

①②

DEMANDE DE BREVET D'INVENTION

A1

②② Date de dépôt : 14.09.00.

③⑦ Priorité :

④③ Date de mise à la disposition du public de la demande : 15.03.02 Bulletin 02/11.

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

⑥⑦ Références à d'autres documents nationaux apparentés :

⑦① Demandeur(s) : RIVIERE JEAN ROLAND — FR.

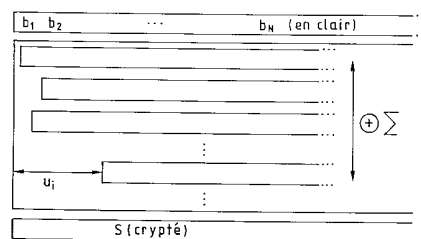
⑦② Inventeur(s) : RIVIERE JEAN ROLAND, FAY CYRIL, LEPRIEUR FREDERIC et BARBOT JEAN PIERRE.

⑦③ Titulaire(s) :

⑦④ Mandataire(s) : RINUY SANTARELLI.

⑤④ PROCÉDE ET DISPOSITIF DE TRANSFORMATION DE DONNÉES A CARACTERE CONVOLUTIF ET DECALAGES VARIABLES, ET SYSTEMES LES METTANT EN OEUVRE.

⑤⑦ Pour transformer une séquence de N données binaires d'origine ($b_1, \dots, b_N$) représentative d'un message, à l'aide d'au moins une clé, N étant un entier supérieur à 1, on élabore une séquence ($u_1, \dots, u_N$) de N valeurs algébriques de décalage et on remplit un tableau à N+1 lignes où: on écrit la séquence d'origine ($b_1, \dots, b_N$) sur la première ligne du tableau; pour chaque entier i compris entre 1 et N, on écrit sur la (i+1)^{ème} ligne du tableau une séquence intermédiaire d'éléments binaires décalée en entier ou par parties de u_i colonnes par rapport à la séquence écrite sur la première ligne; la séquence intermédiaire étant, soit une séquence prédéterminée contenue dans la clé si la $i^{\text{ème}}$ donnée binaire (b_i) de la séquence d'origine vaut 1, soit une séquence de zéros sinon; et on additionne modulo 2, colonne par colonne, les éléments binaires contenus dans le tableau.



**PROCEDE ET DISPOSITIF DE TRANSFORMATION DE DONNEES
A CARACTERE CONVOLUTIF ET DECALAGES VARIABLES,
ET SYSTEMES LES METTANT EN ŒUVRE**

5 La présente invention se rapporte à un procédé et à un dispositif de transformation de données, qui sont à caractère convolutif et décalages de préférence variables, et à des systèmes les mettant en œuvre.

 On considère la situation où un ensemble d'informations à transmettre est représenté par une séquence de symboles appartenant à
10 l'ensemble $\{0,1\}$. Cet ensemble est appelé l'alphabet binaire et ses éléments sont appelés des éléments binaires ou bits.

 Pour transmettre ces éléments binaires, on les convertit en grandeurs électriques. Par exemple, le bit 0 est représenté par un signal électrique positif et le bit 1, par un signal électrique négatif.

15 Ces signaux peuvent prendre toute valeur jugée appropriée selon l'application envisagée, telle que, par exemple, une tension électrique de ± 5 volts.

 Il peut être intéressant de crypter un message formé de tels éléments binaires, par exemple, à des fins de protection de données ou encore
20 de correction d'erreurs.

 Le message qu'on cherche à crypter peut être constitué de signaux représentatifs de parole et/ou d'images et/ou de données.

 On sait par exemple protéger des trames binaires de données en utilisant une clé.

25 On connaît notamment une méthode pour crypter des trames de données binaires qui utilise une clé ainsi que des décalages successifs réguliers et égaux.

 La figure 1 illustre une méthode connue de ce type. Celle-ci consiste à transformer une séquence de N données binaires d'origine ($b_1, \dots, b_N$)
30 représentative d'un message. Cette méthode de l'art antérieur utilise une clé K contenant une séquence déterminée de M éléments binaires ($c_1, \dots, c_M$), N et M

étant des entiers supérieurs à 1. Comme le montre la figure 1, suivant cette méthode, on remplit un tableau à $N+1$ lignes comme suit :

- on écrit la séquence d'origine $(b_1, \dots, b_N)$ en clair sur la première ligne du tableau ;
- 5 - pour chaque entier i compris entre 1 et N , on écrit sur la $(i+1)^{\text{ième}}$ ligne du tableau une séquence intermédiaire d'éléments binaires, décalée, par rapport à la séquence d'origine écrite sur la première ligne, d'autant de bits qu'indiqué par l'indice i de ligne, c'est-à-dire qu'on décale la séquence intermédiaire d'une colonne par rapport à la séquence écrite sur la ligne
- 10 précédente.

Comme le montre la figure 1, la séquence intermédiaire correspond, sur chaque ligne i , au message de départ multiplié bit à bit par la valeur du $i^{\text{ème}}$ bit de la clé K (ou additionné modulo 2, bit à bit, au $i^{\text{ème}}$ bit de la clé K , ce qui revient évidemment au même).

- 15 Le message crypté S est le résultat de l'addition modulo 2, colonne par colonne, des différentes lignes du tableau, soit :

$$S = \oplus \sum_{i=1}^M b_i \times c_i$$

où $\oplus$ désigne l'addition modulo 2.

- 20 **La figure 2** illustre ce mode de cryptage classique de façon plus détaillée à l'aide d'un exemple où $N = 6$ et $M = 4$.

L'invention a pour objet de permettre un codage encore plus fiable, tout en conservant les avantages des codages connus, et pouvant être plus rapide au point de pouvoir être effectué en temps réel.

- 25 Dans ce but, la présente invention propose un procédé transformation d'une séquence de N données binaires d'origine représentative d'un message, à l'aide d'au moins une clé, N étant un entier supérieur à 1, ce procédé étant caractérisé en ce qu'on élabore une séquence $(u_1, \dots, u_N)$ de N valeurs algébriques de décalage et on effectue des étapes suivant lesquelles :

- (a) on remplit un tableau à $N+1$ lignes comme suit :
- 30 - on écrit la séquence d'origine sur la première ligne du tableau ;

- pour chaque entier i compris entre 1 et N , on écrit sur la $(i+1)^{\text{ième}}$ ligne du tableau une séquence intermédiaire d'éléments binaires décalée en entier ou par parties de u_i colonnes par rapport à la séquence écrite sur la première ligne, ladite séquence intermédiaire étant, soit une séquence prédéterminée contenue dans la clé si la $i^{\text{ème}}$ donnée binaire de la séquence d'origine vaut 1, soit une séquence de zéros sinon ; et

(b) on additionne modulo 2, colonne par colonne, les éléments binaires contenus dans le tableau, de façon à obtenir une séquence de données binaires transformée.

Il est important de noter que la notion de ligne utilisée dans la définition donnée ci-dessus de l'invention ne doit pas être considérée comme impliquant une quelconque direction dans l'espace : une telle ligne peut ainsi être aussi bien horizontale (sens habituel du terme) que vertical ; de toute façon, le concept de l'invention n'est en rien modifié si l'on échange les notions de ligne et de colonne.

Ainsi que cela sera montré à propos de la figure 6, la présente invention propose un codage qui se rapproche du codage connu, mais elle permet une meilleure sécurité que ce codage dans la mesure où il y a un décalage entre les lignes intermédiaires qui peut être variable, c'est-à-dire ne pas être systématiquement supérieur d'une unité au décalage de la ligne qui précède. En outre, dans la mesure où chacune de ces lignes intermédiaires dépend que d'un seul terme du signal d'origine, il n'est pas nécessaire d'attendre de disposer du signal complet pour élaborer ces lignes intermédiaires, permettant un codage en temps réel. Il en résulte une plus grande rapidité, rendant ce codage tout à fait approprié pour le codage d'une grande quantité de signaux, par exemple pour le transfert d'images.

L'invention peut ainsi s'appliquer au traitement d'images, au traitement de signaux numériques de signification quelconque, dans un réseau de télécommunications par exemple ; elle peut aussi servir à la correction d'erreurs (traîne de calcul). Elle, permet, en entrant des clés particulières de casser des codes, suivant l'occultation, ou non, de la traîne des messages.

Comme dans les solutions connues, il suffit de connaître la clé et le mode de détermination des décalages pour assurer un décodage fiable du signal parvenu à destination.

Selon une caractéristique particulière préférée, on décale ladite
5 séquence intermédiaire en entier, mais on peut aussi, selon l'invention, ne décaler qu'une partie, par exemple en copiant une première moitié de la clé sans décalage et en n'appliquant un décalage qu'à la deuxième moitié de la clé. En outre, le décalage entre deux lignes intermédiaires successives est de préférence non identique pour toutes les lignes (ou pour toutes les parties de
10 ces lignes que l'on veut décaler).

Les valeurs de décalage peuvent être choisies dans une gamme quelconque : elles sont par exemple des valeurs choisies dans la gamme allant de 1 à 256 (à l'intérieur donc d'un octet) ; il est même envisageable d'admettre des valeurs négatives si on le souhaite (tout dépend de la complexité de la clé
15 que l'on est prêt à accepter).

Selon une autre caractéristique particulière préférée, pour chaque entier i compris entre 1 et N , on détermine la valeur de décalage u_i associée à la $(i+1)^{\text{ème}}$ ligne à partir d'une certaine partie de la clé. Dans toute la suite, la clé est notée K et la partie de la clé pouvant servir à déterminer la valeur de
20 décalage u_i est notée $v(i,K)$.

De manière avantageuse, pour chaque entier i compris entre 1 et N , on obtient cette partie $v(i,K)$ de la clé K à partir de la valeur de l'indice de ligne i et éventuellement d'autres éléments binaires contenus dans la clé K . Ainsi, à titre d'exemple avantageux, la clé K contient une séquence spécifique de P
25 éléments binaires $(d_1, \dots, d_P)$, P étant un entier supérieur à 1, et, pour chaque entier i compris entre 1 et N , on détermine ladite partie $v(i,K)$ de la clé K à partir de la valeur de l'indice de ligne i et de ladite séquence spécifique $(d_1, \dots, d_P)$. Diverses manières pour ce faire sont possibles, par exemple par multiplication de i par la valeur de d_i .

30 Dans le même but que celui indiqué plus haut, la présente invention propose également un dispositif de transformation d'une séquence de N données binaires d'origine représentative d'un message, à l'aide d'au moins

une clé, N étant un entier supérieur à 1, ce dispositif étant caractérisé en ce qu'il comporte des moyens pour élaborer une séquence $(u_1, \dots, u_N)$ de N valeurs algébriques de décalage et :

- (a) des moyens pour remplir un tableau à $N+1$ lignes, comportant :
- 5 - des moyens pour écrire la séquence d'origine sur la première ligne du tableau ;
 - des moyens pour écrire, pour chaque entier i compris entre 1 et N , sur la $(i+1)^{\text{ème}}$ ligne du tableau, une séquence intermédiaire d'éléments binaires décalée en entier ou par parties de u_i
 - 10 colonnes par rapport à la séquence écrite sur la première ligne, u_i étant une valeur de décalage choisie, ladite séquence intermédiaire étant, soit une séquence prédéterminée contenue dans la clé si la $i^{\text{ème}}$ donnée binaire de la séquence d'origine vaut 1, soit une séquence de zéros sinon ; et
 - 15 (b) des moyens pour additionner modulo 2, colonne par colonne, les éléments binaires contenus dans le tableau, de façon à obtenir une séquence de données binaires transformée.

Les commentaires précités concernant le procédé s'appliquent à un tel dispositif.

- 20 La présente invention vise aussi un appareil de traitement de signaux numériques, comportant des moyens adaptés à mettre en œuvre un procédé de transformation tel que ci-dessus.

La présente invention vise aussi un appareil de traitement de signaux numériques, comportant un dispositif de transformation tel que ci-dessus.

- 25 La présente invention vise aussi un réseau de télécommunications, comportant des moyens adaptés à mettre en œuvre un procédé de transformation tel que ci-dessus.

La présente invention vise aussi un réseau de télécommunications, comportant un dispositif de transformation tel que ci-dessus.

- 30 La présente invention vise aussi une station mobile et/ou de base dans un réseau de télécommunications, comportant des moyens adaptés à mettre en œuvre un procédé de transformation tel que ci-dessus.

La présente invention vise aussi une station mobile et/ou de base dans un réseau de télécommunications, comportant un dispositif de transformation tel que ci-dessus.

5 La présente invention vise aussi un dispositif de traitement de signaux représentatifs de parole, comportant des moyens adaptés à mettre en œuvre un procédé de transformation tel que ci-dessus.

La présente invention vise aussi un dispositif de traitement de signaux représentatifs de parole, comportant un dispositif de transformation tel que ci-dessus.

10 Ces appareils de traitement de signaux numériques, réseaux de télécommunications, stations mobiles et/ou de base et dispositifs de traitement de signaux représentatifs de parole ayant des caractéristiques et particularités similaires à celles du procédé de transformation selon l'invention, celles-ci ne sont pas répétées ici.

15 D'autres aspects et avantages de l'invention ressortent de la description détaillée qui suit de modes particuliers de réalisation, donnés à titre d'exemples non limitatifs. La description se réfère aux dessins qui l'accompagnent, dans lesquels :

20 - la figure 1, déjà décrite, illustre schématiquement une technique de cryptage conforme à l'art antérieur ;

- la figure 2, déjà décrite, illustre schématiquement un exemple numérique d'application de la technique de cryptage connue de la figure 1 ;

- la figure 3 illustre la façon d'utiliser la commutativité de l'addition dans la présente invention ;

25 - la figure 4 est un organigramme illustrant des étapes d'un procédé de transformation conforme à la présente invention, dans un mode particulier de réalisation ;

- la figure 5 illustre schématiquement la technique de transformation conforme à la présente invention, dans un mode particulier de réalisation ;

30 - la figure 6 illustre schématiquement un exemple numérique d'application de la technique de transformation de la figure 5, dans un mode particulier de réalisation ;

- la figure 7 illustre schématiquement la façon d'obtenir des valeurs de décalage pour transformer une séquence d'origine conformément à la présente invention, dans un mode particulier de réalisation ;

5 - la figure 8 est un schéma bloc illustrant un dispositif de transformation conforme à la présente invention, dans un mode particulier de réalisation ;

- la figure 9 représente schématiquement un dispositif électronique comportant un dispositif de transformation conforme à la présente invention, dans un autre mode particulier de réalisation ; et

10 - la figure 10 est une vue schématique simplifiée d'un réseau de télécommunications sans fil susceptible de mettre en œuvre l'invention.

On considère dans ce qui suit une séquence de N données binaires d'origine $(b_1, \dots, b_n)$, N étant un entier supérieur à 1, ces données étant représentatives d'un message, et on prévoit une clé comportant également des
15 éléments binaires.

Dans toute la suite, les termes "ligne" et "colonne" utilisés en rapport avec un tableau tel que celui de la figure 2 ou 6 désignent indifféremment la dimension horizontale ou la dimension verticale de ce tableau.

Une parenté entre le codage de l'invention et celui connu, décrit à
20 propos des figures 1 et 2, découle de la constatation de ce que, dans la figure 2, chaque diagonale (voir les séquences de données binaires entourées) est constituée de la clé de codage lorsque le terme correspondant de la séquence d'origine est 1, ou de zéros lorsque le terme correspondant de cette séquence est zéro. Or on peut, dans les lignes intermédiaires qui s'ajoutent pour donner
25 le signal crypté, remplacer chaque séquence diagonale par une ligne, ainsi que cela est schématisé à la **figure 3** pour la première diagonale ; en itérant ce remplacement, le nombre de lignes intermédiaires n'étant plus le nombre de bits dans la clé mais le nombre de bits dans le signal d'origine, on obtient un ensemble de lignes formées soit de la clé, soit d'une succession de zéros. On
30 obtient ainsi le tableau de la figure 6, qui sera commenté plus loin en relation avec le procédé de l'invention. On constate en tout cas que la transformation par rapport au tableau de la figure 2 n'a pas modifié le signal crypté.

Très généralement, le procédé de l'invention, représenté de manière schématique à la **figure 4**, consiste à prévoir les étapes suivantes :

- à partir de la séquence d'origine, on initialise en 10 un tableau en recopiant cette séquence d'origine sur la première ligne (ou colonne) ;
- 5 - on élabore ensuite en 14 sur la ligne suivante une séquence intermédiaire (voir ci-dessous) décalée par rapport à la ligne 1 d'un décalage u_i dont la valeur dépend de i , les valeurs de décalage étant élaborées en une étape 12 ;
- on incrémente en 16 la valeur de i d'une unité ;
- 10 - si, en 18, il apparaît que i vaut $N+1$ (ce qui veut dire qu'on a élaboré autant de lignes intermédiaires qu'il y a de termes dans la séquence d'origine), on procède en 20 à la sommation, colonne par colonne, des valeurs binaires de toutes les lignes intermédiaires, ce qui donne un signal numérique transformé (crypté), sinon on procède pour cette valeur de i aux opérations
- 15 14 et 16.

L'étape 12 d'élaboration des valeurs de décalage (en pratique comprises entre 1 et 256) peut être effectuée en parallèle à l'étape 10 d'initialisation, ou préalablement. La séquence de ces valeurs peut tout simplement être préétablie et contenue telle quelle dans la clé. Il a été indiqué

20 que ces valeurs de décalage déterminent le décalage entre chaque ligne intermédiaire et la ligne 1, mais il faut bien comprendre que cela revient au même de prévoir des valeurs de décalage de chaque ligne intermédiaire par rapport à la ligne qui précède (les nouvelles valeurs de décalage s'en déduisent par soustraction du décalage associé à la valeur de i).

25 Dans un mode particulier de réalisation, la séquence intermédiaire est élaborée comme étant :

- soit une séquence contenue dans la clé K , telle que la séquence prédéterminée $c_1, \dots, c_M$ de la clé de l'art antérieur, décrite plus haut en liaison avec la figure 1, si la $i^{\text{ème}}$ donnée binaire b_i de la séquence d'origine vaut 1,
- 30 - soit une séquence de zéros si $b_i = 0$.

En variante, on peut bien sûr décider inversement que si $b_i = 1$, la séquence intermédiaire est une séquence de zéros, et si $b_i = 0$, la séquence

intermédiaire est une séquence contenue dans la clé K , telle que la séquence prédéterminée $c_1, \dots, c_M$.

La **figure 5** est un schéma représentant le tableau rempli conformément à l'organigramme de la figure 4 : dans ce mode particulier de réalisation, chaque ligne intermédiaire est définie comme étant le produit de la clé par la valeur du terme considéré de la séquence d'origine, ce qui correspond, en d'autres termes, au mode de construction exposé ci-dessus. Cela montre que la construction de ces lignes peut se faire par simple multiplication.

La **figure 6** représente un cas particulier, où la clé est 1011 et se retrouve sur chaque ligne intermédiaire correspondant à une valeur de 1 dans la séquence d'origine, tandis que les autres lignes sont formées de zéros. Le décalage de chaque ligne intermédiaire est égal à la valeur correspondante de i . Cela revient à une configuration où chaque ligne intermédiaire est décalée d'une colonne vers la droite par rapport à la ligne intermédiaire précédente. Cela explique, comme cela a été noté plus haut, que le signal codé soit identique à celui de la figure 2. Toutefois, l'invention a le grand avantage de pouvoir aisément varier les décalages, ce que ne permettait pas le codage connu des figures 1 et 2.

La **figure 7** illustre la manière générale d'élaborer ces valeurs de décalage : dans la clé K sont prévues des valeurs $(d_1, \dots, d_P)$ au nombre de P , P étant un entier supérieur à 1, dont on déduit, pour chaque valeur de i , selon une fonction prédéterminée, une partie $v(i,K)$ de la clé K , d'où on déduit les valeurs de décalage $(u_1, \dots, u_N)$. Les valeurs en mémoire sont avantageusement choisies avec une entropie maximale, c'est-à-dire qu'elles sont choisies comme étant les plus différentes possibles. A titre d'exemple, les P valeurs précitées font partie des M valeurs $c_1, \dots, c_M$ (ou contiennent ces valeurs, si M est inférieur à P), et les valeurs $v(i,K)$ sont déduites de ces valeurs par multiplication par i ; en variante, ces valeurs de décalage sont formées conjointement par P valeurs comptées dans les M valeurs de la clé à partir du terme de rang i (de nombreuses fonctions sont possibles, en fonction des

besoins, et du nombre de termes qu'on est prêt à accepter pour définir la clé dans sa totalité, et il n'est pas possible ici d'en donner une liste exhaustive).

La **figure 8** est un schéma-bloc correspondant à l'organigramme de la figure 4. Il comporte :

- 5 - un module 80 d'élaboration des valeurs de décalage (il peut s'agir d'une simple mémoire, si ces valeurs ont été totalement prédéfinies),
- un bloc de traitement 82 adapté à recevoir les données d'origine et à les traiter en fonction de la clé K , des valeurs $v(i,K)$ et des valeurs de décalage u_i (en les déduisant, si besoin est, de la clé K),
- 10 - une zone d'écriture 84, par exemple formée de mémoires à registre, où peuvent être écrites et temporairement stockées les séquences d'origine et intermédiaires et
- un module d'addition 86 adapté à additionner le contenu des colonnes écrites dans la zone 84.

15 Ce module 86 d'addition modulo 2 peut comporter au moins une porte OU-exclusif.

La **figure 9** illustre schématiquement la constitution d'une station de réseau ou station de codage informatique, sous forme de schéma synoptique.

20 Cette station comporte un clavier 91, un écran 98, une source d'information externe 90, un émetteur hertzien 97, conjointement reliés à un port d'entrées / sorties 95 d'une carte de traitement 100.

La carte de traitement 100 comporte, reliés entre eux par un bus d'adresses et de données 96 :

- 25 - une unité centrale de traitement 92 ;
- une mémoire vive RAM 94 ;
- une mémoire morte ROM 93 ; et
- le port d'entrées / sorties 95.

30 Chacun des éléments illustrés en figure 9 est bien connu de l'homme du métier des micro-ordinateurs et des systèmes de transmission et, plus généralement, des systèmes de traitement de l'information. Ces éléments communs ne sont donc pas décrits ici.

La source d'information 90 est, par exemple, un périphérique d'interface, un capteur, un modulateur, une mémoire externe ou un autre système de traitement d'information (non représenté), et est de préférence adaptée à fournir des séquences de signaux représentatifs de parole, d'images, de messages de service ou de données multimédia, sous forme de séquences de données binaires.

Le terme "registre" utilisé ci-après désigne, dans chacune des mémoires 93 et 94, aussi bien une zone mémoire de faible capacité (quelques données binaires) qu'une zone mémoire de grande capacité (permettant de stocker un programme entier).

La mémoire vive 94 est adaptée à conserver des données, des variables et des résultats intermédiaires de traitement, dans des registres de mémoire portant, dans la description, les mêmes noms que les données dont ils conservent les valeurs. La mémoire vive 94 comporte notamment :

- un registre "*données_source*" (non représenté sur la figure), dans lequel sont conservées, dans l'ordre de leur arrivée sur le bus 96, les données binaires en provenance de la source d'information 90, sous forme d'une séquence $b_1, \dots, b_N$,
- un registre "*l*", qui conserve un nombre entier correspondant à l'indice de ligne du tableau décrit plus haut,
- un registre " $v(i,K)$ ", dans lequel sont conservées les valeurs $v(i,K)$ décrites plus haut,
- un registre " u_i ", dans lequel sont conservées les valeurs de décalage décrites précédemment, et
- un registre "*données_transformées*" (non représenté sur la figure), dans lequel sont conservées les données binaires transformées conformément à la présente invention.

La mémoire morte 93 est adaptée à conserver notamment, dans des registres portant, dans la description, les mêmes noms que les données dont ils conservent les valeurs :

- le programme de fonctionnement de l'unité centrale de traitement 92, dans un registre "*programme*", et

- une séquence prédéterminée contenue dans la clé K, dans un registre "K".

L'unité centrale de traitement 92 est adaptée à mettre en œuvre la présente invention, et notamment l'organigramme de la figure 4.

- 5 Comme le montre la **figure 10**, un réseau selon l'invention est constitué d'une station dite station de base SB désignée par la référence 180, et de plusieurs stations périphériques SPI_i , $i = 1, \dots, F$, où F est un entier supérieur ou égal à 1, respectivement désignées par les références $200_1, 200_2, \dots, 200_F$. Les stations périphériques $200_1, 200_2, \dots, 200_F$ sont éloignées de la
- 10 station de base SB, reliées chacune par une liaison radio avec la station de base SB et susceptibles de se déplacer par rapport à cette dernière.

Chaque station (mobile ou de base) du réseau est adaptée à mettre en œuvre la présente invention, et notamment l'organigramme de la figure 4.

REVENDECATIONS

1. Procédé de transformation d'une séquence de N données binaires d'origine $(b_1, \dots, b_N)$ représentative d'un message, à l'aide d'au moins une clé
5 (K) , N étant un entier supérieur à 1, ce procédé étant caractérisé en ce qu'on élabore une séquence $(u_1, \dots, u_N)$ de N valeurs algébriques de décalage et on effectue des étapes suivant lesquelles :

(a) on remplit un tableau à $N+1$ lignes comme suit :

- on écrit la séquence d'origine $(b_1, \dots, b_N)$ sur la première ligne du
10 tableau ;
- pour chaque entier i compris entre 1 et N , on écrit sur la $(i+1)^{\text{ième}}$ ligne du tableau une séquence intermédiaire d'éléments binaires décalée en entier ou par parties de u_i colonnes par rapport à la séquence écrite sur la première ligne, ladite séquence
15 intermédiaire étant, soit une séquence prédéterminée contenue dans la clé (K) si la $i^{\text{ème}}$ donnée binaire (b_i) de la séquence d'origine vaut 1, soit une séquence de zéros sinon ; et

(b) on additionne modulo 2, colonne par colonne, les éléments binaires contenus dans le tableau, de façon à obtenir une séquence de données
20 binaires transformée.

2. Procédé selon la revendication 1, caractérisé en ce qu'on décale ladite séquence intermédiaire en entier et on choisit une valeur de décalage u_i non identique pour toutes les lignes.

3. Procédé selon la revendication 1, caractérisé en ce qu'on décale
25 ladite séquence intermédiaire par parties et on choisit une valeur de décalage u_i non identique pour toutes les parties.

4. Procédé selon la revendication 1, 2 ou 3, caractérisé en ce que, pour chaque entier i compris entre 1 et N , on détermine la valeur de décalage u_i associée à la $(i+1)^{\text{ième}}$ ligne à partir d'une partie $(v(i,K))$ de la clé (K) .

30 5. Procédé selon la revendication 4, caractérisé en ce que, pour chaque entier i compris entre 1 et N , on obtient ladite partie $(v(i,K))$ de la clé (K) à partir de la valeur de l'indice de ligne i et de la clé (K) .

6. Procédé selon la revendication 5, caractérisé en ce que la clé (K) contient une séquence spécifique de P éléments binaires ($d_1, \dots, d_P$), P étant un entier supérieur à 1, et en ce que, pour chaque entier i compris entre 1 et N, on obtient ladite partie ($v(i,K)$) de la clé (K) à partir de la valeur de l'indice de ligne i et de ladite séquence spécifique ($d_1, \dots, d_P$).

7. Dispositif de transformation d'une séquence de N données binaires d'origine ($b_1, \dots, b_N$) représentative d'un message, à l'aide d'au moins une clé (K), N étant un entier supérieur à 1, ce dispositif étant caractérisé en ce qu'il comporte des moyens pour élaborer une séquence ($u_1, \dots, u_N$) de N valeurs algébriques de décalage et :

(a) des moyens pour remplir un tableau à N+1 lignes, comportant :

- des moyens pour écrire la séquence d'origine ($b_1, \dots, b_N$) sur la première ligne du tableau ;
- des moyens pour écrire, pour chaque entier i compris entre 1 et N, sur la $(i+1)^{\text{ème}}$ ligne du tableau, une séquence intermédiaire d'éléments binaires décalée en entier ou par parties de u_i colonnes par rapport à la séquence écrite sur la première ligne, u_i étant une valeur de décalage choisie, ladite séquence intermédiaire étant, soit une séquence prédéterminée contenue dans la clé (K) si la $i^{\text{ème}}$ donnée binaire (b_i) de la séquence d'origine vaut 1, soit une séquence de zéros sinon ; et

(b) des moyens pour additionner modulo 2, colonne par colonne, les éléments binaires contenus dans le tableau, de façon à obtenir une séquence de données binaires transformée.

8. Dispositif selon la revendication 7, caractérisé en ce qu'il comporte des moyens pour décaler ladite séquence intermédiaire en entier et en ce que la valeur de décalage u_i n'est pas identique pour toutes les lignes.

9. Dispositif selon la revendication 7, caractérisé en ce qu'il comporte des moyens pour décaler ladite séquence intermédiaire par parties et en ce que la valeur de décalage u_i n'est pas identique pour toutes les parties.

10. Dispositif selon la revendication 7, 8 ou 9, caractérisé en ce qu'il comporte en outre des moyens pour déterminer, pour chaque entier i compris

entre 1 et N, la valeur de décalage u_i associée à la $(i+1)^{\text{ième}}$ ligne à partir d'une partie $(v(i,K))$ de la clé (K).

11. Dispositif selon la revendication précédente, caractérisé en ce qu'il comporte en outre des moyens pour obtenir, pour chaque entier i compris
5 entre 1 et N, ladite partie $(v(i,K))$ de la clé (K) à partir de la valeur de l'indice de ligne i et de la clé (K).

12. Dispositif selon la revendication précédente, caractérisé en ce que la clé (K) contient une séquence spécifique de P éléments binaires $(d_1, \dots, d_P)$, P étant un entier supérieur à 1, et en ce que lesdits moyens d'obtention de
10 ladite partie $(v(i,K))$ de la clé (K) fournissent, pour chaque entier i compris entre 1 et N, ladite partie $(v(i,K))$ à partir de la valeur de l'indice de ligne i et de ladite séquence spécifique $(d_1, \dots, d_P)$.

13. Appareil de traitement de signaux numériques, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre un procédé de
15 transformation selon l'une quelconque des revendications 1 à 6.

14. Appareil de traitement de signaux numériques, caractérisé en ce qu'il comporte un dispositif de transformation selon l'une quelconque des revendications 7 à 12.

15. Réseau de télécommunications, caractérisé en ce qu'il comporte
20 des moyens adaptés à mettre en œuvre un procédé de transformation selon l'une quelconque des revendications 1 à 6.

16. Réseau de télécommunications, caractérisé en ce qu'il comporte un dispositif de transformation selon l'une quelconque des revendications 7 à 12.

25 17. Station mobile dans un réseau de télécommunications, caractérisée en ce qu'elle comporte des moyens adaptés à mettre en œuvre un procédé de transformation selon l'une quelconque des revendications 1 à 6.

18. Station mobile dans un réseau de télécommunications, caractérisée en ce qu'elle comporte un dispositif de transformation selon l'une
30 quelconque des revendications 7 à 12.

19. Station de base dans un réseau de télécommunications, caractérisée en ce qu'elle comporte des moyens adaptés à mettre en œuvre un procédé de transformation selon l'une quelconque des revendications 1 à 6.

5 20. Station de base dans un réseau de télécommunications, caractérisée en ce qu'elle comporte un dispositif de transformation selon l'une quelconque des revendications 7 à 12.

21. Dispositif de traitement de signaux représentatifs de parole, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre un procédé de transformation selon l'une quelconque des revendications 1 à 6.

10 22. Dispositif de traitement de signaux représentatifs de parole, caractérisé en ce qu'il comporte un dispositif de transformation selon l'une quelconque des revendications 7 à 12.

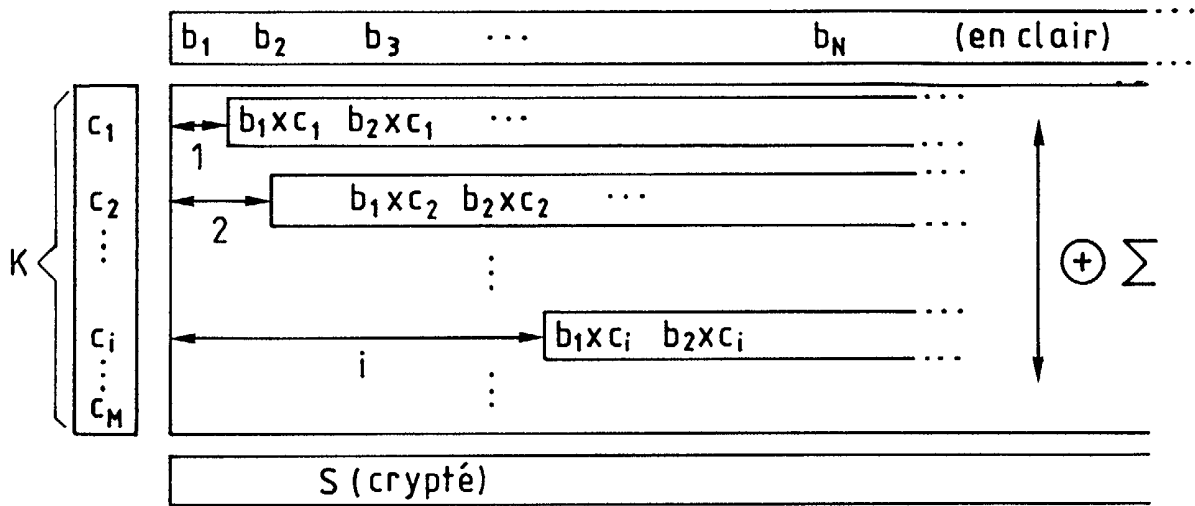


Fig.1

	1	1	0	0	1	1					
1		1	1	0	0	1	1				
0			0	0	0	0	0	0			
1				1	1	0	0	1	1		
1					1	1	0	0	1	1	
	1	0	1	1	1	1	1	1	0	1	

Fig. 2

2/5

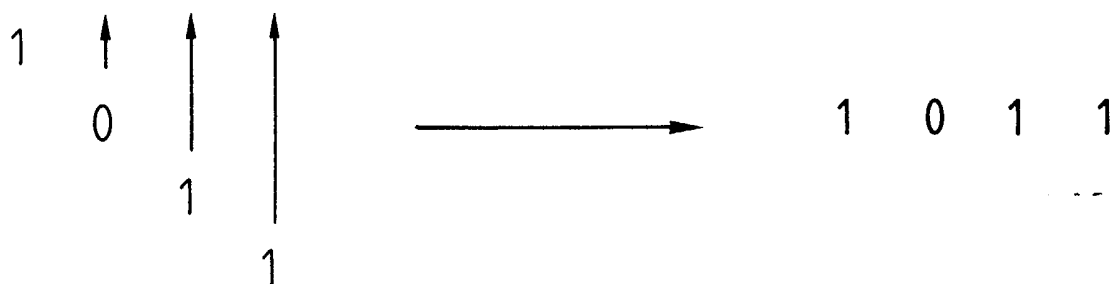


Fig. 3

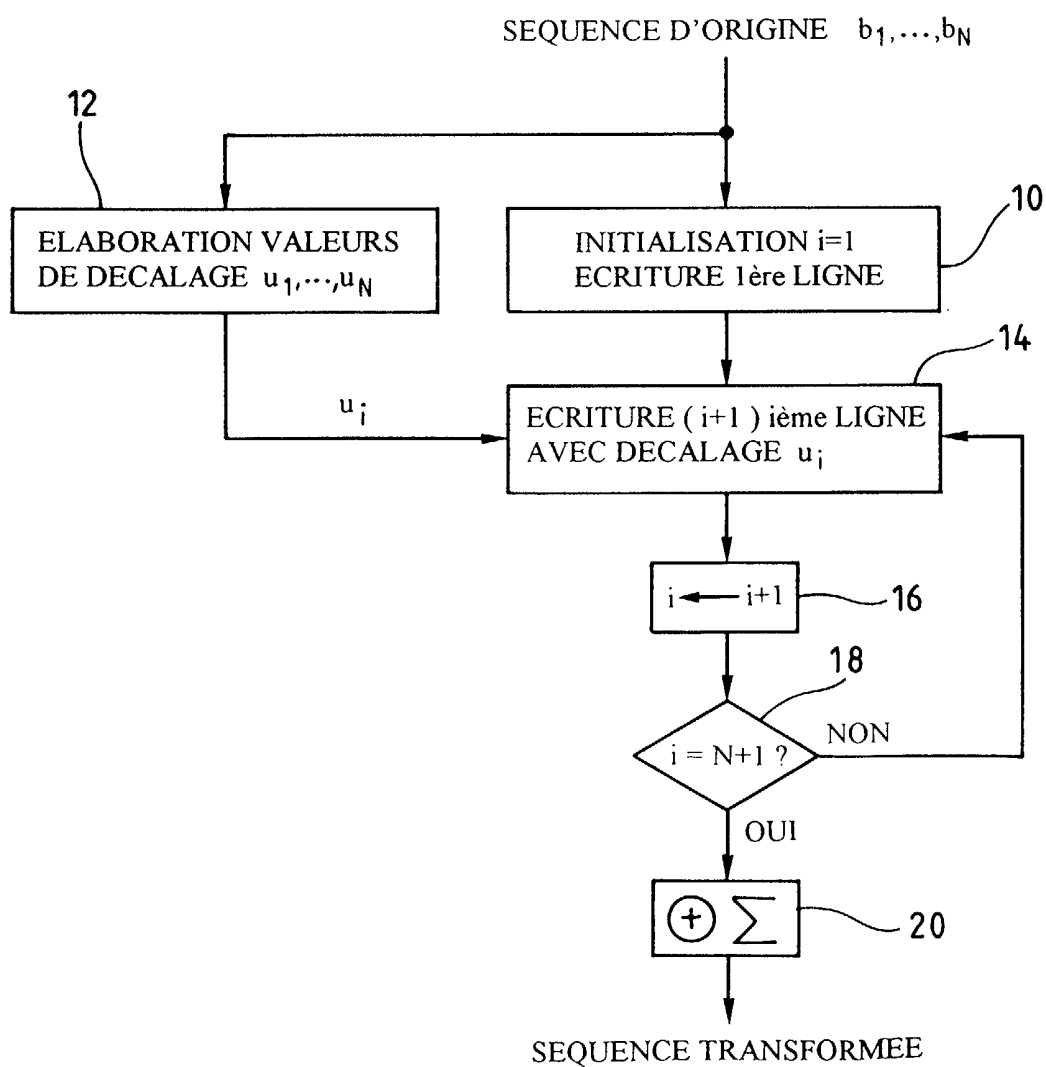


Fig. 4

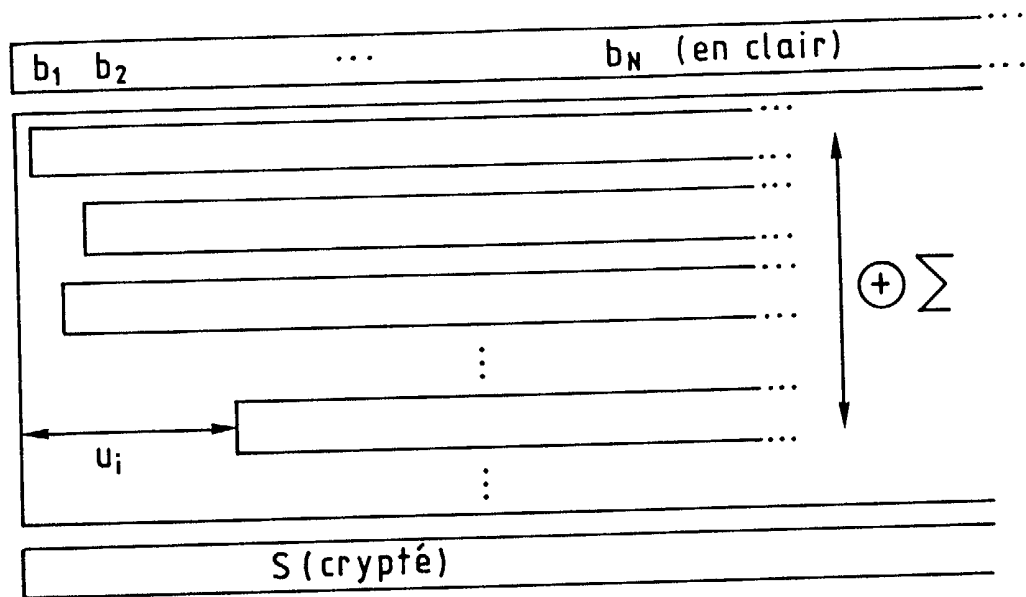


Fig. 5

	1	1	0	0	1	1						
		1	0	1	1							
			1	0	1	1						
				0	0	0	0					
					0	0	0	0				
						1	0	1	1			
							1	0	1	1		
	1	0	1	1	1	1	1	1	0	1		

Fig. 6

4/5

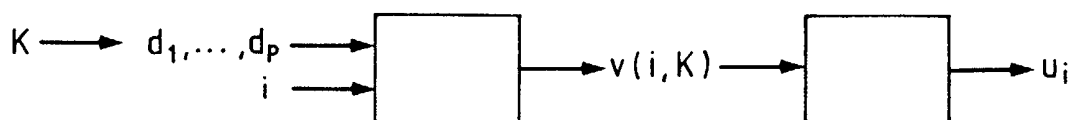


Fig. 7

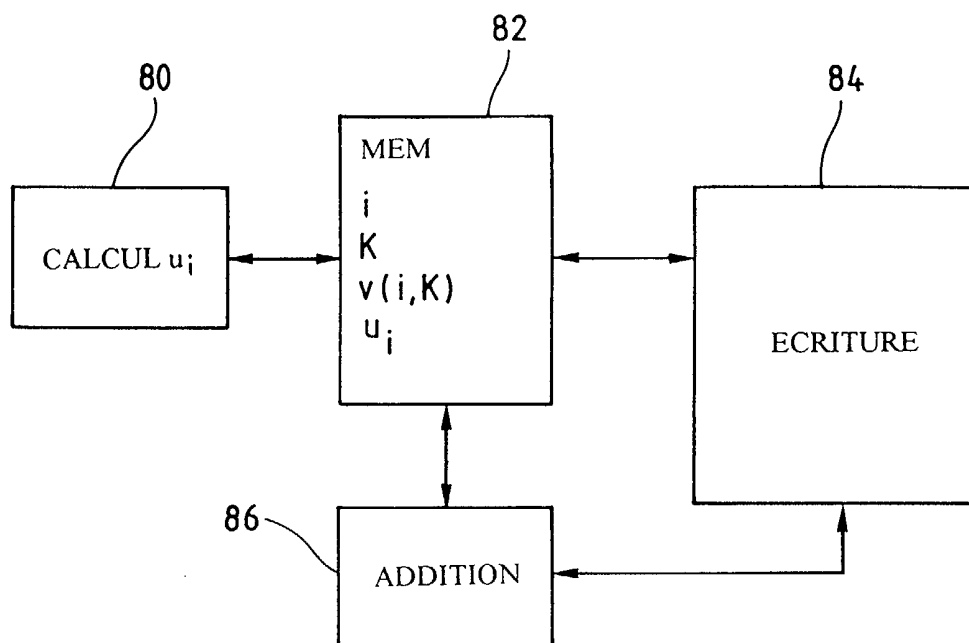


Fig. 8

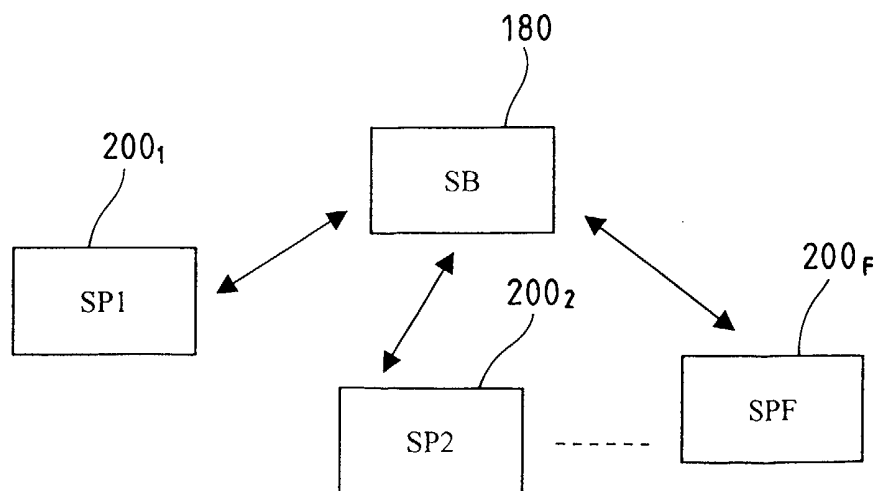


Fig. 10

5/5

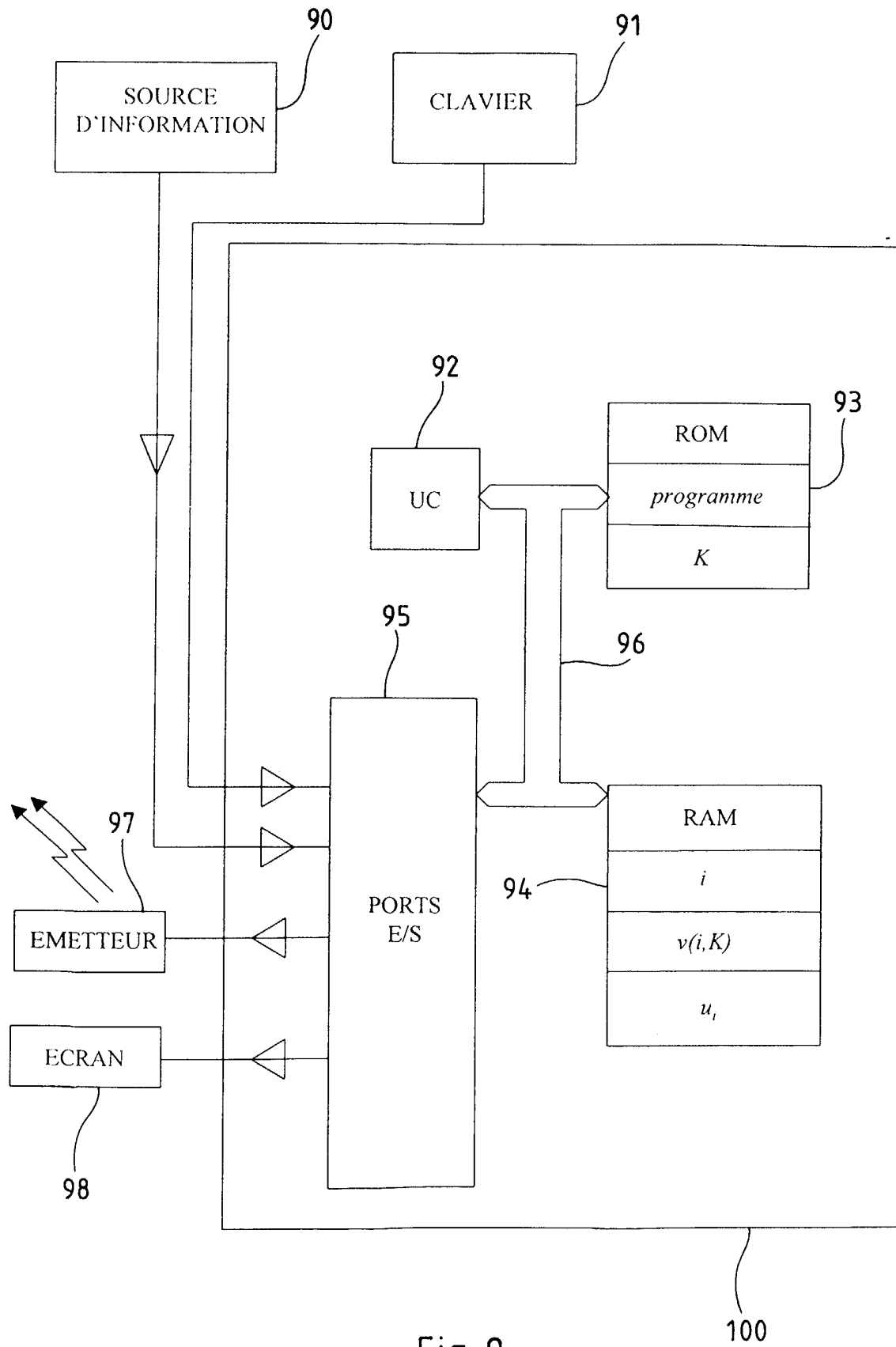


Fig. 9

RAPPORT DE RECHERCHE
PRÉLIMINAIRE

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

2814009
N° d'enregistrement
national

FA 593310
FR 0011747

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
E	EP 1 056 240 A (MATSUSHITA ELECTRIC IND CO LTD) 29 novembre 2000 (2000-11-29) * alinéas '0034!-'0041! * * alinéas '0143!-'0154! * * alinéas '0158!-'0169! * * revendications 1-8 * * figures 12-15 *	1-18	H03M7/00 H04L9/18 H04L1/00 G10L19/00 H04N7/64
A	EP 0 896 452 A (HITACHI LTD) 10 février 1999 (1999-02-10) * abrégé * * alinéa '0007! * * alinéa '0010! * * alinéa '0023! * * alinéa '0049! * * figures 3,16 *	1-18	
A	US 5 724 428 A (RIVEST RONALD L) 3 mars 1998 (1998-03-03) * abrégé *	1-18	
A	CUSICK T W ET AL: "THE REDOC II CRYPTOSYSTEM" ADVANCES IN CRYPTOLOGY - PROCEEDINGS OF CRYPTO, DE, BERLIN, SPRINGER VERLAG, vol. CONF. 10, 1990, pages 545-563, XP000260027 * figure 1 * * page 548 *	1-18	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) H04L
Date d'achèvement de la recherche		Examineur	
3 août 2001		Berbain, F	
CATÉGORIE DES DOCUMENTS CITÉS X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant			