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

(11) **EP 3 776 179 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
27.04.2022 Bulletin 2022/17

(21) Application number: **19847508.9**

(22) Date of filing: **13.02.2019**

(51) International Patent Classification (IPC):
G06F 7/58 *(2006.01)* ***H03K 3/84*** *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G06F 7/588

(86) International application number:
PCT/US2019/017748

(87) International publication number:
WO 2020/033002 (13.02.2020 Gazette 2020/07)

(54) APPARATUS, SYSTEMS, AND METHODS COMPRISING TRITIUM RANDOM NUMBER GENERATOR

VORRICHTUNG, SYSTEME UND VERFAHREN MIT TRITIUMZUFALLSZAHLENGENERATOR

APPAREILS, SYSTÈMES ET PROCÉDÉS COMPRENANT UN GÉNÉRATEUR DE NOMBRE ALÉATOIRE TRITIUM

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

(30) Priority: **09.04.2018 US 201862655172 P**
09.02.2019 US 201962803476 P
12.02.2019 US 201916273365

(43) Date of publication of application:
17.02.2021 Bulletin 2021/07

(73) Proprietor: **RANDAEMON sp. z o.o.**
02-656 Warszawa (PL)

(72) Inventor: **Tatarkiewicz, Jan J.**
San Diego, CA 92130-1528 (US)

(74) Representative: **Schlee, Alexander Richard**
Schlee IP International
Maximilianstraße 33
80539 München (DE)

(56) References cited:
EP-A1- 1 094 603
US-A1- 2003 018 674
US-A1- 2012 030 268
US-A1- 2018 217 817
US-B1- 6 697 829

- **Ammar Alkassar ET AL: "Obtaining True-Random Binary Numbers from a Weak Radioactive Source" In: "ICIAP: International Conference on Image Analysis and Processing, 17th International Conference, Naples, Italy, September 9-13, 2013. Proceedings", 1 January 2005 (2005-01-01), Springer, Berlin, Heidelberg 032548, XP055465780, ISBN: 978-3-642-17318-9 vol. 3481, pages 634-646, DOI: 10.1007/11424826_67, * paragraphs [section2.0], [02.2] ***
- **MIGUEL HERRERO-COLLANTES ET AL: "Quantum Random Number Generators", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 12 April 2016 (2016-04-12), XP080694891,**

EP 3 776 179 B1

Description

TECHNICAL FIELD

[0001] The present disclosure relates generally to true random number generators, specifically random number generator technologies utilizing the spontaneous tritium decay, as well as apparatus, systems, and methods regarding same.

BACKGROUND

[0002] As opposed to pseudo random number generators based on algorithms, there are true random number generator (TRNG) devices that depend on natural random processes: multiple bipolar switches, thermal noise, light scattering by dichroic mirrors, chaotic systems, decay of radioactive nuclei..

[0003] The decay of radioactive nuclei type is considered to be the most independent on the environmental influences like temperature, pressure or acceleration. However, typical nuclear-based TRNGs require large size detectors to enable registration of particles emitted as a result of radioactive decays. Also, many nuclei used in such devices are highly radioactive and poisonous hence dangerous to humans if device is broken.

[0004] Therefore, a safe and small TRNG that will not expose the user to dangerous levels of radiation would be advantageous. Such a TRNG can then be used in compact personal devices. This is achieved by the apparatus having the features as claimed in claim 1 and the method having the features as claimed in claim 12, respectively. Advantageous further embodiments are claimed in the dependent claims.

SUMMARY

[0005] The invention disclosed herein is a true random number generator (TRNG). The TRNG includes a cavity filled with tritium and an electronic sensor constructed to detect energy from the decay of the tritium. The sensor produces a signal for the detected energy and an amplifier amplifies the signal, while a filter filters the signal. A processor (a) determines whether the signal represents decay events for tritium; (b) sets a timer to determine the time period between decay events; (c) based on the time period in step (b), assigns a value of a 0 or a 1; (d) stores the value in a memory; (e) repeat steps (b) - (d) resulting in a string of values; and (f) generates a true random number based on the string of values. And the TRNG may be formed on an integrated circuit.

[0006] In step (b), the processor may further determine a first time period T1 between a first pair of decay events and a second time period T2 between a second pair of decay events. And may in step (c), compare T1 to T2 and assign the value based on the comparison. The first pair of decay events and the second pair of decay events may share a common decay event.

[0007] The processor may generate an array of true random numbers. The processor may provide one of the array of true random numbers to a cryptographic client and then delete the delivered true random number from the memory. The one of the array of true random number provided to the cryptographic client may be the oldest one in the array. When the memory is full, the processor may delete the oldest one in the array of true random numbers. The true random numbers generated may be comprised of 256 bits or 512 bits.

[0008] The volume of tritium may be less than 0.03 μL, and the maximum radioactivity of the tritium may be less than 3×10^{-5} Ci. The amount of tritium may be sufficient to create at least one million decay events per second.

[0009] The amplifier may be a low noise charge-sensitive preamplifier or a pulse shaping amplifier. The timer may have a have a clock frequency of at least 1 GHz.

[0010] A personal electronic device may be constructed from the TRNG. This device may use the true random numbers to encrypt a communication channel, to render computer simulations, or to render computer gaming.

[0011] A method to generate to a true random number using tritium is also disclosed. The method includes: (a) providing a volume of tritium; (b) detecting an energy signal from the decay of the tritium; (c) determining whether the energy signal represents decay events for tritium; (d) setting a timer to determine the time period between decay events; (e) assigning a value of a 0 or a 1 based on the time period; (f) storing the value; (g) repeating steps (b) - (f) resulting in a string of values; and (h) generating an array of true random numbers based on the string of values.

BRIEF DESCRIPTION OF DRAWINGS

[0012] The invention can be better understood with reference to the following figures. The components within the figures are not necessarily to scale, emphasis instead being placed on clearly illustrating example aspects of the invention. In the figures, like reference numerals designate corresponding parts throughout the different views and/or embodiments.

FIG. 1 A is a cross sectional view of a PIN diode detector.

FIG. 1B is a cross sectional view of a CCD detector.
FIG. 2 is a flow diagram of the various components that may be place on the integrated circuit.
FIG. 3 A illustrates the four pulse per random bit schema.
FIG. 3B illustrates the two pulse per random bit schema.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

[0013] The following list of example features corresponds with FIGS. 1 - 4 and is provided for ease of reference, where like reference numerals designate corresponding features throughout the specification and figures:

Cavity 10

Filler Tubes 15

PIN Diode 18

N-type silicon 20

P-type silicon 25

CCD 28

Silicon Substrate 30

Electrodes 35

Insulation 40

Upper casing 45

Lower casing 50

IC 200

Detector 205

Amplifier 210

Filter 215

Processor 220

Signal Processor 225

Timer 230

Memory 235

Cryptographical Client 240

[0014] As opposed to pseudo random number generators based on algorithms, there are many true random number generator (TRNG) devices that depend on natural random processes: multiple bipolar switches, thermal noise, light scattering by dichroic mirrors, chaotic systems, decay of radioactive nuclei. The latter group is considered to be the most independent on the environmental influences like temperature, pressure or acceleration. However, typical nuclear-based TRNGs require large size detectors to enable registration of particles emitted as a result of radioactive decays. Also, many nuclei used in such devices are highly radioactive and poisonous hence dangerous to humans if device is broken. Various example embodiments of the present apparatus, systems, and methods demonstrate that by using gaseous tritium paired with suitable solid-state detector one is able to make a very compact device that can be incorporated into

integrated circuit (IC) chip. Because of small amounts of radioactive material deployed, such an IC can be used inside consumer products like cell phones without endangering people even if the device is destroyed and radioactive material is released. Analog and digital circuits that need to be incorporated into proposed design of TRNG on IC chip can be easily manufactured with standard epitaxial, implantation and laser annealing procedures used throughout industry that makes solid state devices. Various example embodiments of the present apparatus, systems, and methods demonstrate, ICs can be filled with suitable gas after they are manufactured and already packaged; see, e.g., Fig. 1. Even with a very small amount of radioactive tritium each such chip can generate many thousands of random bits per second. Then these bits can be stored for later use in solid state memory incorporated inside ICs. Thus, such standalone TRNG on chip can easily provide on demand thousands of multi-byte random numbers needed for encryption of communication channels (like voice or text messages) or for processes requiring plenty of random numbers (like simulations or gaming).

[0015] Radioactive tritium is simply an isotope of hydrogen that like hydrogen contains in each nucleus one proton with additional two neutrons as well. These two neutrons make tritium an unstable isotope with half-life time of about 12.3 years. Because of that short half-life time, natural abundance of tritium on Earth is only barely traceable. However, tritium can be easily produced inside nuclear reactors by neutron activation of lithium-6 or boron-10 and their subsequent, fast decay to tritium. In heavy-water moderated reactors, deuterium nucleus that captured a neutron is also converted into tritium. Because of the use of tritium in the construction of nuclear weapons, production of that material is being continued all the time, excess of the obtained gas being stored and also available for commercial applications. Recently there's a whole cottage industry that produces devices that are self-illuminating like gun sights, flash lights and jewelry. All these devices are based on the fluorescence of various fluorophores excited by electrons emitted by decaying tritium. Natural decay of tritium into helium produces electrons with the average energy of about 5.7 keV that is sufficient to excite many fluorophores and thus to help emit visible light with different colors depending on fluorophore. Such devices use only minute amounts of tritium and hence are allowed to be sold and used by general public, cf. RoHs list of restricted materials for electronic components that does not contain tritium.

[0016] Using tritium to generate plenty of random numbers (bits or bytes) corresponding to the detection of emitted electrons allows for estimation of the amount of tritium gas needed. Let's assume that one wants to detect on average 1 million spontaneous decays of tritium per second. With density of tritium being 6 grams per mole and half-life time of tritium being about 12.3 years or about 400 million seconds, one can estimate that to have on average 1 million decays per second one will need an amount of about 8×10^{14} tritium atoms. Since one mole of any substance contains about 6×10^{23} atoms (Avogadro's number) and one mole of any gas in normal conditions has the volume of about 22.4 liters, the number of tritium atoms needed for 1 million decays per second will have the volume of about 2.9×10^{-8} liters or 0.029 μL, which is equal to 0.029 mm^3. The latter number means that rectangular volume restricted by dimensions of 0.3 mm $\times$ 0.3 mm $\times$ 0.3 mm will contain desired amount of tritium gas that can emit about 1 million electrons every second for at least 12 years. With the market cost of 1 gram of tritium gas being about $30,000.00, the amount of gas needed for the above calculated decays will cost less than 1 cent. The dose of radiation received by a human person (if all that amount of tritium is digested or otherwise swallowed) is equal to about 7 percent of US natural background dose (about 0.23 mSv/year vs. 3.1 mSv/year). This makes TRNG based on tritium made as per this patent application very safe indeed. These numbers are presented in the Appendix.

[0017] Electrons emitted in the spontaneous decay of tritium that have on average the energy of 5.7 keV can be easily detected by PIN diode (P and N regions being heavily doped semiconductors with intrinsic semiconductor region sandwiched between them) or by typical CCD circuit; both these devices can be easily incorporated in a design of specialized IC with TRNG. Such a detector 205 is shown in FIG. 1A. The cavity 10 is filled with tritium through the filling tubes 15. The PIN diode 18 is formed by the N-type silicon 20 and P-type silicon 25 formed on a silicon substrate 30. Electrodes 35 carry the detected signal. Insulation 40 may be used to better insulate the tritium from both escaping the cavity 10 and to contain the energy emitted by the decay so that the PIN diode can more robustly detect the decay. To further protect the tritium from escape the entire detector (indeed the entire IC) may have and upper and lower casing 45, 50. FIG. 1B illustrates a CCD 28 used as the electronic sensor. Other types of electronic sensors may be used, including as a non-limiting example a CMOS electronic sensor.

[0018] The detector 205 may be included on an IC 200, which may further include an amplifier 210 (such as a low noise charge-sensitive preamplifier and pulse shaping amplifier), a filter 215, and processor 220, as shown in FIG. 2. A cryptographic client 240 may optionally also be on the IC.

[0019] The following is an exemplary method for converting random tritium decays resulting in emission of electrons that are being sensed by PIN diode or CCD-type build-in on-chip detector 205 discussed above:

1. After each decay of a tritium nuclei, one electron with energy of about 5.7 keV is being emitted.
2. Each such electron creates a pulse of electrons in the detector 205 with a very typical time profile that enables detection of just that event and not the other possible types of energetic ionizing particles hitting detector.
3. The analog pulse from the detector 205 is amplified by the amplifier 210. The amplifier may have a pre-amplifier.
4. The amplified signal from the amplifier 210 is filtered by digital filter 215.

5. The filtered signal is processed by processor 220 to determine if the signal corresponds to the electron emitted in a decay of tritium and not by other energetic ionizing particle(s). The processor 220 may include a signal processor 225 that performs this function.
6. If the signal is indeed an electron emitted in a decay or tritium, then the processor 220 starts a timer 230, which may also be part of the processor 220. The time may optimally be at a clock frequency of the order of several GHz (several times 10^9 per second). Because electron pulses will be detected on average every microsecond (10^{-6} seconds or between average number of clock ticks of several thousands), one would have enough accuracy to detect differences of randomness of appearances of pulses in time.
7. Steps 1 - 6 are repeated to detect a second pulse from subsequent decay, which triggers the processor 220 to stop the timer.
8. The value of the timer is stored in the memory 235. This is shown as T1 in FIG. 3A.
9. The next two pulses result in another timer value (T2; FIG. 3A) to be stored in the memory 235. To generate T1 and T2, four pulses are used in FIG. 3A.
10. Two numbers (T1 and T2) stored in memories are compared - if first is larger, then the system creates bit with value 1, in the other case the value is zero. (This schema can be inverted as well). These bit values are stored in the memory 235. In the very rare situation that two numbers are exactly same, the whole sequence may be discarded. So for each random bit, four pulses are used.
11. Steps 1 - 10 are repeated, typically several hundred thousand times per second.
12. The system generates multibyte numbers, typically 256 bits or 512 bits long, and these are stored in the memory bank for further use by the cryptographic client 240 of the chip, providing long (large) random numbers needed for the encryption of communication channels.
13. After a number is used by the cryptographic client 240, the FILO system (first in, last out) moves to the other number while the process described above adds more numbers to the memory until it is filled. In such case of filling the whole memory bank, numbers kept longest in the memory are expunged to make space for new numbers generated by the system. This capability makes the system much more resistant against hacking etc.

[0020] It should be noted that the system may not use four pulses per random bit. Instead, the system may be constructed as shown in FIG. 3B, where the timer resets at each pulse detection and is always counting. The benefit to this system is it only requires two pulses per random bit. But the two time periods are somewhat dependent on each other because they are linked by a pulse event, so the resulting string of bits may not be as random as the schema provided in FIG. 3A.

[0021] The memory can supply necessary number of bytes (bits) on demand for e.g. secure random encryption of communication channels (i.e., cryptographic client 240) of the device in which this specialized IC is mounted or for random processes required by simulations, modelling and gaming. Additional software testing of random number sequences built into IC chip allows for real time quality control of random character of bits generated - if parts of the sequence do not pass test(s), such a sequence would be removed and never used as an output. This type of proofing further improves random character of sequences that are being generated by the chip.

[0022] Various example embodiments of the present apparatus, systems, and methods provide the ability to manufacture TRNG IC on the standard semiconductor production line, the only difference being that the packaging should leave as calculated above the void of the size of about 0.03 mm^3 with suitable openings that can be connected to the source of gaseous tritium to fill this void and after that being sealed by thermal and pressure means (like heat sealer). Otherwise, the produced IC will be very similar in shape and other characteristics to other ICs typically used in the manufacturing of consumer goods because electrons emitted during decay of tritium won't be able to penetrate packaging material (plastic) of IC. The range of 5.7 keV electrons in a material like plastic is less than 1 micrometer. The same packaging also will be shielding embedded detector from any external radiation of comparable or even much higher energies. Even if such high energy particles will pass through packaging plastic, they will generate different type of pulses and these can be differentiated by filtering from 5.7 keV pulses that are being used to generate random numbers.

[0023] RoHS specifies maximum levels for the following 10 restricted materials. The first six applied to the original RoHS while the last four were added under RoHS 3. Following is the RoHs list of restricted materials from http://www.rohs-guide.com/rohs-substances.htm:

- Lead (Pb): < 1000 ppm
- Lead is commonly used in the electrical and electronics industry in solder, lead-acid batteries, electronic components, cable sheathing and in the glass of cathode-ray tubes.
- Mercury (Hg): < 100 ppm
- Mercury is widely used metals in the production of electrical and electronic appliances and is concentrated in batteries, switches and thermostats, and fluorescent lamps.
- Cadmium (Cd): < 100 ppm

- Cadmium is used in electronic equipment, car batteries, and pigments.
- Hexavalent Chromium (Cr VI) < 1000 ppm
- While some forms of chromium are non-toxic, Chromium VI can produce toxic effects.
- Polybrominated Biphenyls (PBB): 1000 ppm
- These are flame retardants found in electronic and electrical appliances. They have been found in indoor dust and air through evaporation from plastics.
- Polybrominated Diphenyl Ethers (PBDE): < 1000 ppm
- These are also flame retardants found in electronic and electrical appliances. Combustion of printed wiring boards release toxic emissions.
- Bis(2-Ethylhexyl) phthalate (DEHP): < 1000 ppm
- These are used to soften PVC and vinyl insulation on electrical wires.
- Benzyl butyl phthalate (BBP): < 1000 ppm
- These are used to soften PVC and vinyl insulation on electrical wires.
- Dibutyl phthalate (DBP): < 1000 ppm
- These are used to soften PVC and vinyl insulation on electrical wires.
- Diisobutyl phthalate (DIBP): < 1000 ppm
- These are used to soften PVC and vinyl insulation on electrical wires.

[0024] Any of the suitable technologies, materials, and designs set forth and incorporated herein may be used to implement various example aspects of the invention as would be apparent to one of skill in the art.

[0025] TRNGs are crucial for secure communications between personal devices (like cell phones and other personal computers), between such devices and internet banking services as well as between any devices that require encrypted channels like police, fire fighters or military ones. True random numbers are also necessary for all types of gaming: computer games, network games as well as all types of casino playing machines (the so called slot machines). Also all types of lotteries that sell tickets with random drawing options need TRNGs. These applications of random numbers are important despite the fact that most playing machines and lotteries use specially skewed number generators to increase odds of winning to attract customers but they have to start with good randomizers to prevent too easy winnings. The methods, systems and devices disclosed herein may be use in all of these applications.

[0026] Although exemplary embodiments and applications of the invention have been described herein including as described above and shown in the included example Figures, there is no intention that the invention be limited to these exemplary embodiments and applications or to the manner in which the exemplary embodiments and applications operate or are described herein. Indeed, many variations and modifications to the exemplary embodiments are possible as would be apparent to a person of ordinary skill in the art. The invention may include any device, structure, method, or functionality, as long as the resulting device, system or method falls within the scope of one of the claims that are allowed by the patent office based on this or any related patent application.

APPENDIX

[0027]

Density of T_2:	6 g/mol
Volume of T_2:	22.4 L/mol
Half-life of T_2	12.32 years 388,523,520 seconds
Needed Decay	1,000,000 decays/second
	1 decay/μsec
Radioactivity	1,000,000 Bq
	2.70×10^{-5} Ci (with e^- energy 5.7 keV per decay; 1 rad = 1 rem = 0.01 Sv; 1 rad = 0.01 J/kg)
Dose per body	7.30×10^{-11} J/(kg-s) or Gy/s
	2.30×10^{-3} Gy/year
	0.23 mSv/year
Natural background Eus	3.1 mSv/year
% of US yearly from T_2	7% (if fully absorbed in lungs)

(continued)

T_2 needed	7.77×10^{14} atoms
T_2 volume needed	2.89×10^{-8} L
	2.89×10^{-2} μL (mm^3)
T_2 mass needed	7.74×10^{-9} g
	7.74×10^{-3} μg
T_2 cost	$30,000.00/gram
Cost of T_2 needed	$0.00023
Cell size [mm^3]	2.70×10^{-2}

Claims

1. A true random number generator comprising:

a cavity (10) filled with tritium;
an electronic sensor (18) constructed to detect energy from the decay of the tritium and to produce a signal for the detected energy;
an amplifier (210) connected to the sensor (18) and constructed to amplify the signal;
a filter (215) connected to the amplifier (210) constructed to filter the signal;
a processor (220) connected to the filter (215), the processor constructed to perform the following steps:

a. determine whether the signal represents decay events for tritium;
b. set a timer (230) to determine the time period between decay events;
c. based on the time period in step (b), assign a value of a 0 or a 1;
d. store the value in a memory (235);
e. repeat steps (b) - (d) resulting in a string of values; and
f. generate a true random number based on the string of values.

2. The true random number generator of claim 1,
wherein step (b) further comprises determining:

a first time period T1 between a first pair of decay events;
a second time period T2 between a second pair of decay events; and wherein step (c) further comprises comparing T1 to T2 and assigning the
value based on the comparison.

3. The true random number generator of claim 2, wherein the first pair of decay events and the second pair of decay events share a common decay event.

4. The true random number generator of claim 1, wherein the cavity (10), sensor amplifier (210), filter (215) and processor (220) are formed on an integrated circuit (200).

5. The true random number generator of claim 1, wherein the volume of tritium is less than 0.03 μL.

6. The true random number generator of claim 1, wherein the maximum radioactivity of the tritium is less than 3×10^{-5} Ci.

7. The true random number generator of claim 1, wherein the processor (220) generates an array of true random numbers.

8. The true random number generator of claim 7, wherein the processor (220) provides one of an array of true random numbers to a cryptographic client (240); and deletes the delivered true random number from the memory.

9. The true random number generator of claim 1, wherein the amount of tritium is sufficient to create at least one million

decay events per second.

10. The true random number generator of claim 1, wherein the timer (230) has a clock frequency of at least 1 GHz.

11. The true random number generator of claim 1, wherein the amplifier (210) comprises a low noise charge-sensitive preamplifier or a pulse shaping amplifier.

12. A method of generating a true random number using tritium, the method comprising:

a. providing a volume of tritium;
b. detecting an energy signal from the decay of the tritium;
c. determining whether the energy signal represents decay events for tritium;
d. setting a timer to determine the time period between decay events;
e. assigning a value of a 0 or a 1 based on the time period;
f. storing the value;
g. repeating steps (b) - (f), resulting in a string of values; and
h. generating an array of true random numbers based on the string of values.

13. The method of claim 12,
wherein step (d) further comprises determining:

a first time period T1 between a first pair of decay events;
a second time period T2 between a second pair of decay events; and wherein step (e) further comprises comparing T1 to T2 and assigning the
value based on the comparison.

14. The method of claim 13, wherein the first pair of decay events and the second pair of decay events share a common decay event.

15. The method of claim 12, the method further comprising:

i. providing one of an array of true random numbers to a cryptographic client; and
j. deleting the delivered true random number from the memory.

Patentansprüche

1. Ein echter Zufallszahlengenerator mit:

einem mit Tritium gefüllten Hohlraum (10);
einem elektronischen Sensor (18), welcher zum Erfassen der Energie ausgebildet ist, welche aus dem radioaktiven Zerfall des Tritiums resultiert und zum Erzeugen eines Signals entsprechend der erfassten Energie ausgebildet ist;
einem mit dem Sensor (18) verbundenen Verstärker (210), welcher zum Verstärken des Signals ausgebildet ist;
einem mit dem Verstärker (210) verbundenen Filter (215), welcher zum Filtern des Signals ausgebildet ist;
einem mit dem Filter (215) verbundenen Prozessor (220), wobei der Prozessor zum Durchführen der folgenden Schritte ausgebildet ist:

a. Bestimmen, ob das Signal ein Zerfallsvorgangsereignis des Tritiums repräsentiert;
b. Setzen eines Zeitgebers (230), um die Zeitspanne zwischen Zerfallsvorgangsereignissen zu messen;
c. Basierend auf der in Schritt (b) gemessenen Zeitspanne, Zuordnen eines Werts von 0 oder von 1;
d. Speichern des Werts in einem Datenspeicher (235);
e. Wiederholen der Schritte (b) - (d), was in einer Wertefolge resultiert; und
f. Erzeugen einer echten Zufallszahl basierend auf der Wertefolge.

2. Der echte Zufallszahlengenerator nach Anspruch 1,

wobei der Schritt (b) weiter versehen ist mit dem Bestimmen:

einer ersten Zeitspanne T1 zwischen einem ersten Paar von Zerfallsvorgangsereignissen;
einer zweiten Zeitspanne T2 zwischen einem zweiten Paar von Zerfallsvorgangsereignissen; und

wobei der Schritt (c) weiter einen Vergleich von T1 und T2 aufweist und basierend auf diesem Vergleich das Zuordnen eines Werts aufweist.

3. Der echte Zufallszahlengenerator nach Anspruch 2, wobei das Paar aus den ersten Zerfallsvorgangsereignissen und den zweiten Zerfallsvorgangsereignissen Teil eines gemeinsamen Zerfallsvorgangsereignisses sind.

4. Der echte Zufallszahlengenerator nach Anspruch 1, wobei der Hohlraum (10), der Sensor-Verstärker (210), der Filter (215) und der Prozessor (220) auf einem integrierten Schaltkreis (200) ausgebildet sind.

5. Der echte Zufallszahlengenerator nach Anspruch 1, wobei das Volumen des Tritiums kleiner als 0,03 μl ist.

6. Der echte Zufallszahlengenerator nach Anspruch 1, wobei die maximale Radioaktivität des Tritiums weniger als 3×10^{-5} Ci beträgt.

7. Der echte Zufallszahlengenerator nach Anspruch 1, wobei der Prozessor (220) eine Matrix aus echten Zufallszahlen erzeugt.

8. Der echte Zufallszahlengenerator nach Anspruch 7, wobei der Prozessor (220) eine der Zufallszahlen der Matrix aus echten Zufallszahlen an einen Kryptografie-Client (240) liefert; und die gelieferte Zufallszahl aus dem Datenspeicher löscht.

9. Der echte Zufallszahlengenerator nach Anspruch 1, wobei die Menge des Tritiums groß genug ist, um wenigstens eine Million von Zerfallsvorgängen pro Sekunde zu erzeugen.

10. Der echte Zufallszahlengenerator nach Anspruch 1, wobei der Zeitgeber (230) eine Taktfrequenz von wenigstens 1 GHz hat.

11. Der echte Zufallszahlengenerator nach Anspruch 1, wobei der Verstärker (210) einen rauscharmen, ladungsempfindlichen Vorverstärker oder einen Impulsformungsverstärker aufweist.

12. Ein Verfahren zum Erzeugen einer echten Zufallszahl unter Verwendung von Tritium, wobei das Verfahren versehen ist mit:

a. Bereitstellen eines Volumens von Tritium;
b. Erfassen eines Energie-Signals, welches aus einem radioaktiven Zerfall des Tritiums resultiert;
c. Bestimmen, ob das Signal Zerfallsvorgangsereignisse des Tritiums repräsentiert;
d. Setzen eines Zeitgebers, um die Zeitspanne zwischen Zerfallsvorgangsereignissen zu messen;
e. Basierend auf der Zeitspanne, Zuordnen eines Werts von 0 oder von 1;
f. Speichern des Werts;
g. Wiederholen der Schritte (b) - (f), was in einer Wertefolge resultiert; und
h. Basierend auf der Wertefolge, Erzeugen einer Matrix aus echten Zufallszahlen.

13. Das Verfahren nach Anspruch 12,

wobei der Schritt (d) weiter versehen ist mit dem Bestimmen:

einer ersten Zeitspanne T1 zwischen einem ersten Paar von Zerfallsvorgangsereignissen;
einer zweiten Zeitspanne T2 zwischen einem zweiten Paar von Zerfallsvorgangsereignissen; und

wobei der Schritt (e) weiter einen Vergleich von T1 und T2 aufweist und basierend auf diesem Vergleich das Zuordnen eines Werts aufweist.

14. Das Verfahren nach Anspruch 13, wobei das Paar aus den ersten Zerfallsvorgangsereignissen und den zweiten

Zerfallsvorgangsereignissen Teil eines gemeinsamen Zerfallsvorgangsereignisses sind.

15. Das Verfahren nach Anspruch 12, wobei das Verfahren weiter versehen ist mit:

i. Liefern von einer der echten Zufallszahlen aus der Matrix aus echten Zufallszahlen an einen Kryptografie-Client; und
j. Löschen der gelieferten echten Zufallszahl aus dem Datenspeicher.

Revendications

1. Générateur de nombre véritablement aléatoire comprenant :

une cavité (10) remplie de tritium ;
un capteur électronique (18) construit pour détecter de l'énergie provenant de la désintégration du tritium et pour produire un signal pour l'énergie détectée ;
un amplificateur (210) connecté au capteur (18) et construit pour amplifier le signal ;
un filtre (215) connecté à l'amplificateur (210) construit pour filtrer le signal ;
un processeur (220) connecté au filtre (215), le processeur étant construit pour effectuer les étapes suivantes consistant à :

a. déterminer si le signal représente des événements de désintégration du tritium ;
b. régler une minuterie (230) pour déterminer la période de temps entre des événements de désintégration ;
c. sur la base de la période de temps à l'étape (b), attribuer une valeur de 0 ou 1 ;
d. stocker la valeur dans une mémoire (235) ;
e. répéter les étapes (b) à (d) résultant en une chaîne de valeurs ; et
f. générer un nombre véritablement aléatoire sur la base de la chaîne de valeurs.

2. Générateur de nombre véritablement aléatoire selon la revendication 1,
dans lequel l'étape (b) comprend en outre la détermination :

d'une première période de temps T1 entre une première paire d'événements de désintégration ;
d'une seconde période de temps T2 entre une seconde paire d'événements de désintégration ; et
dans lequel l'étape (c) comprend en outre la comparaison de T1 et T2 et l'attribution de la valeur sur la base de la comparaison.

3. Générateur de nombre véritablement aléatoire selon la revendication 2, dans lequel la première paire d'événements de désintégration et la seconde paire d'événements de désintégration partagent un événement de désintégration commun.

4. Générateur de nombre véritablement aléatoire selon la revendication 1, dans lequel la cavité (10), l'amplificateur de capteur (210), le filtre (215) et le processeur (220) sont formés sur un circuit intégré (200).

5. Générateur de nombre véritablement aléatoire selon la revendication 1, dans lequel le volume de tritium est inférieur à 0,03 μL.

6. Générateur de nombre véritablement aléatoire selon la revendication 1, dans lequel la radioactivité maximale du tritium est inférieure à 3×10^{-5} Ci.

7. Générateur de nombre véritablement aléatoire selon la revendication 1, dans lequel le processeur (220) génère une matrice de nombres véritablement aléatoires.

8. Générateur de nombre véritablement aléatoire selon la revendication 7, dans lequel le processeur (220) fournit l'un d'une matrice de nombres véritablement aléatoires à un client cryptographique (240) ; et supprime de la mémoire le nombre véritablement aléatoire délivré.

9. Générateur de nombre véritablement aléatoire selon la revendication 1, dans lequel la quantité de tritium est suffisante pour créer au moins un million d'événements de désintégration par seconde.

10. Générateur de nombre véritablement aléatoire selon la revendication 1, dans lequel la minuterie (230) a une fréquence d'horloge d'au moins 1 GHz.

11. Générateur de nombre véritablement aléatoire selon la revendication 1, dans lequel l'amplificateur (210) comprend un préamplificateur sensible à une charge de faible bruit ou un amplificateur de mise en forme d'impulsions.

12. Procédé de génération d'un nombre véritablement aléatoire à l'aide de tritium, le procédé comprenant les étapes consistant à :

a. fournir un volume de tritium ;
b. détecter un signal d'énergie provenant de la désintégration du tritium ;
c. déterminer si le signal d'énergie représente des événements de désintégration pour le tritium ;
d. régler une minuterie pour déterminer la période de temps entre des événements de décroissance ;
e. attribuer une valeur de 0 ou 1 sur la base de la période de temps ;
f. stocker la valeur ;
g. répéter les étapes (b) à (f), résultant en une chaîne de valeurs ; et
h. générer une matrice de nombres véritablement aléatoires sur la base de la chaîne de valeurs.

13. Procédé selon la revendication 12,
dans lequel l'étape (d) comprend en outre la détermination :

d'une première période de temps T1 entre une première paire d'événements de désintégration ;
d'une seconde période de temps T2 entre une seconde paire d'événements de désintégration ; et
dans lequel l'étape (e) comprend en outre la comparaison de T1 et T2 et l'attribution de la valeur sur la base de la comparaison.

14. Procédé selon la revendication 13, dans lequel la première paire d'événements de désintégration et la seconde paire d'événements de désintégration partagent un événement de désintégration commun.

15. Procédé selon la revendication 12, le procédé comprenant en outre :

i. la fourniture de l'un d'une matrice de nombres véritablement aléatoires à un client cryptographique ; et
j. la suppression depuis la mémoire du nombre véritablement aléatoire délivré.

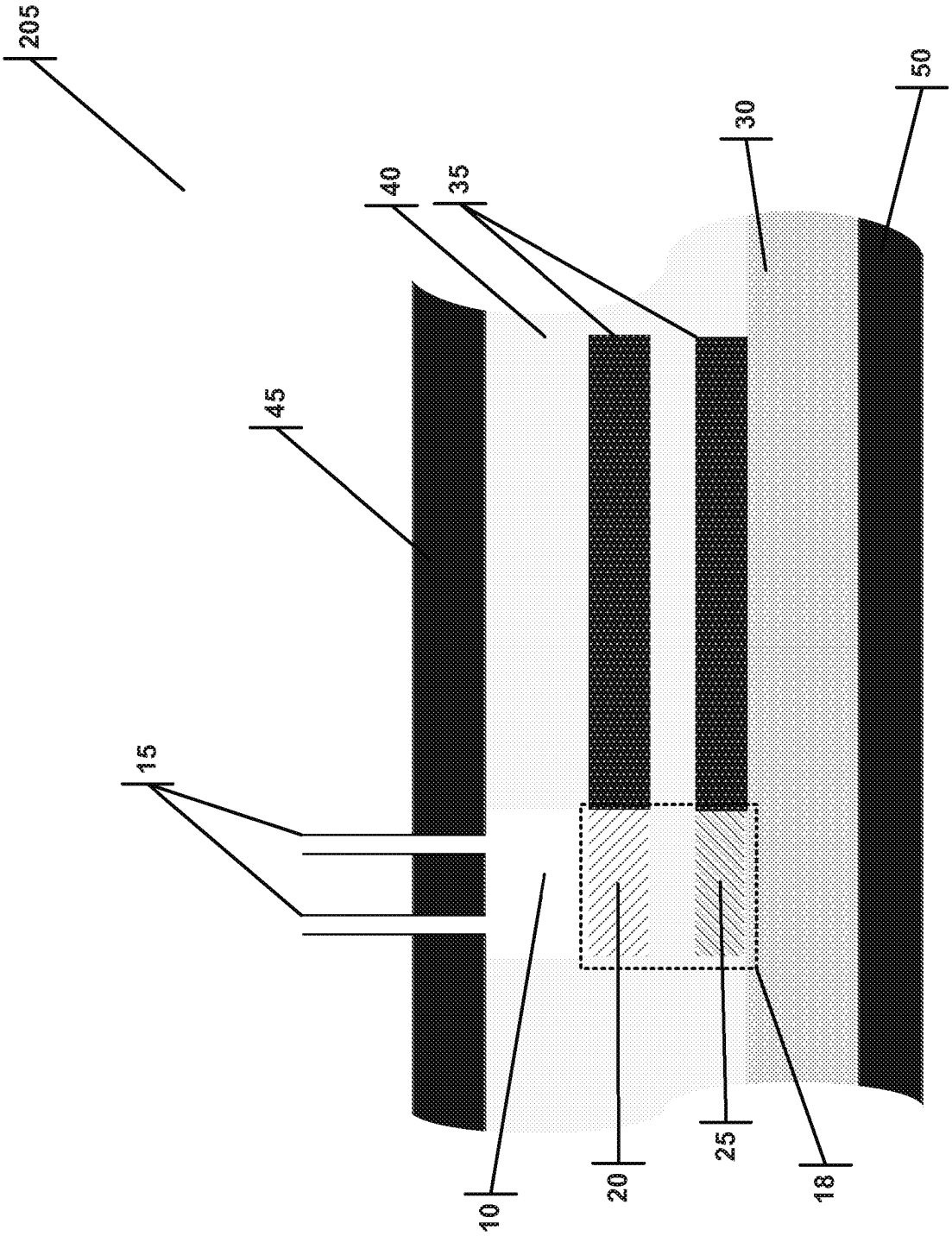

FIG 1A

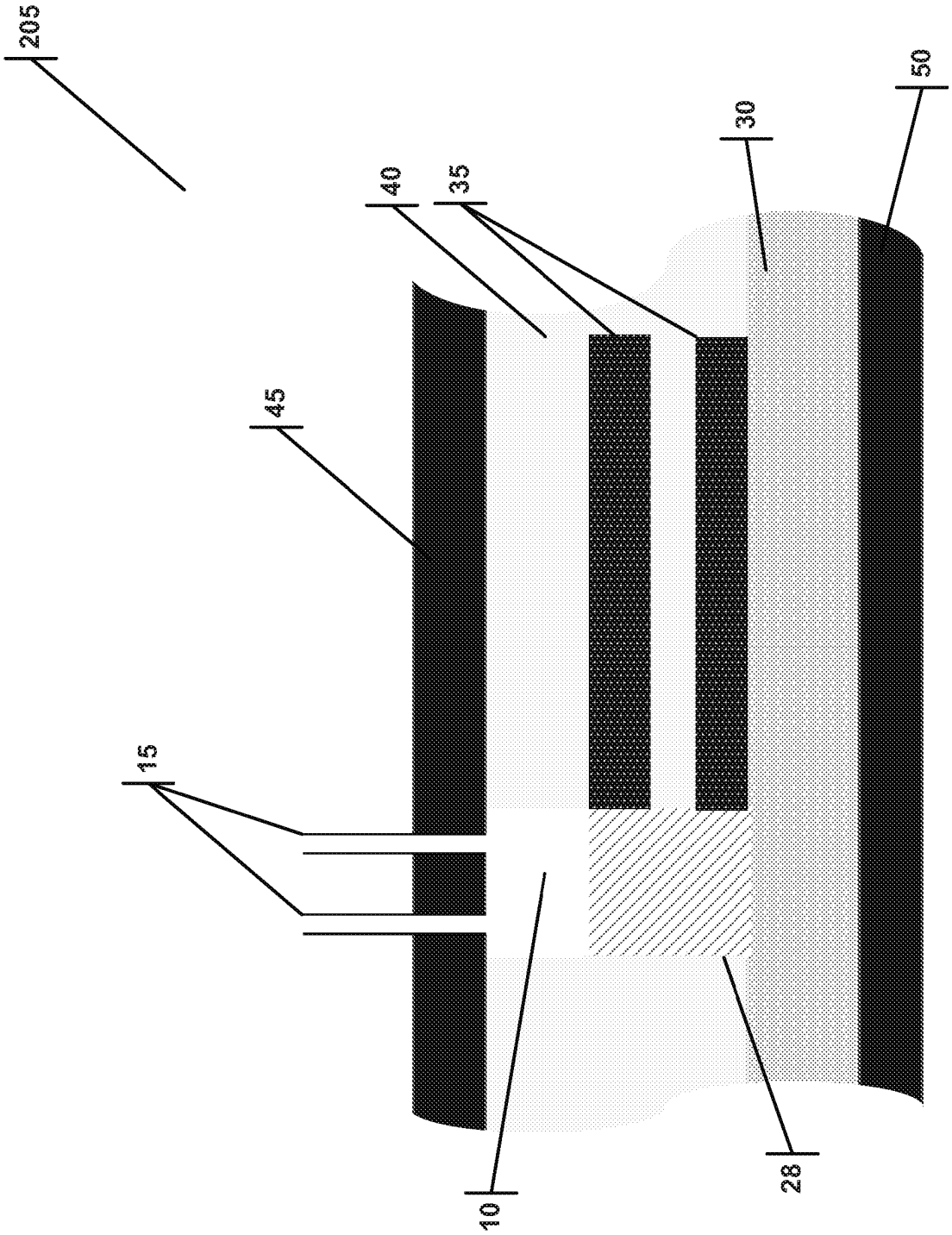

FIG 1B

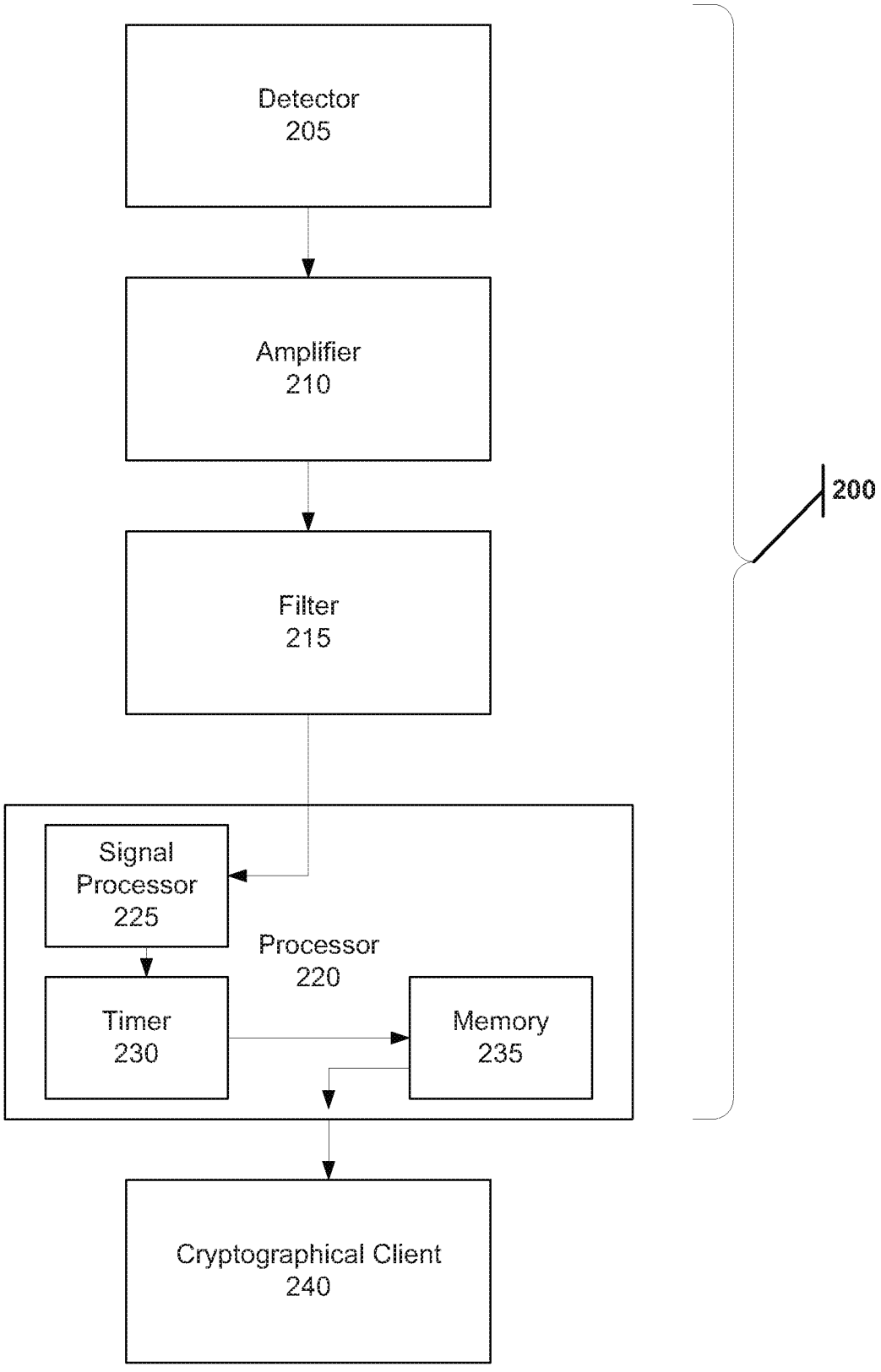
Detector
205
Amplifier
210
Filter
215
Signal
Processor
225
Processor
220
Timer
230
Memory
235
Cryptographical Client
240
200

FIG 2

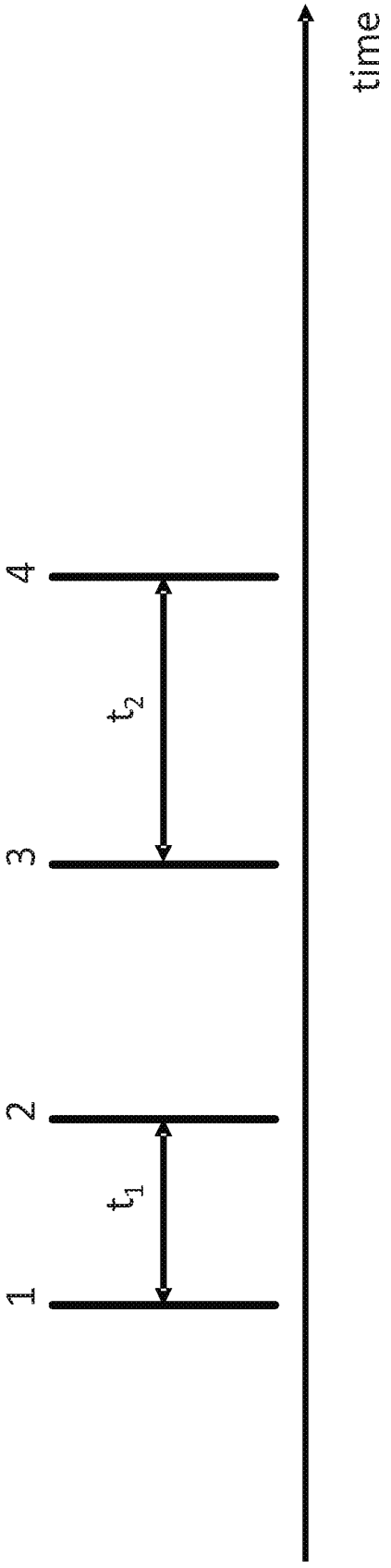

FIG 3A

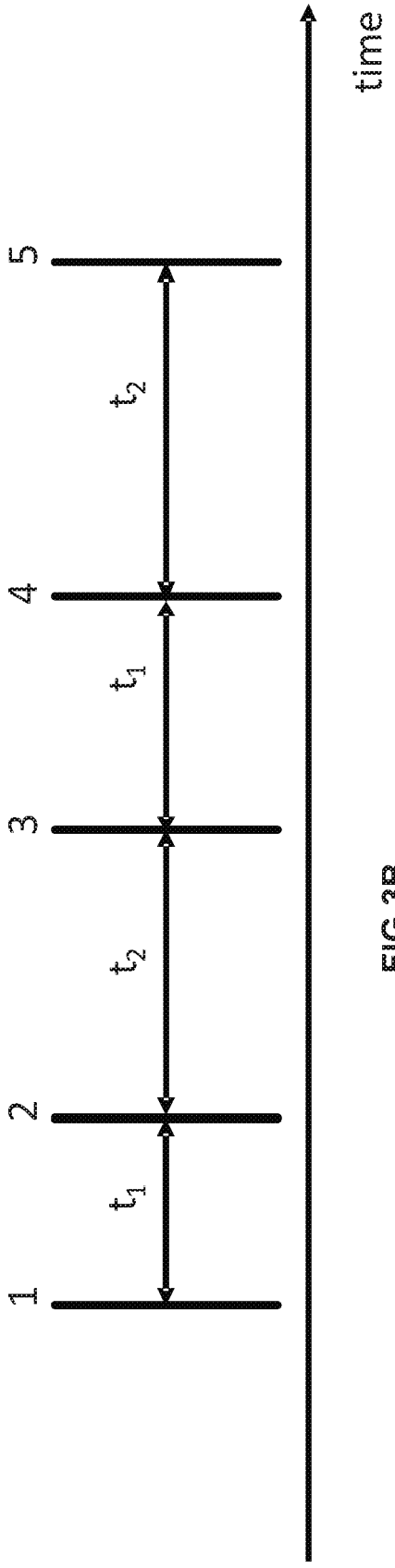

FIG 3B