(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
11 octobre 2018 (11.10.2018)

WIPO | PCT

(10) Numéro de publication internationale
WO 2018/185402 A1

(51) Classification internationale des brevets :
H04L 1/00 (2006.01) *H03M 13/00* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2018/050770

(22) Date de dépôt international :
29 mars 2018 (29.03.2018)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1752861 03 avril 2017 (03.04.2017) FR

(71) Déposant : **ORANGE** [FR/FR] ; 78 rue Olivier de Serres, 75015 PARIS (FR).

(72) Inventeur : **TORTELIER, Patrick** ; ORANGE GARDENS - IMT/OLR/IPL/PATENTS -, 44 avenue de la République -, CS 50010, 92326 CHÂTILLON CEDEX (FR).

(74) Mandataire : **ORANGE IMT/OLR/IPL/PATENTS** ; MUSTAKI Daniel, ORANGE GARDENS -, 44 avenue de la République - CS 50010, 92326 CHÂTILLON CEDEX (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, 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,

WO 2018/185402 A1

(54) Title: METHODS FOR ENCODING AND DECODING DATA PACKETS IN A GALOIS FIELD

(54) Titre : PROCÉDÉS DE CODAGE ET DE DÉCODAGE DE PAQUETS DE DONNÉES DANS UN CORPS DE GALOIS

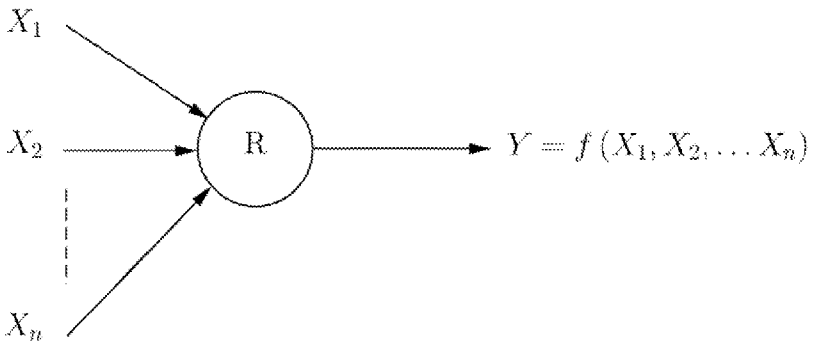


FIG. 1

(57) Abstract: The present invention relates to a method for encoding data packets, comprising the following steps: receiving $r \geq 1$ 1 useful data packets Y_i <sb /> each made up of a linear combination in which the coefficients of the linear combination are taken in an extension field $GF(2^m)$ defined by means of a chosen primitive polynomial, from the same $k \geq 1$ information packets $\{P_1, P_2, ..., P_k\}$ referred to as initial packets, each information packet containing $L \geq 1$ symbols each made up of a series of $m > 1$ bits; calculating an outgoing useful data packet Y' made up of a linear combination of useful data packets Y_i; in which the coefficients α_i are taken from the extension field $GF(2^m)$; and transmitting the outgoing useful data packet Y'. The encoding method is characterized in that the step of calculating the outgoing useful data packet Y' comprises at least one sub-step of multiplying $Q = a \cdot P$ all the symbols in a data packet $P = (x_1, ..., x_L)$, wherein x_j for $j = 1, ..., L$, is a symbol made up of a series of m bits x_{ij}, in which $i = 0, ..., m-1$, by a same number α belonging to $GF(2^m)$, and in that the multiplication is carried out by means of binary operations performed in a vector manner at the level of the symbols of the data packet P. The invention applies to the transmission of binary data packets on erasing channels.

(57) Abrégé : La présente invention concerne un procédé de codage de paquets de données, comprenant les étapes suivantes :

[Suite sur la page suivante]

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))*

réception de $r \geq 1$ l paquets de données utiles $Y_i$constitué chacun par une combinaison linéaire, où les coefficients de ladite combinaison linéaire sont pris dans un corps d'extension $GF(2^m)$ défini au moyen d'un polynôme primitif choisi, des mêmes $k \geq 1$ paquets d'information $\{P_1, P_2, ..., P_k\}$ dits paquets initiaux, chaque paquet d'information contenant $L \geq 1$ symboles constitués chacun d'une suite de $m > 1$ bits; calcul d'un paquet de données utiles sortant Y' constitué par une combinaison linéaire des paquets de données utiles Y_i;, où les coefficients α_i sont pris dans ledit corps d'extension $GF(2^m)$; et émission dudit paquet de données utiles sortant Y'. Ledit procédé de codage est remarquable en ce que ladite étape de calcul du paquet de données utiles sortant Y' comprend au moins une sous-étape de multiplication $Q = a \cdot P$ de tous les symboles d'un paquet de données $P = (x_1, ..., x_L)$ dans lequel x_j pour $j = 1, ..., L$, est un symbole composé d'une suite de m bits x_{ij}, où $i = 0, ..., m - 1$, par un même nombre α appartenant à $GF(2^m)$, et en ce que ladite multiplication est réalisée au moyen d'opérations binaires effectuées de manière vectorielle au niveau des symboles dudit paquet de données P. Application à la transmission de paquets de données binaires sur des canaux à effacements.

PROCEDES DE CODAGE ET DE DECODAGE DE PAQUETS DE DONNEES DANS UN CORPS DE GALOIS

La présente invention concerne les systèmes de communication ou d'enregistrement de données dans lesquels, afin d'améliorer la fidélité de la transmission ou du stockage, on soumet les données à un codage dit « de réseau » (« *Network Coding* » en anglais).

L'invention concerne plus particulièrement la transmission de paquets de données sur un canal affecté par des pertes de paquets. Sur un tel canal, certains paquets sont reçus parfaitement (grâce à une modulation et un codage convenablement définis au niveau de la couche physique) ; en revanche, d'autres paquets ne sont pas reçus, soit parce que ces paquets sont supprimés en raison d'une congestion dans un routeur, soit parce qu'ils sont reçus dans de mauvaises conditions (bruit, interférences) et ne peuvent être décodés correctement. Un tel canal de transmission est appelé « canal à effacements », et les paquets perdus sont dits « effacés ». Les systèmes de transmission de paquets sur des canaux provoquant des effacements comprennent par exemple :

- le stockage de masse, ainsi que le stockage distribué, systèmes dans lesquels les pertes de données sont dues à des pannes de disques durs ou de serveurs ;
- la diffusion en *broadcast* ou en *multicast* eMBMS (evolved Multimedia Broadcast Multicast Services) en LTE (Long Term Evolution), pour la transmission de fichiers ou de programmes audiovisuels en continu (*streaming*) ; et
- la transmission en temps réel de la Voix ou de la Vidéo sur des canaux à pertes, tels que VoLTE (Voice over LTE) ou WebRTC (Web Real-Time Communication).

On notera que, dans certains de ces systèmes, les paquets sont appelés « blocs », mais on utilisera uniformément le terme de « paquets » ci-dessous.

On rappelle que le codage de réseau (cf. par exemple l'article de R. Koetter et M. Medard intitulé « *An algebraic approach to network coding* », IEEE/ACM Transactions on Networking, vol. 11, n° 5, oct. 2003, pages 782 à 795) consiste à transmettre des informations dans des paquets de données de

telle sorte que ces informations suivent plusieurs trajets dans une infrastructure distribuée comprenant des nœuds qui servent de relais (ou de routeurs).

La présente invention concerne plus particulièrement le cas dans lequel les relais peuvent stocker et retransmettre (« *store and forward* » en anglais) les paquets de données utiles entrant dans ces relais, mais peuvent aussi, comme illustré sur la **figure 1,** retransmettre des paquets de données utiles qui résultent d'un traitement sur ces paquets d'entrée, c'est-à-dire qui constituent une certaine fonction f de ces paquets d'entrée.

On supposera que les paquets de données utiles contenus dans tous ces paquets de données ont tous le même nombre de bits. Si ce nombre est un multiple d'un entier m supérieur à 1, on peut considérer que chaque paquet de données utiles est constitué de L symboles de m bits appartenant à un corps d'extension binaire $GF(2^m)$. On rappelle à cet égard que l'on appelle corps de Galois (noté $GF(q)$) un ensemble de q éléments dont les éléments non-nuls peuvent être identifiés comme étant chacun égal à α^{j-1} pour une valeur correspondante de j, où $j = 1,..., q-1$, et où α est une racine $(q-1)^{\text{ème}}$ primitive de l'unité dans $GF(q)$; lorsque, en particulier, $q = 2^m$, où $m > 1$, le corps de Galois est également appelé « corps d'extension binaire ».

Chaque relais peut transférer sans modification les paquets de données utiles qu'il reçoit, ou transmettre sur le lien de sortie une combinaison linéaire de paquets reçus sur les liens d'entrée, étant entendu que, comme expliqué ci-dessus (canal à effacements), certains paquets envoyés par d'autres nœuds du réseau peuvent ne pas avoir être reçus (auxquels cas le relais ne cherche pas à retrouver les paquets effacés).

Lorsque les paquets d'entrée $X_1, ..., X_n$ sont tous constitués de L éléments de $GF(2^m)$, une opération très simple sur ces paquets d'entrée consiste à effectuer une addition bit à bit (on rappelle que l'addition bit à bit est également appelée « OU exclusif », et notée « XOR ») des paquets d'entrée :

$$Y = X_1 \oplus X_2 \oplus \cdots \oplus X_n .$$

Une règle de calcul plus complexe du paquet de sortie Y met en œuvre des combinaisons linéaires des paquets d'entrée $X_1, \ldots, X_n$ avec des coefficients $\alpha_i \in GF(2^m)$, c'est-à-dire :

$$Y = \alpha_1 X_1 \oplus \alpha_2 X_2 \oplus \cdots \oplus \alpha_n X_n \ .$$

Cette relation entrée-sortie fait maintenant intervenir des multiplications dans le corps $GF(2^m)$. Par commodité de notation, nous représenterons ci-après l'opération XOR par le symbole usuel $(+)$ de l'addition, de sorte que la relation précédente s'écrit :

$$Y = \alpha_1 X_1 + \alpha_2 X_2 + \cdots + \alpha_n X_n = \sum_{i=1}^{n} \alpha_i X_i \ .$$

La transmission de paquets d'information d'une source S vers un destinataire (ou récepteur) D via un réseau N peut être décrite par un graphe (voir **figure 2**) dont les nœuds représentent des relais tels que celui illustré sur la figure 1, et les branches représentent les liens existants entre :

- la source et un ou plusieurs relais,
- le destinataire et un ou plusieurs relais, et
- entre les relais eux-mêmes.

La source S émet une suite de paquets d'information $\{P_1, P_2, \ldots, P_k\}$, dits paquets initiaux. Un même paquet P_i peut circuler sur plusieurs chemins du réseau N issus de S. Le destinataire D peut donc recevoir un nombre $n \geq k$ de paquets de données utiles R_i, chacun d'entre eux pouvant être :

- une copie d'un des paquets P_j, s'il a été transmis par des nœuds retransmettant sans modification les paquets qu'ils reçoivent, ou
- une combinaison linéaire de la forme

$$R_i = c_{i,1} P_1 + c_{i,2} P_2 + \cdots + c_{i,k} P_k = \sum_{j=1}^{k} c_{i,j} P_j$$

s'il est passé par des relais effectuant des combinaisons linéaires, les coefficients $c_{i,j}$ étant pris dans un corps d'extension $GF(2^m)$; les relais du réseau N effectuent des combinaisons linéaires sur les paquets d'un même flot (allant de la même source S vers le même destinataire D) avec des coefficients

qui peuvent soit être déterminés une fois pour toutes, soit être tirés au sort à chaque application dans le cas du codage de réseau dit « aléatoire ».

Il faut noter que, les différents chemins entre la source S et le destinataire D ayant potentiellement des longueurs différentes (en nombre de branches) et des retards différents, les paquets reçus le sont dans un ordre qui peut être différent de celui des paquets émis. D'autre part la topologie du réseau n'est pas nécessairement connue du destinataire et/ou de l'émetteur. Cela signifie que le destinataire reçoit un nombre n de paquets qui sont chacun une combinaison linéaire des paquets P_i émis par la source S, ce que l'on peut écrire de la façon suivante :

$$\begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix} = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,k} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,k} \\ \vdots & \vdots & \cdots & \vdots \\ c_{n,1} & c_{n,2} & \cdots & c_{n,k} \end{bmatrix} \times \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_k \end{bmatrix} = \mathbf{K} \times \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_k \end{bmatrix}.$$

Afin de retrouver ces paquets P_j à partir des paquets reçus R_i, il faut que la matrice $\mathbf{K}$ soit connue du destinataire, et, lorsqu'elle est connue, qu'elle soit de rang k. Il faut en particulier que le destinataire dispose d'un nombre $n \geq k$ de paquets reçus R_i, sans quoi la matrice serait de rang inférieur à k et l'on ne pourrait pas remonter aux paquets P_j.

Cette technique du codage de réseau consiste donc en un codage/décodage au moyen d'un code sans rendement prédéfini (« *rateless code* » en anglais) à cause de la contrainte $n \geq k$, n pouvant être (théoriquement) infini. En fait il s'agit d'une instance des codes dits « codes fontaine » (« *fountain codes* » en anglais), avec les différences suivantes :

- il existe plus d'un chemin entre source et destinataire, et les paquets reçus par un même destinataire peuvent avoir suivi des chemins différents ;
- les combinaisons linéaires des paquets d'information P_j ne sont pas effectuées par la source mais par les éléments du réseau (codage distribué) ;
- les coefficients de ces combinaisons linéaires peuvent être prédéterminés et fixes dans le temps, ou bien être tirés au sort par les nœuds du réseau ; ce dernier cas (décrit dans l'article de T. Ho, M. Médard, R. Koetter, D.R. Karger, M. Effros, J. Shi, et B. Leong intitulé « *A random linear Network*

Coding approach to multicast », IEEE Trans. Information Theory, vol. 52, n° 10, oct. 2006, pages 4413 à 4430) est appelé « codage de réseau aléatoire » (« *Random Linear Network Coding* », ou RLNC, en anglais).

On notera que l'utilisation de codes sans rendement prédéfini pour récupérer les paquets perdus durant des phénomènes de congestion permet d'envisager la possibilité de mettre en œuvre des protocoles de transmission de données par paquets sans faire appel au mécanisme de contention classiquement utilisé pour éviter les collisions, d'où un gain en termes de simplicité de mise en œuvre et de rapidité d'exécution.

Cela étant, de simples considérations d'algèbre linéaire permettent de montrer que la résolution d'un système d'équations dans $GF(2^m)$ faisant intervenir des paquets de données peut être ramenée à des additions de paquets et à des multiplications d'un paquet par un même élément de $GF(2^m)$, c'est-à-dire des combinaisons linéaires de paquets avec des coefficients pris dans $GF(2^m)$. Dans le cadre de ces calculs, l'addition bit à bit est simple à mettre en œuvre, mais la multiplication dans $GF(2^m)$ repose classiquement sur un mécanisme logiciel de consultation de table de multiplication.

Or, lorsqu'il faut multiplier tous les éléments d'un vecteur donné $\boldsymbol{X} = (x_1, \ldots, x_n)$ composé d'éléments de $GF(2^m)$ par un même élément a de $GF(2^m)$, on ne peut pas consulter ladite table de multiplication de façon vectorielle ; autrement dit, il faut consulter la table pour chaque élément x_i du vecteur, ce qui est d'autant plus lent que le vecteur est plus long.

La présente invention concerne donc, selon un premier aspect, un procédé de codage de paquets de données dans un réseau (N), comprenant les étapes suivantes :

- réception de $r \geq 1$ paquets de données utiles Y_i constitué chacun par une combinaison linéaire

$$Y_i = \sum_{j=1}^{k} c_j^{(i)} P_j ,$$

où les coefficients $c_j^{(i)}$ sont pris dans un corps d'extension $GF(2^m)$ défini au moyen d'un polynôme primitif choisi, des mêmes $k \geq 1$ paquets d'information $\{P_1, P_2, \ldots, P_k\}$, dits paquets initiaux, chaque paquet d'information contenant $L \geq 1$ symboles constitués chacun d'une suite de $m > 1$ bits ;

- calcul d'un paquet de données utiles sortant Y' constitué par une combinaison linéaire

$$Y' = \sum_{i=1}^{r} \alpha_i Y_i$$

desdits paquets de données utiles Y_i, où les coefficients α_i sont pris dans ledit corps d'extension $GF(2^m)$; et

- émission dudit paquet de données utiles sortant Y'.

Ledit procédé de codage est remarquable en ce que ladite étape de calcul du paquet de données utiles sortant Y' comprend au moins une sous-étape de multiplication $Q = a \cdot P$ de tous les symboles d'un paquet de données $P = (x_1, \ldots, x_L)$ dans lequel x_j, pour $j = 1, \ldots, L$, est un symbole composé d'une suite de m bits x_{ij}, où $i = 0, \ldots, m-1$, par un même nombre a appartenant à $GF(2^m)$, et en ce que ladite multiplication est effectuée de la manière suivante :

a) remplissage d'une matrice binaire $\mathbf{X}$ de dimension $m \times L$ en plaçant les bits x_{ij} composant chaque symbole x_j le long de la j-ième colonne de ladite matrice $\mathbf{X}$;

b) calcul de la matrice binaire

$\mathbf{Y} = M(a) \times \mathbf{X}$,

de dimension $m \times L$, où $M(a)$ est la matrice binaire de dimensions $m \times m$ dont les colonnes respectives contiennent les coordonnées binaires des éléments respectifs $\{a, \alpha a, \ldots, \alpha^{m-1} a\}$, où α est une racine dudit polynôme primitif, en obtenant les lignes de ladite matrice $\mathbf{Y}$ au moyen d'additions binaires de lignes de la matrice $\mathbf{X}$ selon des motifs déterminés par les lignes de la matrice $M(a)$; et

c) obtention du paquet de données $Q = (y_1, \ldots, y_L)$, dans lequel chaque symbole y_j, pour $j = 1,2, \ldots, L$, est composé des m bits y_{ij}, où $i = 0, \ldots, m-1$, situés sur la j-ième colonne de ladite matrice $\mathbf{Y}$.

Grâce à ces dispositions, on peut remplacer le mécanisme classique de consultation de table de multiplication par un ensemble d'opérations binaires effectuées de manière vectorielle au niveau des symboles dudit paquet de données P. La présente invention est donc particulièrement avantageuse car, si elle permet une mise en œuvre logicielle du codage ou du décodage comme les techniques de l'état de l'art, elle permet aussi d'utiliser efficacement un circuit électronique simultanément à des moyens logiciels, ou à leur place.

On notera en particulier que le procédé selon l'invention se prête bien à la virtualisation. On peut en effet supposer que certaines fonctions nécessiteront le recours à des coprocesseurs matériels tels qu'un circuit logique programmable (« *Field-Programmable Gate Array* », ou FPGA, en anglais), un processeur graphique (« *Graphics Processing Unit* », ou GPU, en anglais), ou un processeur de signal numérique (« *Digital Signal Processor* », ou DSP, en anglais), pour accélérer certains traitements nécessitant une grande puissance de calcul, tels que les traitements de chiffrement, mais aussi ceux introduits par le codage de canal et par le codage de réseau. La présente invention est donc particulièrement avantageuse dans le cadre d'une fonctionnalité de codage de réseau virtualisée (« *Virtualized Network Function* », ou VNF, en anglais) principalement écrite sous forme logicielle et recourant à un accélérateur matériel mettant en œuvre la multiplication dans $GF(2^m)$ en mode paquet.

Selon des caractéristiques particulières, lesdites matrices $M(a)$, pour $a = \alpha^i$ et $i = 1,2, \ldots, m-1$, sont extraites d'une matrice de référence $\mathbf{T}$ de dimension $m \times (2^m + m - 2)$.

Grâce à ces dispositions, on peut aisément obtenir les matrices $M(a)$ sans aucun calcul, par simple lecture dans une unique matrice $\mathbf{T}$ construite et stockée préalablement à la mise en œuvre dudit procédé de codage.

Corrélativement, l'invention concerne un procédé de décodage de paquets de données, comprenant les étapes suivantes :

- réception de $n > 1$ paquets de données codés $R_1, R_2, \ldots, R_n$, où, pour $i = 1, \ldots, n$, chaque paquet de données codé

$$R_i = c_{i,1}P_1 + c_{i,2}P_2 + \cdots + c_{i,k}P_k = \sum_{j+1}^{k} c_{i,j}P_j$$

est une combinaison linéaire des mêmes $k \geq 1$ paquets d'information P_j contenant chacun $L \geq 1$ symboles constitués d'une suite de $m > 1$ bits, et où les coefficients $c_{i,j}$ sont pris dans un corps d'extension $GF(2^m)$ défini au moyen d'un polynôme primitif choisi, et

- résolution du système formé par lesdites combinaisons linéaires, de manière à obtenir lesdits paquets d'information P_j .

Ledit procédé de décodage est remarquable en ce que ladite étape de résolution d'un système de combinaisons linéaires comprend au moins une sous-étape de multiplication $Q = a \cdot P$ de tous les symboles d'un paquet de données $P = (x_1, \ldots, x_L)$ dans lequel x_j, pour $j = 1, \ldots, L$, est un symbole composé d'une suite de m bits x_{ij}, où $i = 0, \ldots, m-1$, par un même nombre a appartenant à $GF(2^m)$, et en ce que ladite multiplication est effectuée de la manière suivante :

a) remplissage de la matrice binaire $\mathbf{X}$ de dimension $m \times L$ en plaçant les bits x_{ij} composant chaque symbole x_j le long de la j-ième colonne de ladite matrice $\mathbf{X}$;

b) calcul de la matrice binaire

$\mathbf{Y} = M(a) \times \mathbf{X}$,

de dimension $m \times L$, où la matrice $M(a)$ est la matrice binaire de dimensions $m \times m$ dont les colonnes respectives contiennent les coordonnées binaires des éléments respectifs $\{a, \alpha a, \ldots, \alpha^{m-1}a\}$, où α est une racine dudit polynôme primitif, en obtenant les lignes de ladite matrice $\mathbf{Y}$ au moyen d'additions binaires de lignes de la matrice $\mathbf{X}$ selon des motifs déterminés par les lignes de la matrice $M(a)$; et

c) obtention du paquet de données $Q = (y_1, \ldots, y_L)$, dans lequel chaque symbole y_j, pour $j = 1,2, \ldots, L$, est composé des m bits y_{ij}, où $i = 0, \ldots, m-1$, situés sur la j-ième colonne de ladite matrice $\mathbf{Y}$.

Les avantages offerts par ce procédé de décodage sont essentiellement les mêmes que ceux offerts par le procédé de codage corrélatif succinctement exposé ci-dessus.

Selon des caractéristiques particulières, lesdites matrices $M(a)$, pour $a = \alpha^i$ et $i = 1,2, \ldots, m-1$, sont extraites d'une matrice de référence $\mathbf{T}$ de dimension $m \times (2^m + m - 2)$.

Grâce à ces dispositions, on peut aisément obtenir les matrices $M(a)$ sans aucun calcul, par simple lecture dans une unique matrice $\mathbf{T}$ construite et stockée préalablement à la mise en œuvre dudit procédé de décodage.

Selon un deuxième aspect, l'invention concerne divers dispositifs.

Elle concerne ainsi, premièrement, un dispositif de codage de paquets de données, comprenant des moyens pour :

- recevoir $r \geq 1$ paquets de données utiles Y_i constitué chacun par une combinaison linéaire

$$Y_i = \sum_{j=1}^{k} c_j^{(i)} P_j ,$$

où les coefficients $c_j^{(i)}$ sont pris dans un corps d'extension $GF(2^m)$ défini au moyen d'un polynôme primitif choisi, des mêmes $k \geq 1$ paquets d'information $\{P_1, P_2, \cdots, P_k\}$, dits paquets initiaux, chaque paquet d'information contenant $L \geq 1$ symboles constitués chacun d'une suite de $m > 1$ bits ;

- calculer un paquet de données utiles sortant Y' constitué par une combinaison linéaire

$$Y' = \sum_{i=1}^{r} \alpha_i Y_i$$

des paquets de données utiles Y_i, où les coefficients α_i sont pris dans ledit corps d'extension $GF(2^m)$; et

- émettre ledit paquet de données utiles sortant Y'.

Ledit dispositif de codage est remarquable en ce qu'il comprend en outre, dans le but d'effectuer au moins une multiplication $Q = a \cdot P$, requise pour le calcul du paquet de données utiles sortant Y', de tous les symboles d'un paquet de données $P = (x_1, \ldots, x_L)$ dans lequel x_j, pour $j = 1, \ldots, L$, est un symbole composé d'une suite de m bits x_{ij}, où $i = 0, \ldots, m-1$, par un même nombre a appartenant à $GF(2^m)$, des moyens pour :

- remplir une matrice binaire $\mathbf{X}$ de dimension $m \times L$ en plaçant les bits x_{ij} composant chaque symbole x_j le long de la j-ième colonne de ladite matrice $\mathbf{X}$;
- calculer la matrice binaire $\mathbf{Y} = M(a) \times \mathbf{X}$,

de dimension $m \times L$, où $M(a)$ est la matrice binaire de dimensions $m \times m$ dont les colonnes respectives contiennent les coordonnées binaires des éléments respectifs $\{a, \alpha a, \ldots, \alpha^{m-1} a\}$, où α est une racine dudit polynôme primitif, en obtenant les lignes de ladite matrice $\mathbf{Y}$ au moyen d'additions binaires de lignes de la matrice $\mathbf{X}$ selon des motifs déterminés par les lignes de la matrice $M(a)$; et

- obtenir le paquet de données $Q = (y_1, \ldots, y_L)$, dans lequel chaque symbole y_j, pour $j = 1,2, \ldots, L$, est composé des m bits y_{ij}, où $i = 0, \ldots, m-1$, situés sur la j-ième colonne de ladite matrice $\mathbf{Y}$.

Selon des caractéristiques particulières, ledit dispositif de codage comprend en outre des moyens pour extraire lesdites matrices $M(a)$, pour $a = \alpha^i$ et $i = 1,2, \ldots, m-1$, d'une matrice de référence $\mathbf{T}$ de dimension $m \times \left(2^m + m - 2\right)$.

L'invention concerne aussi, deuxièmement, un dispositif de décodage de paquets de données, comprenant des moyens pour :

- recevoir $n > 1$ paquets de données codés $R_1, R_2, \ldots, R_n$, où, pour $i = 1, \ldots, n$, chaque paquet de données codé

$$R_i = c_{i,1}P_1 + c_{i,2}P_2 + \cdots + c_{i,k}P_k = \sum_{j+1}^{k} c_{i,j}P_j$$

est une combinaison linéaire des mêmes $k \geq 1$ paquets d'information P_j contenant chacun $L \geq 1$ symboles constitués d'une suite de $m > 1$ bits, et où les coefficients $c_{i,j}$ sont pris dans un corps d'extension $GF(2^m)$ défini au moyen d'un polynôme primitif choisi ; et

- résoudre le système formé par lesdites combinaisons linéaires, de manière à obtenir lesdits paquets d'information P_j.

Ledit dispositif de décodage est remarquable en ce qu'il comprend en outre, dans le but d'effectuer au moins une multiplication $Q = a \cdot P$, requise pour la résolution dudit système de combinaisons linéaires, de tous les symboles d'un paquet de données $P = (x_1, \ldots, x_L)$ dans lequel x_j, pour $j = 1, \ldots, L$, est un symbole composé d'une suite de m bits x_{ij}, où $i = 0, \ldots, m-1$, par un même nombre a appartenant à $GF(2^m)$, des moyens pour :

- remplir une matrice binaire $\mathbf{X}$ de dimension $m \times L$ en plaçant les bits x_{ij} composant chaque symbole x_j le long de la j-ième colonne de ladite matrice $\mathbf{X}$;

- calculer la matrice binaire

$\mathbf{Y} = M(a) \times \mathbf{X}$,

de dimension $m \times L$, où $M(a)$ est la matrice binaire de dimensions $m \times m$ dont les colonnes respectives contiennent les coordonnées binaires des éléments respectifs $\{a, \alpha a, \ldots, \alpha^{m-1}a\}$, où α est une racine dudit polynôme primitif, en obtenant les lignes de ladite matrice $\mathbf{Y}$ au moyen d'additions binaires de lignes de la matrice $\mathbf{X}$ selon des motifs déterminés par les lignes de la matrice $M(a)$; et

- obtenir le paquet de données $Q = (y_1, \ldots, y_L)$, dans lequel chaque symbole y_j, pour $j = 1,2, \ldots, L$, est composé des m bits y_{ij}, où $i = 0, \ldots, m-1$, situés sur la j-ième colonne de ladite matrice $\mathbf{Y}$.

Selon des caractéristiques particulières, ledit dispositif de codage comprend en outre des moyens pour extraire lesdites matrices $M(a)$, pour $a = \alpha^i$ et $i = 1,2,...,m-1$, d'une matrice de référence $\mathbf{T}$ de dimension $m \times \left(2^m + m - 2\right)$.

Selon un troisième aspect, l'invention concerne :

- un nœud, dit nœud relais, d'un réseau de communication, comprenant un dispositif de codage tel qu'exposé succinctement ci-dessus, et
- un nœud, dit nœud destinataire, d'un réseau de communication comprenant un dispositif de décodage tel qu'exposé succinctement ci-dessus.

Naturellement, un nœud d'un réseau de communication peut comprendre à la fois un dispositif de codage et un dispositif de décodage tels qu'exposés succinctement ci-dessus.

Les avantages offerts par ces dispositifs et ces nœuds sont essentiellement les mêmes que ceux offerts par les procédés corrélatifs succinctement exposés ci-dessus.

On notera qu'il est possible de réaliser ces dispositifs dans le contexte d'instructions logicielles et/ou dans le contexte de circuits électroniques.

Selon un quatrième aspect, l'invention concerne un réseau de communication, comprenant au moins un nœud relais tel que décrit succinctement ci-dessus et au moins un nœud destinataire tel que décrit succinctement ci-dessus.

On notera que dans un tel réseau de communication, ledit nœud relais et ledit nœud destinataire doivent, pour être mutuellement compatibles, utiliser non seulement le même corps d'extension binaire $GF(2^m)$, c'est-à-dire la même valeur de m, mais en outre la même représentation de ce corps, c'est-à-dire le même polynôme primitif.

L'invention vise également un programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur. Ce programme d'ordinateur est remarquable en ce qu'il comprend des instructions pour l'exécution des étapes du procédé de codage de paquets de données succinctement exposé ci-

dessus, ou du procédé de décodage de paquets de données succinctement exposé ci-dessus, lorsqu'il est exécuté sur un ordinateur.

Les avantages offerts par ce programme d'ordinateur sont essentiellement les mêmes que ceux offerts par lesdits procédés.

D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée ci-dessous de modes de réalisation particuliers, donnés à titre d'exemples non limitatifs. La description se réfère aux figures qui l'accompagnent, dans lesquelles :

- la figure 1, décrite ci-dessus, représente l'opération effectuée par un nœud relais dans le codage de réseau,
- la figure 2, décrite ci-dessus, représente schématiquement un système de transmission T selon l'invention,
- la figure 3 représente schématiquement la structure d'un paquet de données selon un mode de réalisation de l'invention,
- la figure 4 représente la relation entre l'opération effectuée par un nœud relais R dans le codage de réseau, et la structure du paquet de données transmis par ce nœud relais R,
- la figure 5 représente, au niveau d'un nœud relais R, la relation entre les paquets de données entrants et le paquet de données transmis,
- la figure 6 représente, au niveau d'un nœud relais R, la relation entre les paquets de données entrants et le paquet de données transmis lorsqu'un paquet de données entrant est effacé,
- la figure 7 représente schématiquement un nœud relais R selon un mode de réalisation de l'invention,
- la figure 8 représente schématiquement un nœud destinataire D selon un mode de réalisation de l'invention, et
- la figure 9 représente la représentation d'un vecteur de L symboles appartenant à $GF(2^m)$ sous la forme d'une matrice binaire $m \times L$.

On va expliquer pour commencer comment on peut, selon un mode de réalisation de l'invention, transporter dans chaque paquet de données transmis les informations sur la manière dont ce paquet de données transmis a été construit à partir de paquets d'information P_i initiaux (émis par la source S). Pour

ce faire, comme illustré sur la **figure 3**, on insère, par exemple entre l'en-tête (désigné par « header » sur les figures 3, 4, 5 et 6), et la partie utile (désignée par « payload » sur ces mêmes figures) du paquet de données, une suite $\mathbf{C}$ de k symboles de m bits égaux aux coefficients dans $GF(2^m)$ de la décomposition du paquet de données utiles transmis sur k paquets d'information P_i.

Par conséquent, les identifiants des paquets P_i initiaux sont respectivement égaux à $\mathbf{C} = (0,\ldots,0,1,0,\ldots,0)$, où 1 est le i-ème symbole de m bits, les autres symboles étant nuls.

Lorsqu'un relais R du réseau N transmet un paquet d'information sans le modifier, l'identifiant est inchangé. Lorsque ce relais effectue une combinaison linéaire de paquets d'information P_i, l'identifiant contient la liste des coefficients $\{c_1, c_2, \ldots, c_k\}$ utilisés, certains des coefficients pouvant être nuls, comme illustré sur la **figure 4**.

Lorsqu'un relais R effectue une combinaison linéaire :

$$Y' = \alpha_1 Y_1 + \alpha_2 Y_2 + \cdots$$

de paquets de données utiles Y_i déjà codés par d'autres nœuds du réseau, chaque paquet de données utiles Y_i étant caractérisé par un vecteur d'identifiants $\mathbf{C}^{(i)}$, le vecteur d'identifiants $\mathbf{C}'$ du paquet de données sortant contient les combinaisons linéaires des identifiants des paquets d'entrée, comme illustré sur la **figure 5**.

Ainsi, l'opération faite sur les identifiants lors de la combinaison linéaire à coefficients dans $GF(2^m)$ est exactement la même que celle effectuée sur les paquets de données utiles ; le relais R peut donc avantageusement faire ces deux opérations en une seule fois.

On notera que cette méthode fonctionne même en cas de perte de paquets. Par exemple, si un relais R devait combiner trois paquets de données utiles Y_1, Y_2 et Y_3, mais qu'il n'a pas reçu ce dernier pour une raison quelconque, il calcule la combinaison des paquets de données utiles Y_1 et Y_2, et indique dans l'en-tête les coefficients c_i' résultant de cette combinaison, comme illustré sur la

figure 6. Autrement dit, l'en-tête d'un paquet de données utiles R_i reçu par le destinataire D indique toujours correctement la manière dont ce paquet de données utiles R_i a été obtenu à partir de paquets d'information P_i initiaux. Par conséquent, suite à la réception des paquets de données utiles $\{R_1, R_2, \ldots, R_n\}$, la matrice $\mathbf{K}$ mentionnée ci-dessus sera connue du destinataire, comme requis.

On notera également que la mise en œuvre de cette méthode ne nécessite pas de connaître la topologie du réseau, puisque l'information sur la manière dont les paquets ont été codés est transportée dans les paquets eux-mêmes. Elle est dite *non-cohérente* dans la littérature technique.

Pour retrouver les paquets d'information $\{P_1, P_2, \cdots, P_k\}$ à partir des paquets reçus, le destinataire D procède comme suit :

- la source S n'attend pas d'acquittement pour chaque paquet qu'elle transmet ;

- le destinataire D n'envoie pas d'acquittement lorsqu'il reçoit un paquet codé ;

- pour chaque paquet de données utiles $Y_i = [\mathbf{C}_i \mid R_i]$ reçu, le destinataire D extrait l'identifiant $\mathbf{C}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,k})$; on dispose ainsi d'une équation linéaire : $R_i = c_{i,1}P_1 + c_{i,2}P_2 + \cdots + c_{i,k}P_k$;

- dès que le destinataire D dispose de $n \geq k$ telles équations, il vérifie si le rang de la matrice du système est égal à k, en utilisant n'importe quelle méthode classique (par exemple la méthode de Gauss) ; l'article de C. Studholme et I. Blake intitulé « *Random matrices and codes for the erasure channel* », Algorithmica, vol. 56, n° 4, pages 605 à 620 (2010), démontre que, dans le cas d'une matrice remplie aléatoirement, la matrice est de rang égal à k avec une grande probabilité ;

- si le rang est inférieur à k, le destinataire D attend la réception de nouveaux paquets jusqu'à ce que la condition de rang égal à k soit vérifiée ; de préférence, on fixe une limite $n_{\max}$ au nombre de paquets émis par la source S, et le destinataire D envoie un acquittement négatif (NACK) s'il n'arrive pas à obtenir une matrice inversible après la fin de la transmission des $n_{\max}$ paquets ;

dans ce cas, la source envoie des paquets codés supplémentaires jusqu'à ce que le décodage soit possible ;

- une fois que cette condition est vérifiée, on résout le système linéaire suivant :

$$\begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,k} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,k} \\ \vdots & \vdots & \cdots & \vdots \\ c_{n,1} & c_{n,2} & \cdots & c_{n,k} \end{bmatrix} \times \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_k \end{bmatrix} = \begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix},$$

ce qui fait intervenir des opérations d'addition/soustraction, et de multiplication des symboles d'un paquet par un même scalaire $a \in GF(2^m)$, opérations que l'on peut, grâce à l'invention, effectuer par paquets, c'est-à-dire de manière parallélisée.

La **figure 7** représente schématiquement un nœud relais R selon un mode de réalisation de l'invention.

Le relais R comporte un module de réception 10, un module d'extraction 11, un module 12 de calcul du paquet de données utiles sortant, un module mémoire 13, un module de construction 14 et un module de transmission 15.

Le module d'entrée 10 est adapté à recevoir des paquets de données entrants de la part d'autres nœuds du réseau N, et à transmettre ces paquets de données entrants au module d'extraction 11. Le module d'extraction 11 est adapté à extraire de chaque paquet entrant son en-tête (désigné par « H » sur la figure 7), et à transmettre au module de calcul 12 le reste du paquet entrant, c'est-à-dire l'ensemble formé par un vecteur d'identifiants $\mathbf{C}^{(i)}$ et un paquet de données utiles Y_i (désigné par « payload » sur la figure 7). Le module de calcul 12 est adapté à puiser les coefficients α_i dans le module mémoire 13 pour calculer, en parallèle :

- le paquet de données utiles sortant

$Y' = \alpha_1 Y_1 + \alpha_2 Y_2 + \cdots$, et

- le vecteur d'identifiants sortant $\mathbf{C}'$, dont les composantes sont

$$c'_i = \alpha_1 c_i^{(1)} + \alpha_2 c_i^{(2)} + \cdots$$

en mettant en œuvre le procédé de multiplication dans $GF(2^m)$ selon l'invention.

On notera, concernant le module mémoire 13, que :

- ce module peut être intégré dans le relais R comme représenté sur la figure 7, ou constituer une source externe consultable par le relais R, et

- les coefficients α_i peuvent être constants pour un relais R donné, ou varier à chaque nouveau paquet entrant dans le relais R (par exemple au moyen d'un tirage au sort).

Le module de construction 14 est adapté à recevoir, d'une part l'en-tête de paquet H mentionné précédemment, et d'autre part l'ensemble formé par le vecteur d'identifiants sortant $\mathbf{C}'$ et le paquet de données utiles sortant Y', et à construire à partir de ces éléments un paquet de données sortant.

Enfin, le module de transmission 15 est adapté à recevoir le paquet de données sortant de la part du module de construction 14, et à transmettre ce paquet de données sortant sur le réseau N.

La **figure 8** représente schématiquement un nœud destinataire D selon un mode de réalisation de l'invention.

Le destinataire D comporte un module de réception 20, un module d'extraction 21, un module de construction 22, un module de second membre 23, un module de test 27, un module d'inversion 26, un module de résolution 24 et un module de transmission 25.

Le module d'extraction 21 est adapté à séparer, dans chaque paquet reçu, son en-tête (désigné par « H » sur la figure 8), son vecteur d'identifiants $\mathbf{C}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,k})$ et son paquet de données utiles R_i.

Le module de second membre 23 est adapté à recevoir de la part du module d'extraction 21, au fur et à mesure des réceptions de paquets par le module de réception 20, les paquets de données utiles R_i, et à ajouter des lignes égales à ces paquets de données utiles R_i au vecteur de second membre

$$\begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix}.$$

De même, le module de construction 22 est adapté à recevoir de la part du module d'extraction 21, au fur et à mesure des réceptions de paquets par le module de réception 20, les vecteurs d'identifiants $\mathbf{C}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,k})$, et à

ajouter des lignes constituées de ces identifiants à une matrice servant à construire la matrice $\mathbf{K}$.

De même, le module de test 27 est adapté à recevoir, au fur et à mesure des réceptions de paquets par le module de réception 20, ladite matrice en construction de la part du module de construction 22, et à déterminer si le déterminant de cette matrice est différent de zéro, c'est-à-dire si cette matrice est régulière (rang égal à k).

Lorsque ce n'est pas le cas, le fonctionnement décrit ci-dessus continue. Lorsque c'est le cas, le module de réception 20 est adapté à arrêter de recevoir des paquets, et le module d'inversion 26 est adapté à calculer l'inverse de la matrice $\mathbf{K}$ obtenue. Le module de résolution 24 est adapté à recevoir ledit vecteur de second membre de la part du module de second membre 23, ainsi que l'inverse de la matrice $\mathbf{K}$ de la part du module d'inversion 26, et à calculer le produit de ces deux grandeurs en mettant en œuvre le procédé de multiplication dans $GF(2^m)$ selon l'invention, de façon à retrouver les paquets d'information $\{P_1, P_2, \ldots, P_k\}$ initiaux.

Enfin, le module de transmission 25 est adapté à recevoir les paquets d'information $\{P_1, P_2, \ldots, P_k\}$ initiaux de la part du module de résolution 24, et à transmettre ces paquets d'information à l'utilisateur du nœud destinataire D.

Comme expliqué ci-dessus, le codage et le décodage considérés dans la présente invention sont réalisés dans un corps d'extension binaire $GF(2^m)$, où $m > 1$. On entend par là qu'à tout symbole donné composé de m bits x_{ij}, où $i = 0, \ldots, m-1$, on associe l'élément de $GF(2^m)$, noté x_j, dont les coordonnées binaires sur une base canonique $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ choisie sont précisément lesdits bits x_{ij} ; autrement dit :

$$x_j = \sum_{i=0}^{m-1} x_{ij} \alpha^i ,$$

où α est une racine d'un polynôme primitif prédéterminé.

On va expliquer à présent comment on peut effectuer la multiplication dans $GF(2^m)$ uniquement au moyen d'additions binaires (XOR).

Prenons un exemple dans le corps $GF(2^4)$ construit à partir du polynôme primitif $p(X) = X^4 + X + 1$, où α vérifie l'équation : $\alpha^4 = 1 + \alpha$. Le résultat de la multiplication de l'élément $x = x_0 + x_1\,\alpha + x_2\,\alpha^2 + x_3\alpha^3$, de coordonnées binaires $x_i \in \{0,1\}$, par l'élément $a = a_0 + a_1\,\alpha + a_2\,\alpha^2 + a_3\alpha^3$, de coordonnées binaires $a_i \in \{0,1\}$, est l'élément $y = y_0 + y_1\,\alpha + y_2\,\alpha^2 + y_3\alpha^3$ dont les coordonnées binaires $y_i \in \{0,1\}$ sont obtenues comme suit :

$$y = ax = x_0 a + x_1(\alpha a) + x_2(\alpha^2 a) + x_3(\alpha^3 a)$$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} \vdots & \vdots & \vdots & \vdots \\ a & \alpha a & \alpha^2 a & \alpha^3 a \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix} \times \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} = M(a) \times \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

par définition de la matrice $M(a)$, dont les colonnes successives sont constituées par les coordonnées binaires des éléments a, αa, $\alpha^2 a$ et $\alpha^3 a$ de $GF(2^4)$ successivement. Pour calculer ces colonnes, on notera, par exemple, que

$$\begin{aligned} \alpha a &= a_0\,\alpha + a_1\,\alpha^2 + a_2\,\alpha^3 + a_3\alpha^4 = a_0\,\alpha + a_1\,\alpha^2 + a_2\,\alpha^3 + a_3(1+\alpha) \\ &= a_3 + (a_3 + a_0)\alpha + a_1\,\alpha^2 + a_2\,\alpha^3 \end{aligned}.$$

On procède de la même façon pour $\alpha^2 a$ et $\alpha^3 a$. Le résultat final est :

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_3 + a_0 & a_3 + a_2 & a_2 + a_1 \\ a_2 & a_1 & a_3 + a_0 & a_3 + a_2 \\ a_3 & a_2 & a_1 & a_3 + a_0 \end{bmatrix} \times \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}.$$

Dans le cas général d'un corps $GF(2^m)$ pour m quelconque, on calcule :

$$Y = M(a) \times X\,, \qquad (1)$$

où :

- X est le vecteur colonne contenant les m coordonnées binaires $x_i \in \{0,1\}$ de x,
- Y est le vecteur colonne contenant les m coordonnées binaires $y_i \in \{0,1\}$ de y, et

• la matrice $M(a)$, où $a \in GF(2^m)$, est la matrice binaire $m \times m$ dont les colonnes contiennent les coordonnées binaires des éléments $\{a, \alpha a, \ldots, \alpha^{m-1}a\}$ de $GF(2^m)$, soit

$$M(a) = \begin{bmatrix} \vdots & \vdots & & \vdots \\ a & \alpha a & \cdots & \alpha^{m-1}a \\ \vdots & \vdots & & \vdots \end{bmatrix}.$$

On dira que la matrice $M(a)$ est « l'équivalent binaire » de l'élément a pour la multiplication dans $GF(2^m)$.

Comme tous les éléments non-nuls de $GF(2^m)$ peuvent être écrits sous la forme $a = \alpha^k$ pour un certain entier $0 \le k \le 2^m - 2$, on peut se contenter de considérer les matrices

$$M(\alpha^k) = \begin{bmatrix} \vdots & \vdots & & \vdots \\ \alpha^k & \alpha^{k+1} & \cdots & \alpha^{k+m-1} \\ \vdots & \vdots & & \vdots \end{bmatrix}$$

associées aux puissances consécutives de α.

On notera que toutes ces matrices peuvent être obtenues en consultant une « grande » matrice binaire

$$\mathbf{T} = \begin{bmatrix} \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha & \alpha^2 & \alpha^{k+m-1} & \cdots & \alpha^{n-1} & 1 & \alpha & \cdots & \alpha^{m-2} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \end{bmatrix},$$

où $n = 2^m - 1$, de dimension $m \times (2^m + m - 2)$, construite préalablement, dont les colonnes contiennent les coordonnées de α^k pour $k \ge 0$. Dans cette matrice $\mathbf{T}$, que l'on appellera « matrice de référence », les $(m-1)$ dernières colonnes sont une simple copie des $(m-1)$ premières colonnes. $M(\alpha^k)$ est alors la sous-matrice obtenue en extrayant les colonnes n° $(k+1)$ à $(k+m)$ de la matrice de référence $\mathbf{T}$, ce que l'on notera ainsi :

$$M(\alpha^k) = \mathbf{T}(:, k+1 : k+m), \text{ pour } k = 0, 1, \ldots, 2^m - 2.$$

Par définition, le produit de deux éléments $a = \alpha^k$ et $b = \alpha^l$ est égal à $\alpha^{\langle k+l \rangle}$, où $\langle k+l \rangle = (k+l) \bmod (2^m - 1)$, de sorte que la matrice associée au produit $\alpha^k \times \alpha^l$ est $M(\alpha^{\langle k+l \rangle})$, que l'on peut lire directement dans la matrice de

référence $\mathbf{T}$; on peut ainsi obtenir très simplement le produit des matrices $M(\alpha^k)$ et $M(\alpha^l)$ par :

$$M(\alpha^k)\times M(\alpha^l) = M(\alpha^{\langle k+l\rangle}).$$

De la même manière, la matrice associée à l'inverse d'un élément $a=\alpha^k$ est $\left[M\left(\alpha^k\right)\right]^{-1} = M(\alpha^{n-k})$, puisque $M(\alpha^k)\times M(\alpha^{n-k}) = M(\alpha^{\langle k+n-k\rangle}) = M\left(\alpha^0\right)$, qui est la matrice identité.

Si l'on prend le même exemple sur $GF(2^4)$ (construit à partir du polynôme primitif $p(X)=1+X+X^4$), la matrice de référence $\mathbf{T}$ est donnée par :

$$\mathbf{T} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix},$$

de sorte que, par exemple :

$$M(\alpha^4) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, M(\alpha^{10}) = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, M(\alpha^{14}) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

On vérifie facilement, par exemple, que le produit des matrices binaires $M(\alpha^4)\times M(\alpha^{10})$ est bien égal à $M(\alpha^{14})$ comme prévu.

En poursuivant le même exemple, on trouve :

$$M(\alpha^5) = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \text{ et } M(\alpha^5)\times M(\alpha^{10}) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = M(1),$$

de sorte que $M(\alpha^5) = \left[M(\alpha^{10})\right]^{-1}$, ou encore $\left[M(\alpha^5)\right]^{-1} = M(\alpha^{10})$.

Comme autre exemple, la multiplication par $\alpha^9 = \alpha + \alpha^3$ dans $GF(2^4)$ est donnée par le produit matriciel :

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 + x_3 \\ x_0 + x_1 + x_2 + x_3 \\ x_1 + x_2 + x_3 \\ x_0 + x_2 + x_3 \end{bmatrix}.$$

On notera que cette expression n'utilise que des XORs des coordonnées binaires $x_i \in \{0,1\}$ de l'élément x.

On peut ainsi commodément effectuer la multiplication de tout élément x de $GF(2^m)$ par tout élément $a \in GF(2^m)$ sur la base de l'équation (1) ci-dessus et des sous-matrices de la matrice de référence $\mathbf{T}$, ce qui ne fait intervenir que des XORs des coordonnées de x.

On va expliquer à présent comment on peut utiliser cette méthode pour effectuer la multiplication par tout élément $a \in GF(2^m)$ au niveau des paquets.

Le produit matriciel de l'équation (1) peut être aisément parallélisé lorsque chaque x_i est un vecteur binaire de longueur L. Par exemple, la multiplication par un élément a dans $GF(2^4)$ devient :

$$\begin{bmatrix} y_{0,1}, y_{0,2}, \ldots, y_{0,L} \\ y_{1,1}, y_{1,2}, \ldots, y_{1,L} \\ y_{2,1}, y_{2,2}, \ldots, y_{2,L} \\ y_{3,1}, y_{3,2}, \ldots, y_{3,L} \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_3 + a_0 & a_3 + a_2 & a_2 + a_1 \\ a_2 & a_1 & a_3 + a_0 & a_3 + a_2 \\ a_3 & a_2 & a_1 & a_3 + a_0 \end{bmatrix} \times \begin{bmatrix} x_{0,1}, x_{0,2}, \ldots, x_{0,L} \\ x_{1,1}, x_{1,2}, \ldots, x_{1,L} \\ x_{2,1}, x_{2,2}, \ldots, x_{2,L} \\ x_{3,1}, x_{3,2}, \ldots, x_{3,L} \end{bmatrix},$$

où, avantageusement, toutes les opérations sont effectuées dans $GF(2)$.

On utilisera ci-après la notation $x(i,:) = (x_{i,1}, x_{i,2}, \ldots, x_{i,L})$ pour dénoter la ligne n° i d'une matrice x de dimension $m \times L$; le produit matriciel ci-dessus peut alors être commodément vu comme mettant en œuvre des XORs de ces lignes $x(i,:)$. Par exemple, la multiplication par $\alpha^9 = \alpha + \alpha^3$ présentée ci-dessus peut être commodément écrite sous la forme :

$$\begin{bmatrix} y(0,:) \\ y(1,:) \\ y(2,:) \\ y(3,:) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} x(0,:) \\ x(1,:) \\ x(2,:) \\ x(3,:) \end{bmatrix} = \begin{bmatrix} x(1,:) + x(3,:) \\ x(0,:) + x(1,:) + x(2,:) + x(3,:) \\ x(1,:) + x(2,:) + x(3,:) \\ x(0,:) + x(2,:) + x(3,:) \end{bmatrix}.$$

Les considérations ci-dessus expliquent comment on peut, au cours du codage ou du décodage dans un corps de Galois $GF(2^m)$, où $m > 1$, défini au

moyen d'un polynôme primitif prédéterminé, calculer un paquet $Q = a \cdot P$, où le nombre a appartient à $GF(2^m)$, et P est un paquet de données $P = (x_1, \ldots, x_L)$, dans lequel x_j, pour $j = 1,2, \ldots, L,$, avec $L \geq 1$, est un symbole composé d'une suite de m bits x_{ij}, où $i = 0, \ldots, m-1$.

Selon le présent mode de réalisation, on met en œuvre les sous-étapes suivantes.

a) On remplit une matrice binaire $\mathbf{X}$ de dimension $m \times L$ en plaçant les bits x_{ij} composant chaque symbole x_j le long de la j-ième colonne, comme illustré schématiquement sur la **figure 9**. On désigne par $x(i,:)$ la i-ème ligne, où $i = 0, \ldots, m-1$, de cette matrice $\mathbf{X}$. Autrement dit, si l'on regarde le paquet P comme une ligne de bits numérotés de 1 à $m \times L$, la ligne $x(i,:)$ est définie par :

$$x(i,:) = P[i + 1 + lm], \text{ où } l = 0, \ldots, L-1 .$$

b) On calcule la matrice binaire $\mathbf{Y}$, de dimension $m \times L$, au moyen du produit matriciel :

$$\mathbf{Y} = M(a) \times \mathbf{X},$$

où la matrice $M(a)$ est l'équivalent binaire, défini ci-dessus, de l'élément a. Comme expliqué ci-dessus, effectuer ce produit matriciel revient à calculer les lignes de la matrice $\mathbf{Y}$ par des XORs de lignes de la matrice $\mathbf{X}$, selon des motifs binaires déterminés par les lignes de la matrice $M(a)$. On opère ainsi, avantageusement, de manière vectorielle sur les L symboles du paquet P.

c) On obtient finalement le paquet $Q = (y_1, \ldots, y_L)$, dans lequel chaque symbole y_j, pour $j = 1,2, \ldots, L$, est composé des m bits y_{ij}, où $i = 0, \ldots, m-1$, situés sur la j-ième colonne de la matrice $\mathbf{Y}$ obtenue précédemment. Autrement dit, il suffit de lire la matrice $\mathbf{Y}$ colonne par colonne.

On va, pour terminer, expliquer comment on peut utiliser cette méthode pour effectuer, toujours au niveau des paquets, la multiplication par n'importe quelle matrice $\mathbf{A}$ dont les éléments $a_{i,j}$ appartiennent à $GF(2^m)$, où $m > 1$.

En effet, une telle matrice peut être aisément transformée en une matrice binaire, que l'on appellera « image binaire » de la matrice $\mathbf{A}$, en remplaçant tous ses éléments $a_{i,j} \in GF(2^m)$ par leurs équivalents binaires $m \times m$ définis ci-dessus.

L'invention peut être mise en œuvre au sein des nœuds, par exemple un nœud relais ou un nœud destinataire d'un réseau de communication, au moyen de composants logiciels et/ou matériels.

Les composants logiciels pourront être intégrés à un programme d'ordinateur classique de gestion de nœud de réseau. C'est pourquoi, comme indiqué ci-dessus, la présente invention concerne également un système informatique. Ce système informatique comporte de manière classique une unité centrale de traitement commandant par des signaux une mémoire, ainsi qu'une unité d'entrée et une unité de sortie. De plus, ce système informatique peut être utilisé pour exécuter un programme d'ordinateur comportant des instructions pour la mise en œuvre de l'un quelconque des procédés de codage, ou de décodage, de paquets de données selon l'invention.

En effet, l'invention vise aussi un programme d'ordinateur téléchargeable depuis un réseau de communication comprenant des instructions pour l'exécution des étapes d'un procédé de codage, ou de décodage, de paquets de données selon l'invention, lorsqu'il est exécuté sur un ordinateur. Ce programme d'ordinateur peut être stocké sur un support lisible par ordinateur et peut être exécutable par un microprocesseur.

Ce programme peut utiliser n'importe quel langage de programmation, et se présenter sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations, inamovible, ou partiellement ou totalement amovible, lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comprendre un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de

circuit microélectronique, ou un moyen d'enregistrement magnétique, tel qu'un disque dur, ou encore une clé USB (« *USB flash drive* » en anglais).

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme d'ordinateur selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

En variante, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution de l'un quelconque des procédés de codage, ou de décodage, de paquets de données selon l'invention.

REVENDICATIONS

1. Procédé de codage de paquets de données dans un réseau (N), comprenant les étapes suivantes :

- réception de $r \geq 1$ paquets de données utiles Y_i constitué chacun par une combinaison linéaire

$$Y_i = \sum_{j=1}^{k} c_j^{(i)} P_j ,$$

où les coefficients $c_j^{(i)}$ sont pris dans un corps d'extension $GF(2^m)$ défini au moyen d'un polynôme primitif choisi, des mêmes $k \geq 1$ paquets d'information $\{P_1, P_2, \ldots, P_k\}$, dits paquets initiaux, chaque paquet d'information contenant $L \geq 1$ symboles constitués chacun d'une suite de $m > 1$ bits ;

- calcul d'un paquet de données utiles sortant Y' constitué par une combinaison linéaire

$$Y' = \sum_{i=1}^{r} \alpha_i Y_i$$

desdits paquets de données utiles Y_i, où les coefficients α_i sont pris dans ledit corps d'extension $GF(2^m)$; et

- émission dudit paquet de données utiles sortant Y' ;

caractérisé en ce que ladite étape de calcul du paquet de données utiles sortant Y' comprend au moins une sous-étape de multiplication $Q = a \cdot P$ de tous les symboles d'un paquet de données $P = (x_1, \ldots, x_L)$ dans lequel x_j, pour $j = 1, \ldots, L$, est un symbole composé d'une suite de m bits x_{ij}, où $i = 0, \ldots, m-1$, par un même nombre a appartenant à $GF(2^m)$, et en ce que ladite multiplication est effectuée de la manière suivante :

a) remplissage d'une matrice binaire $\mathbf{X}$ de dimension $m \times L$ en plaçant les bits x_{ij} composant chaque symbole x_j le long de la j-ième colonne de ladite matrice $\mathbf{X}$;

b) calcul de la matrice binaire

$\mathbf{Y} = M(a) \times \mathbf{X}$,

de dimension $m \times L$, où $M(a)$ est la matrice binaire de dimensions $m \times m$ dont les colonnes respectives contiennent les coordonnées binaires des éléments respectifs $\{a, \alpha a, \ldots, \alpha^{m-1} a\}$, où α est une racine dudit polynôme primitif, en obtenant les lignes de ladite matrice $\mathbf{Y}$ au moyen d'additions binaires de lignes de la matrice $\mathbf{X}$ selon des motifs déterminés par les lignes de la matrice $M(a)$; et

c) obtention du paquet de données $Q = (y_1, \ldots, y_L)$,, dans lequel chaque symbole y_j, pour $j = 1,2, \ldots, L$, est composé des m bits y_{ij}, où $i = 0, \ldots, m-1$, situés sur la j-ième colonne de ladite matrice $\mathbf{Y}$.

2. Procédé de codage selon la revendication 1, caractérisé en ce que lesdites matrices $M(a)$, pour $a = \alpha^i$ et $i = 1,2, \ldots, m-1$, sont extraites d'une matrice de référence $\mathbf{T}$ de dimension $m \times \left(2^m + m - 2\right)$.

3. Procédé de codage selon la revendication 1 ou la revendication 2, dans lequel chacun desdits paquets de données utiles Y_i est contenu dans un paquet de données contenant en outre un vecteur d'identifiants

$\mathbf{C}^{(i)} = \left(c_1^{(i)}, c_2^{(i)}, \ldots, c_k^{(i)}\right)$

comprenant lesdits coefficients $c_j^{(i)}$, et dans lequel ledit paquet de données utiles Y' est contenu dans un paquet de données contenant en outre un vecteur d'identifiants sortant

$\mathbf{C}' = \left(c'_1, c'_2, \ldots, c'_k\right)$, où $c'_j = \sum_{i=1}^{r} \alpha_i c_j^{(i)}$,

caractérisé en ce que le calcul dudit vecteur d'identifiants sortant $\mathbf{C}'$ est effectué au moyen des mêmes opérations et simultanément au calcul dudit paquet de données utiles sortant Y'.

4. Procédé de décodage de paquets de données, comprenant les étapes suivantes :

- réception de $n > 1$ paquets de données codés $R_1, R_2, \ldots, R_n$, où, pour $i = 1, \ldots, n$, chaque paquet de données codé

$$R_i = c_{i,1}P_1 + c_{i,2}P_2 + \cdots + c_{i,k}P_k = \sum_{j+1}^{k} c_{i,j}P_j$$

est une combinaison linéaire des mêmes $k \geq 1$ paquets d'information P_j contenant chacun $L \geq 1$ symboles constitués d'une suite de $m > 1$ bits, et où les coefficients $c_{i,j}$ sont pris dans un corps d'extension $GF(2^m)$ défini au moyen d'un polynôme primitif choisi, et

- résolution du système formé par lesdites combinaisons linéaires, de manière à obtenir lesdits paquets d'information P_j ,

caractérisé en ce que ladite étape de résolution d'un système de combinaisons linéaires comprend au moins une sous-étape de multiplication $Q = a \cdot P$ de tous les symboles d'un paquet de données $P = (x_1, \ldots, x_L)$ dans lequel x_j, pour $j = 1, \ldots, L$, est un symbole composé d'une suite de m bits x_{ij}, où $i = 0, \ldots, m-1$, par un même nombre a appartenant à $GF(2^m)$, et en ce que ladite multiplication est effectuée de la manière suivante :

a) remplissage d'une matrice binaire $\mathbf{X}$ de dimension $m \times L$ en plaçant les bits x_{ij} composant chaque symbole x_j le long de la j-ième colonne de ladite matrice $\mathbf{X}$;

b) calcul de la matrice binaire

$\mathbf{Y} = M(a) \times \mathbf{X}$,

de dimension $m \times L$, où la matrice $M(a)$ est la matrice binaire de dimensions $m \times m$ dont les colonnes respectives contiennent les coordonnées binaires des éléments respectifs $\{a, \alpha a, \ldots, \alpha^{m-1}a\}$, où α est une racine dudit polynôme primitif, en obtenant les lignes de ladite matrice $\mathbf{Y}$ au moyen d'additions binaires de lignes de la matrice $\mathbf{X}$ selon des motifs déterminés par les lignes de la matrice $M(a)$; et

c) obtention du paquet de données $Q = (y_1, \ldots, y_L)$, dans lequel chaque symbole y_j, pour $j = 1,2, \ldots, L$, est composé des m bits y_{ij}, où $i = 0, \ldots, m-1$, situés sur la j-ième colonne de ladite matrice $\mathbf{Y}$.

5. Procédé de décodage selon la revendication 4, caractérisé en ce que lesdites matrices $M(a)$, pour $a = \alpha^i$ et $i = 1,2, \ldots, m-1$, sont extraites d'une matrice de référence $\mathbf{T}$ de dimension $m \times \left(2^m + m - 2\right)$.

6. Dispositif de codage de paquets de données, comprenant des moyens pour :

- recevoir $r \geq 1$ paquets de données utiles Y_i constitué chacun par une combinaison linéaire

$$Y_i = \sum_{j=1}^{k} c_j^{(i)} P_j ,$$

où les coefficients $c_j^{(i)}$ sont pris dans un corps d'extension $GF(2^m)$ défini au moyen d'un polynôme primitif choisi, des mêmes $k \geq 1$ paquets d'information $\{P_1, P_2, \cdots, P_k\}$,, dits paquets initiaux, chaque paquet d'information contenant $L \geq 1$ symboles constitués chacun d'une suite de $m > 1$ bits ;

- calculer un paquet de données utiles sortant Y' constitué par une combinaison linéaire

$$Y' = \sum_{i=1}^{r} \alpha_i Y_i$$

des paquets de données utiles Y_i, où les coefficients α_i sont pris dans ledit corps d'extension $GF(2^m)$; et

- émettre ledit paquet de données utiles sortant Y' ;

caractérisé en ce qu'il comprend en outre, dans le but d'effectuer au moins une multiplication $Q = a \cdot P$, requise pour le calcul du paquet de données utiles sortant Y', de tous les symboles d'un paquet de données $P = (x_1, \ldots, x_L)$ dans lequel x_j, pour $j = 1, \ldots, L$, est un symbole composé d'une suite de m bits x_{ij},

où $i = 0, \ldots, m-1$, par un même nombre a appartenant à $GF(2^m)$, des moyens pour :

- remplir une matrice binaire $\mathbf{X}$ de dimension $m \times L$ en plaçant les bits x_{ij} composant chaque symbole x_j le long de la j-ième colonne de ladite matrice $\mathbf{X}$;

- calculer la matrice binaire

$\mathbf{Y} = M(a) \times \mathbf{X}$,

de dimension $m \times L$, où $M(a)$ est la matrice binaire de dimensions $m \times m$ dont les colonnes respectives contiennent les coordonnées binaires des éléments respectifs $\{a, \alpha a, \ldots, \alpha^{m-1} a\}$, où α est une racine dudit polynôme primitif, en obtenant les lignes de ladite matrice $\mathbf{Y}$ au moyen d'additions binaires de lignes de la matrice $\mathbf{X}$ selon des motifs déterminés par les lignes de la matrice $M(a)$; et

- obtenir le paquet de données $Q = (y_1, \ldots, y_L)$, dans lequel chaque symbole y_j, pour $j = 1,2, \ldots, L$, est composé des m bits y_{ij}, où $i = 0, \ldots, m-1$, situés sur la j-ième colonne de ladite matrice $\mathbf{Y}$.

7. Dispositif de codage selon la revendication 6, caractérisé en ce qu'il comprend en outre des moyens pour extraire lesdites matrices $M(a)$, pour $a = \alpha^i$ et $i = 1,2, \ldots, m-1$, d'une matrice de référence $\mathbf{T}$ de dimension $m \times \left(2^m + m - 2\right)$.

8. Dispositif de codage selon la revendication 6 ou la revendication 7, caractérisé en ce que, chacun desdits paquets de données utiles Y_i étant contenu dans un paquet de données contenant en outre un vecteur d'identifiants

$\mathbf{C}^{(i)} = \left(c_1^{(i)}, c_2^{(i)}, \ldots, c_k^{(i)}\right)$

comprenant lesdits coefficients $c_j^{(i)}$, et ledit paquet de données utiles Y' étant contenu dans un paquet de données contenant en outre un vecteur d'identifiants sortant

$\mathbf{C}'=(c'_1, c'_2, ..., c'_k)$, où $c'_j = \sum_{i=1}^{r} \alpha_i c_j^{(i)}$,

il comprend en outre des moyens pour effectuer le calcul dudit vecteur d'identifiants sortant $\mathbf{C}'$ au moyen des mêmes opérations et simultanément au calcul dudit paquet de données utiles sortant Y'.

9. Dispositif de décodage de paquets de données, comprenant des moyens pour :

- recevoir $n > 1$ paquets de données codés $R_1, R_2, \ldots, R_n$, où, pour $i = 1, \ldots, n$, chaque paquet de données codé

$$R_i = c_{i,1}P_1 + c_{i,2}P_2 + \cdots + c_{i,k}P_k = \sum_{j+1}^{k} c_{i,j}P_j$$

est une combinaison linéaire des mêmes $k \geq 1$ paquets d'information P_j contenant chacun $L \geq 1$ symboles constitués d'une suite de $m > 1$ bits, et où les coefficients $c_{i,j}$ sont pris dans un corps d'extension $GF(2^m)$ défini au moyen d'un polynôme primitif choisi ; et

- résoudre le système formé par lesdites combinaisons linéaires, de manière à obtenir lesdits paquets d'information P_j ;

caractérisé en ce qu'il comprend en outre, dans le but d'effectuer au moins une multiplication $Q = a \cdot P$, requise pour la résolution dudit système de combinaisons linéaires, de tous les symboles d'un paquet de données $P = (x_1, \ldots, x_L)$ dans lequel x_j, pour $j = 1, \ldots, L$, est un symbole composé d'une suite de m bits x_{ij}, où $i = 0, \ldots, m-1$, par un même nombre a appartenant à $GF(2^m)$, des moyens pour :

- remplir une matrice binaire $\mathbf{X}$ de dimension $m \times L$ en plaçant les bits x_{ij} composant chaque symbole x_j le long de la j-ième colonne de ladite matrice $\mathbf{X}$;

- calculer la matrice binaire

$\mathbf{Y} = M(a) \times \mathbf{X}$,

de dimension $m \times L$, où $M(a)$ est la matrice binaire de dimensions $m \times m$ dont les colonnes respectives contiennent les coordonnées binaires des éléments respectifs $\{a, \alpha a, \ldots, \alpha^{m-1} a\}$, où α est une racine dudit polynôme primitif, en obtenant les lignes de ladite matrice $\mathbf{Y}$ au moyen d'additions binaires de lignes de la matrice $\mathbf{X}$ selon des motifs déterminés par les lignes de la matrice $M(a)$; et

- obtenir le paquet de données $Q = (y_1, \ldots, y_L)$, dans lequel chaque symbole y_j, pour $j = 1,2, \ldots, L,$, est composé des m bits y_{ij}, où $i = 0, \ldots, m-1$, situés sur la j-ième colonne de ladite matrice $\mathbf{Y}$.

10. Dispositif de décodage selon la revendication 9, caractérisé en ce qu'il comprend en outre des moyens pour extraire lesdites matrices $M(a)$, pour $a = \alpha^i$ et $i = 1,2, \ldots, m-1$, d'une matrice de référence $\mathbf{T}$ de dimension $m \times \left(2^m + m - 2\right)$.

11. Nœud, dit nœud relais (R), d'un réseau de communication (N), caractérisé en ce qu'il comprend un dispositif de codage selon l'une quelconque des revendications 6 à 8.

12. Nœud, dit nœud destinataire (D), d'un réseau de communication (N), caractérisé en ce qu'il comprend un dispositif de décodage selon la revendication 9 ou la revendication 10.

13. Réseau de communication (N), comprenant au moins un nœud relais (R) selon la revendication 11 et au moins un nœud destinataire (D) selon la revendication 12.

14. Moyen de stockage de données inamovible, ou partiellement ou totalement amovible, comportant des instructions de code de programme informatique pour l'exécution des étapes d'un procédé de codage de paquets de données selon l'une quelconque des revendication 1 à 3, ou d'un procédé de décodage de paquets de données selon la revendication 4 ou la revendication 5.

15. Programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions pour l'exécution des étapes d'un procédé de codage de paquets de données selon l'une quelconque des revendication 1 à 3, ou d'un procédé de décodage de paquets de données selon la revendication 4 ou la revendication 5, lorsqu'il est exécuté sur un ordinateur.

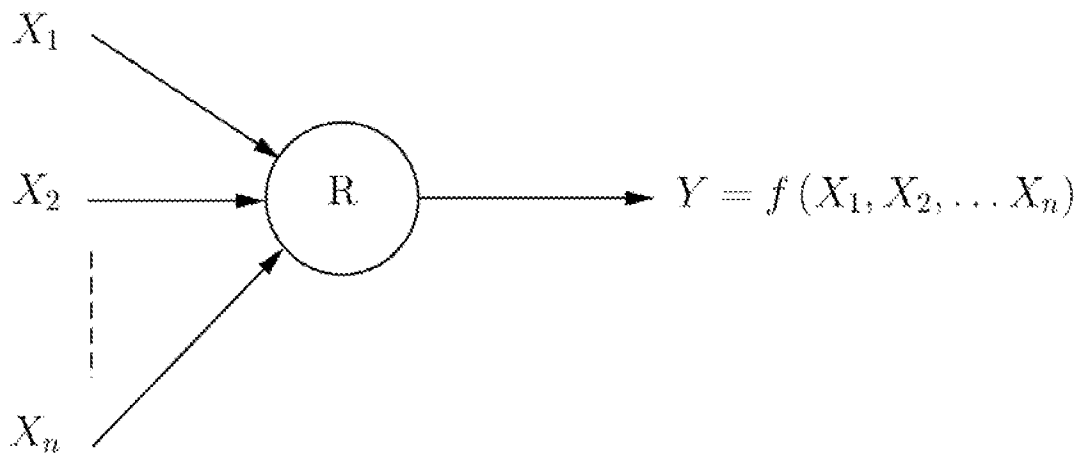

X_1
X_2
X_n
R
$Y = f(X_1, X_2, \ldots X_n)$

FIG. 1

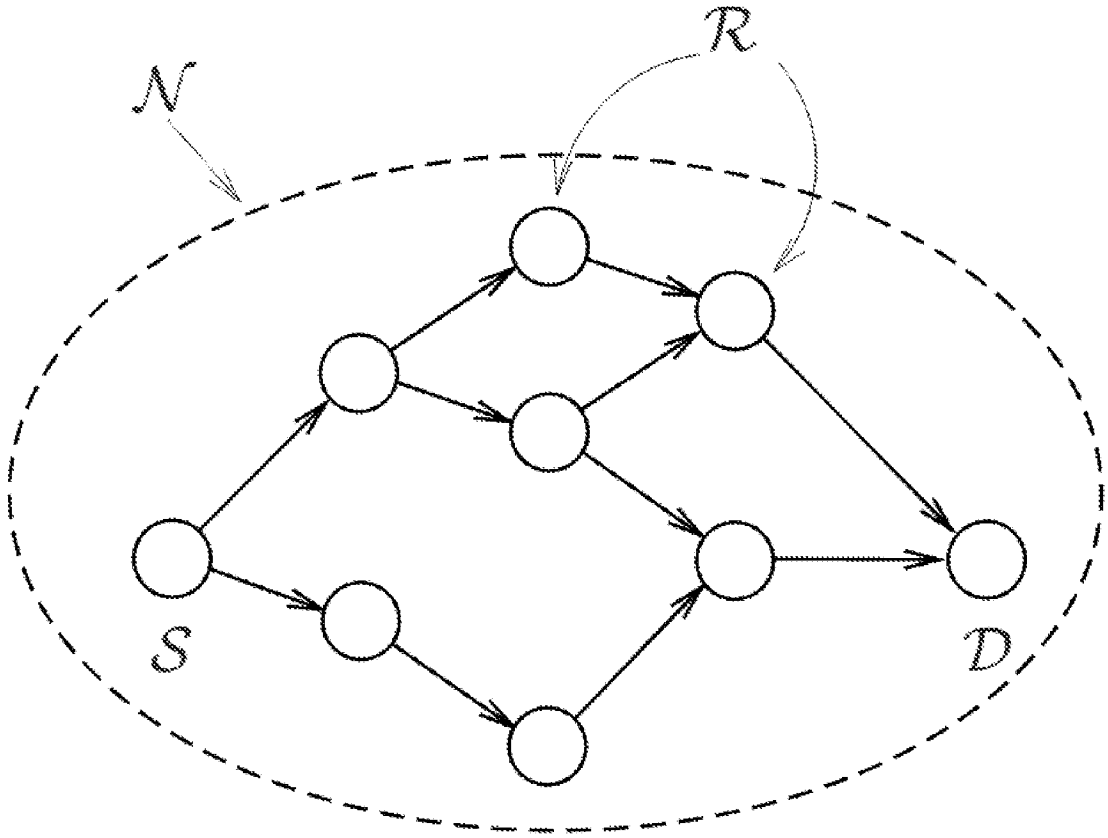

$\mathcal{N}$
$\mathcal{R}$
$\mathcal{S}$
$\mathcal{D}$

FIG. 2

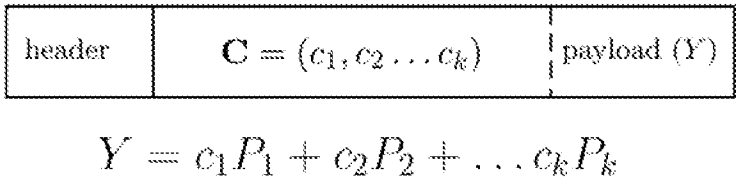


FIG. 3

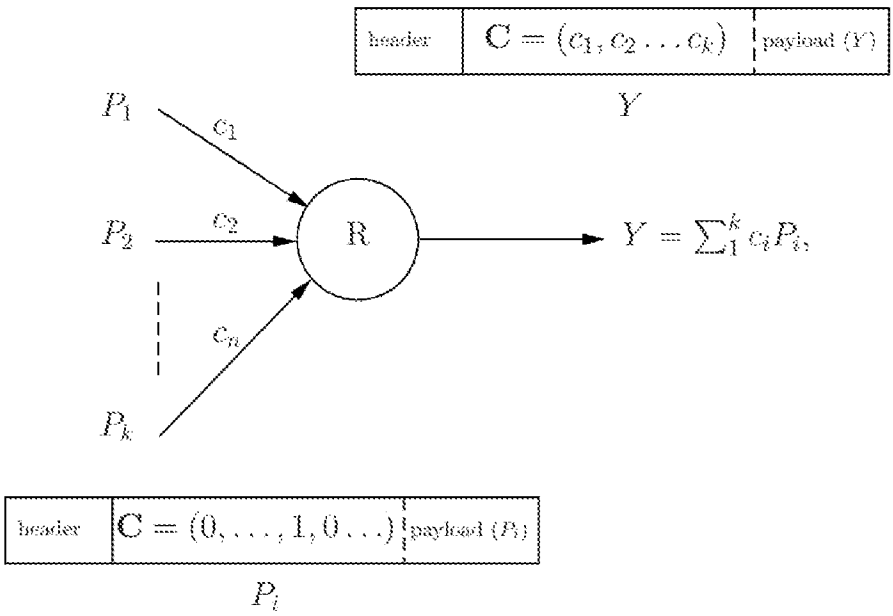


FIG. 4

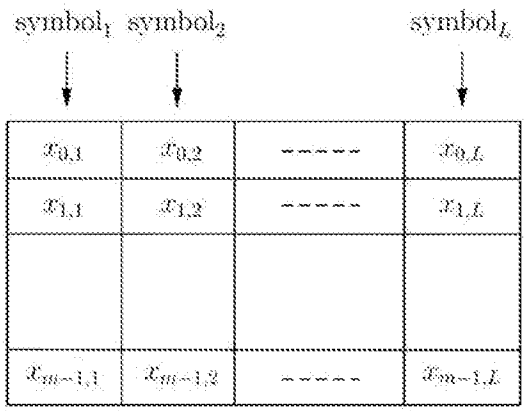


FIG. 9

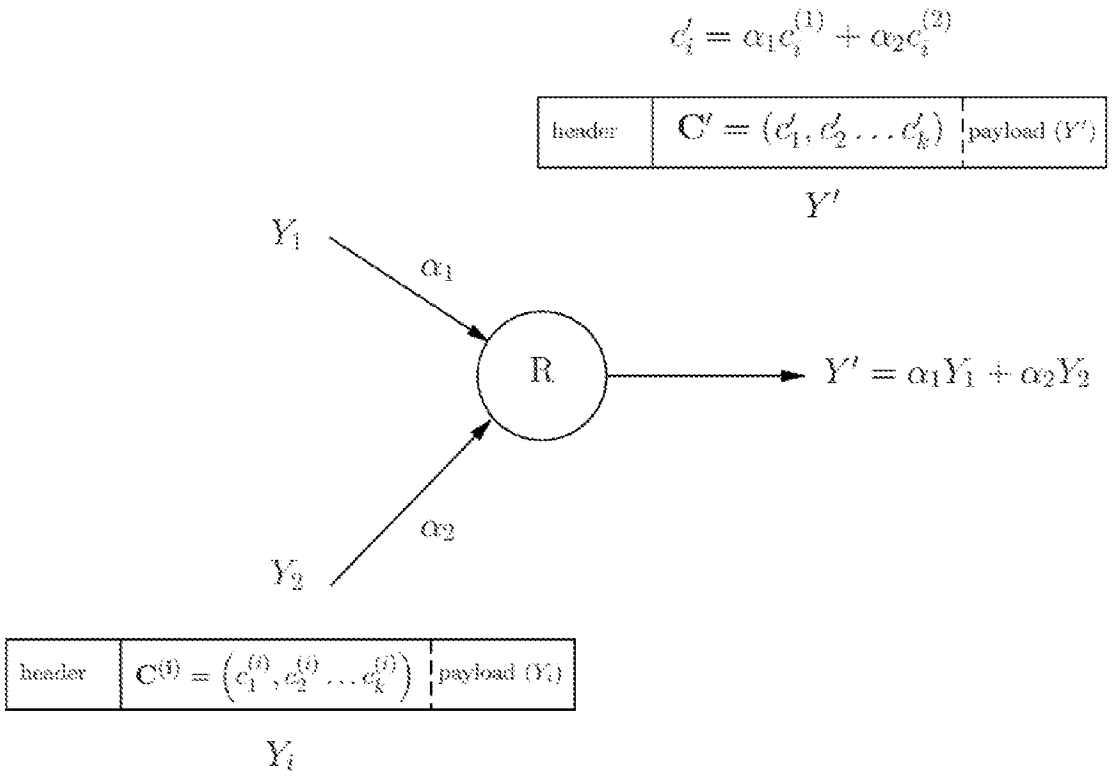

$c'_i = \alpha_1 c_i^{(1)} + \alpha_2 c_i^{(2)}$
header
$\mathbf{C}' = (c'_1, c'_2 \ldots c'_k)$
payload (Y')
Y'
Y_1
α_1
R
$Y' = \alpha_1 Y_1 + \alpha_2 Y_2$
α_2
Y_2
header
$\mathbf{C}^{(i)} = \left(c_1^{(i)}, c_2^{(i)} \ldots c_k^{(i)}\right)$
payload (Y_i)
Y_i

FIG. 5

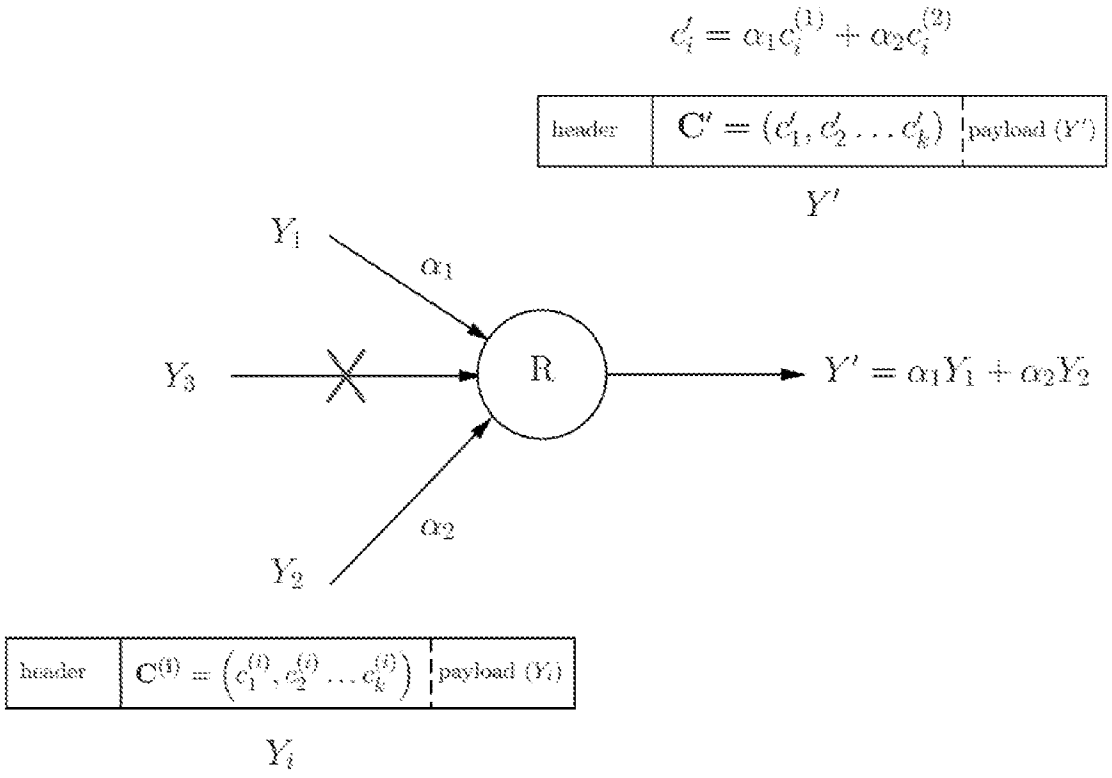

$c'_i = \alpha_1 c_i^{(1)} + \alpha_2 c_i^{(2)}$
header
$\mathbf{C}' = (c'_1, c'_2 \ldots c'_k)$
payload (Y')
Y'
Y_1
α_1
Y_3
R
$Y' = \alpha_1 Y_1 + \alpha_2 Y_2$
α_2
Y_2
header
$\mathbf{C}^{(i)} = \left(c_1^{(i)}, c_2^{(i)} \ldots c_k^{(i)}\right)$
payload (Y_i)
Y_i

FIG. 6

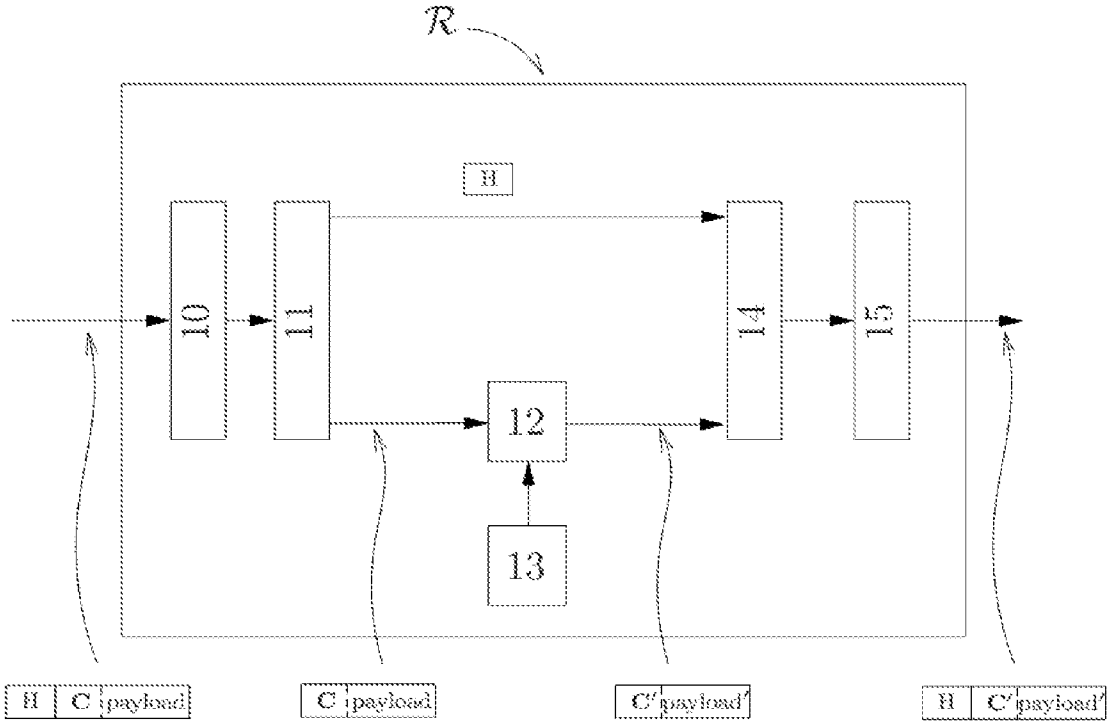

R
H
10
11
12
13
14
15
H C payload
C payload
C' payload'
H C' payload'

FIG. 7

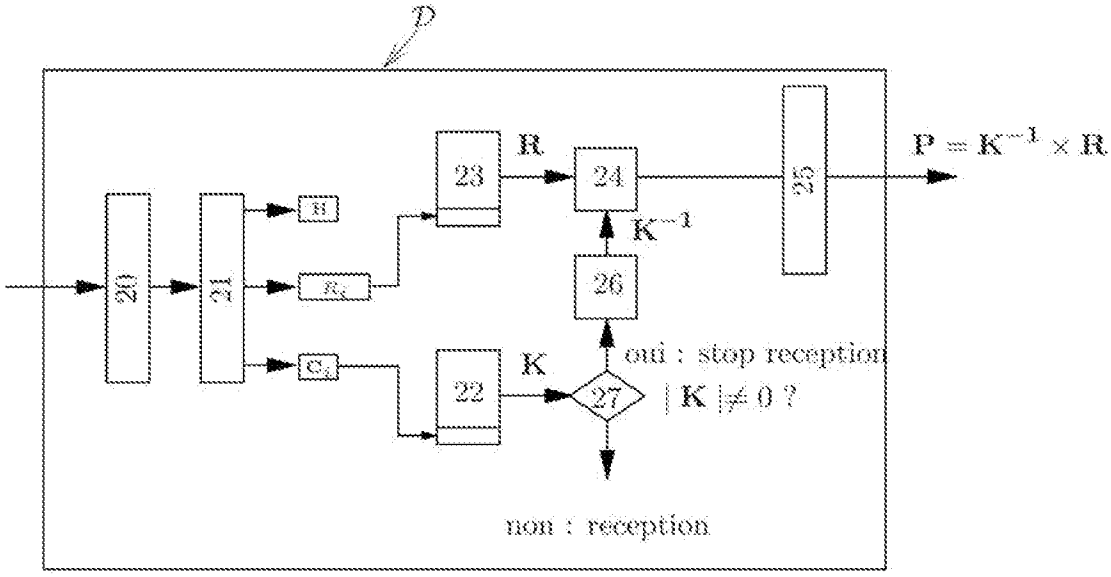

D
20
21
H
K
C
22
23
R
24
K⁻¹
25
26
27
K
out : stop reception
| K | ≠ 0 ?
non : reception
P = K⁻¹ × R

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2018/050770

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L1/00 H03M13/00
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)
H04L H03M

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	AISHWARYA NAGARAJAN ET AL: "Galois field hardware architectures for network coding", ARCHITECTURES FOR NETWORKING AND COMMUNICATIONS SYSTEMS, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA, 25 October 2010 (2010-10-25), pages 1-9, XP058122870, DOI: 10.1145/1872007.1872051 ISBN: 978-1-4503-0379-8	1,3,4,6, 8,9, 11-15
A	Section 2	2,5,7,10
	----- -/--	

[X] Further documents are listed in the continuation of Box C. [ ] 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
20 June 2018	02/07/2018

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	Gabry, Frederic

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2018/050770

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	HAINING FAN ET AL: "A survey of some recent bit-parallel GF(2n) multipliers", FINITE FIELDS AND THEIR APPLICATIONS, vol. 32, no. 32, 1 March 2015 (2015-03-01) , pages 5-43, XP055431227, US ISSN: 1071-5797, DOI: 10.1016/j.ffa.2014.10.008	1,3,4,6, 8,9, 11-15
A	Section 2.1.2; page 15 - page 16	2,5,7,10

A	NICOLA PETRA ET AL: "High speed galois fields GF(2m) multipliers", CIRCUIT THEORY AND DESIGN, 2007. ECCTD 2007. 18TH EUROPEAN CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 27 August 2007 (2007-08-27), pages 468-471, XP031257785, ISBN: 978-1-4244-1341-6 Section II	1-15

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2018/050770

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L1/00 H03M13/00
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)
H04L H03M

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

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	AISHWARYA NAGARAJAN ET AL: "Galois field hardware architectures for network coding", ARCHITECTURES FOR NETWORKING AND COMMUNICATIONS SYSTEMS, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA, 25 octobre 2010 (2010-10-25), pages 1-9, XP058122870, DOI: 10.1145/1872007.1872051 ISBN: 978-1-4503-0379-8	1,3,4,6, 8,9, 11-15
A	Section 2	2,5,7,10
	----- -/--	

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

[ ] 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
20 juin 2018	02/07/2018

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	Gabry, Frederic

1

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	HAINING FAN ET AL: "A survey of some recent bit-parallel GF(2n) multipliers", FINITE FIELDS AND THEIR APPLICATIONS, vol. 32, no. 32, 1 mars 2015 (2015-03-01), pages 5-43, XP055431227, US ISSN: 1071-5797, DOI: 10.1016/j.ffa.2014.10.008	1,3,4,6, 8,9, 11-15
A	Section 2.1.2; page 15 - page 16	2,5,7,10

A	NICOLA PETRA ET AL: "High speed galois fields GF(2m) multipliers", CIRCUIT THEORY AND DESIGN, 2007. ECCTD 2007. 18TH EUROPEAN CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 27 août 2007 (2007-08-27), pages 468-471, XP031257785, ISBN: 978-1-4244-1341-6 Section II	1-15
