

AGING CONTROL OF A SYSTEM ON CHIP

Field of the invention

The present invention relates to security measures implemented in the hardware of systems on chip built on integrated circuits used for example in conditional access systems managing user rights for accessing multimedia content. In particular, aging or reliable operating lifetime time is controlled by hardware devices implemented in the system on chip.

Technical background

The reliability of semiconductor components decreases during operational use. In fact, they are exposed to variable operational constraints such as temperature and voltages. These constraints cause aging effects which are proportional to cumulated stress due to temperature and voltage during operation and varying according to parts more or less involved in a system on chip.

One such aging effect is Hot Carrier Injection (HCI) resulting when charge carriers become trapped within the gate oxide of CMOS (Complementary Metal Oxide Semiconductor) transistors. The trapped charge carriers accumulate over time, creating a built-in charge within the gate oxide of the transistors. This trapped charge decreases the carrier mobility across the channel of the transistors and alters the transistors threshold voltage. The Hot Carrier Injection is aggravated by increasing operating temperatures and voltage, and has a cumulative effect proportional to age.

Another aging effect is Positive Bias Temperature Instability (PBTI) affecting NMOS transistors or Negative Bias Temperature Instability (NBTI) affecting PMOS transistors caused by an electrochemical reaction that involves the electric field, holes, silicon-hydrogen bonds, and temperature. During operation, DC bias voltages generate interface traps between the gate oxide and silicon substrate of a NMOS or PMOS transistor. These interface traps accumulate over time and have the effect of shifting the threshold voltage and reducing drive current and the speed of CMOS transistors.

The HCI and BTI effects may eventually join together and form a conductive path through a gate stack in a process known as Time Dependent Dielectric Breakdown

(TDDDB). For example the document entitled “On-Chip Circuits for Characterizing Transistor Aging Mechanisms in Advanced CMOS Technologies” by John Patrick Keane, University of Minnesota, April 2010, describes in detail the different CMOS transistors aging effects.

- 5 The speed degradation due to transistors aging may be directly measured with on-chip sensors, for example to optimize the circuit clock speed as suggested by recent publications and technology trends, cf. document “Transistor Aging” – IEEE Spectrum of July 2013. Measurement of gate aging may be realized by observing the speed of ring oscillators on any existing electrical path inside a system on chip.
- 10 Accordingly, different internal components of an integrated circuit have varying reliable lifetimes depending on localized environments subjected to localized operational voltages and temperatures and on specific stress history of the circuit component. Components residing in high-use, high-stress environments will have shorter reliable lifetimes.
- 15 In the field of pay-TV, conditional access systems (CAS) or digital rights management (DRM) schemes have as primary goal to warrant that only entitled customers may access media content. A high level of security is usually attained if the rights management at the client side is based on dedicated hardware secure tokens (such as smart cards), which embed private secure multiple-time
- 20 programmable memories such as flash storage.

One feature of CAS systems is to ensure that users actually pay for content they are viewing; a known technique is based on the purchase of credits or “coins” that may be spent over time. An electronic “wallet” containing the coins is usually made up of a file stored on a persistent memory such as flash memory. The electronic wallet may

25 be tied uniquely to a given chip, which embeds a unique identifier (UID), so that users cannot share the credit. The chip UID may be permanently programmed on-chip, and this is generally done with a One-Time Programmable (OTP) memory or fuses.

Fuses may play a central role in design of a system configuration and security. Their

30 implementation in deep-submicron technologies is generally done with expensive

analog semiconductor intellectual property core, (IP core). Moreover, the security of the implementation is left to the IP core provider.

Aging monitoring techniques are described for example by documents US2005/134394A1 and US2014/097856A1.

- 5 Document US2005/134394A1 discloses a method and device to monitor or characterize amounts of transistor degradation, accumulated during the lifetime of a semiconductor device. Pairs of ring oscillators with substantially similar transistor networks or circuits are provided. One of the ring oscillators of the pairs is enabled when the integrated circuits are powered on so that it is under stress during the
- 10 lifetime of the integrated circuit. In one embodiment, an integrated circuit includes one or more functional blocks to perform one or more functions and an integrated on-chip characterization circuit. The integrated on-chip characterization circuit includes a selectively enabled or reference ring oscillator to generate a reference oscillating signal, a free-running ring or pattern driven "aged" oscillator to generate a free-
- 15 running oscillating signal, and a comparison circuit coupled to the selectively enabled ring oscillator and the aged ring oscillator, the comparison circuit to determine a measure of transistor degradation.

- The degradation level output provided by the characterization circuit may be used internal or external to the integrated circuit. Additionally, the collection of data and
- 20 the processing of it may be performed automatically. The integrated circuits while in the field in user systems may pass the transistor degradation information into a central database so that it can be gathered together and evaluated across all integrated circuits in the field. This information can be used to evaluate transistor aging impact to special circuits, critical speed paths and maximum degradation, as
- 25 well as to ascertain the risks and returns associated with using reliability guard bands for an integrated circuit product.

The degradation level measured by the characterization circuit is used for statistic purposes and reliability evaluation without influencing functionalities of devices in the integrated circuit or the global behavior thereof.

- 30 Document US2014/097856A1 discloses a sensor for monitoring aging that changes performance of functional devices in an integrated circuit. The sensor may create

- and characterize dynamic aging stress and/or provide monitoring of aging degradation of a circuit under dynamic voltage scaling and/or dynamic frequency scaling. The aging sensor including a ring oscillator provides information indicating operational degradation of the integrated circuit due to aging. Parameters of a functional device may be controlled by an aging compensation logic which monitors aging information provided by the aging sensor, and determines, based on the aging information, whether a parameter of the functional device should be adjusted to compensate for age induced degradation in performance of the functional device. For example, if the aging compensation logic determines, based on aging information provided by the aging sensor, that timing performance of the functional device, or a portion thereof, is becoming unreliable at a current voltage and/or frequency, then the aging compensation logic may change a parameter of the functional device as for example increase the voltage powering the functional circuitry and/or adjust signal frequency or timing to improve timing performance.
- 15 The role of the aging sensor is to measure a degradation level of functional devices in an integrated circuit in order. The values such as frequency and/or voltage variations are collected by the aging compensation logic further configured to compensate degradation due to the aging by acting on functional parameters in order to maintain the same performances of the integrated circuit as before degradation of one or more devices.
- 20

Summary of the invention

- An aim of the aging control according to embodiments of the invention is to overcome the above mentioned drawbacks of the known concept of fuses implemented in systems on chip requiring high security hardware and software functionalities.
- 25

According to an embodiment, a method to control aging of a system on chip as stated in claim 1 is disclosed.

A system on chip configured to control aging of one or more devices as stated in claim 8 is also disclosed.

The aging may be controlled on devices such as crypto-processors, memory management units, memories, communication interfaces, etc. by monitoring an oscillator circuit which is stressed by commands for varying hardware parameters of the oscillator such as increasing DC supply voltage, setting AC bias voltage, or
5 current in resistor increasing oscillator circuit temperature or a combination thereof. These hardware parameters related to operating conditions of the oscillator affect the signal frequency which decreases proportionally to the operating time and to the stress applied during a given time or periodically.

The oscillator signal frequency is compared with a reference frequency generated for
10 example by an unstressed oscillator in order to determine a difference showing a decrease of the oscillator signal frequency. The frequency difference represents an operating age value of the at least one device associated with the oscillator. If the operating age value equals or exceeds a predetermined threshold age value, a stress state value is determined for example in form of a bit passing from a value 0 to
15 a value 1 or inversely.

The stress state value is monitored in order to determine an age of one or more devices and modify the operating mode of the devices for example by disabling functionalities. In general, several oscillators each associated with one or more devices are stressed in different manners and their individual stress state values may
20 be stored in a memory in form of an array of values indicating a global aging state of the system on chip.

The array of values may be in the form of a string of bits, a table or an array in which each element representing a stress state value is associated with a device of the system on chip. According to an embodiment, a stress state value may be compared
25 with a threshold associated with a device allowing determining if a device is stressed more intensively in relation to other devices. In case, one or more devices show a threshold exceeding, a global behavior of the system on chip may be modified as for example by restricting or disabling one or more functions thereof.

Restricting one or more functions in at least one operating mode of the system on
30 chip may result to at least one or a combination of effects causing a loss of performances such as a processing speed decrease, a lower operating memory

capacity in relation to its nominal capacity, reduction of encryption / decryption capabilities, an earlier expiration date of recorded user rights, etc. The restrictions may also limit system on chip functionalities to a basic operating mode in which a high security level is no more required.

- 5 Disabling one or more functions in at least one operating mode of the system on chip may be induced by stopping operation of one or more devices composing the system on chip. For example, a processor of a decryption device may be stopped or an access to decryption keys or other data related to security stored in a memory may be blocked.
- 10 The aging depends also on the operation mode of the system on chip which devices execute numerous functions going from a stand-by state with negligible or low constraints on the semiconductor components until a high activity rate which leads to stress the oscillator intensively.

15 According to an embodiment, the aging controller may act on other parameters of the electrical signals than the frequency of a ring oscillator, namely timing parameters such as transition time or propagation time of signals produced by the devices of the system on chip. In fact, the aging which decreases oscillator frequency, increases signal propagation time or transition time in relation with a corresponding reference signal.

20 Brief description of the drawings

The following detailed description refers to the attached drawings in which:

Figure 1 shows a diagram of a system on chip according to one embodiment of the invention configured to control aging of various devices by stressing ring oscillators associated thereto.

- 25 Figure 2 shows an example of measured variations of a ring oscillator frequency depending on time and stress caused by over voltage which accelerates the aging.

Figure 3 shows line charts of frequency variations in function of time for a stressed and an unstressed ring oscillator.

Detailed description

According to a preferred configuration, the aging controller is based on ring oscillator RO circuits implemented in the system on chip SOC for measuring the devices aging. A ring oscillator RO circuit comprises at least one inverting element or inverter and a delay element consisting of a buffer, capacitance or an even number of inverters. A well known configuration includes a chain of an odd number of CMOS inverters connected in series where the output of the last inverter is fed back as input of the first inverter forming thus a ring.

A real ring oscillator RO only requires power to operate; above a certain threshold voltage, oscillations begin spontaneously. To increase the frequency of oscillation, two methods are commonly used. Firstly, the applied voltage may be increased; this increases both the frequency of the oscillation and the current consumed. The maximum permissible voltage applied to the circuits limits the speed of a given oscillator. Secondly, a smaller number of inverters in the ring results in a higher frequency of oscillation for a given power consumption. The fundamental frequency F_{osc} at a given supply voltage is calculated by $F_{osc} = 1/(N*T)$ where N represents the number of inverters in the ring and T the time delay for a single inverter.

As the effects of aging impact the switching speed of transistors by rendering them slower, a ring oscillator RO with 10 to 100 MOSFET transistors will see its fundamental frequency slowing with time. The variation with time is thus directly proportional to number of transistors respectively inverters included in the ring oscillator. The variation may be increased by stressing the ring oscillator RO circuit in different ways, such as applying a DC over-voltage, an AC voltage bias, a current increase in a resistor inducing a higher temperature than a normal operating temperature or a combination thereof. The interesting part is that the aging of transistors cannot be reversed.

The documents below describe aging causes and effects observed in CMOS process technology:

[1] "Transistor Aging" – IEEE Spectrum of July 2013

(<http://spectrum.ieee.org/semiconductors/processors/transistor-aging/0>)

[2] Radic: A Standard-Cell-Based Sensor for On-Chip Aging and Flip-Flop Metastability Measurements, Xiaoxiao Wang et al., University of Connecticut (www.engr.uconn.edu/~tehrani/publications/itc-2012-1.pdf)

[3] On-Chip Circuits for Characterizing Transistor Aging Mechanisms in Advanced CMOS Technologies” by John Patrick Keane, University of Minnesota, April 2010 (conservancy.umn.edu/bitstream/123382/1/Keane_umn_0130E_10992.pdf)

[4] ANALYSIS OF IMPACT OF TRANSISTOR AGING EFFECTS ON CLOCK SKEW IN NANO-SCALE CMOS by Mandeep Singh Randhawa, San Francisco State University, California, May 2011 (userwww.sfsu.edu/necrc/files/thesis/thesis_report_Mandeep.pdf)

[5] An On-Chip Test Clock Control Scheme for Circuit Aging Monitoring by Hyunbean Yi, JOURNAL OF SEMICONDUCTOR TECHNOLOGY AND SCIENCE, VOL.13, NO.1, FEBRUARY, 2013 (www.jsts.org/html/journal/journal_files/2013/02/Year2013Volume13_01_11.pdf)

15 There are several causes for gate aging including Hot Carrier Injection (HCI), Bias Temperature Instability (BTI) and Time Dependent Dielectric Breakdown (TDDB) or Oxide Breakdown. All these phenomena contribute to the variation of the threshold voltage of MOS transistors used in a large scale in integrated circuits, and have the global effect of gradually slowing down the gate speed over its lifetime. This slow-
20 down may be directly measured with on-chip sensors, for example to optimize the circuit clock speed as suggested by document [1]. Measurement of gate aging may be realized by observing the speed of ring oscillators. Figure 2 taken from document [3] shows variations in percent (%) of ring oscillator frequency depending on stress time in seconds (s), and when oscillators are stressed with over-voltage. These
25 results verify that BTI is at most weakly dependent on frequency, while HCI degrades with increased switching activity. More switching leads to an increase in current driven through the channels of the device under test, meaning more hot carriers are present. A decrease in the power law exponent (n) of HCI may be observed at higher frequencies, which is apparently due to the quick saturation of degradation in this
30 case. Both aging mechanisms BTI and HCI degrade with voltage and a decrease in HCI's power law exponent (n) at lower voltages may be observed. This has been

explained by a possible decreasing contribution of broken Si-O (Silicon-Oxide) bonds at lower voltages, closer to real operating conditions. The circuit or gate aging measurement may thus be based on any existing electrical path inside a complex system on chip.

5 The system on chip according to one embodiment of the invention represented by the diagram of figure 1 aging of devices D1, D2, D3 is controlled by an aging controller AGC, each device including semiconductor circuit components. The aging controller AGC, generally in form of a hardware device operating with a dedicated software program, addresses commands SI1, SI2, SI3 to the associated ring
10 oscillators RO, i.e. locally connected to each device D1, D2, D3, in order to stress them. These commands act, during a predetermined time or within time periods, on the above mentioned hardware parameters in order to accelerate aging of the ring oscillator corresponding to the aging of the associated device D1, D2, D3.

The system on chip SOC operates within operating modes depending on required
15 functionalities. Most preferably in the example of a pay-TV set top box, the system on chip may be included in a security module involved in data encryption / decryption operations, user rights validity time checking, credit and debit management for content viewing, etc.

The aging of selected devices is accelerated according to their functions by
20 increased stress application through a higher supply voltage in relation to the other devices. Particular commands may thus manage the stress of the ring oscillators associated with the selected devices by increasing their activity rate, power supply voltage or current values contributing also to increase operating temperature. In a stand-by mode of the system on chip, some devices may still fully operate while
25 others are switched off so that devices having, for example, a sophisticated security function will expire faster than the ones having only basic functions.

According to a preferred embodiment, each device D1, D2, D3 may be associated with a specific oscillator circuit called hereafter ring oscillator fuse ROF. The term
"fuse" means that the ring oscillator is capable to modify or disable some features of
30 a device when a given operating age value is reached.

The oscillator circuit, preferably in form of a ring oscillator composed by an odd number N of inverters $IN_1 \dots IN_N$, generates a signal having a frequency F_{osc} during operating of the system on chip SOC. The ring oscillator operates as well as under normal or unstressed operating conditions as under stressed conditions according to the commands SI1, SI2, SI3 received from the aging controller AGC.

A first comparator CP1 compares a value of the F_{osc} with a reference frequency value F_{ref} stored for example in a non-volatile set up memory of the system on chip SOC during an initialization or personalization phase.

The reference frequency F_{ref} may be common to all devices D1, D2, D3 or specific to each device or a predefined group of devices depending on their activity rate.

According to an embodiment, the reference frequency value F_{ref} may correspond to a frequency of a clock signal generated by a reference generator placed inside or outside the system on chip SOC.

When the oscillator signal frequency F_{osc} value differs with the reference frequency value F_{ref} , the first comparator CP1 determines a difference value ΔF corresponding to an operating age of the concerned device D1. Each device D1, D2, D3 of the system on chip SOC may be preferably associated with its own ring oscillator fuse device ROF to enable aging devices selectively. As each device D1, D2, D3 has its specific activity rate, aging effects measured by decrease of the oscillator signal frequency F_{osc} , in relation to the reference frequency F_{ref} , are also device specific.

The operating age value at the output of the first comparator CP1 is compared by a second comparator CP2 with a threshold operating age value TA specific to the device to which the ring oscillator is associated. This threshold operating age value TA is initially stored in a set up memory of the system on chip SOC in a similar way than the reference frequency value F_{ref} according to the concerned embodiment.

Using two comparators has the advantage to allow specific comparisons between different values of reference frequency as well as different values of threshold age according to the functionalities of the different devices composing the system on chip SOC.

If the operating age value is equal or greater than the threshold operating age value TA, the second comparator CP2 outputs for example a binary value 0 or 1 corresponding to a stress state value ST. In a preferred embodiment a stress state value bit set at 1 corresponds to a reached operating age value, i.e. the operating age value represented by ΔF is equal or higher than the threshold age value TA.

According to an embodiment, the frequency difference value ΔF corresponding to an operating age value may be compared to more than one threshold operating age value to provide differentiated stress state values. For example, depending on applied stress, the operating age value reaches a first threshold value TA1 indicated by a first state ST1, then after certain time and stress applied, the operating age value reaches a second threshold value TA2 indicated by a second state ST2, and so on until to a final threshold operating age value TAn. The granularity, i.e. the number of threshold values and the intervals between the threshold operating age values depends on the required information about aging progress in function of device activity rate and applied stress. The operating mode of the concerned device may thus also depend on the different reached threshold age value. In this case, a stress state values table may be established showing the different threshold age value and time period needed to reach them under predefined stress conditions and device operating mode.

String of bits

According to an embodiment, the stress state value associated with each device may form a bit in a string of bits where for example each bit set at 1 corresponds to a reached or exceeded operating age value of said device. In another embodiment, the stress state value may be encoded by a set of bits 0 and 1 and the string results from a concatenation of the sets representing each device stress state value.

Global counter

A counter can be used to determine the general state of the chip. Before a verification process, the counter is initialized. At each device verification, the counter is updated if the age value equals or exceeds a predetermined threshold age value. At the end of the process, the value of the counter represents the number of devices exceeding the threshold showing a global state of the system on chip. Appropriate actions can be taken if the counter reaches a predefined threshold.

Device counter

According to a further embodiment, a counter associated with each device may be updated when an operating age value is reached or exceeded. An update of the counter means that the counter is incremented from a start value (in general set up to zero) or decremented from a predetermined value set up during an initialization or personalization phase of the system on chip. In this case, each stress state value corresponds to the value of the counter which may be used to form a string of values by concatenation as in the string of bits embodiment for example.

Dual thresholds

According to a further embodiment, a threshold stress state value may be attributed to each device. During the comparison with the predetermined threshold age value, the difference between the operating age value and the predetermined threshold age value is stored as a device state stress value. Once all devices are stressed, the array of values represents the behavior of the chip. A further global aging value can be determined for example by summing all stress state values to obtain a global stress state value. The difference of this approach is to give a different weight per device. In the bit approach (see above), each device has the same weight and the global state value is determined according to the number of bits (i.e. device) exceeding the threshold. In the dual threshold approach, in case that a stress state value exceeds the threshold by a high difference, this difference only can trigger the modification of the operating mode.

Example

The table below shows an example with 3 devices D1, D2, D3 having each an individual threshold age value DTA. The current stress state value ST of a current device is compared with this threshold DTA to determine the threshold exceeding value TE. In case that the current stress state value ST is below the threshold DTA, the result TE is set to zero. In the other cases, the result value TE can be further normalized in respect with the device threshold age value DTA to take into account the absolute variation of each threshold DTA. In the example, a threshold exceeding rate TER in percent relatively to the device threshold age value DTA is calculated to allow stress intensity evaluation of each device. The normalized threshold exceeding

value TE therefore produces a value (the threshold exceeding rate TER) which is in the same scale for each device and can be then compared to each other.

The next step is to determine a global stress state value by summing all threshold exceeding rates TER (or calculating an average of the threshold exceeding rates TER). This global stress state value can be then compared with a global threshold value to determine the global stress state of the system on chip.

Devices / system on chip	Device threshold age value DTA	Current stress state value ST	Threshold exceeding value TE	Threshold exceeding rate TER
D1	20	15	0	0
D2	35	40	5	14 %
D3	80	120	40	50 %
Sum (chip)				64 %

The binary values or the string of binary values representing the stress state values of several devices or the global system on chip stress state value may be stored in a secure memory M such as a non volatile memory, a random access memory or a register monitored by the aging controller AGC. These values may be used for cryptographic purposes to form a unique key to perform cryptographic computations that allow for example the chip to acquire rights in a conditional access system.

The ring oscillator fuse ROF of one embodiment of the invention operates according to three operating modes as illustrated by figure 3:

- Off mode: the ring oscillator fuse ROF is inactive for example when the power supply is off
- Read mode: the ring oscillator fuse ROF operates under normal conditions.
- Stress mode: The ring oscillator fuse ROF operates under stress conditions at high temperature or over-voltage for example.

According to figure 3, a nominal initial frequency f_{init} of the oscillator is measured and stored at manufacturing of the chip. The frequency decreases with the time from its

initial value f_{init} according to slopes depending on the stress intensity and time applied on the ring oscillator fuse ROF. The stress thus accelerates the aging as shown by dashed line segments in figure 3. After a given time, the frequency of a stressed ring oscillator fuse ROF becomes significantly lower than the frequency of an unstressed ring oscillator fuse ROF represented by continuous line segments by showing a difference ΔF .

A system on chip may feature several thousand ring oscillator fuses ROF which may be used to determine a large number of data bits indicating the stress status of each devices associated with a ring oscillator fuse ROF. Since ring oscillators may be implemented using standard library cells (elementary CMOS inverters), their integration is seamless and may be freely combined with other available cores.

According to the diagram of figure 1, each device D1, D2, D3 of the system on chip SOC is provided by a ring oscillator fuse ROF1, ROF2, ROF3 respectively which may be stressed individually according to the characteristics of each device D1, D2, D3. A global stress state value may thus be represented by a binary string of three bit with one bit for each device. In the example, a binary string [100] means that the first device D1 has reached the age set by the threshold TA on the second comparator CP2 while the ring oscillator fuses ROF of the other devices D2, D3 have not been stressed sufficiently to reach the threshold age value. The first device D1 may be disabled by the aging controller AGC so that some functionalities of the system on chip may be considered as expired.

The binary value of the string obtained after a certain operating time and stress, corresponding to a global stress state value of the system on chip, may be exploited by a management center or a client support service which may act on the behavior of the apparatus using the system on chip. The global stress state may also be used to determine for example devices stress levels for system or apparatus usage history allowing defining necessity of a hardware and / or software update.

According to an embodiment, the aging controller AGC may control signal timing parameters such as transition time or propagation time of signals produced by a device of the system on chip instead a frequency of a signal generated by an oscillator associated with the device. The transition time of a digital signal

corresponds to the time taken by the signal to pass from a low to a high state or vice versa. The propagation time corresponds to the time taken by a digital signal to flow from a first location in a circuit to a second location, this time being measured as a time shift between the two locations. Beside the decrease of an oscillator frequency, a consequence of the aging of a circuit including semiconductors is an increase of the signal transition time or the signal propagation time in relation with a corresponding reference signal.

In this case, the aging controller stresses devices, during a predetermined time or periodically, by increasing their activity rate with a higher power supply voltage or current for example. Instead of frequency values, the aging controller compares signal timing measured in a stressed device with corresponding timing of a reference signal produced by a device not submitted to stress.

The method and the aging controller as described above are applicable in an efficient way in many kinds of apparatuses wherein expiries of devices or functionalities have to be managed selectively for security purposes.

According to an embodiment of the method of the invention, each device comprises an individual threshold age value DTA, the encoding of each device stress state value comprises steps of:

comparing a current stress state value ST of each device with the threshold age value DTA of said device,

if the current stress state value ST is lower than the threshold age value DTA, setting a threshold exceeding value TE to zero,

if the current stress state value ST is equal or higher than the threshold age value DTA, producing a threshold exceeding value TE,

normalizing the threshold exceeding value TE in respect to the threshold age value DTA to obtain a threshold exceeding rate TER for each device,

determining a global stress state value by calculating a sum or an average value of the threshold exceeding rates TER of each device,

comparing the global stress state value with a global threshold value to determine a global stress state of the system on chip, and modifying the global

behavior of said system on chip if the global stress state value is equal or higher than the global threshold value.

Although embodiments of the present disclosure have been described with reference to specific example embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader scope of these embodiments. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense. The accompanying drawings that form a part hereof, show by way of illustration, and not of limitation, specific embodiments in which the subject matter may be practiced. The embodiments illustrated are described in sufficient detail to enable those skilled in the art to practice the teachings disclosed herein. Other embodiments may be utilized and derived there from, such that structural and logical substitutions and changes may be made without departing from the scope of this disclosure. This Detailed Description, therefore, is not to be taken in a limiting sense, and the scope of various embodiments is defined only by the appended claims, along with the full range of equivalents to which such claims are entitled.

Such embodiments of the inventive subject matter may be referred to herein, individually and/or collectively, by the term "invention" merely for convenience and without intending to voluntarily limit the scope of this application to any single inventive concept if more than one is in fact disclosed. Thus, although specific embodiments have been illustrated and described herein, it should be appreciated that any arrangement calculated to achieve the same purpose may be substituted for the specific embodiments shown. This disclosure is intended to cover any and all adaptations or variations of various embodiments. Combinations of the above embodiments, and other embodiments not specifically described herein, will be apparent to those of skill in the art upon reviewing the above description.

CLAIMS

1. A method to control aging of a system on chip (SOC) comprising one or more devices (D1, D2, D3,...) including semiconductor circuit components and at least one aging controller (AGC) monitoring electrical signals circulating inside the system on chip (SOC), each device having at least one operating mode, the method comprising:

- stressing, by the aging controller (AGC), at least one device (D1, D2, D3,...) of the system on chip (SOC) by varying hardware parameters related to the at least one operating mode of said at least one device (D1, D2, D3,...),
- comparing, by the aging controller (AGC), at least one parameter associated with an electrical signal produced by the at least one device (D1, D2, D3,...) with a reference parameter to determine a difference corresponding to an operating age value of the at least one device (D1, D2, D3,...),
- if the operating age value equals or exceeds a predetermined threshold age value (TA), determining a stress state value (ST),

the method is characterized in that it comprises steps of:

- encoding the stress state value (ST) as a binary value associated with each device (D1, D2, D3,...), and restricting or disabling one or more functions in the at least one operating mode of the system on chip (SOC) according to an array of values formed by one or more binary values.

2. The method according to claim 1, characterized in that the aging controller (AGC) comprises an oscillator circuit (ROF1, ROF2, ROF3,...) associated with at least one device (D1, D2, D3,...), generating a signal having a frequency (F_{osc}) that decreases with the device operating time and applied stress, said frequency (F_{osc}) being compared with a reference frequency (F_{ref}) for determining a difference (ΔF) corresponding to an operating age value of the at least one device.

3. The method according to claim 2, characterized in that the oscillator circuit (ROF1, ROF2, ROF3,...) comprises a ring oscillator made up of a chain including an odd number of CMOS inverters ($IN_1, \dots, IN_N$) connected in series where the output of the last inverter (IN_N) is fed back as input of the first inverter (IN_1).

4. The method according to claim 2 or 3, characterized in that the oscillator circuit (ROF1, ROF2, ROF3,...) is stressed, during a predetermined time or within time periods, with commands (SI1, SI2, SI3,...) managing hardware parameters variations comprising a DC over-voltage, an AC voltage bias, a current increase in a resistor inducing a higher temperature than a normal operating temperature or a combination thereof.
5. The method according to anyone of claim 2 to 4, characterized in that a value of the reference frequency (F_{ref}) is either initially stored in a non-volatile set up memory of the system on chip (SOC) or provided by a clock signal generated by a reference generator, said generator being placed inside or outside the system on chip (SOC).
6. The method according to anyone of claim 1 to 5, characterized in that the array of values forms a binary string representing the stress state values (ST) associated with a set of devices (D1, D2, D3,...), the binary string being stored in a secure memory (M) monitored by the aging controller (AGC) and used to form a unique key to perform cryptographic computations.
7. The method according to claim 1, characterized in that the aging controller (AGC) controls signal timing parameters comprising transition time or propagation time of signals produced by at least one device (D1, D2, D3,...) of the system on chip (SOC), said signal timing parameters increasing with the device operating time and applied stress, said signal timing parameters of a stressed device (D1, D2, D3,...) being compared with a reference signal for determining a difference corresponding to an operating age value of the at least one device (D1, D2, D3,...).
8. A system on chip (SOC) configured to control aging of one or more devices (D1, D2, D3,...) comprising semiconductor circuit components, and at least one aging controller (AGC) configured to monitor electrical signals circulating inside the system on chip (SOC), each device (D1, D2, D3,...) having at least one operating mode, the aging controller (SOC) being further configured to:

stress at least one device (D1, D2, D3,...) of the system on chip (SOC), by varying hardware parameters related to the at least one operating mode of said at least one device (D1, D2, D3,...),

compare at least one parameter associated with an electrical signal produced by the at least one device (D1, D2, D3,...) with a reference parameter to determine a difference corresponding to an operating age value of the at least one device (D1, D2, D3,...),

determine a stress state value (ST) if the operating age value equals or exceeds a predetermined threshold age value (TA),

the system on chip (SOC) is characterized in that the aging controller (AGC) is further configured to:

encode the stress state value (ST) as a binary value associated with each device (D1, D2, D3,...), and restrict or disable one or more functions in the at least one operating mode of the system on chip (SOC) according to an array of values formed by one or more binary values.

9. The system on chip (SOC) according to claim 8, characterized in that the aging controller (AGC) comprises an oscillator circuit (ROF1, ROF2, ROF3,...) associated with at least one device (D1, D2, D3,...) configured to generate a signal having a frequency (F_{osc}) decreasing with the device operating time and applied stress, the aging controller (AGC) being further configured to compare said frequency (F_{osc}) with a reference frequency (F_{ref}) and to determine a difference (ΔF) corresponding to an operating age value of the at least one device associated with at least one device (D1, D2, D3,...).

10. The system on chip (SOC) according to claim 9, characterized in that the oscillator circuit (ROF1, ROF2, ROF3,...) comprises a ring oscillator made up of a chain including an odd number of CMOS inverters ($IN_1, \dots, IN_N$) connected in series where the output of the last inverter (IN_N) is fed back as input of the first inverter (IN_1).

11. The system on chip (SOC) according to claim 9 or 10, characterized in that the stress of the oscillator circuit (ROF1, ROF2, ROF3,...) includes commands (SI1, SI2, SI3,...) acting, during a predetermined time or within time periods, on hardware parameters variations comprising a DC over-voltage, an AC voltage bias, a current

increase in a resistor inducing a higher temperature than a normal operating temperature or a combination thereof.

12. The system on chip (SOC) according to anyone of claim 9 to 11, characterized in that a value of the reference frequency (F_{ref}) is initially stored in a non-volatile set up memory of the system on chip (SOC) or provided by a clock signal generated by a reference generator placed inside or outside the system on chip (SOC).

13. The system on chip (SOC) according to anyone of claim 9 to 12, characterized in that the array of values forms a binary string representing the stress state values (ST) associated with a set of devices (D1, D2, D3,...), the binary string, being stored in a secure memory (M) monitored by the aging controller (AGC), is configured to be used as a unique key to perform cryptographic computations.

14. The system on chip according to claim 8, characterized in that the aging controller (AGC) is configured to control signal timing parameters comprising transition time or propagation time of signals produced by at least one device (D1, D2, D3,...) of the system on chip (SOC), said signal timing parameters increasing with the device operating time and stress applied during a predetermined time or within time periods, the aging controller (AGC) being further configured to compare signal timing parameters of a stressed device (D1, D2, D3,...) with the signal timing parameters of a reference signal and determine a difference corresponding to an operating age value of the at least one device (D1, D2, D3,...).

15. The system on chip according to claim 10, characterized in that the aging controller (AGC) further comprises:

- an input interface configured to receive stressing commands (SI1, SI2, SI3,...) acting on hardware parameters related at least one operating mode of the ring oscillator circuit (ROF1, ROF2, ROF3,...),
- a first comparator (CP1) configured to compare the signal frequency (F_{osc}) with a reference frequency (F_{ref}) and to determine a difference (ΔF) showing a decrease of the signal frequency (F_{osc}) corresponding to an operating age value of the ring oscillator (ROF1, ROF2, ROF3,...),

- a second comparator (CP2) configured to compare the operating age value with a threshold age value (TA) and to output a stress state value (ST).