

⑫

BREVET D'INVENTION

B1

⑤④ Méthode pour la gestion d'une zone de données sensible en mémoire FLASH.

②② Date de dépôt : 25.05.22.

③③ Priorité :

⑥③ Références à d'autres documents nationaux
apparentés :

☐ Demande(s) d'extension :

⑦① Demandeur(s) : *STMICROELECTRONICS (ALPS)*
SAS Société par actions simplifiée — FR.

④③ Date de mise à la disposition du public
de la demande : 01.12.23 Bulletin 23/48.

④⑤ Date de la mise à disposition du public du
brevet d'invention : 30.05.25 Bulletin 25/22.

⑤⑥ Liste des documents cités dans le rapport de
recherche :

Se reporter à la fin du présent fascicule

⑦② Inventeur(s) : BENHAMMADI Jawad.

⑦③ Titulaire(s) : *STMICROELECTRONICS (ALPS) SAS*
Société par actions simplifiée.

⑦④ Mandataire(s) : CABINET BEAUMONT.



Description

Titre de l'invention : *Méthode pour la gestion d'une zone de données sensible en mémoire FLASH*

Domaine technique

[0001] La présente description concerne de façon générale le domaine des mémoires de type FLASH.

Technique antérieure

[0002] Une mémoire non volatile programmable, telle qu'une mémoire électriquement programmable effaçable (EEPROM), permet de stocker certaines données, telles que des clefs de chiffrement ou des paramètres de configuration, dans des dispositifs électroniques même lorsque les dispositifs électroniques sont hors tension. Cependant, compte tenu de la technologie utilisée pour mettre en œuvre une EEPROM, celle-ci ne peut généralement pas être intégrée sur puce. Les implémentations externes (hors puce) d'EEPROM entraînent alors une augmentation de la surface, de la consommation d'énergie et des coûts.

[0003] Une mémoire de type FLASH peut quant à elle, être implémentée sur puce. Cependant, la mémoire FLASH a certaines contraintes d'accès. Par exemple, contrairement à une EEPROM, il n'est pas possible d'écraser ou de modifier individuellement des valeurs de données d'une mémoire FLASH. Par conséquent, il existe des problèmes techniques liés à l'utilisation d'une mémoire FLASH sur puce pour mettre en œuvre un stockage en mémoire similaire à celui offert par une EEPROM.

Résumé de l'invention

[0004] Il existe un besoin d'améliorer l'accès et la manipulation de données sensibles d'une mémoire FLASH.

[0005] Un mode de réalisation pallie tout ou partie des inconvénients des mémoires FLASH connus.

[0006] Un mode de réalisation prévoit un procédé comprenant :

- la modification ou suppression d'une ou plusieurs valeurs de donnée d'une mémoire non volatile, l'une ou plusieurs valeurs de donnée étant stockées dans un premier secteur de la mémoire, le premier secteur étant désigné comme secteur courant par une ou plusieurs valeurs de sélection stockées dans la mémoire non volatile, la modification ou suppression comprenant :

- l'écriture d'une ou plusieurs valeurs de donnée dans un deuxième secteur de la mémoire non volatile, le deuxième secteur étant désigné comme secteur alternatif par l'une ou plusieurs valeurs de sélection.

[0007] Selon un mode de réalisation, la modification ou suppression comprend la modi-

fication d'une première valeur de donnée stockée dans un premier emplacement, en association avec une première adresse, du premier secteur de la mémoire, et l'écriture de l'une ou plusieurs valeurs de donnée dans le deuxième secteur comprend :

- l'écriture d'une deuxième valeur de donnée dans un premier emplacement du deuxième secteur de la mémoire non volatile, le premier emplacement du deuxième secteur étant désigné au moins en partie par la première adresse.

[0008] Selon un mode de réalisation, l'une ou plusieurs valeurs de sélection comprend une première valeur de sélection stockée dans le premier secteur.

[0009] Selon un mode de réalisation, l'une ou plusieurs valeurs de sélection comprend en outre une deuxième valeur de sélection stockée dans le deuxième secteur.

[0010] Selon un mode de réalisation, le procédé ci-dessus comprend, suite à une mise sous tension de la mémoire non volatile :

- la lecture des première et deuxième valeurs de sélection ;
- la détermination, sur la base des première et deuxième valeurs de sélection, du secteur désigné comme alternatif ; et
- si au moins une valeur de donnée est contenue dans le secteur désigné comme secteur alternatif, la réinitialisation du secteur alternatif.

[0011] Selon un mode de réalisation, la modification ou suppression comprend une suppression d'autres premières valeurs de données, et le premier secteur comprend une première plage d'adresses comprenant les autres premières valeurs de données associées à une première valeur de niveau ainsi qu'une deuxième plage d'adresses comprenant des deuxième valeurs de données associées à une deuxième valeur de niveau, la deuxième valeur de niveau étant strictement supérieure à la première valeur de niveau et dans lequel la suppression comprend :

- la génération de la deuxième valeur de niveau par un compteur monotone ;
- l'écriture des deuxième valeurs de données en association avec la première valeur de comptage dans le deuxième secteur ;
- l'écriture d'une deuxième valeur de sélection (SLT2) dans le deuxième secteur, rendant le premier secteur alternatif et le deuxième secteur courant ; et
- la réinitialisation du premier secteur.

[0012] Selon un mode de réalisation, le procédé ci-dessus comprend en outre :

- l'écriture d'une deuxième valeur de sélection dans le deuxième secteur, rendant le premier secteur alternatif et le deuxième secteur courant ; et
- la réinitialisation du premier secteur.

[0013] Selon un mode de réalisation, le procédé ci-dessus comprend en outre, avant l'écriture de la deuxième valeur de sélection dans le deuxième secteur :

- l'écriture d'une ou plusieurs autres valeurs de donnée, stockées dans le premier secteur, dans le deuxième secteur.

- [0014] Selon un mode de réalisation, le procédé ci-dessus comprend en outre, suite à l'écriture desdites une ou plusieurs autres valeurs de donnée dans le deuxième secteur, la modification ou suppression d'une ou plusieurs des valeurs stockées dans le deuxième secteur et, l'écriture d'une troisième valeur de sélection, différente des première et deuxième valeurs de sélection, dans le premier secteur, rendant le premier secteur courant et le deuxième secteur alternatif.
- [0015] Selon un mode de réalisation, chacune des première, deuxième et troisième valeurs de sélection ont au moins les valeurs de deux bits différentes des autres valeurs de sélection.
- [0016] Selon un mode de réalisation, le procédé ci-dessus comprend en outre :
- la lecture de l'état d'un bit stocké dans un registre ; et
 - l'écriture d'une ou plusieurs valeurs de données dans le secteur courant lorsque le bit est dans un premier état, ou l'écriture de l'une ou plusieurs valeurs de données dans le secteur alternatif lorsque le bit est dans un deuxième état.
- [0017] Selon un mode de réalisation, la mémoire non volatile (104) est une mémoire de type FLASH.
- [0018] Un mode de réalisation prévoit un dispositif comprenant :
- une mémoire non volatile comprenant une ou plusieurs valeurs de donnée, stockées dans un premier secteur de la mémoire, la mémoire comprenant en outre un deuxième secteur ainsi qu'une ou plusieurs valeurs de sélection désignant le premier secteur comme secteur courant et désignant le deuxième secteur comme secteur alternatif ; et
 - un contrôleur d'accès configuré pour modifier ou supprimer l'une ou plusieurs valeurs de données en écrivant une ou plusieurs autres valeurs de donnée dans le deuxième secteur de la mémoire non volatile.
- [0019] Selon un mode de réalisation, le contrôleur d'accès est configuré pour modifier une première valeur de donnée stockée dans un premier emplacement du premier secteur de la mémoire, en association avec une première adresse, est modifié en écrivant une deuxième valeur de donnée dans un premier emplacement du deuxième secteur de la mémoire non volatile, le premier emplacement du deuxième secteur étant désigné au moins en partie par la première adresse.
- [0020] Selon un mode de réalisation, le dispositif ci-dessus comprend en outre un compteur monotone configuré pour générer une valeur de niveau, et dans lequel le premier secteur comprend une première plage d'adresses comprenant des autres premières valeurs de données associées à une première valeur de niveau, ainsi qu'une deuxième plage d'adresses comprenant des deuxièmes valeurs de donnée associées à une deuxième valeur de niveau, la deuxième valeur de niveau étant strictement supérieure à la première valeur de niveau, le contrôleur d'accès étant configuré pour supprimer l'une ou plusieurs autres premières valeurs de données, la suppression comprenant :

- l'écriture des deuxièmes valeurs de données en association avec la première valeur de comptage dans le deuxième secteur ;
- l'écriture d'une deuxième valeur de sélection, rendant le premier secteur alternatif et le deuxième secteur courant ; et
- la réinitialisation du premier secteur.

Brève description des dessins

- [0021] Ces 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 :
- [0022] la [Fig.1] représente, de façon très schématique et sous forme de blocs, un dispositif électronique selon un mode de réalisation de la présente description ;
- [0023] la [Fig.2] illustre, de façon schématique et sous forme de blocs, le contenu d'une mémoire FLASH du dispositif électronique de la [Fig.1] selon un mode de réalisation de la présente description ;
- [0024] la [Fig.3] est un organigramme représentant des opérations d'un procédé d'écriture dans une mémoire FLASH selon un exemple de réalisation de la présente description ;
- [0025] la [Fig.4] illustre de manière schématique le contenu des secteurs d'une mémoire FLASH lors de la réalisation d'un procédé de modification d'une donnée ;
- [0026] la [Fig.5] est un organigramme représentant des opérations d'un procédé d'échange de secteur selon un exemple de réalisation de la présente description ;
- [0027] la [Fig.6] illustre de manière schématique le contenu des secteurs de la mémoire FLASH lors de la réalisation d'un procédé de suppression d'une ou plusieurs données ;
- [0028] la [Fig.7] est un organigramme représentant des opérations d'un procédé d'échange de secteur selon un exemple de réalisation de la présente description ;
- [0029] la [Fig.8] illustre, de façon schématique et sous forme de blocs, un exemple de réalisation d'une mémoire FLASH selon un mode de réalisation de la présente description ;
- [0030] la [Fig.9] illustre, de façon schématique, une fonction de contrôle d'accès à une mémoire FLASH selon un mode de réalisation de la présente description ; et
- [0031] la [Fig.10] est un organigramme représentant des opérations suite à la mise sous tension de la mémoire FLASH selon un exemple de réalisation de la présente description.

Description des modes de réalisation

- [0032] De mêmes éléments ont été désignés par de mêmes références dans les différentes figures. En particulier, les éléments structurels et/ou fonctionnels communs aux différents modes de réalisation peuvent présenter les mêmes références et peuvent disposer de propriétés structurelles, dimensionnelles et matérielles identiques.

- [0033] Par souci de clarté, seuls les étapes et éléments utiles à la compréhension des modes de réalisation décrits ont été représentés et sont détaillés. En particulier, la conception de dispositifs de traitement est bien connue de la personne du métier et certains éléments n'ont pas été détaillés dans la description qui suit.
- [0034] Sauf précision contraire, lorsque l'on fait référence à deux éléments connectés entre eux, cela signifie directement connectés sans éléments intermédiaires autres que des conducteurs, et lorsque l'on fait référence à deux éléments reliés (en anglais "coupled") entre eux, cela signifie que ces deux éléments peuvent être connectés ou être reliés par l'intermédiaire d'un ou plusieurs autres éléments.
- [0035] Dans la description qui suit, lorsque l'on fait référence à des qualificatifs de position absolue, tels que les termes "avant", "arrière", "haut", "bas", "gauche", "droite", etc., ou relative, tels que les termes "dessus", "dessous", "supérieur", "inférieur", etc., ou à des qualificatifs d'orientation, tels que les termes "horizontal", "vertical", etc., il est fait référence sauf précision contraire à l'orientation des figures.
- [0036] Sauf précision contraire, les expressions "environ", "approximativement", "sensiblement", et "de l'ordre de" signifient à 10 % près, de préférence à 5 % près.
- [0037] La [Fig.1] représente de façon très schématique et sous forme de blocs, un dispositif électronique 100 comprenant un circuit intégré 102 selon un mode de réalisation de la présente description.
- [0038] Le dispositif électronique 100 est par exemple une carte électronique telle qu'une carte à microcircuits, un matériel à usage informatique, un circuit à microprocesseur, etc.
- [0039] Le circuit intégré 102 comprend par exemple une mémoire non volatile 104 (NV MEM) de type FLASH. La mémoire 104 est reliée à un contrôleur d'accès 106 (ACCESS CTRL) implémenté, par exemple, par un circuit matériel, ou au moins partiellement par une implémentation logicielle. Le contrôleur d'accès 106 est par exemple relié à un bus 108, le bus 108 comprenant par exemple un bus de donnée.
- [0040] Le circuit intégré 102 comprend en outre, par exemple, un compteur monotone 110 (MONOTONIC COUNTER) configuré pour générer des valeurs de comptage. De plus, dans certains modes de réalisation, le circuit intégré 102 comprend également un processeur 112 (CPU), et/ou une mémoire volatile 114 (RAM). La mémoire volatile 114 est, par exemple, une mémoire volatile à accès aléatoire (de l'anglais « Random Access Memory »). Le compteur monotone 110, le processeur 112 et la mémoire volatile 114 sont par exemple reliés au contrôleur d'accès 106 par l'intermédiaire du bus 108.
- [0041] Le contrôleur d'accès 106 comprend par exemple un registre volatile 116 (REGISTER) et un registre volatile ou non volatile 118 (ALT_SECT). Le contrôleur d'accès 106 est par exemple configuré pour recevoir une valeur de niveau TIL générée

par le compteur monotone 110. Dans certains cas, le contrôleur d'accès 106 est également configuré pour recevoir un signal TZ et/ou un signal SEC/NSEC. Le signal SEC/NSEC est par exemple un signal indiquant un fonctionnement du circuit intégré 102 dans un mode sécurisé (SEC) ou non sécurisé (NSEC). Le signal TZ est par exemple un signal indiquant un fonctionnement du circuit intégré 102 dans un mode sécurisé avec un domaine de confiance (en anglais « Trust Zone »). Les signaux TZ et SEC/NSEC sont par exemple transmis par un circuit de configuration du démarrage et de la sécurité du circuit intégré 102 (en anglais « System configuration, Boot and Security »), ce circuit de configuration n'étant pas représenté en [Fig.1].

- [0042] Selon un mode de réalisation de la présente description, la mémoire non volatile 104 comprend un premier secteur 120 (SECT1) et un deuxième secteur 122 (SECT2). La mémoire comprend en outre une zone 124 (CODE/DATA) contenant par exemple des codes, tels que des codes de démarrage et/ ou des codes applicatifs, et/ou des données.
- [0043] Dans les applications visées par la présente description et en mode de fonctionnement usuel, un seul des deux secteurs contient des données et ce secteur est désigné comme étant un secteur courant de la mémoire non volatile 104, l'autre secteur étant quant à lui désigné comme étant un secteur alternatif. L'usage des deux secteurs 120 et 122 permet de modifier ou de supprimer, de manière individuelle, une valeur d'une donnée stockée dans le secteur courant. Pour ce faire, des valeurs de donnée sont écrites dans le secteur alternatif, puis les rôles des secteurs sont par exemple inversés, le secteur alternatif devenant le secteur courant, et le secteur courant devenant le secteur alternatif.
- [0044] Selon un mode de réalisation, le secteur 120 comprend un emplacement 126 et le secteur 122 comprend un emplacement 128. Les deux emplacements 126 et 128 sont réservés au stockage d'une ou plusieurs valeurs de sélection SLT1, SLT2. Suite à une mise sous tension de la mémoire non volatile 104, le contenu des emplacements 126 et 128 est lu et les valeurs de sélection SLT1, SLT2 permettent d'identifier lequel parmi les secteurs 120 et 122 est le secteur courant, et lequel parmi les secteurs 120 et 122 est le secteur alternatif. Dans un exemple, chaque valeur de sélection SLT1, SLT2 peut être soit non programmée, c'est-à-dire que l'emplacement est vierge, soit programmée avec l'une parmi trois valeurs de comptage qui vont être désignées 0, 1 et 2.
- [0045] Selon un mode de réalisation, une règle est établie entre les valeurs de comptage 0, 1 et 2 permettant de décider quel est le secteur courant et quel est le secteur alternatif lorsque les deux emplacements 126 et 128 ne sont pas vierges. A titre d'exemple, lorsque les valeurs de sélection programmées sont les valeurs 0 et 1, le secteur contenant la valeur de sélection 1 est le secteur courant. Lorsque les valeurs de sélection programmées sont les valeurs 1 et 2, le secteur contenant la valeur de sélection 2 est le secteur courant. Lorsque les valeurs de sélection programmées sont

les valeurs 2 et 0, le secteur contenant la valeur de sélection 0 est le secteur courant.

- [0046] Selon un mode de réalisation, lorsque l'emplacement d'un secteur est vierge et l'emplacement de l'autre secteur est non vierge, c'est le secteur comprenant l'emplacement non vierge qui est désigné comme étant le secteur courant.
- [0047] Selon un exemple, les valeurs de sélection sont des valeurs, exprimées en chiffres hexadécimales, 51, 8A et B4. Les valeurs 51, 8A et B4 sont présentées uniquement à titre d'exemple et d'autres valeurs sont bien sûr envisageables. De plus, comme cela est le cas pour les valeurs 51, 8A et B4, dans certains modes de réalisation, chacune des valeurs de sélection a au moins les valeurs de 2 bits différant des deux autres valeurs de sélections.
- [0048] Lorsque le secteur courant est identifié, une indication du secteur courant est alors stockée dans le registre 116. L'indication prend par exemple la forme d'un bit ou d'un complément d'adresse.
- [0049] Selon un mode de réalisation, les emplacements 126 et 128 ne sont pas accessibles par logiciel. Les contenus des emplacements 126 et 128 ne peuvent donc pas être falsifiés facilement.
- [0050] Selon un mode de réalisation, un bit stocké dans le registre 118 est modifiable par le processeur 112, permettant à un logiciel exécuté par le processeur 112 d'indiquer dans lequel des secteurs courant et alternatif une valeur de donnée sera écrite. A titre d'exemple, lorsque le bit est dans l'état 0, cela traduit que le secteur courant est sélectionné pour écriture, et lorsque le bit vaut 1, cela traduit que le secteur alternatif est sélectionné pour écriture.
- [0051] La [Fig.2] illustre, de façon schématique et sous forme de blocs, le contenu de la mémoire 104 selon un mode de réalisation de la présente description.
- [0052] A titre d'exemple, la mémoire 104 comprend, dans la zone 124, des données et des codes 200 (DATA/USER CODES) et des codes 202 (CODES). Les codes parmi les données et codes 200 sont par exemple des codes configurables par un utilisateur du circuit 102 afin de l'adapter à ses besoins pour le dispositif 100. Les codes 200 sont par exemple non sécurisés et sont par exemple stockés sur des adresses mémoire, exprimées en valeurs hexadécimales, allant de 0x081F_FFFF à 0x0800_0000. Les codes 202 sont par exemple des codes de démarrage stockés par le fabricant du circuit 102 et sont par exemple stockés sur des adresses mémoire, exprimées en valeurs hexadécimales, allant de 0x0BF9_FFFF à 0x0BF8_0000.
- [0053] A titre d'exemple, la mémoire FLASH 104 comprend également une zone 204 configurée pour stocker des paramètres de la mémoire FLASH, tel que des paramètres de sécurité 204 (USER OPTIONS), et/ou une zone 206 (ENGI OPTION) configurée pour stocker des paramètres de configuration, tels que des paramètres de configuration d'un ou plusieurs modules, des paramètres de configuration du circuit intégré 102, des

paramètres d'activation ou de désactivation d'une ou plusieurs applications de sécurité, des paramètres indiquant la taille d'une ou plusieurs zones de la mémoire 104, telle que par exemple la zone 204. Les emplacements des zones 204 et 206 ne font pas partie des zones d'adresses mappées dans la mémoire 104, c'est-à-dire qu'ils ne font pas partie de l'espace mémoire visible et accessible par le processeur 112.

[0054] A titre d'exemple, la zone 124 comprend en outre d'autres codes ou données 208.

[0055] La mémoire non volatile 104 comprend en outre une zone 210 comprenant les secteurs 120 et 122. Les secteurs 120 et 122, et plus particulièrement le secteur courant, contiennent des données telles des clefs OBK (OPTION BYTES KEYS). La zone 210 est par exemple mappée aux adresses allant de 0x0BFD_1FFF à 0x0BFD_0000. La zone 210 est implémentée par les secteurs 120 et 122 et les deux secteurs sont alors visible de l'extérieur comme une seule plage d'adresses.

[0056] Les adresses mémoire sont présentées uniquement à titre illustratif et ne sont bien sûr pas limitatives. D'autres tailles et emplacements des différentes zones et des secteurs 120 et 122 sont bien sûr envisageables.

[0057] La [Fig.3] est un organigramme représentant des opérations d'un procédé d'écriture dans la mémoire 104 selon un exemple de réalisation de la présente description. Ce procédé est par exemple mis en œuvre par le processeur 112 et par le contrôleur d'accès 106.

[0058] Le dispositif 100, et en particulier la mémoire 104, est alors sous tension et dans un mode de fonctionnement usuel. Le registre 116 contient alors l'indication du secteur étant courant, par exemple le secteur 120.

[0059] Dans une étape 301 (WRITE REQUEST), une requête d'écriture d'une valeur de donnée dans un des secteurs est initialisée par le processeur 112, la requête étant par exemple accompagnée d'une adresse mémoire. A titre d'exemple, préalablement à la requête d'écriture, le processeur 112 est configuré pour programmer en outre l'état du bit du registre 118 afin d'indiquer si l'écriture est à faire dans le secteur courant ou dans le secteur alternatif.

[0060] Dans une étape 302 (ALT_SEC=1 ?), le circuit de contrôle d'accès 106 est configuré pour lire le contenu du registre 118.

[0061] A titre d'exemple, si le bit contenu dans le registre 118 est dans l'état 0 (branche N), le procédé continue dans une suite d'étapes 303.

[0062] La suite d'étape 303 comprend une étape 304 (READ IN CURRENT SECTOR) dans laquelle le processeur 112 lit la donnée actuellement stockée dans le secteur courant à l'adresse mémoire indiquée lors de l'étape 301.

[0063] Dans une étape 305 (DATA=0 ?), le processeur 112 détermine si la donnée lue dans l'étape 304 est nulle, autrement dit si l'emplacement mémoire associé à l'adresse

indiquée dans l'étape 301 est vierge ou non. Dans le cas où l'emplacement n'est pas vierge (branche N), et par conséquent qu'une valeur de donnée est déjà stockée dans l'emplacement, le procédé continue dans une étape 306 (ERROR SIGNAL) dans laquelle le contrôleur d'accès 106 transmet par exemple un signal d'erreur au processeur 112. Le procédé se termine ensuite dans une étape 307 (END).

[0064] S'il est déterminé dans l'étape 305 que l'emplacement mémoire est vierge (branche Y), le procédé continue dans une étape 308 (WRITE IN CURRENT SECTOR) de la suite d'étape 303.

[0065] Dans l'étape 308, la valeur de donnée est écrite dans le secteur courant, et plus précisément, dans l'emplacement du secteur courant indiqué par l'adresse mémoire.

[0066] Si, dans l'étape 302, il est déterminé que le bit contenu dans le registre 118 a pour valeur 1 (branche Y), le procédé continue dans une suite d'étapes 309 similaire à la suite d'étapes 303 à la différence que les opérations se font dans le secteur alternatif.

[0067] Ainsi, la suite d'étape 309 comprend une étape 310 (READ IN ALTERNATE SECTOR), une étape 311 identique à l'étape 305 et une étape 312 (WRITE IN ALTERNATE SECTOR)

[0068] Suite à la réalisation de l'étape 308 ou 312, le procédé se termine à l'étape 307.

[0069] La [Fig.4] illustre de manière schématique le contenu des secteurs 120 et 122 de la mémoire 104 lors de la réalisation d'un procédé de modification d'une donnée.

[0070] A titre d'exemple, une valeur de sélection (SLT1) est stockée dans l'emplacement 126, la valeur de sélection désignant le secteur 120 comme étant le secteur courant.

[0071] Le secteur courant 120 comprend, par exemple, un nombre $N+1$, N étant un entier, de clefs, telles que des clefs OBK, désignées par KEY i , i étant compris entre 0 et N .

[0072] A titre d'exemple, la clef KEY K stockée dans un emplacement 400 en association avec une adresse mémoire est obsolète et doit être modifiée ou mise à jour. Cependant, la mémoire 104 étant une mémoire de type FLASH, il n'est pas possible de modifier la valeur de la clef KEY K de manière individuelle. En effet, il est uniquement possible d'écrire des valeurs dans des emplacements vierges du secteur, ou d'écraser dans son intégralité le contenu du secteur 120.

[0073] Selon un mode de réalisation, une nouvelle valeur de clefs est alors écrite dans un emplacement 402, associé à la même adresse que l'emplacement 400, du secteur alternatif 122. L'écriture de la nouvelle valeur dans le secteur alternatif est par exemple réalisée selon le procédé décrit en relation avec la [Fig.3].

[0074] La [Fig.5] est un organigramme représentant des opérations d'un procédé d'échange des secteurs. Plus particulièrement, l'organigramme illustré en [Fig.5] représente des opérations effectuées suite à une modification d'une donnée du secteur courant, tel que décrit en relation avec la [Fig.4]. Le procédé de la [Fig.5] est par exemple mis en œuvre par le processeur 112 et par le contrôleur d'accès 106.

- [0075] A titre d'exemple, une modification de la clef KEY K a été réalisée, comme décrit en relation avec la [Fig.4]. Le secteur courant 120 comprend alors les clefs KEY 0 à KEY N, dont la clef KEY K stockée dans l'emplacement 400. Le secteur courant 120 comprend en outre la valeur de sélection SLT1, stockée dans l'emplacement 126. Le secteur alternatif 122 comprend uniquement la modification de la clef KEY K, stockée dans l'emplacement 402, l'emplacement 402 étant désigné par une même adresse que l'emplacement 400.
- [0076] Suite au stockage de la modification de la clef KEY K dans l'emplacement 402, une requête d'échange de secteur est initiée dans une étape 501 (SWAP SECTOR REQUEST).
- [0077] Dans une étape 502 (ADDR INDEX=0), une valeur d'index, correspondant par exemple à une adresse désignant un emplacement mémoire, est initialisée. A titre d'exemple, dans cette étape, la valeur d'index correspond à l'adresse désignant l'emplacement mémoire du secteur 120 contenant la clef KEY 0.
- [0078] Dans une étape 503 (READ DATA @ADDR INDEX), le contenu de l'emplacement mémoire du secteur alternatif 122 et désigné par la valeur d'index est par exemple lu. Le processeur 112 détermine alors, dans une étape 504 (DATA=0) si l'emplacement mémoire du secteur alternatif associé à la valeur d'index est vierge. Si l'emplacement est bien vierge (branche Y) le procédé continue dans une étape 505 (COPY DATA) dans laquelle, par exemple, la clef KEY 0 est réécrite dans l'emplacement du secteur alternatif 122 associé à la valeur d'index.
- [0079] Si, lors de l'étape 504, il est déterminé que l'emplacement mémoire du secteur alternatif 122 désigné par la valeur d'index n'est pas vierge (branche N), le procédé saute directement à une étape 506 (INCREMENT ADDR INDEX).
- [0080] Dans l'étape 506 (INCREMENT ADDR INDEX), postérieure à l'étape 505, ou à l'étape 504 le cas échéant, la valeur d'index est incrémentée. A titre d'exemple, la valeur d'index correspond alors à l'adresse mémoire désignant l'emplacement de la clef KEY 1 dans le secteur courant 120.
- [0081] La succession des étapes 503 à 506 sera désignée dans la suite de la description comme étant une suite d'étapes 507.
- [0082] Dans une étape 508 (END ?), il est déterminé, par exemple en comparant la valeur d'index avec une valeur index limite, si des emplacements mémoire du secteur courant 120 restent à être parcourus. A titre d'exemple, la valeur d'index limite correspond à l'adresse désignant l'emplacement mémoire du secteur 120 dans lequel est stockée la clef KEY N. S'il reste des emplacements mémoire à parcourir (branche N), le procédé reprend à l'étape 503.
- [0083] A titre d'exemple, lorsque que, suite à une réalisation de l'étape 506 dans laquelle la valeur d'index est incrémentée vers la valeur d'index désignant l'emplacement

mémoire du secteur 122 dans lequel la modification de la clef KEY K a préalablement été stockée, l'emplacement sera vu comme non vierge lors de la réalisation de l'étape 504.

- [0084] Dans le cas où il est déterminé, lors de l'étape 508 qu'il ne reste plus d'emplacements à parcourir (branche Y), le procédé continue dans une étape 509 (SWAP THEN ERASE).
- [0085] A titre d'exemple, à cette étape du procédé, le secteur alternatif 122 comprend les clefs KEY 0 à KEY K-1 dans des emplacements mémoire 404, la modification de la clef KEY K dans l'emplacement 402 et les clefs KEY K+1 à KEY N dans des emplacements 406.
- [0086] Dans l'étape 509, une valeur de sélection, différente de la valeur de sélection stockée dans l'emplacement 126 du secteur 120, est stockée dans l'emplacement 128 du secteur 122. A titre d'exemple, lorsque la valeur de sélection SLT1 du secteur courant 120 est désignée par la valeur de comptage 0, 1 ou 2, la valeur de sélection stockée dans le secteur alternatif 122 sera respectivement 1, 2 ou 0.
- [0087] Suite au stockage de la nouvelle valeur de sélection, le secteur alternatif 122 devient le secteur courant, et le secteur courant 120 devient le secteur alternatif. L'intégralité du secteur alternatif 120 est alors effacée. Par conséquent, la valeur de sélection SLT1, dans l'emplacement 126, est également aussi effacée.
- [0088] L'avantage de supprimer le contenu du secteur alternatif 120 uniquement une fois que les valeurs de sélection ont été mises à jour est que la désignation des secteurs courant et alternatif est sauvegardée. Par conséquent, si le dispositif électronique 100 est éteint pour une raison quelconque avant ou pendant la suppression du secteur alternatif 120, au redémarrage, une lecture des valeurs de sélection des emplacements 126 et 128 est effectuée et permet d'identifier que le secteur 122 est le secteur courant.
- [0089] Dans certains cas, après la suppression de l'intégralité du secteur alternatif, le contenu des emplacements 126 et 128 est alors lu. Du fait que l'emplacement 126 est vierge, seule la valeur de sélection du secteur 122 est détectée, signifiant que le secteur 122 est maintenant le secteur courant de la mémoire 104. Le contenu du registre 116 est alors mis à jour, afin d'indiquer que le secteur courant est le secteur 122.
- [0090] Bien que la [Fig.5] représente un exemple dans lequel les données stockées dans les secteurs sont des clefs, le procédé pourrait s'appliquer à tout type de données.
- [0091] La [Fig.6] illustre de manière schématique le contenu des secteurs 120 et 122 de la mémoire 104 lors de la réalisation d'un procédé de suppression d'une ou plusieurs données.
- [0092] A titre d'exemple et de manière similaire à la [Fig.3], la valeur de sélection (SLT1) est stockée dans l'emplacement 126, la valeur de sélection désignant le secteur 120 comme étant le secteur courant.

- [0093] Le secteur courant 120 comprend, par exemple, les N+1 clefs OBK, désignées par KEY i, i étant compris entre 0 et N, les clefs KEY 0 à KEY K étant stockées dans des emplacements 602 et les clefs KEY K+1 à KEY N étant stockées dans des emplacements 604.
- [0094] A titre d'exemple, la suppression des clefs KEY K+1 à KEY N est commandée, par exemple par le contrôleur 106. Cependant, la mémoire 104 étant une mémoire de type FLASH, il n'est pas possible de supprimer les clefs KEY K+1 à KEY N de manière individuelle sans supprimer l'intégralité du secteur 120 et par conséquent les clefs KEY 0 à KEY K.
- [0095] Selon un mode de réalisation, les valeurs de clefs KEY 0 à KEY K sont alors réécrites dans des emplacements 606 du secteur alternatif 122. Les emplacements 606 sont alors désignés par les mêmes adresses que celles désignant les emplacements 602.
- [0096] La [Fig.7] est un organigramme représentant des opérations d'un procédé de suppression d'une ou plusieurs données comprises dans la mémoire 104, et plus particulièrement de données comprises dans le secteur courant. Le procédé de la [Fig.7] est par exemple mis en œuvre par le processeur 112 et par le contrôleur d'accès 106.
- [0097] A titre d'exemple, comme décrit en relation avec la [Fig.6], le secteur courant 120 comprend les clefs KEY 0 à KEY K, stockées dans des emplacements 602 du secteur courant et les clefs KEY K+1 à KEY N stockées dans des emplacements 604 du secteur courant. Le secteur courant 120 comprend en outre la valeur de sélection SLT1, stockée dans l'emplacement 126. Le secteur alternatif 122 est alors vide, c'est à dire que tous les emplacements mémoire le composant sont vides.
- [0098] Une requête de suppression des clefs KEY K+1 à KEY N et d'échange de secteur est initiée dans une étape 701 (SWAP SECTOR REQUEST).
- [0099] Dans une étape 702 ($K \geq 0$?), un nombre K+1 de valeurs de donnée à réécrire dans le secteur alternatif 122 est désigné. Le nombre K+1 correspond à un nombre de données du secteur courant à transférer dans le secteur alternatif avant de procéder à l'échange entre le secteur courant et le secteur alternatif. A titre d'exemple, le nombre de valeurs de donnée à réécrire correspond au nombre de clefs composant l'ensemble des clefs KEY 0 à KEY K, les clefs KEY K+1 à KEY N étant vouées à être supprimées. Si au moins une valeur de donnée est à réécrire (branche Y), le procédé continue dans une étape 703 (ADDR INDEX=0).
- [0100] Dans l'étape 703, une valeur d'index, correspondant par exemple à une adresse désignant un emplacement mémoire, est initialisée. A titre d'exemple, dans cette étape, la valeur d'index correspond à l'adresse désignant l'emplacement mémoire du secteur 120 contenant la clef KEY 0.
- [0101] Suite à l'étape 703, le procédé continue dans la suite d'étapes 507 dans lesquelles le contenu de l'emplacement mémoire du secteur 120 et désigné par la valeur d'index est

réécrit dans l'emplacement mémoire du secteur 122 et désigné par la même valeur d'index, sous condition que ce dernier soit vierge. A titre d'exemple, la valeur de la clef KEY 0 est écrite dans le secteur 122 lors de ces étapes. La valeur d'index est ensuite incrémentée.

- [0102] Suite aux étapes de la suite 507, le procédé continue dans une étape 704 (ADDR INDEX=K+1) dans laquelle il est déterminé si toutes les valeurs à réécrire dans le secteur 122 ont été réécrites, ce qui est par exemple le cas si la valeur d'index est égale à K+1. Si non, le procédé reprend aux étapes 507, dans lesquelles, par exemple, la valeur de la clef KEY 1 est écrite dans le secteur 122.
- [0103] Si, suite à l'étape 704, il est déterminé que toutes les valeurs à réécrire ont été réécrites (branche Y), le procédé continue dans une étape 705 (SWAP AND ERASE) identique à l'étape 509 décrite en relation avec la [Fig.5]. L'étape 705 fait également suite à l'étape 702 lorsqu'il est déterminé qu'aucune valeur de données ne sont à réécrire dans le secteur 122 (branche N).
- [0104] A titre d'exemple, les valeurs de chacune des clefs KEY 0 à KEY K ont été réécrites dans le secteur 122. Une valeur de sélection, différente de la valeur SLT1, est alors stockée dans l'emplacement 128 du secteur 122 et l'intégralité du secteur 120 est effacée. Ainsi, les clefs KEY K+1 à KEY N ne sont plus stockées dans les secteurs 120 et 122, elles sont ainsi supprimées de la mémoire 104.
- [0105] Le procédé se termine ensuite dans une étape 706 (END).
- [0106] Comme dans le procédé décrit en relation avec la [Fig.5], l'avantage de supprimer, dans l'étape 705, le secteur alternatif 120 uniquement une fois que les valeurs de sélection ont été mises à jour est que la désignation des secteurs courant et alternatif est sauvegardée. Par conséquent, si le dispositif électronique 100 est éteint pour une raison quelconque avant ou pendant la suppression du secteur alternatif 120, au redémarrage, une lecture des valeurs de sélection des emplacements 126 et 128 est effectuée et permet d'identifier que le secteur 122 est le secteur courant.
- [0107] Bien que la [Fig.7] représente un exemple dans lequel les données stockées dans les emplacements des secteurs sont des clefs, le procédé pourrait s'appliquer à tout type de données.
- [0108] La [Fig.8] illustre, de façon schématique et sous forme de blocs, un exemple de réalisation de la mémoire 104 selon un mode de réalisation de la présente description.
- [0109] La [Fig.8] illustre différentes zones de stockage dans les secteurs 120 et 122. Outre les emplacements 126 et 128 réservés au stockage des valeurs de sélection, chaque secteur 120 et 122 comprend par exemple 5 zones.
- [0110] A titre d'exemple, le secteur 120 comprend des zones 800 à 804 et le secteur 122 comprend des zones 800' à 804'. Chacune des zones est associée à une valeur de niveau TIL (de l'anglais « Temporal Isolation Level »). Par exemple, à chaque

démarrage du dispositif 100, une valeur de niveau est générée par le compteur monotone 110. La valeur de niveau est par exemple transmise au contrôleur 106. Ainsi un accès à une zone associée par exemple à une valeur de niveau de TIL inférieure à la valeur de niveau générée par le compteur 110 est interdit par le contrôleur 106.

- [0111] A titre d'exemple, des zones 800 et 800' (TIL 0) sont associées à la valeur de niveau de TIL 0 et leur accès est autorisé uniquement lorsque la valeur de niveau générée par le compteur monotone 110 est égale à 0. De même, des zones 801 et 801' (TIL 1) sont associées à la valeur de TIL 1 et sont accessibles par exemple uniquement lorsque la valeur de niveau est égale à 1. Dans un autre exemple, les zones 801 et 801' sont accessibles lorsque la valeur de niveau générée est inférieure ou égale à 1. De manière similaire, des zones 802 et 802' (TIL2) sont associées à la valeur de TIL 2 et des zones 803, 803' (TIL3SEC) et 804, 804' (TIL3NSEC) sont associées à la valeur de TIL 3.
- [0112] A titre d'exemple, le contrôleur 106 est en outre configuré pour commander la suppression du contenu d'une ou plusieurs zones lorsque le compteur monotone 110 incrémente la valeur de niveau. A titre d'exemple, la valeur de niveau est incrémentée de 0 vers la valeur 1, et le contenu de la zone 800 ou 800' associée à la valeur de TIL 0 du secteur courant est supprimé selon le mode de réalisation décrit en relation avec les figures 6 et 7. De même, le contenu des zones associées aux autres valeurs de TIL est par exemple supprimé lorsque la valeur de niveau est incrémentée vers une valeur étant supérieure à la valeur de TIL associée auxdites zones.
- [0113] La [Fig.9] illustre, de façon schématique, une fonction de contrôle d'accès à la mémoire 104, et en particulier au secteur courant de la mémoire 104.
- [0114] A titre d'exemple, la fonction de contrôle d'accès est implémentée par le contrôleur d'accès 106.
- [0115] A titre d'exemple, on considère le cas où le secteur courant est le secteur 120. Le secteur 120 comprend par exemple les 5 zones 800 à 804 décrites en relation avec la [Fig.8].
- [0116] Le contrôleur d'accès 106 est alors configuré pour recevoir la valeur de niveau (TIL) générée par le compteur monotone 110. A titre d'exemple, le contrôleur d'accès 106 est en outre configuré pour interdire l'accès à une ou plusieurs zones parmi les zones 800 à 804 sur la base de la valeur de niveau TIL reçue. A titre d'exemple, le contrôleur d'accès 106 est configuré pour interdire tout accès aux zones étant associées à une valeur de TIL strictement inférieure à la valeur de niveau reçue. Dans un autre exemple, le contrôleur d'accès 106 est configuré pour interdire tout accès aux zones étant associées à une valeur de niveau TIL différente de la valeur de niveau TIL reçue.
- [0117] A titre d'exemple, le contrôleur d'accès 106 est en outre configuré pour recevoir le signal SEC/NSEC, indiquant un fonctionnement du circuit intégré 102 dans un mode sécurisé (SEC) ou non sécurisé (NSEC). A titre d'exemple, le contrôleur d'accès 106

est configuré pour autoriser l'accès à la zone 804 et interdire l'accès à la zone 803 lorsque que circuit 102 est dans le mode non sécurisé.

- [0118] A titre d'exemple, le contrôleur d'accès 106 est en outre configuré pour recevoir le signal TZ, étant par exemple un signal indiquant un fonctionnement du circuit intégré 102 dans un mode sécurisé avec un domaine de confiance. A titre d'exemple, le contrôleur d'accès 106 est configuré pour autoriser l'accès à toutes les zones 800 à 804 lorsque que le signal TZ est reçu, et ce même lorsque la valeur de niveau générée par le compteur monotone 110 ne le permet pas.
- [0119] La [Fig.10] est un organigramme représentant des opérations suite à la mise sous tension du circuit 102.
- [0120] Le dispositif est mis sous tension dans une étape 1001 (BOOTING). Suite à l'étape 1001, le contenu des emplacements 126 et 128 est lu, par exemple par le processeur 112, dans une étape 1002 (LECTURE OF SELECTORS).
- [0121] Suite à l'étape 1002, le procédé continue dans une étape 1003 (VALUES IN BOTH SELECTORS ?), dans laquelle il est déterminé si les deux emplacements 126 et 128 comprend une valeur de sélection, c'est-à-dire qu'un ou l'autre des deux emplacements 126 et 128 n'est pas vierge. Dans le cas où uniquement un seul des deux emplacements comprend une valeur de sélection (branche N), (par exemple la valeur SLT2 dans l'emplacement 128, l'emplacement 126 étant vierge), le procédé continue dans une étape 1004 (DETERMINATION OF CURRENT SECTOR AND UPDATE REGISTER). Dans l'étape 1004, le secteur dont l'emplacement contient une valeur de sélection, par exemple le secteur 122, est déterminé comme étant le secteur courant. De plus, l'indication contenue dans le registre 116 est mise à jour dans l'étape 1004.
- [0122] Le procédé se termine ensuite dans une étape 1005 (END).
- [0123] Si, lors de l'étape 1003, une valeur de sélection est lue dans chacun des emplacements 126 et 128 (branche Y), c'est-à-dire que ni l'emplacement 126, ni l'emplacement 128 ne sont vierges, le procédé continue dans une étape 1006 (DETERMINATION OF CURRENT SECTOR AND UPDATE REGISTER).
- [0124] Lorsque les deux emplacements 126 et 128 contiennent chacun une valeur de sélection suite à une mise sous tension de la mémoire 104, cela traduit que la mémoire 104 est passée hors tension lors d'une réalisation de l'étape 509, ou lors d'une réalisation de l'étape 705. En effet, dans ce cas, suite à la modification ou suppression d'une ou plusieurs données du secteur courant, une nouvelle valeur de sélection est stockée dans l'emplacement du secteur alternatif avant l'effacement complet du secteur alternatif. Si, pour une quelconque raison, la mémoire 104 n'est plus alimentée après le stockage de la nouvelle valeur de sélection mais avant l'effacement du secteur courant, les deux valeurs SLT1 et SLT2, sont stockées dans les emplacements 126 et 128.
- [0125] Dans l'étape 1006, une règle est appliquée afin de déterminer quel secteur est le

secteur courant. A titre d'exemple, la règle appliquée est celle décrite en relation avec la [Fig.1].

- [0126] A titre d'exemple, lors d'une réalisation de l'étape 509 du procédé de la [Fig.5] ou lors d'une réalisation de l'étape 705 du procédé de la [Fig.7], la valeur de sélection du secteur alternatif 122 est programmée avec la valeur de comptage, correspondant à la valeur de comptage programmant la valeur de sélection du secteur courant. A titre d'exemple, si la valeur de comptage programmant la valeur de sélection du secteur courant 120 est la valeur 0, la nouvelle valeur, stockée dans l'emplacement 128 du secteur alternatif 122, sera programmée avec la valeur 1. De même la nouvelle valeur de sélection sera programmée avec la valeur 2 si la valeur du secteur courant 120 est programmée avec la valeur 1. La nouvelle valeur de sélection sera programmée avec la valeur 0 si la valeur de sélection du secteur courant 120 est programmée avec la valeur 2. Lors de la lecture des valeurs de sélection, le secteur 122 sera alors désigné comme étant le secteur courant.
- [0127] Une fois le secteur courant déterminé, l'indication du secteur courant contenue dans le registre 116 est mise à jour.
- [0128] Les anciennes valeurs de données, par exemple les clefs KEY 0 à KEY N, étant toujours stockées dans le secteur désigné alors comme alternatif, ce secteur est ré-initialisé dans une étape 1007 (REINITIALIZATION OF ALTERNATE SECTOR). Le contenu du secteur alternatif, par exemple le secteur 120, est par exemple intégralement effacé. Par conséquent, le secteur alternatif ne contient plus de valeur de sélection.
- [0129] Le procédé se termine ensuite dans l'étape 1005.
- [0130] Un avantage des modes de réalisation décrits est qu'ils permettent de modifier ou de supprimer partiellement le contenu d'une mémoire de type FLASH.
- [0131] Un autre avantage des modes de réalisation décrits est qu'il est possible, par l'intermédiaire d'un logiciel, de choisir dans quel secteur, courant ou alternatif, écrire une ou plusieurs valeurs de données.
- [0132] Un autre avantage des modes de réalisation décrits est que l'accès à la mémoire 104, et en particulier à différentes zones comprises dans les secteurs 120 et 122, est contrôlé par l'incréméntation du compteur monotone 110, ce qui améliore la sécurité des données.
- [0133] Un autre avantage des modes de réalisation décrits est que le contenu des emplacements 126 et 128 permettant de déterminer quel secteur est le secteur courant est uniquement accessible par un circuit matériel.
- [0134] Un autre avantage des modes de réalisation décrits est qu'une indication de quel secteur est le secteur courant est chargée dans un registre 116 du circuit à chaque mise sous tension de la mémoire 104 et suite à une lecture du contenu des emplacement 126

et 128.

- [0135] Divers modes de réalisation et variantes ont été décrits. La personne du métier comprendra que certaines caractéristiques de ces divers modes de réalisation et variantes pourraient être combinées, et d'autres variantes apparaîtront à la personne du métier. En particulier, le choix des valeurs que peuvent prendre les valeurs de sélection est à la portée de la personne du métier. De même, le choix de la règle permettant de déterminer, à partir des valeurs de sélection, quel est le secteur courant et quel est le secteur alternatif est à la portée de la personne du métier.
- [0136] Enfin, la mise en œuvre pratique des modes de réalisation et variantes décrits est à la portée de la personne du métier à partir des indications fonctionnelles données ci-dessus. En particulier, pour ce qui est de l'implémentation du contrôleur d'accès.

Revendications

- [Revendication 1] Procédé comprenant :
- la modification ou suppression d'une ou plusieurs valeurs de donnée d'une mémoire non volatile (104), l'une ou plusieurs valeurs de donnée étant stockées dans un premier secteur (120, 122) de la mémoire, le premier secteur étant désigné comme secteur courant par une ou plusieurs valeurs de sélection (SLT1, SLT2) stockées dans la mémoire non volatile, la modification ou suppression comprenant :
- l'écriture d'une ou plusieurs valeurs de donnée (KEY 0, KEY K-1, KEY K, KEY K+1, KEY N), stockées dans le premier secteur (120), dans un deuxième secteur (122, 120) de la mémoire non volatile, le deuxième secteur étant désigné comme secteur alternatif par l'une ou plusieurs valeurs de sélection.
- [Revendication 2] Procédé selon l'une quelconque des revendications 1, dans lequel la modification ou suppression comprend la modification d'une première valeur de donnée (KEY K) stockée dans un premier emplacement (400), en association avec une première adresse, du premier secteur (120) de la mémoire, et l'écriture de l'une ou plusieurs valeurs de donnée dans le deuxième secteur (122) comprend :
- l'écriture d'une deuxième valeur de donnée dans un premier emplacement (402) du deuxième secteur de la mémoire non volatile, le premier emplacement du deuxième secteur étant désigné au moins en partie par la première adresse.
- [Revendication 3] Procédé selon la revendication 1 ou 2, dans lequel l'une ou plusieurs valeurs de sélection (SLT1, SLT2) comprend une première valeur de sélection (SLT1) stockée dans le premier secteur (120).
- [Revendication 4] Procédé selon la revendication 3 dans lequel, l'une ou plusieurs valeurs de sélection (SLT1, SLT2) comprend en outre une deuxième valeur de sélection (SLT2) stockée dans le deuxième secteur (122).
- [Revendication 5] Procédé selon la revendication 4, comprenant, suite à une mise sous tension de la mémoire non volatile (104) :
- la lecture des première et deuxième valeurs de sélection (SLT1, SLT2) ;
 - la détermination, sur la base des première et deuxième valeurs de sélection, du secteur (120, 122) désigné comme alternatif ; et
 - si au moins une valeur de donnée est contenue dans le secteur désigné comme secteur alternatif, la réinitialisation du secteur alternatif.

- [Revendication 6] Procédé selon l'une quelconque des revendications 1 à 5, dans lequel la modification ou suppression comprend une suppression d'autres premières valeurs de données (KEY K+1, KEY N), et le premier secteur (120) comprend une première plage d'adresses (604, 800, 801, 802) comprenant les autres premières valeurs de données associées à une première valeur de niveau (TIL) ainsi qu'une deuxième plage d'adresses (602, 801, 802, 803, 804) comprenant des deuxième valeurs de données (KEY 0, KEY K) associées à une deuxième valeur de niveau, la deuxième valeur de niveau étant strictement supérieure à la première valeur de niveau et dans lequel la suppression comprend :
- la génération de la deuxième valeur de niveau par un compteur monotone (110) ;
 - l'écriture des deuxième valeurs de données en association avec la première valeur de comptage dans le deuxième secteur (122) ;
 - l'écriture d'une deuxième valeur de sélection (SLT2) dans le deuxième secteur, rendant le premier secteur alternatif et le deuxième secteur courant ; et
 - la réinitialisation du premier secteur.
- [Revendication 7] Procédé selon la revendication 1 ou 2, comprenant en outre :
- l'écriture d'une deuxième valeur de sélection (SLT2) dans le deuxième secteur (122), rendant le premier secteur (120) alternatif et le deuxième secteur courant ; et
 - la réinitialisation du premier secteur.
- [Revendication 8] Procédé selon l'une quelconque des revendications 1 à 7, comprenant en outre, suite à l'écriture desdites une ou plusieurs autres valeurs de donnée (KEY 0, KEY K-1, KEY K, KEY K+1, KEY N) dans le deuxième secteur (122), la modification ou suppression d'une ou plusieurs des valeurs stockées dans le deuxième secteur et, l'écriture d'une troisième valeur de sélection, différente des première et deuxième valeurs de sélection (SLT1, SLT2), dans le premier secteur (120), rendant le premier secteur courant et le deuxième secteur alternatif.
- [Revendication 9] Procédé selon la revendication 8, dans lequel chacune des première, deuxième et troisième valeurs de sélection ont au moins les valeurs de deux bits différentes des autres valeurs de sélection.
- [Revendication 10] Procédé selon l'une quelconque des revendications 1 à 9, comprenant en outre :
- la lecture de l'état d'un bit stocké dans un registre (116) ; et
 - l'écriture d'une ou plusieurs valeurs de données dans le secteur courant

(120, 122) lorsque le bit est dans un premier état, ou l'écriture de l'une ou plusieurs valeurs de données dans le secteur alternatif (122, 120) lorsque le bit est dans un deuxième état.

[Revendication 11] Procédé selon l'une quelconque des revendications 1 à 10, dans lequel la mémoire non volatile (104) est une mémoire de type FLASH.

[Revendication 12] Dispositif comprenant :

- une mémoire non volatile (100) comprenant une ou plusieurs valeurs de donnée, stockées dans un premier secteur (120, 122) de la mémoire, la mémoire comprenant en outre un deuxième secteur (122, 120) ainsi qu'une ou plusieurs valeurs de sélection (SLT1, SLT2) désignant le premier secteur comme secteur courant et désignant le deuxième secteur comme secteur alternatif ; et
- un contrôleur d'accès (106) configuré pour modifier ou supprimer l'une ou plusieurs valeurs de données en écrivant une ou plusieurs autres valeurs de donnée (KEY 0, KEY K-1, KEY K, KEY K+1, KEY N), stockées dans le premier secteur (120), dans le deuxième secteur de la mémoire non volatile.

[Revendication 13] Dispositif selon la revendication 12 dans lequel le contrôleur d'accès (106) est configuré pour modifier une première valeur de donnée (KEY K) stockée dans un premier emplacement (400) du premier secteur de la mémoire, en association avec une première adresse, est modifié en écrivant une deuxième valeur de donnée dans un premier emplacement (402) du deuxième secteur de la mémoire non volatile, le premier emplacement du deuxième secteur étant désigné au moins en partie par la première adresse.

[Revendication 14] Dispositif selon la revendication 12 ou 13, comprenant en outre un compteur monotone (110) configuré pour générer une valeur de niveau (TIL), et dans lequel le premier secteur (120 122) comprend une première plage d'adresses (604, 800, 801, 802) comprenant des autres premières valeurs de données associées à une première valeur de niveau, ainsi qu'une deuxième plage d'adresses comprenant des deuxièmes valeurs de donnée (602, 801, 802, 803, 804) associées à une deuxième valeur de niveau, la deuxième valeur de niveau étant strictement supérieure à la première valeur de niveau, le contrôleur d'accès (106) étant configuré pour supprimer l'une ou plusieurs autres premières valeurs de données, la suppression comprenant :

- l'écriture des deuxièmes valeurs de données en association avec la première valeur de comptage dans le deuxième secteur (122, 120) ;

- l'écriture d'une deuxième valeur de sélection (SLT2, SLT1), rendant le premier secteur alternatif et le deuxième secteur courant ; et
- la réinitialisation du premier secteur.

[Fig. 1]

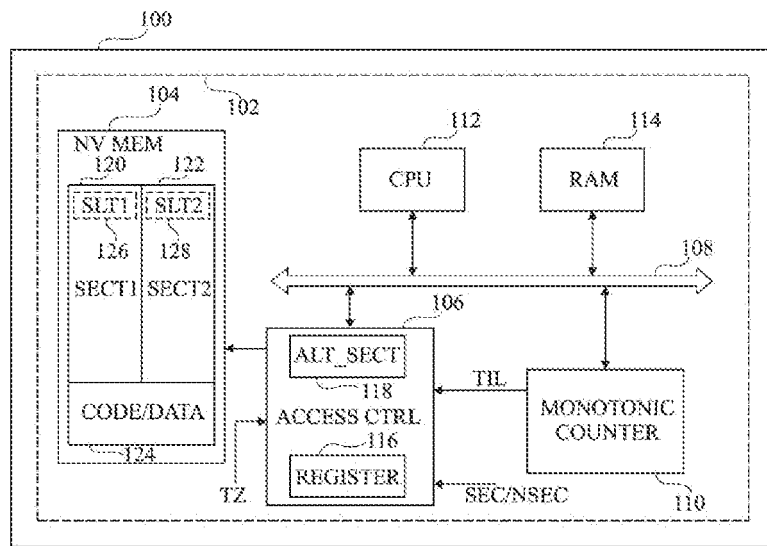


Fig 1

[Fig. 2]

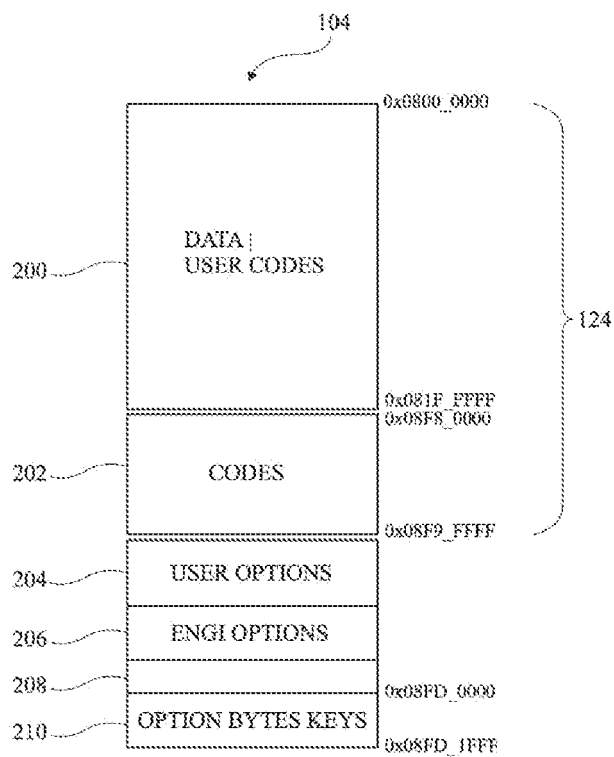


Fig 2

[Fig. 3]

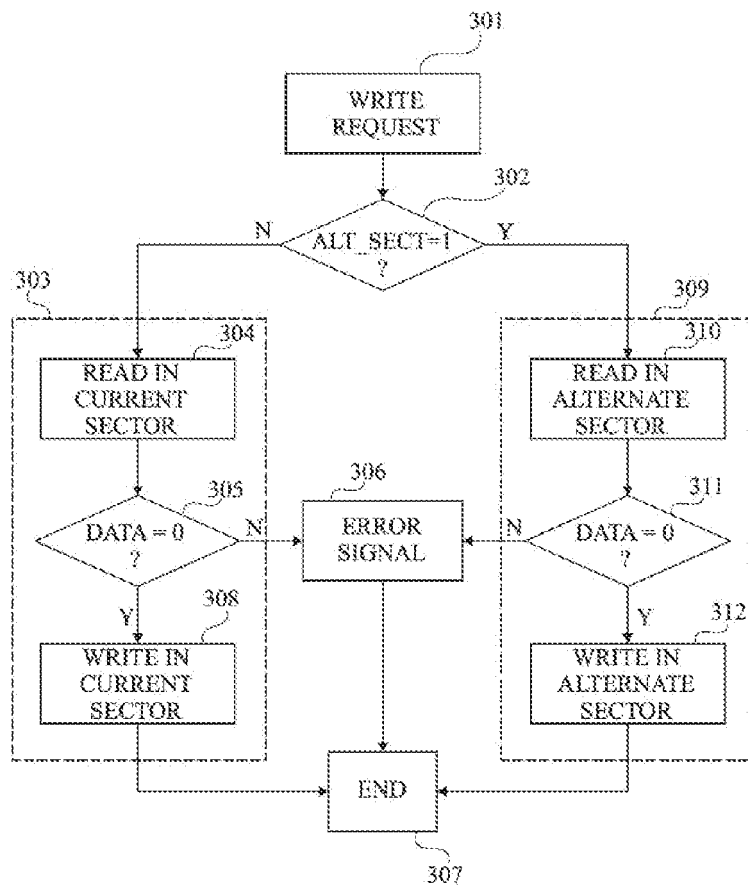


Fig 3

[Fig. 4]

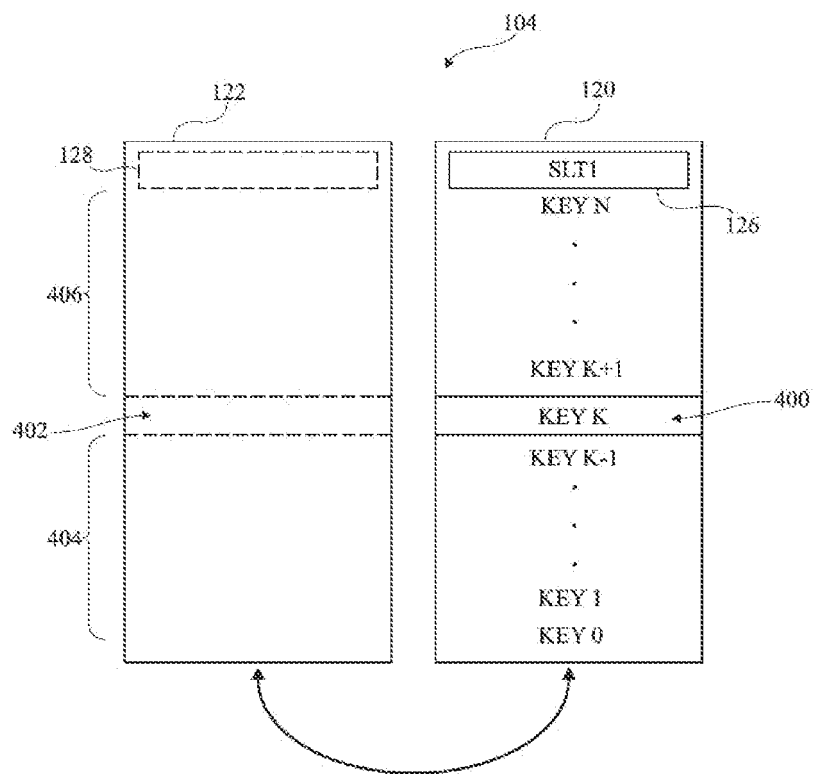


Fig 4

[Fig. 5]

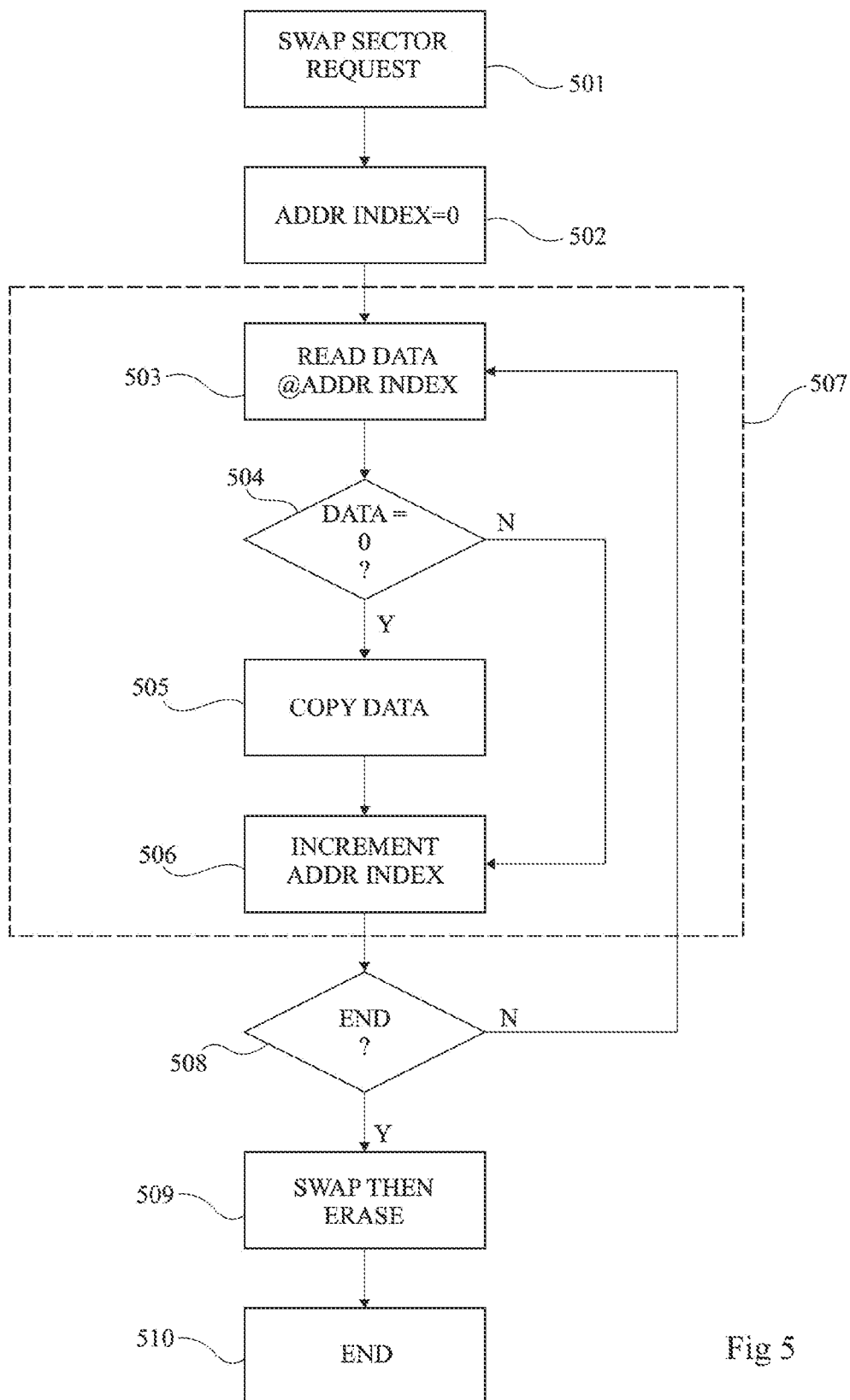


Fig 5

[Fig. 6]

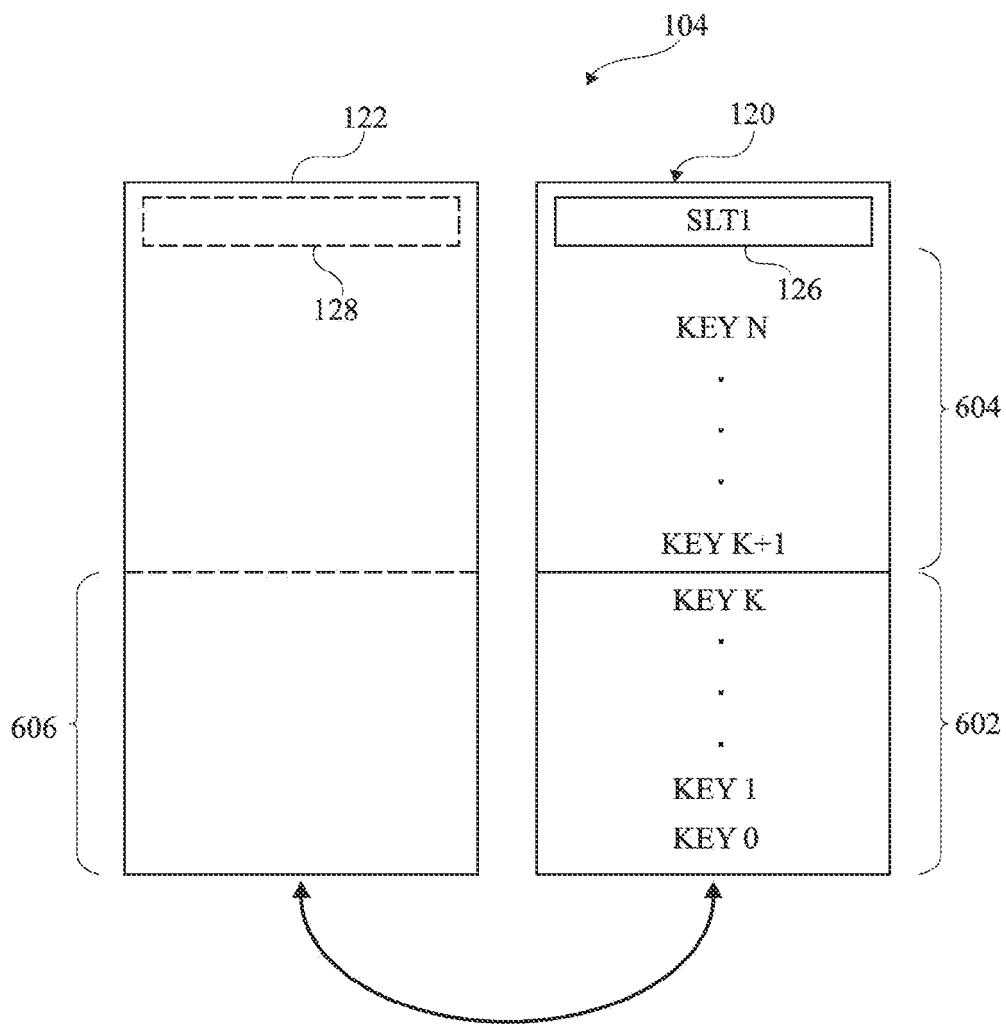


Fig 6

[Fig. 7]

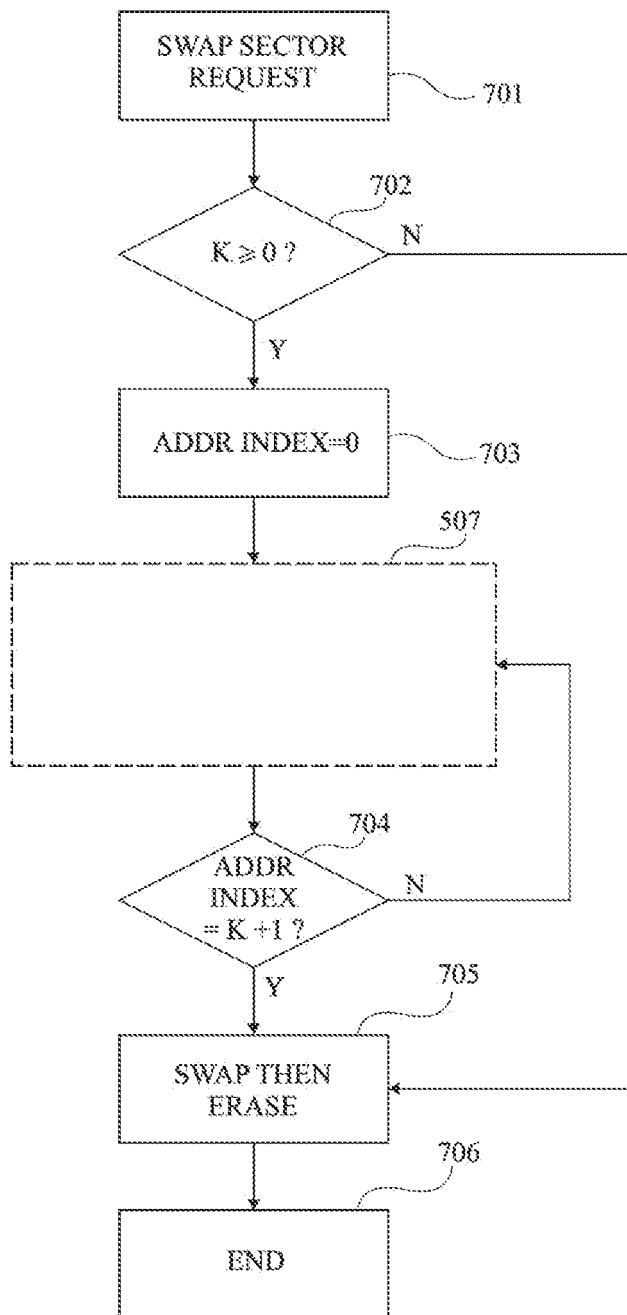


Fig 7

[Fig. 8]

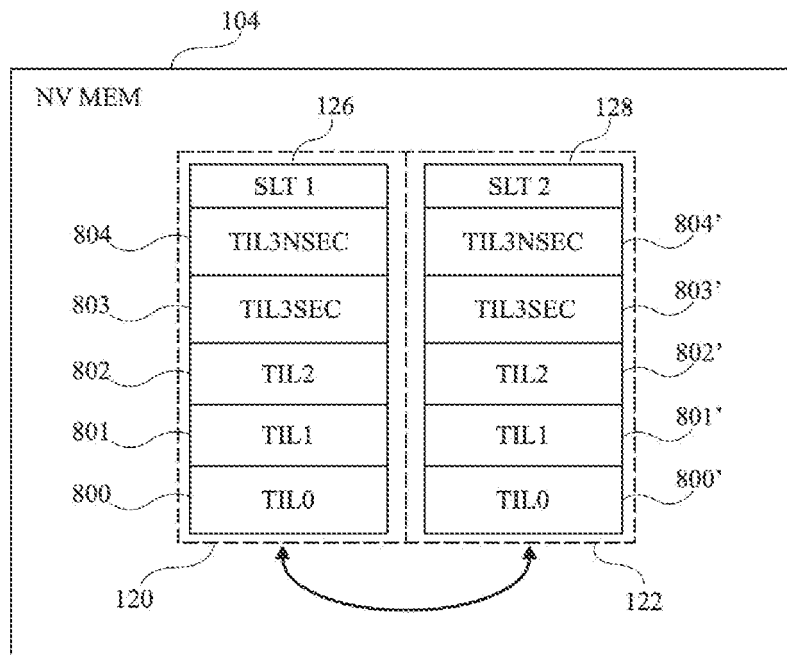


Fig 8

[Fig. 9]

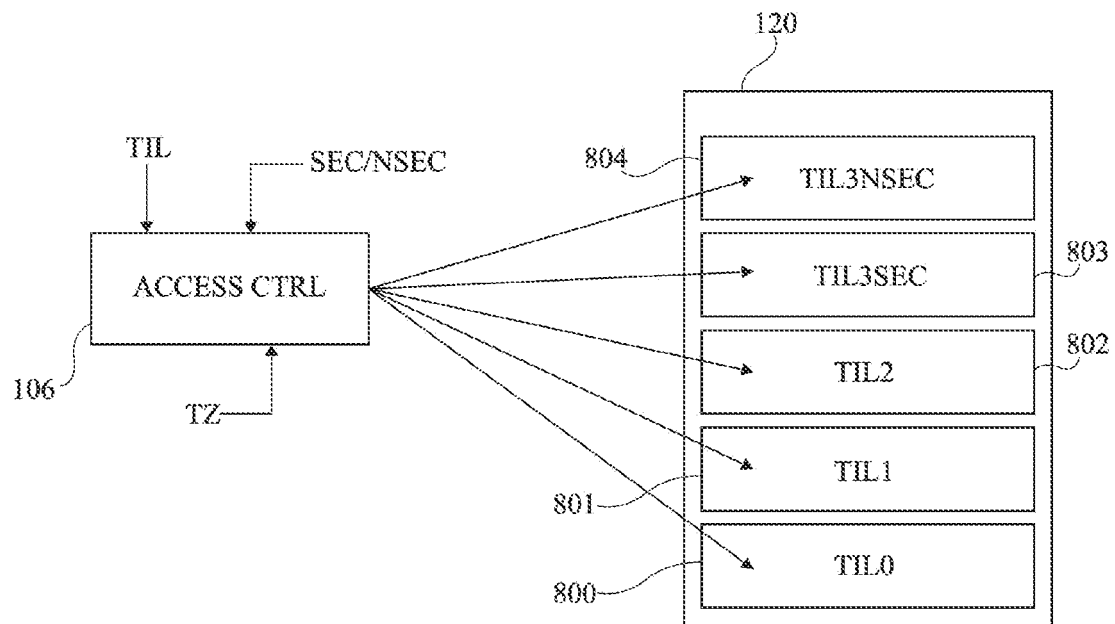


Fig 9

[Fig. 10]

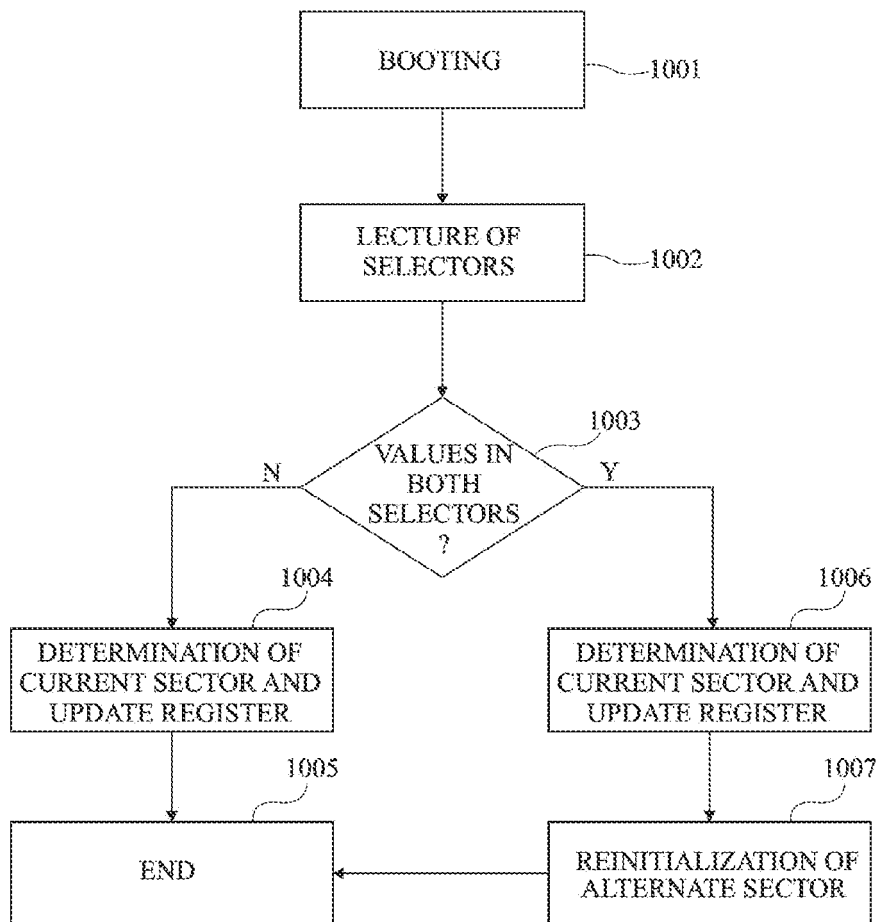


Fig 10

RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveau) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.

Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

☒ Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

☒ Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

☐ Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

☒ Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

**1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN
CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION**

NEANT

**2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN
TECHNOLOGIQUE GENERAL**

WO 2009/088709 A2 (SANDISK IL LTD [IL];
NOCHIMOWSKI ALAIN [IL] ET AL.)
16 juillet 2009 (2009-07-16)

US 2020/089894 A1 (LIU MING-YING [TW] ET
AL) 19 mars 2020 (2020-03-19)

US 2021/034355 A1 (MONTERO ADOLFO S [US]
ET AL) 4 février 2021 (2021-02-04)

**3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND
DE LA VALIDITE DES PRIORITES**

NEANT