ANALYSIS OF SUB THRESHOLD DEVICES TO LOW VOLTAGE FAULT ATTACKS

G.Rajesh

Assistant Professor/ECE Mahendra Engineering College ,Namakkal Dt

ABSTRACT

The continuous scaling of VLSI technology and the possibility to run circuits in sub-threshold voltage range make it possible to implement standard cryptographic primitives within the very limited circuit and power budget of radio frequency identification (RFID) devices. However, such cryptographic implementations raise concerns regarding their vulnerability to both active and passive side-channel attacks. In particular, when focusing on RFID targeted designs, it is important to evaluate their resistance against low-cost physical attacks. A low-cost fault injection attack can be mounted, for example, by lowering the supply voltage of the chip with the goal of causing setup time violations. In this paper, we provide an in-depth characterization of a chip implementation of the AES cipher. Identifying sensitive logic signals allows us to suggest to the designer a tailored countermeasure strategy for thwarting these attacks, with a minimal impact on the circuit's performance.

Keywords: Setup time violation, fault attacks, AES, design Simulation

I. INTRODUCTION

RADIO Frequency Identification (RFID) devices are nowadays used in a wide range of applications, such as health care, supply chain management, and pet identification. Such a pervasive diffusion raises concerns regarding privacy as RFID tags often store sensitive information. The design of RFID devices is commonly constrained by a very strict power and area budget. Thus, incorporating the circuitry needed to guarantee a sound security margin against attackers is a challenging task, as security primitives, if not properly implemented, are quite demanding in terms of area and power. A particularly appealing solution to meet the power consumption constraints is to exploit nanometer CMOS technologies, while adopting known aggressive power saving techniques, and operating the device at a sub threshold voltage [1]. Typical supply voltages employed in this context range between 0.3and0.5V, significantly lower than the common ones needed to work in the saturation region (1-1.2V). Nanometer CMOS technologies also allow to meet the area constraints when implementing standard crypto-graphic algorithms such as AES. As the manufacturing processes for nanometer CMOS technologies become more widespread, a larger number of commercial applications will be able to afford the cost of using RFID tags [2]. Using low power cell libraries and operating the

device at a sub threshold voltage, result in a significant reduction of the power consumption but at the cost of a considerably lower clock frequency at which the device will operate. This, however, is acceptable since, even if speed in RFIDs is an important design parameter, it is not commonly a critical one.

A.THE AES CIPHER

The cipher considered in this work is the Advanced Encryption Standard due to its wide spread adoption. The selected variants of the Rijndael algorithm that the AES standard supports include a plaintext block size of 128 bits and three key sizes of 128, 192 and 256 bits. AES is based on the iteration of a round function composed of four primitives: SUBBYTES, SHIFTROWS, MIXCOLUMNS and ADDROUNDKEY. The number of times the round function is iterated, N_r , is 10, 12 or 14 times depending on the key length. The exceptions to the repetition of the four primitives are: the last round of the encryption is missing the MIXCOLUMNS primitive and an extra ADDROUNDKEY is performed before the first round as a pre-whitening of the input. The inner state of the AES cipher after round r, denoted by S_r , is represented as a 4×4 matrix, where each element is 8-bit wide. We denote the n-th byte, counting from left to right, from top to bottom as S^n. Each primitive of the AES cipher contributes either confusion or diffusion effects to the cipher, or adds a dependency on the value of the key. The SUBBYTES primitive is a non-linear mapping over Z_28 that introduces a non-linear confusion effect. This map-ping is applied to a single byte at a time, S^n, and can be implemented either as a lookup table or computed on the fly. The SHIFTROWS primitive provides a row-wise diffusion effect to the inner state of AES. It rotates the four rows of the state S_r by 0,1,2 or 3 byte positions, respectively. The MIXCOLUMNS primitive provides column-wise diffusion of the state by considering the column as a vector of values over Z_28 , and multiplying the vector by a constant matrix.

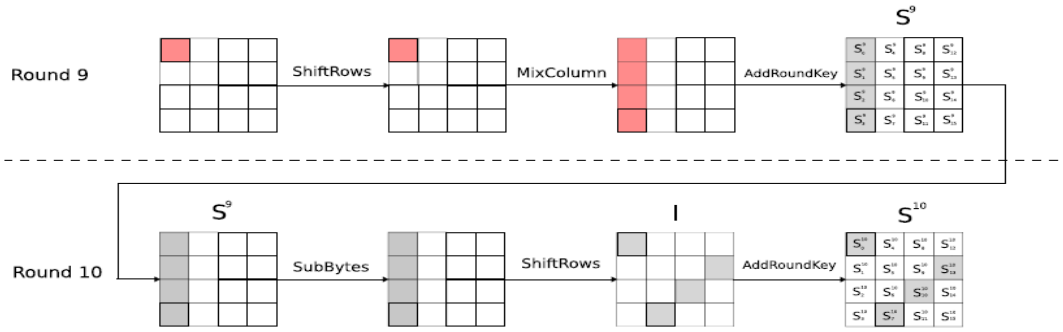

FIGURE 1. Effects of a single fault injected between the MixColumns operations of the eighth and ninth rounds. The fault propagates to only a quarter of the state, allowing the attacker to detect such a situation.

B. ACTIVE SIDE-CHANNEL ATTACKS AGAINST AES

A number of fault injection attacks on the AES cipher have been reported in the literature. Although some of them were not experimentally validated at the time they were presented [6] several other were successfully mounted on real world implementations. It causes the temporary brown outs and glitches on the power supply line of an 8-bit microcontroller running a software implementation of AES. In Schmidt et al. attacked an implementation of AES by blanking selectively the memory where the S-Boxes are held, effectively reducing the entire AES algorithm to the last ADDROUNDKEY, performed on a zero-lled state. A technique which has proven effective in inducing controlled faults is through causing setup time violations by lowering the supply voltage below the level the circuit was designed.

C. THE ATTACK UNDER CONSIDERATION

We now present the attack methodology considered in this paper to determine which faults represent a threat to the security of the AES implementation. Dusart et al. [5] have shown that it is possible to successfully retrieve the whole secret key of an AES-128 cipher, through the injection of a single byte wide fault during the regular functioning of the cipher. The proposed attack relies on the injection of a single byte fault between the MIXCOLUMNS operation of the eighth round and the MIXCOLUMNS of the ninth round, as depicted in Figure 1. Due to the lack of the MIXCOLUMNS operation during the tenth round, the effect of the fault is spread only over 4 of the 16 bytes of the state. Since the key addition is performed byte-wise, the values of these 4 bytes are only by 4 bytes of the last round key. Exploiting this fact and assuming that the injected fault has corrupted only one byte, the attacker may proceed to recover the 4 bytes of the key by comparing the correct and faulty cipher texts.

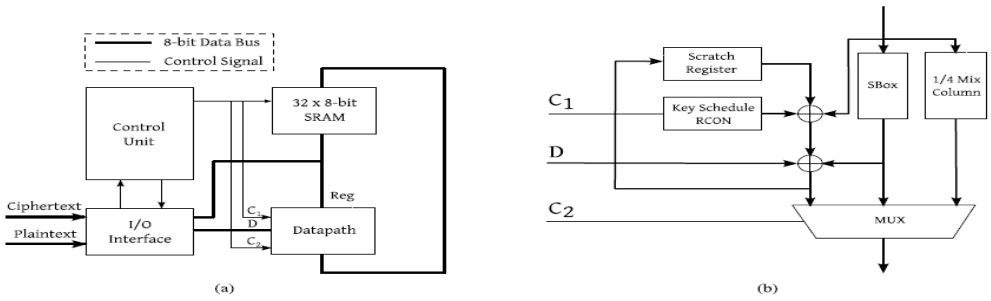

FIGURE 2. **Block diagram of the AES module proposed by Feldhofer *et al.* [19] and implemented with a 65nm subthreshold cell library. (a) AES Component. (b) AES Component Datapath.**

II. ARCHITECTURE OF THE COPROCESSOR

In this Project we describe the structure of the AES co-processor chosen to implement the cipher, given the tight area and power constraints .The selected 8-bit AES implementation is

tailored to be used in low cost, low power devices such as RFIDs and follows the high-level structure proposed by Feldhofer et al. [4], supporting only a 128-bit key. The block diagram of this design is depicted in Figure 2. The chip communicates with the user through an 8-bit wide data bus managed by an I/O interface module. The state and the initial key of the cipher are stored in a 32-byte wide register _le, connected to the 8-bit wide data-path of the chip, and driven by the _nite-state control unit.

III. EXPERIMENTAL SETUP AND FAULT CHARACTERIZATION

This section describes the measurement setup used and the experiments conducted inorder to profile the behavior of the low-power AES implementation and investigate the feasibility of low-cost fault injection attacks based on voltage throttling. It also provides a precise characterization of the setup time violation faults which can be exploited by an attacker

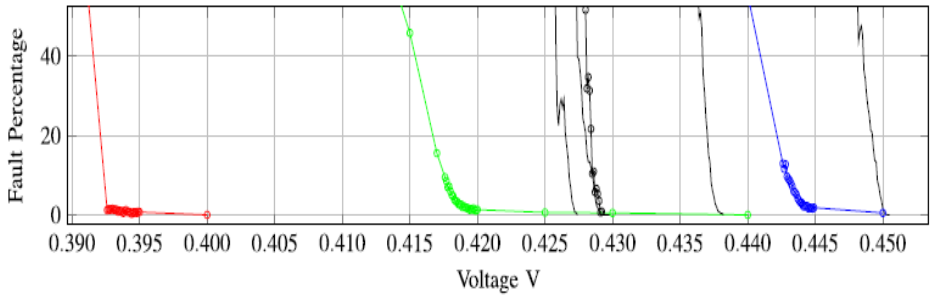

FIGURE 4. Comparison of the voltage threshold of the first appearance of faults among different sample chips implementing the same AES co-processor design. The five chip degradation curves are depicted in black. The impact of temperature variations on the degradation curve of the chip marked by round plotmarks is depicted by the blue (T = 25C), green (T = 50C), and red (T = 75C) curves.

IV. FAULT PREDICTABILITY AT DESIGN TIME

This section describes the EDA flow used to design the circuit under test and discusses how an early assessment of the potential fault attacks is carried out. In particular, we discuss how an early prediction of the points in the circuit which are more sensitive to setup-time violations can be identified using static timing analysis. Finally, we discuss to what extent the results obtained in simulations match the ones measured on the real chip, and we exploit them to propose efficient countermeasures against this attack strategy.

V. CONCLUSIONS

In this paper we have presented a detailed characterization of an AES coprocessor realized with 65nm technology and operating in a sub-threshold voltage region. The characterization showed that it is possible to effectively perform setup time violation attacks on the implemented ciphers through reducing the supply voltage in 0.1mV steps. We were able to

provide a bit-level description of the fault frequencies and provide insights regarding their predictability with common EDA tools. In particular, we report that by employing static timing analysis tools, it is possible to obtain reliable estimates of the worst case timings for the input lines of the cipher state registers and pinpoint which ones are more likely to be vulnerable to setup time violation attacks. Finally, we proposed a countermeasure that designers can use in order to protect their design against these attacks.

VI. FUTURE SCOPE

In future this work can be extended for all wiress devices such as GSM,GPRS which operates in Subthreshold voltages. The 2 encryption algorithms namely AES Secret kay and RSA Public key may be used together which may be used for faster decryption and Secure Secret key transfer which is called " Digital Envelope". Digital Envelope not only reduces the probability of faulty nodes in an Integrated Chip but also enhance the Secure data Transmission over a Wireless channel.The width of Plain text may be increased to 256 bits ,512 bits,1 KB,… and the corresponding Keys used may be 256 bits, 352 bits etc.

ACKNOWLEDGMENT

I thank my Colleagues and my friends who helped me to do this Project without any intervention.

REFERENCES

D. Bol. (2012). Robust and energy-efficient ultra-low-voltage circuit design under timing constraints in 65/45 nm CMOS. J. Low PowerElectron. Appl. [Online]. 1(1), 1_19. Available: http://www.mdpi.com/ 2079-9268/1/1/1

K. H. Brown, ``Announcing the advanced encryption standard AES," NIST, Gaithersburg, MD, USA, Tech. Rep. 197, 2001.

A. Barenghi, C. Hocquet, D. Bol, F.-X. Standaert, F. Regazzoni, and I. Koren, ``Exploring the feasibility of low cost fault injection attacks on sub-threshold devices through an example of a 65 nm AES implementation,"in RFIDSec (Lecture Notes in Computer Science), vol. 7055, A. Juelsand C. Paar, Eds. New York, NY, USA: Springer-Verlag, 2011, pp. 48_60.

C. Hocquet et al., ``Harvesting the potential of nano-CMOS for lightweight cryptography: An ultra-low-voltage 65 nm AES coprocessor for passive RFID tags," J. Cryptograph. Eng., vol. 1, no. 1, pp. 79_86, 2011.

D. Bol, R. Ambroise, D. Flandre, and J. Legat, ``Interests and limitations of technology scaling for subthreshold logic," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 17, no. 10, pp. 1508_1519, Oct. 2012.