A Powerless and Non-volatile Counterfeit IC Detection Sensor in a Standard Logic Process Based on an Exposed Floating-Gate Array

Muqing Liu and Chris H. Kim

Dept. of ECE, University of Minnesota, 200 Union Street SE, Minneapolis, MN 55455, USA (Email: liux3300@umn.edu)

Abstract

Counterfeit ICs pose a threat to designing secure and reliable electronic systems. To better detect and prevent counterfeit ICs from entering the supply chain, an eflash based powerless non-volatile sensor using floating-gate (FG) technology is demonstrated in a 0.35μm standard logic process. By exposing the FG to the environment, the proposed sensor can record any physical tamper attempt affecting the charge stored on the exposed FG. Test results confirm that anomalous events such as temperature spikes, humidity changes, or increased dust particle density can be recorded by the sensor powerlessly, and later read out and analyzed whenever the power is available.

Introduction

Counterfeit ICs have become a growing concern for applications such as IoT where security is of utmost importance. Many different forms of IC counterfeiting have been reported such as IC recycling, remarking, overproduction, cloning, forged documentation and tampering [1]. In particular, recycled ICs recovered from used electronic systems is known to be a prevalent issue. Physical inspection or electrical tests can be performed to detect counterfeit ICs. The former is a straightforward method, but the test time and test cost are prohibitive, and it is usually destructive and not automated. Electrical testing, such as measuring the remaining useful lifetime of a chip using odometer circuits, can be effective [2,3]. However, this method is unable to detect actual physical attacks (e.g. desoldering, die removal). In this work, an embedded flash (eflash) based powerless tamper sensor is demonstrated which utilizes an exposed floating-gate structure to detect whether or not an IC has been physically compromised.

Eflash based Powerless Non-volatile Sensor

The sensing approach presented in this work is based on an eflash cell whose floating-gate (FG) node is exposed to the environment to capture fleeting changes in electron charges stored on it. The eflash cell used in this work is a single-poly design which can be built in a standard logic process without any process modification [4]. The structure and operation of the proposed eflash cell are illustrated in Fig. 1. The memory cell consists of five transistors: coupling device M_1, erase device M_2, program/read device M_3 and two selection devices for the program inhibit operation. The FG node for non-volatile charge storage is formed by connecting the transistors M_1-M_3 in a back-to-back fashion. The width of M_1 is larger than that of M_2 and M_3 to achieve a high coupling ratio (CR). This ensures that the FG voltage closely follows the voltage applied to the coupling device, generating an E-field large enough for Fowler-Nordheim (FN) tunneling across the dielectric of M_2 and M_3. In erase operation, a high voltage (14V) is applied on WWL resulting in electrons removed from FG through M_2. In program operation, a high voltage (14V) is applied to both PWL and WWL, causing electrons to tunnel from M_3 to FG. Electron charges stored on the FG node affect the effective threshold voltage of M_3, and in read operation, the threshold can be read out using peripheral circuits. The FG node is exposed to the chip cavity using pad openings with different window sizes. The cross section view of the eflash structure is shown in Fig. 2. Each sensing pair consists of one working sensor with an exposed FG and a reference sensor with a buried FG. By exposing the FG node to the environment and utilizing the nearby FG nodes to collect electron charges, one can sense physical sources that result in a change in either the surface conductivity (e.g. humidity, chemicals, electrostatic charge, debris, contact with foreign object) or FN tunneling (e.g. temperature). To activate the sensor, the eflash cells must be programmed one time to make the FG populated with electrons. After that, the sensor can record the event history in the non-volatile FG node without any power source.

A 16x16 sensor array was fabricated in a 0.35μm logic process. Note that the eflash cell can be implemented in more advanced technologies using thick oxide I/O transistors [4]. The array architecture is shown in Fig. 3. The detailed readout operation is shown in Fig. 4. In read mode, the BL voltage level is determined by the read current and the pull-up PMOS transistor current. The small difference in eflash cell threshold voltage is amplified by ~30 times using this circuit. The BL voltage is then converted to a frequency output using a voltage controlled oscillator (VCO). Finally, the frequency is converted to a digital count and scanned out.

Fig. 5 shows the counterfeit IC detection scheme using the proposed sensor. After the chip is fabricated and packaged, the sensors are programmed by the authorized manufacturer and the initial frequency f_0 is recorded. After that, the chip enters the supply chain. When a customer receives the chip, the frequency f_1 is read out. If the chip hasn't been tampered or recycled, f_1 should fall within an expected range around f_0, which can be characterized beforehand. If the measured frequency happens to be outside of the normal range, the chip is deemed a counterfeit. The sensor array contains cells with different transistor sizes and different opening sizes to test a wide range of design choices. The detailed sensor configuration and die photo are shown in Fig. 6.

Eflash Sensor Array Measurements

Fig. 7 shows the measured VCO frequency before any program or erase operation. The variation between different VCO frequencies was 1.51% while the frequency variation of the same VCO was 0.27%. Both are small enough to be ignored in our application. Erase, program and program-inhibit operations of the individual sensor cells were verified for the entire 16x16 array (Fig. 8). The retention characteristics were very robust due to the thick oxide layer of this process. To verify whether the sensor can record various tamper attacks, we performed temperature, humidity and particle/debris tests. The temperature test results are shown in Fig. 9. During the short durations of high temperature, the frequency outputs of both exposed and unexposed sensors decrease or increase together. However, after the high temperatures are removed, a low readout frequency is maintained indicating a permanent charge loss. So if a counterfeiter were to desolder the chip from the original PCB, the high temperature will affect the charge stored on the FG and the eflash cell will memorize this information until the sensor is interrogated by the customer. Humidity test results are shown in Fig. 10. The increased moisture in the air enhances the surface conductivity and as a result, there's higher chance that an electron on the FG will escape. Test results confirm that the readout frequency decreases when the humidity is raised. Fig. 11 shows the results for particle/debris test. Rows in the sensor array are programmed and erased in an alternating fashion for better charge collection. The lid was opened so that particles/debris can passively enter the chip cavity. We observed an instant frequency drop in several cells. By cross-checking the microscope image with the location of the cells exhibiting a large frequency drop, we found that particles/debris tend to be attracted to the erased cells while frequency drop occurs 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.

References [1] U. Guin, Proceedings of IEEE, Aug. 2014. [2] X. Zhang, DAC, 2012. [3] T. H. Kim, JSSC, Apr. 2008. [4] S. Song, JSSC, May 2013.

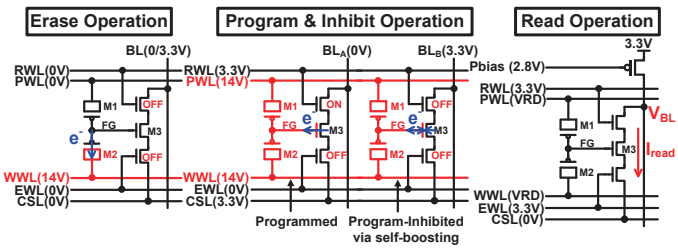


Fig. 1. Single-poly eflash operation modes.

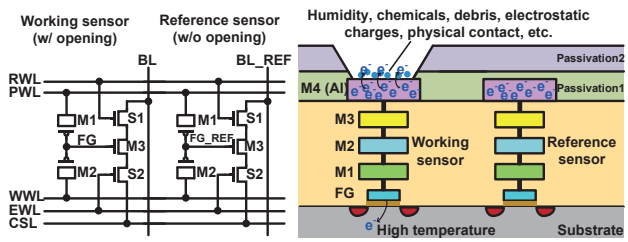


Fig. 2. Powerless non-volatile sensor with exposed floating-gate.

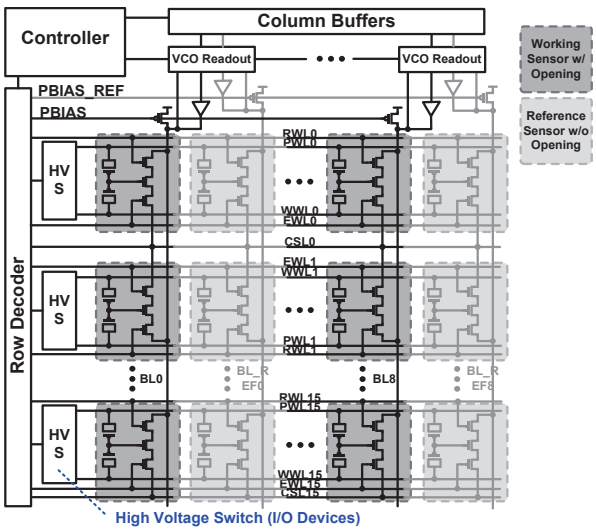


Fig. 3. Sensor array architecture.

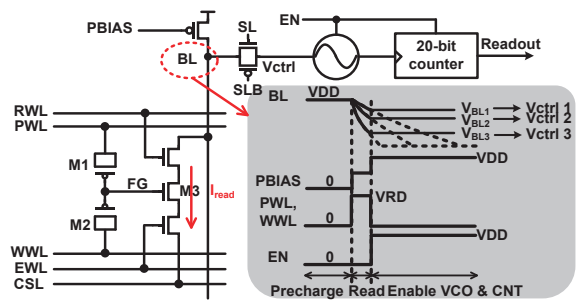
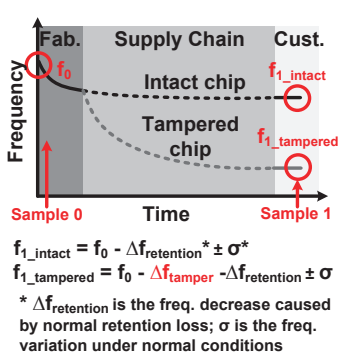


Fig. 4. VCO readout scheme and timing diagram.



$f_{1\_intact} = f_0 - \Delta f_{retention}^{*} \pm \sigma^{*}$

$f_{1\_tampered} = f_0 - \Delta f_{tamper} - \Delta f_{retention} \pm \sigma$

* $\Delta f_{retention}$ is the freq. decrease caused by normal retention loss; σ is the freq. variation under normal conditions

Fig. 5. Counterfeit IC detection scheme using proposed sensor.

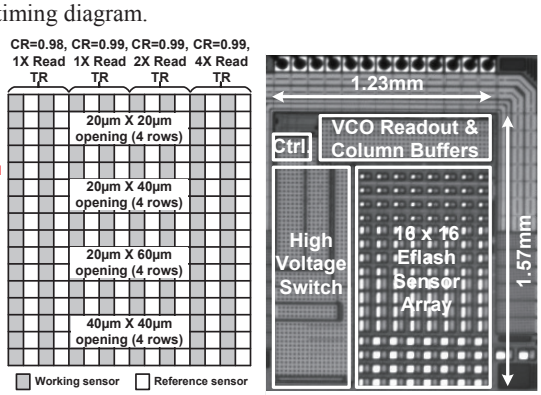


Fig. 6. (Left) Sensor configuration and opening sizing. (Right) Die microphotograph of 0.35μm test chip.

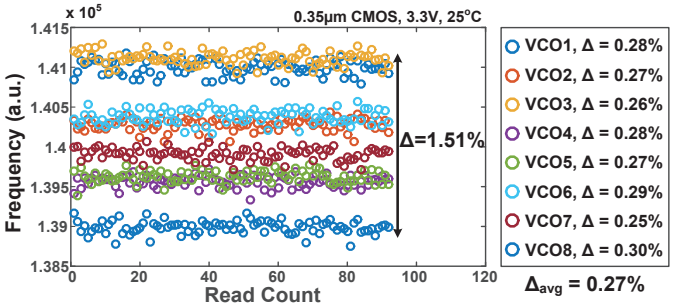


Fig. 7. Readout frequency variation of sensor cells.

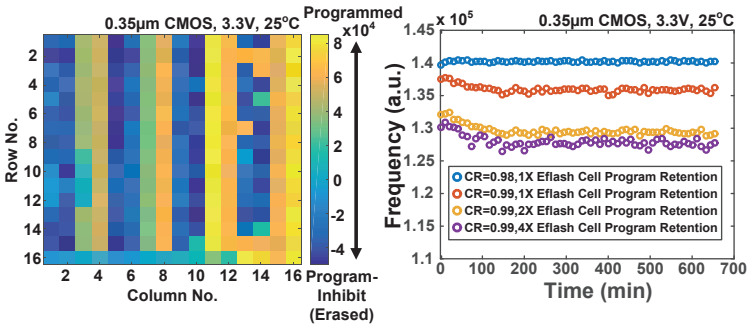


Fig. 8. Erase, program and program-inhibit operation characteristics and program retention test results.

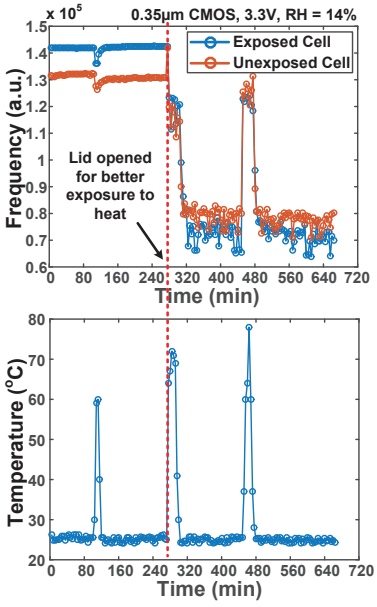


Fig. 9. Temperature test.

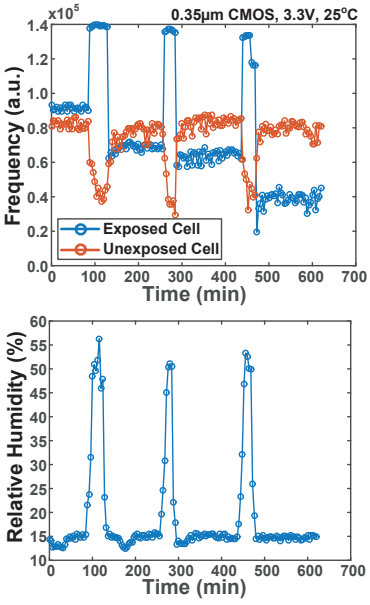


Fig. 10. Humidity test.

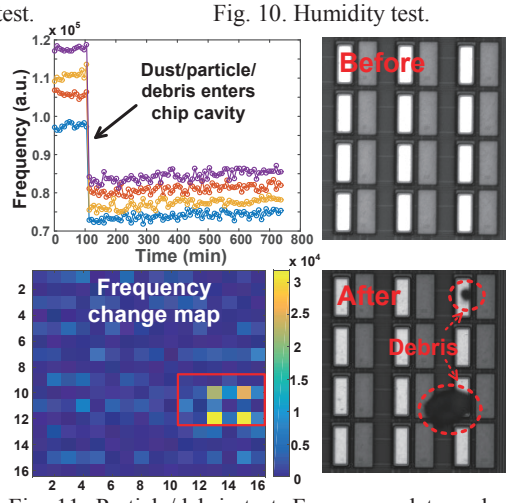


Fig. 11. Particle/debris test. Frequency data and microscope image showing debris location.