Self-powered Sensing and Time-Stamping of Tampering Events

Darshit Mehta
Biomedical Engineering
Washington University in St. Louis
St. Louis, MO 63112, USA

Liang Zhou and Kenji Aono
Computer Science and Engineering
Washington University in St. Louis
St. Louis, MO 63112, USA

Shantanu Chakrabartty
Electrical and Systems Engineering
Washington University in St. Louis
St. Louis, MO 63112, USA
Email: shantanu@wustl.edu

***Abstract*—While many techniques exist for detecting mechanical tampering in an integrated circuit supply-chain, estimating the time-of-occurrence of the tampering event has proven to be challenging. This work builds upon our previously demonstrated self-powered mechanical event detector and self-powered timing device to report a chip-scale system that can accurately time-stamp the occurrence of the tampering event. The proposed system uses a combination of Fowler-Nordheim tunneling for continuous time-keeping and a linear hot-electron injector for sensing and recording of mechanical events. Using devices fabricated in a 0.5 μ-m standard CMOS process, we demonstrate event time-stamping with an accuracy of 95% over a duration of 3 days. This accuracy can be further improved by incorporating a parametric model during the system calibration phase.**

I. Introduction

Detection of malicious tampering (mechanical (Fig. I), electrical or optical) is one of the keys towards securing an integrated circuit supply-chain [1], [2]. While several technologies exist, for example smart labels [3], nano-dots [4], chiplets that can detect tampering by incorporating sensors, these technologies are unable to time-stamp when the tampering occurred in the supply-chain. In many instances, this information is vital because it can help identify the tampering source. The limitation in sensing time-of-occurrence arises due to the lack of a continuously running reference clock that can operate without any external powering. In our previous work, we have shown systems that can sense, harvest energy from and record mechanical events [5]. This system was used for storing cumulative count of measured events. There was no time reference and this system could not record the time stamp of events. We later demonstrated time-keeping abilities of a Fowler–Nordheim (FN)-tunneling-based device [6], which was subsequently developed as self-powered system capable of recording the time-of-occurrence of an event [7]. There, we used a timer and injector hybrid system, and we could achieve an accuracy of 93 % in determining the time of occurrence of an event. One limitation of the system was that the duration of the event had to be known a priori, which might not always be the case. To overcome this limitation, we propose a new differential architecture that can measure the duration of an event as well as its time of occurrence.

The proposed system consists of two timer-injector interfaces from [7]. One of the timers acts as a capacitor with constant charge on its floating gate terminal, while the other is biased in the FN tunneling region, where there is a slow leakage of charge. These timers then control how much charge is injected into the gates of the linear injectors, and this information is recorded on the non-volatile memory of the injectors. The former timer-injector pair provides a response that is proportional only to the duration of the event, while the response from the latter is dependent on the time-of-event and duration of an event. This information can be retrieved later asynchronously and a combination of the two measurements is used to predict the time-of-occurrence and duration of the event.

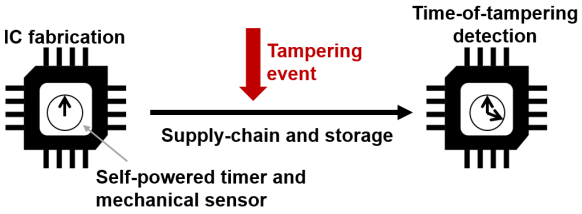

Figure 1. Proposed device can detect time-of-tampering using a self-powered mechanical sensor along with a self-powered timing device

II. Principle of Operation

The principle of operation of the proposed system is shown in Fig. II with an equivalent circuit model. The first timer acts as a constant voltage reference as there is no leakage path for the charge on the capacitor. The second timer can be described by a voltage on a capacitor that is being discharged by a sink current ($I_{\mathrm{timer},2}$). The two timer voltages ($V_{\mathrm{timer},1}$ and $V_{\mathrm{timer},2}$) are used to control rate of injections ($I_{\mathrm{inj},1,2}$) of charge on another pair of capacitors. The signal being sensed controls the switches S1 and S2, which activate the injection circuits.

Several challenges present themselves when implementing a timer using a capacitor and current sink, that is reliable, accurate and can last for several years, without any powered active devices. The discharge current needs to be on the order of 10^{-20} A and its dynamics need to be reliable and well characterized. In our previous work, we have shown that electron discharge through FN tunneling creates a timing device that works dependably for over 3 years.

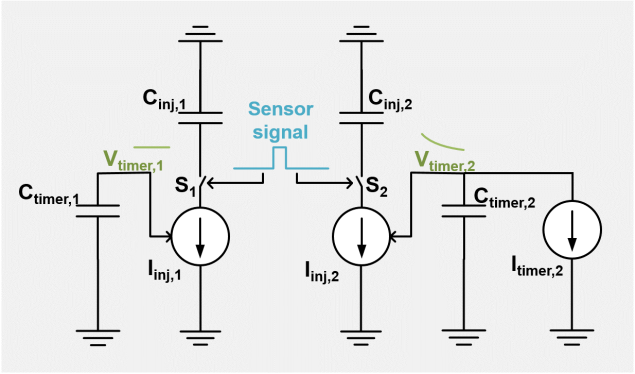

Figure 2. Principle of operation of the proposed time-stamping device

From [6], the timer voltage can be expressed as a function of time (t) and device parameters.

$$V_{\text{timer}}(t) = \frac{k_2}{\ln(k_1 t + k_0)} + V_{\text{sub}} \tag{1}$$

where k_0, k_1 k_2 are model parameters estimated from the device form factors and V_{sub} is the equivalent voltage drop at the substrate of the device. A current sink I_{timer} discharges a pre-charged capacitor, therefore, a change in V_{timer} serves as a measure of time elapsed.

The timer voltage modulates the injector current sink I_{inj}, which in turn discharges another capacitor C_{inj}. This current is supplied by the energy from a sensor transducer, allowing the voltage across the capacitor element to be a measure of the time-of-occurrence of sensor activation event. Circuit details of the injector are shown in Fig. 3c, with the description of the circuit in the next section. Rate of injection for the injector circuit given by [8]

$$I_{\text{inj}}(t) = \beta I_{\text{ref}} \exp\left(\frac{V_{\text{ref}}}{V_{\text{inj0}}}\right) \tag{2}$$

Rate of injection can be made to be a function of time by connecting the timer output to the V_{ref} terminal of the injector.

$$I_{\text{inj}}(t) = \beta I_{\text{ref}} \exp\left(\frac{V_{\text{timer(t)}}}{V_{\text{inj0}}}\right) \tag{3}$$

For a signal with duration Δt_{s} much smaller than the time span of the recording, and occurring at time t_{s}

$$\Delta V_{\text{inj,timer}}(T) = C_{\text{inj}} \beta I_{\text{ref}} \exp\left(\frac{V_{timer(t_{\text{s}})}}{V_{\text{inj0}}}\right) \Delta t_{\text{s}} \tag{4}$$

There are two unknown variables in the equation – t_{s} and Δt_{s}. By adding in a reference injector, for which the output does not depend on the time of occurrence, Δt_{s} can be eliminated. For the reference injector,

$$\Delta V_{\text{inj,ref}}(T) = C_{\text{inj}} \beta I_{\text{ref}} \exp\left(\frac{V_{\text{ref}}}{V_{\text{inj0}}}\right) \Delta t_{\text{s}} \tag{5}$$

Taking the ratio of Eqns. (4) and (5):

$$\frac{\Delta V_{\text{inj,timer}}(T)}{\Delta V_{\text{inj,ref}}(T)} = \exp\left(\frac{V_{timer}(t_{\text{s}}) - V_{\text{ref}}}{V_{\text{inj0}}}\right) \tag{6}$$

t_{s} can now be estimated from equations (1) and (6).

If needed, Δt_{s} can also be empirically estimated from the reference injector output and comparing it to $\Delta V_{\text{inj,ref}}$ measured for signal of known duration

$$\Delta \widehat{t_{\text{s}}} = \Delta V_{\text{inj,ref}} * \frac{\Delta t_{\text{s}}(\text{known})}{\Delta V_{\text{inj,ref}}(\text{known})} \tag{7}$$

III. Circuit Implementation

A top level view of the timer, injector and level shifter circuits is shown in 3. The architecture of the system is similar to the time stamping system found in [7]. The schematic of a timer circuit is shown in Fig. 3b. It consists of a pair of capacitively coupled floating gate transistors, M_{fg}, which is biased in the FN tunneling region, and M_{fgr} which is used for readout. The charge on each floating gate can be precisely controlled through tunneling and charge injection. The readout circuit has been modified from [7] by integrating a level shifter at the readout stage. For detailed description of different sub-circuits, please refer to [7]. The two PMOS diodes act as a level shifter and help in matching the dynamic range of the two systems. They allow V_{SD} for M_{fgr} to be below 4 V, so as to prevent injection; while the output is high enough to induce injection in the injector circuit.

The injector circuit is realized using a PFG (piezoelectric driven floating gate) sensor which is a polysilicon strip fully insulated using high quality dioxide. Briefly, it consists of a PMOS transistor with its gate floating, a feedback amplifier that maintains the source voltage to V_{ref} and sets the gate voltage such that current flowing through the PMOS transistor is equal to I_{ref}. This topology ensures constant rate of injection, and the total injection only depends on time of deactivation of switch RdEn for a constant V_{ref}.

Finally, the two circuits are interfaced with each other by connecting the timer output to the V_{ref} pin of the injector.

IV. Results

A. Chip fabrication and validation

The timers and injectors were implemented using 0.5μ CMOS process on separate IC chips (micrograph of timer chip shown in Fig. 3a). They were independently programmed and tested according to [7]. The floating gate voltage at M_{fg} of timer 1 was programmed to around 2V, while for second timer, it was charged up to 9V using a combination of injection and tunneling. This ensured FN tunneling only occurred in the second timer. The readout voltage for timer 1, which is supposed to hold steady for the duration of the experiment, was programmed to 5V. $V_{timer,2}$ was programmed to 5.5V for each run, so that it would discharge down to 4.8V in 3 days. The timer outputs were then connected to the V_{ref} pins of the injectors.

In a real-world application, external power would be used for programming of the two systems and for asynchronous

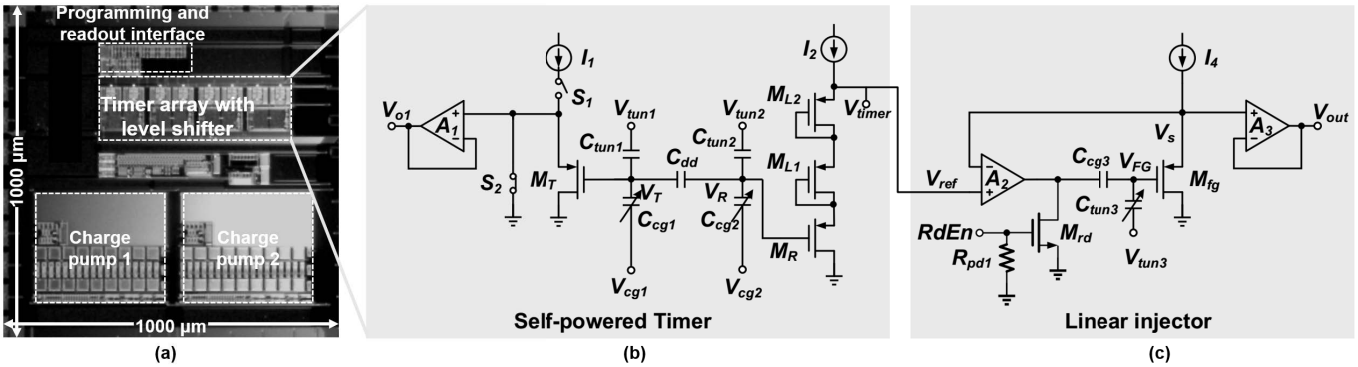

Figure 3. Top level view of timer and injector devices. a) Chip micrograph of the timer array with integrated level shifter. b) Self-powered timer circuit. c) Linear injector circuit

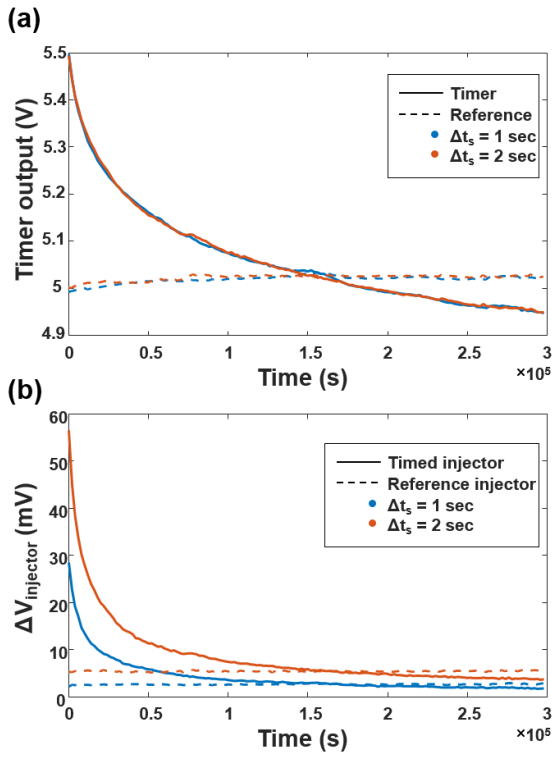

Figure 4. Experimental results from 2 different runs that were each carried over a period of 300,000 seconds, with events occurring every 2,000 sec. In each run the duration of the sensor signal was fixed to 1 or 2 secs. a) Timer outputs b) Injector responses.

readout of the injector output, while the actual operation would be completely self-powered. Since our goal here is to demonstrate an event reconstruction approach, a wired plug-and-play system is used for all experiments. A function generator was used for emulating the sensor signal, with each experimental run lasting for 300,000 sec (3.5 days). For each run, pulse duration was fixed to a value between 0.1 and 3 sec, and the pulse was set to occur every 2000 sec. The time-of-occurrence of each event, readout voltages of the two sets of timers and injectors were measured before and after the injection. A model was fit on a subset of points to relate the measured responses with $t_s$and Δt_s of the events. This model was then used to reconstruct events.

B. Experimental results

Output response of the two timers is shown in Fig. 4a. All the voltages were within the range 4.95V - 5.5V, sufficient for generating an injection current in the injector. Even though, experiments were carried over multiple weeks, the timers were well synchronized. The mean standard deviation of timer outputs at a given time instance was 2.7 mV (0.05%). A small, but consistent, unintentional drift (30 mV) was observed in timer 1 output. But the drift did not have a significant impact on injection (Fig. 4b). The overall standard deviation in the measured output for timer 1 was 7.7 mV.

Injector responses are shown in Figs. 4b. Each event leads to charge injection on to the floating gate. Even though the same event was applied for the experimental span, injected charge monotonically decreases with time, indicating modulation with the timer output. In fact, the measured charge injections had a correlation coefficient of 0.95 ($p < 10^{-20}$) with the exponential of timer voltage.

From the first two runs, 3 data points (out of 300) had to be discarded because they were determined to be outliers. A possible reason for this is charge injection from the read enable switch at the injector. This problem was resolved by lowering the strength of the feedback amplifier and increasing the control voltage at RdEn switch. We did not observe this behavior for the later runs.

C. Estimation of time-of-occurrence

The time stamping methodology was similar to the one employed in [7]. For calibration and model fitting, one of the experimental run was chosen to be the base model. 30% of data from output of injector 2, were selected and smoothed. If Y is the smoothed response then the model $Y = \Delta V_{inj2}(\Delta t_s = \Delta t_{s,base}) = F(t_s)$ to be fitted has the form:

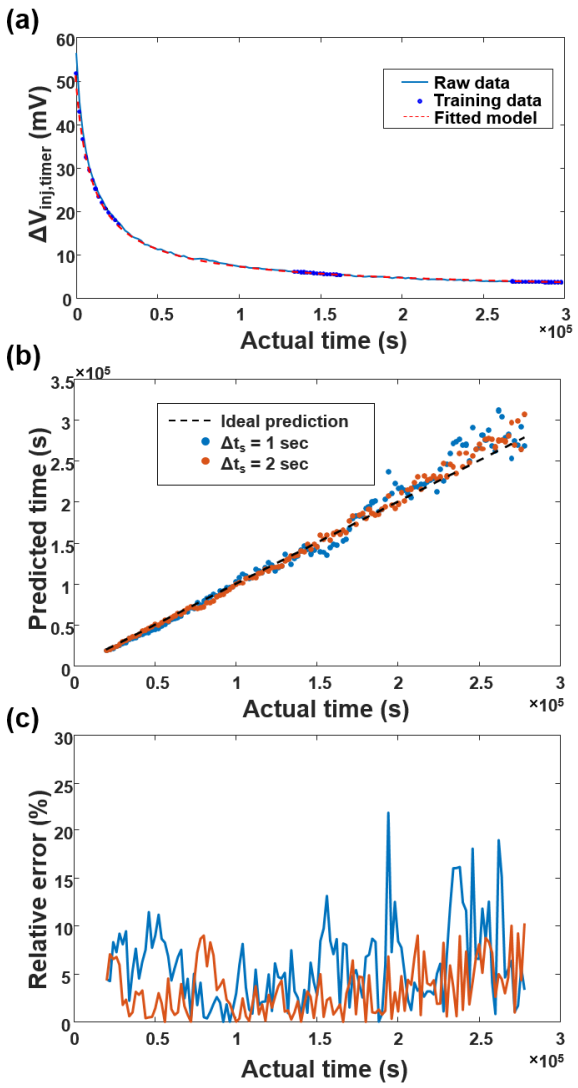

Figure 5. a) Estimation of time-of-occurrence from output of injector 2 and from Δt_s estimated previously b) Relative errors in the estimation when compared with true values as a function of time

$$F(t_s) = a \cdot \exp\left(\frac{b}{\log(c \cdot t_s + d)}\right) \tag{8}$$

The above model was fit in MATLAB using the Curve Fitting toolbox. We chose $\Delta t_{s,base}$ = 2 sec. For t_s measured in seconds and ΔV_{inj2} measured in mV, the estimated parameters had the values:

a	b	c	d
$6\,e{-}06$	285.9	$6.6\,e{+}03$	$6\,e{+}07$

To obtain the time stamp from the model, Eqn. 8 can be analytically inverted.

$$t_s = F^{-1}(Y) = \frac{\exp\left(\frac{b}{log(Y/a)}\right) - d}{c} \tag{9}$$

The time-stamp estimated from this equation is valid for injections with duration 2s. For time stamping events of arbitrary durations, they need to be scaled according to the duration of the event estimated previously. Specifically, from the injector output,

$$Y = \frac{\Delta V_{\text{inj2}}}{\Delta \hat{t}_s} \cdot \Delta t_{s,\text{base}} \tag{10}$$

Time-of-occurrence estimation is shown in IV-C. We observed that the estimated time-of-occurrence of events was off the true value by an average of 4.5%.

V. Conclusion

In this paper, we have described a system capable of recording the time-of-occurrence as well as the duration of an arbitrary event, while scavenging energy from the ubiquitous thermal energy and the sensor signal. By using a combination of timer and injector interfaces, we were able to time-stamp arbitrary events with 95% accuracy. This system could potentially be used for detecting physical tampering events and time stamping them, in IC products supply chain.

Acknowledgment

This work was supported in part by the National Science Foundation under Grant ECCS-1550096,CNS-1646380, DGE-0802267 and DGE-1143954.

References

[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE design & test of computers*, vol. 27, no. 1, 2010.

[2] 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, 2014.

[3] K. G. Conwell and M. Adams, "Tamper evident smart label with rf transponder," Aug. 22 2006. US Patent 7,095,324.

[4] R. Arppe and T. J. Sørensen, "Physical unclonable functions generated through chemical methods for anti-counterfeiting," *Nature Reviews Chemistry*, vol. 1, no. 4, p. 0031, 2017.

[5] C. Huang, P. Sarkar, and S. Chakrabartty, "Rail-to-rail, linear hot-electron injection programming of floating-gate voltage bias generators at 13-bit resolution," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 11, pp. 2685–2692, 2011.

[6] L. Zhou and S. Chakrabartty, "Self-powered timekeeping and synchronization using fowler–nordheim tunneling-based floating-gate integrators," *IEEE Transactions on Electron Devices*, vol. 64, no. 3, pp. 1254–1260, 2017.

[7] L. Zhou, K. Aono, and S. Chakrabartty, "A cmos timer-injector integrated circuit for self-powered sensing of time-of-occurrence," *IEEE Journal of Solid-State Circuits*, 2018.

[8] C. Huang, N. Lajnef, and S. Chakrabartty, "Calibration and characterization of self-powered floating-gate usage monitor with single electron per second operational limit," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 3, pp. 556–567, 2010.