Nr. 482 257 PATENTSCHRIFT Nr. 482 257

SCHWEIZERISCHE EIDGENOSSENSCHAFT

EIDGENÖSSISCHES AMT FÜR GEISTIGES EIGENTUM

V

Internationale Klassifikation: G 09 c 1/10

Gesuchsnummer: 3407/69

Anmeldungsdatum: 6. März 1969, 17½ Uhr

Patent erteilt: 30. November 1969

Patentschrift veröffentlicht: 15. Januar 1970

HAUPTPATENT

AB Transvertex, Varby (Schweden)

Verschlüsselvorrichtung

Bengt Florin, Hägersten (Schweden), und Kalevi Loimaranta, Mattby (Finnland), sind als Erfinder genannt worden

1

Die vorliegende Erfindung betrifft eine Verschlüsselvorrichtung zum Verschlüsseln eines in binärer Form vorliegenden Klartextes durch Überlagerung der Klartextsignale mit veränderbaren Schlüsselsignalen, enthaltend eine Mehrzahl elektrischer Einrichtungen, von denen jede eine unterschiedliche Anzahl bistabiler, in Serie geschalteter Bauelemente enthält, welche Einrichtungen parallel zueinander schrittweise weiterschaltbar sind und in denen der Ausgangszustand der bistabilen Bauelemente nach einem beliebig wählbaren Schema setzbar ist und einander zugeordnete Bauelemente dieser Einrichtungen Kolonnen bilden und der Zustand der eine Kolonne bildenden Bauelemente ein Verschlüsselsignal mit Hilfe eines Satzes von Zahnrädern herzustellen, welche Zahnräder unterschiedliche Anzahlen von Zähnen, vorzugsweise Primzahlen, aufweisen, auf der gleichen Achse angeordnet sind und zusammen mit einem Satz entsprechender, die gleiche Anzahl von Zähnen aufweisender, unabhängig voneinander drehbarer Zahnräder zusammenwirken. In dem zweiten Satz Zahnräder steht jeder Zahn für ein binäres Bit, und die miteinander ausgerichteten Zähne im ganzen Zahnradsatz bestimmen ein durch die entsprechenden binären Bits gebildetes Zeichen. Auf diese Weise können mit dem zweiten Satz Zahnräder gleichzeitig so viele Zeichen bestimmt werden, wie auf dem Umfang des Rads Zähne angeordnet sind. Zu Beginn können die die Zeichen bildenden Bits nach Belieben eingestellt werden. Wenn die Zahnräder des ersten Satzes, welche unterschiedliche Zähnezahlen aufweisen, immer gleichzeitig um einen Zahn weitergedreht werden, versteht sich, dass, sobald das treibende Zahnrad mit der kleinsten Zähnezahl um eine ganze Umdrehung weitergedreht wurde, die Zähne in dem angetriebenen Satz Zahnräder eine Kombination binärer Bits, d.h. ein Zeichen, bestimmen, das gegenüber der ursprünglichen Kombination unterschiedlich ist. Diese Kombinationen können weiter verändert werden, wenn das treibende Zahnrad mit der nächstniedrigen Zähnezahl um eine volle Umdrehung weitergedreht wurde, usw. Wenn die Anzahl der Zähne der treibenden Räder Primzahlen sind, so versteht sich, dass die gleichen Kombinationen, d.h. das gleiche Zeichen, wie ursprünglich eingestellt, erst

2

wieder erhalten wird, wenn der Satz der treibenden Räder um eine Anzahl Schritte weitergedreht wurde, welche gleich dem Produkt der Zähnezahlen aller in diesem Satz enthaltenen Räder ist.

Von den auf dem Umfang des zweiten Zahnradsatzes erscheinenden Zeichen wird für jede Verschlüsselung ein Zeichen ausgewählt, das einer Reihe von Zähnen entspricht, die entweder längs einer gemeinsamen Bezugslinie angeordnet sind oder eine systematische Verschiebung zwischen verschiedenen Bezugslinien aufweisen, wobei im letzteren Falle eine unerwünschte Entschlüsselung zusätzlich erschwert wird.

Das zum Verschlüsseln verwendete Zeichen wird dann dem in Klarschrift vorliegenden Zeichen überlagert, wodurch ein verschlüsseltes Zeichen entsteht.

Diese bekannte Anordnung weist jedoch eine Mehrzahl von Nachteilen auf. Ein für das Verschlüsseln wichtiger Nachteil ist, dass die oben beschriebene, systematische Veränderung der auf dem Umfang von Zahnrädern gebildeten Zeichen aus rein praktischen Gründen nur für nahe nebeneinander angeordnete Zeichen (Zähnereihen) durchgeführt werden kann. Auf diese ist die Anzahl der praktisch möglichen Veränderungen gegenüber der Gesamtzahl der auf allen Zahnrädern angeordneten Zeichen sehr beschränkt.

Es ist das Ziel der vorliegenden Erfindung, diese Nachteile zu beheben.

Die Verschlüsselvorrichtung nach der vorliegenden Erfindung ist gekennzeichnet durch eine Anordnung zum automatischen Auswählen einer Kolonne und zum Weiterleiten von dem Schaltzustand der bistabilen Bauelemente der ausgewählten Kolonne entsprechenden Signalen an ein Addierwerk, das das den Klartextsignalen zu überlagernde Verschlüsselsignal bildet.

Die Erfindung soll nun mit Hilfe der Figuren an einem Ausführungsbeispiel näher erläutert werden.

Fig. 1 zeigt ein Blockschaltbild für eine Verschlüsselvorrichtung, die in Übereinstimmung mit der vorliegenden Erfindung aufgebaut ist.

Fig. 2 und 3 zeigen Verdrahtungsschema für zwei Beispiele von Zeichenwählern, welche in der Vorrichtung nach Fig. 1 verwendet sind.

Fig. 4 zeigt ein Verdrahtungsschema für ein Addierwerk, das ebenfalls in der Vorrichtung nach Fig. 1 verwendet ist.

Bei der in Fig. 1 gezeigten Ausführungsform einer Verschlüsselvorrichtung sind vier Schieberegister S_a, S_b, S_c und S_d vorgesehen, von denen jedes eine Reihe in Serie geschalteter bistabiler Flip-Flops aufweist, die als kleine Blocks eingezeichnet sind.

Jede der Reihen enthält eine andere Anzahl Flip-Flops. Das Schieberegister S_a, das in der gezeigten Ausführungsform durch die oberste Reihe von Flip-Flops gebildet ist, enthält dreizehn Flip-Flop a1 bis a13. Das Schieberegister S_b in der zweiten Reihe enthält zwölf Flip-Flops b1 bis b12, und die Schieberegister S_c und S_d der dritten und vierten Reihe enthalten elf bzw. zehn Flip-Flops c1 bis c11 bzw. d1 bis d10.

In jeder Reihe ist die Ausgangsleitung eines Flip-Flops in bekannter Weise mit der Eingangsleitung des nächstfolgenden Flip-Flips verbunden, so dass, wenn das Register um einen Schritt weitergeschaltet wird, die in jedem Flip-Flop dieser Reihe gespeicherte Information in den nächstfolgenden Flip-Flop weiterverschoben wird. Weiter ist aus Fig. 1 zu ersehen, dass zur Bildung eines geschlossenen Schrittschaltkreises der letzte Flip-Flop jeder Reihe mit dem ersten Flip-Flop der gleichen Reihe verbunden ist.

Am Anfang werden alle Flip-Flops, beispielsweise mit Hilfe von Lochkarten, in eine beliebig wählbare Stellung geschaltet. Der Einfachheit wegen wurde eine solche Einrichtung zum Eingeben von Informationen und auch der normalerweise verwendete Taktgeber zum Schrittschalten nicht in die Figur eingezeichnet.

Die einzelnen Register sind vorgesehen, um parallel miteinander weitergeschaltet zu werden, wobei die Informationsbits in der durch je einen Flip-Flop aus jeder Reihe gebildeten ersten Kolonne k1 (Flip-Flops a1, b1, c1 und d1) in die Flip-Flops a2 bis d2 der zweiten Kolonne k2, und die Inhalte der letzteren in die Flip-Flops a3 bis d3 der dritten Kolonne übertragen werden, usw. Jede Kolonne von Flip-Flops bestimmt ein Zeichen, das im vorliegenden Falle aus vier Bits besteht. Die am Anfang in die erste Kolonne k1 eingegebenen Bits werden bis zum letzten Flip-Flop d10 des Registers S_d parallel weitergeschaltet. Beim nächsten Schaltschritt beginnt wegen der unterschiedlichen Anzahl Flip-Flops in den verschiedenen Schieberegistern für das Schieberegister S_d ein neuer Arbeitszyklus, wobei das am Anfang in den Flip-Flop d1 eingegebene Bit wieder im Flip-Flop d1 erscheint, während die Bits in den anderen Flip-Flops der Kolonne k1 durch die Bits aus den Flip-Flops a_{13}, B_{12} und c_{11} der Register S_a bis S_c ersetzt werden. Beim nächsten Weiterschalten beginnt das Register S_c einen neuen Arbeitszyklus, wobei die Kolonne k1 nunmehr ausser dem «anfänglichen» Bit im Flip-Flop c1 die Bits a12, b12 und d10 enthält. Dieser Arbeitszyklus wiederholt sich für die verbleibenden Register S_b und S_a in entsprechender Weise. Es versteht sich, dass die anfänglich vorhandene Kombination von Bits erst nach einer Anzahl von Schrittschaltungen, die dem Produkt der Schritte, um die jedes der vier Schieberegister weiterschaltbar ist, entspricht, wieder erscheint.

Im folgenden soll die Anordnung, die zur Auswahl des Zeichens, d.h. der Bit-Kombination einer Kolonne, das zum Verschlüsseln eines in der Form eines Impulses gleichzeitig mit dem Weiterschalten der Schieberegister gelieferten Klarschriftzeichens verwendet wird, beschrieben werden.

Zu diesem Zweck ist eine Anzahl von Zeichenwählern T1, T2, T3 und T4 vorgesehen. Jeder Zeichenwähler weist vier Paar Eingangsleitungen i1 bis i4 auf, die mit den entsprechenden Eingangsleitungen der anderen Zeichenwähler parallel geschaltet sind und über einem nicht näher beschriebenen Schalter V (System-Wähler) mit den vier Paaren der Flip-Flip-Ausgangsleitungen irgendeiner Kolonne verbunden werden können.

Im folgenden soll angenommen werden, dass die Wähler, wie es in Fig. 1 gezeigt ist, über die Leiterpaare L1 bis L4 mit den Flip-Flops a1 bis d1 der Kolonne a1 verbunden sind.

Die Ausgangsleitungen U1 bis U4 jedes Zeichenwählers T1, T2, T3 und T4 sind mit einer der Eingangsleitungen von zwei Und-Toren 01, 05; 02, 06; 03, 07; und 04, 08 verbunden. Die andere Eingangsleitung jedes der UND-Tore 01 bis 08 ist mit der Ausgangsleitung eines Addierwerks A1 bis A8 verbunden, das wie der Zeichenwähler vier Paar Eingangsleitungen aufweist, von denen jedes Paar über den Schalter V mit den entsprechenden zwei Ausgangsleitungen der vier Flip-Flops der zugehörigen Kolonne verbunden ist. Bei der gezeigten Ausführungsform ist angenommen, dass der Schalter so eingestellt ist, dass die Addierwerke A1 bis A8 mit den darüberliegend gezeichneten Flip-Flop-Kolonne k2 bis k9 verbunden sind. Die Ausgangsleitungen g1 bis g8 der Tore 01 bis 08 sind alle mit einer ersten Eingangsleitung öv (die der Klarheit wegen nur für die Ausgangsleitung g8 gezeigt) eines letzten Addierwerks SA verbunden, dessen anderer Eingangsleitung k1 ein binär verschlüsseltes Signal in Klarschrift zugeleitet wird, wie das noch im Zusammenhang mit dem schrittweisen Weiterschalten der Schieberegister S1 bis S4 beschrieben werden wird. An der Ausgangsleitung ch des Addierwerks SA kann dann ein Signal, das mit dem in der entsprechenden Kolonne enthaltenen Zeichen überlagert ist, d.h. das verschlüsselte Signal, abgenommen werden.

Bevor die Arbeitsweise der oben beschriebenen Vorrichtung beschrieben werden soll, sei kurz der Aufbau der Zeichenwähler T1 bis T4 und der Addierwerke A1 bis A8 mit Hilfe der Fig. 2 bis 4 erläutert. Wie aus den Fig. 2 und 3 ersehen werden kann, sind die Zeichenwähler T1 und T2 mit den gleichen Bauteilen, d.h. UND-Toren G1 bis G5 aufgebaut. Dagegen unterscheiden sich die Zeichenwähler durch ihre inneren Verbindungen. In Fig. 2 sind die Torpaare G1, G2 und G3, G4 bezüglich der Eingangsleitungspaare i1, i2 und i3, i4 gleichartig angeschlossen, so dass in beiden Torpaaren G1, G2 und G3, G4 der «0»-Leiter im linken Eingangsleiterpaar i1 und i3 an den «1»-Eingang des rechten Tors G2 bzw. G4, und der «1»-Leiter des rechten Eingangsleiterpaars i2 bzw. i4 an die «0»-Eingangsleitung der linken Tore G1 bzw. G3 des Paars geführt ist. In Fig. 3 weist das linke Torpaar G1, G2 die gleichen Verbindungen auf, während beim rechten Torpaar G3, G4 der «0»-Leiter des linken Eingangsleiterpaars i3 mit der «0»-Eingangsleitung des rechten Tors G4 und der «0»-Leiter des rechten Eingangsleiterpaars i4 mit der «0»-Eingangsleitung des linken Tors G3 verbunden ist.

Mit diesen beiden Grundschaltungen, entsprechend dem linken und dem rechten Torpaar A und B, können auch die Verbindungen der beiden verbleibenden Zeichenwähler T3 und T4 hergestellt werden, indem T3 ein linkes Torpaar vom B-Typ und ein rechtes Torpaar vom A-Typ und T4 ein linkes und ein rechtes Torpaar vom B-Typ aufweist.

Die folgende Tabelle zeigt den Aufbau der vier Zeichenwähler T1 bis T4 und die aus den Fig. 2 und 3 ablesbaren Bit-Kombinationen an den Eingangsleitungen in i1 bis i4, welche an den Zeichenwählern Ausgangssignale erzeugen.

Zeichenwähler	*Aufbau*	*Bit-Kombinationen*			
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

Fig. 4 zeigt den Aufbau der Addierwerke A1 bis A8, die alle gleichartig und in bekannter Weise aufgebaut und miteinander verbunden sind. Eine genauere Beschreibung dieser bekannten Schaltungen erscheint darum nicht notwendig.

Die Arbeitsweise der Verschlüssel-Vorrichtung soll nun im folgenden an einem einfachen Beispiel beschrieben werden.

Es sei angenommen, dass zu einem bestimmten Zeitpunkt während des fortgesetzten schrittweisen Weiterschaltens des Felds der Kolonnen k1 bis k9 in den Flip-Flops a1 bis d1 der Kolonne k1 die Bits «0100» vorliegen. Dieses Zeichensignal wird über die entsprechenden Leiterpaare L1 bis L4 an die Eingangsleitungen i1 bis i4 aller Zeichenwähler T1 bis T4 weitergeleitet. Dabei gibt in Übereinstimmung mit der obigen Tabelle nur der Zeichenwähler T3 ein Ausgangssignal an die zugehörigen UND-Tore 03 und 07. An den zweiten Eingangsleitungen dieser Tore erscheint, wie an den zweiten Eingangsleitungen aller anderen Tore, mit Hilfe der Addierwerke A3 (bzw. A7) ein Signal, das der Gesamtheit der Bits in der Kolonne k4 (und der Kolonne k7) entspricht. Es sei angenommen, dass diese Bits die Kombinationen «1101» (und «0011») bilden. Das Total b1 ist dann «1» (bzw. «0»). Sobald das Ausgangssignal des Zeichenwählers das Tor 03 (bzw. 07) öffnet, wird dieses «1-Signal (bzw. «0»-Signal) an die Eingangsleitung des letzten Addierwerks SA weitergeleitet und dort dem zur gleichen Zeit als Klarschriftimpuls ankommenden Text überlagert. (Das «0»-Signal kann möglicherweise als ein zweiter zu überlagernder Impuls verwendet werden).

Bei der nächsten Schrittschaltung der Schieberegister öffnet ein durch die neue Bit-Kombination in der Flip-Flop-Kolonne k1 bestimmter Zeichenwähler den Durchgang für ein neues Signal von einer entsprechenden Kolonne, usw. Für jeden neuen Schaltschritt wird auf diese Weise ein nach vorwärts oder rückwärts gerichteter «Sprung» im praktisch immer gesamthaft verfügbaren Feld aller in der Reihe der Flip-Flops der verschiedenen Verschieberegister gespeicherten Informationen ausgeführt. Auf diese Weise kann eine vielfach grössere Zeichenänderung im Informationsfeld erreicht werden als mit einer mechanischen Ausführung von Schlüsselvorrichtungen. Dass in dem beschriebenen Beispiel für die vier Flip-Flops jeder Kolonne nur vier Zeichenwähler notwendig sind, ist dadurch bedingt, dass sowohl die Zeichen selbst als auch ihre Polumschaltung in der beschriebenen Art auf die Zeichenwähler einwirken können.

In der gleichen Art, wie bei den bekannten, mit einem binären Code arbeitenden Anordnungen zum Verschlüsseln kann das Entschlüsseln durch einfaches Überlagern des verschlüsselten Signalimpulses mit der gleichen Serie von Impulsen, wie sie zum Verschlüsseln verwendet wurde, durchgeführt werden. Infolge der Besonderheiten des binären Systems wird auf diese Weise der Text wiederhergestellt.

Es ist natürlich möglich, die beschriebene Vorrichtung auf vielerlei Arten abzuändern, insbesondere bezüglich der Anzahl der verwendeten Schieberegister und der Beziehung zwischen ihren Arbeitszyklen.

Dabei ist die beschriebene Vorrichtung nicht auf die Verwendung von Schieberegistern begrenzt, sondern es können auch andere elektrische Einrichtungen mit zyklischer Arbeitsweise verwendet werden, beispielsweise binäre Zähler mit zugehörigen logischen Kreisen.

Die Verwendung der vorliegenden Erfindung kann weiter dadurch noch erweitert werden, dass die Arbeitszyklen der elektrischen Anordnung nachregelbar sind.

PATENTANSPRUCH

Verschlüsselvorrichtung zum Verschlüsseln eines in binärer Form vorliegenden Klartextes durch Überlagerung der Klartextsignale mit veränderbaren Verschlüsselsignalen, enthaltend eine Mehrzahl elektrischer Einrichtungen (S_a bis S_d), von denen jede eine unterschiedliche Anzahl bistabiler, in Serie geschalteter Bauelemente (a1 bis a13; b1 bis b12; c1 bis c11; d1 bis d10) enthält, welche Einrichtungen parallel zueinander schrittweise weiterschaltbar sind und in denen der Ausgangszustand der bistabilen Bauelemente nach einem beliebig wählbaren Schema setzbar ist und einander zugeordnete Bauelemente dieser Einrichtungen Kolonnen bilden und der Zustand der eine Kolonne (k1 bis k10) bildenden Bauelemente (a1, b1, c1, d1; a2, b2, c2, d2, . . .) ein Verschlüsselsignal definiert, das nach Beendigung einer Schaltfolge in einer der Einrichtungen automatisch verändert wird, gekennzeichnet durch eine Anordnung (T1 bis T4) zum automatischen Auswählen einer Kolonne (k1) und zum Weiterleiten von dem Schaltzustand der bistabilen Bauelemente der ausgewählten Kolonne entsprechenden Signalen an ein Addierwerk (A1 bis A8), das das den Klartextsignalen zu überlagernde Verschlüsselsignal bildet.

UNTERANSPRÜCHE

1. Vorrichtung nach Patentanspruch, dadurch gekennzeichnet, dass die Einrichtungen (S_a bis S_d) Schieberegister und die bistabilen Bauelemente (a1 bis a13, . . .) Flip-Flops sind.

2. Vorrichtung nach Patentanspruch und Unteranspruch 1, dadurch gekennzeichnet, dass die Anordnung eine Anzahl Zeichenwähler (t1 bis T4) enthält, von denen jeder mindestens einer Kolonne zugeordnet ist und soviel Eingangsleitungen (i1 bis i4) aufweist, wie Einrichtungen (S_a bis S_d) vorhanden sind, wobei die Eingangsleitungen parallel zu den entsprechenden Ausgangsleitungen der Flip-Flops einer Referenzkolonne (z.B. k1) geschaltet sind, und jeder Zeichenwähler mit seiner Ausgangsleitung U1; U2; U3; U4) mit einer Eingangsleitung eines UND-Tors (01, 02, 03, . . . 08) verbunden ist, dessen zweite Eingangsleitung mit der Ausgangsleitung eines Addierwerks (A1; A2; . . . A8) verbunden ist, dessen Eingangsleitungen derart mit den Ausgangsleitungen der Flip-Flops in der entsprechenden Kolonne (k2; k3; . . . k9) verbunden sind, dass für ein bestimmtes Zeichen in der Referenzkokonne (k1) nur ein Zeichen-

wähler ein Ausgangssignal an seinen UND-Kreis abgibt, an dessen anderer Eingangsleitung das Ausgangssignal des Addierwerks immer erscheint, um am UND-Tor ein Ausgangssignal zu bilden, das dem Verschlüsselsignal entspricht.

3. Vorrichtung nach Unteranspruch 2, dadurch gekennzeichnet, dass jeder Zeichenwähler eine Mehrzahl UND-Tore (G1 bis G5) aufweist, deren Eingangsleitungen mit den Ausgangsleitungen der Flip-Flops (a1 bis d1) einer Referenzkolonne (k1) derart verbunden sind, dass das Ausgangssignal der Tore nur für bestimmte definierte Zeichen in der Referenzkolonne erscheint.

4. Vorrichtung nach Unteranspruch 2, dadurch gekennzeichnet, dass für die Verschiebung der Verbindungen zwischen den Kolonnen und den Zeichenwählern (T1 bis T4) zwischen den Ausgangsleitungen der Kolonnen (k1 bis k9) und den zugehörigen Addierwerken (A1 bis A8) ein Schalter (Systemwähler V) vorgesehen ist.

AB Transvertex
Vertreter: Dr. Arnold R. Egli, Zürich

FIG.1

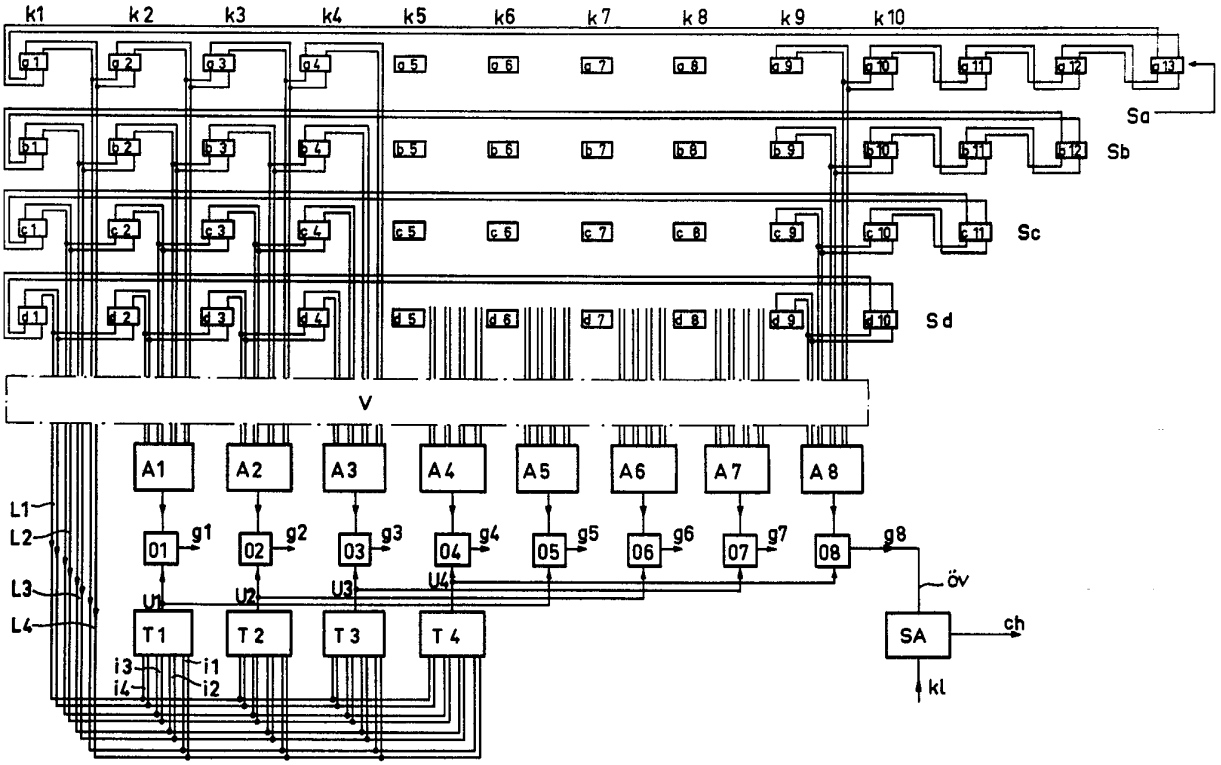
k1
k2
k3
k4
k5
k6
k7
k8
k9
k10
Sa
Sb
Sc
Sd
V
A1
A2
A3
A4
A5
A6
A7
A8
L1
L2
L3
L4
01
02
03
04
05
06
07
08
g1
g2
g3
g4
g5
g6
g7
g8
öv
U1
U2
U3
U4
T1
T2
T3
T4
SA
ch
kl
i3
i4
i1
i2

FIG.2

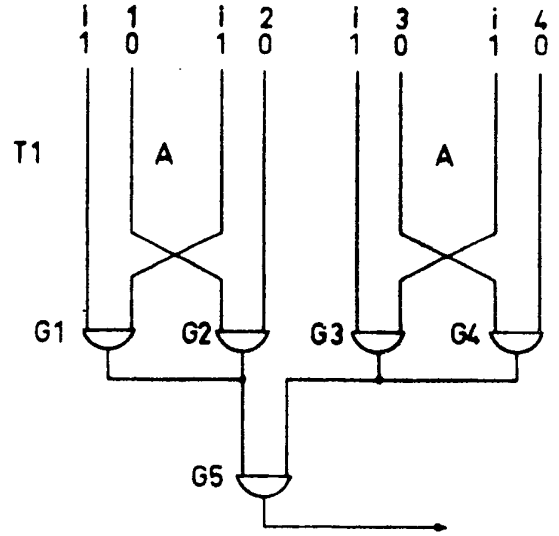

FIG.3

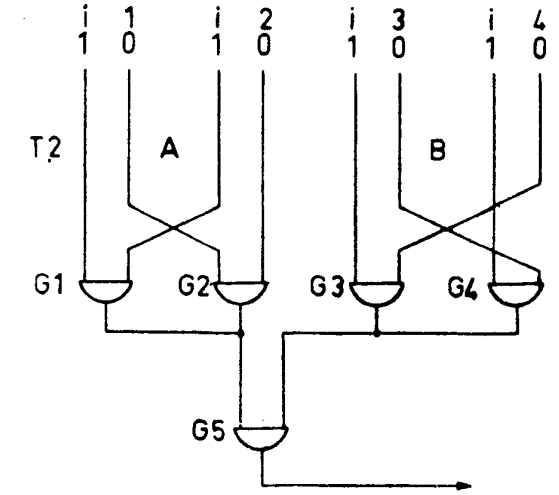

FIG.4