(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
21 juin 2018 (21.06.2018)

WIPO IPCT

(10) Numéro de publication internationale
WO 2018/109346 Al

(51) Classification internationale des brevets :
H03M 13/15 (2006.01) *G06F 7/72* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2017/053495

(22) Date de dépôt international :
11 décembre 2017 (11.12.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1662324 12 décembre 2016 (12.12.2016) FR

(71) Déposant : INSTITUT SUPERIEUR DE L'AERONAUTIQUE ET DE L'ESPACE [FR/FR] ; 10 Avenue Edouard Belin, BP 54031, 31055 TOULOUSE CEDEX (FR).

(72) Inventeurs : DETCHART, Jonathan ; 25 avenue du parc, 31140 AUCAMVILLE (FR). LACAN, Jérôme ; 6, rue du professeur Joseph Anglade, 31500 TOULOUSE (FR). LOCHIN, Emmanuel ; 23, rue Dordogne, 31200 TOULOUSE (FR).

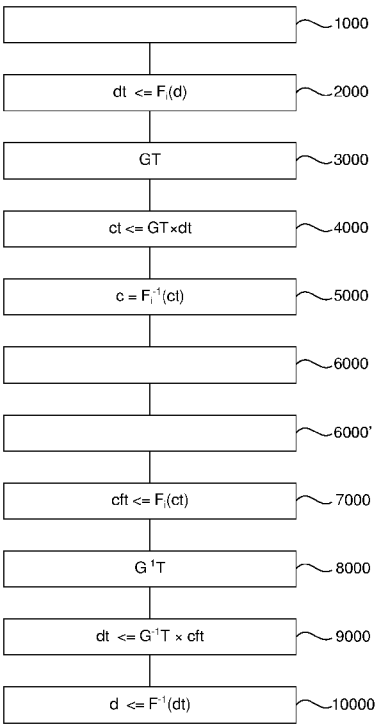
(74) Mandataire : GEVERS & ORES ; 9 Rue Saint Antoine du T, 31000 TOULOUSE (FR).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR,

(54) Title: ERROR CORRECTION CODING AND DECODING BY A GENERATOR MATRLX WITH SIMPLIFIED GALOIS FIELD MULTIPLICATIONS

(54) Titre : CODAGE ET DÉCODAGE CORRECTEUR D'ERREURS PAR MATRICE GÉNÉRATRICE AVEC MULTIPLICATIONS SIMPLIFIÉES DANS COPRS DE GALOIS

Fig.2



(57) Abstract: Method for encoding a data vector into a transformed encoded vector according to a linear error correction code defined by a generator matrix (G), wherein: - the data vector and the generator matrix (G) are in the imite field of polynomials defined by: B;=GF2(x)/(P;(x)), p,(x) being an irreducible polynomial which divides the polynomial x^n+l, i and n being integers, - the transformed encoded vector belonging to a ring and being the image, obtained through an isomorphism, of the product of the generator matrix (G) multiplied by the data vector, the isomorphism of the finite field B in a set A; being defined by: F;, (ρ(χ))=ρ(χ)0_i(χ); where A; is the

WO 2018/109346 A1

[Suite sur la page suivante]

KW, KZ, LA, LC, LK, LR, LS, 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, ST, 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).

Publiée:

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

principal idéal of the ring generated by the polynomial χη+1/ρ,(χ), Q,(x) is the unique idempotent of said principal idéal, and p(x) is a polynomial belonging to the field B, the ring being defined by: R2,n= GF2(x)/(x^n+l), said method comprising: - a step to calculate the image through the isomorphism F of the data vector to obtain a transformed data vector, - a step to détermine a transformed matrix, wherein each élément located in a row and in a column is the sum of the image of the élément located in said row and in said column of a raw matrix (G), obtained through the isomorphism F, and of an élément of the ring which has no component in the principal idéal, the raw matrix (G) being the generator matrix (G), - a step to multiply the transformed matrix by the transformed data vector to obtain said transformed encoded vector.

(57) Abrégé : Procédé d'encodage d'un vecteur de donnée en un vecteur encodé transformé, selon un code correcteur d'erreur linéaire défini par une matrice génératrice (G), dans lequel : - le vecteur de donnée et la matrice génératrice (G) sont dans le corps fini de polynômes défini par : B;=GF2(x)/(P;(x)), p,(x) étant un polynôme irréductible qui divise le polynôme x^n+l, i et n étant des entiers, - Le vecteur encodé transformé appartenant à un anneau et image par un isomorphisme du produit de la matrice génératrice (G) par le vecteur de donnée, l'isomorphisme, du corps fini B, dans un ensemble A;, étant défini par : F;, (ρ(χ))=ρ(χ)0_i(χ); où A;, est l'idéal principal de l'anneau engendré par le polynôme χη+1/ρ,(χ), Q,(x) est l'unique idempotent dudit idéal principal, et p(x) un polynôme appartenant au corps B„ l'anneau étant défini par : R2,n= GF2(x)/(x^n+l) ledit procédé comprenant : - une étape de calcul de l'image par l'isomorphisme F, du vecteur de donnée pour obtenir un vecteur de donnée transformé, - une étape de détermination d'une matrice transformée, dans laquelle chaque élément situé à une ligne et à une colonne est la somme de l'image de l'élément situé à ladite ligne et à ladite colonne d'une matrice brute (G) par l'isomorphisme F, et d'un élément de l'anneau qui n'a aucune composante dans l'idéal principal, la matrice brute (G) étant la matrice génératrice (G), - une étape de multiplication de la matrice transformée par le vecteur de donnée transformée pour obtenir ledit vecteur encodé transformé.

CODAGE ET DÉCODAGE CORRECTEUR D'ERREURS PAR MATRICE GÉNÉRATRICE AVEC MULTIPLICATIONS SIMPLIFIÉES DANS COPRS DE GALOIS

1. Domaine technique de l'invention

L'invention concerne les codes correcteurs qui permettent la correction d'erreurs dans des données, par exemple suite à leur stockage ou à leur transmission. Elle concerne en particulier les codes correcteurs linéaires définis par une matrice génératrice G d'éléments d'un corps fini. Dans un tel code correcteur, l'encodage d'un vecteur de donnée d de z éléments d'un corps fini en un vecteur encodé c de t éléments de ce corps fini, t>z, est obtenu par la multiplication de la matrice génératrice G (de t lignes et z colonnes) par le vecteur de donnée d (c=G x d, ou alors c=d x G).

En particulier, le code correcteur peut être un code systématique, c'est-à-dire, dans lequel les z premiers éléments du vecteur encodé c sont identiques aux z éléments du vecteur de donnée d. Dans ce cas, la notion de matrice génératrice peut omettre les z premières lignes qui constituent une matrice identité, et la notion de vecteur encodé peut omettre z premiers éléments du vecteur encodé identiques aux z éléments du vecteur de donnée d.

En cas d'erreur lors du stockage ou de la transmission d'un vecteur encodé c, on dispose alors d'un vecteur à corriger cf, identique au vecteur encodé c sauf pour les éléments de c qu'on sait erronés, situés à un indice dit « erroné » de cf et qui, dans la suite, sont supprimés de cf (typiquement une liste des indices erronés est mémorisée en plus des éléments du vecteur). Pour retrouver le vecteur de donnée d à partir du vecteur à corriger cf, on multiplie l'inverse de la matrice génératrice (dans le cas d'un code systématique, il faut inverser la matrice génératrice définie comme comprenant les z premières lignes qui constituent une matrice identité) duquel on a supprimé les lignes de numéros identiques aux indices erronés de cf.

2. Inconvénients de l'état de la technique

Dans le cas où le volume des données à encoder ou à décoder est important, les

multiplications précitées entre un vecteur et une matrice nécessaires à l'encodage ou au décodage peuvent exiger des temps ou des ressources de calculs prohibitifs.

3. Définitions

On utilise, dans la suite, des objets et des notations classiques pour l'homme de métier. Toutefois, certaines définitions sont rappelées ci-après.

Soit $GF_2(x)$ l'anneau des polynômes à coefficients binaires. Soit $((x^n+1))$ l'anneau engendré par le polynôme x^n+1, où n entier. Soit $(p_i(x))$ l'anneau engendré par un polynôme irréductible $p_i(x)$ de degré w qui divise le polynôme x^n+1, où i entier (i.e. : $(Pi(x))$ est l'ensemble des multiples de $p_i(x)$).

On note $B_i = GF_2(x)/(Pi(x))$, le corps constitué par le quotient entre l'anneau $GF_2(x)$ et l'anneau engendré par le polynôme irréductible $p_i(x)$ de degré w.

On note $R_{2,n} = GF_2(x)/(x^n+1)$, l'anneau constitué par le quotient entre l'anneau $GF_2(x)$ et l'anneau engendré par le polynôme x^n+1.

On définit également l'ensemble A_i comme l'idéal principal de l'anneau R_{2n} engendré par le polynôme $\chi^n+1/\rho_i(\chi)$ (i.e. : un idéal principal d'un anneau est un sous-groupe additif généré par un seul élément et qui possède la propriété d'absorber la multiplication). On sait que chaque élément de l'anneau $R_{2,n}$ peut s'exprimer sous la forme d'une somme de composantes (autrement dit d'éléments de l'anneau) où chacune des composantes est dans un idéal principal différent de l'anneau $R_{2,n}$. On sait que pour tout idéal A_i, il existe 2^{n-w} éléments, comprenant l'élément nul de l'anneau R_{2n} (i.e. : noté 0, autrement dit l'élément neutre additif) qui n'ont n'aucune composante dans l'idéal A_i.

On rappelle qu'un idempotent est un élément e(x) (ici un polynôme) tel que $e(x)*e(x)=e(x)$. A_i a un unique idempotent.

De manière classique, on dit par extension que le vecteur $i=(i_1,i_2, \ldots i_r, \ldots i_k)$ est l'image par

un isomorphisme I d'un vecteur $o=(\theta_1,o_2, \ldots o_r, \ldots o_k)$, lorsque $i_r = I(o_r)$, quel que soit i appartenant à {1,2, ...,k) (autrement dit lorsque chaque élément du vecteur i d'un indice donné est l'image par l'isomorphisme I de l'élément du même indice dans le vecteur o).

On dit qu'on calcule l'image par l'isomorphisme I du vecteur o pour obtenir le vecteur i, lorsqu'on effectue, pour tout r appartenant à {1,2, ...,k), l'opération $i_r = I(o_r)$. Le résultat de ce calcul est le vecteur i (autrement dit chaque élément du vecteur i d'un indice donné est obtenu par le calcul de (et est égal à) l'image par l'isomorphisme I de l'élément de même indice dans le vecteur o).

On utilise des définitions analogues pour les matrices (« indice » est remplacé par « ligne et colonne »).

De manière classique, on dira qu'un vecteur ou une matrice est dans ou appartient à un ensemble si tous les éléments de ce vecteur ou de la matrice sont dans cet ensemble.

L'utilisation d'une représentation dite à base de XOR (XOR signifie : ou exclusif) est introduite dans l'article suivant : J. BLOEMER, M. KALFANE, M. KARPINSKI, R. KARP, M. LUBY AND D. ZUCKERMAN, D. "An XOR-Based Erasure-Resilient Coding Scheme" in Technical Report ICSI TR-95-048 (August 1995). Elle consiste à représenter chaque élément par une matrice carrée binaire où chaque nombre binaire de cette matrice carrée représente des opérations de XOR sur des nombres binaires à réaliser pour une multiplication avec cet élément (par exemple dans la multiplication d'un élément de la matrice avec un élément d'un vecteur).

Un polynôme est dit AOP (ou polynôme tout à un, ou en anglais « All One Polynomial ») lorsque les coefficients de tous ses monômes sont égaux à 1.

Un polynôme g(x) qui s'écrit $g(x) = x^{sr} + x^{s(r-1)} + x^{s(r-2)} + \ldots + x^s + 1 = p(x^s)$, où p(x) est un polynôme AOP de degré r, est dit ESP (ou polynôme uniformément espacé, ou en anglais « Equally Spaced Polynomial », s et r sont entiers bien entendu).

4. Exposé de l'invention

Pour remédier aux inconvénients précités, l'invention propose un procédé d'encodage d'un vecteur de donnée, en un vecteur encodé transformé, selon un code correcteur d'erreur linéaire défini par une matrice génératrice, dans lequel :

- le vecteur de donnée et la matrice génératrice sont dans le corps fini de polynômes,

noté B_i, défini de la manière suivante : $B_i = GF_2(x)/(Pi(x))$, $p_i(x)$ étant un polynôme irréductible qui divise le polynôme x^n+1, i et n étant des entiers,

- Le vecteur encodé transformé appartenant à l'anneau $R_{2,n}$, et est l'image par un isomorphisme, noté F_i, du produit de la matrice génératrice par le vecteur de donnée, l'isomorphisme F_i du corps fini B_i dans l'ensemble A_i, l'isomorphisme étant défini de la manière suivante : $F_i(p(x)) = p(x)\ Q_i(x)$, où A_i est l'idéal principal de l'anneau $R_{2,n}$ engendré par le polynôme $\chi^n+1/\rho_i(\chi)$, $Q_i(x)$ est l'unique idempotent dudit idéal principal A_i, et p(x) un polynôme appartenant au corps B_i, l'anneau étant défini de la manière suivante : $R_{2,n} = GF_2(x)/(x^n+1)$

ledit procédé comprenant les étapes suivantes :

- Une étape de calcul de l'image par l'isomorphisme F_i du vecteur de donnée pour obtenir un vecteur de donnée transformé,
- une étape de détermination d'une matrice transformée, dans laquelle chaque élément de la matrice transformée (ou plus généralement d'une partie de la matrice transformée comprenant un certain nombre de lignes de la matrice transformée) situé à une ligne et à une colonne est la somme de l'image de l'élément situé à ladite ligne et à ladite colonne d'une matrice brute par l'isomorphisme F_i et d'un élément de l'anneau $R_{2,n}$ qui n'a aucune composante dans l'idéal principal A_i, la matrice brute étant la matrice génératrice,
- une étape de multiplication de la matrice transformée par un vecteur transformé, le vecteur transformé étant le vecteur de donnée transformée, pour obtenir ledit vecteur encodé transformé (ainsi donc le vecteur encodé transformé est le résultat de la multiplication de la matrice génératrice transformée par le vecteur de donnée transformé).

Dans un mode de réalisation du procédé d'encodage, le procédé comprend une étape de calcul de l'image par un isomorphisme inverse, noté F_i^{-1} , du vecteur encodé transformé pour obtenir un vecteur encodé, l'isomorphisme inverse F_i^{-1} étant l'inverse de l'isomorphisme F_i et est défini de la manière suivante : $p(x) = pn(x) \bmod p_i(x)$, pn(x) étant un polynôme de l'anneau $R_{2,n}$, le vecteur encodé étant égal au produit de la matrice génératrice par le vecteur de donnée. Ainsi donc, une fois l'étape de

multiplication réalisée, on peut faire repasser le résultat dans le corps B_i. En variante, le résultat peut rester dans l'anneau $R_{2,n}$ de manière à effectuer ultérieurement le décodage sans avoir à transformer le vecteur à corriger encodé vers l'anneau $R_{2,n}$.

Toujours pour remédier aux inconvénients précités, l'invention concerne aussi un procédé de décodage d'un vecteur à corriger transformé, en un vecteur de donnée selon un code correcteur d'erreur linéaire défini par une matrice génératrice, ledit vecteur à corriger comprenant une pluralité d'indices erronés comprenant un élément erroné (autrement dit, comprenant une pluralité d'éléments erronés situés à des indices erronés) dans lequel :

- le vecteur de donnée et la matrice génératrice sont dans le corps fini B_i, défini de la manière suivante : $B_i = GF_2(x)/(Pi(x))$, $p_i(x)$ étant un polynôme irréductible qui divise le polynôme x^n+1, i et n étant des entiers,
- Le vecteur à corriger transformé appartenant à l'anneau $R_{2,n}$, défini de la manière suivante : $R_{2,n} = GF_2(x)/(x^n+1)$

ledit procédé comprenant les étapes suivantes :

- une étape de détermination d'une matrice transformée, chaque élément de la matrice transformée (ou plus généralement d'une partie de la matrice transformée comprenant un certain nombre de lignes de la matrice transformée) situé à une ligne et à une colonne est la somme de l'image de l'élément situé à ladite ligne et à ladite colonne d'une matrice brute par l'isomorphisme F_i et d'un élément de l'anneau $R_{2,n}$ qui n'a aucune composante dans l'idéal principal A_i, la matrice brute étant l'inverse de la matrice génératrice de laquelle sont supprimées les lignes correspondantes à ladite pluralité d'indices erronés , l'isomorphisme F_i, du corps fini B_i dans un ensemble A_i, étant défini de la manière suivante : $F_i(p(x)) = p(x)\, Q_i(x)$, où A_i est l'idéal principal engendré par le polynôme $\chi^n+1/\rho_i(\chi)$ de l'anneau $R_{2,n}$, $Q_i(x)$ est l'unique idempotent dudit idéal principal A_i, et p(x) un polynôme appartenant au corps B_i,
- une étape de multiplication de la matrice transformée par un vecteur transformé, le vecteur transformé étant le vecteur à corriger transformé, pour obtenir un vecteur de donnée transformé.
- une étape de calcul de l'image par un isomorphisme inverse, noté F_i^{-1}, du vecteur de donnée transformé pour obtenir le vecteur de donnée, l'isomorphisme inverse F_i^{-1} étant

l'inverse de l'isomorphisme F_2 et est défini de la manière suivante :
$p(x) = pn(x) \bmod p_1(x)$, $pn(x)$ étant un polynôme de l'anneau $R_{2,n}$.

Dans un mode de réalisation du procédé de décodage, le procédé comprend, préalablement à l'étape de multiplication, une étape de calcul de l'image par l'isomorphisme F_2 d'un vecteur à corriger pour obtenir le vecteur à corriger transformé, le vecteur de donnée étant égal au produit de l'inverse de la matrice génératrice de laquelle sont supprimées les lignes de même numéro que ladite pluralité d'indices erronés, par le vecteur à corriger. Dans ce cas, le procédé de décodage est compatible avec un procédé d'encodage où le résultat de l'étape de multiplication est repassé dans le corps B_1.

On présente ci-dessous des avantages et des caractéristiques optionnelles communes à la fois au procédé d'encodage et au procédé de décodage.

En réalisant ainsi l'étape de multiplication dans l'anneau $R_{2,n}$ où les multiplications entre éléments peuvent être plus rapides que dans le corps B_1, l'invention permet d'accélérer l'étape de multiplication.

Selon l'invention (décodage ou encodage), l'élément de l'anneau $R_{2,n}$ qui n'a aucune composante dans l'idéal principal A_1 peut soit être nul, soit être non nul. Dans le cas où il est nul, l'élément de la matrice transformée est l'image de l'élément situé à la même ligne et à la même colonne d'une matrice brute (G) par l'isomorphisme F_1.

Lorsque tous les éléments de la matrice transformée sont dans ce cas, la matrice transformée est l'image de la matrice brute par l'isomorphisme F_1.

En variante, au moins un des éléments de la matrice transformée situé à une ligne et à une colonne est la somme de l'image de l'élément situé à ladite ligne et à ladite colonne de la matrice brute par l'isomorphisme F_2 et d'un élément de l'anneau $R_{2,n}$ non nul qui n'a aucune composante dans l'idéal principal A_1. Ainsi donc, l'élément de l'anneau $R_{2,n}$ (nul ou pas), qui n'a aucune composante dans l'idéal principal A_1, peut être choisi de manière à minimiser le nombre de XOR engendrés par l'élément de la matrice transformée ainsi formé dans une multiplication avec un autre élément (dans une représentation dite à base de XOR, il s'agit de la quantité de nombres binaires égaux à 1

dans la représentation de cet élément de la matrice transformée).

Cela permet ainsi de réduire le temps ou les ressources nécessaires à l'étape de multiplication.

Dans un mode de réalisation, le procédé d'encodage ou le procédé de décodage est mis en œuvre dans une représentation dite à base de ou exclusif dans laquelle chaque élément de la matrice transformée est représenté par une matrice carrée élémentaire de n lignes et n colonnes de nombres binaires.

Selon une mise œuvre particulière de ce mode de réalisation, ledit chaque élément est mémorisé sous la forme d'une seule de ces n lignes ou n colonnes, la matrice transformée étant ainsi mémorisée sous la forme d'une matrice transformée compressée constituée de la seule des n lignes ou n colonnes de chaque élément de la matrice transformée.

Grâce au passage dans l'anneau $R_{2,n}$, dans une représentation à base de XOR, les éléments de la matrice transformée n'ont que des diagonales constituées soit que de 1, soit que de 0. C'est pourquoi, on peut se permettre de ne mémoriser qu'une seule ligne ou qu'une seule colonne pour chaque élément. On économise ainsi de l'espace mémoire.

Dans un mode de réalisation (à la fois pour le procédé de décodage et le procédé d'encodage), chaque élément du vecteur transformé est représenté par un vecteur élémentaire de n nombres binaires, ladite étape de multiplication de la matrice transformée par le vecteur transformé comprenant une sous-étape de multiplication de la matrice carrée élémentaire par le vecteur élémentaire, ladite sous-étape de multiplication comprenant les étapes suivantes :

- une étape de lecture en mémoire de ladite seule ligne ou seule colonne de la matrice carrée élémentaire dans la matrice transformée compressée,
- Une étape de traitement dans laquelle, pour chaque nombre binaire occupant une position de ladite une seule ligne ou seule colonne dans la matrice transformée compressée, si ledit bit est égal à une valeur déterminée (la valeur déterminée est souvent égale à 1. De manière générale, il s'agit d'une valeur qui définit un XOR qui peut

bien entendu être différente de 1 selon les implémentations), les ou exclusifs engendrés par toute la diagonale de la matrice carrée élémentaire déterminée par cette position sont calculés.

On réduit ainsi le temps de calcul nécessaire à la réalisation du procédé d'encodage ou du procédé de décodage puisqu'il suffit de ne lire qu'une seule ligne ou colonne par élément pour réaliser la sous-étape de multiplication.

Dans un mode de réalisation, le procédé d'encodage ou le procédé de décodage peut comprendre, préalablement à l'étape de multiplication, les étapes suivantes :

- une étape de détermination d'une sous partie identique comprenant we éléments binaires (ayant une valeur définissant un XOR. Classiquement cette valeur est 1) dans m lignes de la matrice transformée compressée, we supérieur ou égal à deux,
- une étape de calcul d'au moins un résultat intermédiaire à partir de ladite sous partie identique,
- l'étape de multiplication étant réalisée à partir du résultat intermédiaire de manière à éviter n.(we.m-(we+m)) opérations de ou exclusifs durant l'étape de multiplication.

En identifiant ainsi une sous-partie identique, on détermine des XOR communs intervenant dans une pluralité de sous-étapes de multiplication de manière à ne calculer ces XOR qu'une seule fois pour réaliser la pluralité de sous-étapes de multiplication.

Les sous-parties peuvent être alignées ou bien décalées cycliquement dans la matrice transformée. L'utilisation de la matrice transformée compressée permet en particulier de trouver des sous-parties décalées, la recherche de sous parties décalées étant trop complexe et trop longue dans le cas de l'utilisation d'une matrice transformée sans compression.

Le polynôme $p_i(x)$ peut être un polynôme AOP ou un polynôme ESP.

Dans ce cas, deux approches permettent un calcul rapide des images par l'isomorphisme F_i et l'isomorphisme inverse F_i^{-1}.

Selon une première approche :

- chaque élément du corps fini B_i étant représenté par un vecteur de données binaires
- le calcul de l'image de chaque élément du corps fini B_i par l'isomorphisme F_i comprend l'ajout d'un bit (ou donnée binaire) de parité audit vecteur de données binaires.
- le calcul de l'image de chaque élément du corps fini B_i par l'isomorphisme inverse F_i^{-1}

(inverse de l'isomorphisme F_i) comprend la suppression dudit bit de parité audit vecteur de données binaires.

Selon une deuxième approche :

- chaque élément du corps fini B_i étant représenté par un vecteur de données binaires
- le calcul de l'image de chaque élément du corps fini B_i par l'isomorphisme F_i comprend l'ajout d'une donnée binaire (ou bit) égale à l'élément nul (autrement dit, l'élément neutre additif) à une position dudit vecteur de données binaires.
- le calcul de l'image de chaque élément du corps fini B_i par l'isomorphisme inverse F_i^{-1} (inverse de l'isomorphisme F_i) comprend l'ajout de la donnée binaire située à ladite position à une pluralité de données binaires dudit vecteur de données binaires, puis la suppression de ladite donnée binaire située à ladite position dudit vecteur de données binaires.

L'invention concerne aussi un dispositif adapté à la mise en œuvre des étapes du procédé d'encodage ou de décodage.

L'invention concerne également :

- Un programme d'ordinateur comprenant des instructions adaptées à la mise en œuvre de chacune des étapes du procédé d'encodage ou du procédé de décodage lorsque ledit programme est exécuté sur un ordinateur, et
- Un moyen de stockage d'informations, amovible ou non, partiellement ou totalement lisible par un ordinateur ou un microprocesseur comportant des instructions de code d'un programme d'ordinateur pour l'exécution de chacune des étapes du procédé d'encodage ou du procédé de décodage.

On présente ci-dessous d'autres avantages et caractéristiques optionnelles du procédé d'encodage uniquement.

Selon un mode de réalisation, l'étape de détermination de la matrice transformée comprend les étapes suivantes :

- une étape pour engendrer une matrice candidate transformée,
- une étape pour estimer un nombre d'opérations de ou exclusif à réaliser pour l'étape de multiplication de la matrice transformée par le vecteur transformé, lorsque la

matrice candidate transformée est choisie en tant que matrice transformée,

- une étape pour déterminer, en fonction dudit nombre d'opérations de ou exclusif à réaliser, si la matrice candidate transformée est choisie en tant que matrice transformée.

De cette manière, on obtient la matrice transformée qui permet l'étape de multiplication la moins coûteuse possible en temps de calcul.

Selon une mise en œuvre particulière de ce mode de réalisation, la matrice candidate transformée peut être constituée d'éléments dans l'anneau $R_{2,n}$ qui sont, dans une représentation dite à base de XOR, des décalages cycliques de la matrice identité (de n lignes et n colonnes).

En particulier, le procédé d'encodage peut comprendre :

- durant l'étape pour estimer le nombre d'opérations de ou exclusif à réaliser pour l'étape de multiplication de la matrice transformée par le vecteur transformé , une étape de détermination d'une sous partie identique comprenant w éléments binaires dans m lignes de la matrice transformée compressée, w supérieurs ou égal à deux,
- une étape de calcul du nombre d'opérations de ou exclusif évités, égal à n.(we.m-(we+m)), à partir desdites sous parties, dans lequel le nombre d'opérations de ou exclusif à réaliser est estimé à partir dudit nombre d'opérations de ou exclusif évités.

On tient ainsi compte, dans le nombre d'opérations estimées, de la simplification des calculs effectuée grâce à la recherche des sous parties identiques.

Dans un premier mode de réalisation, la matrice candidate transformée est obtenue grâce aux étapes suivantes :

- une étape pour engendrer une matrice candidate génératrice définissant un code correcteur d'erreur qui est MDS (Maximum Distance Séparable).
- une étape de calcul de l'image par l'isomorphisme F_i de la matrice candidate génératrice pour obtenir la matrice candidate transformée .

En variante, la matrice candidate transformée est obtenue grâce aux étapes suivantes :

- une étape de calcul de l'image de la matrice candidate génératrice par l'isomorphisme inverse F_i^{-1} pour obtenir la matrice génératrice candidate,

-Une étape de vérification que la matrice génératrice candidate est MDS.

5. Liste des figures

D'autres buts, caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante donnée à titre uniquement non limitatif et qui se réfère aux figures annexées dans lesquelles :

- La figure 1 représente un dispositif adapté à la mise en œuvre du procédé de la figure 2.
- La figure 2 représente les étapes d'un procédé selon un mode de réalisation de l'invention.
- La figure 3 représente le détail d'une étape de la figure 2, dans un mode de réalisation.
- La figure 4 représente une étape de la figure 3 dans un mode de réalisation et la figure 5 représente cette même étape dans un deuxième mode de réalisation.
- La figure 6 présente en détail une étape de la figure 2 et la mémorisation de la matrice transformée.
- Les figures 7, 8, 9 et 10 donnent des exemples pour l'isomorphisme F_i et son inverse F_i^{-1}.

6. Description détaillée d'un mode de réalisation de l'invention

Les réalisations suivantes sont des exemples. Bien que la description se réfère à un ou plusieurs modes de réalisation, ceci ne signifie pas nécessairement que chaque référence concerne le même mode de réalisation, ou que les caractéristiques s'appliquent seulement à un seul mode de réalisation. De simples caractéristiques de différents modes de réalisation peuvent également être combinées pour fournir d'autres réalisations. Sur les figures, les échelles et les proportions ne sont pas

strictement respectées et ce, à des fins d'illustration et de clarté.

Le dispositif de figure 1 comprend une mémoire 200, des disques durs et 300 à 306 dans lesquels un microprocesseur 100 peut lire et écrire des données par l'intermédiaire d'un bus de données 400. La mémoire 200 (par exemple un disque amovible ou pas, ou bien une mémoire sous forme de circuit intégré (par exemple de type flash EEPROM)) comprend, dans une partie 250, les instructions de code d'un programme d'ordinateur pour l'exécution de chacune des étapes du procédé qui sera décrit en référence à la figure 2. Une entrée/sortie 500 est également connectée au microprocesseur 100 par l'intermédiaire du bus 400. D'autres architectures sont bien entendues possibles.

La figure 2 décrit les étapes réalisées par le microprocesseur 100 dans un mode de réalisation de l'invention. Le microprocesseur comprend une mémoire de travail (non représentée) utilisée dans les étapes du procédé ci-dessous.

A l'étape 1000, le microprocesseur 100 obtient le vecteur de donnée d par exemple en le recevant par l'entrée/sortie 500 et via le bus 400. Le vecteur de donnée d est constituée de z éléments (z étant bien évidemment un entier) du corps B_i défini plus haut.

A l'étape 2000, le microprocesseur 100 calcule l'image du vecteur d par l'isomorphisme F_i défini plus haut et mémorise le résultat dans le vecteur dt constitué de z éléments dans l'anneau $R_{2,n}$.

A l'étape 3000, une matrice transformée GT est obtenue par le microprocesseur 100. Chaque élément de cette matrice transformée GT situé à une ligne et à une colonne est la somme de l'image de l'élément situé à ladite ligne et à ladite colonne d'une matrice génératrice G par l'isomorphisme F_i et d'un élément de l'anneau $R_{2,n}$ qui n'a aucune composante dans l'idéal principal A_i défini plus haut.

De manière générale, dans un mode de réalisation, à l'étape 3000, la matrice transformée GT, peut être préalablement déterminée et mémorisée dans une mémoire, qui peut-être non volatile, par exemple, dans le mode de réalisation de la figure 2, dans la mémoire 200 ou dans la propre mémoire du processeur 100. La matrice transformée

GT est alors obtenue, par exemple par le processeur 100, par lecture de cette mémoire, pour l'encodage d'une pluralité de vecteurs. La figure 3 illustre un mode de réalisation pour prédéterminer la matrice transformée. En variante, la matrice transformée GT peut être recalculée à chaque fois que la matrice génératrice transformée est obtenue, par exemple en appliquant l'isomorphisme F_i défini plus haut à la matrice génératrice G elle-même mémorisée.

La matrice génératrice G est dans le corps B_i, et définit un code correcteur linéaire. Elle peut être constituée de t lignes et z colonnes (t supérieur à z, les z premières lignes de G peuvent constituer classiquement une matrice identité). La matrice génératrice transformée GT, dans l'anneau $R_{2,n}$, a naturellement le même nombre de lignes et de colonnes que la matrice génératrice G.

A l'étape 4000, on multiplie la matrice transformée GT par le vecteur de donnée dt. Le résultat de cette multiplication est le vecteur encodé transformé et constitué de t éléments dans l'anneau $R_{2,n}$.

A l'étape 5000, on applique l'isomorphisme inverse noté F_i^{-1} défini plus haut au vecteur encodé transformé et. Le résultat est un vecteur encodé c. le vecteur encodé c est égal au produit de la matrice génératrice G par le vecteur de données d, autrement dit au résultat de l'encodage du vecteur de donnée selon le code correcteur linéaire défini par la matrice génératrice G. Le vecteur encodé c comprend bien entendu t éléments du corps B_i.

A l'étape 6000, le vecteur encodé c est découpé en sept blocs de données (cbO, cb2, cb3, cb4, cb5, cb6) par le microprocesseur 100 qui mémorise chacun de ces sept blocs dans chacun des sept disques 300, 301, 302, 304, 305, 306. Ici le nombre sept pour le nombre de blocs et le nombre de disques est donné bien entendu à titre d'exemple, et peut-être quelconque. A l'étape 6000', le disque 302, par exemple, est hors service suite à un incident qui a lieu après que ces blocs aient été mémorisés à l'étape 6000. A titre d'exemple, cet incident a pour conséquence que le bloc de données cb2 est considéré comme effacé, perdu ou erroné pour les indices compris entre r et s qui seront dits erronés. Le vecteur résultant est le vecteur à corriger cf.

A l'étape 7000, on calcule l'image du vecteur à corriger cf par l'isomorphisme F_i, pour obtenir le vecteur à corriger transformé cft.

A l'étape 8000, on obtient une matrice transformée $G^{-1}T$. Chaque élément de la matrice transformée $G^{-1}T$ obtenue, situé à une ligne et à une colonne, est la somme de l'image de l'élément situé à ladite ligne et à ladite colonne d'une matrice brute par l'isomorphisme F_i et d'un élément de l'anneau $R_{2,n}$ qui n'a aucune composante dans l'idéal principal A_i, la matrice brute étant l'inverse (G^{-1}) de la matrice génératrice G duquel inverse sont supprimées les lignes correspondantes à ladite pluralité d'indices erronés (dans notre exemple les (numéros de) lignes comprises entre r et s).

De manière générale, lors du décodage, (et pas seulement dans ce mode de réalisation), la matrice transformée $G^{-1}T$ peut être obtenue soit :

- en appliquant l'isomorphisme F_i à l'inverse G^{-1} de la matrice génératrice G duquel inverse sont supprimées les lignes correspondantes aux indices erronés et éventuellement en ajoutant, à certains éléments de la matrice, un élément de l'anneau $R_{2,n}$ qui n'a aucune composante dans l'idéal principal A_i (de manière analogue à ce qui est décrit ci-dessous à l'étape 3100),

- à partir de l'inverse de la matrice transformée GT utilisée pour l'encodage (dans le mode de réalisation de la figure 2 déterminée à l'étape 3000, et utilisée pour encoder le vecteur de donnée à l'étape 4000), duquel inverse G^{-1} on a supprimé les lignes de même numéro que les indices erronés.

A l'étape 9000, un vecteur de donnée transformé dt est obtenu à partir de la multiplication de la matrice transformée $G^{-1}T$ par le vecteur à corriger transformé cft.

A l'étape 10000, on calcule l'image du vecteur de donnée transformé dt par l'application de l'isomorphisme inverse F_i^{-1} défini précédemment. Le résultat est le vecteur de donnée d. Le bloc erroné, (autrement dit effacé ou perdu), dans le mode de réalisation de figure 2 cb2, a été ainsi retrouvé grâce l'utilisation du code correcteur d'erreur linéaire défini par la matrice génératrice G.

Le vecteur de donnée d est alors à nouveau encodé en vecteur encodé c et mémorisé

par exemple dans un nouveau disque 302.

Les étapes 5000 et 7000 peuvent être conjointement omises. On peut en effet mémoriser dans les disques 300 à 306 à l'étape 6000 le vecteur encodé transformé et (en blocs de données), qui est dans l'anneau $R_{2,n}$, au lieu de mémoriser le vecteur encodé c.

Les procédés d'encodage et de décodage sont décrits en référence à la figure 2 et sont mis en œuvre par le même dispositif de la figure 1. Toutefois, en pratique, le procédé d'encodage et le procédé de décodage peuvent bien entendu être réalisés indépendamment et par des machines différentes.

Le microprocesseur 100 peut être remplacé par un ordinateur, par exemple par un serveur internet, ou bien être compris dans un serveur internet ainsi que la mémoire 200, les disques 300 à 306 et le bus 400.

L'invention ne s'applique pas uniquement à l'encodage et au décodage de données en mémoire, par exemple sur un disque dur. Elle peut également s'appliquer à la l'encodage et au décodage de données pour la communication sur un canal de communication par exemple hertzien.

De manière connue, le vecteur encodé c est égal au produit de la matrice génératrice G (définissant le code correcteur linéaire) et du vecteur de donnée d, et le vecteur de donnée d est égal au produit de l'inverse G^{-1} de la matrice génératrice, duquel on a supprimé les lignes de même numéro que les indices erronés du vecteur à corriger.

La figure 3 illustre les étapes pour obtenir la matrice génératrice transformée GT. A l'étape 3500, une matrice candidate transformée GTc dans l'anneau $R_{2,n}$ est engendrée. Les figures 4 et 5 donneront plus loin les détails de cette étape, chacune selon un mode de réalisation de l'invention.

A l'étape 3600, le microprocesseur 100 estime un nombre d'opérations de ou exclusif à réaliser pour l'étape de multiplication de la matrice transformée GT par le vecteur transformé dt lorsque la matrice candidate transformée GTc est choisie en tant que matrice transformée GT. Dans une représentation dite à base de ou exclusif, le nombre

d'opérations de ou exclusif est obtenu à partir du nombre total de 1 dans les éléments de l'anneau $R_{2,n}$ de la matrice candidate transformée GTc (ou de la matrice transformée GT).

A l'étape 3700, le processeur 100 détermine si la matrice candidate transformée GTc est choisie en tant que matrice transformée. De manière générale, dans un mode de réalisation de l'invention, une pluralité de matrices candidates transformées GTc sont engendrées (par exemple à partir de nombres aléatoires). La matrice candidate transformée GTc pour laquelle le nombre d'opérations est le plus petit, parmi la pluralité de matrices, est choisie.

La figure 4 illustre maintenant comment la matrice candidate transformée GTc peut être engendrée notamment durant l'étape 3500, dans un premier mode de réalisation. Dans un mode de réalisation, la matrice transformée GT peut également être obtenue directement de cette manière à l'étape de détermination de la matrice transformée (à l'étape 3000 dans le mode de réalisation de la figure 2) sans effectuer les étapes 3600 et 3700.

A l'étape 3100, une matrice candidate génératrice Gc dans le corps $B_{,,}$ définissant un code correcteur MDS (Maximum Distance Separable) est engendrée, par exemple (dans un mode de réalisation de l'invention) en utilisant de manière connue les méthodes pour construire une matrice de Cauchy, de Vandermonde ou de Cauchy généralisée également connues en soi.

A l'étape 3200, le microprocesseur 100 utilise l'isomorphisme $F_;$ pour obtenir la matrice candidate transformée GTc à partir de la matrice candidate génératrice Gc. Dans un premier mode de réalisation, on calcule l'image par l'isomorphisme $F_;$ de la matrice candidate génératrice Gc pour obtenir la matrice candidate transformée GTc. En variante, on ajoute, pour au moins un élément de la matrice candidate transformée (GTc), à l'image des éléments de matrice candidate génératrice Gc un élément de l'anneau $R_{2,n}$ non nul qui n'a aucune composante dans l'idéal principal $A_{,,}$ par exemple lorsque cet ajout permet de réduire le nombre de 1 (on se place alors ici dans une représentation dite à base de XOR bien entendu) dans l'élément de la matrice candidate transformée. Autrement dit, dans un mode de réalisation de l'invention, un élément de la matrice transformée $(GT, G^{-1}T)$ (ou en particulier, pour cette figure, de la matrice

candidate transformée) situé à une ligne et à une colonne est la somme de l'image de l'élément situé à ladite ligne et à ladite colonne de la matrice brute (ici la matrice génératrice ou la matrice candidate génératrice) par l'isomorphisme F_i et d'un élément de l'anneau $R_{2,n}$ non nul qui n'a aucune composante dans l'idéal principal A_i, par exemple, lorsque cet élément situé à ladite ligne et à ladite colonne de la matrice transformée a un nombre de 1 inférieurs au nombre de 1 présents dans l'image de l'élément situé à ladite ligne et à ladite colonne de la matrice brute. Dans ce mode de réalisation, l'invention permet alors d'obtenir des matrices transformées peu denses, ce qui réduit le nombre d'opérations de ou exclusif à réaliser pour l'étape de multiplication de la matrice transformée par le vecteur transformé, lorsque la matrice candidate transformée est choisie en tant que matrice transformée.

Les éléments l'anneau $R_{2,n}$ qui n'ont aucune composante dans l'idéal principal A_i, sont les multiples de $p_i(x)$ dans cet anneau, et chaque élément peut être obtenu en calculant au moins une partie de ces multiples.

La figure 5 illustre maintenant comment la ou les matrices candidates transformées GTc peuvent être engendrées notamment durant l'étape 3500, dans un deuxième mode de réalisation. A l'étape 3300, une matrice candidate transformée GTc est engendrée. Selon un mode de réalisation de l'invention, la matrice candidate transformée peut être constituée d'éléments dans l'anneau $R_{2,n}$ qui sont, dans une représentation dite à base de XOR, des décalages cycliques de la matrice identité (de n lignes et n colonnes). A l'étape 3400, on calcule l'image de la matrice candidate transformée GTc par l'isomorphisme inverse F_i^{-1} (défini précédemment) pour obtenir une matrice candidate génératrice Gc (on peut choisir de retrancher de l'image, pour tout ou partie des éléments de la matrice candidate transformée, un élément de l'anneau $R_{2,n}$ non nul qui n'a aucune composante dans l'idéal principal A_i). Si la matrice candidate génératrice est MDS, la matrice candidate transformée GTc est retenue (par exemple pour réaliser les étapes 3600 et 3700 de la figure 3). Sinon, la matrice candidate transformée GTc est rejetée.

La figure 6 présente plus en détail l'étape 4000 (l'étape 9000 peut être réalisée de la même manière) et décrit comment la matrice transformée est mémorisée. La figure 6 présente une partie de matrice transformée GT (ou bien la totalité d'une matrice

transformée, par exemple lorsque la notion de matrice génératrice exclue les z premières lignes qui constituent une matrice identité dans un code systématique) comprenant trois lignes et trois colonnes, dans le cas où n=5, et où la matrice transformée est mémorisée dans une représentation dite à base de ou exclusif. Chaque élément dans l'anneau $R_{2,5}$ de la matrice transformée GT est une matrice carrée élémentaire de 5x5 nombres binaires. Les plus petites cases représentent ces nombres binaires. Celles comprenant un point ou une croix sont celles qui mémorisent des 1. Les autres mémorisent des 0. La figure représente en particulier une partie de l'étape 4000 de multiplication d'une partie de la matrice transformée GT par une partie du vecteur de données transformé dt constituée des vecteurs aO, al, a2 dans l'anneau $R_{2,5}$ pour obtenir la partie correspondante du vecteur encodé transformé et constituée des vecteurs pO, pl, p2 dans l'anneau $R_{2,5}$ (dans le cas d'un code systématique où on omet les z éléments identiques au vecteur de donnée, dt et et peuvent représenter respectivement la totalité du vecteur de donnée et la totalité du vecteur encodé transformé).

La matrice transformée GT est par exemple mémorisée sous la forme d'une matrice compressée GT' dans laquelle chaque élément de la matrice transformée GT est mémorisé sous la forme de sa première ligne par exemple 610. Cela est possible car les éléments dans l'anneau ont tous des diagonales pleines de 1 ou pleines de 0.

Au lieu d'utiliser la première ligne, on peut utiliser d'autres lignes ou une colonne. L'utilisation d'une telle matrice compressée permet de réduire l'espace mémoire et le temps de calcul nécessaire à la réalisation du procédé de la figure 2 ou plus généralement de l'invention.

En particulier, l'étape 4000 comprend une sous-étape de multiplication de la matrice carrée élémentaire 610 par le vecteur a_0 de dt lors du calcul du vecteur p_0 de et. Cette étape peut être réalisée par la lecture de la ligne 610 sans lire le reste de la matrice carrée élémentaire 600 en mémoire. Lors de cette lecture, si un nombre binaire, par exemple 612 vaut 1 dans cette ligne 610, on réalise tous les XOR engendrés par la diagonale déterminée par la position de 612, par exemple le XOR déterminé par le fait que le nombre binaire 613 est à 1.

En outre, pour limiter le nombre de XOR réalisés lors de l'étape 4000, on recherche une

sous partie identique dans les trois lignes de la partie de la matrice transformée compressée GT'. Dans les trois lignes de GT', la sous partie comprise entre les deux nombres binaires représentés par une case comprenant un point est identique (on ne tient pas compte des 1 présents entre ces deux nombres binaires). De manière générale, la sous partie identique définit des XOR identiques intervenant dans le calcul de plusieurs éléments du vecteur et. Dans l'exemple de la figure 6, les trois sous-parties identiques définissent des XOR qui interviennent dans le calcul des trois éléments p_0, Pi et p_2 du vecteur et. De manière générale, on calcule donc un résultat intermédiaire qui représente le nombre de XOR déterminés par la sous partie identique et on utilise ce résultat intermédiaire pour le calcul d'autres éléments du vecteur transformé. Ainsi, si la sous partie identique comprend we éléments binaires (i.e. : égaux à 1, ou plus généralement représentant un XOR) et si la sous partie identique est présente dans m lignes, on économise n(we*m-(we+m)) XOR. Dans l'exemple donné à la figure 6, on économise par ainsi 5 XOR.

La figure 6 donne un exemple où les occurrences de la sous partie identique sont alignées dans G' (i.e. : dans la sous partie identique, selon les lignes, les nombres binaires à 1 sont dans les mêmes colonnes), mais celles-ci peuvent être plus généralement, dans un mode de réalisation de l'invention, décalées (i.e. : dans la sous partie identique, selon les lignes, les nombres binaires à 1 (ou plus généralement représentant un XOR dans une multiplication avec un autre élément) sont dans des colonnes différentes, la quantité de nombres binaires (à 0 ou 1) entre chaque couple de 1 de la partie identique étant identique). L'utilisation de la matrice compressée permet de rechercher dans un temps réaliste de telles sous parties identiques décalées, permettant ainsi de réduire encore plus le nombre de XOR réalisés lors de l'étape 4000.

Selon un mode de réalisation, le polynôme $p_i(x)$ est un polynôme AOP ou un polynôme ESP.

Dans une première variante de ce mode de réalisation, l'application de l'isomorphisme F_i comprend l'ajout d'un bit de parité à l'élément du corps, comme l'illustre les figures 7 et 8. L'application de l'isomorphisme inverse F_i^{-1} consiste alors à supprimer le bit de parité.

La figure 7 représente le calcul de l'image par l'isomorphisme $F_i(x)$ pour n=5 pour un

polynôme $p_i(x)$ AOP. Selon cette variante, pour un polynôme AOP, l'application de l'isomorphisme F_i consiste en l'ajout d'un bit de parité (i.e. : résultat du XOR) de tous les nombres binaires constituant l'élément du corps.

La figure 8 représente le calcul de l'image par l'isomorphisme F_i pour un polynôme $p_i(x)$ ESP. On peut montrer que l'idéal correspondant au corps fini déterminé par un ESP est l'ensemble des éléments qui peuvent se décomposer comme un entrelacement de s mots de poids pair de longueur r+1. Dans ce mode de réalisation, le calcul de l'image d'un élément constitué de sr bits formant r blocs de s bits consécutifs (sur la figure 8, r=2, s=3, le bloc 1 et le bloc 2 forment l'élément) consiste à ajouter un bloc de s bits (sur la figure 2, le bloc 3) qui est le XOR (bit à bit) des r blocs de s bits de l'élément (sur la figure 2 qui est le XOR du bloc 1 et du bloc 2. L'image est formée par les bloc 1, 2 et 3) .

Dans une deuxième variante de ce mode de réalisation, le calcul de l'image de chaque élément du corps fini B_i par l'isomorphisme F_i comprend l'ajout d'une donnée binaire égale à 0 à une position dudit vecteur de bit.

Comme l'illustrent les figures 9 et 10, le calcul de l'image de chaque élément du corps fini B_i par isomorphisme inverse F_i^{-1} comprend l'ajout de la donnée binaire située à ladite position à une pluralité de données binaires dudit vecteur de données binaires, puis la suppression de ladite donnée binaire située à ladite position dudit vecteur de bit.

La figure 9 représente le calcul de l'image par l'isomorphisme inverse F_i^{-1} pour n=5 pour un polynôme $p_i(x)$ AOP. Dans ce mode de réalisation, de manière générale, le calcul de l'image de chaque élément du corps fini B_i par l'isomorphisme inverse F_i^{-1} consiste à l'ajout de la donnée binaire située à ladite position à chaque donnée binaire dudit vecteur de données binaires, puis la suppression de ladite donnée binaire située à ladite position dudit vecteur de bit. La figure 10 représente le calcul de l'image par l'isomorphisme inverse noté F^pour un polynôme ESP. Ce calcul consiste à faire des opérations XOR entre le dernier bloc de s bits et chacun des r blocs de s bits de l'élément. Dans la figure 10, s = 3 et r = 2.

REVENDICATIONS

1. Procédé d'encodage d'un vecteur de donnée (d), en un vecteur encodé transformé (et), selon un code correcteur d'erreur linéaire défini par une matrice génératrice (G), dans lequel :

- le vecteur de donnée (d) et la matrice génératrice (G) sont dans le corps fini de polynômes, noté $B_{,,}$ défini de la manière suivante : $B_{;} = GF_2(x)/(Pi(x))$, $p_{,}(x)$ étant un polynôme irréductible qui divise le polynôme x^n+l, i et n étant des entiers,
- Le vecteur encodé transformé (et) appartenant à un anneau, noté R_{2^n}, et est l'image par un isomorphisme, noté $F_{,,}$ du produit de la matrice génératrice (G) par le vecteur de donnée (d), l'isomorphisme $F_{,,}$ du corps fini $B_{;}$ dans un ensemble $A_{,,}$ étant défini de la manière suivante : $F_{;}(p(x)) = p(x)\ Q_{,}(x)$, où $A_{;}$ est l'idéal principal de l'anneau R_{2^n} engendré par le polynôme $x^n+l/p_{,}(x)$, $Q_{,}(x)$ est l'unique idempotent dudit idéal principal $A_{,,}$ et p(x) un polynôme appartenant au corps $B_{,,}$ l'anneau étant défini de la manière suivante : $R_{2n} = GF_2(x)/(x^n+l)$

ledit procédé comprenant les étapes suivantes :

- Une étape de calcul de l'image par l'isomorphisme $F_{;}$ du vecteur de donnée (d) pour obtenir un vecteur de donnée transformé (dt),
- une étape de détermination d'une matrice transformée (GT), dans laquelle chaque élément de la matrice transformée (GT) situé à une ligne et à une colonne est la somme de l'image de l'élément situé à ladite ligne et à ladite colonne d'une matrice brute (G) par l'isomorphisme $F_{;}$ et d'un élément de l'anneau R_{2^n} qui n'a aucune composante dans l'idéal principal $A_{,,}$ la matrice brute (G) étant la matrice génératrice (G),
- une étape de multiplication de la matrice transformée (GT) par un vecteur transformé (dt), le vecteur transformé (dt) étant le vecteur de donnée transformée (dt), pour obtenir ledit vecteur encodé transformé (et).

2. Procédé d'encodage selon la revendication 1 comprenant une étape de calcul de l'image par un isomorphisme inverse, noté $F_{;}^{-1}$, du vecteur encodé transformé (et) pour obtenir un vecteur encodé (c), l'isomorphisme inverse $F_{;}^{-1}$ étant l'inverse de

l'isomorphisme F_i et est défini de la manière suivante : $p(x) = pn(x) \bmod p_i(x)$, $pn(x)$ étant un polynôme de l'anneau $R_{2,n}$, le vecteur encodé (c) étant égal au produit de la matrice génératrice (G) par le vecteur de donnée (d).

3. Procédé de décodage d'un vecteur à corriger transformé (cft), en un vecteur de donnée (d) selon un code correcteur d'erreur linéaire défini par une matrice génératrice (G), ledit vecteur à corriger comprenant une pluralité d'indices erronés comprenant un élément erroné dans lequel :

- le vecteur de donnée (d) et la matrice génératrice (G) sont dans le corps fini de polynômes, noté B_i, défini de la manière suivante : $B_i = GF_2(x)/(Pi(x))$, $p_i(x)$ étant un polynôme irréductible qui divise le polynôme x^n+1, i et n étant des entiers,
- Le vecteur à corriger transformé (cft) appartenant à un anneau, noté $R_{2,n}$, défini de la manière suivante : $R_{2,n} = GF_2(x)/(x^n+1)$

ledit procédé comprenant les étapes suivantes :

- une étape de détermination d'une matrice transformée ($G^{-1}T$), chaque élément de la matrice transformée ($G^{-1}T$) situé à une ligne et à une colonne est la somme de l'image de l'élément situé à ladite ligne et à ladite colonne d'une matrice brute (G^{-1}) par l'isomorphisme F_i et d'un élément de l'anneau $R_{2,n}$ qui n'a aucune composante dans l'idéal principal A_i, la matrice brute étant l'inverse (G^{-1}) de la matrice génératrice (G) de laquelle sont supprimées les lignes correspondantes à ladite pluralité d'indices erronés , l'isomorphisme F_i, du corps fini B_i dans un ensemble A_i, étant défini de la manière suivante : $F_i(p(x)) = p(x)\, Q_i(x)$, où A_i est l' idéal principal engendré par le polynôme $x^n+1/Pi(x)$ de l'anneau $R_{2,n}$, $Q_i(x)$ est l'unique idempotent dudit idéal principal A_i, et $p(x)$ un polynôme appartenant au corps B_i,
- une étape de multiplication de la matrice transformée ($G^{-1}T$) par un vecteur transformé(cft), le vecteur transformé (cft) étant le vecteur à corriger transformé (cft), pour obtenir un vecteur de donnée transformé (dt),
- une étape de calcul de l'image par un isomorphisme inverse, noté F_i^{-1}, du vecteur de donnée transformé (dt) pour obtenir le vecteur de donnée (d), l'isomorphisme inverse F_i^{-1} étant l'inverse de l'isomorphisme F_i et est défini de la manière suivante :

$p(x) = pn(x) \bmod p_i(x)$, $pn(x)$ étant un polynôme de l'anneau $R_{2,n}$.

4. Procédé de décodage selon la revendication 3, comprenant, préalablement à l'étape de multiplication, une étape de calcul de l'image par l'isomorphisme F_i d'un vecteur à corriger(cf) pour obtenir le vecteur à corriger transformé (cft), le vecteur de donnée (d) étant égal au produit de l'inverse (G^{-1}) de la matrice génératrice (G) de laquelle sont supprimées les lignes de même numéro que ladite pluralité d'indices erronés_à ladite pluralité d'indices erronés par le vecteur à corriger (cf).

5. Procédé selon l'une des revendications 1 à 4 dans lequel, la matrice transformée ($GT, G^{-1}T$) est l'image de la matrice brute (G, G^{-1}) par l'isomorphisme F_i

6. Procédé selon l'une des revendications 1 à 4, dans lequel, au moins un des éléments de la matrice transformée ($GT, G^{-1}T$) situé à une ligne et à une colonne est la somme de l'image de l'élément situé à ladite ligne et à ladite colonne de la matrice brute (G, G^{-1}) par l'isomorphisme F_i et d'un élément de l'anneau $R_{2,n}$ non nul qui n'a aucune composante dans l'idéal principal A_i.

7. Procédé selon l'une quelconque des revendications précédentes mis en œuvre dans une représentation dite à base de ou exclusif dans laquelle chaque élément de la matrice transformée ($GT, G^{-1}T$) est représenté par une matrice carrée élémentaire de n lignes et n colonnes de nombre binaires, ledit chaque élément étant mémorisé sous la forme d' une seule de ces n lignes ou n colonnes, la matrice transformée étant ainsi mémorisée sous la forme d'une matrice transformée compressée constituée de la seule des n lignes ou n colonnes de chaque élément de la matrice transformée ($GT, G^{-1}T$).

8. Procédé selon la revendication précédente dans lequel chaque élément du vecteur transformé (dt,cft) est représenté par un vecteur élémentaire de n nombres binaires, ladite étape de multiplication de la matrice transformée ($GT, G^{-1}T$) par le vecteur transformé (dt,cft) comprenant une sous-étape de multiplication de la matrice carrée élémentaire par le vecteur élémentaire, ladite sous-étape de multiplication comprenant les étapes suivantes :

- une étape de lecture en mémoire de ladite seule ligne ou seule colonne de la matrice carrée élémentaire dans la matrice transformée compressée,
- une étape de traitement dans laquelle, pour chaque nombre binaire occupant une position de ladite une seule ligne ou seule colonne dans la matrice transformée compressée, si ledit bit est égal à une valeur déterminée, les ou exclusifs engendrés par toute la diagonale de la matrice carrée élémentaire déterminée par cette position sont calculés.

9. Procédé selon la revendication 8, comprenant, préalablement à l'étape de multiplication, les étapes suivantes :
- une étape de détermination d'une sous partie identique comprenant we éléments binaires dans m lignes de la matrice transformée compressée, we supérieur ou égal à deux,
- une étape de calcul d'un résultat intermédiaire à partir de ladite sous partie identique,
- l'étape de multiplication étant réalisée à partir du résultat intermédiaire de manière à éviter n.(we.m-(we+m)) opérations de ou exclusif durant l'étape de multiplication.

10. Procédé selon l'une quelconque des revendications précédentes prise en dépendance de la revendication 1 comprenant les étapes suivantes :
- une étape pour engendrer une matrice candidate transformée,
- une étape pour estimer un nombre d'opérations de ou exclusif à réaliser pour l'étape de multiplication de la matrice transformée (GT) par le vecteur transformé (dt,cft), lorsque la matrice candidate transformée est choisie en tant que matrice transformée (GT),
- une étape pour déterminer, en fonction dudit nombre d'opérations de ou exclusif à réaliser, si la matrice candidate transformée est choisie en tant que matrice transformée (GT).

11. Procédé selon la revendication 10 prise en dépendance de la revendication 7 comprenant en outre :
- durant l'étape pour estimer le nombre d'opérations de ou exclusif à réaliser pour

l'étape de multiplication de la matrice transformée (GT) par le vecteur transformé (dt,cft), une étape de détermination d'une sous partie identique comprenant w éléments binaires dans m lignes de la matrice transformée compressée, w supérieur ou égal à deux,

- une étape de calcul du nombre d'opérations de ou exclusif évités, égal à n.(we.m-(we+m)), à partir desdites sous parties, dans lequel le nombre d'opérations de ou exclusif à réaliser est estimé à partir dudit nombre d'opérations de ou exclusif évités.

12. Procédé selon l'une quelconque des revendications 10 et 11 comprenant en outre :

-une étape pour engendrer une matrice candidate génératrice définissant un code correcteur d'erreur qui est MDS.

- une étape de calcul de l'image par l'isomorphisme F_γ de la matrice candidate génératrice pour obtenir la matrice candidate transformée .

13. Procédé selon l'une quelconque des revendications 10 et 11 comprenant les étapes suivantes :

- une étape de calcul de l'image de la matrice candidate génératrice par un isomorphisme inverse F_γ^{-1} pour obtenir la matrice génératrice candidate, l'isomorphisme inverse F_γ^{-1} étant l'inverse de l'isomorphisme F_γ et est défini de la manière suivante : p(x) = pn(x) mod p_γ(x), pn(x) étant un polynôme de l'anneau $R_{2,n}$.

-une étape de vérification que la matrice génératrice candidate est MDS.

14. Procédé selon l'une quelconque des revendications précédentes dans lequel le polynôme p_γ(x) est un polynôme AOP.

15. Procédé selon l'une quelconques des revendications précédentes dans lequel le polynôme p_γ(x) est un polynôme ESP.

16. Procédé selon l'une quelconque des revendications 14 ou 15, dans lequel

- chaque élément du corps fini B_γ étant représenté par un vecteur de données binaires

- le calcul de l'image de chaque élément du corps fini B_i par l'isomorphisme F_i comprend l'ajout d'un bit de parité audit vecteur de données binaires.
- le calcul de l'image de chaque élément du corps fini B_i par un isomorphisme F_i^{-1} comprend la suppression dudit bit de parité audit vecteur de données binaires, l'isomorphisme inverse F_i^{-1} étant l'inverse de l'isomorphisme F_i et est défini de la manière suivante : $p(x) = pn(x) \bmod p_i(x)$, $pn(x)$ étant un polynôme de l'anneau $R_{2,n}$.

17. Procédé selon l'une quelconque des revendications 14 ou 15, dans lequel
- chaque élément du corps fini B_i étant représenté par un vecteur de données binaires
- le calcul de l'image de chaque élément du corps fini B_i par l'isomorphisme F_i comprend l'ajout d'une donnée binaire égale à 0 à une position dudit vecteur de bit.
- le calcul de l'image de chaque élément du corps fini B_i par un isomorphisme inverse noté F_i^{-1} comprend l'ajout de la donnée binaire située à ladite position à une pluralité de données binaires dudit vecteur de données binaires, puis la suppression de ladite donnée binaire située à ladite position dudit vecteur de bit, l'isomorphisme inverse F_i^{-1} étant l'inverse de l'isomorphisme F_i et est défini de la manière suivante :
$p(x) = pn(x) \bmod p_i(x)$, $pn(x)$ étant un polynôme de l'anneau $R_{2,n}$.

18. Dispositif adapté à la mise en œuvre des étapes du procédé selon les revendications précédentes.

19. Programme d'ordinateur comprenant des instructions adaptées à la mise en œuvre de chacune des étapes du procédé selon l'une quelconque des revendications 1 à 17 lorsque ledit programme est exécuté sur un ordinateur.

20. Moyen de stockage d'informations, amovible ou non, partiellement ou totalement lisible par un ordinateur ou un microprocesseur comportant des instructions de code d'un programme d'ordinateur pour l'exécution de chacune des étapes du procédé selon l'une quelconque des revendications 1 à 17.

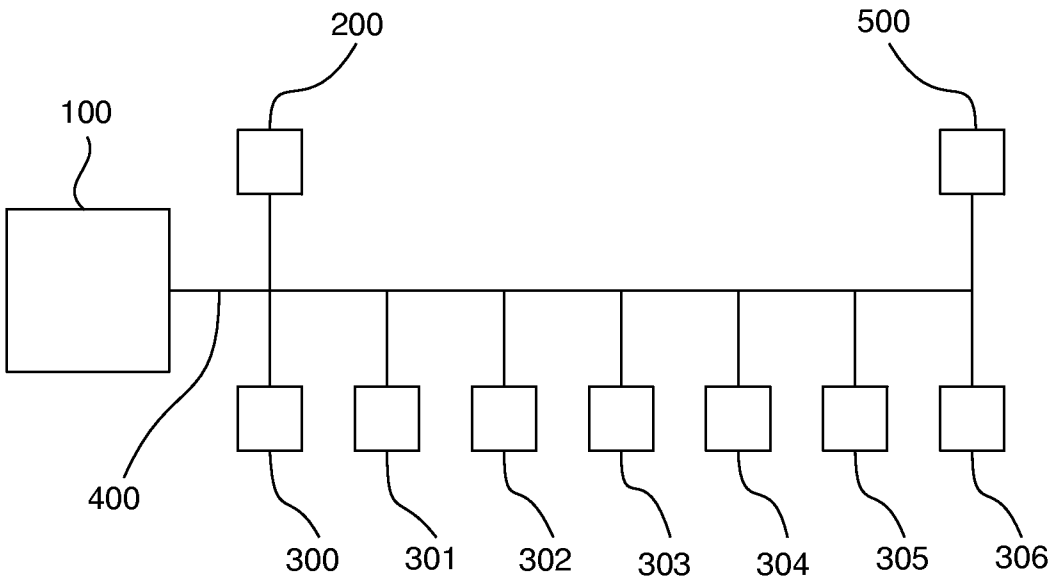


Fig.1

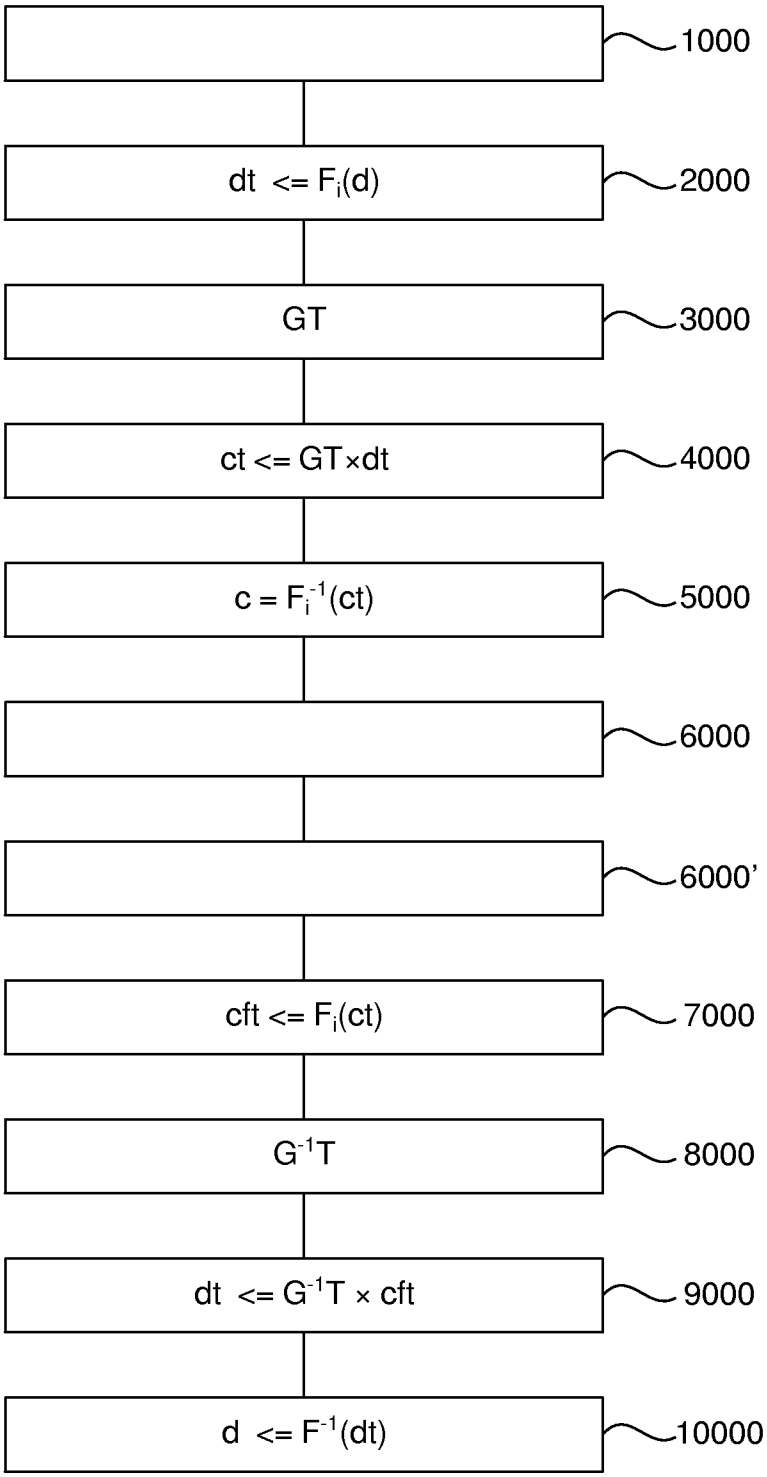

1000
dt <= F_i(d)
2000
GT
3000
ct <= GT×dt
4000
c = F_i^{-1}(ct)
5000
6000
6000'
cft <= F_i(ct)
7000
$G^{-1}T$
8000
dt <= $G^{-1}T$ × cft
9000
d <= F^{-1}(dt)
10000

Fig.2

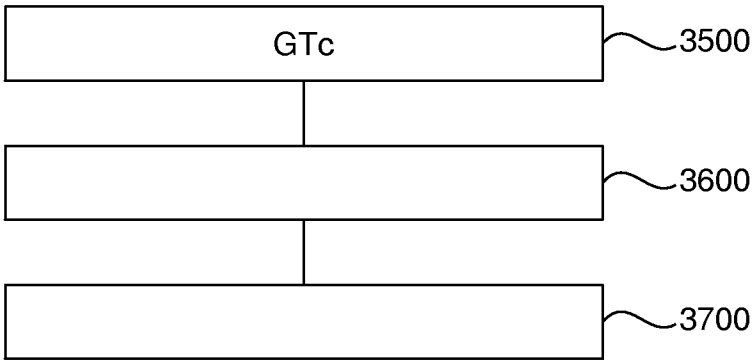


Fig.3

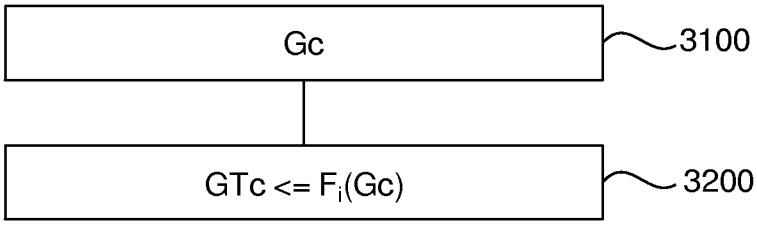


Fig.4

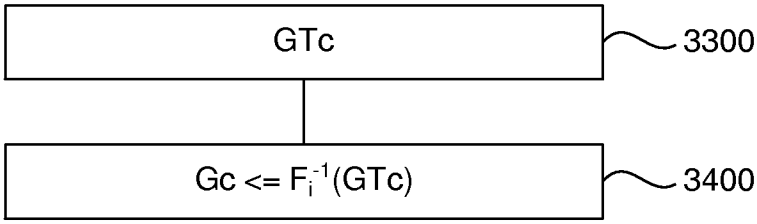


Fig.5

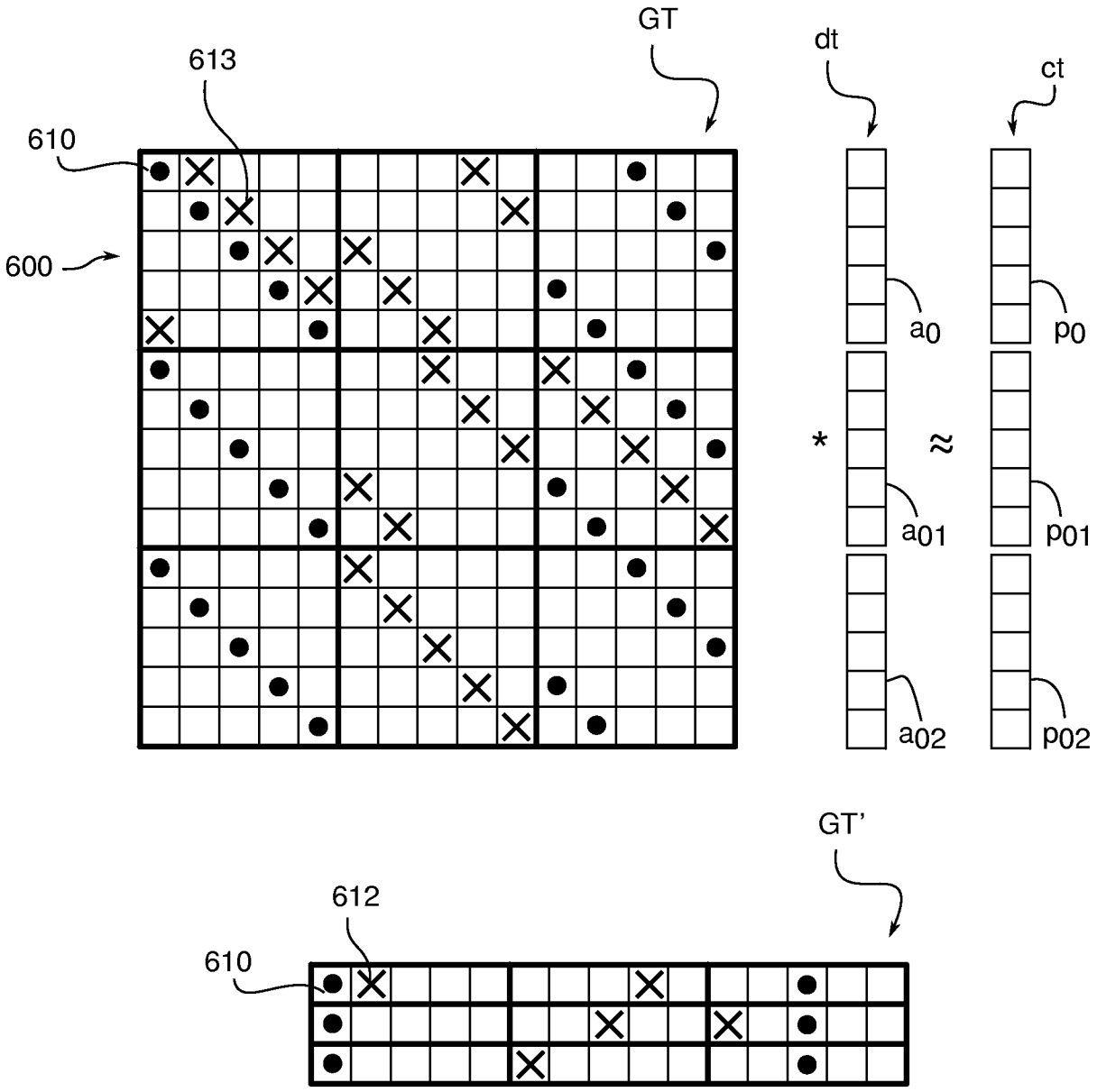


Fig.6

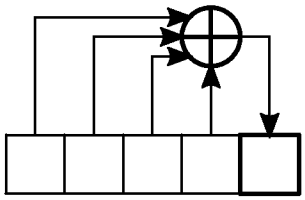


Fig.7

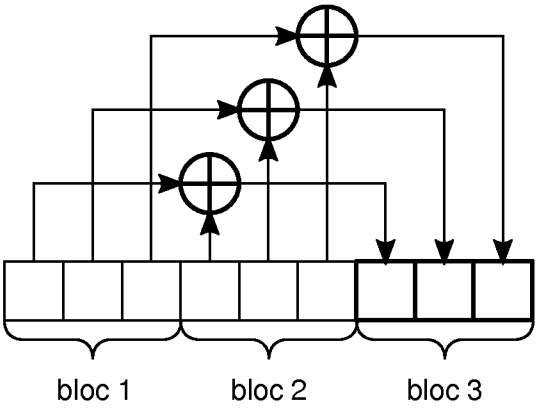


Fig.8

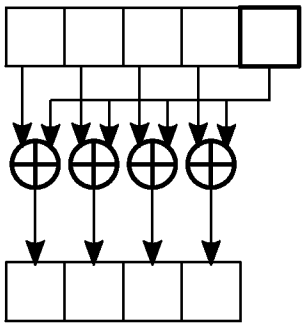


Fig.9

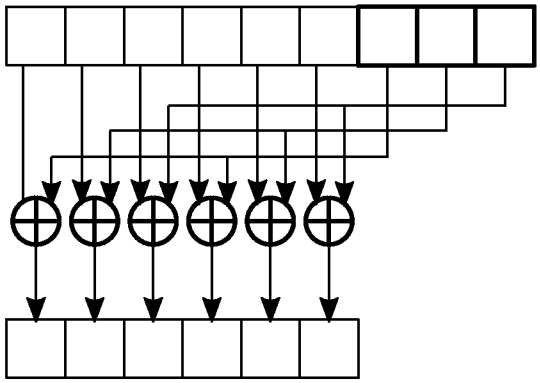


Fig.10

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/053495

A. CLASSIFICATION OF SUBJECT MATTER
INV. H03M13/15 G06F7/72
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification **System** followed **by** classification **symbols)**
H03M 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.
A	DROLET G: "A NEW REPRESENTATION OF ELEMENTS OF FINITE FIELDS GF(2M) YIELDING SMALL COMPLEXITY ARITHMETIC CIRCUITS", IEEE TRANSACTIONS ON COMPUTERS, IEEE, USA, vol. 47, no. 9, September 1998 (1998-09), pages 938-946, XP001028474, ISSN: 0018-9340, DOI: 10.1109/12.713313 the whole document ----	1-20
A	US 2006/212782 Al (LI JIN [US]) 21 September 2006 (2006-09-21) the whole document ----	1-20

-/- ·

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

[X] See patent family annex.

* Spécial catégories of cited documents :

"A" document defining the gênerai 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" documentwhich may throw doubts on priority claim(s) orwhich is cited to establish the publication date of another citation or other spécial 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 ortheory 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
19 March 2018	03/04/2018

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	Farman , Thomas

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/053495

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FRANCISCO ARGUELLO: "Multiplicati on in Cyclotomic Rings and its Appli cati on to Finite Fiθïds", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853 , 23 July 2008 (2008-07-23) , XP080428062 , the whole document -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2017/053495

Patent document oited in searoh report	Publication date	Patent family member(s)	Publication date
US 2006212782 A1	21-09-2006	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2017/053495

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H03M13/15 G06F7/72
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 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
A	DROLET G: "A NEW REPRESENTATION OF ELEMENTS OF FINITE FIELDS GF(2M) YIELDING SMALL COMPLEXITY ARITHMETIC CIRCUITS", IEEE TRANSACTIONS ON COMPUTERS, IEEE, USA, vol. 47, no. 9, septembre 1998 (1998-09), pages 938-946, XP001028474, ISSN: 0018-9340, DOI: 10.1109/12.713313 le document en entier --- US 2006/212782 Al (LI JIN [US]) 21 septembre 2006 (2006-09-21) le document en entier --- -/-	1-20 1-20

[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'appartenenant 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
19 mars 2018	03/04/2018

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	Farman , Thomas

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2017/053495

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	FRANCISCO ARGUELLO: "Multiplicati on in Cyclotomic Rings and its Applicati on to Finite Fiθïds", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853 , 23 juillet 2008 (2008-07-23) , XP080428062 , le document en entier ----	1-20

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2017/053495

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2006212782 A1	21-09-2006	AUCUN	