Abstract—Self-powered timers provide a mechanism to achieve temporal synchronization between two passive devices (for e.g., RF tags, credit/access cards, and thumb drives) without the need for any external powering or clocks. As a result, the timers could be used to implement dynamic SecureID type authentication involving random keys and tokens that need to be periodically generated and synchronized. We report a novel solid-state self-powered timer, which exploits a self-compensating mechanism in the physics of Fowler–Nordheim quantum transport of electrons tunneling onto a floating gate. The proposed devices have been fabricated using standard CMOS processing and are demonstrated to be operational for durations greater than three years using extrapolation studies. The fabricated devices were also found to be extremely robust to device mismatch and as a result of which, the proposed self-powered timers can be synchronized with respect to each other with an accuracy greater than 0.5%.

Index Terms—Floating gate, Fowler–Nordheim tunneling (FNT), quantum tunneling, self-powering, timekeeping, zero-power devices.

I. INTRODUCTION

AUTHENTICATION techniques using encryption, strong hash functions, and pseudorandom number generators [1]–[3] are necessary for providing secure access to critical data and assets. However, for passive assets like credit cards and passive Internet-of-thing (IoT) devices like RF tags and sensors, the use of these techniques is impractical due to limited computational bandwidth and due to limited availability of energy [4], [5]. In addition, the lack of access to a continuously running system clock obviates the use of dynamic authentication techniques like SecureID on these devices, where random keys need to be periodically generated and synchronized [6]. In this regard, zero-power and self-powered timers that operate without any external powering [7] can overcome this limitation and provide a mechanism for dynamic trust verification of passive assets. The approach is shown in Fig. 1 where self-powered timers integrated on different passive assets (for e.g., credit cards and tags) are synchronized with respect to a “gold-standard” timer located on a remote authentication server. Rapid trust verification can then be achieved by comparing synchronized tokens (e.g., random numbers in the case of secureID type approach [6]) that are seeded using the outputs from the self-powered timers. Because the approach does not involve any static identifiers, for example, bar codes or product IDs, compared with a conventional passive authentication methods [4], [8], the proposed dynamic technique should be more secure and will make the passive assets immune to theft, counterfeiting, or tampering.

However, the success of this approach relies on the three key attributes of the self-powered timer: 1) the timers need to continuously operate over a time period that matches the life cycle or the shelf life of the passive asset (at least for three years [9]); 2) different timers can be accurately synchronized with respect to each other, as shown in Fig. 1; and 3) an accurate behavioral model that can be used for implementing the “gold standard” timer on the authentication server, also shown in Fig. 1. All these attributes require predictability in timer operation as well as availability of timer parameters that can be reliably adjusted for calibration and synchronization. In [7], we had proposed a zero-power timer device based on electron-leakage through synthetic oxide traps. While the device was shown to be operational for durations greater than 100 h, the dynamics of the electron-leakage process was found

Fig. 1. Trust verification based on synchronization between self-powered timers on different passive assets like credit cards and passive RFID tags.

Verification Server “Gold Standard” Timer

Synchronization

Rapidi Signature Verification

Fig. 1. Trust verification based on synchronization between self-powered timers on different passive assets like credit cards and passive RFID tags.

and provide a mechanism for dynamic trust verification of passive assets. The approach is shown in Fig. 1 where self-powered timers integrated on different passive assets (for e.g., credit cards and tags) are synchronized with respect to an “gold-standard” timer located on a remote authentication server. Rapid trust verification can then be achieved by comparing synchronized tokens (e.g., random numbers in the case of secureID type approach [6]) that are seeded using the outputs from the self-powered timers. Because the approach does not involve any static identifiers, for example, bar codes or product IDs, compared with a conventional passive authentication methods [4], [8], the proposed dynamic technique should be more secure and will make the passive assets immune to theft, counterfeiting, or tampering.

However, the success of this approach relies on the three key attributes of the self-powered timer: 1) the timers need to continuously operate over a time period that matches the life cycle or the shelf life of the passive asset (at least for three years [9]); 2) different timers can be accurately synchronized with respect to each other, as shown in Fig. 1; and 3) an accurate behavioral model that can be used for implementing the “gold standard” timer on the authentication server, also shown in Fig. 1. All these attributes require predictability in timer operation as well as availability of timer parameters that can be reliably adjusted for calibration and synchronization. In [7], we had proposed a zero-power timer device based on electron-leakage through synthetic oxide traps. While the device was shown to be operational for durations greater than 100 h, the dynamics of the electron-leakage process was found

and provide a mechanism for dynamic trust verification of passive assets. The approach is shown in Fig. 1 where self-powered timers integrated on different passive assets (for e.g., credit cards and tags) are synchronized with respect to an “gold-standard” timer located on a remote authentication server. Rapid trust verification can then be achieved by comparing synchronized tokens (e.g., random numbers in the case of secureID type approach [6]) that are seeded using the outputs from the self-powered timers. Because the approach does not involve any static identifiers, for example, bar codes or product IDs, compared with a conventional passive authentication methods [4], [8], the proposed dynamic technique should be more secure and will make the passive assets immune to theft, counterfeiting, or tampering.

However, the success of this approach relies on the three key attributes of the self-powered timer: 1) the timers need to continuously operate over a time period that matches the life cycle or the shelf life of the passive asset (at least for three years [9]); 2) different timers can be accurately synchronized with respect to each other, as shown in Fig. 1; and 3) an accurate behavioral model that can be used for implementing the “gold standard” timer on the authentication server, also shown in Fig. 1. All these attributes require predictability in timer operation as well as availability of timer parameters that can be reliably adjusted for calibration and synchronization. In [7], we had proposed a zero-power timer device based on electron-leakage through synthetic oxide traps. While the device was shown to be operational for durations greater than 100 h, the dynamics of the electron-leakage process was found

and provide a mechanism for dynamic trust verification of passive assets. The approach is shown in Fig. 1 where self-powered timers integrated on different passive assets (for e.g., credit cards and tags) are synchronized with respect to an “gold-standard” timer located on a remote authentication server. Rapid trust verification can then be achieved by comparing synchronized tokens (e.g., random numbers in the case of secureID type approach [6]) that are seeded using the outputs from the self-powered timers. Because the approach does not involve any static identifiers, for example, bar codes or product IDs, compared with a conventional passive authentication methods [4], [8], the proposed dynamic technique should be more secure and will make the passive assets immune to theft, counterfeiting, or tampering.

However, the success of this approach relies on the three key attributes of the self-powered timer: 1) the timers need to continuously operate over a time period that matches the life cycle or the shelf life of the passive asset (at least for three years [9]); 2) different timers can be accurately synchronized with respect to each other, as shown in Fig. 1; and 3) an accurate behavioral model that can be used for implementing the “gold standard” timer on the authentication server, also shown in Fig. 1. All these attributes require predictability in timer operation as well as availability of timer parameters that can be reliably adjusted for calibration and synchronization. In [7], we had proposed a zero-power timer device based on electron-leakage through synthetic oxide traps. While the device was shown to be operational for durations greater than 100 h, the dynamics of the electron-leakage process was found
to be unpredictable and difficult to control. In this paper, we propose self-powered timers based on the physics of Fowler–Nordheim (FN) quantum transport of electrons tunneling into a floating gate [10]. The physics of FN tunneling (FNT), described in Section II, inherently scavenges the thermal activation energy and can be viewed as the self-powering mechanism for the proposed timers. Note that the power levels in thermal noise (fluctuations) lie well below $10^{-18} \cdot 10^{-16}$ W, which is too scarce for any conventional energy scavenging circuit to be operational. In the proposed self-powered timing device, as shown in Fig. 2, the rectification diode is implemented using the triangular quantum-mechanical tunneling barrier, which is coupled to a floating gate. We will show in Section III that continuous integration of tunneled electrons onto the floating gate leads to an ultrareliable and robust quasi-linear response that can be then used for timekeeping and synchronization. The floating gate also serves as a nonvolatile accumulator (counter), whose value can be asynchronously interrogated using an externally powered circuit, as shown in Fig. 2 and according to previously reported approaches [11]. Section III presents measurement results using timer prototypes fabricated in a 0.5-μm standard CMOS process. The results not only validate the behavioral model of the timer but also show that the timer can be functional for durations greater than three years. In addition, we present measurement results that demonstrate synchronization accuracy up to 0.5%. Sections IV and V conclude this paper with a brief discussion about the effect of ambient temperature variations on the timer response and possible mechanisms for compensation.

II. FN Tunneling-Based Self-Powered Timers

The structure of a generic FN timer comprises of a strip of poly-crystalline silicon (polysilicon) that is completely insulated by high-quality, thermally grown silicon-di-oxide. This polysilicon strip, also referred to as a floating gate, serves as a reservoir of electrons and the surrounding oxide will serve as an energy barrier (shown in Fig. 2) that prevents the electrons to leak out by means of thermionic emission. Electrons, however, can tunnel through the oxide using three mechanisms: 1) trap-assisted tunneling (TAT) where carriers tunnel through the oxide layer with the assistance of trap states [12]; 2) direct tunneling (DT) where carriers directly tunnel through the rectangular barrier formed by the oxide layer [13]; and 3) FNT where carriers tunnel through a triangular-shaped barrier which results from the presence of a strong electric field across the barrier [14]. TAT depends on the number and distribution of traps and is difficult to control and modulate externally. It is also negligible in CMOS floating-gate structures, because the oxide is thermally grown, thus, the interface between the polycrystalline silicon and silicon-di-oxide has very a few defects or electron traps. DT relies on the thickness of the oxide layer and only becomes prominent, when the thickness of the dielectric layer is small (for silicon-di-oxide, less than 5 nm). Oxide thickness is a process specific parameter and cannot be modulated or controlled. However, in the literature, DT current has been exploited to implement large time-constant and ultralow-power watch-dog timers [15].

FNT, on the other hand, depends on the shape of the energy barrier across the dielectric (oxide) layer, which can be controlled and modulated by changing the electric field applied across the dielectric layer. The physics of FNT, as shown in Fig. 2 is a two-step process. Electrons are first thermally excited to an energy level $E$, which then tunnel through the triangular barrier into the floating gate. Note that at the bottom of the energy barrier, the oxide thickness is large enough (greater than 10 nm in a 0.5-μm CMOS process) that the probability of electrons directly tunneling through is negligible. Thus, FNT can be modeled by an equivalent energy scavenging circuit shown in Fig. 2 where the input energy source is the ambient thermal activation or thermal noise and rectification diode is formed by the tunneling barrier, whose output is the floating-gate capacitance. Mathematically, the combination of thermal activation and electron tunneling can be expressed by the FNT current density $J \ (A/m^2)$ as [16]

$$J = \frac{q}{h} \gamma \int_{-\infty}^{\infty} P_T(\zeta) T(\zeta) d\zeta$$

(1)

where $P_T(\zeta)$ is the probability density function corresponding to an electron occupying an energy level $\zeta$ and $T(.)$ represents the tunneling probability of the electron and is a function of the barrier thickness. The parameters $h$ and $q$ correspond to Plank’s constant and charge of free electrons, respectively. $\gamma$ represents a transmission parameter that is a function of the interface properties. In its general form shown in (1), it is practically impossible to obtain a closed form expression for FNT current density $J$, let alone solve a coupled differential equation involving $J$. Therefore, for the sake of simplicity, we will ignore several second-order effects (e.g., effect of image force and temperature variations) and consider the following mathematically tractable form of $J$:

$$J = \alpha E^2 \exp \left( \frac{-\beta}{E} \right)$$

(2)

where $E$ represents the electric field across the oxide barrier and where the parameters $\alpha$ and $\beta$ are a function of the
material properties and are given by

\[ \alpha = \frac{m^* q^3}{8 \pi m^* h \phi} \]

\[ \beta = \frac{4 (2 m^*)^{3/2} \phi^{1/2}}{3 h} \]

where \( m^* \) being the effective mass of electrons in the forbidden gap of the silicon-di-oxide, \( m \) being the mass of a free electron, \( \phi \) is the barrier height at the interface, and \( h \) is Planck’s constant.

The core structure of the timer can be modeled as a parallel connection of the tunneling current source and the capacitance. Thus, timers based on (9) should be robust to device mismatch and can be used to achieve synchronization between different devices.

This regime labeled as the equilibrium region in Fig. 3(b) tracks (11) and reveals two important attributes, which are useful for designing robust long-term timers. First, the floating-gate voltage monotonically decreases and is inversely proportional to a logarithmic function of time. Thus, the rate of decrease is slower than a linear timer and faster than a logarithmic function. The response becomes

\[ V_{fg}(t) = \frac{k_2}{\ln \left( \frac{t}{t_0} \right)} + V_{sub}. \]

This implies that the timer could be functional for a long-term duration relevant to the proposed application. The second attribute shown in (11) is that the response is only a function of the parameters \( k_0, k_1, \) and \( k_2 \), for the time intervals \( t \gg t_0 \gg k_0/k_1 \), the response becomes

\[ V_{fg}(t) = \frac{k_2}{\ln \left( \frac{t}{t_0} \right)} + V_{sub}. \]

Fig 3(b) shows a typical response of the timer according to (9). While the initial timer response is a function of the

---

**RESULTS**

The microphotograph of the timer device fabricated using standard CMOS processing techniques is shown in Fig. 4(a).
The floating gate is formed by the gate of a pMOS transistor, which is also used for programming the initial charge onto the floating gate [18]. Note that the initial charge on the floating gate controls the initial electric field in the oxide barrier and hence the shape of the FNT barrier. Timers with different form factors (floating-gate capacitances and tunneling junction area) were also fabricated and the microphotographs of eight timer structures are shown in Fig. 4(b). Timers labeled as Timer-C1 to Timer-C4 are devices with the same tunneling junction area but with different floating-gate capacitances. Timers labeled as Timer-A1 to Timer-A4 are timers with the same floating-gate capacitance but with different tunneling junction areas. The initial charge (hence the shape of the oxide barrier) on floating gates was programmed using a combination of FNT and hot-electron injection. A relatively high voltage (15 V in 0.5-µm CMOS process) is applied across the parasitic nMOS capacitor $C_{tun}$ [as shown in Fig. 4(a)], which removes the electrons from the floating gate. Hot-electron injection, on the other hand, requires lower voltage (4.2 V in 0.5-µm CMOS process) than tunneling and was used for precise programming of floating gates. Details of precision floating-gate programming can be found in [17] and is omitted here for the sake of brevity.

After the initial programming of the timer, all the calibration terminals are connected to ground and the timer is operated in a self-powered mode without any external powering. The timer value or the floating-gate voltage periodically read out through the buffer shown in Fig. 4(a).

A. FN Timer Measurement Results

The first group of experiments was designed to verify the timer behavior model, as given by (9). Measurement results from Timer-A1 were used for estimating the model parameters. The results are shown in Fig. 5, where also shown the error between the measured data and the behavioral model. The model parameters are summarized in Table I and the model error is measured to be smaller than 6 mV over a range of 700 mV, implying a model accuracy greater than 40 dB. One of the benefits of using a reliable behavioral model is that it can be used for extrapolation studies for predicting the timer’s long-term response, which could be impractical for repeated experimental studies. Fig. 6 shows the result of the extrapolation study, where the behavioral model is plotted for a duration greater than three years. In addition, data points measured from the fabricated timer are overlayed on the behavioral response and is shown to exhibit an accurate fit up to $2 \times 10^6$ s or 550 h.

B. Robustness and Mismatch Characterization

The next set of experiments were designed to verify the timer responses and the corresponding behavioral model for different values of: 1) floating-gate capacitances and 2) tunneling junction areas. Fig. 7 shows the measured values (highlighted by marked points) for floating-gate capacitances of 2, 4, 8, and 16 pF, respectively. For this experiment, the tunneling junction areas for all the four timers were chosen to be 54 µm². The corresponding timer responses estimated using the behavioral model for each of the parameters (FG gate capacitance and tunneling junction area) are also plotted as a solid line overlaying the measured data in Fig. 7(a). Two observations can be inferred from the measured results: 1) the behavioral model can accurately predict the response of the fabricated timers for different device parameters and 2) a smaller capacitance produces a faster change in the timer response. A more interesting result and the verification of (11) are that after the initial differences in respective timer responses, all the timers change in a near identical fashion. This is shown in Fig. 7(b) which plots the change in the timer outputs measured with respect to the output measured at a reference time ($t_0 = 6 \times 10^5$ s or 167 h). The result shows that the response changes by less than 2% even if the capacitances change by more than 800%. A similar experiment was conducted for timers with different tunneling junction areas of 72, 108, 144, and 180 µm² and for a fixed gate capacitance of $C_T = 4$ pF. The measured result is shown in Fig. 8 demonstrating a similar trend as before, where a smaller
Fig. 7. Comparison of timers with different gate capacitances $C_T$ and with tunneling area $A = 54 \ \mu m^2$: (a) Timers operating in transient and equilibrium region (shown in the inset) Marked points: measured data, solid lines: behavioral model; (b) Synchronization between timers operating in the equilibrium region and the measured maximum deviation across the timers.

Fig. 8. Comparison of timers with different tunneling junction areas $A$ and with $C_T = 4pF$: (a) Timers operating in transient and equilibrium region (shown in the inset) Marked points: measured data, solid lines: behavioral model; (b) Synchronization between timers operating in the equilibrium region and the measured maximum deviation across the timers.

In the next set of experiments, we verified the mismatch in the responses of identical timers fabricated on different silicon dies. For this experiment, all the timers were simultaneously programmed to “approximately” the same initial voltage and the set up was housed in an environment with similar conditions (temperature and humidity). Fig. 9(a) shows the measured timer responses, which as expected shows a similar trend, where the initial timer responses vary due to mismatch, but then the responses reach an identical steady-state response. Fig. 9(b) shows the relative deviation in the timer value with respect to each other and the measured result exhibits less than 500-μV variation over a 100-mV operating span. This amounts to a synchronization accuracy greater than 46 dB. Note that for this experiment, the noise and the drift in the read-out circuits could also affect the measured result, and, therefore, it is possible that the synchronization accuracy could be higher than what has been measured. However, optimization of the read-out circuits was not the goal of this paper.

IV. DISCUSSION

The objective of this paper was to demonstrate the functionality of a proof-of-concept self-powered timing device based on FNT of electrons onto a floating gate. When biased in a saturation regime, the timers can exhibit an extremely
robust timekeeping response that is dependent only on the device physics parameters and oxide thickness. However, in our modeling and analysis of the timer, we ignored the effect of temperature and other second-order effects. Although the process of tunneling through the triangular barrier exhibits a weak dependence with respect to temperature, the number of thermally excited electrons is a function of temperature. In addition, the height of the barrier also depends on temperature.

A group of experiments were conducted to measure the temperature dependence of the timer. A fabricated timer with $C_T = 2 \mu F$ and $A = 54 \mu m^2$ was housed in a temperature controlled environment chamber, and timer responses were obtained for four different temperature settings: $10^\circ C$, $20^\circ C$, $30^\circ C$, and $40^\circ C$. The measured responses are shown in Fig. 10 and as expected, the initial timer responses show a faster rate with increase in temperature. This is because for FNT, electrons have to be thermally excited to cross the triangular FN barrier. However, the long-term response of the timer exhibits a self-compensating effect similar to that of the timers with different device parameters. Fig. 10 shows the measured change in timer responses after a reference time of $6 \times 10^5$ s, the FG voltage reduction shows a mismatch less than 0.4 mV across a range of 100 mV. The measured results demonstrate that two timers maintained at two different temperature levels (measured range of $30^\circ C$) can still be synchronized with respect to each other up to an accuracy of 0.5%.

Another important aspect of the proposed FN timer is that it can be implemented on other CMOS processes as well. Even though we have used a 0.5-µm process (with an approximate 13-nm gate oxide thickness) to validate the response of the FN timer, the physics of the timer [summarized by (9)] should still be valid as long as the oxide thickness is greater than 10 nm. Advanced CMOS processes usually provide thick oxide option for I/O modules, which could, therefore, be used for designing the proposed FN timers. The self-compensating effect should still be applicable as long as the floating-gate structure can be reliably fabricated.

V. Conclusion

In this paper, we have presented a self-powered timer based on FNT of electrons onto a floating gate. The timer can be accurately described using a simple behavioral model that incorporates different nonideal effects (image force) and the effect of temperature dependence. The accuracy of the behavioral model has been verified using measured results that were obtained from fabricated timer structures prototyped using standard CMOS processing. Measurement results demonstrate that the long-term response of the timer is very robust to device mismatch and hence can be used for synchronizing time on two passive devices, which do not have access to a continuously running clock. We believe that this attribute would be essential for generating synchronous authentication tokens that can be used for rapid trust verification similar to a secureID type procedure [6].

REFERENCES


Liang Zhou (StM’14) received the B.S. degree in physics from Tsinghua University, Beijing, China, in 2010. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, Washington University in St. Louis, St. Louis, MO, USA.

Shantanu Chakrabartty (StM’99–M’04–SM’09) received the B.Tech. degree from IIT Delhi, New Delhi, India, in 1996, and the M.S. and Ph.D. degrees in electrical engineering from Johns Hopkins University, Baltimore, MD, USA, in 2002 and 2004, respectively.

He is currently a Professor with the School of Applied Sciences and Engineering, Washington University in St. Louis, St. Louis, MO, USA.