(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 025 041**

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

(21) **N° d'enregistrement national :** **15 57759**

(51) Int Cl[8] : ***G 06 F 21/62*** *(2016.01), G 11 C 11/34*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 17.08.15.

(30) **Priorité :** 25.08.14 US 14467724.

(43) **Date de mise à la disposition du public de la demande :** 26.02.16 Bulletin 16/08.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

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

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *HGST NETHERLANDS B.V.* — NL.

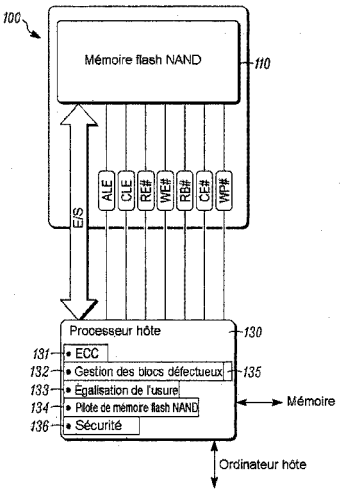
(72) **Inventeur(s) :** GERHART DARIN EDWARD, LAPPI CORY, LIPPS DANIEL ROBERT et WALKER WILLIAM JARED.

(73) **Titulaire(s) :** HGST NETHERLANDS B.V..

(74) **Mandataire(s) :** IPSILON - FERAY LENNE CONSEIL Société à responsabilité limitée.

(54) Procédé et appareil pour générer un contenu de zéros sur des données inutiles lorsque des paramètres de chiffrement sont modifiés.

(57) Dispositif de mémoire comprenant au moins un emplacement de mémoire pour stocker des informations représentant des données écrites au moyen d'un premier procédé de chiffrement/déchiffrement, et un canal de lecture utilisant un second procédé de chiffrement/déchiffrement pour chiffrer et déchiffrer les informations telles qu'écrites. Le dispositif de mémoire comprend également un appareil qui empêche la lecture de l'au moins un emplacement de mémoire au moyen du second procédé de chiffrement/déchiffrement, en réponse à une indication que l'au moins un emplacement de mémoire a été écrit au moyen du premier procédé de chiffrement/déchiffrement. Dans un autre mode de réalisation, une lecture de tous les zéros est retournée en réponse à une indication d'un autre procédé de chiffrement/déchiffrement.



FR 3 025 041 - A1

PROCÉDÉ ET APPAREIL POUR GÉNÉRER UN CONTENU DE ZÉROS SUR DES DONNÉES INUTILES LORSQUE DES PARAMÈTRES DE CHIFFREMENT SONT MODIFIÉS

DOMAINE TECHNIQUE

Les différents modes de réalisation décrits ici concernent un procédé et un appareil qui sont utilisés pour empêcher la génération de données inutiles après que certains paramètres associés aux données, tels qu'un paramètre de chiffrement, ont été modifiés.

CONTEXTE

Le stockage de données comprend d'écrire des informations représentant les données sur un périphérique ou un appareil de stockage. Il existe de nombreux types de périphériques de stockage. Même s'ils sont très variés, la plupart des périphériques de stockage ont des objectifs communs. Parmi ces objectifs, certains consistent à stocker des quantités accrues de données, et à fournir un moyen d'assurer que les données ainsi stockées sont en sécurité. Le chiffrement est une façon de rendre les données sures. Le chiffrement est le processus comprenant de coder les informations de manière à ce que seules les parties autorisées puissent les lire. Le chiffrement n'empêche pas le piratage, mais il réduit la probabilité que le pirate sera en mesure de lire les données chiffrées. Dans un schéma de chiffrement, l'information, appelée texte en clair, est chiffrée au moyen d'un algorithme de chiffrement, transformant celle-ci en un texte chiffré illisible. Cela se fait habituellement à l'aide d'une clé de chiffrement qui spécifie la façon dont le message doit être codé. Tout antagoniste qui peut voir le texte chiffré ne devrait pas être en mesure de déterminer quoi que ce soit concernant l'information originale. Une partie autorisée, cependant, est en mesure de décoder le cryptogramme au moyen d'un algorithme de déchiffrement, qui nécessite habituellement une clé secrète de déchiffrement, à laquelle les antagonistes n'ont pas accès. Pour des raisons techniques, un schéma de chiffrement nécessite généralement un algorithme de génération de clé pour produire des clés de manière aléatoire.

De temps en temps, des paramètres de chiffrement, tels que des clés de chiffrement/déchiffrement, peuvent être modifiés pour un dispositif de stockage. Lorsque les paramètres de chiffrement sont modifiés, tels qu'une clé ou un paramètre d'étendu, il est possible d'avoir des données inutiles avec des erreurs de contrôle de redondance cyclique (« CRC ») dans l'espace d'adresse de bloc logique (« LBA ») du changement.

Actuellement, une solution pour prévenir les erreurs CRC consiste à désactiver toute protection des données sur les lecteurs chiffrés. Cette situation expose les données. Les données ne sont pas en sécurité lorsque le système de protection des données est désactivé. Bien sûr, cette solution est loin de satisfaire certaines normes de sécurité des données. De nombreux fabricants qui utilisent des périphériques de stockage dans les produits qu'ils offrent qualifient les périphériques de stockage sur la base de la conformité avec les normes. La désactivation de la fonction de sécurité empêche la protection des données T10 appropriée sur les périphériques de stockage chiffrés. Une autre norme doit se conformer à la norme Opal SSC. La norme énonce les points suivants :

« Une mémoire SD compatible Opal SSC DOIT mettre en œuvre un plein chiffrage de disque pour toutes les données d'utilisateur accessibles hôtes stockées sur le support. Les standards AES-128 ou AES-256 DOIVENT être supportés [Paragraphe 2.4, page 10 sur 81 de la TCG Storage Opal SSC, version 1.0. »

« Opal SSC est un profil de mise en œuvre pour les périphériques de stockage conçu pour :

• protéger la confidentialité des données d'utilisateur stockées vis-à-vis des accès non autorisés une fois qu'elles ne sont plus sous le contrôle du propriétaire (ce qui implique un cycle de mise sous tension et de fin d'authentification subséquente)

• permettre l'interopérabilité entre plusieurs fournisseurs de mémoire SD

« Une SD compatible Opal SSC :

• facilite l'accessibilité aux fonctionnalités

• fournit des fonctionnalités définissables par l'utilisateur (par exemple, le contrôle d'accès, des plages de verrouillage, les mots de passe utilisateur, etc.)

• prendre en charge des comportements uniques d'Opal SSC (par exemple, la communication, la gestion de table) [Section 2.1, page 10/81]

Si les données sont tout le temps en sécurité, la confidentialité des données utilisateur stockées est protégée contre les accès non autorisés une fois qu'elles sortent du contrôle du propriétaire. En outre, satisfaire à une norme pour la sécurité des données sur un appareil de stockage permet l'interopérabilité entre plusieurs fournisseurs de périphériques de stockage. Satisfaire à une norme facilite également l'accessibilité aux fonctionnalités, offre des fonctionnalités définissables par l'utilisateur (par exemple, le contrôle d'accès, les plages de verrouillage, les mots de passe d'utilisateur, etc.) et supporte des comportements uniques (par exemple, la communication, la gestion de table).

RÉSUMÉ DE L'INVENTION

Dispositif de mémoire comprenant au moins un emplacement de mémoire pour stocker des informations représentant des données écrites au moyen d'un premier procédé de chiffrement/déchiffrement, et un canal de lecture utilisant un second procédé de chiffrement/déchiffrement pour lire et déchiffrer des informations telles qu'écrites. Le dispositif de mémoire comprend également un appareil qui empêche la lecture de l'au moins un emplacement de mémoire à l'aide du second procédé de chiffrement/déchiffrement, en réponse à une indication que l'au moins un emplacement de mémoire a été écrit en utilisant le premier procédé de chiffrement/déchiffrement. L'appareil qui empêche la lecture de l'au moins une adresse de bloc physique comprend un dispositif destiné à associer un indicateur avec l'au moins un emplacement de mémoire écrit à l'aide du premier procédé de chiffrement/déchiffrement. L'appareil qui empêche la lecture de l'au moins une adresse de bloc physique comprend également un dispositif pour renvoyer un contenu nul pour l'au moins un emplacement de mémoire écrit à l'aide du premier procédé de chiffrement/déchiffrement en réponse à une indication que le canal de lecture utilise un second procédé de chiffrement/déchiffrement. L'appareil qui empêche la lecture de l'au moins un emplacement de mémoire écrit avec le premier procédé de chiffrement/déchiffrement, dans un mode de réalisation, comprend un dispositif pour l'écriture de zéros dans l'au moins un emplacement de mémoire écrit à l'aide du premier procédé de chiffrement/déchiffrement.

Un appareil de stockage comprend un dispositif à semi-conducteur ayant une pluralité d'emplacements de mémoire, un canal d'écriture pour écrire des informations représentant des données sur la pluralité d'emplacements de mémoire dans un dispositif à semi-conducteur, et un canal de lecture pour lire des informations représentant des données à partir de la pluralité d'emplacements de mémoire dans un dispositif à semi-conducteur. L'appareil de stockage comprend également un contrôleur qui contrôle les opérations de l'appareil de stockage, y compris l'écriture d'informations sur la pluralité d'emplacements de mémoire dans un dispositif à semi-conducteur et la lecture d'informations représentant des données à partir de la pluralité d'emplacements de mémoire dans un dispositif à semi-conducteur. L'appareil de stockage comprend également un système d'indirection comprenant en outre un ensemble d'adresses de blocs logiques, et un ensemble d'adresses de blocs physiques qui correspondent à la pluralité d'emplacements de mémoire dans le dispositif à semi-conducteur de l'appareil de stockage. Le système d'indirection comprend également une carte qui associe

des adresses de blocs logiques à au moins une adresse de bloc physique. La carte comprend également au moins un indicateur indiquant un procédé de chiffrement/déchiffrement utilisé pour écrire et lire des données depuis l'adresse de bloc physique. Le contrôleur renvoie une lecture de zéros lorsque le procédé de chiffrement/déchiffrement utilisé pour lire l'adresse de bloc physique a changé.

Un procédé pour diminuer la génération de données inutiles dans un appareil de stockage comprend de surveiller un appareil de stockage vis-à-vis d'un changement dans un schéma de chiffrement/déchiffrement utilisé pour lire et écrire des données et, en réponse au changement dans le schéma de chiffrement/déchiffrement, amener au moins une adresse de bloc logique pour retourner une indication d'être écrit en zéros lorsque l'adresse de bloc physique associée à l'adresse de bloc logique avait été chiffrée à l'aide de l'ancien schéma de chiffrement/déchiffrement.

BREVE DESCRIPTION DES DESSINS

Les modes de réalisation seront aisément compris à la lecture de la description détaillée suivante considérée en conjonction avec les dessins annexés, dans lesquels des numéros de référence identiques désignent des éléments structurels identiques, et dans lesquels :

La figure 1A est un diagramme schématique d'une mémoire de type flash NAND, selon un mode de réalisation exemplaire.

La figure 1B est un autre diagramme schématique d'une mémoire de type flash NAND, selon un mode de réalisation exemplaire.

La figure 2 est un diagramme schématique d'un appareil ou d'un dispositif de mémoire, selon un mode de réalisation exemplaire.

La figure 3 est schématique d'un système d'indirection d'un dispositif de mémoire, selon un mode de réalisation exemplaire.

La figure 4 est un type de table associée à un système d'indirection d'un dispositif de mémoire, selon un mode de réalisation exemplaire.

La figure 5 est un procédé pour retourner des « zéros » de données écrites avec un schéma de chiffrement différent ou vieux, selon un mode de réalisation exemplaire.

La figure 6 est un procédé pour retourner des « zéros » de données écrites avec un schéma de chiffrement différent ou vieux, selon un mode de réalisation exemplaire.

La figure 7 est un autre type de table associée à un contrôleur d'indirection d'un dispositif de mémoire, selon un mode de réalisation exemplaire.

La figure 8 est un procédé pour retourner des « zéros » de données écrites avec un schéma de chiffrement différent ou vieux, selon un mode de réalisation exemplaire.

La figure 9 est encore un autre type de table associée à un contrôleur d'indirection d'un dispositif de mémoire, selon un mode de réalisation exemplaire.

La figure 10 est un organigramme d'un procédé pour empêcher la génération de données inutiles, selon un mode de réalisation exemplaire.

DESCRIPTION DÉTAILLÉE

Dans la description qui suit, de nombreux détails spécifiques sont présentés pour apporter une compréhension approfondie des concepts sous-jacents aux modes de réalisation décrits. Il sera cependant évident pour l'homme de l'art que les modes de réalisation décrits peuvent être mis en pratique sans certains ou tous ces détails spécifiques. Dans d'autres cas, des étapes de processus bien connues n'ont pas été décrites en détail afin d'éviter d'obscurcir inutilement les concepts sous-jacents.

En général, cette invention décrit des techniques pour écrite et lire des données sur un dispositif à semi-conducteur ou un autre support de stockage tel que les disques durs, des dispositifs hybrides, et similaires. Dans cette demande particulière, la présente divulgation décrit l'écriture et la lecture d'informations représentant des données sur un dispositif à semi-conducteur basé sur une mémoire flash. Il convient de noter que ce n'est qu'un type de support de stockage ou de dispositif à semi-conducteur, et que l'invention pourrait être utilisée dans des dispositifs à semi-conducteur qui emploient d'autres types de technologies de stockage. En d'autres termes, l'invention ne se limite pas à la mémoire flash et pourrait être utilisée dans d'autres types de mémoire, tels que la mémoire à changement de phase (PCM), la mémoire vive magnétorésistive (MRAM), la mémoire vive résistive (RRAM ou ReRAM), ou similaire.

Revenons maintenant à la discussion portant sur la mémoire flash. Il existe deux principaux types de mémoire flash, qui sont nommés d'après le type des portes logiques utilisées pour former la mémoire flash. Il y a un mémoire flash de type NAND et un type de mémoire flash NOR. Les caractéristiques internes des cellules de mémoire flash individuelles présentent des caractéristiques similaires à celles des portes correspondantes. La mémoire flash de type NAND peut facilement être écrite et lue dans des blocs (ou pages) qui sont généralement beaucoup plus petits que l'ensemble du dispositif. Une mémoire flash de type NOR permet à un seul mot machine (un octet) d'être facilement écrit - à un emplacement effaçable - ou lu de manière indépendante. Le type NAND est principalement utilisé dans les

mémoires principales, les cartes mémoire, les mémoires flash USB, les disques SSD, et des produits similaires, pour le stockage et le transfert des données en général. Le type NOR, qui permet un accès véritablement aléatoire et donc une exécution directe du code, est utilisé en remplacement de l'ancienne EPROM et comme une alternative à certains types d'applications de ROM, tandis que la mémoire flash NOR peut émuler la ROM principalement au niveau du code machine ; de nombreux modèles numériques requièrent des structures ROM (ou PLA) pour d'autres usages, souvent à des vitesses significativement supérieures (économique) à celles que la mémoire flash peut atteindre.

La figure 2 est un diagramme schématique d'un appareil ou d'un dispositif de mémoire 200. La mémoire est constituée d'emplacements de mémoire ou de bits 210, 211, 212, 213, 214 disposés dans une grille à deux dimensions. Les bits 210, 211, 212, 213, 214 sont disposés en colonnes (CAS) 220, 221, 222, 223, 224, 225, 226, 227 et en lignes (RAS) 230, 231, 232, 233, 234, 235, 236, 237. Chaque bit peut être identifié par une colonne et une ligne. Par exemple, le bit 211 se situe dans la colonne 225 et la ligne 232. Ce bit particulier est hachuré pour représenter une valeur « 1 ». Un bit non hachuré, tel que le bit 214, représente une valeur « 0 ».

Pour écrire des données dans une colonne, une colonne est sélectionnée, puis des rangées sont chargées pour écrire des données dans les bits associés à la colonne spécifique. Par exemple, lorsque la colonne 225 est écrite, la colonne 225 est sélectionnée. Les lignes 230, 232, 234, 235 et 236 sont chargées, ce qui conduit à une valeur « 1 » stockée à des emplacements de bits particuliers (représentés hachurés).

Autrement dit, des cellules de mémoire sont gravées sur une plaque de silicium dans un réseau de colonnes (lignes de bits) et de lignes (lignes de mots). L'intersection d'une ligne de bits et d'une ligne de mots constitue l'adresse de la cellule de mémoire.

Une charge est transmise à travers la colonne appropriée (CAS) pour activer le transistor à chaque bit dans la colonne. Lors de l'écriture, les lignes en rangées contiennent l'état que le condensateur doit prendre. Lors de la lecture, un amplificateur de lecture détermine le niveau de charge dans le condensateur. S'il est supérieur à 50 pour cent, il le lit en tant que 1 ; sinon il le lit en tant que 0. Le compteur suit la séquence de rafraîchissement en se basant sur quelles rangées ont été consultées dans quel ordre. La durée nécessaire pour faire tout cela est exprimé en nanosecondes.

Des cellules de mémoire seules ne seraient rien sans une certaine façon d'y placer de l'information ou d'en extraire de l'information. Les dispositifs de mémoire comprennent des circuits associés à la mémoire pour identifier chaque ligne et chaque colonne, pour lire et pour

restaurer des signaux à partir de cellules, et pour activer des charges à différentes adresses de la mémoire.

Les figures 1A et 1B représentent chacune un diagramme schématique de la mémoire de type flash NAND 100 et 100', selon un mode de réalisation exemplaire. Dans chaque cas, un dispositif à semi-conducteur flash NAND 110 est connecté à un ordinateur hôte par l'intermédiaire d'un processeur hôte 130. Dans la figure 1A, le processeur hôte 130 gère la plupart des opérations liées à la lecture et à l'écriture d'informations représentant des données sur le dispositif à mémoire à semi-conducteur flash NAND 110. Le processeur hôte 130 comprend un module de code de correction d'erreur (ECC) 131, un module de gestion de blocs défectueux 132, un module d'égalisation de l'usure 133, un module pilote de mémoire flash NAND 134, et un module d'indirection d'adresse 135. Tous ces modules peuvent être des modules matériels, logiciels ou une combinaison de modules matériels et logiciels. Le module de code de correction d'erreur (ECC) 131 gère la détermination d'une erreur dans la lecture des données et l'application du code de correction d'erreur (ECC) aux données ainsi lues. Le code de correction d'erreur est utilisé pour localiser et corriger l'erreur dans un bloc de données lues.

Le module de gestion de blocs défectueux 132 gère les blocs défectueux dans la mémoire flash NAND 110. Les données provenant d'un hôte proviendront généralement de l'hôte sous la forme d'un bloc de données. Le bloc de données peut être de n'importe quelle longueur, bien que 512 octets et 4000 aient été les longueurs normalisées et soient très fréquentes. La mémoire flash NAND est en mesure de recevoir des blocs de données. La fabrication d'un dispositif à semi-conducteur, dans certains cas, n'est pas parfaite. En conséquence, il peut y avoir un ou plusieurs emplacements de mémoire qui sont défectueux et ne permettront pas à un bloc de données d'y être stocké de manière fiable, de sorte qu'il puisse en être récupéré par la suite. Le module de gestion de blocs erronés 132 stocke ces emplacements de blocs défectueux et empêche les données d'y être stockées. Des blocs défectueux peuvent également apparaître au cours de la vie de la mémoire flash NAND 110 de sorte que le module de gestion de blocs défectueux 132 note également d'autres emplacements de mémoire qui se sont développés en blocs défectueux.

Le module d'indirection d'adresse 135 travaille de concert avec le module de gestion de blocs défectueux 132. Le module d'indirection d'adresse 135 comprend un mappage des adresses réelles des blocs physiques (PBA) avec les adresses logiques des blocs (LBA). Les LBA demeurent constantes. L'hôte peut alors donner pour ordre d'écrire sur une LBA particulière. L'adresse réelle où les données sont stockées (PBA) peut changer. Le module

d'indirection d'adresse 135 suit l'emplacement de la LBA telle qu'écrite ou stockée sur la mémoire flash NAND 110. Ainsi, lorsque l'hôte a besoin de lire des données à partir de la mémoire flash NAND 110, le module d'indirection d'adresse 135 s'assure que la PBA correcte associée à la LBA est lue pour garantir que les informations représentant les données sont lues et présentées pour un traitement supplémentaire pour dupliquer les données comme entrée vers le dispositif à semi-conducteur à mémoire flash NAND. Le module d'indirection d'adresse 135 est également nécessaire pour égaliser l'usure. Si les données sont écrites dans un emplacement de mémoire particulier un nombre de fois supérieur au nombre de cycles d'usure, l'emplacement de mémoire peut se détériorer ou devenir peu fiable. L'égalisation de l'usure le reconnaît et allonge la durée de vie de la mémoire en changeant les emplacements de mémoire ou les emplacements physiques réels où l'information est écrite. La LBA restera la même tandis que la PBA changera pour éviter une usure prématurée excessive.

Le module d'égalisation de l'usure 133 surveille et gère les emplacements où les données sont écrites. Une mémoire flash NAND a de nombreux emplacements de mémoire où les données peuvent être écrites. Ces emplacements de mémoire « s'usent » au fil du temps. Les emplacements de mémoire dans une mémoire flash NAND 110 ne peuvent être réécrits de manière fiable qu'un certain nombre de cycles. Le module d'égalisation de l'usure 133 surveille le nombre de lectures et d'écritures en divers emplacements de mémoire et fera commuter l'emplacement de mémoire pour allonger la durée de vie de la mémoire flash NAND 110. Par exemple, si seulement la moitié des emplacements de mémoire ont été constamment écrits, cette moitié de la mémoire flash NAND aurait alors tendance à s'user. Bien que l'ensemble du dispositif ne soit pas usé, la capacité à stocker des données serait gravement entravée en entraînant de mauvaises performances. Le module d'égalisation de l'usure 133 gère l'usure de la mémoire flash NAND 110. Le module d'égalisation de l'usure 133 allonge effectivement la vie de la mémoire flash NAND 110. Il fonctionne également avec le module d'indirection d'adresse 135 car le module de d'égalisation de l'usure 133 peut décider qu'un ensemble particulier de blocs (PBA) doivent être mis de côté pour éviter une usure prématurée des emplacements de mémoire dans la mémoire flash NAND 110.

Le module pilote de mémoire flash NAND 134 est un jeu d'instructions destiné au fonctionnement de la mémoire flash NAND 110.

Le dispositif à semi-conducteur 100 comprend également un module de sécurité 136. Le module de sécurité 136 chiffre les données lorsqu'elles sont écrites et déchiffre les données lors de leur lecture. Le chiffrement des données maintient les données sécurisées. Il est important de garder les données sécurisées à tout moment conformément au sens commun

ainsi qu'à certains critères relatifs à des produits qui doivent les satisfaire pour le qualifier pour une utilisation dans d'autres produits. Dans certains cas, la qualification d'un produit peut inclure de satisfaire une norme de sécurité des données. Dans certains systèmes de chiffrement et de déchiffrement, un élément clé de l'information (aussi connu comme un paramètre) détermine la sortie fonctionnelle d'un algorithme cryptographique ou un chiffre. Sans une clé, l'algorithme ne produirait aucun résultat utile. En chiffrement, une clé spécifie la transformation particulière de texte en clair en un texte chiffré, ou vice-versa lors du déchiffrement. Des clés sont également utilisées dans d'autres algorithmes cryptographiques, tels que les systèmes de signature numérique et les codes d'authentification de message pour des produits que définissent des organismes de normalisation. Cette invention particulière a trait à des cas où un paramètre est modifié. Par exemple, une clé peut être modifiée. Il convient de noter que, lorsque des informations codées sont lues, la clé associée à l'écriture doit être utilisé en même temps que l'algorithme pour décoder les informations et les transformer en données telles qu'écrites. Sans le paramètre, ou lorsque le paramètre est incorrect, l'algorithme de décodage ne fonctionne pas. Une sortie d'information représentant des données décodées avec la mauvaise clé est généralement qualifiée de données inutiles. Ce ne sont pas les données d'origine telles qu'écrites. Des données inutiles peuvent également s'imposer sur un canal de données lors d'une tentative de lecture. Par exemple, lorsque des informations inutiles sont lues, le module de correction d'erreur déterminera qu'il y a une erreur dans les données en lecture. L'« erreur » résultant des données inutiles ne sera pas corrigeable à la volée. Selon le schéma de correction d'erreur, le module de correction d'erreur pourrait chercher à récupérer les données en utilisant diverses techniques de récupération de données profondes. Cela conduit à une perte de temps et fera également perdre du temps au processeur essayant de corriger l'« erreur ». Bien sûr, cela est juste un exemple des problèmes qui peuvent résulter de la lecture d'informations qui se révèlent être des données inutiles.

La figure 1B représente un diagramme schématique d'un autre type de dispositif de mémoire flash NAND 100', selon un mode de réalisation exemplaire. Dans chaque cas, un dispositif à semi-conducteur flash NAND 110 est connecté à un ordinateur hôte par l'intermédiaire d'un processeur hôte 130. La principale différence entre le dispositif de mémoire 100' et le dispositif de mémoire 100 est le processeur 120, qui est situé avec le dispositif à semi-conducteur de type NAND 100'. Le processeur 120 est distinct du processeur hôte 130. Le processeur hôte 130, dans le cas du dispositif à semi-conducteur de type NAND 100', décharge certains des modules de traitement vers le processeur 120 associé

au dispositif à semi-conducteur de type NAND 100'. Le processeur 120 peut être un processeur à usage général ou peut être un processeur dédié qui gère une ou plusieurs tâches spécifiques. Comme le montre la figure 1B, le processeur 120 comprend le module de correction d'erreur (ECC) 131, le module de gestion de blocs défectueux 132 et un module d'égalisation de l'usure 133, par exemple. Ces opérations sont transmises hors du processeur hôte 130 vers le processeur 120 ou le contrôleur NAND. Ces blocs 131, 132 et 133 fonctionnent de la même manière que décrit ci-dessus par rapport à la figure 1A. Ces fonctions ne seront pas répétées ici par souci de concision. Dans la figure 1B, un bus de données 160, une ligne de commande 161 et un signal d'horloge 162 couplent de façon communicante le processeur hôte et le contrôleur NAND ou le processeur 120. Certaines des commandes passées sur la ligne de commande 161 commandent simplement l'un des modules 131, 132, 133 pour commencer leurs processus spécifiques. Ceci est utile en ce que le processeur hôte 130 est libéré pour effectuer d'autres tâches. Le nombre de tâches transférées hors de l'hôte vers le contrôleur NAND 120 est une question d'équilibre quant à la détermination des tâches qui sont totalement spécialisées et mieux accomplies par le contrôleur NAND 120. D'autres tâches peuvent être plus généralement applicables et maintenues au niveau du processeur hôte 130.

Comme décrit ci-dessus, les données stockés sur une mémoire flash de type NAND 110, 110' peuvent être organisées sous forme de blocs de données. Dans certains modes de réalisation exemplaires, l'indirection d'adresse est utilisée pour écrire des blocs de données sur une mémoire flash de type NAND 110, 110'. Autrement dit, les systèmes de fichiers hôtes opèrent avec des adresses de blocs logiques (LBA) dans les commandes pour écrire des blocs de données sur une mémoire flash de type NAND 110, 110' et pour lire des blocs de données à partir de la mémoire flash de type NAND 110, 110' sans égard pour les emplacements réels dans la mémoire flash de type NAND 110, 110'. L'adresse physique réelle est l'adresse de bloc physique (PBA) utilisée en interne par la mémoire flash de type NAND 110, 110'. Une indirection d'adresse est typiquement mise en œuvre dans la partie de contrôleur de l'architecture du dispositif de mémoire (par exemple, le contrôleur NAND 120 de la figure 1B) en utilisant des tables d'indirection qui sont utilisées pour garder une trace de l'emplacement physique associé à une LBA. Autrement dit, les tables d'indirection cartographient la LBA en PBA dans la mémoire flash de type NAND 110, 110'.

Comme décrit ci-dessus, les données sont généralement écrites ou lues sur une mémoire flash de type NAND 110, 110' en blocs ou secteurs contenus dans un ensemble

d'emplacements de mémoire dans la mémoire flash de type NAND 102. Les tailles de blocs peuvent être de 512 octets ou de 4000 octets, dans certains modes de réalisation.

La figure 3 est schématique d'un système d'indirection d'un dispositif de stockage 300, selon un mode de réalisation exemplaire. Plus spécifiquement, la figure 3 est un diagramme schématique du système de stockage 300 couplé de manière communicative à un ordinateur hôte 310. Le système de stockage 300 reçoit des commandes d'écriture à partir de l'hôte 310. Le système de stockage 300 stocke des informations représentatives de données dans des adresses de blocs logiques (LBA). Le système de stockage 300 récupère également des informations ou lit les données et délivre en retour des adresses de blocs logiques (LBA) à l'hôte 310. Comme représenté, le système de stockage 300 comprend un système d'indirection 320, un premier dispositif de mémoire 330, et un second dispositif de mémoire 332. Le système d'indirection 320 peut mapper des LBA à un ou plusieurs dispositifs de mémoire, tels que les dispositifs de mémoire 330 et 332. Le premier dispositif de mémoire 330 et le second dispositif de mémoire 332 peuvent être une mémoire flash NAND 110, 110', ou un dispositif de mémoire générale, tel que le dispositif 200. Le système hôte 310 peut être un processeur, un système informatique indépendant, un système de serveur, ou un autre composant matériel qui communique avec le dispositif de stockage 300.

Le contrôleur d'indirection 320 comprend un processeur 307, de la mémoire couplé de manière communicative avec le processeur 307, et un support lisible par ordinateur 309. Le processeur 307 peut être un contrôleur logique programmable (PLC), un microprocesseur ou un microcontrôleur. Le support lisible par ordinateur 309 peut être séparé des dispositifs de mémoire 330, 332 ou peut se référer à un espace réservé dans les dispositifs de mémoire 330, 332 pour stocker des structures de données et/ou des instructions pour exécution par le processeur 307.

Le contrôleur d'indirection 320 fournit une couche de traduction dynamique entre des adresses de blocs logiques (LBA) utilisées par le système hôte et des adresses de blocs physiques (PBA) utilisées pour accéder à des données stockées dans le dispositif à semi-conducteur 330, 332. L' « adresse de bloc physique » correspond à un emplacement de mémoire réel ou à une pluralité d'emplacements de mémoire réels dans les dispositifs de mémoire 330, 332. Le contrôleur d'indirection 320 gère l'attribution des LBA aux PBA. Dans certains systèmes de stockage, le mappage des LBA aux PBA reste relativement statique du fait que les cellules de mémoire individuelles peuvent être réécrites très peu souvent. Dans des architectures plus complexes, le mappage entre des LBA et des PBA peut changer à chaque opération d'écriture car le système détermine dynamiquement l'emplacement

physique (à savoir la PBA) attribué à un emplacement logique particulier (à savoir une LBA). Les données pour la même LBA seront écrites dans un emplacement différent la prochaine fois que la LBA hôte sera mise à jour. De cette façon, le contrôleur d'indirection 320 fournit une couche de traduction dynamique entre des LBA fournies par le système hôte 310 et des PBA associées aux dispositifs de mémoire 330, 332. Le contrôleur d'indirection 320 est responsable de la gestion de l'affectation des LBA à la pluralité de PBA.

Afin de maintenir sécurisées les données dans les dispositifs de mémoire 330, 332, les données sont de nombreuses fois chiffrées au moyen d'une clé ou d'un autre paramètre. Tant que la clé ou l'autre paramètre restent les mêmes, les données sont sécurisées. La clé ou le paramètre sont utilisés pour chiffrer les données avant d'écrire les données dans le dispositif de mémoire 330, 332. La clé ou l'autre paramètre sont également utilisés pour déchiffrer les informations telles qu'elles sont lues à partir du dispositif de mémoire 330, 332 pour décoder les informations et les transformer en les données telles qu'écrites. Des problèmes surviennent lorsque la clé ou l'autre paramètre sont modifiés à partir de la clé ou de l'autre paramètre tels qu'écrits. Si une clé ou un autre paramètre utilisés pour écrire les données sont modifiés, décoder ou déchiffrer les informations ne conduira pas aux données telles qu'écrites. En fait, des données dépourvues de sens ou « inutiles » sont alors retournées. Cela peut déclencher de nombreux processus exigeants beaucoup de temps tels que des procédures de recouvrement d'erreur qui peuvent ralentir la réactivité du système de stockage de 300. Il n'est pas souhaitable d'avoir des temps de réponse lents. Plutôt que de déclencher ces procédures qui peuvent dégrader les performances du système de stockage 300, le système de stockage 300 est pourvu d'un procédé pour retourner une réponse plus souhaitable. C'est ce qui est décrit ci-dessous. Le procédé permet d'éviter les données « inutiles » et produit une réponse comme si aucune donnée ou aucune information n'était présente.

Cette divulgation va maintenant décrire des moyens pour générer la lecture d'un contenu de zéros à partir de dispositifs de mémoire qui ont été précédemment écrits avec un paramètre d'écriture différent. Un paramètre d'écriture qui pourrait être modifié est une clé qui est généralement utilisée pour écrire les informations représentant des données. Plutôt que de lire en retour des données ou des informations « inutiles », une indication de contenu constitué de zéros est générée. Par exemple, un contenu de zéros peut être indiqué par une lecture de tous les « 1 » ou de tous les « 0 » pour un bloc ou un ensemble de blocs de données. La génération d'un contenu de zéros est accomplie lorsque les données sont lues tout en gardant les mesures de sécurité en place. Comme mentionné ci-dessus, cette exigence vaut pour de nombreux dispositifs car les fabricants ne veulent pas exposer les données.

La figure 4 est un type de table 400 associée à un contrôleur d'indirection 320 d'un système de mémoire 300, selon un mode de réalisation exemplaire. La table 400 est stockée dans la mémoire 109 du contrôleur d'indirection 300. La table 400 comporte une adresse de bloc logique 410, une adresse de bloc physique 420, un certain nombre de blocs de 430, et un schéma de chiffrement 440. Le nombre de blocs est la longueur de la chaîne d'adresses de blocs logiques ou d'adresses de blocs physiques. Par exemple, l'adresse de bloc logique « 1 » commence ladite adresse de bloc physique « 2 » et a une longueur de huit blocs. Le schéma de chiffrement est désigné par un « 1 ». La table 400 est un mappage des adresses de blocs logiques avec les adresses de blocs physiques dans les dispositifs de mémoire 330, 332. L'adresse de bloc logique 3 a une adresse de départ « SSD 1 », qui correspond à un dispositif à semi-conducteur, tel que le SSD 332 représenté sur la figure 3. La table 400 comprend un certain nombre de pointeurs. Un pointeur est une variable qui contient l'emplacement de mémoire (adresse) de certaines données plutôt que les données elles-mêmes. En d'autres termes, l'adresse de bloc physique 420 pour chacun des blocs de données pourrait être appelée un pointeur car c'est l'adresse du commencement du bloc de données, que ce soit à l'intérieur du premier dispositif de mémoire 330, ou à l'intérieur du second dispositif de mémoire 332.

Il existe plusieurs procédés pour retourner des « zéros » à partir de données qui ont été écrites avec un ancien ou d'un autre système de chiffrement. Les diverses méthodes seront décrites en lien avec les tables, telles que la table 400, et d'autres tables présentées ci-dessous.

La figure 5 est un procédé 500 pour retourner des « zéros » à partir de données écrites avec un schéma de chiffrement ancien ou différent, selon un mode de réalisation exemplaire. Le procédé 500 comprend la surveillance du dispositif de mémoire ou de stockage à la recherche d'un changement dans le schéma de chiffrement/déchiffrement utilisé pour lire et écrire les données 510. Surveiller le dispositif de stockage à la recherche d'un changement dans le schéma de chiffrement/déchiffrement comprend de surveiller une colonne 440 de la table 400. La colonne 440 fournit une indication du schéma de chiffrement utilisé. Comme le montre la figure 4, le schéma de chiffrement utilisé pour les adresses de blocs logiques 1 et 2 est représenté par une valeur « 1 » dans la colonne 440 de la table 400. C'est un autre ou un ancien schéma de chiffrement dans ce mode de réalisation exemplaire. Le schéma de chiffrement utilisé pour les adresses de blocs logiques 3 et 4 est représenté par une valeur « 2 ». C'est un nouveau schéma de chiffrement qui est différent du schéma de chiffrement utilisé pour écrire les données associées à des adresses de blocs logiques 1 et 2. Le procédé 500 comprend de retourner une indication qu'elle est écrite en zéros pour au moins une

adresse de bloc logique lorsque l'adresse de bloc physique associée à l'adresse de bloc logique a été chiffrée au moyen d'un ancien schéma de chiffrement/déchiffrement 512. Dans ce cas, la valeur « 1 » dans la colonne 440 indique qu'un ancien schéma de chiffrement a été utilisé pour les adresses de blocs logiques 1 et 2. Le nouveau schéma de chiffrement, ou le schéma de chiffrement changé ou différent, est représenté par une valeur « 2 » dans la colonne 440 de la table 4. Le schéma de chiffrement courant est représenté par la valeur « 2 ». En conséquence, le canal de lecture sera pourvu d'une entrée constituée que de zéros pour les données associées aux adresses de blocs logiques 1 et 2 car le schéma de chiffrement indiqué associé à ces données a une valeur « 1 ».

La figure 6 est un procédé 600 pour retourner des « zéros » à partir de données écrites avec un schéma de chiffrement différent ou ancien, selon un mode de réalisation exemplaire. Le procédé 600 comprend de surveiller le dispositif de mémoire à la recherche d'un changement dans le schéma de chiffrement/déchiffrement utilisé pour lire et écrire les données 610. Surveiller le dispositif de mémoire à la recherche du changement dans le schéma de chiffrement/déchiffrement comprend de surveiller la colonne 440 de la table 400, représentée sur la figure 4. Une fois qu'il est déterminé que certaines des données associées à certaines adresses de blocs logiques ont été chiffrées au moyen d'un schéma de chiffrement ancien ou différent, des zéros sont écrits à l'adresse de bloc physique laquelle est préalablement chiffrée au moyen de l'ancien schéma de chiffrement/déchiffrement 612. Par conséquent, sur la figure 4, les données qui sont associées aux adresses de blocs logiques 1 et 2 seront écrasées en écriture ou réécrites avec des zéros. Plus particulièrement, l'adresse de bloc physique 2 et les huit adresses de blocs physiques associées à l'adresse de bloc logique 1, seront écrasées en écriture avec des zéros. De manière similaire, l'adresse de bloc physique 172 et les 21 adresses de blocs physiques associées à l'adresse de bloc logique 2 seront également écrasées en écriture avec des zéros. Ainsi, dans les emplacements de mémoire physique réels indiqués par la table 400, il y aura des zéros écrits à ces emplacements de données.

Le procédé comprend également de lire les adresses de blocs physiques réécrites qui correspondent aux adresses de blocs logiques associées 614. En d'autres termes, les adresses de blocs physiques associées à l'adresse de bloc logique contiendront des zéros y étant écrits. Lors de la lecture, de réels zéros seront retournés au canal de lecture plutôt que des données inutiles. Là encore, il convient de noter que les adresses de blocs logiques qui sont réécrites avec des zéros sont celles où un schéma de chiffrement ancien ou différent est utilisé, telles

que les adresses de blocs logiques 1 et 2 indiquées sur la figure 4. Cela suppose que le schéma de chiffrement 2 est le schéma de chiffrement en cours.

La figure 7 est un autre type de table 700 associée à un contrôleur d'indirection de système de stockage 300, selon un mode de réalisation exemplaire. La table 700 comporte des colonnes pour les adresses de blocs logiques 710, les adresses de blocs physiques qui correspondent aux adresses de blocs logiques 720, le nombre de blocs écrits 730, une indication de non validité 734, et une indication du schéma de chiffrement utilisé 740. Comme le montre la figure 7, lorsqu'un schéma de chiffrement ancien ou différent est utilisé, l'adresse de bloc logique est marquée ou indiquée comme non valide comme cela est représenté par la colonne 734 dans la table 700. Le schéma de chiffrement en cours est représenté par le chiffre « 2 » et le schéma de chiffrement ancien ou différent est représenté par le chiffre « 1 » dans la colonne 740 de la table 700. Dans la colonne 734, les deux premières entrées qui correspondent aux adresses de blocs logiques « 1 » et « 2 » portent une valeur de 1 qui indique que les données associées à ces adresses de blocs logiques sont non valides. Les deux autres entrées pour les adresses de blocs logiques « 3 » et « 4 » ont une valeur « 0 », ce qui indique que ces adresses de blocs logiques ou les informations représentant des données à ces adresses de blocs logiques ont été écrites avec le schéma de chiffrement actuel.

La figure 8 illustre un procédé 800 pour retourner des « zéros » à partir de données écrites avec un schéma de chiffrement différent ou ancien, selon un mode de réalisation exemplaire. Le procédé 800 comprend de surveiller le système de stockage, et plus particulièrement un dispositif de mémoire 330, 332, à la recherche d'un changement dans le schéma de chiffrement/déchiffrement utilisé pour lire et écrire les données 810. Surveiller le dispositif de mémoire à la recherche d'un changement dans le schéma de chiffrement/déchiffrement comprend de surveiller la colonne 740 de la table 700, représentée sur la figure 7. Définir la non validité à une valeur « 1 » peut aussi revenir à définir un indicateur par rapport aux adresses de blocs logiques « 1 » et « 2 ». Un indicateur est un marqueur d'un certain type utilisé par un traitement informatique ou des informations d'interprétation. Un indicateur est un signal indiquant l'existence ou l'état d'une condition particulière. Dans ce mode de réalisation exemplaire, la grande condition particulière est que les données ou les informations représentant des données associées à une adresse de bloc logique particulière ont été écrites avec un schéma de chiffrement qui diffère du schéma de chiffrement actuellement utilisé. Ceci est indiqué par la valeur « 1 » dans la colonne d'invalidité 734 de la table 700. Le procédé 800 comprend également d'associer au moins un

indicateur à au moins une adresse de bloc physique qui est associée à une adresse de bloc logique qui indique que les informations représentant des données à l'adresse de bloc physique associée sont écrites au moyen d'un ancien schéma de chiffrement. Le canal de lecture ou le contrôleur qui contrôle un canal de lecture ne liront pas les adresses de blocs physiques des données non valides et retourneront une lecture de tous les zéros pour leur traitement ultérieur. En d'autres termes, des zéros seront retournés sur la base de l'indication de non validité des adresses de blocs logiques. Ceci permet d'éviter le retour de données inutiles à partir des adresses de blocs physiques associées aux adresses de blocs logiques.

La figure 9 est encore un autre type de table 900 associée à un contrôleur d'indirection 300 d'un dispositif de stockage 300, selon un mode de réalisation exemplaire. Dans ce mode de réalisation particulier, lorsqu'il est déterminé que le schéma de chiffrement utilisé ne correspond pas au schéma de chiffrement actuel, l'adresse de bloc physique pour une adresse de bloc logique particulière est supprimée. En d'autres termes, le pointeur qui indique l'adresse de bloc physique de départ est éliminé. Ceci est illustré dans la table 900 dans la colonne 920. Plus spécifiquement, les adresses de blocs physiques indiquant l'adresse de bloc physique de départ pour des adresses de blocs logiques « 1 » et « 2 » ont été supprimées car le schéma de chiffrement, indiqué par une valeur de « 1 » est ancien ou différent du schéma de chiffrement actuel. Sans une adresse de bloc physique pour point de départ, le dispositif de mémoire suppose que l'adresse de bloc logique correspondant aux valeurs « 1 » et « 2 » est vide et retournera donc automatiquement des zéros tels qu'ils sont lus à partir des adresses de blocs logiques.

La figure 10 est un organigramme d'un procédé 1000 pour empêcher la génération de données inutiles, selon un mode de réalisation exemplaire. Le procédé 1000 comprend de surveiller l'appareil de stockage ou le dispositif de mémoire à la recherche d'un changement dans le schéma de chiffrement/déchiffrement utilisé pour lire et écrire les données 1010. Surveiller l'appareil de stockage à la recherche d'un changement dans le schéma de chiffrement/déchiffrement 1010 comprend de surveiller la colonne 440 de la table 900, représentée sur la figure. 9. Le procédé comprend également de supprimer un pointeur de l'adresse de bloc logique vers l'adresse de bloc physique lors d'une indication selon laquelle un nouveau schéma de chiffrement/déchiffrement est utilisé pour lire les données 1012. En d'autres termes, le pointeur associé aux informations représentant des données écrites avec un schéma de chiffrement/déchiffrement ancien ou différent sera supprimé afin que l'adresse de bloc logique apparaisse vide. En l'absence de données à une adresse de bloc logique, le canal

de lecture retournera des zéros pour indiquer qu'aucune donnée n'est présente. De cette façon, la lecture de données inutiles est à nouveau empêchée.

Un dispositif de mémoire comprenant au moins un emplacement de mémoire pour stocker des informations représentant des données écrites au moyen d'un premier procédé de chiffrement/déchiffrement, et un canal de lecture utilisant un second procédé de chiffrement/déchiffrement pour lire et déchiffrer des informations telles qu'écrites. Le dispositif de mémoire comprend également un appareil qui empêche la lecture de l'au moins un emplacement de mémoire au moyen du second procédé de chiffrement/déchiffrement, en réponse à une indication que l'au moins un emplacement de mémoire a été écrit au moyen du premier procédé de chiffrement/déchiffrement. L'appareil qui empêche la lecture de l'au moins une adresse de bloc physique comprend un dispositif destiné à associer un indicateur à l'au moins un emplacement de mémoire écrit au moyen du premier procédé de chiffrement/déchiffrement. L'appareil qui empêche la lecture de l'au moins une adresse de bloc physique comprend également un dispositif pour retourner le contenu de zéros pour l'au moins un emplacement de mémoire écrit au moyen du premier procédé de chiffrement/déchiffrement en réponse à une indication que le canal de lecture utilise un second procédé de chiffrement/déchiffrement. L'appareil qui empêche la lecture de l'au moins un emplacement de mémoire écrit par le premier procédé de chiffrement/déchiffrement, dans un mode de réalisation, comprend un dispositif pour écrire des zéros à l'au moins un emplacement de mémoire écrit au moyen du premier procédé de chiffrement/déchiffrement. Dans un mode de réalisation, les informations représentant des données se trouvent dans un bloc et l'au moins un emplacement de mémoire est au moins une adresse de bloc physique. Dans certains modes de réalisation, le dispositif de mémoire comprend également un système d'indirection. Le système d'indirection comprend au moins une adresse de bloc logique, et une base de données qui met en correspondance l'au moins une adresse de bloc logique à l'au moins une adresse de bloc physique. Dans un mode de réalisation, le système d'indirection comprend un appareil qui permet le mappage de l'au moins une adresse de bloc logique à l'au moins une adresse physique inaccessible en réponse au canal de lecture au moyen d'un second procédé de chiffrement/déchiffrement, lorsque l'au moins une adresse de bloc physique est écrite au moyen du premier procédé de chiffrement/déchiffrement. Le second procédé de chiffrement/déchiffrement diffère du premier procédé de chiffrement/déchiffrement. Un second paramètre de chiffrement associé au second procédé de chiffrement/déchiffrement diffère d'un premier paramètre de chiffrement associé au premier procédé de chiffrement/déchiffrement. Dans un autre mode de

réalisation exemplaire, un second paramètre d'étendue de chiffrement associé au second procédé de chiffrement/déchiffrement diffère d'un premier paramètre d'étendue de chiffrement associé au premier procédé de chiffrement/déchiffrement. Dans encore d'autres modes de réalisation, un second paramètre de clé de chiffrement du second procédé de chiffrement/déchiffrement diffère d'un premier paramètre de clé de chiffrement du premier procédé de chiffrement/déchiffrement.

Un appareil de stockage comprend un dispositif à semi-conducteur ayant une pluralité d'emplacements de mémoire, un canal d'écriture pour écrire des informations représentant des données sur la pluralité d'emplacements de mémoire dans un dispositif à semi-conducteur, et un canal de lecture pour lire des informations représentant des données à partir de la pluralité d'emplacements de mémoire dans un dispositif à semi-conducteur. L'appareil de stockage comprend également un contrôleur qui contrôle les opérations de l'appareil de stockage, y compris l'écriture des informations sur la pluralité d'emplacements de mémoire dans un dispositif à semi-conducteur et la lecture d'informations représentant des données à partir de la pluralité d'emplacements de mémoire dans un dispositif à semi-conducteur. L'appareil de stockage comprend également un système d'indirection, comprenant en outre un ensemble d'adresses de blocs logiques, et un ensemble d'adresses de blocs physiques qui correspondent à la pluralité d'emplacements de mémoire dans le dispositif à semi-conducteur de l'appareil de stockage. Le système d'indirection comprend également un mappage qui associe des adresses de blocs logiques à au moins une adresse de bloc physique. Le mappage comprend également au moins un indicateur indiquant un procédé de chiffrement/déchiffrement utilisé pour écrire et lire des données depuis l'adresse de bloc physique. Le contrôleur retourne une lecture de zéros lorsque le procédé de chiffrement/déchiffrement utilisé pour lire l'adresse de bloc physique a changé. Dans un mode de réalisation exemplaire, le contrôleur entraîne que l'adresse de bloc physique soit écrite avec des zéros en réponse à un changement dans le procédé de chiffrement/déchiffrement. Dans un autre mode de réalisation exemplaire, le contrôleur retourne tous les zéros en réponse à une indication d'un changement dans le procédé de chiffrement/déchiffrement. Dans encore un autre mode de réalisation, le contrôleur supprime un pointeur dans le mappage entre l'adresse de bloc logique et l'adresse de bloc physique en réponse à une indication d'un changement dans le procédé de chiffrement/déchiffrement. Dans encore un autre mode de réalisation, le contrôleur génère un indicateur indiquant que des informations à une adresse de bloc physique ne sont pas valides en réponse à une indication d'un changement dans le procédé de chiffrement/déchiffrement. Le contrôleur

contrôle l'écriture des informations au niveau du dispositif à semi-conducteur et la lecture des informations représentant des données depuis le dispositif à semi-conducteur. Le système d'indirection comprend un ensemble d'adresses de blocs physiques qui correspondent à des emplacements de mémoire réels du dispositif à semi-conducteur. Le mappage pour associer des adresses de blocs logiques à au moins un des emplacements de mémoire réels du dispositif à semi-conducteur comprend également au moins un indicateur indiquant un procédé de chiffrement/déchiffrement utilisé pour écrire et lire des données à partir des emplacements de mémoire réels du dispositif à semi-conducteur. Lorsque l'indicateur est défini, le contrôleur retourne une lecture de zéros lorsque le procédé de chiffrement/déchiffrement utilisé pour lire les emplacements de mémoire réels du dispositif à semi-conducteur a changé.

Un procédé pour diminuer la génération de données inutiles dans un appareil de stockage comprend de surveiller un appareil de stockage à la recherche d'un changement dans un schéma de chiffrement/déchiffrement utilisé pour lire et écrire des données et, en réponse au changement dans le schéma de chiffrement/déchiffrement, entraîner qu'au moins une adresse de bloc logique retourne une indication qu'elle est écrite en zéros lorsque l'adresse de bloc physique associée à l'adresse de bloc logique a été chiffrée au moyen de l'ancien schéma de chiffrement/déchiffrement. Dans un mode de réalisation, l'adresse de bloc physique précédemment chiffrée au moyen de l'ancien schéma de chiffrement/déchiffrement est écrite sous la forme de zéros au moyen du nouveau schéma de chiffrement/déchiffrement. Dans un autre mode de réalisation, un pointeur de l'adresse de bloc logique vers l'adresse de bloc physique est supprimé sur une indication qu'un nouveau schéma de chiffrement/déchiffrement est utilisé pour lire les données. Cela produit une lecture contenant uniquement des zéros et empêche la génération de données inutiles. Dans encore un autre mode de réalisation, il y a une pluralité d'adresses de blocs logiques qui sont associées à une pluralité d'adresses de blocs physiques écrites avec un ancien schéma de chiffrement/déchiffrement. Les pointeurs pour la pluralité d'adresses de blocs logiques sont supprimés vers la pluralité d'adresses de blocs physiques précédemment écrites avec un ancien schéma de chiffrement/déchiffrement. Dans encore un autre mode de réalisation, la pluralité d'adresses de blocs logiques sont mises en correspondance avec les adresses de blocs physiques dans un mappage. Le mappage comprend en outre au moins un indicateur indiquant que des informations représentant des données à une adresse de bloc logique ne sont pas valides lorsque les informations représentant des données écrites à l'adresse de bloc physique associée à l'adresse de bloc logique sont écrites au moyen d'un ancien schéma de chiffrement.

Dans un ou plusieurs exemples, les fonctions décrites peuvent être mises en œuvre dans le matériel, les logiciels, le microprogramme, ou toute combinaison de ceux-ci. Si elles sont implémentées dans des logiciels, les fonctions peuvent être stockées ou transmises, sous la forme d'une ou plusieurs instructions ou d'un code, sur un support lisible par ordinateur et exécutées par une unité de traitement basée sur des composants matériels. Les supports lisibles par ordinateur peuvent inclure des supports de stockage lisibles par ordinateur, ce qui correspond à un support tangible tel que des supports de stockage de données, ou des moyens de communication incluant tout support qui facilite le transfert d'un programme d'ordinateur d'un endroit à un autre, par exemple, selon un protocole de communication. De cette manière, les supports lisibles par ordinateur peuvent généralement correspondre à (1) des supports de stockage lisibles par ordinateur tangibles qui ne sont pas transitoires ou (2) un moyen de communication tel qu'un signal ou une onde porteuse. Les supports de stockage de données peuvent être n'importe quels supports disponibles qui peuvent être accédés par un ou plusieurs ordinateurs ou un ou plusieurs processeurs pour en extraire des instructions, du code et/ou des structures de données pour la mise en œuvre des techniques décrites dans la présente description. Un produit programme informatique peut comprendre un support lisible par ordinateur.

A titre d'exemple, et sans limitation, ces supports de stockage lisibles par ordinateur peuvent comprendre des mémoires RAM, ROM, EEPROM, un CD-ROM ou un autre stockage sur disque optique, un stockage sur disque magnétique, ou d'autres dispositifs de stockage magnétiques, de la mémoire flash, ou tout autre support qui peut être utilisé pour stocker un code de programme souhaité sous la forme d'instructions ou de structures de données, et qui sont accessibles par un ordinateur. En outre, support lisible par ordinateur désigne de manière adéquate n'importe quelle connexion. Par exemple, si des instructions sont transmises à partir d'un site web, d'un serveur, ou d'une autre source distante au moyen d'un câble coaxial, d'un câble à fibre optique, d'une paire torsadée, d'une ligne d'abonné numérique (DSL) ou de technologies sans fil comme des transmission par infrarouge, par ondes radio, par micro-ondes, alors le câble coaxial, le câble à fibre optique, la paire torsadée, ligne DSL, ou des technologies sans fil telles que des transmission par infrarouge, par ondes radio, par micro-ondes sont inclus dans la définition du support. Il doit être toutefois entendu que les supports de stockage lisibles par ordinateur et les supports de stockage de données n'incluent pas les connexions, les ondes porteuses, les signaux, ou d'autres médias transitoires, mais sont plutôt orientés vers des supports de stockage tangibles, non transitoires. Le terme disque, tel qu'utilisé ici, comprend le disque compact (CD), le disque laser, le

disque optique, le disque numérique polyvalent (DVD), la disquette et le disque Blu-ray, où les disques - que l'on désigne par « disks » en anglais - reproduisent généralement les données magnétiquement, tandis que les disques - que l'on désigne par « discs » en anglais - reproduisent les données optiquement avec des lasers. Des combinaisons de ce qui précède doivent également être incluses dans ce que recouvrent les supports lisibles par ordinateur.

Des instructions peuvent être exécutées par un ou plusieurs processeurs, tels qu'un ou plusieurs processeurs de signaux numériques (DSP), des microprocesseurs d'usage général, des circuits intégrés à application spécifique (ASIC), des circuits intégrés prédiffusés programmables (FPGA), ou d'autres circuits logiques discrets ou intégrés équivalents. En conséquence, le terme « processeur », tel qu'utilisé ici, peut se rapporter à l'une quelconque des structures précédentes ou à toute autre structure appropriée pour la mise en œuvre des techniques décrites ici. En outre, les techniques peuvent être entièrement mises en œuvre dans un ou plusieurs circuits ou éléments logiques.

Les techniques de cette invention peuvent être mises en œuvre dans une grande variété de dispositifs ou d'appareils, y compris un combiné sans fil, un circuit intégré (IC) ou un ensemble de circuits intégrés (par exemple, un jeu de puces). Divers composants, modules ou unités sont décrits dans cette description pour mettre en évidence les aspects fonctionnels des dispositifs configurés pour exécuter les techniques décrites, mais ne requièrent pas nécessairement une réalisation par différentes unités matérielles. Au contraire, comme décrit ci-dessus, différentes unités peuvent être combinées dans une unité matérielle ou fournies par un ensemble d'unités matérielles en interopérabilité, y compris un ou plusieurs processeurs comme décrit ci-dessus, en conjonction avec un logiciel et/ou un microprogramme appropriés.

La description qui précède, à des fins d'explication, a utilisé une nomenclature spécifique pour proposer une compréhension complète de l'invention. Cependant, il sera évident pour l'homme de l'art que les détails spécifiques ne sont pas nécessaires pour mettre en pratique l'invention. Ainsi, les descriptions qui précèdent de modes de réalisation spécifiques de la présente invention sont présentées à titre d'illustration et de description. Elles ne sont pas destinées à être exhaustives ni à limiter l'invention aux formes précises décrites. Il sera évident pour l'homme de l'art que de nombreuses modifications et variations sont possibles à la lumière des enseignements ci-dessus.

Les modes de réalisation ont été choisis et décrits afin d'expliquer au mieux les principes de l'invention et ses applications pratiques, pour ainsi permettre à l'homme de l'art d'utiliser au mieux l'invention et divers modes de réalisation avec diverses modifications

telles qu'appropriées à l'utilisation particulière envisagée. Il est prévu que la portée de l'invention soit définie par les revendications suivantes et leurs équivalents.

Bien que les modes de réalisation aient été décrits en termes de plusieurs modes de réalisation particuliers, il existe des modifications, permutations et équivalents, qui entrent dans le champ d'application de ces concepts généraux. Il convient également de noter qu'il existe de nombreuses autres façons de mettre en œuvre les procédés et les appareils des présents modes de réalisation. Il est donc prévu que les revendications annexées suivantes soient interprétées comme comprenant tous ces modifications, permutations et équivalents qui sont couverts par l'esprit et la portée véritables des modes de réalisation décrits. Ceux-ci et d'autres modes de réalisation exemplaires sont couverts par la portée des revendications suivantes.

REVENDICATIONS

1. Dispositif de mémoire comprenant :

au moins un emplacement de mémoire pour stocker des informations représentant des données écrites au moyen d'un premier procédé de chiffrement/déchiffrement ;

un canal de lecture utilisant un second procédé de chiffrement/déchiffrement pour lire et déchiffrer les informations telles qu'écrites ; et

un appareil qui empêche la lecture de l'au moins un emplacement de mémoire à l'aide du second procédé de chiffrement/déchiffrement, en réponse à une indication que l'au moins un emplacement de mémoire a été écrit en utilisant le premier procédé de chiffrement/déchiffrement.

2. Dispositif de mémoire selon la revendication 1, dans lequel l'appareil qui empêche la lecture d'au moins une adresse de bloc physique comprend un dispositif pour

associer un indicateur avec l'au moins un emplacement de mémoire écrit en utilisant le premier procédé de chiffrement/déchiffrement ; et

retourner un contenu nul pour l'au moins un emplacement de mémoire écrit en utilisant le premier procédé de chiffrement/déchiffrement en réponse au canal de lecture utilisant un second procédé de chiffrement/déchiffrement.

3. Dispositif de mémoire selon la revendication 1, dans lequel l'appareil qui empêche la lecture de l'au moins un emplacement de mémoire écrit avec le premier procédé de chiffrement/déchiffrement en utilisant le second procédé de chiffrement comprend un dispositif pour écrire des zéros dans l'au moins un emplacement de mémoire écrit au moyen d'un premier procédé de chiffrement/déchiffrement.

4. Dispositif de mémoire selon la revendication 1, dans lequel les informations représentant des données sont dans un bloc et l'au moins un emplacement de mémoire est au moins une adresse de bloc physique.

5. Dispositif de mémoire selon la revendication 4, comprenant en outre un système d'indirection, qui comprend en outre :

au moins une adresse de bloc logique ; et

une base de données qui met en correspondance l'au moins une adresse de bloc logique à l'au moins une adresse de bloc physique.

6. Dispositif de mémoire selon la revendication 5, dans lequel le système d'indirection comprend un appareil qui procède à la mise en correspondance de l'au moins une adresse de bloc logique à l'au moins une adresse de bloc physique inaccessible en réponse au canal de lecture utilisant un second procédé de chiffrement/déchiffrement lorsque l'au moins une adresse de bloc physique est écrite en utilisant le premier procédé de chiffrement/déchiffrement.

7. Dispositif de mémoire selon la revendication 6, dans lequel un second paramètre de chiffrement associé au second procédé de chiffrement/déchiffrement est différent d'un premier paramètre de chiffrement associé au premier procédé de chiffrement/déchiffrement.

8. Dispositif de mémoire selon la revendication 6, dans lequel un second paramètre d'étendue de chiffrement associé au second procédé de chiffrement/déchiffrement est différent d'un premier paramètre d'étendue de chiffrement associé au premier procédé de chiffrement/déchiffrement.

9. Dispositif de mémoire selon la revendication 6, dans lequel un paramètre de seconde clé de chiffrement du second procédé de chiffrement/déchiffrement est différent d'un paramètre de première clé de chiffrement du premier procédé de chiffrement/déchiffrement.

10. Appareil de stockage comprenant :

un dispositif à semi-conducteur comprenant une pluralité d'emplacements de mémoire ;

un canal d'écriture pour écrire des informations représentant des données sur la pluralité d'emplacements de mémoire dans le dispositif à semi-conducteur ;

un canal de lecture pour lire des informations représentant des données à partir de la pluralité d'emplacements de mémoire dans le dispositif à semi-conducteur ;

un contrôleur qui contrôle les opérations de l'appareil de stockage, y compris l'écriture d'informations sur la pluralité d'emplacements de mémoire dans le dispositif à semi-conducteur et la lecture d'informations représentant des données à partir de la pluralité d'emplacements de mémoire dans le dispositif à semi-conducteur ;

un système d'indirection, comprenant en outre :

un ensemble d'adresses de blocs logiques ;

un ensemble d'adresses de blocs physiques qui correspondent à la pluralité d'emplacements de mémoire dans le dispositif à semi-conducteur de l'appareil de stockage ;

un mappage qui associe des adresses de blocs logiques à au moins une adresse de bloc physique, le mappage comprenant également au moins un indicateur indiquant un procédé de chiffrement/déchiffrement utilisé pour écrire et lire des données à partir de l'adresse de bloc physique, où le contrôleur retourne une lecture de zéros lorsque le procédé de chiffrement/déchiffrement utilisé pour lire l'adresse de bloc physique a changé.

11. Appareil de stockage selon la revendication 10, dans lequel le contrôleur amène l'adresse de bloc physique à être écrite avec des zéros en réponse à un changement dans le procédé de chiffrement/déchiffrement.

12. Appareil de stockage selon la revendication 10, dans lequel le contrôleur retourne tous les zéros en réponse à une indication d'un changement dans le procédé de chiffrement/déchiffrement.

13. Appareil de stockage selon la revendication 10, dans lequel le contrôleur supprime un pointeur dans le mappage entre l'adresse de bloc logique et l'adresse de bloc physique en réponse à une indication d'un changement dans le procédé de chiffrement/déchiffrement.

14. Appareil de stockage selon la revendication 10, dans lequel le contrôleur génère un indicateur indiquant que des informations à une adresse de bloc physique ne sont pas valides en réponse à une indication d'un changement dans le procédé de chiffrement/déchiffrement.

15. Appareil de stockage selon la revendication 10, dans lequel le contrôleur contrôle l'écriture des informations sur le dispositif à semi-conducteur et la lecture des informations représentant des données depuis le dispositif à semi-conducteur ;

le système d'indirection comprenant en outre un ensemble d'adresses de blocs physiques qui correspondent à des emplacements de mémoire réels du dispositif à semi-conducteur, le mappage associant des adresses de blocs logiques à au moins un des emplacements de mémoire réels du dispositif à semi-conducteur, le mappage comprenant

également au moins un indicateur indiquant un procédé de chiffrement/déchiffrement utilisé pour écrire et lire des données depuis les emplacements de mémoire réels du dispositif à semi-conducteur, où le contrôleur retourne une lecture de zéros lorsque le procédé de chiffrement/déchiffrement utilisé pour lire les emplacements de mémoire réels du dispositif à semi-conducteur a changé.

16. Procédé pour diminuer la génération de données inutiles dans un appareil de stockage, le procédé comprenant les étapes suivantes :

surveiller l'appareil de stockage à la recherche d'un changement dans un schéma de chiffrement/déchiffrement utilisé pour lire et écrire des données ; et

en réponse à la modification du schéma de chiffrement/déchiffrement, amener au moins une adresse de bloc logique à retourner une indication qu'elle est écrite en zéros lorsqu'une adresse de bloc physique associée à l'adresse de bloc logique a été chiffrée au moyen d'un ancien schéma de chiffrement/déchiffrement.

17. Procédé selon la revendication 16, dans lequel l'adresse de bloc physique chiffrée au moyen de l'ancien schéma de chiffrement/déchiffrement est écrite sous la forme de zéros au moyen d'un nouveau schéma de chiffrement/déchiffrement.

18. Procédé selon la revendication 16, dans lequel un mappage est utilisé pour mapper l'adresse de bloc logique à l'adresse de bloc physique, où un pointeur depuis l'adresse de bloc logique vers l'adresse de bloc physique est retiré sur une indication qu'un nouveau schéma de chiffrement/déchiffrement est en cours d'utilisation pour lire des données.

19. Procédé selon la revendication 18, dans lequel il y a une pluralité d'adresses de blocs logiques qui sont associées à une pluralité d'adresses de blocs physiques écrites avec un ancien schéma de chiffrement/déchiffrement, où les pointeurs pour la pluralité d'adresses de blocs logiques sont supprimés.

20. Procédé selon la revendication 16, dans lequel il existe une pluralité d'adresses de blocs logiques qui sont associées à une pluralité d'adresses de blocs physiques écrites avec un ancien schéma de chiffrement/déchiffrement, la pluralité d'adresses de blocs logiques mappées aux adresses de blocs physiques dans un mappage, le mappage comprenant en outre au moins un indicateur indiquant que des informations représentant des données à une adresse

de bloc logique ne sont pas valides lorsque les informations représentant les données écrites à l'adresse de bloc physique associée à l'adresse de bloc logique sont écrites au moyen d'un ancien schéma de chiffrement.

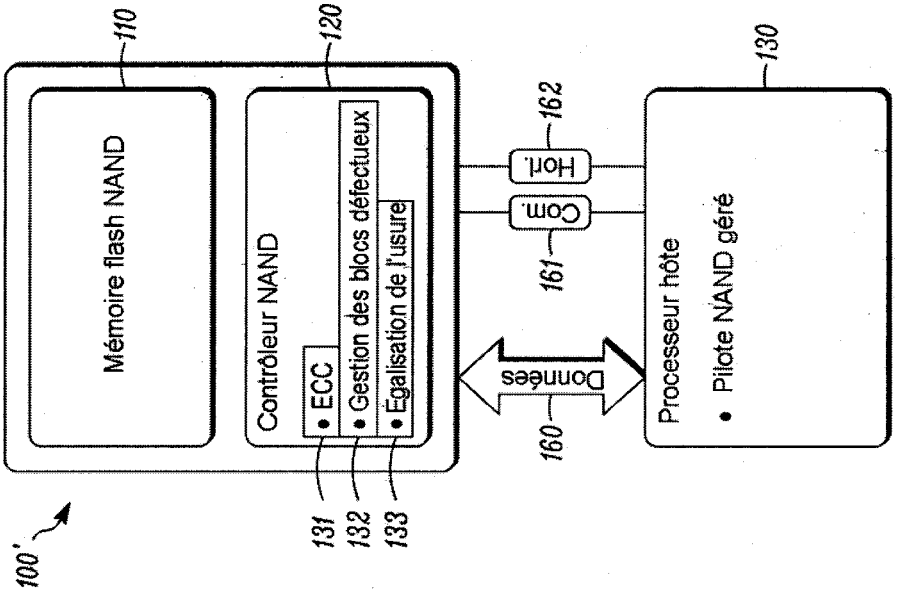

110
120
Mémoire flash NAND
Contrôleur NAND
• ECC
• Gestion des blocs défectueux
• Égalisation de l'usure
Hôt.
Com.
Données
162
161
160
130
Processeur hôte
• Pilote NAND géré
100'
131
132
133

FIG. 1B

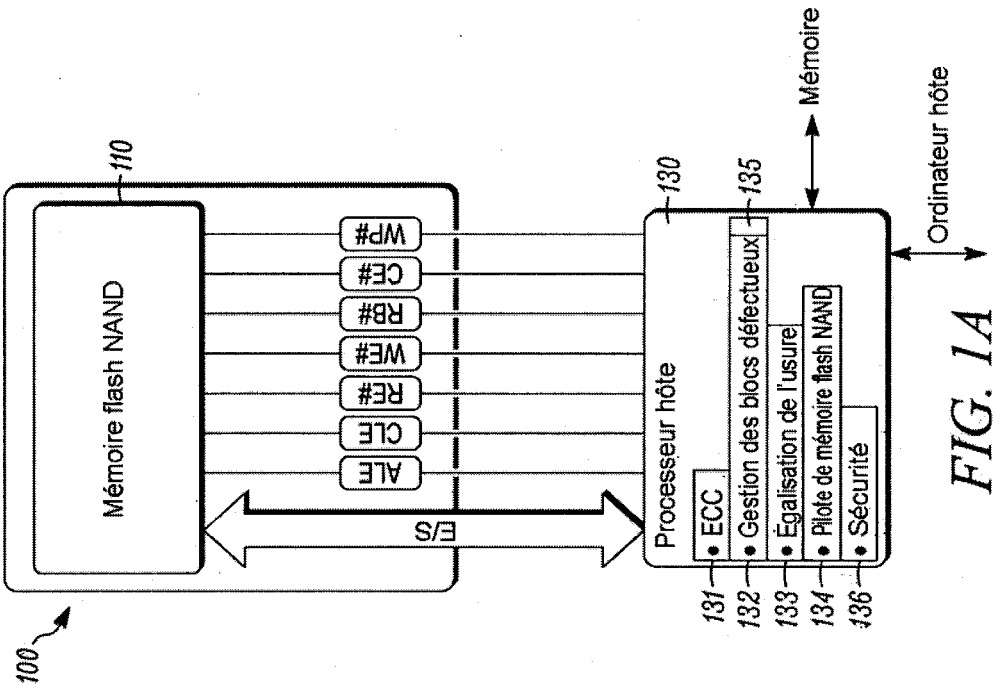

110
Mémoire flash NAND
WP#
CE#
RB#
WE#
RE#
CLE
ALE
E/S
130
135
Processeur hôte
• ECC
• Gestion des blocs défectueux
• Égalisation de l'usure
• Pilote de mémoire flash NAND
• Sécurité
Mémoire
Ordinateur hôte
100
131
132
133
134
136

FIG. 1A

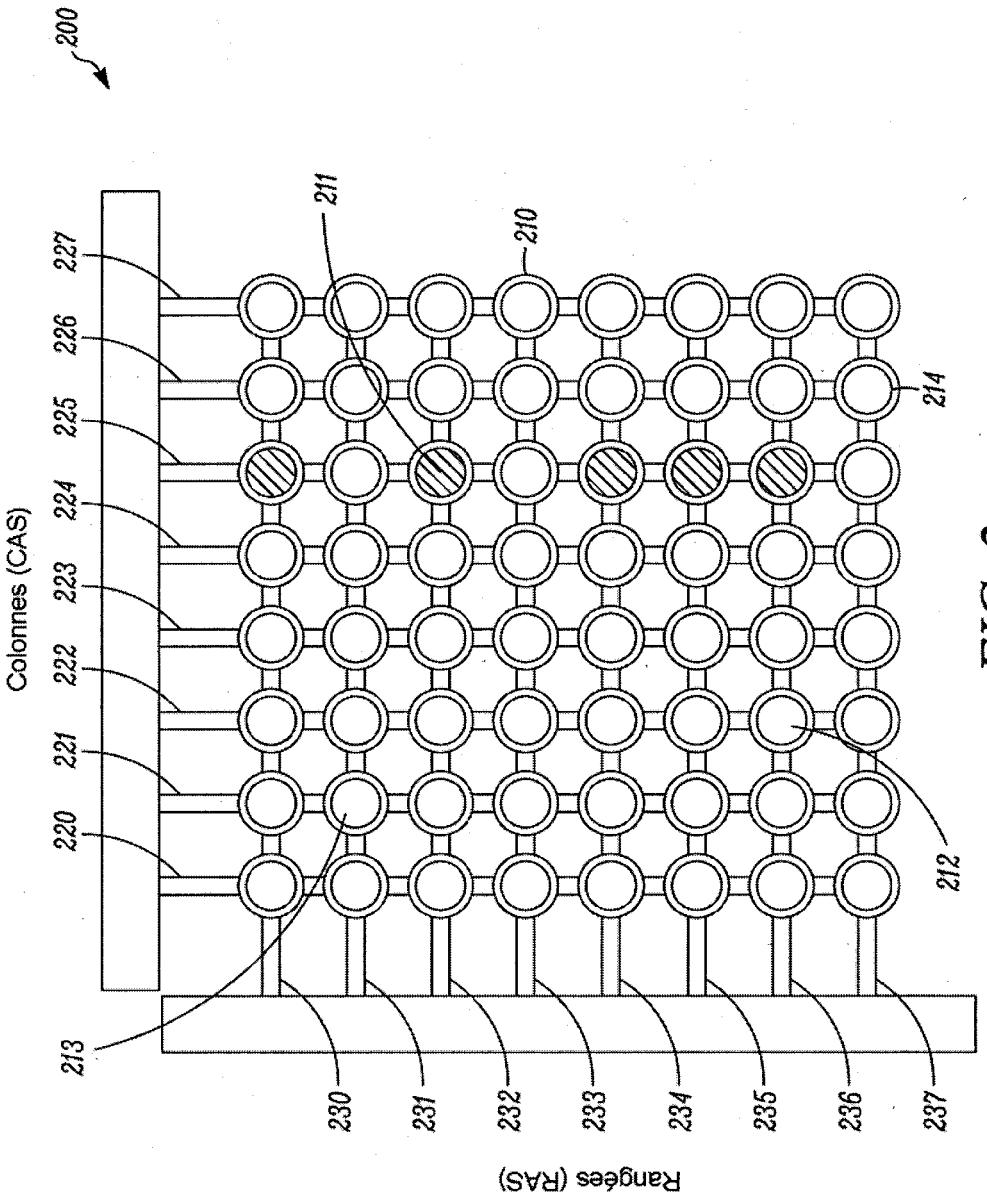
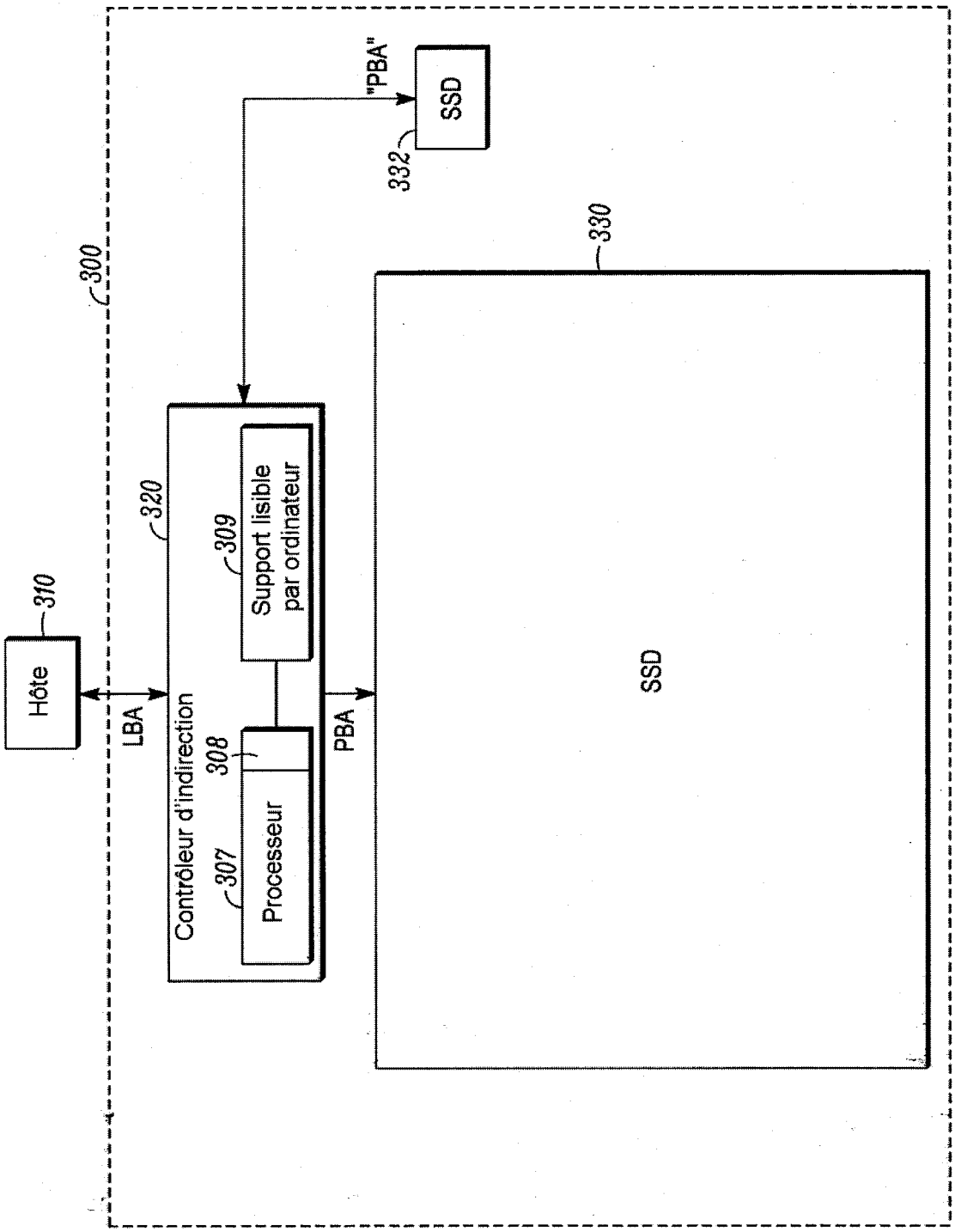

200
211
210
227
226
225
224
223
222
221
220
214
212
213
Colonnes (CAS)
230
231
232
233
234
235
236
237
Rangées (RAS)

FIG. 2

FIG. 3


300
310
Hôte
LBA
320
Contrôleur d'indirection
309
Support lisible par ordinateur
308
307
Processeur
PBA
330
SSD
"PBA"
332
SSD

400

410 Adresse de bloc logique	420 Adresse de bloc physique	430 Nombre de blocs	440 Schéma de chiffrement utilisé
1	2	8	1
2	172	21	1
3	SSD 1	16	2
4	101	32	2

FIG. 4

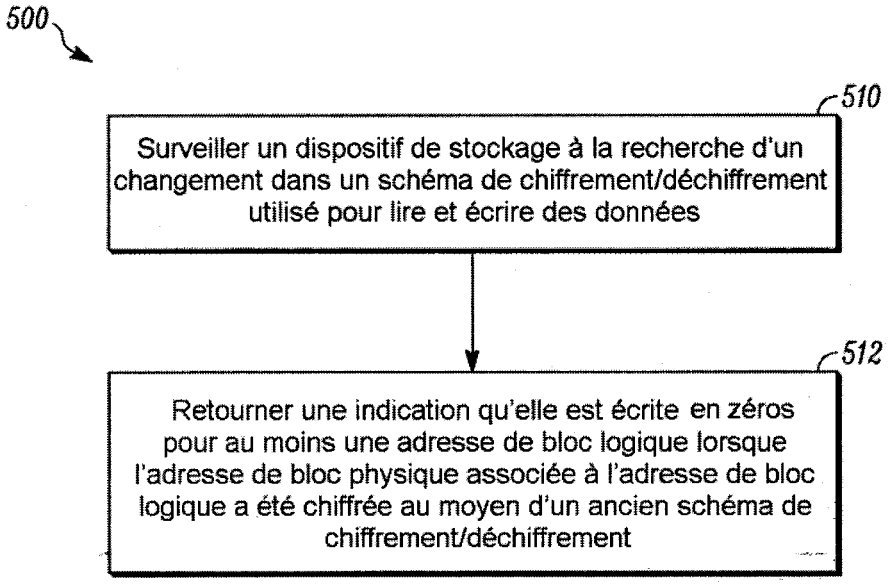


FIG. 5

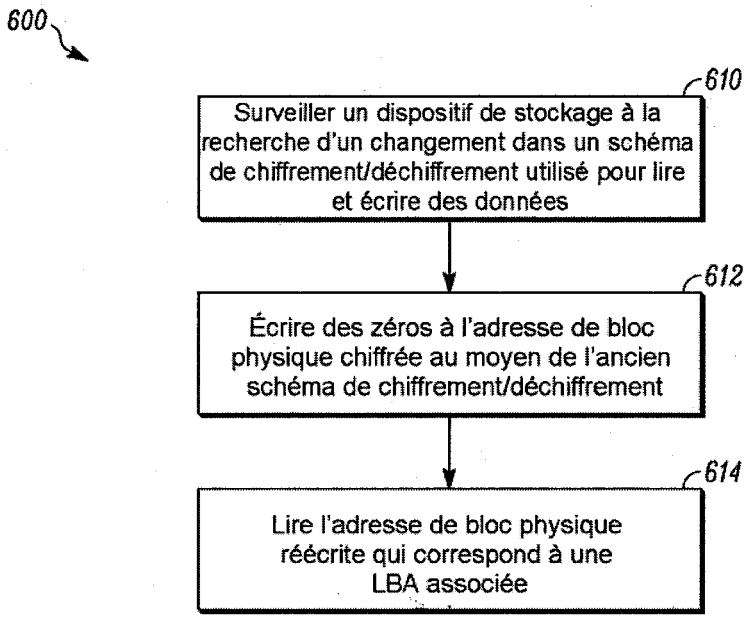


FIG. 6

700

710 Adresse de bloc logique	720 Adresse de bloc physique	730 Nombre de blocs	734 Non valide	740 Schéma de chiffrement utilisé
1	2	8	1	1
2	172	21	1	1
3	SSD 1	16	0	2
4	101	32	0	2

FIG. 7

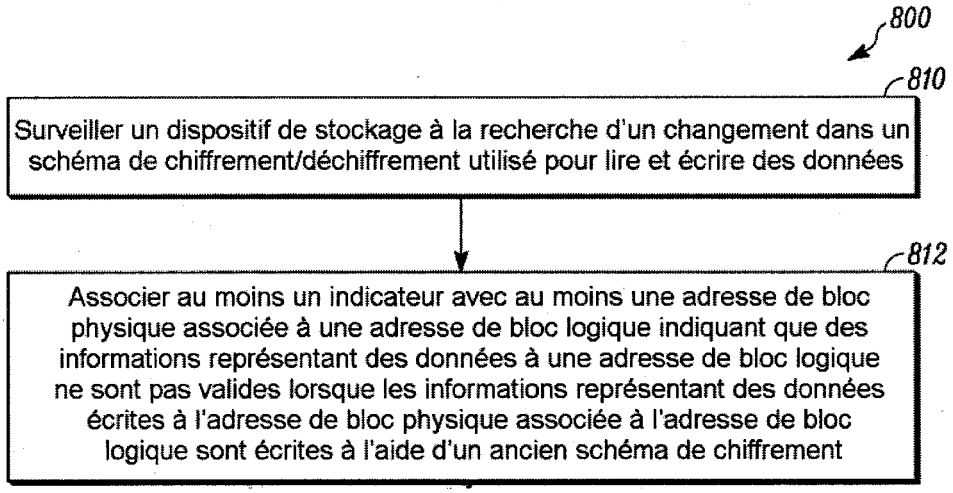


FIG. 8

900

410 Adresse de bloc logique	420 Adresse de bloc physique	430 Nombre de blocs	440 Schéma de chiffrement utilisé
1		8	1
2		21	1
3	SSD 1	16	2
4	101	32	2

FIG. 9

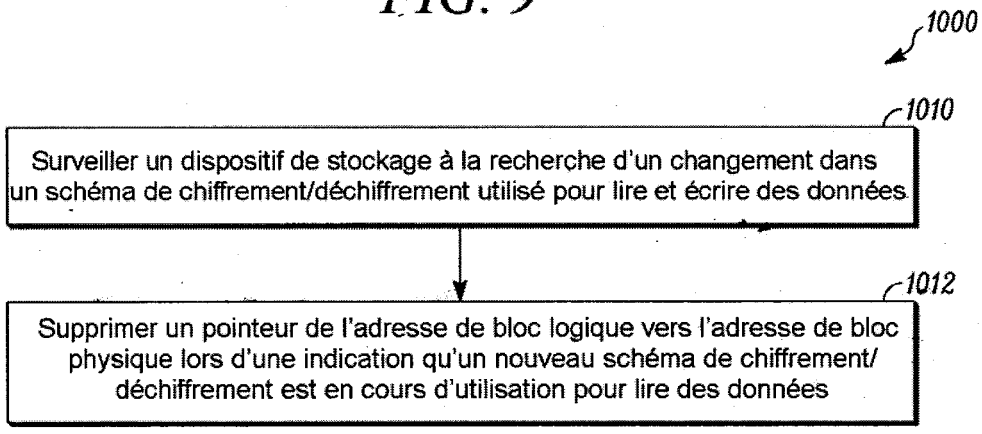


FIG. 10