NVRAM CELLS IN STANDARD CMOS LOGIC PROCESS

KAREN VANESSA FLOREZ RAMIREZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICOMECÁNICAS
ESCUELA DE INGENIERÍAS
ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2021

NVRAM CELLS IN STANDARD CMOS LOGIC PROCESS

KAREN VANESSA FLOREZ RAMIREZ

Trabajo de Grado para optar al título de
Ingeniera Electrónica

Director
Javier Ferney Ardila Ochoa,
PhD, Electrical and Electronics Engineering

Codirector
Elkim Felipe Roa Fuentes,
PhD, Electrical and Electronics Engineering

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICOMECÁNICAS
ESCUELA DE INGENIERÍAS
ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2021

Dedicatoria

A Dios por guiarme en cada paso y poner en mi camino a gente maravillosa.

A mi mamá por sus consejos, paciencia y ejemplo en cada momento de mi vida

A mi hermana Katherine por ser mi mejor amiga, ejemplo y apoyo incondicional, porque con su cariño me ha ayudado a lograr cada éxito.

A mis compañeros y profesores del grupo de investigación Onchip, por enseñarme tanto y darme las bases para ser una gran profesional.

A Edward, por su amor y apoyo incondicional, porque somos el mejor equipo del mundo y juntos logramos esta meta.

A Román y Paula, por ser los amigos que me dejó la UIS, por la alegría y motivación que me dieron cada día durante estos años.

A mi tío Omar, mi tía Neida, Diana y toda mi familia, porque con su ayuda y cariño salimos adelante.

Y a todos aquellos que me han ayudado a lograrlo.

CONTENTS

LIST OF FIGURES

pág.

LIST OF TABLES

pág.

LIST OF ANNEXES

pág.

RESUMEN

TÍTULO: CELDAS NVRAM EN PROCESO LÓGICO CMOS ESTÁNDAR [*]

AUTORES: KAREN VANESSA FLOREZ RAMIREZ [**]

PALABRAS CLAVE: MEMORIA DE ACCESO ALEATORIO NO VOLÁTIL, MODELADO DE TUNELAMIENTO FOWLER-NORDHEIM, FUNCIÓN FÍSICAMENTE NO CLONABLE.

DESCRIPCIÓN:

Las memorias EEPROM y Flash se utilizan en diferentes aplicaciones como almacenamiento de memoria no volátil. Estos tipos de memoria requieren máscaras adicionales al proceso CMOS estándar y hacen que el proceso de fabricación sea complejo y más costoso. Por ello, el interés por la fabricación de NVRAM en tecnología CMOS estándar ha aumentado debido a sus múltiples aplicaciones y a la reducción de tiempo y costos de fabricación que supone su implementación. Junto a las múltiples ventajas de la implementación de NVRAM, existen varios retos de diseño relacionados con el proceso de programación de las celdas, la alta tensión necesaria para su programación, y el escalado de las mismas a diferentes tecnologías CMOS que ponen en riesgo la durabilidad de las celdas y su correcto funcionamiento. En este proyecto, se caracteriza en el laboratorio un macro de NVRAM diseñado e implementado en tecnología CMOS de 180nm, junto con el diseño de celdas NVRAM en tecnología CMOS de 28nm. Este diseño se verifica utilizando dos modelos del fenómeno de tunelamiento Fowler-Nordheim descritos en Verilog A, que fueron desarrollados en este proyecto para la simulación de celdas NVRAM. Además, se muestra la aplicación de las celdas NVRAM como celdas de Función Físicamente No Clonable generando llaves de encriptación $100\,\%$ estables.

---

[*] Trabajo de grado

[**] Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Director: Javier Ferney Ardila Ochoa, PhD, Electrical and Electronics Engineering. Codirector: Elkim Felipe Roa Fuentes, PhD, Electrical and Electronics Engineering.

ABSTRACT

TITLE: NVRAM CELLS IN STANDARD CMOS LOGIC PROCESS [*]

AUTHORS: KAREN VANESSA FLOREZ RAMIREZ [**]

KEYWORDS: NON-VOLATILE RANDOM ACCESS MEMORY, FOWLER-NORDHEIM TUNNELING MODELING, PHYSICALLY UNCLONABLE FUNCTION.

DESCRIPTION:

EEPROM and Flash memories are used in different applications as non-volatile memory storage. These types of memory require additional masks to the standard CMOS process and make the manufacturing process complex and more expensive. As a result, interest in NVRAM fabrication in standard CMOS technology has increased due to its multiple applications and the reduction in time and manufacturing costs that its implementation entails.

Along with the many advantages of NVRAM implementation, there are several design challenges related to the cell programming process, the high voltage required for programming, and the scaling of the cells to different CMOS technology that put cell durability and proper operation at risk.

In this project, an NVRAM macro designed and implemented in 180nm CMOS technology is characterized in the laboratory, along with the design of NVRAM cells in 28nm CMOS technology. This design is verified using two models of the Fowler-Nordheim tunneling phenomenon described in Verilog A, which was developed in this project for NVRAM cells simulation. In addition, the application of NVRAM cells as Physically Unclonable Function cells generating $100\,\%$ stable encryption keys is shown.

---

[*] Bachelor Thesis

[**] Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Director: Javier Ferney Ardila Ochoa, PhD, Electrical and Electronics Engineering. Codirector: Elkim Felipe Roa Fuentes, PhD, Electrical and Electronics Engineering.

INTRODUCTION

Embedded non-volatile memory (NVM) technology is used in system-on-chip applications where low NV-memory capacity is required, such as IP security, RF identification, microcontrollers, or analog trimming and calibration. Conventional embedded NVM technology such as EEPROM and Flash is expensive as it requires additional masks to the standard CMOS process; the need for extra masks makes the manufacturing process complex and delays the baseline logic process [1] [2] [3].

In order to reduce costs and production time, there has been increased interest in manufacturing memories in standard CMOS technology, such as Multi-Time Programmable (MTP) Non-Volatile RAM based on Floating Gates. However, the main challenge in designing NVRAM cells is the mitigation of oxide stress on the transistor gate to ensure data retention and endurance of the cells [4]. It is a challenge because programming this type of NVRAM requires voltages three or four times higher than the nominal power supply of the technology, which risks breaking the oxide and lo-

---

[1] Katsuhiko HOYA y col. "A perspective on NVRAM technology for future computing system". En: *2019 International Symposium on VLSI Technology, Systems and Application (VLSI-TSA)*. 2019, págs. 1-2. DOI: 10.1109/VLSI-TSA.2019.8804706.

[2] Sudarsun KANNAN y col. "Using Active NVRAM for Cloud I/O". En: *2011 Sixth Open Cirrus Summit*. 2011, págs. 32-36. DOI: 10.1109/OCS.2011.12.

[3] J. RASZKA y col. "Embedded flash memory for security applications in a 0.13 /spl mu/m CMOS logic process". En: *2004 IEEE International Solid-State Circuits Conference (IEEE Cat. No.04CH37519)*. 2004, 46-512 Vol.1. DOI: 10.1109/ISSCC.2004.1332586.

[4] Y. WANG B. y MA. "Opportunities and Challenges in Multi-Times-Programmable Floating-Gate Logic Non-Volatile Memories". En: *2008 Joint Non-Volatile Semiconductor Memory Workshop and International Conference on Memory Technology and Design*. 2008, págs. 22-25. DOI: 10.1109/NVSMW.2008.12.

sing the possibility of reprogramming the memory [5]. So it is necessary to carefully design the memory cells, choose the appropriate topology, select the most suitable programming mechanism to ensure the durability of the memory, and have the means to verify the design before being manufactured.

Motivated by the many advantages of implementing NVRAM cells in CMOS technology without extra masks, the research group Onchip implemented and fabricated a macro of NVRAM in standard 180nm technology. This proof-of-concept was a success, but laboratory validation of the design was needed to verify that the read and write processes of the cells were correct. In addition, characterization of the NVRAM cells was necessary to use them as a reference for future designs, either in 180nm CMOS technology or in new technologies.

This project studies the NVRAM macro manufactured in standard 180nm CMOS technology and characterizes each type of cell through laboratory tests. This is done in order to solve the challenges encountered and design NVRAM cells in more modern technology, such as 28nm CMOS technology. This is in addition to the development of a model described in Verilog A of the programming mechanism of the cells, which will be used as a method of verification of the operation of the NVRAM cells and as a support for the design of the cells.

---

[5] Ki y KIM Chris H. SONG Seung-Hwan; CHUL CHUN. "A Bit-by-Bit Re-Writable Eflash in a Generic 65 nm Logic Process for Moderate-Density Nonvolatile Memory Applications". En: *IEEE Journal of Solid-State Circuits* 49.8 (2014), págs. 1861-1871. DOI: 10.1109/JSSC.2014.2314445.

1. OBJECTIVES

1.1. GENERAL OBJECTIVES

To study an NVRAM cell and consider the feasibility of implementation in 28nm CMOS technology.

1.2. SPECIFIC OBJECTIVES

To characterize an NVRAM macro implemented in 180nm CMOS technology.

To design an NVRAM macro cell in standard 28nm CMOS technology.

To validate the design functionality through electrical simulations using a model of the Fowler-Nordheim tunneling phenomenon in CMOS technology.

2. NVRAM CELLS AND MACRO ARCHITECTURE

The NVRAM macro consists of the bit cells, where the data is stored and the sense amplifier, a circuit that allows reading output voltages to determine the value of the data stored in the NVRAM.

2.1. NVRAM BITCELL

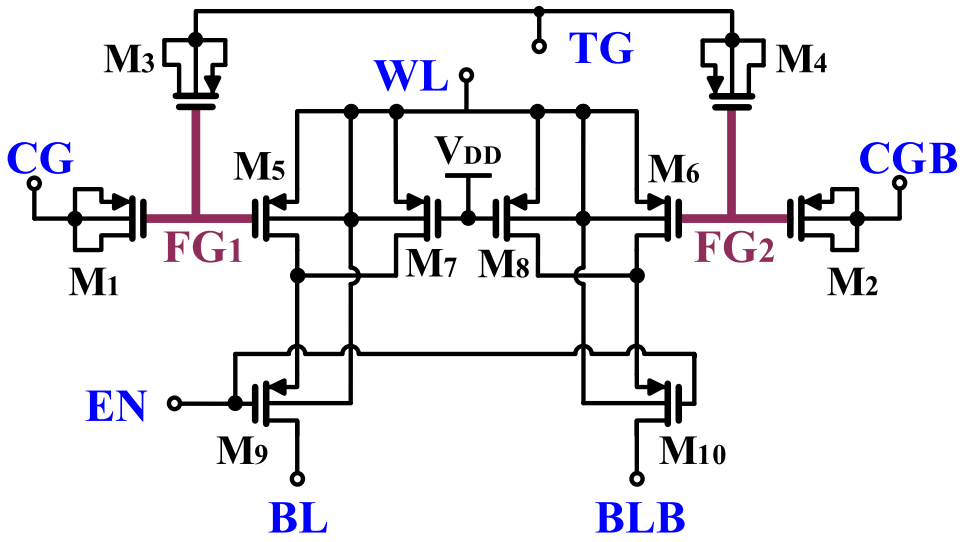
Typically, floating-gate-based NVRAM cells consist of a coupling transistor, a tunneling transistor, and a read transistor; these transistors are implemented using thick gate-oxide I/O devices to ensure a sufficient level of data retention. The three transistors are placed adjacent to each other with an isolated common polysilicon gate. The common gate is known as the floating gate of the cell, as shown in Figure 2.1.
Transistors can be either NMOS or PMOS, but the use of NMOS involves a higher area cost because a p-well is needed to isolate the transistor in CMOS technology. For this reason PMOS transistors are preferred in NVRAM cells. The inversion layer under the PMOS gate and p+ diffusions work as a control node. When a voltage is applied to the control nodes, the floating gate potential is determined by the gate capacitance ratio of the three transistors [6].
NVRAM cells can be single-ended or differential. The differential topology was chosen as it does not require a reference voltage, and is more accurate in situations where power supplies are not reliable or stable [7].

---

[6] Cong LI y col. “Multitime Programmable Memory Cell With Improved MOS Capacitor in Standard CMOS Process”. En: *IEEE Transactions on Electron Devices* 62.8 (2015), págs. 2517-2523. DOI: 10.1109/TED.2015.2443651.

[7] Frédéric J. y HYDE John D. PESAVENTO Alberto; BERNARD. “PFET NONVOLATILE MEMORY”. En: *U.S.Patent 7,221,596 B2* (May 22, 2007).

Figure 2.1. NVRAM bitcell schematic.



The schematic of the NVRAM bit cell is shown in Figure 2.1. where transistors M_1 and M_2 are the coupling devices, M_3-M_6 are the tunneling devices but, in the reading process M_5 and M_6 work as the reading transistors, M_7 and M_8 are connected to the reading transistors to avoid modifying the content of the cells when they have not been selected. Finally, transistors M_9 and M_{10} are used to select the cell in a memory array.

The voltage at the cell's floating gate (V_{FG}) is defined as follows:

$$V_{FG} = V_{CG}\frac{C_{CG}}{C_{tot}} + V_{TG}\frac{C_{TG}}{C_{tot}} + V_{WL}\frac{C_{WL}}{C_{tot}} + \frac{Q_{FG}}{C_{tot}} \tag{1}$$

where V_{CG} is the voltage applied at the coupling gate (CG) node, V_{TG} is the voltage applied at the tunneling gate (TG) node, and V_{WL} is the voltage applied at the writing line (WL) node. C_{CG}, C_{TG}, and C_{WL} are the gate capacitances of the coupling, tunneling, and readout transistors, respectively. And the total gate capacitance (C_{tot}) is defined as follows:

$$C_{tot} = C_{CG} + C_{TG} + C_{WL} \tag{2}$$

Table 2.1. NVRAM bitcell operating voltages

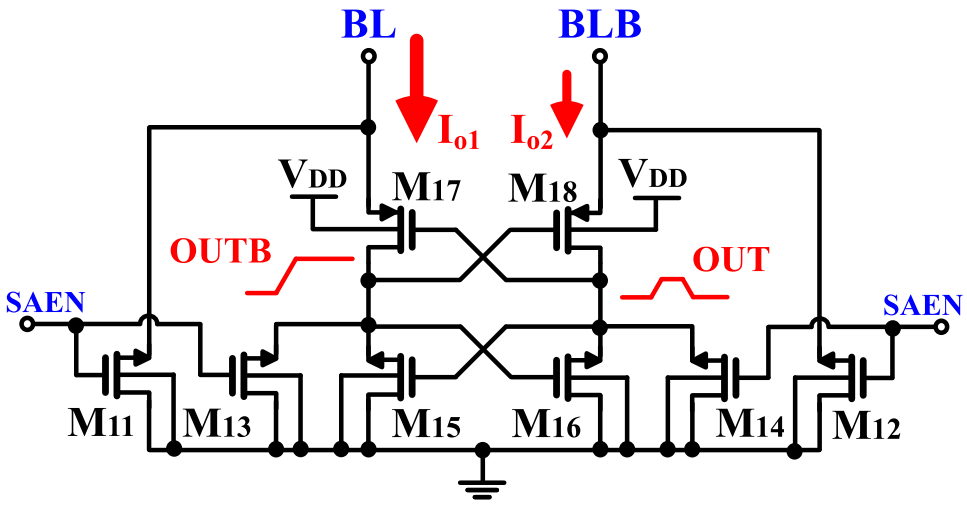
Operation | node	CG	CGB	TG	WL	EN
Programming	VH	0	VH	0	VDD
Stand-by/Locking	0	0	0	VDD	VDD
Reading	0	0	0	VDD	0

The charge stored in the Floating Gate (Q_{FG}) can be modified during the programming process of the NVRAM cells by exposing the floating gate to a high voltage. Here, the threshold voltage of the read transistors is modified, allowing us to sense a change in current through the BL and BLB branches. The differential current between the two branches is amplified and latched by a sense amplifier during the reading process, allowing us to determine the data stored in the memory.
The operating voltages required for the processes of programming, reading and locking the NVRAM cells are shown in Table 2.1. VH refers to the high voltage needed to modify the charge of the floating gates.

2.2. SENSE AMPLIFIER

Figure 2.2. illustrates the schematic of the sense amplifier. In the reading process, the current passing through the BL and BLB branches are converted into output voltages by the latch composed of M_{15}-M_{18}. The SAEN node allows us to discharge the nodes BL, BLB, OUT, and OUTB before each reading to ensure a correct operation of the sense amplifier. Figure 2.2. shows the operation of the sense amplifier when the current of the BL branch is larger than the current of the BLB branch. In this case, the output node OUTB is charged up to the VDD level as opposed to the discharge of the OUT node to 0V after the latch decision.

Figure 2.2. Detailed schematic and operation of the sense amplifier.



2.3. FOWLER-NORDHEIM TUNNELING AS PROGRAMMING MECHANISM

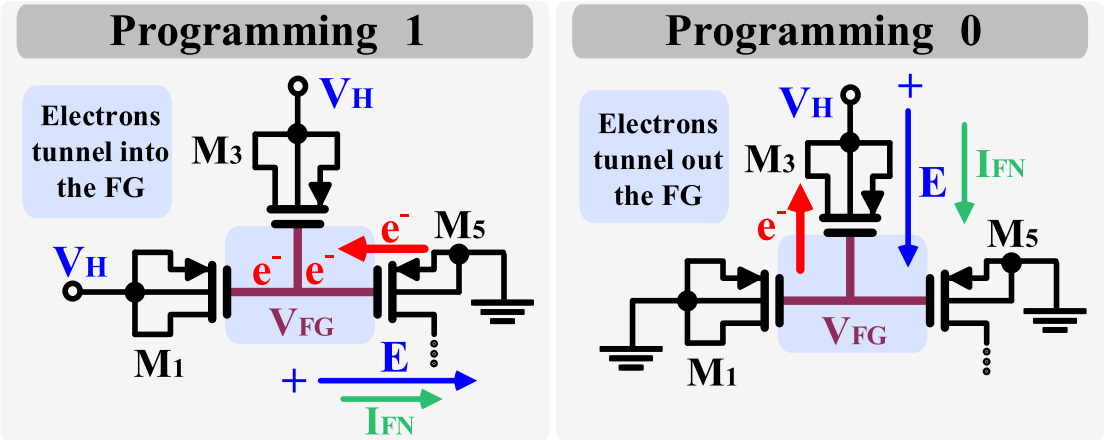
There are different programming mechanisms for non-volatile memories. The one used in these NVRAM cells is Fowler-Nordheim tunneling, which is a quantum-mechanical phenomenon in which electrons can cross a potential barrier due to a strong electric field. The Fowler-Nordheim tunneling current (I_{FN}) is described as:

$$\begin{aligned} I_{FN} &= A(E_{ox})^2 e^{\frac{-B}{Eox}} \\ A &= \frac{q^3 m}{8\pi h \phi m_*} \\ B &= 4(2m^8)^{0.5}\frac{\phi^{1.5}}{3h_* q} \end{aligned} \tag{3}$$

where h is Planck's constant, ϕ is the work function of silicon which is equal to 3.2eV, m is the mass of the free electron, m_* is the effective mass of the electron in the SiO_2 barrier $(0.26m)$, and h_* is equal to $0.16h$ [8].

[8] Ronnie KLANDERMAN. "Flash memory device: Electrical modeling and simulation". En: 2012.

Figure 2.3. Fowler-Nordheim tunneling for programming the NVRAM cells.



This phenomenon is used to program NVRAM cells, and an electric field is generated between the control node and the floating gate of the cells by applying a high voltage (VH) to specific control nodes of the bitcell, generating a current through the transistor oxide.

Figure 2.3. illustrates the operation of Fowler-Nordheim tunneling to program the memory. To program a logic 1 in the NVRAM cell, the control nodes are configured to generate an electric field that causes the electrons to tunnel into the floating gate, causing the current in that branch to be higher during memory reading and interpreted as a logic 1. To program a logic 0 in the NVRAM cell, the control nodes are configured to generate an electric field that causes the electrons to tunnel out of the floating gate, causing the current in that branch to be lower during memory reading and to be interpreted as a logic 0.

The electric field in the floating gates (E_{ox}) is defined as:

$$E_{ox} = \frac{V_{FG} - V_{ControlNode}}{tox} \tag{4}$$

And the minimum electric field to generate Fowler-Nordheim tunneling is defined as

[9]:

$$|E_{ox}| > \frac{\phi}{tox} \tag{5}$$

where tox is the width of the transistor oxide. To ensure the correct operation of the programming mechanism and data retention in the cell, the width of the oxide must be greater than $3nm$. If this condition is not satisfied, the predominant tunneling phenomenon is direct tunneling, not Fowler-Nordheim tunneling [10].

[9] L.R. CARLEY. "Trimming analog circuits using floating-gate analog MOS memory". En: *IEEE International Solid-State Circuits Conference, 1989 ISSCC. Digest of Technical Papers*. 1989, págs. 202-203. DOI: 10.1109/ISSCC.1989.48260.

[10] Razali LIM Ee Wah y ISMAIL. "Conduction Mechanism of Valence Change Resistive Switching Memory: A Survey". En: *Electronics* 4.3 (2015), págs. 586-613. DOI: 10.3390/electronics4030586.

3. NVRAM CELLS IN 180 NM CMOS TECHNOLOGY

The Onchip research group of the Universidad Industrial de Santander designed and implemented a 2X16 NVRAM macro in 180nm CMOS technology, according to the topology explained above. This macro includes one level shifter per row and one sense amplifier per column. The block diagram of the macro is shown in Figure 3.1.
As a proof of concept, the NVRAM macro was designed with cells of different sizes, associated with the dimensions of the coupling transistors (M_1 and M_2). Changing the size of the coupling devices, we modulated the voltage at the floating gate following Equation 1 and thus modulated the capacity to tunnel charges through the floating gates. Table 3.1 provides the different transistor sizes used for the five cells of the NVRAM macro implemented in 180nm CMOS technology.

3.1. NVRAM CELLS CHARACTERIZATION AND MEASUREMENT RESULTS

For characterization of the NVRAM design at 180nm CMOS technology, lab measurements were performed on eight chips that included the NVRAM macro and a microprocessor to register the stored data.
Reading and programming tests were performed on each chip. Figure 3.2. shows the micrograph of the implemented NVRAM macro and the setup used for the laboratory measurements.
To perform the NVRAM reading test, the cell to be read is selected by setting the EN node to 0V and WL to VDD, in this technology 3.3V, control nodes must be asserted to 0 V as well as the SAEN node, which makes it possible to sense the current through the BL and BLB branches. The magnitude of the current will depend on the charge stored in the floating gates of the cell and using the sense amplifier it is determined if the stored data is 0 or 1.

Figure 3.1. Block diagram of the NVRAM macro.

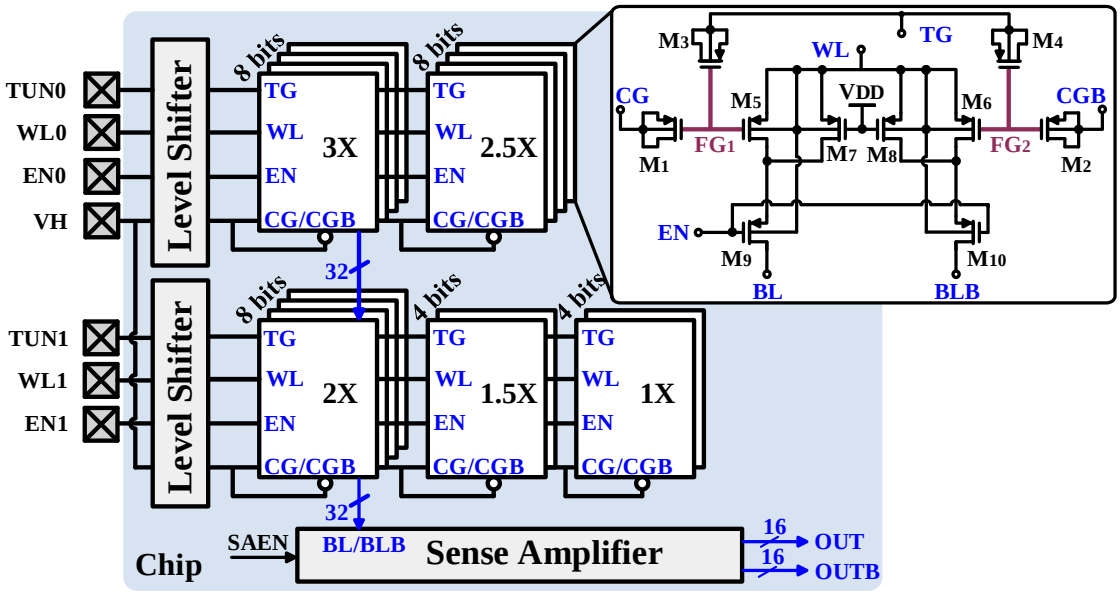


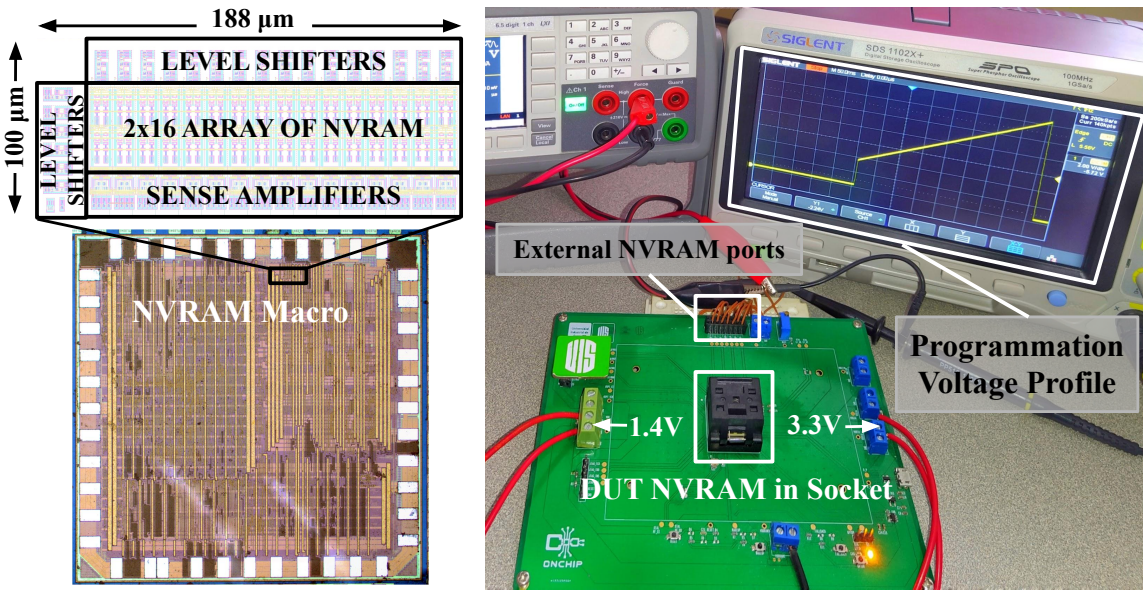
Table 3.1. MOSFET size in each type of cell in 180nm CMOS technology

Devices*		W
NVRAM Cells**	3X	M_1,M_2=3.6μm
	2.5X	M_1,M_2=3μm
	2X	M_1,M_2=2.4μm
	1.5X	M_1,M_2=1.8μm
	1X	M_1,M_2=1.2μm
Sense Amplifier	M_{11}-M_{16}	1μm
	M_{17}, M_{18}	2μm

* All devices have $L = 300nm$.

** M_3-M_{10} in all cells have $W = 300nm$.

Figure 3.2. Micrograph and detailed layout of the NVRAM macro in 180nm and test setup and board for lab tests.



We performed 1000 consecutive readings on each of the chips without programming. These readings allowed us to determine that, due to the manufacturing process, each cell has stored unique and unpredictable data, which can be used as a security key in physically unclonable functions (PUFs) [11].

For the programming process of the NVRAM cells, the high voltage (VH) needed to induce Fowler-Nordheim tunneling was unknown, so a voltage ramp profile was used to avoid overstressing the oxide with an excess of tunneling current or a high voltage difference and damage the memory cells [12]. Different ramp profiles were used, varying the number of pulses, the amplitude and duration of each ramp.

---

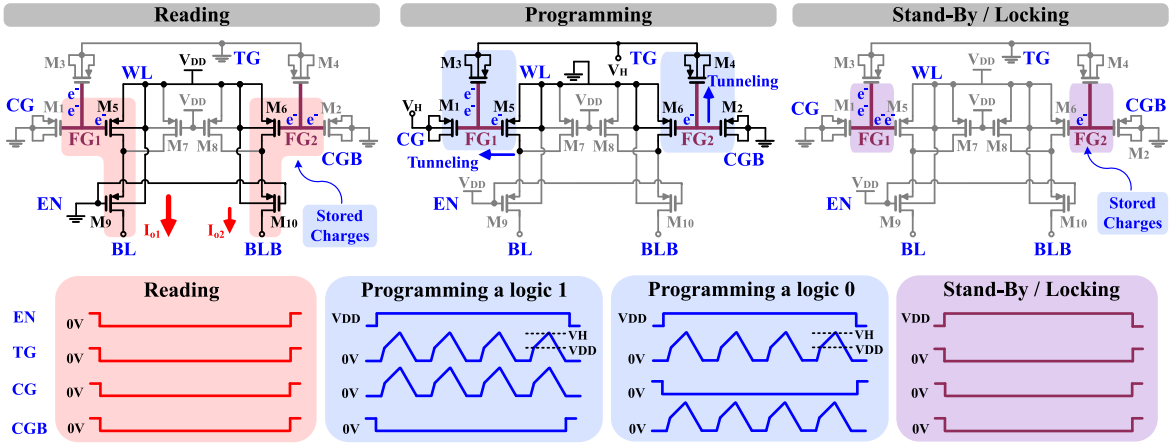
[11] Javier ARDILA y col. “A Stable Physically Unclonable Function Based on a Standard CMOS NVR”. En: *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*. 2020, págs. 1-4. DOI: 10.1109/ISCAS45731.2020.9180411.

[12] Christopher J. PESAVENTO Alberto y DIOIO. “RFID IC tunneling-voltage profile calibration”. En: *U.S.Patent 8,902,627 B1* (Dec 2, 2014).

The objective of these calibration measurements is to find a voltage profile that allows data to be written to the memory without damaging the NVRAM and losing the possibility to rewrite memory.

The voltage ramp profile used is shown in Figure 3.3, along with the voltage profiles used for reading and locking the NVRAM cells.

Figure 3.3. Bitcell schematic of the NVRAM and operation during reading, programming and stand-by/locking process.



The ramp profile consists of three consecutive ramps. The first is a ramp that changes from 0V to VDD in a time interval of 1 s. Immediately after, another ramp continues that changes from VDD to VH in a time interval $t_{program}$. Finally, the last ramp changes from VH to 0V in a time of 10ms. This ramp profile is repeated up to 4 times with a delay of 10ms.

Different programming tests were performed, varying VH from VDD to 13V and varying $t_{program}$ from 8ms to 600ms based on several references on NVRAM tunneling

Table 3.2. Percentage of unstable bits after programming each type of NVRAM cell

Type of NVRAM cell	Percentage of unstable bits
3X	0 %
2.5X	15.5 %
2X	3.375 %
1.5X	10.5 %
1X	24.75 %

[13] [14].

Successful programming was observed in most NVRAM cells using the described ramping profile, a VH voltage of 12V, and a programming time of 400ms. The programmed data remains in memory even after turning off the memory and allowing days to pass between readings, thus proving that the retention of the cells is adequate. The programming voltage for the NVRAM cells implemented in 180nm was determined as VH=12V. In addition, the five different cell types implemented were characterized to determine which cell size is most optimal for a 180nm NVRAM macro.

For characterization of the NVRAM cells, 100 readings were performed on each of the chips just after the programming process and the number of unstable bits in each cell size was determined. The results are shown in Table 3.2.

We observed that the cells where the programming was most effective was the 3X and 2X cells. This proved that increasing the size of the coupling capacitors improves the coupling ratio, generating a larger electric field between the control nodes and

---

[13] Fabrizio y KOVÁCS-VAJNA Zsolt Miklós MILANI Luca; TORRICELLI. "Single-Poly-EEPROM Cell in Standard CMOS Process for Medium-Density Applications". En: *IEEE Transactions on Electron Devices* 62.10 (2015), págs. 3237-3243. DOI: 10.1109/TED.2015.2461660.

[14] Yunlong. y WU Nanjian. FENG Peng; LI. "An ultra low power non-volatile memory in standard CMOS process for passive RFID tags". En: *2009 IEEE Custom Integrated Circuits Conference*. 2009, págs. 713-716. DOI: 10.1109/CICC.2009.5280734.

the floating gate and thus programming the NVRAM cells.

3.2. NVRAM DESIGN CHALLENGES

The main challenges of implementing non-volatile memory in standard CMOS technology are guaranteeing the reliability of the cell and ensuring that the programming voltage is high enough to guarantee Fowler-Nordheim tunneling, but not so high as to damage the transistors of the memory cell. As demonstrated by performing the characterization of the NVRAM implemented in 180nm CMOS technology, not all of the designed memory cells were effective during the programming process. Only the 3X cells were 100 % effective. This could only be known by performing laboratory measurements after the fabrication of the NVRAM, and the exact programming voltage was unknown.

To avoid implementing memory cells that do not work properly, it is necessary to verify the circuit before manufacturing. Therefore, it is necessary to have a Fowler-Nordheim tunneling model for programming NVRAM cells in order to simulate the memory programming process, determine the necessary voltage for programming and the ideal dimensions of each transistor for a correct operation of the memory after its manufacture.

4. FOWLER-NORDHEIM TUNNELING MODEL FOR SIMULATION

In this project, two Fowler-Nordheim tunneling models were implemented for Floating Gates-based memory cells. Both models were described in Verilog A and simulated for 28nm and 180nm CMOS technology.

4.1. FLOATING GATE BASIC MODEL

This model makes it possible to simulate the change in voltage at the floating gates of the NVRAM cell generated by the Fowler-Nordheim tunneling current.
It is built based on Equation 1. The voltage at the floating gate can be determined as a sum of voltages, which depend on the capacitance of the coupling, readout, and tunneling transistors, the voltages applied to the control nodes, and the electric charge on the floating gate (Q_{FG}).
The charge on the floating gate (Q_{FG}) will vary over time due to the Fowler-Nordheim tunneling phenomenon, and if an electric field strong enough to tunnel electrons through the transistor oxide is generated. This charge can be calculated as a function of time as follows [15]:

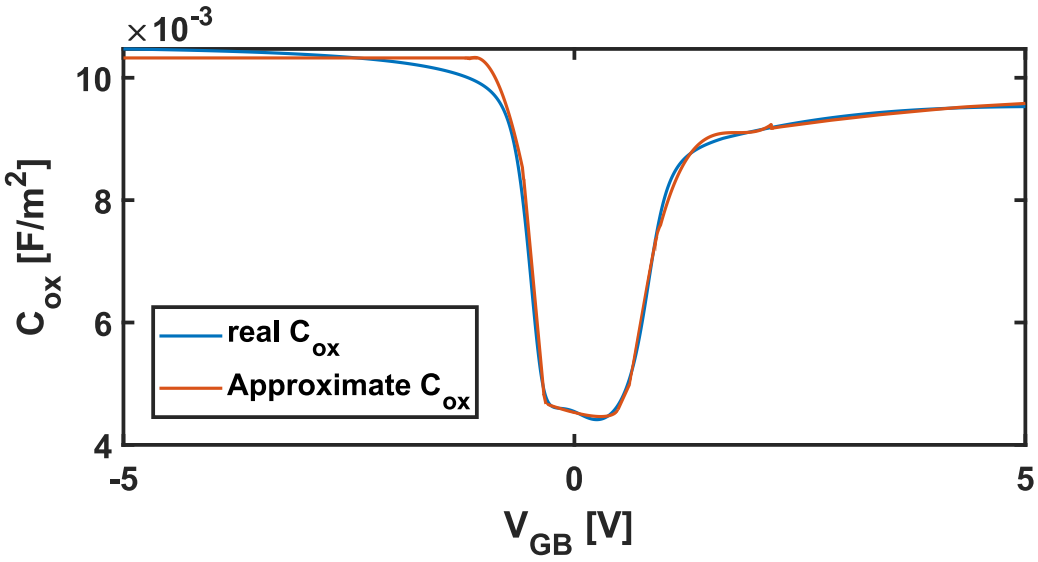
$$Q_{FG} = \int I_{FN} dt \tag{6}$$

where the tunneling current I_{FN} can be calculated from Equations 3 and 4.
It should be noted that the capacitance C_{CG}, C_{TG}, C_{WL}, and therefore C_{tot} are not constant; given the gate capacitance of a MOSCAP, its capacitance varies as a fun-

---

[15] P.-D. MAUROUX y col. “A two-layer SPICE model of the ATMEL TSTAC™ eFlash memory technology for defect injection and faulty behavior prediction”. En: *2010 15th IEEE European Test Symposium*. 2010, págs. 81-86. DOI: 10.1109/ETSYM.2010.5512776.

Figure 4.1. C_{ox} as a function of voltage for a TSMC 28nm transistor, along with the approximation used for the model description in Verilog A.



ction of the voltage difference applied between its terminals [16].

To take into account this capacitance variation in the model described in Verilog A, the $C_{ox}[F/m^2]$ capacitance of a PMOS connected as a capacitor was simulated in the Cadence Virtuoso tool using TSMC's 28nm and 180nm PDK. Then, the C_{ox} capacitance obtained was divided into sections and approximated using polynomials of different orders to obtain a piecewise function approximating the actual capacitance of the technology used.

Figure 4.1. shows the capacitance as a function of the voltage of a 28nm technology transistor and the polynomial approximation used for the description in Verilog A.

By multiplying the area of the coupling, tunneling, and readout transistors by the calculated C_{ox} approximation, the C_{CG}, C_{TG}, C_{WL}, and C_{tot} capacitances as a function of voltage can be obtained.

---

[16] Cong LI y col. "A model for single poly EEPROM cells". En: *2014 12th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT)*. 2014, págs. 1-3. DOI: 10.1109/ICSICT.2014.7021487.

The Verilog A description of the Floating Gate basic model in 28nm is given in Annexe A. The model can be used for any CMOS technology as long as the value of the parameters t_{ox}, L, W_{CG}, W_{TG}, and W_{WL} are changed according to the dimensions of the technology used, and C_{ox} must be calculated and approximated as explained above.

The testbench to simulate the NVRAM cell programming process using this model is shown in Figure 4.2. Where the floating gates are replaced by the model described in Verilog A (blue elements in the figure), whose inputs are the voltages applied to the control nodes, and whose output is the voltage at the floating gate. Using this model, we can vary the dimensions of the transistors in the NVRAM cells or the programming voltage VH and observe how both the voltage on the Floating Gates (V_{FG}) and the current in the BL and BLB branches change.

By simulating the NVRAM programming process with different transistor dimensions, it is possible to determine the ideal dimensions for the NVRAM cells so they can be programmed at a given VH voltage.

It should be remembered that to guarantee the Fowler Nordheim tunneling phenomenon, Equation 5. must be fulfilled. For 28nm technology, the oxide width (t_{ox}) is 4nm, so the minimum electric field for tunneling to occur, and therefore cell programming is:

$$|E_{ox}|_{min} = \frac{\phi}{t_{ox}} = \frac{3.2eV}{4nm} = 800MV/m \tag{7}$$

Figure 4.3. shows different simulations using the model in 28nm technology. For the same voltage VH and varying the dimensions of the coupling capacitors, programming is observed only for cells with larger transistors.

It shows the electric fields that affect the NVRAM programming process. The convention used is $E_{node1-node2}$, where it refers to the electric field between nodes 1 and 2. The figure shows the E_{TG-FG1}, E_{FG1-WL}, E_{TG-FG2}, E_{FG2-WL} and $|E_{ox}|_{min}$ fields for the programming process of a logic 1. Where, theoretically over time, the voltage

Figure 4.2. Floating gates basic model test bench for NVRAM cells, where the blue elements are the model described in Verilog A.

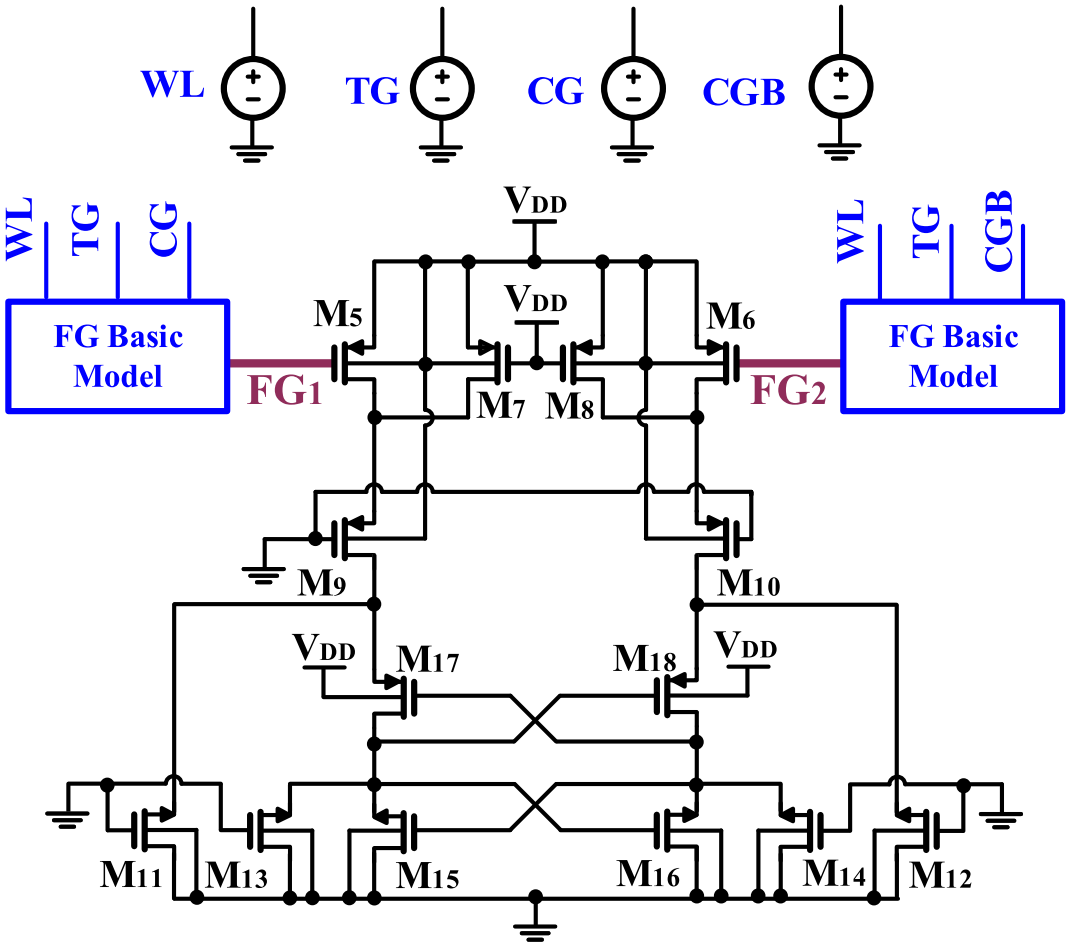
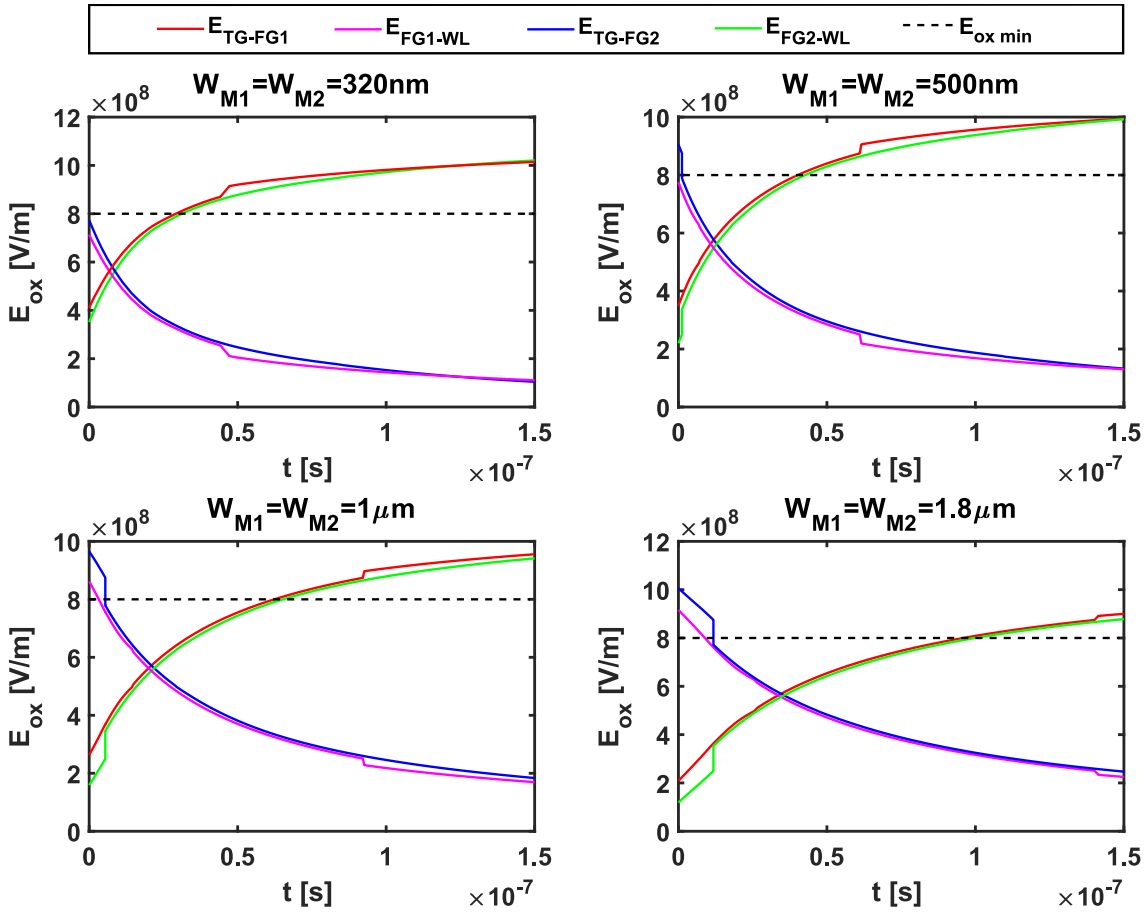


Figure 4.3. Simulation with the Floating Gate Basic Model of the electric fields (E_{ox}) in the floating gates ($FG1$ and $FG2$) of the NVRAM at 28nm. By programming logic 1 with different cell sizes for VH=7V.



at Floating Gate 1 ($FG1$) should decrease while the voltage at Floating Gate 2 ($FG2$) should increase, so the electric fields should vary according to these voltages.

To ensure the NVRAM cell programming, all electric fields must exceed the 800MV/m barrier at some point. The simulations show that this only occurs for cells with larger W_{M1} and W_{M2}, in this example $1\mu m$ and $1.8\mu m$.

This model is effective to determine the high voltage (VH) to be applied to the control nodes to program the memory cells and gives a notion of the proper dimensions for the NVRAM design. However, it is an approximation, as it does not consider the

complete TSMC transistor model, only the gate capacitance variation is taken into account.

For this reason, a more complex model was developed, which integrates the Fowler-Nordheim tunneling current to a TSMC transistor.

4.2. FOWLER-NORDHEIM TUNNELING COMPLETE MODEL

This model simulates the effect of the Fowler-Nordheim tunneling current in a TSMC transistor, taking into account the complete model of the TSMC transistor in 28nm and 180nm technology.

It is built based on Equation 3 and the understanding of the Fowler-Nordheim tunneling phenomenon, by adding a tunneling current source (I_{FN}) described in Verilog A between the Gate and Bulk terminals of the transistor of the technology used.

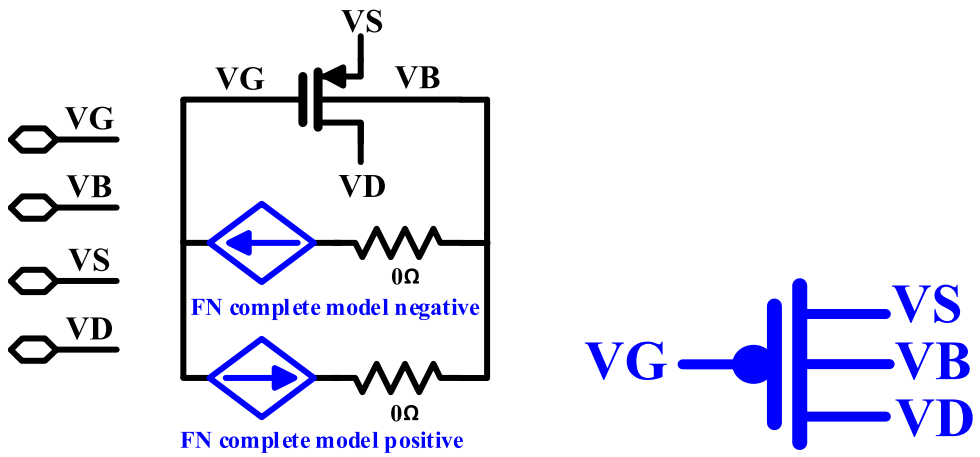
As can be seen in Equation 3 and Equation 4, the magnitude of the tunneling current depends on the magnitude of the electric field between the Gate and Bulk terminals of the transistor. While the direction of the current depends on the direction of the electric field, as illustrated in Figure 2.3.

This model consists of two tunneling current (I_{FN}) descriptions made in Verilog A.

The first model description corresponds to a Fowler-Nordheim tunneling current source (I_{FN}) connected between the terminals Gate and Bulk of the TSMC transistor. This source will be active only when the electric field (E_{ox}) between the transistor terminals is positive following the convention defined in Equation 4. The tunneling current (I_{FN}) will flow from the Gate to the Bulk of the transistor.

The second model description also corresponds to a Fowler-Nordheim tunneling current source (I_{FN}) connected between the Gate and Bulk of the TSMC transistor. The difference is that this source will only be active when the electric field (E_{ox}) between the transistor terminals is negative, and therefore the described current will flow from the Bulk to the Gate of the transistor.

Figure 4.4. TSMC thick oxide transistor with Fowler-Nordheim tunneling current model: a) Schematic; b) Symbol.



(a) (b)

Figure 4.4. shows the connection between the TSMC thick oxide transistor and the two tunneling current sources described in Verilog A. Along with the symbol designed for the TSMC transistor that includes the Fowler-Nordheim tunneling phenomenon. A 0 Ω resistor was connected in series to each source described in Verilog A for simulation purposes to avoid connecting both sources in a short circuit.

The Verilog A description of the Fowler-Nordheim current source for the positive electric field is found in Annexe B. And Annexe C contains the Verilog A current source description for the negative electric field.

In the Verilog A description of the tunneling current (I_{FN}), we avoided the use of conditional sentences which can generate discontinuities and cause severe convergence problems during the simulation. Therefore, the tunneling current (I_{FN}) was multiplied by a factor (f_{pos} or f_{neg}) that would allow each of the current sources to be turned on or off when the electric field (E_{ox}) changed from positive to negative.

The current source factor for the positive electric field (f_{pos}) is defined as follows:

$$f_{pos} = \frac{e^{E_{ox}}}{\lambda + e^{E_{ox}}} \tag{8}$$

Where $f_{pos} \to 0$ if $|E_{ox}| < 0$ and $f_{pos} \to 1$ if $|E_{ox}| > 0$.

The current source factor for the negative electric field (f_{neg}) is defined as follows:

$$f_{neg} = \frac{e^{-E_{ox}}}{\lambda + e^{-E_{ox}}} \tag{9}$$

Where $f_{neg} \to 0$ if $|E_{ox}| > 0$ and $f_{neg} \to 1$ if $|E_{ox}| < 0$.

λ is a constant whose value was calculated to minimize the relative error (ϵ_r) between the real tunneling current (I_{FN}) and the tunneling current multiplied by the factor f_{pos} or f_{neg}.

The calculation of the relative error (ϵ_r) as a function of λ is shown below using the factor for positive electric fields (f_{pos}).

- Calculation of the relative error (ϵ_r) for positive E_{ox} and $|E_{ox}| \to \infty$.

$$\begin{aligned}
\epsilon_r &= \frac{I_{FN} - I_{FN}.f_{pos}}{I_{FN}} \\
\epsilon_r &= 1 - f_{pos} \\
\epsilon_r &= 1 - \frac{e^{E_{ox}}}{\lambda + e^{E_{ox}}} \\
\epsilon_r &= 1 - 1 \\
\epsilon_r &= 0
\end{aligned} \tag{10}$$

- Calculation of the relative error (ϵ_r) for positive E_{ox} and $|E_{ox}|\acute{}1$.

$$\begin{aligned}
\epsilon_r &= \frac{I_{FN} - I_{FN}.f_{pos}}{I_{FN}} \\
\epsilon_r &= 1 - f_{pos} \\
\epsilon_r &= 1 - \frac{e^{E_{ox}}}{\lambda + e^{E_{ox}}} \\
\epsilon_r &= 1 - \frac{1 + E_{ox}}{\lambda + 1 + E_{ox}} \\
\epsilon_r &= 1 - \frac{1}{\lambda + 1}
\end{aligned} \tag{11}$$

Now, the calculation of the relative error (ϵ_r) as a function of λ using the factor for negative electric fields is shown (f_{neg}).

- Calculation of the relative error (ϵ_r) for negative E_{ox} and $|E_{ox}| \to -\infty$.

$$\begin{aligned}
\epsilon_r &= \frac{I_{FN} - I_{FN}.f_{neg}}{I_{FN}} \\
\epsilon_r &= 1 - f_{neg} \\
\epsilon_r &= 1 - \frac{e^{-E_{ox}}}{\lambda + e^{-E_{ox}}} \\
\epsilon_r &= 1 - 1 \\
\epsilon_r &= 0
\end{aligned} \tag{12}$$

- Calculation of the relative error (ϵ_r) for negative E_{ox} and $|E_{ox}|\acute{}1$.

$$\begin{aligned} \epsilon_r &= \frac{I_{FN} - I_{FN}.f_{neg}}{I_{FN}} \\ \epsilon_r &= 1 - f_{neg} \\ \epsilon_r &= 1 - \frac{e^{-E_{ox}}}{\lambda + e^{-E_{ox}}} \\ \epsilon_r &= 1 - \frac{1 - E_{ox}}{\lambda + 1 - E_{ox}} \\ \epsilon_r &= 1 - \frac{1}{\lambda + 1} \end{aligned} \tag{13}$$

It can be observed that the relative error (ϵ_r) for large electric field magnitudes (E_{ox}) is negligible. For electric fields (E_{ox}) close to 0 V/m, there is an error of $\epsilon_r = 1 - \frac{1}{\lambda+1}$. After performing a sweep of possible values, we determined that the most optimal value of λ is $\lambda = 1$. Since it centers the factor for the positive and negative electric fields (f_{pos} and f_{neg}) at $E_{ox} = 0V/m$, which ensures that for $E_{ox} = 0V/m$ the tunneling current I_{FN} is 0A, and that the relative error (ϵ_r) is symmetrically distributed for small positive and negative electric fields (E_{ox}), as shown in Figure 4.5.

The model's performance was tested by applying a voltage difference between the Gate and Bulk terminals of the 28nm technology transistor including the tunneling current (I_{FN}) model.

The current generated between the two terminals corresponds to the magnitude and direction of the Fowler-Nordheim tunneling current (I_{FN}) as a function of the potential difference between Gate and Bulk. Figure 4.6. shows the current obtained from the simulator with the Verilog A model and the expected theoretical tunneling current.

By simulating the programming process of the NVRAM cell using the transistors that include this model, and varying the high programming voltage VH, it is observed how the voltage at the Floating Gate (V_{FG}) and the current through the BL and BLB

Figure 4.5. f_{pos} and f_{neg} as a function of E_{ox} for various values of λ

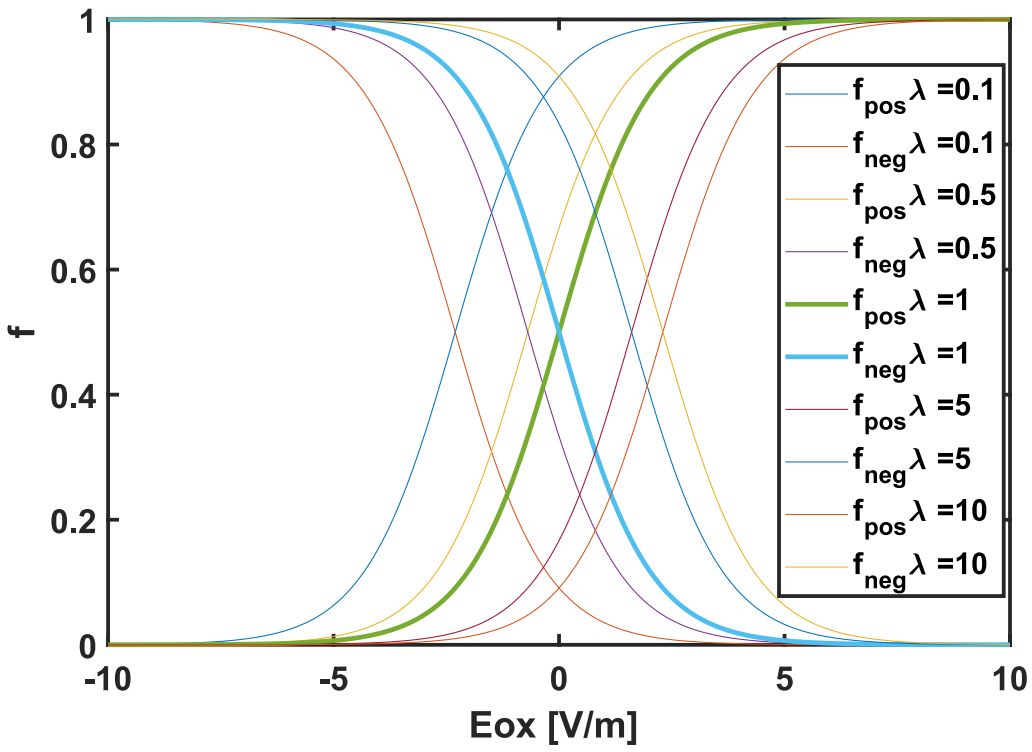
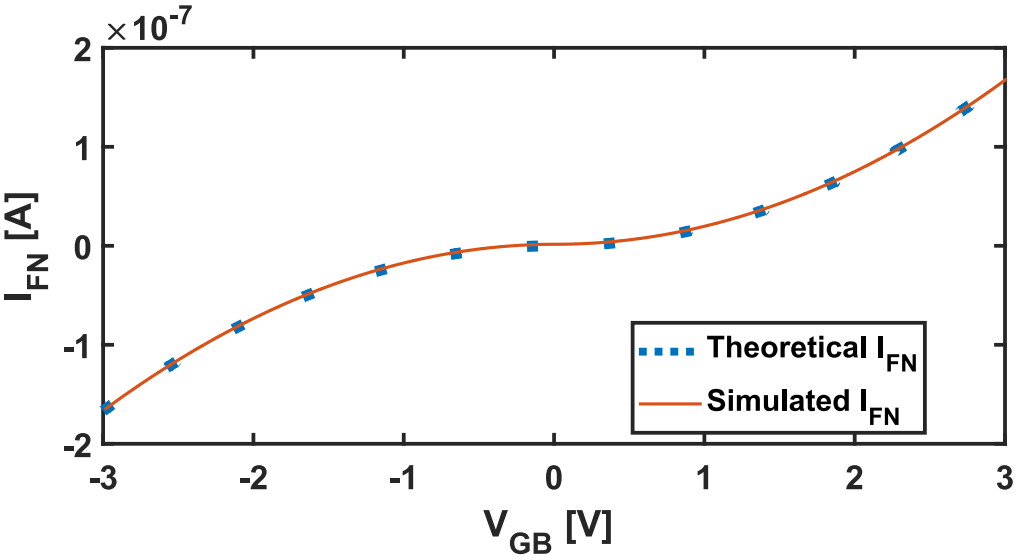


Figure 4.6. Simulated I_{FN} as a function of voltage using the model implemented in 28nm technology and the expected theoretical I_{FN}.



branches varies due to the Fowler Nordheim tunneling phenomenon.

The test bench used to simulate the NVRAM using this model is shown in Figure 4.7. For simulation purposes, a capacitor and resistor were connected in parallel to each floating gate, these devices provide the initial charge condition in the Floating Gates (Q_{FG}) to avoid convergence errors due to the presence of floating nodes. The resistor has a high value of $1M\Omega$, and the capacitance has a small value of $0.1fF$ so that its presence does not significantly affect NVRAM performance.

Figure 4.8 shows the simulation of the NVRAM programming process of a logic 1 in 28nm technology. By varying the programming voltage VH at the control nodes, the voltage at the floating gates (V_{FG}) changes. For low VH voltages, such as $VH = 0.5V$, there is no difference between the voltage of both floating gates, so it is not possible to program the memory cell. As we increase the voltage VH the difference between the voltage of each floating gate increases. When the electric field (E_{ox}) reaches $800MV/m$, the voltage at Floating Gate one ($FG1$) decreases while the voltage at Floating Gate two ($FG2$) increases, increasing the differential voltage and generating a large current difference between the BL and BLB branches, defining the programming of logic 1 in the NVRAM cell.

This model allows us to know the programming voltage VH necessary to program an NVRAM memory based on Floating gates. It, also allows us to define the optimal dimensions of the transistors for the correct operation of the NVRAM programming process.

This model can be used to simulate any CMOS technology if, in the description in Verilog A, the oxide width (t_{ox}) value is modified according to the technology used.

Figure 4.7. Fowler-Nordheim tunneling complete model test bench for NVRAM cells, where the blue elements are the model described in Verilog A.

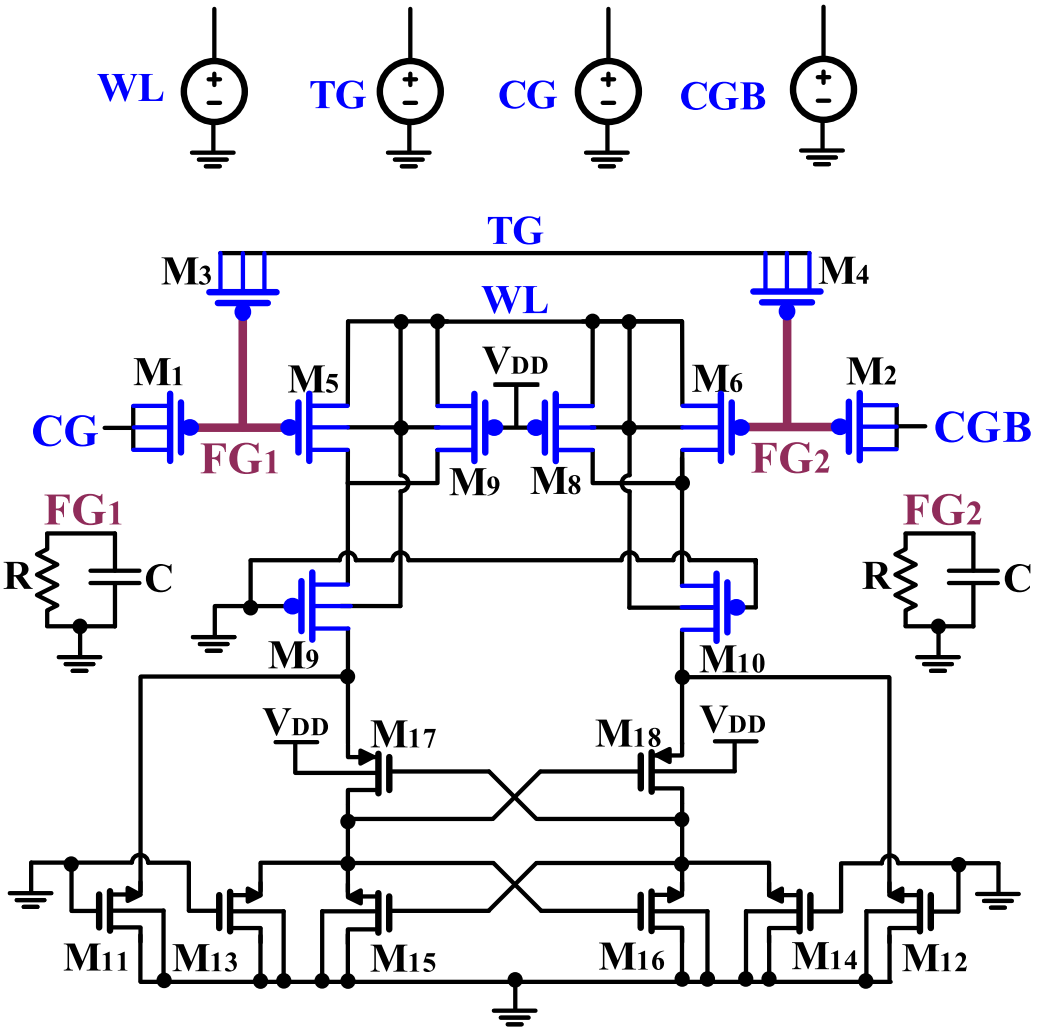
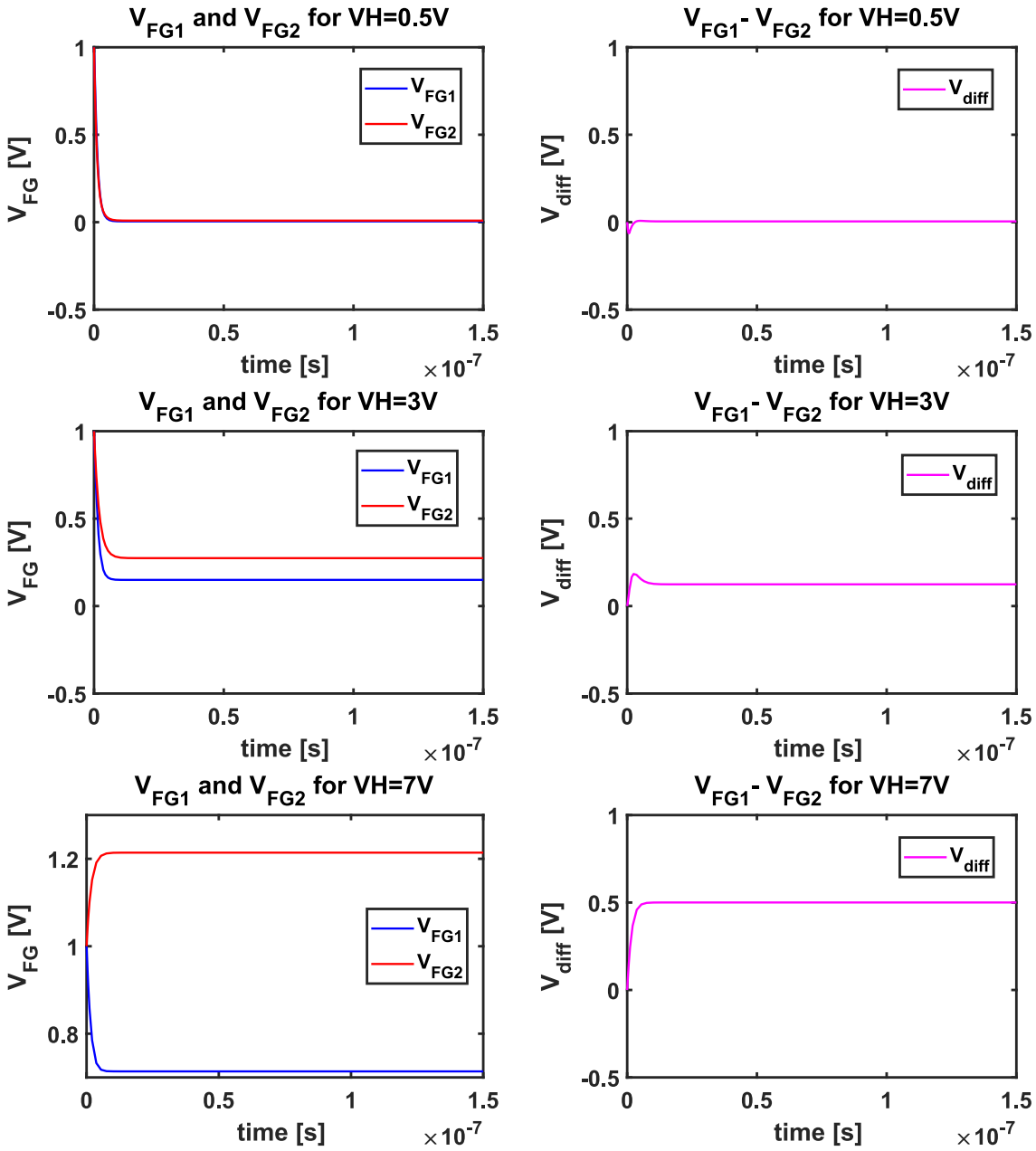


Figure 4.8. Simulation with the complete model of the voltage in the floating gates (V_{FG1} and V_{FG2}). Together with the differential voltage for transistors with $W_{M1} = W_{M2} = 1.2\mu m$ in 28nm technology.



5. NVRAM CELLS DESIGN IN 28 NM CMOS TECHNOLOGY

For the design of the NVRAM in 28nm CMOS technology, both for the memory cells and the Sense Amplifier circuit, the transistors used were the thick gate-oxide I/O devices from TSMC. The width of the oxide (t_{ox}) in this technology is 4nm, and its operating voltage is 1.8V.

The dimensions of each transistor in the NVRAM cells and its programming voltage (VH) were defined using the two Fowler-Nordheim tunneling models developed in this project.

The programming voltage (VH) defined for the NVRAM designed in 28nm is $VH = 7V$. This voltage allows NVRAM cells to generate Fowler-Nordheim tunneling current (I_{FN}) without damaging the oxide and thus ensures the correct operation of the memory during the programming process.

The dimensions of each transistor in the designed NVRAM and Sense Amplifier cells are shown in Table 5.1.

The design of the Sense Amplifier considered the high transient currents generated by the power supply and the BL and BLB nodes. To avoid this problem, the M_{17} and M_{18} transistors of the Latch are wider than the other transistors in the circuit [17].

[17] BEHZAD RAZAVI. "The StrongARM Latch [A Circuit for All Seasons]". En: *IEEE Solid-State Circuits Magazine* 7.2 (2015), págs. 12-17. DOI: 10.1109/MSSC.2015.2418155.

Table 5.1. MOSFET size in NVRAM and Sense Amplifier cells in 28 nm CMOS technology.

Devices*		W
NVRAM Cells	M_1,M_2	1.2μm
	M_3-M_{10}	0.32μm
Sense Amplifier	M_{11}-M_{16}	0.32μm
	M_{17}, M_{18}	2.4μm

* All devices have $L = 0.15\mu m$.

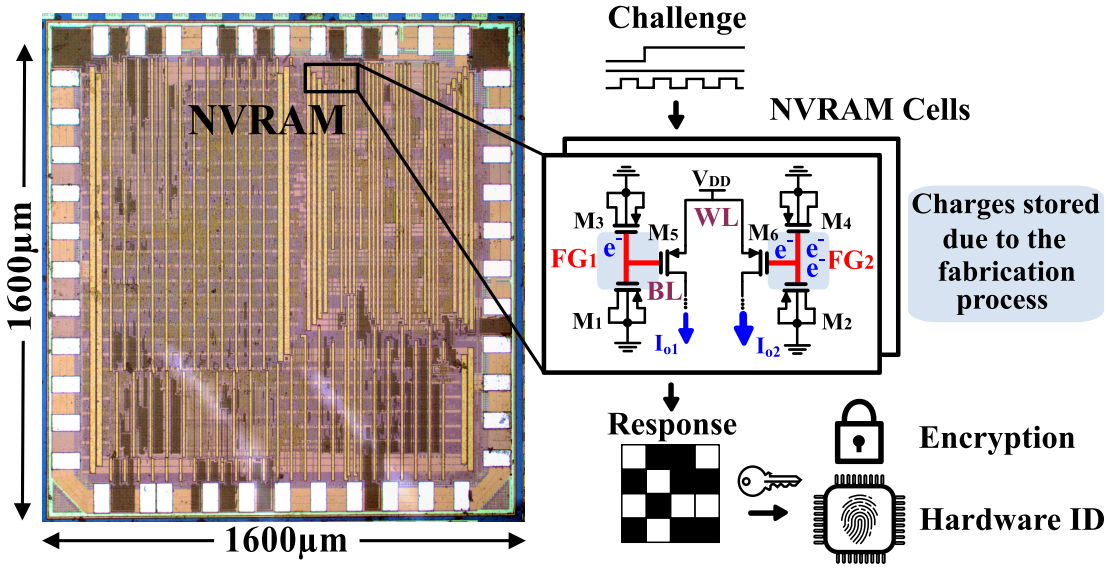
6. NVRAM APPLICATIONS

Typical applications of non-volatile memories include system-on-chip applications with low storage capacity, such as microcontrollers or IP security. New applications for NVRAM cells are constantly being investigated, such as its use in data processing in the Cloud or new computing systems [1] [2]. In the Onchip group of the Universidad Industrial de Santander, we propose the use of NVRAM cells as Physically Unclonable Function cells [11].

6.1. NVRAM CELLS AS PUF CELLS

Physically Unclonable Functions (PUFs) are binary functions of which the behavior depends on IC manufacturing variations. The response of a good PUF is characterized by being random and unique. These characteristics allow PUFs to be used to generate reliable and stable encryption keys for security and authentication applications and therefore have generated interest in the implementation of silicon PUFs.
The proposed PUF based on NVRAM cells takes advantage of the amount of charge residing in each of the Floating Gates due to random intrinsic differences during the memory fabrication process, such as gate ionization during the fabrication process and gate dielectric construction for unprogrammed cells.
These charges generate a differential current that is latched by the Sense Amplifier of the cells and defined as a logic 0 or 1, producing a reliable PUF key that can be used in different encryption and security applications. The PUF cell concept from NVRAM cells is shown in Figure 6.1.

Figure 6.1. Physically Unclonable Function based on NVRAM cell fabricated in 180nm CMOS technology for encryption and hardware identification applications.



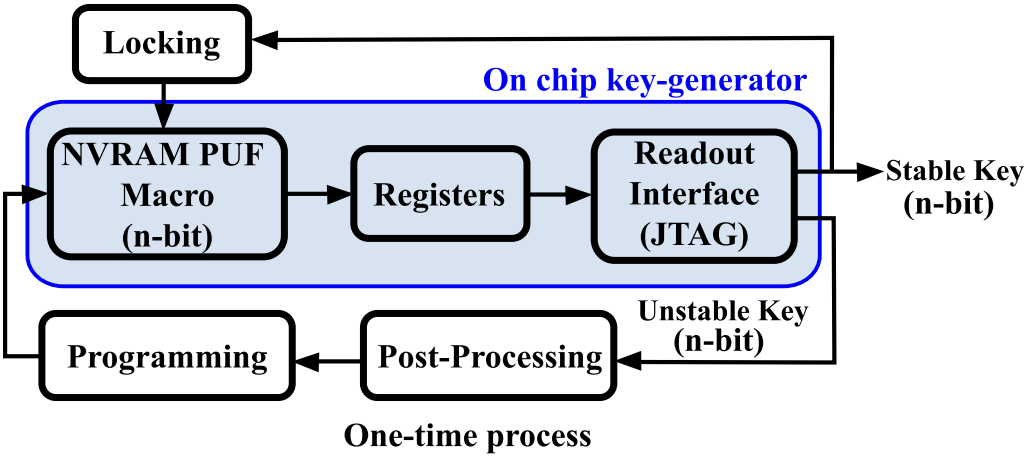
6.2. IMPLEMENTED PUF MACRO IN 180 NM CMOS TECHNOLOGY

From the readings of the NVRAM cells done for the characterization of the NVRAM macro fabricated in 180nm CMOS technology, results of the use of NVRAM cells as PUF cells were obtained and presented at the International Symposium on Circuits and Systems (ISCAS) 2020 conference [11].

We performed 2000 reads of the unprogrammed cells to obtain the raw PUF keys to examine the impact of noise and insufficient random variations in the differential floating gates. We counted the number of occasionally flipping or unstable bits of the repeatedly measured PUF bit cells and determined that this variation was less than $3\,\%$ for raw keys.

To ensure a stable and secure PUF key, the obtained keys were post-processed

Figure 6.2. Block diagram of the proposed PUF key-generator.



using the temporal majority voting (TMV) [18] and UP/DOWN-counter (UDC) [19] mechanisms. We defined that the most effective post-processing mechanism is the UP/DOWN counter since it allows obtaining $100\,\%$ stable keys from the raw PUF keys.

After post-processing, the stable keys are written back into the memory cells and locked against programming attacks using the NVRAM cell programming and locking configurations shown in Figure 3.3.

The process described for obtaining PUF keys from NVRAM cells is shown in Figure 6.2.

---

[18] S. K. MATHEW y col. "A 0.19pJ/b PVT-Variation-Tolerant Hybrid Physically Unclonable Function Circuit for 100 % Stable Secure Key Generation in 22nm CMOS". En: *ISSCC* (2014).

[19] Vinay C. y KUNDU Sandip VIJAYAKUMAR Arunkumar; PATIL. "On Improving Reliability of SRAM-Based Physically Unclonable Functions". En: *Journal of Low Power Electronics and Applications* 7.1 (2017). DOI: 10.3390/jlpea7010002.

Table 6.1. Measured Perfomance Comparison.

	This Work	[22]	[23]	[24]
Technology	180nm	130nm	22nm	65nm
Type	NVR	RRAM	Hybrid	Static
Raw Unst. Bits (Readings)	2.4 % (2000)	NA	25 % (1000)	2.95 % (2000)
Stabilization Method	UDC NVR	Burn-in	TMV +Burn-in +Dark Bits	TMV EVB
Unst. Bits After Stab.	0 %	0 %	0 %	0.024 %
Voltage Typ.	3.3V	1.8V	0.8V	1.2V
Bit Evaluation Current-Range	100nA	500nA	500nA	NA
Reconfigurable	Yes	Yes	No	No
Write-Protection	Yes	No	-	-
Bit Cell Area	20μm^2	2.86μm^2	4.66μm^2	562F^2

6.3. PRIOR ART COMPARISON

Similar recent work produced reliable PUF cells using resistive random access memory technology [20], and single use programmable cells employing the oxide breakdown mechanism [21]. Table 6.1. summarizes the measurement results of the proposed PUF from NVRAM cells and compares them with the prior art.

[20] Y. PANG y col. “A Reconfigurable RRAM Physically Unclonable Function Utilizing Post-Process Randomness Source With $<$6x10^6 Native Bit Error Rate”. En: *ISSCC* (2019).

[21] M. WU y col. “A PUF Scheme Using Competing Oxide Rupture with Bit Error Rate Approaching Zero”. En: *ISSCC* (2018).

7. CONCLUSION

In this work, an NVRAM macro implemented in 180nm CMOS technology was characterized and each type of NVRAM cell was tested in the laboratory for the reading and programming processes. It was concluded that the most optimal cell for the 180nm implementation is the 3X cell, following the terminology used in this project, where the dimensions of the coupling transistors are $W = 3.6\mu m$ and $L = 300nm$.

Two simulation models of the Fowler-Nordheim tunneling phenomenon described in Verilog A were developed. These models can be used in any CMOS technology and allow us to know the programming voltage VH necessary to program NVRAM cells, in addition to providing a notion of the optimal cell dimensions.

NVRAM cells were designed in 28nm CMOS technology together with the sense amplifier. The programming process of the cells was verified using the tunneling models developed in this project.

Finally, the use of NVRAM cells as Physically Unclonable Function cells was proposed and tested, obtaining $100\,\%$ stable and reliable PUF keys. This demonstrated that NVRAM cells manufactured in standard CMOS technology have many applications at a low cost since they do not require the use of additional masks during the manufacturing process, being a better alternative to EEPROM or Flash memories.

BIBLIOGRAPHY

ARDILA, Javier y col. “A Stable Physically Unclonable Function Based on a Standard CMOS NVR”. En: *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*. 2020, págs. 1-4. DOI: 10.1109/ISCAS45731.2020.9180411 (vid. págs. 23, 43, 44).

CARLEY, L.R. “Trimming analog circuits using floating-gate analog MOS memory”. En: *IEEE International Solid-State Circuits Conference, 1989 ISSCC. Digest of Technical Papers*. 1989, págs. 202-203. DOI: 10.1109/ISSCC.1989.48260 (vid. pág. 20).

FENG Peng; LI, Yunlong. y WU Nanjian. “An ultra low power non-volatile memory in standard CMOS process for passive RFID tags”. En: *2009 IEEE Custom Integrated Circuits Conference*. 2009, págs. 713-716. DOI: 10.1109/CICC.2009.5280734 (vid. pág. 25).

HOYA, Katsuhiko y col. “A perspective on NVRAM technology for future computing system”. En: *2019 International Symposium on VLSI Technology, Systems and Application (VLSI-TSA)*. 2019, págs. 1-2. DOI: 10.1109/VLSI-TSA.2019.8804706 (vid. págs. 12, 43).

KANNAN, Sudarsun y col. “Using Active NVRAM for Cloud I/O”. En: *2011 Sixth Open Cirrus Summit*. 2011, págs. 32-36. DOI: 10.1109/OCS.2011.12 (vid. págs. 12, 43).

KLANDERMAN, Ronnie. “Flash memory device: Electrical modeling and simulation”. En: 2012 (vid. pág. 18).

LI, Cong y col. “A model for single poly EEPROM cells”. En: *2014 12th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT)*. 2014, págs. 1-3. DOI: 10.1109/ICSICT.2014.7021487 (vid. pág. 28).

LI, Cong y col. “Multitime Programmable Memory Cell With Improved MOS Capacitor in Standard CMOS Process”. En: *IEEE Transactions on Electron Devices* 62.8 (2015), págs. 2517-2523. DOI: 10.1109/TED.2015.2443651 (vid. pág. 15).

LI, YD. y col. “A 562F2 Physically Unclonable Function with a Zero-Overhead Stabilization Scheme”. En: *ISSCC* (2019) (vid. pág. 46).

LIM Ee Wah y ISMAIL, Razali. “Conduction Mechanism of Valence Change Resistive Switching Memory: A Survey”. En: *Electronics* 4.3 (2015), págs. 586-613. DOI: 10.3390/electronics4030586 (vid. pág. 20).

MATHEW, S. K. y col. “A 0.19pJ/b PVT-Variation-Tolerant Hybrid Physically Unclonable Function Circuit for 100 % Stable Secure Key Generation in 22nm CMOS”. En: *ISSCC* (2014) (vid. págs. 45, 46).

MAUROUX, P.-D. y col. “A two-layer SPICE model of the ATMEL TSTAC™ eFlash memory technology for defect injection and faulty behavior prediction”. En: *2010 15th IEEE European Test Symposium*. 2010, págs. 81-86. DOI: 10.1109/ETSYM.2010.5512776 (vid. pág. 27).

MILANI Luca; TORRICELLI, Fabrizio y KOVÁCS-VAJNA Zsolt Miklós. “Single-Poly-EEPROM Cell in Standard CMOS Process for Medium-Density Applications”. En: *IEEE Transactions on Electron Devices* 62.10 (2015), págs. 3237-3243. DOI: 10.1109/TED.2015.2461660 (vid. pág. 25).

PANG, Y. y col. “A Reconfigurable RRAM Physically Unclonable Function Utilizing Post-Process Randomness Source With $<$6x10^6 Native Bit Error Rate”. En: *ISSCC* (2019) (vid. pág. 46).

PESAVENTO Alberto y DIOIO, Christopher J. “RFID IC tunneling-voltage profile calibration”. En: *U.S.Patent 8,902,627 B1* (Dec 2, 2014) (vid. pág. 23).

PESAVENTO Alberto; BERNARD, Frédéric J. y HYDE John D. “PFET NONVOLATILE MEMORY”. En: *U.S.Patent 7,221,596 B2* (May 22, 2007) (vid. pág. 15).

RASZKA, J. y col. “Embedded flash memory for security applications in a 0.13 /spl mu/m CMOS logic process”. En: *2004 IEEE International Solid-State Circuits Conference (IEEE Cat. No.04CH37519)*. 2004, 46-512 Vol.1. DOI: 10.1109/ISSCC.2004.1332586 (vid. pág. 12).

RAZAVI, BEHZAD. “The StrongARM Latch [A Circuit for All Seasons]”. En: *IEEE Solid-State Circuits Magazine* 7.2 (2015), págs. 12-17. DOI: 10.1109/MSSC.2015.2418155 (vid. pág. 41).

SONG Seung-Hwan; CHUL CHUN, Ki y KIM Chris H. “A Bit-by-Bit Re-Writable Eflash in a Generic 65 nm Logic Process for Moderate-Density Nonvolatile Memory Applications”. En: *IEEE Journal of Solid-State Circuits* 49.8 (2014), págs. 1861-1871. DOI: 10.1109/JSSC.2014.2314445 (vid. pág. 13).

VIJAYAKUMAR Arunkumar; PATIL, Vinay C. y KUNDU Sandip. “On Improving Reliability of SRAM-Based Physically Unclonable Functions”. En: *Journal of Low Power Electronics and Applications* 7.1 (2017). DOI: 10.3390/jlpea7010002 (vid. pág. 45).

WANG B. y MA, Y. “Opportunities and Challenges in Multi-Times-Programmable Floating-Gate Logic Non-Volatile Memories”. En: *2008 Joint Non-Volatile Semicon-*

ductor Memory Workshop and International Conference on Memory Technology and Design. 2008, págs. 22-25. DOI: 10.1109/NVSMW.2008.12 (vid. pág. 12).

WU, M. y col. “A PUF Scheme Using Competing Oxide Rupture with Bit Error Rate Approaching Zero”. En: *ISSCC* (2018) (vid. pág. 46).

ANNEXES

Annexe A. Verilog A description of Floating Gate basic model

```
‘include "constants.vams"
‘include "disciplines.vams"

module FN_model_all_cells_thick_oxide(
input VCG, VTG, VWL,
output VFG
);

electrical VCG, VTG, VWL, VFG;
electrical V1, V2, V3;

parameter real Qfg0=0;
parameter real A=2.966559287731918e-25;
parameter real B=4.372381857356148e-67;
parameter real tox=4e-9;
parameter real L=150e-9;
parameter real Wcg=300e-9;
parameter real Wtg=150e-9;
parameter real Wwl=150e-9;

real Ifn, Qfg, Eox;
real Vtg, Vcg;
real Vfg, Vwl;
```

```
real Ccg, Ctg, Cwl, Ctot;
real Qfg_temp;

analog begin

        @(initial_step) begin
        Qfg=Qfg0;
        Eox=5e3;
        end

        Vtg=V(VTG);
        Vcg=V(VCG);
        Vwl=V(VWL);
        Vfg=V(VFG);

        Ifn=A*Eox*Eox*limexp(-B/Eox);
        Qfg_temp=idt(Ifn,Qfg0);

        // Ccg
        if((Vcg-Vfg) <-1.0) begin
        Ccg=0.01033*Wcg*L;
        end
        if((Vcg-Vfg) >=-1.0 && (Vcg-Vfg)<-0.4) begin
        Ccg=(-0.01411*((Vcg-Vfg)**2)
        -0.02661*(Vcg-Vfg)+0.00271)*Wcg*L;
        end
        if((Vcg-Vfg) >=-0.4 &&(Vcg-Vfg)<0.7) begin
```

```
Ccg=(0.01064*((Vcg-Vfg)**4)-0.004521*((Vcg-Vfg)**3)
+0.0006612*((Vcg-Vfg)**2)-0.0002105*(Vcg-Vfg)
+0.004497)*Wcg*L;
end
if((Vcg-Vfg) >=0.7 && (Vcg-Vfg)<2.0) begin
Ccg=(0.004747*((Vcg-Vfg)**3)-0.02281*((Vcg-Vfg)**2)
+0.03653*(Vcg-Vfg)-0.01052)*Wcg*L;
end
if((Vcg-Vfg)>=2.0) begin
Ccg=(-5.051e-05*((Vcg-Vfg)**2)
+0.0004799*(Vcg-Vfg)+0.008384)*Wcg*L;
end

// Ctg
if((Vtg-Vfg) <-1.0) begin
Ctg=0.01033*Wtg*L;
end
if((Vtg-Vfg) >=-1.0 && (Vtg-Vfg)<-0.4) begin
Ctg=(-0.01411*((Vtg-Vfg)**2)
-0.02661*(Vtg-Vfg)+0.00271)*Wtg*L;
end
if((Vtg-Vfg) >=-0.4 &&(Vtg-Vfg)<0.7) begin
Ctg=(0.01064*((Vtg-Vfg)**4)-0.004521*((Vtg-Vfg)**3)
+0.0006612*((Vtg-Vfg)**2)-0.0002105*(Vtg-Vfg)
+0.004497)*Wtg*L;
end
if((Vtg-Vfg) >=0.7 && (Vtg-Vfg)<2.0) begin
```

```
Ctg=(0.004747*((Vtg-Vfg)**3)-0.02281*((Vtg-Vfg)**2)
+0.03653*(Vtg-Vfg)-0.01052)*Wtg*L;
end
if ((Vtg-Vfg)>=2.0) begin
Ctg=(-5.051e-05*((Vtg-Vfg)**2)+0.0004799*(Vtg-Vfg)
+0.008384)*Wtg*L;
end

// Cwl
if ((Vwl-Vfg) <-1.0) begin
Cwl=0.01033*Wwl*L;
end
if ((Vwl-Vfg) >=-1.0 && (Vwl-Vfg)<-0.4) begin
Cwl=(-0.01411*((Vwl-Vfg)**2)
-0.02661*(Vwl-Vfg)+0.00271)*Wwl*L;
end
if ((Vwl-Vfg) >=-0.4 &&(Vwl-Vfg)<0.7) begin
Cwl=(0.01064*((Vwl-Vfg)**4)-0.004521*((Vwl-Vfg)**3)
+0.0006612*((Vwl-Vfg)**2)-0.0002105*(Vwl-Vfg)
+0.004497)*Wwl*L;
end
if ((Vwl-Vfg) >=0.7 && (Vwl-Vfg)<2.0) begin
Cwl=(0.004747*((Vwl-Vfg)**3)-0.02281*((Vwl-Vfg)**2)
+0.03653*(Vwl-Vfg)-0.01052)*Wwl*L;
end
if ((Vwl-Vfg)>=2.0) begin
Cwl=(-5.051e-05*((Vwl-Vfg)**2)+0.0004799*(Vwl-Vfg)
```

```
        +0.008384)*Wwl*L;
        end

        if(Vtg==Vcg) begin
                Eox=V(VFG,VWL)/tox;
                Qfg=-Qfg_temp;

        end
        else begin
                Eox=V(VTG,VFG)/tox;
                Qfg=Qfg_temp;

        end

        Ctot=Ccg+Cwl+Ctg;

        V(V1) <+ Qfg/Ctot;
        V(V2,V1) <+ V(VWL)*Cwl/Ctot;
        V(V3,V2) <+ V(VTG)*Ctg/Ctot;
        V(VFG,V3) <+ V(VCG)*Ccg/Ctot;


end

endmodule
```

Annexe B. Verilog A description of FN current complete model for positive E_{ox}

```
// VerilogA for FN_model_Macro_Transistor, FN_current,
veriloga

`include "constants.vams"
`include "disciplines.vams"

module FN_current(
input VG,
output VB
);

electrical VG, VB;

parameter real A=2.96659287731918e-25;
parameter real B=4.372381857356148e-67;
parameter real tox=4e-9;

real Eox;
real f;

analog begin
        @(initial_step) begin
                Eox=5e3;
         end
```

```
        Eox=(V(VG,VB))/tox;
        f=limexp(Eox)/(1+limexp(Eox));

        I(VG,VB) <+ A*Eox*Eox*limexp(-B/Eox)*f;
end
endmodule
```

Annexe C. Verilog A description of FN current complete model for negative E_{ox}

```
// VerilogA for FN_model_Macro_Transistor, FN_current_neg,
veriloga

`include "constants.vams"
`include "disciplines.vams"

module FN_current_neg(
input VG,
output VB
);

electrical VG, VB;

parameter real A=2.96659287731918e-25;
parameter real B=4.372381857356148e-67;
parameter real tox=4e-9;

real Eox;
real f;

analog begin
        @(initial_step) begin
                Eox=5e3;
         end
```

```
        Eox=(V(VG,VB))/tox;
        f=limexp(-Eox)/(1+limexp(-Eox));

        I(VB,VG) <+ A*Eox*Eox*limexp(-B/Eox)*f;
end
endmodule
```