

*Translation of the german patent specification number 19926640 C2.
Rolf Freitag, 2005-11-11, First Edition*

File number: 19926640.9-53

Day of registration: 1999-6-11

Day of publication: 2000-12-21

Assignment of patent, day of publication: 2002-8-7

Int. Cl.: G 06 F 7/58, H 03 K 3/84

Patent owner: Freitag, Rolf, Dipl.-Phys., 90461 Nürnberg, DE

Inventor: See patent owner.

For the evaluation have been taken into account: US 5153532A, US 4355366A,
IBM Technical Disclosure Bulletin, Vol. 34, No. 7B, Dec. 1991;
KÜHN, E., SCHMIED, H.: Handbuch integrierte Schaltkreise,
VEB Verlag Technik Berlin, 1979;

Technique for producing true random numbers as well as random number generator

Abstract

Technique for producing true random numbers, characterized by a nondeterministic digital random signal which is generated by noise of digital electronic devices.

Description

[0001] The invention is a method for generating random numbers as well as a random number generator.

[0002] It is known that for true, i. e. nondeterministic random numbers a nondeterministic signal, e. g. shot noise or thermal noise is necessary.

[0003] Usually for this purpose noise is amplified and AD-converted (Patent EP0903665, Fig.1; Numerical Recipes Code CDROM, ISBN 0-521-57608-3, Picture /extras/random/doc/hororan.gif).

[0004] The disadvantage of this method is that at high frequencies (at the cut-off-frequency of the amplifier or the noise source) the so generated random numbers do have a low quality with an entropy cover of less than 0.9 Bit/Bit. That's the reason why such generators can not be used for high speed applications like noise radar (Narayanan, R. M. et. al.: Design and performance of a polarimetric noise radar for detection of shallow buried targets. Proc. SPIE Vol. 2496 Orlando 1995).

[0005] Another disadvantage is that such analog circuits can not be used for large-scale integration. They also have additional disadvantages like aging, dependence on temperature, pressure and magnetic field, so that for long times and not constant environmental effects a slow clock frequency has to be used to ensure a minimum entropy cover.

[0006] From IBM Technical Disclosure Bulletin, Vol. 34, No. 7B, Dec. 1991, a method for generating random numbers using a noise generator for producing white noise as well as a pseudo random number generator, based on a data encryption algorithm, is known.

[0007] From US 4355366A a random number generator is known which consists of a noise generator and a sample register. The random number generator has an additional circuit for reducing the autocorrelation.

[0008] The underlying task of the invention is therefore to produce high quality true random numbers, i. e. with an entropy cover of 0.99 Bit/Bit, at high clock frequencies (above 1 GHz) only with digital electronic components which can be used for large-scale integration.

[0009] This task is solved with a method and respectively a generator due to the patent claims 1 to 11.

[0010] In this way the random numbers from a digital noise source are combined via boolean logic with the random numbers produced by another (or more) noise source(s) or a pseudo random number generator.

[0011] The entropy cover of the random numbers, produced this way, can be increased up to the theoretical limit of 1.0 Bit/Bit arbitrary close by combining them with other random numbers from one or more digital noise sources. In case of the EXOR (= sum modulo 2, least significant bit) and EXNOR this follows from the central limit theorem.

[0012] For applications which do need random numbers without a minimum entropy cover it is enough to do this combination with pseudo random numbers, e. g. with maximum length shift register sequences.

[0013] One advantage of the invention is that it is completely digital and can be integrated e. g. in a CPU. By this means the random numbers can be produced without waiting cycles at full clock speed and does not need latching. This can be used e. g. for Monte-Carlo-Simulations where the CPU time for calculating (pseudo-)random numbers can be economized.

[0014] Another advantage is that the clock frequency can be decreased stepless down to 0.0 Hz (e. g. for a sleep mode).

[0015] Fig. 1 shows the structure of a true random generator which boolean combines a nondeterministic vector (i. e. bunched circuit) from a nondeterministic source n and a deterministic vector d to the true random vector (=random number) as output. A concrete example is shown in Fig. 3.

[0016] Fig. 2 shows the structure of a true random generator which boolean combines a nondeterministic vector (i. e. bunched circuit) from a nondeterministic source n to the true random vector (=random number) as output. A concrete example is shown in Fig. 4.

[0017] Example implementations are shown in the following two circuit diagrams and are described below.

[0018] Because a m -Bit random number generator (with full clock speed) can be composed of m 1-Bit random number generators these circuit diagrams are for 1-Bit random number generators.

[0019] Fig. 3 is a circuit diagram of a random number generator (1 Bit). As nondeterministic digital noise sources two inverting Schmitt triggers **0** and **6** are used, which are oscillating asynchronous to the (system-)clock and with a phase noise of empiric approx. 5 %.

[0020] The following two D Flip-Flops **1** and **8** do read the primary random bits synchro-

nous. To ensure that the random bit sequences therewith produced do contain approximate equal numbers of zeros and ones, the signal from the upper Schmitt trigger **0** after the synchronization (R1) is inverted cyclic with the halved clock ($\text{clk}/2$) from a T Flip-Flop **2** and an EXOR gate **3**. For the same purpose the signal from the lower Schmitt trigger is used to drive a T Flip-Flop **7** to count the rising edges modulo 2 before the synchronizing D Flip-Flop **8**.

[0021] With the 97-stage shift register **5** and the gate **4** a pseudo random bit sequence (PN1) of length $2^{97} - 1$ is produced (Numerical Recipes in C, 2nd ed., ISBN 0-521-43108-5, Page 298-299).

[0022] If the random number generator consists of several of these 1-Bit random number generators, the other pseudo random bit sequence lengths should be coprime.

[0023] These three random bits are finally put together to one (R1 EXOR R2 EXOR PN1 EXOR $\text{clk}/2$), which is the output, by the two EXOR gates **9** and **10**.

[0024] The technology used, CMOS (as yet), ECL, TTL or other, is secondary. Dependent on the technology used, aging and environment effects like temperature and supply voltage the nondeterministic signals R1 and R2 are changed but by the EXOR of R1 and R2 these influences are partially compensated and by the EXOR of the pseudo random bits (PN1) the remaining correlations are dissembled so, that they are practical undetectable.

[0025] Fig. 4 is another circuit diagram of a true random number generator (1 Bit). The chains of inverters **1** do delay the (system-)clock with a delay fluctuation of empiric approx. 5 % per inverter. The runtime through the chain of inverters is, due to the central limit theorem, (nearly) normal distributed and the standard deviation of the runtime is therefore (nearly) proportional to the square root of number of inverters. Thus, if the inverter chain length of 8 in Fig. 2 has too small runtime fluctuations this can be solved by extending them.

[0026] After the rising edge at the clock input the first two D Flip-Flops **2** and **3** do output a 0 (low) when the runtime of the inverter chain at clock input was shorter as the one from the inverter chain at the data input and 1 (high) else. The following two D Flip-Flops **4** and **5** do read these primary random bits synchronous. With the logic gate **6** the EXOR of two random bits is generated to further increase the entropy cover.

Patent claims

1. Method for generating of true random numbers, characterized in that a nondeterministic digital random signal is generated by using the noise of digital components as a signal source.
2. Method according claim 1, characterized in that the non deterministic random signal is generated by using the phase noise of digital components.
3. Method according claim 1 or 2, characterized in that one or more non deterministic

digital random signals are generated out of the time shifts between chains of logic gates.

4. Method according claim 1 to 3, characterized in that the non deterministic random signal is combined boolean with one or more other digital random signals.
5. Method according claim 3, characterized in that as a boolean operation the EXOR or EXNOR is used.
6. Method according one of claims 1 to 5, characterized in that several nondeterministic random signals are combined via boolean logic.
7. Method according one of claims 1 to 6, characterized in that one or more nondeterministic random signals are combined with one or more deterministic random signals via boolean logic.
8. Method according claim 7, characterized in that the deterministic random signals are half of the clock or a shift register sequence of maximum length.
9. Method according one of claims 1 to 8, characterized in that as non deterministic digital random signal source one or more freely oscillating regenerative logic gates are used.
10. Method according one of claims 1 to 9, characterized in that as non deterministic digital random signal source one or more ring oscillators are used.
11. Generator of random numbers for executing the method according one of claims 1 to 10, characterized in that true random numbers are generatable out of the least significant bits of the sums of several non deterministic digital random numbers, e.g. with EXOR.
12. Generator of random numbers according claim 11, characterized in that true random numbers are generatable out of the least significant bits of the sums of one or more non deterministic digital random numbers and one or more deterministic random signals, e.g. with EXNOR.
13. Generator of random numbers according claim 11 or 12, characterized in that as non deterministic digital signal sources inverting Schmitt triggers are used.
14. Generator of random numbers according claim 11 or 12, characterized in that the generator of random numbers have chains of logic gates with inverters.

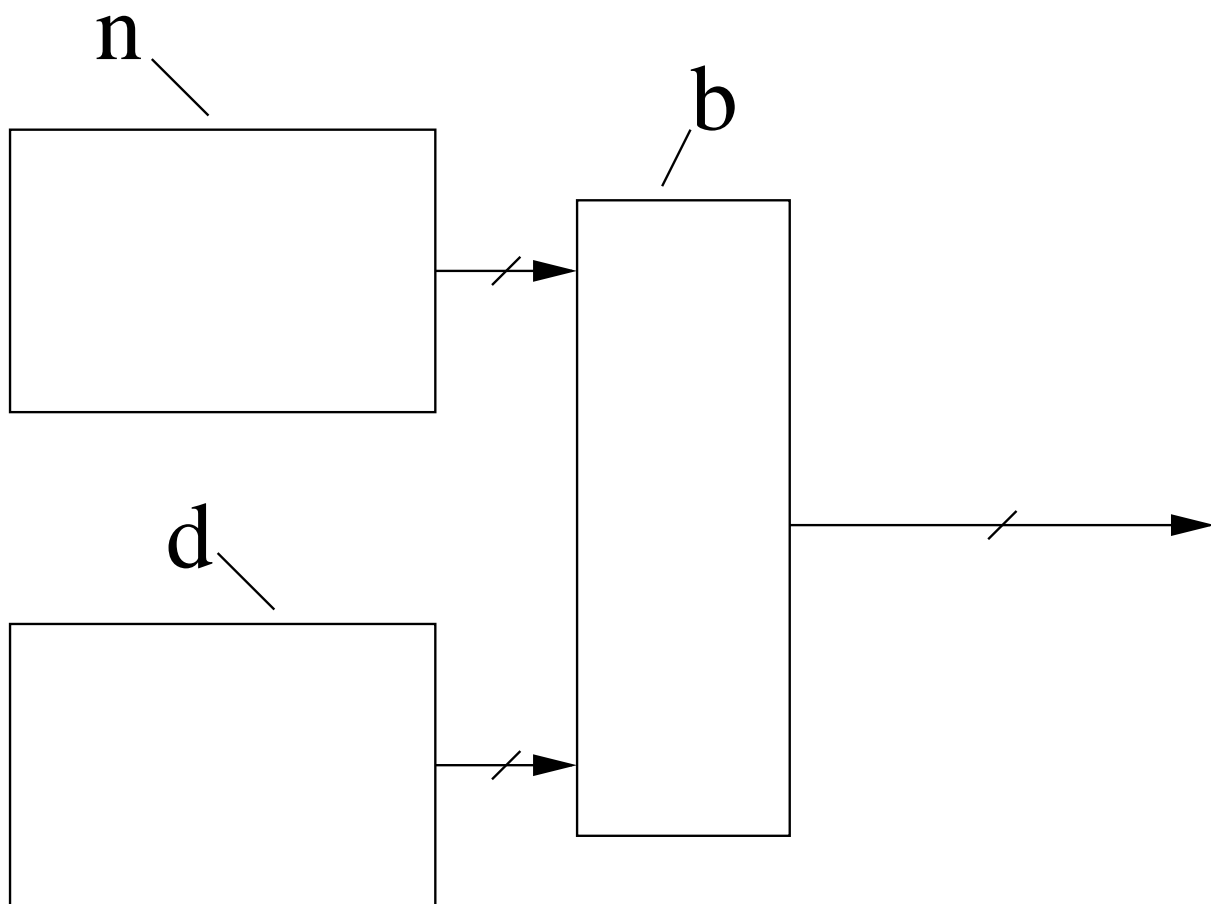


Fig. 1

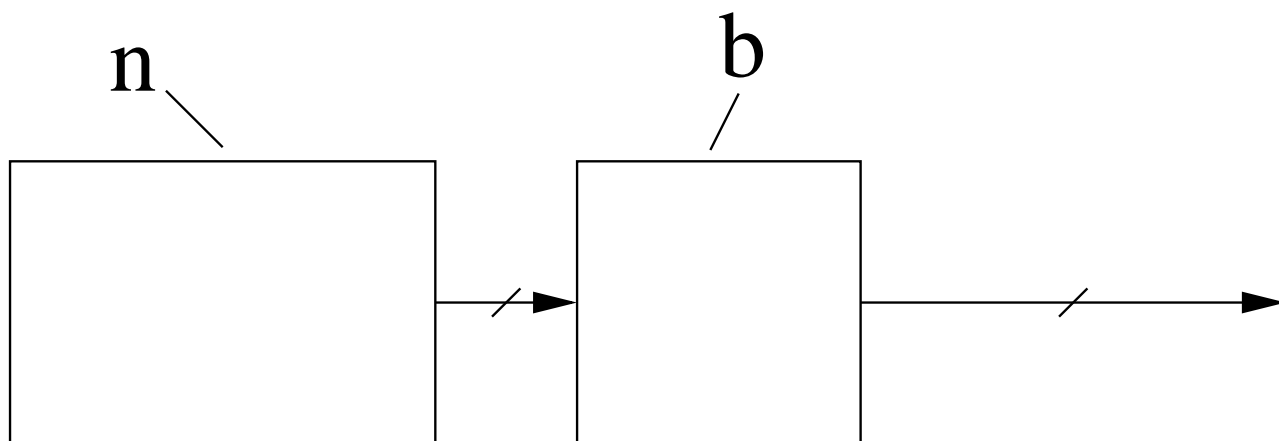


Fig. 2

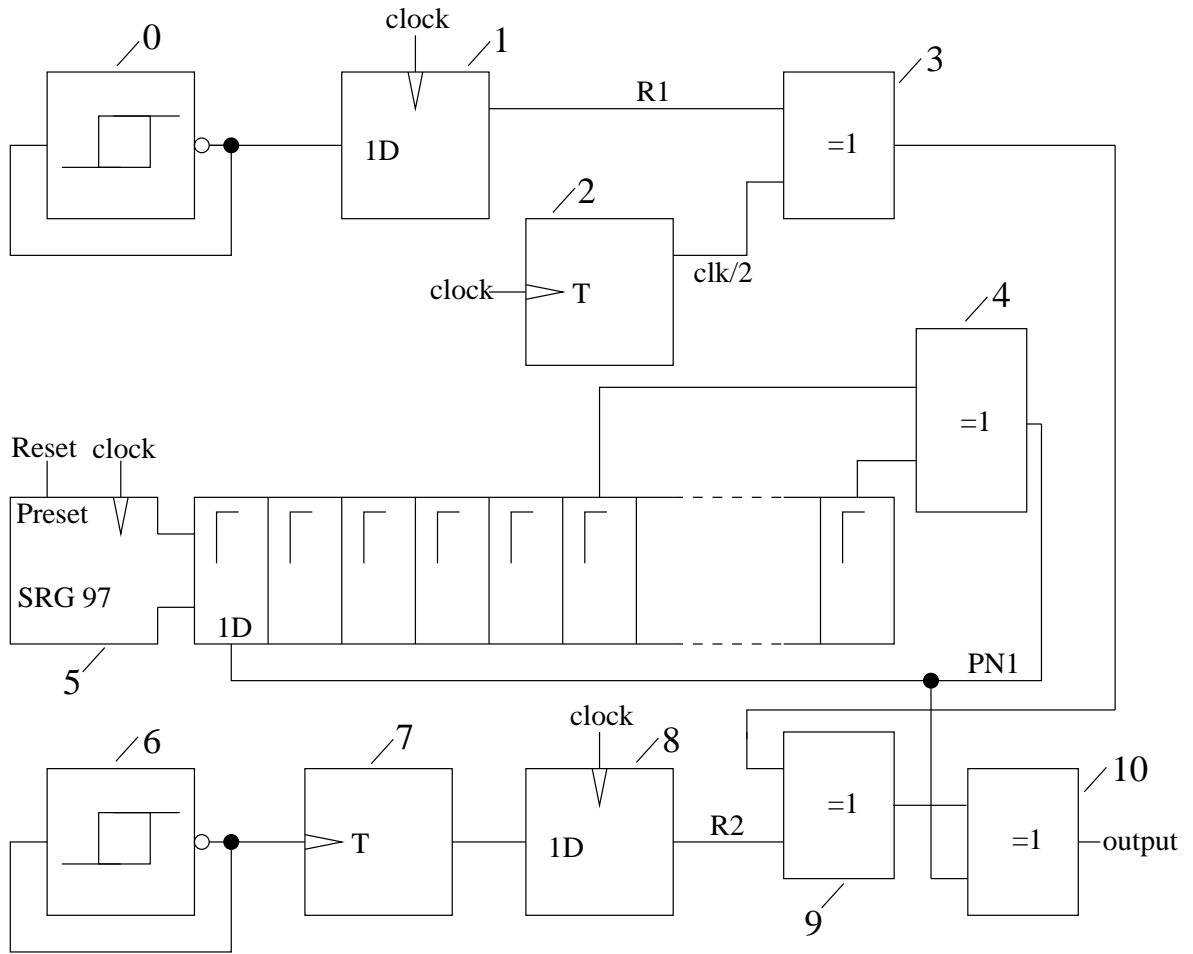


Fig. 3

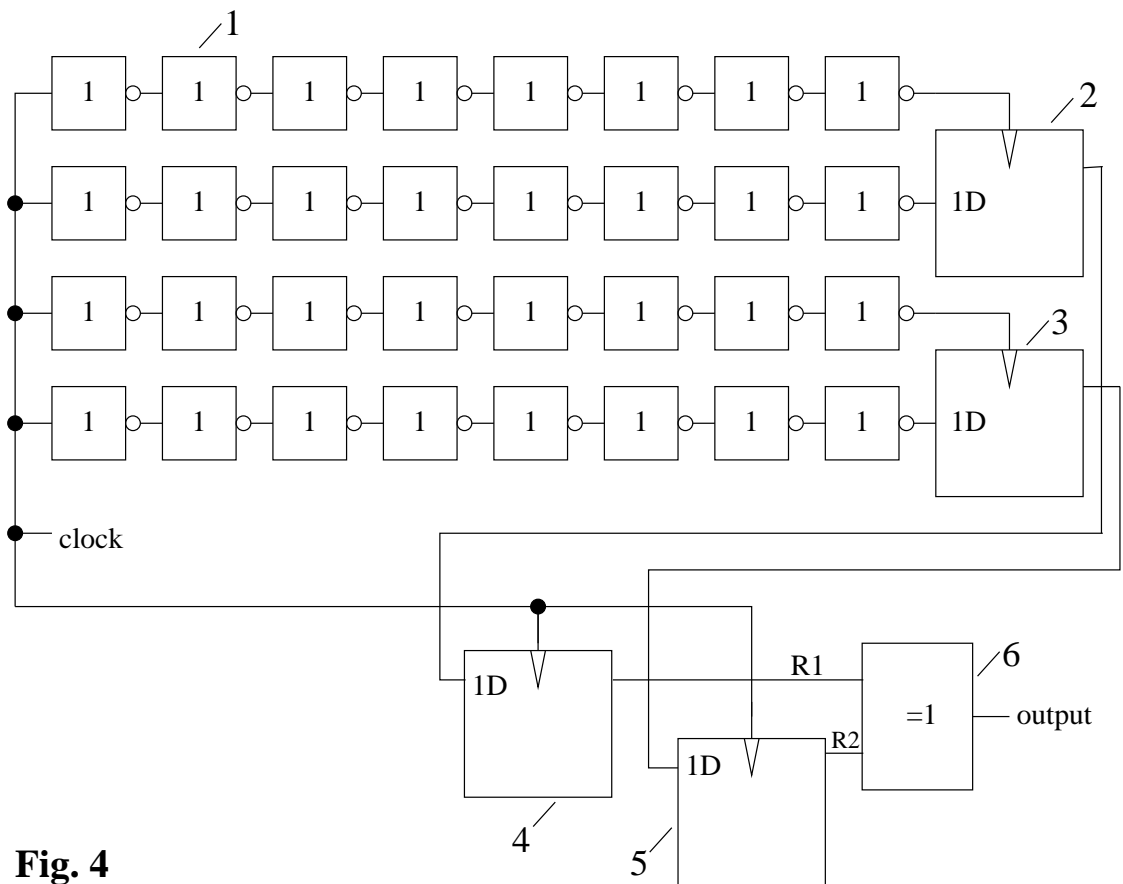


Fig. 4