

①2

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 15.12.15.

③0 Priorité :

④3 Date de mise à la disposition du public de la
demande : 16.06.17 Bulletin 17/24.

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

⑥0 Références à d'autres documents nationaux
apparentés :

○ Demande(s) d'extension :

⑦1 Demandeur(s) : **OBERTHUR TECHNOLOGIES**
Société anonyme — FR.

⑦2 Inventeur(s) : **BARBU GUILLAUME** et **ANDOUARD
PHILIPPE.**

⑦3 Titulaire(s) : **OBERTHUR TECHNOLOGIES** Société
anonyme.

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

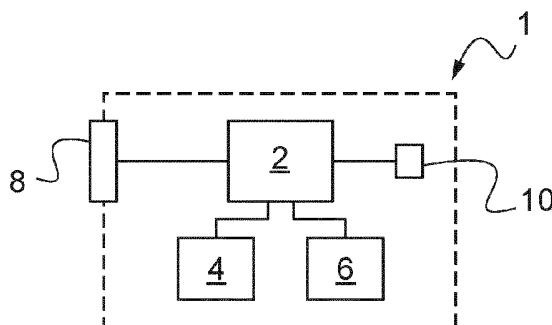
⑤4 **PROCEDE D'ECRITURE DANS UNE MEMOIRE NON-VOLATILE D'UNE ENTITE ELECTRONIQUE ET ENTITE
ELECTRONIQUE ASSOCIEE.**

⑤7 Un procédé d'écriture dans une mémoire non-volatile
(6) d'une entité électronique (1) comprend les étapes
suivantes :

- détermination d'un état de fonctionnement de l'entité
électronique (1);
- en cas de fonctionnement anormal, écriture d'une pre-
mière donnée dans une première zone de la mémoire non-
volatile (6);
- en cas de fonctionnement normal, écriture d'une se-
conde donnée dans une seconde zone de la mémoire non-
volatile (6).

Le procédé comprend une étape de détermination aléa-
toire d'un emplacement de la seconde zone parmi une plu-
ralité d'emplacements de la seconde zone, ladite écriture de
la donnée dans la seconde zone étant réalisée à l'emplace-
ment déterminé.

Une entité électronique associée est également propo-
sée.



DOMAINE TECHNIQUE AUQUEL SE RAPPORTE L'INVENTION

5 La présente invention concerne la protection des entités électroniques contre les attaques.

Elle concerne plus particulièrement un procédé d'écriture dans une mémoire non-volatile d'une entité électronique et une entité électronique associée.

10 L'invention s'applique particulièrement avantageusement dans le cas où il est prévu d'écrire une donnée représentative d'un type d'erreur dans la mémoire non-volatile lorsqu'une anomalie de fonctionnement est détectée.

ARRIERE-PLAN TECHNOLOGIQUE

On connaît du document EP 2 164 031 un procédé d'écriture dans une mémoire non-volatile d'une entité électronique comprenant les étapes suivantes :

- 15 - détermination d'un état de fonctionnement de l'entité électronique ;
- en cas de fonctionnement anormal, écriture d'une première donnée dans une première zone de la mémoire non-volatile ;
- en cas de fonctionnement normal, écriture d'une seconde donnée dans une seconde zone de la mémoire non-volatile.

20 L'écriture de la première donnée dans la première zone de la mémoire non-volatile permet de garder trace de la détection du fonctionnement anormal et éventuellement de conduire à un blocage du fonctionnement de l'entité électronique, par exemple lorsqu'un nombre prédéterminé d'anomalies de fonctionnement ont été détectées au cours des phases successives de
25 fonctionnement de l'entité électronique.

L'écriture de la seconde donnée dans la seconde zone de la mémoire non-volatile vise à simuler l'écriture susmentionnée dans la première zone, de sorte qu'un attaquant ne puisse pas distinguer les cas de détection d'anomalie des cas de fonctionnement normal. L'attaquant cherche en effet à déceler une telle
30 détection d'anomalie par l'entité électronique afin d'empêcher l'écriture de la première donnée et d'éviter ainsi un blocage de l'entité électronique.

Dans cette logique, le document EP 2 164 031 enseigne que l'écriture dans la première zone et l'écriture dans la seconde zone doivent avoir une signature identique quant à leur consommation électrique.

OBJET DE L'INVENTION

Dans ce contexte, la présente invention propose un procédé d'écriture tel que défini ci-dessus, caractérisé par une étape de détermination aléatoire d'un emplacement de la seconde zone parmi une pluralité d'emplacements de la
5 seconde zone, ladite écriture de la donnée dans la seconde zone étant réalisée à l'emplacement déterminé.

Les inventeurs ont en effet constaté que l'écriture dans la première zone et l'écriture dans la seconde zone pouvaient produire des signaux (électriques ou électromagnétiques) observables différents, en particulier lorsque les routines bas-
10 niveau d'écriture en mémoire non-volatile sont conçues sans tenir compte du souhait de produire des signaux observables constants.

On propose donc ici de provoquer une écriture à un emplacement à chaque fois différent (dans la seconde zone) lors du fonctionnement normal.

Ainsi, la différence observable entre écriture dans la première zone et
15 écriture dans la seconde zone sera du même ordre que les différences observables entre écritures successives dans la seconde zone (à des emplacements à chaque fois différents) lors du fonctionnement normal de sorte qu'un attaquant ne pourra pas détecter l'écriture dans la première zone (dans le but d'interrompre cette écriture).

20 Un tel procédé d'écriture fait par exemple partie d'un procédé de traitement de données comprenant les étapes suivantes :

- réception d'une donnée par une interface de communication ;
- traitement de la donnée reçue.

Selon d'autres caractéristiques optionnelles (et donc non limitatives) :

- 25
- le traitement est un traitement cryptographique et/ou utilise une clé cryptographique mémorisée dans la mémoire non-volatile ;
 - l'étape de détermination de l'état de fonctionnement comprend une vérification d'un résultat obtenu par ledit traitement ;
 - l'étape de détermination de l'état de fonctionnement utilise un détecteur
30 d'attaque ;
 - la taille de la seconde zone est supérieure ou égale à la taille de la première zone ;
 - la taille de la première zone est égale à la taille seconde zone ;
 - la première donnée est représentative d'un type d'erreur.

L'invention propose également une entité électronique comprenant une mémoire non-volatile, un module de détermination d'un état de fonctionnement de l'entité électronique, et un module d'écriture en mémoire non-volatile conçu pour écrire une première donnée dans une première zone de la mémoire volatile en cas
5 de fonctionnement anormal et pour écrire une seconde donnée dans une seconde zone de la mémoire volatile en cas de fonctionnement normal, caractérisé en ce que le module d'écriture en mémoire non-volatile est conçu pour déterminer aléatoirement un emplacement de la seconde zone parmi une pluralité d'emplacements de la seconde zone et pour écrire la seconde donnée dans la
10 seconde zone à l'emplacement déterminé.

Une telle entité électronique comprend par exemple un module de lecture en mémoire non-volatile conçu pour lire des données dans la première zone et un mécanisme de blocage apte à bloquer sélectivement le fonctionnement de l'entité électronique en fonction des données lues.

15 Lorsque l'entité électronique comprend un processeur (par exemple un microprocesseur), les modules et le mécanisme susmentionnés peuvent être mis en œuvre par des composants électroniques et/ou du fait de l'exécution, par le processeur, d'instructions de programme d'ordinateur mémorisées dans une mémoire (par exemple la mémoire non-volatile précitée) de l'entité électronique.

20 Par ailleurs, les caractéristiques optionnelles présentées ci-dessus en termes de procédé peuvent éventuellement s'appliquer à une telle entité électronique.

DESCRIPTION DETAILLEE D'UN EXEMPLE DE REALISATION

La description qui va suivre en regard des dessins annexés, donnés à
25 titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

Sur les dessins annexés :

- la figure 1 représente schématiquement les éléments principaux d'une entité électronique au sein de laquelle est mise en œuvre l'invention ; et
- 30 - la figure 2 est un logigramme présentant des étapes d'un procédé mis en œuvre au sein de l'entité électronique de la figure 1.

La figure 1 représente schématiquement les éléments principaux d'une entité électronique 1 au sein de laquelle est mise en œuvre l'invention.

Cette entité électronique est par exemple une carte à microcircuit, telle

qu'une carte à circuit intégré universelle (ou UICC pour "*Universal Integrated Circuit Card*"). En variante, il pourrait s'agir d'un élément sécurisé (ou SE pour "*Secure Element*") – par exemple un microcontrôleur sécurisé, d'un dispositif électronique portatif (ou "*hand-held electronic device*" selon l'appellation anglo-saxonne) – par exemple un terminal de communication ou un passeport électronique, ou d'un ordinateur.

L'entité électronique 1 comprend un microprocesseur 2, une mémoire vive 4 et une mémoire non-volatile 6. L'entité électronique 1 pourrait éventuellement comprendre en outre une mémoire morte.

10 La mémoire non-volatile 6 est par exemple une mémoire non-volatile réinscriptible (par exemple de type EEPROM pour "*Electrically Erasable and Programmable Read-Only Memory*", ou de type Flash), ou une mémoire non-volatile inscriptible une fois (par exemple de type OTP pour "*One-Time Programmable*").

15 La mémoire vive 4 et la mémoire non-volatile 6 (ainsi que le cas échéant la mémoire morte) sont chacune liées au microprocesseur 2 de sorte que le microprocesseur 2 peut lire ou écrire des données dans chacune de ces mémoires.

Une de ces mémoires, par exemple la mémoire non-volatile 6, mémorise
20 des instructions de programme d'ordinateur qui permettent la mise en œuvre au sein de l'entité électronique 1, d'un procédé (tel que par exemple le procédé décrit ci-dessous en référence à la figure 2) lorsque ces instructions sont exécutées par le microprocesseur 2. Dans l'exemple décrit ici, ces instructions comprennent notamment des instructions d'un programme principal (qui correspond aux étapes
25 E2 à 20 et E30 de la figure 2) et des instructions d'un sous-programme (qui correspond aux étapes E22 à E28 de la figure 2).

Les mémoires 4, 6 mémorisent également des données représentatives de variables utilisées lors de la mise en œuvre de divers procédés de traitement de données, notamment le procédé décrit ci-dessous en référence à la figure 2.

30 La mémoire non-volatile 6 comprend en outre une zone d'écriture sécuritaire Z0 et une zone d'écriture systématique Z1 utilisées comme décrit plus bas. Dans le mode de réalisation décrit ici, la zone d'écriture sécuritaire Z0 et la zone d'écriture systématique Z1 ont une taille identique, par exemple comprise entre 2 octets et une valeur prédéterminée dépendant de la politique de sécurité.

La zone d'écriture sécuritaire Z0 et la zone d'écriture systématique Z1 pourraient toutefois avoir en variante des tailles respectives distinctes l'une de l'autre. Dans un cas particulier, la zone d'écriture sécuritaire Z0 pourrait être limitée à 1 octet. La zone d'écriture systématique Z1 comprend quant à elle au moins 2 octets (soit au moins deux emplacements). On note L la longueur (en octets) de la zone d'écriture systématique Z1.

Lors du démarrage du fonctionnement de l'entité électronique 1 (par exemple consécutivement à sa mise sous tension), le microprocesseur 2 lit les données mémorisées dans la zone d'écriture sécuritaire Z0 et peut sélectivement, selon les données lues, bloquer son fonctionnement ou poursuivre son fonctionnement, par exemple en mettant en œuvre le procédé décrit ci-dessous en référence à la figure 2.

Le blocage du fonctionnement de l'entité électronique 1 est par exemple réalisé lorsque le microprocesseur 2 lit dans la zone d'écriture sécuritaire Z0 un octet ayant une valeur prédéterminée (dite "*donnée de blocage*" ou "*verrou*"). En variante, le blocage du fonctionnement de l'entité électronique 1 peut être réalisé lorsque le microprocesseur 2 lit dans la zone d'écriture sécuritaire Z0 un nombre prédéterminé de données (par exemple d'octets) correspondant chacune à un code d'erreur (mémorisé lors de phases antérieures de fonctionnement de l'entité électronique 1 comme décrit ci-dessous dans le cadre du procédé présenté en référence à la figure 2). On prévoit par exemple dans ce dernier cas qu'à chaque démarrage du fonctionnement de l'entité électronique 1, le microprocesseur 2 lise les octets mémorisés dans la zone d'écriture sécuritaire Z0 de manière à déterminer le nombre n de ces octets qui correspondent à un code d'erreur : le nombre n est mémorisé en mémoire vive 4 (voir son utilisation à l'étape E24 décrite plus bas) et le microprocesseur 2 provoque le blocage du fonctionnement de l'entité électronique 1 lorsque ce nombre n atteint (ou dépasse) un seuil prédéterminé.

Dans certains cas, le blocage du fonctionnement de l'entité électronique 1 peut être accompagné d'autres mesures de protection, par exemple l'effacement de certaines données au moins mémorisées dans la mémoire non-volatile 6.

L'entité électronique 1 comprend en outre une interface de communication 8 avec des dispositifs électroniques externes. Dans le cas décrit ici où l'entité électronique 1 est une carte à microcircuit, l'interface de communication

8 comprend par exemple des contacts affleurant sur une face de la carte à microcircuit. En variante, l'interface de communication 8 pourrait être réalisée par un module de communication sans contact. De manière générale, l'interface de communication 8 peut être un module de communication (filaire ou sans fil) avec
5 une autre entité électronique.

Le microprocesseur 2 peut ainsi recevoir des données d en provenance de l'autre entité électronique via l'interface de communication 8, traiter ces données d au moyen d'un algorithme de traitement (par exemple un algorithme cryptographique) afin d'obtenir un résultat r, et émettre ce résultat r à destination
10 de l'autre entité électronique via l'interface de communication 8.

L'entité électronique 1 comprend également un détecteur d'attaque 10 ; un tel détecteur d'attaque 10 est par exemple un capteur de lumière ou, en variante, un détecteur de perturbation dans l'alimentation électrique. De manière générale, il s'agit d'un composant matériel conçu pour détecter des attaques au
15 cours desquels un attaquant cherche à provoquer une anomalie de fonctionnement de l'entité électronique, par exemple en dirigeant un rayonnement laser sur l'entité électronique 1 (attaque détectable au moyen du capteur de lumière précité) ou en perturbant l'alimentation électrique des composants au sein de l'entité électronique 1.

20 La figure 2 représente, sous forme de logigramme, un exemple de procédé conforme à l'invention.

Ce procédé débute à l'étape E2 à laquelle le microprocesseur 2 reçoit des données d via l'interface de communication 8.

Le microprocesseur 2 procède alors à l'étape E4 au traitement des
25 données reçues d. Un tel traitement est par exemple l'application aux données d d'un algorithme cryptographique utilisant une clé cryptographique mémorisée dans la mémoire non-volatile 6.

On désigne par r les données obtenues par le traitement de l'étape E4 :
 $r = F(d)$, où F est la fonction mise en œuvre par le traitement de l'étape
30 E4.

On prévoit ici en outre de réitérer à l'étape E6 le traitement effectué à l'étape E4 pour s'assurer que ce traitement a été réalisé sans anomalie.

Autrement dit, le microprocesseur effectue à l'étape E6 un traitement identique à celui effectué à l'étape E4 (ici l'application aux données d de

l'algorithme cryptographique susmentionné utilisant la clé cryptographique précitée).

On désigne par r' les données obtenues par le traitement de l'étape E6 :

$$r' = F(d).$$

- 5 En fonctionnement normal, les données r et les données r' sont identiques ; ce n'est pas le cas en revanche si une anomalie s'est produite au cours de l'étape E4 ou de l'étape E6 (anomalie qui peut être générée par une attaque par faute).

- 10 On teste ainsi à l'étape E8 si les données r et les données r' sont identiques.

- 15 On remarque qu'en variante, la réitération du traitement de l'étape E4 (étape E6) pourrait être remplacée par l'application aux données r du traitement inverse de celui effectué à l'étape E4 ; les données d' ainsi obtenues ($d' = F^{-1}(r)$) sont dans ce cas comparées aux données d (en remplacement du test de l'étape E8) pour vérification du fonctionnement normal.

S'il est déterminé à l'étape E8 que les données r et les données r' sont identiques (flèche P), le microprocesseur 2 met (étape E10) une variable i à la valeur 1 et une variable v à une valeur quelconque (notée XXX en figure 2), par exemple une valeur prédéfinie.

- 20 Le procédé se poursuit ensuite à l'étape E14 décrite plus bas.

- 25 S'il est déterminée à l'étape E8 que les données r et les données r' ne sont pas identiques (ce qui est le cas si une anomalie s'est produit au cours de l'étape E4 ou de l'étape E6), le microprocesseur 2 met (étape E12) une variable i à la valeur 0 et une variable v à une valeur prédéterminée ERR1 représentative d'un premier type d'erreur.

Le procédé se poursuit à l'étape E14 à laquelle le microprocesseur 2 détermine si une attaque a été détectée par le détecteur d'attaque 10.

- 30 Dans l'affirmative (flèche P), le microprocesseur 2 met (étape E18) une variable i à la valeur 0 et une variable v à une valeur prédéterminée ERR2 représentative d'un second type d'erreur. Le procédé se poursuit ensuite à l'étape E20 décrite plus bas.

Dans la négative (flèche N), le microprocesseur 2 mémorise dans la variable i la valeur précédemment stockée dans cette variable i et met une variable v à une valeur quelconque, par exemple prédéfinie (étape E16).

On remarque que la mémorisation dans la variable i de la valeur précédemment stockée dans cette même variable est au final sans effet sur le contenu de la variable i ; cette opération rend toutefois difficile pour un attaquant de distinguer, par des observations extérieures du fonctionnement de l'entité électronique 1, le cas où une attaque a été détectée du cas de fonctionnement normal.

Le procédé se poursuit également dans ce cas par l'étape E20.

Le microprocesseur 2 lance à l'étape E20 un processus d'écriture de la valeur contenue dans la variable v soit dans la zone d'écriture systématique $Z1$, soit dans la zone d'écriture sécuritaire $Z0$.

Dans l'exemple décrit ici, ce processus est mis en œuvre du fait de l'exécution d'un sous-programme représenté aux étapes E22 à E28. Les valeurs respectives de la variable i et de la variable v sont passées en paramètres lors de l'appel de ce sous-programme, comme schématiquement représenté en figure 2.

Du fait de l'exécution de ce sous-programme, le microprocesseur 2 génère à l'étape E22 un nombre aléatoire a compris entre 0 et $L-1$, où L est comme déjà indiqué la longueur (en octets) de la zone d'écriture systématique $Z1$. En variante, le microprocesseur 2 peut recevoir un tel nombre aléatoire a en provenance d'un crypto-processeur équipant l'entité électronique 1.

Le microprocesseur 2 mémorise ensuite (étape E24), dans une première cellule $ADR[0]$ d'un tableau ADR (mémorisé par exemple en mémoire vive 4), une valeur $z0+n$ désignant une adresse au sein de la zone d'écriture sécuritaire $Z0$ (ou, autrement dit, l'adresse d'un emplacement de la zone d'écriture sécuritaire $Z0$), où on note $z0$ l'adresse (du premier emplacement) de la zone d'écriture sécuritaire $Z0$ et n le nombre d'octets déjà inscrits dans la zone sécuritaire lors de phases antérieures de fonctionnement de l'entité électronique 1 (le nombre n étant par exemple déterminé au démarrage du fonctionnement de l'entité électronique 1 et mémorisé en mémoire vive 4 comme indiqué plus haut).

Le microprocesseur 2 mémorise également (étape E26), dans une seconde cellule $ADR[1]$ du tableau ADR , une valeur $z1+a$ désignant une adresse choisie aléatoirement au sein de la zone d'écriture systématique $Z1$ (ou, autrement dit, l'adresse d'un emplacement choisi de manière aléatoire parmi les L emplacements de la zone d'écriture systématique $Z1$), où on note $z1$ l'adresse (du premier emplacement) de la zone d'écriture systématique $Z1$.

Le microprocesseur 2 commande alors à l'étape E28 l'écriture de la valeur v dans la mémoire non-volatile 6 à l'adresse désignée par la valeur mémorisée dans la cellule $ADR[i]$: la valeur v est inscrite dans la mémoire non-volatile 6 à l'adresse mémorisée dans la première cellule $ADR[0]$ du tableau ADR si la variable i vaut 0, ou bien à l'adresse mémorisée dans la seconde cellule $ADR[1]$ du tableau ADR si la variable i vaut 1. On peut prévoir par ailleurs que, lorsque la variable i vaut 0, le microprocesseur 2 incrémente le nombre n mentionné plus haut (mémorisé en mémoire vive 4).

Ainsi, s'il a été déterminé au cours des étapes E8 et E14 qu'un risque d'attaque était présent (auquel cas la variable i a été mise à 0 à l'étape E12 ou à l'étape E18), l'étape E28 provoque l'écriture d'une valeur représentative d'un type d'erreur dans la zone d'écriture sécuritaire $Z0$.

Dans les autres cas (c'est-à-dire en fonctionnement normal), l'étape E28 provoque l'écriture d'une valeur quelconque dans la zone d'écriture systématique $Z1$, à un emplacement déterminé à chaque fois de manière aléatoire parmi les différents emplacements de la zone d'écriture systématique $Z1$.

Ainsi, les signaux électriques et/ou électromagnétiques générés lors de cette écriture et observables par un attaquant varient d'une écriture à l'autre dans la zone d'écriture systématique $Z1$.

La mise en œuvre d'une écriture dans la zone d'écriture sécuritaire $Z0$ provoquerait une variation des signaux observables du même ordre et ne pourrait donc pas être distinguée des écritures en zone d'écriture systématique $Z1$ par un attaquant, qui ne pourrait ainsi pas interrompre (par exemple en coupant l'alimentation électrique de l'entité électronique 1) l'écriture en zone d'écriture sécuritaire $Z0$.

Les valeurs représentatives d'un type d'erreur (pouvant conduire au blocage de l'entité électronique 1) sont ainsi correctement inscrites dans la zone d'écriture sécuritaire $Z0$.

Une fois l'écriture en mémoire non-volatile effectuée à l'étape E28, le processus lancé à l'étape E20 est terminé et le procédé se poursuit (ici par retour au programme principal) à l'étape E30, à laquelle l'entité électronique 1 émet par exemple le résultat r obtenu à l'étape E4 via l'interface de communication 8.

REVENDECATIONS

1. Procédé d'écriture dans une mémoire non-volatile (6) d'une entité électronique (1) comprenant les étapes suivantes :

- 5 - détermination (E8 ; E14) d'un état de fonctionnement de l'entité électronique (1) ;
- en cas de fonctionnement anormal, écriture (E12, E18, E24, E28) d'une première donnée (ERR1 ; ERR2) dans une première zone de la mémoire non-volatile (6) ;
- 10 - en cas de fonctionnement normal, écriture (E10, E16, E26, E28) d'une seconde donnée dans une seconde zone de la mémoire non-volatile (6),
- caractérisé par une étape de détermination aléatoire (E22, E26) d'un emplacement de la seconde zone parmi une pluralité d'emplacements de la seconde zone, ladite écriture (E10, E16, E26, E28) de la donnée dans la seconde
- 15 zone étant réalisée à l'emplacement déterminé.

2. Procédé d'écriture selon la revendication 1, comprenant les étapes suivantes :

- réception (E2) d'une donnée (d) par une interface de communication
- 20 (8) ;
- traitement (E4) de la donnée (d) reçue.

3. Procédé d'écriture selon la revendication 2, dans lequel le traitement (E4) est un traitement cryptographique.

25

4. Procédé d'écriture selon la revendication 2 ou 3, dans lequel le traitement (E4) utilise une clé cryptographique mémorisée dans la mémoire non-volatile (6).

30 5. Procédé d'écriture selon l'une des revendications 2 à 4, dans lequel l'étape de détermination de l'état de fonctionnement comprend une vérification (E8) d'un résultat (r) obtenu par ledit traitement (E4).

6. Procédé d'écriture selon l'une des revendications 1 à 5, dans lequel

l'étape de détermination de l'état de fonctionnement utilise un détecteur d'attaque (10).

5 7. Procédé d'écriture selon l'une des revendications 1 à 6, dans lequel la taille de la seconde zone est supérieure ou égale à la taille de la première zone.

8. Procédé d'écriture selon l'une des revendications 1 à 7, dans lequel la première donnée (ERR1 ; ERR2) est représentative d'un type d'erreur.

10 9. Entité électronique (1) comprenant :
- une mémoire non-volatile (6) ;
- un module de détermination d'un état de fonctionnement de l'entité électronique ; et
- un module d'écriture en mémoire non-volatile conçu pour écrire une
15 première donnée (ERR1 ; ERR2) dans une première zone de la mémoire volatile (5) en cas de fonctionnement anormal et pour écrire une seconde donnée dans une seconde zone de la mémoire volatile (6) en cas de fonctionnement normal,
caractérisé en ce que le module d'écriture en mémoire non-volatile est
conçu pour déterminer aléatoirement un emplacement de la seconde zone parmi
20 une pluralité d'emplacements de la seconde zone et pour écrire la seconde donnée dans la seconde zone à l'emplacement déterminé.

10. Entité électronique selon la revendication 9, comprenant un module de lecture en mémoire non-volatile conçu pour lire des données dans la première
25 zone et un mécanisme de blocage apte à bloquer sélectivement le fonctionnement de l'entité électronique (1) en fonction des données lues.

1/1

Fig.1

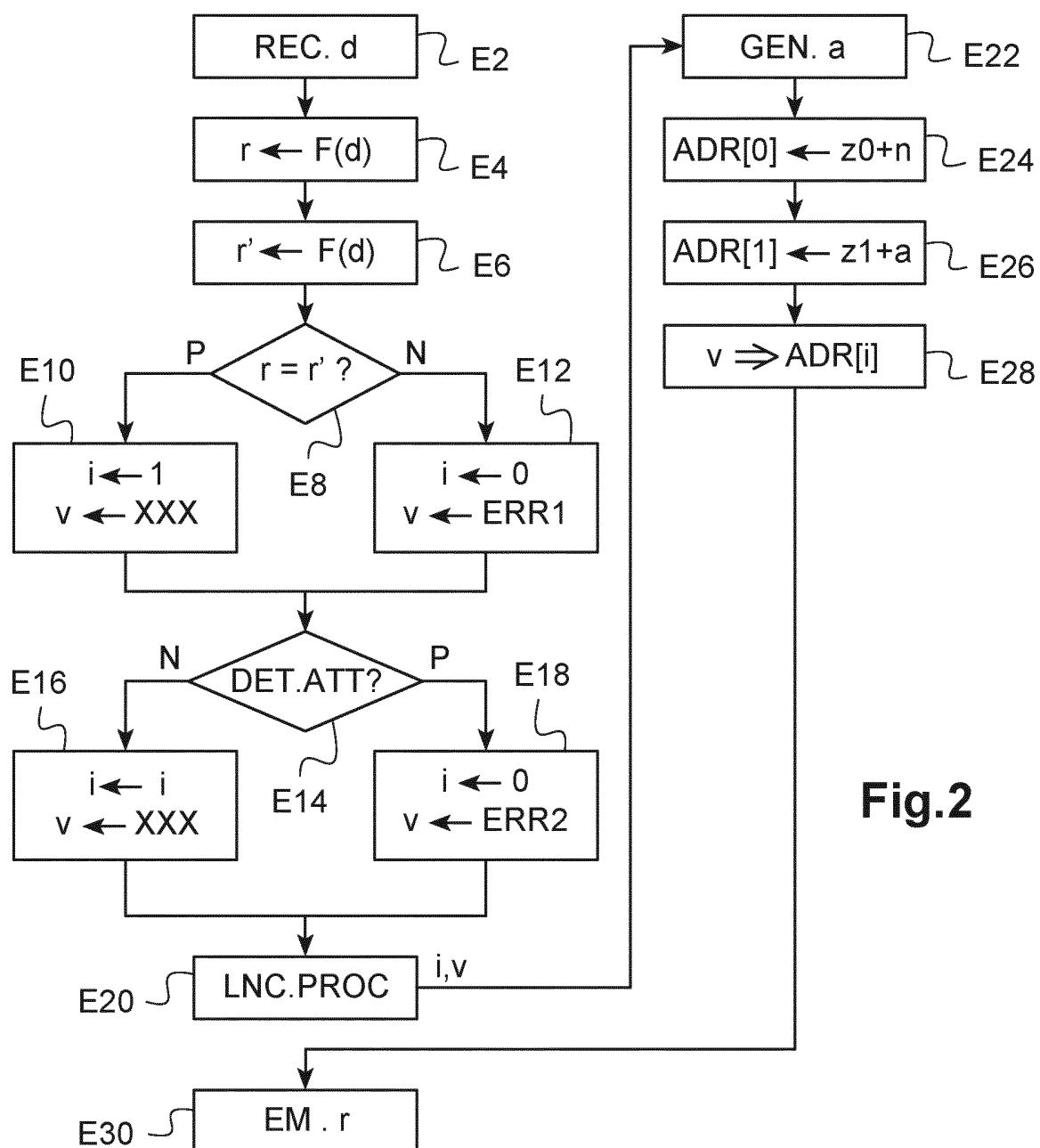
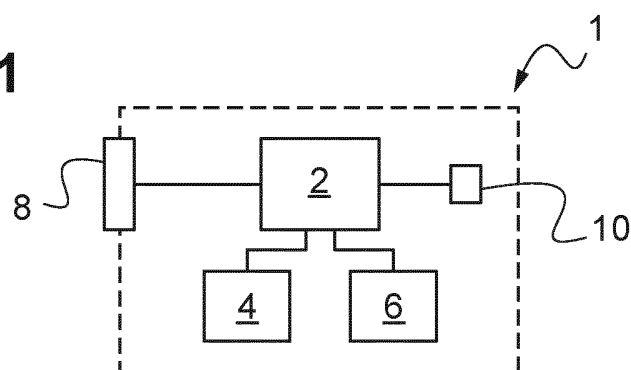


Fig.2



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 822306
FR 1562376

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	EP 2 164 031 A1 (OBERTHUR TECHNOLOGIES [FR]) 17 mars 2010 (2010-03-17)	1-4,6-10	G06F12/14 G06K19/073 G11C7/24
Y	* figures 1, 2 * * alinéas [0001], [0002], [0014], [0015], [0047], [0051], [0052], [0058] *	5	
A	US 2012/331309 A1 (SCOTT JEFFREY W [US] ET AL) 27 décembre 2012 (2012-12-27) * alinéas [0003], [0004], [0014], [0015] * * figure 3 *	1-10	
A	US 2009/113217 A1 (DOLGUNOV BORIS [IL] ET AL) 30 avril 2009 (2009-04-30) * abrégé * * alinéas [0002], [0007] * * figure 1 *	1-10	
A	US 2013/145177 A1 (CORDELLA THOMAS [US] ET AL) 6 juin 2013 (2013-06-06) * alinéa [0042] - alinéa [0045] * * figure 11 *	1-10	
A	US 2011/145595 A1 (KIM JU HAN [KR] ET AL) 16 juin 2011 (2011-06-16) * figure 2 * * alinéas [0005], [0013] *	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06F G06K
----- -/--			
Date d'achèvement de la recherche		Examineur	
12 juillet 2016		Freitas, Arthur	
CATÉGORIE DES DOCUMENTS CITÉS X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant			



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 822306
FR 1562376

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	VEYRAT-CHARVILLON NICOLAS ET AL: "Shuffling against Side-Channel Attacks: A Comprehensive Study with Cautionary Note", 2 décembre 2012 (2012-12-02), CORRECT SYSTEM DESIGN; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 740 - 757, XP047328912, ISSN: 0302-9743 ISBN: 978-3-540-72913-6 * page 1, ligne 1 - ligne 21 *	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC)
Y	EP 2 180 631 A1 (GEMALTO SA [FR]) 28 avril 2010 (2010-04-28)	5	
A	* alinéa [0020] - alinéa [0024] * * figure 1 *	1-4,6-10	
A	US 2011/128030 A1 (WUIDART SYLVIE [FR]) 2 juin 2011 (2011-06-02) * alinéa [0048] * * figure 1 *	1-10	
Date d'achèvement de la recherche		Examineur	
12 juillet 2016		Freitas, Arthur	
CATÉGORIE DES DOCUMENTS CITÉS			
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire		T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE**RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1562376 FA 822306**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **12-07-2016**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 2164031	A1	17-03-2010	DK	2164031 T3	22-10-2012
			EP	2164031 A1	17-03-2010
			ES	2390638 T3	14-11-2012
			FR	2935823 A1	12-03-2010
			JP	5517535 B2	11-06-2014
			JP	2010068523 A	25-03-2010
			US	2010064370 A1	11-03-2010

US 2012331309	A1	27-12-2012	AUCUN		

US 2009113217	A1	30-04-2009	US	2009113217 A1	30-04-2009
			US	2012317423 A1	13-12-2012
			WO	2009057094 A1	07-05-2009

US 2013145177	A1	06-06-2013	AUCUN		

US 2011145595	A1	16-06-2011	KR	20110066700 A	17-06-2011
			US	2011145595 A1	16-06-2011

EP 2180631	A1	28-04-2010	EP	2180631 A1	28-04-2010
			EP	2351286 A1	03-08-2011
			JP	2012506658 A	15-03-2012
			JP	2014197222 A	16-10-2014
			KR	20110088509 A	03-08-2011
			US	2011274268 A1	10-11-2011
			WO	2010046251 A1	29-04-2010

US 2011128030	A1	02-06-2011	CN	101996125 A	30-03-2011
			EP	2285038 A2	16-02-2011
			FR	2949163 A1	18-02-2011
			JP	5581147 B2	27-08-2014
			JP	2011041280 A	24-02-2011
			US	2011128030 A1	02-06-2011
