Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results

Jörn-Marc Schmidt[1,2] and Michael Hutter[2]

[1]Secure Business Austria (SBA),
Favoritenstraße 16, 1040 Vienna, Austria
[2]Institute for Applied Information Processing and Communciations (IAIK),
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
{joern-marc.schmidt, michael.hutter}@iaik.tugraz.at

Abstract

RSA is a well-known algorithm that is used in various cryptographic systems like smart cards and e-commerce applications. This article presents practical attacks on implementations of RSA that use the Chinese Remainder Theorem (CRT). The attacks have been performed by inducing faults into a cryptographic device through optical and electromagnetic injections. We show optical attacks using fibre-optic light guides. Furthermore, we present a new non-invasive electromagnetic fault-attack using high-frequency spark gaps. All attacks have been performed using low-cost equipment.

Keywords: *Fault Attacks, EM Attacks, Optical Fault-Injections, CRT-RSA.*

1 Introduction

Side-channel attacks are among the most powerful attacks against cryptographic devices nowadays. They exploit interesting information that is leaked by the device in order to disclose its secret. A common way to access a side-channel source is to measure the power consumption of the device while it performs cryptographic operations. The so-called Differential Power Analysis was first introduced by P. Kocher et al. [13] in 1998 and it makes use of statistical methods to extract the secret key. There are also electromagnetic emanations [1, 9], timing informations [12], or even sound side-channels [18] that can be used to recover sensitive data. Besides passive attacks which do not conspicuously interfere the device under attack, there exist active attacks which influence the system by applying external or internal changes, e.g. the temperature or the power supply. Optical fault-injection attacks are a typical example of active attacks which require the decapsulation of the chip from its package. In addition, these attacks can be performed with slight effort and low-cost equipment. In [20], S. Skorobogatov and R. Anderson induced optical faults in a smart card by using a simple laser pointer or a flashgun of a conventional camera.

Another kind of active attacks are electromagnetic fault-attacks. In contrast to optical fault-injections, electromagnetic attacks avoid the need of decapsulating the chip from its package and they allow attacks to be performed at a distance. J.-J. Quisquater and D. Samyde [16] presented EM fault-attacks using eddy currents in order to affect the behavior of the cryptographic device. They have been able to insert permanent and transient faults into transistors and memory cells of common smart-card processors.

Fault attacks pose a serious threat in cryptographic systems and they can be applied on a multitude of physical implementations of various cryptographic algorithms like AES [7], DES [5], ECC [4], or RSA [8].

In particular, RSA [17] is one of the most common public-key algorithms and it is widely used in common smart-card payment and electronic-commerce systems. The Chinese Remainder Theorem (CRT) is applied in practice in order to increase the calculation speed of the signature generation process. Actually, a speed-up improvement by a factor of about four is achieved. However, there are many publications so far which discuss fault-injection attacks on CRT-based RSA implementations. The first fault attack has been announced by Boneh et al. [8] in 1996. The so-called Bellcore attack extracts the secret by factoring the RSA modulus using one faulty and one correct RSA signature. A. Lenstra [14] improved the attack and showed that the RSA modulus can be factorized by using only one faulty signature. Furthermore, Biham et al. [5] introduced the term Differential Fault Analysis and presented a related hardware-fault attack that can be applied on secret-key cryptosystems like DES. Nevertheless, there are many articles that focus on theoretical fault-models and countermeasures, see for example [23, 2, 6, 22, 10, 8], but there are only two publications so far which provides results of practical investigations. C. Aumüller et al. [3] presented concrete results on how to attack CRT-based RSA using non-invasive spike attacks that have been coupled into the power-supply lines of a cryptographic device. C. H. Kim and J.-J. Quisquater showed that some fault countermeasures for RSA using CRT can be defeated by non-invasive methods [11].

In this article, we present practical investigations of optical and electromagnetic fault-injection attacks on an implementation of the CRT-based RSA signature-generation process. First, we present optical fault-injection attacks on a decapsulated microcontroller using a simple fibre-optic light guide. Second, we provide practical results of a new electromagnetic fault-injection attack on a capsulated, rear-side decapsulated, and front-side decapsulated microcontroller. This article is the first article that discusses concrete results of optical and EM fault-injection attacks on CRT-based RSA. All attacks have been performed at low cost.

This article is organized as follows. In Section 2, the attack on the CRT-based RSA algorithm is described. Section 3 describes the measurement setups in order to perform optical and electromagnetic fault-analysis. Section 4 presents the results of the attacks. Conclusion is given in Section 5.

2 Review - Attacking the CRT-based RSA Algorithm

Let $n = pq$ denote a RSA modulus, where p and q are two large prime numbers (e.g. 1024 bits). Let d denote a private exponent and $e = d^{-1} \bmod \varphi(n)$ the corresponding public exponent. Furthermore, let $z = \text{CRT}\ (x, y)$ denote the CRT recombination of the value $z \in \mathbf{Z}_n$ from values x, y of the subgroups $\mathbf{Z}_p$ and $\mathbf{Z}_q$ where

$$\text{CRT}\ (x, y) = xc_p + yc_q \bmod n$$

with $c_p = q\ (q^{-1} \bmod p)$ and $c_q = p\ (p^{-1} \bmod q)$. This method is often called Gauss's algorithm [15].

In general, the CRT is used in order to optimize the signature generation $S = m^d \bmod n$ of a message m. As opposed to calculate the modulus of n, the modulus of each prime is calculated using the following equation:

$$S = \text{CRT}\ ((m^d \bmod p), (m^d \bmod q)) \bmod n.$$

Boneh et al. [8] showed that it is possible to factor the RSA modulus if an error Δ occurs during the signature generation. Note that it is entirely unimportant neither what kind of fault has been induced nor the time when the fault has occured during the computation of the signature parts. A faulty calculation of the signature S leads to a faulty signature that we further denote as $\tilde{S}$:

$$\begin{aligned} \tilde{S} &= \text{CRT}\ ((m \bmod p)^d, (m \bmod q)^d + \Delta) \bmod n \\ &= m^d + \Delta p\ (p^{-1} \bmod q) \bmod n. \end{aligned}$$

Now, if the attacker is in possession of both a faulty signature and a correct signature, the modulus n can be easily factorized by calculating

$$p = \gcd(\tilde{S} - S, n).$$

As A. Lenstra has shown in [14], it is also possible to factorize the modulus by holding the input m and one faulty signature $\tilde{S}$. It can be calculated using the following equation:

$$p = \gcd(\tilde{S}^e - m, n).$$

In this article, we consider a rather simple fault model. Every fault-injection that results in an error during the modulo computation of one prime will succeed the attack. Thus, we do not have to fulfill time-critical constrains due to the fact that the calculation of the CRT-based RSA of our implementation takes at least several seconds. Moreover, we can neglect exact positioning issues of optical and electromagnetic sensors in order to affect specific parts of the device under attack. It is of no importance whether the faulty computation is caused by SRAM switches, register variations, or excecution changes.

3 Fault-Injection Setups

This chapter describes the setup used in order to perform optical and electromagnetic fault-injection attacks. For both kind of attacks, an own evaluation board has been designed. Each device has a microcontroller on the board. In addition, the microcontrollers have been programmed with a CRT-based RSA software implementation which neither have any hardware protections enabled nor that have any software countermeasures implemented in order to prevent fault attacks. The CRT-based RSA implementation uses a square and multiply algorithm to compute the two partial RSA signatures. Furthermore, a PC has been connected to the evaluation boards to communicate over the serial interface. The CRT-based RSA is thereby used in a challenge-response protocol.

3.1 Optical Fault-Injection Attacks

The idea of optical fault-injections has been firstly presented by S. Skorobogatov and R. Anderson [20] in 2003. The photon of a light beam can cause SRAM cells to switch. Basically, a photon that hits a metal plate can behave as follows. If the photon has an energy more than 1.1 eV, an electron-hole pair is created. The electron absorbes the single photon whereas the electron is liberated from atomic binding. An eletric field like in a transistor can separate the pair, which results in current [21]. This is termed photovoltaic effect. The induced current may cause SRAM cells to switch. However, S. Skorobogatov and R. Anderson used a modified laser pointer in combination with a microscope in order to get a concentrated light beam. They have been able to flip single bits in memory rather reliably after they have decapsulated the chip from its package.

Nevertheless, we present a way to circumvent the need of a proper and cost-intensive microscope in order to perform optical fault-injection attacks. Note that our fault model allows the use of less accurate light-injections since we are not up to flip single bits in the circuit. We thus designed a board where we have assembled a simple laser

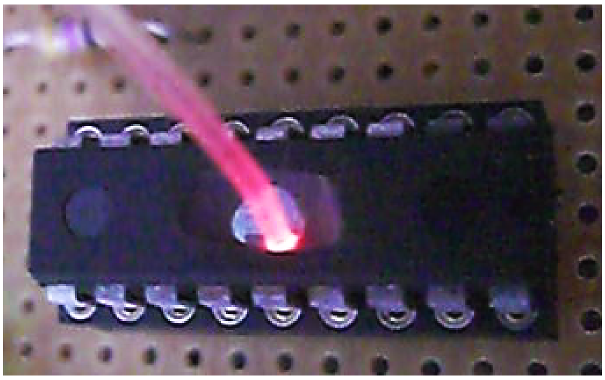

Figure 1. Laser attack on a microcontroller using a fibre-optic light guide

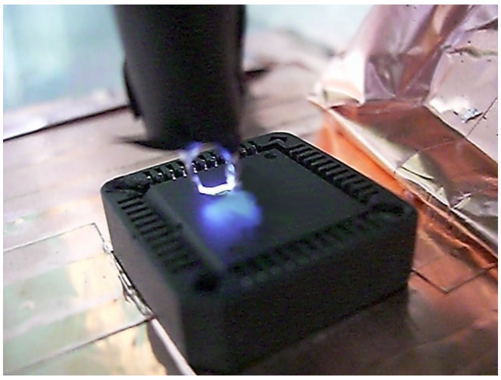

Figure 2. Spark-gap burst right above the surface of a microcontroller

diode as a light source for our investigations. The laser diode emitts a light beam of 100 mW with a wavelength of 785 nm. Furthermore, we used a fibre-optic light guide that has been attached onto the laser diode using an according light-guide port. The light guide has a cross-section dimension of 1 mm. As a trigger signal for the light diode the output port of the microcontroller has been used. It is also possible to set the trigger manually using an on/off-switch. The device under attack is an 8-bit microcontroller that has a flash-memory size of 1 KByte and 68 KByte of SRAM. The microcontroller has been clocked by a 9.216 MHz crystal oscillator.

3.2 Electromagnetic Fault-Injection Attacks

The first article that discusses electromagnetic investigations on cryptographic devices using EM fault-injections has been published by J.-J. Quisquater and D. Samyde [16]. They pointed out that it is possible to influence devices using a simple self-made EM probe [16]. They have used a camera flash-gun to inject a high voltage into the coil of the probe. This high voltage causes a magnetic field that then again generates an eddy current on the surface of the chip. This current leads to faulty computations.

We have followed another approach by using high-frequency spark gaps instead of magnetic fields. The induced spark gaps involve a very fast change of the flowing current. In addition, this leads to a very strong electromagnetic burst and radiation, respectively, which can be measured even at a very large distance. The characterization of such high-frequency EM pulses is a rather difficult task and needs appropriate measurement setups. The setup of the EM fault-attack and the measurement setup to characterize the EM spark-gaps are described in the following.

The overall electromagnetic measurement setup has been carried out onto an Earth Reference Plane (ERP). We used an aluminium plate that has a length of about two meters and a width of about 1 meter. Every device which has been used during the measurement has been placed on top of this plate. The plate itself has been connected to the earth ground in order to provide the same capacitive potential for all devices involved by the measurement process.

For the electromagnetic fault-injection attack the following devices have been used: the microcontroller board, power supply, PC, spark-gap generator, and a digital oscilloscope. The used microcontroller has an 8-bit architecture. It has 12 KByte of internal flash memory and it has 256 Bytes of static RAM. The spark-gap generator consists of a simple gas lighter that can be bought at almost every tool store. Of course, the gas has been removed so as to provide only the spark-generation assembling. We further attached a coaxial cable to our spark generator. The endpiece of the coaxial cable now consists of two cables that form an air gap which in fact constitutes the spark gap. Figure 2 shows a generated spark gap right above the surface of a microcontroller. However, the greater the spacing of the gap the stronger will be the EM burst. If the spacing of the gap is greater than the distance to a surrounding conductor, for example the decapsulated chip-surface, the generated spark is discharged into the die of the chip. Our experiments showed that this can lead to a total destruction of the chip.

In addition to our ERP plate, we mounted another smaller aluminium plate at right angle to the ERP plate. This plate serves as an additional shield against electromagnetic radiation that is caused by the spark-generator. At the front side of the shield, we have placed a PLCC socket including the microcontroller. Moreover, the shield contains a tiny hole which is used to connect the socket of the microcontroller with the rest of the board, i.e. the power-supply connectors, the crystal oscillator, and the serial-interface circuit. The device under attack has been placed on front of the shield, the rest of the devices have been placed behind the shield. Furthermore, we fixed all cables that are involved with a copper tape which has a contact to the ERP plate as well. For contact-based high-voltage protection, we used ferrite cores that are plugged onto cables which are connected to the PC, the digital oscilloscope, and the power-supply unit. This shielded environment avoids the measurement of interfering signals caused by the generated sparks.

In order to characterize the induced voltage, we have

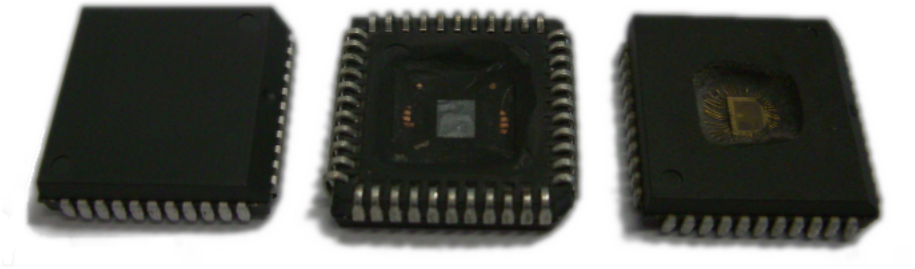

Figure 3. Capsulated, rear-side decapsulated, and front-side decapsulated microcontroller

assembled a special measuring bar in front of the microcontroller. The measuring bar allows a very accurate positioning of the endpiece of our spark-generator. It has a precision of 100 µm.

We have characterized the induced voltage of three different chip-capsulation scenarios. First, a standard capsulated microcontroller has been used. Second, the rear-side of the microcontroller has been removed and the induced voltage has been measured. In the third scenario, a front-side decapsulated microcontroller has been used to inject faults into the die surface of the chip. In Figure 3, the capsulated, rear-side decapsulated, and front-side decapsulated microcontroller is shown.

The decapsulation process of the front-side package has been accomplished in two steps. First, a hole has been milled into the front side of the chip package. Second, a fuming nitric acid has been poured into the hole. After that, the chip has been cleaned in a beaker with acetone by ultrasonic treatment. The last step has to be repeated until the surface of the die has been exposed.

The rear-side decapsulation of the chip can be carried out without the need of chemicals. It is possible to mill a hole into the rear-side package. Under the substrate layer of the chip exists a copper plate that can be easily removed using a screw driver [19].

4 Results

This section will present the results of the performed optical and electromagnetic fault-injection attacks. All attacks have been performed successfully.

4.1 Optical Fault-Injection Attacks

The first step of our attack has been to fix the light guide direct above the SRAM of the microcontroller (see Figure 1). The location of the SRAM on the die surface can be found by using a common loupe or microscope. The light beams have been injected manually. The experiments showed that various bits of the SRAM memory cells can be flipped. Due to the imprecise concentration of the light beam, we have not been able to set specific bits of the memory. Nevertheless, the attack has led the microcontroller to compute faulty signatures of the CRT-based RSA algorithm.

4.2 Electromagnetic Fault-Injection Attacks

First, we have performed electromagnetic fault-injection attacks on a capsulated microcontroller. Second, we have characterized the induced voltage by measuring the power consumption of the device. Three different capsulation scenarios (capsulated, rear-side decapsulated, and front-side decapsulated) have been considered in order to discuss the differences.

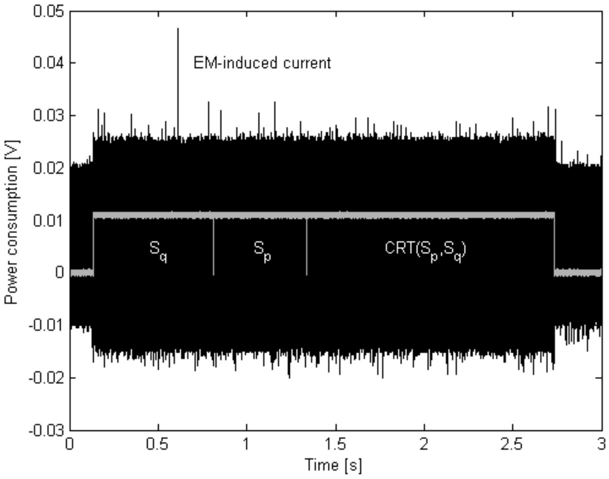

Figure 4. Power-consumption trace during EM fault-injections

In Figure 4, the power consumption during the computation of the CRT-based RSA is shown. The black signal denotes the power consumption whereas the gray line indicates the trigger signal. The computation of the signatures S_q and S_p and the computation of the CRT are clearly discernable. After approximately 600 milliseconds from the beginning of the RSA computation, an EM spark has been generated on the front-side of the chip. The EM power-injection is clearly observable as a peak in the power-consumption trace. Thus, the computation of S_q has been disturbed while the computation of S_p remaind correct. However, this single fault has led to a successful

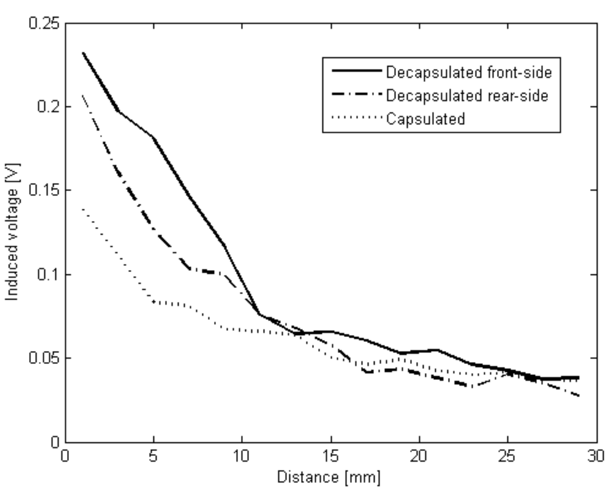

Figure 5. Induced voltage of three different decapsulation methods

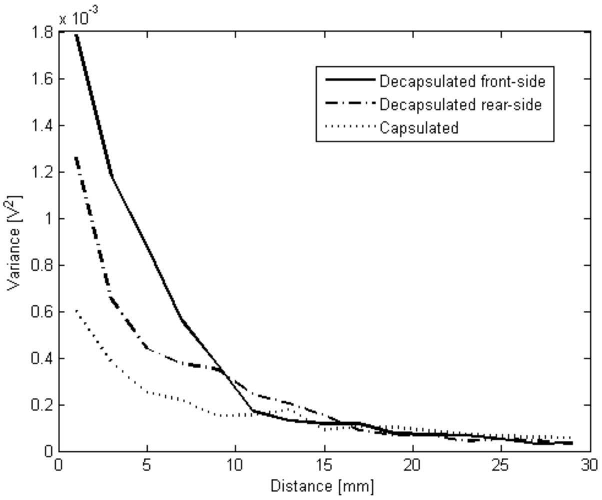

Figure 6. Variance of the induced voltages of three different decapsulation methods

attack and the modulus n of the faulty signature computation has been successfully factorized.

Other experiments showed that the faults can affect program flow as well as the SRAM content. During the research we have also injected errors that affected the flash memory. For a couple of hours, various bytes of the memory have not been programmable any more. The chip recovered completely after tens of hours.

Next, we have investigated the difference between the decapsulation scenarios. Therefore, we have measured the voltage, which has been induced into the device, using the oscilloscope. The sampling rate of the oscilloscope has been set to 4 GS/s due to the fact that the injected EM pulses have a duration of only a few nanoseconds. Furthermore, we have used the measuring bar in front of the chip surface in order to vary the distance between the chip and the generated spark gap. Figure 5 shows the results of the experiment. As expected, the most current has been injected in the front-side decapsulated microcontroller. Notice that the success probability of the fault-injection attacks on the front-side decapsulated microcontroller is higher than on the capsulated or even rear-side decapsulated microcontroller. The lowest voltage has been induced into the conventional capsulated microcontroller. However, after a distance of about 10 mm from the die surface of the chip, the same voltage has been induced in all kinds of the performed attacking scenarios.

In Figure 6, the variance of the induced voltages of the three different decapsulation methods is shown. It turns out that the variance of the induced voltages decreases the higher the distance to the die surface of the chip.

5 Conclusion

This article presents low-cost methods to attack CRT-based RSA implementations. We have performed optical and electromagnetic fault-injection attacks on a microcontroller. A new approach has been shown that uses spark gaps in order to induce high-voltage pulses during the computation of the cryptographic operations. Furthermore, we investigated the impact of EM injections on three different decapsulation methods. All attacks have been performed successfully and at low cost.

Acknowledgements.

The authors would like to thank Gunter Winkler for a lot of fruitful discussions and his help with the measurement setup as well as Christoph Marschner for his help with the chip-decapsulation procedure. This work has been funded by the *Secure Business Austria (SBA)* research center.

References

[1] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The EM Side-channel(s). In Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, volume 2523 of *Lecture Notes in Computer Science*, pages 29–45. Springer, 2003.

[2] Ross J. Anderson and Markus G. Kuhn. Low Cost Attacks on Tamper Resistant Devices. In M. Lomas et al. editor, *Security Protocols, 5th International Workshop*, volume 1361 of *Lecture Notes in Computer Science*, pages 125–136. Springer, 1997.

[3] Christian Aumüller, Peter Bier, Wieland Fischer, Peter Hofreiter, and Jean-Pierre Seifert. Fault Attacks on RSA with CRT: Concrete Results and Practical

Countermeasures. In Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, volume 2523 of *Lecture Notes in Computer Science*, pages 260–275. Springer, 2002.

[4] Ingrid Biehl, Bernd Meyer, and Volker Müller. Differential Fault Attacks on Elliptic Curve Cryptosystems. In Mihir Bellare, editor, *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, volume 1880 of *Lecture Notes in Computer Science*, pages 131–146. Springer, 2000.

[5] Eli Biham and Adi Shamir. Differential Fault Analysis of Secret Key Cryptosystems. In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, volume 1294 of *Lecture Notes in Computer Science*, pages 513–525. Springer, 1997.

[6] Johannes Blömer, Martin Otto, and Jean-Pierre Seifert. A new CRT-RSA algorithm secure against bellcore attacks. In Sushil Jajodia, Vijayalakshmi Atluri, and Trent Jaeger, editors, *Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS 2003, Washington, DC, USA, October 27-30, 2003*, pages 311–320. ACM, October 2003.

[7] Johannes Blömer and Jean-Pierre Seifert. Fault Based Cryptanalysis of the Advanced Encryption Standard (AES). In Rebecca N. Wright, editor, *Financial Cryptography, 7th International Conference, FC 2003, Guadeloupe, French West Indies, January 27-30, 2003, Revised Papers*, volume 2742 of *Lecture Notes in Computer Science*, pages 162–181. Springer, January 2003.

[8] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the Importance of Checking Cryptographic Protocols for Faults (Extended Abstract). In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceedings*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer, 1997.

[9] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In Çetin Kaya Koç, David Naccache, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, volume 2162 of *Lecture Notes in Computer Science*, pages 251–261. Springer, 2001.

[10] Marc Joye, Arjen K. Lenstra, and Jean-Jacques Quisquater. Chinese Remaindering Based Cryptosystems in the Presence of Faults. *Journal of Cryptology*, 12(4):241–245, December 1999. ISSN 0933-2790.

[11] Chong Hee Kim and Jean-Jacques Quisquater. Fault Attacks for CRT Based RSA: New Attacks, New Results, and New Countermeasures. In Damien Sauveron, Constantinos Markantonakis, Angelos Bilas, and Jean-Jacques Quisquater, editors, *Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems, First IFIP TC6 / WG 8.8 / WG 11.2 International Workshop, WISTP 2007, Heraklion, Crete, Greece, May 9-11, 2007, Proceedings.*, volume 4462 of *Lecture Notes in Computer Science*, pages 215–228. Springer, 2007.

[12] Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, number 1109 in Lecture Notes in Computer Science, pages 104–113. Springer, 1996.

[13] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.

[14] Arjen K. Lenstra. Memo on RSA signature generation in the presence of faults, September 1996.

[15] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. Series on Discrete Mathematics and its Applications. CRC Press, 1997. ISBN 0-8493-8523-7, Available online at http://www.cacr.math.uwaterloo.ca/hac/.

[16] Jean-Jacques Quisquater and David Samyde. Eddy current for magnetic analysis with active sensor. In *Proceedings of Esmart*, pages 185–194, 2002.

[17] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978. ISSN 0001-0782.

[18] Adi Shamir and Eran Tromer. Acoustic cryptanalysis - On nosy people and noisy machines. http://www.wisdom.weizmann.ac.il/

~tromer/acoustic/. preliminary proof-of-concept presentation.

[19] Sergei P. Skorobogatov. *Semi-invasive attacks - A new approach to hardware security analysis*. PhD thesis, University of Cambridge - Computer Laboratory, 2005. Available online at http://www.cl.cam.ac.uk/TechReports/.

[20] Sergei P. Skorobogatov and Ross J. Anderson. Optical Fault Induction Attacks. In Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, volume 2523 of *Lecture Notes in Computer Science*, pages 2–12. Springer, 2003.

[21] K.T. Tan, S.H. Tan, and S.H. Ong. Functional failure analysis on analog device by optical beam induced current technique. In *Physical & Failure Analysis of Integrated Circuits, 1997., Proceedings of the 1997 6th International Symposium on*, pages 296–301. IEEExplore, July 1997.

[22] David Wagner. Cryptanalysis of a provably secure CRT-RSA algorithm. In Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick Drew McDaniel, editors, *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC, USA, October 25-29, 2004*, pages 92–97. ACM, October 2004.

[23] Sung-Ming Yen, Sang-Jae Moon, and JaeCheol Ha. Hardware Fault Attack on RSA with CRT Revisited. In Pil Joong Lee and Chae Hoon Lim, editors, *Information Security and Cryptology - ICISC 2002, 5th International Conference Seoul, Korea, November 28-29, 2002, Revised Papers*, volume 2587 of *Lecture Notes in Computer Science*, pages 374–388. Springer, 2003.