



(43) Date de la publication internationale
27 septembre 2012 (27.09.2012)

WIPO | PCT

(10) Numéro de publication internationale
WO 2012/127135 A1

- (51) Classification internationale des brevets :
G06K 19/073 (2006.01) *H03K 3/037* (2006.01)
G06F 21/00 (2006.01)
- (21) Numéro de la demande internationale :
PCT/FR2012/000103
- (22) Date de dépôt international :
23 mars 2012 (23.03.2012)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
1100889 24 mars 2011 (24.03.2011) FR
- (71) Déposants (*pour tous les États désignés sauf US*) : **UNIVERSITÉ MONTPELLIER 2 SCIENCES ET TECHNIQUES** [FR/FR]; 2, Place Eugène Bataillon, F-34095 Montpellier (FR). **CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE** [FR/FR]; 3 Rue Michel-Ange, F-75794 Paris Cedex 16 (FR).
- (72) Inventeurs; et
- (75) Inventeurs/Déposants (*pour US seulement*) : **MAURINE Philippe** [FR/FR]; 135 Chemin des Costètes, F-30260 Quissac (FR). **VAQUIE, Bruno** [FR/FR]; 79 Rue Romy Schneider, F-34070 Montpellier (FR).
- (74) Mandataire : **TOLBOT, Alexandre**; Cabinet Hecké, 10, Rue d'Arménie - Europole, BP 153, F-38025 Grenoble Cedex 1 (FR).
- (81) États désignés (*sauf indication contraire, pour tout titre de protection nationale disponible*) : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title : SECURE MEMORY ELEMENT

(54) Titre : ÉLÉMENT MÉMOIRE SÉCURISÉS

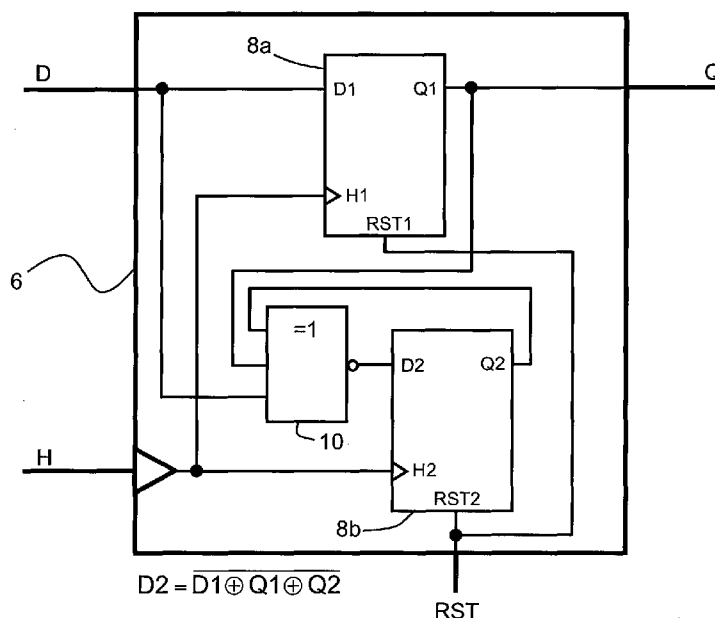


Fig. 4

(57) Abstract : The memory element comprises a clock, a first flip-flop (8a) of master-slave D type regulated by the clock and a second flip-flop (8b) of master-slave D type, structurally identical to the first flip-flop, regulated by the clock and connected to the first flip-flop (8a) in such a way that the second flip-flop (8b) switches upon each active edge of the clock where the first flip-flop does not switch.

(57) Abrégé :

[Suite sur la page suivante]



(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— relative à la qualité d'inventeur (règle 4.17.iv))

Publiée :

— avec rapport de recherche internationale (Art. 21(3))

L'élément mémoire comprend une horloge, une première bascule (8a) de type D maître-esclave cadencée par l'horloge et une seconde bascule (8b) de type D maître-esclave, structurellement identique à la première bascule, cadencée par l'horloge et connectée à la première bascule (8a) de sorte que la seconde bascule (8b) commute à chaque front actif de l'horloge où la première bascule ne commute pas.

ELEMENT MEMOIRE SECURISE

Domaine technique de l'invention

L'invention est relative aux circuits intégrés sécurisés, et plus particulièrement à une bascule de type D maître-esclave résistante aux
5 attaques par canaux cachés.

État de la technique

Les circuits électroniques sécurisés sont destinés à traiter des données secrètes ou confidentielles. Ils sont, par exemple, utilisés dans les cartes à puce pour effectuer des transactions bancaires. De manière générale, ce
10 type de circuit est construit autour d'un microprocesseur associé à une mémoire. Le microprocesseur met en œuvre des algorithmes de cryptographie pour chiffrer ou déchiffrer des messages, ou bien utilise un certificat pour authentifier un utilisateur.

Une donnée secrète, telle qu'une clé de cryptographie, peut transiter entre le
15 microprocesseur et la mémoire par un registre. Un registre est une mémoire tampon formée de bascules, généralement de type D maître-esclave (flip-flop D). A chaque bascule correspond un bit du registre.

La figure 1 représente le symbole d'une bascule D maître-esclave classique. La bascule comprend une entrée de données D, une entrée d'horloge H et
20 une sortie Q. Un signal RST permet d'initialiser l'état de la bascule lors de la mise sous tension, c'est-à-dire la valeur du bit mémorisé dans la bascule.

A chaque front montant du signal d'horloge H, la sortie Q recopie la valeur d'entrée D. La bascule maintient ensuite cette valeur jusqu'au prochain front montant. Ainsi, lorsque la donnée présentée en entrée D est identique à la
25 valeur stockée dans la bascule, l'état de la sortie Q ne varie pas. Par contre, lorsque l'entrée D diffère de la valeur stockée, la sortie Q change d'état. On parle alors de commutation ou de basculement.

La figure 2 représente la consommation en courant d'une telle bascule. La courbe en traits pointillés correspond au courant consommé par la bascule

lors d'une commutation, tandis que la courbe en trait plein représente la consommation de la bascule en absence de commutation.

On distingue donc deux profils de consommation selon que la donnée mémorisée dans la bascule change ou ne change pas. Ainsi, la
5 consommation de la bascule dépend de l'état de la donnée en entrée et de l'état courant dans la bascule.

Les attaques par canaux cachés (« Side Channel Attacks » en anglais), et plus particulièrement les attaques de type analyse différentielle (« Differential Power Analysis », DPA) et en corrélation (« Correlation Power Analysis », CPA) de puissance ou des émissions électromagnétiques, exploitent cette
10 différence de consommation pour retrouver la clé cryptographique stockée dans le circuit sécurisé.

Les fabricants de circuits sécurisés prévoient des systèmes de contre-mesure pour protéger les registres contre les attaques DPA. En particulier, la
15 demande de brevet FR2802733 vise à masquer la différence de consommation d'une bascule D maître-esclave.

La figure 3 représente schématiquement la bascule D décrite dans cette demande. La bascule comprend classiquement un étage maître 2M et un étage esclave 2S, de structure identique et connectés en série. La bascule
20 comprend en outre un circuit de masquage de la consommation. Le circuit de masquage se compose d'un étage témoin 4M monté en parallèle de l'étage maître 2M et d'un étage témoin 4S monté en parallèle de l'étage esclave 2S.

Le fonctionnement de cette bascule est en bref le suivant. Lorsque la donnée en entrée D est identique à la donnée en mémoire, les étages maître et esclave ne commutent pas. Par contre, les deux étages témoins commutent.
25 Lorsque la donnée en entrée diffère de celle en mémoire, l'un des étages maître et esclave commute, ainsi que l'un des étages témoins. En d'autres termes, il y a toujours deux des quatre étages qui commutent à chaque front d'horloge.

30 On observe cependant que la différence de consommation n'est pas suffisamment réduite et on parvient encore à distinguer l'état dans lequel se trouve la bascule. Cela est dû au fait que l'étage témoin n'est pas

rigoureusement identique à l'étage correspondant de la bascule (maître ou esclave). En effet, un nœud des étages témoins est déconnecté, comme cela est visible sur la figure 3. La consommation due au basculement d'un étage témoin est alors différente de celle de l'étage maître ou esclave.

- 5 En outre, la consommation électrique de cette bascule est fortement augmentée, en raison du basculement systématique de deux étages.

Résumé de l'invention

On constate qu'il existe un besoin de prévoir un élément mémoire robuste aux attaques, tout en ayant une consommation électrique maîtrisée.

- 10 On tend à satisfaire ce besoin en prévoyant une horloge, une première bascule de type D maître-esclave cadencée par l'horloge et une seconde bascule de type D maître-esclave, structurellement identique à la première bascule, cadencée par l'horloge et connectée à la première bascule de sorte que la seconde bascule commute à chaque front actif de l'horloge où la
15 première bascule ne commute pas.

Dans un mode de réalisation, l'élément mémoire comprend un circuit logique configuré pour détecter une commutation de la première bascule et pour commander la commutation de la seconde bascule lorsque la première bascule ne commute pas.

- 20 Selon un développement, le circuit logique reçoit en entrée un signal d'entrée de la première bascule, un signal de sortie de la première bascule et un signal de sortie de la seconde bascule, le circuit logique étant configuré pour faire commuter la seconde bascule lorsque aucun des trois signaux est dans un état actif ou lorsque deux des trois signaux sont dans un état actif.
- 25 Dans un autre mode de réalisation, l'élément mémoire comprend un circuit générateur de l'horloge à partir d'un signal externe, configuré pour introduire un retard aléatoire entre chaque front actif de l'horloge et un front actif associé du signal externe.

- Selon un développement, l'horloge est générée à l'aide d'une pluralité
30 d'inverseurs à partir du signal externe et le circuit générateur comprend un circuit de modulation du nombre d'inverseurs.

Description sommaire des dessins

D'autres avantages et caractéristiques ressortiront plus clairement de la description qui va suivre de modes particuliers de réalisation donnés à titre d'exemples non limitatifs et illustrés à l'aide des dessins annexés, dans
5 lesquels :

- la figure 1, précédemment décrite, est une représentation symbolique d'une bascule D maître-esclave ;
- la figure 2, précédemment décrite, représente la consommation en courant d'une bascule selon la figure 1, avec et sans commutation ;
- 10 - la figure 3, précédemment décrite, est un schéma synoptique d'une bascule D maître-esclave sécurisée selon l'art antérieur ;
- la figure 4 représente un mode de réalisation d'un élément mémoire sécurisé muni de deux bascules D maître-esclave interconnectées par un circuit logique ;
- 15 - les figures 5 à 9 sont des chronogrammes illustrant un fonctionnement global de l'élément mémoire de la figure 4 ;
- la figure 10 représente des profils de consommation en courant de l'élément mémoire selon la figure 4 ;
- la figure 11 est un schéma synoptique d'un élément mémoire muni
20 d'un arbre d'horloge interne ;
- les figures 12 à 18 sont des chronogrammes de signaux internes de l'élément mémoire de la figure 11 ;
- la figure 19 représente des profils de consommation en courant de l'élément mémoire selon la figure 11 ; et
- 25 - la figure 20 représente un mode de réalisation du circuit logique de la figure 4.

Description d'un mode de réalisation préféré de l'invention

On propose ici de dupliquer une bascule de type D maître-esclave classique pour former un élément mémoire sécurisé. Les deux bascules sont interconnectées de manière à obtenir la commutation d'une seule de ces
5 bascules à chaque front actif d'un signal d'horloge. Ainsi, la consommation électrique de l'élément mémoire est sensiblement constante. Cela permet de contrer efficacement les attaques faisant appel à une analyse de puissance.

On définit un front actif comme étant le front, ou la transition, d'un signal qui déclenche la commutation d'une des bascules. Dans la description qui suit,
10 on a choisi de façon arbitraire le front montant comme front actif du signal d'horloge. De façon similaire, l'état actif d'un signal correspondra à l'état logique haut ou niveau logique '1'. Le fonctionnement de l'élément mémoire serait toutefois similaire à celui décrit ci-dessous en considérant le front descendant comme front actif et l'état bas comme état actif.

La figure 4 représente un mode de réalisation d'un élément mémoire 6 ayant une consommation équilibrée. L'élément mémoire 6 comprend une entrée de données D, une entrée d'horloge H et une sortie Q connectées respectivement aux entrées-sorties D1, H1 et Q1 d'une première bascule 8a de type D maître-esclave. L'élément comprend en outre une seconde
20 bascule 8b, structurellement identique à la bascule 8a et cadencée par la même horloge H. Les entrées H1 et H2 des bascules 8a et 8b sont donc reliées à l'entrée H de l'élément mémoire. Les entrées d'initialisation RST1 et RST2 des bascules 8a et 8b sont reliées à une entrée RST de l'élément 6. Pour des raisons de commodité, les signaux des bascules ont ci-après le
25 même nom que les entrées-sorties auxquelles ils sont affectés.

La bascule 8b est reliée à la bascule 8a par l'intermédiaire d'un circuit logique 10. Le circuit 10 reçoit en entrée le signal d'entrée D1 de la bascule 8a, le signal de sortie Q1 de la bascule 8a et le signal de sortie Q2 de la bascule 8b. La sortie du circuit 10 est connectée à l'entrée D2 de la bascule
30 8b. Ainsi, le signal D2 est une fonction logique des signaux D1, Q1 et Q2 dont le calcul est effectué de manière décalée par rapport au front actif de l'horloge.

- Dans cette configuration, les entrées D et D1 reçoivent le même signal. La bascule 8a réalise la fonction mémoire de l'élément 6 et la bascule 8b permet d'équilibrer la consommation électrique. En fait, l'élément mémoire a la même fonction que celle d'une bascule D maître-esclave. Le circuit 10 est configuré pour détecter une commutation de la bascule 8a et provoquer la commutation de la bascule 8b lorsque la bascule 8a ne commute pas.

La fonction logique du circuit 10 correspond à celle d'une porte NON-OU exclusif à trois entrées. En considérant D1, Q1 et Q2 comme les entrées du circuit 10 et D2 sa sortie, on obtient :

10

$$D2 = \overline{D1 \oplus Q1 \oplus Q2}$$

La table de vérité du circuit logique 10 est donnée ci-dessous :

D1	Q1	Q2	D2
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

On constate que la sortie D2 du circuit 10 passe à l'état haut lorsque aucune des entrées D1, Q1 et Q2 est à l'état haut ou lorsque deux de ces trois entrées sont à l'état haut.

- 15 Les figures 5 à 9 représentent, de manière simplifiée, des chronogrammes de signaux de l'élément mémoire de la figure 4. Le tracé de la figure 5 correspond au signal d'horloge H qui cadence les bascules 8a et 8b. Les

tracés des figures 6 à 9 représentent les signaux en entrées et sorties des bascules 8a et 8b, respectivement D1, Q1, D2 et Q2.

Les bascules sont préalablement initialisées à l'aide du signal RST. Les signaux Q1 et Q2, qui correspondent aux données mémorisées dans les bascules, sont initialement à l'état bas (ou niveau logique '0').

Lors d'un premier front montant d'horloge, à l'instant t_1 , l'entrée D1 est à l'état bas (Fig.6 : D1='0'). Ainsi, conformément au fonctionnement d'une bascule D maître-esclave décrit en relation avec la figure 1, la sortie Q1 reste à l'état bas (Fig.7 : Q1='0'). Il n'y a donc pas de commutation dans la bascule 8a.

Les signaux D1, Q1, et Q2 étant initialement tous à '0', le signal D2 vaut '1' (Fig.8) d'après la table de vérité du circuit logique 10. Au front montant, la sortie Q2 recopie l'entrée D2 de la bascule 8b. Le signal Q2 passe donc de '0' à '1' (Fig.9), ce qui signifie que la bascule 8b commute.

A l'instant t_2 , l'entrée D1 étant maintenue à l'état bas, la bascule 8a ne commute toujours pas. Le signal D2 vaut '0' à l'instant t_2 car une seule des entrées du circuit 10 est à l'état haut (D1='0', Q1='0', Q2='1'). De ce fait, la bascule 8b commute et le signal Q2 retombe à '0'.

A l'instant t_3 , le signal d'entrée D1 de la bascule 8a vaut '1' alors que la valeur précédemment stockée dans la bascule 8a est '0' (Fig.7 : Q1(t_2)='0'). On observe donc la commutation de la bascule 8a (Q1(t_3)='1'). A cet instant, le signal D2 vaut '0' car seule l'entrée D1 est à l'état haut. En conséquence, la bascule 8b ne commute pas (Fig.9 : Q2(t_3) = Q2(t_2) = '0').

Au quatrième front montant (t_4), le signal D1 se maintient à '1' donc la bascule 8a ne commute pas. Par contre, le signal D2 est passé à '1', ce qui provoque la commutation de la bascule 8b.

Ainsi, on peut montrer qu'on a systématiquement un seul basculement par front montant de l'horloge, quel que soit l'état de l'entrée D et l'état courant des bascules 8a et 8b. En effet, on constate sur les figures 7 et 9 qu'un seul des signaux Q1 et Q2 change de niveau à chaque front montant.

Le signal D2 tient compte du signal D1 (ou D) et de l'état en sortie de la bascule 8a (Q1) pour savoir s'il y aura une commutation de la bascule 8a. Il tient également compte de l'état de la sortie de la bascule 8b (Q2) pour générer, le cas échéant, la commutation de la bascule 8b.

- 5 La mise à jour du signal D2 est réalisée à un instant différent de celui des bascules 8a et 8b, par exemple sur les fronts descendants de l'horloge H (Fig.8). On évite ainsi des aléas dans la bascule 8b qui provoqueraient une surconsommation.

- 10 La figure 10 représente l'enveloppe de la consommation en courant définie à partir de tous les modes de fonctionnement de l'élément mémoire 6. La courbe en trait plein représente la limite inférieure de l'enveloppe de consommation, c'est-à-dire la consommation minimale quel que soit le mode de fonctionnement de l'élément 6. La courbe en traits pointillés correspond à la limite supérieure de l'enveloppe de consommation, c'est-à-dire la
15 consommation maximale quel que soit le mode de fonctionnement.

L'écart entre les deux courbes correspond à la différence maximale de consommation (dans le pire des cas) selon que la donnée mémorisée dans l'élément 6 change d'état ou non. Cette différence de consommation, inévitable, est attribuable à la polarisation des nœuds internes des bascules.

- 20 On constate que, par rapport à la figure 2, cet écart est considérablement réduit, ce qui rend plus difficiles les attaques DPA.

La figure 11 est une vue détaillée de certains constituants de l'élément mémoire 6 : les bascules 8a et 8b, ainsi qu'un arbre d'horloge interne 20. Le circuit logique 10 n'est pas représenté sur cette figure.

- 25 Chaque bascule 8a, 8b comprend un étage maître 2M et un étage esclave 2S. Les étages maître et esclave sont de structure identique et connectés en série.

- Dans l'exemple de réalisation de la figure 11, chaque étage maître 2M (respectivement esclave 2S) comprend un inverseur 12 suivi d'une première
30 porte de transfert TM (respectivement TS), et une boucle de mémorisation 14. La boucle de mémorisation 14 comprend deux autres inverseurs 16, 18

et une seconde porte de transfert TM' (respectivement TS') en série. Les portes de transfert sont par exemple formées de deux transistors MOS connectées en parallèle, l'un de type N et l'autre de type P.

5 La porte de transfert TM relie la sortie de l'inverseur 12 à un nœud de stockage de la boucle de mémorisation 14 situé entre la porte de transfert TM' et l'inverseur 16. Le nœud de stockage est noté NM1 dans l'étage maître de la bascule 8a, NS1 dans l'étage esclave de la bascule 8a, NM2 dans l'étage maître de la bascule 8b et NS2 dans son étage esclave. La sortie de l'inverseur 16 de l'étage maître est connectée à l'entrée de
10 l'inverseur 12 de l'étage esclave.

On notera que les signaux aux nœuds NM1 et NM2 des étages maîtres correspondent respectivement aux compléments des signaux d'entrée D1 et D2. En outre, les signaux aux nœuds NS1 et NS2 des étages esclaves correspondent respectivement aux signaux $\overline{Q1}$ et $\overline{Q2}$. On ajoute alors dans
15 chaque bascule 8a, 8b un inverseur 19 en parallèle avec l'étage esclave 2S pour obtenir les sorties Q1 et Q2 de la figure 4.

Les bascules 8a et 8b, et plus particulièrement les portes de transfert TM, TM', TS et TS', sont commandées par des signaux d'horloge interne CPI et CPN. Ces signaux sont affectés sur les grilles des transistors NMOS et
20 PMOS de chaque porte de transfert. Les signaux CPI, CPN sont complémentaires. Ainsi, les deux transistors d'une porte sont simultanément bloqués ou passants.

Les signaux CPI, CPN proviennent de l'arbre d'horloge 20 intégré à chaque élément mémoire. Ils sont générés à l'aide d'une pluralité d'inverseurs à
25 partir de l'horloge externe H.

L'arbre d'horloge 20 est habituellement constitué de deux inverseurs 22 et 24 connectés en série. Le signal d'horloge externe H se propage au travers des deux inverseurs. Le signal CPN est récupéré en sortie du premier inverseur 22 et le signal CPI est récupéré en sortie du deuxième inverseur 24. Ainsi, le
30 signal CPN correspond au complément du signal externe H et le signal CPI correspond au signal H.

Les portes de transfert TM et TM' sont commandées en opposition de phase : lorsque la porte TM est passante, la porte TM' est bloquée, et inversement. Pour cela, on inverse l'affectation des signaux CPI et CPN entre les portes de transfert TM et TM'. De même, les portes TS et TS' sont commandées en opposition de phase. Par contre, les portes TM et TS' sont commandées simultanément, ainsi que les portes TM' et TS.

Les figures 12 à 18 représentent, de manière simplifiée, des chronogrammes de signaux internes des bascules 8a et 8b. Les tracés des figures 12 à 14 représentent respectivement les signaux d'horloge interne, CPI et CPN, et l'entrée D1 de la bascule 8a (équivalant à l'entrée D de l'élément mémoire). Les tracés des figures 15 à 18 représentent les signaux aux nœuds de stockage NM1, NS1, NM2 et NS2 des bascules 8a et 8b.

Le fonctionnement des bascules 8a et 8b est décrit en détail ci-dessous, en relation avec le schéma synoptique de la figure 11 et les chronogrammes des figures 12 à 18.

Entre les instants t_1 et t_2 , la donnée présentée en entrée D1 (ou D) correspond déjà à celle stockée dans la bascule 8a, au nœud NM1 ($NM1=1=\overline{D1}$). Il n'a donc pas de commutation de la bascule 8a, ni dans l'étage maître (NM1 : Fig.15), ni dans l'étage esclave (NS1 : Fig.16) pendant cette période.

Par contre, on observe la commutation de la bascule 8b. Au front descendant du signal CPI (ou front montant du signal CPN), la porte de transfert TM de la bascule 8b devient passante et le nœud NM2 change d'état (Fig.17). Au front suivant, c'est-à-dire au front montant du signal CPI, la porte TS devient passante. L'étage esclave recopie alors la valeur du nœud NM2 dans le nœud NS2 (Fig.18).

A l'instant t_2 , l'entrée D1 de la bascule 8a change d'état ($D1='1'$). Cela occasionne d'abord le basculement de l'étage maître 2M de la bascule 8a. En effet, en activant la porte TM au front descendant du signal CPI, le signal au nœud NM1 passe à '0' (Fig.15). Puis, l'étage esclave 2S bascule au front montant suivant du signal CPI (à l'instant t_3). La porte TS est activée et le nœud NS1 recopie la valeur du nœud NM1 (Fig.16).

Puisque la commutation de la bascule 8a a eu lieu, le circuit 10 ne provoque aucun changement du signal D2 (non représenté) de la bascule 8b entre les instants t_2 et t_3 . On n'observe donc aucun basculement dans les étages maître et esclave associés.

- 5 Entre les instants t_3 et t_4 , l'entrée D1 reste à '1'. Lors de l'activation des portes TM et TS, il n'y a donc pas d'évolution dans l'état des nœuds NM1 et NS1 de la bascule 8a.

10 Le circuit 10 commande alors la commutation de la bascule 8b, avec une nouvelle valeur de l'entrée D2. Le nœud NM2 passe à '0' au front descendant du signal CPI, suite à l'activation de la porte TM, puis le nœud NS2 recopie cette valeur lors de l'activation de la porte TS, au front montant du signal CPI (instant t_4).

15 Ainsi, on peut montrer qu'à chaque front descendant du signal H (ou front descendant du signal CPI), seul l'un des étages maîtres commute. Au front montant du signal H (ou front montant du signal CPI), seul l'un des étages esclaves commute. Pour résumer, un seul des quatre étages de l'élément mémoire bascule à chaque front du signal d'horloge H, contrairement à la bascule D maître-esclave sécurisée de l'art antérieur.

20 Il n'y a donc pas d'augmentation de la consommation instantanée relative à la commutation systématique de deux étages. L'élément mémoire consomme moins d'énergie qu'une bascule sécurisée classique.

La bascule D maître esclave décrite dans cette demande est plus robuste aux attaques par canaux cachés que les circuits de l'art antérieur.

25 Dans le document WO00/26746 par exemple, chaque circuit de traitement de données dont on veut masquer la consommation électrique est muni d'un circuit complémentaire de masquage, contrôlé en parallèle du circuit de traitement. Lorsqu'une transition (montante ou descendante) a lieu dans le circuit de traitement de données, la transition opposée s'effectue dans le circuit de masquage (descendante ou montante respectivement).

30 Cependant, il est toujours possible de distinguer l'activité ou l'inactivité de ce circuit de traitement, en analysant la consommation en courant selon que le

circuit commute ou ne commute pas. La différence de consommation est même doublée, puisqu'on observe deux transitions (au lieu d'une seule) lorsque le circuit est actif et aucune transition lorsqu'il est inactif. Il est donc encore plus facile de mener des attaques qui exploitent cette différence de consommation.

Ici, la consommation en puissance de la bascule D maître esclave est équilibrée dans le temps car il y a systématiquement (i.e. à chaque front d'horloge) une seule des deux bascules qui commute.

Dans un mode de réalisation préférentiel représenté par des pointillés sur la figure 11, on modifie l'arbre d'horloge 20 pour former un générateur de délai aléatoire entre le signal d'horloge externe H et les signaux d'horloge interne CPI et CPN qui commandent les bascules 8a, 8b.

Le générateur de délai aléatoire 20 comporte, en plus des inverseurs 22 et 24 de l'arbre d'horloge, deux inverseurs 26 et 28 connectés en série et disposés entre les inverseurs 22 et 24. Le générateur comprend également deux portes de transfert 30 et 32. La porte 30 relie la sortie de l'inverseur 22 à l'entrée de l'inverseur 24 et la porte 32 relie la sortie de l'inverseur 28 à l'entrée de l'inverseur 24. Chaque inverseur est caractérisé par un temps de propagation du signal d'horloge externe H au travers de l'inverseur.

On distingue deux états de fonctionnement du générateur 20, selon l'état des portes 30 et 32. Celles-ci sont commandées en opposition de phase par un signal DJIT.

Lorsque le signal DJIT est à l'état bas ($DJIT=0$), la porte 30 est passante et le signal d'horloge H traverse les inverseurs 22 et 24. Le signal CPN est alors inversé et décalé du temps de propagation de l'inverseur 22 par rapport au signal H. De la même manière, le signal CPI est inversé et décalé du temps de propagation de l'inverseur 24 par rapport au signal CPN. Le signal CPI correspond donc au signal H décalé de deux temps de propagation. Cet état de fonctionnement correspond en fait à celui d'un arbre d'horloge classique.

Par contre, lorsque la porte 36 est passante ($DJIT=1$), le signal H traverse deux inverseurs supplémentaires, 26 et 28. Les retards appliqués aux

signaux CPN et CPI sont alors augmentés du temps de propagation de l'inverseur 26 et du temps de propagation de l'inverseur 28.

On peut donc, à l'aide du signal DJIT, moduler le retard temporel entre chaque front montant du signal de commande CPI et un front montant associé du signal externe H. Ce retard peut prendre deux valeurs distinctes, selon le nombre d'inverseurs utilisés pour générer le signal CPI, deux ou quatre dans l'exemple de la figure 11. Le retard est largement inférieur à la durée d'une période du signal H. Il est de l'ordre de la moitié du délai de propagation du signal entre l'entrée H et la sortie Q de la bascule de la figure 1, c'est-à-dire entre 50 ps et 100 ps en technologie 130 nm.

Le générateur 20 peut également comprendre des inverseurs et portes de transfert additionnels, agencé de manière à former d'autres boucles de propagation du signal H. On augmente ainsi le nombre de valeurs de retard possibles. Le signal DJIT est alors codé sur plusieurs bits.

Le signal DJIT correspond, de préférence, à la sortie d'un générateur de nombre aléatoire (non représenté). Le générateur de délai 20 est alors commandé de manière stochastique.

Le temps de propagation du signal H dans un inverseur varie en fonction de la taille des transistors qui constituent l'inverseur, typiquement un transistor MOS de type N et un transistor MOS de type P connectés en série. En jouant sur la taille des transistors, par exemple ceux des inverseurs 26 et 28, il est possible de faire varier les retards appliqués aux signaux CPI et CPN d'un élément mémoire à l'autre.

Dans un mode de réalisation préférentiel, un registre comprend plusieurs éléments mémoire et au moins une des deux valeurs de retard diffère d'un élément mémoire à l'autre.

La figure 19 représente l'enveloppe du courant électrique consommé par un élément mémoire 6 muni du générateur de délai aléatoire 20. On constate que l'écart entre la limite supérieure et la limite inférieure de l'enveloppe est plus faible que sur la figure 10, mais aussi que cette enveloppe s'étale sur une durée plus grande.

En fait, le délai aléatoire, introduit sur les signaux CPI et CPN, retarde la mise à jour du signal Q1 (ou du signal Q2) par rapport au front de l'horloge externe H. La consommation électrique moyenne de la bascule est donc étalée sur une période de temps plus grande.

- 5 En d'autres termes, la consommation en courant de l'élément mémoire est moyennée sur plusieurs cycles ou calculs cryptographiques. Cela a pour effet de réduire encore la différence moyenne de consommation entre tous les modes de fonctionnement de l'élément mémoire. Il devient donc difficile de distinguer l'état de l'élément mémoire à partir des relevés de
10 consommation.

Pour mener des attaques par canaux cachés sur un registre, la commutation des bascules et leurs consommations associées doivent être synchronisées par rapport au signal d'horloge externe H. Lorsque ce n'est pas le cas, l'attaquant effectue une opération dite de resynchronisation. Or, dans le cas
15 d'éléments mémoire selon la figure 11, chaque élément est légèrement désynchronisé de l'horloge H grâce au générateur 20 intégré dans chaque bascule. Cette désynchronisation est d'une part variable au sein d'une même bascule, entre deux basculements successifs, grâce au signal DJIT. D'autre part, elle peut différer d'un élément mémoire à l'autre en adaptant le
20 générateur 20, par exemple en modifiant la taille des transistors des inverseurs. La resynchronisation de tous les éléments mémoire est dès lors impossible, ce qui améliore davantage la robustesse aux attaques par canaux cachés.

En outre, le générateur de délai aléatoire 20 a pour effet de limiter les fuites
25 d'informations des circuits logiques situées en aval de l'élément mémoire. En effet, les calculs de ces circuits sont retardés, ce qui réduit également leur différence moyenne de consommation. L'élément mémoire est non seulement sécurisé, mais les circuits logiques placés en sortie sont également plus robustes aux attaques.

30 Dans un circuit logique simple rail, une valeur binaire est codée sur un fil, ce qui correspond à deux états distincts : '0' et '1'. En logique double rail, la valeur binaire est codée sur deux fils. Il est alors possible de coder jusqu'à quatre états : '00', '01', '10' et '11'. Le codage double rail est intrinsèquement

plus robuste aux attaques car il permet un premier équilibrage de la consommation.

L'élément mémoire sécurisé décrit ci-dessus peut être utilisé dans un circuit logique simple rail, en exploitant seulement le signal D1 en sortie de l'élément mémoire. Toutefois, on remarque que l'élément mémoire est aussi adapté au codage double rail avec retour à état invalide. Il suffit pour cela d'utiliser la sortie Q2 de la seconde bascule 8b. On peut ainsi combiner, de façon simple et sécurisée, des registres simple rail et des registres double rail dans un même circuit, en utilisant un seul type d'élément mémoire.

Comme cela a été décrit précédemment, le signal D2 de la bascule 8b est mis à jour avant la mise à jour des bascules 8a et 8b, c'est-à-dire avant chaque front montant du signal CPI, par exemple sur chaque front descendant.

La figure 20 représente un mode de réalisation préférentiel de circuit logique dans lequel le signal D2 est synchronisé sur les fronts descendants du signal CPI.

On souhaite dans un premier temps synchroniser le signal D1 sur les fronts descendants du signal CPI. Pour cela, on a reproduit une portion du schéma synoptique de la bascule 8a (Fig.11). Cette portion en entrée de la bascule 8a comprend successivement l'inverseur 12, la porte de transfert TM et l'inverseur 16. Le signal D1', en sortie de l'inverseur 16, correspond au signal D1 synchronisé sur les fronts descendants du signal CPI. En effet, la porte TM est passante lors d'un état bas du signal CPI.

Dans l'exemple des figures 12 à 18, le signal D1 est synchronisé sur les fronts montants du signal CPI. Le signal D1' sera alors décalé d'une moitié de cycle d'horloge par rapport au signal D1. Le signal D1' correspond en fait au complément du signal au nœud NM1 (Fig.15).

Sur la figure 20, deux portes de transfert TG et TG' permettent d'obtenir les signaux Q1' et Q2' à partir des signaux Q1 et Q2. Les signaux Q1' et Q2' correspondent respectivement aux signaux Q1 et Q2 synchronisés sur les fronts montants du signal CPI et dont les valeurs sont maintenues sur l'état bas du signal CPI.

La fonction NON-OU exclusif du circuit 10 est réalisée par une pluralité d'inverseurs et de portes de transfert agencés de manière à définir différents chemins de propagation du signal D1'.

5 Le circuit 10 comprend un premier inverseur 34 recevant en entrée le signal D1' et connecté en série à une première branche 36a munie d'une porte de transfert 38a. Une seconde branche 36b, en parallèle de la branche 36a, comprend une porte de transfert 38b et un inverseur 34b. Les portes 38a et 38b sont commandées en opposition de phase par les signaux Q1' et $\overline{Q1'}$.

10 Une troisième branche 36c est connectée en série avec les branches 36a et 36b. Elle comprend une porte de transfert 38c. Connectée en parallèle de la branche 36c, une branche 36d comprend une porte de transfert 38d et un inverseur 34d. Les portes 38c et 38d sont commandées en opposition de phase par les signaux Q2' et $\overline{Q2'}$.

15 Le signal D1' se propage systématiquement au travers deux des quatre branches, l'une des branches 36a et 36b, puis l'une des branches 36c et 36d, selon l'état des portes 38a-d. Ainsi, le signal D' traverse un, deux ou trois inverseurs selon l'état des signaux Q1', Q2', $\overline{Q1'}$ et $\overline{Q2'}$. A titre d'exemple, lorsque les signaux Q1' et Q2' sont à l'état bas ('0'), le signal D1' se propage au travers des branches 36a et 36c et ne traverse qu'un seul
20 inverseur (34). Le signal D2 vaut alors '1' si le signal D1' est à '0' et '0' si le signal D1' est à '1'.

Avec cette configuration, on parvient à associer une valeur du signal D2 à chaque combinaison de valeurs des signaux D1, Q1 et Q2, selon la table de vérité du circuit logique 10. Le signal D2 évolue en même temps que le
25 signal D1', c'est-à-dire en synchronisme avec les fronts montants du signal d'horloge CPI.

De nombreuses variantes et modifications de l'élément mémoire apparaîtront à l'homme du métier. En particulier, d'autres implémentations de bascule D maître-esclave, de porte NON-OU exclusif et d'inverseur que celles qui sont
30 décrites ici peuvent être employées.

Revendications

1. Élément mémoire comprenant une horloge (CPI), une première bascule (8a) de type D maître-esclave cadencée par l'horloge, caractérisé en ce qu'il comprend une seconde bascule (8b) de type D maître-esclave,
5 structurellement identique à la première bascule, cadencée par l'horloge (CPI) et connectée à la première bascule de sorte que la seconde bascule (8b) commute à chaque front actif de l'horloge où la première bascule (8a) ne commute pas.
2. Élément mémoire selon la revendication 1, comprenant un circuit logique
10 (10) configuré pour détecter une commutation de la première bascule (8a) et pour commander la commutation de la seconde bascule (8b) lorsque la première bascule (8a) ne commute pas.
3. Élément mémoire selon la revendication 2, dans lequel le circuit logique
15 (10) reçoit en entrée un signal d'entrée (D1) de la première bascule (8a), un signal de sortie (Q1) de la première bascule (8a), et un signal de sortie (Q2) de la seconde bascule (8b), le circuit logique (10) étant configuré pour faire commuter la seconde bascule (8b) lorsque aucun des trois signaux (D1, Q1, Q2) est dans un état actif ou lorsque deux des trois signaux sont dans un état actif.
- 20 4. Élément mémoire selon la revendication 3, dans lequel le circuit logique (10) est une porte NON-OU exclusif agencée pour fonctionner en décalage avec le front actif de l'horloge.
5. Élément mémoire selon la revendication 1, comprenant un circuit
25 générateur (20) de l'horloge (CPI) à partir d'un signal externe (H), configuré pour introduire un retard aléatoire entre chaque front actif de l'horloge (CPI) et un front actif associé du signal externe (H).
6. Élément mémoire selon la revendication 5, dans lequel l'horloge (CPI) est
30 générée à l'aide d'une pluralité d'inverseurs (22, 24, 26, 28) à partir du signal externe (H), et dans lequel le circuit générateur (20) comprend un circuit de modulation (30, 32) du nombre d'inverseurs.

7. Élément mémoire selon la revendication 6, dans lequel le retard varie entre une première valeur et seconde valeur en fonction du nombre d'inverseurs (22, 24, 26, 28) utilisés pour générer l'horloge (CPI).
- 5 8. Circuit intégré comprenant des premier et second éléments mémoire selon la revendication 7, caractérisé en ce que la première valeur de retard du premier élément diffère de la première valeur de retard du second élément.

1/7

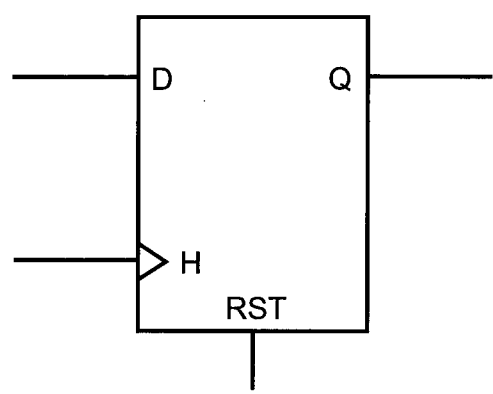


Fig. 1 (art antérieur)

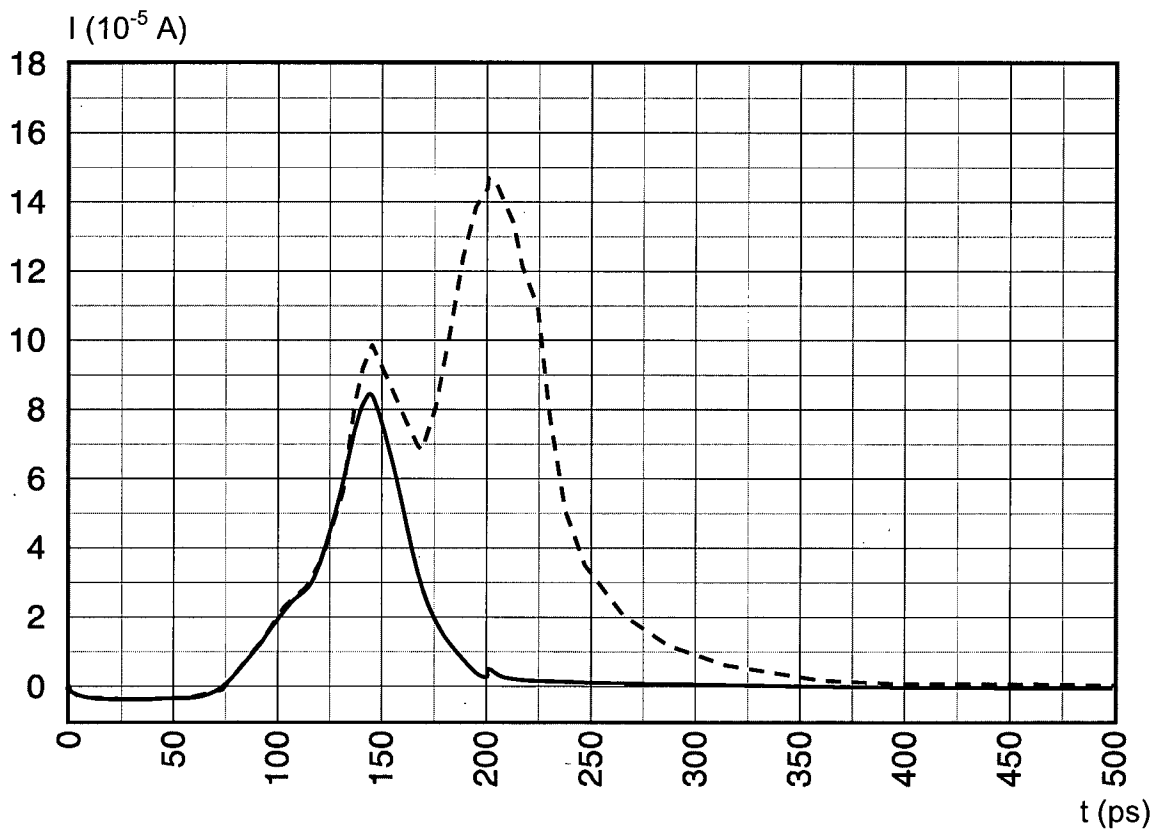


Fig. 2 (art antérieur)

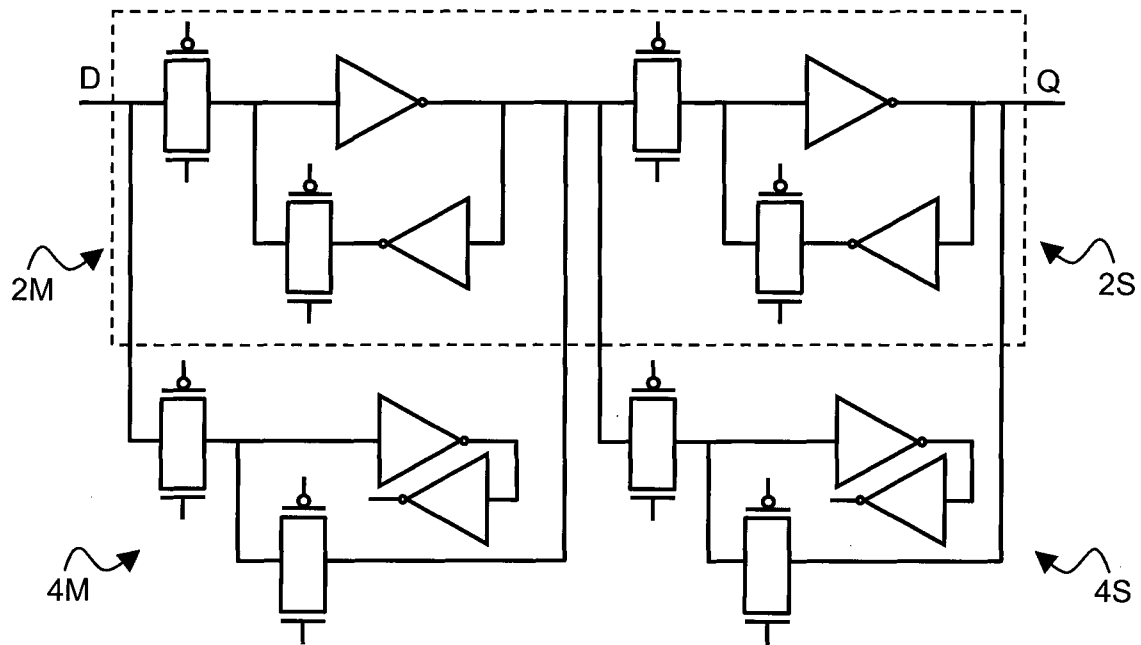


Fig. 3 (art antérieur)

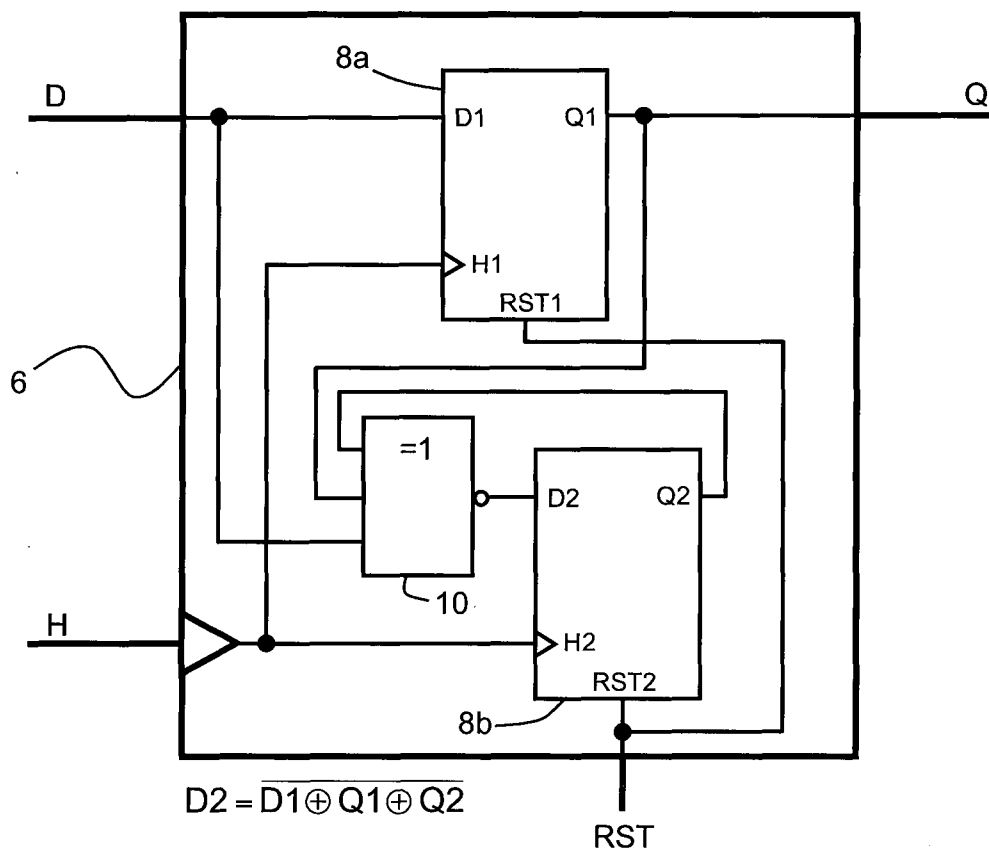


Fig. 4

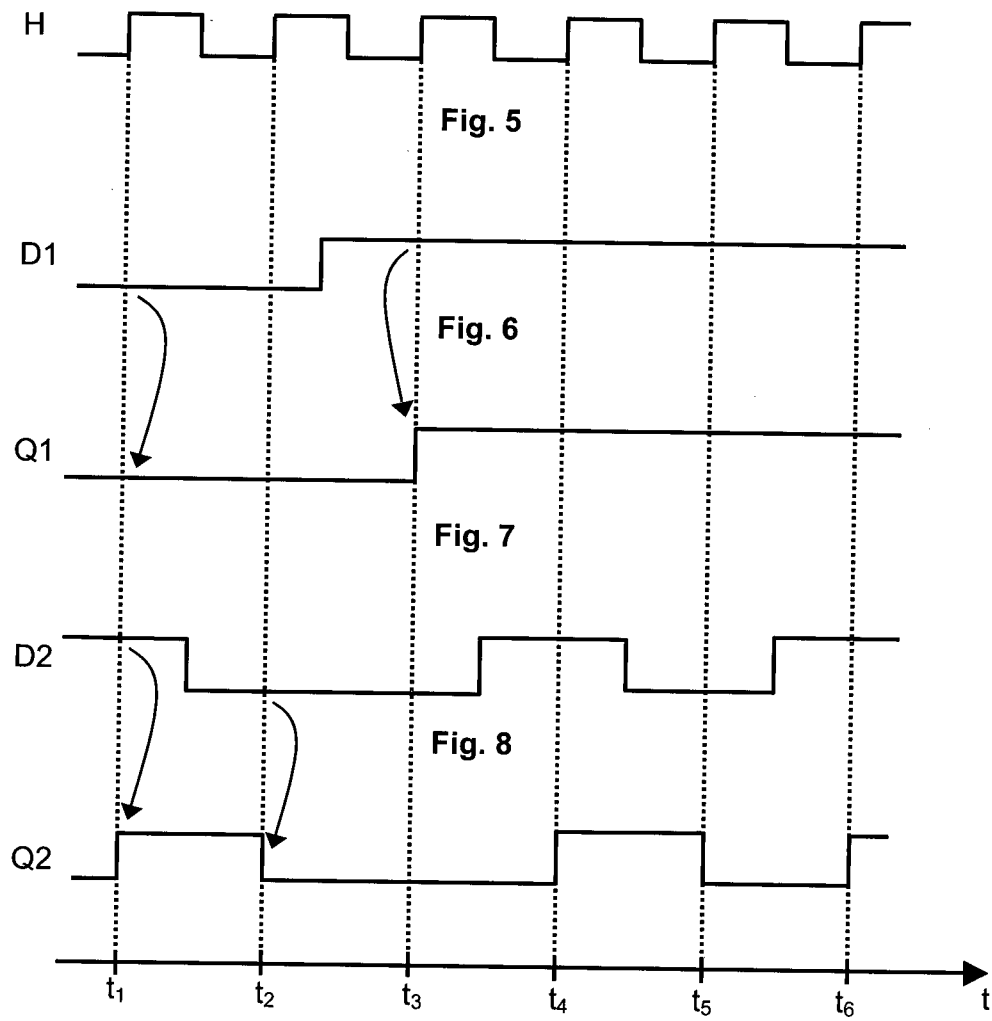


Fig. 9

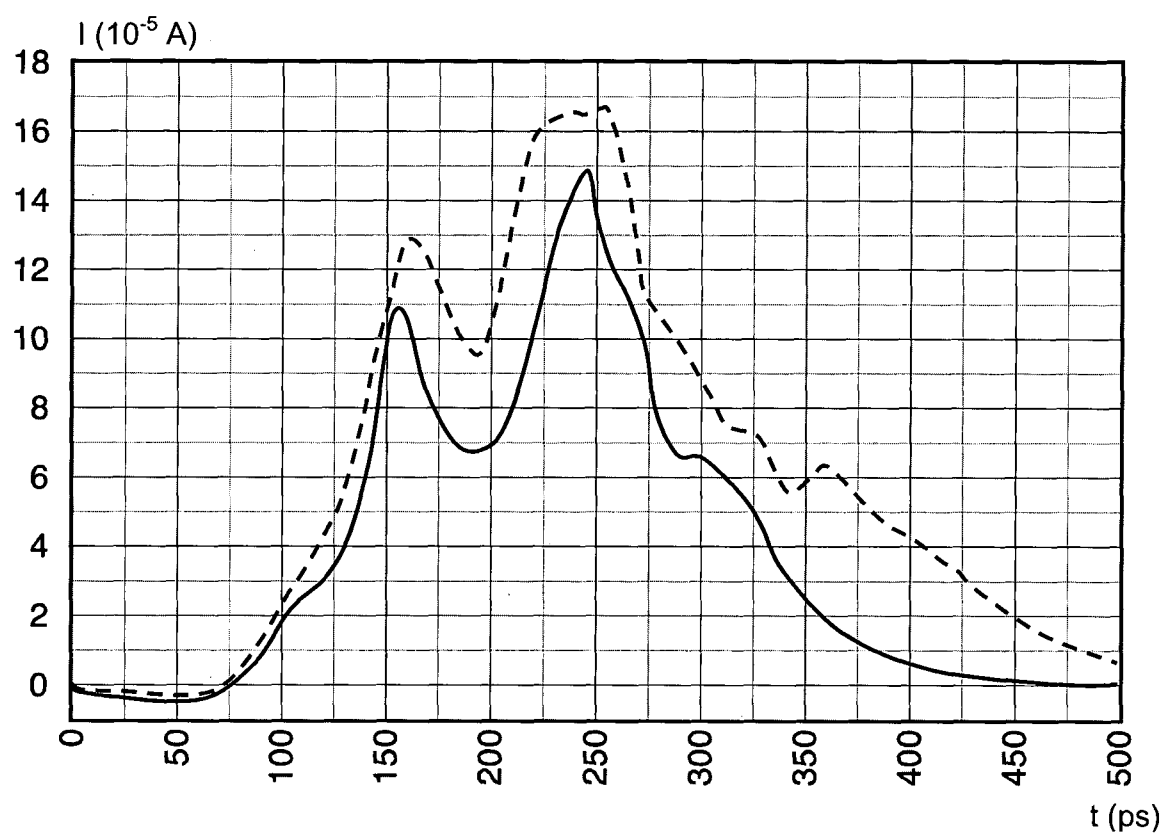


Fig. 10

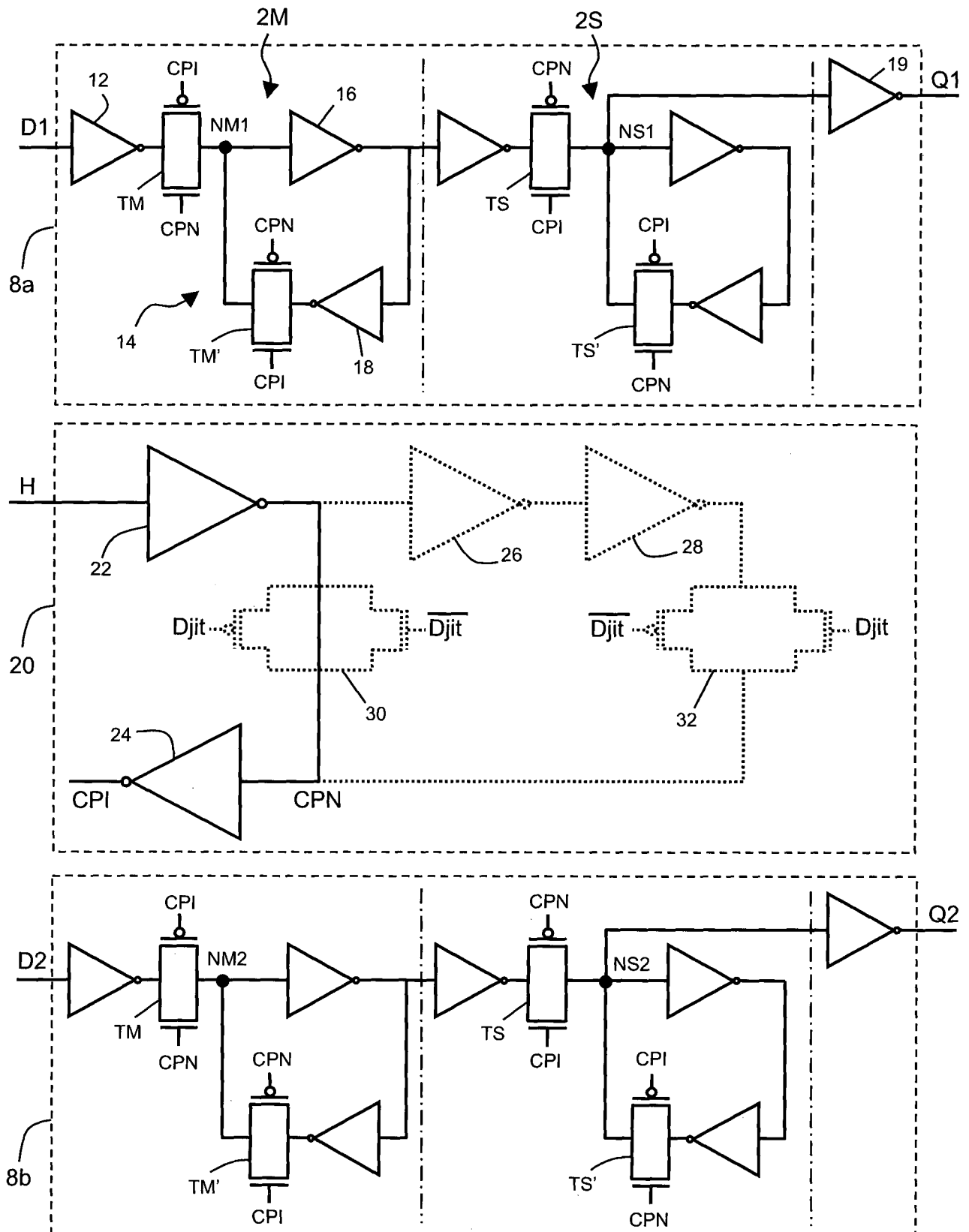


Fig. 11

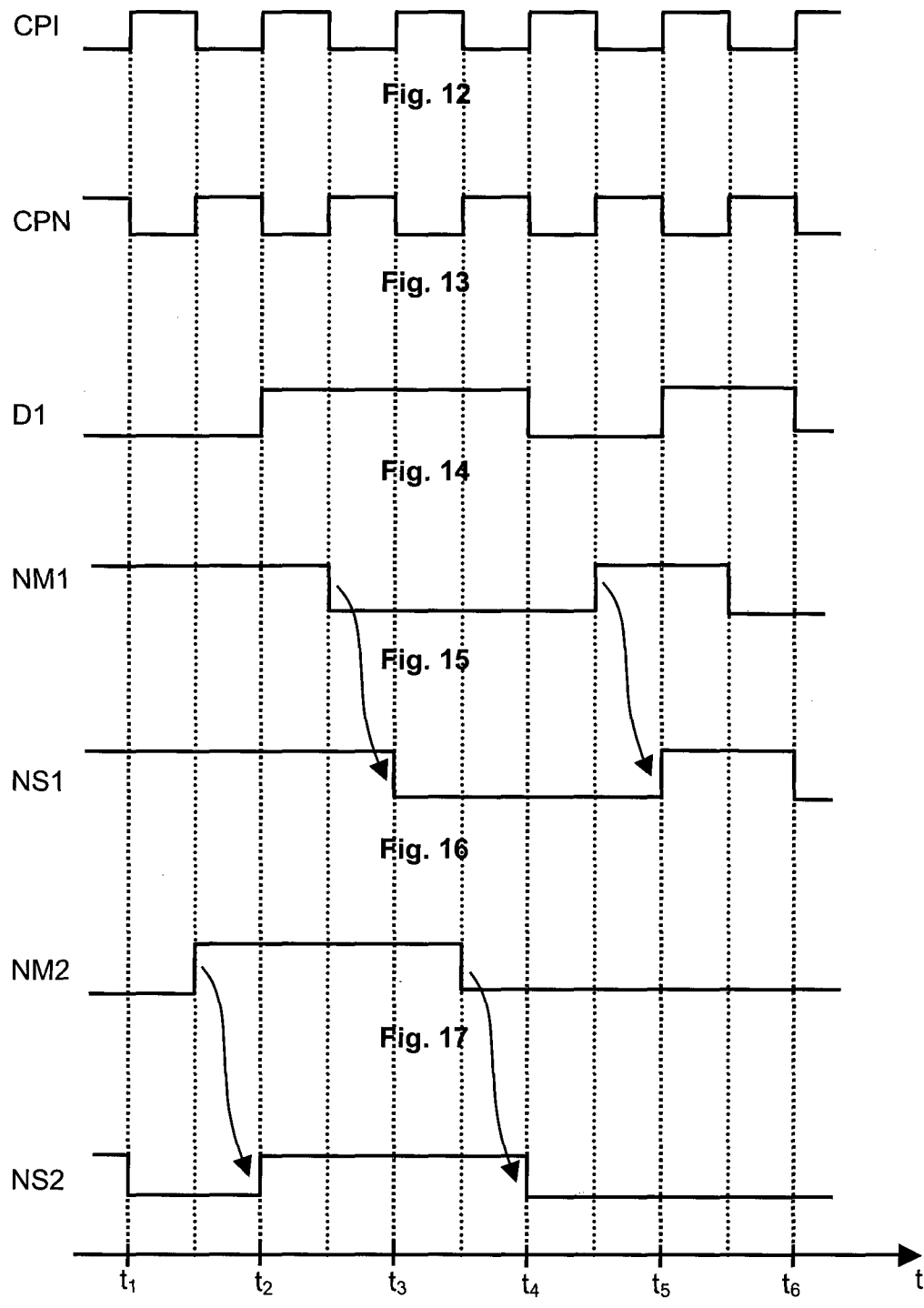


Fig. 18

7/7

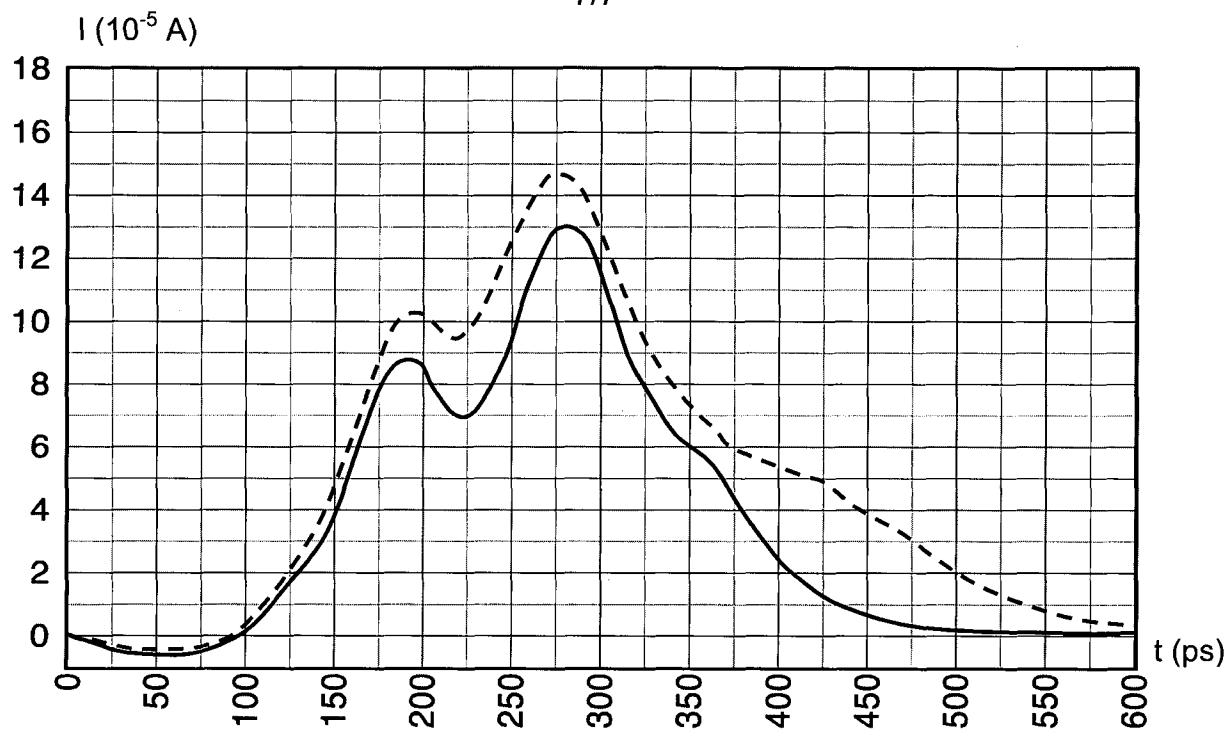


Fig. 19

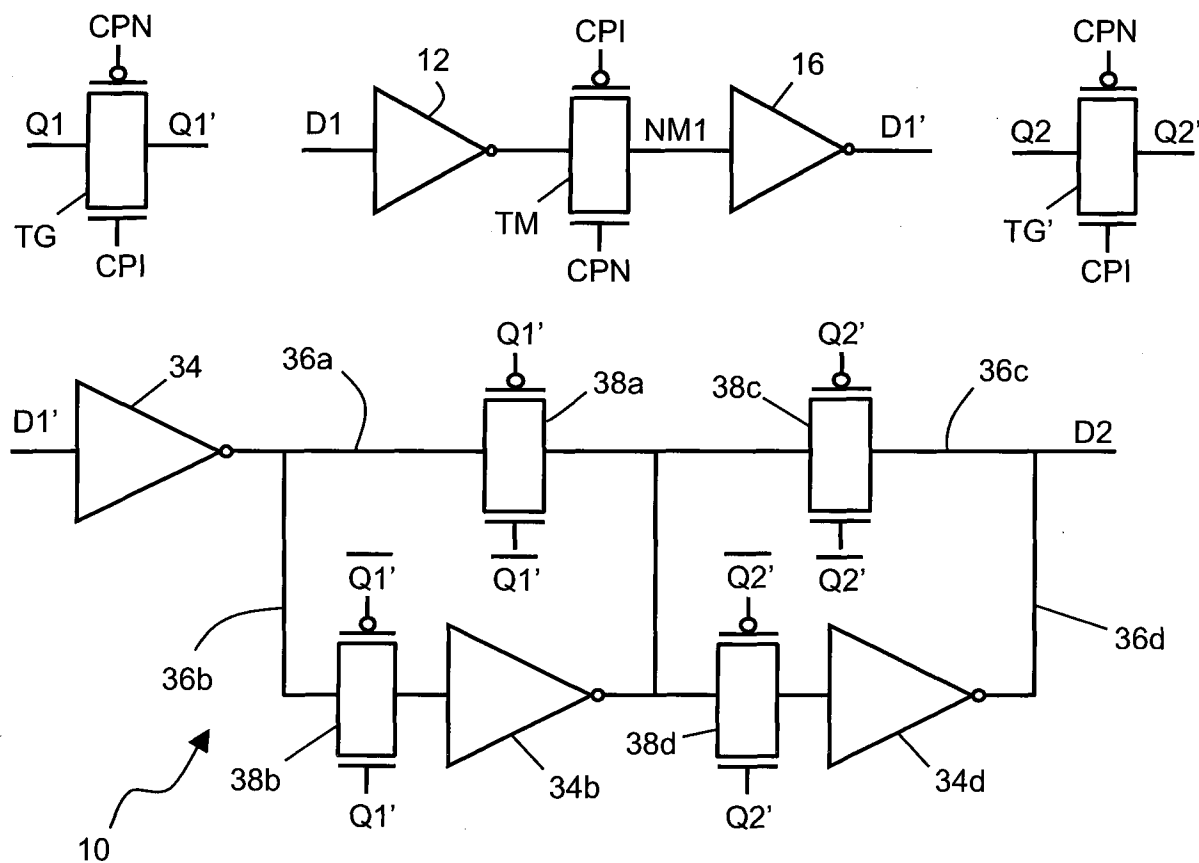


Fig. 20

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2012/000103

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06K19/073 G06F21/00 H03K3/037
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06K G06F H03K

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/26746 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; THUERINGER PETER [NL]; ULLY KLAUS) 11 May 2000 (2000-05-11) page 1, line 11 - page 3, line 14 -----	1-4



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

29 June 2012

Date of mailing of the international search report

10/07/2012

Name and mailing address of the ISA/

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

Authorized officer

Gronau, H

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2012/000103

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0026746	A2	11-05-2000	
		AT 315801 T	15-02-2006
		CN 1292111 A	18-04-2001
		DE 19850721 A1	18-05-2000
		EP 1057096 A2	06-12-2000
		JP 2003526134 A	02-09-2003
		TW 460774 B	21-10-2001
		US 6498404 B1	24-12-2002
		WO 0026746 A2	11-05-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2012/000103

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06K19/073 G06F21/00 H03K3/037
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06K G06F H03K

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 00/26746 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; THUERINGER PETER [NL]; ULLY KLAUS) 11 mai 2000 (2000-05-11) page 1, ligne 11 - page 3, ligne 14 -----	1-4



Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

29 juin 2012

Date d'expédition du présent rapport de recherche internationale

10/07/2012

Nom et adresse postale de l'administration chargée de la recherche internationale

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

Fonctionnaire autorisé

Gronau, H

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2012/000103

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0026746	A2	11-05-2000	
		AT 315801 T	15-02-2006
		CN 1292111 A	18-04-2001
		DE 19850721 A1	18-05-2000
		EP 1057096 A2	06-12-2000
		JP 2003526134 A	02-09-2003
		TW 460774 B	21-10-2001
		US 6498404 B1	24-12-2002
		WO 0026746 A2	11-05-2000
