The Pennsylvania State University
The Graduate School

HARDWARE FUNCTIONAL OBFUSCATION WITH FERROELECTRIC ACTIVE INTERCONNECTS

A Thesis in
Computer Science and Engineering
by
Tongguang Yu

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Master of Science

May 2022

The thesis of Tongguang Yu was reviewed and approved by the following:

Vijaykrishnan Narayana
Robert Noll Chair Professor, Department of Computer Science and Engineering
Pennsylvania State University

John Morgan Sampson
Associate Professor, Department of Computer Science and Engineering
Pennsylvania State University

Sumitha George
Assistant Professor, Department of Electrical and Computer Engineering
North Dakota State University

Kai Ni
Assistant Professor, Department of Electrical and Microelectronic Engineering
Rochester Institute of Technologies

Chitaranjan Das
Department Head and Distinguished Professor, Department of Computer Science and Engineering
Pennsylvania State University

Abstract

Camouflaging gate techniques enhance hardware security, preventing reverse engineering. Layout level camouflaging by adding dummy contacts ensures some level of protection against extracting the correct netlist. Threshold voltage manipulation for multi-functional logic with identical layouts has also been introduced for functional obfuscation. All these techniques increase circuit-complexity with significant area, energy, and delay penalty. In this paper, we propose an efficient hardware encryption technique with minimal complexity and overheads based on ferroelectric field-effect transistor (FeFET) active interconnects. The active interconnect provides run-time reconfigurable inverter-buffer logic by utilizing the threshold voltage programmability of the FeFETs. Our method utilizes only two FeFETs and an inverter to realize the masking function compared to recent reconfigurable logic gate designs using several FeFETs and complex differential logic. We fabricate the proposed circuit and demonstrate the functionality. Judicious placement of the proposed logic in the IC makes it acts as a hardware encryption key and enables encoding and decoding of the functional output without affecting the critical path timing delay. Also, we achieve comparable encryption probability with a limited number of encryption units. In addition, we show a peripheral programming scheme for reconfigurable logic by reusing the existing scan chain logic, hence obviating the need for specialized programming logic and circuitry for keybit distribution. Our analysis shows an average encryption probability of 97.43% with an increase of 2.24%/ 3.67% delay for the most critical path/ sum of 100 critical paths delay for ISCAS85 benchmarks.

Table of Contents

List of Figures

List of Tables

Acknowledgments

First and foremost, I would like to have my deepest appreciation for my advisor Dr. Vijay Narayanan. It is my privilege to work with him. He gave me a wonderful opportunity in research and always has valuable instructions not only for academics but also for life. I am also thanks to Dr. Sumitha George for providing guidance and all the late night meetings to resolve my questions, Dr. Kai Ni for providing instructions on device level, Yixin Xu for resolving strange SPICE simulation resultsand Akshay Ramanathan for his assistance and helpful discussions. Without them, I will not have such successful research.
Lastly, I am thankful for my girlfriend Sishi Cheng, as she takes care of my life and encourages me when I'm facing challenges.
This device and circuit level analysis is supported by the U.S. Department of Energy, Office of Science, Office of Basic Energy Sciences Energy Frontier Research Centers program under Award Number DESC0021118. The architecture evaluation is supported part by the NSF under grant number 2008365 and part by ND EPSCoR. The device fabrication is funded by the German Bundesministerium für Wirtschaft (BMWI) and by the State of Saxony in the frame of the "Important Project of Common European Interest (IPCEI)".

Chapter 1
Introduction

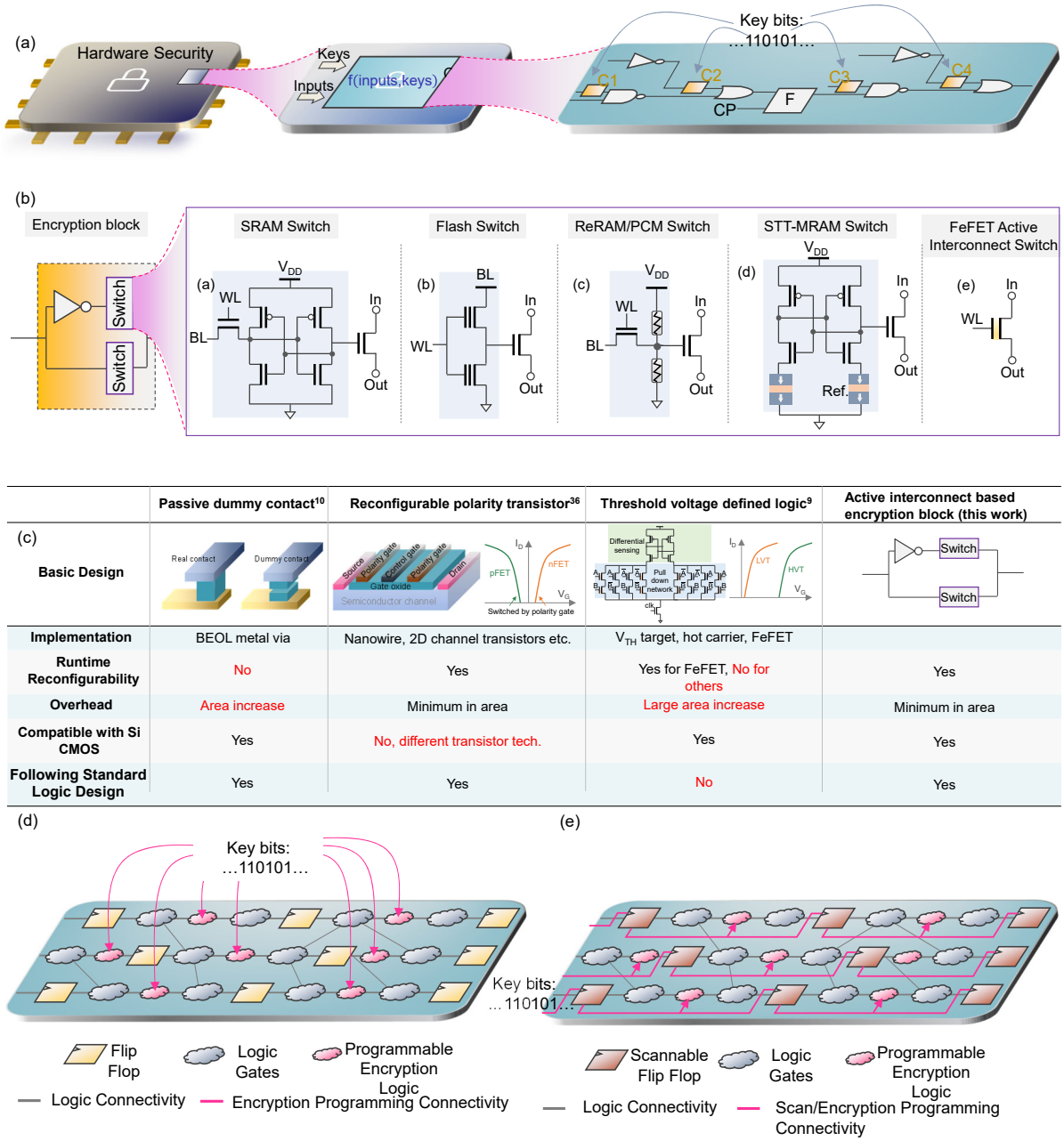
1.1 Background and Previous Work

Hardware security is becoming increasingly prominent with globalization and outsourcing integrated circuit (IC) fabrication to various foundries [4]. A major threat to hardware security is reverse engineering (RE). Objects ranging from large aircraft to the smallest microchips are vulnerable to RE [5]. Attackers' motives may include commercial piracy, intelligence, patent laws [6]. RE techniques can enable the attacker to inject a hardware Trojan, copy propriety IPs, extract hard-coded keys, and copy instruction sequences [7]. Such scenarios necessitate the need for hardware encryption in chips, which adds a level of difficulty to IC analysis [8] and reverse engineering. Reverse engineering extracts information from an integrated circuit utilizing techniques like depackaging, delayering, high resolution imaging and side-channel probing, etc [6]. For example, attackers often depackage the target chip, take high definition image of each layer, and then use an image recognition software to extract netlists [7]. Different layout shapes of different logic cells make this process easy for the attackers to gather logic information. To mitigate such risks, an effective technique is to add camouflaged cells in the design such that discerning logic process through reverse engineering is difficult or impossible. Camouflaged cells prevent the interpretation of correct functionality by being logically obscured.

Various gate-level camouflaging techniques have been developed with conventional CMOS devices [9–13]. Traditional CMOS-based camouflaging implementations incur overheads in circuit area, power, and delay. Recent explorations have investigated emerging devices such as spin-transfer-torque devices [14], tunnel-FETs [15], ferroelectric devices [16, 17], tungsten diselenide (WSe_2) devices [18], etc., for provisioning hardware security by leveraging unique properties such as their non-volatile behavior. Rajendran et al. [19] proposed a gate camouflaging technique by inserting dummy via/contacts in

the layout and creating look-alike layouts for NAND, NOR, and XNOR cells (Fig. 1.1(c)). With layout look-alike camouflaged gates, the attackers may interpret the function incorrectly and end up with a faulty netlist. However, advances in imaging and computer vision technology have made such methods less effective and susceptible to direct probing attacks [9]. One approach to avoid probing attacks is to use internal parameters of devices, such as product invariability or different states of the devices, for the implementation of different functions while retaining identical physical layouts [3, 9]. Wu et al. [17] proposed that two-dimensional black phosphorus field-effect transistors with reconfigurable polarities are suitable for hardware security applications (Fig. 1.1(c)). These transistors can be dynamically switched between p-FET and n-FET operations through electrostatic gating. Though this approach achieves minimum area overhead, its integration with Si CMOS technology is challenging.

Erbagci et al. [9] proposed a gate camouflaging technique using threshold voltage defined (TVD) logic topology. The key idea relies on the usage of different threshold voltage (V_{TH}) transistors but with identical physical layouts. Their work introduced a generic 2-input TVD logic gate capable of realizing multiple logic functions (NAND, NOR, and XNOR). They achieved this by setting pull-down transistors with different V_{TH} implantations (i.e. low-V_{TH} (LVT), and high-V_{TH} (HVT)). However, this circuit does not provide flexible reconfigurability as the V_{TH} of conventional CMOS transistors are not run-time programmable. Dutta et al. [3] further enhanced the TVD device design (Fig. 1.1(c)) by replacing the pull-down logic transistors with emerging ferroelectric FETs (FeFETs). By utilizing the feature of voltage-dependent polarization switching of FeFET, pull down transistors can be reprogrammed into LVT and HVT states. Exploiting the programmable V_{TH} of the FeFETs makes the TVD logic gate-level camouflaging and run-time reconfigurable simultaneously. However, these features come at the expense of complex design with differential logic, high area, power, timing expense.



	Passive dummy contact[10]	Reconfigurable polarity transistor[36]	Threshold voltage defined logic[9]	Active interconnect based encryption block (this work)
Implementation	BEOL metal via	Nanowire, 2D channel transistors etc.	V_{TH} target, hot carrier, FeFET	
Runtime Reconfigurability	No	Yes	Yes for FeFET, No for others	Yes
Overhead	Area increase	Minimum in area	Large area increase	Minimum in area
Compatible with Si CMOS	Yes	No, different transistor tech.	Yes	Yes
Following Standard Logic Design	Yes	Yes	No	Yes

Figure 1.1: Overview of the proposed encryption of IC logic design harnessing the ultra-compact FeFET active interconnect reconfigurable switch. (a)Illustration of utilizing the active interconnect based encryption block for obfuscating the IC logic. The keys are to dynamically reconfigure the interconnect such that the logic function is hidden. (b)The encryption block and implementations of switches using various technologies to realize camouflaging logic function. FeFET realizes a reconfigurable ultra-compact active interconnect switch. (c)Comparison between different camouflage logic designs. The proposed active interconnect based approach is advantageous in realizing the camouflage logic. (d)Distribution challenge of key bits to the programmable encryption logic block. (e)Distribution of key bits to the programmable encryption logic block via scan chain.

1.2 This Work

This thesis provides RTL analysis and SPICE simulation for a broader research project published on Nature Communication that proposes a simple area efficient reconfigurable logic which can act as encryption key logic. To avoid IC counterfeiting, the functional IP is locked with key logic and the IP can be unlocked with a correct sequence of keys given to the trusted customer. Therefore protection can be achieved by intentionally programming the device with incorrect keys. Our proposed scheme for securing the ICs by hardware encryption is shown in Fig. 1.1(a). In this scheme, an active interconnect based encryption block is designed and is chosen to judiciously place them at different locations in the chip. Keybits are used to program encryption logic. An example arrangement of encryption blocks C1,C2,C3 & C4 in an IC is shown in Fig. 1.1(a). In this scheme, not all gates need to be camouflaged. Rajendran et al. [19] has shown that choosing a subset of gates to be camouflaged is sufficient to make the IC immune to reverse engineering. One advantage with this simple yet but powerful technique is that, the placement of key logic can be in the non-critical timing branch of the logic, yet the output function will be encrypted. Further analysis shows that the strategic placement of the key circuit influences the output without posing challenges in the timing closure. In this way, the proposed scheme causes only minimal interference to the actual circuit in terms of delay, area and power.

It is crucial to develop an encryption logic with efficient functional implementation, resistance to hardware attacks, CMOS compatibility, high density and minimal overheads. The ability to program the encryption block multiple times during run-time is significant for enhanced security. To satisfy aforementioned requirements, a compact encryption block is designed as shown in Fig. 1.1(b). Here the block needs to be developed in such a way that the output signal gets inverted or non-inverted based on the internal state of the switch. The switch can be either in closed or in open state. Note that complementary states are maintained in the upper and lower branches. If the switch in the upper branch is in a conducting (closed) state then inverted input appears in the output and if the switch in the lower branch is in a conducting (closed) state then the output follows input. Thus with reconfigurability, the proposed encryption block can act as either an inverter or buffer. The vision is to integrate the reconfigurability to switch's internal state such that physical layout looks identical in both modes of operation. Hence the block can act

as a camouflaging buffer-inverter standalone gate. In addition, the usage of this block in conjunction with other complex gates by placing it at their input or output, the overall functionality changes, extending the camouflage to complex circuits.

There are many promising memory technologies available to realize the switch in the reconfigurable encryption block, each with its own unique features. Fig. 1.1(b) shows the potential implementations of the switch using SRAM, Flash, resistive RAM (ReRAM), phase change memory (PCM), spin transfer torque magnetic RAM (STT-MRAM), and ferroelectric field-effect transistors (FeFETs). SRAM is the most straightforward memory to use but is volatile and typically requires at least six transistors, dissipating significant leakage power while suffering from low memory density.A Flash memory-based switch is nonvolatile and compact [20], but memory programming is slow ($\sim$ms) and requires a high programming voltage ($\sim$10 volts). In addition, it is challenging to scale the embedded flash memory to 28 nm and below due to the thick gate stack and also added costs from the additional masks with scaling [21]. Therefore, for embedded flash memory to use as a compact nonvolatile switch, significant challenges remain. Emerging nonvolatile memory (NVM)-based switches have also been proposed and superior performance has been demonstrated [22–24]. Resistive memories are a class of two terminal NVM devices, including ReRAM, PCM, and STT-MRAM. Information is stored as conductive filament formation or rupture (ReRAM), film crystallization or amorphization (PCM), or parallel or anti-parallel orientation of the magnetization in a magnetic tunnel junction (STT-MRAM). These devices are nonvolatile and compact, but usually require a large conduction current to program the devices, consuming a significant write power. The limited on/off resistance ratio ($\sim$100 for ReRAM/PCM and $\sim$5 for STT-MRAM) usually requires additional circuitry, such as the 1T2R structure in ReRAM/PCM [22, 24] and an even more complex supporting structure for STT-MRAM [23] to realize a nonvolatile switch.

In this thesis, a nonvolatile active interconnect switch, based on a single FeFET is proposed to build the reconfigurable encryption block. In a FeFET, the ferroelectric layer is integrated as the gate dielectric of a MOSFET, where the information is stored in the direction of the ferroelectric polarization, which can be switched with an applied electric field. By configuring the direction of the polarization to point towards the semiconductor channel or the gate electrode, the device is set to either low-V_{TH} or high-V_{TH} state respectively. This makes FeFET an integrated single transistor memory, a great advantage to realize the nonvolatile switch. The dynamic reconfigurability of V_{TH} state has been harnessed in many applications, for instance, on memory-centric

computing [3,25–30]. Since the ferroelectric memory is written with an electric field rather than a large conduction current [28], this technology becomes highly energy efficient (e.g., down to ∼1 fJ/bit write energy). Therefore the dynamic reconfigurability of V_{TH}, along with its intrinsic three-terminal structure, nonvolatility, superior write performance, excellent CMOS compatibility, and scalability [31,32], shape FeFET a prime candidate for the nonvolatile switch. Demonstrations of FeFET on advanced transistor technologies, such as the 22 nm fully-depleted silicon-on-insulator (FDSOI) [33], FinFET [34] and gate-all-around transistor [35,36], have been reported, demonstrating the great promise of scaling for FeFET. The three terminal device structure makes the FeFET a very compact active interconnect. The key idea behind our proposed active interconnect based reconfigurable encoding circuit leverages the run time reconfigurability of the encryption block by manipulating the threshold voltage of FeFET [1,37–39].

Note that design variants of our proposed active interconnect based dynamically configurable block can be extended to offer various chip design applications. For example, an active configurable route switching can be enabled, as shown in Fig. 5.1, to route a signal to different functional units. The directions can be tuned with programming configuration. Another example is a configurable path connector that connects/disconnects inputs to destination units. This is especially beneficial for controlling the logic towards redundant functional units. Redundant functional units are typically used in chips as means to increase the reliability against fault tolerance. Reconfigurable logic gate is another byproduct of the proposed method which is realizable by programming the control inputs gates. Many combinations such as inverter, NAND, AND, OR, NOR, XOR and XNOR are possible (Fig. 5.1). In addition, recongfigurable gates can be deployed in chips to tackle Engineering Change Orders (ECO) [40,41], where functional logic changes need to be met with minimal layout changes. The ability to meet functional changes with existing gates in the design is relevant for both pre-mask and post-mask ECOs.

All dynamic logic programming schemes including the aforementioned dynamic encryption programming pose a challenge in getting the desired input values to the configurable logic which mostly requires appropriate write voltages to set its internal state. This necessitates a robust peripheral logic and circuitry. However, a systematic approach for peripheral programming has rarely been explored in recent reconfigurable logic research works. Nowadays application specific integrated circuit(ASIC)/system on a chip (SoC) implementations come with more than a million gates and flipflops spread across the entire chip. As the amount of logic increases, the number of encryption gates is also expected to increase proportionally. In such cases, it is not trivial to program umpteen

configurable gates. Fig. 1.1(d) shows an example distribution of logical blocks that need to be programmed in a dynamically configurable security circuit. Explicit addition of auxiliary logic and peripheral circuitry is required to support dynamic programming of the configurable logic in this case. The amount of additional logic required and the resultant overhead, increase with the amount of programmability incorporated in the chip, which does not favor turning all gates reconfigurable.

In summary, this thesis proposes a fundamentally different design scheme for logic obfuscation by having a reconfigurable active interconnect, rather than adopting poor performance polymorphic logic gates in conventional approaches, with no interference to the conventional CMOS gates. Thanks to its intrinsic transistor structure and nonvolatility, FeFET can be applied as an active interconnect. Building on this concept, the key contributions are as follow: An encryption circuit with FeFET active interconnects for functional obfuscation is proposed and experimentally demonstrated; The proposed scheme places our compact encryption logic on non-critical timing branches of the logic path, which achieves the functional obfuscation without escalating the time closure challenges; Area and energy efficient design with only 4 transistors (Previous FeFET based circuit design from Dutta et al. [3] consists a total of 28 transistors); The proposed design with active interconnects encryption blocks is highly scalable where increased encryption can be achieved by inserting more encryption blocks on the non-critical timing branches.

The rest of the article is organized as follows. Experimental verification of our proposed reconfigurable encryption block is discussed first. Details on SPICE simulation for functional verification of the circuit is followed. Our placement strategy and analysis of encryption probability on ISCAS benchmarks are discussed in subsequent sections. The results and conclusions are discussed in the final section. In addition, a supplementary section with additional details on device fabrication, circuit simulation, variation analysis, and, block layout and analysis is also included.

Chapter 2
Verification of the Reconfigurable Block

To verify the functionality of the proposed reconfigurable block, measurements and circuit simulations are performed. For experimental demonstration, 28nm high-κ metal gate FeFET devices are tested, as shown in the transmission electron microscopy (TEM) cross-section images of the device Fig. 2.1(a) [1, 2]. The device features a doped HfO_2 as the ferroelectric layer and SiO_2 as the interlayer in the gate stack, as shown in Fig. 2.1(b). Detailed device information can be found in [1, 28]. The FeFET memory performance is characterized by standard I_D-V_G measurements after applying $\pm$4 V, 1μs write pulses on the gate. Note that a 0.1 s delay is inserted between the I_D-V_G sweep and the memory write pulses for the trapped charges to release [29, 42, 43]. It is known that the charge trapping induced by write pulses counteracts the V_{TH} shift caused by the polarization switching , thus reducing the memory window and degrading the endurance cycling of FeFET [29, 42, 43]. Inserting a delay after memory write leaves enough time for the trapped carriers to release, thus manifesting the polarization effects. Fig. 2.1(c) shows a memory window about 1.2 V, i.e., the V_{TH} separation between the LVT and HVT states, which enables a large ON/OFF conductance ratio. Note that, for the nucleation-limited polarization switching [44, 45], a tradeoff can be realized between the write pulse amplitude and pulse width, as shown in Fig. 2.1(d), which presents the switching dynamics of FeFET as a function of applied pulse width for different pulse amplitudes. It clearly suggests that 4 V is not absolutely necessary and lower write voltages possible with a tradeoff of a large pulse width. This could help alleviate the design of peripheral supporting circuitry with lower write voltages in applications where the FeFET configuration is occasional and high speed write operation is not necessary, as the proposed logic camouflaging application in this work.

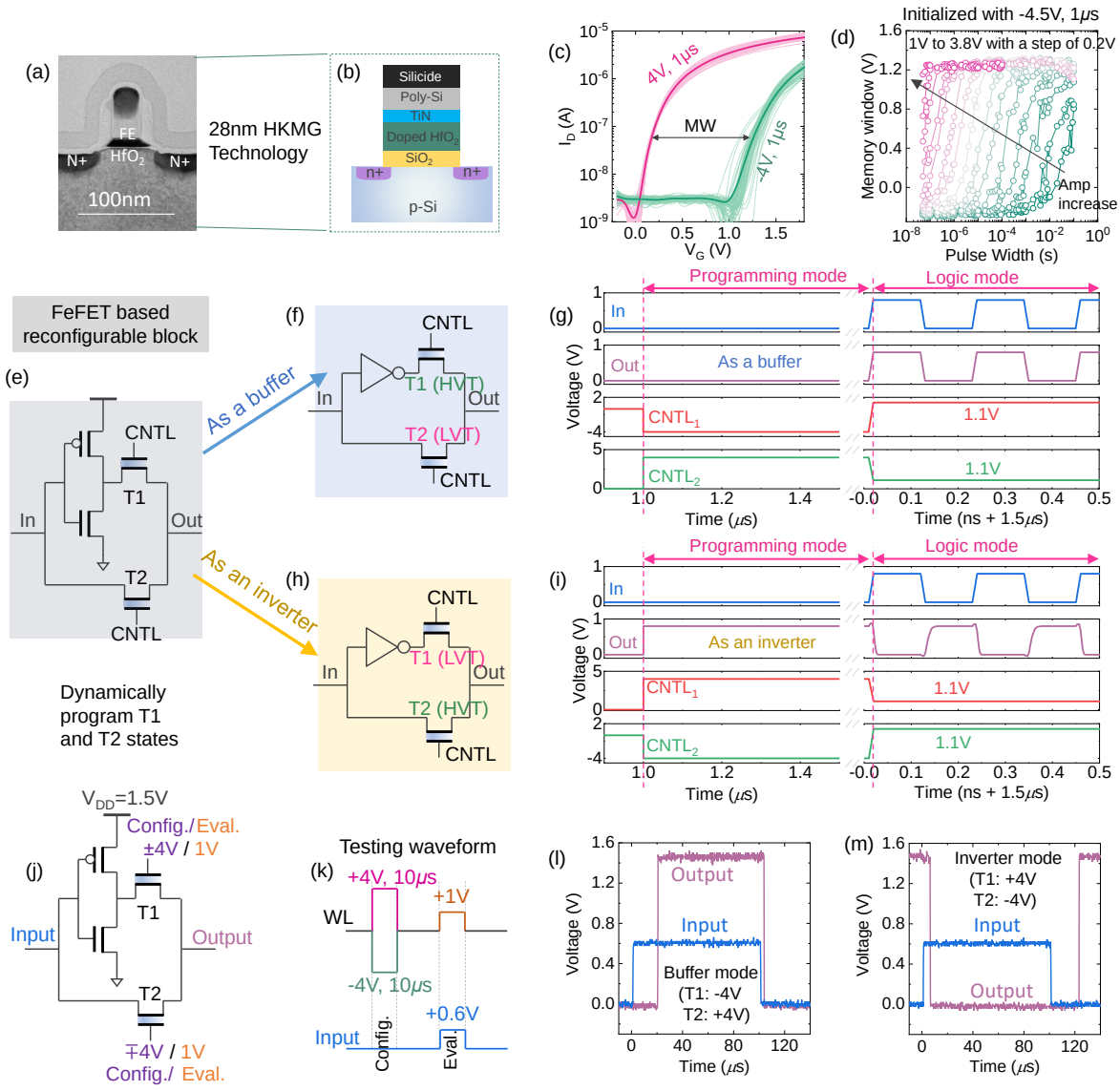


Figure 2.1: FeFET reconfigurable encryption block and its functionality verification. (a) TEM cross section [1, 2] and (b) schematic cross section of an 28nm high-κ metal gate FeFET device. (c) I_D-V_G characteristics of 60 different FeFETs measured after $\pm$4 V, 1 μs write pulses. Good control over the device variability and a memory window of 1.2 V are demonstrated. (d) The dynamic switching characteristics of the FeFET as a function of write pulse width at different pulse amplitudes. Tradeoff between amplitudes and pulse widths are present. (e) Schematic of the proposed active interconnect based reconfigurable encryption block. (f) Buffer mode configuration and (g) Simulated waveforms in buffer mode showing the programming and logic modes (h) Inverter mode configuration (i) Simulated waveforms in inverter mode. (j) Applied voltages on the encryption block in experiment. (k) The applied waveform for functionaltiy verification in experiment. Captured transient waveforms in the logic evaluation mode for (l) buffer and (m) inverter modes. For all tested FeFETs, W/L=500 nm/500 nm are used.

As mentioned above, the large memory window and ON/OFF conductance ratio present a unique opportunity for FeFETs to design an active interconnect based camouflaging pass transistor (switch). In addition, the capability to dynamically shift the V_{TH} makes the proposed active interconnect based FeFET-switch immune for the attacker to reverse engineer the netlist simply from layout (GDS) level. Fig. 2.1(e) shows the proposed encryption block utilizing V_{TH} manipulation. The proposed encryption block consists of an inverter and two FeFETs. It operates in two modes, the programming mode, and the logic mode. In programming mode, relatively high write voltages are used to program the device to set the V_{TH}. Once it is programmed, the device is all set to operate in the logic mode, where a small read voltage at the gate between the V_{TH} of LVT and HVT states is applied to read the FeFET state. The pass transistor either conducts or blocks the input signal based on the internal programmed V_{TH} state, as shown in Fig. 2.1(f) and (h), respectively. Hence an inverted input or a non inverted input is obtained at the output of our proposed reconfigurable circuit.

The functionality of the proposed reconfigurable buffer-inverter encryption block has been verified in SPICE simulations, using a calibrated FeFET model [2] and 45 nm (NCSU FreePDK) logic transistor technology [46]. In the program mode, V_{TH} of the two FeFETs pass transistors are set by applying write pulses. For this study, write pulses of ± 4 V, 500 ns are adopted. In the logic mode, an INPUT signal of 0.8 V at the *In* terminal and control signal of 1.1 V(read voltage chosen between the V_{TH} of LVT and HVT states) at the gates of FeFETs (*CNTL1* and *CNTL2*) is asserted. In the buffer mode of encryption, as illustrated in Fig. 2.1(f), FeFETs T1/T2 are written into HVT/LVT state respectively by asserting write voltages in CNTL1 and CNTL2 terminals, as shown in the transient waveform in Fig. 2.1(g). In the logic (evaluation) mode, it can be seen that the output(*Out*) follows the input (*In*) as shown in Fig. 2.1(g). On the other hand, by writing the FeFETs T1/T2 into LVT/HVT state, the inverter mode of encryption shown in Fig. 2.1(h) can be realized, which will output an inverted input signal during the logic evaluation mode, as shown in Fig. 2.1(i).

The reconfigurability of the inverter-buffer block has also been verified experimentally using the testing setup shown in Fig. 2.1(j) and (k). Discrete inverter and FeFETs are assembled together for experimental verification. The relevant applied voltages are shown in Fig. 2.1(j) and (k). The buffer mode and inverter mode operations are shown in Fig. 2.1(l) and (m), respectively. Here only the evaluation phase waveforms are shown for clarity. Correct operations of both working modes are demonstrated. Due to the

large parasitics present in the testing setup, the speed is limited to tens of μs. But it is expected that with the fully integrated circuit, high speed operations can be achieved as demonstrated in the SPICE simulations in Fig. 2.1(g) and (i). SPICE analysis on threshold voltage and delay variation of the proposed encryption block is given in Fig. B.2. A layout of the same is shown in Fig. C.1.

To prevent reverse engineering, any camouflaging technique needs to meet two conditions [19] such as resiliency to reverse engineering and corrupted outputs. Resiliency to reverse engineering implies that an attacker will not be able to discern the functionality of the camouflaged gates. Corrupted output indicates outputs of the original netlist and deceived netlist are different. In our proposed technique, both these conditions are met. Experimental results with Fig. 2.1(j) show that the same circuit is capable of producing both the inverted and non inverted output. Note, we apply same input voltages (both Input and Eval terminals in Fig. 2.1(j)) and the circuit gives two different outputs depending on the previously programmed (configured to either HVT or to LVT) state. This ensures that, the attacker will not be able to identify the functionality of the gate just by inspecting the physical layout. Also, the programming (configuring to LVT/HVT) of FeFETs is also done by just by applying voltages at the Config/Eval (in Fig. 2.1(j)) dynamically. The extracted netlist by the attacker will yield a different outcome, without the correct knowledge of the programmed state (buffer/inverter state) of our proposed encryption gate. Moreover, in the proposed technique, it is easy to add as many number of encryption unit (thanks to compact implementation and the easy peripheral logic) throughout the IC. This increases the functional ambiguity in the overall logic, and there by making the overall IC more immune for reverse engineering. In summary, the proposed encryption circuit with the same input results in two different logical outputs based on the programmed states of FeFETs, making it a strong candidate for reverse engineering resilient hardware (Fig. 2.1(g),(i)).

There may be several concerns related with the constant bias applied on the FeFET gates for the logic evaluation mode. First, the constant bias (+1 V in the experiment in this work) may incur significant gate leakage current, which increases the power consumption. However, this is not necessarily true for FeFETs. This is because for FeFETs, typically the ferroelectric layer thickness is rather high for a decent memory window (8 nm doped HfO_2 in this work), which significantly suppresses the leakage current even at 1 V, as shown in the measured gate leakage current in Fig. A.1. Second concern could be stability of the FeFET states, especially under the constant bias stress for evaluation. For properly designed gate stack of HfO_2 FeFET, the extrapolated retention

could reach 10 years at 85°C [47, 48]. We have also measured the retention of our FeFETs at different temperatures. Though it is not the best retention performance reported so far on Si FeFET, it still demonstrates window opening at 85°C when extrapolated to 10 years, as shown in Fig. A.2(a). We also measured the stability of the HVT state while stressed at the evaluation gate bias (+1 V) during retention. As shown in Fig. A.2(b), the state is stable even at high temperature. At the end, what really determines the stability of FeFET states is the energy barrier separating the two polarization states, which can be engineered through the gate stack engineering [45]. In the last, the evaluation bias can be shifted to a lower bias value if needed through various engineering techniques, such as the channel doping or the gate work function shift [3]. Therefore, FeFET can be an excellent candidate for the proposed active interconnect based logic obfuscation application. In the next section, the encryption probability and timing beneficial placement are discussed.

Chapter 3
Encryption and Critically of Placement

For the proposed active interconnect based encryption blocks to function and enable resistance for reverse engineering, a judicious placement of the blocks enabling the encryption engine in a timing aware fashion is required. The location of the placement, the neighboring cells and input pattern have an impact on encryption. All these factors can contribute to logic masking effect and prevent the encrypted bit propagation to the output. In order to understand the impact of an encrypted bit and how it propagates, a circuit having a single encryption bit cell is analysed first. Fig. 3.1(a) shows an example of an encrypted circuit. C1 is the proposed buffer-inverter encryption block. Suppose I_1, I_2, I_3, I_4 to be 0, 0, 0, 1. With C1 programmed in buffer mode, the output will be a "0". However C1 in inversion mode will alter the output to be a "1". Note, if the input I_2 changes to bit "1" as shown in Fig. 3.1(b), the inverted bit from C1 will not make an impact on the output, as OR gate with input 1 masks the other input. To improve the encryption strength, additional encryption key circuit can be inserted as shown in Fig. 3.1(c). Note, 100 % inversion in the output all the time is also not reliable for security purposes as the attacker can simply resort to the negation of the output.

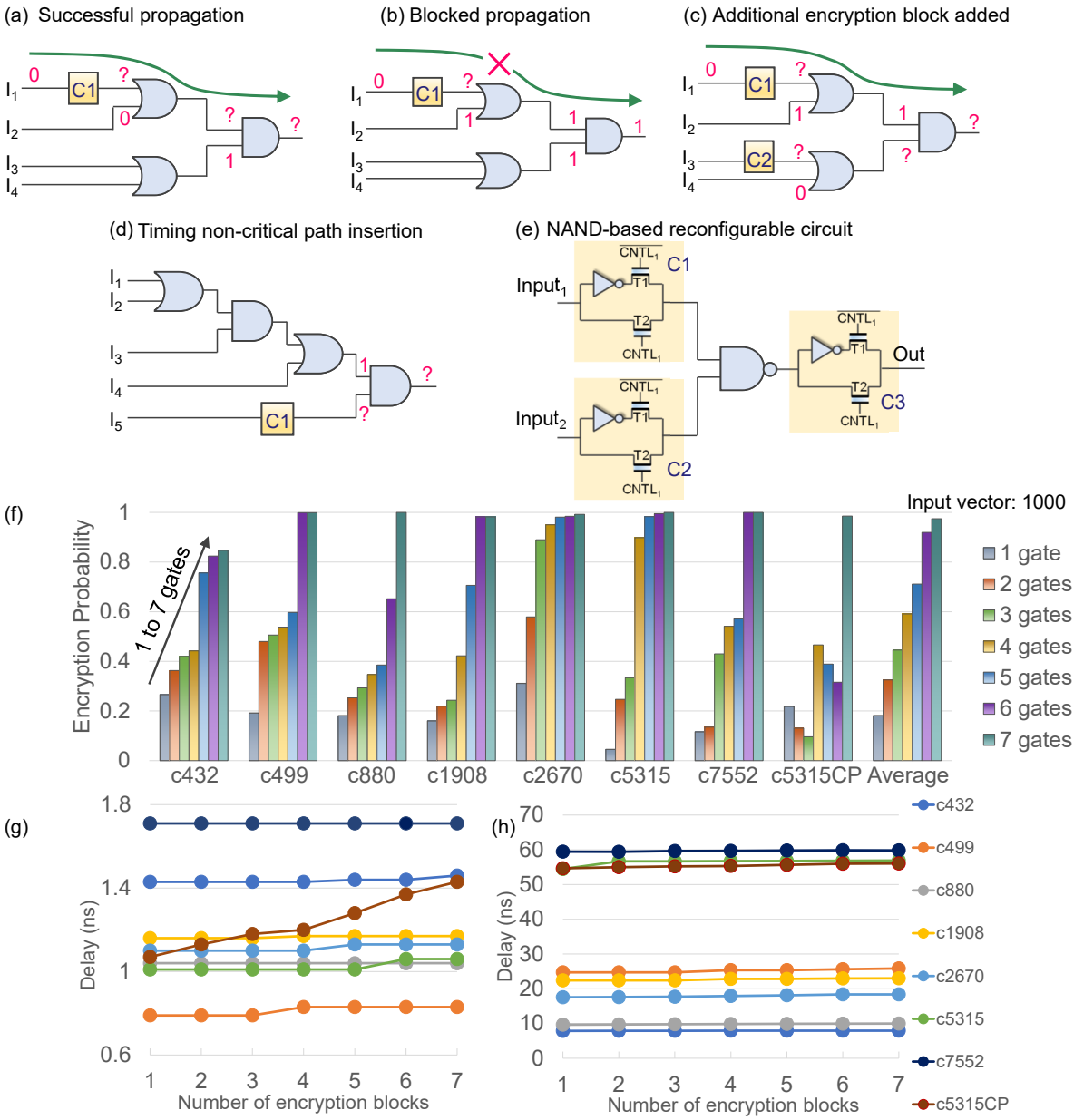


Figure 3.1: Analysis of placement ultra-compact FeFET encryption logic on encryption probability, timing and logic reconfigurability. (a) Successful propagation of an encrypted bit from C1. (b) Encrypted bit from C1 blocked by OR gate. (c) Enhancing encryption probability by inserting additional encryptor. (d) Placement of interconnect based encryption unit in a noncritical timing path. (e) Reconfigurable logic based on NAND and active interconnect based encryption logic. (f) Encryption probability with increasing number of encryption blocks on ISCAS85 benchmarks (number of input test vectors: 1000). (g) Critical path delay with increasing number of encryption elements. (h) Sum of top100 critical path delays on ISCAS circuits.

Timing closure is one of the most critical challenges in ASIC/SoC designs with ever increasing clock rates [49–51]. In this work, the aim is to incorporate encryption in

the IC with minimal impacts on timing critical paths. Critical paths are the longest delay paths that limit clocking. Changing the standard logic gate design to adaptable camouflaging gate design [52] for security purposes increases the critical path delay. In the proposed method, encryption gates are inserted in a non critical timing path to overcome the potential timing failure. For example, in Fig. 3.1(d), the path from input I_5 to output is the least timing critical path, as it has the minimal number of gates from the input to output. In this case, C1 is inserted in the logical branch from I_5 to the output. Though C1 is not in the timing critical path, it still logically affects output as evident from Fig. 3.1(d).

In this study, ISCAS85 benchmarks [53] are simulated to analyze the encryption probability. Synopsis Design Compiler is used for logic synthesis. PRIMETIME [54] is used for timing analysis. The simulations are based on the NCSU FreePDK 45 nm logic technology [55] and a calibrated Verilog-A model of FeFET. Delay simulation of the encryption circuits is done with SPECTRE. Functional correctness is verified with test vectors using Vivado Simulator [56]. Random test vectors are generated for benchmarking. In this analysis, a non-critical path is chosen as a candidate for placement and the encryption circuit is placed randomly in the chosen path. Then test input pattern is applied to the modified circuit with encryption blocks. If the output generates an incorrect result, then output is considered to be encrypted for this input pattern. In this work, the encryption probability is defined as the fraction of times we get the incorrect output out of the total number of attempted tests.

Fig. 3.1(f) shows the number of encryption element versus encryption probability for ISCAS benchmarks(c432, c499, c880, c1908, c2670, c5315 and c7552). C5315CP is the same benchmark as C5315, but with encryption blocks placed in a critical timing path and is used to show the difference in impacts compared to the proposed method. The analysis shows 84.7% to 100% encryption probability with an average 97.43% with a total of 7 encryption blocks in the circuit. In general, the trend shows that the encryption probability increases initially with the increase in the number of encryption circuits. However, c5315CP does not show a monotonic increase in encryption probability with increase in the number of encryption blocks. For c5315CP, as mentioned earlier, encryption gates are added in the same input to the output path. This leads to double inversions in some cases and decreases the encryption probability. Here, double inversion is defined as the two time negation of data in the input-output path and a detailed example is given in Fig.4.2 and Fig.4.3. Also, it is observed from Fig. 3.1(f) that a comparable level of encryption probability can be achieved with a smaller number of

encryption blocks for many benchmarks. For example, in C499 increasing the number of encryption blocks from 6 to 7 does not change encryption probability and it maintains at 99.9%. Similarly, also in C1908, increasing the number of encryption blocks from 6 to 7 does not increase the encryption probability from 98.2%. In C2670, increasing the number of encryption blocks from 5 to 6 increases the encryption probability only by 0.3% from 98.1% to 98.4%.

Fig. 3.1(g) shows the critical timing path delay versus the added number of encryption circuits. The placement of 7 encryption blocks gives an average encryption probability of 97.43% with the increase in most critical path delay by 2.24% on average. It is observed that for most benchmarks adding encryption logic does not change the delay of the most critical path as gates are placed in different non-critical paths. For example, adding a single encryption gate does not affect the critical path delay, and adding 6 gates changes the critical path delay by only 2.04%. Note that for c5315CP, the average delay on the most critical path gets worsened by 41.58% after the insertion of 7 gates. Further, sum of delays on the top 100 critical paths is taken for each of the benchmarks to analyze the overall delay impact in the IC after the placement of our encryption blocks. Insertion of multiple encryption units on the same path can make a previously non-critical timing logic path to a critical timing path. Such occurrences are restricted by spreading out placement of encryption blocks on different logic branches. Fig. 3.1(h) shows the sum of top 100 delays on ISCAS benchmarks. The impact of insertions is seen to be minimal. The placement of 5 encryption blocks gives an average encryption probability of 71.13% with an overall delay increase by 1.34%. The placement of 7 encryption blocks gives an average encryption probability of 97.43% with an overall delay increase by 2.24%.

Correlation of encryption probability with the placement of encryption logic is not linear. In the analysis, it is observed that encryption probability is at the highest if the encryption circuit is placed closer to the output node and becomes unpredictable as we move away from the output node due to logical masking. The analysis of the placement of the encryption logic in the same input-output path by varying the distance from output node is shown in supplementary materials Fig. 4.1. The analysis on ISCAS85 benchmarks demonstrates the ability to control output encryption probability without affecting the timing closure. It also shows, addition of a large number of encryption units is not necessary to get a satisfactory encryption level, which is beneficial for overall area and power savings. Typically,the placement of generic programmable gates [57] worsen the timing closure challenges, where as the proposed techniques alleviate it by restricting the placements to non critical timing paths. Another advantage with our methodology is

that instantiation of the interconnect based encryption gate from a standard cell logic library is possible on a need basis, making it easier for automation and eliminating the need for a specialized custom design of cells.

The encryption analysis shows that random placement of encryption block in the logic circuit results in different functional outputs. This concept can be extended to construct reconfigurable logic gates by systematically placing the encryption logic around standard gates. Reconfigurable logic is a known camouflaging method to obfuscate the IP. Here the attacker will not be able to discern the logic and extract the correct netlist by observing the layout. Standard cell is the building block in ICs for logic operations. The more functions it has with the same layout, the harder to be attacked. The proposed active interconnect based encryption gate can be used in conjunction with standard cells to make a very easy implementable reconfigurable logic. An example is shown with NAND gate in Fig. 3.1(e). Instantiating encryption logic in the inverter mode to the output of NAND gate makes the combination an "AND" gate. Adding encryption circuit to the inputs of NAND gates makes it further programmable. This makes the combination reconfigurable to NOR/OR. The internal programmed state of the instantiated interconnect based logic and potential logic gates centered around NAND gate are shown in the supplementary material Table. 5.1.

Chapter 4
Positional Effective Analysis

In this section, the impact of the position of placement of the proposed encryption block on encryption probability is analysed. Analysis begins by placing one encryption block at the output of critical path and measuring the encryption probability. Then the encryption block is moved to the input of the current gate and the corresponding encryption probability is recorded. This placement process is repeated till the primary input of the critical path is reached. The experiment results with ISCAS85 benchmarks are shown in Fig. 4.1. The different levels denote the gate distance from the output. C432 and C499 are small circuits with lesser than 20 levels from the output.

Fig. 4.1 indicates that for most of the benchmark circuits, encryption probability is at the highest when at level 1. This is where the encryption circuit is placed closest to the output. Then as the encryption element moves away to the center of critical path, encryption probability decreases. This is attributed to the increased potential for logic masking effect with the increase in distance from the output. Also it is observed that, encryption probability further gets increased with further movement towards the input.As the placement moves closer to input, there is an increased potential for higher fanout and more logic branches getting influenced by the encryption logic and hence the potential for altering multiple outputs. In benchmark C5315, encryption probability decreases with level 1, level2, level3 etc. A similar behaviour is observed with C432 as well. C2670 and C1908 show increased encryption probability while moving encryption unit towards the input.

Note, for all encryption and timing analysis in this article, below motioned methodology is adopted. PRIMETIME [54] is used for timing analysis. SPECTRE simulation is used to model the delay of our encryption circuit. Verilog-A is used to capture FeFET behaviour. The simulations are based on NCSU FreePDK 45 nm technology [55]. Functional correctness is verified with Xilinx Vivado [56] on the circuits with encryption

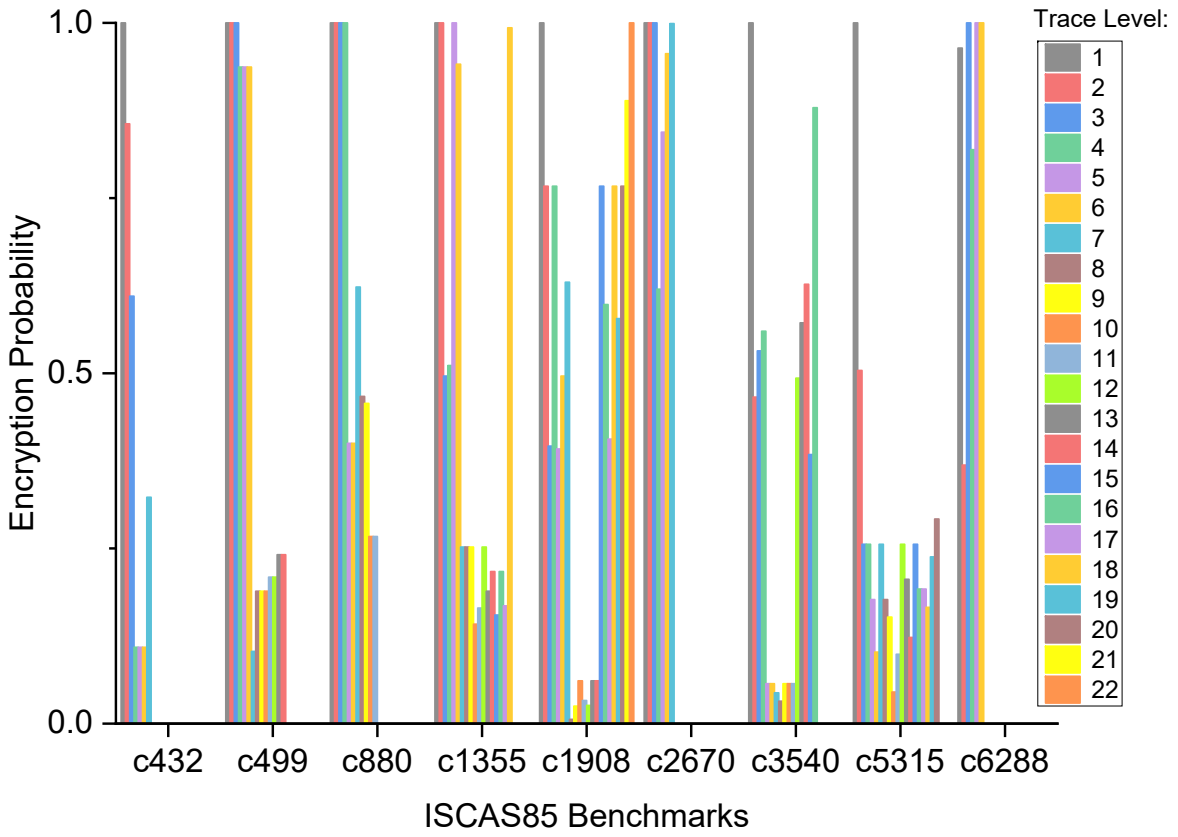


Figure 4.1: Impact on encryption probability when encryption unit is randomly placed at increasing logic distances from the output pin (number of input test vectors: 1000).

blocks for the generated test vectors.In addition these analyses incorporated a timing scaling factor to match the SPICE simulation delay with PRIME TIME library delay . The proposed circuit has used a best case scaling factor of 0.94 and a worst case scaling factor of 2.29 to match the PRIMETIME library delay values.

4.1 Double Inversion

In this section, a possibility of a double inversion of data is shown when adding more than one encryption block to the same input-output path. The experiment is conducted by adding multiple active interconnect based encryption blocks to an input-output path in C5315CP. This is done for analysing the impact of double inversion on timing and encryption probability in such paths. A double inversion is defined as two times negation of data in an input-output path. More than one encryption blocks programmed in the inverter mode in a path may lead to double inversion of data with some input data

combinations. To demonstrate the logic impact of a double inversion on a final output, a specific path having two encryption blocks from C5315CP is chosen. The screenshot of the timing report of the chosen input-output path is shown in Fig. 4.2. INVMOD in the timing report is the name of our encryption unit. Fig. 4.3a shows the schematic of a segment from the chosen path (Fig. 4.2) before the insertion of encryption units. Fig. 4.3b shows the same segment of the circuit after inserting one encryption unit in the inverter mode. Fig. 4.3c shows the circuit segment after inserting two encryption units (both programmed in the inverter mode). It can be observed that for a set of specific inputs, the intermediate output O_{inter} is "1" as shown in Fig. 4.3a. After inserting a single encryption unit, O_{inter} value is switched to "0" as shown in Fig. 4.3b. After inserting two encryption units, O_{inter} value is switched back to "1" as shown in Fig. 4.3c (double inversion at O_{inter}). Fig. 4.3d shows that changes in intermediate output (O_{inter}) gets transmitted to the final output with certain input combinations. This implies that having more than one encryption units in the same path may leave the original output unchanged in certain conditions decreasing the encryption probability.

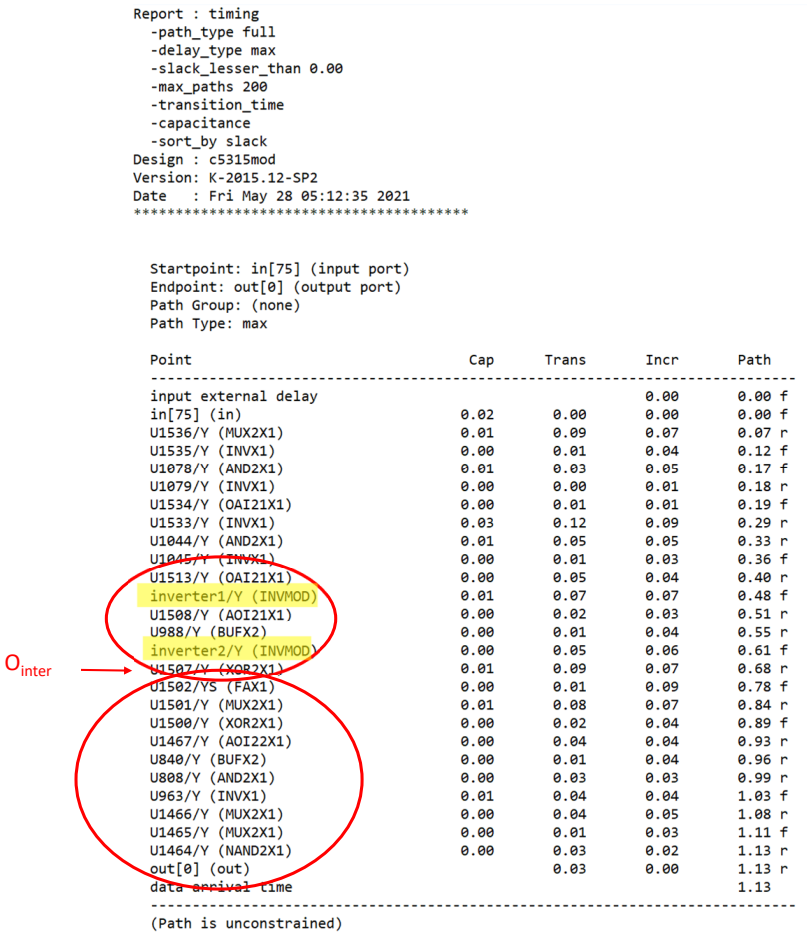


Figure 4.2: Timing report a path from C5315CP

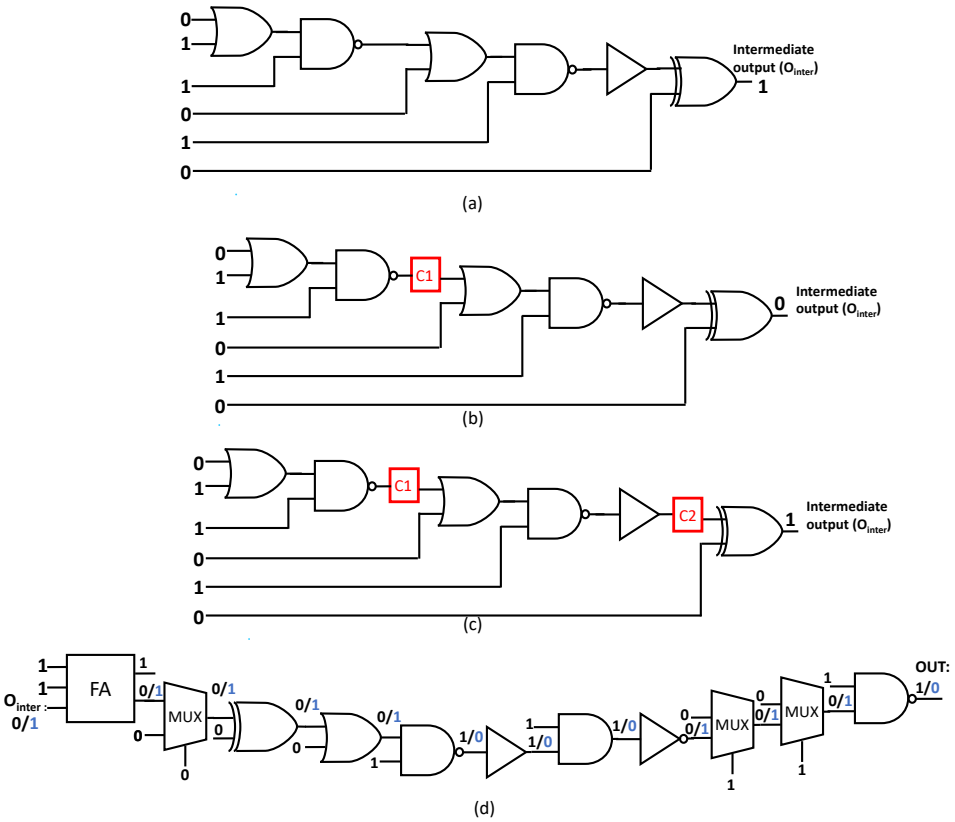


Figure 4.3: (a) A segment of input-output path. The segment output is named O_{inter}. O_{inter} is "1" with the current set of inputs. (b) Segment in (a) after adding one encryption logic(C1). C1 is programmed in the inverter mode which causes O_{inter} to be "0". (c) Segment in (a) after adding two encryption logic units(C1 & C2). Both C1 & C2 are programmed in the inverter mode which makes O_{inter} to be "1" again. (d) Rest of the schematic from the intermediate output to the selected path's final output. It is seen that changes in intermediate output O_{inter} (due to double inversion) affects the outcome of final output with the given input combinations.

Chapter 5
Other Important Applications of FeFET Active Interconnects

The variants of our ultra-compact FeFET active inter-connect design can be extended to apply in various chip design applications. Three potential applications that can be used in IC designs are listed in Fig. 5.1. An example is the design of a configurable path connector capable of connecting/disconnecting inputs to destination units. This is especially beneficial for controlling the logic signal flow towards redundant computation units. Inclusion of redundant functional units is a common method to develop reliable fault tolerant systems. In this application, active ferroelectric based pass transistors can be utilized as path connectors and such units can be used to control the path connectivity between different functional units with ease.

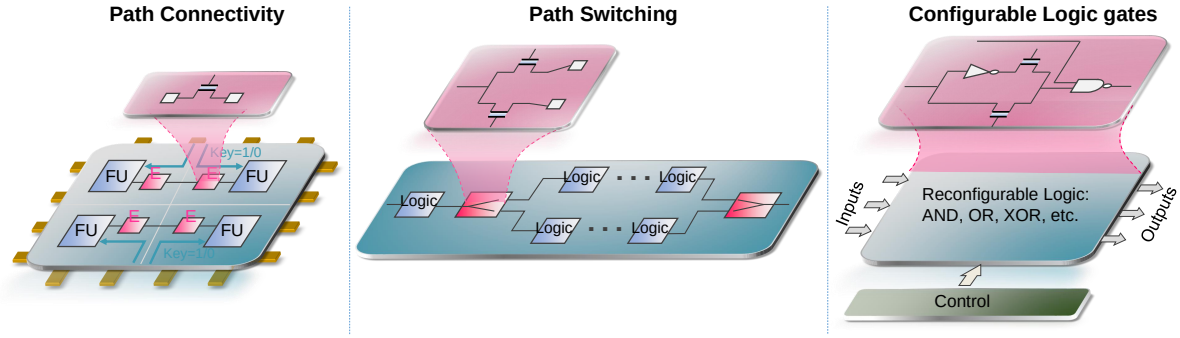


Figure 5.1: Other important applications that can benefit from ultra-compact FeFET active interconnect. It can be used as path connector, reconfigurable route switching, and reconfigurable logic.

Another potential application is configurable path switching which can essentially act as a router. Multiple active interconnect based pass transistors will be able route/block signals to different functional units as shown in Fig. 5.1. In addition, active interconnect

INPUT1	INPUT2	NAND (C1=BUF, C2=BUF,C3=BUF)	AND (C1=BUF, C2=BUF,C3=INV)	OR (C1=INV, C2=INV,C3=BUF)	NOR (C1=INV, C2=INV,C3=INV)
0	0	1	0	0	1
0	1	1	0	1	0
1	0	1	0	1	0
1	1	0	1	1	0

Table 5.1: Truth table of NAND based reconfigurable logic

blocks can also be used to construct reconfigurable logic gates by dynamically programming their control inputs. Many combinations such as such as NAND, AND, OR, NOR, XOR, XNOR etc are possible by the appropriate design (Fig. 5.1).

Chapter 6
Conclusion

In this work, ultra compact active interconnect based on ferroelectric FET for hardware encryption is presented. FeFET leverages threshold voltage manipulation to attain run-time configurablity. The proposed encryption circuit encompassing an inverter and an active interconnect, is layout obfuscated and is capable of producing either inverted or non-inverted output. This encryption circuit is fabricated and functionality is experimentally verified. Further analysis showed that the placement of active interconnect encryption blocks in non critical timing logic branches produces satisfactory level of encryption without jeopardizing the timing closure requirement of ICs. Analysis on ISCAS benchmark shows a 97.43% encryption probability with an average delay increase of 3.68% in the top 100 timing critical paths in ISCAS benchmarks. This work also introduced peripheral schemes for programming the reconfigurable encryption keys by reusing the scan circuity and thereby eliminating the dedicated dynamic key input distribution logic and circuitry.

Appendix A
Device Fabrication and Electrical Characterization

This part is done by Dr. Kai Ni from Rochester institute of Technology and provided here for completeness of this thesis.

A.1 Device Fabrication

In this paper, the fabricated ferroelectric field effect transistor (FeFET) features a poly-crystalline Si/TiN/doped HfO_2/SiO_2/p-Si gate stack. The devices were fabricated using a 28nm node gate-first high-κ metal gate CMOS process on 300 mm silicon wafers. Detailed information can be found in [1, 28]. The ferroelectric gate stack process module starts with growth of a thin SiO_2 based interfacial layer, followed by the deposition of the doped HfO_2 film. A TiN metal gate electrode was deposited using physical vapor deposition (PVD), on top of which the poly-Si gate electrode is deposited. The source and drain n+ regions were obtained by phosphorous ion implantation, which were then activated by a rapid thermal annealing (RTA) at approximately 1000 °C. This step also results in the formation of the ferroelectric orthorhombic phase within the doped HfO_2. For all the devices electrically characterized, they all have the same gate length and width dimensions of 1μm x 1μm, respectively.

A.2 Electrical Characterization

The FeFET device characterization was performed with a Keithley 4200-SCS semiconductor parameter analyser. Two 4225-PMUs (pulse measurement units) were utilized to make the pulsed current–voltage measurement. In the experiment, program and

erase pulses were applied and the pulsed I_D–V_G (I_D, drain current; V_G, gate voltage) measurement was performed. The total sweep duration is 5 ms. Note that, to minimize the charge trapping effects on the sensing of the programmed or erased state of the device, we inserted a delay of 100 ms between the measurement and the write pulses to allow a full trapped charge release. For the pulsed measurements, the current resolution is close to 3 nA in our set-up. The reconfigurable block characterization was performed using two FeFETs on the same chip and an externally connected inverter circuit (Texas Instruments CD74AC04E). We connected the reconfigurable block with an inverter on a breadboard. Input pulses, FeFET memory write pulses, and evaluation pulses were generated with an Keithley 4200-SCS. A 1.5V amplitude VDD supply of the inverter was provided through an Agilent 81150A arbitrary function generator. The output voltage transient was sampled through an Tektronix TDS 2012B digital oscilloscope. All the write pulses have a pulse width of 10 μs. The input pulses have a pulse width of 100 μs and the evaluation pulse with a rising edge 5 μs ahead of the input rising edge and a falling edge 5 μs lagging behind the input falling edge. The large pulse width is chosen due to the large parasitics in our set-up. In a fully integrated reconfigurable block, the operation speed will greatly improve, as shown in the single-FeFET measurement (successful write under 20 ns, $\pm$4 V) in Fig. 2.1(d).

A.2.1 FeFET DC IV Characteristics

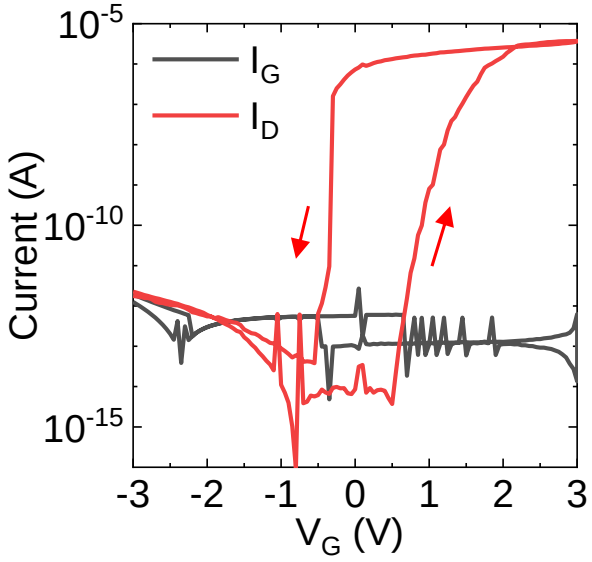


Figure A.1: DC Transfer characteristics of a FeFET. I_{D}-V_{G} curve shows a large memory window. The I_{G}-V_{G} shows a negligible gate current, which is below the noise floor of the instrument, due to a thick ferroelectric layer in the gate stack. This shows that applying a constant evaluation gate bias does not necessarily incur much additional power consumption. Due to its thick gate dielectric, FeFET may actually has a lower gate leakage than normal logic transistor.

A.2.2 FeFET State Stability

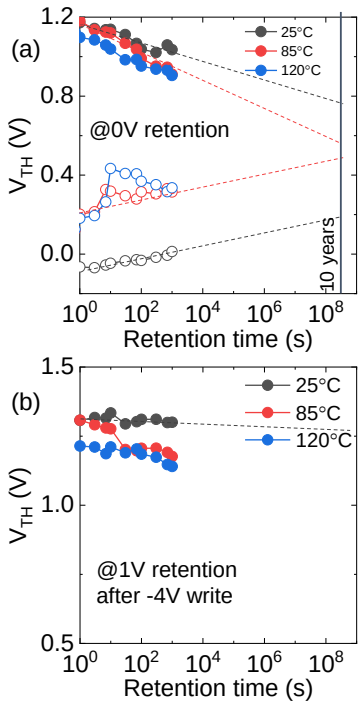


Figure A.2: FeFET state stability. (a) Retention characteristics of the LVT and HVT states of FeFET at different temperatures at 0 V retention voltage. (b) Stability of HVT state subjected to +1 V constant stress. Though not the best retention performance reported in FeFET, the device maintains 0.6 V memory window when extrapolated to 10 years at room temperature. In addition, because the evaluation gate bias is constantly applied to FeFET, which might cause concern over the stability of HVT state. Fig. A.2(b) clearly suggests that our device could be free from the disturb. Also note that evaluation bias can be shifted close to 0 V by V_{TH} engineering.

Appendix B
SPICE Simulation

This section is done in part with Yixin Xu.

B.1 Simulation And Waveform

Dynamic programming simulation of the proposed active inter-connect based encryption block is shown in Fig. B.1. Spectre is used simulation verification and the schematic of the encryption unit is given in Fig. 2.1(e). Table. B.1 shows simulation parameters. Simulations are carried out using NCSU FreePDK 45 nm technology [55]. FeFET uses verilog-A model to capture its characteristics. In this analysis, a programming pulse (V_P ±4 V) with a pulsewidth of 500 ns is used to set the threshold states of two FeFET pass transistors.

Technology	45 nm
Width	90 nm
Thickness of the ferroelectric	8 nm
Number of domains	20
Supply Voltage	0.8 V
CNTL	1.1 V
V_p	± 4 V, pulsewidth = 500 ns
INPUT	0.8 V

Table B.1: Simulation Parameters

First, the block is programmed for buffer mode of operation. Second, the device is reprogrammed for inverter mode of operation. In the buffer mode of encryption, T1 (Fig. 2.1(f)) is programmed to HVT and T2 is programmed to LVT by asserting the

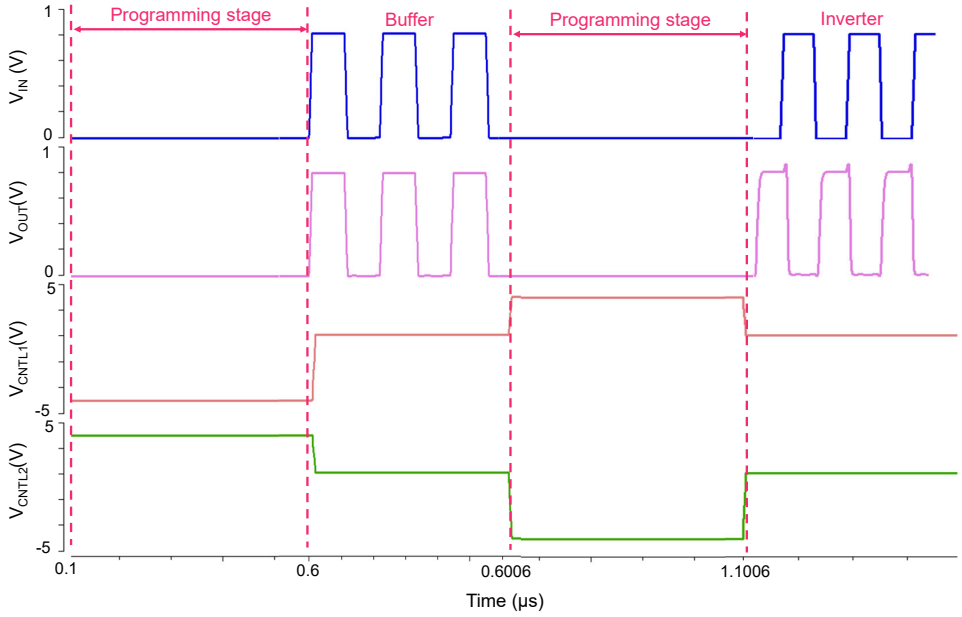


Figure B.1: Simulated waveforms of the dynamic programming of the FeFET active inter-connect encryption block (Fig. 2.1(e)). In the buffer mode programming stage, T1/ T2 is programmed to HVT/ LVT respectively by asserting write voltage on CNTL signals. In the logic mode, read voltage is asserted on CNTL signals and V_{OUT} follows V_{IN}. In the inverter mode programming stage, T1/T2 is programmed to LVT/HVT respectively by asserting write voltage on CNTL signals. In the logic mode, read voltage is asserted on CNTL signals and V_{OUT} shows inverted V_{IN}.

write voltages in CNTL terminals. During this period, the polarizations of these two FeFETs are set in opposite directions. In the evaluation mode, CNTL1 (V_{CNTL1}) and CNTL2 (V_{CNTL2}) are asserted with 1.1V and output (Out) follows the input (In). This is shown as Programming stage/Buffer in Fig. B.1.

In the inverter mode of encryption, T1 (Fig. 1.1(h)) is programmed to LVT and T2 is programmed to HVT by asserting the write voltages in CNTL terminals. In the logic mode, CNTL1 (V_{CNTL1}) and CNTL2 (V_{CNTL2}) are asserted with 1.1V and logic input (V_{IN}) is set at 0.8 V for logic high and 0 V for logic low. The output (Out) shows the inverted input (In). In short, the proposed encryption circuit can produce two different outputs from the same input based on FeFETs' programmed states making a strong case for reverse engineering resilient hardware.

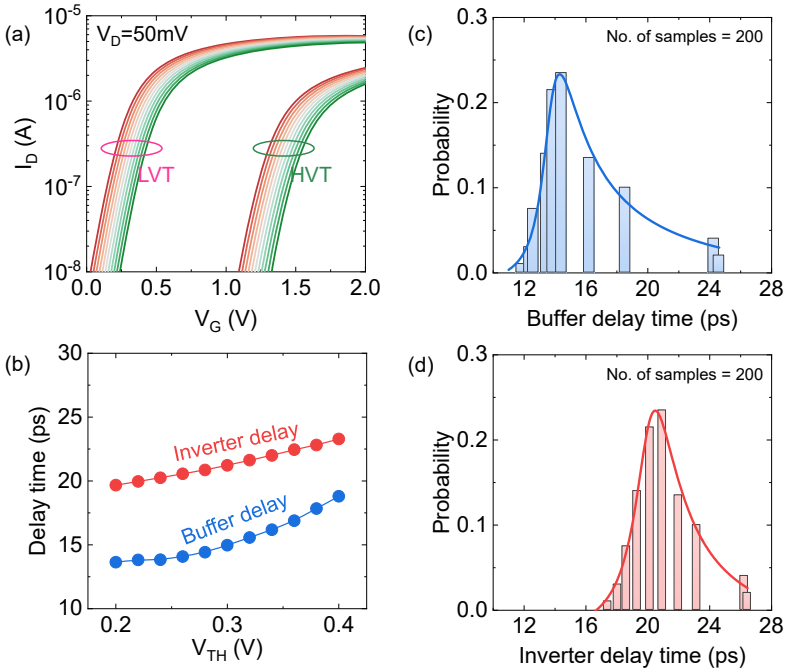


Figure B.2: Threshold voltage and delay variation analysis of the FeFET active interconnect encryption block. (a) Equivalent NMOS I-V characteristics of the FeFET in LVT and HVT states. (b) Delay of the proposed reconfigurable encryption circuit with equivalent nmos transistors in buffer mode and inverter mode. (c) Probability distribution of the delay in reconfigurable encryption circuit with V_T variation when working as a buffer (number of samples: 200). (d) Probability distribution of the delay in encryption circuit with V_T variation when working as an inverter (number of samples: 200).

B.2 Variation Analysis

Variation analysis is conducted to study the delay impact of our proposed circuit. Fig. B.2(a) shows I_d - V_g characteristics of the calibrated NMOS transistor of the equivalent FeFET in LVT and HVT states. Monte Carlo simulations are performed to model threshold voltage gaussian variation. The delay variation of the encryption circuits in inverter mode and buffer mode with respect to threshold voltage change are shown in Fig. B.2(b). The probabilistic distribution of the buffer delay and inverter delay with respect to threshold voltage variation is given in Fig. B.2(c),(d). The analysis shows an overall delay variation of 6.4 ns/4.5 ns for the proposed circuit in respective buffer/inverter modes .

Appendix C
Layout and Device Analysis

This Siction is done in part with Dr. Nico Jao.

Fig. C.1 shows the layout of one encryption block consisting of two FeFETs and one inverter. The block has 1.35 μm (30F) width and 0.81 μm (18F) height. The area is calculated as 1.09 μm^2. Note, compared to the TVD implementation [3] needing 30 transistors, our implementation needs only 4 transistors while maintaining the camouflaging functionality.

Table. C.1 gives a comparison between TVD implementation [3] and reconfigurable logic centred on NAND gate (Tabe. 5.1) using active interconnect blocks (AIB) based on the number of transistors. Using one active interconnect block at the output of NAND gives reconfigurable AND/NAND logic. The above mentioned circuit takes 8 transistors. In addition, adding 2 more AIBs at the input of NAND give 4 reconfigurable logic possibilities with 16 Transistors.

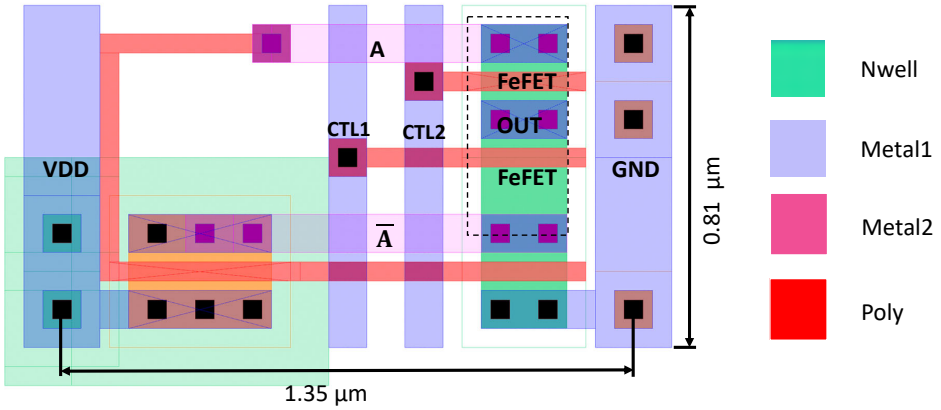


Figure C.1: Layout of a single active interconnect based encryption block.

	FeFET-TVD[19]	ReConfig with 1 AIB	ReConfig with 3 AIB
AND	31T	8T	16T
NAND	31T	8T	16T
OR	31T	N/A	16T
NOR	31T	N/A	16T

Table C.1: Number of transistor required for previous FeFET-TVD [3] Circuit and Proposed Reconfigurable logic with active interconnect blocks

Bibliography

[1] Trentzsch, M., S. Flachowsky, R. Richter, J. Paul, B. Reimer, D. Utess, S. Jansen, H. Mulaosmanovic, S. Müller, S. Slesazeck, et al. (2016) "A 28nm HKMG super low power embedded NVM technology based on ferroelectric FETs," in *2016 IEEE International Electron Devices Meeting (IEDM)*, IEEE, pp. 11–5.

[2] Deng, S., G. Yin, W. Chakraborty, S. Dutta, S. Datta, X. Li, and K. Ni (2020) "A comprehensive model for ferroelectric FET capturing the key behaviors: Scalability, variation, stochasticity, and accumulation," in *2020 IEEE Symposium on VLSI Technology*, IEEE, pp. 1–2.

[3] Dutta, S., B. Grisafe, C. Frentzel, Z. Enciso, M. S. Jose, J. Smith, K. Ni, S. Joshi, and S. Datta (2021) "Experimental Demonstration of Gate-Level Logic Camouflaging and Run-Time Reconfigurability Using Ferroelectric FET for Hardware Security," *IEEE Transactions on Electron Devices*, **68**(2), pp. 516–522.

[4] Rahman, M. T., M. S. Rahman, H. Wang, S. Tajik, W. Khalil, F. Farahmandi, D. Forte, N. Asadizanjani, and M. Tehranipoor (2020) "Defense-in-Depth: A Recipe for Logic Locking to Prevail," *Integr. VLSI J.*, **72**(C), p. 39–57. URL `https://doi.org/10.1016/j.vlsi.2019.12.007`

[5] Rahman, M. T., D. Forte, Q. Shi, G. K. Contreras, and M. Tehranipoor (2014) "CSST: Preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly," in *2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pp. 46–51.

[6] Torrance, R. and D. James (2011) "The state-of-the-art in semiconductor reverse engineering," in *2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 333–338.

[7] Rajarathnam, R. S., Y. Lin, Y. Jin, and D. Z. Pan (2020) "ReGDS: A Reverse Engineering Framework from GDSII to Gate-level Netlist," in *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 154–163.

[8] Torrance, R. and D. James (2009) "The State-of-the-Art in IC Reverse Engineering," in *Cryptographic Hardware and Embedded Systems - CHES 2009* (C. Clavier and K. Gaj, eds.), Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 363–381.

[9] Erbagci, B., C. Erbagci, N. E. C. Akkaya, and K. Mai (2016) "A secure camouflaged threshold voltage defined logic family," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 229–235.

[10] Akkaya, N. E. C., B. Erbagci, and K. Mai (2018) "A secure camouflaged logic family using post-manufacturing programming with a 3.6GHz adder prototype in 65nm CMOS at 1V nominal VDD," in *2018 IEEE International Solid - State Circuits Conference - (ISSCC)*, pp. 128–130.

[11] Nirmala, I. R., D. Vontela, S. Ghosh, and A. Iyengar (2016) "A novel threshold voltage defined switch for circuit camouflaging," in *2016 21th IEEE European Test Symposium (ETS)*, pp. 1–2.

[12] Mohan, P., N. E. C. Akkaya, B. Erbagci, and K. Mai (2018) "A compact energy-efficient pseudo-static camouflaged logic family," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 96–102.

[13] Iyengar, A. S., D. Vontela, I. Reddy, S. Ghosh, S. Motaman, and J.-w. Jang (2018) "Threshold Defined Camouflaged Gates in 65nm Technology for Reverse Engineering Protection," in *Proceedings of the International Symposium on Low Power Electronics and Design*, ISLPED '18, Association for Computing Machinery, New York, NY, USA.
URL https://doi.org/10.1145/3218603.3218641

[14] Roy, K., M. Sharad, D. Fan, and K. Yogendra (2014) "Computing with Spin-Transfer-Torque Devices: Prospects and Perspectives," in *2014 IEEE Computer Society Annual Symposium on VLSI*, pp. 398–402.

[15] Sedighi, B., X. S. Hu, J. J. Nahas, and M. Niemier (2014) "Nontraditional Computation Using Beyond-CMOS Tunneling Devices," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, **4**(4), pp. 438–449.

[16] Iyengar, A. S., S. Ghosh, and K. Ramclam (2015) "Domain Wall Magnets for Embedded Memory and Hardware Security," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, **5**(1), pp. 40–50.

[17] Wu, P., D. Reis, X. S. Hu, and J. Appenzeller (2021) "Two-dimensional transistors with reconfigurable polarities for secure circuits," *Nature Electronics*, **4**(1), pp. 45–53.
URL https://doi.org/10.1038/s41928-020-00511-7

[18] Lee, S.-J., Z. Lin, J. Huang, C. S. Choi, P. Chen, Y. Liu, J. Guo, C. Jia, Y. Wang, L. Wang, Q. Liao, I. Shakir, X. Duan, B. Dunn, Y. Zhang,

Y. Huang, and X. Duan (2020) "Programmable devices based on reversible solid-state doping of two-dimensional semiconductors with superionic silver iodide," *Nature Electronics*, **3**(1), p. 630–637.
URL https://doi.org/10.1038/s41928-020-00472-x

[19] Rajendran, J., M. Sam, O. Sinanoglu, and R. Karri (2013) "Security Analysis of Integrated Circuit Camouflaging," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, Association for Computing Machinery, New York, NY, USA, p. 709–720.
URL https://doi.org/10.1145/2508859.2516656

[20] Greene, J., S. Kaptanoglu, W. Feng, V. Hecht, J. Landry, F. Li, A. Krouglyanskiy, M. Morosan, and V. Pevzner (2011) "A 65nm flash-based FPGA fabric optimized for low cost and power," in *Proceedings of the 19th ACM/SIGDA international symposium on Field programmable gate arrays*, pp. 87–96.

[21] Strenz, R. (2020) "Review and outlook on embedded nvm technologies–from evolution to revolution," in *2020 IEEE International Memory Workshop (IMW)*, IEEE, pp. 1–4.

[22] Huang, K., Y. Ha, R. Zhao, A. Kumar, and Y. Lian (2014) "A low active leakage and high reliability phase change memory (PCM) based non-volatile FPGA storage element," *IEEE Transactions on Circuits and Systems I: Regular Papers*, **61**(9), pp. 2605–2613.

[23] Zhao, W., E. Belhaire, C. Chappert, and P. Mazoyer (2009) "Spin transfer torque (STT)-MRAM–based runtime reconfiguration FPGA circuit," *ACM Transactions on Embedded Computing Systems (TECS)*, **9**(2), pp. 1–16.

[24] Tanachutiwat, S., M. Liu, and W. Wang (2010) "FPGA Based on Integration of CMOS and RRAM," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, **19**(11), pp. 2023–2032.

[25] George, S., K. Ma, A. Aziz, X. Li, A. Khan, S. Salahuddin, M.-F. Chang, S. Datta, J. Sampson, S. Gupta, and V. Narayanan (2016) "Nonvolatile Memory Design Based on Ferroelectric FETs," in *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, IEEE Press, p. 1–6.
URL https://doi.org/10.1145/2897937.2898050

[26] George, S., X. Li, M. J. Liao, K. Ma, S. Srinivasa, K. Mohan, A. Aziz, J. Sampson, S. K. Gupta, and V. Narayanan (2018) "Symmetric 2-D-Memory Access to Multidimensional Data," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, **26**(6), pp. 1040–1050.

[27] Li, X. and L. Lai (2018) "Nonvolatile Memory and Computing Using Emerging Ferroelectric Transistors," in *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 750–755.

[28] Ni, K., X. Yin, A. F. Laguna, S. Joshi, S. Dünkel, M. Trentzsch, J. Müller, S. Beyer, M. Niemier, X. S. Hu, et al. (2019) "Ferroelectric ternary content-addressable memory for one-shot learning," *Nature Electronics*, **2**(11), pp. 521–529.

[29] Ni, K., P. Sharma, J. Zhang, M. Jerry, J. A. Smith, K. Tapily, R. Clark, S. Mahapatra, and S. Datta (2018) "Critical Role of Interlayer in Hf0.5Zr0.5O2 Ferroelectric FET Nonvolatile Memory Performance," *IEEE Transactions on Electron Devices*, **65**(6), pp. 2461–2469.

[30] Thirumala, S. K., A. Raha, V. Narayanan, V. Raghunathan, and S. K. Gupta (2019) "Non-volatile Logic and Memory based on Reconfigurable Ferroelectric Transistors," in *2019 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH)*, pp. 1–6.

[31] Khan, A. I., A. Keshavarzi, and S. Datta (2020) "The future of ferroelectric field-effect transistor technology," *Nature Electronics*, **3**(10), pp. 588–597.

[32] Mikolajick, T., U. Schroeder, and S. Slesazeck (2020) "The past, the present, and the future of ferroelectric memories," *IEEE Transactions on Electron Devices*, **67**(4), pp. 1434–1443.

[33] Dünkel, S., M. Trentzsch, R. Richter, P. Moll, C. Fuchs, O. Gehring, M. Majer, S. Wittek, B. Müller, T. Melde, et al. (2017) "A FeFET based super-low-power ultra-fast embedded NVM technology for 22nm FDSOI and beyond," in *2017 IEEE International Electron Devices Meeting (IEDM)*, IEEE, pp. 19–7.

[34] Yan, S.-C., G.-M. Lan, C.-J. Sun, Y.-H. Chen, C.-H. Wu, H.-K. Peng, Y.-H. Lin, Y.-H. Wu, and Y.-C. Wu (2021) "High speed and large memory window ferroelectric HfZrO FinFET for high-density nonvolatile memory," *IEEE Electron Device Letters*, **42**(9), pp. 1307–1310.

[35] Huang, W., H. Zhu, Y. Zhang, X. Yin, X. Ai, J. Li, C. Li, Y. Li, L. Xie, Y. Liu, et al. (2021) "Ferroelectric Vertical Gate-All-Around Field-Effect-Transistors With High Speed, High Density, and Large Memory Window," *IEEE Electron Device Letters*, **43**(1), pp. 25–28.

[36] Lee, S.-Y., C.-C. Lee, Y.-S. Kuo, S.-W. Li, and T.-S. Chao (2021) "Ultrathin Sub-5-nm Hf ZrO for a Stacked Gate-all-Around Nanowire Ferroelectric FET With Internal Metal Gate," *IEEE Journal of the Electron Devices Society*, **9**, pp. 236–241.

[37] Dünkel, S., M. Trentzsch, R. Richter, P. Moll, C. Fuchs, O. Gehring, M. Majer, S. Wittek, B. Müller, T. Melde, H. Mulaosmanovic, S. Slesazeck, S. Müller, J. Ocker, M. Noack, D. . Löhr, P. Polakowski, J. Müller, T. Mikolajick, J. Höntschel, B. Rice, J. Pellerin, and S. Beyer (2017) "A FeFET based super-low-power ultra-fast embedded NVM technology for 22nm FDSOI and beyond," in *2017 IEEE International Electron Devices Meeting (IEDM)*, pp. 19.7.1–19.7.4.

[38] Jerry, M., P. Chen, J. Zhang, P. Sharma, K. Ni, S. Yu, and S. Datta (2017) "Ferroelectric FET analog synapse for acceleration of deep neural network training," in *2017 IEEE International Electron Devices Meeting (IEDM)*, pp. 6.2.1–6.2.4.

[39] Jerry, M., S. Dutta, A. Kazemi, K. Ni, J. Zhang, P.-Y. Chen, P. Sharma, S. Yu, X. S. Hu, M. Niemier, and S. Datta (2018) "A ferroelectric field effect transistor based synaptic weight cell," *Journal of Physics D: Applied Physics*, **51**(43), p. 434001.
URL `https://doi.org/10.1088/1361-6463/aad6f8`

[40] Chen, H.-T., C.-C. Chang, and T. Hwang (2010) "Reconfigurable ECO Cells for Timing Closure and IR Drop Minimization," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, **18**(12), pp. 1686–1695.

[41] Roy, J. A. and I. L. Markov (2007) "ECO-System: Embracing the Change in Placement," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **26**(12), pp. 2173–2185.

[42] Yurchuk, E., J. Müller, S. Müller, J. Paul, M. Pešić, R. van Bentum, U. Schroeder, and T. Mikolajick (2016) "Charge-trapping phenomena in HfO 2-based FeFET-type nonvolatile memories," *IEEE Transactions on Electron Devices*, **63**(9), pp. 3501–3507.

[43] Gong, N. and T.-P. Ma (2017) "A study of endurance issues in HfO 2-based ferroelectric field effect transistors: Charge trapping and trap generation," *IEEE Electron Device Letters*, **39**(1), pp. 15–18.

[44] Mulaosmanovic, H., J. Ocker, S. Muller, U. Schroeder, J. Muller, P. Polakowski, S. Flachowsky, R. van Bentum, T. Mikolajick, and S. Slesazeck (2017) "Switching kinetics in nanoscale hafnium oxide based ferroelectric field-effect transistors," *ACS applied materials & interfaces*, **9**(4), pp. 3792–3798.

[45] Mulaosmanovic, H., S. Dünkel, M. Trentzsch, S. Beyer, E. T. Breyer, T. Mikolajick, and S. Slesazeck (2020) "Investigation of Accumulative switching in ferroelectric FETs: enabling universal modeling of the switching behavior," *IEEE Transactions on Electron Devices*, **67**(12), pp. 5804–5809.

[46] "FreePDK45," .
URL https://www.eda.ncsu.edu/wiki/FreePDK45:Contents

[47] Müller, J., T. Böscke, S. Müller, E. Yurchuk, P. Polakowski, J. Paul, D. Martin, T. Schenk, K. Khullar, A. Kersch, et al. (2013) "Ferroelectric hafnium oxide: A CMOS-compatible and highly scalable approach to future ferroelectric memories," in *2013 IEEE International Electron Devices Meeting*, IEEE, pp. 10–8.

[48] Beyer, S., S. Dünkel, M. Trentzsch, J. Müller, A. Hellmich, D. Utess, J. Paul, D. Kleimaier, J. Pellerin, S. Müller, et al. (2020) "FeFET: A versatile CMOS compatible device with game-changing potential," in *2020 IEEE International Memory Workshop (IMW)*, IEEE, pp. 1–4.

[49] Kahng, A. B., J. Lienig, I. L. Markov, and J. Hu (2011) *VLSI physical design: from graph partitioning to timing closure*, Springer Science & Business Media.

[50] Gosti, W., S. Khatri, and A. Sangiovanni-Vincentelli (2001) "Addressing the timing closure problem by integrating logic optimization and placement," in *IEEE/ACM International Conference on Computer Aided Design. ICCAD 2001. IEEE/ACM Digest of Technical Papers (Cat. No.01CH37281)*, pp. 224–231.

[51] Yang, J., H. Shen, L.-k. Liu, and D.-s. You (2012) "Multi-mode timing closure of D6000 Collective Communication Chip," in *2012 IEEE 11th International Conference on Solid-State and Integrated Circuit Technology*, pp. 1–3.

[52] Iyengar, A. and S. Ghosh (2015) "Threshold Voltage-Defined Switches for Programmable Gates," *CoRR*, **abs/1512.01581**, 1512.01581.
URL http://arxiv.org/abs/1512.01581

[53] Hansen, M., H. Yalcin, and J. Hayes (1999) "Unveiling the ISCAS-85 benchmarks: a case study in reverse engineering," *IEEE Design Test of Computers*, **16**(3), pp. 72–80.

[54] "PRIMETIME from Synopsys," .
URL https://www.synopsys.com/support/training/signoff/primetime1-fcd.html

[55] Stine, J. E., I. Castellanos, M. Wood, J. Henson, F. Love, W. R. Davis, P. D. Franzon, M. Bucher, S. Basavarajaiah, J. Oh, and R. Jenkal (2007) "FreePDK: An Open-Source Variation-Aware Design Kit," in *2007 IEEE International Conference on Microelectronic Systems Education (MSE'07)*, pp. 173–174.

[56] "Xilinx Vivado Design Suite," .
URL https://www.xilinx.com/products/design-tools/vivado.html

[57] Liu, B. and B. Wang (2015) "Reconfiguration-Based VLSI Design for Security," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, **5**(1), pp. 98–108.