

ProCamo: A Fast Post-Manufacturing Programmable Camouflaged Logic Family

Seo Hyun Kim¹, Minhyeok Jeong², Jongmin Lee^{1,3}

¹*Dept. of Intelligence Semiconductor Engineering, Ajou University, Suwon, Republic of Korea.*

²*Dept. of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea.*

³*Dept. of Electrical and Computer Engineering, Ajou University, Suwon, Republic of Korea*
jongmin@ajou.ac.kr

Abstract—Advances in semiconductor scaling and integration have increased design complexity, concentrating valuable IP in single chips. Reverse engineering using high-resolution microscopy techniques, such as scanning electron microscopy (SEM) and transmission electron microscopy (TEM), enables detailed circuit analysis and extraction of layout-level information. At the same time, reliance on external foundries increases the risks of design information leakage. To address these challenges, we propose a Fast Post-Manufacturing Programmable Camouflaged (FP2C) Logic Family, which consists of physically identical logic structures that are activated by applying a post-programming code (PC) after fabrication. The proposed FP2C logic-embedded Flip-Flop (FP2C logic-eFF) was implemented using a 28nm CMOS process, achieving a 67% reduction in cell area compared to prior Post-Manufacturing Programmed Threshold Voltage Defined (PMP-TVD) logic cells on the same technology node. Furthermore, this paper presents a systematic design methodology that integrates FP2C logic-eFF into an EDA tool-based digital circuit design flow. This enables FP2C logic to move beyond prior camouflaged logic that was limited to full-custom arithmetic unit implementations, and extend to complex digital IPs. To validate its feasibility, an AES module was designed and its functionality was verified through SPICE simulation, thereby demonstrating the applicability of FP2C logic to complex digital modules.

Keywords—*Camouflaged Logic, Reverse Engineering, Differential Power Analysis, Hardware Security*

I. INTRODUCTION

The globalized semiconductor value chain has evolved into a highly distributed, multi-party outsourcing structure spanning design, front-end and back-end manufacturing, packaging, and test/verification. In this process, the possibility of involvement by untrusted foundries or subcontractors remains [1]. While such specialization has improved cost and development velocity, it has also expanded the attack surface for supply-chain threats such as IP leakage and circuit cloning. Moreover, continued technology scaling has increased integration density, concentrating diverse IPs on a single die and further incentivizing physical/functional reverse engineering that seeks to recover functionality directly from silicon without prior design knowledge [2].

Reverse engineering is the process in which an attacker systematically removes the layer of a fabricated chip to analyze its circuit configuration in detail and reconstruct the corresponding schematic [3]. With advances in high-resolution imaging tools such as SEM and TEM, attackers can examine chip structures in great detail and extract candidate standard cells without a reference library [4]. Combined with plasma focused ion beam (FIB)-based delayering, advances in deprocessing automation using image stitching, X-ray tomography, and FIB-SEM platforms enable precise layer-by-layer analysis of integrated circuits [5]. Although the chip is

physically destroyed during this process, a successful reverse engineering attack can lead to the complete replication of the original circuit, thereby enabling IP theft.

In addition to reverse engineering threats, reliance on untrusted foundries poses another critical vulnerability [6]. Since only a limited number of companies possess advanced manufacturing facilities, most fabless firms are inevitably forced to outsource fabrication to external foundries. In this process, attackers within the foundry can access the entire physical layout, leading to supply chain threat such as IP theft and unauthorized cloning.

As a countermeasure to these threats, camouflaged logic gates have been developed with physically identical structures, making it impossible to deduce the circuit design based on physical appearances. These gates employ techniques such as threshold voltage defined (TVD) logic using transistors with varying threshold voltages to realize different functions [7] - [10] or utilize Ferroelectric Field-Effect Transistors (FeFET) devices [11]. Despite this functional diversity, they maintain identical physical structures, thereby achieving resistance against reverse engineering. However, when using transistors with distinct threshold voltages or FeFET devices, additional design rules are required. In this process, layout-level information about the implemented functionality may be unintentionally exposed, which can eventually compromise the security of the design.

To address this vulnerability, physical programming using charge trap phenomenon has been employed for post-manufacturing programming to mitigate the risk of information leakage from untrusted foundries [12], [13]. However, these approaches are limited by slow programming speeds and a restricted number of reprogramming cycles, making them unsuitable for frequent updates [13].

As a promising solution, this paper proposes FP2C logic, which enables rapid post-manufacturing programming of the desired logic through code injection. When an incorrect code is applied, it disables the intended circuit operation, which improves the security robustness of the design. Furthermore, FP2C logic is implemented as standard cells, and library characterization enables automated design (e.g., synthesis, placement and route (P&R)) with EDA tools. It is also compatible with conventional standard cells, allowing seamless integration into digital IP designs.

The remainder of this paper is organized as follows: Section II discusses the state-of-the-art CMOS-compatible camouflaged logic structures as well as the operating principles and characteristics of the proposed FP2C logic. Section III outlines the methodology for implementing digital systems using FP2C logic, along with results from an FP2C logic-based AES-128 implementation. Section IV evaluates

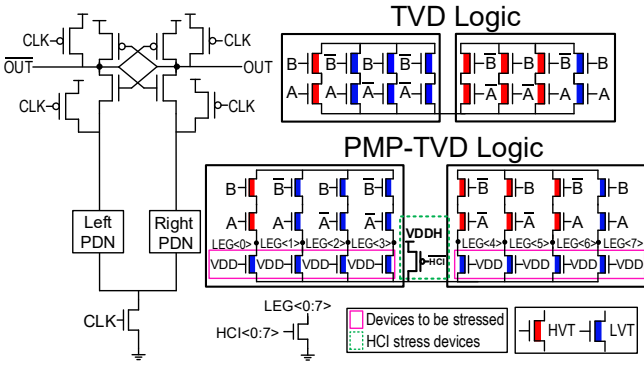


Fig. 1. Prior TVD-based logic [7]-[10], TVD-PMP logic [12], [13].

and compares the resistance against differential power analysis (DPA) attacks of AES-128 implementations using FP2C logic and conventional standard cells. Finally, Section V concludes the paper.

II. FAST POST-MANUFACTURING PROGRAMMABLE LOGIC FAMILY DESIGN

A. Threshold Voltage Defined Camouflaged Logic

A representative example of prior-art camouflaged logic where all conventional logic gates have the same physical layout is TVD logic, which utilizes devices with various threshold voltages. As shown in the upper-right of Fig. 1, TVD logic is constructed by placing a pull-down network (PDN) beneath a sense amplifier-based logic (SABL) structure [7] - [13]. TVD logic achieves its functionality by exploiting the difference in driving strength between two pull-down paths, which are constructed with high-threshold voltage (HVT) and low-threshold voltage (LVT) transistors, depending on its functionality. Because TVD logic gates are physically indistinguishable, they demonstrate strong resistance to reverse engineering.

However, when TVD logic is fabricated by an external foundry, the placement of the HVT and LVT transistors is exposed, posing a significant risk of information leakage from untrusted foundries. To address this issue, PMP-TVD logic, depicted in the lower-right of Fig. 1, was proposed to eliminate information leakage risks by leveraging the charge trap phenomenon of high-K metal gates for post-manufacturing programmability [12], [13]. Although PMP-TVD logic effectively prevents information leakage, even when fabricated in an untrusted foundry, its reliance on charge trap programming introduces critical limitations. Applying high-voltage stress to the transistor is essential for charge trap-based programming, making the process inherently slow. Additionally, the nature of the charge trap phenomenon makes it challenging to achieve high-speed programming and prohibits multiple reprogramming cycles [13].

B. Proposed Fast Post-Manufacturing Programmable Camouflaged Logic

As shown in Fig. 2, the proposed FP2C logic gate is constructed using the SABL structure with symmetric pull-down logic on both sides, exclusively employing RVT transistors. The PDN of the FP2C logic gate consists of NMOS transistors that control the on/off state based on inputs A , \bar{A} , B , and \bar{B} , together with eight pairs of transmission gates controlled by the PC values $X[7:0]$ which dictate the logic operation. As the PC values are applied after fabrication, the

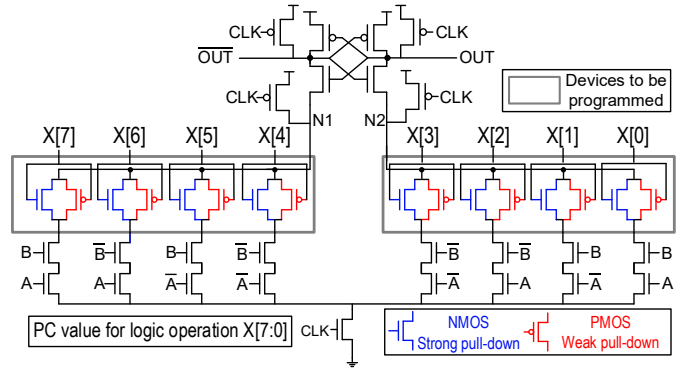


Fig. 2. Schematic of proposed FP2C logic.

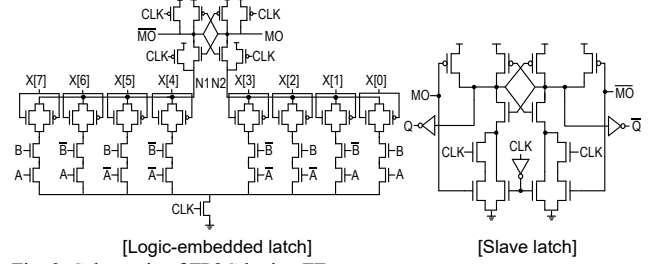


Fig. 3. Schematic of FP2C logic-eFF.

design inherently eliminates information leakage risks from untrusted foundries.

When PC values are applied, either an NMOS or PMOS transistor in the transmission gate is activated. NMOS transistors, with their stronger driving strength, can more effectively pull the PDN down to a low potential. In contrast, PMOS transistors exhibit significantly weaker driving strength when pulling the PDN to a low potential, and thus do not sufficiently pull it down. Exploiting this characteristic, the FP2C logic gate can be configured to function as a NAND-AND, INV-BUF, NOR-OR, or XNOR-XOR gate, enabling it to serve as a versatile configurable logic gate.

The FP2C logic gate, based on the SABL architecture, operates as a logic-embedded latch. When the clock signal CLK is low, it performs a pre-charge operation; when CLK is high, it evaluates the logic function and stores the result in an internal latch. To facilitate timing analysis for large digital block designs, the FP2C logic-eFF was implemented as shown in Fig. 3. It consists of the FP2C logic gate in Fig. 3 (left), acting as a logic-embedded master latch, and a slave latch in Fig. 3 (right), which captures the result from the master latch during the rising edge of the clock signal.

The operation principle of the proposed FP2C logic-eFF is shown in Fig. 4. For example, with the PC value set to 8'b0111_0001, the FP2C logic-eFF is configured to operate as a NAND-AND logic. During the evaluation phase shown in the left-top of Fig. 4, when the input signals $(A, B) = (1, 1)$ are applied, the pull-down path of the left PDN involves a PMOS transistor, whereas the right PDN consists only of NMOS transistors. Immediately after the rising edge of the CLK signal, node N2 is discharged more strongly than node N1 due to the difference in pull-down strength between NMOS and PMOS transistors. This creates a significant voltage difference between the two nodes, which is then amplified by the sense amplifier located at the top, generating the outputs MO and $\bar{M}\bar{O}$. In contrast, when the input signals are $(A, B) = (0, 0)$, $(0, 1)$, or $(1, 0)$, the pull-down path in the left PDN consists of NMOS transistors, while the right PDN includes PMOS

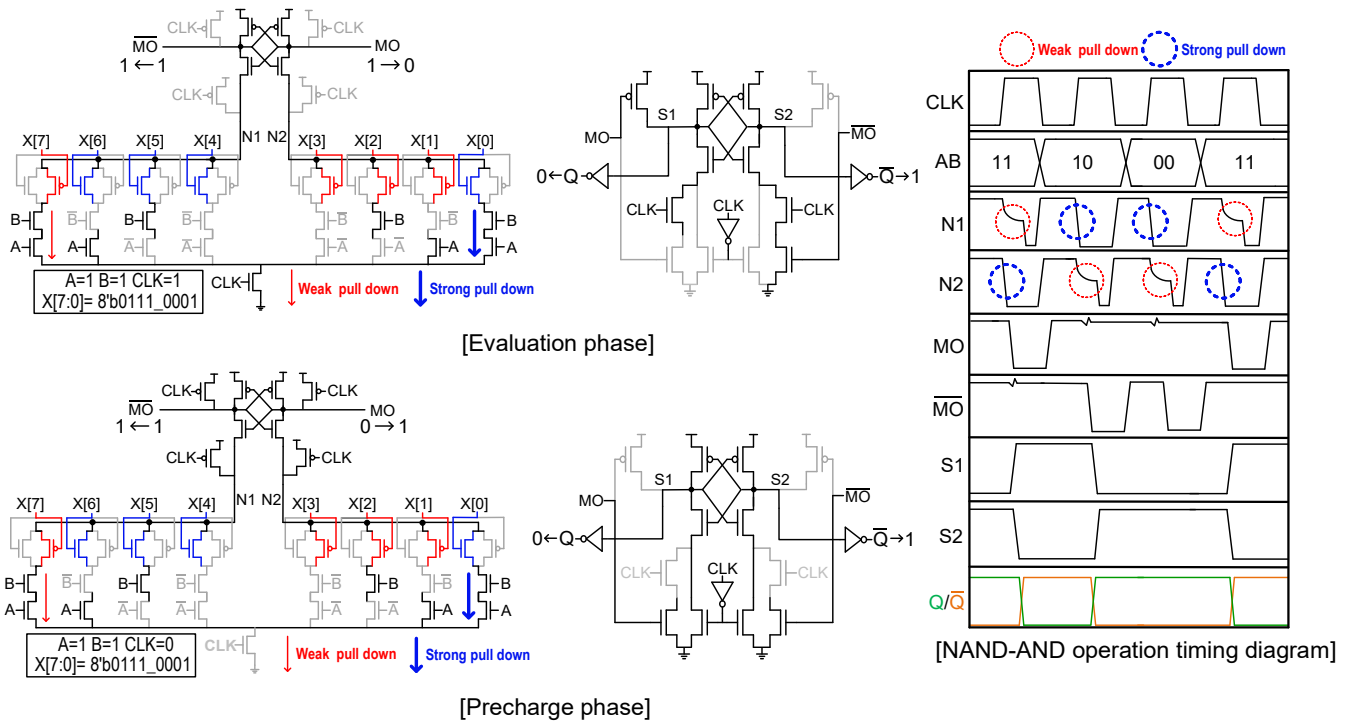


Fig. 4. Operation principle of FP2C logic-eFF.

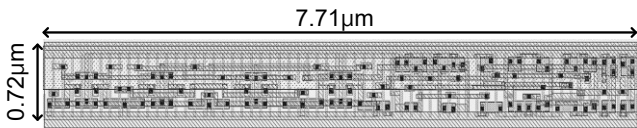


Fig. 5. Cell layout of FP2C logic-eFF.

transistors. As a result, a voltage difference of opposite polarity compared to the (1, 1) state appears between nodes N1 and N2, enabling the FP2C logic gate to perform the NAND-AND function.

The outputs \overline{MO} and MO generated at the master latch are delivered to the slave latch, where positive feedback ensures stable operation, ultimately producing the final outputs Q and \overline{Q} of the FP2C logic-eFF. During the pre-charge phase, the nodes N1, N2, MO , and \overline{MO} in the master latch are precharged to V_{DD} as shown in the left-bottom side of Fig. 4. However, the slave latch on the right preserves the data determined in the previous phase without erasing it during the pre-charge phase, ensuring its operation as a logic-embedded flip-flop.

Fig. 5 shows the layout of the designed FP2C logic-eFF. It can be implemented as a standard cell, making it suitable for automated design flows leveraging EDA tools. Notably, exclusively using RVT transistors allows for a compact and dense layout, optimizing the design for scalability in large digital systems. Furthermore, by maintaining the same physical structure while enabling various functions through post-manufacturing programming, the FP2C logic-eFF conceals its operation unless the PC is known. As a result, the cell itself exhibits resistance to reverse engineering and can effectively hide circuit functionality from potential adversaries within the foundry.

As shown in the left graph of Fig. 6, the proposed FP2C logic significantly outperforms PMP-TVD logic [12], [13] in terms of post-manufacturing programming time and area. While the PMP-TVD logic requires approximately 20-seconds for the first post-manufacturing programming, the

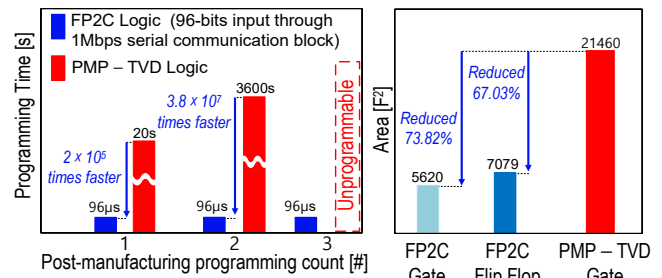


Fig. 6. Programming time (left) and normalized area comparison with prior art PMP-TVD logic (right).

FP2C logic achieves drastically faster programming speed as shown in Fig. 6 (left). This improvement is attributed to the fact that FP2C logic requires only the PC values to reach the PDN, making its programming time dependent on the throughput of the serial communication block that applies the PC values. For example, when using a serial communication block operating at 1-Mbps to input a 96-bit PC value, the programming time is reduced to 96-μs, demonstrating a significant improvement compared to PMP-TVD logic. Even for longer PC values, FP2C logic maintains more than 5 orders of magnitude faster programming speed than PMP-TVD logic, rendering the comparison nearly negligible. Additionally, while PMP-TVD logic suffers from an extremely increased post-manufacturing programming time of up to 1-hour for the second programming cycle [13], FP2C logic sustains consistent programming time regardless of the cycle count. Furthermore, unlike PMP-TVD logic, which is limited to a maximum of two programming cycles due to the reliance on high-K metal gate charge trap phenomenon, FP2C logic enables unlimited post-manufacturing programming cycles.

According to the normalized area comparison in Fig. 6 (right), the proposed FP2C logic gate and FP2C logic-eFF achieve area reductions of 73.82% and 67.03%, respectively, compared to PMP-TVD logic gates. This demonstrates that the proposed cell structure provides a more cost-efficient

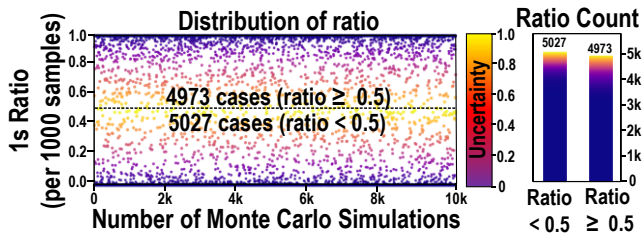


Fig. 7. Distribution of output ‘1’ ratio across Monte Carlo simulations (left) and the aggregated ratio counts (right).

solution than existing post-manufacturing programmable camouflaged logic.

Furthermore, it is important to highlight the behavior of the FP2C logic cell when an incorrect PC is applied. With the correct PC, the cell operates as intended, producing the correct logic output for all inputs. However, when an incorrect PC is applied, the output behavior can be categorized into three cases depending on the input conditions: (1) generating the correct outputs, (2) generating inverted outputs, (3) generating unpredictable outputs. This phenomenon arises from the analog characteristics of the sense amplifier, which detects differences in the driving strength of the two PDNs depending on the applied PC value.

For example, consider a cell intended to operate as NOR_OR with $X[7:0] = 8'b0001_0111$. If an incorrect PC value of $X[7:0] = 8'b1001_1110$ is applied, the cell exhibits three types of aforementioned output behaviors. First, when the input $(A,B) = (1,1)$ is applied, an inverted output is generated. Second, when the input $(A,B) = (1,0)$ is applied, a correct output is obtained. Third, when the input $(A,B) = (0,0)$ is applied, the left and right PDNs possess identical driving strengths. In this case, the output is determined by the response of the sense amplifier, which is influenced by process variations and noise, ultimately resulting in an unpredictable output.

To quantitatively analyze this phenomenon, 10k Monte Carlo simulations were performed to model 10k cells, each under different process variations. The simulations were conducted under conditions where the pull-down strengths of the left and right PDNs were identical, with transient noise applied. The output of each cell was sampled 1000 times. For each of the 10k cells, the number of occurrences of output ‘1’ among the 1000 samples was converted into a ratio and plotted as shown in the left side of Fig. 7. Notably, when the ratio of ‘0’ to ‘1’ approaches 0.5, the probability of obtaining either ‘0’ or ‘1’ under the same input condition becomes nearly equal, thereby making the output more unpredictable. This behavior was visualized using an uncertainty metric, where the closer the ratio of output ‘0’ and ‘1’ is to 0.5, the closer the uncertainty value approaches 1.

In addition, the right side of Fig. 7 presents the aggregated distribution for ratios greater than 0.5 versus less than 0.5. The results show that the proportions of cells biased toward output ‘0’ and output ‘1’ are approximately 51% and 49%, respectively, indicating an almost uniform distribution. Furthermore, the left side of Fig. 7 confirms that there is no systematic bias in the ratio across the Monte Carlo simulation samples. This implies that although an individual FP2C logic cell may exhibit a ratio bias, the overall distribution across all cells remains balanced and, therefore, unpredictable. Since such bias arises from process variations, which are inherently random, the output of camouflaged cells becomes difficult to

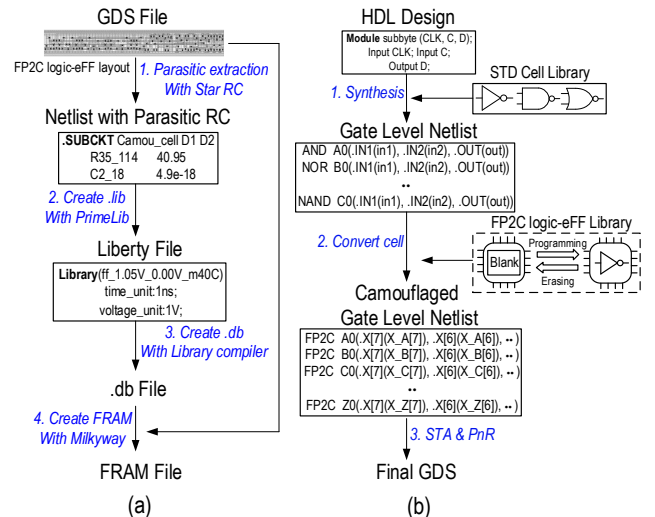


Fig. 8. (a) FP2C logic-eFF library characterization flow. (b) Digital module design flow using FP2C logic-eFF.

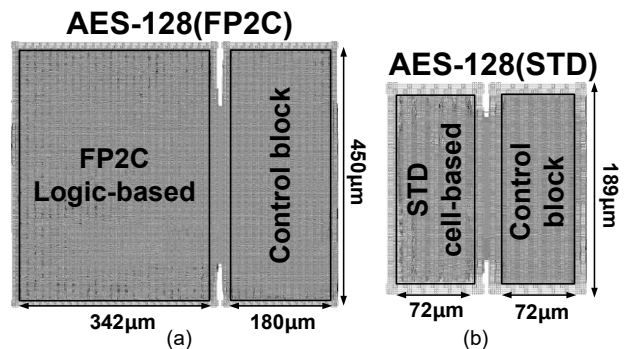


Fig. 9. P&R result of AES-128. (a): FP2C logic-eFF based, (b): Standard cell-based

predict when an incorrect PC is applied. This uncertainty degrades the reproducibility and consistency of the output, ultimately complicating circuit analysis. Therefore, to ensure correct functionality, all IPs implemented with FP2C logic require the correct PC value, underscoring the unique security implications of FP2C logic.

III. DIGITAL SYSTEM DESIGN METHODOLOGY UTILIZING FP2C LOGIC AND AES-128 IMPLEMENTATION RESULTS

A. Library Characterization of FP2C logic-eFF

To characterize the FP2C logic-eFF for library generation, the process depicted in Fig. 8(a) was performed. First, a netlist with extracted parasitic-components was generated based on the layout of the FP2C logic-eFF. Based on this netlist, a liberty file containing timing, power, and load characteristics was generated with Synopsys PrimeLib. To enable the use of the liberty file in Synopsys IC Compiler, it was converted into a .db file using Synopsys Library Compiler. Additionally, for P&R, a Milkyway-format cell library was separately created using Synopsys Milkyway. This comprehensive library characterization process establishes the foundation for the logic synthesis and P&R of digital circuit designs that incorporate the FP2C logic-eFF.

B. Digital Circuit Design Utilizing FP2C logic-eFF and AES-128 Implementation Results

The design process for digital modules using the FP2C logic-eFF library follows the EDA tool-based digital circuit design flow and is summarized in Fig. 8(b). First, the RTL code of the target digital module is prepared and synthesized

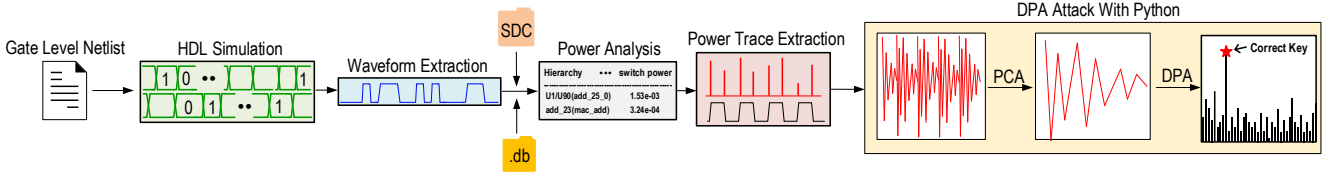


Fig. 10. DPA attack process applied to the AES-128 Module.

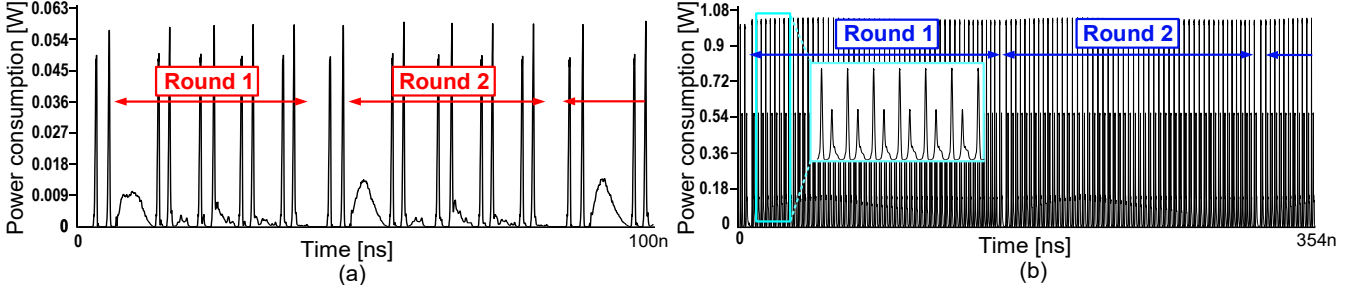


Fig. 11. Power consumption pattern obtained through SPICE simulation (a): Standard cell-based AES-128, (b): FP2C logic-eFF-based AES-128.

using a standard cell library. Next, the generated gate-level netlist is replaced with a camouflaged gate netlist through a script-based procedure. Subsequently, static timing analysis (STA) is performed to identify and verify any timing violations. After STA, the FP2C logic-eFF-based netlist undergoes P&R. In particular, FP2C logic-eFF cells are designed in a unit tile-format identical to standard cell, ensuring full compatibility with other standard cells required for clock tree generation or as delay cells. This design process demonstrates that FP2C logic-eFF enables digital block designs at a higher level of complexity, overcoming the limitations of previous camouflaged logic implementations, which were restricted to small block such as SBOX [9] or simple arithmetic unit designs based on full-custom design methodologies [12], [13]. A reference design using standard cells was also implemented enabling direct comparison with the FP2C logic-eFF-based design. Both designs were implemented using a 28nm CMOS process, and the results are summarized in Fig. 9.

IV. RESISTANCE TO DPA ATTACKS IN FP2C LOGIC-EFF-BASED AES-128

In addition to mitigating the previously discussed threats, ensuring resistance against DPA attacks remains a critical challenge in security IP design [14]-[16]. To this end, countermeasures based on dual-rail structures [17]-[21] and novel logic styles [22]-[24] have been investigated. Unlike these conventional approaches, the proposed FP2C logic-eFF inherently exhibits a symmetric structure, which is expected to reduce the correlation between input values and power consumption patterns. To validate this property, we conducted DPA attacks to evaluate the resistance of FP2C logic-eFF against such threats.

The applied DPA attack process is illustrated in Fig. 10. First, an HDL simulation was performed using a post P&R netlist to extract a dump file capturing internal signal activities during the first SubBytes operation in the AES encryption process. Next, power traces were obtained using Synopsys PrimeTime PX (PTPX), based on the extracted dump files along with the corresponding design constraints and library files. For a conservative power analysis, noise modeling of external factors such as power supply fluctuations was excluded. Instead, the extracted traces focus solely on the intrinsic power consumption of each cell while performing

specific logic functions. This approach eliminates the influence of noise unrelated to power analysis, ensuring that the power traces accurately represent only the circuit's functional operation characteristics. By analyzing power consumption solely from the cell's functional behavior, the evaluation corresponds to a more conservative scenario and enables a clear and quantifiable evaluation of the module's resistance to DPA attacks. Since only functional power consumption is considered, the natural masking effect that could arise from noise is absent, making the attack scenario even more stringent.

Subsequently, the processed traces were fed into a Python-based DPA attack script using the Hamming weight model. Since FP2C logic-eFF inherently exhibits distinct power consumption patterns during the evaluation phase at the rising edge of the clock, principal component analysis (PCA) was applied to reduce the dimensionality of the extracted power traces, facilitating more effective analysis. To compare and validate the DPA attack results for FP2C logic-eFF, a standard cell-based AES-128 module with the same structure was implemented as a baseline. The power consumption patterns of the standard cell-based AES-128 and FP2C logic-eFF-based AES-128 modules were analyzed through SPICE simulation. As shown in Fig. 11(a), the standard cell-based AES-128 module exhibits noticeably different power consumption patterns for each round function. In contrast, as shown in Fig. 11(b), the FP2C logic-eFF-based AES-128 module maintains a consistent power consumption pattern during encryption and does not exhibit significant correlation with the input data between rounds.

In this process, the 128-bit secret key was divided into sixteen 8-bit subkeys, which were individually targeted for extraction and the results of the DPA attacks are shown in Fig. 12. For the standard cell-based module, as depicted in Fig. 12(a) and (b), analysis of power trace differences for each subkey clearly revealed significant differences corresponding to the correct subkey after only 8k and 9k traces, as indicated by the red markers in the graphs. Consequently, the correct subkey could be explicitly identified, allowing the secret key to be inferred byte by byte. Furthermore, as shown in Fig. 12 (e) and (f), the candidate subkey exhibiting maximum peak difference among the 256 possible subkey values was consistently identified across a given number of traces, further verifying the correct subkey. In contrast, for the FP2C logic-

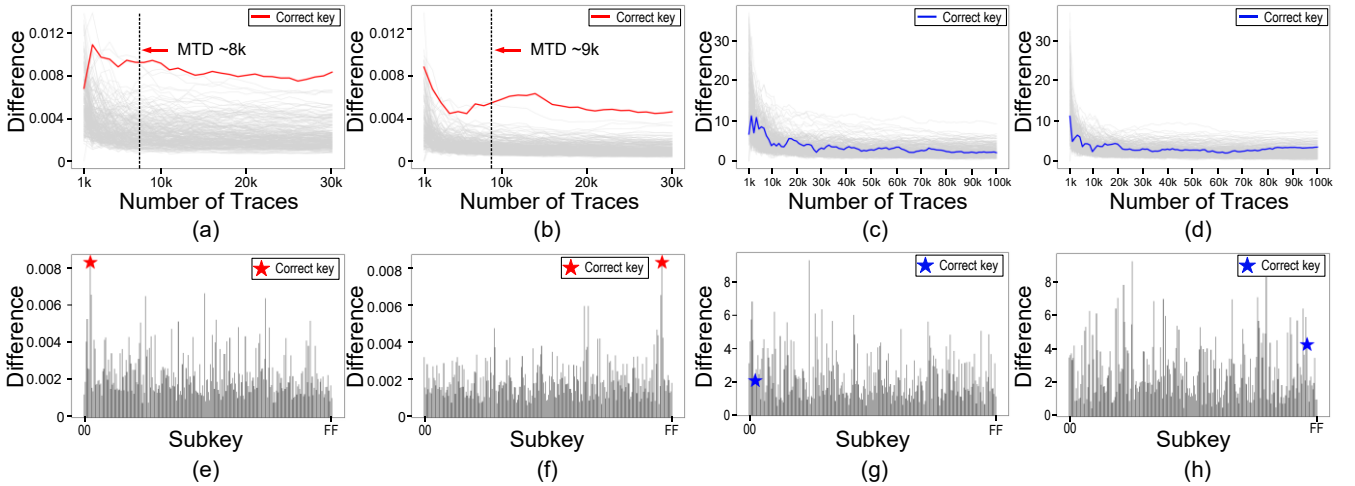


Fig. 12. DPA attack resistance evaluation result with (a), (b), (e), (f) standard cell-based AES-128 module and (c), (d), (g), (h) FP2C logic-eFF-based AES-128 module using power traces from PTPX.

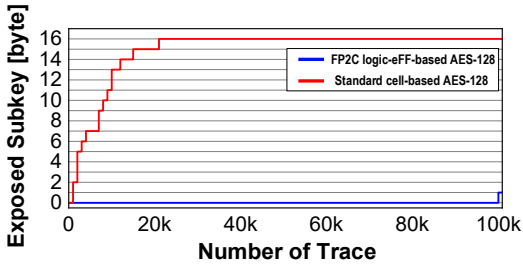


Fig. 13. Success rate of DPA attack based on the number of power traces.

eFF-based module, as shown in Fig. 12(c) and (d), 100k power traces were analyzed, which is significantly more than those used for the standard cell-based module. Nevertheless, no meaningful differences were observed between the correct and incorrect subkeys. Additionally, Fig. 12(g) and (h) indicate that no discernible peak difference for the correct subkey, making it difficult to deduce the correct key. Except for one key byte that was exposed with 100k traces, similar trends were consistently observed for the remaining 13 subkeys that are not shown in Fig. 12. These results suggest that the FP2C logic-eFF-based design offers enhanced resistance to DPA attacks relative to the standard-cell implementation. Fig. 13 summarizes the success rate of DPA attacks over multiple power traces.

Table I summarizes the comparison between the FP2C logic-eFF-based AES-128 module and the standard cell-based AES module. The standard cell-based AES core was synthesized at a relatively low clock frequency due to the timing limitations of combinational logic, whereas the FP2C logic-eFF-based AES module achieves higher operating frequencies by producing an effect equivalent to pipelining. However, since multi-stage FP2C logic-eFF is required for complex logic, encryption speed is slower due to the larger number of clock cycles, despite the higher clock frequency. Additionally, due to its larger cell size and repeated pre-charge and evaluation operations, the FP2C logic-eFF-based design incurs area and performance, and power consumption overhead. Nevertheless, unlike the standard cell-based AES module, it exhibits lower correlation between input data and power consumption, is composed entirely of camouflaged cells that provide resistance to reverse engineering, and via PC values supports post-manufacturing activation to prevent information leakage in untrusted fabrication environments. Therefore, despite the overhead, the proposed FP2C logic-eFF is well-suited for security-critical hardware systems.

TABLE I. COMPARISON OF AES-128 DESIGNS

	FP2C logic-eFF - based AES	Standard Cell -based AES
Technology	28nm CMOS	28nm CMOS
Supply Voltage [V]	0.9	0.9
Frequency [MHz]	333	125
Core Area [mm^2]	0.153	0.013
Power Consumption [mW]	21.7 ¹⁾	0.335 ²⁾
Encryption Speed [μ s]	1.67 ³⁾	0.440
Reverse Engineering Resistance	High	Low
DPA Attack Resistance	Improved	Limited
Untrusted Fab Leakage	Low	High
Post-Manufacturing Activation	Yes	No

¹⁾@0.9V, 333MHz, 25°C ²⁾@0.9V, 125MHz, 25°C
³⁾Worst case delay @0.9V, 333MHz, 25°C

V. CONCLUSION

The proposed FP2C logic leverages physically identical logic gates and post-manufacturing programmability to defend against reverse engineering and prevent information leakage in untrusted fabrication environments. Unlike previous approaches that required a combination of HVT and LVT transistors, FP2C logic utilizes only RVT transistors. In addition, by externally applying PC values, FP2C logic enables extremely fast post-manufacturing programming and improves reprogrammability, thereby addressing the challenges of prior PMP-TVD camouflaged logic. Moreover, FP2C logic-eFF is designed in a standard cell-like structure, allowing it to be compatible with EDA tools through a library characterization process. This enables automated digital circuit design using FP2C logic-eFF, overcoming the limitations of prior camouflaged logic that were restricted to simple arithmetic units. As a result, FP2C logic-eFF enables the construction of more complex and diverse digital modules while ensuring robust hardware-level security.

ACKNOWLEDGEMENT

This research was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government (MSIT) (RS-2023-00249784, RS-2024-00408040), BK21 FOUR (Department of Intelligence Semiconductor Engineering, Ajou University) and Ajou University research fund. The EDA tool was supported by the IC Design Education Center (IDEC), Korea.

REFERENCES

- [1] T. D. Perez and S. Pagliarini, "A survey on split manufacturing: Attacks, defenses, and challenges," *IEEE Access*, vol. 8, pp. 184013–184035, Dec. 2020.
- [2] M. Fyrbiak, D. Nedospasov, C. Helfmeier, J. Tajik, C. Boit, and J. Becker, "Hardware reverse engineering: Overview and open challenges," in *Proc. IEEE 2nd Int. Verification and Security Workshop (IVSW)*, pp. 88–94, Jul. 2017.
- [3] R. Torrance and D. James, "The state-of-the-art in semiconductor reverse engineering," in *Proc. 48th Design Automation Conf. (DAC)*, pp. 333–338, Jun. 2011.
- [4] M. Zhu, M. Xu, H. Liu, Y. Zhang, and U. Rührmair, "Genetic algorithm-assisted golden-free standard cell library extraction from SEM images," in *Proc. 26th Int. Symp. Quality Electronic Design (ISQED)*, pp. 1–8, Mar. 2025.
- [5] E. L. Principe, N. Asadizanjani, D. Forte, M. M. Tehranipoor, R. Chivas, M. DiBattista, S. E. Silverman, M. Marsh, N. Piche, and J. T. Mastovich, "Steps toward automated deprocessing of integrated circuits," in *Proc. 43rd Int. Symp. Testing and Failure Analysis (ISTFA)*, pp. 1–10, Nov. 2017.
- [6] R. S. Rajarathnam, Y. Lin, Y. Jin, and D. Z. Pan, "ReGDS: A reverse engineering framework from GDSII to gate-level netlist," in *Proc. IEEE Int. Symp. Hardware Oriented Security and Trust (HOST)*, pp. 154–163, Dec. 2020.
- [7] B. Park, "Logic obfuscation through enhanced threshold voltage defined logic family," *IEEE Trans. Circuits and Systems II: Express Briefs*, vol. 67, no. 12, pp. 3407–3411, Dec. 2020.
- [8] B. Erbagci, C. Erbagci, N. E. C. Akkaya, and K. Mai, "A secure camouflaged threshold voltage defined logic family," in *Proc. IEEE Int. Symp. Hardware Oriented Security and Trust (HOST)*, pp. 229–235, May 2016.
- [9] P. Mohan, N. E. C. Akkaya, B. Erbagci, and K. Mai, "A compact energy-efficient pseudo-static camouflaged logic family," in *Proc. IEEE Int. Symp. Hardware Oriented Security and Trust (HOST)*, pp. 96–102, Apr. 2018.
- [10] V. S. Rathor, B. Garg, and G. K. Sharma, "New lightweight threshold voltage defined camouflaged gates for trustworthy designs," *J. Electron. Test.*, vol. 33, no. 5, pp. 657–668, Oct. 2017.
- [11] S. Dutta, A. K. Saha, Y. Xie, S. Datta, and S. K. Gupta, "Experimental demonstration of gate-level logic camouflaging and run-time reconfigurability using ferroelectric FET for hardware security," *IEEE Trans. Electron Devices*, vol. 68, no. 2, pp. 516–522, Feb. 2021.
- [12] N. E. C. Akkaya, B. Erbagci, and K. Mai, "A secure camouflaged logic family using post-manufacturing programming with a 3.6 GHz adder prototype in 65 nm CMOS at 1 V nominal V_{dd}," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, pp. 128–130, Feb. 2018.
- [13] K. Mai, "Post-manufacturing programmable camouflaged logic," *Air Force Research Laboratory*, 2020.
- [14] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptology Conf. Advances in Cryptology (CRYPTO)*, pp. 388–397, Aug. 1999.
- [15] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Berlin, Germany: Springer, 2008.
- [16] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. IEEE Eur. Solid-State Circuits Conf. (ESSCIRC)*, pp. 403–406, Sep. 2002.
- [17] J. Lim, W.-G. Ho, K.-S. Chong, and B.-H. Gwee, "DPA-resistant QDI dual-rail AES S-box based on power-balanced weak-conditioned half-buffer," in *Proc. IEEE Int. Symp. Circuits and Systems (ISCAS)*, pp. 1–4, May 2017.
- [18] S. Lu, Z. Zhang, and M. Papaefthymiou, "A 1.25 pJ/bit 0.048 mm² AES core with DPA Resistance for IoT Devices," *IEEE Asian Solid-State Circuits Conference (A-SSCC)*, pp. 65–68, 2017.
- [19] S. Lu, Z. Zhang, and M. Papaefthymiou, "1.32GHz High-Throughput Charge-Recovery AES Core with Resistance to DPA Attacks," *IEEE Symposium on VLSI Circuits (VLSIC)*, C246 C247, 2015.
- [20] N. E. C. Akkaya, B. Erbagci, R. Carley, and K. Mai, "A DPA-resistant self-timed three-phase dual-rail pre-charge logic family," in *Proc. IEEE Int. Symp. Hardware Oriented Security and Trust (HOST)*, pp. 112–117, May 2015.
- [21] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "A flip-flop for the DPA resistant three-phase dual-rail pre-charge logic family," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 12, pp. 2128–2132, Dec. 2011.
- [22] M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish, "DPA-secured quasi-adiabatic logic (SQAL) for low-power passive RFID tags employing S-boxes," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 62, no. 1, pp. 149–165, Jan. 2018.
- [23] S. D. Kumar, H. Thapliyal, and A. Mohammad, "EE-SPFAL: A novel energy-efficient secure positive feedback adiabatic logic for DPA resistant RFID and smart card," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 2, pp. 281–293, Apr.–Jun. 2016.
- [24] S. D. Kumar, H. Thapliyal, and A. Mohammad, "FinSAL: FinFET-based secure adiabatic logic for energy-efficient and DPA resistant IoT devices," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 37, no. 1, pp. 110–122, Jan. 2018.