



⑫

**BREVET D'INVENTION**

**B1**

⑤④ **PROCEDE D'ENCODAGE DE DONNEES MINIMISANT LES VARIATIONS DE FUITES D'UN COMPOSANT ELECTRONIQUE.**

②② **Date de dépôt :** 24.04.15.

③③ **Priorité :**

⑥⑥ **Références à d'autres documents nationaux  
apparentés :**

☐ **Demande(s) d'extension :**

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

④③ **Date de mise à la disposition du public  
de la demande :** 28.10.16 Bulletin 16/43.

④⑤ **Date de la mise à disposition du public du  
brevet d'invention :** 27.07.18 Bulletin 18/30.

⑤⑥ **Liste des documents cités dans le rapport de  
recherche :**

*Se reporter à la fin du présent fascicule*

⑦② **Inventeur(s) :** MAGHREBI HOUSSEM, SERVANT  
VICTOR et BRINGER JULIEN.

⑦③ **Titulaire(s) :** MORPHO Société anonyme.

⑦④ **Mandataire(s) :** REGIMBEAU.

**FR 3 035 532 - B1**



## DOMAINE DE L'INVENTION

Le domaine de l'invention est celui de l'encodage de données par des composants électroniques, pour sécuriser leur utilisation ultérieure.

L'invention s'applique notamment à l'encodage de données de type clé  
5 secrète ou code PIN, pour des composants électroniques de type carte à puce.

## ETAT DE LA TECHNIQUE

De nombreux composants électroniques, tels que par exemple des cartes à  
puces, mettent en œuvre des opérations de calcul ou de comparaison sur des  
10 données secrètes. Certaines applications de ces opérations sont par exemple des applications bancaires, des applications pour téléphonie mobile, etc.

Les opérations sur les données secrètes peuvent faire l'objet d'attaques pour déterminer lesdites données secrètes.

Certaines de ces attaques, dites « sides channels » en anglais ou encore  
15 attaques sur canaux cachés, consistent à étudier le comportement physique du composant électronique, notamment en termes de fuites électromagnétiques, ou encore en termes de variations de consommation électrique, ou de temps de réponse.

Par exemple, pour un composant électronique de type carte à puce, dont  
20 l'activation est conditionnée à la saisie d'un code secret, il est connu de surveiller l'évolution de la consommation électrique lors de la saisie du code pour déterminer le code.

Pour lutter contre ce type d'attaque, des contre-mesures ont déjà été  
proposées, comme par exemple dans le document WO 2014/131546 de la  
25 Demanderesse.

Les contre-mesures existantes sont basées sur l'hypothèse selon laquelle le degré de fuite d'informations d'un composant électrique sur un canal caché dépend linéairement du poids de Hamming de la donnée manipulée, de sorte que la manipulation de données de poids de Hamming identiques induit des fuites  
30 identiques.

Il a donc été proposé d'encoder des données avec des mots de code de poids de Hamming constant pour rendre constant les courants de fuite (c'est-à-dire la consommation électrique du composant lors de l'utilisation des mots de code) et

ainsi rendre indifférenciée l'utilisation d'une donnée secrète de celle de toute autre donnée.

Or l'implémentation de ces contre-mesures montre que la relation entre la consommation du composant électronique et le poids de Hamming du mot de code  
5 utilisé n'est pas exactement linéaire, de sorte qu'à mot de code de poids de Hamming constant, des variations de consommation électrique existent.

Par conséquent les contre-mesures proposées ne sont pas parfaitement fiables.

## 10 PRESENTATION DE L'INVENTION

L'invention a pour but de pallier les inconvénients de l'art antérieur, en proposant un procédé d'encodage de données qui soit plus fiable que les contre-mesures de l'art antérieur.

15 A cet égard, l'invention a pour objet un procédé d'encodage, par un composant électronique, d'une donnée de  $n$  bits en un mot de code de  $m$  bits, caractérisé en ce que le mot de code codant la donnée est choisi dans un sous-ensemble de  $2^n$  mots de code parmi l'ensemble des  $2^m$  mots de code possibles, tel que la variance des émanations physiques du composant électronique lors de  
20 l'utilisation des mots de code du sous-ensemble sur la variance du bruit du composant électronique est inférieure ou égale à un seuil prédéterminé ou tel qu'une différence maximale, entre deux mots de code du sous-ensemble, d'émanations physiques du composant électronique lors de l'utilisation des mots de code, est minimale parmi tous les sous-ensembles de  $2^n$  mots de code compris  
25 dans l'ensemble.

Avantageusement, mais facultativement, le procédé selon l'invention peut en outre comprendre au moins l'une des caractéristiques suivantes :

- Le procédé peut comprendre une étape de construction du sous-ensemble  
30 des mots de code à choisir pour l'encodage.
- La construction du sous-ensemble peut comprendre une étape préliminaire de détermination d'un niveau d'émanation physique du composant électronique pour chacun des  $2^m$  mots de code possibles.

- un niveau d'émanation physique du composant électronique pour un mot de code peut être calculé à partir d'un ensemble de  $m$  valeurs de consommation électrique élémentaire, chaque valeur correspondant à la consommation d'un bit d'un rang donné dans le mot de code.
- 5      - Le niveau d'émanation physique du composant électronique pour un mot de code peut être calculé selon la formule :

$$C = \sum_{i=1}^m a_i x_i$$

où  $a_i$  est la consommation électrique élémentaire du composant pour le bit de rang  $i$ , et  $x_i$  est la valeur du bit de rang  $i$ .

- Le procédé peut en outre comprendre les étapes consistant à :
  - 10      ○ calculer, pour au moins un sous-ensemble de  $2^n$  mots de code parmi l'ensemble des  $2^m$  mots de code, une valeur de ratio de la variance des émanations physiques du composant électronique lors de l'utilisation des mots de code du sous-ensemble sur la variance du bruit du composant électronique,
  - 15      ○ comparer ladite valeur au seuil prédéterminé, et
  - si la valeur est inférieure audit seuil pour au moins un sous-ensemble, générer le sous-ensemble des mots de code à choisir pour l'encodage comme un sous-ensemble pour lequel la valeur est inférieure audit seuil.
- 20      - Si la valeur de ratio est supérieure au seuil pour tous les sous-ensembles de  $2^n$  mots de code parmi l'ensemble des  $2^m$  mots de code, le procédé peut en outre comprendre une étape de construction du sous-ensemble des mots de code à choisir pour l'encodage tel qu'une différence maximale, entre deux mots de code du sous-ensemble, d'émanations physiques du composant électronique lors de l'utilisation des mots de code, est minimale parmi tous les sous-ensembles de  $2^n$  mots de code compris dans l'ensemble.
- 25      - le sous-ensemble de  $2^n$  mots de code peut être construit par la mise en œuvre des étapes consistant à :
  - 30      ○ classer les mots de code par ordre de consommation électrique du composant électronique dans un tableau indexé,

- déterminer un index  $j_0$  d'un mot de code du tableau pour lequel une différence de consommation électrique entre le mot de code d'indice  $j_0$  et le mot de code d'indice  $j_0 + 2^n$  est minimale, et
  - former le sous-ensemble avec les mots de code d'indice  $j$  compris entre  $j_0$  et  $j_0 + 2^n$ .
- 5
- Les émanations physiques du composant électronique peuvent comprendre une consommation électrique du composant ou un rayonnement électromagnétique du composant.
  - L'étape préliminaire peut être mise en œuvre par le composant électronique,
- 10
- ou par une unité de traitement distincte du composant électronique.

L'invention a également pour objet un produit programme d'ordinateur, comprenant des instructions de code pour la mise en œuvre du procédé selon la description qui précède lorsqu'il est exécuté par un processeur.

15

L'invention a enfin pour objet un composant électronique, comprenant un processeur configuré pour la mise en œuvre du procédé selon la description qui précède, ce composant électronique pouvant être une carte à puce.

20

Le procédé d'encodage selon l'invention est plus fiable que les procédés de l'art antérieur. En effet, il est basé sur une modélisation des courants de fuite plus précise qu'auparavant, selon laquelle chaque bit d'une donnée induit une consommation électrique ou un rayonnement électromagnétique différent du composant électronique manipulant ladite donnée.

25

Le procédé tient compte de cette modélisation en sélectionnant, parmi un ensemble de mots de code possible pour coder une donnée sur un nombre de bits déterminé, un sous-ensemble de mots de code utilisables, pour lesquelles les consommations électriques du composant sont les plus proches les unes des autres.

30

Ceci permet en particulier de réduire les différences de consommation par rapport à une contre-mesure basée sur un poids de Hamming constant, et rend donc plus difficilement différenciables les données utilisées par un composant électronique.

## DESCRIPTION DES FIGURES

D'autres caractéristiques, buts et avantages de la présente invention apparaîtront à la lecture de la description détaillée qui va suivre, au regard des figures annexées, données à titre d'exemples non limitatifs et sur lesquelles :

- 5       - La figure 1 représente schématiquement un composant électronique devant traiter une ou plusieurs données secrètes,
- La figure 2 représente schématiquement la sélection des mots de code du sous-ensemble pour l'encodage conforme à un mode de réalisation de l'invention,
- 10       - La figure 3 représente les principales étapes d'un exemple de mise en œuvre du procédé d'encodage.
- La figure 4 illustre des résultats obtenus par la mise en œuvre du procédé d'encodage.

## 15 DESCRIPTION DETAILLEE D'AU MOINS UN MODE DE MISE EN ŒUVRE

En référence à la figure 1, on a représenté un exemple de composant électronique encodant des données, dont notamment des données secrètes de type code secret.

20       Ce composant électronique 1 est avantageusement une carte à puce, comprenant un processeur 10, une mémoire 11 et une interface de communication 12, avec ou sans contact, avec un lecteur et/ou tout autre unité de traitement.

Le processeur 10 est configuré pour encoder des données, les données étant des séquences de  $n$  bits, en mots de code, les mots de code étant des séquences de  $m$  bits, avec  $m$  strictement supérieur à  $n$ .

25

### Procédé d'encodage de données

En référence à la figure 3, on a représenté les principales étapes d'un procédé d'encodage d'une donnée mis en œuvre par le composant électronique 1 décrit ci-avant.

30       Ce procédé est basé sur une modélisation affinée des fuites électromagnétiques d'un composant électronique lors de la manipulation d'un mot de code.

En effet, il s'avère que chaque bit d'une variable  $X$  fuit différemment en fonction de son rang, de sorte que la consommation électrique totale ou le

rayonnement électromagnétique total  $C$  du composant électronique pour la variable  $X$  peut s'écrire comme suit :

$$C = \sum_{i=1}^m a_i x_i$$

Où  $a_i$  est un coefficient statistique de pondération, et  $x_i$  est le bit de rang  $i$  de la variable  $X$ , égal à 0 ou 1.

5

Le procédé décrit ci-après tient compte de cette modélisation affinée.

Il comprend une étape 200 d'encodage d'une donnée de  $n$  bits en un mot de code de  $m$  bits. Le mot de code est utilisé pour représenter la donnée dans des opérations ultérieures telles que des opérations de chiffrement, de déchiffrement, des opérations arithmétiques, etc, la donnée est remplacée ou représentée par le mot de code.

Lors de cette étape 200 d'encodage, le mot de code est choisi parmi un sous-ensemble SE comprenant  $2^n$  mots de code, parmi l'ensemble  $E$  des  $2^m$  mots de code d'une longueur de  $m$  bits possibles.

Le sous-ensemble SE est sélectionné, en fonction des coefficients de pondération de fuite du composant correspondant à des bits respectifs, pour augmenter la résistance du composant aux attaques par canaux cachés en diminuant des variations de consommation électrique ou de rayonnement électromagnétique du composant électronique 1 lorsque le composant utilise les mots de code du sous-ensemble ensemble.

Dans toute la suite, on désigne par le terme général « émanation physique » la consommation électrique ou le rayonnement électromagnétique du composant électronique lors de l'utilisation d'un mot de code, cette utilisation pouvant être une opération de comparaison du mot de code avec un code secret, une opération arithmétique, ou plus généralement toute opération induisant la mise à jour d'un registre interne du composant lors d'une manipulation du mot de code.

Ainsi, le procédé d'encodage 200 comprend avantageusement une étape préliminaire 100 de génération du sous-ensemble SE. Cette étape peut être mise en œuvre par une unité de traitement distincte du composant électronique 1, et dans ce

cas les mots de code composant le sous-ensemble SE sont ensuite stockés dans la mémoire du composant électronique.

Alternativement, le composant électronique 1 génère lui-même le sous-ensemble SE et mémorise ensuite les mots de code le composant.

5 L'étape de génération du sous-ensemble SE est avantageusement mise en œuvre comme suit.

Une première sous-étape 110 comprend la détermination d'un niveau d'émanation physique du composant électronique 1, par exemple un niveau de consommation électrique, lorsque celui-ci utilise un mot de code, pour tous les mots  
10 de code possibles de l'ensemble E des mots de code de m bits.

Cette étape peut être mise en œuvre empiriquement, en mesurant la consommation électrique ou le rayonnement électromagnétique du composant électronique lors d'une utilisation de ce composant qui est identique pour tous les mots de code. Cette utilisation est dans ce cas typiquement une opération de  
15 comparaison du mot de code avec un code secret, une opération arithmétique, ou plus généralement toute opération induisant la mise à jour d'un registre interne du composant.

Alternativement, et de préférence, cette sous-étape est mise en œuvre en calculant la consommation électrique totale ou le rayonnement électromagnétique  
20 du composant électronique lors de l'utilisation d'un mot de code, à partir des fuites élémentaires  $a_i$  correspondant à la part de consommation ou de rayonnement de chaque bit du mot de code.

Ainsi à la sous-étape 110, les émanations physiques du composant électronique 1 pour tous les mots de code de l'ensemble sont-elles plus  
25 avantageusement calculées à partir de l'équation indiquée précédemment, et des coefficients  $a_i$  de consommation correspondant à chaque rang des bits. Ces coefficients sont avantageusement déterminés par une analyse statistique de la consommation d'un composant électrique en fonction des mots de code utilisés.

Avantageusement, cette analyse est une analyse stochastique basée sur  
30 une régression linéaire de la consommation du composant électronique en fonction des mots de code utilisés, pour caractériser la relation qui relie la consommation et les mots de code. On peut par exemple se référer à la publication de W. Schindler, K. Lemke et C. Paar, « A Stochastic Model for Differential Side Channel

Cryptanalysis », CHES 2005 in Lecture Notes in Computer Science volume 3659 pour la mise en œuvre d'une telle analyse.

Une fois cette étape réalisée, on obtient un ensemble de  $2^m$  valeurs de consommations électriques correspondant aux  $2^m$  mots de code possibles.

5

Le sous-ensemble est ensuite sélectionné comme comprenant des mots de code pour lesquels le ratio signal sur bruit du composant électronique lors de l'utilisation des mots de code du sous-ensemble est inférieur à un seuil déterminé en fonction d'un niveau de sécurité exigé. A défaut de disposer d'un sous-ensemble  
10 de  $2^n$  mots de code satisfaisant à ce niveau de sécurité, les mots de code du sous-ensemble SE sont choisis de sorte qu'une différence maximale d'émanation physique du composant électronique parmi des mots de code du sous-ensemble soit minimale parmi tous les sous-ensembles possibles.

15 On va décrire en détail la construction du sous-ensemble satisfaisant à ces exigences.

D'abord, une sous-étape 120 est mise en œuvre pour déterminer un sous-ensemble éventuel pour lequel le ratio signal sur bruit du composant électronique est inférieur à un seuil déterminé. Le signal sur bruit est en effet un indicateur de  
20 sécurité car plus il est faible, et plus il est difficile de déterminer le mot de code manipulé par le composant électronique.

La sous-étape 120 comprend d'abord la fixation 121 d'une valeur seuil de ratio signal sur bruit à atteindre pour obtenir un niveau de sécurité satisfaisant.

Le seuil sur la valeur du ratio signal sur bruit est déterminé en fonction des  
25 besoins en sécurité pour un composant électronique donné. Par exemple, l'article de Stefan Mangard, « Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness (CT-RSA, volume 2964 of Lecture Notes in Computer Science, pages 222-235, Springer, 2004) donne un lien entre le ratio signal sur bruit et le nombre d'échantillons statistiques nécessaires pour réussir une attaque, ce qui  
30 correspond directement au taux de succès d'une attaque, comme visible dans la figure 4 décrite ci-après.

Par exemple, on cherche à imposer l'utilisation de 100000 échantillons statistiques (appelés traces) au minimum pour pouvoir mener à bien une attaque par observation des émanations physiques.

Des protocoles bancaires utilisant une clé secrète donnée limitent en général le nombre d'utilisation à 65536, ainsi le choix d'un nombre de 100000 échantillons statistiques laisse une certaine marge par rapport à cette limite.

En utilisant l'article cité ci-avant, on peut calculer que le ratio signal sur bruit pour atteindre ce nombre de 100000 échantillons statistiques doit être d'environ  $5.10^{-5}$  indépendamment du circuit électronique. Cette dernière valeur peut donc constituer un exemple de cible privilégiée à atteindre.

La sous-étape 120 comprend ensuite le calcul d'un ratio signal sur bruit du composant électronique pour au moins un sous-ensemble de  $2^n$  mots de code parmi l'ensemble des  $2^m$  mots de code possibles.

Le ratio signal sur bruit est calculé comme le ratio de la variance des émanations physiques du composant électronique sur les mots de code du sous-ensemble de  $2^n$  mots de code, divisé par la variance du bruit lors de la manipulation par le composant de tout mot de code.

La variance des émanations physiques du composant électronique sur les mots de code est la variance de la consommation totale ou du rayonnement électromagnétique C fourni par l'équation décrite ci-avant et calculée à l'étape 110, pour tous les mots de code du sous-ensemble.

La variance du bruit est quant à elle constante pour un composant électronique donné.

Avantageusement, la variance du bruit peut être déterminée conformément à la méthode décrite dans la publication « How to compare profiled Side-channel attacks ? » par F.-X. Standaert, F. Koeune, W.Schindler, publié dans Applied Cryptography and Network Security (ACNS) 2009, et résumée comme suit :

- Réaliser l'analyse stochastique de l'étape 110 pour caractériser le signal du composant électronique (cette étape est déjà faite à l'étape 110),
- Acquérir de nouvelles émanations physiques du composant lors de son utilisation avec plusieurs séquences de bits différentes,
- Soustraire des émanations acquises celles qui étaient normalement attendues en vertu de l'analyse stochastique,
- Effectuer la caractérisation stochastique du signal résultant, et calculer la variance des paramètres obtenus.

Puis le ratio signal sur bruit est comparé au seuil lors d'une étape 123. Si le ratio est inférieur au seuil, alors le sous-ensemble pour lequel le ratio signal sur bruit a été calculé à l'étape 120 est choisi pour former (étape 124) le sous-ensemble SE contenant les mots de code pour l'encodage 200 de la donnée.

5            La mise en œuvre des sous-étapes 122 et 123 peut faire l'objet de variantes. Les étapes 122 et 123 peuvent être successivement itérées à chaque fois sur un nouveau sous-ensemble parmi l'ensemble des  $2^m$  mots de code possibles, jusqu'à ce qu'un sous-ensemble satisfasse au test de l'étape 123, et termine cette itération, ou que tous les sous-ensembles possibles aient été testés (flèche en pointillés sur  
10 la figure 3 de l'étape 123 à l'étape 122).

En variante, les sous-étapes 122 et 123 peuvent être mises en œuvre directement sur tous les sous-ensembles possibles (flèche en pointillé sur la figure 3 rebouclant sur l'étape 122), puis le sous-ensemble SE est sélectionné comme le ou l'un parmi les sous-ensembles ayant satisfait au test de l'étape 123.

15            Dans le cas où le critère de sécurité imposé lors de l'étape 121 est tel qu'aucun sous-ensemble de mots de code n'a satisfait à ce critère de sécurité, alors le procédé comprend ensuite une étape 130 de construction du sous-ensemble SE comme le sous-ensemble pour lequel une différence maximale de consommation  
20 entre deux mots de code choisis dans le sous-ensemble est minimale parmi tous les sous-ensembles de  $2^n$  mots de code de l'ensemble E. En d'autres termes, quels que soient deux mots de code choisis dans le sous-ensemble SE, la différence de consommation du composant électronique 1 lors de l'utilisation de chacun de ces deux mots de code est toujours inférieure à la différence de consommation du  
25 composant pour deux mots de code choisis hors du sous-ensemble.

De ce fait, les variations de consommation du composant électronique sont minimisées et il est plus difficile de différencier, en analysant la consommation électrique ou le rayonnement électromagnétique du composant, le traitement d'une clé secrète du traitement d'une autre donnée quelconque.

30            On comprend que la mise en œuvre de l'étape 120 ne présente un avantage que si le niveau de sécurité fixé à cette étape est plus strict que celui obtenu par la mise en œuvre de l'étape 130. Donc si le niveau de sécurité obtenu à l'étape 130 est satisfaisant vis-à-vis des applications envisagées, cette étape pourrait

également être mise en œuvre directement sans mettre en œuvre l'étape 120 pour économiser des temps de calculs.

Pour déterminer rapidement le sous-ensemble SE sans nécessiter de  
 5 moyens de calculs importants, le procédé comprend une sous-étape 131 au cours de laquelle les valeurs de consommation obtenues à l'étape 110 sont ordonnées dans un tableau T indexé de 0 à  $2^m-1$ .

Les valeurs de consommation peuvent être ordonnées par ordre croissant ou décroissant.

10 Puis, une sous-étape 132 comprend la détermination de l'index  $j_0$  du tableau pour lequel une différence de consommation électrique entre le mot de code d'indice  $j_0$  et le mot de code d'indice  $j_0 + 2^n$  est minimale en valeur absolue, notamment pour le cas où les valeurs de consommation sont ordonnées par ordre croissant (dans le cas où les valeurs sont ordonnées par ordre décroissant, la  
 15 différence est déjà positive).

L'index  $j_0$  est donc compris entre 0 et  $2^m-2^n-1$ .

On minimise, sur j :

$$|T[j] - T[j + 2^n]|$$

Le tableau ayant été préalablement ordonné, la différence de consommation maximale sur un sous-ensemble de  $2^n$  mots de code est la différence entre les mots  
 20 de code correspondant aux index respectivement minimum et maximum du tableau.

La recherche de l'indice  $J_0$  est de fait de complexité linéaire.

Enfin, l'étape 130 de génération du sous-ensemble 100 comprend une sous-étape 133 de formation du sous-ensemble au cours de laquelle tous les mots de code présentant un indice compris entre le mot de code d'indice  $j_0$  et le mot de  
 25 code d'indice  $j_0+2^n$  sont sélectionnés, et de préférence mémorisés dans la mémoire 11 du composant électronique 1.

Le sous-ensemble SE est représenté schématiquement en figure 2, où l'on a représenté des profils de consommation du composant électronique pour différents mots de code, et sélectionné les profils présentant une différence minimale.

30 Tout encodage de donnée 200 subséquent par le composant électronique est donc réalisé en choisissant un mot de code du sous-ensemble SE pour encoder une donnée.

On a représenté sur la figure 4 les résultats d'attaques par canaux cachés obtenus par la mise en œuvre du procédé ci-avant.

L'attaque consiste à mesurer la consommation électrique ou le rayonnement électromagnétique d'un composant électronique 1 lors du traitement d'un échantillon statistique de mots de code, dans le but de déterminer un mot de code  
5 correspondant à une clé secrète à protéger du composant électronique.

En abscisse est fournie le nombre d'échantillons statistiques (appelés traces) utilisés, et en ordonnée le taux de succès de l'attaque, pour un écart-type du bruit  $\sigma_b$  de 0,2 et pour un écart type de la déviation des coefficients  $a_i$  par rapport  
10 au modèle du poids de Hamming (représentatif de la déviation entre les valeurs des coefficients et la valeur 1 du poids de Hamming) de 0,05.

Le procédé décrit ci-avant est testé pour différentes longueurs (« m ») de mots de code, et est comparé au procédé d'encodage Dual Rail de l'art antérieur, et au procédé d'encodage par poids constant décrit dans le document WO  
15 2014/131546 de la Demanderesse.

On constate en premier lieu que le procédé décrit ci-après protège mieux le composant électronique que les procédés de l'art antérieur, car le nombre d'échantillons statistiques nécessaire pour obtenir un taux de succès de l'attaque de l'ordre de 90% est de l'ordre de deux fois celle requise pour le code Dual Rail.

20 En second lieu, la sécurité du procédé augmente avec la longueur des mots de code sélectionnée, car la différence de consommation maximale entre deux mots de code du sous-ensemble SE diminue lorsque la longueur des mots de code augmente.

Par conséquent, la longueur des mots de code est avantageusement choisie  
25 en fonction d'un compromis entre le niveau de sécurité requis et la quantité de mémoire disponible du composant électronique 1.

## REVENDICATIONS

1. Procédé d'encodage (200), par un composant électronique (1), d'une donnée de n bits en un mot de code de m bits,

- 5 caractérisé en ce qu'il comprend une étape (100) de construction d'un sous-ensemble (SE) de  $2^n$  mots de code parmi l'ensemble (E) des  $2^m$  mots de code possibles, tel que la variance des émanations physiques du composant électronique (1) lors de l'utilisation des mots de code du sous-ensemble (SE) sur la variance du bruit du composant électronique est inférieure ou égale à un seuil prédéterminé ou
- 10 tel qu'une différence maximale, entre deux mots de code du sous-ensemble (SE), d'émanations physiques du composant électronique (1) lors de l'utilisation des mots de code, est minimale parmi tous les sous-ensembles de  $2^n$  mots de code compris dans l'ensemble (E),

la construction (100) du sous-ensemble (SE) comprenant une étape préliminaire

15 (110) de détermination d'un niveau d'émanation physique du composant électronique pour chacun des  $2^m$  mots de code possibles, mise en œuvre soit :

- par mesure de la consommation électrique ou du rayonnement électromagnétique du composant électrique lors de l'utilisation d'un mot de code, ladite utilisation étant identique pour tous les mots de code, soit
- 20 - par calcul selon la formule :

$$C = \sum_{i=1}^m a_i x_i$$

où  $a_i$  est une valeur de consommation électrique élémentaire du composant pour le bit de rang i, et  $x_i$  est la valeur du bit de rang i,

et en ce que le mot de code codant la donnée est choisi dans ledit sous-ensemble (SE).

25

2. Procédé d'encodage selon la revendication 1, comprenant en outre les étapes consistant à :

- calculer (122), pour au moins un sous-ensemble de  $2^n$  mots de code parmi l'ensemble des  $2^m$  mots de code, une valeur de ratio de la variance des émanations physiques du composant électronique lors de l'utilisation des mots de code du sous-ensemble sur la variance du bruit du composant électronique,
- 30

- comparer (123) ladite valeur au seuil prédéterminé, et
- si la valeur est inférieure audit seuil pour au moins un sous-ensemble, générer (124) le sous-ensemble des mots de code à choisir pour l'encodage comme un sous-ensemble pour lequel la valeur est inférieure audit seuil.

5

3. Procédé d'encodage selon la revendication 2, dans lequel, si la valeur de ratio est supérieure au seuil pour tous les sous-ensembles de  $2^n$  mots de code parmi l'ensemble des  $2^m$  mots de code, le procédé comprend en outre une étape (130) de construction du sous-ensemble (SE) des mots de code à choisir pour l'encodage tel qu'une différence maximale, entre deux mots de code du sous-ensemble (SE), d'émanations physiques du composant électronique (1) lors de l'utilisation des mots de code, est minimale parmi tous les sous-ensembles de  $2^n$  mots de code compris dans l'ensemble (E).

15

4. Procédé d'encodage selon l'une des revendications 1 à 3, dans lequel le sous-ensemble de  $2^n$  mots de code est construit (130) par la mise en œuvre des étapes consistant à :

- classer les mots de code (131) par ordre de consommation électrique du composant électronique dans un tableau indexé,
- déterminer (132) un index  $j_0$  d'un mot de code du tableau pour lequel une différence de consommation électrique entre le mot de code d'indice  $j_0$  et le mot de code d'indice  $j_0 + 2^n$  est minimale, et
- former (133) le sous-ensemble avec les mots de code d'indice  $j$  compris entre  $j_0$  et  $j_0 + 2^n$ .

20

25

5. Procédé d'encodage selon l'une des revendications précédentes, dans lequel les émanations physiques du composant électronique comprennent une consommation électrique du composant ou un rayonnement électromagnétique du composant.

30

6. Procédé d'encodage selon l'une des revendications 1 à 5, dans lequel l'étape préliminaire (110) est mise en œuvre par le composant électronique.

7. Procédé d'encodage selon l'une des revendications 1 à 6, dans lequel l'étape préliminaire (110) est mise en œuvre par une unité de traitement distincte du composant électronique.
- 5    8. Produit programme d'ordinateur, comprenant des instructions de code pour la mise en œuvre du procédé selon l'une des revendications 1 à 6 lorsqu'il est exécuté par un processeur (10).
9. Composant électronique (1), comprenant un processeur (10) configuré pour la
- 10    mise en œuvre du procédé selon l'une des revendications 1 à 6.
10. Composant électronique (1) selon la revendication 9, le composant étant une carte à puce.

1/3

FIG. 1

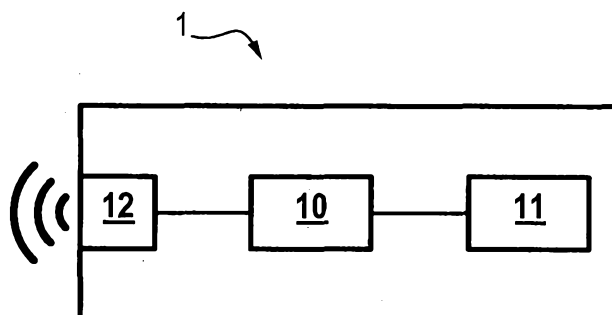
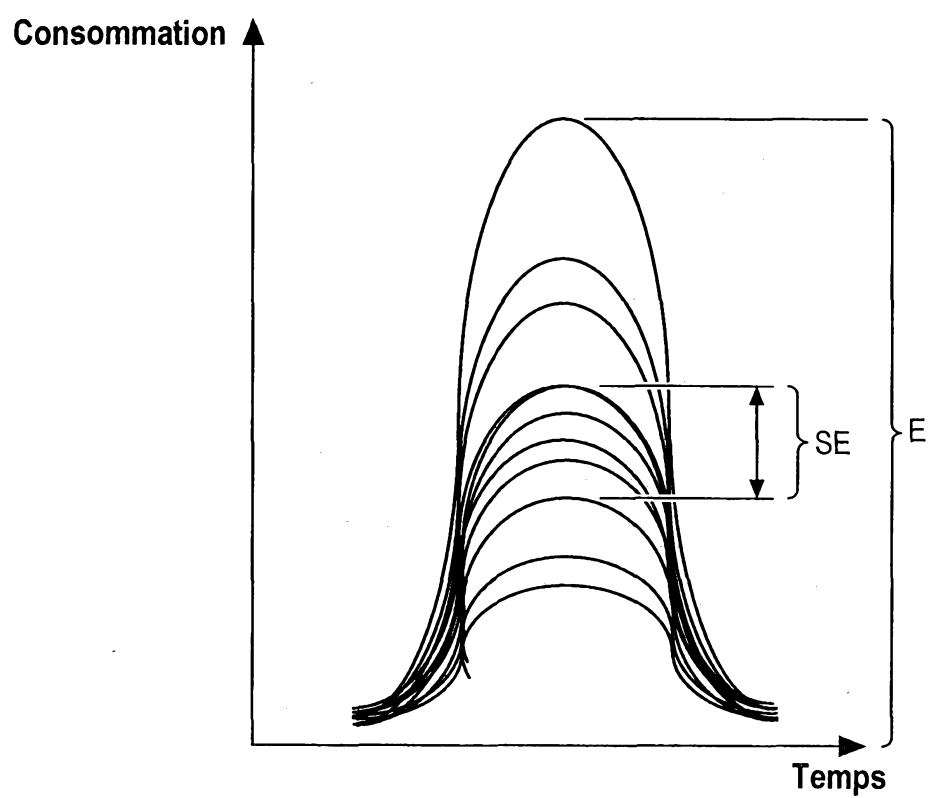
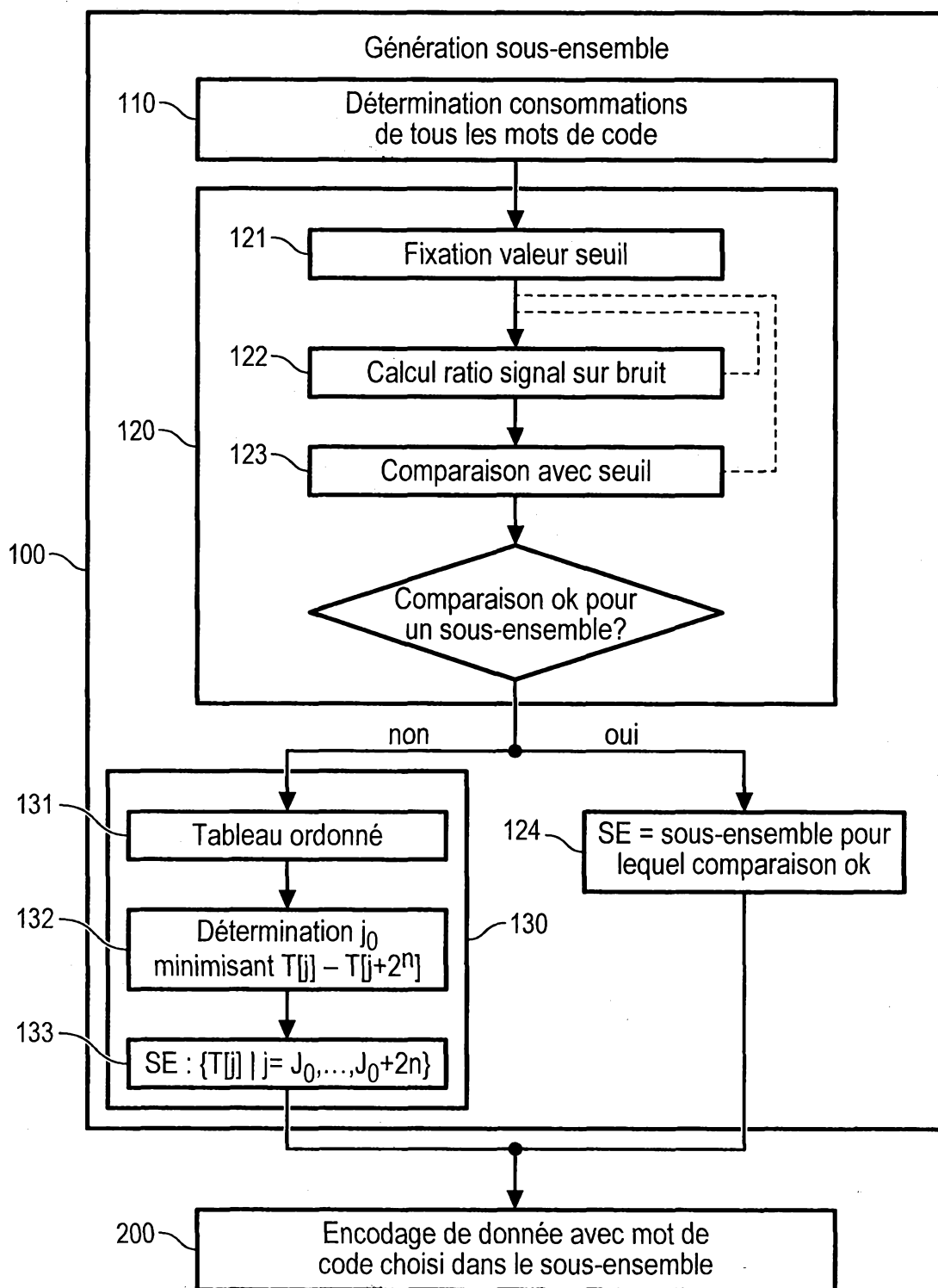


FIG. 2



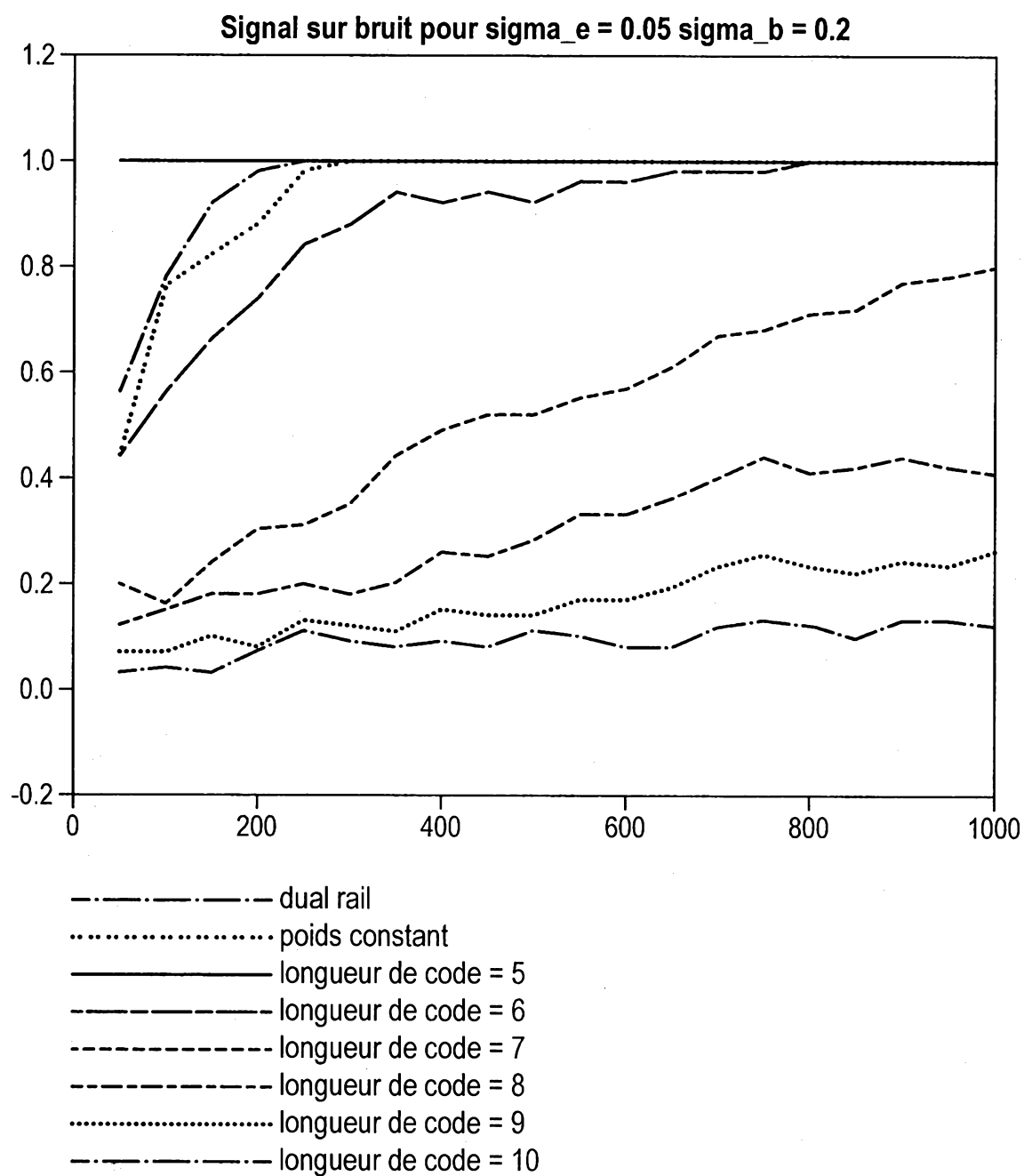
2/3

FIG. 3



3/3

FIG. 4



# RAPPORT DE RECHERCHE

articles L.612-14, L.612-17 et R.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'ÉTABLISSEMENT DU PRÉSENT 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 CITÉS DANS LE PRÉSENT 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**

CONG CHEN ET AL: "Balanced Encoding to Mitigate Power Analysis: A Case Study", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20141121:072458, 20 novembre 2014 (2014-11-20), pages 1-15, XP061017438, [extrait le 2014-11-20]

VICTOR SERVANT ET AL: "Study of a Novel Software Constant Weight Implementation", CORRECT SYSTEM DESIGN, vol. 8968, 1 janvier 2015 (2015-01-01), pages 35-48, XP055250347, Cham ISSN: 0302-9743 ISBN: 978-3-642-22877-3

WO 2014/131546 A1 (MORPHO [FR])  
4 septembre 2014 (2014-09-04)

FR 2 855 286 A1 (GEMPLUS CARD INT [FR])  
26 novembre 2004 (2004-11-26)

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

NEANT

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

NEANT