(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
4 septembre 2014 (04.09.2014)

WIPO | PCT

(10) Numéro de publication internationale
WO 2014/131546 A1

(51) Classification internationale des brevets :
H03M 7/20 (2006.01) *G06F 11/08* (2006.01)
G06K 19/07 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2014/050867

(22) Date de dépôt international :
17 janvier 2014 (17.01.2014)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1351712 27 février 2013 (27.02.2013) FR

(71) Déposant : **MORPHO** [FR/FR]; 11, boulevard Gallieni, F-92130 Issy-les-Moulineaux (FR).

(72) Inventeurs : **BRINGER, Julien**; Morpho, 11 boulevard Gallieni, F-92130 Issy Les Moulineaux (FR). **SERVANT, Victor**; Morpho, 27 rue Leblanc, F-75015 Paris (FR).

(74) Mandataire : **REGIMBEAU**; 20, rue de Chazelles, F-75847 Paris Cedex 17 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

(54) **Title** : METHOD FOR ENCODING DATA ON A CHIP CARD BY MEANS OF CONSTANT-WEIGHT CODES

(54) **Titre** : PROCEDE D'ENCODAGE DE DONNEES SUR UNE CARTE A PUCE PAR DES CODES DE POIDS CONSTANT

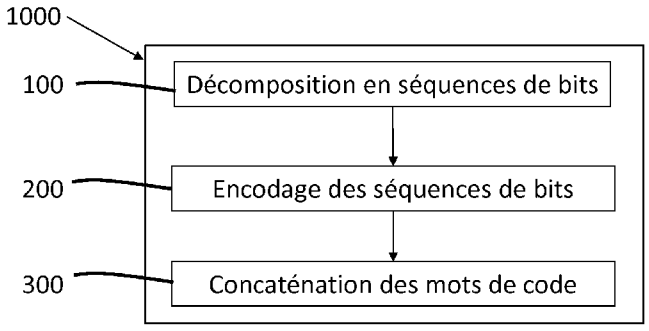

FIG.2

100 Decompose into bit sequences
200 Encode bit sequences
300 Concatenate code words

(57) **Abstract** : The invention relates to a data-processing method that includes encoding a plurality of data of n bits into code words having a predefined constant Hamming weight, characterized in that said method also includes using (4000) encryption operations or arithmetic operations on the resulting code word(s) and also in that encoding each datum includes: decomposing (100) the datum into a plurality of m bit sequences to be encoded, m strictly being less than n; encoding (300) each bit sequence into a partial code word, each having a predefined Hamming weight, such that the sum of the Hamming weights of the partial code words are equal to the Hamming weights of the code word; and concatenating (300) the partial code words such as to produce the code word corresponding to the datum. The invention also relates to a data transmission method and to an electronic circuit configured to implement said methods.

(57) **Abrégé** :

[Suite sur la page suivante]

WO 2014/131546 A1

L'invention concerne un procédé de traitement de données comprenant l'encodage, d'une pluralité de données de n bits en des mots de code présentant un poids de Hamming constant prédéfini, le procédé étant caractérisé en ce qu'il comprend en outre la mise en œuvre (4000) d'opérations de chiffrement ou d'opérations arithmétiques sur le ou les mots de code obtenus, et en ce que l'encodage de chaque donnée comprend : - la décomposition (100) de la donnée en une pluralité de m séquences de bits à coder, m étant strictement inférieur à n, - le codage (300) de chaque séquence de bits en un mot de code partiel présentant chacun un poids de Hamming prédéfini, de sorte que la somme des poids de Hamming des mots de code partiels soit égale au poids de Hamming du mot de code, et la concaténation (300) des mots de code partiels pour obtenir le mot de code correspondant à la donnée. L'invention concerne également un procédé de transmission de données, et un circuit électronique configuré pour la mise en œuvre desdits procédés.

PROCEDE D'ENCODAGE DE DONNEES SUR UNE CARTE A PUCE PAR DES CODES DE POIDS CONSTANT

DOMAINE DE L'INVENTION

Le domaine de l'invention est celui de l'encodage de données dans des cartes à puces, pour sécuriser leur utilisation ultérieure, notamment dans des applications de cryptographie.

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 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 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.

D'autres attaques, qualifiées d'attaques « par injection de fautes » ont également été développées, qui consistent en la corruption de certaines données utilisées lors d'un calcul mis en œuvre par le composant électronique pour obtenir les données secrètes. Ces attaques comprennent par exemple le bombardement du composant électronique par laser ou par lumière, la génération de champs électromagnétiques parasites, l'injection de pics de tension dans l'alimentation du composant, etc.

Pour contrer ces types d'attaques, il a été proposé d'ajouter aux données secrètes une valeur aléatoire, décorrélant ainsi les données utilisées de leur valeur d'origine. Cette méthode n'est pourtant pas pleinement efficace car il est possible, à partir de l'observation de plusieurs calculs successifs, de retrouver la donnée secrète d'origine.

Une autre proposition a consisté en l'encodage des données secrètes avec des codes dits « de poids constant », c'est-à-dire des codes associant à chaque donnée un mot de code présentant un poids de Hamming constant prédéterminé. Le poids de Hamming d'une série de bits est le nombre de bits à 1 de la série.

Grâce à cet encodage, toutes les données utilisées présentent le même poids de Hamming, ce qui permet de rendre également constant la consommation électrique du composant électronique lors de l'utilisation desdites données (la consommation électrique du composant dépend en effet du poids de Hamming des données utilisées). Le composant est donc protégé des attaques par canaux cachés.

De plus, il est possible de détecter une attaque par injection de faute si une donnée encodée présente un poids de Hamming différent du poids de Hamming prédéterminé.

Cependant, l'encodage par codes de poids constant ne permet pas actuellement de mettre en œuvre des opérations sur données encodées dans un composant électronique de faible mémoire tel qu'une carte à puce.

Par exemple, on connaît un encodage appelé Dual Rail, qui consiste à encoder un 0 par la combinaison 1-0 et un 1 par la combinaison 0-1. Ce procédé double donc la taille de la séquence de bits encodée par rapport à la donnée initiale, et la mise en œuvre d'opérations sur ces données encodées n'est pas possible sur une carte à puce car elle requiert trop de mémoire.

De même, on connait du brevet FR2855286 un procédé de transmission de données encodées à l'aide de codes de poids constant, mais ce procédé ne permet pas la mise en œuvre d'opérations sur les données encodées, car ces opérations nécessiteraient encore trop de mémoire que la mémoire disponible dans une carte à puce.

PRESENTATION DE L'INVENTION

L'invention a pour but de remédier aux inconvénients de l'art antérieur mentionnés ci-avant, en proposant un procédé d'encodage de données limitant la taille des mots de code obtenus afin de permettre la mise en œuvre ultérieure de calculs à partir desdits mots de code sur un composant électronique de type carte à puce.

L'invention a également pour but de fournir un procédé d'encodage de données permettant de résister à des attaques de types à canaux cachés ou de détecter des attaques par injection de fautes.

A cet égard, l'invention a pour objet un procédé de traitement de données comprenant l'encodage d'une pluralité de données de n bits en des mots de code présentant un poids de Hamming constant prédéfini,
le procédé étant caractérisé en ce qu'il comprend en outre la mise en œuvre d'opérations de chiffrement ou d'opérations arithmétiques sur le ou les mots de code obtenus, et en ce que l'encodage de chaque donnée comprend :

- la décomposition de la donnée en une pluralité de m séquences de bits à coder, m étant strictement inférieur à n,
- le codage de chaque séquence de bits en un mot de code partiel présentant chacun un poids de Hamming prédéfini, de sorte que la somme des poids de Hamming des mots de code partiels soit égale au poids de Hamming du mot de code, et
- la concaténation des mots de code partiels pour obtenir le mot de code correspondant à la donnée.

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

- la taille du mot de code obtenu est strictement inférieure à 2n bits.
- la taille n des données est une puissance de 2 bits.
- la taille des séquences de bits est une puissance de 2 bits.
- les données comprennent 4 bits, chaque donnée étant décomposée en une séquence de 3 bits, et une séquence d'un bit, la première séquence étant codée en un mot de code partiel de taille 5 bits et de poids de Hamming égal à 2 ou 3, et le bit restant étant codé en un mot de code partiel de taille 2 bits et de poids de Hamming égal à 1.
- les données comprennent 8 bits, le procédé comprenant la décomposition de chaque donnée en deux séquences de 4 bits, les deux séquences de 4 bits étant codées en deux mots de code partiels de 6 bits et de poids de Hamming égal à 3.

- L'encodage est mis en œuvre par une première unité de traitement, le procédé comprend en outre la transmission à la seconde unité de traitement d'au moins un mot de code obtenu à partir de la ou les données, et les opérations de chiffrement ou les opérations arithmétiques sont mises en œuvre sur ledit au moins un mot de code par la seconde unité de traitement.
- le procédé comprend en outre la vérification, par la seconde unité de traitement, de la valeur du poids de Hamming du mot de code reçu.
- la mise en œuvre des opérations arithmétiques ou les opérations de chiffrement est réalisée sur au moins un mot de code, et produit en sortie le résultat codé de l'opération appliquée à la donnée correspondant au mot de code.
- les opérations arithmétiques ou les opérations de chiffrement comprennent des opérations linéaires appliquées sur au moins un mot de code, et la mise en œuvre d'une opération linéaire comprend :
    - la génération d'au moins une table prenant en entrée au moins un mot de code partiel, et produisant en sortie le résultat de l'opération appliquée au(x) mot(s) de code partiel(s),
    - la décomposition de chaque mot de code sur lequel l'opération est mise en œuvre en mots de code partiels, et
    - le calcul de l'opération par application des mots de code partiels aux tables, et la concaténation des résultats obtenus.
- les opérations arithmétiques ou les opérations de chiffrement sont non-linéaires, et la mise en œuvre d'une opération non linéaire comprend :
    - la génération d'au moins une table prenant en entrée au moins un mot de code partiel d'au moins un mot de code, et produisant en sortie le résultat codé de l'opération appliquée à au moins une donnée complète dont sont tirés les mots de codes partiels,
    - la décomposition de chaque mot de code sur lequel l'opération est mise en œuvre en mots de code partiels, et
    - le calcul de l'opération par application des mots de code partiels aux tables.
- les opérations de chiffrement ou les opérations arithmétiques des étapes de traitement de d'algorithmes cryptographiques, d'algorithmes de calcul de

fonctions de hachage, ou d'algorithmes de calcul d'intégrité adaptés pour recevoir en entrée lesdits mots de code.

L'invention a également pour objet un circuit électronique comprenant :

- un module d'encodage comportant une unité de traitement adaptée pour coder des données de n bits en des mots de code présentant un poids de Hamming constant prédéfini et pour mettre en œuvre sur lesdits mots de code des opérations de chiffrement ou des opérations arithmétiques par la mise en œuvre du procédé de traitement décrit ci-avant.

Avantageusement, mais facultativement, le circuit électronique selon l'invention peut en outre comprendre les caractéristiques suivantes : le module d'encodage comporte en outre des moyens de transmission de données, et le circuit comprend en outre :

- un module de décodage comportant une unité de traitement adaptée pour décoder un mot de code transmis par le premier module, et
- un module de génération de signal d'erreur, adapté pour générer un signal d'erreur lorsque le poids de Hamming d'un mot de code transmis par le premier module est différent d'un poids de Hamming prédéfini.

L'invention a enfin pour objet une carte à puce comportant un tel circuit électronique.

Le procédé de traitement proposé comprend un encodage de données en mots de code de taille suffisamment faible pour que des algorithmes puissent être mis en œuvre sur lesdits mots de code, même dans des unités informatiques à faible mémoire telles que des cartes à puce.

En outre, l'utilisation de codes de poids constant permet de sécuriser les données contre des attaques par canaux cachés comme les attaques nommées SPA, DPA, MIA, CPA, ASCA, car la consommation électrique de la carte à puce est la même pour toutes les données utilisées.

En outre, l'utilisation de codes de poids constant permet de détecter certaines attaques par injection de faute comme notamment les attaques par impulsion laser.

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 :

- La figure 1 représente schématiquement un exemple de composant électronique traitant une ou plusieurs données secrètes,
- La figure 2 représente les principales étapes d'un mode de mise en œuvre d'un procédé d'encodage.
- La figure 3 représente un exemple de mise en œuvre du procédé d'encodage.
- La figure 4 représente les principales étapes d'un exemple de mise en œuvre d'un procédé de traitement de données.

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

Unité informatique d'encodage de données

En référence à la figure 1, on a représenté un exemple d'unité informatique pouvant encoder des données, dont notamment des données secrètes et réaliser des opérations à partir desdites données. Cette unité informatique est avantageusement une carte à puce 1, qui comprend un circuit électronique comportant un module d'encodage 10 et un module de décodage 20. Alternativement, le module d'encodage et le module de décodage peuvent appartenir à deux unités informatiques distinctes connectées entre elle pour autoriser une communication de données.

Le module d'encodage 10 est avantageusement intégré à un processeur de la carte à puce, et le module de décodage peut être intégré à un périphérique tel qu'une mémoire ou un coprocesseur de la carte à puce.

Le module d'encodage 10 comporte des moyens de transmission de données, par exemple un bus 11 de communication de données, et une unité de traitement 12, adaptée pour mettre en œuvre des opérations d'encodage et de chiffrement sur des données, ladite unité étant avantageusement une unité arithmétique et logique (ALU). Une unité arithmétique et logique est un circuit intégré dans un processeur permettant la mise en œuvre des calculs sur les données.

Le module 20 comporte des moyens de réception de données 21 comme un bus de réception de données, ainsi qu'une unité de traitement 22, configurée pour décoder des données reçues du module d'encodage, l'unité étant avantageusement une unité arithmétique et logique 22.

Procédé d'encodage de données

En référence à la figure 2, l'unité de traitement 12 du module d'encodage 10 est adaptée pour encoder une pluralité de données, dont notamment des données secrètes, afin que ces données ne soient pas obtenues au cours de leur utilisation par une attaque par canaux cachées.

Pour une donnée D de taille égale à n bits, ou n est une puissance de 2, le procédé d'encodage 1000 comporte une étape 100 consistant à scinder la donnée en plusieurs séquences de bits de taille inférieure à n, avantageusement en m séquences de bits $d_1,\ldots, d_m$, m étant strictement inférieur à n. Il existe donc au moins une séquence de bits comprenant au moins deux bits. Cette décomposition de la donnée est une partition, c'est-à-dire qu'aucun bit de la donnée n'est présent dans deux séquences de bits.

Cette décomposition permet de réduire la taille de chaque séquence de bits pour le calcul ultérieur d'opérations binaires à deux opérandes comme par exemple le ou exclusif.

Les séquences de bits obtenus présentent une taille égale à une puissance de deux bits. Ceci permet d'obtenir un bon compromis entre la capacité de détection de fautes et la mémoire occupée par le procédé. Par exemple, dans la figure 3, on a représenté une donnée D d'une longueur de n = 8 bits, scindée en deux séquences de bits d_1, d_2 de 4 bits chacune.

Selon un autre exemple, une donnée d'une longueur de n=4 bits est scindée en deux séquences de 2 bits chacune.

Au cours d'une étape 200, l'unité de traitement encode la donnée au moyen d'un code de poids constant pour obtenir un mot de code correspondant M, présentant un poids de Hamming ω constant et déterminé.

Dans toute la suite, on note *x,y-code* la fonction qui transforme une donnée en une donnée de poids de Hamming « x » sur « y » bits. L'ensemble image de cette fonction contient donc $\binom{y}{x}$ éléments.

On note également "$x_1, y_1 - x_2, y_2 - code$" le codage d'une première partie d'une donnée par un $x_1, y_1 - code$ et de sa seconde partie par un $x_2, y_2 - code$.

L'ensemble image de cette fonction contient donc $\binom{y_1}{x_1} \times \binom{y_2}{x_2}$ éléments.

Selon la notation précédente, l'unité de traitement met en œuvre, pour réaliser l'encodage de la donnée, un encodage de type $x_0, y_0 - x_1, y_1 - \cdots - x_m, y_m - code$, où m>0 est le nombre de séquence de bits en lesquelles la donnée a été décomposée. En d'autres termes, l'unité de traitement encode au cours de l'étape 200, au moyen d'un codage de poids constant, chaque séquence de bits $d_1,\ldots,d_m$ de la donnée pour former un mot de code partiel correspondant $m_1,\ldots m_m$.

De retour à l'exemple de la figure 3, les séquences de bits d_1, d_2 sont encodées chacune au moyen d'un 3,6-code pour obtenir des mots de codes respectifs m_1, m_2.

Le mot de code M correspondant à la donnée totale D est la concaténation des mots de code partiels $m_1,\ldots m_m$, réalisée par l'unité de traitement au cours d'une étape 300.

Très avantageusement, la somme des y_m, c'est-à-dire des longueurs (en bits) des mots de code partiels, qui correspond à la longueur totale en bits du mot de code obtenu, est strictement inférieure à 2n. Ceci permet d'obtenir un mot de code plus cours que notamment dans le procédé Dual Rail, qui le rend plus simple à mettre en œuvre dans un système informatique à faible mémoire tel qu'une carte à puce.

On donne également des exemples de codes préférés pour la mise en œuvre du procédé ; dans le cas où la taille des données D à encoder est de 4 bits, on emploie de préférence un *3,5-1,2-code* ou un *2,5-1,2-code*, à permutation du premier et du deuxième codes près, c'est-à-dire que la donnée D est décomposée en une séquence de 3 bits, puis un bit. La première séquence étant codée en un mot de code partiel de taille 5 bits et de poids de Hamming égal à 2 ou 3, et le bit restant étant codé en un mot de code partiel de taille 2 bits et de poids de Hamming égal à 1.

Dans le cas où la taille des données D à encoder est de 8 bits, on emploie de préférence un *3,6-3,6-code*, la donnée D est décomposée en deux séquences de bits de 4 bits, chacune étant codée en un mot de code partiel de 6 bits et de poids de Hamming égal à 3, comme dans l'exemple de la figure 3.

Procédé de traitement de données

Le procédé d'encodage de données 1000 décrit ci-avant permet la transmission sécurisée de données secrètes d'un module à un autre, pour leur utilisation ultérieure, par exemple au cours d'opérations de chiffrement.

Il permet également la mise en œuvre d'opérations de chiffrement et/ou d'opérations arithmétiques sur les données encodées, par des unités de traitement à faibles capacités de calcul telles que des cartes à puce.

On a représenté en figure 4 un procédé de traitement de données comprenant l'encodage, la transmission, et l'exploitation ultérieure des données transmises.

Dans l'exemple d'une carte à puce comprenant un module d'encodage 10 et un module de décodage 20 comme illustré en figure 1, une première étape de transmission de données comprenant l'encodage 1000 desdites données par l'unité de traitement 12 du module d'encodage 20.

Au cours d'une étape 2000, le bus de communication de données 11 transfère au bus de réception 21 du module de décodage 20 les mots de code obtenus par l'encodage des données.

Avantageusement, la carte à puce peut également comprendre un module 30 de génération de signal d'erreur, qui peut être intégré au module de décodage (comme illustré sur la figure 1) ou connecté à celui-ci. Avantageusement, mais facultativement, ce module 30 vérifie au cours d'une étape 3000 que le poids de Hamming des mots de code transmis par le module d'encodage est égal au poids de Hamming constant ω qui est convenu avant la mise en œuvre du procédé de transmission.

Si le poids de Hamming d'un mot de code diffère du poids de Hamming ω, ou si le mot de code reçu n'est pas conforme au mot attendu (bien que présentant le poids de Hamming ω) le module 30 détecte un signal d'erreur au cours d'une étape 3100. L'étape de vérification du poids de Hamming permet notamment de détecter

une attaque par injection de faute, qui aurait pour conséquence de modifier le poids de Hamming des données transmises.

Si le poids de Hamming est conforme au poids attendu, l'unité de traitement 22 décode les mots de code et/ou les exploite pour mettre en œuvre une opération de chiffrement ou une opération arithmétique, par exemple de type booléenne, au cours d'une étape 4000.

Les résultats des opérations arithmétiques ou de chiffrement appliqués aux données non codées peuvent être obtenus à partir des mots de codes générés à partir desdites données, comme décrit ci-après.

Alternativement, le décodage et/ou l'exploitation 4000 des mots de code pour mettre en œuvre une opération de chiffrement est réalisé sans vérifier au préalable l'exactitude des mots de code.

Alternativement les opérations 4000 de chiffrement et/ou les opérations arithmétiques peuvent être réalisées par la première unité de traitement sans ou avant qu'une étape 2000 de transmission des données à la deuxième unité de traitement soit mise en œuvre.

Par exemple, une opération de chiffrement peut être une étape d'un algorithme cryptographique tel que l'AES (pour « Advanced Encryption Standard » ou « standard de chiffrement avancé ») ou le LED, d'un algorithme de calcul d'une fonction de hachage tel que par exemple SHA-1,SHA-2 ou le futur SHA-3, ou encore un algorithme de calcul d'intégrité tel que de contrôle de redondance cyclique (connu sous l'acronyme « CRC ») ou le LRC (acronyme anglais de « longitudinal redundancy check »), un tel algorithme ayant été préalablement adapté pour recevoir en entrée les mots de code obtenus par le procédé décrit ci-avant.

Plusieurs types d'adaptations peuvent être réalisés en fonction de la nature des opérations mises en œuvre dans les algorithmes.

Dans de nombreux algorithmes, des opérations arithmétiques sont pré calculées sous forme de tableaux ou tables de vérité.

Dans le cas où les fonctions de chiffrement sont des fonctions non linéaires, l'adaptation de la fonction aux mots de code consiste à reprendre les tableaux pré calculés et de les adapter au calcul en prenant pour entrées et sorties les valeurs correspondant aux mots de code sur lesquels on réalise le calcul. En d'autres termes, on génère au moins une table ayant pour entrées les mots de code partiels

sur la base desquels on réalise le calcul ou le mot de code complet, et fournissant en sortie le résultat codé de l'opération appliquée à la donnée complète non codée, qui est la concaténation des séquences de bits dont sont tirés les mots de code partiels. L'opération est donc appliquée à l'ensemble des mots de code partiels.

Ainsi par exemple, on note A une donnée comprenant la concaténation de deux séquences de bits a_0, a_1 de tailles respectives L_0 et L_1. B est une donnée comprenant la concaténation de deux séquences de bits b_0, b_1, de tailles respectives L_0 et L_1.

On note $A = a_1||a_0$, et $B = b_1 || b_0$, où « || » est le symbole de concaténation.

Soit K_0 un code prenant L_0 bits en entrée fournissant en sortie un mot de code de taille lk_0 bits, et K_1 un code prenant L_1 bits en entrée, et fournissant en sortie un mot de code de taille lk_1 bits.

On note $CW(A)=K_1(a_1) || K_0(a_0)$, et $CW(B) = K_1 (b_1) || K_0(b_0)$, qui sont de taille lk_0+lk_1 bits.

Un premier exemple de calcul d'une opération non-linéaire est donné pour une fonction à un seul opérande. En appelant cette fonction « NLF », on pré-calcule une table T_NLF donnant :

T_NLF [CW(A)] = CW (NLF (A)).

En d'autres termes, T_NLF est une table prenant en entrée un mot de code complet CW(A) et fournissant en sortie le mot de code obtenu par un encodage identique de l'image de A par la fonction NLF.

Un deuxième exemple est donné pour le calcul d'une fonction à deux opérandes, par exemple l'addition modulo 2^{L0+L1}.

On génère trois tables définies comme suit :

- ADD-K_0[K_0(a), K_0(b)] = K_0[(a+b) modulo 2^{L0}]

Cette table prend en entrées deux données codées par K_0, et produit en sortie le reste de la division euclidienne de la somme des deux données par 2^{L0}, codé par K_0.

- REM-K_0[K_0(a), K_0(b)] = K_1[(a+b) / 2^{L0}]

Cette table prend en entrées deux données codées par K_0, et produit le quotient de la division euclidienne de la somme des deux données par 2^{L0}, codé par K_1,

- ADD-K_1[K_1(a) || K_1(b)] = K_1[(a+b) modulo 2^{L1}]

Cette table prend en entrées deux données codées par K1, et produit le reste de la division euclidienne de la somme des deux données par 2^{L1}, codé par K1.

On va maintenant décrire l'obtention de CW(A+B modulo 2^{L0+L1}) en partant de CW(A) et CW(B).

CW(A+B modulo 2^{L0+L1}) est l'encodage de A+B modulo 2^{L0+L1}. En reprenant les mêmes notations que précédemment :

$A+B = a_1||a_0 + b_1||b_0 = (a_1+b_1).\ 2^{L0} + a_0 + b_0$

Que l'on peut noter : $X.\ 2^{L0+L1} + Y.\ 2^{L0} + R_0$, d'où A+B mod 2^{L0+L1} : $Y.\ 2^{L0} + R_0$.

Où :

- R_0 est le résultat de a_0+b_0 modulo 2^{L0}, c'est-à-dire le reste de la division euclidienne de a_0+b_0 par 2^{L0}
- X est le quotient de la division euclidienne de a+b par 2^{L0+L1}
- Y est le résultat de a+b modulo 2^{L0+L1}, c'est-à-dire le reste de le division euclidienne de a+b par 2^{L0+}L1, qui se décompose en C_0+R_1, où C_0 est le quotient de la division euclidienne de a_1+b_1 par 2^{L1}, et R_1 est la retenue de l'addition a_0+b_0 modulo 2^{L0}.

CW(A+B modulo 2^{L0+L1}) est donc égal à $K_1(Y)+K_0(R_0)$. Pour l'obtenir à partir de CW(A) et CW(B), on calcule, avec les tables introduites ci-avant :

$K_0(R_0)$ = ADD-K_0[K_0(a_0) , K_0(b_0)]

$K_1(C_0)$ = REM-K_0[K_0(a_0) , K_0(b_0)]

$K_1(R_1)$ = ADD-K_1[K_1(a_1) , K_1(b_1)]

$K_1(Y)$ = ADD-K_1[C_0 , R_1]

On a alors CW((A+B) modulo 2^{L0+L1}) = $K_1(Y)||K_0(R_0)$.

Dans le cas où les fonctions de chiffrement sont des fonctions linéaires, cette étape d'adaptation pour l'exploitation ou le décodage des mots de code peut par

exemple être réalisée en décomposant le mot de code M en les mots de code partiels $m_1,\ldots, m_m$ qui le composent, et en réalisant l'opération sur chacun des mots de code partiels avant de concaténer les résultats obtenus.

Dans le cas d'une fonction à plusieurs opérandes, chaque mot de code sur lequel l'opération est mise en œuvre est décomposé en ses mots de codes partiels, et l'opération est appliquée de façon séparée sur les mots de codes partiels correspondants de chaque mot de code.

Ainsi par exemple, la mise en œuvre d'une opération de type « ou exclusif » (XOR) sur deux données codées comprend la mise en œuvre d'opérations « ou exclusifs » sur chaque mot de code partiel.

Avec la même notation que précédemment, on note XOR-K_0 la fonction ou exclusif appliquée à deux données concaténées, codés par K_0, et qui renvoie leur XOR en représentation codée par K_0. De même avec XOR-K_1 qui s'applique à des données codées par K_1 et renvoie leur XOR en représentation codée par K_1.

$XOR\text{-}K_0[K_0(a),K_0(b)] = K_0\ [a\ XOR\ b]$

Le résultat de A XOR B sous forme codée est donc calculé de la manière suivante :

$R_0 = XOR\text{-}K_0\ [K_0\ (a_0)\ ,\ K_0\ (b_0)]$

$R_1 = XOR\text{-}K_1\ [K_1\ (a1)\ ,\ K_1\ (b_1)]$

$R = R_1\ ||\ R_0.$

R est bien de la même forme que CW(A) et CW(B), c'est-à-dire la concaténation de deux mots de code codés respectivement par K_1 et K_0.

Dans le cas présent, les tableaux pré calculés présentent des tailles adaptées à celles des mots de code partiels utilisés pour les opérations arithmétiques. A titre d'exemple non limitatif, pour des mots de code M de type 2,5-1,3-2,5-code, sur lesquels on souhaite réaliser une opération « ou exclusif », on précalcule deux tables de type « A XOR B », une pour A et B de poids de Hamming 2 sur une taille de 5 bits, et une pour A et B de poids de Hamming 1 sur une taille de 3 bits.

De la même manière, si l'unité de traitement veut décoder les mots de code, elle sépare chaque mot de code M en les mots de code partiels $m_1,\ldots,m_m$, et met en œuvre sur chaque mot de code partiel un décodage correspondant à l'encodage mis en œuvre pour les obtenir. L'algorithme de décodage dépend bien entendu de l'algorithme d'encodage utilisé au préalable.

A titre d'exemples non limitatifs, on décrit ci-après d'autres possibilités d'encodage et de décodage dans le cadre du procédé décrit ci-avant.

Selon un premier exemple, on cherche à coder des données d'un ensemble de départ E contenant les entiers de 0 à 15, c'est-à-dire les entiers binaires représentés sur 4 bits.

On choisit comme code d'arrivée l'ensemble des mots de poids 3 parmi 6 bits, qui est le suivant : {7, 11, 13, 14, 19, 21, 22, 25, 26, 28, 35, 37, 38, 41, 42, 44, 49, 50, 52, 56}. Cet ensemble comporte 20 éléments ; il est donc adapté pour coder l'ensemble E qui en contient 16. On note J l'ensemble des 16 premiers éléments du code précédent. En binaire J= [111, 1011, 1101, 1110, 10011, 10101, 10110,11001, 11010, 11100, 100011, 100101, 100110, 101001, 101010, 101100].

A l'élément E[a] (« a-ième » élément de E) est associé l'élément J[a].

Si la table J est conservée en mémoire, alors on obtient le procédé de codage, qui est un simple accès à un tableau. Un mot « a » se code en accédant en mémoire à la valeur J[a].

Pour décoder, on crée la table K, de taille 2^6 éléments (=64), qui à l'emplacement J[i], i allant de 0 à 15, prendra la valeur de i.

On a alors K[J[i]]=i, donc le décodage du mot de code de « i » permet bien d'obtenir « i » lui-même.

La table K s'écrit alors [X, X, X, X, X, X, X, 0, X, X, X, 1, X, 2, 3, X, X, X, X, 4, X, 5, 6, X, X, 7, 8, X, 9, X, X, X, X, X, X, 10, X, 11, 12, X, X, 13, 14, X, 15, X, X, X, X, X, X, X, X, X, X, X, X, X, X, X, X, X, X, X, X], où X est une valeur qui n'est pas dans l'ensemble E de départ.

Pour un mot de 8 bits M que l'on souhaite coder, ce mot est scindé en deux séquences de 4 bits chacune, codées chacune sur 6 bits comme décrit précédemment, puis on concatène les mots de code partiels obtenus.

Pour les opérations sur le mot de code, on prépare une table qui reçoit en entrée les mots de code partiels et fournit en sortie le résultat de l'opération appliquée à la concaténation des mots de code partiels.

D'autres possibilités d'encodage et de décodage des données applicables dans le cadre de la présente invention sont connues et à la portée de l'Homme du Métier.

REVENDICATIONS

1. Procédé de traitement de données, comprenant l'encodage d'une pluralité de données (D) de n bits en des mots de code (M) présentant un poids de Hamming constant prédéfini,
le procédé étant caractérisé en ce qu'il comprend en outre la mise en œuvre (4000) d'opérations de chiffrement ou d'opérations arithmétiques sur le ou les mots de code obtenus, et en ce que l'encodage de chaque donnée (D) comprend :
- la décomposition (100) de la donnée en une pluralité de m séquences de bits ($d_1,\ldots,d_m$) à coder, m étant strictement inférieur à n,
- le codage (300) de chaque séquence de bits en un mot de code partiel présentant chacun un poids de Hamming prédéfini, de sorte que la somme des poids de Hamming des mots de code partiels ($m_1,\ldots,m_m$) soit égale au poids de Hamming du mot de code (M), et
- la concaténation (300) des mots de code partiels ($m_1,\ldots,m_m$) pour obtenir le mot de code (M) correspondant à la donnée (D).

2. Procédé de traitement selon la revendication 1, dans lequel la taille du mot de code obtenu est strictement inférieure à 2n bits.

3. Procédé de traitement selon l'une des revendications 1 ou 2, dans lequel la taille n des données (D) est une puissance de 2 bits.

4. Procédé de traitement selon l'une des revendications précédentes, dans lequel la taille des séquences de bits ($d_1,\ldots,d_m$) est une puissance de 2 bits.

5. Procédé de traitement selon l'une des revendications précédentes, dans lequel les données (D) comprennent 4 bits, chaque donnée étant décomposée en une séquence de 3 bits, et une séquence d'un bit, la première séquence étant codée en un mot de code partiel de taille 5 bits et de poids de Hamming égal à 2 ou 3, et le bit restant étant codé en un mot de code partiel de taille 2 bits et de poids de Hamming égal à 1.

6. Procédé de traitement selon l'une des revendications 1 à 4, dans lequel les données comprennent 8 bits, le procédé comprenant la décomposition de chaque donnée en deux séquences de 4 bits, les deux séquences de 4 bits étant codées en deux mots de code partiels de 6 bits et de poids de Hamming égal à 3.

7. Procédé de traitement de données selon l'une des revendications précédentes, l'encodage (1000) étant mis en œuvre par la première unité de traitement (12), le procédé comprenant en outre la transmission (2000) à la seconde unité de traitement (22) d'au moins un mot de code (M) obtenu à partir de la ou les données (D) et les opérations de chiffrement ou les opérations arithmétiques étant mises en œuvre sur ledit au moins un mot de code (M) par la seconde unité de traitement (22).

8. Procédé de traitement de données selon la revendication précédente, comprenant en outre la vérification (3000), par la seconde unité de traitement (22), de la valeur du poids de Hamming du mot de code reçu.

9. Procédé de traitement de données selon l'une des revendications précédentes, dans lequel la mise en œuvre des opérations arithmétiques ou les opérations de chiffrement est réalisée sur au moins un mot de code, et produit en sortie le résultat codé de l'opération appliquée à la donnée correspondant au mot de code.

10. Procédé de traitement de données selon l'une des revendications précédentes, dans lequel les opérations arithmétiques ou les opérations de chiffrement comprennent des opérations linéaires appliquées sur au moins un mot de code, et la mise en œuvre d'une opération linéaire comprend :

- la génération d'au moins une table prenant en entrée au moins un mot de code partiel, et produisant en sortie le résultat de l'opération appliquée au(x) mot(s) de code partiel(s),
- la décomposition de chaque mot de code sur lequel l'opération est mise en œuvre en mots de code partiels, et
- le calcul de l'opération par application des mots de code partiels aux tables, et la concaténation des résultats obtenus.

11. Procédé de traitement de données selon l'une des revendications 1 à 9, dans lequel les opérations arithmétiques ou les opérations de chiffrement sont non-linéaires, et la mise en œuvre d'une opération non linéaire comprend :

- la génération d'au moins une table prenant en entrée au moins un mot de code partiel d'au moins un mot de code, et produisant en sortie le résultat codé de l'opération appliquée à au moins une donnée complète dont sont tirés les mots de codes partiels,
- la décomposition de chaque mot de code sur lequel l'opération est mise en œuvre en mots de code partiels, et
- le calcul de l'opération par application des mots de code partiels aux tables.

12. Procédé de traitement de données selon l'une des revendications précédentes, dans lequel les opérations de chiffrement ou les opérations arithmétiques sont des étapes de traitement d'algorithmes cryptographiques, d'algorithmes de calcul de fonctions de hachage, ou d'algorithmes de calcul d'intégrité adaptés pour recevoir en entrée lesdits mots de code.

13. Circuit électronique comprenant un module d'encodage (10) comportant une unité de traitement (12) adaptée pour encoder des données de n bits en des mots de code présentant un poids de Hamming constant prédéfini et pour mettre en œuvre sur lesdits mots de code des opérations de chiffrement ou des opérations arithmétiques par la mise en œuvre du procédé selon l'une des revendications 1 à 12.

14. Circuit électronique selon la revendication 13, dans lequel le module d'encodage (10) comporte en outre des moyens de transmission de données (11), et le circuit comprend en outre :

- un module de décodage (20) comportant une unité de traitement (22) adaptée pour décoder un mot de code transmis par le premier module, et
- un module de génération de signal d'erreur (30), adapté pour générer un signal d'erreur lorsque le poids de Hamming d'un mot de code transmis par le premier module est différent d'un poids de Hamming prédéfini.

15. Carte à puce (1) comportant un circuit électronique selon l'une des revendications 13 ou 14.

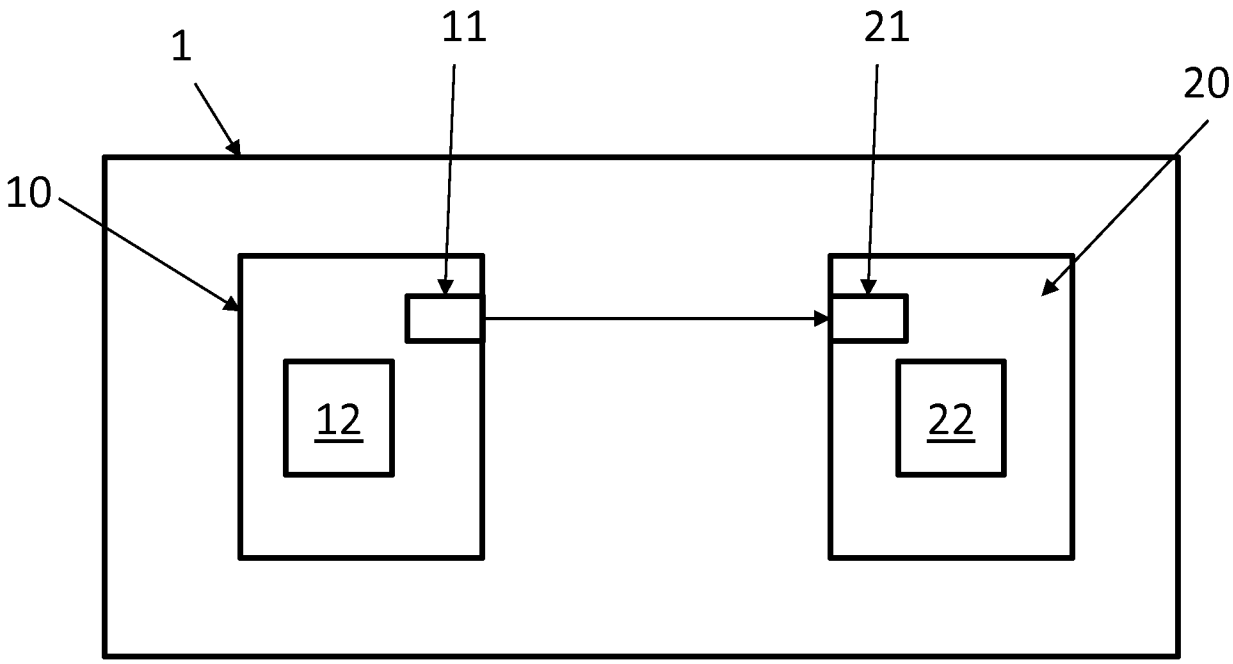
1
11
21
20
10
12
22

FIG.1

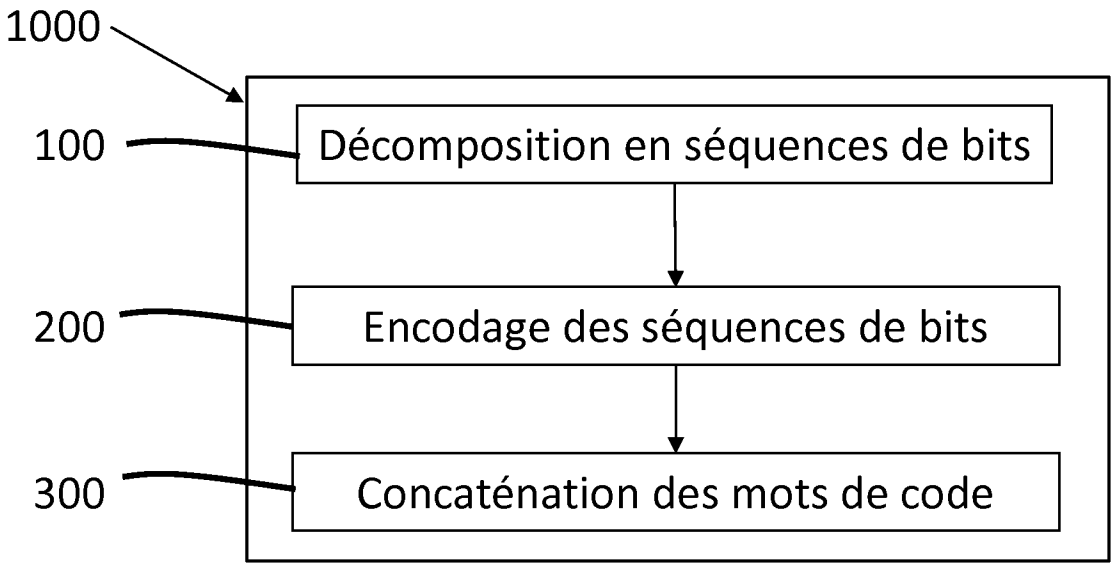
1000
100
Décomposition en séquences de bits
200
Encodage des séquences de bits
300
Concaténation des mots de code

FIG.2

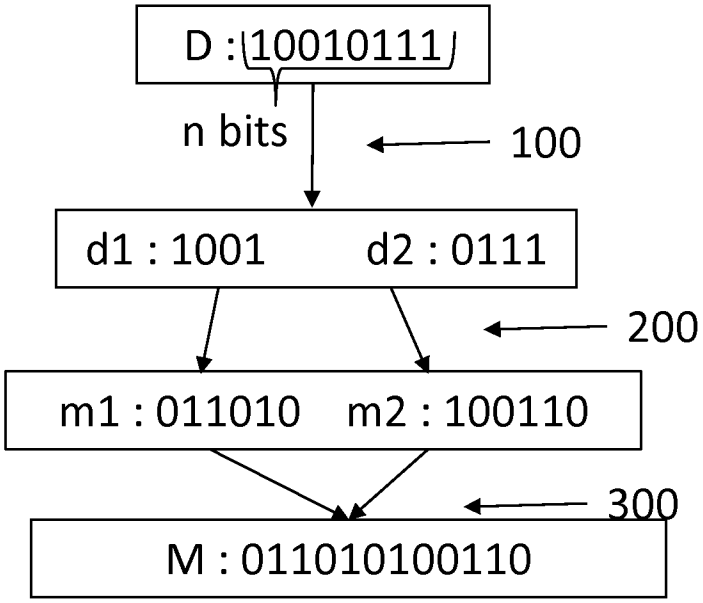
D : 10010111
n bits
100
d1 : 1001
d2 : 0111
200
m1 : 011010
m2 : 100110
300
M : 011010100110

FIG. 3

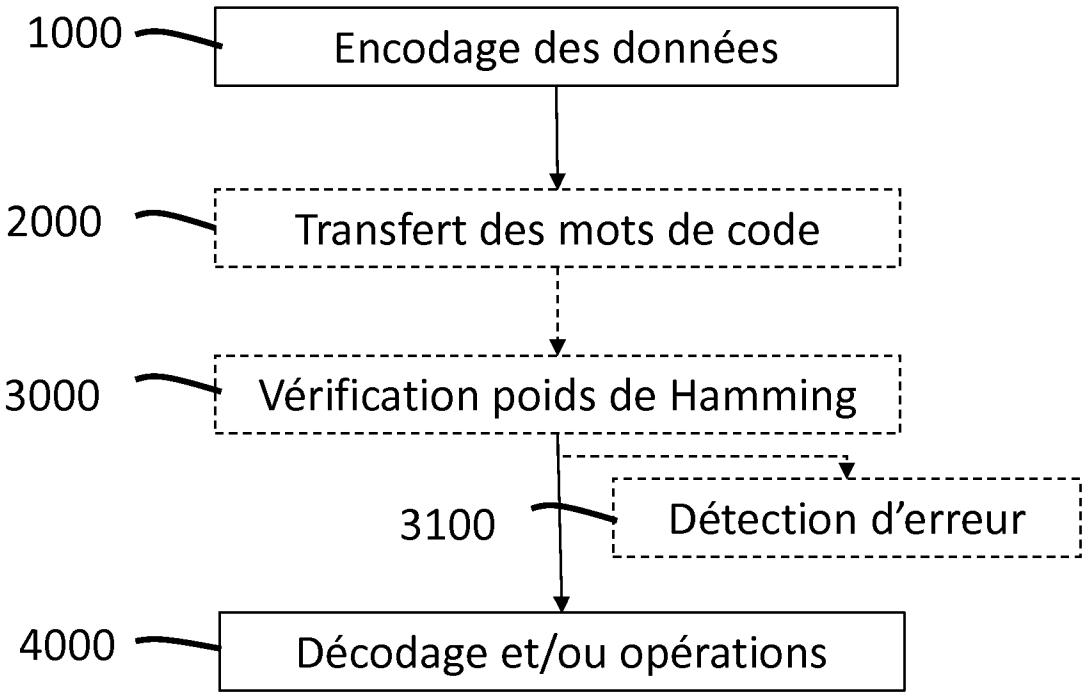
1000
Encodage des données
2000
Transfert des mots de code
3000
Vérification poids de Hamming
3100
Détection d'erreur
4000
Décodage et/ou opérations

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/050867

A. CLASSIFICATION OF SUBJECT MATTER
INV. H03M7/20 G06K19/07 G06F11/08
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H03M G06K G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GYORI S: "Signature coding over multiple access or channel", INFORMATION THEORY WORKSHOP, 2003. PROCEEDINGS. 2003 IEEE 31 MARCH - 4 APRIL 2003, PISCATAWAY, NJ, USA,IEEE, 31 March 2003 (2003-03-31), pages 115-118, XP010647723, ISBN: 978-0-7803-7799-8 page 1294 - page 1297; tables I-III	1-15
X	US 6 844 833 B2 (CORNELIUS WILLIAM P [US] ET AL) 18 January 2005 (2005-01-18) column 1 - column 2 column 5 - column 17	1-15

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 March 2014	07/04/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Belardinelli, Carlo

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/050867

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MAO-CHAO LIN: "CONSTANT WEIGHT CODES FOR CORRECTING SYMMETRIC ERRORS AND DETECTINGUNIDIRECTIONAL ERRORS", IEEE TRANSACTIONS ON COMPUTERS, IEEE SERVICE CENTER, LOS ALAMITOS, CA, US, vol. 42, no. 11, 1 November 1993 (1993-11-01), pages 1294-1302, XP000418192, ISSN: 0018-9340, DOI: 10.1109/12.247835 the whole document	1-15
A	WO 2004/105304 A1 (GEMPLUS CARD INT [FR]; BRIER ERIC [FR]; FOURNIER JACQUES [FR]; MOITREL) 2 December 2004 (2004-12-02) the whole document & FR 2 855 286 A1 (GEMALTO SA) 26 November 2004 (2004-11-26) cited in the application	1-15
A	WO 2010/049276 A1 (IBM [US]; HARVEY MIKE [GB]) 6 May 2010 (2010-05-06) the whole document	1-15
A	US 2008/212776 A1 (MOTOYAMA MASAHIKO [JP]) 4 September 2008 (2008-09-04) paragraph [0001] - paragraph [0102] paragraph [0170] - paragraph [0178]	1-15

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2014/050867

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6844833 B2	18-01-2005	JP 4617039 B2	19-01-2011
		JP 2002261618 A	13-09-2002
		US 2002118126 A1	29-08-2002
		US 2004113650 A1	17-06-2004
		US 2004135709 A1	15-07-2004
		US 2005122823 A1	09-06-2005
WO 2004105304 A1	02-12-2004	CN 1792059 A	21-06-2006
		EP 1629625 A1	01-03-2006
		FR 2855286 A1	26-11-2004
		US 2007055868 A1	08-03-2007
		WO 2004105304 A1	02-12-2004
WO 2010049276 A1	06-05-2010	NONE	
US 2008212776 A1	04-09-2008	JP 5203594 B2	05-06-2013
		JP 2008118566 A	22-05-2008
		US 2008212776 A1	04-09-2008

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2014/050867

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H03M7/20 G06K19/07 G06F11/08
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H03M G06K G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	GYORI S: "Signature coding over multiple access or channel", INFORMATION THEORY WORKSHOP, 2003. PROCEEDINGS. 2003 IEEE 31 MARCH - 4 APRIL 2003, PISCATAWAY, NJ, USA,IEEE, 31 mars 2003 (2003-03-31), pages 115-118, XP010647723, ISBN: 978-0-7803-7799-8 page 1294 - page 1297; tableaux I-III	1-15
X	US 6 844 833 B2 (CORNELIUS WILLIAM P [US] ET AL) 18 janvier 2005 (2005-01-18) colonne 1 - colonne 2 colonne 5 - colonne 17	1-15

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
31 mars 2014	07/04/2014

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Belardinelli, Carlo

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2014/050867

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	MAO-CHAO LIN: "CONSTANT WEIGHT CODES FOR CORRECTING SYMMETRIC ERRORS AND DETECTINGUNIDIRECTIONAL ERRORS", IEEE TRANSACTIONS ON COMPUTERS, IEEE SERVICE CENTER, LOS ALAMITOS, CA, US, vol. 42, no. 11, 1 novembre 1993 (1993-11-01), pages 1294-1302, XP000418192, ISSN: 0018-9340, DOI: 10.1109/12.247835 le document en entier	1-15
A	WO 2004/105304 A1 (GEMPLUS CARD INT [FR]; BRIER ERIC [FR]; FOURNIER JACQUES [FR]; MOITREL) 2 décembre 2004 (2004-12-02) le document en entier & FR 2 855 286 A1 (GEMALTO SA) 26 novembre 2004 (2004-11-26) cité dans la demande	1-15
A	WO 2010/049276 A1 (IBM [US]; HARVEY MIKE [GB]) 6 mai 2010 (2010-05-06) le document en entier	1-15
A	US 2008/212776 A1 (MOTOYAMA MASAHIKO [JP]) 4 septembre 2008 (2008-09-04) alinéa [0001] - alinéa [0102] alinéa [0170] - alinéa [0178]	1-15

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2014/050867

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 6844833 B2	18-01-2005	JP 4617039 B2	19-01-2011
		JP 2002261618 A	13-09-2002
		US 2002118126 A1	29-08-2002
		US 2004113650 A1	17-06-2004
		US 2004135709 A1	15-07-2004
		US 2005122823 A1	09-06-2005
WO 2004105304 A1	02-12-2004	CN 1792059 A	21-06-2006
		EP 1629625 A1	01-03-2006
		FR 2855286 A1	26-11-2004
		US 2007055868 A1	08-03-2007
		WO 2004105304 A1	02-12-2004
WO 2010049276 A1	06-05-2010	AUCUN	
US 2008212776 A1	04-09-2008	JP 5203594 B2	05-06-2013
		JP 2008118566 A	22-05-2008
		US 2008212776 A1	04-09-2008