RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2.036.379**
(A n'utiliser que pour le classement et les commandes de reproduction.)

(21) *N° d'enregistrement national* : ***69.07005***
(A utiliser pour les paiements d'annuités, les demandes de copies officielles et toutes autres correspondances avec l'I.N.P.I.)

BREVET D'INVENTION

PREMIÈRE ET UNIQUE PUBLICATION

(22) Date de dépôt..... 12 mars 1969, à 16 h 4 mn.
Date de la décision de délivrance..... 14 décembre 1970.
Publication de la délivrance..... B.O.P.I. — « Listes » n° 47 du 24-12-1970.

(51) Classification internationale (Int. Cl.)..... **G 06 f 3/00.**
(71) Déposant : Société dite : AB TRANSVERTEX, résidant en Suède.

Mandataire : Cabinet Beau de Loménie, Ingénieurs-Conseils, 55, rue d'Amsterdam, Paris (8e).

(54) **Machine à chiffrer.**

(72) Invention :

(33) (32) (31) Priorité conventionnelle :

La présente invention concerne une machine à chiffrer un texte en clair sour forme binaire par superposition d'un signal variable de chiffrage au signal de caractère en clair. Une telle machine comprend un certain nombre de dispositifs électriques du type pas-à-pas fonctionnant cycliquement en parallèle, par exemple des registres à décalage et dont les cycles sont de longueurs différentes, lesdits dispositifs étant par exemple des chaînes ou lignes comportant des nombres différents de bascules bistables. Les états initiaux des bascules, —— déterminés de préférence par un choix aléatoire, et la progression pas-à-pas des états des bascules constituant les différents régistres à décalage parallèle, définissent dans chaque colonne verticale un caractère de chiffrage. La nature de ces colonnes ou caractères est ainsi automatiquement modifiée dès qu'un régistre à décalage a effectué un cycle complet.

Il est classique d'obtenir des signaux de chiffrage modifiés pour chaque caractère au moyen d'un ensemble de roues dentées ayant chacune un nombre différent de dents (de préférence un nombre premier) qui sont montées sur un arbre commun et sont entraînées par des roues respectives mobiles indépendamment et ayant toutes le même nombre de dents. Chaque dent de ce second ensemble de roues représente un chiffre binaire et les dents alignées de toutes les roues dentées du second ensemble définissent un caractère constitué par les chiffres binaires correspondants. Le second ensemble de roues dentées peut ainsi définir un nombre de caractère égal au nombre de dents des roues. Au début, les chiffres binaires formant les caractères sont choisis de manière aléatoire. Si les roues dentées du premier ensemble (dont les nombres de dents sont différents) sont entraînées simultanément d'une dent à la fois, il est évident, lorsque la roue menante ayant le plus petit nombre de dents a effectué un tour complet, que les dents alignées de l'ensemble de roues menées représentent des combinaisons de chiffres binaires, c'est-à-dire des caractères, différentes des combinaisons initiales. Les combinaisons subissent une nouvelle modification lorsque la roue menante ayant le second plus petit nombre de dents, a effectué son tour complet et ainsi de suite. Si, par exemple, les nombres de dents des roues menantes

sont des nombres premiers, on comprendra que les combinaisons, (ou caractères) initiales, ne sont obtenues que lorsque l'ensemble des roues menantes a avancé d'un nombre de dents égal au produit des nombres respectifs de dents des roues constituant l'ensemble.

On choisit l'un des caractères se déplaçant périphériquement sur l'ensemble mené pour chaque opération de chiffrage, ledit caractère correspondant à une rangée de dents alignées, soit selon une ligne fixe de références, soit selon une ligne systématiquement déplacée pour compliquer le déchiffrage par des personnes non autorisées.

Le caractère de chiffrage obtenu (sous forme d'un signal) est superposé au caractère en clair appliqué simultanément à la machine, de manière à obtenir le caractère chiffré.

La disposition ci-dessus présente cependant plusieurs inconvénients.

Sur le plan du chiffrage, les modifications systématiques des caractères parmi les séries périphériques de caractères (ou lignes de dents) sont limitées, pour des raisons purement pratiques, aux caractères relativement voisins d'une ligne de référence. Les possibilités de modifications mentionnées sont par conséquent réduites à une fraction du nombre théorique total de caractères générés sur toute la périphérie des roues.

La présente invention a pour objet une machine à chiffrer éliminant ces inconvénients et caractérisée en ce qu'elle comprend un dispositif permettant à tout moment de choisir automatiquement une ou plusieurs colonnes d'une matrice de bascules et de transférer les signaux correspondants à l'état desdites bascules à un additionneur pour composer le signal de chiffrage supperposé au signal en clair.

D'autres objets et avantages de l'invention seront mieux compris à l'aide de la description détaillée qui va suivre et des dessins annexés sur lesquels :

- la figure 1 est un shéma synoptique simplifié de la machine à chiffrer de la présente invention ;
- les figures 2 et 3 sont des schémas électriques de deux systèmes sélecteurs de caractères utilisables dans la machine de la figure 1 ;

- la figure 4 est un schéma électrique d'un circuit d'addition également applicable à la présente invention.

La figure 1 illustre quatre registres à décalage S_a, S_b, S_c et S_d constitué chacun d'une chaîne de bascules bistables qui sont représentées schématiquement par des rectangles.

Les chaînes ou lignes sont constituées par des nombres différents de bascules. Le registre à décalage S_a qui, sur la figure 1 est constitué par la ligne de bascules la plus haute, peut comprendre 13 bascules a1-a13. Le registre à décalage S_b constitué par la seconde ligne comprend 12 bascules b1-b12 et de même les registres à décalage S_c et S_d sont respectivement constitués par les troisième et quatrième lignes de bascules comprenant 11 et 10 bascules c1-c11 et d1-d10.

Dans chaque chaîne la sortie d'une bascule est reliée de manière classique à l'entrée de la bascule suivante de manière que les informations circulent dans le registre d'une bascule à l'autre. De même, la dernière bascule de chaque chaîne est reliée à l'entrée de la première bascule de la même chaîne pour constituer un registre à cycle bouclé.

Au début, les différentes bascules sont positionnées de manière aléatoire, par exemple avec des cartes perforées. Pour plus de clarté, ce système d'introduction des informations initiales n'est pas représenté sur la figure 1, de même que les circuits classiques rythmant la circulation des registres.

Les informations circulent en parallèle dans les différents registres, c'est-à-dire que les chiffres binaires ou bits contenus dans la première colonne k1 comprenant les bascules a1, b1, c1 et d1, sont transférés aux bascules a2-d2 de la seconde colonne k2 dont le contenu est transféré aux bascules a3-d3 de la troisième colonne k3, et ainsi de suite. Chaque colonne de bascules définit un caractère qui, dans le cas illustré, est constitué par quatre bits. Du fait de la différence des cycles des différents registres à décalage, les bits initialement introduits dans chaque colonne, par exemple dans la colonne k1, sont transférés sans modification jusqu'à la"dernière" bascule d10 du registre S_d correspondant à la colonne k10. Au signal de circulation suivant du registre S_d, un nouveau cycle commence à

la colonne k1, dont le bit d1 a sa valeur initiale, mais dont les autres bits sont remplacés par ceux contenus dans les bascules a_{13}, b_{12} et c_{11} respectivement, ces bits étant issus initialement des bascules a_4, b_3 et c_2. A l'avance suivante le registre S_c commence un nouveau cycle dans la bascule c1 de la colonne k1 qui comporte en outre les bits a13, b12 et d10. Cette modification se répète de la même manière pour les autres registres S_b et S_a. Il va de soi que les combinaisons initiales des bits ne se reproduisent que lorsque les registres ont avancé d'un nombre de pas égal au produit du nombre de bascules des quatre registres.

La description qui suit concerne un dispositif de sélection d'un caractère, c'est-à-dire d'une combinaison de bits dans une même colonne, utilisé pour chiffrer un caractère en clair appliqué sous forme d'impulsions appliquées au moment de la circulation des registres à décalage.

Pour ceci, l'appareil comprend un certain nombre de sélecteurs de caractères, dans ce cas quatre, T1, T2, T3 et T4. Chaque sélecteur de caractères comprend quatre paires d'entrées, i1-i4, qui sont connectées en parallèle aux entrées correspondantes des autres sélecteurs de caractères et peuvent être reliées aux quatre paires de sorties des bascules d'une colonne arbitraire par un sélecteur de système V (qui n'est pas décrit en détail ci-après). Dans ce qui suit, on suppose que les sélecteurs sont respectivement connectés, comme indiqué sur la figure, aux bascules a1-d1 de la colonne k1, par des paires de lignes L1-L4.

Les sorties U1-U4, des sélecteurs de caractères T1-T4, sont connectées dans ce cas à l'une des entrées de deux portes ET, respectivement 01 et 05 pour T1, 02 et 06 pour T2, 03 et 07 pour T3 et 04 et 08 pour T4. La seconde entrée de chacune des portes 01-08 est connectée à la sortie de circuit d'addition A1-A8, qui, comme les sélecteurs de caractère, comporte quatre paires d'entrées, chacune connectée à une paire de sortie des bascules de sa colonne associée à travers le sélecteur de système V. Dans la forme illustrée, le sélecteur de système ou commutateur est représenté comme connectant les circuits d'addition A1-A8 aux colonnes de bascules k2 à k9 situées directement au-dessus de

chaque circuit sur la figure. Les sorties respectives g1-g8, des portes 01-08 sont toutes connectées (seule la sortie de g8 étant représentée pour clarifier la figure) à une première entrée de el, d'un circuit d'addition final SA dont l'autre entrée e2 reçoit un signal en clair codé en binaire appliqué en synchronisme avec la circulation du registre Sa à Sd par des circuits non représentés. La sortie ch du circuit SA contient la superposition du caractère de la colonne choisie au caractère en clair et constitue le signal chiffré.

Avant de décrire le fonctionnement du système ci-dessus, il faut examiner brièvement la réalisation des sélecteurs de caractères T1-T4 et des circuits d'addition A1-A8 illustrés aux figures 2 à 4. Comme illustré sur les figures 2 et 3, les sélecteurs de caractère T1 et T2 comprennant les mêmes composants élémentaires, c'est-à-dire des portes ET G1-G5 mais dont les connections internes sont différentes de manière que chaque sélecteur de caractères ait son fonctionnement propre. Sur le figure 2, les paires de portes G1, G2 et G3,G4 sont connectées de la même manière aux deux paires d'entrées associées i1, i2 et i3, i4, c'est-à-dire que les portes G1 et 63 sont reliées de la même manière aux lignes "a1" respectivement des paires i1, i2, i3, i4, alors que les portes G2 et G4 sont reliées aux lignes "a0" respectivement des paires i1,i2 et i3,i4. Cette connection de deux paires à deux portes est repérée par la lettre A sur la figure 2.

Sur la figure 3, les deux paires i1 et i2 sont connectées comme précédemment aux portes G1 et G2, mais la porte G3 est connectée à la ligne "a1" de i3 et à la ligne "a0" de i4, alors que la porte G4 est connectée à la ligne"a0" de i3 et à la ligne "a1" de i4. Ce mode de couplage est indiqué par la lettre B sur la figure 3.

Ces deux types élémentaires de couplage des portes de gauche et de droite, permettent d'imaginer les connections des autres sélecteurs de caractères T3 et T4. La partie gauche de T3 est connectée en configuration B alors que sa partie droite est connectée en configuration A. Les deux paires de portes de T4 sont connectées en configuration B.

Le tableau ci-après donne les caractéristiques des quatres sélecteurs de caractères T1 à T4 et les combinaisons de bits (voir figures 2 et 3) dont l'application aux entrées i1 à i4 provoque un signal de sortie du sélecteur de caractères associés.

Sélecteur de caractères	configuration	combinaisons de bits			
T1	A + A	1111	1100	0011	0000
T2	A + B	1110	1101	0010	0001
T3	B + A	0111	0100	1000	1011
T4	B + B	0101	0110	1001	1010

La figure 4 illustre les circuits d'addition A1-A8 qui sont tous identiques et dont le schéma est classique, ne nécessite pas une description détaillée.

Un exemple simple illustre le fonctionnement de la machine à chiffrer décrite ci-dessus.

On suppose qu'à un certain moment, au cours de la circulation continue des colonnes k1 à k9, la colonne k1 contient dans ses bascules a1-d1 la suite de bits "0 1 0 0". Ce signal de caractères est appliqué par les lignes respectives L1-L4 aux entrées i1-i4 de tous les sélecteurs de caractères T1-T4. D'après le tableau ci-dessus, seul le sélecteur de caractères T3 répond par un signal de sortie vers les portes ET associées 03 et 07. Les secondes entrées de ces portes, de même que les secondes entrées de toutes les autres portes, reçoivent un signal appliqué par le circuit d'addition A3 pour la porte 03 (et A7 pour la porte 07) qui représente le total des bits contenus dans la colonne k3 (ou dans la colonne k7) ces bits sont par exemple "1 1 0 1" (ou "0 0 1 1"). Le total b1 est alors "1" ou ("0" pour le circuit 17). La sortie du sélecteur de caractères T3 ouvrant la porte 03 (et la porte 07), ce signal "1" (ou "0") est appliqué à l'entrée du circuit d'addition final SA pour y être superposé à l'impulsion en clair arrivant au même instant. (Le signal "0" de la porte 07 peut être utilisé comme seconde impulsion de superposition).

Au décalage suivant des registres, un sélecteur de caractères déterminé par la nouvelle combinaison de bits dans les bascules de la colonne k1, ouvre le passage pour un nouveau signal, somme de la combinaison d'une certaine colonne et ainsi de suite. A chaque nouveau décalage des registres, le caractère de codage est ainsi obtenu par un "saut" en avant ou en arrière sur toute l'étendue des informations contenues dans les lignes

de bascules des différents registres à décalage. Ceci améliore considérablement l'utilisation des combinaisons de caractères par rapport aux machines à chiffrer du type mécanique. Dans le système illustré, l'emploi de quatre sélecteurs de caractères associés à quatre bascules dans chaque colonne est justifié par le fait que tant le caractère lui-même que ses commutations de pôles, peuvent agir sur le sélecteur.

Comme dans les autres systèmes de chiffrage fonctionnant en code binaire, le déchiffrage s'effectue par simple superposition aux impulsions chiffrées de la même série d'impulsions que celle utilisée au cours de l'opération de chiffrage. Le texte est alors rétabli en clair grâce à une propriété particulière de l'addition binaire.

L'invention n'est pas limitée à la forme décrite ci-dessus et diverses variantes peuvent être imaginées, particulièrement quant au nombre de registres à décalage et aux relations entre leurscycles propres.

L'emploi de registres à décalage n'est pas limitatif et l'on peut imaginer des systèmes basés sur d'autres circuits à fonctionnement cyclique, tels que les compteurs binaires et les circuits logiques associés.

Le domaine d'application de la machine peut être étendu dans une large mesure en rendant variables les relations entre les cycles électriques.

REVENDICATIONS

1 - Machine à chiffrer un texte en clair présenté sous forme binaire, par superposition à chaque signal représentant un caractère en clair du texte, d'un signal variable de chiffrage, la machine étant constituée par un certain nombre de circuits électriques décalés cycliquement en parallèle, par exemple des registres à décalage, les cycles étant différents les uns des autres et lesdits circuits électriques étant par exemple assemblés en une matrice de lignes ou chaînes comprenant des nombres différents de bascules bistables dont les états initiaux sont déterminés en fonction d'un choix, de préférence aléatoire, les états des différentes bascules étant décalés en parallèle, colonne par colonne, sur tous les registres à la fois, de façon que chaque colonne définisse un caractère de chiffrage dont la nature se modifie automatiquement dès que l'un des registres à décalage a effectué un cycle complet, ladite machine étant caractérisée en ce qu'elle comprend un dispositif permettant à chaque instant du chiffrage de choisir automatiquement l'une des différentes colonnes de bascules de la matrice de bascules et de transférer les signaux correspondant à l'état des bascules de ladite colonne vers un circuit d'addition dans lequel est généré le signal de chiffrage destiné à être superposé au signal du texte en clair.

2 - Machine selon la revendication 1, caractérisée en ce que le dispositif permettant de choisir automatiquement au moins l'une des colonnes de bascules, comprend un certain nombre de sélecteurs de caractères, associés chacun à une ou plusieurs colonnes et comportant chacun un nombre d'entrées égal au nombre de lignes de bascules, lesdites entrées étant connectées en parallèle aux sorties correspondantes des bascules d'une colonne de référence et la sortie de chacun desdits sélecteurs étant appliquée comme l'une des entrées d'une porte ET, dont la seconde entrée est reliée à la sortie d'un circuit d'addition dont les entrées respectives sont constituées par les sorties des bascules de la colonne correspondante, de manière que pour un caractère donné contenu dans la colonne de référence, un sélecteur unique de caractères fournisse un signal de sortie à sa porte ET associés dont l'autre entrée est en permanence appliquée par la sortie du

circuit d'addition de manière que la sortie de ladite porte ET constitue ledit signal de chiffrage.

3 - Procédé selon la revendication 2 caractérisé en ce que chaque sélecteur de caractère comprend un système de portesET dont les entrées respectives sont connectées aux sorties des bascules de la colonne de références, de manière à ne fournir un signal de sortie que lorsque la colonne de référence contient un caractère prédéterminé.

4 - Machine selon les revendications 2 ou 3, caractérisée en ce qu'un commutateur ou sélecteur de système est placé entre les sorties des colonnes de bascules et les circuits d'addition associés pour permettre le décalage des connexions entre les colonnes de bascules et les sélecteurs de caractères.

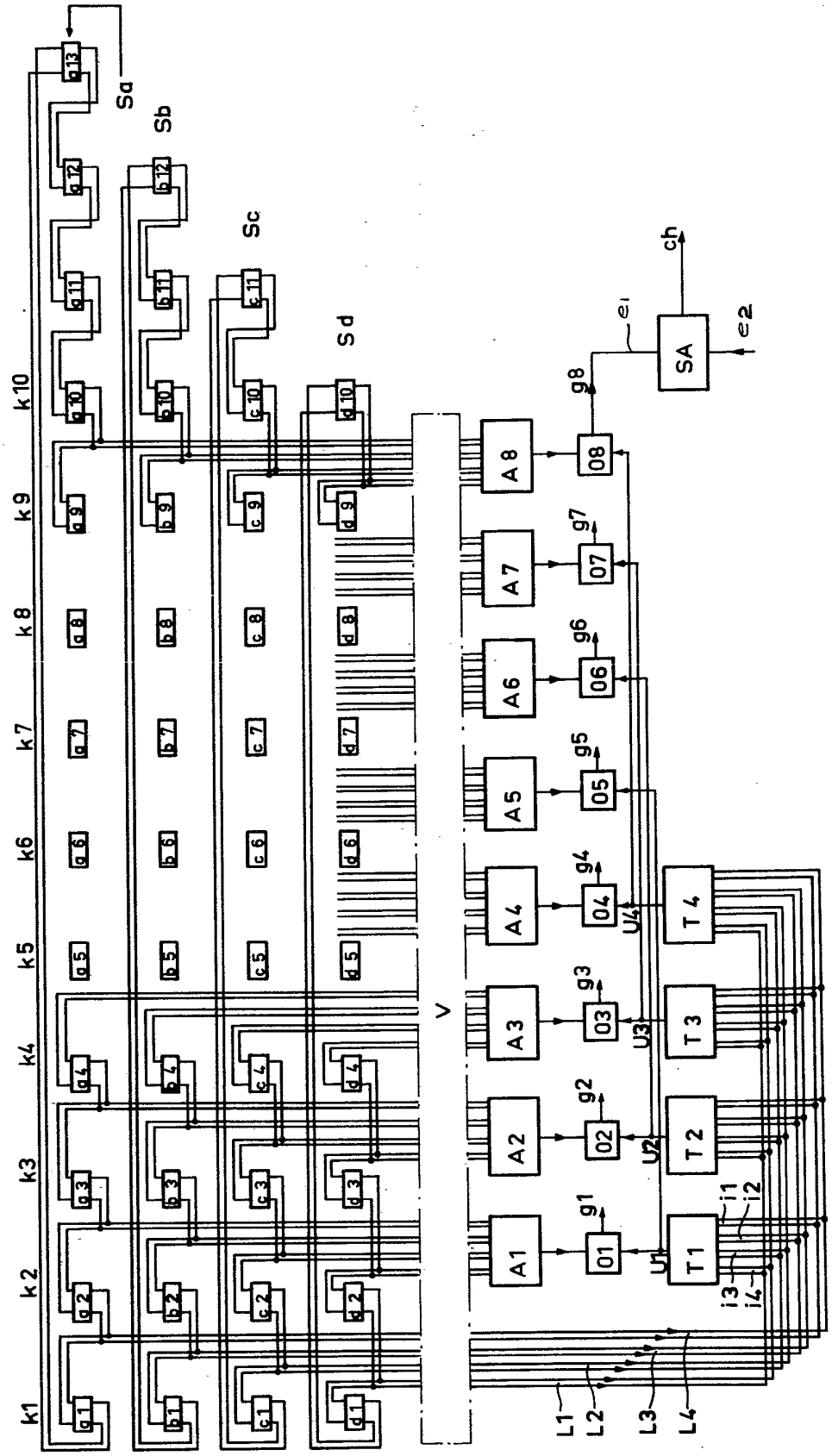
Sa
Sb
Sc
Sd
k1
k2
k3
k4
k5
k6
k7
k8
k9
k10
V
A1
A2
A3
A4
A5
A6
A7
A8
01
02
03
04
05
06
07
08
T1
T2
T3
T4
U1
U2
U3
U4
SA
ch
e1
e2
i1
i2
i3
i4
L1
L2
L3
L4

FIG.1

FIG.2

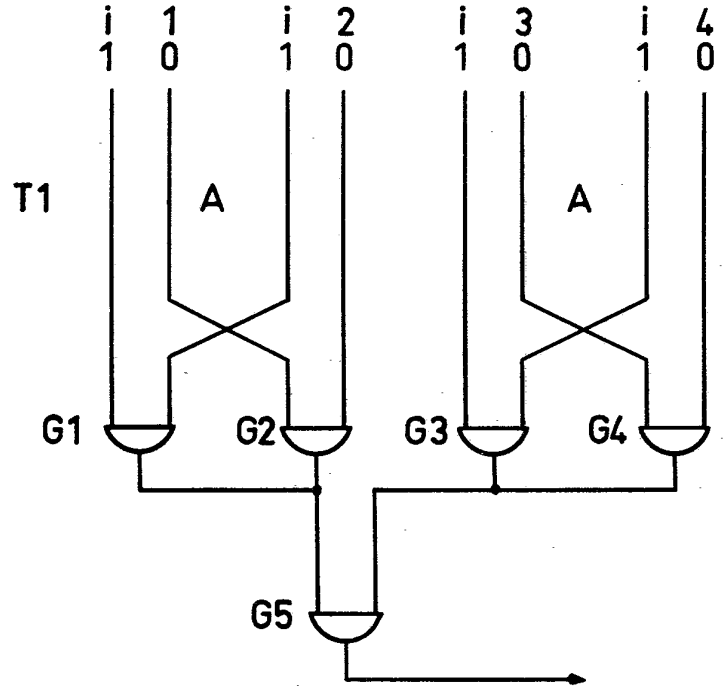
i 1 1 0
i 2 1 0
i 3 1 0
i 4 1 0
T1
A
A
G1
G2
G3
G4
G5

FIG.3

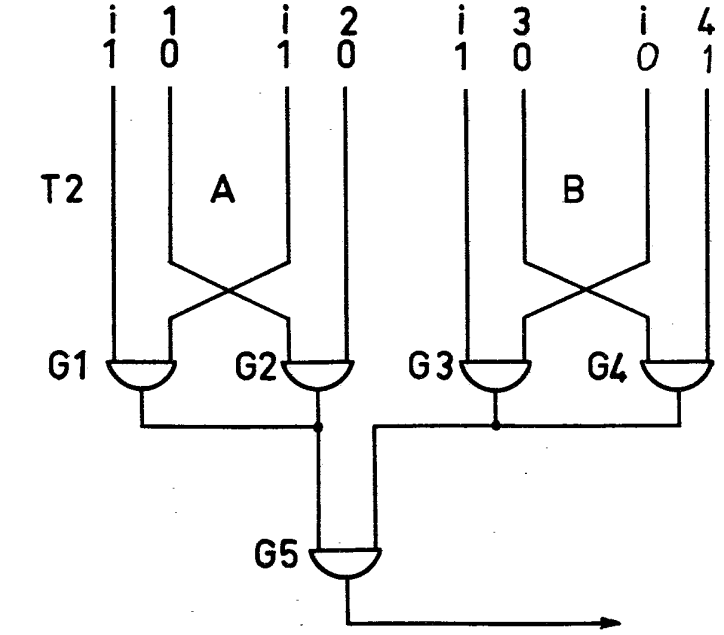
i 1 1 0
i 2 1 0
i 3 1 0
i 4 0 1
T2
A
B
G1
G2
G3
G4
G5

FIG.4