(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 926 382**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **08 50169**

(51) Int Cl[8] : ***G 06 K 19/073*** *(2006.01), H 04 L 9/32, G 07 F 19/00*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 11.01.08.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 17.07.09 Bulletin 09/29.

(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) :** *PROTON WORLD INTERNATIONAL NV* — BE.

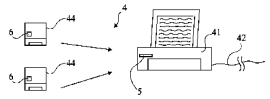
(72) **Inventeur(s) :** MODAVE JEAN LOUIS et HUQUE THIERRY.

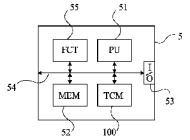
(73) **Titulaire(s) :**

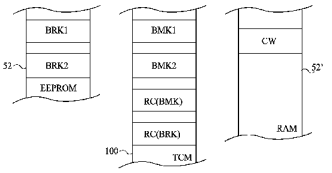
(74) **Mandataire(s) :** CABINET BEAUMONT.

(54) HIERARCHISATION DE CLES CRYPTOGRAPHIQUES DANS UN CIRCUIT ELECTRONIQUE.

(57) L'invention concerne un procédé d'obtention, dans un circuit électronique (5), d'au moins une première clé destinée à être utilisée dans un mécanisme cryptographique, à partir d'au moins une deuxième clé contenue dans le même circuit, ladite première clé étant stockée dans au moins un premier élément de mémorisation (100) du circuit, ledit premier élément de mémorisation étant réinitialisé automatiquement au bout d'une durée indépendante du fait que le circuit soit alimenté ou non. L'invention concerne également des applications de ce procédé à des transmissions chiffrées, des contrôles d'utilisation, ainsi qu'un circuit électronique mettant en oeuvre ces procédés.







FR 2 926 382 - A1

HIÉRARCHISATION DE CLÉS CRYPTOGRAPHIQUES DANS UN CIRCUIT ÉLECTRONIQUE

Domaine de l'invention

La présente invention concerne de façon générale les circuits électroniques et, plus particulièrement les circuits comportant une unité de traitement numérique capable de manipuler des clés de chiffrement ou d'authentification.

La présente invention concerne plus particulièrement la protection de clés de chiffrement ou d'authentification contenues dans un circuit intégré pourvu de moyens de calcul, par exemple d'une carte à puce ou analogue.

Exposé de l'art antérieur

La protection de clés de chiffrement ou d'authentification contenues dans un circuit électronique contre des tentatives de piratage est un problème récurrent en cryptographie. En particulier, on cherche souvent à protéger une ou plusieurs clés, dites natives, initiales ou primaires, stockées dans une mémoire non volatile d'un circuit lors de sa fabrication, plus précisément dans une phase de personnalisation qui termine son processus de production. Le but de cette protection est notamment d'éviter les problèmes liés à un phénomène dit de révocation de clé qui consiste à considérer une clé comme plus suffisamment sûre et à ne plus l'utiliser. Si cette clé est une

clé initiale du circuit, ce dernier doit alors être considéré comme inutilisable. Pour éviter cela, on a souvent recours à un mécanisme de dérivation de clés faisant que seules des clés dérivées de cette clé initiale ou maître soient utilisées. Si une des clés dérivées n'est plus sûre, le circuit peut alors être en mesure d'en générer une nouvelle. Une autre contremesure à des tentatives de piratage consiste à utiliser des clés temporaires transmises par un élément distant de confiance et stockées dans une mémoire vive du circuit (pour une utilisation courte ou dans laquelle le circuit reste alimenté) ou dans une mémoire non volatile reprogrammable (pour une utilisation plus longue ou s'étendant sur plusieurs périodes d'alimentation). Ces clés temporaires peuvent également être dérivées par le circuit à partir d'un identifiant transmis par l'élément distant.

Par exemple, dans une application de télévision à péage, un mot de contrôle, utilisé pour déchiffrer côté récepteur un flux vidéo, est obtenu (dérivé) à partir de clés temporaires contenues dans une carte à puce. Ces clés temporaires dites de diffusion sont obtenues suite à un processus d'échanges sécurisés entre le fournisseur d'accès et le récepteur lors duquel les clés sont soit directement téléchargées, soit elles-mêmes dérivées par la carte à puce du récepteur à partir d'un identifiant transmis par le fournisseur d'accès. Les clés de diffusion sont les mêmes pour plusieurs utilisateurs et ne sont utilisées par l'émetteur que pendant une certaine durée (par exemple, un mois).

Un problème est lié au fait que les clés de diffusion sont largement utilisées en usage normal. Elles sont donc très exposées aux attaques. En effet, les attaques visant à pirater des clés sont le plus souvent basées sur une analyse récurrente appelant les clés un grand nombre de fois.

De plus, la fréquence élevée d'utilisation des clés de diffusion par le récepteur pour obtenir les mots de contrôle (généralement toutes les quelques secondes ou dizaines de secondes) rend inenvisageable un mécanisme requérant un échange avec le

fournisseur d'accès à chaque utilisation de la clé de diffusion. Par conséquent, une même clé peut être utilisée par plusieurs utilisateurs sans que le fournisseur d'accès ne s'en aperçoive. Cela conduit à des attaques dites sans carte, c'est-à-dire à l'utilisation des clés de diffusion par des utilisateurs ne possédant pas la carte à puce dédiée. En outre, les moyens de calcul et de communication actuels de type Internet permettent, en raison de la rapidité de traitement, à plusieurs utilisateurs connectés par réseau, d'utiliser une même clé de diffusion sans nuire à l'affichage des médias sur leurs postes respectifs. Ce type d'attaque est connu sous la dénomination d'attaque par partage de clé (sharing attacks).

Dans un autre exemple d'application à des cartes à puce de paiement, par exemple satisfaisant à la norme dite EMV, des clés de session sont utilisées et dérivées à partir d'une clé de base contenue dans une carte à puce qu'il est souhaitable de protéger contre d'éventuelles tentatives de piratage.

Dans encore un autre exemple d'application à des cartouches d'imprimante, par exemple de type jet d'encre ou laser, il peut être souhaitable de s'assurer que les cartouches utilisées par une imprimante donnée sont bien des cartouches autorisées, c'est-à-dire des cartouches certifiées par le fabricant. Dans une telle application, le piratage de clés d'authentification contenues dans un circuit électronique attaché à la cartouche d'encre ou à l'imprimante permet, par exemple, de réutiliser une même cartouche rechargée un trop grand nombre de fois.

Résumé de l'invention

Il serait souhaitable de disposer d'un mécanisme de protection de clés dans un système de clés hiérarchiques qui pallie les inconvénients des mécanismes usuels.

Un objet vise plus particulièrement une solution compatible avec les traitements usuels de clés de chiffrement ou d'authentification. En particulier, cet objet vise une solution ne requérant aucune modification des algorithmes d'authenti-

fication et de chiffrement proprement dits, ni des éventuels algorithmes de dérivation de clés.

Plus généralement, un objet vise un mécanisme de dérivation de clés autorisant un contrôle de l'utilisation de ces clés dans le temps.

Pour atteindre tout ou partie de ces objets ainsi que d'autres, il est prévu un procédé d'obtention, dans un circuit électronique, d'au moins une première clé destinée à être utilisée dans un mécanisme cryptographique, à partir d'au moins une deuxième clé contenue dans le même circuit, ladite première clé étant stockée dans au moins un premier élément de mémorisation du circuit, ledit premier élément de mémorisation étant réinitialisé automatiquement au bout d'une durée indépendante du fait que le circuit soit alimenté ou non.

Un mode de mise en oeuvre du procédé prévoit que le nombre d'utilisations de la première clé en une période donnée est limité par un compteur stocké dans un deuxième élément de mémorisation réinitialisé automatiquement au bout d'une durée indépendante du fait que le circuit soit alimenté ou non.

Un mode de mise en oeuvre du procédé prévoit que la deuxième clé est contenue dans un élément de mémorisation non volatile du circuit.

Un mode de mise en oeuvre du procédé prévoit que la première clé est obtenue par dérivation de la deuxième clé.

Un mode de mise en oeuvre du procédé prévoit que la deuxième clé sert à obtenir la première clé par déchiffrement.

Un mode de mise en oeuvre du procédé prévoit que la première clé sert de base à la dérivation d'une troisième clé utilisée pour chiffrer ou authentifier des informations provenant de l'extérieur du circuit.

Il est également prévu un procédé de transmission chiffrée de données numériques, dans lequel une clé de déchiffrement de ces données correspond à la troisième clé.

Il est également prévu un procédé de dérivation d'une clé de session d'une application EMV, dans lequel la clé de session correspond à la troisième clé.

Il est également prévu un procédé de contrôle d'utilisation de cartouches d'encre au moyen d'un circuit associé à une imprimante et d'une clé dérivée d'un identifiant fournit par une cartouche, dans lequel ladite clé dérivée correspond à la première clé.

Il est également prévu un circuit électronique comportant des moyens de traitement cryptographique et au moins une mémoire non volatile, ledit premier élément de mémorisation étant formé d'au moins un élément de mémorisation comportant au moins un premier élément capacitif présentant une fuite au travers de son espace diélectrique.

Un mode de réalisation du circuit comporte des moyens adaptés pour mettre en oeuvre l'un des procédés ci-dessus.

Il est également prévu une carte à puce ou une clé électronique, comportant un tel circuit électronique.

Il est également prévu un système de télédiffusion d'un contenu numérique comportant :

un émetteur apte à chiffrer le contenu à partir d'un mot de contrôle changeant périodiquement et transmis, avec le contenu chiffré, de façon chiffré à partir d'au moins une première clé temporaire de période supérieure à celle du mot de contrôle ; et

un récepteur associé à un circuit électronique apte à déchiffrer le mot de contrôle à partir de ladite première clé, puis à déchiffrer le contenu à partir de ce mot de contrôle.

Il est également prévu un récepteur d'un tel système.

Un mode de réalisation d'un récepteur comporte un lecteur de carte à puce.

Il est également prévu un système de contrôle d'utilisation de cartouches d'encre par une imprimante, comportant :

au moins une imprimante associée à au moins un circuit électronique ; et

au moins une cartouche d'encre adaptée à transmettre un identifiant permettant au circuit de l'imprimante de générer ladite première clé.

Il est également prévu une imprimante d'un tel système.

Il est également prévu une cartouche d'un tel système comportant un circuit électronique pourvu d'un élément de mémorisation réinitialisé automatiquement au bout d'une durée indépendante du fait que le circuit soit alimenté ou non, cet élément contenant ledit identifiant.

Il est également prévu un système de transactions bancaires utilisant des cartes à puce, ladite première clé servant à dériver des clés de session des transactions.

Brève description des dessins

Ces objets, caractéristiques et avantages, ainsi que d'autres 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 représente une carte à puce du type à laquelle s'applique à titre d'exemple la présente invention ;

la figure 2 illustre un système de télédiffusion du type auquel s'applique à titre d'exemple la présente invention ;

la figure 3 illustre un système de carte de paiement du type auquel s'applique à titre d'exemple la présente invention ;

la figure 4 illustre un système d'imprimante à cartouche du type auquel s'applique à titre d'exemple la présente invention ;

la figure 5 est un schéma-blocs d'un mode de réalisation d'un circuit électronique ;

la figure 6 illustre un exemple de contenus de mémoires d'un circuit électronique dans l'application de la figure 2 ;

la figure 7 est un organigramme illustrant un mode de mise en oeuvre selon cet exemple d'application ;

la figure 8 est un organigramme simplifié d'un mode de mise en oeuvre d'un mécanisme de ratification ;

la figure 9 est un schéma-blocs simplifié d'un compteur utilisé dans le mécanisme de la figure 8 ;

la figure 10 illustre un exemple de contenus de mémoires d'un circuit électronique dans l'application de la figure 3 ;

la figure 11 illustre un exemple de contenus de mémoires d'un circuit électronique dans l'application de la figure 4 ;

la figure 12 représente un mode de réalisation d'un circuit électronique de rétention de charges ;

la figure 13 est un graphe courant-tension illustrant le fonctionnement du circuit de la figure 12 ;

la figure 14 est un chronogramme illustrant le fonctionnement du circuit de la figure 12 ;

la figure 15 représente un autre mode de réalisation d'un circuit de rétention de charges dans un exemple d'environnement ;

la figure 16 est un graphe courant-tension illustrant le fonctionnement du circuit de la figure 15 ;

les figures 17A, 17B, 17C sont respectivement une vue de dessus, une vue en coupe selon une première direction et le schéma électrique équivalent d'un mode de réalisation d'un circuit électronique de rétention de charges à partir de cellules EEPROM ;

les figures 18A, 18B et 18C sont respectivement une vue de dessus, une vue en coupe selon une deuxième direction et le schéma électrique équivalent d'un premier élément du circuit des figures 17A à 17C ;

les figures 19A, 19B, 19C sont respectivement une vue de dessus, une vue en coupe selon la deuxième direction et le schéma électrique équivalent d'un deuxième élément du circuit des figures 17A à 17C ;

les figures 20A, 20B, 20C sont respectivement une vue de dessus, une vue en coupe selon la deuxième direction et le schéma électrique équivalent d'un troisième élément du circuit des figures 17A à 17C ; et

les figures 21A, 22B, 21C sont respectivement une vue de dessus, une vue en coupe selon la deuxième direction et le schéma électrique équivalent d'un quatrième élément du circuit des figures 17A à 17C.

De mêmes éléments ont été désignés par de mêmes références aux différentes figures qui ont été tracées sans respect d'échelle. Par souci de clarté, seuls les éléments et étapes qui sont utiles à la compréhension de l'invention ont été représentés et seront décrits. En particulier, les ressources utilisées par un circuit électronique exploitant des clés n'ont pas été détaillées, l'invention étant compatible avec toute utilisation habituelle d'une ressource matérielle ou logicielle. De plus, les mécanismes de communication de données entre le circuit électronique et son environnement n'ont pas non plus été détaillés, l'invention étant là encore compatible avec les mécanismes usuels. En outre, les algorithmes de chiffrement ou d'authentification utilisant une ou plusieurs des clés mises en oeuvre n'ont pas été exposés, l'invention étant là encore compatible avec les algorithmes usuels.

Description détaillée

La figure 1 représente, de façon schématique, une carte 1 à puce du type auquel s'applique à titre d'exemple la présente invention. Une telle carte est, par exemple, constituée d'un support 12 en matière plastique dans ou sur lequel est rapportée une puce 5 de circuit électronique, susceptible de communiquer avec l'extérieur au moyen de contacts 13 ou au moyen d'éléments non représentés d'émission-réception sans contact. Le circuit 5 de la carte contient une unité de traitement exploitant une ou plusieurs clés de chiffrement, déchiffrement, authentification, ou plus généralement une ou plusieurs clés exploitées par un mécanisme cryptographique.

La figure 2 est un schéma-bloc d'un exemple d'application à un système de télédiffusion à accès contrôlé. Cet exemple concerne la diffusion par satellite de média numérique. Côté diffuseur 21, un contenu numérique MEDIA (le cas échéant provenant d'un codage numérique d'un contenu analogique) est chiffré au moyen d'un mot de contrôle CW, préalablement à sa radiodiffusion. Après transmission, par exemple par l'intermédiaire d'un satellite 22, d'un réseau câblé, de l'Internet, etc., un décodeur 23 convertit, côté réception, les signaux pour les rendre interprétables (par exemple, en les convertissant en signaux vidéo), et déchiffre les données à partir du même mot de contrôle CW (chiffrement symétrique) ou d'un mot de contrôle lié à celui d'émission par un mécanisme asymétrique (clé publique - clé privée). Côté récepteur 23, le mot de contrôle est obtenu à partir d'une clé temporaire contenue, par exemple, dans le circuit 5 d'une carte à puce 1 dédiée à chaque utilisateur. La clé temporaire est changée périodiquement (par exemple, tous les mois). Elle est soit transmise à la carte par le fournisseur d'accès par un mécanisme sécurisé, soit dérivée par la carte à partir d'un identifiant diffusé par l'émetteur et d'une clé de base contenu dans la carte depuis sa fabrication. Le décodeur 23 et le circuit 5 de déchiffrement, souvent appelé module d'accès conditionnel ou CAM pour "Conditionnal Acces Module" sont généralement distincts. Ce module peut également être porté par une carte électronique du décodeur.

La figure 3 est un schéma-blocs d'un autre exemple d'application à un système 3 de cartes de paiement. Cet exemple concerne l'utilisation d'une carte à puce 1 (CARD) pour des opérations de paiement, par exemple, respectant la norme EMV. La carte 1 est introduite dans un lecteur 31 (READER) du système 3 et a pour rôle de permettre une authentification du porteur de la carte pour autoriser une transaction bancaire. Cette transaction est effectuée par l'intermédiaire d'un système central 32 (ISSUER), généralement la banque du titulaire du lecteur 31. Cet établissement bancaire communique alors avec celui (non

représenté) du porteur de la carte pour effectuer la transaction.

La figure 4 est un schéma-blocs d'encore un autre exemple d'application à un système 4 d'imprimante à cartouches. Une imprimante 41, destinée à être reliée (liaison 42) avec ou sans fil à un système informatique (non représenté), contient une ou plusieurs cartouches d'encre 44. Chaque cartouche est pourvue d'un circuit électronique 6 susceptible au moins de communiquer un identifiant numérique à un circuit électronique 5 dont est équipée l'imprimante 41. L'identifiant permet au circuit 5, entre autres, d'authentifier la cartouche 44.

La figure 5 est un schéma-blocs d'un mode de réalisation d'un circuit électronique 5, par exemple contenu dans une carte à puce 1 des figures 1, 2, 3, dans une imprimante de la figure 4 ou dans un autre module de contrôle d'accès (de type clé électronique ou autre). Le circuit 5 comporte, entres autres, une unité de traitement numérique 51 (PU), une ou plusieurs mémoires 52 (MEM) parmi lesquelles au moins une mémoire non volatile (par exemple, de type EEPROM) et une mémoire vive (RAM), et un circuit 53 d'entrée/sortie (I/O) pour communiquer avec l'extérieur du circuit 5 (pour connexion aux contacts 13 ou à une antenne par exemple). Les différents éléments internes au circuit 5 communiquent entre eux et avec l'interface 53 par ou plusieurs bus 54 de données, d'adresses et de commandes ainsi que par d'éventuelles liaisons directes entre certains de ces éléments. Le circuit 5 peut également intégrer d'autres fonctions logicielles ou matérielles, symbolisées par un bloc 55 (FCT) en figure 5.

Dans les différentes applications visées, le circuit 5 comporte également au moins un circuit 100 (TCM) d'éléments de mémorisation temporaire à rétention de charges dont le niveau de charge évolue avec le temps, même lorsque le circuit 5 n'est pas alimenté. Ce circuit 100 constitue un ou plusieurs éléments de mémorisation contrôlés dans le temps (Time Controled Memory).

Des exemples détaillés de circuits 100 seront décrits ultérieurement en relation avec les figures 12 et suivantes. Pour l'instant, on se contente de noter que chaque cellule mémoire d'un circuit 100 est susceptible d'être programmée ou activée (placée dans un état noté arbitrairement 1) par injection ou extraction de charges dans un élément capacitif qui présente une fuite au travers de son espace diélectrique, de telle sorte que son état actif disparaît (l'élément rebascule vers l'état 0) au bout d'un temps donné, indépendamment de l'alimentation éventuelle du circuit.

Un tel circuit 100 de rétention de charges stocke un état binaire ou plusieurs états formant un mot binaire constituant une clé temporaire.

Les figures 6 et 7 illustrent un exemple d'application à un système de télédiffusion du type de celui de la figure 2. La figure 6 illustre le contenu de zones de trois mémoires distinctes du circuit 5 parmi lesquelles une mémoire non volatile reprogrammable 52 de type EEPROM, une mémoire vive 52' de type RAM et une mémoire 100 contrôlée dans le temps (TCM).

Un mot de contrôle CW est utilisé par l'émetteur (21, figure 2) pour chiffrer le contenu média et doit être connu du récepteur (23, figure 2), plus particulièrement, du circuit 5 qui lui est associé (que ce soit dans une carte à puce 1, dans un circuit embarqué ou dans un module de contrôle d'accès). Le mot CW est stocké en mémoire vive dans le circuit 5 car il change à une fréquence relativement élevée, typiquement moins d'une minute.

Le fournisseur du service (pour simplifier, supposé confondu avec l'émetteur 21) et, dans cet exemple, la carte 1 partagent une clé de diffusion BMK (Broadcast Monthly Key) qui est une clé temporaire de durée (par exemple d'un mois) supérieure à celle du mot CW et qui est utilisée par le circuit 5 pour déchiffrer les mots de contrôle CW transmis par l'émetteur en étant chiffrés par la clé BMK. Sans cette clé BMK, le décodeur n'est pas en mesure de déchiffrer les mots successifs

pendant sa période de validité, donc de décoder le contenu transmis. La clé BMK est généralement une clé commune à plusieurs circuits 5 de différents utilisateurs.

La transmission de la clé temporaire BMK aux différents utilisateurs est précédée d'un contrôle de leurs droits (par exemple, des droits d'abonnement). Pour cela, le circuit 5 contient au moins une clé de base BRK (Broadcast Root Key) en mémoire non volatile EEPROM. Dans l'exemple, on prévoit deux clés de base BRK1 et BRK2 soit pour permettre la répudiation d'une des deux si nécessaire, soit pour dédier chaque clé à une application (une catégorie de contenus numériques). Le nombre de clés de base peut varier selon l'application et selon la taille de la mémoire EEPROM disponible. Cette ou ces clés BRK sont, de préférence, stockées dans la carte dans sa phase de personnalisation. En variante, ces clés de base peuvent être stockées dans une mémoire non volatile programmable une seule fois (OTP) en étant, de préférence, individualisées par circuit. Les clés BRK sont utilisées par le diffuseur pour envoyer à la carte les clés temporaires BMK (BMK1 et BMK2) qui sont stockées dans la mémoire 100. Ces clés temporaires BMK sont de préférence stockées dans des endroits dédiés de la mémoire 100. Le temps de rétention de charges de la mémoire 100 définit leur durée de vie maximale. En choisissant une durée au moins égale à la période de durée de validité maximale prévue, on garantit qu'une clé mensuelle ne puisse pas être utilisée ou attaquée pendant une période supérieure à cette durée de rétention dans la mesure où elle aura disparu de la mémoire 100 à l'issue de cette période. Cela empêche que des programmes enregistrés soient rejoués (exécutés) a posteriori.

Dans l'exemple ci-dessus, on suppose que la résistance du circuit 5 à des attaques est telle que la probabilité pour un pirate de retrouver une clé BMK en un mois est négligeable. Cet exemple peut être adapté à d'autres durées de clés BMK. Par exemple, on pourra utiliser des clés hebdomadaires.

La figure 7 illustre une mise en oeuvre de l'exemple de la figure 6.

Le diffuseur 21 possède les quantités BRK, BMK et CW. Initialement, le circuit 5 ne possède que la clé BRK (ou les clés BRK). Tous les mois, le fournisseur d'accès 21 change la clé BMK et la transmet de façon chiffrée (bloc 71, $E_{BRK}(BMK)$) au décodeur 23, plus précisément à son module ou circuit 5. Le circuit 5 déchiffre la clé BMK (bloc 72, $D_{BRK}(E_{BRK}(BMK))$) puis la stocke dans la mémoire 100 (bloc, 73, BMK -> TCM).

Par la suite, lors de la diffusion, l'émetteur 21 brouille ou chiffre (bloc 75, $E_{BMK}(CW)$, $E_{CW}(MEDIA)$) chaque mot de contrôle avec la clé BMK et les données MEDIA avec le mot de contrôle CW avant de transmettre les deux au décodeur. Le circuit 5 côté décodeur, déchiffre le mot de contrôle CW en utilisant la clé BMK (bloc 76, $D_{BMK}(E_{BMK}(CW))$), puis les données au moyen de ce mot de contrôle (bloc 77, $D_{CW}(E_{CW}(MEDIA))$). Les algorithmes de chiffrement et de déchiffrement E et D peuvent être différents pour la clé BMK, le mot de contrôle CW et les données MEDIA. De même, on a illustré un cas d'algorithme symétrique où la même clé est partagée et utilisée pour chiffrer et déchiffrer, mais on pourra utiliser des algorithmes asymétriques à clés publiques et privées au moins pour les chiffrements des clés BMK et CW.

De préférence, un ou plusieurs mécanismes de ratification sont ajoutés pour limiter le nombre d'utilisations possibles de la clé temporaire BMK et/ou de la clé de base BRK dans une période de temps donnée. Ces ratifications sont effectuées au moyen de compteurs RC (Ratification Counter) qui permettent de décompter le nombre de fois que sont utilisées les clés BRK et BMK pendant une période donnée. En stockant les compteurs RC(BMK) et RC(BRK) dans des éléments de mémorisation à contrôle temporel du circuit 100, le contrôle de la période est effectué de façon automatique par le circuit de rétention de charges 100 dans la mesure où les états des compteurs disparaissent à l'issue de la période pour laquelle le circuit 100 est conçu.

La figure 8 est un schéma-blocs fonctionnel simplifié, un mode de mise en oeuvre du mécanisme de ratification par compteur, par exemple, de la clé BRK.

A chaque appel de la clé BRK (bloc 81, CALL BRK), on commence par vérifier (bloc 82, RC(BRK) < TH ?) l'état d'un compteur RC(BRK) par rapport à un seuil TH. Ce seuil est choisi en fonction d'un nombre raisonnable d'utilisations en conditions normales.

Si le seuil TH n'est pas atteint par le compteur (sortie Y du bloc 82), le compteur est incrémenté (bloc 83, RC(BRK) =RC(BRK) + 1), puis l'utilisation de la clé est autorisée (bloc 85, ACCESS BRK).

Si le nombre d'utilisations excède le seuil (sortie N du bloc 82), l'accès à la clé est refusé. Par exemple, le mécanisme passe directement au traitement postérieur (le mot CW n'est alors pas déchiffré et est inutilisable) ou met en oeuvre un traitement d'erreur (bloc 84 en pointillés, ERR/STOP), voire un blocage temporaire ou définitif du circuit.

Grâce à l'utilisation d'un circuit de rétention de charges dont l'état activé disparaît au bout d'un temps donné, le compteur RC(BRK) se réinitialise automatiquement et indépendamment de l'alimentation du circuit électronique 10'. Par conséquent, il est désormais possible de limiter le nombre d'utilisations sur une période donnée. Cette utilisation du compteur RC(BRK) permet de rendre plus compliqué des attaques, par exemple par analyse de la consommation du circuit (DPA - Differential Power Analysis) sur la clé BRK.

Bien entendu, au lieu d'incrémenter le compteur RC(BRK), il est possible d'initialiser le compteur au nombre limite TH, de le décrémenter et de détecter lorsqu'il s'annule.

Le compteur RC(BMK) est par exemple incrémenté à chaque utilisation de la clé BMK pour décoder un mot de contrôle CW. Le compteur RC(BMK) permet de limiter le nombre d'usages de la clé BMK dans la durée fixée. Cette durée est courte par rapport à celle de rétention du compteur RC(BRK). Par exemple,

en limitant le nombre d'utilisations du mot de contrôle, à deux toutes les dix secondes, on empêche les attaques par partage de carte pour des mots CW changeant toutes les dix secondes, tout en permettant un deuxième décodage en cas de besoin (par exemple pour une redondance en cas d'erreur).

La figure 9 représente, de façon très schématique et sous forme de blocs, un exemple de circuit 90 de comptage contenant n circuits électroniques de rétention de charges 100_0, 100_1, ..., 100_n stockant chacun un bit B_0, B_1, ..., B_n du compteur RC(BMK) ou RC(BRK). Le circuit 50 est de préférence commandé par un circuit interne 91 (CTRL) provoquant, comme il sera mieux compris par la suite en relation avec les figures 12 et suivantes, l'incrémentation du compteur suite à une détection de dysfonctionnement (entrée INC du bloc 90), ainsi que la lecture de l'état d'un ou plusieurs bits du compteur.

Dans l'exemple illustré par la figure 9, on suppose que le bit B_n de rang le plus élevé définit le seuil TH. En effet, un changement d'état de ce bit représente un débordement par rapport au compte $2^{n-1} - 1$. La lecture de ce seul bit suffit alors pour fournir un signal OK/NOK indicateur du résultat du test 82 (figure 8).

Un avantage d'une telle comparaison par débordement est qu'il rend une même réalisation matérielle du circuit 90 versatile. En effet, le seuil TH peut alors être aisément adapté quel que soit le nombre de bits structurels du compteur 90 en sélectionnant celui des bits du compteur à prendre en compte pour fournir le résultat OK/NOK du test 82.

Pour le compteur RC(BMK), le mécanisme ci-dessus fonctionne de préférence en mode décomptage à partir d'une valeur initialisée à la valeur 2 à chaque nouvelle réception d'un mot CW (par exemple, toutes les dix secondes) et décrémentée à chaque utilisation du mot CW. Une nouvelle utilisation est alors interdite si le compteur est à zéro. L'intérêt d'un compteur stocké dans la mémoire 100 plutôt qu'en mémoire vive est que sa valeur disparaît de toute façon au bout de la durée

fixée par le circuit 100 (par exemple, la même que la fréquence de changement du mot CW), interdisant une poursuite d'utilisation frauduleuse.

On notera que l'émetteur du système de diffusion n'a pas besoin d'être modifié. Si les circuits de déchiffrements sont embarqués dans le récepteur, seul ce dernier a besoin d'être adapté. Si le récepteur utilise une carte à puce comme circuit de déchiffrement, il n'a pas non plus besoin d'être modifié.

La figure 10 illustre un autre exemple d'utilisation du circuit 5 dans une application à un système de carte de paiement. Cette figure représente un exemple de contenu des trois mémoires 52, 52' et 100 du circuit 5 d'une carte à puce 1 selon cet exemple d'application.

Dans un système bancaire de type EMV, il n'est pas possible de transférer des clés hebdomadaires ou mensuelles dans la carte, ne serait-ce qu'en raison des difficultés de contrôle de l'intervalle de temps entre deux transactions pouvant être effectuées en ligne (on line), c'est-à-dire avec une liaison entre la carte et l'établissement bancaire de contrôle, un grand nombre de transactions s'effectuant hors ligne (off line), c'est-à-dire sans communication avec l'établissement de contrôle. On peut néanmoins dériver des clés temporaires à partir de clés contenues dans la mémoire 52 et remplacer ainsi les mécanismes usuels de dérivation de clés dans une carte à puce.

Dans l'exemple illustré, une clé native RK (Root Key) est stockée dans la carte à puce lors de la personnalisation de sa mémoire EEPROM. Cette clé RK est associée à un compteur du nombre de ses dérivations RKDC (Root Key Derivation Counter) ainsi qu'à un compteur de transactions ATC (Authorization Transaction Counter) également stocké en mémoire non volatile reprogrammable 52.

Avec une périodicité définie à l'avance (par exemple, toutes les semaines), la clé RK est dérivée par le circuit 5 pour obtenir une clé de base BK (Base Key) qui est stockée dans

la mémoire à rétention de charges contrôlée 100. Cette clé de base BK est ensuite dérivée à chaque transaction en utilisant le compteur de transaction ATC pour obtenir une clé de session SK stockée en mémoire vive et qui est utilisée pour les échanges d'autorisation de la transaction entre le lecteur et la carte. Le compteur de transactions constitue l'identifiant de l'indice de la clé de session dans l'arbre de dérivation de clé, permettant au système central avec lequel la carte communique de retrouver la même clé de session.

La durée de vie d'une carte étant fixée (généralement de quelques années, par exemple 4) le compteur RKDC de dérivation de la clé RK fixé dans la mémoire EEPROM peut être codé sur un seul octet pour une dérivation par semaine. Sa valeur est par exemple envoyée au fournisseur de la carte en plus du numéro de la transaction à chaque message d'autorisation pour valiser une dérivation d'une clé de session.

De préférence, le nombre d'utilisations possibles d'une clé de base par intervalle de temps (par exemple par heure) est limité au moyen d'un compteur de ratification RC(BK) stocké dans la mémoire 100. Par exemple, on peut limiter à 20 le nombre d'utilisations possibles, par conséquent, le nombre possible de transactions par heure. Comme dans l'exemple d'application précédent, la réinitialisation du compteur est automatique.

Selon une autre variante, un compteur similaire RC(RK) est utilisé pour les dérivations de la clé RK. Cela apporte une sécurité supplémentaire par rapport au compteur RKDC en limitant le nombre de dérivations dans un temps donné.

Dans les systèmes de transaction ci-dessus, seuls la carte à puce et le module de cryptographie du système d'autorisation ont besoin d'être adaptés, les lecteurs et autres serveurs du système peuvent demeurer inchangés.

La figure 11 illustre un exemple d'application associé au système d'imprimante de la figure 4. Dans cet exemple, une clé de base contenue dans l'imprimante 42 est dérivée un nombre

de fois donné pour communiquer avec une cartouche insérée dans l'imprimante et qui possède une clé depuis sa fabrication. Deux facteurs peuvent conduire à un besoin de changer de clé. Un premier facteur est un trop grand nombre d'utilisations de la clé par un nombre d'utilisations trop grandes de la cartouche (nombre de recharges trop importantes). Un deuxième cas est lié à la date de péremption de l'encre, la cartouche étant périmée.

Côté imprimante, le circuit intégré 5 comporte une zone de mémoire à rétention de charges temporelle 100 permettant de limiter le nombre d'utilisations de la clé, c'est-à-dire le nombre d'introductions de la cartouche dans l'imprimante.

On crée ainsi une clé de session temporaire au moyen d'un algorithme de dérivation de clés usuelles (par exemple, de type AES) à partir d'une clé de base BK contenue dans la carte de l'imprimante. L'indice ID de la clé dérivée dans un arbre de dérivation de clé dépend d'un identifiant de la cartouche (bloc 61, ID) communiqué par celle-ci lors de son introduction dans l'imprimante et permettant, en cas de conformité entre la cartouche et l'imprimante, de retrouver la bonne clé de session. La clé dérivée côté imprimante (bloc 45, DERIVE BK(ID)) est stockée dans une zone de mémoire 100 du circuit 5.

Le démarrage de l'imprimante est conditionné par l'utilisation et l'obtention des clés de session correcte, ce qui permet d'authentifier la cartouche (AUTHENTICATE) et de réserver l'utilisation de l'imprimante à l'emploi de cartouches d'origine ou, au moins autorisées par le fabricant. Le test d'authentification est effectué, par exemple, à chaque utilisation de l'imprimante.

Le fait de stocker la clé temporaire BK(ID) dans la mémoire 100 permet de rendre sa durée de validité indépendante de l'alimentation de l'imprimante. Cela est particulièrement intéressant dans la mesure où une imprimante n'est que rarement allumée en permanence.

Dans l'exemple ci-dessus, les cartouches n'ont pas besoin d'être modifiées, seuls les circuits électroniques des

imprimantes sont adaptés pour contenir les éléments de mémorisation 100.

De préférence, une durée d'utilisation de la cartouche 44 est fixée également au moyen d'une mémoire à rétention de charges temporelle 100 contenue dans le circuit 6 de la cartouche. Un ou plusieurs bits sont activés dans la puce de la cartouche lors de sa fabrication et/ou lors de son rechargement par un intervenant autorisé et cet état actif disparaît automatiquement lorsque la durée est expirée. Un avantage induit est qu'une réinitialisation de la durée d'utilisation de la cartouche ne peut être effectuée qu'avec un outil capable de reprogrammer la zone dédiée de la mémoire 100, par conséquent, a priori un élément autorisé. Une fois la durée prévue expirée, l'identifiant contenue dans la cartouche disparaît et celle-ci ne sera pas reconnue par l'imprimante.

La figure 12 représente un exemple préféré d'un circuit de rétention de charges 100. Un tel circuit constitue un élément de stockage d'un bit d'une clé ou d'un compteur décrit précédemment.

Le circuit 100 comporte un premier élément capacitif C1 dont une première électrode 121 est connectée à un noeud flottant F et dont l'espace diélectrique 123 est conçu (par sa permittivité et/ou par son épaisseur) pour présenter des fuites non négligeables dans le temps. Par noeud flottant F, on entend un noeud non directement connecté à une quelconque région diffusée du substrat semiconducteur dans lequel est réalisé préférentiellement le circuit 100 (et le circuit 10') et, plus particulièrement, séparé par un espace diélectrique de toute borne d'application de potentiel. La deuxième électrode 122 de l'élément capacitif C1 est, soit reliée (pointillés en figure 12) à une borne 112 destinée à être reliée à un potentiel de référence (par exemple la masse), soit laissée en l'air.

Un deuxième élément capacitif C2 a une première électrode 131 connectée au noeud F et une deuxième électrode 132 connectée à la borne 112. L'élément capacitif C2 présente une

capacité de rétention de charges supérieure à celle de l'élément capacitif C1.

De préférence, un troisième élément capacitif C3 a une première électrode 141 connectée au noeud F et une deuxième électrode 142 reliée à une borne 113 du circuit 100, destinée à être connectée à une source d'alimentation lors d'une initialisation d'une phase de rétention de charges (activation du bit stocké à l'état 1).

Un rôle de l'élément capacitif C2 est de stocker une charge électrique. Un rôle de l'élément de l'élément capacitif C1 est de décharger relativement lentement l'élément de stockage C2 (par rapport à une connexion directe de son électrode 131 à la masse) grâce à une fuite à travers son espace diélectrique. La présence de l'élément capacitif C2 permet de dissocier le niveau de charge présent dans le circuit 100 par rapport à l'élément de décharge (capacité C1). L'épaisseur du diélectrique de l'élément C2 est supérieure à celle de l'élément C1. La capacité de l'élément C2 est supérieure, de préférence dans un rapport d'au moins 10, à celle de l'élément C2.

Un rôle de l'élément capacitif C3 est de permettre une injection de charges dans l'élément capacitif C2 par effet Fowler-Nordheim ou par un phénomène d'injection d'électrons chauds. L'élément C3 permet d'éviter les contraintes (stress) sur l'élément C1 lors de la charge des éléments C2 et C1 en parallèle. L'épaisseur de l'espace diélectrique de l'élément C3 est supérieure à celle de l'élément C1, de façon à éviter d'introduire un chemin de fuite parasite.

Le noeud F est relié à une grille G d'un transistor à borne de commande isolée (par exemple, un transistor MOS 150) dont les bornes de conduction (drain D et source S) sont connectées à des bornes de sortie 114 et 115 pour mesurer la charge résiduelle contenue dans l'élément C2 (en négligeant la capacité de l'élément C1 en parallèle). Par exemple, la borne 115 est reliée à la masse et la borne 114 est reliée à une

source de courant (non représentée) permettant une conversion courant-tension du courant de drain I_{114} dans le transistor 150.

L'épaisseur du diélectrique de grille du transistor 150 est supérieure à celle du diélectrique de l'élément C1 de façon à éviter d'introduire une fuite supplémentaire sur le noeud F. De préférence, l'épaisseur de grille du transistor 150 est même supérieure à l'épaisseur du diélectrique de l'élément C3, de façon à éviter d'introduire un chemin parasite de programmation (d'injection ou d'extraction de charges du noeud F).

L'interprétation du niveau stocké peut être effectuée de façon simple au moyen d'un comparateur dont le basculement s'opère tant que la charge du noeud F reste suffisante. Le niveau pour lequel le comparateur bascule définit alors le niveau de changement d'état du bit stocké par l'élément 100. D'autres solutions de lecture peuvent être envisagées, par exemple, une interprétation multiniveaux dans une réalisation où le circuit 100 stocke directement plusieurs bits.

La figure 13 représente un exemple d'allure du courant I_{114} de drain du transistor 150 en fonction de la tension V_F au noeud F, référencée par rapport à la borne 115. La tension V_F exprime alors la tension grille/source du transistor 150. Elle dépend de la charge résiduelle aux bornes des capacités C1 et C2 en parallèle, donc essentiellement de la charge résiduelle dans la capacité C2. L'évaluation du courant de drain I_{114} peut être effectuée en maintenant les bornes 112 et 115 au même potentiel (par exemple la masse) et en appliquant une tension connue sur la borne 114.

La figure 14 illustre l'évolution de la charge Q_F au point F en fonction du temps. A un instant t0 où une tension d'alimentation (de programmation) cesse d'être appliquée sur la borne 113, la charge Q_F part d'une valeur initiale Q_{INIT} pour s'annuler à un instant t1 avec une allure de décharge capacitive. L'intervalle de temps entre les instants t0 et t1 dépend non seulement de la capacité de fuite du diélectrique de

l'élément C1 mais également de la valeur (donc de la capacité de stockage) de l'élément C2 qui conditionne la valeur Q_{INIT}.

En supposant que les bornes 112 et 115 et la deuxième électrode 122 de l'élément capacitif C1 sont à des potentiels de référence et que la borne 114 est polarisée à un niveau déterminé pour qu'une variation du courant I_{114} ne provienne que d'une variation du potentiel du noeud F, cette variation ne dépend alors que du temps écoulé depuis l'instant t0. Ce résultat est, dans le mode de réalisation représenté, obtenu grâce à la dissociation opérée entre l'élément de fuite temporel (C1) et l'élément représentatif de la charge résiduelle (C2).

La programmation ou activation du circuit 100 (passage à l'état 1 du bit stocké) à travers l'élément capacitif C3 protège l'élément capacitif C1 dont l'épaisseur d'oxyde (diélectrique) est relativement mince et qui risquerait autrement d'être détériorée lors de la programmation. Cela permet notamment de rendre les mesures fiables et reproductibles dans le temps.

Le cas échéant, plusieurs éléments capacitifs C3 sont connectés en parallèle entre la borne 113 et le noeud F de façon à accélérer le temps de programmation.

De même, la durée de rétention peut être adaptée non seulement en réglant les épaisseurs et/ou les permittivités des diélectriques des éléments C1 et C2 mais également en prévoyant plusieurs éléments C1 et/ou C2 en parallèle.

La figure 15 représente le schéma électrique d'un autre mode de réalisation d'un circuit de rétention de charges 100'.

Par rapport au mode de réalisation de la figure 12, le transistor 150 est remplacé par un transistor 160 à grille flottante FG reliée au noeud F. La grille de commande CG du transistor 160 est reliée à une borne 116 de commande en lecture de la charge résiduelle dans le circuit 100' (donc de l'état du bit stocké). L'épaisseur du diélectrique, entre la grille flottante FG et le canal (zone active) du transistor 160, est

supérieure à celle de l'élément C1 et préférentiellement supérieure à celle de l'élément C3.

Une autre différence est que l'élément C3 d'injection ou d'extraction de charges est un transistor MOS 170 à grille flottante. La grille flottante 141 du transistor 170 est reliée au noeud F.

Dans l'exemple de la figure 15, le circuit a été représenté dans une partie de son environnement. Le drain 142 du transistor 170 est relié à une source de courant 118 recevant une tension d'alimentation Valim et sa source 173 est connectée à la masse. Sa grille de commande 174 reçoit un signal de commande CTRL destinée à rendre le transistor 170 passant lors d'un besoin d'injection de charges. Le drain (borne 114) du transistor 160 reçoit la tension d'alimentation Valim et sa source est reliée à la masse par une source de courant 119 (variante inversée par rapport au mode de réalisation décrit en relation avec la figure 12). La tension V_{119} aux bornes de la source de courant 119 est représentative de la tension au point F et est utilisée pour faire basculer la sortie d'un comparateur (non représenté).

La figure 16 illustre, par un graphe du courant I_{114} en fonction de la tension V_{116} appliquée sur la grille de commande, le fonctionnement du circuit de la figure 15. Pour les besoins de l'explication, on suppose que la tension aux bornes 114 de drain et 115 de source du transistor 160 est maintenue constante par le circuit de lecture extérieur. La chute de tension entre la grille flottante et la borne 115 dépend alors de la charge électrique présente au noeud F, de la capacité totale entre les noeuds F et 112 (essentiellement les capacités C1 et C2), et de la tension appliquée sur la grille de commande 116 du transistor 160. En figure 16, trois courbes a, b et c ont été illustrées. La courbe a représente le cas où le noeud F est entièrement déchargé. La courbe b représente le cas d'une charge positive présente sur le noeud F (extraction d'électrons). Le seuil du transistor 160 est alors abaissé. La courbe c repré-

sente le cas d'une charge négative au noeud F (injection d'électrons) qui engendre un seuil supérieur pour le transistor MOS 160.

Selon les applications, on pourra injecter ou extraire des charges du noeud F de façon à modifier la caractéristique du transistor 160 depuis la courbe a vers l'une des courbes b et c. Une fois isolée de la tension de programmation, la fuite de la capacité C1 permet de retrouver avec le temps la courbe a. Une mesure du courant I_{114} (donc de la tension V_{119}) à tension V_{116} nulle permet de détecter une expiration du temps (réinitialisation du bit à zéro) quand le courant I_{114} s'annule.

Par la suite, on suppose une extraction d'électrons (application sur la borne 113 d'une tension d'activation ou de programmation positive par rapport à la borne 112) par effet Fowler-Nordheim. Le fonctionnement qui va être décrit se transpose toutefois sans difficulté à une injection d'électrons au noeud F, par exemple, par un phénomène dit de porteurs chauds en appliquant des tensions adaptées entre les bornes 142, 173 et 174.

Des tensions différentes peuvent être utilisées en programmation et en lecture à condition de disposer d'une référence exploitable entre la charge résiduelle et l'interprétation de l'état du bit stocké.

Selon un exemple particulier de réalisation, un circuit de rétention de charges est réalisé avec les valeurs suivantes :

Capacité C1 : environ 2 fF, épaisseur de diélectrique : environ 40 Å ;

Capacité C2 : environ 20 fF, épaisseur de diélectrique : environ 160 Å ;

Capacité C3 : environ 1 fF, épaisseur de diélectrique : environ 80 Å.

Un tel circuit peut être initialisé par application d'une tension de l'ordre de 12 volts et se trouve déchargé au bout d'environ une semaine. Il ne s'agit bien entendu que d'un

exemple, les épaisseurs de diélectrique et l'éventuelle association en parallèle de plusieurs éléments C1 ou C2 conditionnant la durée de rétention des charges.

Les figures 17A, 17B, 17C, 18A, 18B, 18C, 19A, 19B, 19C, 20A, 20B, 20C, 21A, 21B et 21C représentent un exemple de réalisation d'un circuit 100' selon le mode de réalisation de la figure 15 dans une structure intégrée, dérivée d'une architecture de mémoire EEPROM.

Les figures 17A, 18A, 19A, 20A et 21A sont des vues de dessus schématiques, respectivement du circuit électronique de rétention de charges et de ses éléments C2, 170, C1 et 160. La figure 17B est une coupe selon la ligne AA' de la figure 17A. Les figures 18B, 19B, 20B et 21B sont respectivement des vues en coupe selon les lignes BB' des figures 18A, 19A, 20A et 21A. Les figures 17C, 18C, 19C, 20C et 21C représentent les schémas électriques équivalents respectifs du circuit électronique de rétention de charges et de ses éléments C2, 170, C1 et 160.

Dans l'exemple décrit, on suppose une réalisation de transistors à canal N dans un substrat 180 (figure 17B) de silicium de type P. L'inverse est bien entendu possible.

Chaque élément ou cellule C2, 170, C1 ou 160 est obtenu à partir d'un transistor à grille flottante connecté en série avec un transistor de sélection T2, T3, T1 ou T4 à simple grille pour sélectionner, par exemple dans un réseau matriciel de cellules mémoire EEPROM, le circuit électronique de rétention de charges.

Les grilles flottantes des différents transistors constitutifs des éléments C2, 170, C1 et 160 sont interconnectées (ligne conductrice 184) pour former le noeud flottant F. Leurs grilles de commande sont reliées ensemble à une ligne conductrice 185 d'application du signal CG de commande en lecture. Leurs sources respectives SC2, S7, SC1 et S6 sont interconnectées à la borne 112 (la masse) et leurs drains respectifs DC2, D7, DC1 et D6 sont reliés aux sources respectives des transistors de sélection T2, T3, T1 et T4.

Les grilles des transistors T1 à T4 sont reliées ensemble à une ligne conductrice 186 d'application d'un signal SEL de sélection du circuit. Leurs drains respectifs D1 à D4 sont connectés à des lignes de bit BL1 à BL4 commandables individuellement. L'ordre des lignes de bit dans la figure 17C a été illustré de façon arbitraire BL2, BL3, BL1 et BL4 mais l'ordre des différents éléments C2, 170, C1 et 160 dans la direction horizontale des rangées (dans l'orientation des figures) est indifférent.

Dans cet exemple de réalisation, on suppose des régions de source et drain de type N (figure 17B) séparées les unes des autres dans la direction des lignes par des zones isolantes 181. Les grilles flottantes sont réalisées dans un premier niveau conducteur M1 séparé des régions actives par un niveau isolant 182 et les grilles de commande sont réalisées dans un deuxième niveau conducteur M2 séparé du premier par un troisième niveau isolant 183. Les grilles des transistors de sélection sont réalisées, par exemple, dans le niveau M2.

Une différence par rapport à un réseau de cellules mémoire EEPROM usuel est que les grilles flottantes sont interconnectées par groupe de quatre transistors pour réaliser le noeud flottant F. Une autre différence est que les transistors à grille flottante réalisant les différents éléments du circuit sont différents les uns des autres dans l'épaisseur de leur fenêtre tunnel et/ou dans leur connexion de drain et source.

Les figures 18A à 18C illustrent la réalisation du condensateur C2 de stockage. Les drain DC2 et source SC2 du transistor à grille flottante correspondant sont court-circuités (par extension de l'implantation de type N+ dans toute la zone active, figure 18B) pour former l'électrode 132 du condensateur. Par ailleurs, la fenêtre tunnel est éliminée par rapport à une cellule EEPROM standard.

Les figures 19A à 19C illustrent la réalisation du transistor 170 formant l'élément capacitif C3 de programmation. Il s'agit d'une cellule EEPROM standard dont l'extension 201 de

la zone dopée N sous la fenêtre tunnel 202 (figure 19B) permet d'obtenir un plateau dans la zone d'injection de charges. A la manière d'une cellule EEPROM standard, la zone de drain D7 est reliée à la source du transistor de sélection T3. La zone de source S7 est reliée à la borne 112.

Les figures 20A à 20C illustrent la réalisation de l'élément capacitif C1 constituant l'élément de fuite du circuit de rétention de charges. Par rapport à une cellule EEPROM standard, une différence consiste à amincir (zone 212, figure 20B) la fenêtre diélectrique servant à l'effet tunnel pour augmenter les fuites. Par exemple, l'épaisseur du diélectrique 212 est choisie pour être d'environ la moitié (par exemple entre 30 et 40 angströms) de celle (par exemple entre 70 et 80 angströms) d'une fenêtre tunnel (202, figure 19B) d'une cellule non modifiée.

Les figures 21A à 21C illustrent la réalisation du transistor de lecture 160 dans lequel la fenêtre tunnel a été supprimée de même que, de préférence, la zone implantée habituelle (201, figure 19B) d'une cellule EEPROM. La zone active limitée par les source S6 et drain D6 est donc similaire à celle d'un transistor MOS normal.

Les représentations des figures 17A à 21C sont schématiques et pourront être adaptées à la technologie utilisée. En particulier, les grilles ont été représentées alignées avec les limites des zones de drain et source mais un léger recouvrement est souvent présent.

Un avantage de la réalisation au moyen d'une technologie de cellules EEPROM est que le circuit de rétention de charges peut être programmé et réinitialisé en appliquant les mêmes niveaux de tension et les mêmes fenêtres temporelles que ceux utilisés pour effacer ou écrire dans des cellules mémoire EEPROM.

Un autre avantage est que cela préserve une stabilité dans le temps en évitant les dégradations de l'oxyde mince de

l'élément de fuite (C1) lors des opérations d'écritures successives.

Les connexions respectives des lignes de bit BL1 à BL4 dépendent des phases de fonctionnement du circuit et notamment de la phase de programmation (activation) ou de lecture.

Le tableau I ci-dessous illustre un mode de mise en oeuvre d'une activation (SET) et d'une lecture (READ) d'un circuit électronique de rétention de charges tel qu'illustré par les figures 17A à 21C.

Tableau I

	SEL	CG	BL2	BL3	BL1	BL4	112
SET	VPP_1	0	HZ	VPP_2	HZ	HZ	HZ
READ	V_{SEL}	V_{READ}	HZ	HZ	HZ	V_{114}	0

Dans une phase d'activation SET (passage du bit stocké à l'état 1), le signal de sélection SEL est porté à un premier potentiel haut VPP_1 par rapport à la masse pour rendre passants les différents transistors T1 à T4 tandis que le signal CG appliqués sur les grilles de commande des transistors à grille flottante reste au niveau bas 0 de façon à ne pas rendre passant le transistor 160. Les lignes de bit BL1, BL2 et BL4 restent en l'air (état de haute impédance HZ) tandis que la ligne BL3 se voit appliquée un potentiel positif V_{PP2} permettant la charge du noeud flottant F. La ligne 112, commune aux sources des transistors à grille flottante, est préférentiellement laissée en l'air (état HZ).

Pour la lecture READ, les différents transistors de sélection sont activés par le signal SEL à un niveau V_{SEL} et une tension V_{READ} de lecture est appliquée sur les grilles de commande des différents transistors à grille flottante. Les lignes BL1, BL2 et BL3 sont dans un état de haute impédance HZ alors que la ligne BL4 reçoit un potentiel V_{114} permettant d'alimenter la source de courant de lecture. La ligne 112 est ici connectée à la masse.

Les relations entre les différents niveaux VPP_1, VPP_2, V_{SEL}, V_{READ} et V_{114} sont, de préférence, les suivantes :

VPP_1 supérieur à VPP_2 ;

V_{SEL} supérieur à V_{READ} ;

V_{READ} du même ordre de grandeur que V_{114}.

Selon un exemple particulier de réalisation :

VPP_1 = environ 14 volts ;

VPP_2 = environ 12 volts ;

V_{SEL} = environ 4 volts ;

V_{READ} = environ 2 volts ; et

V_{114} = environ 1 volt.

Ce qui a été décrit ci-dessus en relation avec une cellule EEPROM par élément du circuit de rétention de charges peut bien entendu être remplacé par une structure dans laquelle des sous-ensembles de plusieurs cellules identiques en parallèle sont utilisés pour les différents éléments respectifs. En particulier :

plusieurs éléments C2 peuvent être utilisés en parallèle pour accroître la capacité du noeud F de façon à augmenter le temps de décharge du circuit électronique ;

plusieurs éléments 170 peuvent être utilisés en parallèle pour accroître la vitesse d'injection ou d'extraction d'électrons au noeud F lors d'une programmation ;

plusieurs éléments de fuite C1 peuvent être utilisés en parallèle pour réduire le temps de décharge du système ; et/ou

plusieurs éléments de lecture 160 peuvent être introduits en parallèle pour fournir un courant supérieur lors de l'évaluation du circuit.

Un circuit électronique de rétention de charges peut être introduit dans n'importe quelle position d'un réseau de cellules mémoire EEPROM standard, ce qui permet de rendre plus difficile sa localisation par un éventuel utilisateur mal intentionné.

Le cas échéant, les transistors de sélection des cellules formant le circuit de rétention de charges sont partagés avec des cellules EEPROM normales sur les mêmes lignes de bits, pourvu de prévoir des moyens d'adressage et de commutation adaptés.

Des modes de réalisation et de mises en oeuvre particuliers ont été décrits. Diverses variantes et modifications apparaîtront à l'homme de l'art. En particulier, le choix des durées de rétention de charges dépend de l'application et de la durée souhaitée pour les clés temporaires.

De plus, le circuit de rétention de charges pourra être constitué par n'importe quel circuit susceptible de présenter, de façon reproductible, une perte de charge au cours du temps indépendamment de l'alimentation du circuit. Par exemple, on pourra avoir recours à un circuit tel que décrit dans la demande internationale WO-A-03/083769.

En outre, la mise en oeuvre pratique du circuit à partir des indications fonctionnelles données ci-dessus et des besoins de l'application est à la portée de l'homme du métier. Les compteurs pourront être de toute nature et la fonction de comptage peut être de n'importe quel incrément ou décrément. Par exemple (notamment dans des modes de réalisation, par exemple figure 12 et suivantes, où les cellules de comptage ne peuvent pas être réinitialisées autrement que de façon temporelle), on pourra utiliser deux compteurs incrémentiels de taille finie dont la différence fournit la valeur à considérer. Par ailleurs, bien que l'on ait fait plus particulièrement référence à des mémoires EEPROM et RAM, ces mémoires sont plus généralement n'importe quelle mémoire ou élément de mémorisation non volatile reprogrammable (par exemple, des mémoires flash) et n'importe quelle mémoire ou élément de mémorisation volatile (par exemple des registres).

Enfin, notamment comme elle ne requiert pas d'alimentation permanente, l'invention peut être mise en oeuvre dans des dispositifs sans contact (de type transpondeur électro-

magnétique) qui tirent leur alimentation d'un champ électro-magnétique dans lequel il se trouve (généré par un terminal).

REVENDICATIONS

1. Procédé d'obtention, dans un circuit électronique (5), d'au moins une première clé (BMK, BK, BK(ID)) destinée à être utilisée dans un mécanisme cryptographique, à partir d'au moins une deuxième clé (BRK, RK, ID) contenue dans le même circuit, caractérisé en ce que ladite première clé est stockée dans au moins un premier élément de mémorisation (100) du circuit, ledit premier élément de mémorisation étant réinitialisé automatiquement au bout d'une durée indépendante du fait que le circuit soit alimenté ou non.

2. Procédé selon la revendication 1, dans lequel le nombre d'utilisations de la première clé (BMK, BK) en une période donnée est limité par un compteur (RC(BMK), RC(BK)) stocké dans un deuxième élément de mémorisation (100) réinitialisé automatiquement au bout d'une durée indépendante du fait que le circuit soit alimenté ou non.

3. Procédé selon la revendication 1 ou 2, dans lequel la deuxième clé (BRK, RK) est contenue dans un élément de mémorisation non volatile (52) du circuit.

4. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel la première clé (BK, BK(ID)) est obtenue par dérivation de la deuxième clé (RK, ID).

5. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel la deuxième clé (BRK) sert à obtenir la première clé (BMK) par déchiffrement.

6. Procédé selon l'une quelconque des revendications 1 à 5, dans lequel la première clé (BMK, BK) sert de base à la dérivation d'une troisième clé (CW, SK) utilisée pour chiffrer ou authentifier des informations provenant de l'extérieur du circuit (5).

7. Procédé de transmission chiffrée de données numériques (MEDIA), dans lequel une clé (CW) de déchiffrement de ces données correspond à la troisième clé du procédé selon la revendication 6.

8. Procédé de dérivation d'une clé de session (SK) d'une application EMV, dans lequel la clé de session correspond à la troisième clé du procédé selon la revendication 6.

9. Procédé de contrôle d'utilisation de cartouches d'encre (44) au moyen d'un circuit (5) associé à une imprimante (41) et d'une clé (BK(ID)) dérivée d'un identifiant (ID) fournit par une cartouche, dans lequel ladite clé dérivée correspond à la première clé du procédé selon la revendication 4.

10. Circuit électronique (5) comportant des moyens de traitement cryptographique et au moins une mémoire non volatile (52), caractérisé en ce qu'il comporte au moins un élément de mémorisation (100) pourvu d'au moins un premier élément capacitif (C1) présentant une fuite au travers de son espace diélectrique, ce premier élément de mémorisation formant ledit premier élément de mémorisation du procédé selon l'une quelconque des revendications 1 à 9.

11. Circuit selon la revendication 10, comportant des moyens adaptés pour mettre en oeuvre le procédé selon l'une quelconque des revendications 1 à 9.

12. Carte à puce (1), caractérisée en ce qu'elle comporte un circuit (5) conforme à la revendication 10 ou 11.

13. Clé électronique, caractérisée en ce qu'elle comporte un circuit (5) conforme à la revendication 10 ou 11.

14. Système de télédiffusion d'un contenu numérique (MEDIA) comportant :

un émetteur (21) apte à chiffrer le contenu à partir d'un mot de contrôle (CW) changeant périodiquement et transmis, avec le contenu chiffré, de façon chiffré à partir d'au moins une première clé temporaire (BMK) de période supérieure à celle du mot de contrôle ; et

un récepteur (23) associé à un circuit électronique (5) apte à déchiffrer le mot de contrôle à partir de ladite première clé, puis à déchiffrer le contenu à partir de ce mot de contrôle, ledit circuit étant conforme à la revendication 10 ou 11.

15. Récepteur d'un système selon la revendication 14, comportant ledit circuit électronique (5).

16. Récepteur d'un système selon la revendication 14, comportant un lecteur de carte à puce, ladite carte (1) étant conforme à la revendication 12.

17. Système de contrôle d'utilisation de cartouches d'encre par une imprimante, comportant :

au moins une imprimante (41) associée à au moins un circuit électronique (5) selon la revendication 10 ou 11 ; et

au moins une cartouche d'encre (44) adaptée à transmettre un identifiant (ID) permettant au circuit de l'imprimante de générer ladite première clé.

18. Imprimante (41) d'un système selon la revendication 17.

19. Cartouche (44) destinée à une imprimante selon la revendication 18, comportant un circuit électronique (6) pourvu d'un élément de mémorisation (100) réinitialisé automatiquement au bout d'une durée indépendante du fait que le circuit soit alimenté ou non, cet élément contenant ledit identifiant (ID).

20. Système de transactions bancaires utilisant des cartes à puce (1) conformes à la revendication 12, ladite première clé (BK) servant à dériver des clés de session (SK) des transactions.

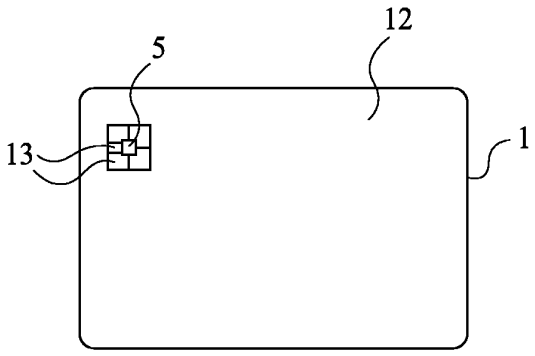


Fig 1

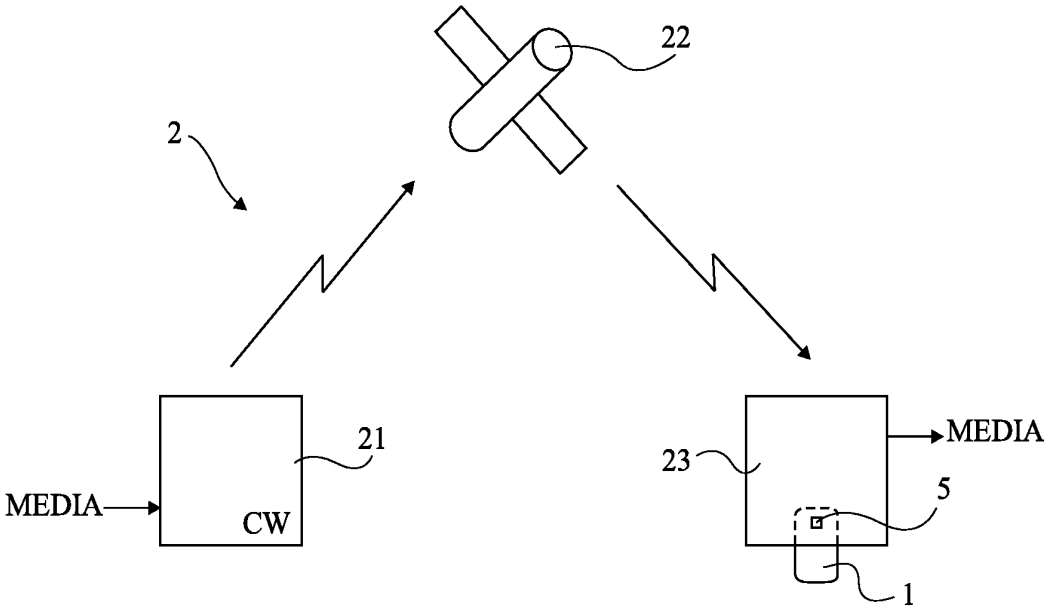


Fig 2

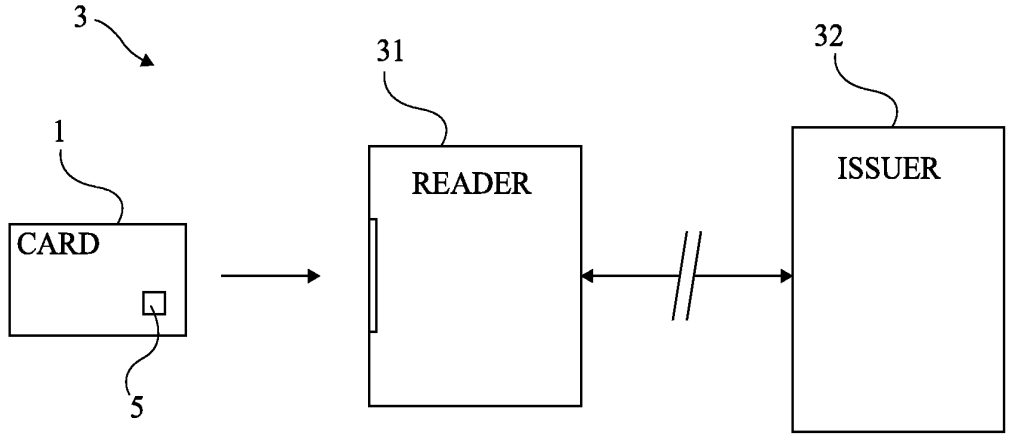


Fig 3

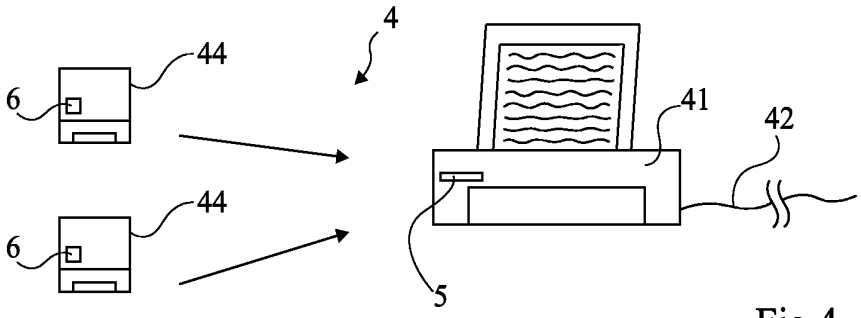


Fig 4

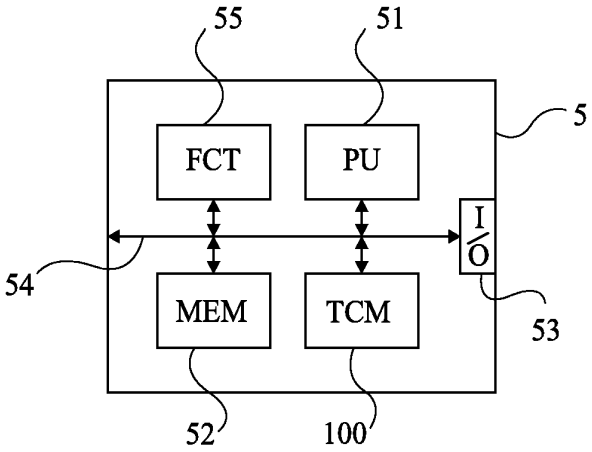


Fig 5

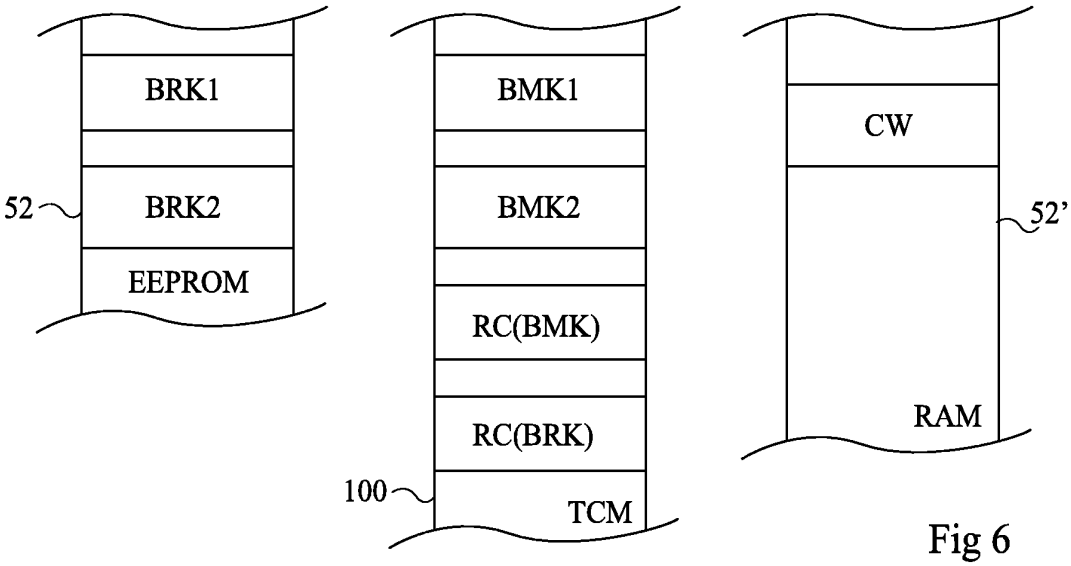


Fig 6

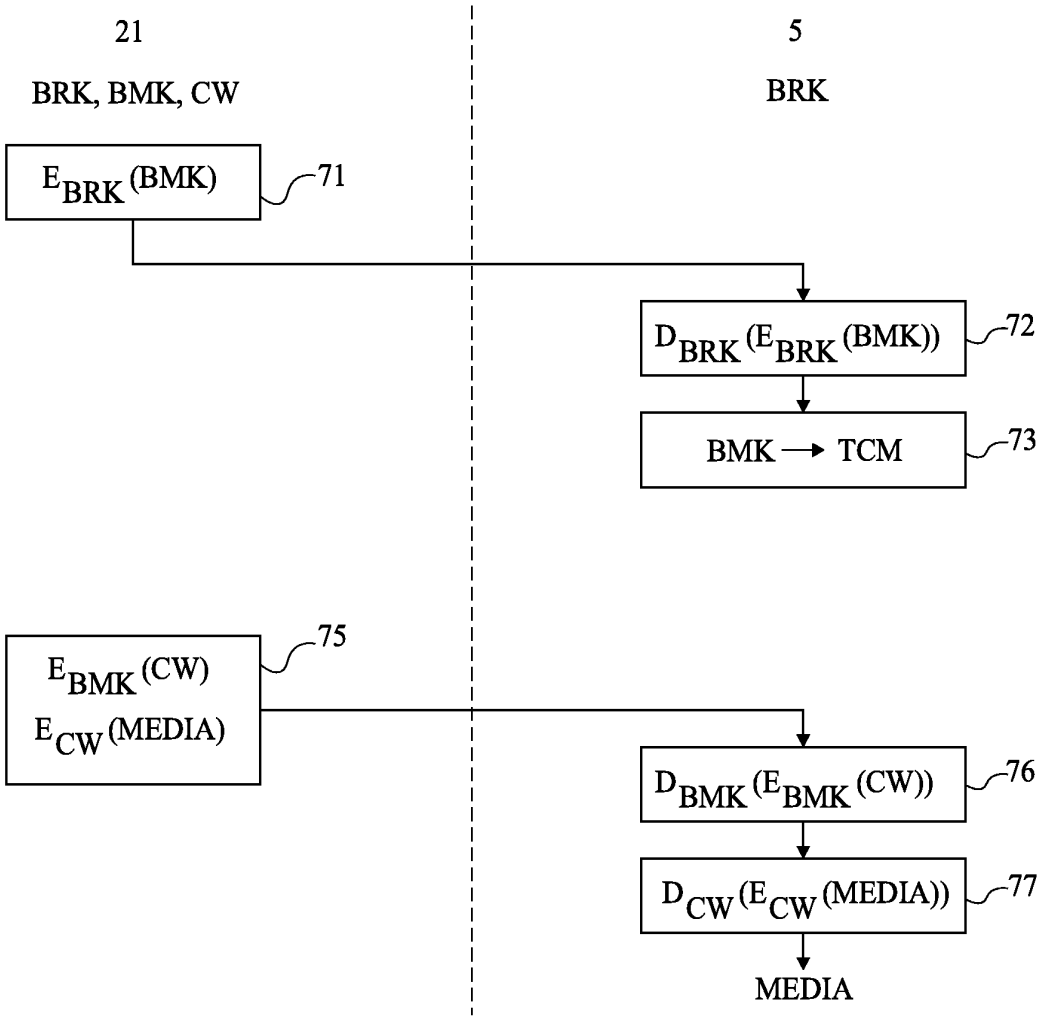

21
BRK, BMK, CW
5
BRK
E_{BRK} (BMK)
71
D_{BRK} (E_{BRK} (BMK))
72
BMK → TCM
73
E_{BMK} (CW)
E_{CW} (MEDIA)
75
D_{BMK} (E_{BMK} (CW))
76
D_{CW} (E_{CW} (MEDIA))
77
MEDIA

Fig 7

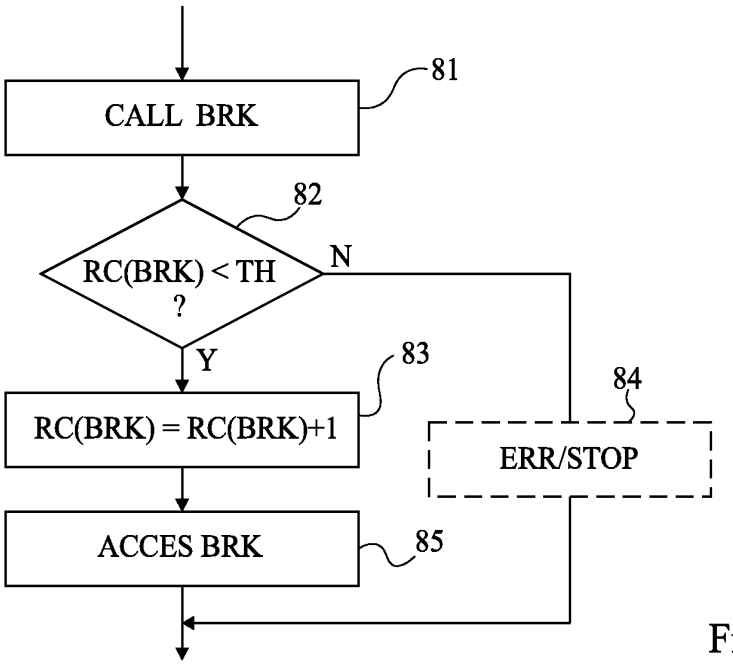

CALL BRK
81
82
RC(BRK) < TH ?
N
Y
83
RC(BRK) = RC(BRK)+1
84
ERR/STOP
ACCES BRK
85

Fig 8

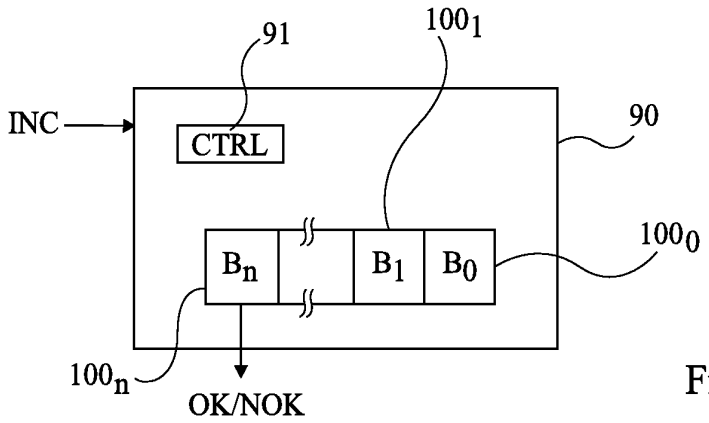


Fig 9

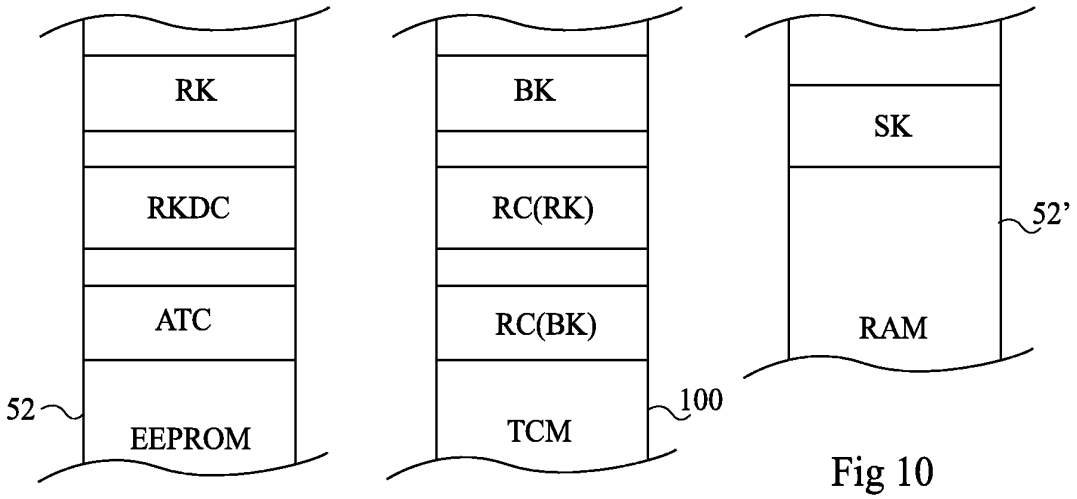


Fig 10

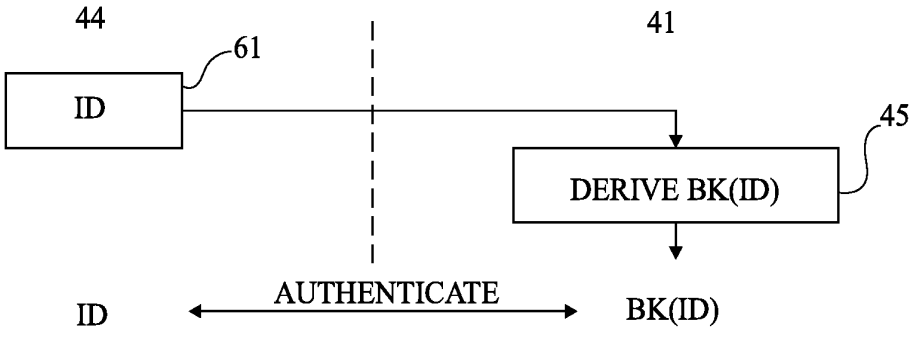


Fig 11

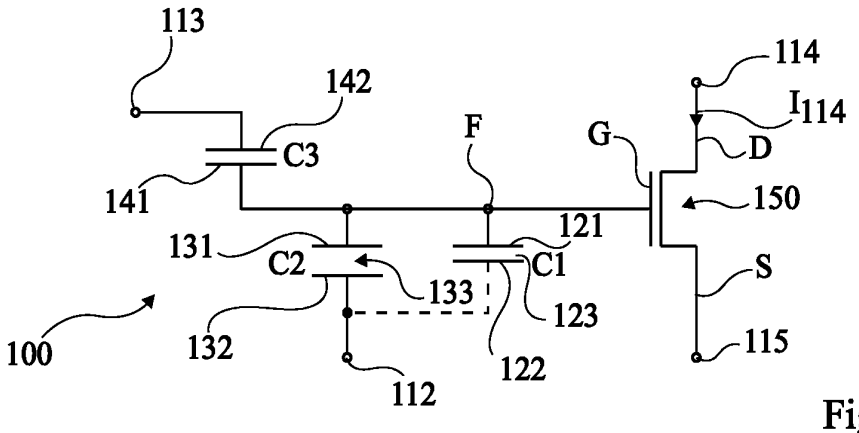


Fig 12

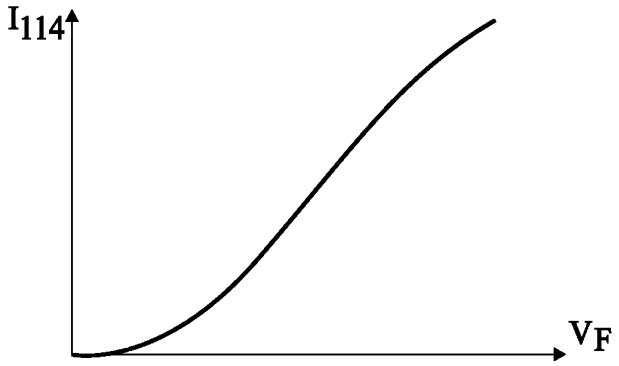


Fig 13

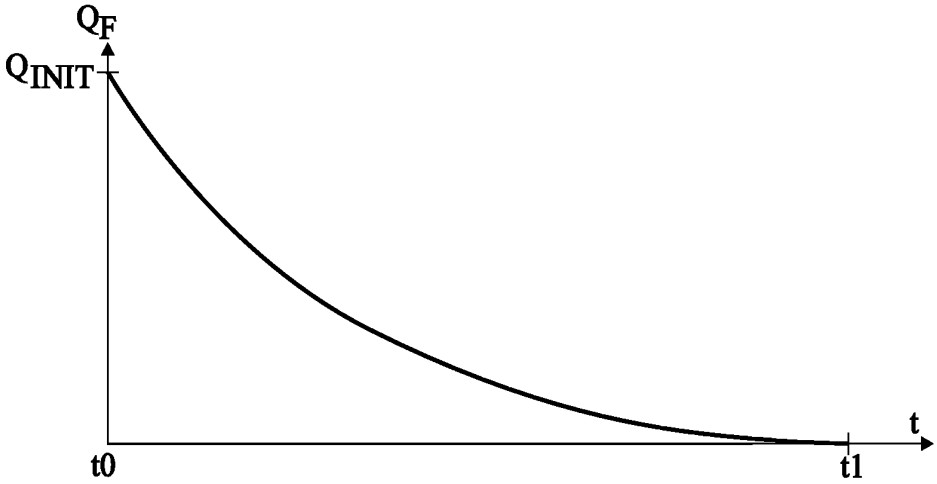


Fig 14

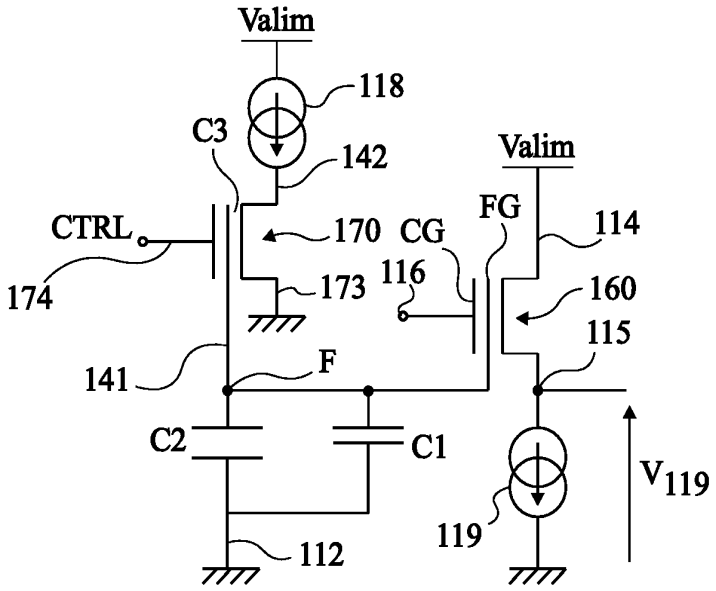

Valim
118
C3
142
Valim
CTRL
170
CG
FG
114
174
173
116
160
115
141
F
C2
C1
V_{119}
119
112

Fig 15

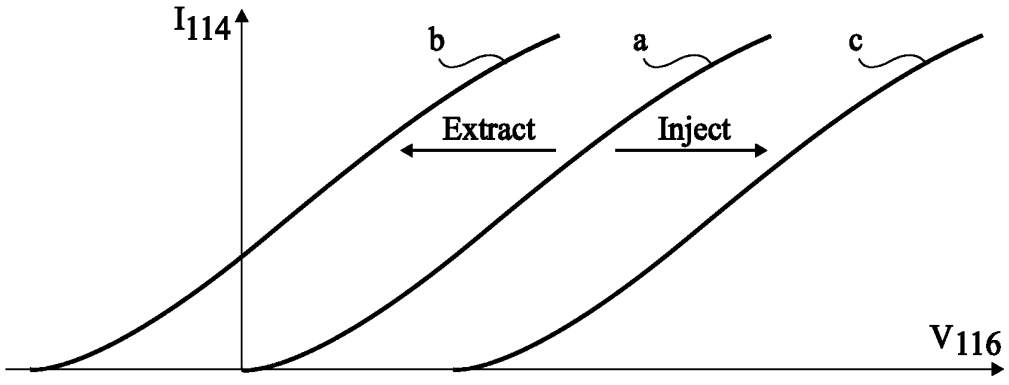

I_{114}
b
a
c
Extract
Inject
V_{116}

Fig 16

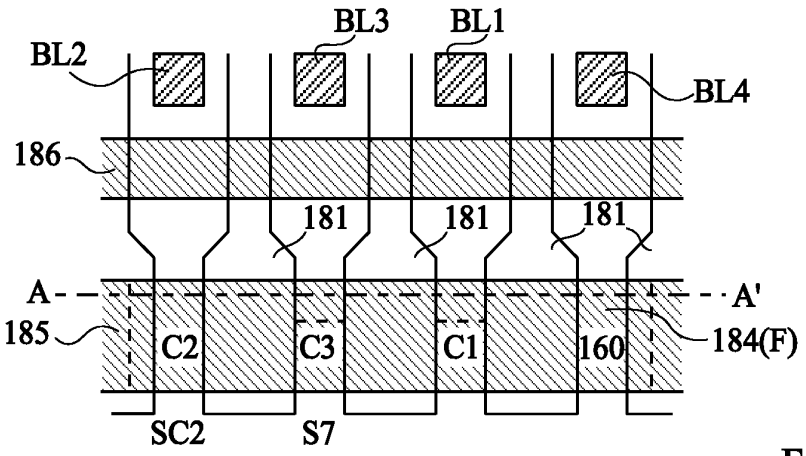


Fig 17A

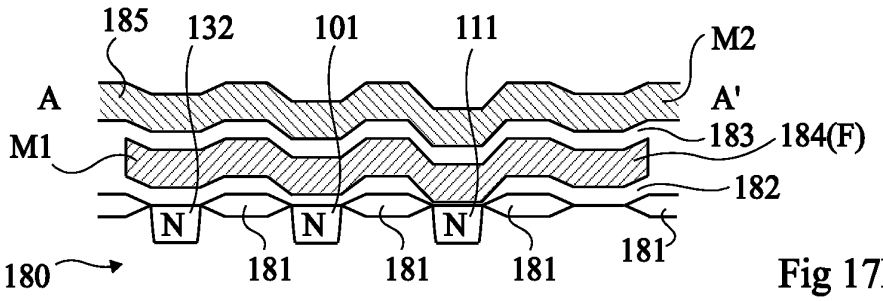


Fig 17B

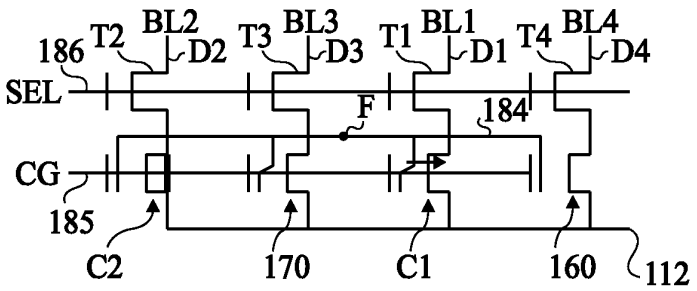


Fig 17C

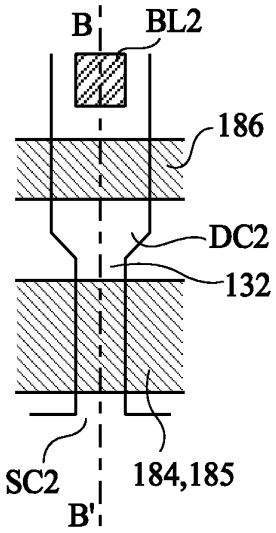


Fig 18A

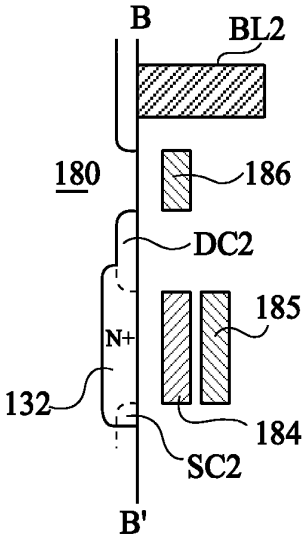


Fig 18B

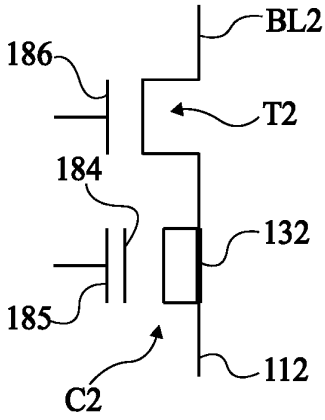


Fig 18C

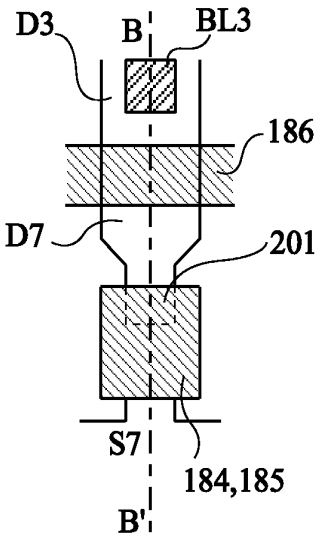


Fig 19A

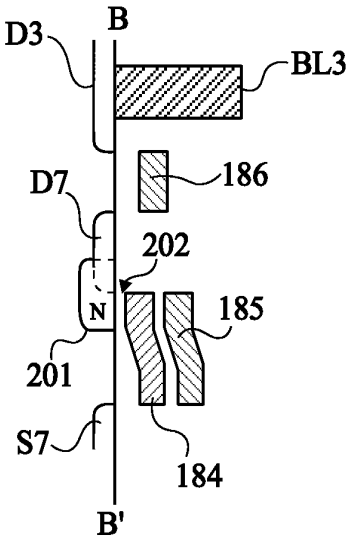


Fig 19B

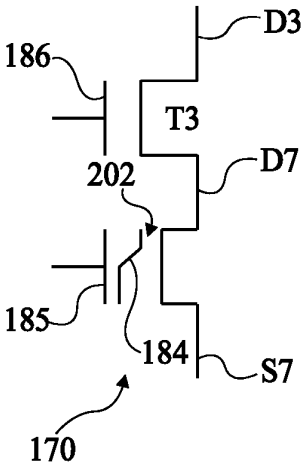


Fig 19C

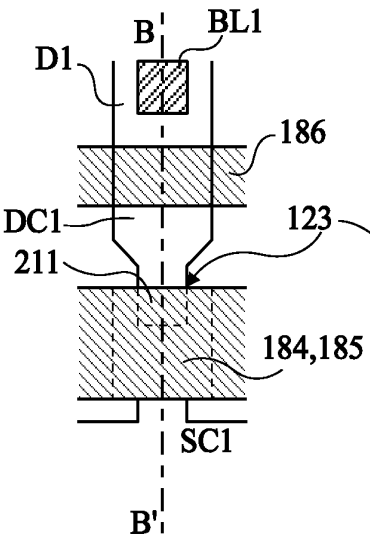


Fig 20A

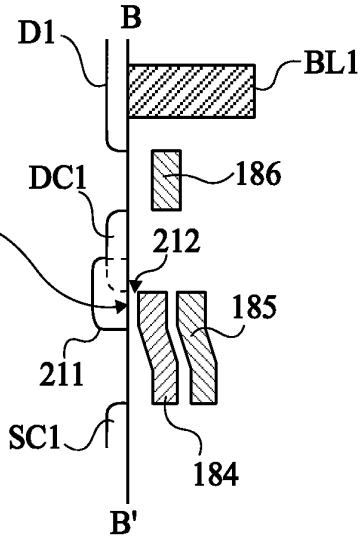


Fig 20B

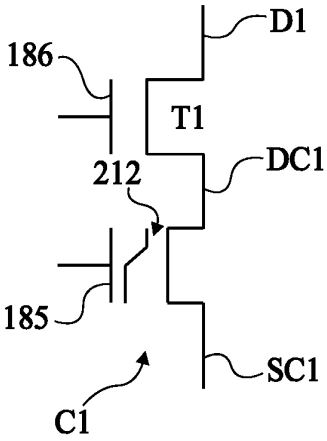


Fig 20C

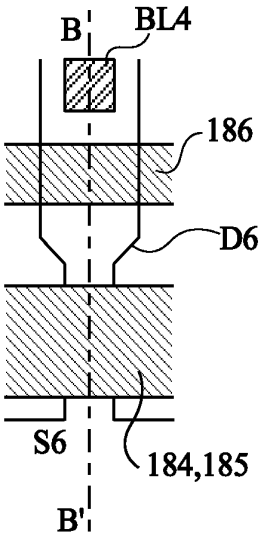


Fig 21A

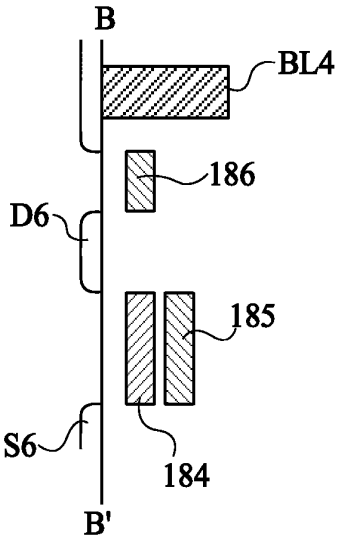


Fig 21B

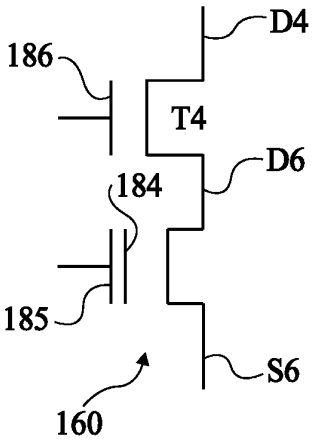


Fig 21C

RÉPUBLIQUE FRANÇAISE

2926382

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 705935
FR 0850169

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		
Y	US 2007/003062 A1 (MIZIKOVSKY SEMYON B [US] ET AL) 4 janvier 2007 (2007-01-04) * alinéa [0033] * * figure 1 * -----	1-20	G06K19/073 H04L9/32 G07F19/00
Y	WO 01/54057 A (INFINEON TECHNOLOGIES AG [DE]; HORVAT HELMUT [AT]; WALLSTAB STEFAN [DE]) 26 juillet 2001 (2001-07-26) * page 2, ligne 6 - ligne 10 * * page 3, ligne 25 - page 4, ligne 25 * -----	1-20	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06F H04L G07F

Date d'achèvement de la recherche	Examinateur
19 août 2008	Chabot, Pedro

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 0850169 FA 705935

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 19-08-2008
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
US 2007003062 A1	04-01-2007	EP 1897330 A1	12-03-2008
		KR 20080018213 A	27-02-2008
		WO 2007005309 A1	11-01-2007
WO 0154057 A	26-07-2001	AT 263989 T	15-04-2004
		DE 50006022 D1	13-05-2004
		US 2003005315 A1	02-01-2003

EPO FORM P0465