A 1.25pJ/bit 0.048mm^2 AES Core with DPA Resistance for IoT Devices

Shengshuo Lu[1], Zhengya Zhang[1], Marios Papaefthymiou[1,2]
[1] University of Michigan, Ann Arbor, MI, USA. [2] University of California, Irvine, CA, USA.

***Abstract*—An AES core designed for low-cost and energy-efficient IoT security applications is fabricated in a 65nm CMOS technology. A novel Dual-Rail Flush Logic (DRFL) with switching-independent power profile is used to yield intrinsic resistance against Differential Power Analysis (DPA) attacks with minimum area and energy consumption. Measurement results show that this 0.048mm^2 core achieves energy consumption as low as 1.25pJ/bit while providing at least 2604x higher DPA resistance over its conventional CMOS counterpart, marking the smallest, most energy-efficient and most secure full-datapath AES core.**

***Keywords*—Advanced Encryption Standard, Differential Power Analysis, Dual-Rail Flush Logic, Instrinsic DPA Resistance.**

I. Introduction

The Advanced Encryption Standard (AES) is a widely-used algorithm for symmetric cryptography. Although AES is extremely difficult to break in theory, AES chips can be subject to side-channel attacks that use information such as the chip's power profile to reveal the secret key stored in the chip. Differential Power Analysis (DPA) is one of the most effective side-channel attacks [1]. In a DPA attack, a switching-dependent power profile of the chip is generated through monitoring its power supply current. This profile is then correlated with a switching behavior model to reveal the secret key [2-5].

Previous AES chips report 66x to 2500x DPA resistance over DPA-unprotected cores [2-5]. One defense mechanism is to augment an unprotected core with countermeasure circuits that scramble its supply voltage and current [2, 3]. This approach is not amenable to voltage scaling, however, because the scrambled supply voltage is limited to a certain minimum level, and no work reports on its performance under voltage scaling. Another defense is to use intrinsically DPA-resistant logic gates that exhibit constant energy consumption during operation and hide the impact of switching activity from the power trace [4, 5]. This approach typically suffers from high area overheads.

This paper presents a voltage-scalable full-datapath 128-bit AES chip with intrinsic DPA resistance that is suitable for Internet-of-Things (IoT) applications thanks to its energy-efficient operation and small die area. Compared to previous DPA-protected cores [2-5], this chip is the smallest, most energy-efficient, and most DPA-resistant.

This work was supported in part by NSF under grants No. CCF 1320027 and No. CCF 1161505.

II. Dual-Rail Flush Logic and Architecture

Logic gates designed to be intrinsically DPA-resistant have the potential to provide superior resilience to DPA attacks. However, published designs fall short of fulfilling this potential while at the same time suffering from 2x to 4x high area overheads [4, 5]. This paper proposes Dual-Rail Flush Logic (DRFL), a logic family whose gate structure and architecture are designed and optimized to achieve a switching-independent energy profile. With balanced gate topology and pipeline flushing mechanism, DRFL provides robust and intrinsic resistance to DPA attacks with minimal area overhead.

DRFL is a derivative of static dual-rail CMOS logic [6]. Fig. 1 shows a DRFL XOR gate. When inputs A (A_b) and B (B_b) present valid complementary logic values, the gate is in evaluation mode, and output Y (Y_b) presents valid complementary values. When all inputs are set to the same value, the gate is in precharge mode, and both outputs present the opposite values. During consecutive cycles in its operation, the gate alternates between evaluation mode and precharge mode. For example, when the XOR gate in Fig. 1 changes from precharge mode to evaluation mode, one of the outputs goes high, with the other output remaining low, depending on the input values. When the gate changes from evaluation mode back to precharge mode, the high output node is discharged low, and the gate consumes the same amount of energy as during evaluation. Therefore, irrespective of input values, the energy consumption of each individual DRFL gate remains the same throughout its operation.

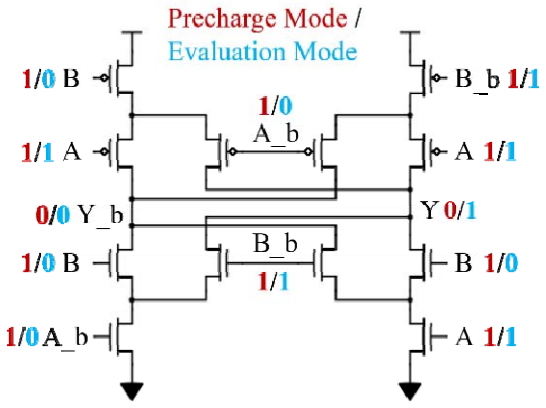

Fig. 1. DRFL XOR gate. Input and output values are shown for precharge and evaluation mode.

One of the advantages of static dual-rail gate is that it fully utilizes the benefit of complementary inputs, yielding intrinsic DPA resistance with only modest area overheads over static CMOS. For example, a relatively complex function like XOR, which is the function used most often in AES, requires 10 transistors when implemented as a single-rail static CMOS gate. A dual-rail implementation of XOR uses 12 transistors by sharing transistors in the pull-up and pull-down branches as shown in Fig. 1, only incurring a 20% overhead. In general, as functions become more complex, more transistor sharing is possible, and dual-rail implementations use much less than twice as many devices as their single-rail counterparts. For this reason, DRFL designs eventually achieve much better area efficiency than other intrinsic solutions [4, 5]. The area of the DRFL AES core in this paper is only 50% higher than its CMOS counterpart. By comparison, the WDDL-based design in [5] has 4x the area of its CMOS counterpart, because it uses CMOS gates and inverters to mimic the functionality of dual-rail logic gate. The BBL-based design in [4] has twice the area of its CMOS counterpart, because each BBL gate has a boost structure for charge recovery.

In addition to balanced gate design, pipeline flushing is essential for DRFL to achieve superior DPA resistance. To ensure correct operation and pipeline flushing, in cascades of DRFL gates, adjacent gates precharge to opposite values, as shown in Fig. 2, with the gates precharging to 1/0 denoted as P/N gates. P gates must connect to N gates, and N gates must connect to P gates. To that end, buffers must be inserted as necessary to balance paths and ensure the proper polarity of connected gates. Due to the regular and balanced topology of the AES datapath, the number of balancing buffers is relatively small. Moreover, unlike WDDL [5], which introduces two inverters at the output of each gate, DRFL avoids inverters thanks to the alternating P/N architecture, eliminating the area and energy consumption overhead associated with inverters and offsetting in part the buffer overheads.

After each pipeline stage, a pair of CMOS flip-flops is used to store logic values. Each flip-flop pair alternates between precharge mode (both flip-flops store the same value) and evaluation mode (flip-flops store complementary values). Hence, the flip-flops consume the same amount of energy when alternating between precharge and evaluation, ensuring switching-independent energy consumption.

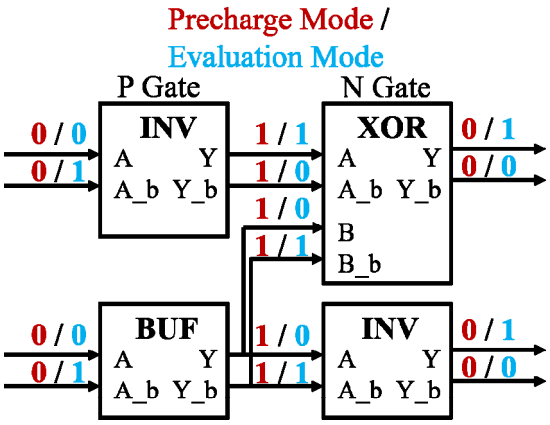

Fig. 2. Cascade of DRFL gates.

In DRFL pipelines, evaluation data and precharge data propagate in an interleaved manner, as shown in Fig. 3. During consecutive cycles, each pipeline stage alternates between evaluation mode and precharge mode.

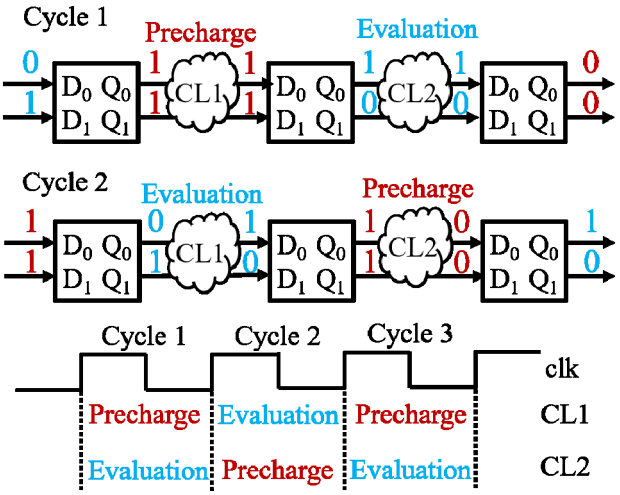

Fig. 3. Pipeline of DRFL gates, and interleaving of precharge and evaluation mode.

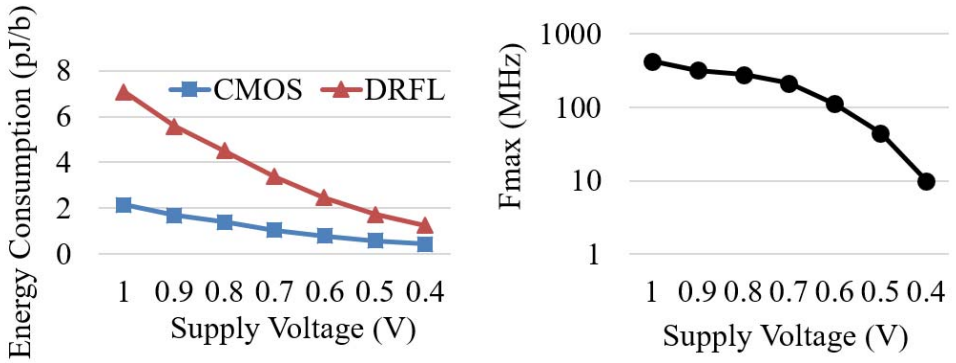

Fig. 4. Measured frequency vs. supply voltage.

III. Experimental Evaluation

The DPA-resistant AES core has been fabricated in a 65nm CMOS process. Its standard CMOS counterpart has been included on the same die. The two cores have the same RTL specification from [7], architecture, and target frequency.

Leveraging its CMOS underpinnings, the DRFL core functions correctly across a wide voltage range, as shown in Fig. 4. At the nominal supply of 1V, the core achieves a clock frequency of 430MHz and consumes 7.09pJ/bit. With a near-threshold supply of 0.4V, the core operates at 10MHz and consumes 1.25pJ/bit.

DPA attacks are performed on both cores at the nominal voltage, the weakest operating point for DPA attacks. (As energy consumption decreases with voltage scaling, the chip's power profile is masked by noise, and DPA attacks require more traces [8].) Fig. 5 shows Measurements to Disclosure (MTD) for the standard CMOS core. MTD of a byte in the key is the number of measurements needed for the correlation of the correct key value to surpass the correlation of all other 255 values [2]. In the CMOS core, the key byte that requires the least number of power traces to be disclosed (a.k.a. the 1st key byte) is revealed relatively soon, as its correlation crosses the maximum correlation among all other 255 values after 768 measurements and continues to increase with the number of measurements. Fig. 6 illustrates the hardness of disclosing the key in the DRFL core. Even after 2 million measurements, the normalized correlation value of the correct key remains relatively stable and is indistinguishable from the other key hypotheses.

Measurement results from the two cores are illustrated in Table I. Both cores attain a maximum frequency of 430MHz at the nominal 1V supply level. The DRFL core has half the throughput of its CMOS counterpart, since its pipelines are in precharge mode every other cycle. The DRFL core is 50% larger than the CMOS core, due to the overheads of dual-rail logic and balancing buffers. Measured at 1V and 0.4V, the DRFL core consumes 2.3x and 1.8x more energy, respectively, than the CMOS core. However, the DRFL core exhibits at least 2604x higher DPA resistance than the CMOS core. Die photo of the two cores is shown in Fig. 7.

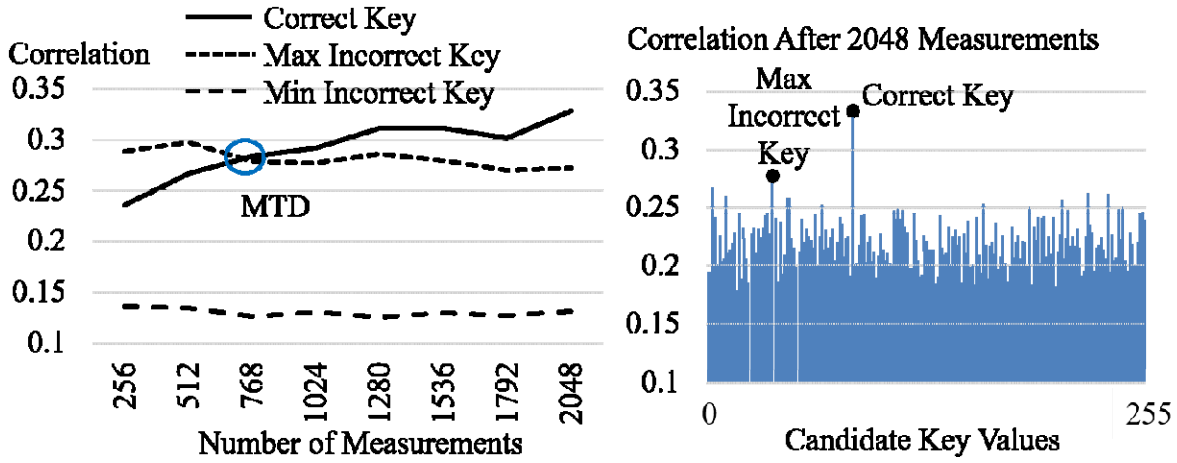

Fig. 5. DPA attack on standard CMOS AES.

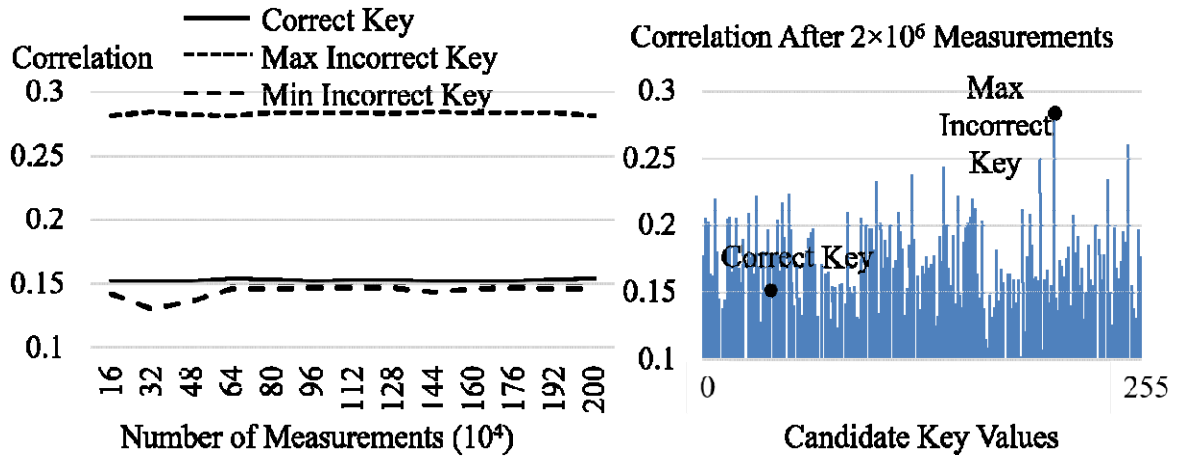

Fig. 6. DPA attack on DRFL AES core.

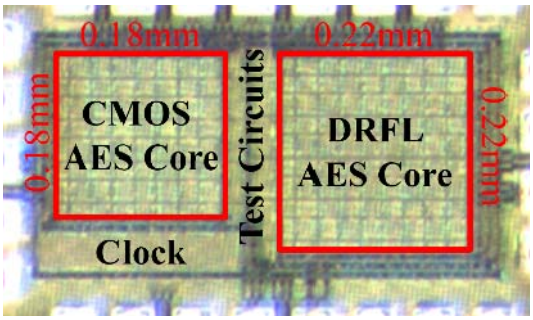

Fig. 7. Die photo.

Table II compares the area, performance, energy efficiency, and DPA resistance of the DRFL core and other published AES cores [2-5, 9]. The designs in [2-5] are DPA resistant with MTD of 1st key byte ranging from 66x to 2500x compared to an unprotected AES core. The design in [9] achieves superior throughput and energy efficiency, but is not DPA resistant. Consuming 1.25pJ/bit, the 0.048mm^2 DRFL core achieves superior balance between area, energy efficiency and DPA resistance.

TABLE I. DRFL AND CMOS DESIGNS CHARACTERISTICS

	DRFL		CMOS	
Technology	65nm			
Area (mm^2)	0.048		0.032	
Supply Voltage (V)	1.0	0.4	1.0	0.4
Frequency (MHz)	430	10	430	10
Throughput (Gb/s)	2.752	0.064	5.504	0.128
Power (mW)	19.5	0.080	11.8	0.056
Energy Efficiency (pJ/b)	7.09	1.25	2.14	0.44
DPA resistance	2×10^6 measurements without cracking any key		768 measurements to disclosure of first key byte	
Key bytes disclosed (out of 16 keys bytes)	0		16	
DPA resistance comparison	At least 2604x			

TABLE II. COMPARISON WITH PREVIOUSLY PUBLISHED AES CHIPS.

	DRFL		[2]	[3]	[4]	[5]	[9]	
Technology	65nm		130nm	90nm	65nm	180nm	45nm	
Area(mm^2)	0.048		0.364	0.104	0.291	2.45	0.026	
Supply Voltage (V)	1	0.4	1.2	1	0.41	1.8	1.1	0.36
Maximum Frequency (MHz)	430	10	110	255	1320	85.5	2100	Not reported
Maximum Throughput (Gb/s)	2.752	0.064	1.28	2.97	16.9	0.99	26.5	Not reported
Power (mW)	19.5	0.08	44.34 (100MHz)	7.10 (200MHz)	98	200 (50MHz)	62.5	Not reported
Energy Efficiency (pJ/b)	7.09	1.25	38.10	3.04	5.79	345	2.358	0.455
DPA Resistance	2604x		2500x	1086x	720x	66x	DPA unprotected	

REFERENCES

[1] Kocher, Paul, Joshua Jaffe, and Benjamin Jun. "Differential power analysis." In Annual International Cryptology Conference, pp. 388-397. Springer Berlin Heidelberg, 1999.

[2] Tokunaga, Carlos, and David Blaauw. "Secure AES engine with a local switched-capacitor current equalizer." In International Solid-State Circuits Conference-Digest of Technical Papers, pp. 64-65. IEEE, 2009.

[3] Liu, Po-Chun, Ju-Hung Hsiao, Hsie-Chia Chang, and Chen-Yi Lee. "A 2.97 Gb/s DPA-resistant AES engine with self-generated random sequence." In ESSCIRC, 2011 Proceedings of the, pp. 71-74. IEEE, 2011.

[4] Lu, Shengshuo, Zhengya Zhang, and Marios Papaefthymiou. "1.32 GHz high-throughput charge-recovery AES core with resistance to DPA attacks." In VLSI Circuits, 2015 Symposium on, pp. C246-C247. IEEE, 2015.

[5] Hwang, David D., Kris Tiri, Alireza Hodjat, B-C. Lai, Shenglin Yang, Patrick Schaumont, and Ingrid Verbauwhede. "AES-Based Security Coprocessor IC in 0.18um CMOS With Resistance to Differential Power Analysis Side-Channel Attacks." IEEE Journal of Solid-State Circuits 41, no. 4 (2006): 781-792.

[6] Weste, N. H. E., and D. Harris. "Array subsystems." CMOS VLSI design: a circuits and systems perspective (4th edition)(M. Goldstein and M. Suarez-Rivas, eds.) (2011).

[7] Canright, David. "A very compact S-box for AES." In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 441-455. Springer Berlin Heidelberg, 2005.

[8] Haider, Syed Imtiaz, and Leyla Nazhandali. "Utilizing sub-threshold technology for the creation of secure circuits." In International Symposium on Circuits and Systems, pp. 3182-3185. IEEE, 2008.

[9] Mathew, Sanu K., Farhana Sheikh, Michael Kounavis, Shay Gueron, Amit Agarwal, Steven K. Hsu, Himanshu Kaul, Mark A. Anders, and Ram K. Krishnamurthy. "53 Gbps Native GF(2^4)^2 Composite-Field AES-Encrypt/Decrypt Accelerator for Content-Protection in 45 nm High-Performance Microprocessors." IEEE Journal of Solid-State Circuits 46, no. 4 (2011): 767-776.