HARDWARE SECURITY IN CASE OF SCAN-BASED ATTACK ON CRYPTO-HARDWARE

Jayesh Popat[1] and Usha Mehta[2]
[1&2] EC Department, Nirma University, Gujarat, India

ABSTRACT

The latest innovation technology in computing devices has given a rise of compact, speedy and economical products which also embeds cryptography hardware on-chip. This device generally holds secret key and confidential information, more attention has been given to attacks on hardware which guards such secure information. The attacker may leak secret information from symmetric crypto-hardware (AES, DES etc.) using side-channel analysis, fault injection or exploiting existing test infrastructure. This paper examines various DFT based attack implementation method applied to cryptographic hardware. The paper contains an extensive analysis of attacks based on various parameters. The countermeasures are classified and analyzed in details.

KEYWORDS

Hardware Security, Cryptography, Side-channel analysis, fault injection, scan-based attack, testability, security.

1. INTRODUCTION

Nowadays, the computing hardware becomes small, cheap and fast due to emerging of new fabrication technology and increased design complexity. Hence, Crypto-hardware can now easily be integrated in everything from smart cards to pay TVs to smart handset to prepaid cards. The research in cryptography focuses on mathematical complexity of crypto algorithms, ciphers and protocols. Since main purpose of cryptography is to make secure communication with confidentiality, the security of such cryptography hardware is essential. Hence an attack on hardware which actually performs cryptographic algorithm is getting attention. Countermeasures to such attacks are being developed and analyzed. The paper describes practical implementation attacks especially based on test infrastructure on cryptographic hardware, which focuses on embedded system and portable devices. Also, the detail understating of the countermeasures against test attack is reviewed. The paper is organized in following sections. The basics of Encryption decryption and security attacks are described in section 2. Section 3 describes different hardware attacks on crypto hardware. Countermeasures against attack based on test infrastructure are presented in Section 4. Finally, the concluding remarks are presented in Section 5.

2. CIPHER PROCESS AND SECURITY ATTACKS

2.1 ENCRYPTION-DECRYPTION

The encryption and decryption process performed by crypto algorithm is illustrated in figure 1.

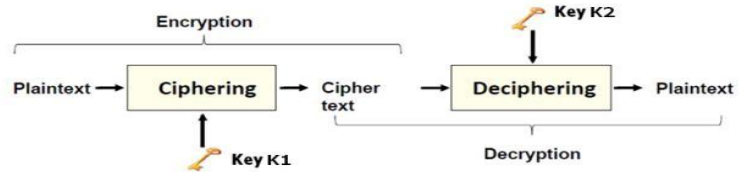

Figure 1. Basic Encryption/Decryption Process

As shown in figure 1, the plaintext or input text/message is converted into unintelligible form called cipher text during encryption process. Cipher text is again converted back into original form called plaintext during decryption process.

A cryptographic algorithm that uses the same key to encrypt and decrypt data is called symmetrical key algorithm (K1=K2). In Asymmetric cryptography algorithm, secret key can be divided into two parts, a public key and a private key. Either of the keys can be used to encrypt a message, the opposite key is used for decryption (K1 ≠ K2) [1].

2.2. SECURITY ATTACKS

The information embedded into crypto-devices is often secret like keys and confidential information, so attack applied on sensitive information or on the device that holds it may result in private information loss, fake access and financial thievery.

Because of easy availability of crypto-devices, the internal structure of hardware with implementation details can be analyzed and learnt by malicious user. Implementation knowledge can be used to perform attack on device without breaking mathematics of algorithm. That is to say, the attacker can still be able to retrieve secrete sensitive data from internal implementation although highly secure algorithm is implemented. Even though the confidential key is not retrieved by attacker, there are still chances of disrupting hardware or denial of service attack which results in failures in secure system.

Numerous attacks are reported in literature. Security system can be attacked for the benefit of attacker which is in terms of side-channel analysis, fault injection or exploiting existing test infrastructure. For example, Data Encryption Standard (DES) [2], Advance Encryption Standards (AES) [3], stream ciphers [4], RSA [5] and Elliptic Curve Cryptosystems (ECC) [6] can be attacked.

3. IMPLEMENTATION ATTACKS ON CRYPTO-HARDWARE

Numbers of possible hardware attacks are described in [7-25]. Based on the implementation methods, we have categorized this all methods in three different categories of hardware attack on crypto-hardware system as shown in fig.2: 1. Side channel attacks, 2. fault attacks and 3. Test-infrastructure based attacks.

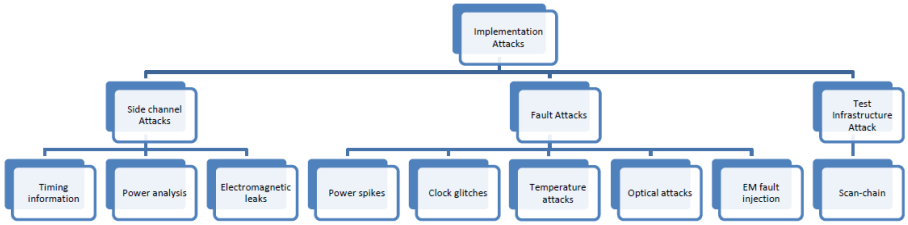

Figure 2. Classification of Attacks on Secure Hardware

The main focus of attacker is to retrieve secret key from crypto-hardware as mentioned in literature even though traditionally having multiple goals in mind. In next section, countermeasure against attacks based on test infrastructure will be examined. All mentioned attacks are practically implementable (also called Implementation attack), resulted in compromising the mostly used crypto-device.

3.1. SIDE CHANNEL ATTACKS

Side channel attacks generally are generally performed based on information gained from the non-primary interface of the physical implementation of a crypto system like timing, power and EM leaks. Based on these parameters, we have further classified the side channel attacks as below.

3.1.1. TIMING INFORMATION-BASED ATTACKS

The side-channel attack, exhibits that computing time discloses the crucial information regarding secret keys [7], [8]. The assumption made here is that how cryptographic algorithm implemented in hardware is in the knowledge of an adversary, and this attack totally relies on particular implementation. The variable run time cryptosystem can be exploited by attacker. For instance, modular algorithm RSA (m=c ˆ d mod n , where attacker wants to find private key d), where only single bit key is used determine the only square operation if key bit is reset or else multiply-square operation if key bit is set. This can be used to disclose information regarding secret key. An adversary can begin the procedure by predicating first key bit as zero or one, and observing which assumption gives the highest match between actual and guessed computing time. This procedure is repeated till all the key bits are predicted. Hence, the entire key search space is reduced. This attack is termed as computationally quite easy.

3.1.2. POWER ANALYSIS-BASED ATTACKS

There are two power kind of power analysis technique mentioned in literature: Simple Power Analysis (SPA) and Differential Power Analysis (DPA).Both of them physically measures current consumes per unit time. For example, a modular exponentiation algorithm of RSA (m=c ˆ d mod n, where attacker wants to find private key d), which performs square operation if key bit is zero and multiply operation if key bit is 1. As shown in fig. 3, the square and multiply operation are clearly visible from current traces of the device. Along with SPA attacker can also include other attack if required to retriever private key. A Differential Power Analysis (DPA) [9] that requires the knowledge of the algorithm but not its physical implementation. It is easy and cheap to perform. The basic idea is to correlate the power consumed by the device and the encryption data including the key. More advanced attack is DPA which is used to reveal multiple key bits at a time, and hence time to retrieve entire key will be reduced. The numbers of power samples are collected for thousands of iterations of cryptographic process with the help of high speed ADC (analog to digital converters) and DSO. Key bits are assumed based on collected power samples. Respective input bits are estimated from pre-assumed key bits. If this hypothesis is correct, then corresponding bits at next stage is going to be assumed. The case when assumption goes wrong, it is observed that 50% of test scenarios are appeared to similar with hypothesis. After retrieving one part of key, attack may perform brute force attack for the remaining key bits to retrieve entire key.

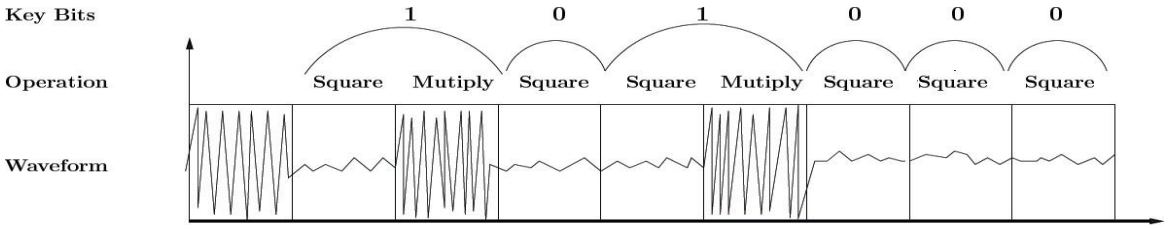

Figure 3. SPA traces of square-multiply operation of RSA [9]

3.1.3. ELECTROMAGNETIC ANALYSIS-BASED ATTACKS

These attacks are based on EM signals that are generated due to flow of current in devices [10], [11]. There are two types of Electromagnetic Analysis: Simple Electromagnetic Analysis (SEMA) and Differential Electro-Magnetic Analysis (DEMA). However, power analysis attack and electromagnetic analysis attack have certain dissimilarities. Power analysis only uses power consumption of circuit while EM analysis mainly focuses on placing antenna.

Generally, the EM attacks can be performed by attacker available from remote places. For example, Amplitude demodulators are required to carry out the attack which is quite far from circuit. EM attacks are not always perfect as they might be degraded due to being affected by environment noise and measurement errors.

3.2. FAULT ATTACKS

The basic idea behind this attack is to inject faults in a chip because the occurrence of fault may be exploited. State-of-art fault injection techniques with their properties are discussed here.

3.2.1. UNDER-POWERING AND POWER SPIKES

A very low-cost solution for fault injection method is to play around with the power supply of chip. Under-powering is a method to excite the faulty behavior. The beauty of this attack that faults invoked by this technique will occur throughout the computations and attacker can easily remove incorrect outcomes produced by non-desirable faults.

Second method is to induce high variations in power supply which in turn results in erroneous computation. Not only misinterpretation/skipping of an instruction but also memory related faulted can be resulted by high power supply spikes. For example, the memory location can be read at the time of power supply spike by microprocessor, it may result in erroneous data read from memory bus. The main motive of an attacker using this technique is to change program counter or a loop bound [12], [13], [14]. In both the fault injection technique are simple in hardware implementation but in need of an adversary to direct control over the supply rails of the chip.

3.2.2. CLOCK GLITCHES

The clock signal attack is only possible the chip which is powered by external clock. The external clock circuit can be disturbed by different clock, i.e. a signal that has many pulses having short time period. As shown in figure 4, the glitch in clock signal can be injected with much shorter time period, Tg, than the normal clock period TCLK. With this method, processor can be made to execute upcoming instruction earlier than the normal time which causes invalid data to be stored on memory address [12], [15]. Using this method to induce faults, attacker must have access to clock line. (E.g. smartcard). Clock glitches can be invoked by hardware equipment called low end FPGA board [16], [14].

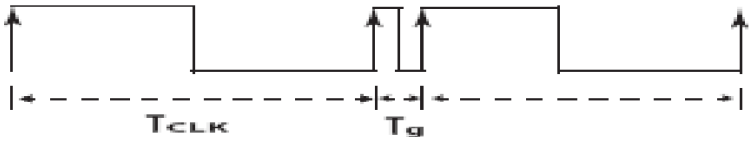

Figure 4. A glitch in the clock signal

3.2.3. TEMPERATURE ATTACKS

The functionality of hardware device is proper in typical temperature range. When subjected to very high/low temperature may invoke faults [17], [18], [19]. This technique is used to tamper data saved in memory, but segment of data cannot be focused.

3.2.4. OPTICAL ATTACKS

Optical faults are typically introduced by a strong light source like photo flash or laser beam [20] to a bare chip. Laser exposure make semiconductor device to conduct or switch. With the help of focused ion beam (FIB), one bit saved in memory can be flipped. Top side or bottom side of IC can be attacked as shown in fig. 5.

As metal layers are always on front side, it is hard to reach at transistors located at front side. The other method is to reach the transistor through a specific wavelength laser light from back side by adequate penetration in substrate.

Nowadays, the laser spot is constantly shrinking which again is limited by a wavelength of photons.

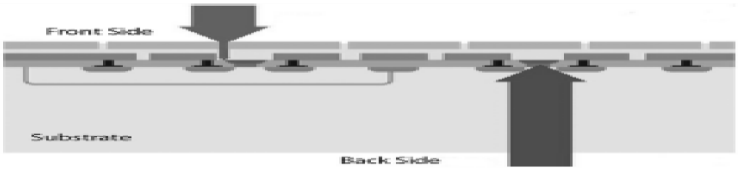

Figure 5. The effect of focused laser beam [21]

A smaller spot size 6×1.4μm can be achieved by a diode-based laser [21]. Furthermore, precise timing for exposure of laser is adapted by triggering mechanism of laser station, which in turn causes multiple faults in very short duration of time i.e. multi-glitching.

3.2.5. ELECTROMAGNETIC (EM) FAULT INJECTION

Inducing electromagnetic field to a chip can cause malfunctioning to the memory data. Electromagnetic field causes eddy current to flow on chip surface which will result in one-bit fault in memory [22]. A simple method to induce EM fault is to use gas lighter [23]. All presented fault injection techniques works on same principle: by changing physical property of chip, they make transistor to switch improperly. But, they differ in fault injecting property. The first three techniques don't aim to a specific segment of the chip. At the same time, they are not in need of costly equipment to execute fault injection. On the contrary, EM and optical fault injection techniques focus on a restricted part of the device with requirement of highly expensive setup.

3.3. TEST-INFRASTRUCTURE ATTACK

Testing of ICs is necessary to determine manufacturing defects in circuit and thus guarantee products quality. Nevertheless, design itself nowadays is DFT (Design for Testability-Test infrastructure) enabled in order to easy test effort and increase testability by improving fault coverage and diagnostic facility. The below section describes how existing test infrastructure is exploited for the benefit of attacker.

3.3.1. SCAN-BASED ATTACK

One of the widely used DFT techniques is to insert Scan-chain on chip, which permits to shift test patterns in and shift response out of the chip. However, Scan-based testing nowadays most common, it will impose a great security risk for crypt-chips. An attacker may use scan chain data to observe internal nodes of crypto-chips and exploit it to retrieve secret key. [2 - 6]

For instance, consider the AES algorithm implemented on hardware. The fig. 6 shows the AES algorithm along with scan-chain connected to round register (which stores internal states after each round operation).

AES algorithm can produce secure cipher text after 10 rounds if key size is 128-bit. The round register is a part of entire scan-chain on chip of SoC and round register flops position is deterministic. Attacker can run a cipher in normal mode with pre-determined plain text. The attacker can easily switch a cipher to test mode after one round. The intermediate state of a cipher can be observed by shifting out round register content. Furthermore, attacker can again run the same procedure with another plaintext having 1-bit difference. With the help of two different round register output, attacker will be able to retrieve key [24], [25].

The attack is also applicable on other symmetric ciphers like RSA, DES, and ECC. It can simply be applied using 1-bit different plaintext without knowledge of physical implementation of algorithm. Thus, it is also called differential attack. The next section deals with countermeasures against this attack in detail.

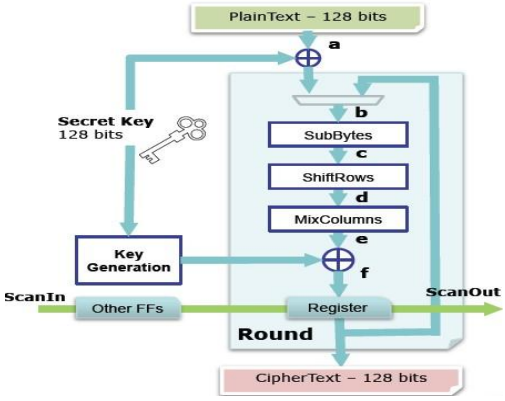

Figure 6. AES cipher and scan-chain [25]

4. COUNTERMEASURES AGAINST SCAN-BASED ATTACK ON CRYPTO-HARDWARE

In this section, state-of-art countermeasures against scan-based attack on crypto-hardware are discussed in brief. As shown in fig. 7, countermeasure can be applied during Frontend (pre-layout) or back-end design (layout) stages

4.1. BACK-END DESIGN APPROACHES

The countermeasures that are implemented through extra hardware and can be easily integrated during back-end design of crypto-chips are presented in this section.

4.1.1. BUILT-IN SELF-TEST (BIST)

Self-test procedure can be implemented by using iterative method involved in encryption process. [26] Encryption hardware is given its own output and after certain round, the output gets compared with signature. This method requires extra hardware for Test-pattern generator, response compactor and a ROM for golden signature storage on-chip. Technique can be implemented at layout level as BIST infrastructure can be included while making physical design layout. If BIST is a part of crypto-chip IP Core, it is suitable for testing and security purpose in standalone mode. Although, it is not suitable when crypto IP core is integrated with other blocks to form complete system.

4.1.2. ON-CHIP TEST COMPARISON

The method allows transferring of expected response into the chip along with scan-in test vector using the pin (that would have been scan-out pin in standard scheme) from external tester. [27] Instead of shifting it out, actual captured response is going to be compared against expected one pair-wise on-chip. After comparison only one-bit pass/fail is sent outside. Extra hardware needed on chip for comparing bit stream of actual response along with expected one. Technique can be applied at layout level as extra comparator on-chip needs to be fabricated. It is Suitable for crypto-chip IP core if core is designed along with mismatch comparator. No secret leaks out as an adversary may get notification of passing or failing using single bit for individual test pattern. This method allows diagnosis for modeled faults only. At the same time diagnosis time becomes very large.

4.2. FRONT-END DESIGN APPROACHES

Another category of countermeasures that are integrated during RTL/Behavioural description of crypto-chip are discussed here.

4.2.1. INSERTING INVERTERS IN SCAN-PATH

In this method, the entire scan-chain of chip is partitioned in several sub-chains and values of certain scan cells are complemented with the help of NOT gates inserted in the scan paths [28]. The placement of inverters is only identified by testing engineer or design engineer. This technique can be applied at behavioral level as only inverters need to be inserted in during scan-chain creation. Hardware required as extra inverters need to be fabricated along with scan FFs. Not suitable for IP Core based design as internal structure is hidden in third-party IP Cores. We may have to change DFT architecture of whole SoC. As sub-chains are inserted in arbitrary manner, it is hard for an adversary to get intermediate result of cipher. Exact response can only be retrieved by tester or designer. The flipped result will only be seen by an adversary. A method cannot resist differential attack on crypto-hardware as complementation effect will be nullified on the output difference.

4.2.2. MASKING (ROUND REGISTER OR COMPACTOR OUTPUT)

There are two masking method published in literature. First, mask round register output and then unmask it for upcoming operation. Input plaintext and key will generate mask value. During test-mode, scan cells capture the mask output of the chip. Designer can unmask and retrieve actual response. Extra hardware required as masking function has to be EX-ORed before round register and after round register (for unmasking). The method can be applied at RTL description of crypto-chip. For standalone AES IP core, it is only suitable if already masking function is built-in the core. But if AES IP core is integrated with other block of system, it's not suitable.

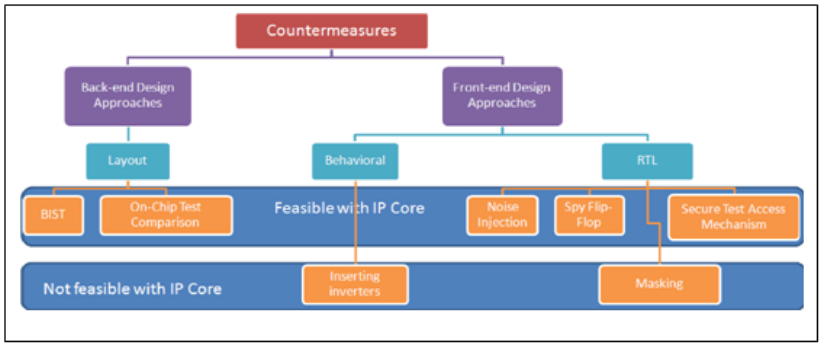

Figure 7. Classification of countermeasures against scan-based attack on crypto-hardware

Second method mask response compactor output by using (Extended LFSR) eLFSR. In test mode, the scan out compacted response is getting EX-ORed with eLFSR 128- pseudorandom bit stream. This method does not allow an adversary to recover starting status of LFSR. This also can be integrated during RTL description of crypto-chip. It is suitable for crypto IP core as only extra eLFSR required which may not change flow of encryption /description of crypto-chip. In both the method, attack will unable to retrieve actual scan-out response. Due to the area overhead and longer critical path, the performance of chip will be degraded. [24]

4.2.3. NOISE INJECTION IN SCAN OUTPUT

The method provides two level security: LFSR (linear feedback shift register) and TRNG (True Random Number Generator). In this method, only 50% of scan cell bits becoming noisy but remaining bits are not modified. Area reduction is only possible by selecting compact size LFSR because a TRNG conceal some bits of LFSR output. An approach can be included during RTL description of crypto-chip. Extra hardware requires implementing this approach for LFSR and TRNG and other combinational logic. However, area overhead reduces compared to previous

masking method. The disadvantage is to perform masking in every clock cycle to make attack unsuccessful. That means success rate is on how speedily masking is performed. [29].

4.2.4. SPY FLIP-FLOP

In this method, the extra flops (spy flops) are inserted in scan-chain. The current status of these flops is used to check scan path integrity. In functional mode, the input of spy flops is set to fixed value (s-a-1 or s-a-0). The output only varies when scan-chain is activated. Any unwanted transition from normal mode to test mode is detected. Hence, attacker cannot apply differential analysis after first iteration of cipher. The spy flops are designed at front-end level with few synthesis constraints. It is also suitable for crypto IP core if already spy flops are built-in the core description. The method can be adapted to automated design flow and IP reuse technology. However, the technique will make scan-path longer, with increase in test-time and test data volume. Hence, tester memory is also increased. [30]

4.2.5. SECURE TEST ACCESS MECHANISM

The security of crypto chips depends on small key stored in few registers while testability depends on how data and control signals are travelling to primary output through internal node. It is called secure-scan DFT method. Secure scan-DFT architecture has two modes of operation: 1.) Secure mode (Functional Mode) 2.) Insecure mode (Test Mode). When in insecure mode, the crypto chip can be switched between shift mode and normal mode same as traditional scan-based DFT. While in secure mode, it can only be in normal mode. Switching from secure to insecure mode is only done through power-off reset i.e. the round registers (Scan-flops) data will be reset by turning off power supply. The registers in secure mode hold secret key information and the content are not scanned out until being reset. While in insecure mode, fake test key is applicable. The method can be applied in RTL description of crypto chip. To hold secret key related information extra set of registers needs to be inserted. Test session starting needs to be changed and hence test controller modification must be required. This method is suitable for standalone crypto core. [3]

5. CONCLUSIONS

Encryption and decryption process for crypto-chips are covered in this paper. Although being one of the most popular DFT method, scan insertion in crypto devices, opens a backdoor for security threat. Secret key can be retrieved by performing attack on side-channels, injection faults in devices or exploiting existing test-infrastructure. Survey of state-of-art countermeasures against scan-based attack is presented. Area overhead and increase in test time are driving performance parameters to find out countermeasure that balance between security and testability of hardware.

ACKNOWLEDGEMENTS

The authors would like to thank research progress committee members Dr. K. S. Dasgupta and Dr. Virendra Singh for detail review, insightful comments and constructive suggestions.

REFERENCES

[1] Schneier, Bruce,Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons, 1996

[2] B. Yang, K. Wu, R. Karri, “Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard,” Proceedings of IEEE International Test Conference. 2004 pp. 339- 344.

[3] B. Yang, K. Wu, R. Karri, “Secure Scan: A Design-for-Test Architecture for Crypto Chips,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 25 (10) (2006) 2287-2293.

[4] Y. Liu, K. Wu, R. Karri, "Scan-based Attacks on Linear Feedback Shift Register Based Stream Ciphers," In ACM Transactions on Design Automation of Electronic Systems (TODAES), 2011, 16, 2, 1-15.

[5] R. Nara, K. Satoh, M. Yanagisawa, T. Ohtsuki, N. Togawa, "Scan-based side-channel attack against RSA cryptosystems using scan signatures," IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 12, 2481-2489.

[6] R. Nara, N. Togawa, M. Yanagisawa, T. Ohtsuki, "Scan-based attack against elliptic curve cryptosystems," 15th IEEE Asia and South Pacific Design Automation Conference (ASP-DAC10). 407-412.

[7] Kocher, P. C. (1996). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz (Ed.), CRYPTO, Lecture Notes in Computer Science (Vol. 1109, pp. 104113). Berlin:Springer.

[8] Dhem, J. -F. , Koeune, F. , Leroux, P. -A. , Mestr, P. , Quisquater, J. J. & Willems, J. -J. (1998). A practical implementation of the timing attack. In J. Quisquater & B. Schneier (Eds.). CARDIS, Lecture Notes in Computer Science (Vol. 1820, pp. 167-182). Berlin: Springer.

[9] Paul Kocher, Joshua Jaffe, and Benjamin Jun, "Differential Power Analysis", Advances in Cryptology -CRYPTO 99, LNCS 1666, Aug. 1999, pp. 388-397

[10] Quisquater, J. -J. , Samyde, D. (2001). ElectroMagnetic analysis (EMA): Measures and counter-measures for smart cards. In I. Attali & T. P. Jensen (Eds.), E-smart, Lecture Notes in Computer Science (Vol. 2140, pp. 200210). Berlin: Springer.

[11] Gandolfi, K. , Mourtel, C. , Olivier, F. (2001). Electromagnetic analysis: concrete results. In . K. Ko et al. [cKKNP01], (pp. 251261).

[12] O. Kommerling and M. G. Kuhn, "Desig Principles for Tamperresistant Smartcard Processors," in Proceedings of the USENIX Workshop on Smartcard Technology. Berkeley, CA, USA: USENIX Association, 1999, pp. 22.

[13] C. Aumuller, P. Bier, W. Fischer, P. Hofreiter, and J. -P. Seifert, "Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures," 2002.

[14] J. Balasch, B. Gierlichs, and I. Verbauwhede, "An In-depth and Blackbox Characterization of the Effects of Clock Glitches on 8-bit MCUs," in Workshop on Fault Diagnosis and Tolerance in Cryptography, ser. FDTC 2011. Washington, DC, USA: IEEE Computer Society, 2011, pp. 105114.

[15] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The Sorcerers Apprentice Guide to Fault Attacks," Proceedings of the IEEE, vol. 94, no. 2, pp. 370382, Feb. 2006.

[16] S. Endo, T. Sugawara, N. Homma, T. Aoki, and A. Satoh, "An On-chip Glitchy Clock Generator for Testing Fault Injection Attacks," Journal of Cryptographic Engineering, vol. 1, pp. 265270, 2011.

[17] I. Peterson, "Chinks in Digital Armor: Exploiting Faults to Break Smartcard Cryptosystems," Science News, vol. 151, pp. 7879, 1997.

[18] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," in 16th Annual International Conference on Theory and Application of Cryptographic Techniques, ser. EUROCRYPT 1997, Berlin, Heidelberg, 1997, pp. 3751.

[19] S. Skorobogatov, "Low Temperature Data Remanence in Static RAM," University of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CL-TR-536, Jun.-2002. [Online]. Available: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-536.pdf

[20] S. P. Skorobogatov and R. J. Anderson, "Optical Fault Induction Attacks," in International Workshop on Cryptographic Hardware and Embedded Systems -CHES 2002, 2002, pp. 212.

[21] J. Van Woudenberg, M. Witteman, and F. Menarini, "Practical Optical Fault Injection on Secure Microcontrollers," in Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2011), Sept. 2011, pp. 9199.

[22] J. -J. Quisquater and D. Samyde, "Eddy current for Magnetic Analysis with Active Sensor," in Esmart 2002, Nice, France, Sept. 2002.

[23] J. -M. Schmidt and M. Hutter, "Optical and EM Fault-Attacks on CRTbased RSA: Concrete Results," in Austrochip 2007, 15th Austrian Workhop on Microelectronics, 11 October 2007, Graz, Austria, Proceedings, J. W. Karl C. Posch, Ed. Verlag der Technischen Universitat Graz, 2007, pp. 6167.

[24] J. DaRolt, G. Di Natale, M. L. Flottes and B. Rouzeyre, "Scan Attacks and Countermeasures in Presence of Scan Response Compactors," 2011 Sixteenth IEEE European Test Symposium, Trondheim, 2011, pp. 19-24.

[25] J. Da Rolt, G. Di Natale, M. L. Flottes and B. Rouzeyre, "Are advanced DfT structures sufficient for preventing scan-attacks?" 2012 IEEE 30th VLSI Test Symposium (VTS), Hyatt Maui, HI, 2012, pp. 246-251

[26] G. D. Natale, M. Doulcier, M. L. Flottes and B. Rouzeyre, "Self-Test Techniques for Crypto-Devices," in IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, vol. 18, no. 2, pp. 329-333, Feb. 2010.

[27] Da Rolt, J. , Di Natale, G. , Flottes, M. L. , Rouzeyre, B. , "On-chip test comparison for protecting confidential data in secure ICS," In 2012 17th IEEE European Test Symposium (ETS), p. 1, May 2012

[28] Sengar, G. , Mukhopadhayay, D. , Roy Chowdhury, D. ,"An efficient approach to develop secure scan tree for crypto-hardware," In International Conference on Advanced Computing and Communications, ADCOM 2007, pp. 2126, December 2007

[29] A. Das, B. Ege, S. Ghosh, L. Batina and I. Verbauwhede, "Security Analysis of Industrial Test Compression Schemes," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 32, no. 12, pp. 1966-1977, Dec. 2013.

[30] David Hly , Frdric Bancel , Marie-Lise Flottes , Bruno Rouzeyre, "A secure scan design methodology", Proceedings of the conference on Design, automation and test in Europe: Proceedings, March 06-10, 2006, Munich, Germany.