

⑤④ Procédé d'exécution d'un programme d'ordinateur par un appareil électronique.

②② Date de dépôt : 09.03.21.

③③ Priorité :

⑥⑥ Références à d'autres documents nationaux
apparentés :

☐ Demande(s) d'extension :

⑦① Demandeur(s) : COMMISSARIAT A L'ENERGIE
ATOMIQUE ET AUX ENERGIES ALTERNATIVES
*Etablissement public à caractère industriel et
commercial* — FR.

④③ Date de mise à la disposition du public
de la demande : 16.09.22 Bulletin 22/37.

④⑤ Date de la mise à disposition du public du
brevet d'invention : 10.02.23 Bulletin 23/06.

⑤⑥ Liste des documents cités dans le rapport de
recherche :

Se reporter à la fin du présent fascicule

⑦② Inventeur(s) : SAVRY Olivier et HISCOCK Thomas.

⑦③ Titulaire(s) : COMMISSARIAT A L'ENERGIE
ATOMIQUE ET AUX ENERGIES ALTERNATIVES
*Etablissement public à caractère industriel et
commercial*.

⑦④ Mandataire(s) : INNOV-GROUP.



Description

Titre de l'invention : Procédé d'exécution d'un programme d'ordinateur par un appareil électronique

- [0001] L'invention concerne un procédé d'exécution d'un programme d'ordinateur par un appareil électronique comportant un microprocesseur, une mémoire déchiffrée, une mémoire chiffrée et un module matériel de sécurisation.
- [0002] L'invention concerne également :
- un programme d'ordinateur apte à être exécuté par un microprocesseur en mettant en œuvre ce procédé, et
 - un module matériel de sécurisation pour la mise en œuvre de ce procédé.
- [0003] Pour des raisons de sécurité, il est connu d'enregistrer les données traitées, lors de l'exécution d'un programme d'ordinateur, sous forme chiffrée dans une mémoire. Par la suite, la mémoire ou partie de mémoire qui contient ces données chiffrées est appelée « mémoire chiffrée ». Dans ce cas, à chaque fois qu'une donnée doit être chargée dans le microprocesseur pour y être traitée, la donnée chiffrée est d'abord transférée de la mémoire chiffrée vers une mémoire déchiffrée. Par la suite, on appelle « mémoire déchiffrée », une mémoire dans laquelle les données sont enregistrées sous forme déchiffrée. Lors de ce transfert, l'intégrité de la donnée à charger est d'abord vérifiée. Seulement si l'intégrité de la donnée est confirmée, alors la donnée est déchiffrée puis enregistrée dans la mémoire déchiffrée.
- [0004] Dans ce contexte, des données sont également transférées, en sens inverse, de la mémoire déchiffrée vers la mémoire chiffrée pour y être enregistrées. Lors de ce transfert, la donnée est chiffrée, puis le code d'authentification permettant de vérifier son intégrité est calculé. Enfin, la donnée chiffrée et son code d'authentification sont enregistrés dans la mémoire chiffrée.
- [0005] Les opérations de vérification de l'intégrité d'une donnée et de déchiffrement de cette donnée sont relativement longues. De même, les opérations de chiffrement et de calcul d'un code d'authentification sont aussi relativement longues. Ainsi, pour accélérer les transferts de données entre la mémoire déchiffrée et la mémoire chiffrée, il a déjà été proposé de faire ces transferts par bloc de plusieurs données, plutôt qu'individuellement pour chaque donnée. Dans ce cas, le bloc de données est enregistré dans la mémoire chiffrée sous la forme d'un bloc de données chiffrées et authentifiées.
- [0006] Un tel bloc de données chiffrées et authentifiées comprend notamment :
- un cryptogramme du bloc de données en clair, et
 - un code d'authentification de ce cryptogramme.

- [0007] Le cryptogramme du bloc de données en clair est obtenu en traitant le bloc de données comme un seul bloc de bits et sans distinguer les données les unes des autres. Ainsi, pour obtenir ce cryptogramme, une seule opération de chiffrement est exécutée au lieu d'une opération de chiffrement pour chaque donnée de ce bloc de données. Ceci accélère l'opération de chiffrement des données. En contrepartie, le cryptogramme ne peut être déchiffré qu'en une seule opération de déchiffrement. En particulier, il n'est pas possible de déchiffrer qu'une partie seulement des données sans déchiffrer la totalité du cryptogramme.
- [0008] De façon similaire, le code d'authentification est commun à l'ensemble des données du bloc de données. Il est donc calculé en une seule opération et en traitant le bloc de données comme un seul bloc. Ainsi, on évite de construire un code d'authentification pour chaque donnée de ce bloc de données. Cela accélère aussi la construction du code d'authentification.
- [0009] Par ailleurs, pour obtenir des informations sur un programme d'ordinateur ou provoquer un fonctionnement inattendu de ce programme d'ordinateur, de nombreuses attaques sont possibles. Certaines de ces attaques sont basées sur un usage erroné d'un pointeur de donnée. On rappelle ici qu'un pointeur de donnée est une donnée qui contient l'adresse de la donnée à traiter et non pas directement la valeur de la donnée traitée.
- [0010] L'usage de tels pointeurs de données est fréquent dans un programme d'ordinateur. Par exemple, un tel pointeur est utilisé pour pointer vers la première cellule d'un tableau de plusieurs cellules. Ensuite, pour traiter la cellule suivante de ce tableau, il suffit simplement d'incrémenter l'adresse contenue dans le pointeur d'un pas prédéterminé.
- [0011] Lors de la conception du programme d'ordinateur, le pointeur est prévu pour manipuler et traiter un groupe de données d'une taille prédéterminée. Toutefois, lors de l'exécution du programme d'ordinateur, il est parfois possible de s'arranger pour que ce pointeur pointe sur une donnée située en dehors de ce groupe de données. Par exemple, un tel usage erroné de ce pointeur est provoqué en saisissant, dans un champ de saisie, une donnée dont la taille est bien plus grande que celle prévue initialement par les développeurs du programme d'ordinateur. Grâce à cela, il est possible d'écrire des données dans des plages d'adresses où cela ne devrait pas être fait. Autrement dit, le pointeur est utilisé pour pointer vers des adresses invalides. Un exemple de ce premier type d'attaque est connu sous le terme de « attaque par dépassement de tampon » ou « stack overflow attack », lorsque cette attaque vise la pile utilisée par une fonction du programme d'ordinateur. Lorsque le pointeur est utilisé pour écrire des données avant la plage d'adresses prévue à cet effet dans la pile, l'attaque est également connue sous le terme de « stack underflow attack ».

- [0012] Ce premier type d'attaque peut être mis en œuvre de façon assez similaire pour écrire des données à des adresses invalides dans d'autres parties de la mémoire que la pile, comme par exemple, dans une partie connue sous le terme de « tas » (« heap » en anglais).
- [0013] Ces premiers types d'attaques ont en commun d'utiliser un pointeur valide pour pointer sur des adresses invalides. On dit alors qu'elles concernent ce qui touche au domaine de la « sécurité spatiale » (« spatial safety » en anglais).
- [0014] Il existe aussi des usages erronés des pointeurs qui touchent au domaine de la sécurité temporelle (« temporal safety » en anglais). Dans ce cas, un pointeur invalide est utilisé pour pointer sur une adresse valide. Un pointeur invalide est un pointeur qui a été utilisé de façon valide pour traiter des données dans un contexte limité, et qui est ensuite utilisé à nouveau en dehors de ce contexte limité. Cela peut se produire si, par exemple, ce pointeur n'a pas correctement été réinitialisé ou initialisé. Ce type de pointeur invalide est connu sous le terme anglais de « dangling pointer ».
- [0015] Certaines attaques repèrent donc ces pointeurs invalides, puis les utilisent pour lire ou écrire des données à des instants où ils ne devraient pas être utilisés pour cela. À titre d'illustration de ce second type d'attaque, on peut citer l'attaque connue sous l'expression anglaise de « use-after-free ».
- [0016] On notera aussi que les attaques basées sur des usages erronés de pointeurs ne concernent pas que les pointeurs de données, c'est-à-dire, les pointeurs qui pointent vers une donnée à traiter par le microprocesseur. Ce type d'attaque concerne également les pointeurs appelés ici « pointeurs de fonctions », c'est-à-dire, un pointeur qui contient l'adresse non pas d'une donnée, mais d'une instruction à exécuter par le microprocesseur.
- [0017] Plusieurs solutions ont déjà été proposées pour rendre plus difficile un usage erroné d'un pointeur. Par exemple, une solution est décrite dans la demande US2021-0004456. Cette solution est intéressante mais n'est pas applicable dans un contexte où les données sont chiffrées et déchiffrées par bloc. En effet, comme expliqué ci-dessus les avantages du chiffrement/déchiffrement par bloc découlent du fait, notamment, qu'il n'y a qu'un seul code d'authentification commun à toutes les données du bloc. À l'inverse, le procédé décrit dans la demande US2021-0004456 impose d'utiliser un code d'authentification pour chaque donnée accédée avec un pointeur. Cette dernière condition est donc incompatible avec un chiffrement/déchiffrement par bloc des données.
- [0018] L'invention vise donc à proposer un procédé d'exécution d'un programme d'ordinateur, robuste vis-à-vis d'un large spectre d'attaques basées sur un usage erroné d'un pointeur tout en étant compatible avec un chiffrement/déchiffrement par bloc des données.

[0019] L'invention a donc pour objet un tel procédé d'exécution d'un programme d'ordinateur par un appareil électronique comportant un microprocesseur, une mémoire déchiffrée, une mémoire chiffrée et un module matériel de sécurisation, dans lequel, lors de l'exécution du programme d'ordinateur, le transfert des lignes de code entre la mémoire déchiffrée et la mémoire chiffrée se fait par bloc entier de plusieurs lignes de code chiffrées et authentifiées, ce procédé comportant les étapes suivantes:

a) l'enregistrement dans la mémoire chiffrée d'un bloc de lignes de code chiffrées et authentifiées contenant une ligne de code à accéder à l'aide d'un pointeur, ce bloc de lignes de code chiffrées et authentifiées contenant :

- un cryptogramme de l'ensemble des lignes de code de ce bloc, ce cryptogramme pouvant uniquement être déchiffré dans sa totalité pour obtenir un bloc de lignes de code en clair et non pas ligne de code par ligne de code,

- un code d'authentification calculé à partir du bloc de lignes de code en clair ou à partir du cryptogramme du bloc de lignes de code en clair, et

- des métadonnées,

b) l'obtention, par le microprocesseur, d'un pointeur contenant l'adresse à laquelle est enregistrée la ligne de code à accéder, puis

c) le chargement du bloc contenant la ligne de code à accéder depuis la mémoire chiffrée vers le microprocesseur, puis

d) la vérification, par le module matériel de sécurisation et à l'aide du code d'authentification contenu dans le bloc chargé, de l'intégrité :

- du bloc de lignes de codes en clair obtenu à partir du cryptogramme contenu dans le bloc chargé, ou

- du cryptogramme contenu dans le bloc chargé,

e) lorsque cette vérification échoue, l'inhibition du traitement, par le microprocesseur, des lignes de code de ce bloc chargé et, lorsque cette vérification réussie :

- le déchiffrement du cryptogramme contenu dans le bloc chargé pour obtenir le bloc de lignes de code en clair, et

- l'enregistrement du bloc de lignes de code en clair obtenu dans la mémoire déchiffrée et l'enregistrement des métadonnées du bloc chargé,

dans lequel :

- l'étape a) comporte l'incorporation, dans les métadonnées du bloc contenant la ligne de code à accéder, d'un premier identifiant de pointeur associé à la ligne de code à accéder, ce premier identifiant de pointeur permettant à lui seul d'identifier de façon unique un pointeur parmi un ensemble contenant plusieurs pointeurs différents mis en œuvre lors de la même exécution du programme d'ordinateur par le microprocesseur,

- l'étape b) d'obtention du pointeur comporte l'obtention d'un pointeur comprenant :

- une première plage de bits contenant l'adresse de la ligne de code à accéder, et

- une seconde plage différente de bits contenant un second identifiant de pointeur,
- après l'étape c), le procédé comporte une étape f) de vérification, par le module matériel de sécurisation, que le second identifiant de pointeur contenu dans le pointeur obtenu lors de l'étape b) correspond au premier identifiant de pointeur associé à la ligne de code à accéder et contenu dans les métadonnées du bloc chargé, et lorsque les premier et second identifiants de pointeur ne correspondent pas, alors le module de sécurisation déclenche le signalement d'une faute d'exécution et, dans le cas contraire, le module de sécurisation inhibe le déclenchement du signalement d'une faute d'exécution et le microprocesseur traite la ligne de code à accéder.

[0020] Les modes de réalisation de ce procédé d'exécution peuvent comporter une ou plusieurs des caractéristiques suivantes :

1) l'étape e) comporte l'enregistrement du premier identifiant de pointeur contenu dans les métadonnées du bloc chargé dans une mémoire uniquement accessible par le module matériel de sécurisation.

2) avant l'étape a), le code d'authentification du bloc de lignes de code chiffrées et authentifiées à enregistrer, est aussi calculé à partir des métadonnées.

3) avant l'étape a), le procédé comporte :

- le chiffrement du bloc de lignes de code en clair en utilisant un vecteur d'initialisation et la génération d'un nouveau vecteur d'initialisation avant chaque chiffrement du bloc de lignes de code en clair, et
- l'incorporation dans les métadonnées du bloc de lignes de code chiffrées et authentifiées, du vecteur d'initialisation utilisé pour obtenir le cryptogramme de ce bloc de lignes de code chiffrées et authentifiées, et
- lors du déchiffrement du cryptogramme, le module matériel de sécurisation extrait des métadonnées du bloc de lignes de code chiffrées et authentifiées, le vecteur d'initialisation à utiliser pour réaliser ce déchiffrement.

4) lors de l'étape a), l'adresse à laquelle est enregistrée le bloc de lignes de code chiffrées et authentifiées est reliée, par une fonction bijective, à une adresse $@_{BDCi}$ définie par la relation suivante : $@_{BDCi} = @_{BDi} \cdot T_b / T_{BD}$, où :

- $@_{BDi}$ est l'adresse où débute, dans l'espace d'adressage du programme d'ordinateur, le bloc de lignes de code en clair,
- T_b est la taille, en nombre d'octets, du bloc de lignes de code chiffrées et authentifiées,
- T_{BD} est la taille, en nombre d'octets, du bloc de lignes de code en clair.

5)

- après l'étape b) et avant l'étape c), le module matériel de sécurisation détermine l'adresse $@_{BDCi}$ à l'aide de la première relation suivante : $@_{BDCi} = E(@_{Di,j} / T_{BD}) \cdot T_b$, où
- $E()$ est la fonction qui retourne la partie entière du nombre situé entre les pa-

renthèses, et

- $@_{Di,j}$ est l'adresse contenue dans le pointeur obtenu à l'étape b),

- T_b et T_{BD} sont tous les deux des puissances de deux,

lors de cette détermination, la division et la multiplication de la première relation sont exécutées par des registres à décalage du module matériel de sécurisation, puis

- lors de l'étape c), le bloc contenant la ligne de code à accéder est chargé, depuis la mémoire chiffrée, à partir de l'adresse reliée, par la fonction bijective, à l'adresse $@_{BDCi}$ déterminée.

6)

- après l'étape b) et avant l'étape c), le module matériel de sécurisation détermine

l'adresse $@_{BDCi}$ à l'aide de la seconde relation suivante : $@_{BDCi} = E(@_{Di,j}/T_{BD}).T_{BD} + E(@_{Di,j}/T_{BD}).(T_b - T_{BD})$, où

- $E()$ est la fonction qui retourne la partie entière du nombre situé entre les parenthèses, et

- $@_{Di,j}$ est l'adresse contenue dans le pointeur obtenu à l'étape b),

- $(T_b - T_{BD})$ et T_{BD} sont tous les deux des puissances de deux,

lors de cette détermination, chaque division et chaque multiplication de la seconde relation sont exécutées par des registres à décalage du module matériel de sécurisation, et

- lors de l'étape c), le bloc contenant la ligne de code à accéder est chargé, depuis la mémoire chiffrée, à partir de l'adresse reliée, par la fonction bijective, à l'adresse $@_{BDCi}$ déterminée.

[0021] L'invention a également pour objet un programme d'ordinateur apte à être exécuté par un microprocesseur en mettant en œuvre le procédé ci-dessus, dans lequel le code binaire du programme d'ordinateur comporte :

- un bloc de lignes de code chiffrées et authentifiées contenant une ligne de code à accéder à l'aide d'un pointeur respectif, ce bloc de lignes de code chiffrées et authentifiées contenant :

- un cryptogramme de l'ensemble des lignes de code de ce bloc, ce cryptogramme pouvant uniquement être déchiffré dans sa totalité pour obtenir un bloc de lignes de code en clair et non pas ligne de code par ligne de code,

- un code d'authentification calculé à partir du bloc de lignes de code en clair ou à partir du cryptogramme du bloc de lignes de code en clair, et

- des métadonnées,

- un pointeur contenant l'adresse à laquelle est enregistrée la ligne de code à accéder dans lequel:

- les métadonnées comporte un premier identifiant de pointeur associé à la ligne de code à accéder, ce premier identifiant de pointeur permettant à lui seul d'identifier de

façon unique un pointeur parmi un ensemble contenant plusieurs pointeurs différents mis en œuvre lors de la même exécution du programme d'ordinateur par le micro-processeur, et

- le pointeur comprend :

- une première plage de bits contenant l'adresse de la ligne de code à accéder, et
- une seconde plage différente de bits contenant un second identifiant de pointeur, ce second identifiant de pointeur étant égal au premier identifiant de pointeur.

[0022] L'invention a également pour objet un module matériel de sécurisation pour la mise en œuvre du procédé d'exécution ci-dessus, dans lequel le module matériel est configuré pour :

a) déclencher l'enregistrement dans la mémoire chiffrée d'un bloc de lignes de code chiffrées et authentifiées contenant une ligne de code à accéder à l'aide d'un pointeur, ce bloc de lignes de code chiffrées et authentifiées contenant :

- un cryptogramme de l'ensemble des lignes de code de ce bloc, ce cryptogramme pouvant uniquement être déchiffré dans sa totalité pour obtenir un bloc de lignes de code en clair et non pas ligne de code par ligne de code,

- un code d'authentification calculé à partir du bloc de lignes de code en clair ou à partir du cryptogramme du bloc de lignes de code en clair, et

- des métadonnées,

b) recevoir un pointeur contenant l'adresse à laquelle est enregistrée la ligne de code à accéder, puis

c) déclencher le chargement du bloc contenant la ligne de code à accéder depuis la mémoire chiffrée vers le microprocesseur, puis

d) vérifier, à l'aide du code d'authentification contenu dans le bloc chargé, l'intégrité :

- du bloc de lignes de codes en clair obtenu à partir du cryptogramme contenu dans le bloc chargé, ou

- du cryptogramme contenu dans le bloc chargé,

e) lorsque cette vérification échoue, inhiber le traitement, par le microprocesseur, des lignes de code de ce bloc chargé et, lorsque cette vérification réussie :

- déchiffrer le cryptogramme contenu dans le bloc chargé pour obtenir le bloc de lignes de code en clair, et

- déclencher l'enregistrement du bloc de lignes de code en clair obtenu dans la mémoire déchiffrée et l'enregistrement des métadonnées du bloc chargé,

dans lequel le module de sécurisation est également configuré :

- pour incorporer, dans les métadonnées du bloc contenant la ligne de code à accéder, un premier identifiant de pointeur associé à la ligne de code à accéder, ce premier identifiant de pointeur permettant à lui seul d'identifier de façon unique un pointeur parmi un ensemble contenant plusieurs pointeurs différents mis en œuvre lors de la

même exécution du programme d'ordinateur par le microprocesseur,

- en réponse à l'exécution d'une instruction d'accès à la ligne de code à accéder à l'aide d'un pointeur, pour extraire un second identifiant de pointeur dans une plage de bits de ce pointeur, puis
- pour vérifier que le second identifiant de pointeur correspond au premier identifiant de pointeur associé à la ligne de code à accéder et contenu dans les métadonnées du bloc chargé, et si les premier et second identifiants de pointeur ne correspondent pas, alors déclencher le signalement d'une faute d'exécution et, dans le cas contraire, inhiber le déclenchement du signalement d'une faute d'exécution et autoriser le micro-processeur à traiter la ligne de code à accéder.

[0023] L'invention sera mieux comprise à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple non limitatif et faite en se référant aux dessins sur lesquels :

- la [fig.1] est une illustration schématique de l'architecture d'un appareil électronique apte à exécuter un code binaire d'un programme d'ordinateur,
- la [fig.2] est une illustration schématique d'une partie d'une mémoire principale de l'appareil de la [fig.1],
- la [fig.3] est une illustration schématique de la structure d'un bloc de données chiffrées et authentifiées contenu dans la partie de la mémoire de la [fig.2],
- la [fig.4] est une illustration schématique de la structure d'un pointeur enrichi utilisé lors de l'exécution du code binaire par l'appareil de la [fig.1],
- la [fig.5] est un organigramme d'un procédé d'exécution du code binaire par l'appareil de la [fig.1],
- la [fig.6] est un organigramme d'un procédé détaillant les opérations réalisées lorsque l'instruction exécutée du code binaire est une instruction de chargement ou d'écriture d'une donnée,
- la [fig.7] est une illustration schématique d'un compilateur apte à générer le code binaire exécuté par l'appareil de la [fig.1].

[0024] Les conventions, notations et définitions utilisées dans cette description sont données dans le chapitre I. Ensuite, un exemple détaillé de mode de réalisation est décrit dans le chapitre II à l'aide des figures. Dans un chapitre III suivant, des variantes de ce mode de réalisation détaillé sont présentées. Enfin, les avantages des différents modes de réalisation sont présentés dans un chapitre IV.

[0025] Chapitre I : Conventions, notations et définitions :

[0026] Dans les figures, les mêmes références sont utilisées pour désigner les mêmes éléments. Dans la suite de cette description, les caractéristiques et fonctions bien connues de l'homme du métier ne sont pas décrites en détails.

[0027] Dans cette description, les définitions suivantes sont adoptées.

- [0028] Un « programme » désigne un ensemble d'une ou de plusieurs fonctions prédéterminées que l'on souhaite faire exécuter par un microprocesseur.
- [0029] Un « code source » est une représentation du programme dans un langage informatique. Le code source n'est pas directement exécutable par un microprocesseur. Le code source est destiné à être transformé par un compilateur en un code binaire directement exécutable par le microprocesseur.
- [0030] Un programme ou un code est dit être « directement exécutable » lorsqu'il est apte à être exécuté par un microprocesseur sans que ce microprocesseur n'ait besoin au préalable de le compiler au moyen d'un compilateur ou de l'interpréter au moyen d'un interpréteur.
- [0031] Une « instruction » désigne une instruction machine exécutable par un microprocesseur. Une telle instruction est constituée :
- d'un opcode, ou code d'opération, codant la nature de l'opération à exécuter, et
 - d'un ou plusieurs opérandes définissant la ou les valeurs des paramètres de cette opération.
- [0032] Le jeu d'instructions machines d'un microprocesseur est formé par l'ensemble des opcodes utilisables pour former des instructions exécutables par le microprocesseur. Le jeu d'instructions machines peut être différent d'un microprocesseur à un autre.
- [0033] Un « code machine » est un ensemble d'instructions machines. Il s'agit typiquement d'un fichier contenant une succession de bits portant la valeur « 0 » ou « 1 », ces bits codant les instructions à exécuter par le microprocesseur. Le code machine est directement exécutable par le microprocesseur, c'est-à-dire sans nécessiter une compilation ou une interprétation préalable.
- [0034] Un « code binaire » est un fichier contenant une succession de bits portant la valeur « 0 » ou « 1 ». Ces bits codent des données et des instructions à exécuter par le microprocesseur. Ainsi, le code binaire comprend au moins un code machine et en plus, généralement, des données numériques traitées par ce code machine.
- [0035] Pour être exécuté par un microprocesseur, le code binaire est enregistré dans des lignes d'une mémoire principale. Typiquement, le code binaire comporte plusieurs centaines ou milliers de lignes. Ici, chacune de ces lignes est appelée "ligne de code". Chaque ligne de code est enregistrées à une adresse qui lui est propre dans la mémoire principale. Chaque ligne de code contient une seule instruction ou une seule donnée. Par la suite, lorsque le code contenu dans la ligne de code correspond à une instruction, cette ligne de code est simplement appelée "instruction". Lorsque le code contenu dans la ligne de code correspond une donnée, la ligne de code est simplement appelée "donnée". Le terme "ligne de code" est utilisé pour désigner aussi bien une donnée qu'une instruction.
- [0036] Au niveau du code binaire, une instruction et une donnée correspondent tous les deux

à des bits. Toutefois, les instructions et les données ne sont pas traitées de la même façon par un microprocesseur. Par exemple, une instruction est seulement chargée puis exécutée par le microprocesseur lorsque le compteur ordinal pointe sur cette instruction. Une donnée est chargée par le microprocesseur seulement en réponse à l'exécution par ce microprocesseur d'une instruction de chargement de cette donnée.

[0037] On parle d'exécution d'une fonction pour désigner l'exécution des instructions réalisant cette fonction.

[0038] Chapitre II : Exemple de mode de réalisation détaillé :

[0039] La [fig.1] représente un appareil électronique 1 comportant un microprocesseur 2, un ensemble 4 de mémoires et un support 6 de stockage de masse. Par exemple, l'appareil 1 est un ordinateur, un smartphone, une tablette électronique ou similaire.

[0040] Le microprocesseur 2 comporte ici :

- une unité arithmétique et logique 10 ;
- un ensemble 12 de registres ;
- un tampon 14 de données ;
- une interface 16 d'entrée/sortie de lignes de code,
- un chargeur 18 d'instructions comportant un compteur ordinal 26,
- une file 22 d'instructions à exécuter, et
- un module matériel 28 de sécurisation comportant une mémoire non-volatile sécurisée 29.

[0041] L'ensemble 4 est configuré pour stocker les lignes de code d'un code binaire 30 d'un programme devant être exécuté par le microprocesseur 2. L'ensemble 4 est une mémoire à accès aléatoire. Typiquement, l'ensemble 4 est une mémoire volatile. Chaque ligne de code est associée à une adresse physique qui est utilisée pour la charger ou l'écrire sans modifier les autres lignes de code. Ainsi, par la suite, on dit que ces lignes de code sont adressables individuellement. A titre d'illustration, dans ce mode de réalisation, les lignes de code sont chacune codées sur 64 bits et sont donc chacune formée par huit octets. Par la suite, la taille d'une ligne de code, en nombre d'octets, est notée T_d .

[0042] Ici, chaque ligne de code est aussi associée à une adresse virtuelle dans l'espace d'adressage du programme d'ordinateur. Il existe une relation bijective qui relie chaque adresse virtuelle d'une ligne de code à l'adresse physique de cette même ligne de code. La conversion d'une adresse virtuelle en adresse physique est typiquement réalisée par une unité de management de mémoire connue sous l'acronyme MMU ("Management Memory Unit").

[0043] Par exemple, l'ensemble 4 comporte :

- trois niveaux de mémoires caches, et
- une mémoire principale MP.

- [0044] Les mémoires caches permettent d'accélérer le transfert de données entre la mémoire principale MP et le microprocesseur 2. Les trois niveaux de mémoire cache sont appelés habituellement L1, L2 et L3. Sur la [fig.1], les symboles "L1", "L2" et "L3" sont utilisés pour désigner, respectivement, les trois mémoires caches L1, L2 et L3. Ici, pour simplifier la [fig.1], la mémoire cache L1 est représentée à l'extérieur du microprocesseur 2 alors que, souvent, elle est intégrée à l'intérieur du microprocesseur 2. Les mémoires L1 à L3 sont classées par ordre de rapidité de lecture, la mémoire L1 étant la plus rapide. Généralement, la taille des mémoires cache est inversement proportionnelle à leur rapidité.
- [0045] Classiquement, après le chargement du code binaire 30 dans la mémoire MP, la mémoire MP comporte notamment les parties suivantes :
- une première partie 42 contenant les instructions à exécuter,
 - une deuxième partie 44 contenant des données à traiter,
 - une troisième partie 46 utilisée pour sauvegarder le contexte d'exécution d'une fonction lorsqu'elle appelle une autre fonction, et
 - une quatrième partie 48 utilisée pour allouer dynamiquement de la mémoire au programme en cours d'exécution afin d'y enregistrer des données.
- [0046] La partie 42 est connue sous le terme de "segment de code" ("code segment" ou "text segment" en anglais).
- [0047] La partie 44 contient typiquement les variables statiques et globales du programme exécuté. La partie 44 est elle-même classiquement divisée en une première et une seconde sections. La première section contenant les variables statiques et globales qui ont été initialisées lors de la compilation. Cette première section est connue sous le terme de segment de données et souvent notée ".data". La seconde section comporte les variables statiques et globales qui n'ont pas été initialisées lors de la compilation du code binaire 30. Cette seconde section est également connue sous le terme de "segment bss" et souvent notée ".bss". Généralement, ces deux sections sont contiguës.
- [0048] La partie 46 est connue sous le terme de "pile d'exécution" ("call stack" en anglais). Par conséquent, par la suite, la partie 46 est également appelée "pile 46". Enfin la partie 48 est connue sous le terme de "tas" ("heap" en anglais). Ainsi, par la suite, la partie 48 est également appelée "tas 48".
- [0049] Le code binaire 30 comporte notamment un code machine 32 et un bloc 34 de données nécessaires à l'exécution du code binaire 30. Le code machine 32 et le bloc 34 sont enregistrés dans, respectivement, les parties 42 et 44.
- [0050] L'exécution du code binaire 30 débute par le chargement et le traitement de données du bloc 34. Ici, en particulier, le bloc 34 comporte un cryptogramme ka^* obtenu en chiffrant une clé secrète ka à l'aide d'une clé publique pk_{CPU} du microprocesseur 2.
- [0051] L'ensemble 4 de mémoire est raccordé au microprocesseur 2 par un bus de données et

un bus d'adresses. Pour simplifier la [fig.1], ces deux bus sont représentés par une double flèche 50 et désignés collectivement dans la suite de cette description par le terme "bus 50".

- [0052] La taille du bus d'adresses détermine la taille $N_{@}$, en nombre de bits, des adresses utilisées pour accéder à la mémoire 4. Typiquement, la taille $N_{@}$ est supérieure ou égale à 8, 16, 32 ou 64 bits. Par exemple, dans ce mode de réalisation, la taille $N_{@}$ est égale à 64 bits.
- [0053] L'ensemble 4 est un ensemble de mémoires chiffrées, c'est-à-dire un ensemble dans lequel les lignes de code sont enregistrées sous forme chiffrée. Par la suite, la description est faite dans le cas particulier où les lignes de code chiffrées sont des données contenues dans la partie 44.
- [0054] Un découpage en blocs de données chiffrées et authentifiées de la partie 44 est représenté sur la [fig.2]. Dans cette figure et dans la suite de la description, on note "BDCi" un bloc de données chiffrées et authentifiées, enregistré dans la mémoire MP à l'adresse @BDCi, où l'indice i est un identifiant de ce bloc BDCi. Ici, l'indice i est le numéro d'ordre du bloc de données compté à partir du premier bloc BDC1, c'est-à-dire celui situé au début de la partie 44. L'adresse @BDCi est ici égale à l'adresse à laquelle débute le bloc BDCi. Dans cet exemple, l'indice i varie de 1 à n de sorte que la partie 44 est divisée en n blocs BDCi distincts. Sur la [fig.2] et les suivantes, le symbole "..." indique qu'une partie des éléments n'a pas été représentée.
- [0055] Ici, tous les blocs BDCi sont structurellement identiques. Ainsi, seul le bloc BDCi représenté sur la [fig.3] est décrit en détail. La taille du bloc BDCi en nombre d'octets est noté Tb par la suite. La taille Tb est supérieure à huit ou seize et, généralement supérieur ou égale à 32 ou 64 octets. Généralement, la taille Tb est inférieure à 1 ko ou 1 Mo. Dans ce premier mode de réalisation, à titre d'illustration la taille Tb est égal à 128 octets.
- [0056] Le bloc BDCi comporte, dans l'ordre en partant de son adresse @BDCi de début :
- un cryptogramme BD_i^* ,
 - des métadonnées MD_i , et
 - un code d'authentification MAC_i ,
- [0057] Le cryptogramme BD_i^* est obtenu en chiffrant un bloc BD_i de N_d données $D_{i,j}$ en clair à l'aide de la clé cryptographique ka , où N_d est un nombre entier supérieur à un ou deux ou quatre. Ici, le nombre N_d est égal à huit. L'indice j est un identifiant de la donnée $D_{i,j}$ qui permet de la distinguer des autres données contenues dans le même bloc BD_i . Ici, l'indice j est le numéro d'ordre de la donnée $D_{i,j}$ compté à partir de la première donnée $D_{i,1}$ du bloc BD_i , c'est-à-dire à partir de la donnée $D_{i,1}$ situé à l'adresse @BDCi à laquelle débute le bloc BDCi.
- [0058] Plus précisément, le cryptogramme BD_i^* est obtenu à l'aide de la relation suivante :

$BD_i^* = f_{ka}(BD_i ; iv_i)$, où :

- f_{ka} est une fonction de chiffrement, correspondant à une fonction de déchiffrement f_{ka}^{-1} , et

- iv_i est un vecteur d'initialisation également connu sous le nom de "nonce".

[0059] Les fonctions f_{ka} et f_{ka}^{-1} sont préprogrammées dans le module 28. Typiquement, la fonction f_{ka} est une fonction de chiffrement symétrique.

[0060] Le vecteur iv_i est un vecteur d'initialisation dont la valeur est modifiée à chaque fois que la fonction f_{ka} est utilisée pour chiffrer un bloc BD_i de données en clair. A l'inverse, la clé ka est toujours la même. Dès lors, la clé ka permettant de déchiffrer le cryptogramme BD_i^* est préenregistrée dans la mémoire 29 afin de permettre au module 28 de déchiffrer chaque cryptogramme BD_i^* .

[0061] Dans ce mode de réalisation, chaque bloc BD_i contient N_d données $D_{i,j}$ associées à des adresses virtuelles respectives et consécutives. Par la suite, l'adresse virtuelle d'une donnée $D_{i,j}$ est notée $@_{Di,j}$. Chaque bloc BD_i correspond donc à une plage continue de N_d adresses virtuelles consécutives. Ces plages d'adresses virtuelles sont distinctes les unes des autres. En particulier, elles ne se chevauchent pas de sorte qu'une même donnée $D_{i,j}$ ne peut pas être contenue dans plusieurs blocs BD_i différents. De plus, ces plages d'adresses sont contiguës les unes aux autres de sorte qu'il n'existe pas, entre un premier bloc BD_i et un second bloc BD_{i+1} contigus, des données qui n'appartiennent ni au bloc BD_i ni au bloc BD_{i+1} . Ainsi, les blocs BD_i forment, dans l'espace d'adressage du programme d'ordinateur, une succession de blocs de données consécutifs. A l'intérieur d'un même bloc BD_i , les N_d données $D_{i,j}$ sont, par exemple, classées par ordre d'adresses croissantes de sorte que la donnée $D_{i,1}$ est la première donnée du bloc BD_i . Dans ces conditions, l'adresse $@_{BDi}$ de début du bloc BD_i est égale à l'adresse $@_{Di,1}$ de la donnée $D_{i,1}$.

[0062] La taille T_{BD} du bloc BD_i est égale à $N_d T_d$, où T_d est la taille d'une donnée $D_{i,j}$ en nombre d'octets. Ici, la taille du cryptogramme BD_i^* est égale à la taille du bloc BD_i .

[0063] Les métadonnées MD_i contiennent ici:

- pour chaque donnée $D_{i,j}$, un emplacement réservé pour y enregistrer les bits d'un identifiant de pointeur $IP_{i,j}$ associé spécifiquement à cette donnée $D_{i,j}$, et
- le vecteur iv_i utilisé pour obtenir le cryptogramme BD_i^* .

[0064] Dans les métadonnées MD_i , il y a autant d'emplacements réservés pour y enregistrer un identifiant de pointeur qu'il y a de données $D_{i,j}$ dans le bloc BD_i . Sur la [fig.3], chacun de ces emplacements est désignés par la référence " $IP_{i,j}$ " de l'identifiant $IP_{i,j}$ qu'il est destiné à contenir. Ici, la taille de chaque identifiant $IP_{i,j}$, et donc la taille de chaque emplacement réservé, est égale à 8 bits.

[0065] L'identifiant $IP_{i,j}$ est un identifiant qui permet d'identifier de façon unique un pointeur $PD_{i,j}$ parmi un ensemble d'autres pointeurs utilisés lors de la même exécution du code

binaire 30. Le pointeur $PD_{i,j}$ est un pointeur qui contient l'adresse de la donnée $D_{i,j}$ et qui permet d'accéder à cette donnée.

- [0066] L'identifiant $IP_{i,j}$ est construit de manière à limiter la probabilité que deux pointeurs différents aient le même identifiant de pointeur. Par exemple, les identifiants de pointeurs sont construits pour que cette probabilité soit inférieure à une chance sur dix et, de préférence, une chance sur cinquante ou une chance sur cent ou une chance sur mille.
- [0067] L'identifiant $IP_{i,j}$ peut être généré soit lors de la compilation du code source pour obtenir le code binaire 30 soit dynamiquement lors de l'exécution du code binaire 30.
- [0068] Par exemple, lorsque le pointeur $PD_{i,j}$ est déclaré dans le code source, l'identifiant $IP_{i,j}$ est généré lors de la compilation. Dans ce cas, classiquement, un tel pointeur pointe sur un variable globale ou une variable statique ou une variable locale. Lors de la compilation du code source, pour minimiser la probabilité que deux pointeurs différents aient le même identifiant de pointeur, par exemple, le compilateur génère l'identifiant $IP_{i,j}$ du pointeur par tirage aléatoire ou pseudo-aléatoire de cet identifiant dans un ensemble EIP. L'ensemble EIP contient toutes les valeurs possibles pour un identifiant de pointeur sauf les valeurs déjà attribuées à un identifiant de pointeur. Dans un autre mode de réalisation, l'identifiant $IP_{i,j}$ est à chaque fois tirée de façon aléatoire ou pseudo-aléatoire dans l'ensemble EIP. A titre d'illustration, pour faire cela, dans le cas d'un compilateur utilisant LLVM ("Low Level Virtual Machine"), l'instruction "Alloca" est modifiée pour générer en même temps le pointeur $PD_{i,j}$ et l'identifiant $IP_{i,j}$ de ce pointeur. L'instruction "Alloca" génère un pointeur qui pointe typiquement sur une variable locale enregistrée dans la pile 46.
- [0069] Lorsque le code binaire comporte des instructions qui, lorsqu'elles sont exécutées par le microprocesseur 2, alloue dynamiquement une zone de mémoire libre pour y enregistrer des données, alors le pointeur $PD_{i,j}$ et son identifiant $IP_{i,j}$ sont générés lors de l'exécution du code binaire 30. Plus précisément, lorsque de telles instructions sont exécutées, elles génèrent un pointeur qui pointe vers la zone de mémoire allouée dynamiquement. De telles instructions sont fréquemment utilisées pour allouer une zone de mémoire dans le tas 48. Par exemple, dans un code source utilisant les bibliothèques standards du langage C, de telles instructions correspondent aux fonctions "malloc()", "calloc()", "realloc()", ...etc. Dans ce cas, ces fonctions "malloc()", "calloc()", "realloc()", ...etc sont modifiées pour générer l'identifiant $IP_{i,j}$ en même temps qu'elle génère le pointeur $PD_{i,j}$. De préférence, chaque exécution d'une telle fonction doit générer un identifiant $IP_{i,j}$ aussi différent que possible de l'identifiant $IP_{i,j}$ généré lors de la précédente exécution de cette même fonction. Pour cela, par exemple, à chaque exécution d'une telle fonction :
- l'identifiant $IP_{i,j}$ est tirée, de façon aléatoire ou pseudo-aléatoire, dans l'ensemble

EIP, ou

- l'identifiant $IP_{i,j}$ est pris égale à l'empreinte numérique obtenue en appliquant une fonction de hachage à l'adresse $@_{Di,j}$ de la donnée Di,j vers laquelle le pointeur PDi,j pointe.

[0070] Le rôle de ces identifiant $IP_{i,j}$ est détaillé plus loin en référence à la [fig.6].

[0071] Le code MAC_i est une étiquette d'intégrité qui permet de vérifier l'intégrité du bloc BD_i de données. A cet effet, ici, le code MAC_i est un code permettant de vérifier l'intégrité et l'authenticité du cryptogramme BD_i^* . De plus, dans ce mode de réalisation, le code MAC_i permet aussi de vérifier l'intégrité et l'authenticité des métadonnées MD_i . Ce code MAC_i est communément appelé « code d'authentification de message » et connu sous l'acronyme MAC (« Message Authentication Code »). Un tel code MAC_i est obtenu en construisant une empreinte numérique à partir du cryptogramme BD_i^* et des métadonnées MD_i . Cette empreinte numérique comporte normalement moins de bits que le cryptogramme BD_i^* . Une telle empreinte numérique est plus connue sous le terme anglais de "digest" ou "hash". Cette empreinte numérique est construite à l'aide d'une fonction prédéterminée et d'une clé secrète k' connue seulement de l'auteur du code binaire 30 et du microprocesseur 2. Ici, la clé k' est pré-enregistrée dans la mémoire 29 du module 28 de sécurisation. Par exemple, la fonction prédéterminée est une fonction à sens unique telle qu'une fonction de hachage. Dans ce cas, généralement, l'empreinte numérique est le résultat de l'application de cette fonction de hachage à une combinaison, par exemple une concaténation, du cryptogramme BD_i^* et des métadonnées MD_i . La taille du code MAC_i est typiquement supérieure ou égale à 32 bits ou 64 bits. Ici, la taille du code MAC_i est égale à seize octets.

[0072] Dans ce mode de réalisation, pour accélérer les transferts de données entre le microprocesseur 2 et l'ensemble 4 de mémoires, les tailles T_b et T_{BD} sont toutes les deux des puissances de deux. Pour cela la taille T_b est égale à deux fois la taille T_{BD} . Ainsi, dans cet exemple, T_{BD} est égale à 64 octets. Dans ces conditions, la taille des métadonnées MD_i est égale à quarante huit octets. Sur ces quarante huit octets, huit d'entre-eux sont utilisés pour stocker les identifiant $IP_{i,j}$ et huit octets sont utilisés pour stocker le vecteur ivi .

[0073] Enfin, l'adresse $@_{BDC_i}$ à laquelle débute le bloc BDC_i est définie par la relation (1) suivante : $@_{BDC_i} = @_{BD_i} \cdot T_b / T_{BD}$. Le ratio $@_{BD_i} / T_{BD}$ est ici nécessairement un nombre entier puisque l'adresse $@_{BD_i}$ est égale au cumul des tailles des blocs BD_1 à BD_{i-1} . De plus, de préférence, la relation qui convertit chaque adresse $@_{BDC_i}$ en une adresse physique dans la mémoire MP est une relation linéaire. Ainsi, les blocs BDC_i sont classés dans la mémoire MP dans le même ordre que les blocs BD_i , c'est-à-dire par ordre croissant des adresses physiques des données Di,j qui sont chiffrées dans ce bloc BDC_i . De plus, la relation (1) impose que les blocs BDC_i sont, dans la mémoire MP, immédiatement consécutifs les uns aux autres et ne se chevauchent pas.

- [0074] Dans cet exemple, le jeu d'instructions machines du microprocesseur 2 comporte notamment une instruction d'écriture et une instruction de chargement.
- [0075] Une instruction d'écriture est une instruction qui, lorsqu'elle est exécutée par l'unité 10, provoque l'écriture d'une donnée dans l'ensemble 4.
- [0076] Une instruction de chargement est une instruction qui, lorsqu'elle est exécutée par l'unité 10, provoque le chargement d'une donnée dans le microprocesseur 2 à partir de l'ensemble 4. Généralement, la donnée chargée est enregistrée dans un registre du microprocesseur comme, par exemple, un des registres de l'ensemble 12.
- [0077] A titre d'illustration, le microprocesseur 2 est conforme à l'architecture RISC (« Reduced Instructions Set Computer ») et il met en œuvre le jeu d'instructions "RISC-V".
- [0078] Ici, l'unité 10 est une unité arithmétique et logique de N_{inst} bits. Typiquement, N_{inst} est un entier supérieure ou égale à 8, 16, 32 ou 64. Dans cet exemple, N_{inst} est égal à 32.
- [0079] Le chargeur 18 charge dans la file 22 la prochaine instruction à exécuter par l'unité 10 à partir de l'ensemble 4 de mémoires. Plus précisément, le chargeur 18 charge l'instruction sur laquelle pointe le compteur ordinal 26.
- [0080] L'unité 10 est notamment configurée pour exécuter les unes après les autres les instructions chargées dans la file 22. Les instructions chargées dans la file 22 sont généralement systématiquement exécutées dans l'ordre où ces instructions ont été enregistrées dans cette file 22. L'unité 10 est aussi capable d'enregistrer le résultat de ces instructions exécutées dans un ou plusieurs des registres de l'ensemble 12.
- [0081] Dans cette description, on utilisera comme synonymes « exécution par le microprocesseur 2 » et « exécution par l'unité 10 ».
- [0082] Le tampon 14 est utilisé pour accélérer encore plus les transferts de données entre le microprocesseur 2 et l'ensemble 4 de mémoire. Pour cela, les données transférées entre le microprocesseur 2 et l'ensemble 4 sont systématiquement transférées par bloc entier contenant exactement N_d données. Plus précisément, lors du chargement d'une donnée à partir de l'ensemble 4, c'est le bloc BDC_i qui contient cette donnée qui est transféré, dans sa totalité, au microprocesseur 2 par l'intermédiaire du bus 50. A l'inverse, lorsqu'une donnée doit être écrite dans l'ensemble 4 de mémoires, c'est un bloc BDC_i complet, qui contient cette donnée écrite, qui est transféré du microprocesseur 2 vers l'ensemble 4 par l'intermédiaire du bus 50.
- [0083] Ici, le tampon 14 est une mémoire déchiffrée, c'est-à-dire une mémoire dans laquelle les données sont enregistrées en clair. Ce tampon 14 est apte à contenir au moins un bloc BD_i de données en clair. Dans ce mode de réalisation, à titre d'illustration, il est apte à contenir un seul bloc de données BD_i .
- [0084] Le module 28 est capable d'exécuter automatiquement les différentes opérations décrites en détails en référence au procédé de la [fig.6] pour sécuriser l'exécution du

programme d'ordinateur. En particulier, il est apte à transformer un bloc BDC_i en un bloc BD_i de données en clair et vice versa. Le module 28 fonctionne indépendamment et sans utiliser l'unité 10. Ainsi, il est capable de traiter des blocs de données avant et/ou après que ceux-ci soient traités par l'unité 10. A cet effet, il comporte notamment la mémoire non-volatile sécurisée 29. Aucun accès à cette mémoire 29 sans passer par l'intermédiaire du module 28 n'est prévu. En particulier, l'unité 10 ne peut pas adresser cette mémoire 29. Dans ce mode de réalisation, le module 28 est pré-programmé, par exemple lors de sa conception, pour exécuter des opérations telles que les opérations suivantes :

- vérifier l'intégrité et l'authenticité d'un bloc BDC_i à partir du code MAC_i qu'il contient,
- calculer un code MAC_i ,
- chiffrer le bloc BD_i pour obtenir le cryptogramme BD_i^* ,
- déchiffrer le cryptogramme BD_i^* pour obtenir le bloc BD_i de données en clair.

[0085] La mémoire 29 est utilisée pour stocker les informations secrètes nécessaires à la mise en œuvre du procédé de la [fig.6]. Ici, elle comporte donc notamment des informations secrètes pré-enregistrées avant le début de l'exécution du code binaire 30. En particulier, elle comporte les informations pré-enregistrées suivantes :

- une clé secrète k' utilisée pour le calcul et la vérification des codes MAC_i ,
- une clé privée secrète sk_{CPU} qui permet de déchiffrer les données qui ont été chiffrées à l'aide de la clé publique pk_{CPU} .

[0086] Dans ce mode de réalisation, la mémoire 29 comporte aussi :

- un registre R_{iv} pour stocker un vecteur d'initialisation iv_i , et
- un registre B_{IP} pour stocker les identifiants de pointeur.

[0087] Dans cet exemple de réalisation, l'ensemble 12 comporte des registres généraux utilisables pour stocker tout type de données.

[0088] Un bus d'échange de données 24 relie les différents composants du microprocesseur 2 entre eux. Il est représenté sur la [fig.1] pour indiquer que les différents composants du microprocesseur 2 peuvent échanger des données entre eux.

[0089] Le support 6 est typiquement une mémoire non volatile. Par exemple, il s'agit d'une mémoire du type EEPROM ou Flash. Il contient ici une copie 40 de sauvegarde du code binaire 30. Typiquement, c'est cette copie 40 qui est automatiquement recopiée dans la mémoire 4 pour restaurer le code 30, par exemple, après une coupure de courant ou similaire ou juste avant que débute l'exécution du code 30.

[0090] La [fig.4] représente la structure du pointeur PDi,j . Ici, la taille du pointeur PDi,j est égale à la taille $N@$ des adresses mémoires. Le pointeur PDi,j comporte :

- une plage P_1 de bits contenant l'adresse $@_{Di,j}$ vers laquelle le pointeur PDi,j pointe, et
- une plage P_2 distincte de bits contenant l'identifiant $IP_{i,j}$ du pointeur PDi,j .

- [0091] Les données $D_{i,j}$ sont contenues dans une plage d'adresses de l'espace d'adressage du programme dont la taille est strictement inférieure à $2^{N@}$ afin de laisser suffisamment de place pour coder l'identifiant $IP_{i,j}$ à l'intérieur du pointeur $PD_{i,j}$. Pour cela, la taille de la plage P_1 est inférieure à $N@ - N_P$ bits, où N_P est la taille, en nombre de bits, de l'identifiant $IP_{i,j}$. De préférence, la taille N_P est supérieure à 4 bits ou 8 bits ou 16 bits et, généralement, inférieure à 32 bits ou 54 bits. Ici, la taille N_P est égale à 8 bits et les adresses $@_{D_{i,j}}$ sont donc codées sur moins de 56 bits. Dans ce mode de réalisation, la plage P_1 correspond aux $N@ - N_P$ bits de poids faibles du pointeur $PD_{i,j}$ et la plage P_2 correspond au N_P bits de poids forts du pointeur $PD_{i,j}$. Pour obtenir l'adresse $@_{D_{i,j}}$ de la donnée $D_{i,j}$ à partir du pointeur $PD_{i,j}$, il suffit donc de masquer les bits de poids forts du pointeur $PD_{i,j}$ utilisés pour enregistrer l'identifiant $IP_{i,j}$.
- [0092] Un tel pointeur $PD_{i,j}$ qui contient, en plus de l'adresse $@_{D_{i,j}}$, d'autres informations, c'est-à-dire ici l'identifiant $IP_{i,j}$, est appelé "pointeur enrichi".
- [0093] La [fig.5] représente un procédé d'exécution du code binaire 30 par le microprocesseur 2.
- [0094] Le procédé débute par une étape 150 de génération puis de fourniture du code binaire 30 dans la mémoire MP. La génération du code binaire 30 est typiquement réalisée par un compilateur tel que celui décrit, plus loin, en référence à la [fig.7].
- [0095] Lors de la compilation du code source, à chaque fois que le compilateur construit un bloc BDC_i , pour chaque donnée $D_{i,j}$ qui est chargée à l'aide d'un pointeur $PD_{i,j}$, il enregistre l'identifiant $IP_{i,j}$ de ce pointeur dans les métadonnées MD_i . Pour les données $D_{i,j}$ qui ne sont pas accédées à l'aide d'un pointeur, les bits situés à l'emplacement, dans les métadonnées MD_i , réservé pour y enregistrer l'identifiant de pointeur associé à cette donnée, sont initialisés à zéro. Autrement dit, l'identifiant de pointeur associé à une donnée qui n'a pas été accédée à l'aide d'un pointeur, est nul.
- [0096] La fourniture du code binaire 30 consiste ensuite à enregistrer la copie 40 dans le support 6. Puis, par exemple, le microprocesseur 2 recopie la copie 40 à l'intérieur de la mémoire MP pour obtenir le code binaire 30 enregistré dans la mémoire MP. Ainsi, lors de l'étape 150, les blocs BDC_i construits lors de la compilation du code source et contenus dans le code binaire 30, sont enregistrés dans la mémoire MP et, généralement, dans la partie 44.
- [0097] Ensuite, lors d'une phase 152, le microprocesseur 2 exécute le code binaire 30 et, en particulier, le code machine 32.
- [0098] Au début de la phase 152, lors d'une étape 154, le module 28 charge notamment le cryptogramme ka^* contenu dans le bloc 34 et le déchiffre à l'aide de la clé sk_{CPU} contenue dans la mémoire 29. À l'issue de l'étape 154, la clé ka est contenue dans la mémoire 29.
- [0099] Ensuite, lors de l'étape 162, le microprocesseur 2 exécute, les unes après les autres,

les instructions du code machine 32. Lors de cette étape 162, des instructions de chargement d'une donnée à l'aide d'un pointeur et des instructions d'écriture d'une donnée à l'aide d'un pointeur sont exécutées. Par la suite, ces deux types d'instructions sont collectivement désignées par l'expression "instruction d'accès" ou "instruction d'accès à la mémoire". A chaque fois qu'une instruction d'accès à la mémoire est exécutée par le microprocesseur 2, le procédé de la [fig.6] est exécuté.

[0100] Le procédé de sécurisation des données enregistrées dans l'ensemble 4 va maintenant être décrit à l'aide de la [fig.6] et dans le cas où la donnée accédée est une donnée $D_{i,j}$ accédée à l'aide du pointeur $PD_{i,j}$.

[0101] Tout d'abord, lors d'une étape 166, le pointeur $PD_{i,j}$ est obtenu. Typiquement, l'instruction d'accès à la donnée $D_{i,j}$ exécutée par l'unité 10 comporte un opérande qui contient l'adresse à laquelle le pointeur $PD_{i,j}$ est enregistré. Ainsi, l'exécution de cette instruction d'accès par l'unité 10 déclenche d'abord le chargement du pointeur $PD_{i,j}$ dans un registre du microprocesseur 2.

[0102] Ensuite, lors d'une étape 170, le pointeur $PD_{i,j}$ est transmis au module 28.

[0103] Lors d'une étape 172, le module 28 détermine l'adresse $@_{BDCi}$ du bloc BDC_i qui contient cette donnée $D_{i,j}$. Pour cela, le module 28 calcule ici l'adresse $@_{BDCi}$ selon la relation (2) suivante : $@_{BDCi} = E(@_{Di,j}/T_{BD}).T_b$, où :

- $E(...)$ est la fonction qui retourne la partie entière du nombre entre parenthèses, et
- T_{BD} et T_b sont les tailles, en nombre d'octets, respectivement du bloc BD_i et du bloc BDC_i .

[0104] La fonction $E(...)$ est connue sous le terme anglais de "floor".

[0105] Le terme $E(@_{Di,j}/T_{BD})$ donne le numéro d'ordre du bloc BDC_i à partir duquel la donnée $D_{i,j}$ peut être chargée. Étant donné que dans ce mode de réalisation, les tailles T_{BD} et T_b sont toutes les deux des puissances de deux, la division par la taille T_{BD} et la multiplication par la taille T_b peuvent toutes les deux être réalisées par un registre à décalage. Un registre à décalage décale les bits du nombre qu'il contient vers la droite pour réaliser une division et vers la gauche pour réaliser une multiplication. Plus précisément, dans ce mode de réalisation, la taille T_{BD} est égale à 2^6 octets et la taille T_b est égale à 2^7 octets. Ici, le module 28 comporte donc un registre matériel à décalage. Dans ces conditions, le module 28 est capable de calculer très rapidement, et typiquement en un cycle d'horloge, l'adresse $@_{BDCi}$.

[0106] Ainsi, ici, pour calculer l'adresse $@_{BDCi}$, le module 28 enregistre l'adresse $@_{Di,j}$ dans son registre à décalage puis décale de six bits vers la droite les bits de l'adresse enregistrée dans ce registre pour obtenir le résultat du ratio $@_{Di,j}/T_{BD}$. Ensuite le module 28 calcule la partie entière du ratio obtenu puis enregistre cette partie entière dans le registre à décalage. Enfin, le registre à décalage décale de sept bits vers la gauche les bits de cette partie entière pour obtenir l'adresse $@_{BDCi}$.

- [0107] Il est préférable que le calcul de l'adresse $@_{BDC_i}$ soit très rapide, car ce calcul est réalisé à chaque fois qu'une donnée est accédée.
- [0108] Une fois l'adresse $@_{BDC_i}$ déterminée, lors d'une étape 174, le module 28 vérifie si l'adresse $@_{BDC_i}$ est égale à une adresse $@_{BDC_c}$. L'adresse $@_{BDC_c}$ est l'adresse du bloc BDC_c à partir duquel le bloc BDC_c actuellement contenu dans le tampon 14 a été obtenu. L'adresse $@_{BDC_c}$ est, par exemple, enregistrée dans la mémoire 29.
- [0109] Dans l'affirmative, cela signifie que le bloc BD_i qui contient la donnée $D_{i,j}$ à accéder est déjà enregistré dans le tampon 14. Autrement dit, les blocs BD_i et BD_c sont les mêmes. Dans ce cas, le procédé se poursuit :
- directement par une étape 176 si l'instruction d'accès exécutée est une instruction de chargement, ou
 - directement par une étape 190 si l'instruction d'accès exécutée est une instruction d'écriture.
- [0110] Lors de l'étape 176, pour la donnée $D_{i,j}$ à charger, le module 28 relève le premier identifiant $IP_{i,j}$ contenu dans les métadonnées MD_i du bloc BDC_i et associé à cette donnée $D_{i,j}$. Ici, comme expliqué plus loin, ce premier identifiant $IP_{i,j}$ se trouve dans le registre B_{IP} . Le premier identifiant $IP_{i,j}$ est donc extrait de ce registre B_{IP} . Le module 28 relève aussi le second identifiant $IP_{i,j}$ contenu dans le pointeur $PD_{i,j}$ transmis lors de l'étape 170. Pour cela, le module 28 extrait le second identifiant $IP_{i,j}$ de la plage P_2 du pointeur $PD_{i,j}$ reçu. Ensuite, le module 28 vérifie si les premier et second identifiants $IP_{i,j}$ extraits correspondent. Ici, les premier et second identifiants $IP_{i,j}$ correspondent uniquement s'ils sont égaux.
- [0111] Si les premier et second identifiants $IP_{i,j}$ correspondent, lors d'une étape 178, le traitement de la donnée $D_{i,j}$ par le microprocesseur 2 est autorisé. Dans ce cas, la donnée $D_{i,j}$ est alors directement chargée à partir du tampon 14 puis, par exemple, transférée dans l'un des registres de l'ensemble 12. Ensuite, l'unité 10 exécute des instructions de traitement de cette donnée $D_{i,j}$ enregistrée dans un registre de l'ensemble 12.
- [0112] Si les premier et second identifiants $IP_{i,j}$ ne correspondent pas, c'est-à-dire qu'ils sont différents, dans ce cas, le procédé se poursuit par une étape 180. Lors de l'étape 180, le module 28 déclenche le signalement d'une faute d'exécution du code binaire 30. De plus, ici, lors de l'étape 180, le traitement, par le microprocesseur 2, de la donnée $D_{i,j}$ est interdit. Par exemple, lors de l'étape 180, la donnée $D_{i,j}$ n'est pas chargée dans un registre de l'ensemble 12.
- [0113] Ensuite, lors d'une étape 182, en réponse à ce signalement d'une faute d'exécution, le microprocesseur 2 met en œuvre une ou plusieurs mesures correctives et/ou une ou plusieurs contre-mesures.
- [0114] De très nombreuses contre-mesures sont possibles. Les contre-mesures mises en

œuvre peuvent avoir des degrés de sévérité très différents. Par exemple, les contre-mesures mises en œuvre peuvent aller d'un simple affichage ou une simple mémorisation d'un message d'erreur sans interrompre l'exécution normale du code binaire, jusqu'à une mise hors service définitive du microprocesseur 2. Le microprocesseur 2 est considéré comme étant hors service lorsqu'il est définitivement placé dans un état où il est incapable d'exécuter un quelconque code binaire. Entre ces degrés de sévérité extrêmes, il existe de nombreuses autres contre-mesures possibles telles que :

- l'indication par l'intermédiaire d'une interface homme-machine de la détection des fautes,
- l'interruption immédiate de l'exécution du code binaire et/ou sa réinitialisation, et
- la suppression du code binaire de la mémoire MP et/ou la suppression de la copie 40 de sauvegarde et/ou la suppression des données secrètes.

- [0115] Lors de l'étape 190, la valeur à écrire dans la donnée $D_{i,j}$ est directement écrite dans la donnée $D_{i,j}$ du bloc de données BD_i actuellement enregistré dans le tampon 14.
- [0116] Ensuite, lors d'une étape 192, le module 28 remplace, dans le registre B_{IP} , le précédent identifiant $IP_{i,j}$ associé à la donnée $D_{i,j}$ par l'identifiant $IP_{i,j}$ du pointeur $PD_{i,j}$ transmis lors de l'étape 170.
- [0117] Ici, lors de l'écriture de la donnée $D_{i,j}$ dans le tampon 14, le module 28 ne procède pas à la vérification de l'identifiant $IP_{i,j}$ associé à cette donnée. Au contraire, à chaque fois qu'une donnée est écrite dans le tampon 14, le module 28 autorise l'utilisation du pointeur $PD_{i,j}$ pour charger ultérieurement la donnée $D_{i,j}$.
- [0118] De plus, lors de l'étape 192, le module 28 bascule un indicateur d'écriture vers son état actif. Ainsi, l'état actif de cet indicateur d'écriture indique que le bloc BD_c actuellement présent dans le tampon 14 a été écrit. A l'inverse, l'état inactif de cet indicateur d'écriture indique que le bloc BD_c actuellement enregistré dans le tampon 14 n'a pas été écrit. Un tel indicateur d'écriture est connu sous le terme anglais de « bit dirty ».
- [0119] Si lors de l'étape 174, l'adresse $@_{BDC_i}$ est différente de l'adresse contenue dans la mémoire 29, cela signifie que le bloc BD_c actuellement contenu dans le tampon 14 ne contient pas la donnée $D_{i,j}$ à accéder. Dans ce cas, le procédé se poursuit par une étape 200.
- [0120] Lors de l'étape 200, le module 28 vérifie si le bloc BD_c actuellement contenu dans le tampon 14 a été écrit. Typiquement, pour faire cela, le module 28 vérifie l'état de l'indicateur d'écriture.
- [0121] Si l'indicateur d'écriture est dans son état inactif, il n'est pas nécessaire d'enregistrer le bloc BD_c dans l'ensemble 4. Dans ce cas, le procédé se poursuit directement par une étape 300 de transfert du bloc BDC_i qui contient la donnée $D_{i,j}$ chiffrée depuis l'ensemble 4 vers le tampon 14.
- [0122] Dans le cas contraire, le bloc BD_c actuellement enregistré dans le tampon 14 doit être

sauvegardé dans l'ensemble 4. Dans ce cas, le procédé se poursuit par une étape 400 de transfert du bloc BD_c actuellement contenu dans le tampon 14 vers l'ensemble 4.

[0123] L'étape 300 débute par une opération 302 de chargement du bloc BDC_i situé à l'adresse $@_{BDC_i}$ déterminée lors de l'étape 172. Typiquement, lors de l'opération 302, l'adresse $@_{BDC_i}$ est convertie automatiquement en une adresse physique par l'unité MMU ("Management Memory Unit"). De préférence, le bloc BDC_i est chargé depuis l'ensemble 4 vers le microprocesseur en utilisant un mode de transfert accéléré de bloc de données sur le bus 50. Un tel mode est par exemple connu sous le terme anglais de « burst mode ».

[0124] Le bloc BDC_i chargé est alors temporairement stocké dans le microprocesseur 2. Par exemple, il est enregistré dans l'ensemble 12 ou dans la mémoire 29 ou dans le tampon 14.

[0125] Lors de l'opération 304, le module 28 vérifie l'intégrité du bloc BDC_i chargé. Ici, il vérifie l'intégrité et l'authenticité du cryptogramme BD_i^* et des métadonnées MD_i à l'aide du code MAC_i . Pour cela, le module 28 calcule un code MAC_i' en utilisant le même algorithme que celui mis en œuvre pour construire le code MAC_i sauf qu'il utilise le cryptogramme BD_i^* et les métadonnées MD_i chargés lors de l'opération 302. Si le code MAC_i' ainsi construit est identique au code MAC_i chargé, alors l'intégrité et l'authenticité du cryptogramme BD_i^* et des métadonnées MD_i est confirmée.

[0126] Dans ce cas, le module 28 procède, lors d'une opération 306, au déchiffrement du cryptogramme BD_i^* en utilisant pour cela la clé k_a enregistrée dans sa mémoire 29 et le vecteur iv_i extrait des métadonnées MD_i du bloc BDC_i chargé.

[0127] Après l'opération 306, lors d'une opération 308, le bloc BD_i en clair obtenu est enregistré dans le tampon 14 à la place du précédent bloc de données. A cette occasion, l'indicateur d'écriture est basculé dans son état inactif.

[0128] Lors de l'opération 308, le module 28 enregistre également les identifiants $IP_{i,j}$ contenus dans les métadonnées MD_i du bloc BDC_i chargé dans le registre B_{IP} de la mémoire 29. Le vecteur iv_i contenu dans les métadonnées MD_i du bloc BDC_i chargé est lui aussi enregistré dans le registre R_{iv} de la mémoire 29. Enfin, l'adresse $@_{BDC_i}$ du bloc BDC_i chargé est aussi enregistrée dans la mémoire 29. Cette adresse $@_{BDC_i}$ enregistrée devient la nouvelle adresse $@_{BDC}$.

[0129] Dans le cas où la vérification de l'intégrité du bloc BDC_i échoue, le module 28 procède à une opération 310 d'inhibition du traitement des données de ce bloc. Par exemple, ici, lors de l'opération 310, le module 28 remplace le bloc BD_c enregistré dans le tampon 14 par un bloc BD_i vierge. Lors de cette opération 310, le module 28 initialise toutes les données du bloc BD_i vierge à une valeur prédéterminée. Typiquement, cette valeur prédéterminée est la valeur zéro. Ensuite, ce bloc BD_i vierge est enregistré dans le tampon 14 à la place du bloc BD_c . Toujours lors de cette opération 310, le module 28 initialise aussi à zéro tous les identifiants $IP_{i,j}$ contenus dans le registre B_{IP} de la mémoire 29. Il ré-initialise aussi la valeur du vecteur iv_i contenue dans le registre R_{iv} . Par exemple, la nouvelle valeur du vecteur

iv_i contenu dans le registre R_{iv} est générée par tirage aléatoire ou pseudo-aléatoire. Enfin, l'adresse $@BDC_i$ du bloc BDC_i chargé est aussi enregistrée dans la mémoire 29. Ainsi, dans le cas où la vérification de l'intégrité du bloc BDC_i échoue, c'est un bloc BD_i vierge qui est enregistré dans le tampon 14.

- [0130] Après l'opération 308 ou 310, le procédé se poursuit par l'étape 176 ou l'étape 190 selon que l'instruction à exécuter est une instruction de chargement ou une instruction d'écriture.
- [0131] L'étape 400 débute par une opération 402 de transformation du bloc BD_c en un bloc BDC_c .
- [0132] Pour cela, lors d'une sous-opération 404, le module 28 commence par générer un nouveau vecteur iv_i . Le nouveau vecteur iv_i est par exemple généré à partir de l'ancienne valeur de ce vecteur iv_i enregistrée dans le registre R_{iv} . Par exemple, le nouveau vecteur iv_i est obtenu en incrémentant cette ancienne valeur d'un pas prédéterminé.
- [0133] Ensuite, lors d'une sous opération 406, le module 28 chiffre le bloc BD_c actuellement contenu dans le tampon 14 en utilisant pour cela la clé ka et le nouveau vecteur iv_i généré lors de la sous-opération 404. A l'issue de cette opération, le cryptogramme BD_{c*} est obtenu.
- [0134] Lors d'une sous-opération 408, le module 28 construit les métadonnées MD_c . Pour cela, le module enregistre, dans les emplacements réservés à cet effet, les identifiants $IP_{i,j}$ actuellement contenus dans le registre B_{IP} et le vecteur iv_i enregistré dans le registre R_{iv} . Ensuite, le module 28 calcule le nouveau code MAC_c à partir du cryptogramme BD_{c*} obtenu à l'issue de la sous-opération 406 et des métadonnées MD_c construites.
- [0135] Enfin, une fois le nouveau code MAC_c calculé, à la fin de la sous-opération 408, le module 28 regroupe dans un même bloc de données, le cryptogramme BD_{c*} , les métadonnées construites MD_c et le nouveau code MAC_c afin d'obtenir un nouveau bloc BDC_c .
- [0136] Après, lors d'une opération 410, le nouveau bloc BDC_c est enregistré dans l'ensemble 4 à l'adresse physique correspond à l'adresse $@_{BDC_c}$ actuellement contenue dans la mémoire 29.
- [0137] L'étape 400 s'achève alors et le procédé se poursuit par l'étape 300.
- [0138] La [fig.7] représente un compilateur 500 apte à générer automatiquement le code binaire 30 à partir d'un code source 502 du programme d'ordinateur. À cet effet, le compilateur 500 comporte typiquement un microprocesseur 504 programmable et une mémoire 506. La mémoire 506 contient les instructions et les données nécessaires pour, lorsqu'elles sont exécutées par le microprocesseur 504, générer automatiquement le code binaire 30 à partir du code source 502. Par exemple, pour cela, le compilateur parcourt le code source 502 et génère, pour chaque pointeur PDi,j à protéger, l'identifiant IPi,j de ce pointeur. L'identifiant IPi,j ainsi généré est enregistré dans la

plage P2 de ce pointeur I_{Pi,j}. Après cela, les bloc BDC_i qui seront ensuite enregistrés dans la partie 44 de la mémoire MP après chargement de ce code binaire 30 dans cette mémoire MP, sont générés. Plus précisément, lors de la compilation, le compilateur 500 transforme chaque bloc BDi en clair destiné à être enregistré dans la partie 44 de la mémoire MP en un bloc BDC_i de façon similaire à ce qui a été décrit en référence au procédé de la [fig.6]. En particulier, pour chaque donnée Di,j du bloc BDi accédée à l'aide d'un pointeur PDi,j, le compilateur insère automatiquement l'identifiant I_{Pi,j} de ce pointeur à l'emplacement réservé à cet effet dans les métadonnées MDi. La conception et la réalisation d'un tel compilateur sont à la portée de l'homme du métier à partir des explications données dans cette description.

[0139] CHAPITRE III : VARIANTES

[0140] Variantes de l'appareil 1 :

[0141] D'autres modes de réalisation de l'ensemble 4 sont possibles. Par exemple, l'ensemble 4 peut comporter un plus grand nombre ou un plus petit nombre de mémoires caches. Dans un cas très simplifié, l'ensemble 4 ne comporte pas de mémoire cache et comporte, par exemple, seulement la mémoire principale MP.

[0142] La mémoire MP peut être une mémoire non volatile. Dans ce cas, il n'est pas nécessaire de copier le code binaire 30 à l'intérieur de cette mémoire avant le lancement de son exécution puisqu'il s'y trouve déjà.

[0143] Le fait qu'une mémoire de l'ensemble 4 soit intégrée ou non à l'intérieur du microprocesseur 2 peut être librement modifié. Ainsi, en variante, une ou plusieurs des mémoires caches L1, L2 et L3 sont intégrées à l'intérieur du microprocesseur 2, c'est-à-dire réalisées sur la même puce semi-conductrice que l'unité 10 du microprocesseur 2. En variante, la mémoire MP peut aussi être une mémoire interne intégrée à l'intérieur du microprocesseur 2.

[0144] De nombreuses architectures matérielles différentes sont possibles pour réaliser le module 28. En particulier, le module 28 peut être composé par la combinaison de plusieurs blocs matériels du microprocesseur 2 remplissant des fonctions respectives et situés chacun dans une aire différente de la puce du microprocesseur 2.

[0145] En variante, le tampon 14 est apte à contenir simultanément plusieurs blocs de données en clair.

[0146] Variantes du code d'authentification :

[0147] D'autres méthodes de calcul du code d'authentification sont possibles. Par exemple, en variante, le module 28 calcule un premier code d'authentification uniquement à partir du cryptogramme BD_{i*} et un second code d'authentification uniquement à partir des métadonnées MD_i. Dans ce cas, le code d'authentification contenu dans le bloc BDC_i est le résultat, par exemple, de la concaténation de ce premier et de ce second codes d'authentification. Ensuite, les premier et second codes d'authentification sont

utilisés par le module 28 pour vérifier l'intégrité, respectivement, du cryptogramme BD_i^* et des métadonnées MD_i lors de l'opération 304.

[0148] Dans un autre mode de réalisation, le code MAC_i est calculé à partir du cryptogramme BD_i^* et sans prendre en compte les métadonnées MD_i . Dans ce cas, de préférence, les métadonnées MD_i sont alors chiffrées de sorte qu'elles n'apparaissent pas en clair dans le bloc BDC_i . Par exemple, elles sont chiffrées à l'aide de la fonction f_{ka} .

[0149] Dans une autre variante, le code MAC_i est calculé à partir des données $D_{i,j}$ en clair et non pas à partir du cryptogramme BD_i^* . Dans ce cas, il faut inverser l'ordre des opérations de vérification de l'intégrité du code d'authentification et de déchiffrement du cryptogramme BD_i^* . En effet, dans ce cas, les données doivent d'abord être déchiffrées et seulement ensuite, le module 28 est en mesure d'en vérifier l'intégrité.

[0150] Variantes des métadonnées :

[0151] En variante les métadonnées MD_i comportent d'autres données que les identifiants $IP_{i,j}$ et que le vecteur iv_i . Par exemple, les métadonnées peuvent en plus comporter des indicateurs de validité tels que ceux décrits dans la demande américaine déposée le 02/12/2020 sous le numéro 17/109,424. A l'inverse, dans un mode de réalisation simplifié, les métadonnées MD_i ne comportent pas le vecteur iv_i . Dans ce dernier cas, le vecteur iv_i à utiliser pour déchiffrer le cryptogramme BD_i^* est alors stocké différemment. Par exemple, un registre associant, à chaque bloc BDC_i , le vecteur iv_i nécessaire pour déchiffrer le cryptogramme BD_i^* est enregistré dans la mémoire MP.

[0152] Les métadonnées peuvent être enregistrées dans le tampon 14 ou dans un registre indépendant du tampon 14 et de la mémoire 29. Dans le cas où les métadonnées MD_i sont enregistrées dans le tampon 14, celles-ci sont, de préférence, enregistrées dans une plage d'adresses distincte de la plage d'adresses où sont enregistrées les données $D_{i,j}$. Typiquement, cette plage d'adresses distincte n'est pas adressable par l'unité 10 de sorte que la présence des métadonnées MD_i dans le tampon 14 ne modifie en rien l'adressage des données $D_{i,j}$. Par contre, les métadonnées MD_i sont accessibles par le module 28 pour qu'il puisse mettre en œuvre les différentes étapes décrites dans le chapitre II.

[0153] En variante, lorsque le nouveau vecteur iv_i d'un bloc BDC_i est généré sans prendre en compte sa précédente valeur, il n'est pas nécessaire de sauvegarder sa précédente valeur dans le registre R_{iv} après le chargement du bloc BDC_i dans le tampon 14. C'est par exemple le cas lorsque, à chaque transfert d'un bloc de données du tampon 14 vers l'ensemble 4, le nouveau vecteur iv_i est généré par tirage aléatoire ou pseudo aléatoire.

[0154] D'autres méthodes de génération d'un nouveau vecteur iv_i sont possibles. Par exemple, le nouveau vecteur iv_i est pris égal à la précédente valeur du code MAC_i . Dans ce cas, à chaque fois qu'un bloc BDC_i est transféré de l'ensemble 4 vers le

tampon 14, le code MAC_i contenu dans ce bloc BDC_i est enregistré dans le micro-processeur, par exemple, dans la mémoire 29.

- [0155] Le nouveau vecteur iv_i peut aussi être complété par d'autres informations pour obtenir un vecteur d'initialisation complet ivc_i puis, lors de l'opération 406 de chiffrement, c'est ce vecteur ivc_i qui est utilisé à la place du vecteur iv_i . Dans ce cas, le cryptogramme BD_{i*} est le résultat de la fonction $f_{ka}(BD_i ; ivc_i)$. L'opération 306 de déchiffrement doit alors être adaptée en conséquence. Autrement dit, le bloc BD_i en clair est le résultat de la fonction $f_{ka}^{-1}(BD_{i*} ; ivc_i)$. Par exemple, le vecteur ivc_i est obtenu en combinant le vecteur iv_i et l'adresse $@_{BDC_i}$ contenue dans la mémoire 29. Par exemple, le vecteur iv_i et l'adresse $@_{BDC_i}$ sont concaténés. Le vecteur ivc_i peut aussi être obtenu en combinant le vecteur iv_i avec un identifiant du code binaire 30. Dans ce cas, le cryptogramme BD_{i*} obtenu est fonction du code binaire 30 à exécuter. Le vecteur ivc_i peut aussi être obtenu en combinant le vecteur iv_i , l'adresse $@_{BDC_i}$ et l'identifiant du code binaire 30.
- [0156] Variantes du procédé :
- [0157] D'autres modes de réalisation de l'étape 176 sont possibles. Par exemple, lors de l'étape 176, deux identifiants de pointeurs sont dit correspondant si l'écart entre ces deux identifiants est inférieur, en valeur absolue, à un seuil prédéterminé.
- [0158] L'étape 176 peut aussi être exécutée avant l'étape 304 de vérification de l'intégrité du bloc de données chargés. Dans ce cas, par exemple, les étapes 304, 306, 308 et 310 sont exécutées entre les étapes 176 et 178.
- [0159] Lorsque la vérification de l'intégrité du code MAC_i échoue, une ou plusieurs des contre-mesures précédemment décrites peuvent être déclenchées et exécutées.
- [0160] En variante, une autre relation que la relation (1) est utilisée pour déterminer l'adresse $@_{BDC_i}$ où est enregistré le bloc BDC_i . Dans ce cas, la relation (2) doit être adaptée en conséquence. Par exemple, dans un mode de réalisation particulièrement souple, le module 28 comporte une table de correspondance qui, à chaque adresse $@_{BD_i}$ d'un bloc BD_i en clair associe l'adresse $@_{BDC_i}$ du bloc BDC_i contenant les données $D_{i,j}$ sous forme chiffrée. Dans un tel cas, le module 28 peut déterminer l'adresse $@_{BDC_i}$ du bloc contenant la donnée $D_{i,j}$ située à l'adresse $@_{Di,j}$ en mettant en œuvre les étapes suivantes :
- Étape 1 : le module 28 calcule l'adresse $@_{BD_i}$ du bloc BD_i qui contient la donnée $D_{i,j}$ à l'aide de la relation suivante : $@_{BD_i} = E(@_{Di,j}/T_{BD}).T_{BD}$, puis
 - Étape 2 : le module 28 recherche dans la table de correspondance l'adresse $@_{BDC_i}$ associée à l'adresse $@_{BD_i}$ calculée.
- [0161] Le fait que les tailles T_b et T_{BD} soient toutes les deux des puissances de deux impose que la taille T_b est deux fois plus grande que la taille T_{BD} . Ainsi à chaque fois que la taille T_{BD} est augmentée, la taille T_b doit aussi être augmentée de façon proportionnelle.

Cela revient donc à augmenter l'espace disponible pour stocker les métadonnées MD_i et le code MAC_i . Or, il n'est pas toujours souhaitable d'augmenter l'espace disponible pour stocker les métadonnées MD_i et le code MAC_i car cela revient à occuper plus de place en mémoire, sans que cela se traduise nécessairement par une amélioration des performances de l'appareil 1. Ainsi, en variante, la taille T_b n'est pas égale à deux fois la taille T_{BD} . Par exemple, la taille T_b est plus petite que $2T_{BD}$. Dans ce dernier cas, de préférence, les tailles T_b et T_{BD} sont alors choisies de manière à ce que le nombre $(T_b - T_{BD})$ et la taille T_{BD} sont tous les deux des puissances de deux. Dans ce cas, la relation (1) est remplacée par la relation (3) suivante : $@_{BDCi} = @_{BDi} + @_{BDi}(T_b - T_{BD})/T_{BD}$. La relation (2) est remplacée par la relation (4) suivante : $@_{BDCi} = E(@_{Di,j}/T_{BD}).T_{BD} + E(@_{Di,j}/T_{BD})(T_b - T_{BD})$. Dans les relations (3) et (4), les multiplications et les divisions peuvent toujours être réalisées en utilisant les registres à décalage du module 28 et donc très rapidement. Par contre, par rapport au cas où ce sont les relations (1) et (2) qui sont utilisées, il faut réaliser une opération d'addition en plus pour calculer l'adresse $@_{BDCi}$. Par conséquent, cette variante est un peu moins rapide que ce qui a été décrit dans le chapitre II. Par contre, elle présente l'avantage d'autoriser une taille T_{BD} qui est supérieure à la taille $(T_b - T_{BD})$, c'est-à-dire supérieure à la taille des métadonnées MD_i et du code MAC_i .

[0162] Ce qui a été décrit en détail dans le cas particulier de la partie 44 de la mémoire MP, s'applique à tout autre partie de la mémoire MP contenant des données à protéger. Par exemple, cela peut aussi être appliqué à la pile 46 ou au tas 48. Dans le cas du tas 48, comme déjà indiqué précédemment, l'identifiant $IP_{i,j}$ est généré en même temps que le pointeur $PD_{i,j}$, c'est-à-dire non pas lors de la compilation mais lors de l'exécution du code binaire 30. Ensuite, l'identifiant $IP_{i,j}$ est enregistré dans le registre B_{IP} , de préférence, à chaque fois qu'une donnée $D_{i,j}$ est écrite, à l'aide de ce pointeur $PD_{i,j}$, dans la zone de mémoire allouée dynamiquement.

[0163] Dans l'exemple détaillé de mode de réalisation, le transfert par blocs entiers entre l'ensemble 4 et le microprocesseur 2 est uniquement mis en œuvre pour les données et pas pour les instructions du code machine 30. Dans ce cas, les instructions sont enregistrées dans l'ensemble 4 de façon conventionnelle. Ainsi, dans ce mode de réalisation, les instructions sont transférées une par une vers le microprocesseur 2. De plus, dans ce cas, les instructions ne sont pas nécessairement enregistrées sous forme chiffrée dans l'ensemble 4. Toutefois, ce qui a été décrit ici dans le cas particulier des données peut aussi être appliqué aux instructions du code machine 32. Par la suite, lorsqu'un bloc contient des instructions, il est appelé "bloc d'instructions". Par exemple, comme décrit dans le cas particulier des données, le code machine est divisé en blocs d'instructions successifs et contigus. Par exemple, dans un premier mode de réalisation, la structure des bloc de données et des blocs d'instructions sont identiques. De plus, les

fonctionnements dans le cas des blocs de données et dans le cas des blocs d'instructions sont identiques. A partir de l'enseignement donné ici dans le cas particulier des blocs de données, l'homme du métier est capable de le transposer, sans difficulté, au cas des instructions. Il est donc seulement souligné que, dans le cas des instructions, l'adresse de la prochaine instruction à charger dans le microprocesseur 2 est contenue dans le compteur ordinal 26 et non pas dans une instruction de chargement exécutée par l'unité 10. Il est également souligné que, de préférence, le tampon utilisé pour stocker un bloc d'instructions en clair est un tampon, par exemple structurellement identique au tampon 14, mais distinct du tampon 14 et dédié au stockage d'un bloc d'instruction. Enfin, il faut remarquer que dans le cas des instructions, les pointeurs d'instructions sont souvent utilisés pour appeler des fonctions et ils sont donc également connus sous le terme de "pointeur de fonction". L'intérêt de traiter exactement de la même manière les instructions et les données est aussi d'harmoniser ces traitements et, par conséquent, de simplifier la réalisation du module 28 de sécurisation.

[0164] Autres variantes :

[0165] Les différents modes de réalisation et les différentes variantes ont jusqu'à présent été décrits dans le cas particulier où la mémoire déchiffrée est le tampon 14 et la mémoire chiffrée est l'ensemble 4 de mémoire, c'est-à-dire la mémoire de rang juste supérieur. Toutefois, l'enseignement donné ici s'applique à toutes mémoires déchiffrée et chiffrée entre lesquelles des données sont transférées par bloc entier de données chiffrées et authentifiées. Par exemple, en variante, la mémoire déchiffrée est la mémoire cache L1 et la mémoire chiffrée est la mémoire cache L2. Dans ce cas, le module de sécurisation est, par exemple, implémenté dans la mémoire cache L1 pour chiffrer et déchiffrer les blocs BDC_i qui sont transférés entre ces deux mémoires cache L1 et L2. On notera que dans ce cas, les données sont en clair dans la mémoire cache L1 et sont chiffrées dans la mémoire cache L2. A partir du moment où les données sont chiffrées dans la mémoire cache L2, celles-ci seront nécessairement chiffrées dans les mémoires de rang supérieur. Ce qui est décrit ici peut aussi être appliqué entre les mémoires cache L2 et L3 ou entre la mémoire cache L3 et la mémoire principale MP.

[0166] Dans le cas où le module de sécurisation est seulement implémenté entre deux niveaux de mémoire supérieure au tampon 14, le tampon 14 peut être supprimé.

[0167] Les modes de réalisation décrits ici peuvent aussi être mis en œuvre dans un appareil dépourvu de mécanisme de mémoire virtuelle. Dans ce cas, la fonction bijective qui relie les adresses virtuelles aux adresses physiques correspondantes est la fonction identité. L'unité MMU est alors omise.

[0168] Chapitre IV : Avantages des modes de réalisation décrits

[0169] L'étape 176 de vérification de la correspondance entre les premier et second identifiants $IP_{i,j}$ permet de détecter pratiquement tous les usages erronés d'un pointeur. Par

exemple, l'étape 176 détecte une utilisation incorrecte d'un pointeur PD_k pour lire la donnée $D_{i,j}$. Plus précisément, si un autre pointeur PD_k , différent du pointeur $PD_{i,j}$ attendu, est utilisé pour lire la donnée $D_{i,j}$, c'est l'identifiant IP_k qui est comparé à l'identifiant $IP_{i,j}$ extrait des métadonnées MD_i . Par conséquent, cet usage erroné du pointeur PD_k est détecté et déclenche donc le signalement d'une faute d'exécution. Si le pointeur PD_k est utilisé pour écrire une donnée D_k à la place de la donnée $D_{i,j}$, alors l'identifiant IP_k du pointeur PD_k est enregistré à la place de l'identifiant $IP_{i,j}$. Par la suite, si le pointeur $PD_{i,j}$ est utilisé pour lire la donnée D_k , l'identifiant $IP_{i,j}$ contenu dans le pointeur $PD_{i,j}$ est différent de l'identifiant IP_k contenu dans les métadonnées MD_i . Dès lors, cette utilisation erronée du pointeur PD_k est aussi détectée. Grace à cela, les attaques par dépassement de tampon sont détectées.

- [0170] De même, l'étape 176 permet de détecter l'utilisation du pointeur $PD_{i,j}$ après que la zone de mémoire contenant la donnée $D_{i,j}$ ait été libérée. En effet, typiquement, après la libération de cette zone de mémoire, celle-ci est réutilisée pour y enregistrer d'autres données. Pour réutiliser cette zone de mémoire, un nouveau pointeur PD_k est généré puis utilisé pour enregistrer des données dans cette zone de mémoire. Ce nouveau pointeur PD_k comporte un identifiant IP_k différent de l'identifiant $IP_{i,j}$. Ensuite, si le pointeur $PD_{i,j}$ est utilisé pour lire l'une des données écrites en utilisant le pointeur PD_k , ceci est détecté. En effet, dans ce cas là aussi, les identifiants de pointeur contenus, d'un côté dans le pointeur $PD_{i,j}$, et de l'autre côté, dans les métadonnées MD_{kne} correspondent pas. Ainsi, l'étape 176 permet de détecter des attaques utilisant des "dangling pointer" ou des attaques du type "use-after-free".
- [0171] Le fait de calculer le code MAC_i contenu dans le bloc BDC_i à partir des identifiant $IP_{i,j}$ rend la falsification des valeurs de ces identifiants très difficile. Cela accroît donc la sécurité du procédé d'exécution.
- [0172] Le fait d'enregistrer le vecteur iv_i dans les métadonnées MD_i permet simplement d'enregistrer puis de retrouver chaque vecteur iv_i nécessaire pour déchiffrer le cryptogramme BD_{i*} .
- [0173] Le fait que le module 28 exécute lui-même les différentes opérations liées au chiffrement, déchiffrement et vérification des données rend transparent le procédé de sécurisation des données pour l'unité 10. En pratique, l'unité 10 fonctionne comme si toutes les données étaient en clair sans avoir à se préoccuper du chiffrement et du déchiffrement ni de la présence des métadonnées MD_i dans la mémoire chiffrée.
- [0174] Le fait que le module 28 calcule lui-même l'adresse $@_{BDC_i}$ du bloc BDC_i à partir de laquelle peut être chargée une donnée $D_{i,j}$ à accéder rend la présence des métadonnées MD_i et du code MAC_i transparente pour l'unité 10. En effet, c'est le module 28 qui réalise la conversion d'adresse et non pas l'unité 10.

Revendications

[Revendication 1]

Procédé d'exécution d'un programme d'ordinateur par un appareil électronique comportant un microprocesseur, une mémoire déchiffrée, une mémoire chiffrée et un module matériel de sécurisation, dans lequel, lors de l'exécution du programme d'ordinateur, le transfert des lignes de code entre la mémoire déchiffrée et la mémoire chiffrée se fait par bloc entier de plusieurs lignes de code chiffrées et authentifiées, ce procédé comportant les étapes suivantes:

a) l'enregistrement (410) dans la mémoire chiffrée d'un bloc de lignes de code chiffrées et authentifiées contenant une ligne de code à accéder à l'aide d'un pointeur, ce bloc de lignes de code chiffrées et authentifiées contenant :

- un cryptogramme de l'ensemble des lignes de code de ce bloc, ce cryptogramme pouvant uniquement être déchiffré dans sa totalité pour obtenir un bloc de lignes de code en clair et non pas ligne de code par ligne de code,

- un code d'authentification calculé à partir du bloc de lignes de code en clair ou à partir du cryptogramme du bloc de lignes de code en clair, et
- des métadonnées,

b) l'obtention (166), par le microprocesseur, d'un pointeur contenant l'adresse à laquelle est enregistrée la ligne de code à accéder, puis

c) le chargement (302) du bloc contenant la ligne de code à accéder depuis la mémoire chiffrée vers le microprocesseur, puis

d) la vérification (304), par le module matériel de sécurisation et à l'aide du code d'authentification contenu dans le bloc chargé, de l'intégrité :

- du bloc de lignes de codes en clair obtenu à partir du cryptogramme contenu dans le bloc chargé, ou

- du cryptogramme contenu dans le bloc chargé,

e) lorsque cette vérification échoue, l'inhibition (310) du traitement, par le microprocesseur, des lignes de code de ce bloc chargé et, lorsque cette vérification réussie :

- le déchiffrement (306) du cryptogramme contenu dans le bloc chargé pour obtenir le bloc de lignes de code en clair, et

- l'enregistrement (308) du bloc de lignes de code en clair obtenu dans la mémoire déchiffrée et l'enregistrement des métadonnées du bloc chargé, caractérisé en ce que :

- l'étape a) comporte l'incorporation (408), dans les métadonnées du bloc

contenant la ligne de code à accéder, d'un premier identifiant de pointeur associé à la ligne de code à accéder, ce premier identifiant de pointeur permettant à lui seul d'identifier de façon unique un pointeur parmi un ensemble contenant plusieurs pointeurs différents mis en œuvre lors de la même exécution du programme d'ordinateur par le microprocesseur,

- l'étape b) d'obtention (166) du pointeur comporte l'obtention d'un pointeur comprenant :

- une première plage de bits contenant l'adresse de la ligne de code à accéder, et

- une seconde plage différente de bits contenant un second identifiant de pointeur,

- après l'étape c), le procédé comporte une étape f) de vérification (176), par le module matériel de sécurisation, que le second identifiant de pointeur contenu dans le pointeur obtenu lors de l'étape b) correspond au premier identifiant de pointeur associé à la ligne de code à accéder et contenu dans les métadonnées du bloc chargé, et lorsque les premier et second identifiants de pointeur ne correspondent pas, alors le module de sécurisation déclenche (180) le signalement d'une faute d'exécution et, dans le cas contraire, le module de sécurisation inhibe (178) le déclenchement du signalement d'une faute d'exécution et le microprocesseur traite la ligne de code à accéder.

[Revendication 2] Procédé selon la revendication 1, dans lequel l'étape e) comporte l'enregistrement (308) du premier identifiant de pointeur contenu dans les métadonnées du bloc chargé dans une mémoire uniquement accessible par le module matériel de sécurisation.

[Revendication 3] Procédé selon l'une quelconque des revendications précédentes, dans lequel, avant l'étape a), le code d'authentification du bloc de lignes de code chiffrées et authentifiées à enregistrer, est aussi calculé (408) à partir des métadonnées.

[Revendication 4] Procédé selon l'une quelconque des revendications précédentes, dans lequel, avant l'étape a), le procédé comporte :

- le chiffrement (406) du bloc de lignes de code en clair en utilisant un vecteur d'initialisation et la génération (404) d'un nouveau vecteur d'initialisation avant chaque chiffrement du bloc de lignes de code en clair, et
- l'incorporation (408) dans les métadonnées du bloc de lignes de code chiffrées et authentifiées, du vecteur d'initialisation utilisé pour obtenir le cryptogramme de ce bloc de lignes de code chiffrées et authentifiées,

et

- lors du déchiffrement (306) du cryptogramme, le module matériel de sécurisation extrait des métadonnées du bloc de lignes de code chiffrées et authentifiées, le vecteur d'initialisation à utiliser pour réaliser ce déchiffrement.

[Revendication 5]

Procédé selon l'une quelconque des revendications précédentes, dans lequel, lors de l'étape a), l'adresse à laquelle est enregistrée le bloc de lignes de code chiffrées et authentifiées est reliée, par une fonction bijective, à une adresse $@_{BDCi}$ définie par la relation suivante : $@_{BDCi} = @_{BDi} \cdot T_b / T_{BD}$, où :

- $@_{BDi}$ est l'adresse où débute, dans l'espace d'adressage du programme d'ordinateur, le bloc de lignes de code en clair,
- T_b est la taille, en nombre d'octets, du bloc de lignes de code chiffrées et authentifiées,
- T_{BD} est la taille, en nombre d'octets, du bloc de lignes de code en clair.

[Revendication 6]

Procédé selon la revendication 5, dans lequel :

- après l'étape b) et avant l'étape c), le module matériel de sécurisation détermine (172) l'adresse $@_{BDCi}$ à l'aide de la première relation suivante : $@_{BDCi} = E(@_{Di,j} / T_{BD}) \cdot T_b$, où
- $E()$ est la fonction qui retourne la partie entière du nombre situé entre les parenthèses, et
- $@_{Di,j}$ est l'adresse contenue dans le pointeur obtenu à l'étape b),
- T_b et T_{BD} sont tous les deux des puissances de deux,

lors de cette détermination, la division et la multiplication de la première relation sont exécutées par des registres à décalage du module matériel de sécurisation, puis

- lors de l'étape c), le bloc contenant la ligne de code à accéder est chargé, depuis la mémoire chiffrée, à partir de l'adresse reliée, par la fonction bijective, à l'adresse $@_{BDCi}$ déterminée.

[Revendication 7]

Procédé selon la revendication 5, dans lequel :

- après l'étape b) et avant l'étape c), le module matériel de sécurisation détermine l'adresse $@_{BDCi}$ à l'aide de la seconde relation suivante : $@_{BDCi} = E(@_{Di,j} / T_{BD}) \cdot T_{BD} + E(@_{Di,j} / T_{BD}) \cdot (T_b - T_{BD})$, où
 - $E()$ est la fonction qui retourne la partie entière du nombre situé entre les parenthèses, et
 - $@_{Di,j}$ est l'adresse contenue dans le pointeur obtenu à l'étape b),
 - $(T_b - T_{BD})$ et T_{BD} sont tous les deux des puissances de deux,
- lors de cette détermination, chaque division et chaque multiplication de la seconde relation sont exécutées par des registres à décalage du

module matériel de sécurisation, et

- lors de l'étape c), le bloc contenant la ligne de code à accéder est chargé, depuis la mémoire chiffrée, à partir de l'adresse reliée, par la fonction bijective, à l'adresse $@_{BDCi}$ déterminée.

[Revendication 8]

Programme d'ordinateur apte à être exécuté par un microprocesseur en mettant en œuvre un procédé conforme à l'une quelconque des revendications précédentes, dans lequel le code binaire du programme d'ordinateur comporte :

- un bloc de lignes de code chiffrées et authentifiées contenant une ligne de code à accéder à l'aide d'un pointeur respectif, ce bloc de lignes de code chiffrées et authentifiées contenant :

- un cryptogramme (BD_i^*) de l'ensemble des lignes de code de ce bloc, ce cryptogramme pouvant uniquement être déchiffré dans sa totalité pour obtenir un bloc de lignes de code en clair et non pas ligne de code par ligne de code,

- un code d'authentification (MAC_i) calculé à partir du bloc de lignes de code en clair ou à partir du cryptogramme du bloc de lignes de code en clair, et

-des métadonnées (MD_i),

- un pointeur contenant l'adresse à laquelle est enregistrée la ligne de code à accéder

caractérisé en ce que:

- les métadonnées (MD_i) comporte un premier identifiant de pointeur associé à la ligne de code à accéder, ce premier identifiant de pointeur permettant à lui seul d'identifier de façon unique un pointeur parmi un ensemble contenant plusieurs pointeurs différents mis en œuvre lors de la même exécution du programme d'ordinateur par le microprocesseur, et

- le pointeur comprend :

- une première plage de bits contenant l'adresse de la ligne de code à accéder, et

- une seconde plage différente de bits contenant un second identifiant de pointeur, ce second identifiant de pointeur étant égal au premier identifiant de pointeur.

[Revendication 9]

Module matériel (28) de sécurisation pour la mise en œuvre d'un procédé conforme à l'une quelconque des revendications 1 à 7, dans lequel le module matériel est configuré pour :

a) déclencher l'enregistrement dans la mémoire chiffrée d'un bloc de

lignes de code chiffrées et authentifiées contenant une ligne de code à accéder à l'aide d'un pointeur, ce bloc de lignes de code chiffrées et authentifiées contenant :

- un cryptogramme de l'ensemble des lignes de code de ce bloc, ce cryptogramme pouvant uniquement être déchiffré dans sa totalité pour obtenir un bloc de lignes de code en clair et non pas ligne de code par ligne de code,

- un code d'authentification calculé à partir du bloc de lignes de code en clair ou à partir du cryptogramme du bloc de lignes de code en clair, et
- des métadonnées,

b) recevoir un pointeur contenant l'adresse à laquelle est enregistrée la ligne de code à accéder, puis

c) déclencher le chargement du bloc contenant la ligne de code à accéder depuis la mémoire chiffrée vers le microprocesseur, puis

d) vérifier, à l'aide du code d'authentification contenu dans le bloc chargé, l'intégrité :

- du bloc de lignes de codes en clair obtenu à partir du cryptogramme contenu dans le bloc chargé, ou

- du cryptogramme contenu dans le bloc chargé,

e) lorsque cette vérification échoue, inhiber le traitement, par le microprocesseur, des lignes de code de ce bloc chargé et, lorsque cette vérification réussie :

- déchiffrer le cryptogramme contenu dans le bloc chargé pour obtenir le bloc de lignes de code en clair, et

- déclencher l'enregistrement du bloc de lignes de code en clair obtenu dans la mémoire déchiffrée et l'enregistrement des métadonnées du bloc chargé,

caractérisé en ce que le module de sécurisation est également configuré :

- pour incorporer, dans les métadonnées du bloc contenant la ligne de code à accéder, un premier identifiant de pointeur associé à la ligne de code à accéder, ce premier identifiant de pointeur permettant à lui seul d'identifier de façon unique un pointeur parmi un ensemble contenant plusieurs pointeurs différents mis en œuvre lors de la même exécution du programme d'ordinateur par le microprocesseur,

- en réponse à l'exécution d'une instruction d'accès à la ligne de code à accéder à l'aide d'un pointeur, pour extraire un second identifiant de pointeur dans une plage de bits de ce pointeur, puis

- pour vérifier que le second identifiant de pointeur correspond au

premier identifiant de pointeur associé à la ligne de code à accéder et contenu dans les métadonnées du bloc chargé, et si les premier et second identifiants de pointeur ne correspondent pas, alors déclencher le signalement d'une faute d'exécution et, dans le cas contraire, inhiber le déclenchement du signalement d'une faute d'exécution et autoriser le microprocesseur à traiter la ligne de code à accéder.

[Fig. 1]

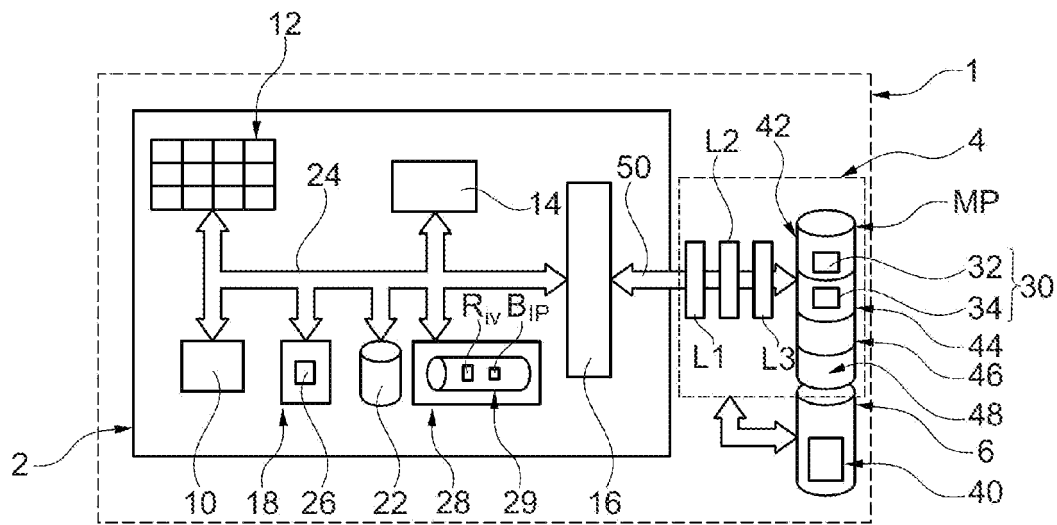


Fig. 1

[Fig. 2]

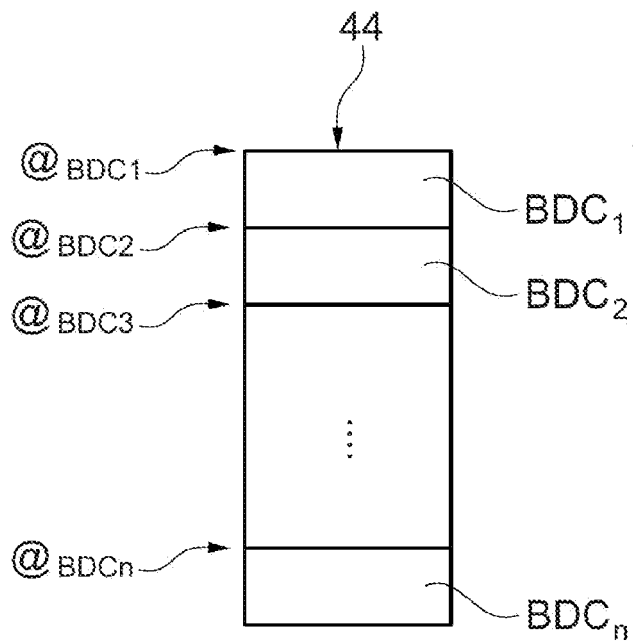


Fig. 2

[Fig. 3]

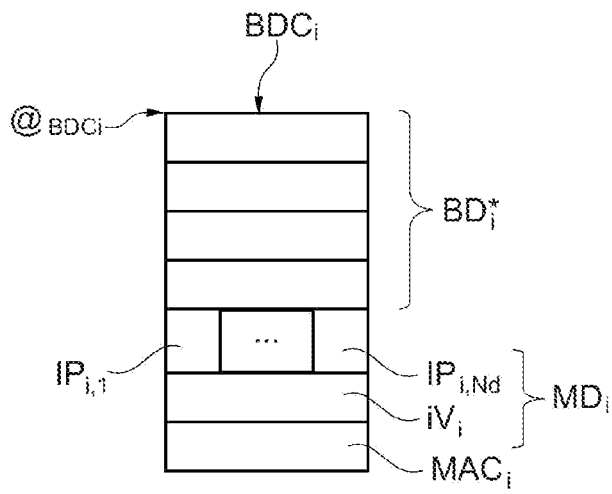


Fig. 3

[Fig. 4]

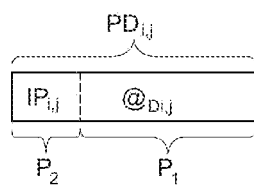


Fig. 4

[Fig. 5]

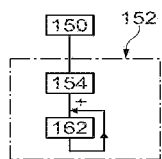


Fig. 5

[Fig. 6]

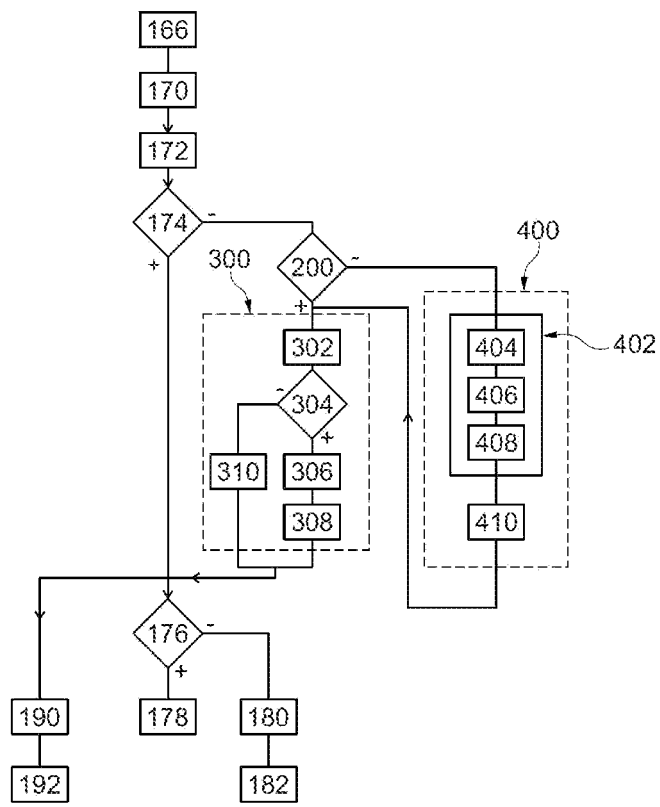


Fig. 6

[Fig. 7]

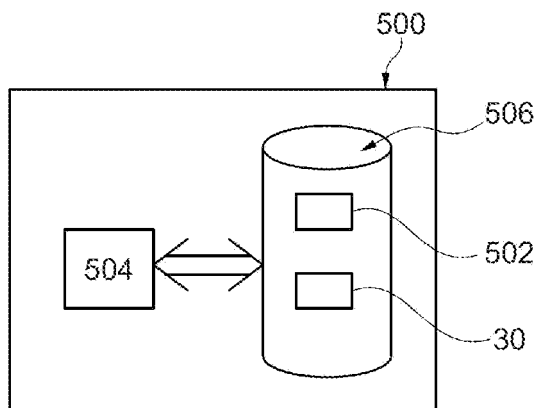


Fig. 7

RAPPORT DE RECHERCHE

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

OBJET DU RAPPORT DE RECHERCHE

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

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

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

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

☒ Le demandeur a maintenu les revendications.

☐ Le demandeur a modifié les revendications.

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

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

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

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

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

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

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

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

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

NEANT

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

CLERCQ RUAN DE ET AL: "SOFIA: Software and control flow integrity architecture", 2016 DESIGN, AUTOMATION & TEST IN EUROPE CONFERENCE & EXHIBITION (DATE), EDAA, 14 mars 2016 (2016-03-14), pages 1172-1177, XP032895110, [extrait le 2016-04-25]

EP 3 761 199 A1 (COMMISSARIAT ENERGIE ATOMIQUE [FR]) 6 janvier 2021 (2021-01-06)

US 2019/087566 A1 (HOSIE SIMON [US]) 21 mars 2019 (2019-03-21)

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

NEANT