EM-Based On-Chip Aging Sensor for Detection of Recycled ICs

Kai He, Xin Huang, and Sheldon X.-D. Tan
University of California

Editor's notes:
Counterfeiting integrated circuits (ICs), especially recycled ICs, have become a major security threat for commercial and military systems. This paper proposes a new lightweight on-chip aging sensor, which is based on electromigration-induced aging effects for fast detection and prevention of recycled ICs. Compared to other existing aging sensors, the proposed sensor can provide more accurate prediction of the chip usage time with smaller area footprints, as demonstrated by the statistical simulation results presented in the article.

—Xin Li, Carnegie Mellon University

■ **The counterfeiting and** recycling of integrated circuits (ICs) have become major problems in recent years, potentially impacting the security of electronic systems, especially for military, aerospace, medical, and other critical applications. In addition to diminishing system dependability and usability, counterfeiting reduces the total revenue of companies from their research and development efforts, discourages innovation through the theft of intellectual properties (IPs), and produces low-quality products under established brand names [2]. A counterfeit component is defined as an electronic part that is not genuine because it is an unauthorized copy; it does not conform to the original component manufacturer's (OCM) design, model, and/or performance; or it is not produced by the original component manufacturer or is produced by unauthorized contractors; it is an off-specification, defective, or used OCM product sold as "new" or working; it has incorrect or false markings and/or documentation.

Today the most widely reported type of counterfeit parts is the recycled type. It is reported that in today's supply chain, more than 80% of the counterfeit components are recycled [3]. These used or defective ICs enter the market when electronic "recyclers" divert scrapped circuit boards away from their designated place of disposal for the purposes of removing and reselling the ICs on those boards. The recycling process involves removing ICs from the board or even dies in the ICs. There are several security issues associated with these ICs. First, a used IC can act as a ticking time bomb [4] since it does not meet the specification of the OCM of the ICs; second, additional die on top of the recovered die can carry a back-door attack, sabotage circuit functionality under certain conditions, or cause a denial of service.

The detection methods for recycled chips can be classified into physical methods and electrical methods [2]. Physical methods consist of incoming inspection methods such as visual inspection, X-ray imaging, package analysis method such as laser scanning microscopy, delid method, and the material analysis method such as using Fourier transform infrared, and X-ray fluorescence. Electrical methods contain the parameter tests, function

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/MDAT.2016.2582830
Date of publication: 21 June 2016; date of current version: 19 August 2016.

2168-2356/16 © 2016 IEEE Copublished by the IEEE CEDA, IEEE CASS, IEEE SSCS, and TTTC

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 07:47:19 UTC from IEEE Xplore. Restrictions apply.

tests, built-in tests, and structural tests. In general, physical methods can be applied to all part types, but some of the methods are destructive and take hours to test. As a result, sampling is required to certify a batch of parts by observing a small number of parts. On the other hand, conventional electrical test methods are nondestructive and time efficient, yet they can be very expensive because such techniques are not necessarily designed for counterfeit detection. Electrical test techniques are advantageous because the sampling is not required, and all parts can be tested. However, there are some issues associated with electrical tests that must be addressed.

In order to detect and prevent counterfeit chip, one viable approach is to insert a lightweight detecting sensor. In [5], a temperature sensor is used to detect the chip defect. There are also some early efforts for telling the usage of chips [6]. Method in [6] designed the ring-oscillator-based (OR-based) aging sensor that relies on the aging effects of MOSFETs to change a ring oscillator frequency in comparison with the reference one embedded in the chip. As the chip ages owing to the wearout mechanisms such as negative biased temperature instability (NBTI) and hot carrier injection (HCI), the shift threshold voltage of MOSFET devices, thus the frequency of ring oscillator, indicates the level of aging, and provides a simple readout of the value. However, this method can only give very rough estimation of the usage age of the chip as the shift of the frequency depends on many factors. In order to mitigate this problem, the antifuse-based (AF-based) sensor was developed in [2]. The AF-based sensor essentially is a counter, which counts the clocks or derivatives of the clock events to log the usage of the chip. The antifuse memory is used to make sure the data in the count will not be erased or altered by attackers. However, the AF-based sensors suffer large area overhead especially when more accurate usage is required [2]. Another problem with this method is that it may not reflect the true aging-dependent usage of a chip. For instance, it will log the same usage time for a chip for different on-chip temperatures, however, which can have dramatic impacts on the aging effects from electromigration, NBTI, and HCI [7].

In this article, we propose a new lightweight on-chip aging sensor, which is based on the electromigration-induced aging effects for fast detection and prevention of recycled ICs. The new aging sensor has the following new features and new contributions.

1) Instead of using traditional aging effects from devices (such as MOSFETs), the new EM-based aging sensor exploits the natural aging/failure mechanism of interconnect wires to time the aging of the chip. As a result, compared with the existing ring-oscillator-based aging sensor, the structure of the new sensor is much simpler as it only requires metal interconnect wires, which was driven by direct current (dc). In comparison, the ring oscillator has to be used to detect the threshold voltage shift.
2) It is more accurate as we can measure the EM-induced failure (such as wire resistance changes) time with more accurate than the frequency shift over time. The new sensor is based on a newly proposed hydrostatic stress evolution model of EM effects for accurate prediction of the EM failure [8], [9]. As a result, we can design the interconnect wire structures based on the copper interconnect technology so that the resulting wires can have detectable EM failure at a specific time with sufficient accuracy. The aging sensor can also be used as the on-chip timer for timed services for some chip level or system functions.
3) In order to mitigate the problem of the inherent variations in the metal grain sizes and assess its impacts on the nucleation time of metal wires, a number of parallel properly structured wires are employed in the sensor. The parameters of the wires are optimized with using the new EM model.

Our numerical results show that the proposed aging sensor can accurately predict the targeted failure times in the presence of both inherent uncertainties. Our study also shows that more parallel wires will lead to more accurate statistical predictions at the cost of bigger area.

This article is organized as follows. Review of EM effects and EM models reviews the EM effect and recently proposed physics-based EM model. In Proposed EM-based aging sensor circuit, we present the new lightweight on-chip

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 07:47:19 UTC from IEEE Xplore. Restrictions apply.

aging sensor circuit as well as the interconnect wire structures. Several statistical analyses are presented in Performance analysis and experimental results.

Review of EM effects and EM models

The proposed on-chip aging sensor is based on the observation that the EM-induced failure of interconnect wires can be designed such that the wires can fail at a specific time frame detected by the increase of their resistances over a predefined threshold. EM is a physical phenomenon of the migration of metal atoms along a direction of the applied electrical field. Atoms (either lattice atoms or defects/impurities) migrate toward the anode end of the metal wire along the trajectory of conducting electrons. This oriented atomic flow, which is caused mostly by the momentum exchange between atoms and the conducting electrons, results in metal density depletion at the cathode, and a corresponding metal accumulation at the anode ends of the metal wire. This depletion and accumulation happen because atoms cannot easily escape the metal volume.

Over time, the lasting unidirectional electrical load increases these stresses, as well as the stress gradient along the metal line. In some cases, usually when a line is long, this stress can reach a critical level, resulting in void nucleation at the cathode and/or hillock formation at the anode end of the line. Different physical mechanisms can be responsible for generating these damages. In the case of voiding, existing cohesive or interfacial microcracks near or at the barrier/Cu interfaces can develop into a void by the action of the appropriate stresses. Hillock formation, which is a compression-induced extrusion of metal into the surrounding dielectric that can cause a shortage between neighboring metal lines, can be initiated by microcracks in the adhesion/barrier layers. However, typically the voids are the major defects from EM.

One important observation of EM effects is that the time to failure (TTF) of a wire show some degree of randomness. This TTF represents the instant in time when an increase in line electrical resistance caused by the void growth reaches a critical level (for example, a 10% increase over the original value). The reason is that the grain boundaries (GB) of metal wires has random sizes and orientations, which lead to variations in the atomic diffusivities. Actually, the EM-induced TTF follows the lognormal distribution [10]. This inherent uncertainty in TTF is one of the challenges to designing accurate aging sensor.

Traditionally the EM effects are modeled by the semi-empirical Black's equation. However, Black's equation suffers from several problems for accurate TTF estimation. The major drawback of this model is that it fails to consider impacts of wire length and residual stresses.

Recently, a more accurate and physics-based EM model has been proposed [10], [11]. In this model, the EM kinetics consists of two phases: 1) the void nucleation phase and 2) the void growth phase. The TTF for the void nucleation phase and the resistance change over time in the void growth phases can be computed in analytic forms as proposed in [9].

Proposed EM-based aging sensor circuit

Wire structure for accurate EM-induced aging detection

In the section, we investigate the new wire structures so that we can have more accurate detection of the EM induced resistance changes based on the new physics-based EM models. There are several factors we need to consider to design the right interconnect wire structures as the critical component of the aging sensors. First, there are the inherent variations in the metal wires, which will lead to the uncertainties in the nucleation time and the growth time. For a metal wire, its GBs may have different crystallographic orientations, which are characterized by different atomic diffusivities. Second, the grain sizes have a random distribution. As a result, the lifetime of the metal wires obeys the lognormal distributions [10]. Hence, we cannot use only one metal wire as the aging sensor. Third, how to design the geometry of the wires (length and width) to have a small area and power overhead for the sensors. We want the sensors to have a small footprint with considering their power consumptions and areas. In addition, they will meet the design rules, which are compatible with given design technologies. Fourth, we need to have an accurate estimation of the residual stresses σ_{Res}

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 07:47:19 UTC from IEEE Xplore. Restrictions apply.

(mainly the thermal stresses), which largely depend on the temperature of the manufacturing process and even the packaging process.

In order to mitigate the inherent uncertainties in the atomic diffusivities in a metal line, one solution is to use a number of wires connected in parallel, as shown in Figure 1a, in which each wire will have its own diffusion barriers at both ends (so they are treated as individual wires in the EM sense). However, they are connected in parallel by another metal layer through vias. The color in the figure shows the simulated stress distributions in each wire. Those wires will be stressed all the time (with constant current running through them). We can design the wires such that they will fail at a specific time such as one year, two years, ..., or n years. Assume that the resistance value of the stressed wire at $t = 0$ is r_0. The failure time can be defined as the time when the wire resistance increases 10% of its values, i.e., $1.1 * r_0$, which can be predicted by the physics-based EM model. We also need to design a *reference* wire, which is not normally stressed (unless its resistance value is read during the detection time). The resistance value of the reference wire should be set to $1.1 * r_0/k$, where k is the number of wires in the stressed wire set. For the reference wire, we only need one wire segment as it will not age (the uncertainties in the EM-induced aging will not affect it). Our preliminary study shows that depending on the inherent variations, we can determine the number of wires such that we can confine the lifetime variations to a sufficiently small range. The exact number wires used will be explored and validated by the actual silicon data. We remark that the intradie process variations will affect the resistance values of those wires. However, if they are placed very closely, as this should be the case, the impact will not be significant.

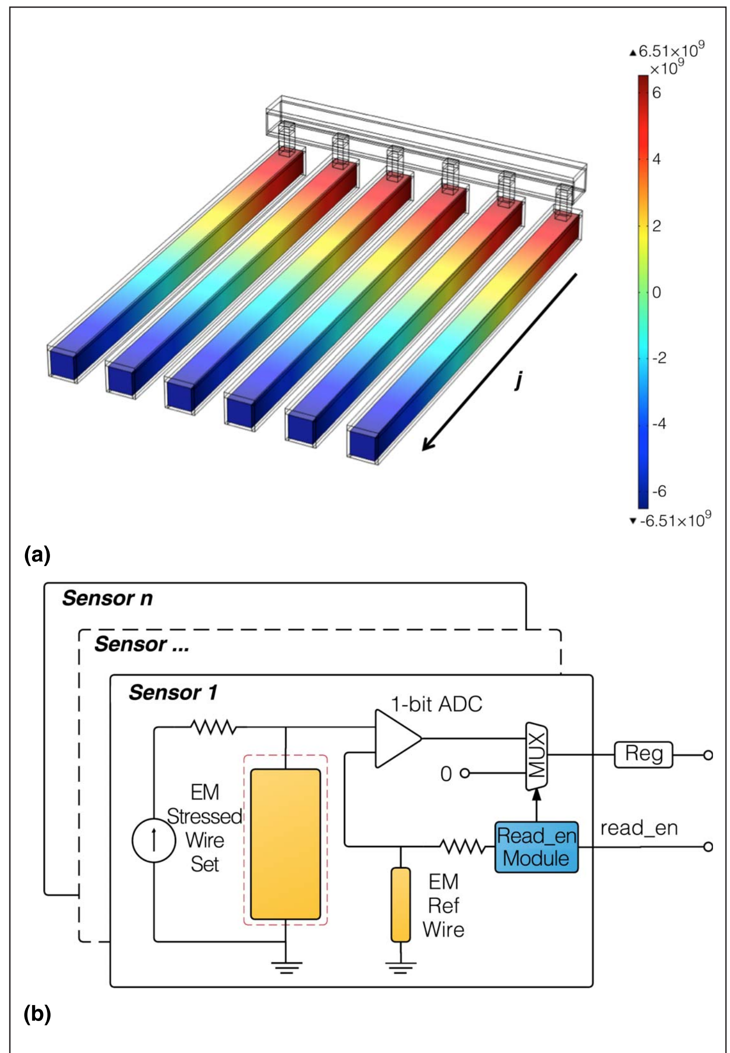

Figure 1. The structure of EM-based aging sensor. (a) The multiwire structure for the aging sensor and its stressed condition. (b) The circuit of the EM-based aging sensor.

Resistance detection sensor circuit

Figure 1b shows the schematic of the proposed EM-based aging sensor circuit. The circuit is composed of a constant current source, an EM stressed parallel wire (EMS) set, an EM reference wire (EMR), which will not be stressed in normal operation, a one-bit ADC (essentially an op-amp circuit), two resistors, one multiplex (MUX), one read_en module and one register to store the sensor digital output. The EMS contains a number of parallel wires (such as six in our initial analysis) with identical geometries. The EMR is just a single wire. The constant current source provides the current to stress EMS when the power is on. The one-bit ADC is used as a comparator to decide if the stressed EMS has a larger resistance than the EMR. If the voltage on EMS is higher than the voltage on EMR, it outputs 1, which indicates that the failure happens, otherwise 0, which indicates that the failure has not happened yet. The MUX and the switch are controlled by the *Read_en* signal from outside. When *Read_en* is off, the output of one-bit ADC will not be read into the register and there is no current on EMR as it is in an open circuit. When

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 07:47:19 UTC from IEEE Xplore. Restrictions apply.

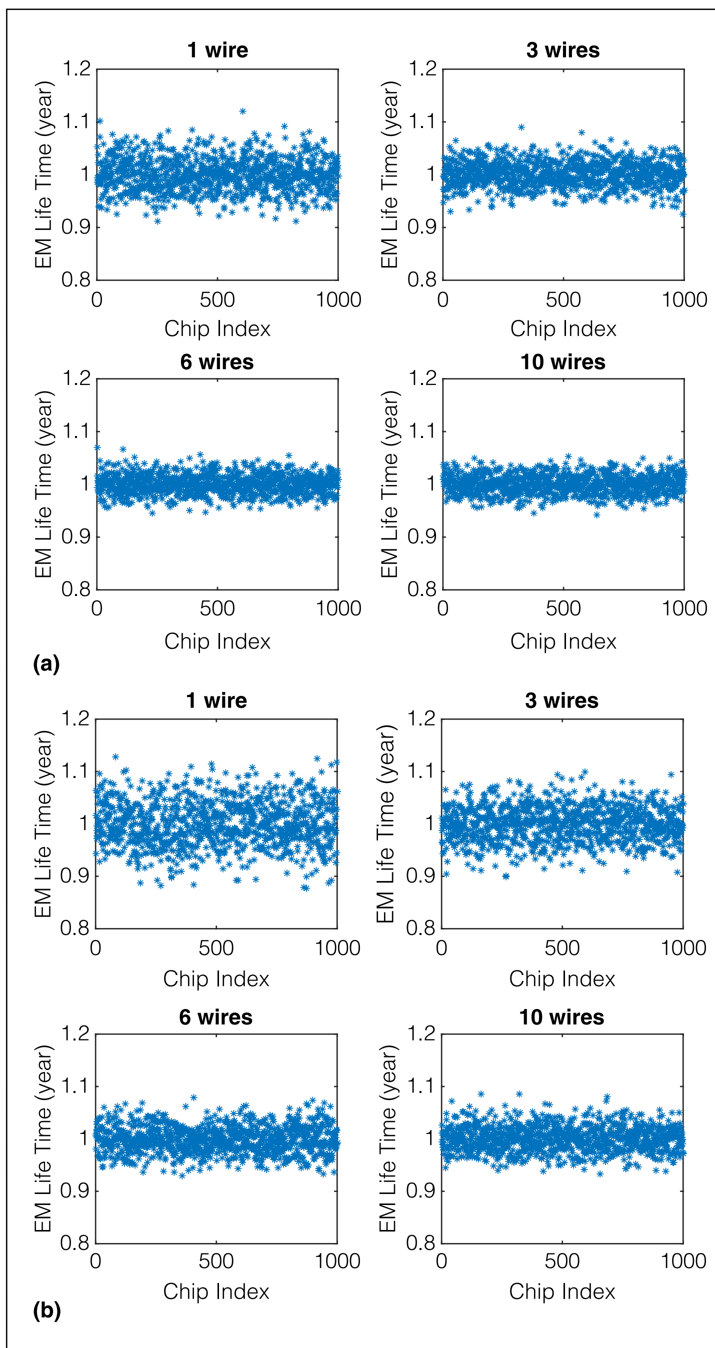

Figure 2. (a) and (b) The statistical study of stressed wires connected in parallel with different wire numbers and variations. (a) Variance $\theta = 0.001$. (b) Variance $\theta = 0.002$.

Read_en is on, there will be a voltage on EMR, which is 10% higher than the original voltage on EMS and the comparison result from one-bit ADC can be written into the register. With time, the resistance of the EMS will increase due to the EM effect, which means the voltage of the noninverting input of the one-bit ADC will increase. If the chip has been used for time longer than the designed failure time, the output of one-bit ADC will be 1 instead of 0.

We will design a number of such aging sensors for the specific years (for instance one year to ten years) in this project for validation purpose. Similar to the other on-chip aging sensors, the output registers can be connected by the JTAG circuits of the chip design so that one can read the aging information out *in situ* during the testing or diagnosis time. The aging information can also be read out before the chips are put into the system. Note that the proposed EM-based sensor can automatically consider the temperature impacts on the lifetime of the chips as it is based on the EM aging effects.

Performance analysis and experimental results

In this section, we will present the performance analysis of the proposed EM-based aging sensor including simulation results.

Effect of number of wires

For the proposed EM-based aging sensor, if the inherent variations are the same for all the wires, then the wire (wire set), which fails at a longer time, will have less absolute accuracy. For instance, 10% lifetime variation for a one-year wire will have an accuracy of about one month, while 10% lifetime variation for a ten-year wire will lead to errors of about one year. In order to mitigate this problem, one solution is to add more parallel wires for a longer year wire set, since the larger the number of parallel wires is, the smaller the lifetime deviation of the wire set will be. Figure 2a and 2b shows statistical analysis results for the EM lifetime of the stressed wire set connected in parallel versus the number of wires in each set and different variations. These results come from 1000 Monte Carlo simulation runs and the aging sensor wires are set for the one-year lifetime. The EM-induced lifetime follows the lognormal distribution [11] and the variances are set to 0.001 and 0.002, respectively, for the two figures. With the 0.001 variance, we can see that with one wire, the EM lifetime will fall into the ±10% lifetime mean with a 99.83% chance and into the ±5% lifetime mean with a 88.64% chance.

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 07:47:19 UTC from IEEE Xplore. Restrictions apply.

If we use six wires, we can have a 100% chance to achieve the ±10% life mean and a 98.66% chance for the ±5% life mean, which is good enough. If we increase the variance to 0.002, then one wire can reach a 97.46% chance for the ±10% life time mean; six wires can achieve a 99.95% chance for the ±10% lifetime mean and a 92.00% chance for the ±5% lifetime mean. For ten wires, we can achieve a 99.99% chance for the ±10% lifetime mean and a 95.33% chance for the ±5% lifetime mean. As we can see, with large inherent variations, we have to increase the number of wires to mitigate to reduce lifetime variations. We remark that the intradie environmental variations will also affect the resistance values of those wires. However, if they are placed very closely, as this should be the case, the impact will not be significant.

Figure 3 studies the lifetime variations versus the number of parallel wires used in each stressed wire set for specific years (one year, three years, six years, ten years). If we use the constant six wires for each set as the dash lines showing in Figure 3, we can see that the lifetime prediction variation in the ten-year wire set is quite significant for a given variance ($\theta = 0.001$). But if we use varying numbers of wires for the same design (six wires for one year, ten wires for six years, and 14 wires for ten years), the variations for the wire sets at the longer time lifetimes will be reduced as the solid lines showing in Figure 3.

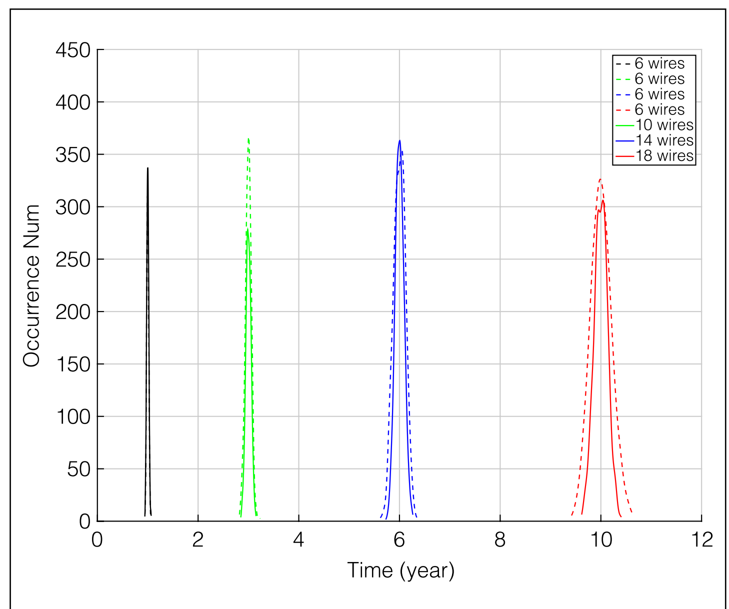

Figure 3. The statistical lifetime detections from the stressed wires: using the constant number and varying number wires.

Effect of length of wires

Figure 4a shows the relationship between wire length L and wire EM lifetime. The current density j is constant and set to $3 * 10^{10}$ A/m^2. We show both the nucleation time and the growth phase time predicted by the new EM models. As we can see, the total lifetime increases with decreasing L (so does the area), which shows that shorter failure time will need larger area compared to the longer failure time.

For a specific failure year designed, the area for the sensor wires can be estimated as $A = W * L * k$, where W is the width of each stressed wire (assuming that all the stressed wires are same) and L is the length of the stressed wire. The area of the reference wire is $1.1 * W * L/k$, which is typically less significant compared to the stressed wires. The power consumption for the total stressed wires can be estimated as $P = k * I^2 * R = k * (j * A)^2 * \rho * L/A = k * j^2 * L * \rho * A = k * j^2 * L * \rho * W * H$, where ρ is the resistivity of the metal wire, j is current density, and H is the height of the wire segment, as shown in Figure 1a. From the two formulas above, we can see that we should try to use the minimum width allowed by the technology node to save both area and power in theory. Our initial study shows that area and power are two performance metrics for trading off in the design. Figure 4b shows the power values versus the possible wire length (L) and current density j. The four red curves show the possible L and j values for one year, three years, six years, and ten years. We can clearly see the tradeoff between L (area) and power.

Bear in mind that tens of EM-based aging sensors can be inserted into commercial chips, which would easily detect the counterfeit and recycled ICs and show the age of the chip. Such a method is practical because the area overhead is small. An EM-based aging sensor with ten stressed wires costs 100–500 μm^2 with an SMIC 180-nm technology, which depends on the length of the wire. Assuming a total of ten sensors, the overhead is only 0.02% of the 25 000 000 μm^2 area available in a 5-mm × 5-mm chip.

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 07:47:19 UTC from IEEE Xplore. Restrictions apply.

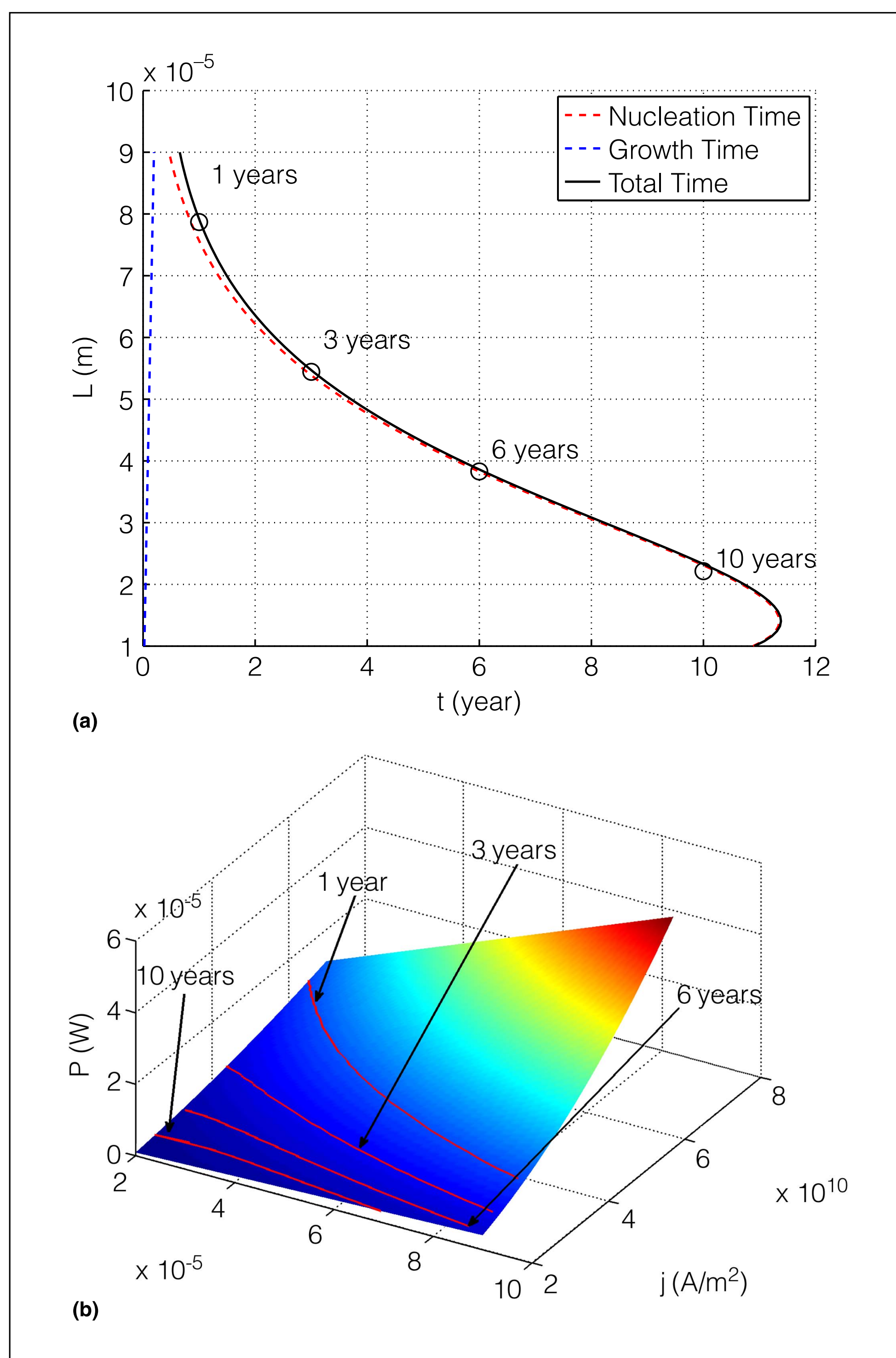

Figure 4. (a) Length versus EM lifetime of a wire. (b) Power consumption of stress wires versus wire length and current density.

simulation. We performed 1000 Monte Carlo simulation runs considering the variation of the nucleation time for the stressed wires. We design the wires such that they will fail (its resistance increases just 10%) around one year with lognormal distribution (standard deviation is set to 0.001) in their nucleation times.

Figure 5 shows the voltage waveforms at the two inputs of the ADC. In the beginning, the two inputs are clearly different. At around 0.68 year, the voltages on the stress wires start to increase, which is also the nucleation time for the wires. Then, the voltage of the stressed wires starts to increase gradually until it runs across 2.5 V, and then the ADC output will change "1" from "0." Figure 5 also shows that the sensor output will start to change from "0" (0 V) to "1" (5 V) around one year. As we can see, when the input voltage of the stressed wires reaches the reference voltage, the output signal starts to change, which happens at one year in this case.

Numerical results and discussions

The proposed EM-based aging sensor circuit has been designed and validated using SPICE

In this article, we have proposed a new on-chip aging sensor based on the EM-induced failure mechanisms to fast detect the recycled integrated circuits, which is one of the major hardware security issues facing the semiconductor industry. The new sensor is based on failure

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 07:47:19 UTC from IEEE Xplore. Restrictions apply.

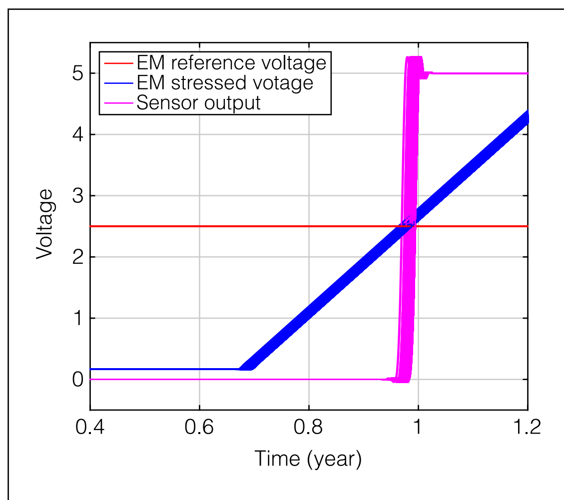

Figure 5. Statistical voltage inputs and outputs of the ADC.

detections of dc stressed metal wires to time the usage of chips over time. Compared with the existing ring-oscillator-based aging sensors, it can offer a simpler circuit implementation and smaller area footprints. It also provides a more accurate prediction of the chip usage time. The new aging sensor design is based on a newly proposed physics-based EM model. Experimental results show that the proposed aging sensor can accurately predict the targeted failure times in the presence of both inherent uncertainties. Our study also shows that more parallel wires will lead to more accurate statistical predictions at the cost of bigger area. ■

Acknowledgment

This work was supported in part by the National Science Foundation (NSF) under Grants CCF-1255899 and CCF-1527324, and in part by Semiconductor Research Corporation (SRC) under Grant 2013-TJ-2417. Initial results of this work were presented at the 2015 International Conference on Computer-Aided Design (ICCAD) [1].

■ References

[1] K. He, X. Huang, and S. X.-D. Tan, "EM-based on-chip aging sensor for detection and prevention of counterfeit and recycled ICs," in *Proc. Int. Conf. Comput. Aided Design*, Nov. 2015, pp. 146–151.

[2] M. Tehranipoor, H. Salmani, and X. Zhang, *Integrated Circuit Authentication*. New York, NY, USA: Springer-Verlag, 2014.

[3] L. Kessler and T. Sharpe, "Faked parts detection," 2010. [Online]. Available: https://www.cicuitsassembly.com/cms/component/content/article/159/9937-smt

[4] M. Times, "Officials: Fake electronics ticking time bombs." [Online]. Available: http://www.militarytimes.com/news/2011/11/ap-fake-electronics-ticking-time-bomb-110811/

[5] L. Abdallah, H. Stratigopoulos, S. Mir, and J. Altet, "Defect-oriented non-intrusive RF test using on-chip temperature sensors," in *Proc. IEEE 31st VLSI Test Symp.*, Apr. 2013, pp. 1–6.

[6] X. Zhang and M. Tehranipoor, "Path delay fingerprinting for identification of recovered ICs," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst.*, 2012, pp. 13–18.

[7] "Failure mechanisms and models for semiconductor devices," in *JEDEC Publ. JEP122-A*, JEDEC Solid State Technol. Assoc., 2002.

[8] X. Huang, T. Yu, V. Sukharev, and S. X.-D. Tan, "Physics-based electromigration assessment for power grid networks," in *Proc. Design Autom. Conf.*, Jun. 2014, pp. 1–6.

[9] X. Huang, A. Kteyan, X. Tan, and V. Sukharev, "Physics-based electromigration models and full-chip assessment for power grid networks," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, Feb. 2016, doi: 10.1109/TCAD.2016.2524540.

[10] J. R. Black, "Electromigration—A brief survey and some recent results," *IEEE Trans. Electron Devices*, vol. 16, no. 4, pp. 338–347, 1969.

[11] V. Sukharev, "Beyond Black's equation: Full-chip EM/SM assessment in 3D IC stack," *Microelectron. Eng.*, vol. 120, pp. 99–105, 2014.

Kai He is currently working toward a PhD in electrical engineering at the University of California, Riverside, Riverside, CA, USA. His research interests include hardware security and parallel computing for circuit simulation. He has an MS in microelectronics from Nanjing University, Nanjing, China.

Xin Huang is currently working toward a PhD in electrical and computer engineering at the University of California, Riverside, Riverside, CA, USA. Her research interest include reliability modeling, assessment and signoff analysis, and reliability-aware performance optimization. Huang has an MS in microelectronics from Peking University, Beijing, China.

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 07:47:19 UTC from IEEE Xplore. Restrictions apply.

Sheldon X.-D. Tan is a Professor in the Department of Electrical Engineering, University of California, Riverside, Riverside, CA, USA. He is also a Guest Professor of Shanghai Jiao Tong University and a Guest Professor of University of Electronic Science and Technology of China. His research interests include VLSI reliability modeling, optimization and management at circuit and system levels, thermal modeling, statistical modeling, simulation and optimization of mixed-signal/RF/analog circuits, parallel circuit simulation techniques based on GPU and multicore systems. Tan has a PhD in electrical and computer engineering from the University of Iowa, Iowa City, IA, USA. He is a Senior Member of the IEEE.

■ Direct questions and comments about this article to Kai He, Department of Electrical and Computer Engineering, University of California, Riverside, Riverside, CA 92521 USA; njuhekai@gmail.com.

Authorized licensed use limited to: Univ of Calif Riverside. Downloaded on June 24,2026 at 07:47:19 UTC from IEEE Xplore. Restrictions apply.