AES-Based Cryptographic and Biometric Security Coprocessor IC in 0.18-µm CMOS Resistant to Side-Channel Power Analysis Attacks

Kris Tiri, David D. Hwang, Alireza Hodjat, Bo-Cheng Lai, Shenglin Yang,
Patrick Schaumont, and Ingrid Verbauwhede

Electrical Engineering Department
University of California, Los Angeles, CA, 90095
{tiri, dhwang, ahodjat, bclai, shengliny, schaum, ingrid}@ee.ucla.edu

Abstract

This paper describes an embedded security coprocessor that consists of four components: an Advanced Encryption Standard (AES) based cryptographic engine, a fingerprint matching oracle, template storage, and an interface unit. Two functionally-identical coprocessors are fabricated using a TSMC 6M 0.18-µm process. The first coprocessor uses standard cells and encrypts at 3.84 Gb/s. The second coprocessor uses Wave Dynamic Differential Logic (WDDL) combined with differential routing to combat side-channel information leakage through power analysis attacks. It encrypts at 0.99 Gb/s. The coprocessor is part of a security-partitioned embedded system called ThumbPod.

Keywords: Advanced Encryption Standard (AES), cryptography, differential power analysis, coprocessor, biometrics.

Introduction

In recent years, the integrated circuit has emerged as a weak link in embedded security applications. The IC broadcasts information that is related to the secret key being used in the encryption operation. Several attacks have been reported that use information such as power consumption, time delay, and electromagnetic radiation to find the secret key. These side-channel attacks (SCAs) are a real threat for any device in which the security IC is easily observable, such as smart cards and other embedded devices [1],[2]. As an example of the potency of SCAs, Schneier wrote in 1998 that there is not enough silicon in the galaxy or enough time before the sun burns out to perform a brute-force attack (trying all possible keys) on the 3-DES cipher with a 112-b key [3]. With the differential power analysis (DPA) side-channel attack, however, we were able to find the key of a standard cell IC AES implementation with a 128-b key in less than three minutes with standard laboratory equipment. Clearly, SCAs pose serious concerns for the embedded IC security community.

There are two steps required to secure an embedded system from such side-channel attacks. The first step is security partitioning, in which an embedded system is partitioned into two parts: a secure and an insecure module. Such partitioning ensures that the processing and storage of non-sensitive information is done on the insecure module, and the processing and storage of all sensitive information is done on the secure module. The second step is to use circuit and physical techniques to combat side-channel attacks on the secure module only. Though such techniques require considerable overhead in terms of area and power, due to security partitioning only the secure module must be protected for the system to remain secure, thus minimizing such overhead.

We have designed such a partitioned secure embedded system called ThumbPod, which is used for biometric and cryptographic embedded authentication, as shown in Fig. 1. Security partitioning has been performed to divide the system into an insecure module (an FPGA LEON 32-b RISC processor) and a secure module (a coprocessor IC).

This paper discusses the secure coprocessor IC. The coprocessor consists of four components: an Advanced Encryption Standard (AES) based cryptographic engine, fingerprint matching oracle, template storage, and an interface unit.

Two functionally-identical coprocessors were fabricated on the same die using a TSMC 6M 0.18-µm process. The first coprocessor was implemented using standard cells and regular routing techniques. The second coprocessor was implemented using a logic style called Wave Dynamic Digital Logic (WDDL) and a layout technique called differential routing to combat side-channel power analysis attacks. We fabricated two functionally-identical coprocessors to allow us to compare the side-channel resistance of a typical IC versus one with special circuit techniques.

The remainder of this paper is as follows. The next section describes the IC system architecture. The third section describes power analysis countermeasures. Subsequently, area, timing and power numbers are presented together with the power attack resistance. Finally related state-of-the-art and a conclusion are presented.

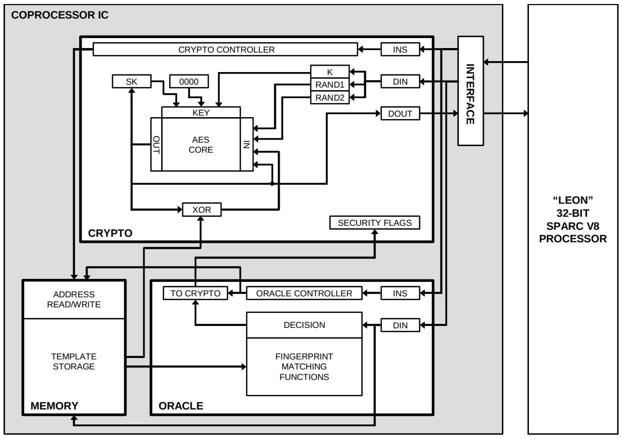

Fig. 1. ThumbPod system architecture (fabricated IC is shaded).

IC System Architecture

The section of the paper describes the four components of the coprocessor IC as shown in Fig. 1: an Advanced Encryption Standard (AES) based cryptographic engine, fingerprint matching oracle, template memory, and an interface unit.

The cryptographic engine consists of the AES core in Fig. 2 together with a controller, registers, and an interface to read/hash the memory. The datapath is based on one round of the AES-128 algorithm along with on-the-fly key scheduling. The AES core is optimized for speed, with a goal of minimizing delay for one round. A full encryption of 128-b data using a 128-b key takes a total of 11 cycles. The crypto engine performs AES encryption in ECB (Electronic CodeBook), OFB (Output FeedBack), and CBC-MAC (Cipher Block Chaining Message Authentication Code) modes without any loss in throughput.

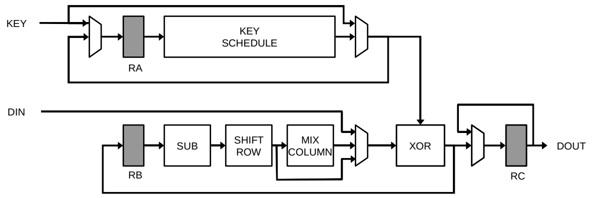

Fig. 2. Architecture of the AES core.

A neighbor-based fingerprint matching algorithm is performed on the oracle. The feature extraction of a candidate fingerprint is done on the LEON, which then sends the oracle a fixed number of queries, each query consisting of an angle value, distance to neighbor, angle to neighbor, and angle of neighbor along with indexing terms. At each query, the oracle loads a section of the pre-stored template and implements correlation functions. After the final query, the oracle makes a final accept/reject decision that is passed to the cryptographic engine as a security flag. To prevent adaptive query attacks, the oracle does not provide intermediate feedback to the LEON during the query phase, hence its name. The matching oracle algorithm has a false accept rate (FAR) of 0.01% and a false reject rate (FRR) of 1.5%.

The register file for the storage of the fingerprint template can store up to 30 minutiae of 119 bits each. Each minutia consists of its own angle value (5-b) and information for six minutiae neighbors: distance to neighbor (8-b), angle to neighbor (6-b), and angle of neighbor (5-b). The maximum secure storage size of a template is 3570 bits.

The interface unit allows access to the IC by means of a 20-b instruction/data input bus and a 17-b output bus. The unit uses pipelined registers with logic gates to ensure stable data processing with one- or two-sided handshaking protocols. The coprocessor can operate with a 50 MHz processor within a range of clock frequencies from 1 MHz to 288 MHz.

Differential Power Analysis Countermeasures

Of all side-channel attacks, differential power analysis is a SCA of particular concern as it is very effective in finding a secret key. The attack is based on the fact that logic operations in standard static CMOS have power characteristics that depend on the input data. Power is only drawn from the power supply when a 0 to 1 output transition occurs. (During 0 to 0 and 1 to 1 transitions, no power is drawn. During a 1 to 0 transition, the stored capacitance is discharged to ground.) Therefore, by measuring the power supply of an IC as it encrypts, and then performing statistical analysis of the measured power traces, the secret key can be determined. DPA has been proven effective in extracting the key of both microprocessor-based and ASIC-based encryption systems.

To combat DPA, this paper presents a technique which provides a constant power dissipating logic: in one clock cycle the power consumption of each individual logic gate is constant and independent of its input signals. In other words, 0 to 0, 0 to 1, 1 to 0, and 1 to 1 output transitions all draw the same power from the supply. The major advantages of employing a constant power dissipating logic style are that this approach is a distributed countermeasure, is correct by construction, and is independent of the cryptographic algorithm or arithmetic implemented. Two conditions must be satisfied to have constant power dissipating logic: a logic gate must have exactly one charging event per clock cycle; and the logic gate must charge a constant capacitance in that event.

Dynamic differential logic, also known as dual rail with precharge logic, has a single charging event per cycle. The fabricated IC uses Wave Dynamic Differential Logic [4], depicted in Fig. 3, to implement dynamic differential behavior using static CMOS standard cells.

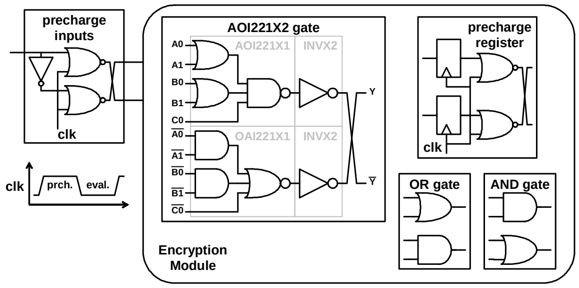

Fig. 3. Wave dynamic differential logic (WDDL).

A WDDL gate consists of a parallel combination of two positive complementary gates. In the precharge phase, both true and false inputs are set to 0. This puts the output of the gate at 0. This 0 precharge value travels as the input to the next gate, creating a precharge “wave”. In the evaluation phase, each input signal is differential and the WDDL gate calculates a differential output. Fig. 3 shows the composition of the WDDL AOI221 gate with drive strength 2. Special registers and input converters, shown in Fig. 3, launch the precharge value. They produce an all-zero output in the precharge phase (clk-signal high) but let the differential signal through during the evaluation phase (clk-signal low).

Besides a 100% switching factor, it is essential that a fixed amount of capacitance is charged during the transition. Thus, the total load at the true output of the differential gate should match the total load at the false output. The load capacitance has three main components: the intrinsic output capacitance of the gate, the interconnect capacitance, and the intrinsic input capacitance of the load. For high security applications, the contribution of all components must be constant. However, as the channel-length of transistors shrinks the interconnect capacitances become the dominant capacitance [5]. Hence, the issue of matching the interconnect capacitances of the signal wires is crucial.

The best strategy to achieve matched interconnect capacitances is to route the true and false output signals with parallel routes that are at all times in adjacent tracks of the routing grid, on the same layers, and of the same length [6]. Then independent of the placement, the two routes have the same first order parasitic effects. We forced the place & route tool to route all true and false signals at all times in adjacent tracks by the following method. Each differential output pair is abstracted as a single “fat” wire, which has the width of 2 parallel wires plus spacing. The design is routed with the fat wire and at the end the fat wire is decomposed into the differential wires. Fig. 4 demonstrates the place & route approach.

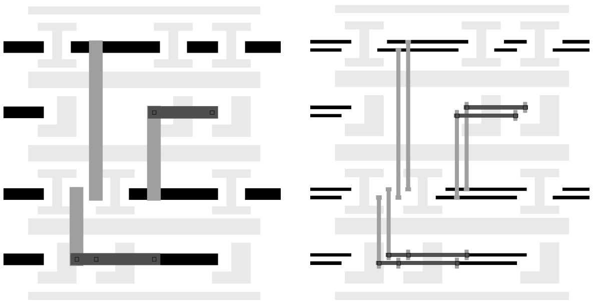

Fig. 4. Place & route approach: fat design (left); and differential design (right).

Results

The prototype IC consists of two functionally-identical coprocessors fabricated on the same die. An *insecure* coprocessor is implemented using standard cells and regular routing techniques. A *secure* coprocessor is implemented using WDDL and differential routing. Both coprocessors have been implemented starting from the same synthesized gate level netlist. The WDDL gates have been derived from the commercial 0.18μm, 1.8V static CMOS standard cell library used in the regular insecure design.

Fig. 5 shows the encryption start signal and the supply current of the coprocessors in OFB mode. The supply current of the insecure coprocessor exhibits large variations. It broadcasts the eleven encryption rounds. The high power peak at the starting point of each new encryption can be used as a synchronization signal. The power consumption profile of the secure implementation on the other hand is invariant and does not reveal any information in a simple power analysis. In each clock cycle, the same total load capacitance is charged.

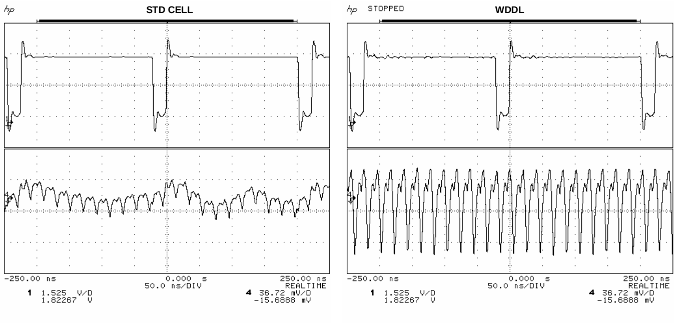

Fig. 5. Transient measurement (2 encryptions; 22 clock cycles) of encryption start signal (top) and core supply current (bottom).

We performed DPA on each coprocessor as it executed AES, measuring 15,000 and 1,500,000 supply current acquisitions for the standard cell and WDDL coprocessors, respectively. In other words, we performed 15,000 encryptions on the standard cell coprocessor using the same key (with different inputs) while measuring the current fluctuations from the power supply. Using these current fluctuations we performed the correlation DPA attack. With WDDL, we performed 1.5 million encryptions.

The resistance against DPA is quantified with the number of measurements to disclosure (MTD), which is the cross-over point between the correlation coefficient of the correct key and the maximum correlation coefficient of all the wrong keys guesses. For both coprocessors, an attack on one key byte is shown in Fig. 6. MTD is shown in the “Correlation vs. Number of Measurements” graphs as the point where the black line crosses the grey envelope. Though only one of the sixteen key-bytes (128-b key = 16 key bytes) is shown, the results for the other fifteen key bytes are similar.

For the insecure coprocessor, 2,000 measurements are on average required to disclose a secret key byte. For one of the sixteen key bytes, a mere 320 samples are sufficient to mount a successful attack. As seen on Fig. 6, the peaks of the correlation graphs are large. There is no doubt about the correct key byte. For the secure coprocessor, on the other hand, our measurements show that out of sixteen keys bytes, WDDL effectively protects five key bytes. One and a half million measurements are not sufficient to disclose these five key bytes; one example is shown on the bottom of Fig. 6. The eleven key bytes that have been found required on average 255,000 measurements. The improvement in DPA resistance makes the at-

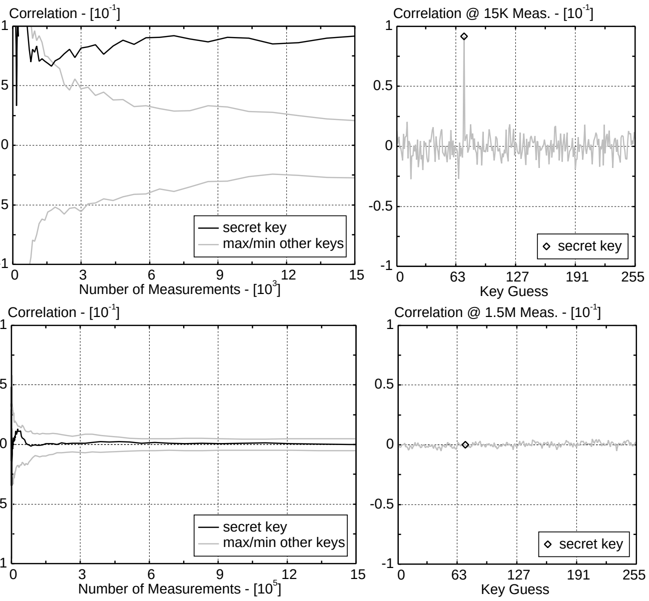

Fig. 6. Cracking the secret key with differential power analysis: Standard cells and regular routing using 15K measurements (top); and WDDL and differential routing using 1.5M measurements (bottom).

tack de facto infeasible. The required number of measurements is larger than the lifetime of the secret key in most practical systems.

The analysis also showed that for a dual rail design, the correlation coefficient of the correct key guess can be negative. This means that the more bits change the less power is consumed. This actually means that the 0 to 1 switching of the false net uses more power than the 0 to 1 switching of the true net. The parasitic capacitances affected by the false signals are larger than the ones affected by the true signals. On the other hand, for the five bytes that have not been found, the capacitances have an almost perfect matching between the differential nets. Hence it is crucial to guarantee matched capacitances consistently for all the logic. Matching can be improved by shielding the differential routes on either side with a power line to eliminate cross-talk effects. Alternatively, increasing the distance between different differential pairs would reduce the effect, or an improved iterative design flow could be used to identify and correct mismatches.

Table I summarizes the results of the fabricated IC, whose micrograph is in Fig. 7. The standard cell coprocessor has 199 Kgates with an area of 1.98-mm^2 (0.79-mm^2 for AES). The AES can operate at 330-MHz for a 3.84 Gb/s encryption rate. As far as we know, this is the fastest non-pipelined AES encryption rate published in silicon. At 50 MHz, power consumption results for the AES and full system architecture are 0.054 W and 0.036 W, respectively.

The WDDL coprocessor has 596 Kgates with an area of 5.95-mm^2 (2.45-mm^2 for AES). The AES can operate at 85.5 MHz for a 0.99 Gb/s encryption rate. For WDDL at 50 MHz, power consumption results are 0.200 W and 0.486 W for the AES and full system architecture, respectively.

TABLE I. IC RESULTS SUMMARY

Parameter	Standard Cell	WDDL
Gate Count (eq. gates) [K]	199	596
Area [mm^2]		
AES	0.79	2.45
Oracle	0.11	0.26
Memory	1.05	3.21
Entire System	1.98	5.95
Maximum Frequency (@1.8V) [MHz]		
AES	330.0	85.5^{*}
Entire System	288.2	69.0^{*}
Maximum Throughput (@1.8V) [Gb/s]		
AES	3.84	0.99
Power Consumption (@1.8V, 50 MHz) [W]		
AES	0.054	$0.200^{\dagger}$
Entire System	0.036	0.486
Measurements to Disclosure		
min – mean – max‡	320 – 2,133 – 8,168	21,185 – 255,391 – 1,276,186
Key bytes not found (@1.5M Meas.)	n/a	5

*Duty factor of clock > 50% to guarantee precharge of all gates
†Estimation based on area ratio AES vs. Entire System
‡Based on correctly guessed key bytes

Related Work

As far as we know, this paper reports the first DPA-resistant circuit-plus-routing technique implemented and tested in actual silicon. [8] presents a dual-rail asynchronous technique in silicon, but does not use differential routing for matched capacitances. We are aware of one silicon implementation of an algorithmic countermeasure [9]. Measurements and assessment of the DPA resistance, however, have not yet been performed.

Conclusions

WDDL and differential routing is a functioning technique to thwart power attacks. Experimental results showed that 1,500,000 acquisitions are not sufficient to fully disclose the 128-b secret key. The trade-off is a three times increase in area, and a four times increase in power consumption and minimum clock period. Security partitioning [7] minimizes the cost for complex systems. Even with the penalties, the secure coprocessor still runs orders of magnitude faster and expends less energy than a software implementation on the main processor.

Acknowledgements

This work was supported in part by the National Science Foundation (CCR-0098361), UC-Micro 02-079, Panasonic Foundation, SUN Microsystems, Atmel Corporation and the Fannie and John Hertz Foundation (DH).

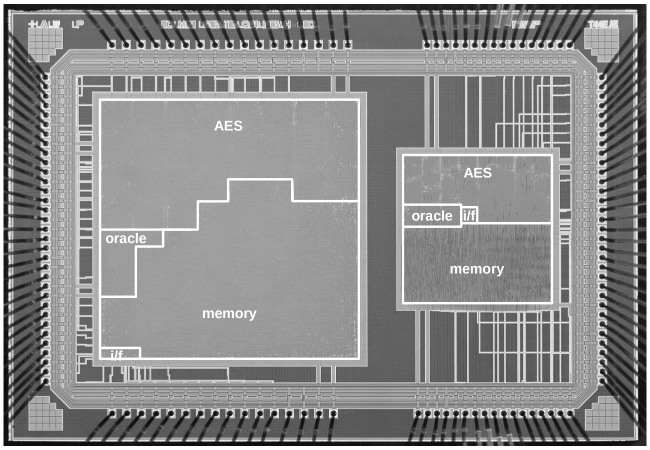

Fig. 7. IC micrograph.

References

[1] M. Renaudin, F. Bouesse, P. Proust, J. Tual, L. Sourgen and F. Germain, “High Security Smart-cards,” *DATE*, pp. 228-233, 2004.

[2] P. Kocher, R. Lee, G. McGraw, A. Raghunathan and S. Ravi, “Security as a New Dimension in Embedded System Design,” *DAC*, pp. 753-760, 2004.

[3] B. Schneier, “A Hardware DES Cracker,” Crypto-Gram Newsletter, http://www.schneier.com/crypto-gram-9808.html#descracker, August 1998.

[4] K. Tiri and I. Verbauwhede, “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” *DATE*, pp. 246-251, 2004.

[5] ITRS, “Interconnect,” International Technology Roadmap for Semiconductors, http://public.itrs.net/Files/2003ITRS/Interconnect2003.pdf, 2003.

[6] K. Tiri and I. Verbauwhede, “Place and Route for Secure Standard Cell Design,” *CARDIS*, pp. 143-158, 2004.

[7] D. Hwang, P. Schaumont, K. Tiri and I. Verbauwhede, “Making Embedded Systems Secure,” submitted *IEEE Security & Privacy Magazine*.

[8] J. Fournier, S. Moore, H. Li, R. Mullins and G. Taylor, "Security Evaluation of Asynchronous Circuits," *CHES*, pp. 137-151, 2003.

[9] N. Pramstaller, F. Gürkaynak, S. Häne, H. Kaeslin, N. Felber, and W. Fichtner, “Towards an AES Crypto-chip Resistant to Differential Power Analysis,” *ESSCIRC*, pp. 307-310, 2004.