US 20230221926A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2023/0221926 A1**

Hershman et al. (43) **Pub. Date: Jul. 13, 2023**

(54) **STARVATION-VOLTAGE BASED RANDOM NUMBER GENERATOR**

(71) Applicant: **Nuvoton Technology Corporation**, Hsin-chu (TW)

(72) Inventors: **Ziv Hershman**, Givat Shmuel (IL); **Tamir Golan**, Kibbutz Givat-Chaim Meuchad (IL)

(21) Appl. No.: **17/571,549**

(22) Filed: **Jan. 10, 2022**

Publication Classification

(51) **Int. Cl.**

G06F 7/58 (2006.01)

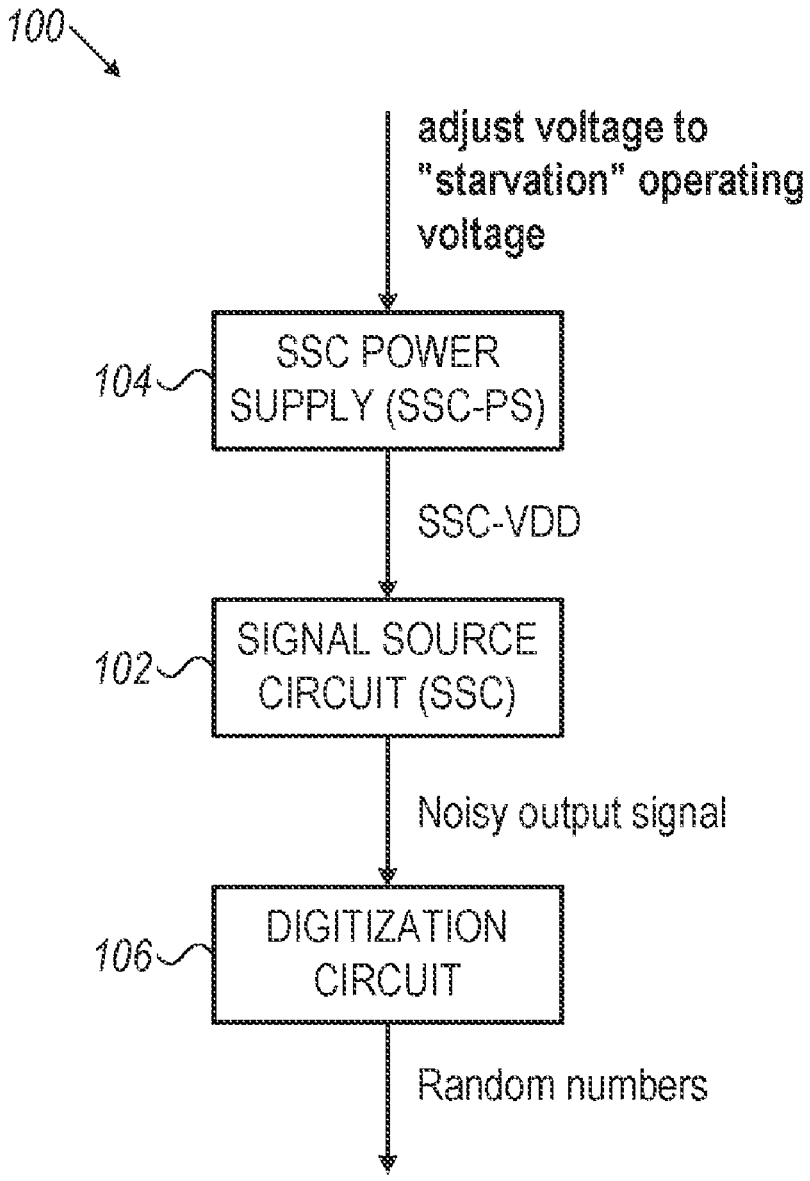
H03K 3/84 (2006.01)

(52) **U.S. Cl.**

CPC ***G06F 7/58*** (2013.01); ***H03K 3/84*** (2013.01)

(57) **ABSTRACT**

An integrated circuit includes signal-source circuitry (SSC), an SSC power supply circuit (SSC-PS) and a digitization circuit. The SSC is configured to generate an output signal, which is guaranteed to meet specified electrical parameters provided that a supply voltage to the SSC is within a specified operating voltage range. The SSC-PS is configured to power the SSC with a reduced voltage that is below the specified operating voltage range, thereby causing the output signal to be noisy. The digitization circuit is configured to digitize the noisy output signal so as to generate a respective sequence of random numbers.



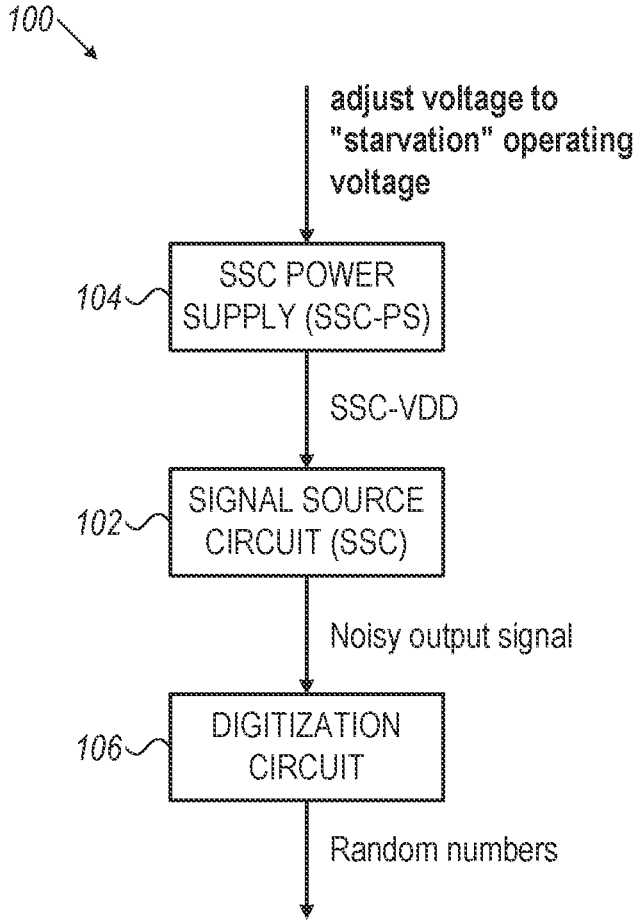

100
adjust voltage to "starvation" operating voltage
104
SSC POWER SUPPLY (SSC-PS)
SSC-VDD
102
SIGNAL SOURCE CIRCUIT (SSC)
Noisy output signal
106
DIGITIZATION CIRCUIT
Random numbers

FIG. 1

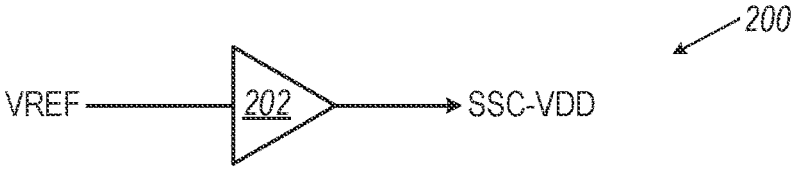


FIG. 2A

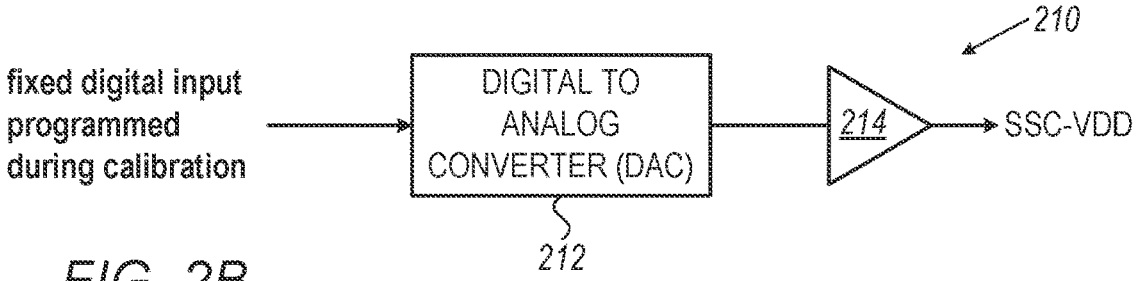


FIG. 2B

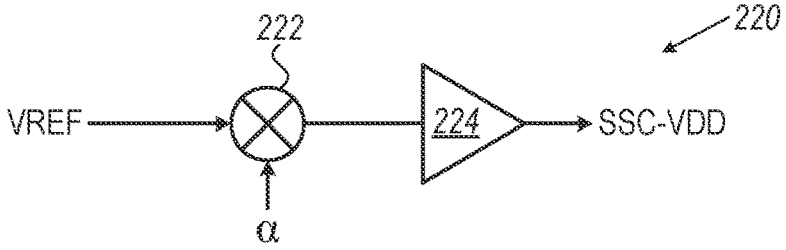


FIG. 2C

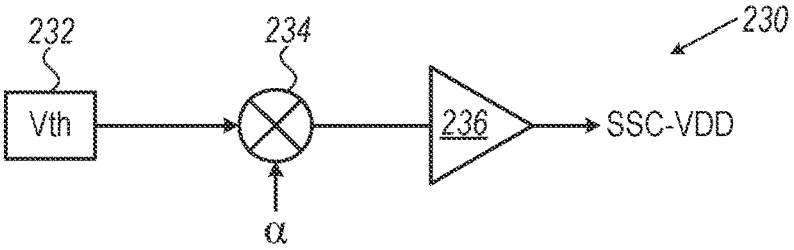


FIG. 2D

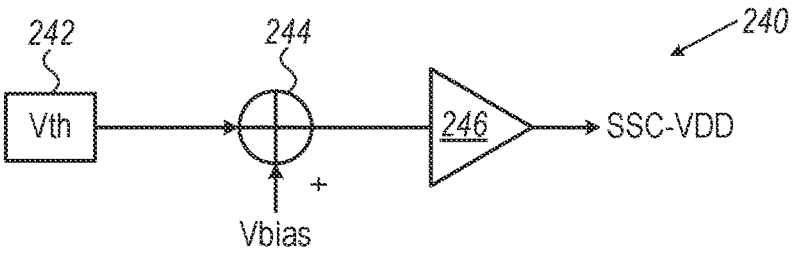


FIG. 2E

FIG. 3

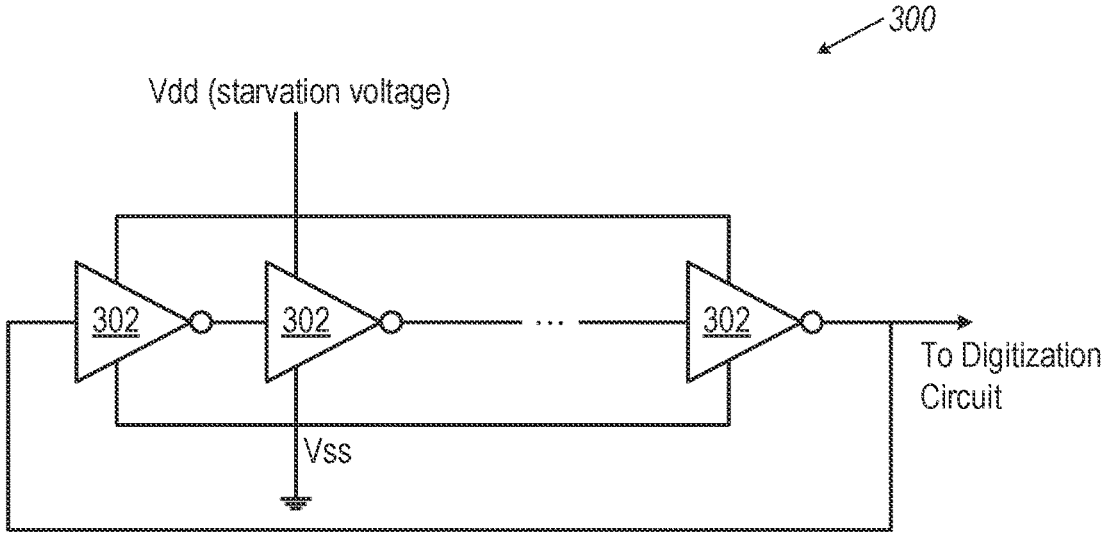
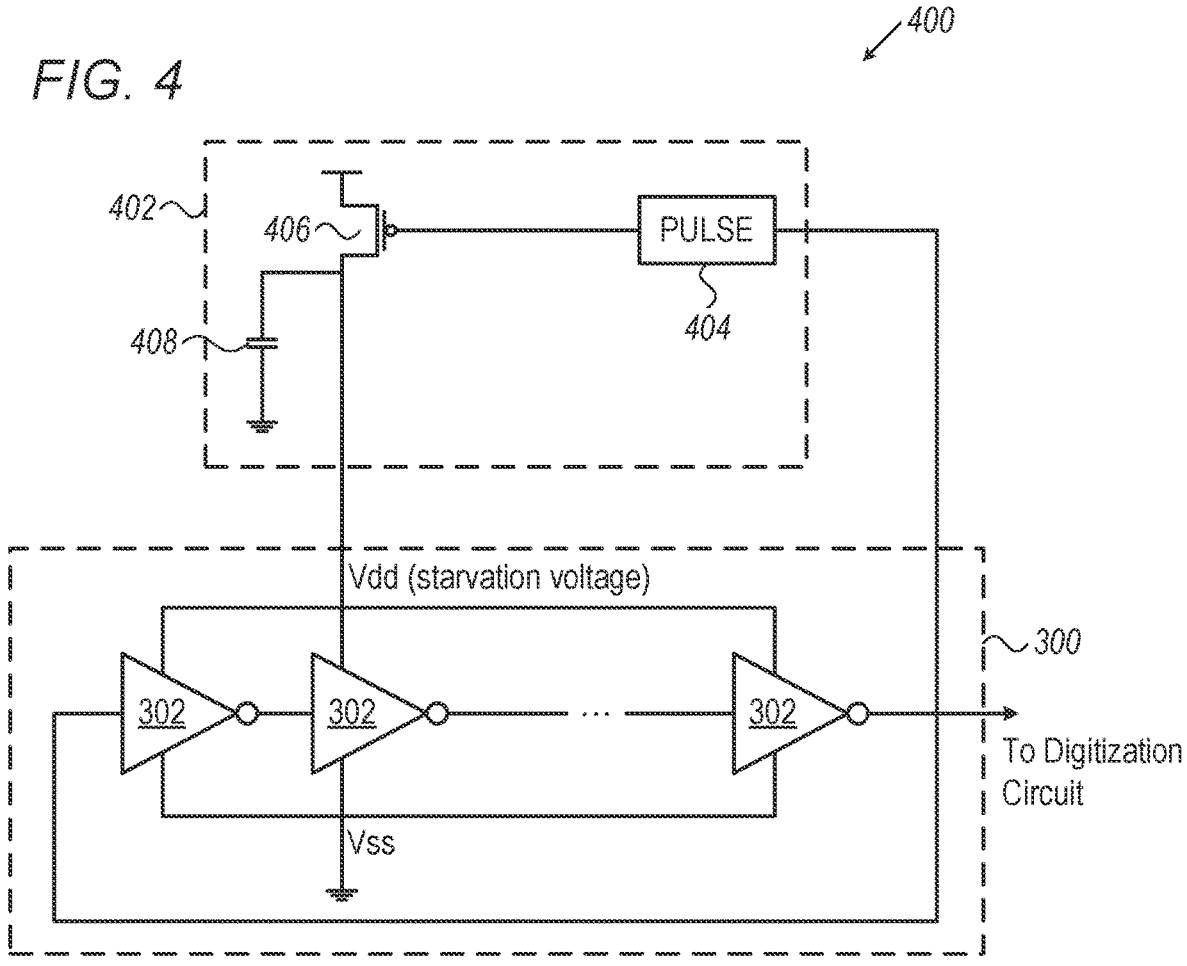

300
Vdd (starvation voltage)
302
302
302
To Digitization Circuit
Vss

FIG. 4


400
402
406
PULSE
404
408
Vdd (starvation voltage)
300
302
302
302
To Digitization Circuit
Vss

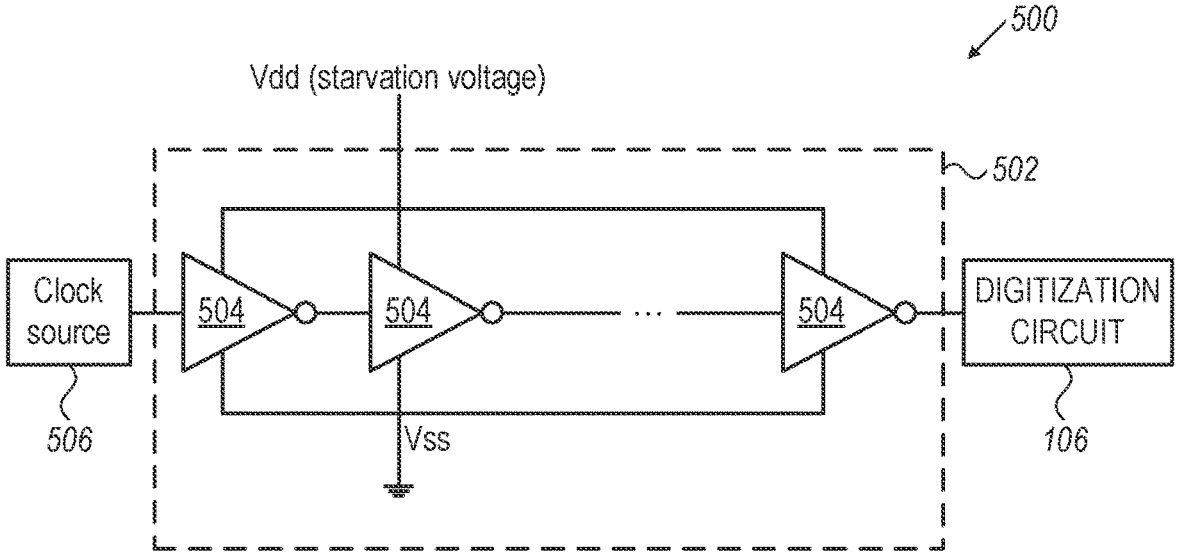


FIG. 5

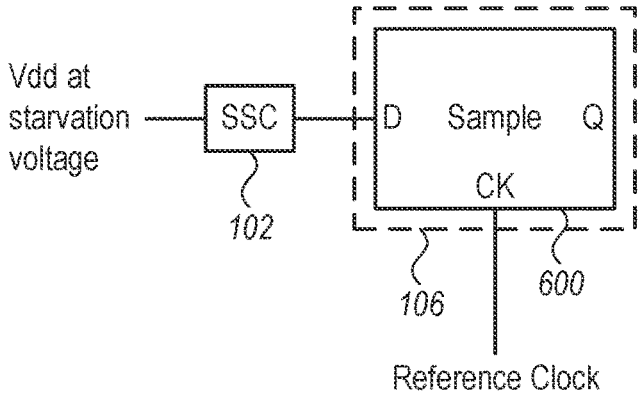


FIG. 6A

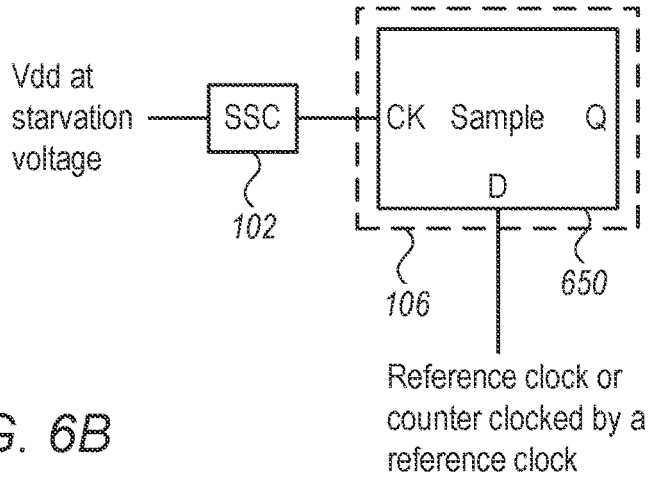


FIG. 6B

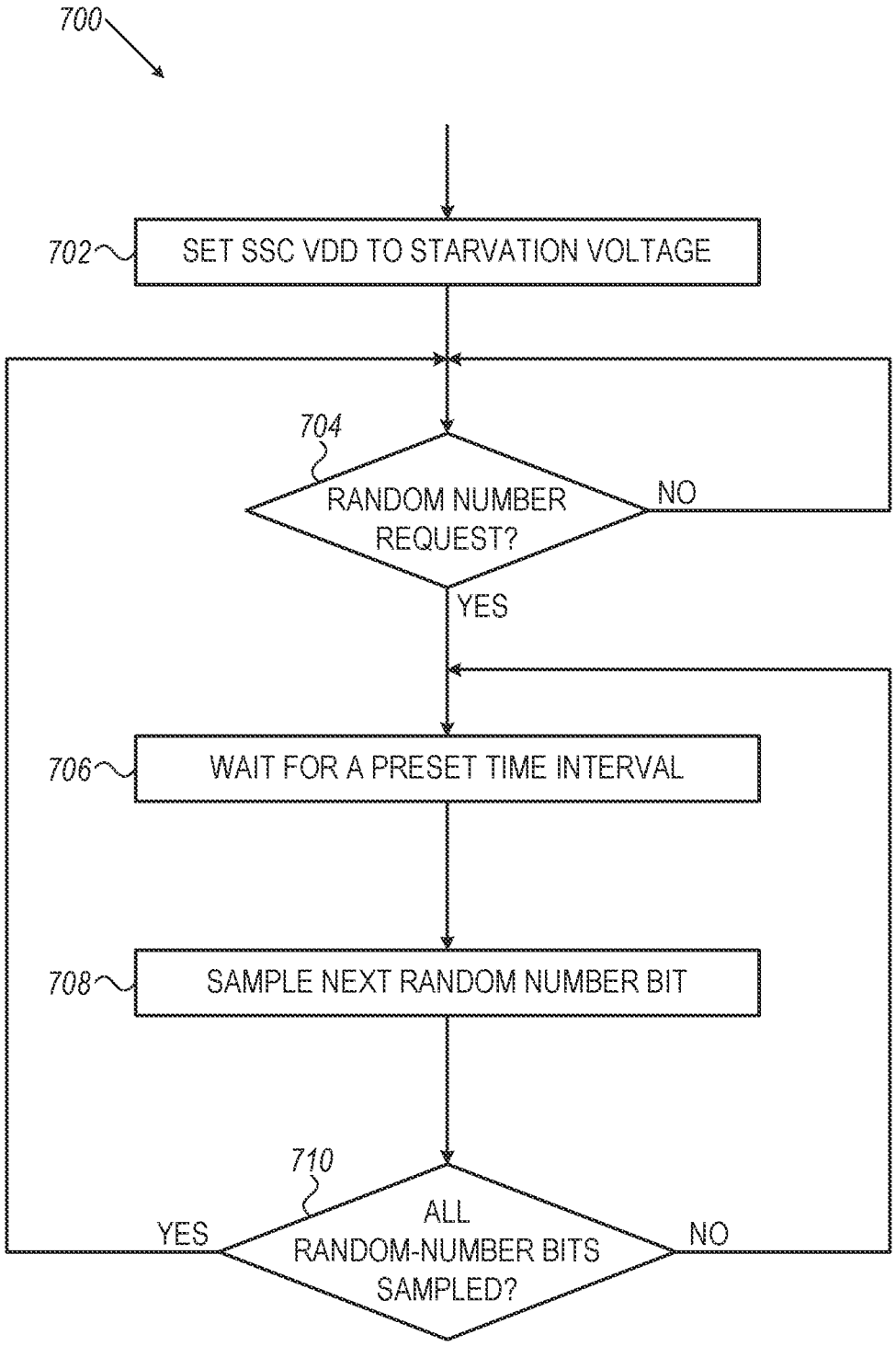

700
702
SET SSC VDD TO STARVATION VOLTAGE
704
RANDOM NUMBER REQUEST?
NO
YES
706
WAIT FOR A PRESET TIME INTERVAL
708
SAMPLE NEXT RANDOM NUMBER BIT
710
ALL RANDOM-NUMBER BITS SAMPLED?
YES
NO

FIG. 7

STARVATION-VOLTAGE BASED RANDOM NUMBER GENERATOR

FIELD OF THE INVENTION

[0001] The present invention relates to integrated circuits, and particularly to methods and apparatuses for hardware generation of random numbers.

BACKGROUND OF THE INVENTION

[0002] In digital systems, generation of random numbers is often required, for example, in the generation of security keys.

[0003] For example, U.S. Pat. No. 9,531,354 describes a random number generator; in some embodiments, the random number generator comprises two cross-coupled inverter chains, wherein each inverter chain comprises an odd number of gates including an input NAND gate; wherein when a clock signal input into the NAND gate of both inverter chains switches from low to high, the inverter chains start toggling until a noise induced phase difference automatically collapses the toggling after a random number of cycles; and wherein a random number generated by the random number generator is based on the random number of cycles.

[0004] U.S. Pat. No. 6,792,438 describes a random number generator comprising random number generation circuitry to generate and output random bits. The random number generator includes interface circuitry to receive and store random bits output by the random number generation circuitry and to output random bits. The interface circuitry prevents outputting the same random bits more than once.

[0005] Lastly, U.S. Pat. No. 8,583,713 describes a physical random number generation device including a physical random number generation source which generates a white noise, an AD conversion module which inputs the white noise for conversion to a physical prime random number as digital data, a physical prime random number sequence generation module which inputs two or more physical prime random numbers to generate a physical prime random number sequence, a white noise array, generation module for inputting the physical prime random number sequence and for generating a white noise array, a white noise composition module for generating multiple physical random numbers from the input white noise array, and an interface for externally outputting the generated physical random numbers as physical random number data. With this arrangement, multiple physical random numbers are generated at high speeds from the physical prime random number(s) taken out of the physical random number generation source as digital data.

SUMMARY OF THE INVENTION

[0006] An embodiment of the present invention that is described herein provides an integrated circuit including signal-source circuitry (SSC), an SSC power supply circuit (SSC-PS) and a digitization circuit. The SSC is configured to generate an output signal, which is guaranteed to meet specified electrical parameters provided that a supply voltage to the SSC is within a specified operating voltage range. The SSC-PS is configured to power the SSC with a reduced voltage that is below the specified operating voltage range, thereby causing the output signal to be noisy. The digitization circuit is configured to digitize the noisy output signal so as to generate a respective sequence of random numbers.

[0007] In some embodiments, the SSC-PS is configured to set the reduced voltage to meet a specified logical functionality of the SSC but to fail meeting one or more electrical parameter specifications of the SSC. In an embodiment, the SSC-PS is configured to connect the SSC power supply to a fixed reduced voltage. In a disclosed embodiment, the SSC-PS is configured to calibrate the reduced voltage.

[0008] In some embodiments, the SSC is an oscillator. In an embodiment, the SSC-PS includes a closed-loop circuit that is configured to adjust the reduced voltage so as to decrease the difference between an oscillation frequency of the oscillator and a preset frequency. In an example embodiment, the SSC includes a chain of at least two buffers. In a disclosed embodiment, the SSC is implemented using one or more logic cells that are drawn from a library, and the reduced voltage is below the operating voltage range specified for the library.

[0009] There is additionally provided, in accordance with an embodiment of the present invention, a method including, using signal-source circuitry (SSC), generating an output signal, which is guaranteed to meet specified electrical parameters provided that a supply voltage to the SSC is within a specified operating voltage range. The SSC is powered with a reduced voltage that is below the specified operating voltage range, thereby causing the output signal to be noisy. The noisy output signal is digitized so as to generate a respective sequence of random numbers.

[0010] The present invention will be more fully understood from the following detailed description of the embodiments thereof, taken together with the drawings in which:

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. **1** is a block diagram that schematically illustrates circuitry for random number generation in an integrated circuit, in accordance with an embodiment of the present invention;

[0012] FIG. **2**A is a block diagram that schematically illustrates a circuit for generating a starvation operating voltage by buffering an external voltage reference, in accordance with an embodiment of the present invention;

[0013] FIG. **2**B is a block diagram that schematically illustrates a circuit for generating a starvation operating voltage using calibration, in accordance with an embodiment of the present invention;

[0014] FIG. **2**C is a block diagram that schematically illustrates a circuit for generating a starvation operating voltage by multiplying an external voltage reference, in accordance with an embodiment of the present invention;

[0015] FIG. **2**D is a block diagram that schematically illustrates a circuit for generating a starvation operating voltage by multiplying a threshold voltage, in accordance with an embodiment of the present invention;

[0016] FIG. **2**E is a block diagram that schematically illustrates a circuit for generating a starvation operating voltage by biasing a transistor threshold voltage, in accordance with an embodiment of the present invention;

[0017] FIG. **3** is a block diagram that schematically illustrates a ring oscillator signal-source circuit (SSC), in accordance with an embodiment of the present invention;

[0018] FIG. **4** is a block diagram that schematically illustrates circuitry for random number generation in an integrated circuit, wherein the SSC is a ring-oscillator, and

wherein the operating voltage is indirectly set by controlling the oscillator frequency, in accordance with an embodiment of the present invention;

[0019] FIG. **5** is a block diagram that schematically illustrates circuitry for random number generation in an integrated circuit, wherein the SSC is a multi-stage buffer, in accordance with an embodiment of the present invention;

[0020] FIG. **6**A is a block diagram that schematically illustrates circuitry for random number generation wherein the digitization circuit samples the SSC output responsively to edges in a clock source, in accordance with an embodiment of the present invention;

[0021] FIG. **6**B is a block diagram that schematically illustrates circuitry for random number generation wherein the digitization circuit samples a reference clock or a counter that is clocked by a reference clock, responsively to edges in the SSC output, in accordance with an embodiment of the present invention; and

[0022] FIG. **7** is a flow chart that schematically illustrates a method for generating random numbers in an integrated circuit, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Overview

[0023] Random numbers are useful in a wide variety of applications, such as security and statistical computations. Often, pseudo-random numbers can be used, such as those generated by a linear-feedback-shift-register; however, in applications like security, such random numbers are sometimes considered a security hazard, and random numbers that are generated by physical phenomena (e.g., thermal noise), are preferred.

[0024] In electrical circuits, thermal noise is generated by electronic components that operate at any temperature greater than absolute-zero; such noise, however, may be weak, and the generation of random numbers from the thermal noise may be tricky.

[0025] Embodiments of the present invention that are disclosed herein provide for improved circuits and methods for the generation of random numbers. The disclosed embodiments utilize a signal source circuit (SSC) that operates at a "starvation" power-supply voltage. Generally, when logic gates operate at a supply voltage that is below a certain threshold, the gate may still perform its designated logic function (e.g., an inverter will still invert the input logic level) but is not guaranteed to meet one or more of its specified electrical parameters (e.g., the propagation delay of the gate may be above a maximum specifications). When a gate is in such low operating voltage, the variations in the propagation delay due to the thermal noise increase.

[0026] In the present context, the term "starvation power-supply voltage" means a power-supply voltage with which a digital logic circuit performs at least some aspects of its designated logic functionality correctly, but is not guaranteed to perform all its designated logic functionality, or to meet one or more of its specified electrical parameters; a circuit with power supply at the starvation voltage will be referred to as a circuit "in starvation".

[0027] The delays that circuits in starvation produce are not random, as they have a bias and a distribution around the bias; however, within a limited timing window that is substantially lower than the distribution variance, the delay values have high entropy and may be considered random.

[0028] In embodiments, the random number generation circuit comprises, in addition to the SSC that is operating at starvation power-supply voltage, a signal-source-power-supply (SSC-PS) that generates the starvation-voltage supply for the SSC, and a digitization circuit that samples the output of the SSC and generates random numbers. (In the context of the present disclosure, digitization circuits usually comprise samplers. We will sometimes refer to "digitization circuit" and "samplers" interchangeably.)

[0029] In some embodiments, the SSC comprises a ring oscillator; the oscillation frequency of the ring oscillator varies, and, if the ring oscillator is in starvation, the variations of the cycle time have high entropy and may be used to generate random numbers. In other embodiments, the SSC comprises a multi-gate buffer, which, when in starvation, adds a high-entropy delay to input edges.

[0030] In an embodiment, the SSC-PS connects the power supply of the SSC to a fixed starvation-voltage source; in some embodiments the starvation voltage may be calibrated. In other embodiments, the SSC-PS comprises an analog multiplier that multiples a reference voltage by a constant to generate the starvation voltage.

[0031] In yet other embodiments, the SSC-PS comprises a self-calibrating circuit that multiplies the threshold voltage (Vth) of the SSC's transistors by a constant. In some embodiments the SSC-PS adds a bias voltage to Vth to generate the starvation voltage.

[0032] In an embodiment, the SSC is a ring-oscillator, and the SSC-PS controls the ring oscillator supply voltage indirectly, by setting the frequency of the ring oscillator to a frequency that corresponds to a power supply at starvation voltage.

[0033] In embodiments, the SSC comprises a multi-stage buffer that buffers a clock source. The delay in the buffer is significantly larger than the cycle time of the clock and hence, if the output of the buffer is sampled with the same clock source, and if the buffer is in starvation, the sampling will yield a series of values which may be considered random.

[0034] Lastly, we disclose two sampler-circuit variants. In one embodiment the sampler samples the output of the SSC with a separate clock source; in another embodiment, the output of the SSC is used as a clock input to a sampler that samples a separate clock.

[0035] Thus, in embodiments, random numbers may be generated by sampling a starved buffer or a starved ring oscillator.

System Description

[0036] The basic building blocks of a Metal-Oxide-Silicon (MOS) integrated circuit are N-MOS and P-MOS transistors. In most cases, however, designers of digital integrated circuits use an off-the-shelf library of basic logic cells such as inverters and gates, wherein each logic cell comprises a plurality of interconnected transistors. The library of basic cells is typically characterized, for any given integrated circuit process technology, to specify a set of electrical parameters and respective operating conditions. The parameters and operating conditions are provided (typically by the silicon manufacturer) to the designers. A typical set of electrical parameters includes (among others), a minimum and a maximum value for the propagation delay of cells with

predefined loads; a typical set of operating conditions includes a power-supply range (e.g., minimum and maximum Vdd) in which the propagation delay is more than the minimum and less than the maximum propagation delay parameters.

[0037] When the operating conditions of the cell are not within the specified operating conditions limits, the cell sometimes continues to be logically functional (e.g., an inverter will still invert its input reliably), but may not meet the specified minimum or maximum electrical parameters. For example, if the supply voltage (Vdd) is set to a level that is slightly lower than the minimum value specified in the operation conditions, the cell will typically function, but the propagation delay may be slower than the specified minimum.

[0038] When the Vdd is further reduced, the propagation delay typically increases, until the Vdd reaches a point where the cell loses functionality.

[0039] The variations in propagation delay as a result of thermal and flicker noise grow when Vdd decreases, mainly because slow rise and fall times enable the accumulation of substantial noise.

[0040] In embodiments according to the present invention, the power supply of cells is set to supply a voltage which is substantially lower than the specified cell library voltage, for which the timing behavior of the cells is less predictable, but the voltage is sufficiently high to guarantee the logical functionality that the cells. When operating at this voltage, cells will be noisy and, subsequently, the cell propagation delay will exhibit high entropy. We will refer to such Vdd operating voltage as a Starvation Operating voltage (or, sometimes, "starvation voltage"); we will refer to cells with Vdd at the starvation operating voltage as cells in starvation. A starvation operating voltage may be chosen from a range of voltage values, referred to as "starvation range" below. When a series of pulses is input to a cell at starvation, the propagation delay values contain a large random component; the accumulated delay of a plurality of cells may be used to generate a high-entropy series of random numbers.

[0041] FIG. **1** is a block diagram that schematically illustrates circuitry **100** for random number generation in an integrated circuit, in accordance with an embodiment of the present invention. Circuitry **100** may be embedded in an integrated circuit, such as an application specific integrated circuit (ASIC) or a field-programmable gate-array (FPGA).

[0042] Circuitry **100** comprises a Noise Source Circuit (SSC) **102**, an SSC power supply (SSC-PS) **104** and a digitization circuit **106**. SSC **102** comprises one or more logic cells, and receives a power supply at the starvation voltage. In some embodiments SSC **102** may be a free-running oscillator; in other embodiments SSC **102** may be a multi-stage buffer that receives the output of an oscillator (not shown) as an input.

[0043] SSC-PS **104** is a voltage source that is configured to output a starvation-voltage power input to SSC **102**. Configurations of SSC-PC **104** according to a variety of example embodiments will be described below, with reference to FIGS. **2**A through **2**E.

[0044] Digitization circuit **106** samples the output of SSC **102**, to produce a series of random numbers. Configurations of digitization circuit **106** according to example embodiments will be described below, with reference to FIGS. **6**A and **6**B.

[0045] As SSC **102** is at starvation, the input-to-output delay of SSC **102** will have high entropy; thus, digitization circuit **106** will generate a series of random numbers.

[0046] The configuration of random number generation circuitry **100** as shown in FIG. **1** and described hereinabove is an example configuration that is cited purely for conceptual clarity. Other configurations may be used in alternative embodiments. For example, in some embodiments a plurality of SSC circuits may be used for the concurrent generation of more than one random number.

Example SSC-PS Configurations

[0047] We next present various embodiments of an SSC-PS circuit **104** (FIG. **1**), that generates the power supply source of SSC **102** within the starvation range.

[0048] FIG. **2**A is a block diagram that schematically illustrates a circuit **200** for generating a starvation operating voltage by the buffering of an external voltage reference, in accordance with an embodiment of the present invention.

[0049] The starvation voltage is supplied by an external voltage reference VREF; in some embodiments VREF may be input to the integrated circuit from an external voltage reference; in other embodiments VREF may be generated within the integrated circuit.

[0050] According to the example embodiment illustrated in FIG. **1**, VREF is input to a unity-gain amplifier **202**, which produces a low-internal-impedance supply voltage, at the starvation voltage, to SSC **102**.

[0051] In some embodiments, the starvation range may vary between same-type devices due to minute changes in the electrical parameters. In embodiments, a starvation voltage may be calibrated—e.g., during device final test. In embodiments, recalibration may be occasionally applied to compensate for device aging.

[0052] FIG. **2**B is a block diagram that schematically illustrates a circuit **210** for generating a starvation operating voltage using calibration, in accordance with an embodiment of the present invention. A digital to analog (DAC) converter **212** converts a digital input to an analog voltage; a unity-gain buffer **214** then produces a low-internal-impedance supply voltage, at the starvation voltage, to SSC **102** (FIG. **1**).

[0053] The digital input to DAC **212** may be set during calibration to generate an output voltage within the starvation range. In some embodiments, the calibration is done by programming a group of fuses. In other embodiments the calibration is done by programming a non-volatile memory. In an embodiment, DAC **212** produces a voltage that is the sum of a fixed bias and the conversion to analog of the digital inputs (this may increase accuracy and/or allow usage of low-resolution DAC). In some embodiments, DAC **212** comprises an analog selector, which is configured to select one of a plurality of input voltage references, e.g., outputs of a resistor ladder.

[0054] FIG. **2**C is a block diagram that schematically illustrates a circuit **220** for generating a starvation operating voltage by multiplying an external voltage reference, in accordance with an embodiment of the present invention. An input reference voltage (from a source within or outside the integrated circuit) is input to an analog multiplier **234** that multiplies VREF by a constant α. The analog multiplier may be, for example, a resistor-ladder, or by an operational

amplifier. A unity-gain buffer **224** then produces a low-internal-impedance starvation supply voltage to SSC **102** (FIG. **1**).

[0055] The main contributor to starvation voltage variations is typically the variation in the transistor's threshold voltage—Vth. In embodiments, such variations may be mitigated by producing a starvation voltage that reflects the actual Vth.

[0056] FIG. **2**D is a block diagram that schematically illustrates a circuit **230** for generating a starvation operating voltage by multiplying a threshold voltage, in accordance with an embodiment of the present invention. A Vth circuit **232** outputs a reference voltage that is equal to the threshold of transistors in the integrated circuit. Vth circuit **232** may be, for example, a reference transistor that conducts a reference current, with its gate connected to its source. In embodiments, the reference transistor is identical to transistors of SSC **102**.

[0057] According to the example embodiment illustrated in FIG. **2**D, an analog multiplier **234** multiplies the voltage output of Vth circuit **232** by a constant α (analog multiplier **234** may be similar or identical to analog multiplier **222**, FIG. **2**C). A unity-gain buffer **236** then produces a low-internal-impedance starvation supply voltage to SSC **102** (FIG. **1**).

[0058] In some embodiments, a bias voltage should be added to Vth, to produce the starvation voltage. FIG. **2**E is a block diagram that schematically illustrates a circuit **240** for generating a starvation operating voltage by biasing a transistor threshold voltage, in accordance with an embodiment of the present invention. A Vth cell **242** (similar or identical to Vth cell **232**, FIG. **2**D) outputs a reference voltage that is equal to the threshold of transistors in the integrated circuit. An analog adder **244** adds a bias voltage Vbias to the output of Vth cell **242**, and a unity-gain buffer **246** outputs a low-internal-impedance starvation supply voltage that is equal to Vth+Vbias, to SSC **102** (FIG. **1**).

[0059] In some embodiments, the multiplication by constant and the addition of biases in circuits **220**, **230** and **240** (FIGS. **2**C, **2**D, and **2**E) can be done using one or more operational amplifiers; see, for example, "Designing Gain and Offset in Thirty Seconds", Texas Instruments Application Report SLOA097, February 2002.

[0060] The configurations of circuits **200**, **210**, **220**, **230** and **240**, illustrated in FIGS. **2**A through **2**E and described hereinabove are examples that are cited merely for the sake of conceptual clarity. Other circuits that produce a starvation-voltage power supply may be used in alternative embodiments. For example, a Vth-based circuit may be fine-tuned during calibration. For another example, a Vth may be both multiplied by a constant and summed with a bias voltage. In an embodiment, a starvation voltage power supply is indirectly controlled, e.g., by adjusting a frequency of an oscillator SSC (an example embodiment of this technique will be described with reference to FIG. **4**).

Example SSC Configurations

[0061] We next present various embodiments of SSC circuit **102** (FIG. **1**).

[0062] FIG. **3** is a block diagram that schematically illustrates a ring oscillator SSC **300**, in accordance with an embodiment of the present invention. The ring oscillator comprises an odd number of daisy-chained inverters **302**, with the output of the last inverter connected to the input of the first inverter. Inverters **302** share a negative (Vss) and a positive (Vdd) power-supply ports; the positive power supply port is set to the starvation voltage by an SSC power supply circuit **104** (FIG. **1**; not shown).

[0063] The configuration of ring oscillator **300**, illustrated in FIG. **3** and described above is cited by way of example. Other configurations may be used in alternative embodiments. For example, in some embodiments, one or more of inverters **302** may be replaced by a gate (e.g., a NOR gate), to facilitate a turn-off input for the oscillator (e.g., to save power when random number generation is not needed).

[0064] In some embodiment, circuit **100** (FIG. **1**) is configured to set the voltage level of the SSC power input in the starvation range indirectly. For example, the oscillation frequency of ring-oscillators is typically a function of the power supply voltage; the starvation range of the ring oscillator power supply corresponds, therefore, to a range of oscillation frequencies.

[0065] FIG. **4** is a block diagram that schematically illustrates circuitry **400** for random number generation in an integrated circuit, wherein the SSC is a ring-oscillator, and wherein the operating voltage is indirectly set by controlling the oscillator frequency, in accordance with an embodiment of the present invention. Circuitry **400** comprises a ring-oscillator SSC **300** (FIG. **3**) and an SSC power supply **402**, which, in turn, comprises a Pulse circuit **404**, a transistor **406** and a capacitor **408**. The output of ring oscillator **300** is coupled to a pulse circuit **404**, which outputs a fixed-width pulse in response to transitions in the outputs of the ring oscillator.

[0066] According to the example embodiment illustrated in FIG. **4**, transistor **406** is a P-type transistor that stops conducting when pulse circuit **404** outputs a pulse (in alternative embodiments, the pulse is negative and transistor **406** is an n-type transistor). Thus, when the frequency of the ring oscillator increases, the duty cycle of the pulses that pulse circuit **404** generates increases, the conduction time of transistor **406** decreases and the Vdd voltage decreases. This negative feedback configuration adjusts the frequency to a preset value, which corresponds to Vdd at the starvation voltage.

[0067] The configuration of circuit **400**, illustrated in FIG. **4** and described hereinabove is an example that is cited merely for the sake of conceptual clarity. Other configurations may be used in alternative embodiments. For example, in an embodiment, circuit **402** controls the voltage level at the drain (rather than the source) of transistor **406** (in which case transistor **406** is an NMOS transistor). In some embodiments transistor **406** may be bipolar.

[0068] FIG. **5** is a block diagram that schematically illustrates circuitry for random number generation in an integrated circuit, wherein the SSC is a multi-stage buffer, in accordance with an embodiment of the present invention. A multi-stage-buffer-type SSC **502** comprises a plurality of cascaded inverters **504**. The input of the first inverter is connected to a clock source **506**, and the output of the last inverter is connected to a digitization circuit **106**. The operating voltage of SSC **502** is within the starvation range.

[0069] Since inverters **504** operate at a starvation voltage supply, the propagation delay within SSC **102** comprises a large random component and varies with large entropy. Therefore, digitization circuit **106**, which samples the output of SSC **502**, receives a series of ones and zeros which may

be considered random. In an embodiment, digitization circuit **106** samples the output of SSC **502** with the same clock source **506**.

[0070] To further increase the entropy, the minimum accumulated delay of inverted **504** is considerably larger than the cycle time of clock source **506**.

[0071] In summary, according to the example embodiment illustrated in FIG. **5** and described hereinabove, a buffer that comprises multiple inverters operating at the starvation voltage delays a clock source by a random time. Digitization circuit **106** is configured to sample the delayed clock source, producing a series of ones and zeroes; the series may be considered random.

Example Digitization Circuit Configurations

[0072] FIG. **6**A is a block diagram that schematically illustrates circuitry for random number generation wherein the digitization circuit samples the SSC output responsively to edges in a clock source, in accordance with an embodiment of the present invention. An SSC **102** (e.g., a ring oscillator **300**, or a multi-stage buffer **502** that is connected to a clock source), with a power supply at the starvation voltage, outputs an oscillating signal to a digitization circuit **106**. The digitization circuit comprises a sampler **600**, and the SSC output signal is connected to the clock input of the sampler. The D input of the sampler is connected to a reference frequency source. Since the delays of the inverters in the ring oscillator at starvation vary (due to the high noise in the inverters), sampler **600** will randomly sample a logic-zero or a logic-one.

[0073] To mitigate metastability, sampler **600** may comprise two or more daisy-chained D-type flip-flops.

[0074] FIG. **6**B is a block diagram that schematically illustrates circuitry for random number generation wherein the digitization circuit samples a reference clock or a counter that is clocked by a reference clock, responsively to edges in the SSC output, in accordance with an embodiment of the present invention. SSC **102** (e.g., a ring oscillator **300**, or a multi-stage buffer **502** that is connected to a clock source), with a power supply at the starvation voltage, outputs an oscillating signal to digitization circuit **106**. The digitization circuit comprises a sampler **650**, which samples the SSC output signal responsive to edges in a clock input of the sampler. Since the delays of the inverters in the ring oscillator vary (due to the high noise in the inverters), sampler **650** will sample a logic-zero or a logic-one in a series that may be considered random.

[0075] The configurations of digitization circuit **106**, illustrated in FIGS. **6**A and **6**B, are cited by way of example. Other configurations may be used in alternative embodiments. For example, in some embodiments, digitization circuit **106** comprises a T-type flip-flop that toggles if the SSC output is at logic one when the clock input toggles.

RNG Method Description

[0076] FIG. **7** is a flowchart **700** that schematically illustrates a method for generating random numbers in an integrated circuit, in accordance with an embodiment of the present invention. The flowchart is executed by random-number-generator circuitry **100** (FIG. **1**).

[0077] The flowchart starts at a set-Vdd-at-starvation stage **702**, wherein an SSC-PS **104** circuit (FIG. **1**) sets the power supply voltage of an SSC circuit **102** to a starvation voltage, which is below the minimum operating voltage range that guarantees that the electrical parameters of the SSC will meet predefined specifications, and yet above the voltage that guarantees functionality. As explained above, when working at this voltage level, the SSC is noisy, and exhibit delays with large random component.

[0078] Next, at a check-random-number-request stage **704**, the random number generation circuitry waits until a random number is needed (for example, request by a processor). If a random number is requested, the random-number-generator circuitry, in a wait-time-interval stage **706**, waits for a preset time interval and then, in a sample-random-bit stage **708**, samples the output of the SSC. Due to the noisy operation of SSC **102** at the starvation voltage, the logic level of the SSC after an uncorrelated time interval is expected to be random. In some embodiments, the random-number generator, in step **704**, uses the SSC output edges to sample a fast-toggling clock or a counter.

[0079] At a check-last-bit stage **710**, the random number generation circuitry checks if all bits of the random number were sampled; if more bits are needed, the random number generation circuitry returns to step **706** to sample the next bit. When the complete number has been sampled (e.g., after **32** iterations of stages **706** and **708** for 32-bit random numbers), the random number generation circuit reenters stage **704** to wait for the next random number generation request.

[0080] The configuration of flowchart **700** illustrated in FIG. **7** and described above is cited by way of example. Other configurations may be used in alternative embodiments. For example, wait stage **706** may be skipped if the sampling frequency is significantly lower than the SSC frequency.

Multiple SSCS

[0081] Embodiments according to the present invention are not limited to a single SSC. In some embodiments, a plurality of SSCs, sampled by one or more digitization circuits, are used. The outputs of the digitization circuits may be combined to a single random output using, for example an exclusive-or (xor) function of the digitization circuits. Such arrangement may, in some embodiments, further increase the entropy of the generated random numbers.

[0082] The configurations of random number generation circuit **100**, including SSC **102**, SSC-PS **104**, digitization circuit **106**, and flowchart **700**, as shown in FIGS. **1** through **7**, and described herein are example configurations and flowchart that are shown purely for the sake of conceptual clarity. Any other suitable system configurations and flowcharts can be used in alternative embodiments. The different elements of random number generation circuit **100** may be implemented using suitable software, using hardware, or using a combination of hardware and software elements.

[0083] It will thus be appreciated that the embodiments described above are cited by way of example, and that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and sub-combinations of the various features described hereinabove, as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description and which are not disclosed in the prior art. Documents incorporated by reference in the present patent

application are to be considered an integral part of the application except that to the extent any terms are defined in these incorporated documents in a manner that conflicts with the definitions made explicitly or implicitly in the present specification, only the definitions in the present specification should be considered.

1. An integrated circuit, comprising:

signal-source circuitry (SSC), configured to generate an output signal, which is guaranteed to meet specified electrical parameters provided that a supply voltage to the SSC is within a specified operating voltage range;

an SSC power supply circuit (SSC-PS), configured to power the SSC with a reduced voltage that is below the specified operating voltage range, thereby causing the output signal to be noisy; and

a digitization circuit, configured to digitize the noisy output signal so as to generate a respective sequence of random numbers.

2. The integrated circuit according to claim **1**, wherein the SSC-PS is configured to set the reduced voltage to meet a specified logical functionality of the SSC, but to fail meeting one or more electrical parameter specifications of the SSC.

3. The integrated circuit according to claim **1**, wherein the SSC-PS is configured to connect the SSC power supply to a fixed reduced voltage.

4. The integrated circuit according to claim **1**, wherein the SSC-PS is configured to calibrate the reduced voltage.

5. The integrated circuit according to claim **1**, wherein the SSC is an oscillator.

6. The integrated circuit according to claim **5**, wherein the SSC-PS comprises a closed-loop circuit that is configured to adjust the reduced voltage so as to decrease the difference between an oscillation frequency of the oscillator and a preset frequency.

7. The integrated circuit according to claim **1**, wherein the SSC comprises a chain of at least two buffers.

8. The integrated circuit according to claim **1**, wherein the SSC is implemented using one or more logic cells that are drawn from a library, and wherein the reduced voltage is below the operating voltage range specified for the library.

9. A method, comprising:

using signal-source circuitry (SSC), generating an output signal, which is guaranteed to meet specified electrical parameters provided that a supply voltage to the SSC is within a specified operating voltage range;

powering the SSC with a reduced voltage that is below the specified operating voltage range, thereby causing the output signal to be noisy; and

digitizing the noisy output signal so as to generate a respective sequence of random numbers.

10. The method according to claim **9**, wherein powering the SSC comprises setting the reduced voltage to meet a specified logical functionality of the SSC, but to fail meeting one or more electrical parameter specifications of the SSC.

11. The method according to claim **9**, wherein powering the SSC comprises connecting the SSC power supply to a fixed reduced voltage.

12. The method according to claim **9**, wherein powering the SSC comprises calibrating the reduced voltage.

13. The method according to claim **9**, wherein the SSC is an oscillator.

14. The method according to claim **13**, wherein powering the SSC comprises adjusting the reduced voltage using a closed-loop circuit, so as to decrease the difference between an oscillation frequency of the oscillator and a preset frequency.

15. The method according to claim **9**, wherein the SSC comprises a chain of at least two buffers.

16. The method according to claim **9**, wherein the SSC is implemented using one or more logic cells that are drawn from a library, and wherein the reduced voltage is below the operating voltage range specified for the library.

* * * * *