(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 199 26 640 C 2**

(51) Int. Cl.[7]:
G 06 F 7/58
H 03 K 3/84

(21) Aktenzeichen: 199 26 640.9-53
(22) Anmeldetag: 11. 6. 1999
(43) Offenlegungstag: 21. 12. 2000
(45) Veröffentlichungstag der Patenterteilung: 14. 8. 2002

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Freitag, Rolf, Dipl.-Phys., 90461 Nürnberg, DE

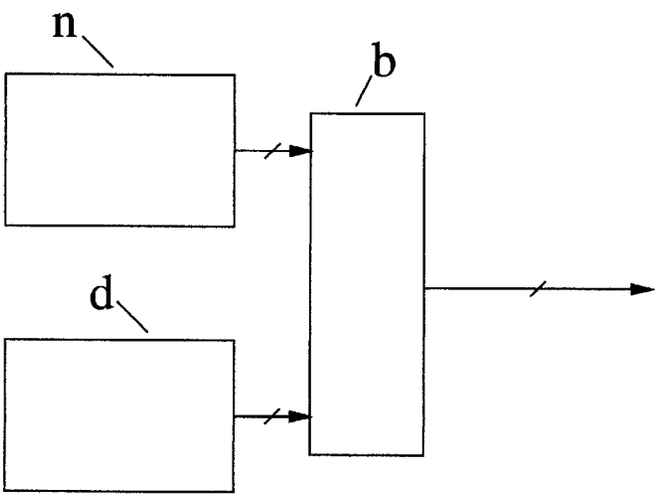
(72) Erfinder:
gleich Patentinhaber

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US 51 53 532 A
US 43 55 366 A
IBM Technical Disclosure Bulletin, Vol. 34, No. 7B, Dec. 1991;
KÜHN, E., SCHMIED, H.: Handbuch Integrierte Schaltkreise, VEB Verlag Technik Berlin, 1979;

(54) Verfahren zur Erzeugung von echten Zufallszahlen sowie Zufallszahlengenerator

(57) Verfahren zur Erzeugung von echten Zufallszahlen, dadurch gekennzeichnet, dass ein nichtdeterministisches digitales Zufallssignal durch Verwendung des Rauschens digitaler Bauelemente als Signalquelle erzeugt wird.



DE 199 26 640 C 2

DE 199 26 640 C 2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Erzeugung von Zufallszahlen sowie einen Zufallszahlengenerator.

[0002] Es ist bekannt, dass zur Erzeugung echter, d. h. nichtdeterministischer Zufallszahlen ein nichtdeterministisches Signal wie z. B. Schrotrauschen, oder thermisches Rauschen benötigt wird.

[0003] Üblicherweise wird hierzu Rauschen verstärkt und AD-gewandelt (Patent EP 0903665 C, **Fig.** 1; Numnerical Recipes Code CDROM, ISBN 0-521-57608-3, Bild/extras/random/doc/hororan.gif).

[0004] Der Nachteil bei diesem und ähnlichen Verfahren ist, dass bei hohen Frequenzen (bei der Grenzfrequenz des Verstärkers oder der Rauschquelle) die Qualität der so generierten Zufallszahlen mit einem Entropiebelag kleiner als 0,9 Bit/Bit sehr schlecht wird. Dadurch sind solche Generatoren für schnelle Anwendungen wie z. B. Rausch-Radar (Narayanan, R. M. et. al.: Design and performance of a polarimetic noise radar for detection of shallow buried targets. Proc. SPIE Vol. 2496 Orlando **1995**) prinzipiell ungeeignet.

[0005] Außerdem eignen sich solche analogen Schaltungen nicht für die Höchstintegration. Hinzu kommen Probleme wie Alterung und Umgebungseinflüsse wie Temperatur, Druck und Magnetfeld, so dass die Taktfrequenz, mit der die Zufallszahlen ausgelesen werden, erniedrigt werden muss, um auch über längere Zeit und bei veränderten Umgebungseinflüssen einen Mindest-Entropiebelag garantieren zu können.

[0006] Aus IBM Technical Disclosure Bulletin, Vol. 34, NO. 7B, December **1991** ist ein Verfahren zur Erzeugung von Zufallszahlen mittels eines Rauschgenerators zur Erzeugung weißen Rauschens sowie mittels eines Pseudo-Zufallsgenerators basierend auf einem Datenverschlüsselungsalgorithmus bekannt.

[0007] Aus US 43 55 366 A ist ein Zufallszahlengenerator bekannt, der aus einem Rauschgenerator sowie aus einem Abtastregister aufgebaut ist. Der Zufallszahlengenerator umfasst weiter einen Schaltkreis zur Reduzierung einer Autokorrelation des Zufallszahlengenerators.

[0008] Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren zur Erzeugung von Zufallszahlen bzw. einen Zufallszahlengenerator anzugeben, das bzw. der die Erzeugung von Zufallszahlen hoher Qualität ermöglicht, insbesondere sollen auch bei hohen Taktfrequenzen (oberhalb von 1 GHz) echte Zufallszahlen hoher Qualität, d. h. mit einem Entropiebelag größer 0,99 Bit/Bit, nur mit digitalen und höchstintegrierbaren Bauelementen erzeugbar sein.

[0009] Diese Aufgabe wird durch ein Verfahren bzw. einen Zufallszahlengenerator mit den in den Ansprüchen 1 bzw. 11 angegeben Merkmalen gelöst.

[0010] Dabei werden die Zufallszahlen von einer digitalen Rauschquelle mit den Zufallszahlen von einer (oder mehreren) anderen Rauschquelle oder einem Pseudozufallszahlengenerator boolsch verknüpft.

[0011] Der Entropiebelag der so erzeugten Zufallszahlen kann durch Verknüpfen von weiteren Zufallszahlen aus einer oder mehreren weiteren digitalen Rauschquellen beliebig nahe dem theoretischen Limit von 1,0 Bit/Bit angenähert werden. Im Spezialfall des EXOR (= Summe modulo 2, least significant bit) und EXNOR ergibt sich dies direkt aus dem zentralen Grenzwertsatz.

[0012] Bei Anwendungen, bei denen nur echte Zufallszahlen ohne einen Mindest-Entropiebelag benötigt werden, ist es ausreichend die Verknüpfung mit Pseudozufallszahlen, z. B. von Schieberegisterfolgen maximaler Länge, durchzuführen.

[0013] Ein mit der Erfindung erreichter Vorteil ist, das sie vollständig digital ist und z. B. in eine CPU integriert werden kann. Dadurch können die Zufallszahlen ohne Wartezyklen mit vollem Systemtakt erzeugt werden, so dass kein Zwischenspeichern der Zufallszahlen erforderlich ist und Rechenzeit, die z. B. bei Monte-Carlo-Simulationen für die Berechnung von (Pseudo-) Zufallszahlen aufgewendet werden muss, eingespart werden kann.

[0014] Ein weiterer Vorteil ist, dass die Taktfrequenz kontinuierlich bis auf 0,0 Hz verringert werden kann (z. B. für einen sleep-Modus).

[0015] **Fig.** 1 zeigt die Grobstruktur eines echten Zufallszahlengenerators, der aus einem nichtdeterministischen Vektor (d. h. Leitungsbündel) von der nichtdeterministischen Quelle n und einem deterministischen Vektor von der deterministischen Quelle d mit der boolschen Verknüpfung b boolsch verknüpft und diesen echten Zufallsvektor (= Zufallszahl) ausgibt. Ein konkretes Beispiel zeigt **Fig.** 3.

[0016] **Fig.** 2 zeigt die Grobstruktur eines echten Zufallszahlengenerators, der aus einem nichtdeterministischen Vektor (d. h. Leitungsbündel) von der nichtdeterministischen Quelle n durch eine boolsche Verknüpfung b einen neuen echten Zufallsvektor (= Zufallszahl) erzeugt und ausgibt. Ein konkretes Beispiel zeigt **Fig.** 4.

[0017] Ausführungsbeispiele der Erfindung sind in den folgenden zwei Schaltplänen dargestellt und werden im Folgenden näher beschrieben.

[0018] Da ein m-Bit-Zufallszahlengenerator (mit vollem Systemtakt) einfach aus m 1-Bit-Zufallszahlengeneratoren aufgebaut werden kann, sind es nur Schaltpläne von 1-Bit-Zufallszahlengeneratoren.

[0019] **Fig.** 3 ist ein Schaltplan eines echten Zufallszahlengenerators (1 Bit). Als nichtdeterministische digitale Rauschquellen werden zwei invertierende Schmitt-Trigger 0 und 6 verwendet, die asynchron zum (System-)Takt und mit einem Phasen-Rauschen von erfahrungsgemäß ca. 5% schwingen.

[0020] Die anschließenden zwei D-Flip-Flops **1** und **8** lesen die primären Zufalls-Bits synchron aus. Um sicherzustellen, dass daraus generierten Zufallsbitfolgen ungefähr gleich viele binäre Nullen und Einsen enthalten, wird das Signal vom oberen Schmitt-Trigger 0 nach der Synchronisierung R1 mit einem vom T-Flip-Flop **2** halbierten Takt (clk/2) und einem EXOR-Gatter **3** zyklisch invertiert. Zum selben Zweck wird von dem Signal vom unteren Schmitt-Trigger, noch vor dem synchronisierenden D-Flip-Flop **8**, mit einem T-Flip-Flop **7** die Anzahl der steigenden Flanken modulo 2 gezählt.

[0021] Mit dem 97-stufigen Schieberegister **5** und dem Schaltgatter **4** wird ein Pseudozufallsbitzyklus PN1 der Länge 2^{97}-**1** erzeugt (Numerical Recipes in C, 2nd ed., ISBN 0-521-43108-5, Seite 298–299).

[0022] Falls der Zufallszahlengenerator aus mehreren solchen 1-Bit-Zufallszahlengeneratoren besteht, sollten die anderen Pseudozufallsbitzykluslängen teilerfremd sein.

[0023] Mit den EXOR-Gattern **9** und **10** schließlich werden diese drei Zufallsbits zu einem verknüpft (R1 EXOR R2 EXOR PN1 EXOR clk/2), das ausgegeben wird.

[0024] Es ist nebensächlich ob diese Schaltung in CMOS (wie bisher), ECL, TTL o. a. realisiert wird. Abhängig von der Logik-Familie, Alterung und Umgebungs-Einflüssen wie Temperatur und Versorgungsspannung werden sich die nichtdeterministischen Zufallssignale R1 und R2 ändern, aber durch das EXOR von R1 und R2 werden diese Einflüsse zum Teil kompensiert und durch das EXOR mit den Pseudozufallsbits PN1 werden die Restkorrelationen so überdeckt, dass sie am Ausgang praktisch nicht nachweisbar sind.

[0025] **Fig.** 4 ist ein anderer Schaltplan eines echten Zu-

fallszahlengenerators (1 Bit). Durch die mit Invertern **1** aufgebauten Ketten wird der (System-)Takt mit einer Verzögerungs-Schwankung von erfahrungsgemäß ca. 5% je Inverter verzögert. Die Laufzeit durch eine Inverter-Kette ist nach dem zentralen Grenzwertsatz (annähernd) normalverteilt und die Standardabweichung der Laufzeit ist dadurch (annähernd) proportional der Quadratwurzel der Inverteranzahl. Dadurch kann, falls die in **Fig.** 2 nur 8 Inverter langen Inverter-Ketten zu kleine Laufzeitschwankungen aufweisen, dieser Mangel durch ein Verlängern der Inverter-Ketten beseitigt werden.

[0026] Die ersten zwei D-Flip-Flops **2** und **3** geben nach der steigenden Flanke am Takt-Eingang eine 0 (Low) aus, wenn die Laufzeit der Inverter-Kette am Takt-Eingang kürzer war als die der Inverter-Kette am Daten-Eingang, und eine 1 (High) sonst. Die folgenden zwei D-Flip-Flops **4** und **5** lesen diese primären Zufalls-Bits synchron aus. Mit dem Logik-Gatter **6** wird das EXOR der zwei Zufallsbits gebildet, um den Entropiebelag weiter zu erhöhen.

Patentansprüche

1. Verfahren zur Erzeugung von echten Zufallszahlen, **dadurch gekennzeichnet**, dass ein nichtdeterministisches digitales Zufallssignal durch Verwendung des Rauschens digitaler Bauelemente als Signalquelle erzeugt wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das nichtdeterministische Zufallssignal unter Verwendung des Phasenrauschens digitaler Bauelemente erzeugt wird.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass ein oder mehrere nichtdeterministische digitale Zufallssignale aus Laufzeitschwankungen zwischen Logik-Gatter-Ketten erzeugt werden.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das nichtdeterministische Zufallssignal mit einem oder mehreren anderen digitalen Zufallssignalen boolsch verknüpft wird.
5. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass als boolsche Verknüpfung das EXOR oder EXNOR verwendet wird.
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass mehrere nichtdeterministische Zufallssignale boolsch verknüpft werden.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass ein oder mehrere nichtdeterministische Zufallssignale mit einem oder mehreren deterministischen Zufallssignalen boolsch verknüpft wird.
8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass die deterministischen Zufallssignale der halbierte Takt oder eine Schieberegisterfolge maximaler Länge sind.
9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass als nichtdeterministische digitale Zufallssignalquelle ein oder mehrere frei schwingende rückgekoppelte Logikgatter verwendet werden.
10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass als nichtdeterministische digitale Zufallssignalquelle ein oder mehrere Ringoszillatoren verwendet werden.
11. Zufallszahlengenerator zur Ausführung des Verfahrens nach einem der Patentansprüche 1 bis 10, dadurch gekennzeichnet, dass echte Zufallszahlen aus den least siginificant bits der Summen von mehreren nichtdeterministischen digitalen Zufallssignalen erzeugbar sind, z. B. mittels EXOR.
12. Zufallszahlengenerator nach Anspruch 11, dadurch gekennzeichnet, dass echte Zufallszahlen aus den least siginificant bits der Summen von einem oder mehreren nichtdeterministischen digitalen Zufallssignalen und einem oder mehreren deterministischen Zufallssignalen erzeugbar sind, z. B. mittels EXNOR.
13. Zufallszahlengenerator nach einem der Ansprüche 11 oder 12, dadurch gekennzeichnet, dass als nichtdeterministische digitale Rauschquellen invertierende Schmitt-Trigger verwendet werden.
14. Zufallszahlengenerator nach einem der Ansprüche 11 oder 12, dadurch gekennzeichnet, dass der Zufallszahlengenerator Logikgatterketten mit Invertern aufweist.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: **DE 199 26 640 C2**
Int. Cl.[7]: **G 06 F 7/58**
Veröffentlichungstag: 14. August 2002

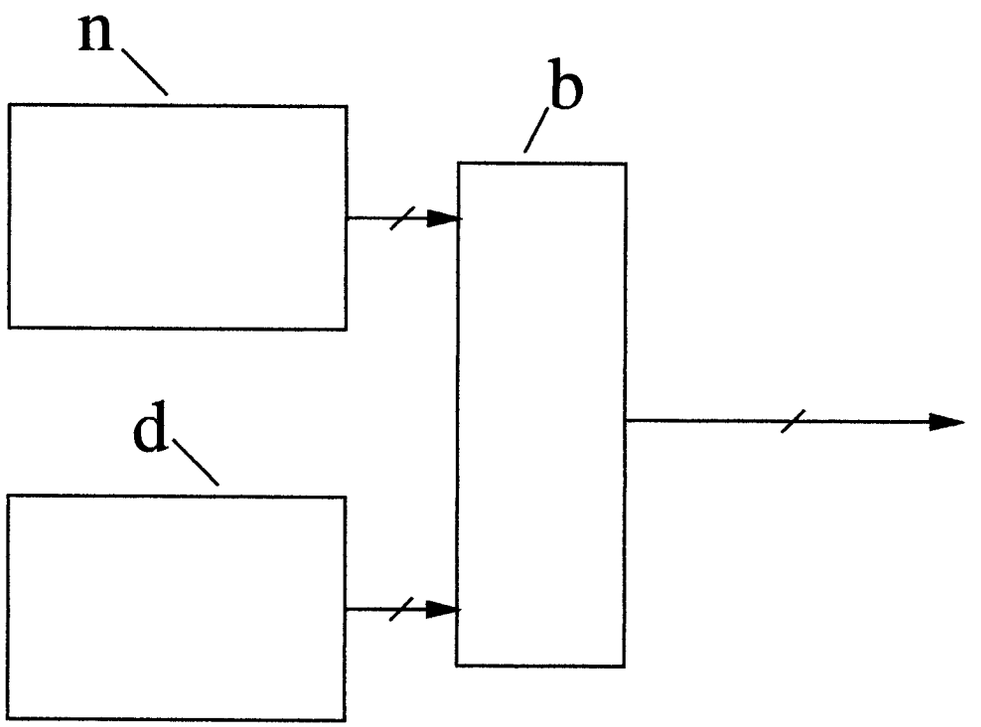


Fig. 1

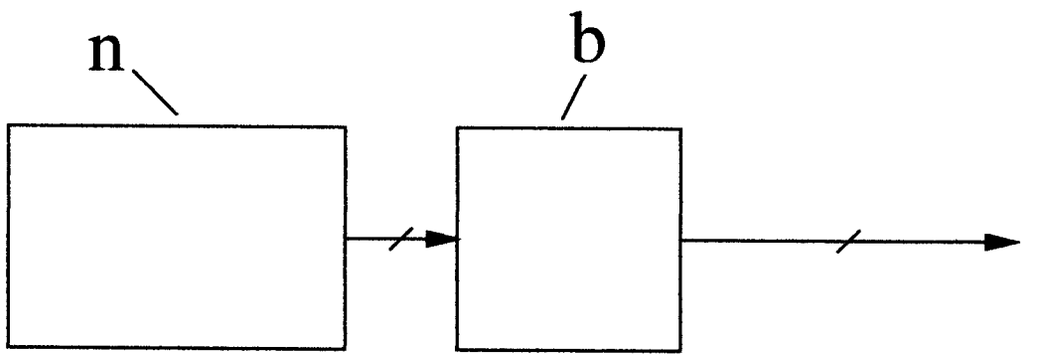


Fig. 2

Nummer: DE 199 26 640 C2
Int. Cl.[7]: G 06 F 7/58
Veröffentlichungstag: 14. August 2002

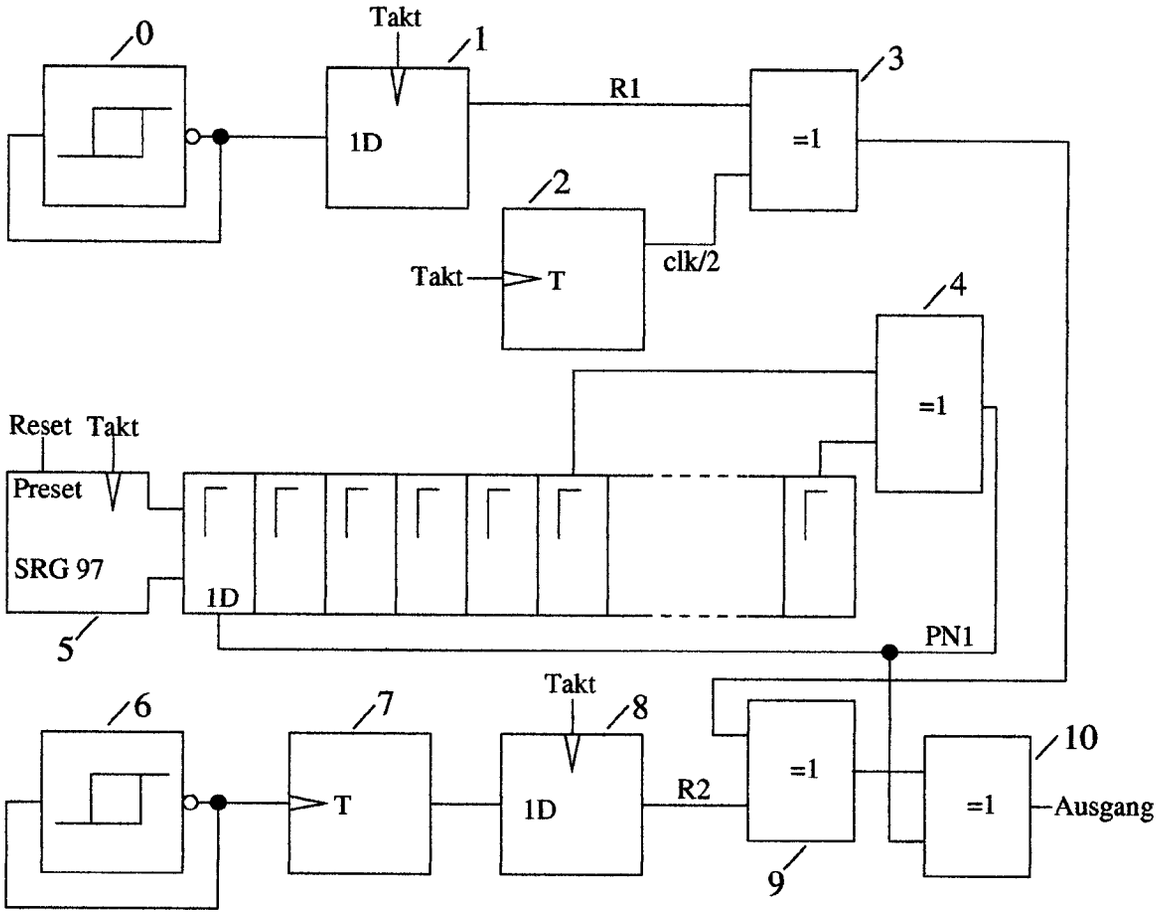


Fig. 3

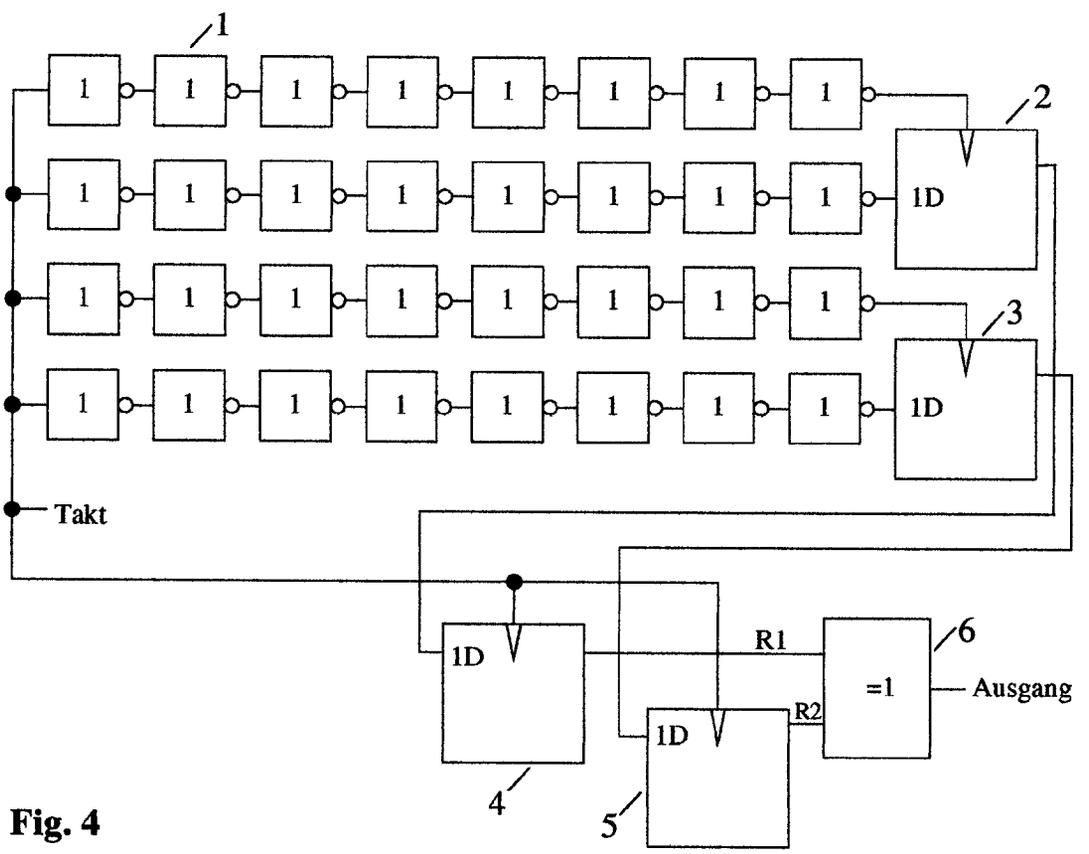


Fig. 4