(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 100 219 B9

(12) CORRECTED EUROPEAN PATENT SPECIFICATION

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Description
Claims EN 1

(48) Corrigendum issued on:
12.10.2011 Bulletin 2011/41

(45) Date of publication and mention
of the grant of the patent:
13.10.2010 Bulletin 2010/41

(21) Application number: **08776532.7**

(22) Date of filing: **26.06.2008**

(51) Int Cl.:
G06F 7/58 $^{(2006.01)}$

(86) International application number:
PCT/IB2008/052574

(87) International publication number:
WO 2009/074889 (18.06.2009 Gazette 2009/25)

(54) BIT GENERATOR

BIT-GENERATOR

GÉNÉRATEUR DE BITS

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR

(30) Priority: **12.12.2007 IL 18808907**

(43) Date of publication of application:
16.09.2009 Bulletin 2009/38

(73) Proprietor: **NDS Limited**
Staines, Middlesex TW18 4EX (GB)

(72) Inventor: **KALUZHNY, Uri**
99729 Jerusalem (IL)

(74) Representative: **Hoarton, Lloyd Douglas Charles**
Forrester & Boehmert
Pettenkoferstrasse 20-22
80336 Munich (DE)

(56) References cited:
US-A1- 2004 205 095 US-A1- 2005 097 153
US-A1- 2006 161 610

Printed by Jouve, 75001 PARIS (FR)

Description

FIELD OF THE INVENTION

[0001] The present invention relates to random or pseudo-random bit generators, and in particular to, non-linear feedback shift registers.

BACKGROUND OF THE INVENTION

[0002] By way of introduction, the use of random delays, also known as random wait-states, is often proposed as a generic counter-measure against side-channel analysis and fault attacks by stalling a CPU during execution of embedded software. The efficiency of a random delay triggering scheme improves as the variance of the random wait-states increases. However, systems typically incorporate random wait-states that are uniformly distributed.

[0003] The following references are also believed to represent the state of the art:

US Patent 6,167,553 to Dent;

US Patent 6,785,389 to Sella, et al.;

US Published Patent Application 2003/0085286 of Kelley, et al.;

US Published Patent Application 2004/0076293 of Smeets, et al.;

US Published Patent Application 2004/0205095 of Gressel, et al.;

US Published Patent Application 2006/0161610 of Goettfert, et al.;

Article entitled "Efficient Use of Random Delays" by Olivier Benoit and Michael Tunstall of Royal Holloway, University of London; and

Chapter 6 of Handbook of Applied Cryptography (CRC Press Series on Discrete Mathematics and Its Applications) by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone.

[0004] The disclosures of all references mentioned above and throughout the present specification, as well as the disclosures of all references mentioned in those references, are hereby incorporated herein by reference.

SUMMARY OF THE INVENTION

[0005] The present invention seeks to provide an improved feedback shift-register.

[0006] There is thus provided in accordance with a preferred embodiment of the present invention, a system, including a feedback shift-register having L serially connected stages including a first stage and a final stage, the stages being denoted 0 to L-1 from the first stage to the final stage respectively, the stages being operative to store a plurality of bits such that each of the stages is operative to store one of the bits, and a non-linear feedback sub-system, at least some of the stages having an output operationally connected to the non-linear feedback sub-system, the non-linear feedback sub-system being operative to receive input from a stage n and a stage 2n+1 of the stages, the non-linear feedback sub-system including a first AND logic gate, the first AND logic gate having a first input operationally connected to the output of the stage n, a second input operationally connected to the output of the stage 2n+1, and an output, the non-linear feedback sub-system having an output based, at least in part, on a value of the output of the first AND logic gate, a clock operationally connected to the feedback shift-register, the clock being operative to control the movement of the bits along the stages, a bit generator having an output, the bit generator being operative to generate a plurality of random/ pseudo-random bits for outputting via the output of the bit generator, and a main XOR logic gate having a first and second input and an output, the output of the bit generator being operationally connected to the first input of the main XOR logic gate, the output of the non-linear feedback sub-system being operationally connected to the second input of the main XOR logic gate, the output of the main XOR logic gate being operationally connected to the input of the first stage of the non-linear feedback register.

[0007] Further in accordance with a preferred embodiment of the present invention the non-linear feedback sub-system is operative to receive input from a stage m and a stage 2m+1 of the stages, the non-linear feedback sub-system includes a second AND logic gate and a first XOR logic gate, the second AND logic gate having a first input operationally connected to the output of the stage m, a second input operationally connected to the output of the stage 2m+1, and an output, the first XOR logic gate of the feedback sub-sub-system has a first input operationally connected to the output of the first AND logic gate, and a second input operationally connected to the output of the second AND logic gate, and the output of the non-linear feedback sub-system is based, at least in part, on a value of the output of the first XOR logic gate of the non-linear feedback sub-system.

[0008] Still further in accordance with a preferred embodiment of the present invention the non-linear feedback sub-system is operative to receive input from a stage k and a stage 2k+1 of the stages, the non-linear feedback sub-system includes a third AND logic gate and a second XOR logic gate, the third AND logic gate having a first input operationally connected to the output of the stage k, a second input operationally connected to the output of the stage 2k+1, and an output, the second XOR logic gate of the feedback sub-sub-system has a first input operationally connected to the output of the first XOR logic gate, and a second input operationally connected to the output of the third AND logic gate, and the output of the non-linear feedback sub-system is based, at least in part, on a value of the output of the second XOR logic gate of the non-linear feedback sub-system.

[0009] Additionally in accordance with a preferred embodiment of the present invention the bit generator is operative such that the output of the bit generator is biased a state of the stages of the feedback shift-register.

[0010] Moreover in accordance with a preferred embodiment of the present invention, the system includes a scheduler having an input operationally connected to the main XOR logic gate or the feedback shift-register, the scheduler being operative to schedule a plurality of wait-states data received by the input of the scheduler.

[0011] There is also provided in accordance with still another preferred embodiment of the present invention a wait-state system to schedule a plurality of wait-states, including a feedback shift-register having a plurality of serially connected stages including a first stage, the stages being operative to store a plurality of bits such that each of the stages is operative to store one of the bits, and a non-linear feedback sub-system, at least one of the stages having an output operationally connected to the non-linear feedback sub-system, the non-linear feedback sub-system being operative to receive input from at least one of the stages, the non-linear feedback sub-system being operative such that an output of the non-linear feedback sub-system is a non-linear function of the input of the non-linear feedback sub-system, the output of the non-linear feedback sub-system being operationally connected to the first stage, a clock operationally connected to the feedback shift-register, the clock being operative to control the movement of the bits along the stages, and a scheduler having an input operationally connected to the feedback shift-register, the scheduler being operative to schedule a plurality of wait-states data received by the input of the scheduler.

[0012] There is also provided in accordance with still another preferred embodiment of the present invention a method, including providing a feedback shift-register having L serially connected stages including a first stage and a final stage, the stages being denoted 0 to L-1 from the first stage to the final stage respectively, the stages being operative to store a plurality of bits such that each of the stages is operative to store one of the bits, and performing the following a plurality of times performing an AND logic gate operation with the output of a stage n and a stage 2n+1 of the stages as input, generating a random/pseudo-random bit, performing an XOR logic gate operation with the bit and a result of the AND logic gate operation as input, shifting the bits along the stages, and inserting a result of the XOR logic gate operation into the first stage.

[0013] There is also provided in accordance with still another preferred embodiment of the present invention a method including providing a feedback shift-register having a plurality of serially connected stages including a first stage and a final stage, the stages being operative to store a plurality of bits such that each of the stages is operative to store one of the bits, performing the following a plurality of times performing a non-linear function on the output of at least one of the stages, shifting the bits along the stages, inserting a new value in to the first stage, the new value being based on the result of the non-linear function, and scheduling a wait-state based on an output of the feedback shift-register.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a block diagram view of a secure device constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 2 is a block diagram view of a random wait-state scheduler for use with the secure device of Fig. 1;

Fig. 3 is a first preferred embodiment of the random wait-state scheduler of Fig. 2;

Figs. 4a and 4b are partly pictorial, partly block diagram views illustrating operation of the random wait-state scheduler of Fig. 3;

Fig. 5 is a second preferred embodiment of the random wait-state scheduler of Fig. 2;

Figs. 6a and 6b are partly pictorial, partly block diagram views illustrating operation of the random wait-state scheduler of Fig. 5;

Fig. 7 is a third preferred embodiment of the random wait-state scheduler of Fig. 2;

Fig. 8 is a partly pictorial, partly block diagram view illustrating operation of the random wait-state scheduler of Fig. 7; and

Fig. 9 is a partly pictorial, partly block diagram view of a random bit generator for use with the secure device of Fig. 1.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

[0015] Reference is now made to Fig. 1, which is a block diagram view of a secure device 10 constructed and operative in accordance with a preferred embodiment of the present invention. The secure device 10 preferably includes a random wait-state scheduler 12 to schedule a plurality of wait-states.

[0016] The random wait-state scheduler 12 preferably includes a random bit generator 14, a feedback shift-register 16, a main exclusive-OR (XOR) logic gate 18, a clock 20 and a scheduler 22.

[0017] Reference is now made to Fig. 2, which is a block diagram view of the random wait-state scheduler 12 for use with the secure device 10 of Fig. 1.

[0018] The feedback shift-register 16 preferably includes L serially connected stages 24, typically implemented as flip-flops, including a first stage 26 and a final stage 28. The stages 24 are typically denoted 0 to L-1 from the first stage 26 to the final stage 28, respectively. In other words the stages are numbered 0, 1, ... L-2, L-1. The stages 24 are preferably operative to store a plurality of bits such that each of the stages 24 is operative to store one of the bits. Each of the stages 24 typically includes an input 30 and an output 32 for serially connecting the stages 24. The content of the stages 24 at a time t is called the state at the time t.

[0019] The feedback shift-register 16 preferably includes a non-linear feedback sub-system 34 which is operationally connected to the output 32 of the stages 24, as appropriate. Generally, the non-linear feedback sub-system 34 only needs to be operationally connected to the output 32 of the stages 24 needed for the non-linear feedback sub-system 34, as will be explained in more detail with reference to Figs. 3, 5 and 7. Therefore, the non-linear feedback sub-system 34 is typically operative to receive input from at least some of the stages 24. The non-linear feedback sub-system 34 preferably has an output 36 which is operationally connected to the first stage 26 via the main exclusive-OR logic gate 18 as will be described in more detail below.

[0020] The non-linear feedback sub-system 34 is preferably operative to perform a Boolean feedback function F such that the output of the non-linear feedback sub-system 34 is a non-linear function of the input of the non-linear feedback sub-system 34. The feedback function F is described in more detail below.

[0021] The clock 20 is preferably operationally connected to the non-linear feedback shift-register 16. The clock 20 is generally operative to control the movement of the bits along the stages 24 and through the non-linear feedback sub-system 34.

[0022] The random bit generator 14 typically has an output 38. The random bit generator 14 is preferably operative to generate a plurality of random/pseudo-random bits for outputting via the output 38 of the random bit generator 14. The random bit generator 14 is described in more detail with reference to Fig. 9.

[0023] The main exclusive-OR logic gate 18 has preferably an input 40, an input 42 and an output 44.

[0024] The output 38 of the random bit generator 14 is preferably operationally connected to the input 42 of the main exclusive-OR logic gate 18. The output 36 of the non-linear feedback sub-system 34is preferably operationally connected to the input 40 of the main exclusive-OR logic gate 18. The output 44 of the main exclusive-OR logic gate 18 is preferably operationally connected to an input 46 of the scheduler 22 and to the input 30 of the first stage 26 of the feedback shift-register 16.

[0025] The scheduler 22 is preferably operative to schedule a plurality of wait-states according to data received by the input 46 of the scheduler 22. For example, when the data at the input 46 is a "1" then a wait-state is scheduled for a certain time period, typically one clock cycle.

[0026] In accordance with an alternative preferred embodiment of the present invention, the input 46 of the scheduler 22 may be operationally connected to any of the outputs 32 of the stages 24 or to the output 36 of the non-linear feedback sub-system 34.

[0027] Operation of the random wait-state scheduler 12 is briefly described below.

[0028] During each unit of time (clock cycle) the following operations are preferably performed. The non-linear feedback sub-system 34 performs a non-linear function F on the output of one or more of the stages 24, described in more detail with reference to Figs. 3-9. The random bit generator 14 generates a random/pseudo-random bit. The main exclusive-OR logic gate 18 performs an exclusive-OR (XOR) logic gate operation with the bit and a result of the function F of the non-linear feedback sub-system 34. The clock 20 causes the bits to shift along the stages 24, so that for each stage 24 from 0 to L-2, the content S_i of stage i is moved to stage i + 1. A new value is inserted into the first stage 26 by inserting a result of the XOR logic gate operation (which is based on a result of the non-linear function F) into the first stage 26. The scheduler 22 schedules a wait-state based on the output of the main exclusive-OR logic gate 18 (which is based on the output of the non-linear feedback sub-system 34 and the random bit generator 14).

[0029] The random wait-state scheduler 12 is typically implemented in hardware using commercially available chips and/or logic gates or custom made chips and circuitry. However, it will be appreciated by those ordinarily skilled in the art that the random wait-state scheduler 12 can easily be implemented in software or partially in software and partially in hardware.

[0030] Reference is now made to Fig. 3, which is a first preferred embodiment of the random wait-state scheduler 12 of Fig. 2.

[0031] In accordance with the first preferred embodiment of the random wait-state scheduler 12, the feedback function F of Fig. 2 typically has the form:

$$F(S_0, S_1, \ldots S_{L-1}) = S_n \,\&\, S_{(2n+1)},$$

where 2n+1 is less than L, the number of stages 24 in the feedback shift-register 16. In other words, the output of the non-linear feedback function F is a result of performing an AND logic gate operation on the value of the output of the n^{th} stage and the value of the output of the $(2n+1)^{th}$ stage.

[0032] Therefore, the non-linear feedback sub-system 34 is preferably operative to receive input from the n^{th} stage and the $(2n+1)^{th}$ stage of the stages 24. In the example of Fig. 3, n is equal to 4 so the non-linear feedback sub-system 34 is operationally connected to the output 32 of stage 4 and the output 32 of stage 9.

[0033] The non-linear feedback sub-system 34 preferably includes an AND logic gate 48. The AND logic gate 48 typically has: an input 50 operationally connected to the output 32 of the n^{th} stage; an input 52 operationally connected to the output 32 of the $(2n+1)^{th}$ stage; and an output 54. The output 54 of the AND logic gate 48 is generally operationally connected to the input 40 of the main exclusive-OR logic gate 18. Therefore, the output of the non-linear feedback sub-system 34 is preferably based on the value of the output of the AND logic gate 48.

[0034] Reference is now made to Fig. 4a, which is a partly pictorial, partly block diagram view illustrating operation of the random wait-state scheduler 12 of Fig. 3. Figs. 4a shows the state of the stages 24 of the feedback shift-register 16 of Fig. 3 and how the feedback function, F, is calculated over a plurality of times, from time t to time t+5.

[0035] The random bit generator 14 (Fig. 3) is typically biased so that a plurality of random/pseudo-random bits 56, outputted via the output 38 (Fig. 3) of the random bit generator 14, has a very high probability of yielding the value "0". The biasing of the random bit generator 14 is discussed in more detail with reference to Fig. 9. Therefore, at some point in time, the stages 24 are typically all empty. In other words, S_i is equal to "0" for all i. All the stages 24 being empty is also known as the state of the feedback shift-register 16 being empty.

[0036] If the random/pseudo-random bits 56 produced by the random bit generator 14 include two bits equal to "1" separated by n stages, the feedback function F returns a result 58 equal to "1" after another n clock cycles. Fig. 4a shows that at time t, the state of stage 4 and stage 9 are both equal to "1". Therefore, performing an AND logic gate operation on the output of stage 4 and stage 9 gives "1" (the result 58). Assuming, the random/pseudo-random bit 56 is equal to "0", a result 60 of XORing "1" and "0" gives "1", which is now the new input into the first stage 26. In this way, a periodic sequence 62 of "1"s separated by n stages is set up, as shown at time t+5. The "1"s are typically used to schedule wait-states by the scheduler 22 of Fig. 3.

[0037] Reference is now made to Fig. 4b, which is a partly pictorial, partly block diagram view illustrating operation of the random wait-state scheduler 12 of Fig. 3. Fig. 4b shows the state of the stages 24 of the feedback shift-register 16 of Fig. 3 and how the feedback function, F, is calculated over a plurality of times, from time t+5 to time t+21.

[0038] At time t+5 the state of stage 4 and stage 9 are both equal to "1". In such a case, the result 58 of the feedback function is equal to "1".

[0039] If the random/pseudo-random bit 56 is equal to "1", which is a rare occurrence, then the result 60 of XORing the result 58 with the random/pseudo-random bit 56 is equal to "0". Therefore, the periodic sequence 62 is broken and the state of the feedback shift-register 16 (Fig. 2) will be empty at time t+21.

[0040] Therefore, the feedback shift-register 16 typically results in a plurality of random/pseudo-random bursts of the periodic sequences 62. Each periodic sequence 62 has "1"s spaced by n clock cycles apart. The scheduler 22 preferably translates the "1"s into wait-states. The periodic sequences 62 generally commence and terminate randomly/pseudo-randomly resulting in a high-variance for the wait-states.

[0041] The random wait-state scheduler 12 of Figs 3, 4a and 4b, generally provides the initialization and termination of a regular periodic sequence (the sequence 62) as a rare event. The random wait-state scheduler 12 may be enhanced by increasing the probability of "1"s in the random/pseudo-random bits 56 when the state is empty by suitably biasing the random bit generator 14, as described with reference to Fig. 9. Additionally, the random wait-state scheduler 12 may be enhanced by using a more complex feedback function F, as described with reference to the second and third preferred embodiments, described with reference to Figs. 5-7.

[0042] Reference is now made to Fig. 5, which is a second preferred embodiment of the random wait-state scheduler 12 of Fig. 2.

[0043] The second preferred embodiment of the random wait-state scheduler 12 is substantially the same as the first preferred embodiment of the random wait-state scheduler 12 described with reference to Fig. 3 except for the following differences described below.

[0044] In accordance with the second preferred embodiment of the random wait-state scheduler 12, the feedback function F of Fig. 2 typically has the form:

$$F(S_0, S_1,....S_{L-1}) = [S_n \,\&\, S_{(2n+1)}] \text{ XOR } [S_m \,\&\, S_{(2m+1)}],$$

where 2n+1 is less than L, 2m+1 is less than L, and m is not equal to n.

[0045] In other words, the output of the non-linear feedback function F is typically a result of performing: a first AND logic gate operation on the value of the output of the n^{th} stage and the value of the output of the $(2n+1)^{th}$ stage; a second AND logic gate operation on the value of the output of the m^{th} stage and the value of the output of the $(2m+1)^{th}$ stage; XORing the result of the first AND logic gate operation with the result of the second AND logic gate operation.

[0046] Therefore, the non-linear feedback sub-system 34 is preferably operative to receive input from the n^{th} stage, the $(2n+1)^{th}$ stage, the m^{th} stage, the $(2m+1)^{th}$ stage, of the stages 24. In the example of Fig. 5, n is equal to 4 and m is equal to 6, so the non-linear feedback sub-system 34 is operationally connected to the output 32 of stage 4, the output 32 of stage 6, the output 32 of stage 9 and the output 32 of stage 13.

[0047] In addition to the AND logic gate 48 described above with reference to Fig. 3, the non-linear feedback sub-system 34 preferably includes an AND logic gate 64 and an XOR logic gate 66.

[0048] The AND logic gate 64 preferably includes: an input 68 operationally connected to the output 32 of the m^{th} stage; an input 70 operationally connected to the output of the $(2m+1)^{th}$ stage; and an output 72.

[0049] The XOR logic gate 66 generally includes: an input 74 operationally connected to the output 72 of the AND logic gate 64; an input 76 operationally connected to the output 54 of the AND logic gate 48; and an output 78 operationally connected to the input 40 of the main exclusive-OR logic gate 18.

[0050] Therefore, the output of the non-linear feedback sub-system 34 is preferably based on a value of the output of the XOR logic gate 66.

[0051] Reference is now made to Figs. 6a and 6b, which are partly pictorial, partly block diagram views illustrating operation of the random wait-state scheduler 12 of Fig. 5. Figs. 6a and 6b show the state of the stages 24 of the feedback shift-register 16 of Fig. 5 and how the feedback function, F, is calculated over a plurality of times, from time t to time t+20.

[0052] Fig. 6a shows at time t: a periodic sequence 80 of "1"s each separated by n stages; and a periodic sequence 82 of "1"s each separated by m stages.

[0053] Depending on the choice of m and n and the separation between the periodic sequence 80 and the periodic sequence 82, the periodic sequences 80, 82 may act like separate periodic sequences which terminate in a similar manner to the periodic sequence 62 of Fig. 4b and/or the periodic sequences 80,82 may collide as will be described below.

[0054] The feedback function from the state at time t+2 is typically calculated as follows. Both the AND logic gates operations based on the state at time t+2 yield a result 84 of "1". Performing an XOR logic gate operation on the results 84, yields a result 86 of "0". Performing an XOR logic gate operation on the result 84 with the random bit 56, yields a value 88 equal to "0".

[0055] At time t+3 for the periodic sequences to continue, it is necessary for the value of the first stage 26 to be "1" and not "0". The value "1" in the first stage 26 would be part of both the n periodic sequence 80 and the m periodic sequence 82.

[0056] However, due to a collision of the periodic sequences 80 and 82 when calculating the feedback function from the state at time t+2, calculated above, the value 88 of the first stage 26 is "0" at time t+3, thereby breaking both the periodic sequence 80 and the periodic sequence 82. The broken periodic sequences 80, 82 slowly work themselves out of the stages 24 until the state of the feedback shift-register 16 (Fig. 3) is empty at time t+20 (Fig. 6b).

[0057] Adding the monomial S_m & $S_{(2m+1)}$ to the feedback function, F, makes the pattern of the output of the main exclusive-OR logic gate 18 (Fig. 5) more complex. By adding a third suitably chosen monomial preferably adds the possibility of a third periodic sequence being created from two other sequences, as will be described with reference to Figs. 7 and 8 below. The possibility of creating a third sequence based on the remains of two other sequences further adds "chaos" to the output the random wait-state scheduler 12.

[0058] Reference is now made to Fig. 7, which is a third preferred embodiment of the random wait-state scheduler 12 of Fig. 2.

[0059] The third preferred embodiment of the random wait-state scheduler 12 is substantially the same as the second preferred embodiment of the random wait-state scheduler 12 described with reference to Fig. 3 except for the following differences described below.

[0060] In accordance with the third preferred embodiment of the random wait-state scheduler 12, the feedback function F, of Fig. 2, is a sum (which is an XOR) of several monomials, so that F typically has the form:

$$F(S_0, S_1, \ldots S_{L-1}) =$$

$$[S_k \,\&\, S_{(2k+1)}] \text{ XOR } [S_m \,\&\, S_{(2m+1)}] \text{ XOR } [S_n \,\&\, S_{(2n+1)}],$$

where 2k+1 is less than L, 2m+1 is less than L, 2n+1 is less than L, and k, m and n are different.

[0061] In other words, the output of the non-linear feedback function F is typically a result of performing: a first AND logic gate operation on the value of the output of the k^{th} stage and the value of the output of the $(2k+1)^{th}$ stage; a second AND logic gate operation on the value of the output of the m^{th} stage and the value of the output of the $(2m+1)^{th}$ stage; a third AND logic gate operation on the value of the output of the n^{th} stage and the value of the output of the $(2n+1)^{th}$ stage; and XORing the results of the AND logic gate operations together.

[0062] Therefore, the non-linear feedback sub-system 34 is typically operative to receive input from the k^{th} stage, the $(2k+1)^{th}$ stage, the m^{th} stage, the $(2m+1)^{th}$ stage, the n^{th} stage, the $(2n+1)^{th}$ stage, of the stages 24. In the example of Fig. 7, k is equal to 8, n is equal to 4 and m is equal to 6, so the non-linear feedback sub-system 34 is operationally connected to the output 32 of stages 4, 6, 7, 8, 9, 13, and 17.

[0063] With suitably chosen k, m, n and a suitably chosen probability of "1"s appearing in the input bit stream, unpredictable bursts of random delays will be produced. To make the bursts closer to each other, the probability of "1"s appearing in the input bit stream is increased, for example, but not limited to, in a situation when the state of the feedback shift-register 16 is empty. When the probability of "1"s is increased, for example, by suitably biasing the random bit generator 14, the output 38 of the random bit generator 14 may be directly connected to the input 30 of the first stage 26, bypassing the main exclusive-OR logic gate 18, so that the scheduler 22 does not schedule wait-states based on the output of the random bit generator 14.

[0064] In the above feedback function, a k periodic sequence of "1"s and/or an m periodic sequence of "1"s and/or an n periodic sequence of "1"s may be set-up in the feedback shift-register 16. The periodic sequences may exist separately or at the same time. Depending on the choice of k, m and n and the spacing between the periodic sequences, an individual periodic sequence may terminate due to a "1" produced by the random bit generator 14 at a certain time or two or more of the periodic sequences may terminate due to a collision, as explained above with reference to Figs. 6a and 6b or two sequences may create a third sequence as described in more detail with reference to Fig. 8.

[0065] In addition to the AND logic gate 48, the AND logic gate 64, and the XOR logic gate 66 described above with reference to Fig. 5, the non-linear feedback sub-system 34 preferably includes an AND logic gate 90 and an XOR logic gate 92.

[0066] The AND logic gate 90 typically has: an input 94 operationally connected to the output of the k^{th} stage; an input 96 operationally connected to the output of the $(2k+1)^{th}$ stage; and an output 98.

[0067] The XOR logic gate 92 generally has: an input 100 operationally connected to the output 78 of the XOR logic gate 66; an input 102 operationally connected to the output 98 of the AND logic gate 90; and an output 104 operationally connected to the input 40 of the main exclusive-OR logic gate 18.

[0068] Therefore, the output of the non-linear feedback sub-system 34 is preferably based on a value of the output of the XOR logic gate 92 of the non-linear feedback sub-system 34.

[0069] It will be appreciated by those ordinarily skilled in the art that 1, 2 or 3 monomials in the feedback function F is by way of example only, and that any suitable number of monomials may be used. One monomial generally results in the creation and termination of a single periodic sequence. A second suitably chosen monomial additionally results in the periodic sequences colliding and thereby terminating. A third suitably chosen monomial additionally results in two periodic sequences creating a third sequence.

[0070] It will be appreciated by those ordinarily skilled in the art that any suitable number of stages may be used in the feedback shift-register 16.

[0071] Reference is now made to Fig. 8, which is a partly pictorial, partly block diagram view illustrating operation of the random wait-state scheduler 12 of Fig. 7.

[0072] A time t, the state of the random wait-state scheduler 12 (Fig. 7) includes: a periodic sequence 116 having a spacing of n (4 in the example of Fig. 8); and a periodic sequence 118 having a spacing of m (6 in the example if Fig. 8).

[0073] At time t, the periodic sequence 116 and the periodic sequence 118 collide. The collision of the periodic sequences 116, 118 interrupts the sequences and over time it appears that the sequences will terminate.

[0074] However, at time t+4, a value 120 from the periodic sequence 116 and a value 122 from the periodic sequence 118 coincide with the input for the feedback function for the k^{th} and $(2k+1)^{th}$ stage (stage 8 and 17 in the example of Fig. 8), respectively. Therefore, an output 124 of the feedback function, F, is equal to "1" and the input to the first stage 26 is equal to "1". Therefore, a new periodic sequence 126 having a spacing of k is established.

[0075] In the above way, the terminating periodic sequences 116, 118 develop into the new periodic sequence 126.

[0076] Reference is now made to Fig. 9, which is a partly pictorial, partly block diagram view of the random bit generator 14 for use with the secure device 10 of Fig. 1.

[0077] The random bit generator 14 preferably includes an unbiased random number generator 114 for generating a plurality of random/pseudo-random bits 106 (zeros or ones) with an equal probability of zeros and ones, as is known to those ordinarily skilled in the art.

[0078] The random bit generator 14 also typically includes an output weighting module 108 operationally connected to the unbiased random number generator 114. The output weighting module 108 is generally operative to receive the random/pseudo-random bits 106 and group the random/pseudo-random bits 106 into groups of P bits. If all the bits in a group are "1"s, the output weighting module 108 preferably produces a result 110 equal to "1". If the group includes even one "0", then the output weighting module 108 preferably produces a result 112 equal to "0".

[0079] The results 110, 112 are then generally outputted via the output 38 of the random bit generator 14.

[0080] The probability of the random bit generator 14 outputting a "1" is equal to 2^{-P}.

[0081] Therefore, the output of the random bit generator 14 may be biased by increasing or decreasing P as appropriate.

[0082] The value of P may take any suitable value, for example, but not limited to, between 5 and 15.

[0083] Typically, the output of the random bit generator 14 is biased according to the state of the stages 24 (Fig. 2) of the feedback shift-register 16 so that when the state is empty, or almost empty, the value of P is decreased, and when the state is populated the value of P is increased to the previous value of P. The state is typically defined as "almost empty" when all the values of the stages 24 are equal to zero up to and including the greater of: the k^{th}, m^{th} or n^{th} stage. It will be appreciated by those ordinarily skilled in the art that the definition of "almost empty" may be adjusted if the function F includes more than 3 monomials.

[0084] The following is a non-limiting example of the random wait-state scheduler 12 of Fig. 2. The feedback shift-register 16 includes 30 stages. The non-linear feedback sub-system 34 is configured such that k=14, m=9, n= 11. P of the random bit generator 14 is set to 7 when the state is empty and set to 13 when the state is populated.

[0085] It will be appreciated by those ordinarily skilled in the art that the number of stages and the values of k, m, n and P may be any suitable values. Additionally more monomials may be added to the feedback function F.

[0086] The random wait-state scheduler 12 is typically implemented in hardware using commercially available chips and/or logic gates or custom made chips and circuitry. However, it will be appreciated by those ordinarily skilled in the art that the random wait-state scheduler 12 can easily be implemented in software or partially in software and partially in hardware.

[0087] It will be appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable sub-combination. It will also be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only by the claims which follow.

Claims

1. A system, comprising:

a feedback shift-register having:

L serially connected stages including a first stage and a final stage, the stages being denoted 0 to L-1 from the first stage to the final stage respectively, the stages being operative to store a plurality of bits such that each of the stages is operative to store one of the bits; and

a clock operationally connected to the feedback shift-register, the clock being operative to control the

movement of the bits along the stages;
a non-linear feedback sub-system, at least some of the stages having an output operationally connected to the non-linear feedback sub-system, **characterised by**
the non-linear feedback sub-system being operative to receive input from a stage n, a stage 2n+1, a stage m, a stage 2m+1, a stage k and a stage 2k+1 of the stages, n, m and k being different, the non-linear feedback sub-system including : (i) a first AND logic gate, the first AND logic gate having: a first input operationally connected to the output of the stage n; a second input operationally connected to the output of the stage 2n+1; and an output; (ii) a second AND logic gate and a first XOR logic gate, the second AND logic gate having: a first input operationally connected to the output of the stage m; a second input operationally connected to the output of the stage 2m+1; and an output, the first XOR logic gate having: a first input operationally connected to the output of the first AND logic gate; and a second input operationally connected to the output of the second AND logic gate; and (iii) a third AND logic gate and a second XOR logic gate, the third AND logic gate having: a first input operationally connected to the output of the stage k; a second input operationally connected to the output of the stage 2k+1; and an output, the second XOR logic gate having: a first input operationally connected to the output of the first XOR logic gate; a second input operationally connected to the output of the third AND logic gate; and an output, wherein the non-linear feedback sub-system has an output based, at least in part, on a value of the output of the second XOR logic gate; and

the feedback shift-register further having:

a bit generator having an output, the bit generator being operative to generate a plurality of random/pseudo-random bits for outputting via the output of the bit generator; and
a main XOR logic gate having a first and second input and an output, the output of the bit generator being operationally connected to the first input of the main XOR logic gate, the output of the non-linear feedback subsystem being operationally connected to the second input of the main XOR logic gate, the output of the main XOR logic gate being operationally connected to the input of the first stage of the feedback shift-register.

2. The system according to claim 1, wherein the bit generator is operative such that the output of the bit generator is biased according to a state of the stages of the feedback shift-register.

3. The system according to any of claims 1-2, further comprising a scheduler having an input operationally connected to the main XOR logic gate or the feedback shift-register, the scheduler being operative to schedule a plurality of wait-states according to data received by the input of the scheduler.

4. A method, comprising:

providing a feedback shift-register having L serially connected stages including a first stage and a final stage, the stages being denoted 0 to L-1 from the first stage to the final stage respectively, the stages being operative to store a plurality of bits such that each of the stages is operative to store one of the bits; and
performing the following a plurality of times:

performing an AND logic gate operation with the output of a stage n and a stage 2n+1 of the stages as input yielding a first result;
performing an AND logic gate operation with the output of a stage k and a stage 2k+1 of the stages of input yielding a second result;
performing an AND logic gate operation with the output of a stage m and a stage 2m+1 of the stages as input yielding a third result, n, m and k being different;
performing an XOR logic gate operation using the first result, the second result and the third result as input yielding a fourth result;
generating a random/pseudo-random bit;
performing an XOR logic gate operation with the bit and the fourth result as input yielding a fifth result shifting the bits along the stages; and
inserting the fifth result into the first stage.

5. The method according to claim 4, further comprising biasing the generation of the random/pseudo random bit according to a state of the stages of the feedback shift-register.

6. The method according to claim 4 or claim 5, further comprising scheduling a plurality of wait-states according to the fifth result.

Patentansprüche

1. System, umfassend:

ein rückgekoppeltes Schieberegister mit:

L in Reihe geschaltete Stufen, die eine erste Stufe und eine letzte Stufe umfassen, wobei die Stufen von der ersten Stufe bis zur letzten Stufe jeweils von 0 bis L-1 bezeichnet sind, wobei die Stufen betriebsbereit sind, um eine Vielzahl von Bits zu speichern, so dass jede der Stufen betriebsbereit ist, um eines der Bits zu speichern; und
einen Taktgeber, der betriebsmäßig an das rückgekoppelte Schieberegister angeschlossen ist, wobei der Taktgeber betriebsbereit ist, um die Bewegung der Bits an den Stufen entlang zu steuern;
ein nicht lineares rückgekoppeltes Teilsystem, wobei mindestens einige der Stufen einen Ausgang aufweisen, der betriebsmäßig an das nicht lineale rückgekoppelte Teilsystem angeschlossen ist,

dadurch gekennzeichnet, dass
das nicht lineare rückgekoppelte Teilsystem betriebsbereit ist, um eine Eingabe von einer Stufe n, einer Stufe 2n+1, einer Stufe m, einer Stufe 2m+1, einer Stufe k und einer Stufe 2k+1 der Stufen zu empfangen, wobei n, m und k unterschiedlich sind, wobei das nicht lineare rückgekoppelte Teilsystem Folgendes umfasst: (i) ein erstes logisches UND-Gatter, wobei das erste logische UND-Gatter Folgendes aufweist: einen ersten Eingang, der betriebsmäßig an den Ausgang der Stufe n angeschlossen ist; einen zweiten Eingang, der betriebsmäßig an den Ausgang der Stufe 2n+1 angeschlossen ist; und einen Ausgang; (ii) ein zweites logisches UND-Gatter und ein erstes logisches Exklusiv-ODER-Gatter, wobei das zweite logische UND-Gatter Folgendes aufweist: einen ersten Eingang, der betriebsmäßig an den Ausgang der Stufe m angeschlossen ist; einen zweiten Eingang, der betriebsmäßig an den Ausgang der Stufe 2m+1 angeschlossen ist; und einen Ausgang, wobei das erste logische Exklusiv-ODER-Gatter Folgendes umfasst: einen ersten Eingang, der betriebsmäßig an den Ausgang des ersten logischen UND-Gatters angeschlossen ist; und einen zweiten Eingang, der betriebsmäßig an den Ausgang des zweiten logischen UND-Gatters angeschlossen ist; und (iii) ein drittes logisches UND-Gatter und ein zweites logisches Exklusiv-ODER-Gatter, wobei das dritte logische UND-Gatter Folgendes aufweist: einen ersten Eingang, der betriebsmäßig an den Ausgang der Stufe k angeschlossen ist; einen zweiten Eingang, der betriebsmäßig an den Ausgang der Stufe 2k+1 angeschlossen ist; und einen Ausgang, wobei das zweite logische Exklusiv-ODER-Gatter Folgendes aufweist: einen ersten Eingang, der betriebsmäßig an den Ausgang des ersten logischen Exklusiv-ODER-Gatters angeschlossen ist; einen zweiten Eingang, der betriebsmäßig an den Ausgang des dritten logischen UND-Gatters angeschlossen ist; und einen Ausgang, wobei das nicht lineare rückgekoppelte Teilsystem einen Ausgang aufweist, der mindestens teilweise auf einem Wert des Ausgangs des zweiten logischen Exklusiv-ODER-Gatters basiert, und
das rückgekoppelte Schieberegister ferner Folgendes aufweist:
einen Bitgenerator, der einen Ausgang aufweist, wobei der Bitgenerator betriebsbereit ist, um eine Vielzahl von Zufalls-/ Pseudozufallsbits zur Ausgabe über den Ausgang des Bitgenerators zu erzeugen; und
ein Haupt-Exklusiv-ODER-Gatter, das einen ersten und zweiten Eingang und einen Ausgang aufweist, wobei der Ausgang des Bitgenerators betriebsmäßig an den ersten Eingang des Haupt-Exklusiv-ODER-Gatters angeschlossen ist, wobei der Ausgang des nicht linearen rückgekoppelten Teilsystems betriebsmäßig an den zweiten Eingang des Haupt-Exklusiv-ODER-Gatters angeschlossen ist, wobei der Ausgang des Haupt-Exklusiv-ODER-Gatters betriebsmäßig an den Eingang der ersten Stufe des rückgekoppelten Schieberegisters angeschlossen ist.

2. System nach Anspruch 1, wobei der Bitgenerator derart betriebsbereit ist, dass der Ausgang des Bitgenerators je nach einem Zustand der Stufen des rückgekoppelten Schieberegisters voreingestellt ist.

3. System nach einem von Anspruch 1 und 2, ferner umfassend ein Steuerprogramm, das einen Eingang aufweist, der betriebsmäßig an das Haupt-Exklusiv-ODER-Gatter oder an das rückgekoppelte Schieberegister angeschlossen ist, wobei das Steuerprogramm betriebsbereit ist, um eine Vielzahl von Wartezuständen je nach den von dem Eingang des Steuerprogramms empfangenen Daten zu planen.

4. Verfahren, umfassend folgende Schritte:

Bereitstellen eines rückgekoppelten Schieberegisters mit L in Reihe geschalteten Stufen, die eine erste Stufe und eine letzte Stufe umfassen, wobei die Stufen von der ersten Stufe bis zur letzten Stufe jeweils von 0 bis L-1 bezeichnet sind, wobei die Stufen betriebsbereit sind, um eine Vielzahl von Bits zu speichern, so dass jede der Stufen betriebsbereit ist, um eines der Bits zu speichern; und
mehrmaliges Ausführen der folgenden Schritte:

Ausführen einer logischen UND-Gatteroperation mit der Ausgabe einer Stufe n und einer Stufe 2n+1 der Stufen als Eingabe, wodurch ein erstes Ergebnis hervorgebracht wird;
Ausführen einer logischen UND-Gatteroperation mit der Ausgabe einer Stufe k und einer Stufe 2k+1 der Stufen als Eingabe, wodurch ein zweites Ergebnis hervorgebracht wird;
Ausführen einer logischen UND-Gatteroperation mit der Ausgabe einer Stufe m und einer Stufe 2m+1 der Stufen als Eingabe, wodurch ein drittes Ergebnis hervorgebracht wird, wobei n, m und k unterschiedlich sind;
Ausführen einer logischen Exklusiv-ODER-Gatteroperation unter Verwendung des ersten Ergebnisses, des zweiten Ergebnisses und des dritten Ergebnisses als Eingabe, wodurch ein viertes Ergebnis hervorgebracht wird;
Erzeugen eines Zufalls-/ Pseudozufallsbits;
Ausführen einer logischen Exklusiv-ODER-Gatteroperation mit dem Bit und dem vierten Ergebnis als Eingabe, wodurch ein fünftes Ergebnis hervorgebracht wird;
Verschieben der Bits über die Stufen; und
Einfügen des fünften Ergebnisses in die erste Stufe.

5. Verfahren nach Anspruch 4, ferner umfassend das Voreinstellen der Erzeugung des Zufalls-/ Pseudozufallsbits je nach einem Zustand der Stufen des rückgekoppelten Schieberegisters.

6. Verfahren nach Anspruch 4 oder 5, ferner umfassend das Planen einer Vielzahl von Wartezuständen gemäß dem fünften Ergebnis.

Revendications

1. Système comprenant :

un registre à décalage à rétroaction ayant :

L étages connectés en série comprenant un premier étage et un dernier étage, les étages étant dénotés de 0 à L-1 respectivement du premier étage au dernier étage respectivement, les étages étant opérationnels pour stocker une pluralité de bits de sorte que chacun des étages soit opérationnel pour stocker l'un des bits ; et
une horloge connectée opérationnellement au registre à décalage à rétroaction, l'horloge étant opérationnelle pour contrôler le mouvement des bits le long des étages ;
un sous-système de rétroaction non linéaire, au moins certains des étages ayant une sortie connectée opérationnellement au sous-système de rétroaction non linéaire,

caractérisé par
le sous-système de rétroaction non linéaire étant opérationnel pour recevoir une entrée d'un étage n, d'un étage 2n+1, d'un étage m, d'un étage 2m+1, d'un étage k et d'un étage 2k+1 parmi les étages, n, m et k étant différents, le sous-système de rétroaction non linéaire comprenant : (i) une première grille logique AND, la première grille logique AND ayant : une première entrée connectée opérationnellement à la sortie de l'étage n ; une deuxième entrée connectée opérationnellement à la sortie de l'étage 2n+1 ; et une sortie ; (ii) une deuxième grille logique AND et une première grille logique XOR, la deuxième grille logique AND ayant : une première entrée connectée opérationnellement à la sortie de l'étage m ; une deuxième entrée connectée opérationnellement à la sortie de l'étage 2m+1 ; et une sortie ; la première grille logique XOR ayant : une première entrée connectée opérationnellement à la sortie de la première grille logique AND ; et une deuxième entrée connectée opérationnellement à la sortie de la deuxième grille logique AND ; et (iii) une troisième grille logique AND et une deuxième grille logique XOR, la troisième grille logique AND ayant : une première entrée connectée opérationnellement à la sortie de l'étage k ; une deuxième entrée connectée opérationnellement à la sortie de l'étage 2k+1 ; et une sortie ; la deuxième grille logique XOR ayant : une première entrée connectée opérationnellement à la sortie de la première grille logique XOR ; une deuxième entrée connectée opérationnellement à la sortie de la troisième grille logique AND ; et une

sortie, dans lequel le sous-système de rétroaction non linéaire a une sortie basée, au moins en partie, sur une valeur de la sortie de la deuxième grille logique XOR ; et
le registre à décalage à rétroaction ayant en outre :
un générateur de bits ayant une sortie, le générateur de bits étant opérationnel pour générer une pluralité de bits aléatoires/pseudo-aléatoires à délivrer par le biais de la sortie du générateur de bits ; et
une grille logique XOR principale ayant des première et deuxième entrées et une sortie, la sortie du générateur de bits étant connectée opérationnellement à la première entrée de la grille logique XOR principale, la sortie du sous-système de rétroaction non linéaire étant connectée opérationnellement à la deuxième entrée de la grille logique XOR principale, la sortie de la grille logique XOR principale étant connectée opérationnellement à l'entrée du premier étage du registre à décalage à rétroaction.

2. Système selon la revendication 1, dans lequel le générateur de bits est opérationnel de sorte que la sortie du générateur de bits soit contrainte en fonction d'un état des étages du registre à décalage à rétroaction.

3. Système selon l'une quelconque des revendications 1 et 2, comprenant en outre un planificateur ayant une entrée connectée opérationnellement à la grille logique XOR principale ou au registre à décalage à rétroaction, le planificateur étant opérationnel pour planifier une pluralité d'états d'attente en fonction des données reçues par l'entrée du planificateur.

4. Procédé comprenant les étapes consistant à :

fournir un registre à décalage à rétroaction ayant L étages connectés en série comprenant un premier étage et un dernier étage, les étages étant dénotés de 0 à L-1 respectivement du premier étage au dernier étage, les étages étant opérationnels pour stocker une pluralité de bits de sorte que chacun des étages soit opérationnel pour stocker l'un des bits ; et
effectuer ce qui suit une pluralité de fois :

effectuer une opération de grille logique AND avec la sortie d'un étage n et d'un étage 2n+1 des étages en tant qu'entrée donnant un premier résultat ;
effectuer une opération de grille logique AND avec la sortie d'un étage k et d'un étage 2k+1 des étages en tant qu'entrée donnant un deuxième résultat ;
effectuer une opération de grille logique AND avec la sortie d'un étage m et d'un étage 2m+1 des étages en tant qu'entrée donnant un troisième résultat, n, m et k étant différents ;
effectuer une opération de grille logique XOR en utilisant le premier résultat, le deuxième résultat et le troisième résultat en tant qu'entrée donnant un quatrième résultat ;
générer un bit aléatoire/pseudo-aléatoire ;
effectuer une opération de grille logique XOR avec le bit et le quatrième résultat en tant qu'entrée donnant un cinquième résultat ;
décaler les bits le long des étages ; et
insérer le cinquième résultat dans le premier étage.

5. Procédé selon la revendication 4, comprenant en outre l'étape consistant à contraindre la génération du bit aléatoire/pseudo-aléatoire en fonction d'un état des étages du registre à décalage à rétroaction.

6. Procédé selon la revendication 4 ou 5, comprenant en outre l'étape consistant à planifier une pluralité d'états d'attente en fonction du cinquième résultat.

FIG. 1

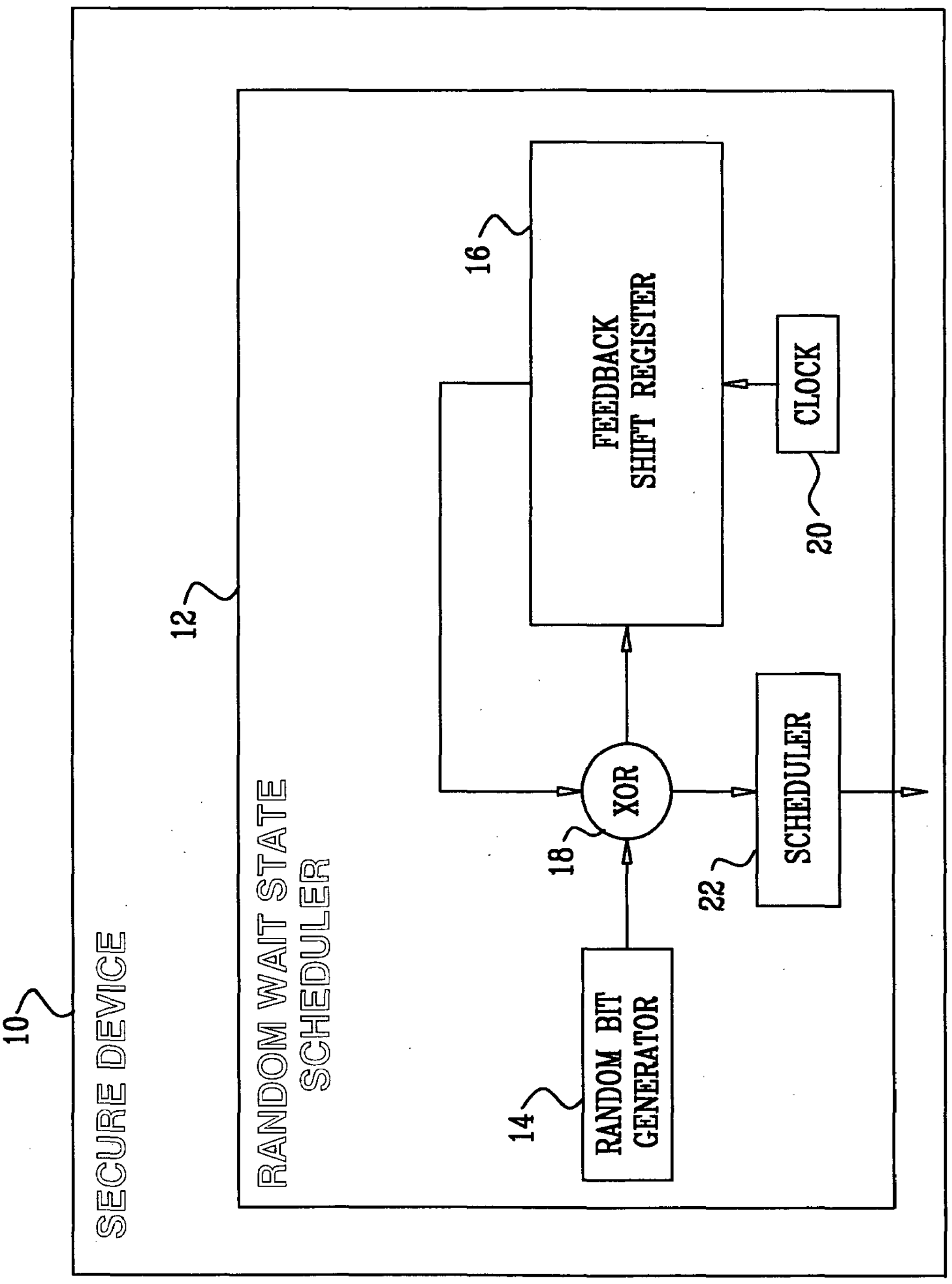

10
SECURE DEVICE
12
RANDOM WAIT STATE SCHEDULER
14
RANDOM BIT GENERATOR
16
FEEDBACK SHIFT REGISTER
18
XOR
20
CLOCK
22
SCHEDULER

FIG. 2

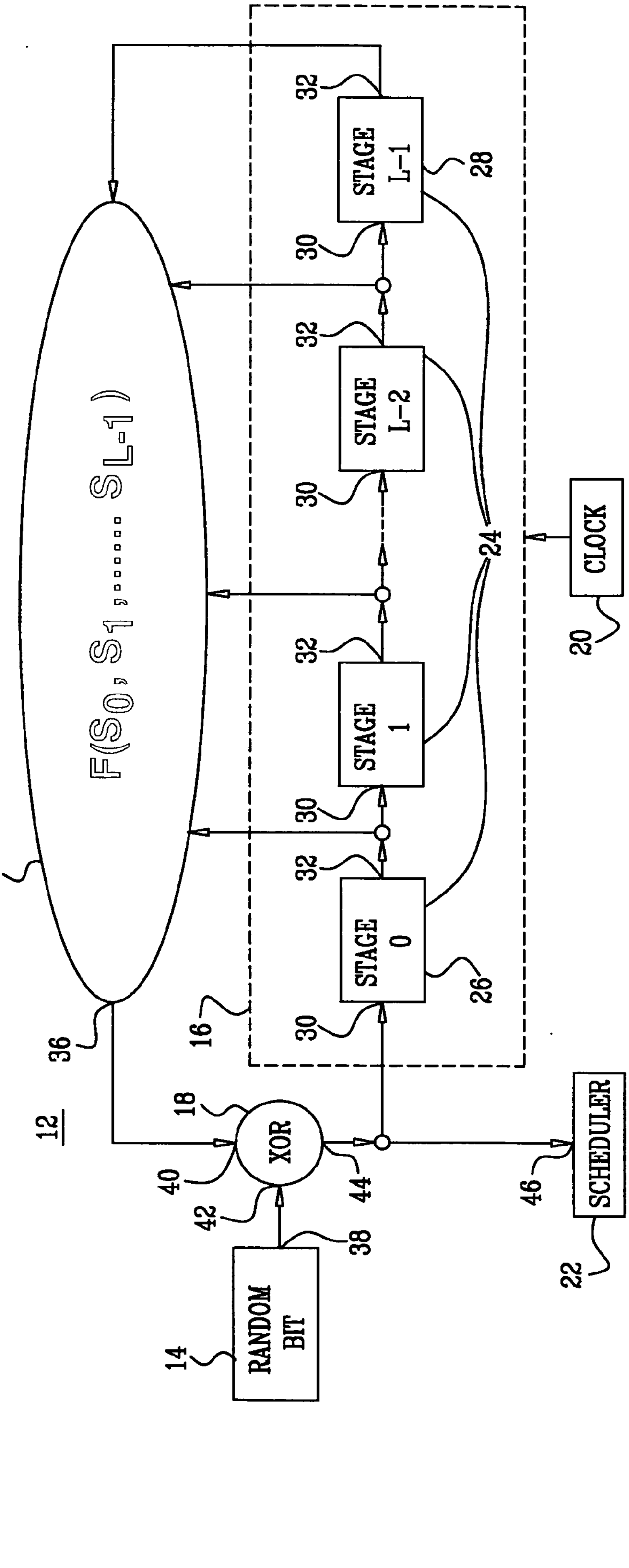

12
14
RANDOM BIT
38
42
40
XOR
18
44
46
SCHEDULER
22
36
16
30
STAGE 0
26
32
34
STAGE 1
24
CLOCK
20
STAGE L-2
STAGE L-1
28
F(S0, S1,...... SL-1)

FIG. 3

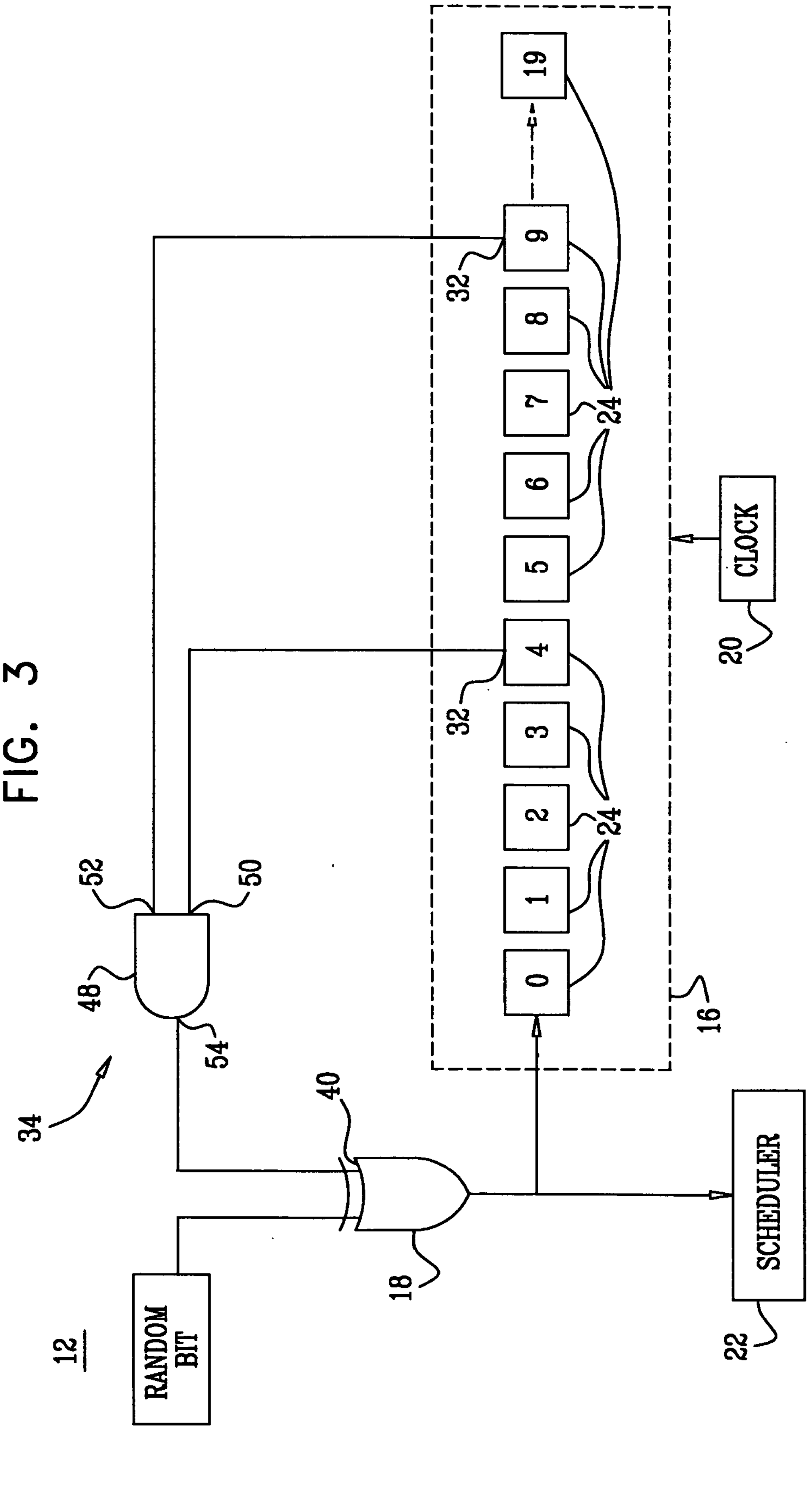
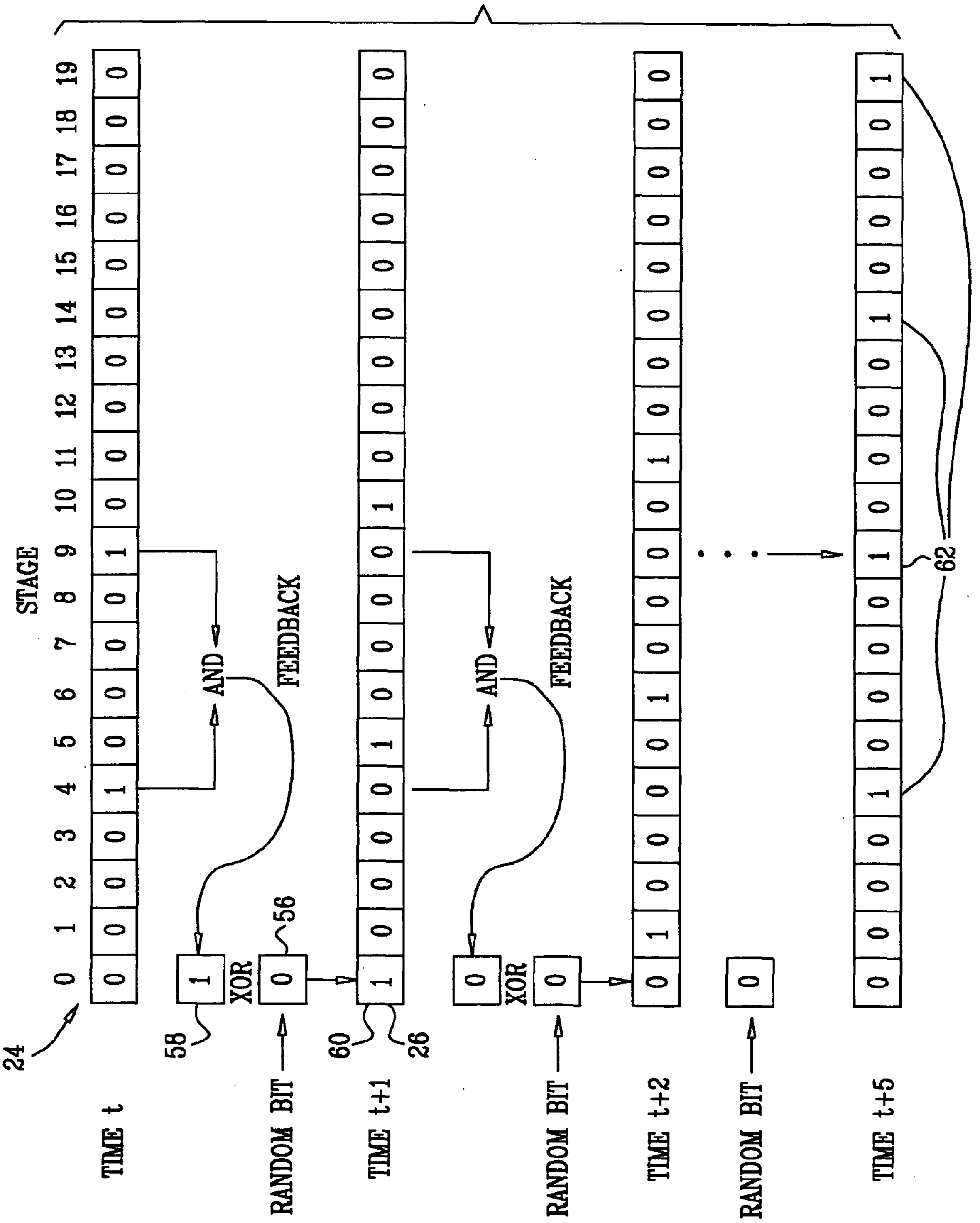
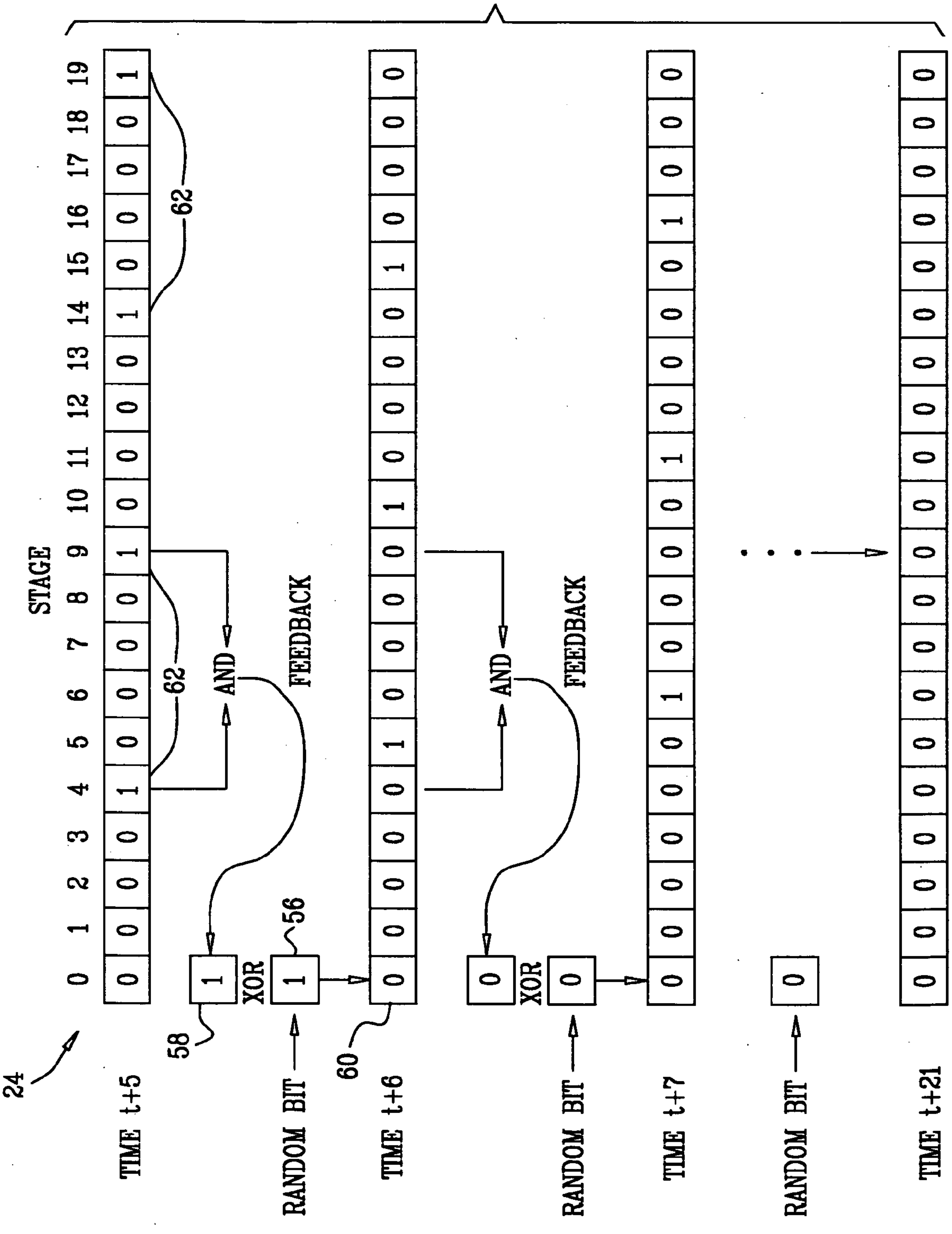

12
RANDOM BIT
18
40
34
48
52
50
54
0
1
2
3
4
5
6
7
8
9
19
24
24
32
32
16
CLOCK
20
SCHEDULER
22

FIG. 4A


STAGE
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
TIME t
0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0
AND
FEEDBACK
1
XOR
RANDOM BIT
0
TIME t+1
1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0
AND
FEEDBACK
0
XOR
RANDOM BIT
0
TIME t+2
0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0
RANDOM BIT
0
TIME t+5
0 0 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1
24
58
56
60
26
62



STAGE	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
TIME t+5	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1
TIME t+6	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0
TIME t+7	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0
TIME t+21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

FIG. 4B

FIG. 5

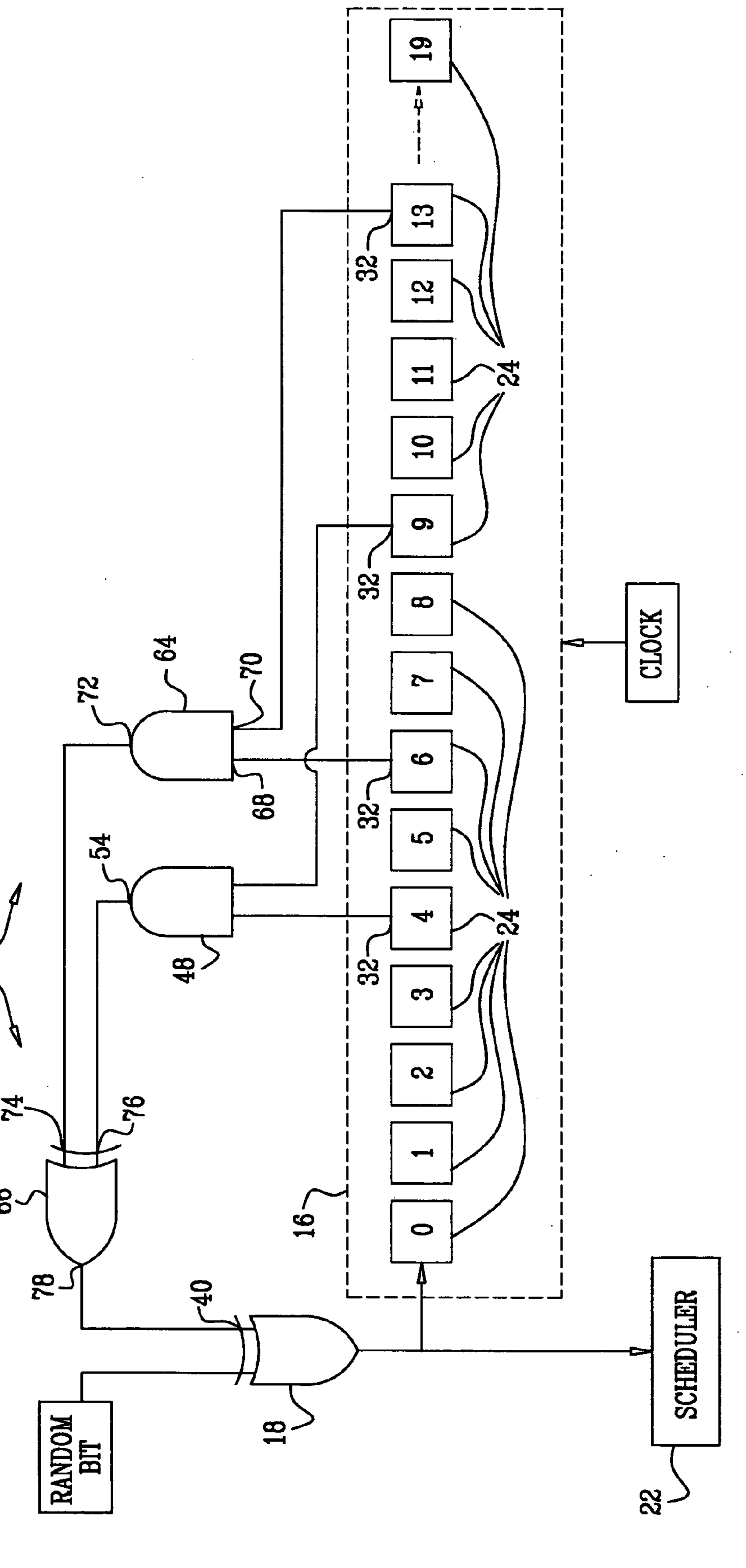

12
34
RANDOM BIT
18
40
78
66
74
76
54
48
72
64
70
68
16
0
1
2
3
4
5
6
7
8
9
10
11
12
13
19
32
32
32
32
24
24
24
24
CLOCK
SCHEDULER
22

FIG. 6A

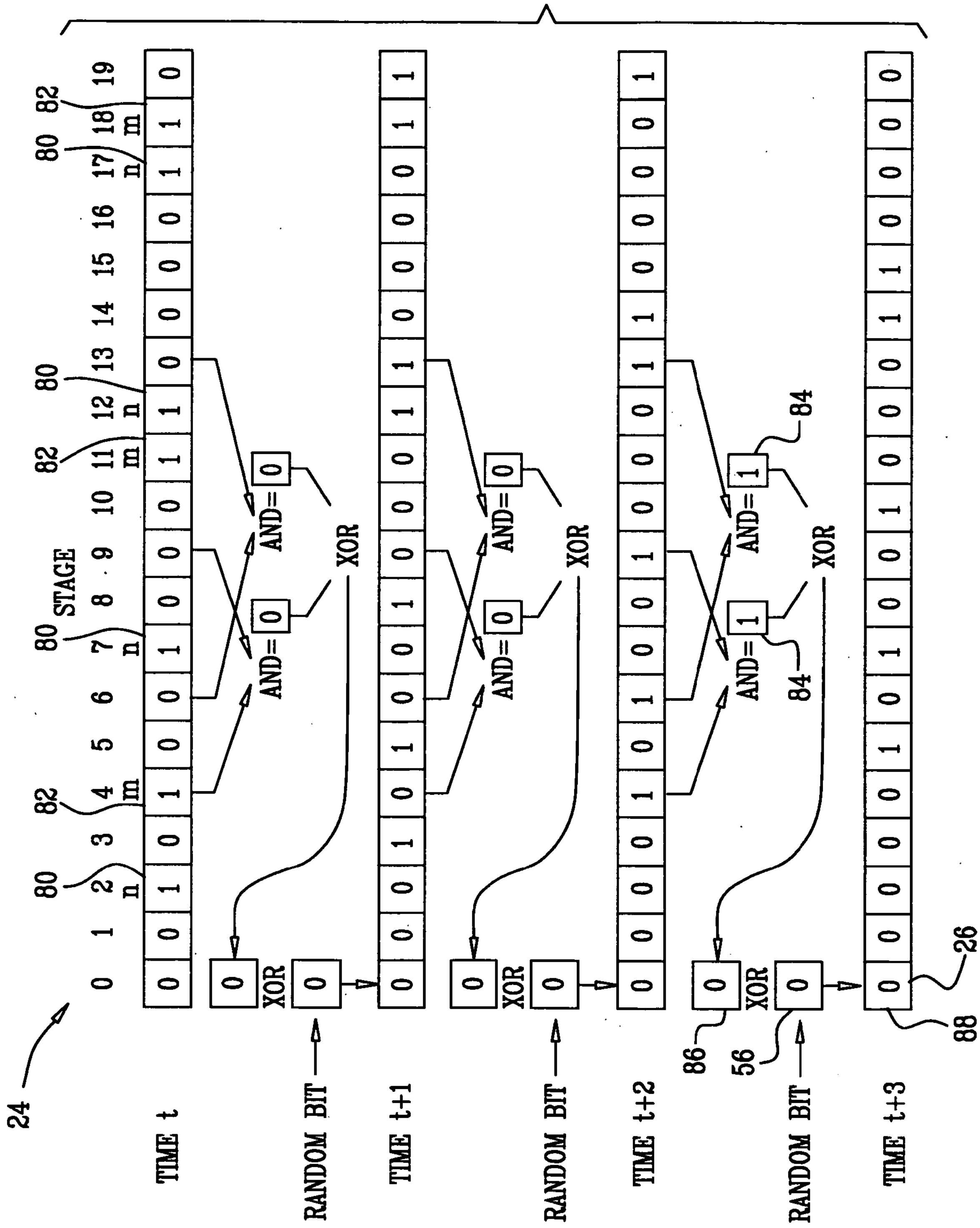
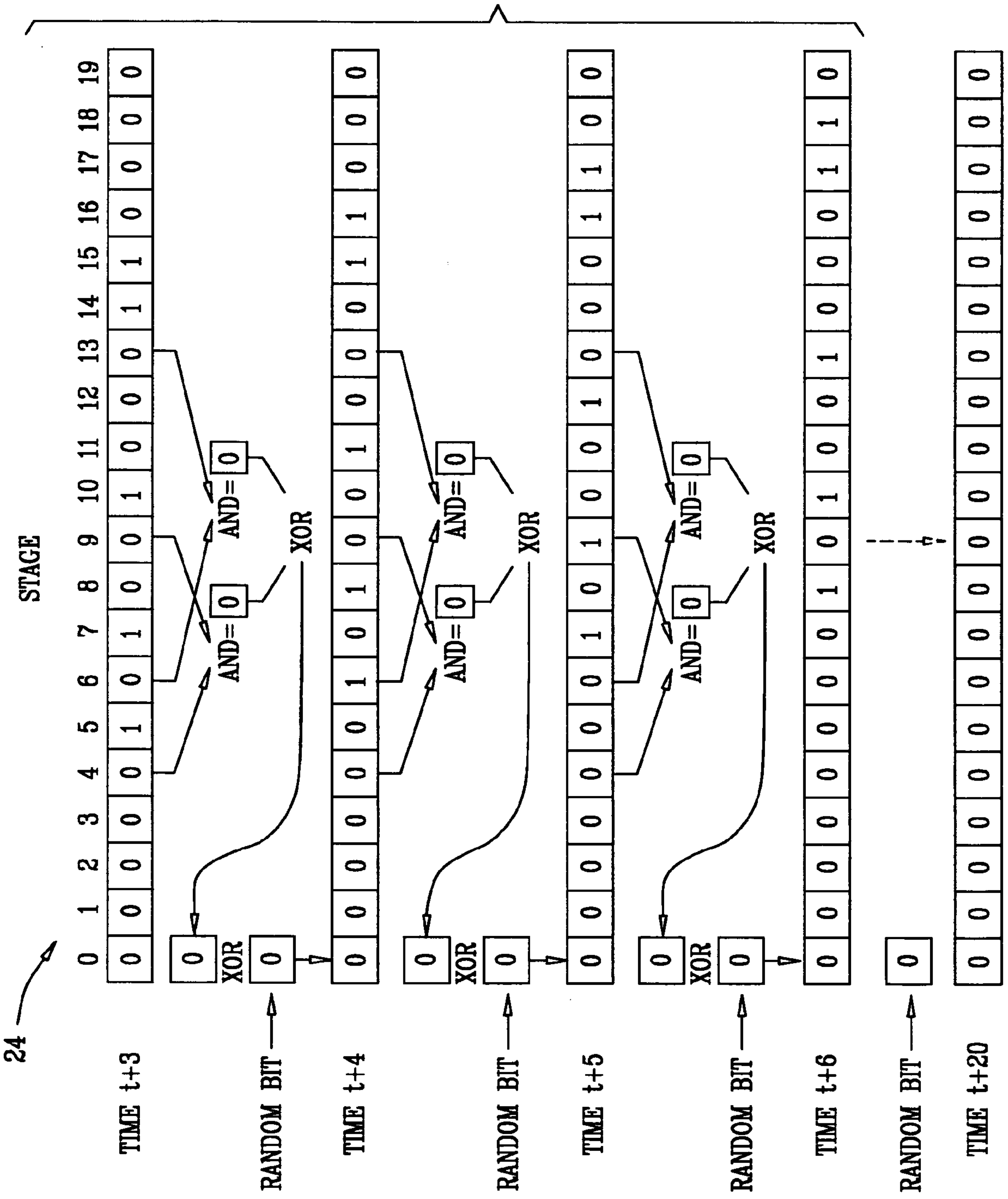
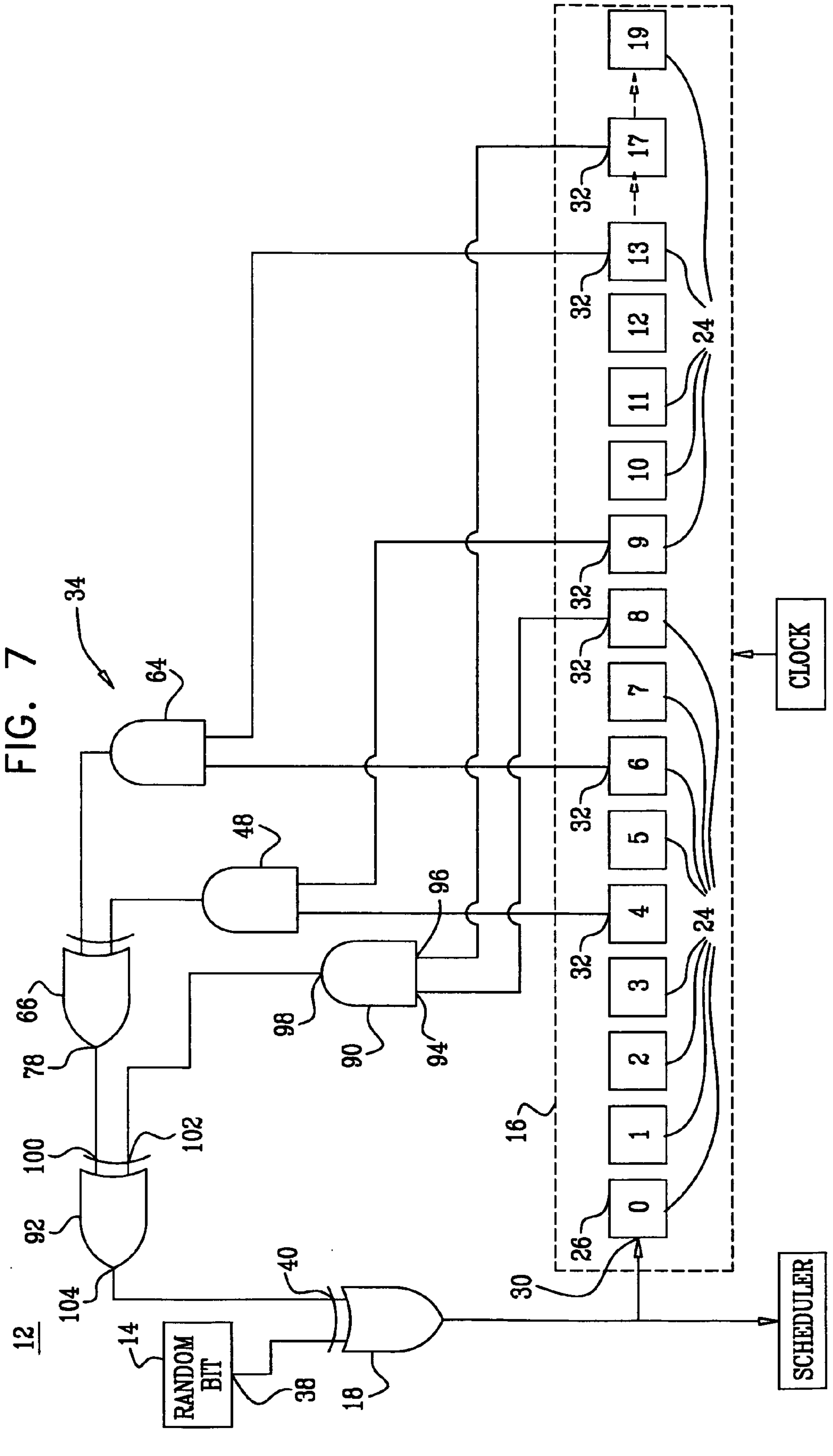

24
STAGE
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
80 n
82 m
80 n
80 n
82 m
80 n
82 m
TIME t
0 0 1 0 1 0 0 1 0 0 0 1 1 0 0 0 0 1 1 0
AND= 0
AND= 0
XOR
0 XOR
RANDOM BIT
0
TIME t+1
0 0 0 1 0 1 0 0 1 0 0 0 1 1 0 0 0 0 1 1
AND= 0
AND= 0
XOR
0 XOR
RANDOM BIT
0
TIME t+2
0 0 0 0 1 0 1 0 0 1 0 0 0 1 1 0 0 0 0 1
AND= 1
AND= 1
84
84
XOR
0 XOR
86
56
RANDOM BIT
0
TIME t+3
0 0 0 0 0 1 0 1 0 0 1 0 0 0 1 1 0 0 0 0
26
88

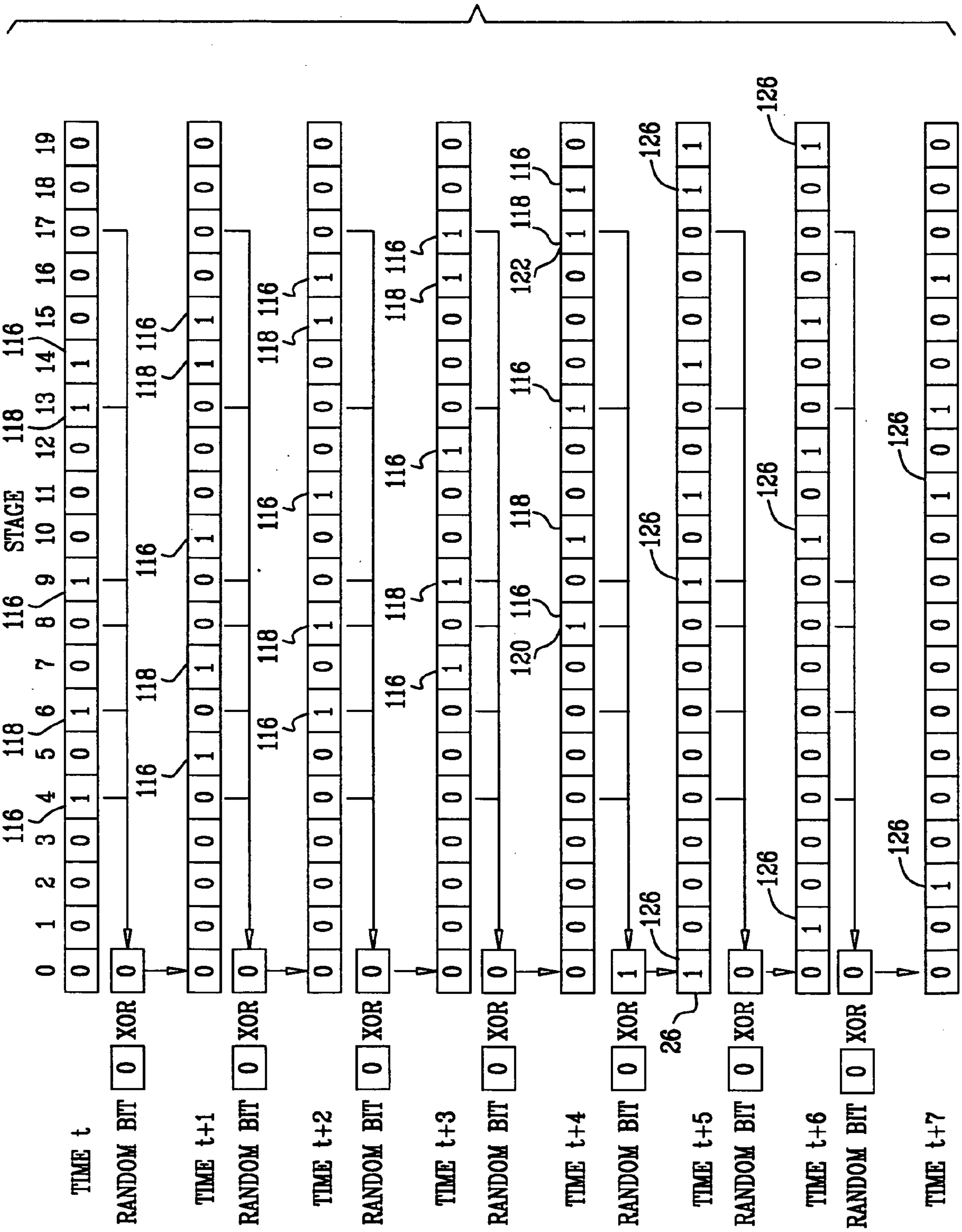
FIG. 6B



STAGE	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
TIME t+3	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0	0	0	0
TIME t+4	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0	0	0
TIME t+5	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0	0
TIME t+6	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0
TIME t+20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

FIG. 7

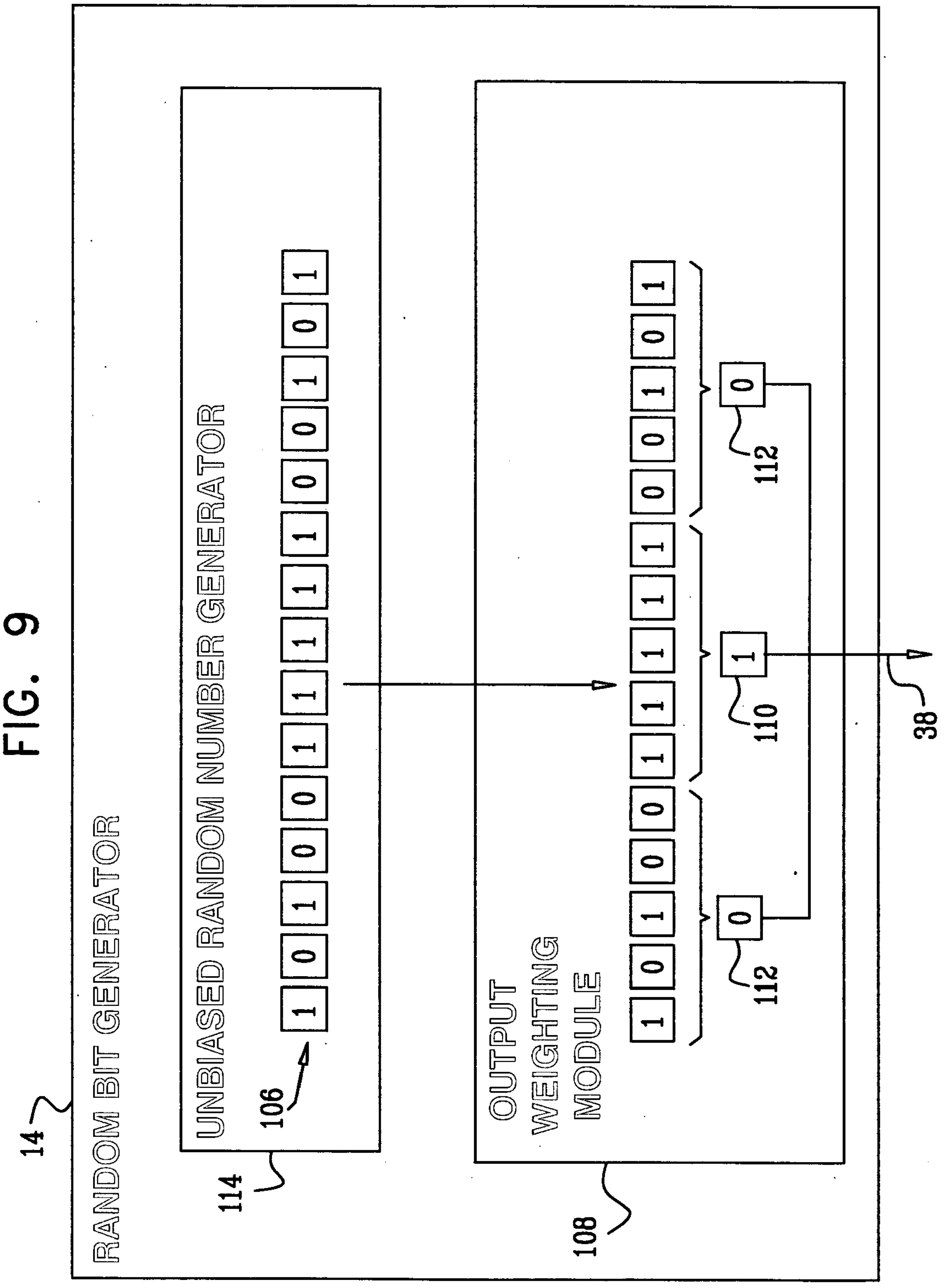

12
RANDOM BIT
14
38
18
40
104
92
100
102
78
66
98
90
94
96
48
64
34
16
26
30
0
1
2
3
4
5
6
7
8
9
10
11
12
13
17
19
32
24
CLOCK
SCHEDULER



		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
TIME t		0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0	0	0	0	0
RANDOM BIT	0 XOR	0																			
TIME t+1		0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0	0	0	0
RANDOM BIT	0 XOR	0																			
TIME t+2		0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0	0	0
RANDOM BIT	0 XOR	0																			
TIME t+3		0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0	0
RANDOM BIT	0 XOR	0																			
TIME t+4		0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0
RANDOM BIT	0 XOR	1																			
TIME t+5		1	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1
RANDOM BIT	0 XOR	0																			
TIME t+6		0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1
RANDOM BIT	0 XOR	0																			
TIME t+7		0	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0

FIG. 8

FIG. 9


14
RANDOM BIT GENERATOR
114
UNBIASED RANDOM NUMBER GENERATOR
106
1 0 1 0 0 1 1 1 1 1 0 0 1 0 1
108
OUTPUT
WEIGHTING
MODULE
1 0 1 0 0 1 1 1 1 1 0 0 1 0 1
0
112
1
110
0
112
38

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 6167553 A, Dent **[0003]**
- US 6785389 B, Sella **[0003]**
- US 20030085286 A, Kelley **[0003]**
- US 20040076293 A, Smeets **[0003]**
- US 20040205095 A, Gressel **[0003]**
- US 20060161610 A, Goettfert **[0003]**

Non-patent literature cited in the description

- **Olivier Benoit ; Michael Tunstall.** Efficient Use of Random Delays **[0003]**
- Discrete Mathematics and Its Applications. **Alfred J. Menezes ; Paul C. van Oorschot ; Scott A. Vanstone.** Handbook of Applied Cryptography. CRC Press **[0003]**