SIDE CHANNEL ATTACKS AND FAULT ATTACKS ON CRYPTOGRAPHIC ALGORITHMS

L. Batina, P. Buysschaert, E. De Mulder, N. Mentens, S.B. Örs, B. Preneel, G. Vandenbosch, I. Verbauwhede

K.U.Leuven, Department Electrical Engineering–ESAT,
Kasteelpark Arenberg 10, B-3001 Leuven, Belgium

ABSTRACT

In the mid 1990s cryptanalysis was extended from a research area that focused mainly on theoretical work to practical implementations. In 1996 Kocher introduced the idea that a cryptosystem can be broken by use of a side channel, i.e. timing information or power consumption. This triggered a whole new research area in cryptanalysis which also includes attacks based on electromagnetic radiation and hardware faults. This paper gives an overview on these so-called implementation attacks which can be applied to both secret key and public key cryptosystems. It summarizes relevant recent work; it covers both attacks and countermeasures, and outlines some research challenges.

Key words: cryptography, cryptanalysis, side channel attacks, fault attacks, countermeasures.

1 INTRODUCTION

Secure communication is of crucial importance in everyday digital applications. Examples are digital signatures, encryption of data, secure e-mail, financial transactions, e-commerce, etc. Cryptographic algorithms are essential building blocks of various security protocols. These algorithms can be implemented both in software and hardware. Software solutions are cheaper and more flexible, while hardware implementations provide more speed and intrinsic security. A trade-off in cost and speed can be achieved by hardware-software co-design.

A smart card is an example of a platform where the core part, *i.e.* the most computation intensive part, is hardware-based and some other building blocks of cryptographic protocols can run on a processor. Smart cards are cryptographic tokens that are used more and more nowadays in financial applications, e-government, health insurance, etc. Because of

the computation complexity and the constraints in speed and area it is vitally important to focus on efficient implementations of the algorithms.

On the other hand, the security of the implementation also needs to be considered. Namely, attacks on cryptographic algorithms are usually divided into mathematical (theoretical) and implementation (practical) attacks. The latter are based on weaknesses in the implementation and can be passive or active. Passive attacks are also called side-channel attacks as they benefit from side channel information which is achieved by measuring some physical quantity. More precisely, while secret data are being processed they can be deduced by observing the execution time, the power consumption, the electromagnetic radiation, etc. The second type of implementation attacks, *i.e.* the active attacks, are more invasive as they are based on the introduction of faults which result in erroneous calculations leading to the exposure of the secret key. The usual cause of these faults can be sudden changes, *i.e.* glitches, in various parameters such as power supply, clock, voltage, temperature, etc. An attacker could also use a light flash with equipment such as a camera flash or a laser in order to induce a fault. In the following, we will explain implementation attacks in more detail and give some examples as well.

This paper is organized as follows. Section 2 and Sect. 3 describe timing and power attacks respectively, which are often combined. In Sect. 4 we introduce electromagnetic attacks. Countermeasures are similar for all passive implementation attacks and are given in Sect. 5. Section 6 deals with fault attacks and countermeasures. Conclusions and open problems are presented in Sect. 7.

2 TIMING ANALYSIS ATTACKS

Timing analysis attacks are based on the fact that algorithms with a non-constant execution time can leak secret information. A non-constant execution time can be caused by conditional branches in the algorithm, various optimization techniques, cache hits [57], etc.

In 1996 Kocher [30] described timing based attacks on public key algorithms such as RSA, Diffie-Hellman, etc. The usual targets for the RSA cryptosystem are implementations using the Montgomery multiplication algorithm [37] and the CRT technique [46]. In [49] Schindler *et al.* presented a timing attack against RSA with Montgomery multiplication which allows to break 512-bit RSA with only 5000 timing measurements. The non-constant execution time is the consequence of the conditional reduction in the algorithm of Montgomery [48, 49]. Another timing attack on the RSA cryptosystem can be found in [59].

In [30] Kocher also outlines some ideas on potential attacks on secret key algorithms such as DES, IDEA, etc. Handschuh and Heys explained how to perform a timing attack on RC5 in [26].

Unlike power attacks, the use of these attacks is not restricted to cryptographic tokens. Timing attacks can also be applied to network based cryptosystems [9] and to other applications whenever the attacker can get hold of timing information.

An example of an algorithm which is vulnerable to a timing attack is given in Algorithm 1. It is the main part of Elliptic Curve (EC) protocols such as EC digital signature algorithm, EC Diffie-Hellman key exchange, etc. [27]. In this algorithm a point P on an elliptic curve is multiplied with a scalar k which represents the secret key. It is easy to see that Step 5 of the algorithm is performed only if the processed key bit is 1. Otherwise this step is skipped. This difference is observable in timing as well as in the power trace. Therefore, the attacker can use this knowledge to recover information about the secret key.

Algorithm 1 Elliptic Curve Point Multiplication

Require: EC point $P = (x, y)$, $k = (k_{l-1}, k_{l-2}, \cdots, k_0)_2$, $k_{l-1} = 1$
Ensure: $Q = (x', y') = kP$
1: $Q \leftarrow P$
2: **for** i from $l-2$ downto 0 **do**
3: $\quad Q \leftarrow 2Q$
4: $\quad$ **if** $k_i = 1$
5: $\quad\quad Q \leftarrow Q + P$

The obvious way to prevent timing attacks is to implement cryptographic algorithms with a constant execution time. For example, an improved version of the Montgomery multiplication algorithm should be used which excludes any conditional operation by adjusting the bound on the Montgomery parameter [58].

All modern implementations tend to be time constant which makes a timing-only attack impossible. However, the threat remains in combining timing information with other side-channels. For example, timing information can be used by an attacker in order to locate specific parts of the algorithm.

3 POWER ANALYSIS ATTACKS

Nowadays, CMOS is by far the most commonly used technology to implement digital integrated circuits. The dominating factor for the power consumption of a CMOS gate is the dynamic power consumption. Two types of power consumption leakage can be observed. The *transition count leakage* gives information about the number of changed bits, while the *Hamming weight leakage* is related to the number of 1 bits being processed simultaneously.

Two types of power analysis attacks are distinguished. In a *simple power analysis* (SPA) attack, an attacker uses the side-channel information from one measurement directly to determine (parts of) the secret key. In *differential power analysis* (DPA), many measurements are used in order to filter out noise. While SPA exploits the relationship between the operations that are executed and the power leakage, DPA exploits the relationship between the processed data and the power leakage.

In DPA, an attacker uses a so-called hypothetical model of the attacked device. The model is used to predict several values for the side-channel output of a device. These predictions are compared to the measured side-channel output of the device. The most popular comparison ways are the *distance-of-mean test* and the *correlation analysis*. For the correlation analysis, the model predicts the amount of side-channel leakage for a certain moment of time in the execution [44].

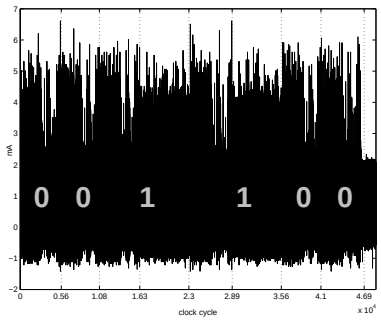

Figure 1: Power consumption trace of a 160-bit EC point multiplication.

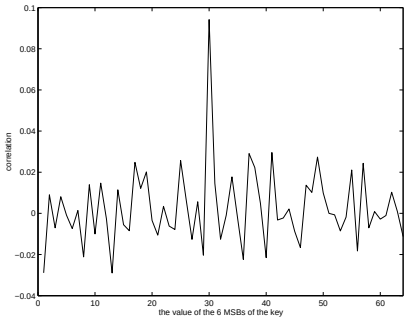

Figure 2: A correlation attack on DES.

Most research papers discuss these attacks only from a theoretical viewpoint, such as [8]; there are very few exceptions. Practical implementations on software implementations are reported in [31, 14, 33, 39] and practical attacks on hardware implementations of block ciphers are described in [42, 53].

An SPA Attack on an FPGA Implementation of EC Cryptosystems (ECC). Typical operations in ECC are point addition and doubling that differ from each other in performed steps. In the EC doubling algorithm a modular addition/subtraction occurs in different places than in the EC point addition algorithm. This means that a simple power-analysis attack is easy to perform. The EC point multiplication is implemented with Algorithm 1. The power consumption trace of a 160-bit EC point multiplication is shown in Fig. 1. It can be easily seen that the key used during this measurement is 1001100. Our measurement setup is introduced in [43].

A DPA Attack on an FPGA Implementation of DES. In 1977, the Data Encryption Standard (DES) algorithm was adopted as a Federal Information Processing Standard for unclassified government communication [18] . DES encrypts 64-bit blocks with a 56-bit key. DES is an iterated block cipher that applies 16 rounds to the plaintext. The round function can be described as $L_{i+1} = R_i$ and $R_{i+1} = L_i \oplus f(R_i, K_i)$, $i = 0, \ldots 15$. Here $L_{16}||R_{16}$ is the ciphertext. We have performed our experiments on the sequential DES implementation that takes one clock cycle to perform one round [54]. In order to identify the correct six most significant bits (MSBs) of the final round key, we used the correlation coefficient between the measurements at $16th$ clock cycle and the power consumption prediction for $16th$ round of DES. As shown in Fig. 2, the highest correlation occurs when the key guess is $1E_{hex} = 30_{dec}$.

4 ELECTROMAGNETIC ANALYSIS (EMA) ATTACKS

The most recently published side-channel attack is based on electromagnetic emanation. The attack explores the information in the electromagnetic field that is induced by the currents flowing through each component of the cryptographic device. According to Agrawal *et al.* there are two types of emanations: intentional and unintentional [1]. The first

type results from direct current flows. The second type is caused by various couplings, modulations (AM and FM), etc.

It is well known that the US government has been aware of electromagnetic leakage since the 1950s. The resulting standards are called TEMPEST; partially declassified documents can be found in [40]. The first published papers are work of Quisquater and Samyde [47] and the Gemplus team [20]. Quisquater and Samyde showed that it is possible to measure the electromagnetic radiation from a smart card. Their measurement setup consisted of a sensor which was a simple flat coil, a spectrum analyzer or an oscilloscope and a Faraday cage. Quisquater also introduced the terms Simple EMA (SEMA) and Differential EMA (DEMA). The work of Gemplus deals with experiments on three algorithms: DES, RSA and COMP128. They observed the feasibility of EMA attacks and compared them with PA attacks in favor of the first. Namely, EM emanation can also exploit local information and, although more noisy, the measurements can be performed from a distance. This fact broadens the spectrum of targets to which side-channels attacks can be applied. Of concern are not only smart cards and similar tokens but also SSL accelerators and many other cryptographic devices.

The two papers mentioned above deal exclusively with intentional emanations. To the contrary, the real advantage over other side-channel attacks lies in exploring unintentional emanations [1]. More precisely, EM leakage consists of multiple channels. Therefore, compromising information can be available even for DPA resistant devices for which no contact measurements are available.

More theoretical considerations related to all side-channel attacks, but mainly induced by work on EMA, are also given by Agrawal *et al.* in [15]. They discussed so-called template attacks in which the attacker uses a device that is identical to the target device. The only difference is that this replica is programmable which makes it possible to handle the noise in each measurement sample. Unlike previous considerations, which all try to eliminate noise, this approach attempts to model the noise in order to extract more useful information. As an example, they detailed the template attack on RC4 using only one single measurement sample. Other case studies listed include DES and RSA exponentiation. At that moment, template attacks were envisioned as the strongest possible side-channel attacks from an information theoretical point of view, but the authors themselves came up with an even stronger approach afterwards. Namely, besides carefully exploring all available EM emanations an attacker can also focus on a combination of two or more side-channels. Agrawal *et al.* defined these so-called multi-channel attacks in which the side-channels are not necessarily of a different kind [2]. For example, they discussed combined power and EM analysis but also multi-channel DPA attacks. The former uses a CMOS leakage model and the maximum-likelihood principle for performing and analyzing. Agrawal *et al.* showed that it is even more effective than template attacks. Another example of a multi-channel attack is introduced by Walter and Thompson in [59]. They were the first to combine power and timing analysis.

Up to now, most papers on EMA applied similar techniques as power analysis while apparently much more information is available to be explored. It is likely that future work will also deal with combinations of EMA with other side channel attacks.

A SEMA Attack on an FPGA Implementation of EC Cryptosystems. Figure 3 depicts the antenna and the FPGA we have used [13]. The electromagnetic emanation

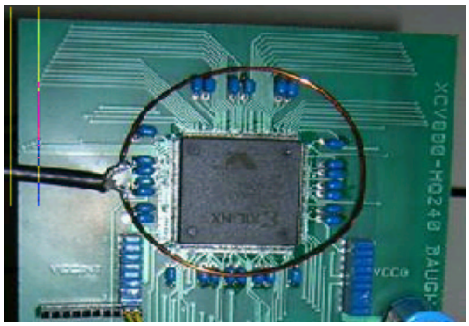

Figure 3: Measurement setup.

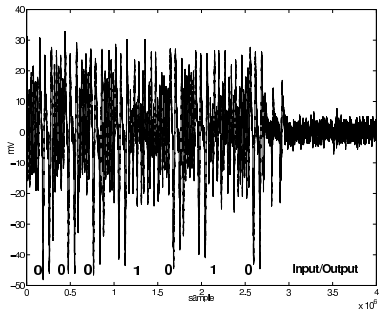

Figure 4: Electromagnetic emanation trace of a 160-bit EC point multiplication.

trace of a 160-bit EC point multiplication after amplitude (AM) demodulation is shown in Fig. 4. The measurement is done by an oscilloscope and AM demodulation is performed by MATLAB [35] . The attack is implemented on the same EC processor as mentioned in Sect. 3. It can be easily seen from Fig. 4 that the key used during this measurement is 10001010.

5 FAULT ATTACKS

Fault attacks are based on hardware faults; they were introduced by Boneh *et al.* in [10]. The idea behind the attack is as follows: if a wrong result is released the adversary can use that information to break the cryptosystem. Boneh *et al.* classified the faults into three categories. The first type are transient faults which can occur randomly causing a faulty computation to be executed. The second type are latent faults which are hardware or software bugs that are difficult to locate. The third type are induced faults for which physical access to the hardware is necessary. These are the most interesting because of the active role of the attacker. For example, optical fault induction attacks, as introduced by Scorobogatov and Anderson [50], use a flashgun targeting a transistor to change the state of a memory cell in a micro-controller. The authors have proven this optical probing to be feasible as they managed to change an arbitrary bit of an SRAM array. They also suggested to use self-timed dual-rail logic as a defense to these attacks, which could also help for power analysis attacks.

Biham and Shamir introduced differential fault attacks (DFAs) on secret key cryptosystems (SKC) in [7]. They show that it is applicable to any SKC proposed that time. In particular, they performed a DFA on DES and showed that they can recover full DES key by analyzing between 50 and 200 ciphertexts.

In [10] the fault analysis based attack on RSA with CRT is introduced. The authors showed how to factor the RSA modulus by using one faulty and one correct signature. Lenstra improved the attack by using only one faulty signature together with the message to be signed [29]. Other theoretical work on fault based attacks on RSA was published in [61, 62]. The first practical result was given by Aumüller *et al.* in [4]. They successfully introduced a spike, *i.e.* a certain deviation from a standard interval for a smart card param-

eter *e.g.* the supply voltage. Two attacks on a smart card with an RSA coprocessor were performed. In the first attack the countermeasures against fault attacks were switched off. The other attack was performed with Shamir's software countermeasures [51]. Furthermore they introduced a new software countermeasure which was resistant to these so-called spike attacks.

Differential fault attacks on EC cryptosystems were outlined in the work of Biehl *et al.* [6]. They presented three types of attacks which were verified via software simulation.

Yen and Joye demonstrated one type of new and powerful hardware fault-based attack based on the safe error concept in [60].

Fault attacks can be considered as the biggest threat of all implementation attacks as countermeasures usually include more complex techniques which are not easy to implement on constraint environment such as smart cards.

6 COUNTERMEASURES

As already mentioned, constant time-implementations should remove all vulnerabilities of cryptographic applications with respect to timing attacks. A great deal of work has been devoted to this topic [58, 12, 41].

A nice survey for countermeasures can be found in the work of Borst [11] and Mangard [34]. The main software countermeasures against PA attacks are as follows. *Time randomization* is proposed in [14, 17, 32, 45, 25, 28, 5]. In this type of countermeasure, operations occur during random intervals in an execution. *Permuting the execution* is put forward in [24]. *Masking techniques* are shown in [24, 36, 16, 3, 23, 22, 56]. The main hardware countermeasures against PA attacks are as follows. *The measurement noise can be increased* with a random number generator [17]. *Power signal filtering* can be added to the implementation [52, 16]. Several *novel circuit designs* have been suggested including detachable power supplies [52] and modifications at the logic level [55]. The latter method employs logic gates with a power consumption that is independent of the data signals and therefore the technique removes the foundation for DPA. Asynchronous circuits can be used as well [19, 38]. Usage of reversible logic in order to reverse computation which returns the consumed energy during the computation back to the circuit was considered in [21].

As EMA attacks are still under intensive development the countermeasures are an active research area. It is obvious that PA countermeasures can also be applied to EMA. However, because the EM signal contains more information than the power signal, other techniques have to be applied to defeat EMA attacks. Countermeasures can be divided into two types. The first one tries to lower the signal intensity while the second one attempts to reduce the information contained in the signal. The first type is mainly already included in the design strategy of most silicon vendors. Another example of the first type is shielding. Examples of the second type are asynchronism, dual-line logic, etc. [47, 20].

The main idea to prevent fault attacks is to check the intermediate computations as often as possible [4]. However, Yen and Joye [60] showed that checking the correctness of the

computed result before giving it to others may not be enough to prevent a hardware fault-based cryptanalysis. They suggested that cryptographic hardware designers should carefully consider each possible implementation detail when developing a secure system.

Ideally, hardware countermeasures such as sensors, filters, dual rails, etc. and software countermeasures should be applied at each level; due to smart card limitations this is usually not feasible in practice.

Acknowledgements. This work was supported in part by the FWO projects G.0141.03 and G.0450.04 and by the EU IST FP6 projects SCARD and ECRYPT.

7 CONCLUSIONS

In this paper we reviewed the current state-of-the-art in implementation attacks, *i.e.* side channel and fault attacks, and countermeasures. In the category of side channel attacks we first discussed timing attacks. These exploit the fact that algorithms with a non-constant execution time can leak secret information. Next, power and EMA attacks were dealt with. Both can be performed using simple or differential analyses. In the section on fault attacks we explained how hardware faults causing a wrong result can be used to break the cryptosystem. Finally, we lined up the most effective countermeasures that make the attacks much more difficult or even infeasible.

The challenges for the future lie in foreseeing new combinations of attacks and creative strategies of informed adversaries. Therefore, designers should know about possible attacks in other to come up with designs that are robust against side channel and fault attacks.

REFERENCES

[1] D. Agrawal, B. Archambeault, S. Chari, J. R. Rao, and P. Rohatgi. Advances in side-channel cryptanalysis. *RSA Laboratories Cryptobytes*, 6(1):20–32, Spring 2003.

[2] D. Agrawal, J. R. Rao, and P. Rohatgi. Multi-channel attacks. In C. Walter, Ç. K. Koç, and C. Paar, editors, *Proc. 5th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2779 of *LNCS*, pages 2–16. Springer-Verlag, 2003.

[3] M.-L. Akkar and C. Giraud. An implementation of DES and AES, secure against some attacks. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Proc. 3rd Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2162 of *LNCS*, pages 309–318. Springer-Verlag, 2001.

[4] C. Aumüller, P. Bier, W. Fischer, P. Hofreiter, and J.-P. Seifert. Fault attacks on RSA with CRT: Concrete results and practical countermeasures. In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *Proc. 4th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2523 of *LNCS*, pages 260–275. Springer-Verlag, 2002.

[5] L. Benini, A. Macii, E. Macii, E. Omerbegovic, M. Poncino, and F. Pro. Energy-aware design techniques for differential power analysis protection. In *Proc. the 40th Design Automation Conference (DAC)*, 2003.

[6] I. Biehl, B. Meyer, and V. Müller. Differential fault attacks on elliptic curve cryptosystems. In M. Bellare, editor, *Advances in Cryptology: Proc. CRYPTO'00*, volume 1880 of *LNCS*, pages 131–146. Springer-Verlag, 2000.

[7] E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems. In B. S. Kaliski Jr., editor, *Advances in Cryptology: Proc. CRYPTO'97*, volume 1294 of *LNCS*, pages 513–525. Springer-Verlag, 1997.

[8] E. Biham and A. Shamir. Power analysis of the key scheduling of the AES candidates. In *Proc. the Second Advanced Encryption Standard (AES) Candidate Conference*, Rome, Italy, 1999.

[9] D. Boneh and D. Brumley. Remote timing attacks are practical. In *Proc. the 12th Usenix Security Symposium*, 2003.

[10] D. Boneh, R. A. DeMillo, and R. J. Lipton. On the importance of checking cryptographic protocols for faults (extended abstract). In W. Fumy, editor, *Advances in Cryptology: Proc. EUROCRYPT'97*, volume 1233 of *LNCS*, pages 37–51. Springer-Verlag, 1997.

[11] J. Borst. *Block Ciphers: Design, Analysis and Side-Channel Analysis.* PhD thesis, K.U.Leuven, September 2001.

[12] E. Brier and M. Joye. Weierstrass elliptic curves and side-channel attacks. In D. Naccache and P. Paillier, editors, *Proc. the 5th Int. Workshop on Practice and Theory in Public Key Cryptosystems (PKC)*, volume 2274 of *LNCS*, pages 335–345. Springer-Verlag, 2002.

[13] P. Buysschaert and E. De Mulder. Elektromagnetische analyse (EMA) van een FPGA implementatie van een elliptische krommen cryptosysteem. Master's thesis, K.U.Leuven, Departement Elektrotechniek - ESAT, Belgium, 2004.

[14] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi. Towards sound approaches to counteract power-analysis attacks. In M. Wiener, editor, *Advances in Cryptology: Proc. CRYPTO'99*, volume 1666 of *LNCS*, pages 398–412. Springer-Verlag, 1999.

[15] S. Chari, J. R. Rao, and P. Rohatgi. Template attacks. In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *Proc. 4th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2523 of *LNCS*, pages 172–186. Springer-Verlag, 2002.

[16] J.-S. Coron and L. Goubin. On Boolean and arithmetic masking against differential power analysis. In Ç. K. Koç and C. Paar, editors, *Proc. 2nd Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 1965 of *LNCS*, pages 231–237. Springer-Verlag, 2000.

[17] J. Daemen and V. Rijmen. Resistance against implementation attacks: A comparative study of the AES proposals. In *Proc. the Second Advanced Encryption Standard (AES) Candidate Conference*, March 1999. `http://csrc.nist.gov/encryption/aes/round1/Conf2/aes2conf.htm`.

[18] Data Encryption Standard DES). NIST Documents, 1988. Available at: http://www.itl.nist.gov/fipspubs/fip46-2.htm.

[19] J. J. A. Fournier, S. Moore, H. Li, R. Mullins, and G. Taylor. Security evaluation of asynchronous circuits. In C. Walter, Ç. K. Koç, and C. Paar, editors, *Proc. the 5th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2779 of *LNCS*, pages 137–151. Springer-Verlag, 2003.

[20] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Proc. 3rd Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2162 of *LNCS*, pages 255–265. Springer-Verlag, 2001.

[21] J. D. Golić. DeKaRT: A new paradigm for key-dependent reversible circuits. In C. Walter, Ç. K. Koç, and C. Paar, editors, *Proc. the 5th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2779 of *LNCS*, pages 98–112. Springer-Verlag, 2003.

[22] J. D. Golić and C. Tymen. Multiplicative masking and power anaylsis of AES. In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *Proc. 4th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2535 of *LNCS*, pages 198–212. Springer-Verlag, 2002.

[23] L. Goubin. A sound method for switching between boolean and arithmetic masking. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Proc. the 3rd Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2162 of *LNCS*, pages 3–15. Springer-Verlag, 2001.

[24] L. Goubin and J. Patarin. DES and differential power analysis the "duplication" method. In Ç. K. Koç and C. Paar, editors, *Proc. the 1st Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 1717 of *LNCS*, pages 158–172. Springer-Verlag, 1999.

[25] J. C. Ha and S. J. Moon. Randomized signed-scalar multiplication of ECC to resist power attacks. In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *Proc. 4th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2523 of *LNCS*, pages 129–143. Springer-Verlag, 2002.

[26] H. Handschuh and H. M. Heys. A timing attack on RC5. In S. E. Tavares and H. Meijer, editors, *Proc. Selected Areas in Cryptography (SAC)*, volume 1556 of *LNCS*, pages 306–318. Springer-Verlag, 1998.

[27] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag, 2004.

[28] T. Izu and T. Takagi. A fast parallel elliptic curve multiplication resistant against side channel attacks. In D. Naccache and P. Paillier, editors, *Proc. the 5th Int. Workshop on Practice and Theory in Public Key Cryptosystems (PKC)*, volume 2274 of *LNCS*, pages 280–296. Springer-Verlag, 2002.

[29] M. Joye, A. K. Lenstra, and J.-J. Quisquater. Chinese remaindering based cryptosystem in the presence of faults. *Journal of Cryptology*, 4(12):241–245, 1999.

[30] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems. In N. Koblitz, editor, *Advances in Cryptology: Proc. CRYPTO'96*, volume 1109 of *LNCS*, pages 104–113. Springer-Verlag, 1996.

[31] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology: Proc. CRYPTO'99*, volume 1666 of *LNCS*, pages 388–397. Springer-Verlag, 1999.

[32] P. Y. Liardet and N. P. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Proc. 3rd Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2162 of *LNCS*, pages 391–401. Springer-Verlag, 2001.

[33] S. Mangard. A simple power-analysis attack (SPA) attack on implementations of the AES key expansion. In P. J. Lee and C. H. Lim, editors, *Proc. 5th Int. Conference on Information Security and Crytography (ICISC)*, volume 2587 of *LNCS*, pages 343–358. Springer-Verlag, 2002.

[34] S. Mangard. *Securing Implementations of Block Ciphers Against Side-Channel Attacks*. PhD thesis, Institute for Applied Information Processing and Communications (IAIK), TU Graz, 2004.

[35] The MathWorks. Available at: http://www.itl.nist.gov/fipspubs/fip46-2.htm.

[36] T. S. Messerges. Securing the AES finalists against power analysis attacks. In B. Schneier, editor, *Proc. the 7th Int. Workshop on Fast Software Encryption Workshop (FSE)*, volume 1978 of *LNCS*. Springer-Verlag, 2000.

[37] P. Montgomery. Modular multiplication without trial division. *Mathematics of Computation*, Vol. 44:519–521, 1985.

[38] S. Moore, R. Anderson, R. Mullins, G. Taylor, and J. Fournier. Balanced self-checking asynchronous logic for smart card applications. *to appear in the Microprocessors and Microsystems Journal*, 2003.

[39] R. Novak. Side-channel attack on substitution blocks. In J. Zhou, M. Yung, and Y. Han, editors, *Proc. the First Int. Conference on Applied Cryptography and Network Security (ACNS)*, volume 2846 of *LNCS*, pages 307–318. Springer-Verlag, 2003.

[40] NSA. NSA TEMPEST Documents. `http://www.cryptome.org/nsa-tempest.htm`.

[41] K. Okeya, H. Kurumatani, and K. Sakurai. Elliptic curves with the Montgomery-form and their cryptographic applications. In H. Imai and Y. Zheng, editors, *Proc. the 3rd Int. Workshop on Practice and Theory in Public Key*

Cryptography (PKC), volume 1751 of *LNCS*, pages 238–257. Springer-Verlag, 2000.

[42] S. B. Örs, F. K. Gürkaynak, E. Oswald, and B. Preneel. Power-analysis attack on an ASIC AES implementation. In *Proc. the Int. Conference on Information Technology (ITCC)*, 2004.

[43] S. B. Örs, E. Oswald, and B. Preneel. Power-analysis attacks on an FPGA – first experimental results. In C. Walter, Ç. K. Koç, and C. Paar, editors, *Proc. the 5th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2779 of *LNCS*, pages 35–50. Springer-Verlag, 2003.

[44] E. Oswald. *On Side-Channel Attacks and the Application of Algorithmic Countermeasures*. PhD thesis, Institute for Applied Information Processing and Communications (IAIK), TU Graz, Inffeldgasse 16a, A–8010 Graz, Austria, June 2003.

[45] E. Oswald and M. Aigner. Randomized addition-subtraction chains as a countermeasure against power attacks. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Proc. the 3rd Int. Workshop on Cryptograpic Hardware and Embedded Systems (CHES)*, volume 2162 of *LNCS*, pages 39–50. Springer-Verlag, 2001.

[46] J.-J. Quisquater and C. Couvreur. Fast decipherment algorithm for RSA public-key cryptosystem. *Electronics Letters*, 18:905–907, October 1982.

[47] J.-J. Quisquater and D. Samyde. Electromagnetic analysis (EMA): Measures and counter-measures for smard cards. In I. Attali and T. Jensen, editors, *Proc. the Int. Conference on Research in Smart Cards: Smart Card Programming and Security (E-smart)*, volume 2140 of *LNCS*, pages 200–210. Springer-Verlag, 2001.

[48] W. Schindler. A timing attack against RSA with the chinese remainder theorem. In C. Paar and Ç. K. Koç, editors, *Proc. the 2nd Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 1965 of *LNCS*, pages 109–124. Springer-Verlag, 2000.

[49] W. Schindler, F. Koeune, and J.-J. Quisquater. Unleashing the full power of timing attack. Technical Report 2002-3, UCL Crypto Group, 2002.

[50] S. P. Scorabogatov and R. J. Anderson. Optical fault induction attacks. In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *Proc. the 4th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2523 of *LNCS*, pages 2–12. Springer-Verlag, 2002.

[51] A. Shamir. Method and apparatus for protecting public key schemes from timing and fault attacks. US patent number 5,991,415, November 1999.

[52] A. Shamir. Protecting smart cards from passive power analysis with detached power supplies. In C. Paar and Ç. K. Koç, editors, *Proc. the 2nd Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 1965 of *LNCS*, pages 71–77. Springer-Verlag, 2000.

[53] F.-X. Standaert, S. B. Örs, and B. Preneel. Power analysis attack on an FPGA implementation of AES. In *Proc. the 6th Int. Workshop on Cryptograpic Hardware and Embedded Systems (CHES)*, LNCS. Springer-Verlag, 2004.

[54] F.-X. Standaert, S. B. Örs, B. Preneel, and J.-J. Quisquater. Power analysis attacks against FPGA implementations of DES. In *Proc. Int. Conference on Field-Programmable Logic and its Applications (FPL)*, LNCS. Springer-Verlag, 2004.

[55] K. Tiri and I. Verbauwhede. Securing encryption algorithms against DPA at the logic level: Next generation smart card technology. In C. Walter, Ç. K. Koç, and C. Paar, editors, *Proc. 5th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2779 of *LNCS*, pages 125–136. Springer-Verlag, 2003.

[56] E. Trichina, D. De Seta, and L. Germani. Simplified adaptive multiplicative masking for AES. In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *Proc. 4th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2535 of *LNCS*, pages 187–197. Springer-Verlag, 2002.

[57] Y. Tsunoo, T. Saito, T. Suzaki, M. Shigeri, and H. Miyauchi. Cryptanalysis of DES implemented on computers with cache. In C. Walter, Ç. K. Koç, and C. Paar, editors, *Proc. the 5th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2779 of *LNCS*, pages 62–76. Springer-Verlag, 2003.

[58] C. D. Walter. Precise bounds for Montgomery modular multiplication and some potentially insecure RSA moduli. In B. Preneel, editor, *Proc. Topics in Cryptology- CT-RSA*, volume 2271 of *LNCS*, pages 30–39. Springer-Verlag, 2002.

[59] C. D. Walter and S. Thompson. Distinguishing exponent digits by observing modular subtractions. In D. Naccache, editor, *Proc. Topics in Cryptology - CT-RSA*, volume 2020 of *LNCS*, pages 192–207. Springer-Verlag, 2001.

[60] S.-M. Yen and M. Joye. Checking before output may not be enough against fault-based cryptanalysis. *IEEE Transactions on Computers*, 49(9):967–970, September 2000.

[61] S.-M. Yen, S. J. Moon, and J. C. Ha. Hardware fault attacks on RSA with CRT revisited. In P. J. Lee and C. H. Lim, editors, *Proc. the 5th Int. Conference on Information Security and Cryptology - (ICISC)*, volume 2587 of *LNCS*, pages 374–388. Springer-Verlag, 2002.

[62] S.-M. Yen, S. J. Moon, and J. C. Ha. Permanent fault attack on the parameters of RSA with CRT. In R. Safavi-Naini and J. Seberry, editors, *Proc. the 8th Australasian Conference on Information Security and Privacy (ACISP)*, volume 2727 of *LNCS*, pages 285–296. Springer-Verlag, 2003.