Turning Liabilities into Assets: Exploiting Deep Submicron CMOS Technology to Design Secure Embedded Circuits

Patrick Schaumont
Virginia Tech
Blacksburg, VA 24061
schaum@vt.edu

David D. Hwang
George Mason University
Fairfax, VA 22030
dhwang@gmu.edu

***Abstract*— This paper explores an unexpected link between system-level security considerations and deep-submicron CMOS circuits. Many deep-submicron effects including increased leakage power, process variability, noise-level, power-density and integration density are thought of to be liabilities for integrated design. However, we show how they may instead be an asset for certain types of secure circuits. These circuits are useful for secure embedded systems design, where stringent cost-, power- and implementation constraints, as well as the increased risk towards physical attacks, are among the design issues. We also conclude that not all deep sub-micron liabilities are secure-circuit assets, and point out some of the open challenges in secure circuit design.**

I. Introduction

Secure embedded circuits, such as those found in smartcards, RFIDs, secure tokens and secure storage peripherals, are quickly becoming ubiquitous. New applications such as sensor networks, in addition to traditional applications such as secure data storage, have increased the need for building security from the ground up into embedded systems.

Most secure embedded systems are ultimately constituted of integrated circuits at the transistor level. Thus, as integrated circuits migrate to deep submicron process nodes, it would seem all the problems which plague deep submicron design would automatically plague security chips in deep submicron as well. In some cases, this is true. However, this paper presents the notion that certain deep submicron CMOS liabilities can actually become assets—rather than liabilities—in the hand of a security designer.

Of course, it should be kept in mind that no point-solution is adequate in the context of a secure system design. We see a very important role for well-designed secure CMOS circuits as essential components in larger security protocols – but the security protocols themselves still need to be sound. We will describe how secure CMOS circuits, and their apparent liabilities, can add strength in areas that are typically hard to address at system-level, in software.

This paper is organized as follows. In section II, we review several classic security challenges faced by embedded system designers today. These include the need for lightweight cryptography, tamper resistance, non-reproducibility, end-point security and emission security. In Section III, we review deep submicron CMOS circuit characteristics, both negative and positive, which must be handled by modern IC designers. These issues include leakage current, process variability, noise and noise margin issues. In Section IV we discuss how these deep submicron liabilities can actually be turned into security assets. Section V discusses future challenges in designing secure embedded circuits.

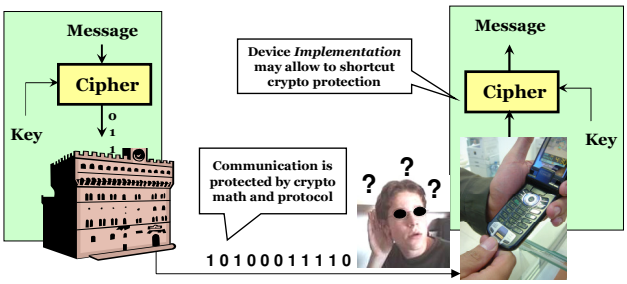

Figure 1: Main challenge in Embedded Security

II. Embedded Security Concepts and Challenges

Traditional security architectures assume that only the communication link between trusted parties needs protection. Embedded systems, on the other hand, are deeply immersed in their environment. Their implementation becomes part of the non-trusted communication link (Figure 1). This makes the embedded system environment very hostile from a security perspective. Many attacks consist of simply copying confidential information from accessible, unprotected interfaces which are abundant in embedded systems [1][2][3]. In this chapter, we will highlight typical security requirements for embedded system implementations, and clarify the link between circuit design and secure embedded systems.

A. Cryptography

Cryptography is the driving force behind many secure embedded applications. There is a threefold challenge for secure circuit- and system-designers in this area. First, traditional crypto algorithms tend to require increasingly stronger versions and longer keys over the years [4]. This implies stronger performance requirements to maintain real-time operation. Second, novel wireless applications such as RFID have very stringent power - and area requirements, leading to the need for crypto 'on a speck of dust' [5]. Third, novel applications of secure protocols are a source of new and usually complex algorithms in embedded systems context. Identity-based cryptography for example uses common identifiers as public-keys, but requires additional computations to derive a corresponding private-key [6]. These three challenges require energy- and area-efficient crypto-circuits. Besides this, many cryptographic protocols involving identification and authentication rely on the use of random numbers and/or unique numbers. These cryptographic primitives must be created using efficient secure circuits. The operation of a secure protocol is critically dependent upon such cryptographic primitives and the assumptions that it allows.

B. Tamper Resistance

Embedded electronics that store secure keys require tamper resistance or tamper detection. The challenge for the circuit designer is to create an implementation that provides protection at the lower, physical abstraction levels. In smart-cards active sensors as well as passive defenses (special layout techniques) are used, and attacked [7].

A more recently identified challenge is the detection of a malicious insertion (so-called Trojan) in a regular circuit [8]. Trojans are a concern when all steps in the manufacturing of a security-sensitive circuit are not under control of the designer.

C. Non-reproducibility

The ability to uniquely determine the identity of a chip enables many useful applications, including anti-counterfeiting [9] and protection of software intellectual property [10]. Even though the introduction of chip identifiers (in processors) has met significant user-end concerns for privacy, the ability to detect uniqueness in a circuit remains an essential element for mutual authentication schemes. Thus, while Intel removed the 'chip-tracking ID' years ago, a recent generation of Xilinx Spartan FPGA has introduced it [11]. By making a careful distinction between user-level privacy and intellectual-property privacy (stored data and software), a sensible use of chip identification may be possible and desired.

D. End-Point Security

As pointed out in Figure 1, the non-trusted channel for the case of embedded systems extends right up to the system's peripherals. Secure peripherals (such as video cards and disks) enable one to build secure tunnels from the information source, across software and hardware, into the peripheral [12]. For the circuit designer, end-point-security may imply the use of tight information security concepts even up to the individual pins of a chip.

E. Emission Security

A final key aspect for secure embedded system design is emission security [13], which makes use of the physical implementation effects of systems to circumvent their cryptographic - and other defenses. After a decade of intense research as side-channel attacks, this has resulted in an array of powerful techniques. Circuit techniques are needed that enable control of the signature of a circuit (such as power consumption, radiation, time) at a reasonable implementation cost.

III. Deep Submicron CMOS Liabilities

The scaling of deep submicron CMOS integrated circuits has been motivated largely by three factors: reduced dynamic power, increased clock frequency, and increased density. Dynamic power decreases due to lower VDD and smaller capacitance (compared to larger technologies per a given function). Deep submicron systems are faster than their larger counterparts due largely to lower threshold and switching voltages. In addition deep submicron ICs exhibit increased density: more transistors can fit on a given die, or the same number of transistors can fit in a smaller area. This property has been exploited to miniaturize circuitry for cell phones, PDAs, and other embedded devices. With these benefits of deep submicron CMOS, a number of liabilities also have emerged. A few of these liabilities include:

A. Subthreshold Leakage Power

Due to decreased threshold voltages, subthreshold leakage current is becoming an unwanted and dominant source of power in deep submicron CMOS. As shown in [14] subthreshold leakage current increases exponentially with the decrease of threshold voltage; this results in the potential for deep submicron static power to be a large percentage of total power consumption, particularly given process variability.

Characteristic	CMOS Liability	Security Asset
Subthreshold Leakage Power	Increased static power consumption	Increased side-channel resistance
Process Variability	Reduces yield	A basis for implementing silicon physical unclonable functions
Noise Issues and Signal Integrity	Reduced noise margin, capacitive crosstalk increases propagation delay	Can be harnessed for random noise generation
Power Density	Cooling difficulties and thermal issues	Potentially useful to as a noise mask against side-channel attacks on power consumption

Table 1. CMOS Liabilites and Secure IC Assets.

B. Process Variation

CMOS process variation is another liability in deep submicron CMOS, affecting yield. Process parameter variation during manufacturing can cause minimum clock frequencies to vary by 30% and subthreshold leakage current to vary by 20X, as shown in [15]. Clearly, designing for an aggressive minimum frequency and maximum total power budget for a given IC would cause yield to suffer greatly, ultimately increasing the cost of the part.

C. Noise Issues and Signal Integrity

Signal integrity and noise margin is another liability in deep submicron design; lower threshold voltages and supply voltages imply lower absolute noise margins. This fact, combined with the reduction in interconnect pitch and an associated increase in coupling capacitance, make signal integrity an issue which requires accurate modeling and simulation to prevent logical chip failure via noise [16].

D. Power Density

Power density, measured in W/cm^2, is also a difficult issue to control [17]. As more functionality and transistors are being implemented on a single die as systems-on-chip, proper cooling of the die is crucial. In addition, leakage current and temperatures reinforce one another with positive feedback, stressing the need to control thermal issues.

IV. Turning Liabilities Into Assets

In a general sense, security ICs receive the same benefits and liabilities from deep submicron CMOS than any other processing domain (i.e. signal processing chips, microprocessor chips, multimedia chips, etc.). However, looking deeper into the matter reveals that there are certain security functions which actually benefit from deep submicron "problems." In other words, liabilities become assets in the hands of a security engineer. For example:

A. Subthreshold Leakage Power

Side-channel attacks rely on dynamic power consumption measurements to reveal correlations with internal secret circuit nodes. However, subthreshold leakage is, in first order, independent of the data patterns processed by circuits: it contributes only to a circuit's static power consumption. Therefore, the relative increase of subthreshold leakage power in the total power consumption budget of a circuit has the effect of a relative decrease in side-channel leakage. This effect comes in addition to the reduction of side-channel leakage in absolute terms, which is obtained by reducing the operating voltage of the circuit.

B. Process Variability

A textbook example of turning a liability into an asset is process variability. In embedded security, silicon physical unclonable functions (PUFs) serve an important role in various security protocols [18]. PUFs are functions that map a series of challenges to unique responses, serving as an integrated circuit's unique set of fingerprints. Each IC, though implementing the same digital function, has slightly different nuances and physical characteristics due to process variation in manufacturing. PUFs attempt to harness this variability to ensure each unique IC gives a different set of responses to a set of challenges, thus giving the ability to uniquely identify a chip. PUFs have widespread use in digital rights management, anti-counterfeiting, and authentication. Besides PUFs, process variability and its effect on ring oscillators can also be used for random-number generation [19].

C. Noise Issues and Signal Integrity

Another way of turning a liability into an asset is to view noise in deep submicron circuits as a useful resource, rather than a burden. As mentioned

previously, embedded security often requires power-efficient random noise generators on-chip. CMOS noise, combined with a logical technique called probabilistic CMOS (PCMOS), can be harnessed to energy-efficient random noise generators [20]. In such noise-harnessing random noise generators, CMOS noise is an ally.

D. *Power Density*

Increased power density helps by masking power-based side-channels. In differential power-analysis side-channel attacks, an attacker monitors the power fluctuations or electromagnetic emissions of a circuit implementing a cipher and processes this data to extract information about the secret encryption key. However, to mount this attack and attacker must be able to isolate the power traces caused by the encryption algorithm and have sensitive enough probes to pick up these signals [21]. On a system-on-chip implementing multiple functions in parallel, including encryption, it is feasible that the dynamic switching power of the other components on the chip can effectively mask the power variations of the encryption core below the relative sensitivity of the probe. Thus power density works to the advantage of security to safeguard secret information.

V. Open Challenges

The liabilities of deep-submicron CMOS are not a universal benefit for secure CMOS circuits. Several recently-proposed side-channel-resistant circuit styles are based on dual-rail circuits. These circuits require precisely-matched rails for each gate in order to provide maximal side-channel resistance; certainly intra-die process variation makes this challenging.

In addition, active security attacks such as fault attacks may become easier as circuits get more sensitive. Fault attacks introduce controlled faults into circuits, for example using voltage glitches or optical pulses. By observing the response of a circuit to a fault, internal secrets can be extracted. Some fault-attack countermeasures require on-chip sensors for voltage, light, and clock. These analog features have to coexist with the other digital deep-submicron elements on the chip.

Finally, intellectual-property reuse is rapidly becoming a security challenge. For private IP, adequate protection and exchange is needed; for third-party IP, trustworthiness is needed. A recent DARPA project focuses on the issue of trust in fabrication [22]; in complex ICs, malicious hardware may be added that avoids detection from design-for-test and BIST. The detection of such tampering after fabrication is a challenge.

VI. Conclusions.

Matching the requirements of secure embedded circuits with the properties of deep-submicron CMOS reveals a number of exciting opportunities. By harnessing the effects of apparent liabilities in deep-submicron, novel applications in circuit identification, random-number generation, circuit protection and – side-channel-resistance are possible.

References

[1] A. Huang, "Keeping Secrets in Hardware: the Microsoft XBOX Case Study," CHES 2002, p. 13-15., 2002.

[2] J. Grand, "Research lessons from hardware hacking," Communications of the ACM, 49(6):44{49, 2006.

[3] A. Bylund, 2006, "Apple's DRM Cracked Again," Arstechnica online (http://arstechnica.com/news.ars/post/20060830-7619.html).

[4] D. Giry, "Keylength.com - Cyrptographic Key Length Recommendation," Online at http://www.keylength.com.

[5] J.-P. Kaps, G. Gaubatz, and B. Sunar, "Cryptography on a Speck of Dust", Computer, volume 40, number 2, pages 38--44, Feb, 2007.

[6] D. Boneh, M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," Advances in Cryptology - Proceedings of CRYPTO 2001 (2001).

[7] S. Skorobogatov, "Semi-Invasive Attacks - A new approach to hardware security analysis," Tech Rep UCAM-CL-TR-630, U Cambridge, April 2005.

[8] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar, "Trojan Detection using IC Fingerprinting," IBM Research Report RC24110, April 2006.

[9] P. Tuyls, and L. Batina, "RFID-Tags for Anti-Counterfeiting," In Topics in Cryptology - CT-RSA 2006.

[10] E. Simpson, P. Schaumont, "Offline Hardware/Software Authentication for Reconfigurable Platforms," CHES 2006.

[11] M. Moran, "How to implement high-security in low-cost FPGAs," Programmable Logic DesignLine, CMP Publishers, 12/4/06.

[12] R. Thibadeau, "Trusted Computing for Disk Drives and Other Peripherals," IEEE Security and Privacy, Sep/Oct 2006, 4(5):26-33.

[13] R. Anderson, "Security Engineering," Chapter 15, Wiley, 2001.

[14] J. Kao, S. Narendra, and A. Chandrakasan, "Subthreshold leakage modeling and reduction techniques," IEEE International Conference on Computer-Aided Design, pp. 141-148, 2002.

[15] S. Borkar, T. Karnik, S. Narendra, J. Tschanz, A. Keshavarzi, V. De "Parameter Variations and Impact on Circuits and Microarchitecture," Design Automation Conference, pp. 338-342, 2003.

[16] K. Shepard, V. Narayanan, "Conquering Noise in Deep-Submicron Digital ICs," IEEE Design & Test of Computers, vol. 15, no. 1, pp. 51-62, January-March 1998.

[17] S. Borkar, "Design Challenges of Technology Scaling," IEEE Micro, vol. 19, no. 4, pp.23-29, July/August 1999.

[18] D. Lim, J. Lee, B. Gassend, G. Suh, M. van Dijk, S. Devadas, "Extracting Secret Keys from Integrated Circuits," IEEE Transactions on VLSI Systems, vol. 13, no. 10, pp. 1200-1205, October 2005.

[19] B. Sunar, W. Martin, D. Stinson, "A Provably Secure True Random Number Generator with built-tin Tolerance to Active Attacks," IEEE Trans. Comp., 58(1):109-119, Jan 2007.

[20] L. Chakrapani, B. Akgul, S. Cheemalavagu, P. Korkmaz, K. Palem, B. Seshasayee, "Ultra-Efficient (Embedded) SOC Architectures based on Probabilistic CMOS (PCMOS) Technology," DATE Conference, pp. 1110-1115, 2006.

[21] P. Yu, "Implementation of DPA-Resistant Circuit for FPGA," M.S. Thesis, Virginia Tech, 2007.

[22] DARPA, "Trust in Integrated Circuits," http://www.darpa.mil/MTO/solicitations/baa07-24/index.html.