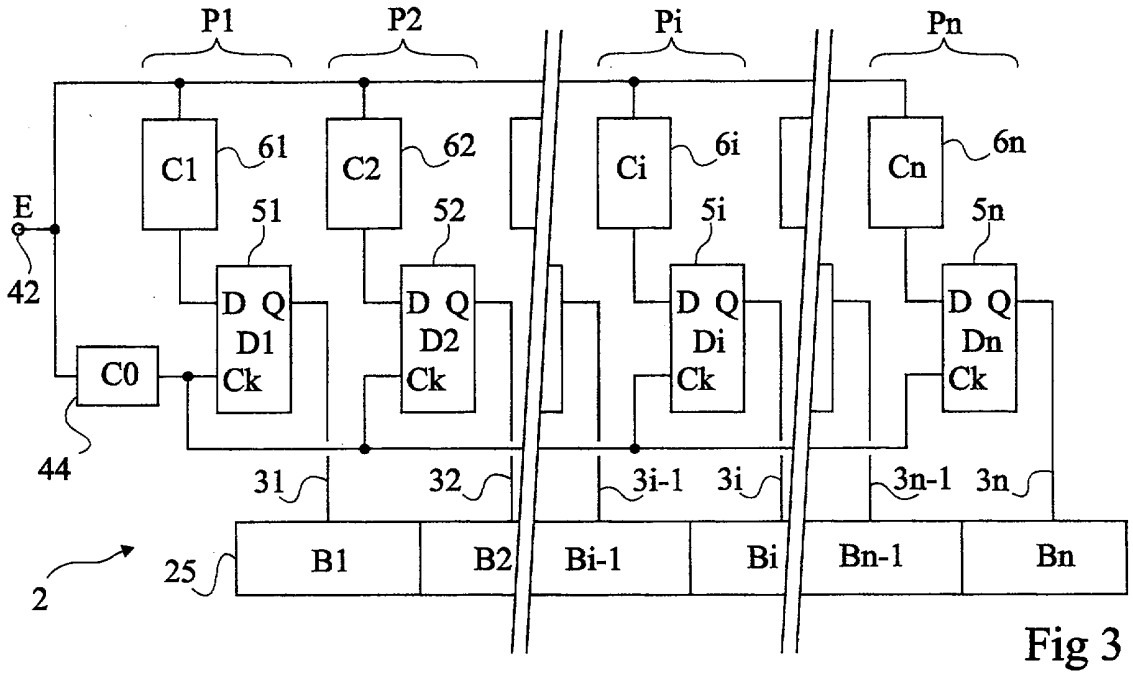


Fig 3

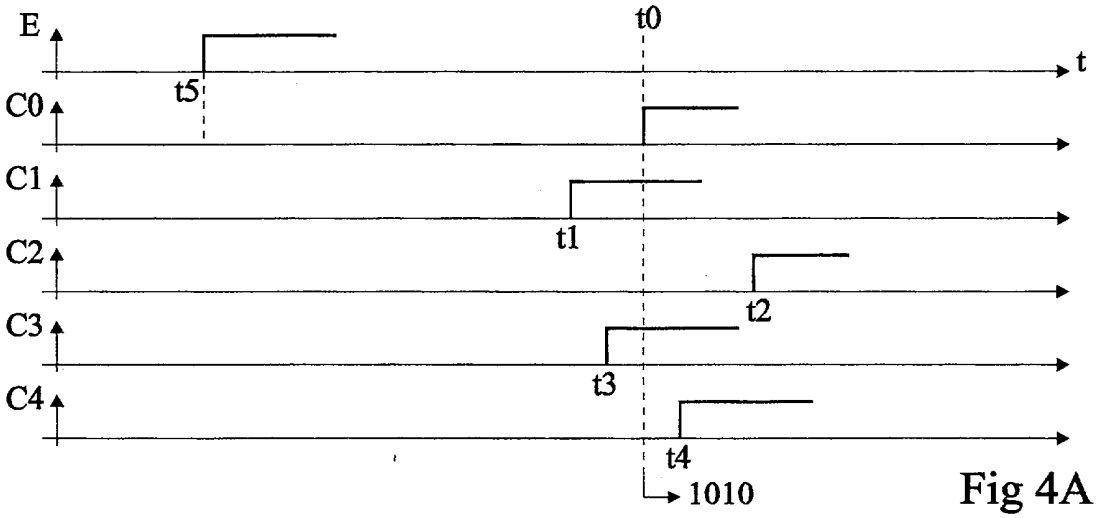


Fig 4A

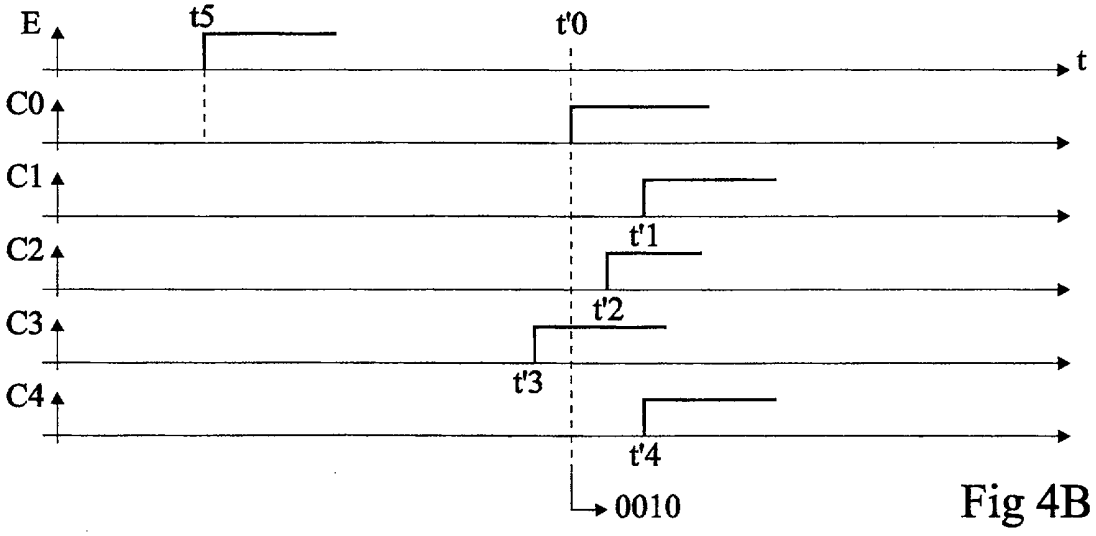


Fig 4B

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2823398

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 602829
FR 0104586

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	DE 198 43 424 A (FRAUNHOFER GES FORSCHUNG) 23 mars 2000 (2000-03-23) * abrégé * * colonne 2, ligne 14 - colonne 4, ligne 5; figure 2 * * colonne 9, ligne 37 - ligne 62 *	1-17	H04L9/32 G06K19/07

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

G07F
G06K

Date d'achèvement de la recherche	Examinateur
30 avril 2002	Carnerero Álvaro, F

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
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 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0104586 FA 602829

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 30-04-2002
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
DE 19843424 A	23-03-2000	DE 19843424 A1	23-03-2000
		WO 0017826 A1	30-03-2000
		EP 1099197 A1	16-05-2001

EPO FORM P0465