(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 979 443**

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

(21) **N° d'enregistrement national :** **11 57656**

(51) Int Cl[8] : ***G 06 F 12/14*** *(2013.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 30.08.11.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 01.03.13 Bulletin 13/09.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

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

(71) **Demandeur(s) :** *MAXIM INTEGRATED PRODUCTS, INC.* — US.

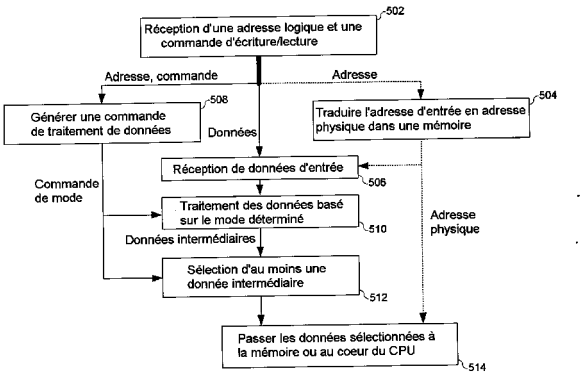
(72) **Inventeur(s) :** DEBOUT VINCENT, VICTOR, ALFRED, LHERMET FRANK et ROLLET ALAIN-CHRISTOPHE.

(73) **Titulaire(s) :** MAXIM INTEGRATED PRODUCTS, INC..

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

(54) MICROCONTROLEUR SECURISE A BASE DE MODE.

(57) Divers modes de réalisation de la présente invention sont liés à des circuits intégrés pour le traitement de données au niveau d'une interface de microcontrôleur, et plus particulièrement à des systèmes, des dispositifs et des procédés de programmation d'un chemin de données au niveau de l'interface de microcontrôleur en sélectionnant au moins un d'une pluralité de modes de traitement de données pour traiter (par ex., chiffrer, déchiffrer, formater, etc.) des données dans le chemin de données. Le microcontrôleur s'interface avec une mémoire. Le procédé est employé pour traiter des données d'entrée fournies par le microcontrôleur pendant une opération d'écriture mémoire, ou des données d'entrée extraites de la mémoire pendant une opération de lecture mémoire, respectivement. Une commande d'écriture/lecture est utilisée pour indiquer l'opération d'écriture ou de lecture mémoire, et une adresse logique est traduite en au moins une adresse physique dans la mémoire. La commande d'écriture/lecture et l'adresse logique sont en outre employées pour déterminer un signal de commande de mode indiquant un mode de traitement de données. Dans divers modes de traitement de données, les données d'entrée sont traitées selon au moins un d'une pluralité de procédés de traitement de données pour aboutir à des données traitées dans différents formats de données. Des données dans différents formats peuvent être stockées dans diverses régions de la mémoire.



FR 2 979 443 - A1

MICROCONTROLEUR SECURISE A BASE DE MODE

ARRIERE-PLAN

A. Domaine technique

La présente invention concerne le domaine du circuit intégré, et plus particulièrement, des systèmes, des dispositifs et des procédés de programmation d'un chemin de données (« data path » en anglais) d'un microcontrôleur en sélectionnant au moins un d'une pluralité de modes de traitement de données pour traiter (par ex., chiffrer, déchiffrer, formater, etc.) des données dans le chemin de données.

B. Arrière-plan de l'invention

Un microcontrôleur est normalement un circuit intégré unique comprenant un cœur d'unité centrale de traitement (CPU pour central processing unit), une mémoire, et des périphériques d'entrée/sortie (E/S). Le cœur de CPU va de processeurs simples de 3 bits à des processeurs complexes de 22 bits ou de 54 bits. Un microcontrôleur compatible 8051 communément utilisé est basé sur un cœur de CPU de 8 bits. Les périphériques d'E/S sont utilisés pour interfacer le microcontrôleur avec des dispositifs d'E/S standard, comme des capteurs et des afficheurs à cristaux liquides (LCD pour « liquid crystal display» en anglais), et des interfaces de communication série sont normalement utilisées dans les périphériques d'E/S. La mémoire dans le microcontrôleur inclut une mémoire vive (RAM pour « random access memory » en anglais) non volatile et une mémoire morte (ROM pour « read-only memory » en anglais) pour stocker des données et des

programmes, respectivement. L'architecture du microcontrôleur peut varier pour inclure plus de cœurs de CPU, de mémoire ou de fonctions d'E/S pour diverses applications.

Un microcontrôleur sécurisé est utilisé pour des applications qui impliquent des opérations de confiance sur des actifs de valeur dans un environnement non sécurisé où un voleur ou un pirate informatique peut avoir accès à des cœurs de processeur, des dispositifs de mémoire ou des périphériques d'E/S qui sont utilisés pour communiquer et traiter des données sensibles. Ces données sensibles peuvent inclure des numéros de compte, des codes d'accès, des transactions financières/soldes de compte, la gestion des droits, le comptage (par ex., énergie, unités), des algorithmes de programme et d'autres informations. Le microcontrôleur sécurisé utilise une RAM non volatile, par ex., une mémoire flash, plutôt qu'une ROM pour le stockage de programmes, et des fonctions de sécurité améliorées additionnelles sont employées pour éviter les accès non autorisés. A ce jour, le microcontrôleur sécurisé a été appliqué dans une large gamme d'applications cruciales du point de vue de la sécurité comme la banque électronique, les transactions commerciales, et le contrôle d'accès à la TV payante, ou toute application qui requiert la protection de logiciels et de procédés propriétaires.

Etant donné que des programmes et des données peuvent être stockés dans une mémoire externe du microcontrôleur sécurisé, la sécurité des données et l'intégrité des données sont deux menaces distinctes que la mémoire externe d'un microcontrôleur sécurisé doit prendre en compte. La première menace est la divulgation d'informations sensibles (c'est-à-dire, la sécurité des données) où des données confidentielles sont révélées et la faiblesse d'un programme est exposée. La seconde menace est la modification du comportement de l'application (c'est-à-dire, l'intégrité des données) qui implique que des programmes et des données soient modifiés dans la mémoire externe et se solde par un problème quant à l'intégrité des données.

Le microcontrôleur sécurisé est conçu pour offrir un niveau de sécurité aux données stockées dans la mémoire externe. Par exemple, la sécurité physique est établie contre la sonde (« probing » en anglais), et un exemple est l'utilisation d'une protection anti-violation (« anti-tampering enclosure » en anglais. Cette solution peut être onéreuse et

ne couvre pas de nouvelles méthodes d'attaque basées sur l'injection de fautes à partir d'une défaillance dans l'alimentation électrique, de la lumière, d'un laser synchrone ou asynchrone, ou de particules radioactives. Les fonctions de sécurité peuvent également comprendre le chiffrement de mémoire où des données et des adresses stockées dans la mémoire sont chiffrées ou déchiffrées pendant le processus d'échange de données. En conséquence, le périmètre de sécurité physique peut être limité au microcontrôleur tandis que la mémoire externe et ses bus de communication peuvent rester exposés physiquement.

Un contrôle d'intégrité des données est mis en œuvre pour les programmes et les données stockés dans la mémoire externe. Le contrôle d'intégrité des données est utilisé pour détecter toute corruption volontaire ou involontaire entre ce qui a été envoyé pour l'écriture dans la mémoire par le microcontrôleur et ce qui a été stocké dans la mémoire. La figure 1 illustre un microcontrôleur sécurisé 102 s'interfaçant avec une mémoire externe 104 où les préoccupations liées à la sécurité des données et à l'intégrité des données susmentionnées sont considérées. Le microcontrôleur sécurisé 102 comprend un cœur de CPU 106, un bloc de chiffrement et de protection d'intégrité 108, un contrôleur de mémoire 110, un stockage de clé 112 et des bus pour les données, les adresses et les clés. Des procédés pour la vérification d'intégrité, le chiffrement de données ou le déchiffrement de données sont incorporés dans le bloc de chiffrement et de protection d'intégrité 108. Pendant des cycles d'écriture ou de lecture mémoire, le bloc 108 chiffre les données en provenance du cœur de CPU 106 en données de charge utile (ou « payload data » en anglais) pour le stockage dans la mémoire 104 ou déchiffre les données de charge utile en provenance de la mémoire 104 en données reçues par la suite par le cœur de CPU 106, respectivement.

Résumé de l'invention

Divers modes de réalisation de la présente invention sont liés à des circuits intégrés pour le traitement de données au niveau d'une interface de microcontrôleur, et plus particulièrement à des systèmes, des dispositifs et des procédés de programmation d'un chemin de données au niveau de l'interface de microcontrôleur en sélectionnant au moins un d'une pluralité de modes de traitement de données pour

traiter (par ex., chiffrer, déchiffrer, formater, etc.) des données dans le chemin de données. Le procédé est employé pour traiter des données d'entrée fournies par le microcontrôleur pendant une opération d'écriture mémoire, ou des données d'entrée extraites de la mémoire pendant une opération de lecture mémoire, respectivement. Une commande d'écriture/lecture est utilisée pour indiquer l'opération d'écriture ou de lecture mémoire, et une adresse logique est traduite en au moins une adresse physique dans la mémoire. La commande d'écriture/lecture et l'adresse logique sont en outre employées pour déterminer un signal de commande de mode indiquant un mode de traitement de données. Dans divers modes de traitement de données, les données d'entrée sont traitées selon au moins un d'une pluralité de procédés de traitement de données pour aboutir à des données traitées dans différents formats de données.

Un système de traitement de données à base de mode est utilisé comme une unité matérielle dédiée au niveau d'une interface entre un microcontrôleur et une mémoire. Le système de traitement de données à base de mode comprend un traducteur d'adresse, un générateur de mode, et une unité de traitement de données multimode. Le traducteur d'adresse traduit l'adresse d'entrée en au moins une adresse physique dans la mémoire. Le générateur de mode est couplé pour recevoir l'adresse d'entrée et une commande d'écriture/lecture et génère un signal de commande de mode associé à un mode de traitement de données. L'unité de traitement de données multimode génère au moins une donnée traitée selon le mode de traitement de données.

Une unité de traitement de données multimode est employée au niveau d'une interface entre un microcontrôleur et une mémoire pour mettre en œuvre un traitement de données à base de mode. L'unité de traitement de données multimode comprend un premier démultiplexeur, un 2ème démultiplexeur, une pluralité d'unités de traitement de données, un premier multiplexeur et un 2ème multiplexeur. Certaines unités de traitement de données sont employées avec le premier démultiplexeur et le premier multiplexeur pour traiter (par ex., chiffrer, formater) des données d'entrée en provenance du microcontrôleur pendant des cycles d'écriture mémoire. Certaines unités de traitement de données sont employées avec le 2ème multiplexeur et le 2ème démultiplexeur pour traiter (par ex., déchiffrer,

reformater) des données d'entrée en provenance de la mémoire pendant des cycles de lecture mémoire

Certaines caractéristiques et avantages de la présente invention ont été décrits de manière générale dans cette section de résumé ; toutefois, des caractéristiques, avantages et modes de réalisation additionnels sont présentés ici ou seront évidents pour un homme du métier ordinaire au vu des dessins, du mémoire, et des revendications de celle-ci. En conséquence, il convient de comprendre que la portée de l'invention ne doit pas être limitée par les modes de réalisation particuliers décrits dans cette section de résumé.

BREVE DESCRIPTION DES DESSINS

Il va maintenant être fait référence aux modes de réalisation de l'invention, dont des exemples sont illustrés sur les figures jointes. Ces figures sont destinées à être illustratives, non limitatives. Bien que l'invention soit généralement décrite dans le contexte de ces modes de réalisation, il convient de comprendre que cela n'est pas destiné à limiter la portée de l'invention à ces modes de réalisation particuliers.

La figure (« FIG. ») 1 illustre un microcontrôleur sécurisé s'interfaçant avec une mémoire externe où les préoccupations de sécurité et d'intégrité sont considérées.

La figure 2 illustre un schéma de principe d'un système de microcontrôleur sécurisé comprenant un microcontrôleur sécurisé s'interfaçant avec une mémoire selon divers modes de réalisation de l'invention.

La figure 3 illustre un schéma de principe d'un système de traitement de données à base de mode au niveau d'une interface de microcontrôleur selon divers modes de réalisation de l'invention.

La figure 4 illustre un schéma de principe d'une unité de traitement de données multimode selon divers modes de réalisation de l'invention.

La figure 5 illustre un procédé de mise en œuvre d'un traitement de données à base de mode dans un microcontrôleur selon divers modes de réalisation de l'invention.

DESCRIPTION DETAILLEE DES MODES DE REALISATION PREFERES

Divers modes de réalisation de la présente invention sont liés à des circuits intégrés pour le traitement de données au niveau d'une interface de microcontrôleur, et plus particulièrement à des systèmes, des dispositifs et des procédés de programmation d'un chemin de données au niveau de l'interface de microcontrôleur en sélectionnant au moins un d'une pluralité de modes de traitement de données pour traiter (par ex., chiffrer, déchiffrer, formater, etc.) des données dans le chemin de données. Dans certains modes de réalisation, ces dispositifs et ces systèmes de traitement de données à base de mode sont des unités matérielles dédiées placées au niveau d'une interface entre le microcontrôleur et une mémoire. Dans la description suivante, à des fins d'explication, des détails spécifiques sont exposés afin de procurer une bonne compréhension de l'invention. Toutefois, il sera évident pour un homme du métier que l'invention puisse être pratiquée sans ces détails. Un homme du métier reconnaîtra que les modes de réalisation de la présente invention, décrits ci-dessous, peuvent être effectués de diverses manières et en utilisant diverses structures. L'homme du métier reconnaîtra également que des modifications, applications, et modes de réalisation additionnels soient dans sa portée, de même que des domaines additionnels dans lesquels l'invention peut procurer une utilité. En conséquence, les modes de réalisation décrits ci-dessous sont illustratifs de modes de réalisation spécifiques de l'invention et sont destinés à éviter d'obscurcir l'invention.

La référence dans le mémoire à « un mode de réalisation » (point de vue quantitatif) ou « un mode de réalisation » (point de vue indéfini) signifie qu'une particularité, structure, caractéristique ou fonction particulière décrite en relation avec le mode de réalisation est incluse dans au moins un mode de réalisation de l'invention. L'apparition de l'expression « dans un mode de réalisation » (point de vue quantitatif), « dans un mode de réalisation » (point de vue indéfini), ou similaire à divers endroits dans le mémoire ne font pas forcément toutes référence au même mode de réalisation.

Les connexions entre composants ou entre étapes de procédé sur les figures ne sont pas restreintes à des connexions qui sont effectuées directement. Au contraire, les connexions illustrées sur les figures entre

composants ou étapes de procédé peuvent être modifiées ou sinon changées en y ajoutant des composants ou étapes de procédé intermédiaires, sans s'écarter des enseignements de la présente invention.

La figure 2 illustre un schéma de principe 200 d'un système de microcontrôleur sécurisé comprenant un microcontrôleur sécurisé 220 s'interfaçant avec une mémoire 240 selon divers modes de réalisation de l'invention. Le microcontrôleur sécurisé 220 comprend un cœur de CPU 206, un bloc de chiffrement et de protection d'intégrité 208, un contrôleur de mémoire 210, un stockage de clé 212 et des bus pour les données, les adresses et les clés. Dans la présente invention, le microcontrôleur sécurisé 220 comprend en outre un générateur de mode 218. Le générateur de mode 218 est couplé pour recevoir une adresse logique et une commande d'écriture/lecture, et génère un signal de commande de mode qui est utilisé pour déterminer un procédé de traitement de données selon un mode de traitement de données spécifique. L'adresse logique est une adresse de données relative à l'intérieur d'un bloc de données.

La mémoire 240 qui s'interface avec le microcontrôleur sécurisé 220 peut comprendre diverses mémoires externes incluant une mémoire vive (RAM), une mémoire morte (ROM) et une mémoire flash. La mémoire 240 peut être partitionnée pour le stockage en une région de contenu en clair 214 et une région de données de charge utile 216. Les données de charge utile comprennent normalement des en-têtes/en-queues de données et des données traitées qui sont des données chiffrées ou formatées associées à des informations confidentielles (par ex., des noms d'utilisateurs, des mots de passe, des transactions, des programmes etc.). Une adresse physique est utilisée pour identifier un emplacement à l'intérieur de la mémoire 240.

Pendant un cycle d'écriture mémoire, des données d'entrée sont prétraitées avant d'être transmises à et stockées dans la mémoire 240. Le cœur de CPU 206 génère les données d'entrée, une adresse logique et une commande d'écriture/lecture. La commande d'écriture/lecture est utilisée pour déterminer un signal de commande de mode. Le bloc de chiffrement et de protection d'intégrité 208 est couplé pour recevoir les données d'entrée, l'adresse logique et le signal de commande de mode. Le signal de commande de mode est associé à un mode de traitement de

données. Le bloc 208 traite en outre les données et génère des données de charge utile (c'est-a-dire, les données traitées) sur la base d'au moins un procédé de traitement de données. Le procédé de traitement de données est sélectionné parmi une pluralité de procédés de traitement de données sur la base du mode de traitement de données. De plus, le bloc 208 traduit également l'adresse logique en au moins une adresse physique pour le stockage des données de charge utile. Le contrôleur de mémoire 210 stocke les données de charge utile comme spécifié dans l'adresse physique dans la mémoire 240.

Pendant un cycle de lecture mémoire, des données de charge utile (ou « payload data » en anglais) (c'est-à-dire, les données d'entrée) sont post-traitées après être extraites de la mémoire 240. Une adresse logique est fournie par le cœur de CPU 206 pour sélectionner des données de charge utile spécifiques qui sont extraites de la mémoire 240. Le bloc de chiffrement et de protection d'intégrité 208 traduit l'adresse logique en au moins une adresse physique. Un mode de traitement de données est indiqué par un signal de commande de mode généré par le générateur de mode 218. Le contrôleur de mémoire 210 permet l'accès aux contenus de mémoire dans l'adresse physique où les données de charge utile sont extraites. Au moins un procédé de traitement de données est sélectionné parmi une pluralité de procédés de traitement de données pour obtenir des données traitées sur la base du mode de traitement de données. Le procédé de traitement de données utilisé pour la lecture mémoire peut être l'inverse du procédé de traitement de données employé pour prétraiter les données pour l'écriture mémoire. En conséquence, les données traitées peuvent être utilisées pour un traitement de données subséquent, et en particulier, pour vérifier les données de charge utile.

Plus d'un procédé de traitement de données peut être mis en œuvre dans le bloc de chiffrement et de protection d'intégrité 208 dans un mode de traitement de données. Dans certains modes de réalisation pour une opération d'écriture mémoire, les données d'entrée sont traitées par une pluralité de procédés de traitement de données afin de générer une pluralité de données de charge utile (c'est-à-dire, de données traitées), et l'adresse logique associée est également traduite en une pluralité d'adresses physiques pour le stockage de la pluralité de données de charge utile, respectivement. Dans un mode de réalisation

particulier, les données d'entrée peuvent non seulement être chiffrées pour générer des données de charge utile chiffrées sur la base d'un procédé de chiffrement de données, mais également être employées pour générer des données de contrôle d'intégrité sur la base d'un procédé de vérification d'intégrité. Les données traitées (données de charge utile chiffrées et données de contrôle d'intégrité) sont stockées dans des adresses physiques respectives.

Dans certains modes de réalisation pour une opération de lecture mémoire, au moins une donnée d'entrée (c'est-à-dire, donnée de charge utile) est extraite de la mémoire 240 selon au moins une adresse physique traduite à partir d'une adresse logique. Les données d'entrée sont traitées par au moins un procédé de traitement de données à diverses fins. Dans un mode de réalisation particulier, les données d'entrée incluent des données chiffrées et des données de contrôle d'intégrité. Les données chiffrées peuvent être déchiffrées pour générer des données traitées sur la base d'un procédé de déchiffrement de données, tandis que les données de contrôle d'intégrité sont utilisées pour vérifier l'intégrité des données entre les données traitées et les données originales sur la base d'un procédé de vérification d'intégrité.

La mémoire 240 est partitionnée en une région de contenu en clair 214 et une région de données de charge utile 216. La région de données de charge utile 216 est utilisée pour stocker des données chiffrées ou formatées. Dans la présente invention, la région de données de charge utile 216 peut en outre être partitionnée en diverses régions où chaque région est associée à un format de données. Par conséquent, des données dans des régions différentes sont chiffrées ou formatées différemment selon leurs procédés de chiffrement ou de formatage respectifs. Pour chaque mode de traitement de données, une adresse logique peut être traduite en adresses physiques correspondant à diverses régions, et des procédés de traitement de données correspondants sont sélectionnés pour traiter les données d'entrée conformément.

La figure 3 illustre un schéma de principe 300 d'un système de traitement de données à base de mode au niveau d'une interface de microcontrôleur selon divers modes de réalisation de l'invention. Le d'un système de traitement de données à base de mode 300 est couplé pour recevoir une adresse logique, une commande d'écriture/lecture et

des données d'entrée. Conformément à la commande d'écriture/lecture, des données d'entrée peuvent être des données d'un côté hôte (par ex., le cœur de CPU 206) ou des données de charge utile d'un côté interface (par ex., la mémoire 240). Le système 300 comprend un générateur de mode 318, un traducteur d'adresse 302 et une unité de traitement de données multimode 304. Le traducteur d'adresse traduit directement l'adresse logique en au moins une adresse physique. Le générateur de mode détermine un mode de traitement de données, et génère un signal de commande de mode selon l'adresse logique et la commande d'écriture/lecture. Le signal de commande de mode est en outre utilisé par l'unité de traitement de données multimode 304 pour générer des données traitées selon au moins un procédé de traitement de données. Dans certains modes de réalisation, un mode de traitement de données peut concerner plus d'un procédé de traitement de données, et aboutir à plus d'une donnée traitée et plus d'une adresse physique. Par conséquent, le chemin de données est programmé selon le mode de traitement de données au niveau de l'interface du microcontrôleur avec la mémoire.

Le signal de commande de mode inclut de multiples bits, et est associé à une pluralité de modes de traitement de données. Le signal de commande de mode est dérivé principalement de l'adresse logique d'entrée dans le générateur de mode 318, tandis que la commande d'écriture/lecture est utilisée pour différencier si une opération d'écriture ou de lecture mémoire est impliquée. En particulier, pendant les processus d'écriture ou de lecture mémoire, le signal de commande de mode configure l'unité de traitement de données multimode pour chiffrer/formater les données du côté hôte ou déchiffrer/reformater les données de charge utile chiffrées/formatées du côté interface, respectivement. Par conséquent, le signal de commande de mode généré par le générateur de mode 318 sélectionne efficacement un chemin de données qui peut être de l'une ou l'autre direction entre le côté hôte et le côté interface.

Le chemin de données entre le côté hôte et le côté interface est programmé selon le mode de traitement de données. Un flux de données peut comprendre une séquence de données d'entrée associée à des modes de traitement de données différents, et par conséquent, des données d'entrée dans la séquence peuvent être associées à des

chemins de données différents. La sécurité des données est améliorée pour le flux de données en raison d'un tel chemin de données programmable. Dans divers modes de réalisation de la présente invention, le générateur de mode 318 et l'unité de traitement de données multimode 304 sont le matériel dédié pour introduire ce chemin de données programmable comme une fonction de sécurité des données.

La figure 4 illustre un schéma de principe 400 d'une unité de traitement de données multimode selon divers modes de réalisation de l'invention. L'unité de traitement de données multimode 400 est couplée pour recevoir un signal de commande de mode et des données d'entrée. Conformément à la commande d'écriture/lecture, les données d'entrée peuvent être des données d'un côté hôte (par ex., le cœur de CPU 206) ou des données de charge utile d'un côté interface (par ex., la mémoire 240). L'unité de traitement de données multimode 400 comprend un premier démultiplexeur 402, un premier multiplexeur 404, un 2ème multiplexeur 406, un 2ème démultiplexeur 408 et une pluralité d'unités de traitement de données 450. La pluralité d'unités de traitement de données 450 sont groupées en deux ensembles 452 et 454. L'ensemble 452 comprend les unités de traitement de données 412, 414 et 416 qui sont employées avec le premier démultiplexeur 402 et le premier multiplexeur 404 pour traiter (par ex., chiffrer, formater) les données d'entrée en données de charge utile pendant des cycles d'écriture mémoire. L'ensemble 454 comprend les unités de traitement de données 418, 420 et 422 qui sont employées avec le 2ème multiplexeur 406 et le 2ème démultiplexeur 408 pour traiter les données d'entrée et fournir les données traitées au cœur de CPU 202 pendant des cycles de lecture mémoire. Lorsqu'une première unité de traitement de données dans l'ensemble 452 est utilisée pour chiffrer ou formater des données d'entrée en données de charge utile, une seconde unité de traitement de données correspondante dans l'ensemble 454 peut être utilisée pour déchiffrer ou reformater les données de charge utile en données originales respectives. Les procédés de traitement de données respectifs employés dans les première et seconde unités de traitement de données sont l'inverse l'un de l'autre.

Pendant un cycle d'écriture mémoire, le démultiplexeur 402 fournit les données d'entrée à au moins une de la pluralité d'unités de

traitement de données (DPU pour « data processing unit » en anglais) 412, 414 et 416. L'unité de traitement de données génère des données traitées (c'est-à-dire, données de charge utile chiffrées ou formatées), dont au moins une est sélectionnée par le multiplexeur 404 comme une sortie vers le contrôleur de mémoire 210. Pendant un cycle de lecture mémoire, le démultiplexeur 408 est couplé pour recevoir une pluralité de données d'entrée (c'est-à-dire, données de charge utile chiffrées/formatées) stockées dans la mémoire, et fournir les données de charge utile à au moins une de la pluralité d'unités de traitement de données 418, 420 et 422. L'unité de traitement de données déchiffre les données de charge utile en données traitées, et au moins une des données traitées est sélectionnée par le multiplexeur 406 comme une sortie vers le cœur de CPU 202. Les multiplexeurs 404, 406 et les démultiplexeurs 402, 408 sont tous commandés par un signal de commande de mode.

Dans un mode de réalisation, l'unité de traitement de données est basée sur un procédé de contournement où un chemin de données direct est formé entre le cœur de CPU 202 et la mémoire 240. Des données d'entrée de leur format d'origine (c'est-à-dire, en texte clair) sont stockées directement dans ou récupérées depuis la mémoire.

Dans un mode de réalisation, l'unité de traitement de données configure simplement le format des données d'entrée selon leurs adresses et le mode d'écriture/lecture, tandis qu'une autre unité de traitement de données inverse peut rétablir les données formatées à leur format d'origine pendant un cycle de lecture mémoire.

Dans un mode de réalisation, l'unité de traitement de données chiffre les données d'entrée en données de charge utile en utilisant un procédé de chiffrement de données basé sur une clé, une adresse logique ou le mode d'écriture/lecture. Une unité de traitement de données inverse peut également exister pour déchiffrer les données de charge utile en utilisant un procédé de déchiffrement de données basé sur la clé, l'adresse logique ou le mode d'écriture/lecture. Bien que des procédés de chiffrement/déchiffrement de données propriétaires puissent être appliqués, un procédé de contrôle par redondance cyclique (CRC) standard peut être utilisé de façon appropriée pour chiffrer/déchiffrer les données, mais l'attaqueur peut facilement

inverser le processus de chiffrement/déchiffrement, et une sécurité de haut niveau peut ne pas être fournie par un procédé CRC.

Dans un mode de réalisation, un procédé de vérification d'intégrité est employé dans une unité de traitement de données pour générer des données de contrôle d'intégrité qui seront stockées par la suite dans la mémoire identifiée par une adresse physique. Plusieurs procédés de vérification d'intégrité peuvent être employés. Le procédé le plus simple est une vérification de parité pair/impair d'1 bit, où un bit de contrôle d'intégrité est généré pour maintenir une parité paire ou impaire parmi tous les bits dans les données. Des procédés de vérification d'intégrité alternatifs vont d'un simple contrôle par redondance cyclique (CRC) qui a une faible résistance de sécurité à des procédés forts et éprouvés, comme le code d'authentification de message (MAC pour « message authentication code » en anglais).

Dans certains modes de réalisation, deux unités de traitement de données peuvent être impliquées dans un mode de traitement de données activé par le signal de commande de mode. Les données résultantes peuvent être dans deux formats stockés dans deux régions de mémoire différentes. En particulier, pendant des cycles d'écriture mémoire, des données de contrôle d'intégrité sont communément générées en compagnie des données de charge utile qui peuvent être identiques à, formatées depuis, ou chiffrées depuis les données d'entrée originales. Les données de charge utile et les données de contrôle d'intégrité sont générées par une première unité de traitement de données et une deuxième unité de traitement de données, respectivement. Pendant un cycle de lecture mémoire, les données de charge utile qui peuvent être d'origine, formatées ou chiffrées sont rétablies en données d'origine dans une troisième unité de traitement de données, et la validité des données rétablies est vérifiée sur la base des données de contrôle d'intégrité dans une quatrième unité de traitement de données. Les première et troisième unités de traitement de données sont l'inverse l'une de l'autre, tandis que dans la quatrième unité de traitement de données, les données d'origine rétablies peuvent être utilisées pour regénérer des données de contrôle d'intégrité pour la comparaison avec les données de contrôle d'intégrité extraites de la mémoire, et les données de contrôle d'intégrité extraites de la mémoire peuvent également subir un certain traitement pour vérifier la validité

des données. Deux unités de traitement de données sont impliquées pour générer deux résultats pour chaque mode de traitement de données correspondant à une opération de lecture ou d'écriture mémoire.

Dans un autre mode de réalisation particulier, des données ont besoin d'être stockées dans la mémoire 240 sous deux formes, un texte clair et une forme chiffrée. Une première unité de traitement de données comprenant un bus de contournement est employée pour permettre le stockage de données en texte clair dans une première région de mémoire, et une seconde unité de traitement de données mettant en œuvre un procédé de chiffrement de données est également activée pour générer des données de charge utile sous la forme chiffrée pour le stockage dans une seconde région de mémoire. Un traitement de données parallèle est mis en œuvre par l'unité de traitement de données multimode 400 pour éviter un traitement de données logicielles ou une reconfiguration de chemin de données compliquée pour basculer entre traitement de données.

Une adresse physique peut être associée à plus d'une adresse logique, et ainsi, différents procédés de traitement de données sont applicables au contenu au niveau de l'adresse physique. Dans certains modes de réalisation, l'unité de traitement de données chiffre les données d'entrée en données de charge utile au niveau d'une adresse physique en utilisant un procédé de chiffrement de données basé sur une clé et une adresse logique. Pendant un cycle de lecture mémoire, la même adresse logique peut être utilisée pour extraire et rétablir les données d'entrée en utilisant un procédé de déchiffrement de données basé sur la même clé, tandis qu'une adresse logique différente peut également être appliquée pour relire ces données en utilisant un mode de texte clair. Par conséquent, indépendamment de la forme des données originales, l'utilisation de diverses adresses logiques permet qu'une donnée stockée au niveau d'une adresse physique soit extraite en différentes formes de données pendant un cycle de lecture mémoire.

La figure 5 illustre un procédé 500 de mise en œuvre d'un traitement de données à base de mode dans un microcontrôleur selon divers modes de réalisation de l'invention. Une adresse logique et une commande d'écriture/lecture sont reçues à l'étape 502. La commande d'écriture/lecture est utilisée pour spécifier s'il s'agit d'un processus

d'écriture ou de lecture mémoire. L'adresse logique identifie l'emplacement relatif des données d'entrée à l'intérieur d'un bloc de données. A la fois dans les processus d'écriture et de lecture mémoire, l'adresse logique est traduite en au moins une adresse physique dans la mémoire à l'étape 504.

Des données d'entrée sont reçues à l'étape 506. Les données d'entrée peuvent être soit des données d'un côté hôte (par ex., le cœur de CPU 206) soit des données chiffrées/formatées d'un côté interface (par ex., la mémoire 240). Pour l'écriture mémoire, des données d'entrée sont d'abord traitées puis stockées dans la mémoire selon l'adresse physique, tandis que pour la lecture mémoire, des données d'entrée sont les données de charge utile extraites d'abord de l'adresse physique puis traitées dans les étapes subséquentes.

A l'étape 508, l'adresse d'entrée et la commande d'écriture/lecture sont employées pour générer un signal de commande de mode qui spécifie un mode de traitement de données pour un traitement de données subséquent. Les données d'entrée sont traitées par au moins un mode de traitement de données déterminé par le signal de commande de mode à l'étape 508. Dans divers modes de réalisation, les données d'entrée peuvent être directement transférées, chiffrées, formatées, déchiffrées, ou inversement formatées pour aboutir à des données traitées selon le mode de traitement de données. Au moins une des données traitées est sélectionnée pour la sortie à l'étape 512. Dans une étape 514 subséquente, la donnée traitée sélectionnée pour la sortie est passée à la mémoire 240 dans une opération d'écriture mémoire ou vers le cœur de CPU 206 dans une opération de lecture mémoire, respectivement.

Un homme du métier reconnaîtra que ce système ou dispositif de traitement de données à base de mode est une unité matérielle dédiée qui peut éviter efficacement des programmes logiciels complexes sinon nécessaires. Le taux de traitement de données et la capacité de débit du microcontrôleur sont également améliorés.

Un homme du métier reconnaîtra également qu'un tel traitement de données à base de mode est applicable pour configurer une mémoire fonctionnant comme un registre d'entrée/sortie au niveau de l'interface d'un microcontrôleur sécurisé avec un composant externe. Un flux de données est formaté ou chiffré avant d'être transmis du microcontrôleur

sécurisé au composant externe. Dans un mode de réalisation, des paquets de données en provenance d'un microcontrôleur sécurisé sont traités et stockés dans la mémoire pour la transmission via un réseau Ethernet, et divers modes de traitement de données peuvent être utilisés selon le domaine des paquets de données. Un tel traitement de données à base de mode permet au réseau Ethernet d'obtenir un avantage du chiffrement/codage/formatage à la volée, et le débit des données est amélioré.

Bien que l'invention soit susceptible de diverses modifications et formes alternatives, des exemples spécifiques de celle-ci ont été montrés sur les dessins et sont décrits ici en détail. Toutefois, il convient de comprendre que l'invention ne doive pas être limitée aux formes particulières décrites, mais au contraire, l'invention doit couvrir toutes les modifications, équivalents, et alternatives se trouvant à l'intérieur de la portée des revendications annexées.

REVENDICATIONS

1. Procédé de stockage de données dans une mémoire s'interfaçant avec un microcontrôleur sécurisé, le procédé comprenant :

la génération (502) d'une adresse logique, de données d'entrée et d'une commande d'écriture/lecture dans le microcontrôleur, la commande d'écriture/lecture identifiant une opération de lecture ou d'écriture mémoire ;

la traduction (504) de l'adresse logique en au moins une adresse physique dans la mémoire qui est partitionnée en une pluralité de régions ;

la génération (508) d'un signal de commande de mode sur la base de l'adresse logique et de la commande d'écriture/lecture, le signal de commande de mode identifiant un mode de traitement de données parmi une pluralité de modes de traitement de données ;

l'association du mode de traitement de données à au moins un procédé de traitement de données sélectionné parmi une pluralité de procédés de traitement de données, chaque procédé de traitement de données étant associé à au moins une région de la mémoire ;

la génération de données devant être stockées à l'intérieur de la au moins une région de la mémoire selon le au moins un procédé de traitement de données sélectionné.

2. Procédé de stockage de données dans une mémoire s'interfaçant avec un microcontrôleur sécurisé selon la revendication 1, dans lequel la pluralité de procédés de traitement de données comprend un procédé de contournement contournant les données d'entrée, et les données traitées sont en texte clair identiques aux données d'entrée.

3. Procédé de stockage de données dans une mémoire s'interfaçant avec un microcontrôleur sécurisé selon l'une quelconque des revendications 1 à 2, dans lequel la pluralité de procédés de traitement de données comprend au moins un procédé de vérification d'intégrité utilisé pour générer des données de contrôle d'intégrité correspondant aux données d'entrée.

4. Procédé de stockage de données dans une mémoire s'interfaçant avec un microcontrôleur sécurisé selon l'une quelconque des revendications 1 à 3, dans lequel la pluralité de procédés de traitement de données comprend au moins un procédé de formatage

utilisé pour varier le format des données d'entrée pour le stockage dans la mémoire.

5. Procédé de stockage de données dans une mémoire s'interfaçant avec un microcontrôleur sécurisé selon l'une quelconque des revendications 1 à 4, dans lequel la pluralité de procédés de traitement de données comprend au moins un procédé de chiffrement de données pour chiffrer les données d'entrée.

6. Procédé de stockage de données dans une mémoire s'interfaçant avec un microcontrôleur sécurisé selon l'une quelconque des revendications 1 à 5, où le au moins un procédé de chiffrement est basé sur une clé extraite d'un stockage de clé.

7. Procédé de stockage de données dans une mémoire s'interfaçant avec un microcontrôleur sécurisé selon l'une quelconque des revendications 1 à 6, dans lequel au moins un de la pluralité de procédés de traitement de données est propriétaire.

8. Procédé de stockage de données dans une mémoire s'interfaçant avec un microcontrôleur sécurisé selon l'une quelconque des revendications 1 à 7, dans lequel un de la pluralité de modes de traitement de données implique deux procédés de traitement de données, de sorte que deux données traitées soient générées, et l'adresse logique est traduite en deux adresses physiques qui sont localisées à l'intérieur de régions différentes dans la mémoire.

9. Procédé de stockage de données dans une mémoire s'interfaçant avec un microcontrôleur sécurisé selon la revendication 8, dans lequel les deux procédés de traitement de données incluent un procédé de contournement et un procédé de chiffrement de données, respectivement, de sorte que les deux données traitées soient en texte clair et dans un format chiffré, respectivement.

10. Procédé de stockage de données dans une mémoire s'interfaçant avec un microcontrôleur sécurisé selon la revendication 8, dans lequel les deux procédés de traitement de données sont un procédé de chiffrement de données et un procédé de vérification d'intégrité, respectivement, de sorte que les deux données traitées soient une données chiffrée et une donnée de contrôle d'intégrité, respectivement.

11. Microcontrôleur à base de mode, comprenant :

un traducteur d'adresse (302), couplé pour recevoir une adresse d'entrée, le traducteur d'adresse étant agencé pour traduire l'adresse d'entrée en au moins une adresse physique dans une mémoire externe qui s'interface au microcontrôleur ;

un générateur de mode (318), couplé pour recevoir l'adresse d'entrée et une commande d'écriture/lecture, le générateur de mode étant agencé pour générer un signal de commande de mode qui identifie un mode de traitement de données parmi une pluralité de modes de traitement de données selon la commande d'écriture/lecture et l'adresse d'entrée ;

une unité de traitement de données multimode (304), couplée pour recevoir le signal de commande de mode et des données d'entrée, l'unité de traitement de données multimode étant agencée pour générer au moins une donnée traitée sur la base d'au moins un d'une pluralité de procédés de traitement de données qui sont identifiés selon le mode de traitement de données ; et

dans lequel la mémoire externe est partitionnée en une pluralité de régions, et chacun de la pluralité de procédés de traitement de données est associé à une de la pluralité de régions dans la mémoire externe.

12. Microcontrôleur à base de mode selon la revendication 11, dans lequel lorsque la commande d'écriture/lecture identifie une opération de lecture mémoire, les données d'entrée sont lues depuis au moins une de la pluralité de régions dans la mémoire externe, et lorsque la commande d'écriture/lecture identifie une opération d'écriture mémoire, la au moins une donnée traitée est stockée dans au moins une région sélectionnée parmi la pluralité de régions dans la mémoire externe.

13. Microcontrôleur à base de mode selon l'une quelconque des revendications 11 à 12, dans lequel dans un mode de traitement de données, l'unité de traitement de données multimode (304) génère deux données traitées à partir des données d'entrée, et les deux données traitées sont chiffrées et en texte clair, respectivement, pour le stockage dans deux régions différentes de la pluralité de régions dans la mémoire externe.

14. Microcontrôleur à base de mode selon l'une quelconque des revendications 11 à 13, dans lequel dans un mode de traitement de

données, l'unité de traitement de données multimode (304) génère deux données traitées à partir des données d'entrée, et les deux données traitées sont une donnée chiffrée et une donnée de contrôle d'intégrité, respectivement, pour le stockage à l'intérieur de deux régions différentes de la pluralité de régions dans la mémoire externe.

15. Microcontrôleur à base de mode selon l'une quelconque des revendications 11 à 14, dans lequel l'unité de traitement de données multimode (304) comprend en outre :

un premier démultiplexeur (402) qui passe les données d'entrée selon le mode de traitement de données pendant une opération d'écriture mémoire ;

un 2ème démultiplexeur (408), couplé à la mémoire externe, le démultiplexeur passe les données d'entrée selon le mode de traitement de données pendant une opération de lecture mémoire ;

une pluralité d'unités de traitement de données (412, 414, 416, 418, 420, 422), couplée aux premier et 2ème démultiplexeurs, la pluralité d'unités de traitement de données génère une pluralité de données traitées selon une pluralité de procédés de traitement de données, où chaque unité de traitement de données est associée à un procédé de traitement de données ;

un premier multiplexeur (404), couplé à la mémoire externe, le premier multiplexeur sélectionne au moins une de la pluralité de données traitées selon le mode de traitement de données pendant l'opération d'écriture mémoire ; et

un 2ème multiplexeur (406) qui sélectionne au moins une de la pluralité de données traitées selon le mode de traitement de données pendant l'opération de lecture mémoire.

16. Microcontrôleur à base de mode selon la revendication 15, dans lequel une unité de traitement de données dans l'unité de traitement de données multimode contourne les données d'entrée et génère des données traitées qui sont en texte clair identiques aux données d'entrée.

17. Microcontrôleur à base de mode selon l'une quelconque des revendications 15 à 16, dans lequel deux unités de traitement de données sont incluses dans l'unité de traitement de données multimode pour deux processus inverses de chiffrement de données ou de déchiffrement de données, respectivement, et ces deux processus

inverses sont employés respectivement pour chiffrer les données d'entrée lorsque les données d'entrée sont fournies par le microcontrôleur pour le stockage dans la mémoire externe, et pour déchiffrer les données d'entrée lorsque les données d'entrée sont extraites dans un format chiffré de la mémoire externe.

18. Unité de traitement de données multimode au niveau d'une interface d'un microcontrôleur, comprenant :

un premier démultiplexeur (402) qui passe des données d'entrée selon un mode de traitement de données pendant une opération d'écriture mémoire ;

un 2ème démultiplexeur (408), couplé à une mémoire externe, le démultiplexeur passe les données d'entrée selon le mode de traitement de données pendant une opération de lecture mémoire ;

une pluralité d'unités de traitement de données (412, 414, 416, 418, 420, 422), couplée aux premier et 2ème démultiplexeurs, la pluralité d'unités de traitement de données génère une pluralité de données traitées selon une pluralité de procédés de traitement de données, où chaque unité de traitement de données est associée à un procédé de traitement de données ;

un premier multiplexeur (404), couplé à la mémoire externe, le premier multiplexeur sélectionne au moins une de la pluralité de données traitées selon le mode de traitement de données pendant l'opération d'écriture mémoire ; et

un 2ème multiplexeur (406) qui sélectionne au moins une de la pluralité de données traitées selon le mode de traitement de données pendant l'opération de lecture mémoire ;

dans laquelle la mémoire externe est partitionnée en une pluralité de régions, et les données traitées générées par un de la pluralité de procédés de traitement de données sont associées à une de la pluralité de régions dans la mémoire externe.

19. Unité de traitement de données multimode selon la revendication 18, dans laquelle une unité de traitement de données dans la pluralité d'unités de traitement de données contourne les données d'entrée et génère des données traitées qui sont en texte clair identiques aux données d'entrée.

20. Unité de traitement de données multimode selon l'une quelconque des revendications 18 ou 19, dans laquelle deux unités de

traitement de données dans la pluralité d'unités de traitement de données sont incluses pour deux processus inverses de chiffrement de données ou de déchiffrement de données, respectivement, et ces deux processus inverses sont employés respectivement pour chiffrer les données d'entrée lorsque les données d'entrée sont fournies par le microcontrôleur pour le stockage dans la mémoire externe, et pour déchiffrer les données d'entrée lorsque les données d'entrée sont extraites dans un format chiffré de la mémoire externe.

21. Unité de traitement de données multimode selon l'une quelconque des revendications 18 à 20, dans laquelle une unité de traitement de données dans la pluralité d'unités de traitement de données génère des données de contrôle d'intégrité selon un procédé de vérification d'intégrité pendant une opération d'écriture mémoire.

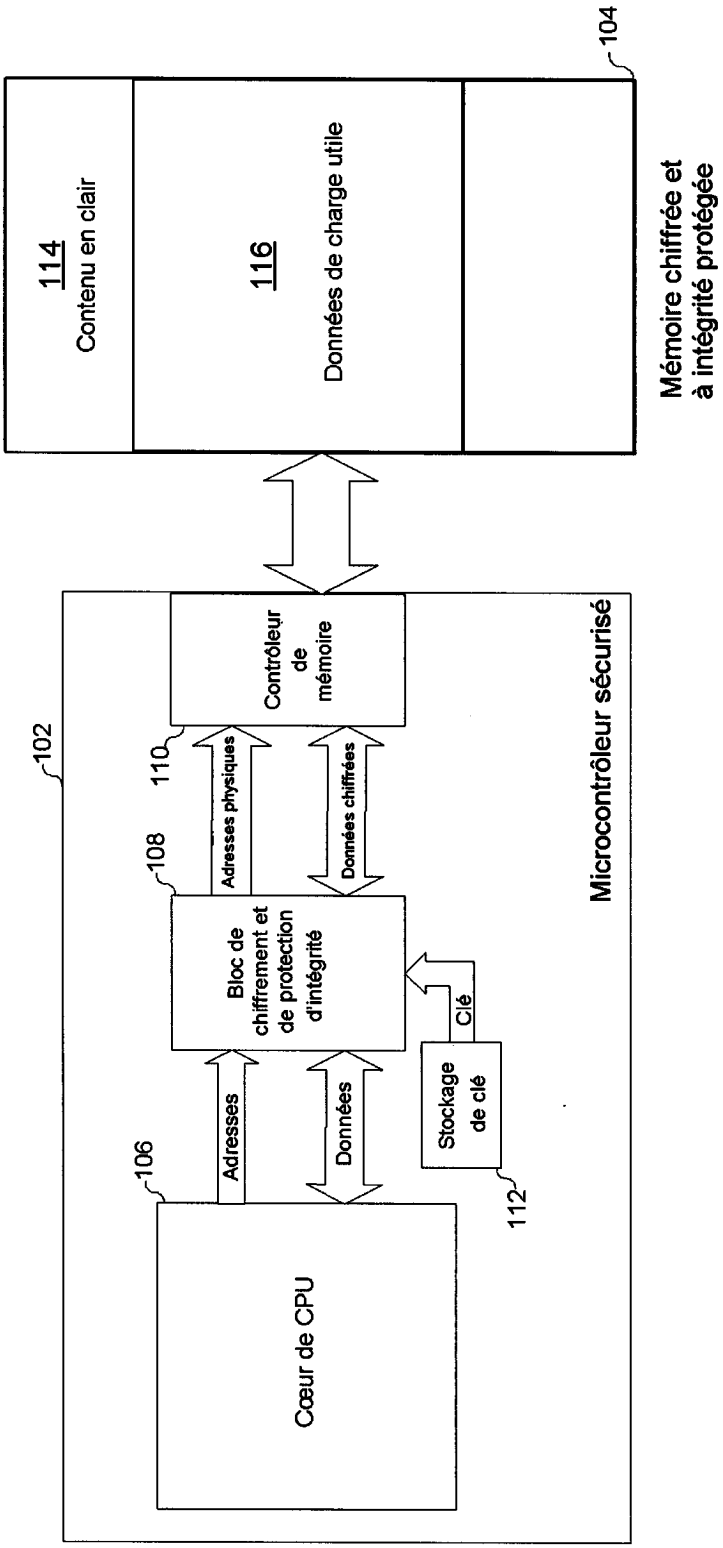


FIG. 1
(ART ANTÉRIEUR)

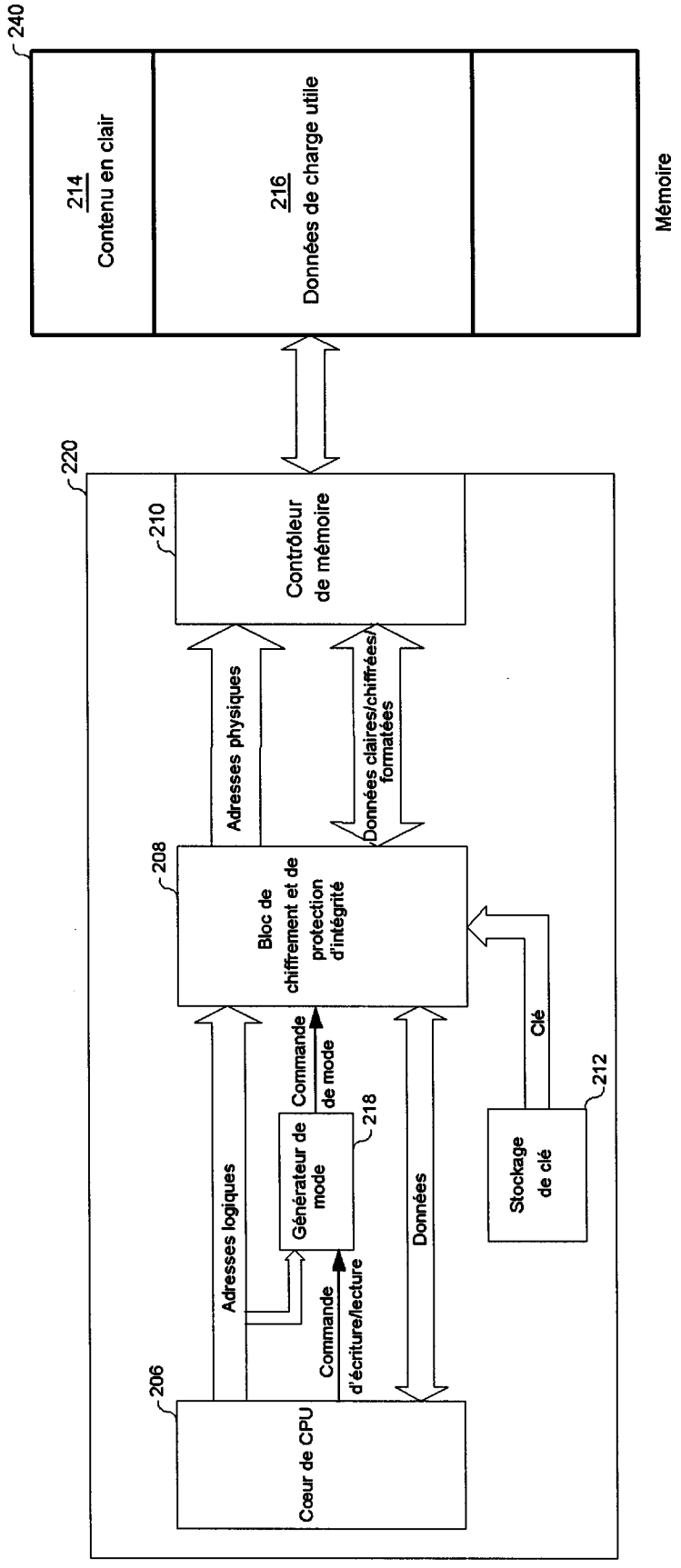

240
214
Contenu en clair
216
Données de charge utile
Mémoire
220
210
Contrôleur de mémoire
Adresses physiques
Données claires/chiffrées/formatées
208
Bloc de chiffrement et de protection d'intégrité
Commande de mode
218
Générateur de mode
Adresses logiques
Commande d'écriture/lecture
Données
Clé
212
Stockage de clé
206
Cœur de CPU

FIG. 2

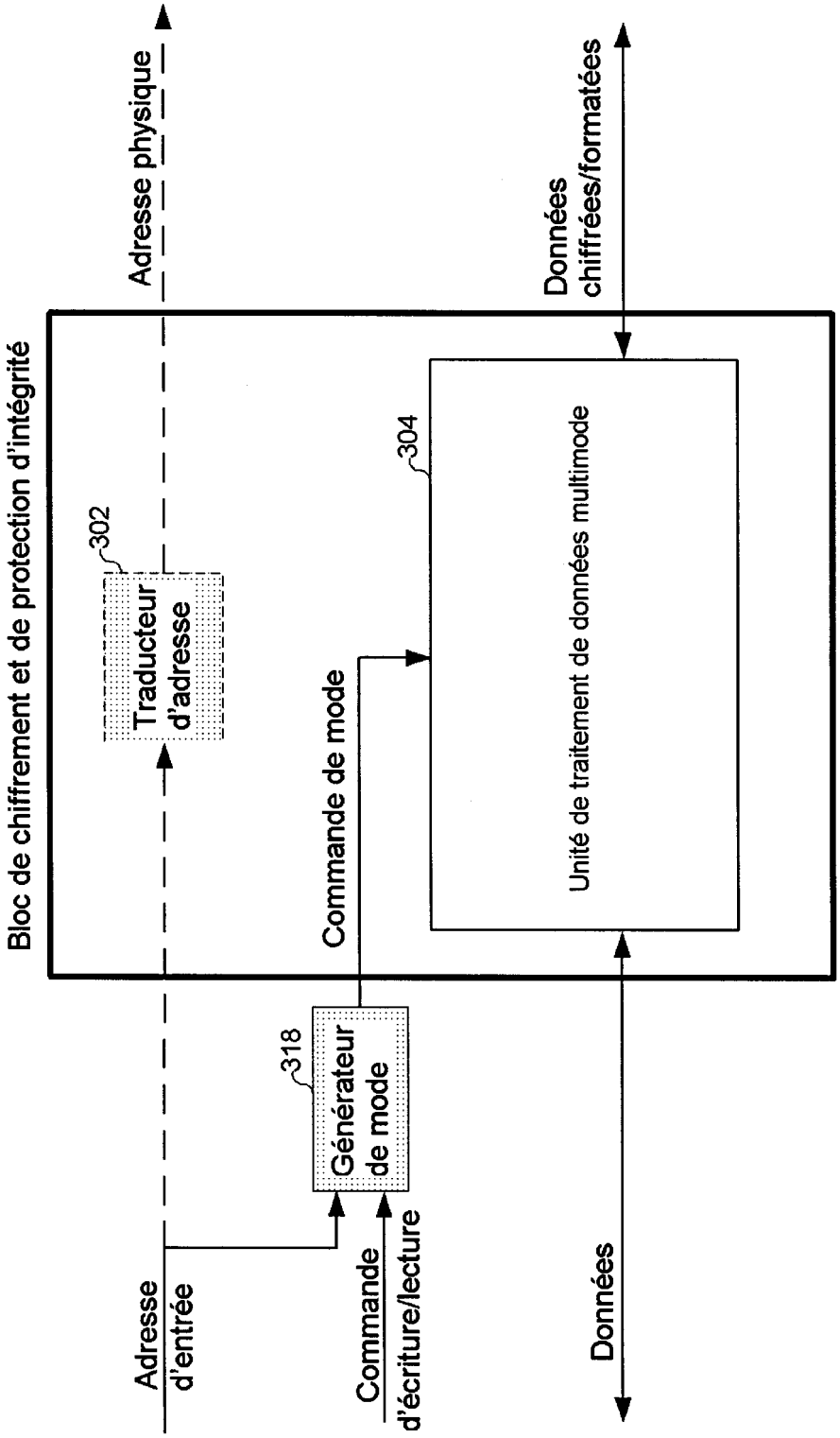

Bloc de chiffrement et de protection d'intégrité
Adresse physique
Données chiffrées/formatées
302
Traducteur d'adresse
304
Unité de traitement de données multimode
Commande de mode
318
Générateur de mode
Adresse d'entrée
Commande d'écriture/lecture
Données

FIG. 3

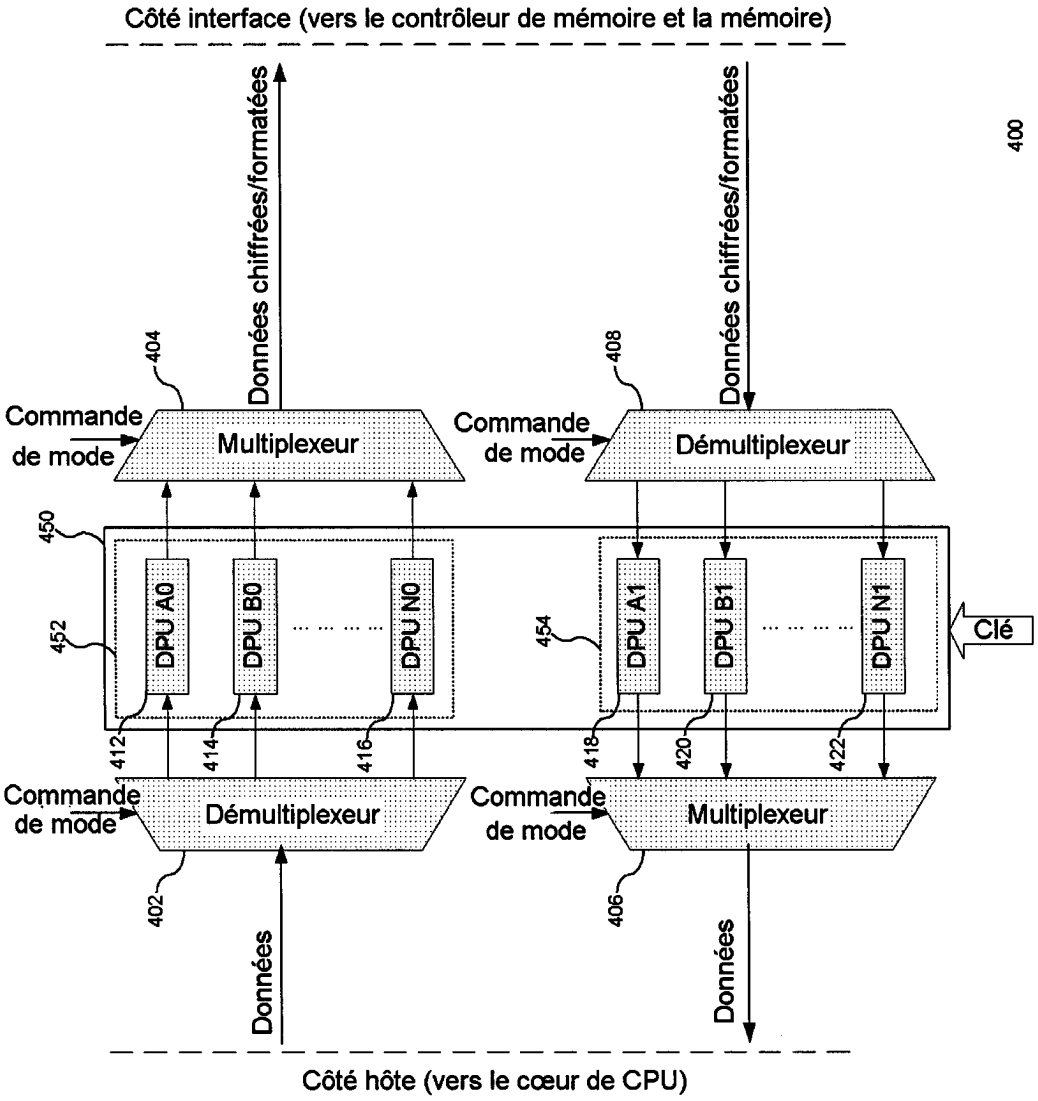

Côté interface (vers le contrôleur de mémoire et la mémoire)
Données chiffrées/formatées
Données chiffrées/formatées
400
404
408
Commande de mode
Multiplexeur
Commande de mode
Démultiplexeur
450
452
454
DPU A0
DPU B0
DPU N0
DPU A1
DPU B1
DPU N1
Clé
412
414
416
418
420
422
Commande de mode
Démultiplexeur
Commande de mode
Multiplexeur
402
406
Données
Données
Côté hôte (vers le cœur de CPU)

FIG. 4

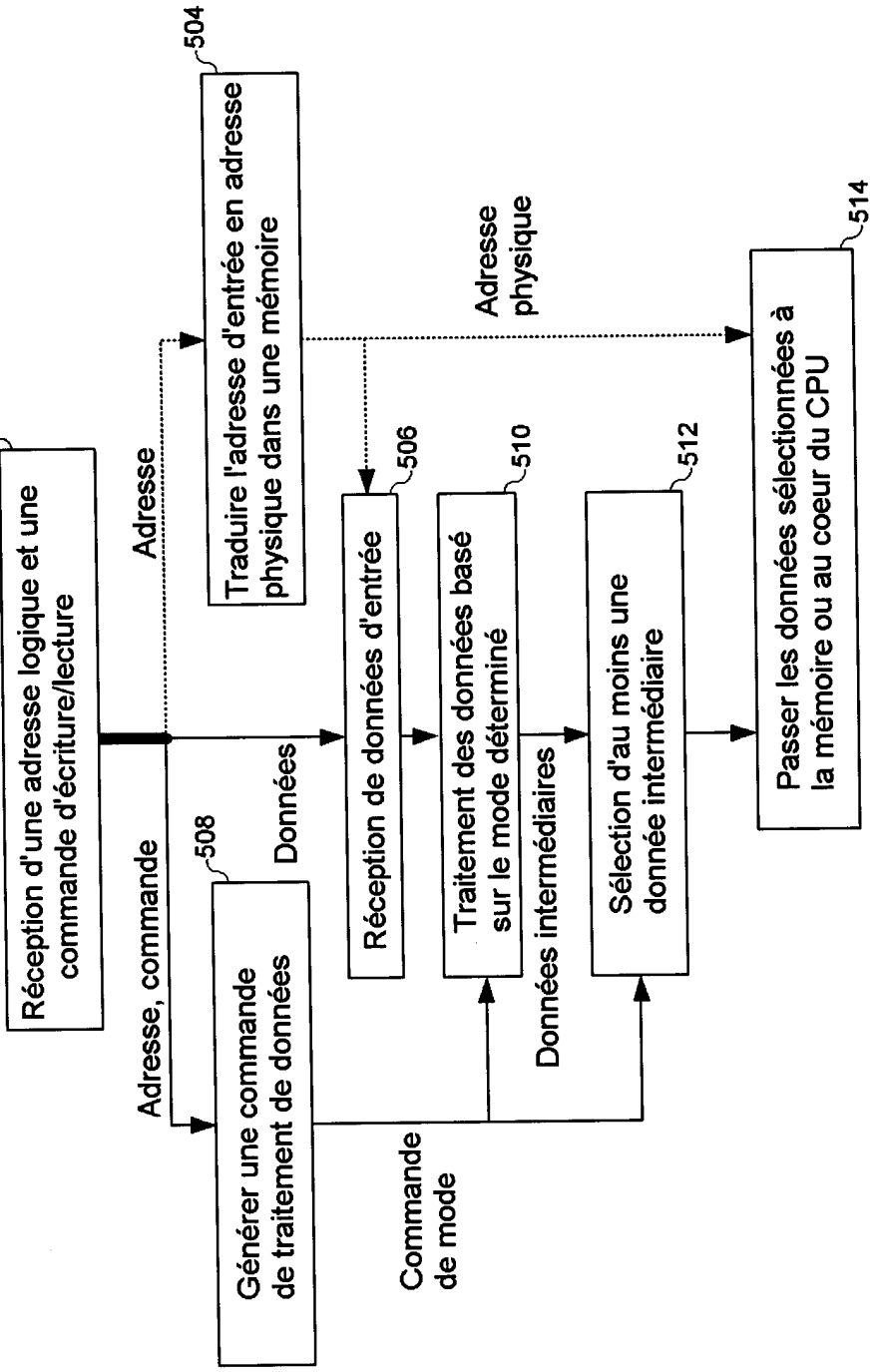

502
Réception d'une adresse logique et une commande d'écriture/lecture
Adresse
504
Traduire l'adresse d'entrée en adresse physique dans une mémoire
Adresse physique
514
Passer les données sélectionnées à la mémoire ou au coeur du CPU
Adresse, commande
508
Générer une commande de traitement de données
Données
506
Réception de données d'entrée
510
Traitement des données basé sur le mode déterminé
512
Sélection d'au moins une donnée intermédiaire
Données intermédiaires
Commande de mode

FIG. 5

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 760135
FR 1157656

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	EP 1 801 725 A2 (NVIDIA CORP [US]) 27 juin 2007 (2007-06-27) * alinéa [0019] - alinéa [0039]; revendications 1-7; figures 1, 5, 6 * -----	1-21	G06F21/02
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06F

Date d'achèvement de la recherche	Examinateur
25 avril 2012	Savvides, George

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1157656 FA 760135

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 25-04-2012
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1801725 A2	27-06-2007	CN 1984298 A	20-06-2007
		EP 1801725 A2	27-06-2007
		JP 4740830 B2	03-08-2011
		JP 2007215159 A	23-08-2007
		KR 20070063465 A	19-06-2007

EPO FORM P0465