A Side-Channel Leakage Free Coprocessor IC in 0.18µm CMOS for Embedded AES-based Cryptographic and Biometric Processing

K. Tiri[1], D. Hwang[1], A. Hodjat[1], B. Lai[1], S. Yang[1], P. Schaumont[1], I. Verbauwhede[1,2]
{tiri,dhwang,ahodjat,bclai,shengliny,schaum,ingrid}@ee.ucla.edu

[1]Electrical Engineering Dept.
UC Los Angeles, USA

[2]Dept. ESAT/SCD-COSIC
K.U.Leuven, Belgium

ABSTRACT

Security ICs are vulnerable to side-channel attacks (SCAs) that find the secret key by monitoring the power consumption and other information that is leaked by the switching behavior of digital CMOS gates. This paper describes a side-channel attack resistant coprocessor IC and its design techniques. The IC has been fabricated in 0.18µm CMOS. The coprocessor, which is used for embedded cryptographic and biometric processing, consists of four components: an Advanced Encryption Standard (AES) based cryptographic engine, a fingerprint-matching oracle, a template storage, and an interface unit. Two functionally identical coprocessors have been fabricated on the same die. The first, 'secure', coprocessor is implemented using a logic style called Wave Dynamic Digital Logic (WDDL) and a layout technique called differential routing. The second, 'insecure', coprocessor is implemented using regular standard cells and regular routing techniques. Measurement-based experimental results show that a differential power analysis (DPA) attack on the insecure coprocessor requires only 8,000 acquisitions to disclose the entire 128b secret key. The same attack on the secure coprocessor still does not disclose the entire secret key at 1,500,000 acquisitions. This improvement in DPA resistance of at least 2 orders of magnitude makes the attack de facto infeasible. The required number of measurements is larger than the lifetime of the secret key in most practical systems.

Categories and Subject Descriptors

B.7 [**Hardware**]: Integrated Circuits; E.3 [**Data**]: Data encryption.

General Terms

Design, Security.

Keywords

Countermeasure, Side-Channel Attack, Differential Power Analysis, Encryption, Smart Card, Security IC.

DAC 2005, June 13–17, 2005, Anaheim, California, USA.

1. INTRODUCTION

The integrated circuit is the emerging vulnerability in the security of an embedded application. Due to physical and electrical effects, the IC broadcasts information that is related to the secret key used in the encryption operation. In recent years, several attacks have been reported that use information from so-called side-channels to find the secret key. These side-channel attacks are non-invasive and observe the device under normal operation. They analyze information ranging from time delay and power consumption to electromagnetic radiation. SCAs are a real threat for any device in which the security IC is easily observable, such as smart cards and embedded devices [1],[2].

Side-channel attacks are not a new practice. One of the most well-known examples is a safecracker who uses his fingers and ears to feel and listen to the tumblers impacting each other while turning the dial. By observing when the lock's tumblers fall into place, he can crack the combination lock quickly and much faster than anyone who attempts to open the safe by trying every possible combination.

In electronic circuits, the variations in power consumption can be used as the equivalent of the falling tumblers in a lock. The effect on the circuit's secure operation is devastating. For example, a brute force attack on the AES algorithm, in which you try each and every possible value of the 128b key, is impossible with today's technology. With the differential power analysis attack, however, we have been able to find the key of the unprotected coprocessor in less than three minutes, from the start of the measurements to the end of the analysis. It shows that security is only as strong as its weakest link.

Constant power consuming logic gates are used to protect ThumbPod, a next-generation portable biometric and cryptographic authentication device, against power analyses. When the power consumption of the smallest building block is a constant and independent of the signal activity, no information is leaked through the power supply and power attacks are impossible. To minimize the area and power overhead, only the sensitive parts of the embedded system are adjusted. Architectural partitioning has been performed to divide the system into an insensitive and a sensitive module.

The remainder of the paper is organized as follows. The next section describes the IC system architecture. It discusses (1) the Thumbpod architecture; (2) the AES-based cryptographic engine; (3) the reference template storage; (4) the fingerprint matching

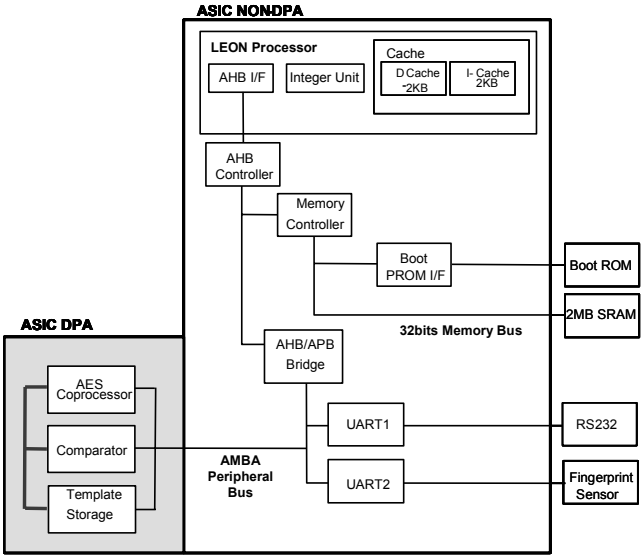

Figure 1. System block diagram (fabricated IC is shaded).

algorithm; (5) the coprocessor interface; and (6) the build-in self test and functional tests. Section 3 describes the DPA countermeasure. It discusses (1) a methodology to achieve a 100% switching factor with standard single ended static complementary CMOS gates; and (2) a place & route methodology to control the parasitic effects on the interconnect wires for constant load capacitance. In section 4, the concept of a DPA is explained together with our measurement setup and an attack is mounted on the fabricated IC to asses the increase in DPA resistance of the secure coprocessor. This section also presents area, timing and power numbers. Section 5 presents related state-of-the-art.

2. IC SYSTEM ARCHITECTURE

2.1 ThumbPod embedded system architecture

The coprocessor is part of the embedded system (ThumbPod) in Figure 1, which is a portable biometric and cryptographic authentication device. ThumbPod is a biometrically-driven electronic key that establishes a strong and secure bond between the owner of the key and the key itself. ThumbPod scans a person's fingerprint, analyzes the spatial features of the fingerprint, compares them to a prestored template and generates a positive or negative authentication. It also implements a variety of AES-based symmetry key cryptography primitives for secure interaction with a remote server.

Architectural partitioning has been performed to divide the system into insecure (LEON SPARC V8 processor) and secure (coprocessor) modules, such that the processing and storage of all sensitive information is done on the secure module. This ensures that the entire system does not need to be protected by the circuit techniques described here, which require additional power and area. Only the secure module must be protected for the system to remain secure, thus minimizing such overhead.

2.2 AES-based cryptographic engine

The cryptographic engine consists of an AES core with multiple modes of operation, along with a controller, registers, and an interface to read/hash the memory. The datapath is based on one round of the AES-128 algorithm which consists of byte substitution, shift row, mix column, and key addition phases along with on-the-fly key scheduling in Figure 2. The core is optimized for speed, with a goal of minimizing delay for one round. Byte substitution is implemented using look-up tables. A full encryption of 128b data using a 128b 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.

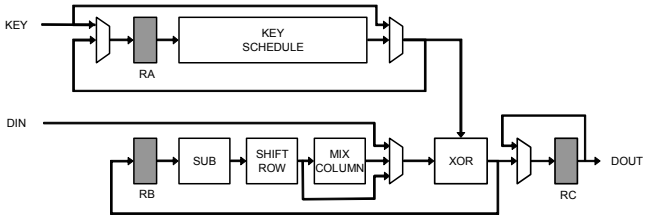

Figure 2. Architecture of AES core.

2.3 Reference template storage

The storage of a fingerprint template is performed as a two-module register file, allowing storage of a single template with up to 30 minutiae, each of 119b and consisting of its own angle value (5b) and information for six minutiae neighbors: distance to neighbor (8b), angle to neighbor (6b), and angle of neighbor (5b). The maximum size of a template is thus 3570b.

2.4 Oracle: fingerprint matching algorithm

A neighbor-based fingerprint matching algorithm is performed on the oracle. To prevent adaptive query attacks, the oracle does not provide intermediate feedback to the LEON during the query phase, hence its name. 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. The matching oracle algorithm has a false accept rate (FAR) of 0.01% and a false reject rate (FRR) of 1.5%.

2.5 Coprocessor interface and secure controllers

The interface unit allows access to the IC by means of a 20b instruction/data input bus and a 17b 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 50MHz LEON within a range of clock frequencies from 1MHz to 288MHz. The coprocessor contains two controllers, one each for the cryptographic engine and the oracle. These controllers are programmed with a fixed instruction set and are able to communicate with each other using a set of security flags (a set of registers shared between them.) Different biometric authentication protocols involving both encryption and matching functions can thus be implemented. Security is provided by monitoring the proper sequence of instructions and rejecting invalid instructions.

For example, a protocol requires an encryption operation only after a fingerprint match has been made. If an encryption instruction arrives either before a match or after a rejection, the cryptographic engine will generate a false encryption token indicating an illegal query.

2.6 Built-in self test (BIST) and functional test

BIST was implemented on the AES portion of the device both in hardware and software modes. In hardware, a BIST_ENABLE pin can be set, which feeds a hardwired instruction into the coprocessor. Upon reset, the coprocessor loads a zero-vector of data, encrypts this with a zero-vector key, and operates in output feedback mode (OFB) for 120 encryptions. Upon completion, the coprocessor holds its state as the BIST_DONE flag is enabled and 7 bits of output appear on the BIST_OUTPUT pins, which are verified against pre-known values.

BIST for the AES can also be operated as a software instruction sent from the LEON (or any external processor) to the coprocessor. Testing of the entire system was performed against a series of pre-defined test scripts operating in C on the LEON, which test the software BIST, all modes of the cryptographic engine, the matching oracle, as well as a number of protocols to ensure secure operation.

3. RESISTING DPA ATTACKS WITH WDDL AND DIFFERENTIAL ROUTING

In standard static CMOS, 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 readily be determined. DPA has been effective in extracting the key of both microprocessor-based and ASIC-based encryption systems.

Makeshift measures, such as the addition of a random power consuming module or a current sink, have been proven unsuccessful in thwarting power attacks. Currently, two approaches prevail: algorithmic countermeasures and hardware techniques. The former tries to decorrelate the power consumption and the data. Algorithmic countermeasures however, need to be reformulated for each algorithm and often proposed solutions actually appear insecure and/or inefficient afterwards [3]. The latter tries to *not create* any side-channel information. The goal is to make the power consumption of the individual logic gates constant and independent of their input signals. The major advantages are that this approach 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: (1) a logic gate must have exactly one charging event per clock cycle; and (2) the logic gate must charge a constant capacitance in that event. The fabricated IC uses a technique called Wave Dynamic Differential Logic (WDDL) to fulfill the first condition, and a differential routing technique to fulfill the second condition.

3.1 WDDL: constant power dissipating logic

Dynamic differential logic, also known as dual rail with precharge logic, has one charging event per cycle. Since dynamic logic alternates precharge and evaluation phases and differential logic uses true and false signals, exactly one output node becomes 0 in the evaluation phase and both output nodes are charged to 1 in the precharge phase.

The fabricated IC uses Wave Dynamic Differential Logic [4] to implement dynamic differential behavior using static CMOS standard cells. A WDDL gate consists of a parallel combination of two positive complementary gates. A positive gate produces a zero output for an all-zero input. A complementary (or dual) gate computes the false output of the original logic gate using the false inputs of the original gate. Figure 3 (bottom right) shows the WDDL AND and OR 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. Special registers and input converters 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).

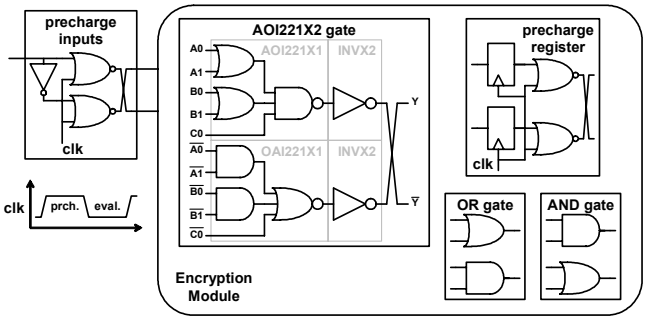

Figure 3. Wave dynamic digital logic (WDDL): precharge generation and compound gate composition.

3.2 Differential routing: matching interconnect capacitances of dual rail logic

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: (1) the intrinsic output capacitance of the gate, (2) the interconnect capacitance, and (3) the intrinsic input capacitance of the load. For high security applications, the contribution of all components must be constant. However, the share of the interconnect capacitance in the total load capacitance is dominant [5]. Hence, the issue of matching the interconnect capacitances of the signal wires is crucial for the countermeasure to succeed.

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. Then independent of the placement, the two routes have the same first order parasitic effects.

Differential pair routing has been available through gridless routers. But their goal is to route a few critical signals, such as the clock or general reset signal. High-capacity gridded routers on the other hand have no or only limited capability to route differential pairs. We have recently presented a way to work around tool limitations [6]. In the technique, each differential output pair is abstracted as a single 'fat' wire, which has among other characteristics the width of two parallel wires plus spacing. The differential design is routed with the fat wire and at the end the fat wire is decomposed into the differential wire. Figure 4 demonstrates the place & route approach. At the left, the result of the fat routing is shown. At the right, the result after decomposition is shown. For the secure part of the prototype IC, the capacitances at the true and the corresponding false signal nets, directly reported from Silicon Ensemble using Simcap, have exactly the same values.

The second order parasitics are not reported by this tool, as described later.

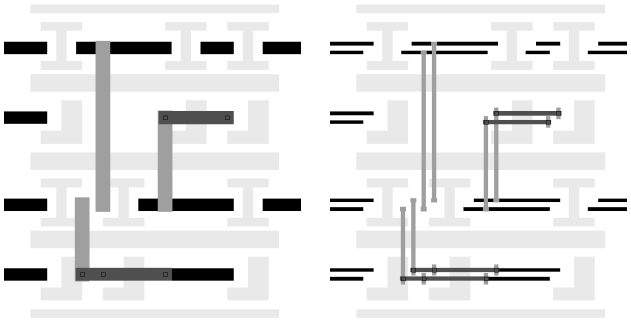

Figure 4. Differential pair routing methodology: fat design (left); and differential design (right).

3.3 Prototype IC

The prototype IC, depicted in Figure 10, consists of two functionally-identical coprocessors, fabricated on the same die using a TSMC 6M 0.18µm process. An *insecure* coprocessor, which serves as benchmark, 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 static CMOS standard cell library used in the regular insecure design.

4. DPA RESISTANCE: EXPERIMENTAL RESULTS

4.1 Measurement setup

The measurement and analysis setup is depicted in Figure 5. The core supply current is measured between the PCB decoupling capacitances and the IC. A CT1 current probe from Tektronix with a 25KHz to 1GHz bandwidth measures the supply current variations. For every mA, it provides a 5mV output to the HP54542C oscilloscope. The oscilloscope filters the waveform transients at 500MHz and digitizes with a 2GHz sampling frequency. To facilitate the synchronization of the measurements, we also have access to the encryption start signal. A clock of 50MHz is provided to the coprocessor under attack, for which only the AES core processes data. The other circuits and modules on the insecure coprocessor are quiet, while for the attack on the secure coprocessor, they always have the same switching events.

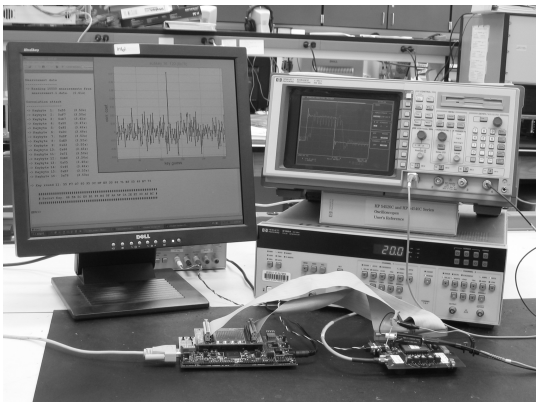

Figure 5. DPA measurement and attack setup.

Figure 6 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 and a high power peak exposes the starting point of each new encryption. 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.

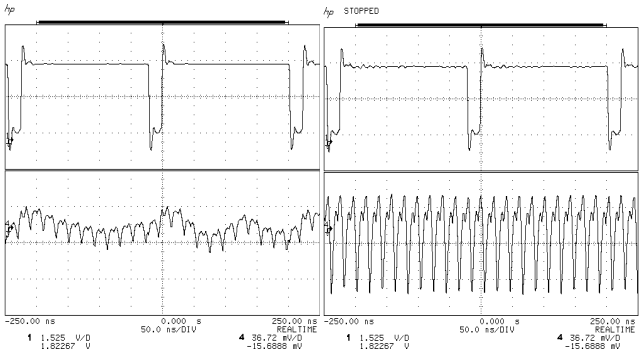

Figure 6. Transient measurement (2 encryptions, 22 clock cycles) of encryption start signal (top) and core supply current (bottom). Standard cells and regular routing (left) and WDDL and differential routing (right).

4.2 Differential power analysis

In DPA, measured power traces are compared with a prediction on the power consumption. Only if the secret key hypothesis is correct will the predicted and the actual power consumption be correlated. The influence of the datapath on the power consumption of the AES core is estimated through the Hamming distance of two successive values of register RB, shown on Figure 2, or in other words, through the number of changing state bits in a clock cycle. Most AES operations work with bytes and eight state bits can be predicted using a guess on one key byte. A brute force attack on the AES algorithm requires 2^{128} key guesses to try all the 128b keys. DPA however, working byte per byte, only requires $16*2^8$ key guesses.

If the guess was correct, the outcome is always equal to the actual bit changes and is therefore correlated with the power consumption of the logic operations affected by the bits. Measurement errors and the power consumption of the other logic operations are uncorrelated. We compare the estimations and the measurements with the correlation test. The correct key guess is the one that results in the highest correlation coefficient between the vector of Hamming distances and the vector of representative measurements, for which we use the maximum supply current in a clock cycle.

For the insecure design, we compare round eleven and the one after that. As shown in Figure 7, RB in round eleven (D_{11}) can be found by tracing back the signal obtained after xor-ing the final ciphertext (C_{11}) and a key guess (K_{11}) through both the shift row operation and the substitution box. RB in the next round, during which we perform the supply current measurement, is the final ciphertext (C_{11}). The correct key byte is found by evaluating:

$$\max_{K_{11}} f_{cost}(K_{11}) = \mathrm{corr}(P_{model}, P_{measurement}) \quad (1)$$

$$\textit{where } P_{model} = \mathrm{HamDist}(\mathrm{sub}^{-1}(\mathrm{shiftrow}^{-1}(K_{11} \otimes C_{11})), C_{11})$$

$$P_{measurement} = \max(I_{supply,11+1})$$

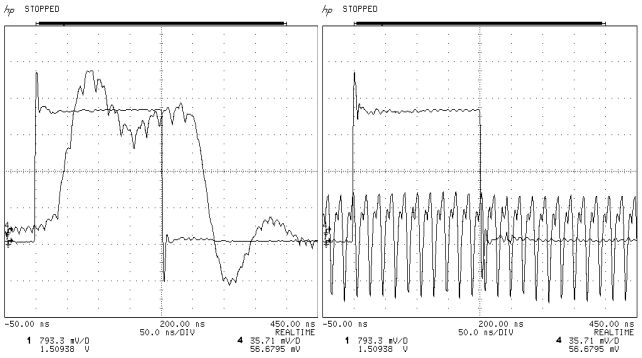

Figure 8. Transient measurement of encryption start signal and core supply current for single encryption: Standard cells and regular routing (left); and WDDL and differential routing (right).

For the secure design, we only need to look at one round, as all signals are at 0 at the start of the evaluation phase. The number of changing bits of RB in round eleven, during which we also do the measurements, is the Hamming weight of RB.

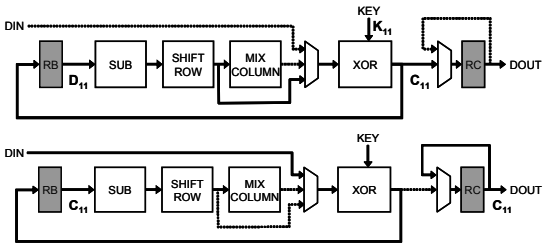

Figure 7. AES core: round 11 (top); and round 11 + 1 (bottom).

Figure 8 shows the encryption start signal and the core supply current during the attack. The supply current of the insecure coprocessor reveals the encryption operation. One can count exactly eleven peaks. The secure coprocessor has a continuous current whether or not data is being processed. It has an identical power consumption profile in Figure 7 and in Figure 8. Without the encryption start signal, it is virtually impossible to isolate the encryption. For the actual attack, we only measure the round of interest. The dynamic range is set to cover the variation of the maximum current. The other irrelevant samples may be clipped. For the remainder of this manuscript, we will refer to the maximum value of one acquisition as the measurement.

4.3 DPA resistance

The resistance against DPA is quantified with the number of measurements to disclosure (MTD). We define MTD as 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 Figure 9. MTD is shown in the 'Correlation vs. Number of Measurements' graphs as the point where the black line (correct key) crosses the grey envelope (wrong keys). The results for the other fifteen key bytes are similar. The maximum number of measurements is 15,000 and 1,500,000 for the insecure and the secure coprocessor respectively. For the insecure implementation, the correct key bytes are found very easily. On average, 2,000 measurements are required to disclose a key byte. In one case, a mere 320 samples were sufficient to mount a successful attack. There is also a large resolution; there is no doubt about the correct key guess.

The secure coprocessor on the other hand substantially reduces this resolution of correlation, shown by the small correlation peaks in the 'Correlation vs. Key Guess' graph in Figure 9. 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 the correct key bytes. One example is shown on the bottom of Figure 9. The eleven key bytes that are found require on average 255,000 measurements, an increase of more than *two orders of magnitude* when compared with the insecure coprocessor.

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.

Further techniques to improve matching include making every other metal layer a ground plane, which would completely control the capacitance to other layers. Shielding the differential routes on either side with a power line would eliminate the cross-talk to adjacent wires in the same metal layer. Alternatively, increasing the distance between different differential pairs would reduce the effect, or an iterative design flow could be used to identify and correct mismatches.

Table 1 summarizes the results. WDDL and differential routing is a functioning technique to thwart power attacks. 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], the careful division of the architecture into two parts (a secure and a non-secure part) as shown in Figure 1, minimizes the cost for

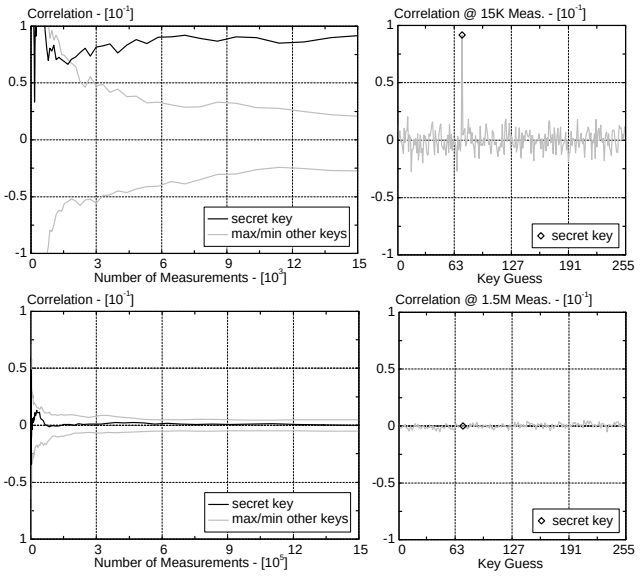

Figure 9. Cracking the secret key: Standard cells and regular routing using 15K measurements (top); and WDDL and differential routing using 1.5M measurements (bottom).

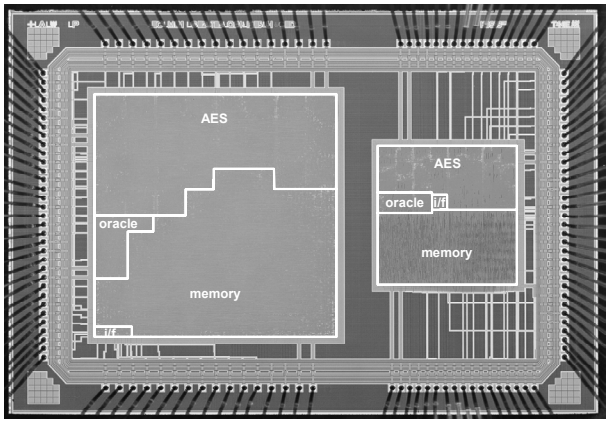

Figure 10. IC micrograph: Secure coprocessor using WDDL and differential routing (left); and Insecure coprocessor using standard cells and regular routing (right).

complex systems. Only the relatively small part that processes sensitive information requires realization in a coprocessor with specialized logic and routing. This minimizes the area and reduces the power and time penalty. Even with these penalties, the secure coprocessor still runs orders of magnitude faster and expends less energy than a software implementation on the main processor.

Table 1. 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†
Entire System	0.036	0.486
Measurements to Disclosure‡		
min	320	21,185
mean	2,133	255,391
max	8,168	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

5. RELATED WORK

As far as we know, this paper will be the first published DPA-resistant circuit-plus-routing technique implemented and tested in actual silicon. All other published countermeasures have never been implemented in silicon, or have never been measured and attacked, or did not offer any significant DPA resistance.

A dual rail asynchronous chip has been presented previously [8]. The implementation did not provide a significant increase in DPA resistance. This failure has been attributed to unbalanced signal paths caused by routing differences. Note that if asynchronous logic is used to increase the DPA resistance, dual rail encoded asynchronous logic must be used. Because of the dual rail logic, there is also a factor 3 area increase compared with a single ended synchronous benchmark.

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.

6. CONCLUSIONS

We have presented a secure coprocessor that does not leak information through the power supply, which is a major and easy to access side-channel leakage source. Built in a 0.18µm CMOS technology, we believe that this is the first IC that is practically immune to DPA attacks. Its immunity has been experimentally verified and compared to a second IC, built with a regular standard cell approach. The coprocessor processes the sensitive information in a biometric and cryptographic authentication device. The design approach relies on a logic style that has constant power consumption and a place & route technique that controls the parasitic effects. An actual power attack has been mounted on the IC to experimentally asses the increase in DPA resistance. We have presented the measurement setup and analysis technique. Experimental results showed that 1,500,000 acquisitions are not sufficient to fully disclose the 128b secret key.

ACKNOWLEDGEMENTS

This work was supported in part by the National Science Foundation (CCR-0098361), UC-Micro 02-079 and 03-088, Panasonic Foundation, SUN Microsystems, Atmel corporation and the Fannie and John Hertz Foundation.

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] E. Oswald, S. Mangard and N. Pramstaller, "Secure and Efficient Masking of AES – A Mission Impossible?," *IACR Cryptology ePrint*, 2004.

[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] K. Tiri and I. Verbauwhede, "A Digital Design Flow for Secure Integrated Circuits," submitted *IEEE TCAD*.

[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," accepted *IEEE Security & Privacy Magazine*.

[8] S. Moore, R. Anderson, R. Mullins, G. Taylor and J. Fournier, "Balanced self-checking asynchronous logic for smart card applications" *Microprocessors and Microsystems 27.9*, pp. 421-430, 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.