A small tamper-resistant anti-recycling IC sensor with a reused I/O interface and DC signalling

Alexandros Dimopoulos[1], *Member, IEEE*, Mihai Sima[1], *Member, IEEE*, and Stephen W. Neville[1], *Member, IEEE*

[1]Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada

Corresponding author: Alexandros Dimopoulos (email: adimopou@uvic.ca).

This work was supported in part by CMC Microsystems.

ABSTRACT Counterfeit electronic components are known to enter supply chains through recycling, with these already-aged components creating serious reliability risks, particularly for critical infrastructure systems. A number of recycled integrated circuit (IC) risk mitigation approaches have been proposed, but these generally lack pragmatic feasibility. This work proposes a novel real-world deployable on-board sensor that: 1) is tamper-resistant by exploiting near-permanent changes caused by hot carrier injection (HCI); 2) generates a DC signal measurable by common low-cost test equipment; and 3) reuses an existing I/O interface, including existing pins; while 4) requiring a very small footprint. Combining this sensor with a random sample-based testing strategy allows for low-cost and time efficient detection of fraudulently recycled batches of ICs. Through simulation-based validation using process-accurate models of a 65 nm technology we show that employing a random sample size as small as 60 is sufficient for identifying such batches with a statistical significance level of 0.01.

INDEX TERMS recycled integrated circuits, counterfeit detection, hot carrier injection (HCI).

I. Introduction

MODERN electronic industry supply chains span the globe and are of such high complexity that they lie outside the observability and control of individual companies and countries. This has made the industry a tempting target for counterfeiters. Beyond the economic impact, which is on the scale of $100 billion annually [1], counterfeit electronic components can severely impact the safety and reliability of critical systems in areas such as health care, defense, and transportation [2]. Recycled integrated circuits (ICs), where used components are diverted from waste streams, relabeled, and resold as new, are a particularly vexing class of counterfeits. Such components are still functional; however, their true ages and remaining useful lifetimes are unknown, leading to unexpected system failures. The U.S. Department of Defense has identified this as the greatest threat to the reliability of its systems [3].

Any proposed mitigation approaches to recycled ICs must be low-cost and efficiently deployable at real-world scales of tens of thousands to millions of ICs. Existing approaches, such as comparing electrical or physical characteristics against a golden reference are slow and cumbersome, and so lack scalability. Hence, focus has shifted to on-board sensors which can provide clear measures of an IC's age [4]. To be viable, such a sensor should: 1) be lightweight and easily integrable; 2) easily interface with low-cost, high-volume testing; 3) provide clear, consistent, and accurate age measures; and 4) be tamper-resistant.

A commonly explored approach has been ring-oscillator (RO) based sensors [5]–[8], whose RO frequencies decrease over time due to bias temperature instability (BTI) induced shifts in transistor threshold voltage. This approach has several limitations relative to the above-listed requirements. First, BTI degradation largely and quickly reverses once the responsible stress is removed [9]. Second, this approach requires accurate frequency measurements, which, if performed on chip requires an increased footprint to accommodate frequency counters, non-volatile memories, and associated control paths. Performing the measurements off-chip would entail higher-cost, less efficient AC testing as compared to simple DC measurements. In either case, a specialized I/O interface, possibly including a dedicated pin,

is required. Also, a major goal of RO sensors has been the higher resolution detection of relatively short IC ages, down to the scale of hours. However, by using the average age of mobile phones when discarded by users, which globally is in excess of 20 months [10], as a proxy for the age of recycled components, such counterfeits can reasonably be expected to range in age from months to years. The problem at hand is not to exhaustively determine the exact powered-on age of every IC, but instead to assess with reasonable accuracy whether a purchased batch of components is beyond a chosen powered-on age threshold set well below the expected age of recycled components, e.g., whether a batch is older than 6 months. At real-world scales of tens of thousands to millions of devices, exhaustive testing is untenable; low-cost, time efficient, random sample-based testing and assessment approaches must be used instead.

This work proposes a novel IC sensor to address the above problem which differs from the existing IC age sensor literature in the following ways:

1) it has improved tamper-resistance through exploiting hot carrier injection (HCI) which is known to be non-reversible [11];
2) it produces an DC signal that is easily measurable via standard low-cost testing equipment;
3) it makes use of existing I/O interfaces, thereby requiring no specialized interface circuitry, nor any extra pins;
4) it has a comparatively small footprint, allowing easy integration into an existing IC design;
5) it is designed to allow for low-cost, coarse time resolution age detection suitable to efficiently assess fraudulent reuse within larger volume IC batches.

The rest of this paper is organized as follows. Section II gives an overview of relevant background material. We present our sensor design in section III and describe its operation in IV. Section V demonstrates that our sensor enables the detection of 6 month old counterfeits through a random sampling approach applied to batches of uniformly aged devices. Section VI then provides the conclusions and future work.

II. Background

This section provides the background on hot carrier injection (HCI), which is chosen due to its ability to enact non-reversible changes. The HCI mechanism is reviewed, as is its modelling in the used technology.

A. HCI description

When a transistor's drain is held at a high voltage, energetic carriers in the channel, traditionally called hot carriers, can gain sufficient energy so as to be injected into the gate oxide. This creates defects in the oxide-channel interface which causes a near permanent shift in the threshold voltage [11], [12]. HCI has a greater impact on nMOSFETs than pMOSFETs and is inversely related to channel length [12]. HCI in long channel devices has been described by the lucky electron model, where the driving force is the lateral electric field [12]. Under this model peak HCI degradation is correlated with peak substrate current, which is generally estimated to occurs when $V_{\mathrm{GS}} = \frac{1}{2}V_{\mathrm{DS}}$. For modern technologies with channel lengths shorter than 250 nm, hot carriers are better described by an energy driven model where the effect depends on the total available energy. Peak HCI degradation occurs when $V_{\mathrm{GS}} = V_{\mathrm{DS}}$ under this regime [12].

B. HCI Modeling

Design and simulation were carried out using Synopsys HSPICE and the included MOSFET Reliability Analysis (MOSRA) facility [13] which models HCI effects as a percentage change in a MOSFET's drain current relative to initial conditions:

$$\Delta I_D(\%) = A_{\mathrm{p}} \cdot \mathrm{e}^{(G \cdot V_{\mathrm{GS}})} \cdot \mathrm{e}^{(D \cdot V_{\mathrm{DS}})} \cdot \mathrm{e}^{\left(\frac{-E_{\mathrm{a}}}{kT}\right)} \cdot \mathrm{e}^{(-m \cdot L)} \cdot t^n \quad (1)$$

where V_{GS}, V_{DS}, T, L, and t are respectively the gate voltage, drain voltage, temperature, drawn gate length, and time. The empirical parameters A_{p}, G, D, E_{a}, m, and n are technology-specific. Fitting data for these parameters can generally come from specially fabricated test devices or public domain data, with the latter introducing a 0.5 % error [14].

C. Technology

We designed and simulated our sensor using a foundry process design kit (PDK) for a 65 nm technology [15]. Such mature CMOS technologies, e.g., 40 nm and older, remain relevant as they represent 54 % of the existing fab capacity [16] and continue to dominate in safety and reliability critical domains, including the automotive industry [16]. Our design employs both core and I/O devices, the latter being larger and having thicker gates so as to operate at higher voltages but slower speeds. Using both types of devices allows us to better control the relative HCI degradation rate in different devices.

III. Sensor Design

Our sensor, dubbed the tamper-resistant HCI-based anti-recycling countermeasure with DC signalling (THARC-DC), shown in FIGURE 1, has the following features: 1) it is tamper-resistant due to its reliance on HCI; 2) it generates an easily measured DC signal; 3) it reuses an existing I/O interface, including the pins; and 4) it has a small footprint. To our knowledge, concurrently achieving 1-4 is unique to our design. FIGURE 1 also shows the integration of the THARC-DC into a typical I/O block consisting of a pin, an electrostatic discharge (ESD) protection composed of grounded gate MOSFETs [17], and a pair of buffers.

The sensor is embedded into an I/O block to: 1) enable access via an existing I/O pin thus simplifying integration and lowering cost and complexity; and 2) allow for easy access to the I/O power rail enabling larger voltages to be applied to $\mathrm{m}_{\mathrm{age}}$.

THARC-DC has a very simple structure. At its heart is the nMOSFET $\mathrm{m}_{\mathrm{age}}$ which experiences accelerated HCI degra-

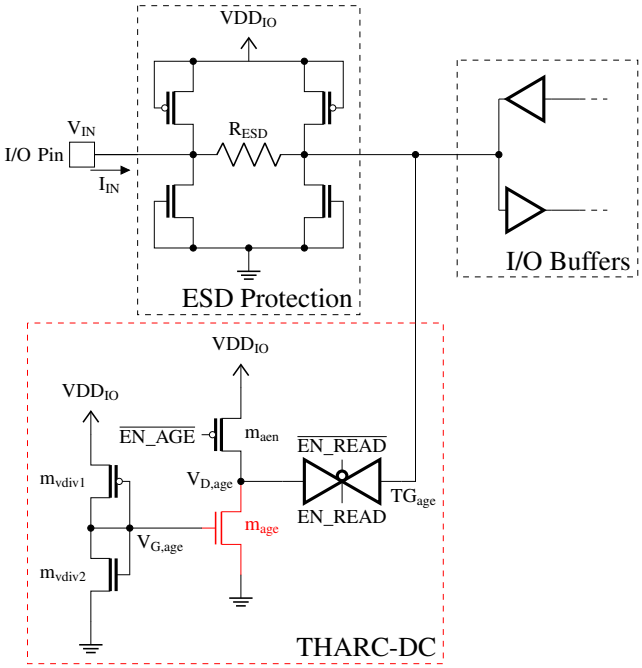

FIGURE 1. THARC-DC embedded into an existing I/O block. It is designed to subject m_{age} to an accelerated HCI degradation. It's state is assessed by the current it draws (I_{IN}) from the pin under a reference DC voltage (V_{IN}). I/O devices are depicted with thicker gates to differentiate them from the core device m_{age}.

dation. A voltage divider (m_{div1} and m_{div2}) and pMOSFET pass gate (m_{aen}) set the voltages on m_{age}. The sensor is connected to the I/O block through the transmission gate TG_{age}, allowing it to be read at the pin via standard DC testing.

The majority of THARC-DC comprises of I/O type devices, with m_{age} being a core type device. In this way, we can amplify the HCI stress on m_{age} while ensuring that all other devices experience no appreciable degradation. HCI in m_{age} can be maximized by: 1) minimizing the channel length; and 2) maximizing the gate and drain voltages. By using a minimum-sized core device for m_{age}, its channel is as short as possible.

It is well known that transistors operated at or below their technology's nominal voltages do not experience any appreciable degradation due to HCI or other mechanisms. This is by design so as to ensure a technology's reliability. Thus to subject m_{age} to a large HCI stress, its drain and gate voltages must exceed VDD_{core}, the nominal core voltage. This is easily done by tapping into the I/O power rail. However, the full I/O voltage, VDD_{IO}, cannot be applied to m_{age}'s gate without significantly increasing the risk of a gate oxide failure. The voltage divider sets $V_{G,age}$ higher than VDD_{core}, but not so high as to endanger the gate oxide. The size of m_{aen} is such that $V_{D,age}$ matches $V_{G,age}$, thus enabling the conditions for the maximum possible HCI stress. None of the I/O devices experience any appreciable HCI degradation since they are not subjected to any voltages in excess of VDD_{IO}.

IV. Sensor Operation

THARC-DC has the mutually exclusive operating modes of: **AGE**, for applying HCI stress to m_{age}, and **READ**, for assessing the accumulated HCI degradation of m_{age}. These modes are controlled respectively by the signals EN_AGE and EN_READ. **AGE** mode is concurrent with normal system operation so that IC powered-on age may be tracked. On the other hand, **READ** mode cannot be active during normal system operation since THARC-DC reuses an existing I/O pin and data collisions must be avoided. This does not present a problem as THARC-DC is intended to be read during standard DC testing arising between the IC's purchase and deployment. Additionally, the measurement benefits from the quieter electrical environment resulting from the lack of activity in the IC. As a result, EN_AGE and EN_READ can be tied to an existing control signal such as chip enable, clock enable, or reset, and as such do not need any dedicated control pins of their own. Both EN_AGE and EN_READ can be tied to the same signal since **AGE** and **READ** are mutually exclusive. In the following discussion, the sensor is assumed to be controlled by a system reset signal, named RESET, such that $\overline{\text{EN\_AGE}} = \text{RESET}$ and $\text{EN\_READ} = \text{RESET}$.

During normal system operation, $\text{RESET} = 0$ and THARC-DC is kept in **AGE** mode. The pass gate m_{aen} is activated ($\overline{\text{EN\_AGE}} = 0$) and the transmission gate TG_{age} is deactivated ($\text{EN\_READ} = 0$). This sets $V_{D,age}$ to a voltage higher than VDD_{core}, ensuring that m_{age} is subjected to an enhanced HCI stress. It also isolates the sensor from the rest of the I/O block so that it will not interfere with normal system operation.

When an end-user decides to place THARC-DC in **READ** mode, they set and maintain $\text{RESET} = 1$. This deactivates m_{aen} ($\overline{\text{EN\_AGE}} = 1$) and activates TG_{age} ($\text{EN\_READ} = 1$). The drain of m_{age} is disconnected from VDD_{IO} and connected to the I/O pin through the ESD protection. To read the sensor's state, a DC voltage V_{IN} is applied to the pin and I_{IN}, the resulting current drawn by m_{age}, is measured. With passing time, I_{IN} decreases due to the increasing HCI degradation of m_{age} accumulated during **AGE** mode. This very simple usage model is an intentional aspect of the sensor's design.

V. Results and Discussion

We simulated THARC-DC along with a typical ESD protection, as depicted in FIGURE 1, using Synopsys HSPICE [13] and a foundry process design kit (PDK) for a 65 nm technology [15]. HCI effects were only simulated in nMOSFETs since PMOSFETs are impacted to a far lesser extent [12].

The voltage divider and m_{aen} were sized so as to set both $V_{G,age}$ and $V_{D,age}$ to 1.1 V, which exceeds the VDD_{core} value

of 1.0 V but remains low enough to ensure a gate oxide lifetime in excess of 10 years in a core device [17]. Predicted typical HCI effects on m_{age} over 10 years are shown in FIGURE 2. While $V_{D,age}$ is pulled towards VDD_{IO} due to the diminishing voltage drop across m_{aen} as I_D falls, $V_{G,age}$ is held constant by the voltage divider and m_{age} is protected from a premature oxide failure.

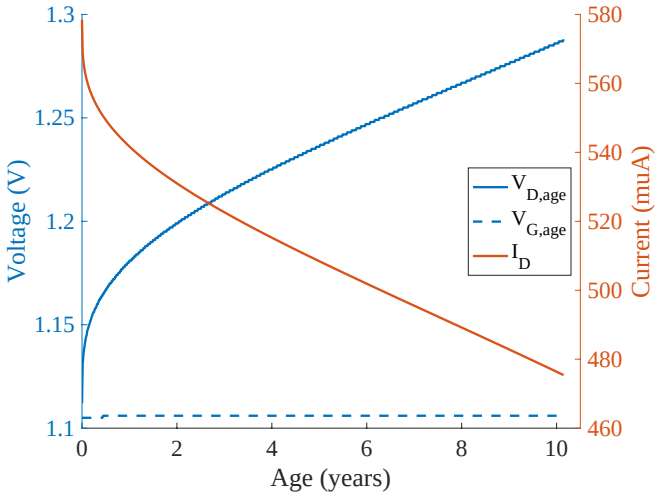

FIGURE 2. Predicted m_{age} degradation due to HCI while the sensor is operating in AGE mode. Results are from typical corner models.

FIGURE 3 shows I_{IN} measured during **READ** mode for different levels of V_{IN} as THARC-DC ages. As shown in FIGURE 3b, increasing V_{IN} leads to an increase in the measured degradation signal. For example, after one year I_{IN} will be measured to have degraded by 5.6 % when V_{IN} is 1.0 V and 5.9 % when V_{IN} is 1.8 V, a relative difference of about 5 %. The highest possible V_{IN} should therefore be used when measuring THARC-DC.

The results shown in FIGURE 3 are idealized since they were generated using typical corner models which do not account for manufacturing process variations [15]. For real sensors these variations must be taken into account, consequently the sensor measurements are described by the stochastic process $I_{IN}(t)$. At a given age t, $I_{IN}(t)$ is a random variable drawn from a distribution with a mean $\mu(t)$ and variance $\sigma^2(t)$, both of which exist but are assumed unknown.

Authenticating a batch of devices under test (DUTs) therefore consists of testing the hypothesis that $I_{IN}(t)$ is drawn from the same distribution as $I_{IN}(0)$. To simplify the situation for the end-user, we focus on the mean rather than the entire distribution. The Wald test is well-suited to testing the null hypothesis $H_0 : \mu(t) = \mu(0)$ [18]. The size α Wald test rejects H_0 if $\mu(0) \notin C$ where

$$C = \left(\hat{\mu}_n(t) - \frac{\hat{\sigma}_n(t)}{\sqrt{n}} z_{\alpha/2}, \hat{\mu}_n(t) + \frac{\hat{\sigma}_n(t)}{\sqrt{n}} z_{\alpha/2} \right) \quad (2)$$

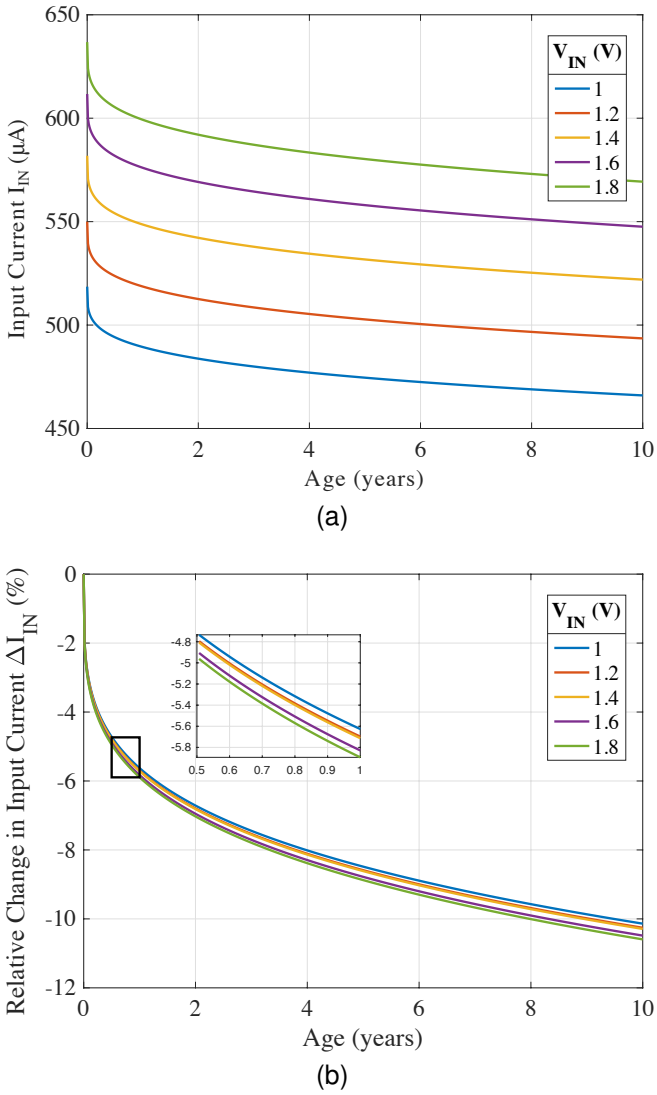

FIGURE 3. Input current drawn under different input voltages when the sensor is in READ mode: (a) absolute values and (b) relative degradation over time. Results are from typical corner models.

is the $1 - \alpha$ confidence interval on $\mu(t)$. Computing C requires the sample mean

$$\hat{\mu}_n(t) = \frac{1}{n} \sum_{i=1}^{n} I_{IN,i}(t), \quad (3)$$

the sample standard deviation

$$\hat{\sigma}_n(t) = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (I_{IN,i}(t) - \hat{\mu}_n)^2}, \quad (4)$$

the sample size n, and the $\alpha/2$ upper quantile of the standard Normal distribution $z_{\alpha/2}$. The only information not available to an end-user is $\mu(0)$, which can be easily provided by an IC manufacturer in a data sheet.

Minimizing the sample size is important for economical testing; however, too small an n can increase the chance of committing a type II error, where H_0 is incorrectly

retained, resulting in an incorrect authentication of the batch in question. The situation is illustrated in FIGURE 4. The sample size determines how how well $\hat{\mu}_n(t)$ estimates $\mu(t)$, as evidenced by $|C| \propto 1/\sqrt{n}$. As n increases, the confidence interval on $\mu(t)$ narrows and the chance of a type II error reduces. For every $t > 0$ there is a minimum sample size $n_{min}(t)$ for which $\mu(0) \notin C$. If $n < n_{min}(t)$, the Wald test will fail to reject H_0 and the batch will be erroneously accepted as authentic. For small t, $n_{min}(t)$ may be quite large, resulting in a practical lower limit on t below which a fraudulent batch is not detectable. As t increases, $\mu(t)$ moves away from $\mu(0)$, resulting in a decreasing $n_{min}(t)$.

It is impossible to prove that H_0 is correct, it can only be shown to be incorrect through sufficient evidence [18]. The goal of authentication is therefore to search for evidence that a batch is not authentic. An efficient strategy is to iteratively perform the Wald test with an increasing n until either H_0 is rejected or n becomes impractically large.

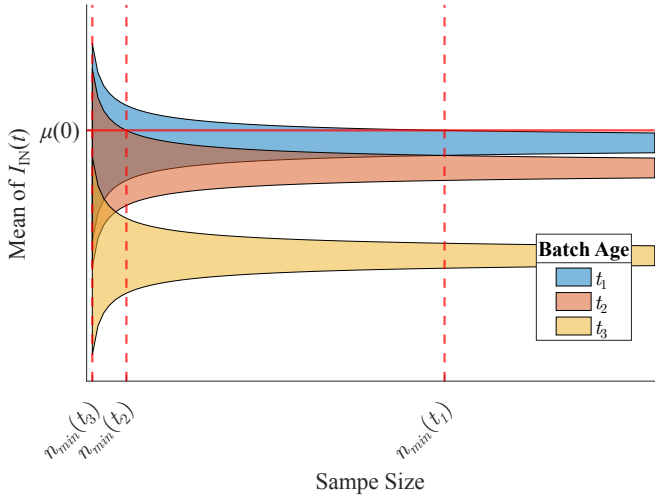

FIGURE 4. Illustration of the Wald test. Shaded regions show confidence intervals on $\mu(t)$ as a function of sample size. Confidence intervals for batches of three different ages $0 < t_1 < t_2 < t_3$ are shown. The Wald test rejects $H_0 : \mu(t) = \mu(0)$ if $\mu(0)$ falls outside of the shaded region. If $n < n_{min}(t)$, the Wald test will incorrectly fail to reject H_0 resulting in an erroneous authentication of the batch.

Knowledge of $n_{min}(t)$ is not required for carrying out an authentication, though it can make the process more efficient by aiding an end-user to select the initial n, decide how to increase it, and when to stop testing. An IC manufacturer would have to provide information about $n_{min}(t)$, for example by including a figure similar to FIGURE 5 in a data sheet. It shows $n_{min}(t)$ as a function of t for three levels of statistical significance. To produce it, a batch of 1000 THARC-DC was generated and aged over 10 years in 5-day steps through a Monte Carlo simulation using global variation models from the foundry PDK [15]. For each time step a sequence of random samples ranging in size from 50 to 1000 were drawn from the batch and each used to compute $C^{1-\alpha}_{\mu(t),n}$, the $1-\alpha$ confidence interval on $\mu(t)$ using n samples. Values for $C^{1-\alpha}_{\mu(t),n}$ computed in this way

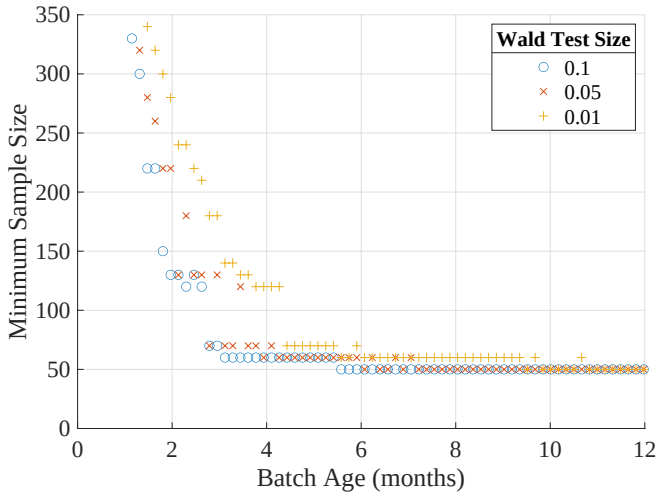

FIGURE 5. Minimum sample size as a function of batch age required to guard against erroneous authentication. Results are for Wald tests of sizes 0.1, 0.05 and 0.01.

depend on a specific draw of data. In order to find values for $n_{min}(t)$ which generalize, the variance of $C^{1-\alpha}_{\mu(t),n}$ must be estimated. This was done by constructing 99 % bootstrap pivotal confidence intervals [18] for both $\min\left(C^{1-\alpha}_{\mu(t),n}\right)$ and $\max\left(C^{1-\alpha}_{\mu(t),n}\right)$ through a 1000-fold bootstrap resampling. These new confidence intervals are expected to contain $C^{1-\alpha}_{\mu(t),n}$ 99 % of the time a random sample is drawn from the batch. These were then used to find $n_{min}(t)$.

Relying on FIGURE 5 for guidance, an end-user might choose to begin the authentication process by performing a Wald test of size 0.01 with an initial sample size of 60. If the test were to fail to reject H_0, they may then measure an additional 60 devices for a combined sample size of 120 and repeat the test. They would then continue in this fashion until either the test rejected H_0 or the sample size exceeded 330. If the test were to reject H_0 at any point, they would have strong evidence that the batch was fraudulent. If the test were to fail to reject H_0 with a sample size of 330, they could conclude that the batch age is no older than 1.5 months.

Our results show that a 6-month old batch, which we believe to be a reasonable lower bound on the age of fraudulently recycled devices, is detectable at a statistical significance level of $\alpha = 0.01$ by testing a random sample as small as 60. The youngest detectable batch at the same statistical significance level is 1.5 months old, which requires a sample size of 330. Batches younger than this may be detectable with a sample size in excess of 1000. The differences in $n_{min}(t)$ for the different values of α is minimal. Therefore using a size 0.01 Wald test requires only slightly more effort than a less rigorous size 0.1 test.

VI. Conclusions

We have demonstrated that THARC-DC, a small sensor designed to degrade under accelerated HCI, can be effectively

used to determine if a batch of ICs have been fraudulently recycled. THARC-DC exploits HCI degradation for tamper-resistance. Its interface piggy-backs onto an existing I/O interface and requires no additional pins or specialized control signals. Querying the sensor involves a DC measurement which requires only commonly available, low-cost, low-effort equipment and processes. It can be easily integrated into many systems thanks to its very small footprint. Authenticating a batch of ICs is rapidly done since exhaustive measurements are not required. Instead, successfully larger random samples are measured and analyzed until the status of the batch can be determined with the desired level of statistical significance. We have found that a sample size of 60 is sufficient to identify a batch of recycled ICs with a statistical significance of 0.01. Further simulations and analysis to examine sensor accuracy when a batch consists of mixed-aged devices may be of interest. To our knowledge, this is the first anti-recycling sensor proposed that concurrently: 1) is tamper-resistant due to its reliance on HCI, 2) generates an easily measured DC signal, 3) reuses an existing I/O interface, and 4) has a small footprint.

References

[1] U.S. Department of Commerce and U.S. Department of Homeland Security, "Assessment of the critical supply chain supporting the U.S. information and communications technology industry," Washington, DC, USA, Feb. 2022. [Online]. Available: https://www.dhs.gov/publication/assessment-critical-supply-chains-supporting-us-ict-industry.

[2] European Union Intellectual Property Office, "Intellectual property crime threat assessment 2022," Luxembourg, 2022. [Online]. Available: https://data.europa.eu/doi/10.2814/830719.

[3] U.S. Senate Committee on Armed Services, "Inquiry into counterfeit electronic parts in the department of defense supply chain," Washington, DC, USA, 112-167, May 21, 2012. [Online]. Available: https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf.

[4] 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," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014. DOI: 10.1109/JPROC.2014.2332291.

[5] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a lightweight on-chip sensor," in *Proceedings of the 49th Annual Design Automation Conference*, San Francisco, CA: ACM Press, Jun. 2012, pp. 703–708. DOI: 10.1145/2228360.2228486.

[6] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ICs," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 5, pp. 1016–1029, May 2014. DOI: 10.1109/TVLSI.2013.2264063. [Online]. Available: http://ieeexplore.ieee.org/document/6545382/.

[7] U. Guin, D. Forte, and M. Tehranipoor, "Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 4, pp. 1233–1246, Apr. 2016. DOI: 10.1109/TVLSI.2015.2466551.

[8] J. Diaz-Fortuny, P. Saraza-Canflanca, E. Bury, M. Vandemaele, B. Kaczer, and R. Degraeve, "A ring-oscillator-based degradation monitor concept with tamper detection capability," in *2022 IEEE International Reliability Physics Symposium (IRPS)*, Mar. 2022, pp. 1–7. DOI: 10.1109/IRPS48227.2022.9764609.

[9] T. Grasser, B. Kaczer, P. Hehenberger, *et al.*, "Simultaneous extraction of recoverable and permanent components contributing to bias-temperature instability," in *Proc. IEEE Electron Devices Meeting*, Washington, DC, USA: IEEE, Dec. 2007, pp. 801–804. DOI: 10.1109/IEDM.2007.4419069.

[10] A. Ng. "Smartphone users are waiting longer before upgrading — here's why," CNBC. (May 17, 2019), [Online]. Available: https://www.cnbc.com/2019/05/17/smartphone-users-are-waiting-longer-before-upgrading-heres-why.html (visited on 10/14/2023).

[11] M. Vandemaele, K.-H. Chuang, E. Bury, S. Tyaginov, G. Groeseneken, and B. Kaczer, "The influence of gate bias on the anneal of hot-carrier degradation," in *2020 IEEE International Reliability Physics Symposium (IRPS)*, Apr. 2020, pp. 1–7. DOI: 10.1109/IRPS45951.2020.9128218.

[12] T. Grasser, Ed., *Hot Carrier Degradation in Semiconductor Devices*, 1st ed, Cham, Switzerland: Springer International Publishing, 2015. DOI: 10.1007/978-3-319-08994-2.

[13] "HSPICE user guide: Basic simulation and analysis," Synopsys, Inc., Mountain View, CA, Jun. 2017.

[14] A. Dimopoulos, M. Sima, and S. W. Neville, "Leveraging public information to fit a compact hot carrier injection model to a target technology," *IEEE Access*, vol. 11, pp. 21 417–21 426, 2023. DOI: 10.1109/ACCESS.2023.3251340.

[15] "TSMC 65 nm CMOS RF mixed signal general purpose plus 1P9M+ salicide Cu_lowK 1.0&2.5V SPICE model 65RS," Taiwan Semiconductor Manufacturing Co., LTD, Dec. 30, 2011.

[16] S. K. Moore, D. Johnson, M. Harris, E. Waltz, P. Patel, and M. Hampson, "The latest developments in technology, engineering, and science: News," *IEEE Spectr.*, vol. 58, no. 8, pp. 5–12, Aug. 2021. DOI: 10.1109/MSPEC.2021.9502948.

[17] "TSMC 65 nm/ 55 nm CMOS LOGIC/MS_RF DESIGN RULE (CLN65 G/GP/LP/LPG/ULP, CLN55 GP/LP, CMN65 GP/LP, CMN55LP)," Taiwan Semiconductor Manufacturing Co., LTD, Apr. 20, 2012.

[18] L. Wasserman, *All of statistics: a concise course in statistical inference* (Springer texts in statistics). New York, NY: Springer, 2004, ISBN: 978-0-387-40272-7.

Alexandros Dimopoulos(M'04) received the B.Eng. degree in electrical engineering from the University of Victoria, Victoria, Canada in 2005 and the M.A.Sc. degree in electrical engineering from the University of British Columbia, Vancouver, Canada in 2012. He is currently pursuing the Ph.D. degree in electrical engineering at the University of Victoria, Victoria, Canada.

His research interests include hardware security; statistical data analysis, machine learning, and AI.

Mr. Dimopoulos is the recipient of a Doctoral Postgraduate Scholarship (Natural Sciences and Engineering Research Council of Canada).

Mihai Sima(S'00–M'04) received his B.Eng. degree in electronics engineering from Polytechnic Institute of Bucharest, Romania in 1989, and his Ph.D. degree in computer engineering from Delft University of Technology, The Netherlands, in 2004.

He was a guest scientist in Philips Research Laboratories, Eindhoven, The Netherlands, between 1999–2003. Since 2003, he has been a faculty member in the Department of Electrical and Computer Engineering at the University of Victoria, British Columbia, Canada. His research interests include computer architecture, reconfigurable computing, embedded systems, and circuit design.

Dr. Sima is a registered Professional Engineer in the province of British Columbia. He received the Best Paper Award in the IEEE International Conference on Computer Design in 2001.

Stephen W. Neville(M'85) received his B.Eng, M.A.Sc., and Ph.D. from the University of Victoria, Canada in 1990, 1992, and 1998 respectively.

He joined the University of Victoria in 2003, after serving in Canadian and S.F. Bay area industry positions. He is currently a Professor of Software Engineering in the Department of Electrical and Computer Engineering. He also serves as the Director of Software Engineering and co-manager of Entrepreneurship@UVic, through which he has co-founded seven successful high-tech companies. Dr. Neville's research focuses on at-scale industry-applied issues spanning: software engineering; statistical data analysis, machine learning, and AI; cyber-security and privacy; and high-tech entrepreneurship.