Modeling of CMOS Zero-power Timers for Dynamic Authentication of Passive Assets

Liang Zhou and Shantanu Chakrabartty
Department of Computer Science and Engineering
Washington University in St. Louis
St. Louis, MO, U.S.A.
{liang.zhou, shantanu}@wustl.edu

Abstract—A major limitation in authenticating passive and remotely powered sensors, tags and cards (e.g. radio-frequency identification tags or credit cards) is that these devices do not have access to a continuously running system clock. This obviates the use of dynamic SecureID type authentication techniques involving random keys and tokens that need to be periodically generated and synchronized. Zero-power timing devices that are driven by thermal and quantum fluctuations can overcome this limitation by generating a continuously running clock without the need for any external powering. In this paper we present a behavioral model of zero-power timers that are based on Fowler-Nordheim tunneling of electrons into or out of a floating-gate. The parameters of the model have been estimated using responses measured using timer prototypes fabricated in a standard 0.5 μm CMOS process. We use the behavioral model to understand the effect of different device parameters on dynamics of the timer and for extrapolation studies to determine the life-span of the FN timers.

I. INTRODUCTION

Authentication techniques using encryption, strong hash functions and pseudorandom number generators[1], [2], [3] are necessary for providing secure access to critical data and assets. However, for passive devices like credit cards and radio-frequency tags, the use of these techniques are impractical due to limited computational bandwidth and due to limited availability of energy. Also, the lack of access to a continuously running system clock on these devices obviates the use of dynamic authentication techniques like SecureID where random keys are periodically generated and synchronously refreshed [4]. In this regard, zero-power timers which operate without any external powering [5] can overcome this limitation and provide a mechanism for dynamic authentication of passive assets. The approach is illustrated in Fig. 1 where zero-power 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 centralized server. Rapid trust and signature verification can then be achieved by comparing synchronized tokens (example random numbers) that are seeded using the outputs from the synchronized timers. Compared to a conventional static authentication method (using bar-codes or static hardware signatures), this dynamic approach using zero-power timers should be more secure and will make the passive assets immune to counterfeiting or tampering.

An important feature of dynamic authentication procedure, as illustrated in Fig. 1, is the behavioral model of the timer that is used to implement the “gold-standard”. Existence of a behavioral model is predicated on implementing reliable zero-power timers whose dynamics can be precisely adjusted. In [5], 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 hours, the dynamics of the electron leakage process was found to be difficult to control. In this paper, we propose a behavior model of a zero-power timer structure based on Fowler-Nordheim (FN) tunneling of electrons through thin gate-oxide [6]. The physics of FN tunneling is reliable and is described in Section II and the underlying devices can be easily implemented using standard CMOS process layers. When constraints are imposed on the total number of electrons that can leak due to FN tunneling, a log-linear response is obtained which is described using a behavioral model, as described in Section III. The parameters of the model have been estimated and verified using prototypes of timers that have been fabricated in a standard 0.5μm double-poly CMOS process and in Section IV we present measurement and modeling results.
II. FN TUNNELING BASED ELECTRON-LEAKAGE

The electronic structure of a generic zero-power timer comprises of a strip of poly-crystalline silicon (polysilicon) that is completely isolated by high-quality, thermally-grown silicon-di-oxide, as shown in Fig. 2(a). This polysilicon strip, also referred to as a floating-gate, serves as a reservoir of electrons and the surrounding silicon-di-oxide will serve as an energy barrier (shown in Fig. 2(a)) that prevents the electrons to leak out (by thermal excitation or quantum tunneling). Electrons can leak through the oxide using three mechanisms of quantum tunneling:(a) Trap-assisted tunneling (TAT) where carriers tunnel through the dielectric layer with the assistance of trap states, (b) direct tunneling (DT) where carriers directly tunnel through the rectangular barrier formed by the dielectric layer, and (c) Fowler-Nordheim tunneling (FNT) where carriers tunnel through a triangular-shape barrier resulted from a strong electric field. Trap-assisted tunneling 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 few defects or electron traps. Direct tunneling relies on the dielectric thickness and becomes prominent when the thickness of the dielectric layer is small (for silicon-di-oxide, less than 4 nm). This is a process specific parameter and cannot be modulated or controlled. In standard 500 nm CMOS processes, it is also negligible because the minimum oxide thickness is larger than 10 nm. FN tunneling, on the other hand, depends on the shape of the energy barrier across the dielectric layer which can be controlled and modulated by changing the electric field across the dielectric layer. Electron leakage due to FN tunneling dominates when the electric field across the layer reaches a critical range. This is illustrated using the energy-band diagrams of the MOS structure with positive and negative bias applied to the gate poly shown in Fig. 2(b) and (c) respectively. Since the energy barrier at the interface of holes (3.8 eV) is larger than that of electrons (3.2 eV), the probability of hole emissions is negligible compared to that of electrons. Positive bias of the gate electrode results in degenerate silicon surface in the n-type substrate, therefore inducing metal-like behavior because the conduction band of the silicon is lower than the Fermi potential at the interface, as illustrated in Fig. 2(c). As a result, most of the voltage drop occurs across the silicon-di-oxide barrier.

The expression for the total FN tunneling current density $J$ depends on the electric field $E$ across the insulator and can be expressed in the form [7]

$$J = \frac{1}{t^2(y)} \gamma(T) E^2 e^{\frac{-\beta \psi(y)}{E}}$$  \hspace{1cm} (1)

where $\alpha$ and $\beta$ are a function of physical parameters as

$$\alpha = \frac{m^3 q}{8 \pi m^* h \phi}$$  \hspace{1cm} (2)

$$\beta = \frac{4(2m^*) \frac{1}{2} \phi^2}{3hq}$$  \hspace{1cm} (3)

$m$ and $q$ are the mass and charge of free electrons respectively, $m^*$ is the effective mass of electrons in the forbidden gap of the silicon-di-oxide, $\phi$ is the barrier height at the interface, and $h$ is the Planck’s constant. The coefficients $\alpha$ and $\beta$ is a function of material properties as $m^*$ and $\phi$ are different for different materials.

The image force effect leads to a lowering of the triangular barrier and is calibrated using two correction items, $t(y)$ and $\psi(y)$, as shown in Equation 1, which are both tabulated elliptic integrals, and $y$ is a function of the barrier height and electric field as

$$y = \frac{1}{\phi} \left( \frac{q^3 E}{4 \pi \varepsilon_0} \right)^{\frac{1}{2}}$$  \hspace{1cm} (4)

Although the tunneling process itself is temperature independent, the number of electrons of a given incident energy on the barrier is a function of temperature and the barrier height $\phi$ also depends on temperature. The dependence of electron momentum distribution on temperature as shown in Fig. 2(b) and (c) can be corrected by adding a multiplicative term

$$\gamma(T) = \frac{\pi c k T}{\sin(\pi c k T)}$$  \hspace{1cm} (5)

where

$$c = \frac{4\pi(2m^* \phi)^{\frac{1}{2}} t(y)}{h q E}$$  \hspace{1cm} (6)

Ravindra [8] proposed a linear dependence model to accommodate the temperature effect on the barrier height, and can be expressed as

$$\phi(T) = \phi_0 + \lambda \Delta T$$  \hspace{1cm} (7)

where $\lambda$ is a constant parameter. Notice that the barrier height $\phi$ in equation 1 should be replaced with the temperature dependent form $\phi(T)$. 

Fig. 2. Energy-band for tunneling in Floating-gate structure: (a) cross-sectional layout and its energy band diagram; (b) negative bias for FN tunneling and (c) positive bias for FN tunneling.
### III. Behavioral Model of FN Tunneling Based Zero-power Timers

The core structure of the FN tunneling based timers is a floating gate transistor combined with programming and readout interface as shown in Fig. 3. The timer can be modeled as a charge storage capacitor \( C_T \) and a tunneling MOSFET \( M_{fg} \), as illustrated in Fig. 3(a). FN tunneling occurs at the tunneling junction which leads to the change of cumulative charge storage on the capacitor \( C_T \). As a result, the total residual charge on \( C_T \) shows time-dependent characteristics which can be used to extract the timing information. It is impossible to derive a closed form using the FN tunneling equation 1 as it is a function of image force effect and temperature. However, if we neglect the image force effect and view the temperature as constant, equation 1 reduces to equation 8. In this case, it is possible to obtain a closed-from relationship between the floating-voltage \( V_{fg} \) and elapsed time \( t \). In this simple scenario, the FN tunneling current density (rate of electron leakage) can be expressed as:

\[
J = \alpha E^2 \exp\left(-\frac{\beta}{E}\right) \tag{8}
\]

The floating-gate voltage \( V_{fg} \) depends on the floating-gate charge \( Q \) differentially in the form of

\[
dV_{fg} = \frac{dQ}{C_T} = \frac{AJdt}{C_T} \tag{9}
\]

where \( A \) is the tunneling junction area, \( C_T \) is the FG capacitance. Notice that \( V_{fg} \) and \( E \) are related by the oxide thickness \( t_{ox} \) as

\[
V_{fg} = t_{ox}E + V_{sub} \tag{10}
\]

where \( V_{sub} \) is the effective voltage drop across the substrate. By integrating equation 8, 9 and 10, the dependence of electric field \( E \) on time \( t \) can be expressed in the form of

\[
E = \frac{\beta}{\ln(k_1 t + k_0)} \tag{11}
\]

where \( k_0 \) and \( k_1 \) are constants that are given by

\[
k_0 = \exp\left(\frac{\beta}{E_0}\right), \quad k_1 = \frac{A\alpha\beta}{C_T t_{ox}} \tag{12}
\]

here \( E_0 \) is the initial electric field across the gate oxide. Substituting \( E \) into equation 10, the floating-gate voltage change over time can be expressed as

\[
V_{fg} = \frac{k_2}{\ln(k_1 t + k_0)} + V_{sub} \tag{13}
\]

where

\[
k_2 = \beta t_{ox} \tag{14}
\]

Thus, we have

\[
t = \frac{1}{k_1} \exp\left(\frac{k_2}{(V_{fg} - V_{sub})}\right) - \frac{k_0}{k_1} \tag{15}
\]

Equation 13 shows that the change in floating-gate voltage is monotonic with respect to time (decreases with time) and is a function of the initial charge on the floating-gate which is modeled by the parameter \( k_0 \). The voltage-time dependence can be modulated by changing the tunneling junction area \( A \) and the FG capacitance \( C_T \), both of which determine the parameter \( k_1 \). As illustrated, if we want to implement a long-term timer, the tunneling junction area \( A \) needs to be small while the capacitance \( C_T \) should be large.

### IV. Experimental Results

Fig. 4. Micro-photograph of the fabricated timers.

Timers with different form factors were fabricated on a standard 0.5-μm CMOS process and were used to validate the proposed behavioral model. The micro-photograph of the die is shown in Fig. 4, where eight timers occupy an area of 800×600 μm². Timer-C1 to Timer-C4 refer to timers with same tunneling junction area but with different gate capacitances, and Timer-A1 to Timer-A4 are timers with the same gate capacitance but with different tunneling junction areas.

**TABLE I. Model parameters for the FN tunneling timer**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( k_2 )</td>
<td>87.49</td>
</tr>
<tr>
<td>( k_0 )</td>
<td>2.341×10^6</td>
</tr>
<tr>
<td>( k_1 )</td>
<td>1.037×10^4</td>
</tr>
<tr>
<td>( V_{sub} )</td>
<td>3.94</td>
</tr>
</tbody>
</table>

The first group of experiments were designed to verify the behavior model given by Equation 13. Measurement results from Timer-A1 were used for fitting the model parameters. The results are shown in Fig. 5, where the regression error is also shown. The fitted parameters are listed in Tab. I and behavioral model shows an accumulated error smaller than 6mV across a recording range of 700mV, which implies an accuracy larger than 40 dB.

The next set of experiments were designed to validate the behavioral model for two different device parameters:
Fig. 5. Measured timer characteristics and comparison with the proposed behavioral model.

Fig. 6. Comparison of timers for different gate capacitance $C_T$ with tunneling area $A=54 \mu m^2$. (Marked points represent measured data and solid lines correspond to the behavior model.)

(a) floating-gate capacitance; and (b) tunneling junction area. Fig. 6 shows the measured values (highlighted by marked points) with gate capacitances of 2 pF, 4 pF, 8 pF and 16 pF respectively. For this experiment, the tunneling junction areas for all the four timers were chosen to be 54 $\mu m^2$. The corresponding response from the behavioral model is plotted in the Fig. 6 as solid line, emphasizing the accuracy of the proposed model. The similar set of measurement and regression analysis were conducted on Timers with different tunneling junction areas, as shown in Fig. 7. The four timers have a tunneling junction area of 72 $\mu m^2$, 108 $\mu m^2$, 144 $\mu m^2$ and 180 $\mu m^2$ and all have the gate capacitance of $C_T=4$ pF. There are two observations from the results: (a) the behavior model can accurately predict the response of the fabricated timers; and (b) larger capacitance and smaller junction area produces a larger time constant and is captured by the model parameter $k_1$.

V. SUMMARY

In this paper we have presented a behavioral model of a zero-power timer based on FN tunneling of electrons from a floating-gate structure. Even though the model incorporates different non-ideal effects (image force) and the effect of temperature dependence, a simple and closed form model faithfully captures the response of the timer. The accuracy of the behavioral model has been verified using measured results that were obtained from fabricated timer structures prototyped in a standard 0.5-$\mu$m CMOS process. Measurement results confirm that the timing characteristics can be adjusted by changing device parameters like gate capacitance and tunneling junction area. Future work will focus on determining statistical accuracy of this behavioral model using measured results for multiple timing structures integrated within and across different silicon dies. The future model will also capture the statistical variance of the timer response due to fabrication mismatch.

VI. ACKNOWLEDGEMENT

This work was supported in part by Semiconductor Research Corporation ( SRC).

REFERENCES