Demonstration of a Passive IC Tamper Sensor Based on an Exposed Floating Gate Device in a Standard Logic Process

Muqing Liu, *Student Member, IEEE*, and Chris H. Kim, *Fellow, IEEE*

***Abstract*— We present an embedded Flash (eFlash) memory-based powerless nonvolatile tamper sensor for efficiently detecting counterfeit ICs. By exposing the floating gate (FG) node of a logic-compatible eFlash cell to the environment, the proposed sensor can record any subtle physical event that affects the charge stored on the exposed FG. The proposed sensor is demonstrated in both 65-nm and 0.35-μm standard CMOS technologies. Extensive test results confirm that suspicious activities such as temperature charge injection, humidity rises, and increased dust particle density in the cavity can be recorded powerlessly using the proposed sensor.**

***Index Terms*— Counterfeit electronics, embedded Flash (eFlash), floating gate (FG), logic-compatible, physical attack, recycled chips.**

I. Introduction

COUNTERFEIT ICs entering the supply chain have been causing significant financial damage to the electronics industry. According to recent estimates, the electronics industry is losing $100 billion in terms of worldwide revenue every year because of counterfeit parts [1]–[4]. Different types of counterfeit methods have been reported, including recycling, remarking, overproducing, cloning, forged documentation, defective, and tampered chips [5]. Among them, recycled and remarked counterfeit electronics account for more than 80% of all reported counterfeiting cases [6]. Recycled ICs are usually recovered from old printed circuits boards (PCBs) and then relabeled and disguised as new parts. Recycled ICs can pose great concern for customers, since they may function correctly initially, but cause early failures down the road. Detecting these counterfeit electronics efficiently is a critical aspect of preventing counterfeit ICs. Several techniques have been proposed to detect counterfeit electronics. They can be broadly classified into two categories: physical inspection and electrical test [7]. Physical tests are usually destructive and must utilize test instruments, making it very costly and time-consuming. Furthermore, it usually requires a human expert to interpret the test results [8]. Electrical inspection, on the other hand, uses on-chip sensors [9] to automatically flag compromised chips. Despite their promise, on-chip sensors cannot stop untrusted foundries from overproducing chips [7], and they cannot fully detect physical attacks such as die removal and desoldering. These physical attacks are known to be very common in today's global supply chain. To avoid recycled and remarked counterfeits, several specialized sensors and package identity techniques have been proposed. For instance, the combating die and IC recycling (CDIR) sensor in [10] relies on device aging effect to detect the usage of the chip, while in [11], DNA makers were placed on the chip package for authentication purposes. The CDIR sensor can only be implemented on new products, while product marking can be used to label currently used or obsolete components that are no longer manufactured.

In this paper, we present a logic-compatible embedded Flash (eFlash)-based tamper sensor that utilizes an exposed floating gate (FG) structure to detect whether or not an IC has been physically compromised. The proposed eFlash-based sensor does not require any power source for the sensing operation, which is a critical requirement for counterfeit IC detection. In addition, the sensor can be implemented using I/O devices readily available in any standard CMOS technology. Part of this work was presented in [12].

II. 5T eFlash Basics

The sensor utilizes an eFlash cell whose FG node is exposed to the environment such as the chip cavity. Fleeting changes in the electron charge stored in the eFlash cell can be captured by the proposed sensor. The eFlash circuit is implemented using discrete I/O devices available in a standard CMOS process so no modification is required to the process technology [13]. The proposed eFlash-based sensing has the advantage of offering a secure nonvolatile storage solution as well as the ability to retain stored data without a power source. Fig. 1 shows the 5T eFlash cell schematic and layout along with the bird's eye view of the cell [14]. The eFlash cell consists of five transistors: coupling device M_1, erase device M_2, program/read device M_3, and two selection devices S_1 and S_2. The FG node is formed by connecting the transistors M_1–M_3 in a back-to-back fashion. The width of M_1 is made larger than those of M_2 and M_3 to achieve a high coupling ratio (CR). A large

Manuscript received January 17, 2019; revised March 20, 2019; accepted March 23, 2019. Date of current version May 21, 2019. The review of this paper was arranged by Editor D. J. Young. *(Corresponding author: Chris H. Kim.)*

M. Liu is with the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN 55455 USA.

C. H. Kim is with the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN 55455 USA (e-mail: kimchris@snu.ac.kr).

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/TED.2019.2909558

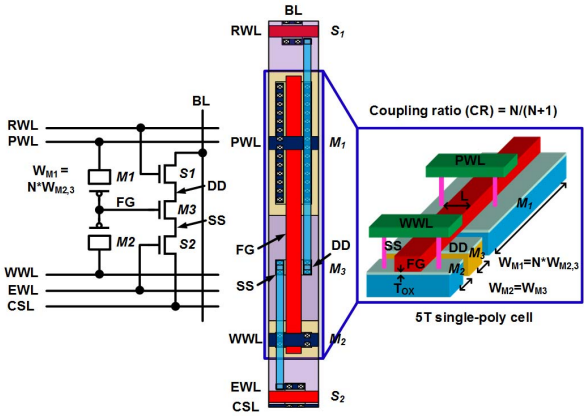

Fig. 1. 5T eFlash cell structure (left). Layout view (middle). Bird's eye view of the cell (right).

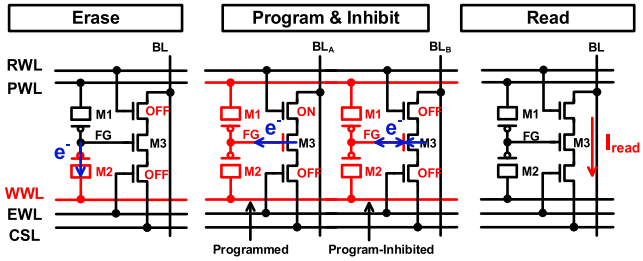

Fig. 2. Three operating modes of the 5T eFlash cell.

CR ensures that the FG voltage closely follows the PWL voltage applied to the coupling device, maximizing the electric field for efficient Fowler–Nordheim (FN) tunneling through the dielectric of M_2 and M_3.

Fig. 2 shows the three operating modes of the proposed eFlash cell. In erase mode, a high erase voltage is applied to write wordline (WWL), which removes the electrons from FG through M_2. In program mode, the upper selection device is turned on, while a high program voltage is applied to both PWL and WWL, causing electrons to tunnel from M_3 into FG. The 5T eFlash cell also has program-inhibit capability, which is achieved by turning off the upper selection device during the program operation. During program inhibition, the source voltage of the read device is boosted, preventing the electrons from being injected to the FG node via M_3, thus the program operation in this cell is inhibited. This allows us to selectively program a specific eFlash cell in a row.

Electron charge stored on the FG node affects the threshold voltage of M_3, and in read mode, the threshold is read out by measuring the bitline (BL) current. In our proposed eFlash-based sensor, the FG node is exposed to the chip cavity through pad openings, so any physical sources that affect the number of electrons in the FG node can be detected. To activate the sensor, the eFlash cells must be programmed once to populate the FG with electrons. After that, the sensor can record tamper events without a power source.

III. Sensor Test Structure in 65-nm Technology

A. Basic Concept

To validate the proposed eFlash-based sensor concept, we first implemented a single test structure shown in Fig. 3

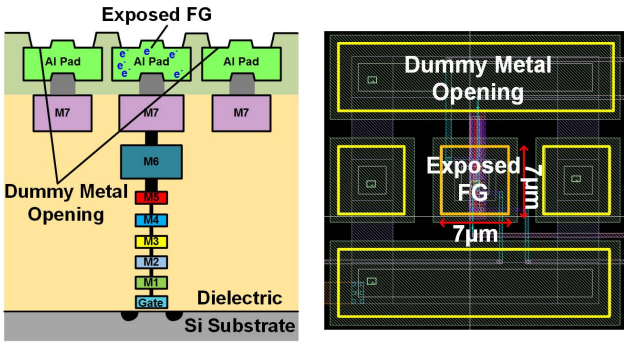

Fig. 3. Cross-sectional view of eFlash with exposed FG (left). Top layout view of exposed FG and surrounding dummy metals (right).

in a 65-nm CMOS technology. All the transistors in the eFlash cell are standard 2.5-V I/O devices with a tunnel oxide thickness (T_{OX}) of approximately 5 nm [13]. The FG node of the eFlash cell is exposed to the environment by connecting a stack of metals from the bottom M1 layer to the top M7 layer as shown in Fig. 3. The dimension of the opening window is 7 μm $\times$ 7 μm. Dummy floating metals are placed around the FG opening window to serve as charge collection metals. The opening windows of the surrounding dummy metals can be seen in Fig. 3 (left). Since the FG node is populated with electrons, so it is at a lower potential than the dummy metals. In addition, the dummy metals are very close to the FG, they can help attract and collect electrons from the FG, which enhances the sensitivity. The threshold voltage of the read transistor is a function of the FG charge, i.e., fewer electrons on the FG node translates into a lower threshold voltage and hence a higher BL current.

Since recycled ICs are usually recovered from a discarded circuit board, the chips are likely to be exposed to high temperatures during the removal process. High temperature facilitates FN tunneling of electrons, so this type of physical attack can be detected by our proposed eFlash sensor. Another form of physical attack is opening the chip package to gain access to the silicon die. When the chip package is opened, even temporarily, the humidity or the dust particle density may change. Increased moisture in the air increases the surface conductivity of the FG node, thereby causing electrons on the FG to escape more rapidly. Dust particles with a positive net charge are attracted to the exposed FG node containing electrons with a negative charge. It is also possible that the parasitic capacitance surrounding the FG node changes due to the presence of extra particles, which affects the erase and program operations. These can cause variations in the FG node charge and thus can be detected by the proposed sensor.

B. Measurement Results

We performed temperature and humidity tests mimicking physical attacks that a chip may encounter. Fig. 4 (left column) shows a permanent BL current jump after the temperature spike. This indicates that the electrons on the FG node are permanently lost, allowing the sensor to successfully record the event. Note that between the readout intervals, the power supply of the eFlash sensor was shut down. In other words, the sensor is able to record physical attacks without any power.

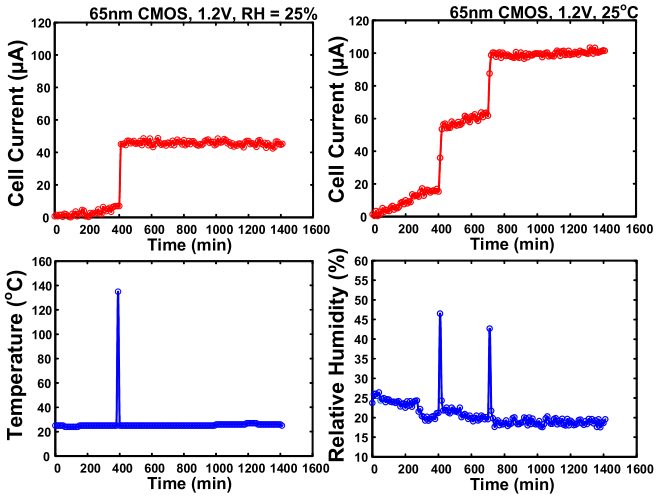

Fig. 4. Temperature (left) and humidity (right) attack test results of 65-nm eFlash sensor test structure.

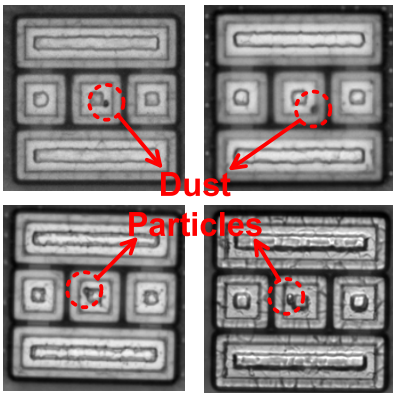

Fig. 5. Microscope images of four different chips with particles landed on the FG node of 65-nm eFlash sensor test structure.

Humidity test results are shown in Fig. 4 (right). We opened the lid of the chip and increased the moisture content in the air. The experiment was performed in an enclosed room, and the relative humidity near the chip was monitored. When the relative humidity was increased, a permanent jump in the cell current was observed. The measurements were highly repeatable, which indicate that the proposed sensor can reliably detect humidity changes.

After several humidity tests, we were no longer able to erase or program the sensor. The same behavior was found in multiple chips. Interestingly, we found that all chips with this specific behavior had particles landed on the FG node as shown in Fig. 5. The erase and program characteristics of the cells before and after the particle landing are shown in Fig. 6. Note that the Vth is defined as the minimum wordline (PWL and WWL) voltage applied to turn on the read transistor, not the intrinsic threshold voltage of the transistor. This suggests that the proposed sensor can even detect particles entering the chip cavity, which is another indication that a chip has been compromised.

IV. 16 × 16 Sensor Array in 0.35-μm Technology

Encouraged by the 65-nm test structure results, we implemented an array-based test chip with complete peripheral

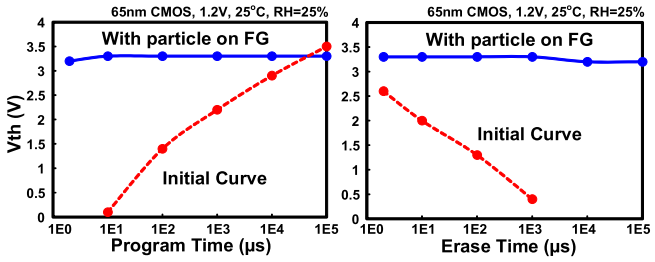

Fig. 6. Program and erase characteristics for eFlash sensor with particles landed on the FG node.

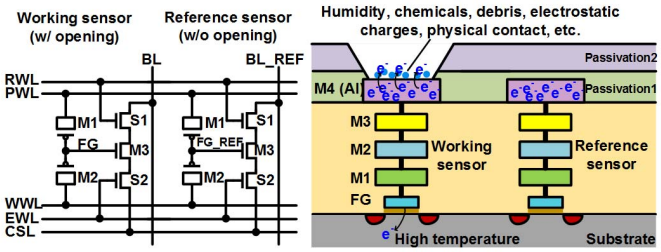

Fig. 7. Differential eFlash sensor cell with exposed and buried FGs implemented in 0.35-μm technology.

circuitry. The new chip was fabricated in a 0.35-μm technology for cost reasons. It is worth reiterating that the proposed sensor is agnostic to process technology so as long as transistors with an oxide thickness greater than 5 nm are available.

A. Implementation

A 16 × 16 sensor array was fabricated in a 0.35-μm logic process. The differential cell structure with exposed and buried FGs is shown in Fig. 7 [12]. The exposed cell is the working sensor and the buried cell is the reference cell. A differential read out enables higher sensitivity. Standard core devices in the 0.35-μm technology with a nominal supply voltage of 3.3 V, and a typical 7.6-nm tunnel oxide thickness (T_{OX}) was used for the cell implementation. No special devices were needed for the sensor implementation. Each sensing unit consists of one working sensor with an exposed FG and a reference sensor with a buried FG.

The complete 16 × 16 array architecture is shown in Fig. 8. A high voltage switch (HVS) circuit [13] is used to generate the high voltage signals for erase and program operations with correct timing as well as the read voltages. Cascoding (or device stacking) was used extensively to prevent overstress issues in the HVS circuit. The working sensors and reference sensors share the same readout path, which cancels out common process, voltage, and temperature (PVT) variation effects. The readout circuit consists of a voltage-controlled oscillator (VCO) and a counter. The detailed readout operation is shown in Fig. 9. The BL voltage, which reflects the charge stored on the FG node, is converted to the corresponding frequency by the VCO circuit. Simulation results show that a 10-mV difference caused by the FG node charge difference translates to a BL voltage of 0.3 V. As mentioned earlier, more electrons on the FG mean a higher threshold voltage and a lower BL current. This means that the final BL voltage is higher for the same pull-up bias voltage pmos bias, resulting in

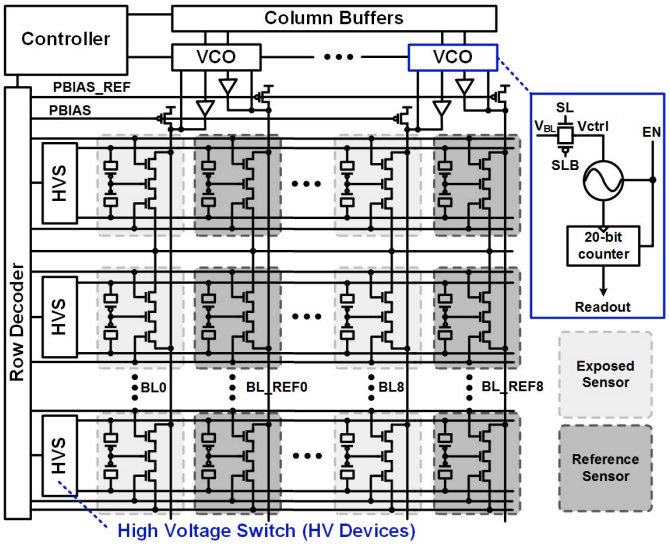

Fig. 8. 16 × 16 sensor array architecture.

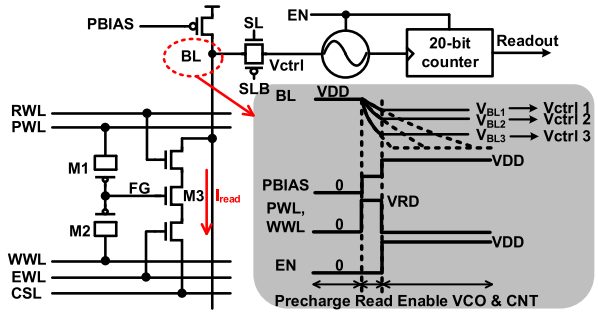

Fig. 9. VCO-based sensor readout circuit and timing diagram.

a higher output frequency count. The pull-up pMOS transistor is designed so that it is large enough to precharge a long BL with 16 rows of sensors, and small enough so that the nMOS pull-down transistors on BL can compete with it when it is partially on.

To test a wide range of design choices, the sensor array consists of eFlash cells with different transistor sizes and different opening sizes. The detailed sensor size and opening size configuration are shown in Fig. 10 (left). There are 16 different transistor size and opening size combinations. The die photograph is shown in Fig. 10 (right).

B. Basic Functionality Tests

Fig. 11 shows the VCO frequency characterization results before any program or erase operations. The frequency variation of the same VCO for different readout trials was 0.27%, while the frequency variation between different VCOs was 1.51%. PVT effects can be canceled out by measuring the frequency difference between the working sensor and the reference sensor. Also, note that the frequency shift caused by physical attacks, which will be shown later, is usually 20% or more. This shift is significantly higher than the frequency variation induced by PVT effects.

Fig. 12 (left) shows the erase, program, and program-inhibit characteristics of the 16 × 16 sensor array. The entire array was initially erased, and alternating columns were programmed,

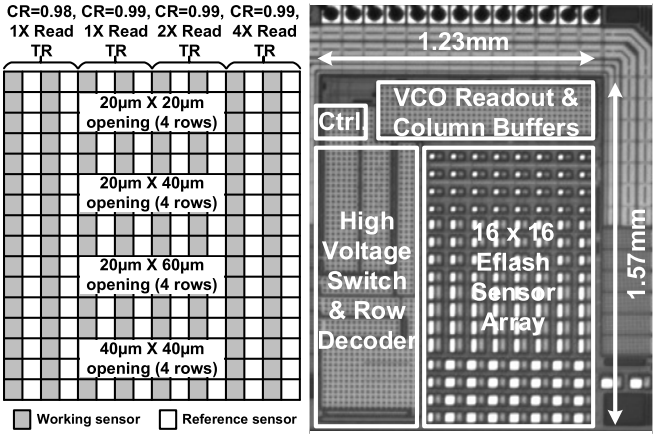

Fig. 10. Sensor circuit and opening size configurations (left). Die photograph (right).

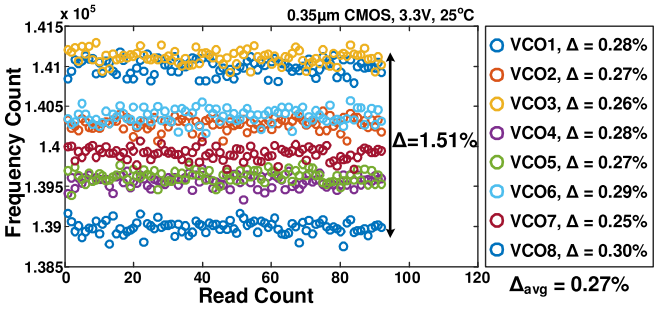

Fig. 11. Characterization of VCO frequency variation of the readout circuits.

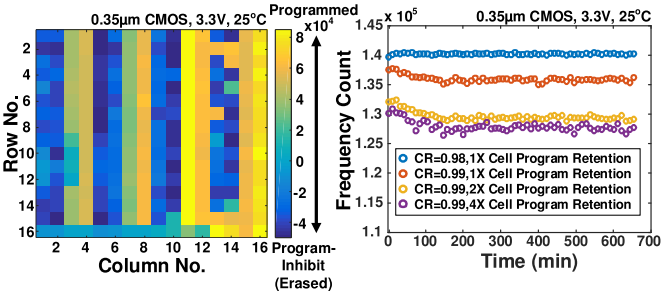

Fig. 12. Erase, program, and program-inhibit characteristics (left) and cell retention results (right).

while the other columns were program inhibited. The program-inhibited cells remain in the erased state. Since the electron charge stored on the FG is directly proportional to the readout frequency count, the programmed cells have a higher count and the erased cells have a lower count. Fig. 12 (left) displays the frequency change of the sensor array after the erase and program operations. Yellow blocks represent frequency increase (electron increase), corresponding to the programmed cells, and blue blocks correspond to the erased cells. The cell color becomes darker on the right side of the color map, meaning that with higher CR, the eFlash cell can be more efficiently programmed/erased and with larger read transistor size, a similar threshold change can be amplified further. The retention characteristics of the program operation are shown in Fig. 12 (right). This figure displays the frequency count over time for four cells on the same row with different CR and read transistor size. Note that in this figure, the raw frequency count

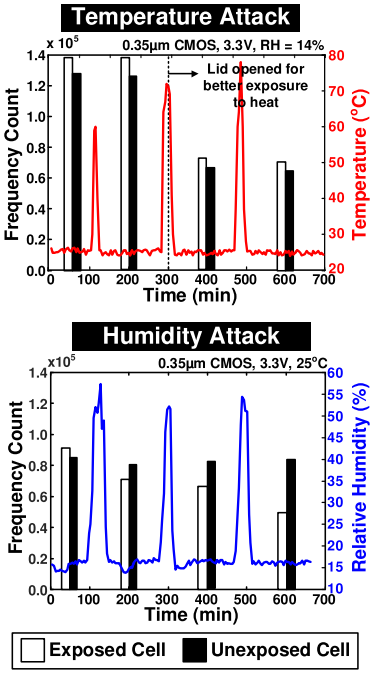

Fig. 13. Temperature (top) and humidity (bottom) attack test results.

is plotted without canceling the intrinsic frequency variation between different VCOs, so only the frequency change of different curves over time matters in this figure. Comparing the top two curves, we can see that eFlash cells with a higher CR of 0.99 have a larger retention loss. This might due to the eFlash cell with a higher CR has more abundance of charges on the FG, so there is also a higher amount of charge loss. Comparing the bottom three curves with the same CR but different device sizing, a larger device size results in a higher retention loss. For a given amount of the charge loss on the FG nodes, which results in a similar threshold change on the read transistors, the larger device will have a larger current change, reflected as a larger frequency count drop. Due to the limited number of chips and the lack of an accurate temperature control setup, we only performed retention tests at room temperature. Considering that the gate oxide thickness of this 0.35-μm process is 50% thicker than that in a previous work [13], we expect the cell retention to be adequate at different PVT conditions. We have verified that under normal operating conditions, the sensor readout frequency is relatively constant. Therefore, we can say with high confidence that any significant changes in the output frequency are attributed to a physical attack.

C. Physical Attack Tests

We performed temperature, humidity, and particle/debris attack tests to evaluate the array-based sensor. Before the tests, the rows of the sensor array were alternately erased and programmed. The programmed rows are the sensing nodes, and the erased rows serve as the charge collection metals. Fig. 13 (top) shows the temperature test results. We used a simple heat gun to raise the temperature of the chip, mimicking an attempt to desolder the package from the printed

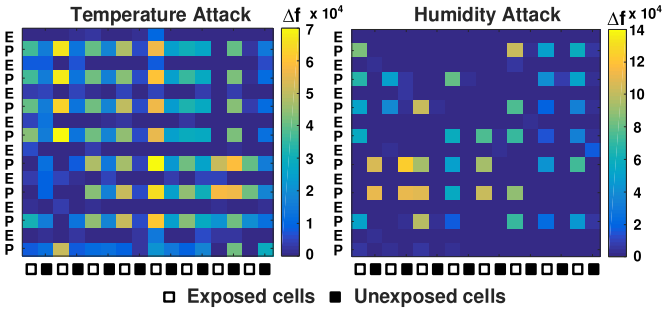

Fig. 14. Frequency change maps of temperature attack (left) and humidity attack (right). The temperature attack causes frequency change generally in both the exposed and unexposed sensor cells with the exposed cells showing a larger drop, while humidity attack only causes frequency change in the exposed cells.

circuit board. This was repeated three times. The red curve in Fig. 13 (top) plots the temperature profile during the test. The sensor frequency was readout between the temperature spikes, and the power supply of the test chip was shut off between the readouts. The test chip was packaged in a ceramic DIP48 package with a removable lid. During the first attack, the lid of the chip was kept closed. This did not result in any appreciable frequency change so for the second and third attacks, we opened the lid for better heat exposure. Note that this was necessary only because of the large dual in-line package (DIP) package and small test dies used in our experiments. Smaller packages are expected to be significantly more susceptible to temperature attacks due to their low thermal mass. After the second temperature attack was over, the readout frequency of the exposed and unexposed cells went down, indicating a charge loss in the FG nodes. After the third temperature attack, the readout frequency remained low. This indicates that high temperature facilitates the FN tunneling and once the electrons have gained enough energy to pass the barrier, later attacks with similar temperature would not cause further frequency change. FN tunneling induced by high temperature affects both exposed and unexposed cells, so as expected, permanent charge loss occurs in both type of cells.

Fig. 13 (bottom) shows humidity attack test results. High humidity was applied three times, which is shown in the blue curve. The black/white bars in Fig. 13 (bottom) plot the frequency readout of the exposed and unexposed cells before and after humidity attacks. After each humidity attack, the frequency of only the exposed sensor decreased further, which matches the previous results in Section III from the 65-nm test structure. The frequency of the unexposed reference sensor remained at the same level after each humidity attack. These measurement results indicate that humidity causes a permanent charge loss only in the exposed sensor. Humidity attack only changes the surface conductivity of the exposed sensors, so we can only observe frequency shift in the exposed sensors. By comparing the frequency change of the exposed sensor and unexposed sensor, we can determine the source of the attack.

By analyzing the entire frequency map data for the sensor array, which is shown in Fig. 14, we can extract further information on the type of attack. For instance, temperature attack results in frequency change in both the exposed and

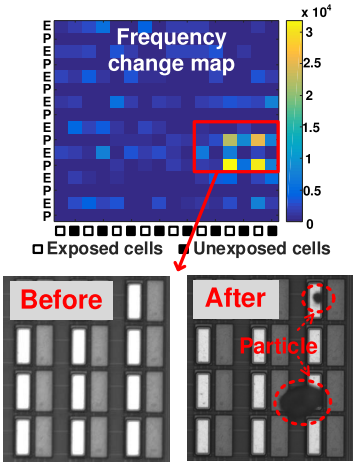

Fig. 15. Particle/debris test results. Frequency change map (top) and microscope images of the region that was affected by particles (bottom).

unexposed sensors, while the exposed cells have a larger drop due to better exposure to the heat source. This trend can be seen in Fig. 14 (left), where the cells on the programmed rows generally have a brighter color, with the exposed cells having the brightest color. Abnormal behavior can be seen in the upper right or lower left regions, which underscores the importance of having an array structure rather than a single node sensor. Unlike temperature attack, humidity attack causes a large frequency drop only in the exposed cells, which is illustrated in Fig. 14 (right). Most of the nonblue color blocks appear on the odd columns, which represent the frequency change in exposed cells. Some abnormal cells can be found in the bottom left corner. Note that in this frequency change map, the programmed working sensors are only on the even rows, so the frequency change happens only in the even rows.

Finally, particle/debris attacks were performed, which is shown in Fig. 15. We introduced some fine particles to the chip cavity intentionally to speed up the test. Rows in the sensor array were programmed and erased in an alternating fashion for better charge collection. During the measurement, the frequency of the sensor cells was continuously recorded. The chip lid was opened and some talc particles were introduced right after 100 min. The frequency of some cells dropped almost instantaneously. The locations of the four cells showing large frequency drops are highlighted in the red box in Fig. 15 (top). The microscope images before and after the particle/debris attack show the sensor array area inside the red box in the frequency change map. By cross-checking the microscope image with the location of the sensor cells showing a large frequency drop, we found that the particles/debris tend to be attracted to the erased sensor cells, while frequency drops occur in the adjacent programmed cells. This suggests that either the electrons on those programmed cells have been collected by the nearby particles/debris or the parasitic capacitance of the FG changes because of the particles/debris landed on the die. We could also observe that in the frequency change map of particles attack, there are only several nearby exposed cells showing frequency change, illustrated by the yellow blocks, which indicates the possible locations of the particles. This pattern is different from the temperature and humidity tests, so the proposed sensor array can also discriminate the particle/debris effects from other forms of attacks.

V. Conclusion

In this paper, we presented an eFlash-based counterfeit IC detection sensor with an exposed FG node. The proposed 5T eFlash cell is built using I/O transistors readily available in any logic process and hence incurs no process overhead. Measurement results from a 65-nm sensor test structure and a 0.35-μm sensor array test chip validate that the proposed eFlash sensor can sense and distinguish between different physical attacks. Any physical source that changes the charge stored on the exposed FG can be detected by this sensor. This includes humidity, high temperature, dust particles, chemicals, and electrostatic charges. Test chip results show that the proposed eFlash-based sensor can efficiently and reliably detect many types of counterfeit attempts.

References

[1] *Internet of Things Global Standards Initiative*. Accessed: Jul. 2015. [Online]. Available: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[2] A. Nordrum. (Aug. 18, 2016). *Popular Internet of Things Forecast of 50 Billion Devices by 2020 is Outdated*. [Online]. Available: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

[3] G. Fink, D. V. Zarzhistsky, T. E. Carroll, and E. D. Farquhar, "Security and privacy grand challenges for the Internet of Things," in *Proc. Int. Conf. Collaboration Technol. Syst. (CTS)*, Jun. 2015, pp. 27–34. doi: 10.1109/CTS.2015.7210391.

[4] M. Pecht and S. Tiku, "Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics," *IEEE Spectr.*, vol. 43, no. 5, pp. 37–46, May 2006. doi: 10.1109/MSPEC.2006.1628506.

[5] U. Guin and M. Tehranipoor, "On selection of counterfeit IC detection methods," in *Proc. IEEE North Atlantic Test Workshop*, May 2013, pp. 1–5.

[6] L. W. Kessler and T. Sharpe. (2010). *Faked Parts Detection*. [Online]. Available: http://publish-it-online.com/article/Faked+Parts+Detection/411055/39826/article.html

[7] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014. doi: 10.1109/JPROC.2014.2332291.

[8] S. Shahbazmohamadi, D. Forte, and M. Tehranipoor, "Advanced physical inspection methods for counterfeit IC detection," in *Proc. Conf. 40th Int. Symp. Test. Failure Anal. (ISTFA)*, Nov. 2014, pp. 55–64.

[9] T.-H. Kim, R. Persaud, and C. H. Kim, "Silicon odometer: An on-chip reliability monitor for measuring frequency degradation of digital circuits," *IEEE J. Solid-State Circuits*, vol. 43, no. 4, pp. 874–880, Apr. 2008. doi: 10.1109/JSSC.2008.917502.

[10] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Proc. IEEE Design Autom. Conf.*, Jun. 2012, pp. 703–708.

[11] M. Miller, J. Meraglia, and J. Hayward, "Traceability in the age of globalization: A proposal for a marking protocol to assure authenticity of electronic parts," in *Proc. SAE Aerosp. Electron. Avion. Syst. Conf.*, Oct. 2012, p. 8. doi: 10.4271/2012-01-2104.

[12] M. Liu and C. H. Kim, "A powerless and non-volatile counterfeit IC detection sensor in a standard logic process based on an exposed floating-gate array," in *Proc. IEEE Symp. VLSI Technol.*, Jun. 2017, pp. T102–T103. doi: 10.23919/VLSIT.2017.7998211.

[13] S.-H. Song, K.-C. Chun, and C. H. Kim, "A logic-compatible embedded flash memory for zero-standby power system-on-chips featuring a multi-story high voltage switch and a selective refresh scheme," *IEEE J. Solid-State Circuits*, vol. 48, no. 5, pp. 1302–1314, May 2013. doi: 10.1109/JSSC.2013.2247691.

[14] S.-H. Song, J. Kim, and C. H. Kim, "A comparative study of single-poly embedded flash memory disturbance, program/erase speed, endurance, and retention characteristic," *IEEE Trans. Electron Devices*, vol. 61, no. 11, pp. 3737–3743, Nov. 2014. doi: 10.1109/TED.2014.2359388.