An Effective Active Attack on Fiat-Shamir Systems

Artemios G. Voyiatzis and Dimitrios N. Serpanos

{bogart,serpanos}@ee.upatras.gr

Department of Electrical and Computer Engineering
University of Patras
GR-26500 Rion Patras
Greece

Abstract

Hardware or side-channel cryptanalysis, in contrast to mathematical cryptanalysis, targets on implementations of cryptographic algorithms and exploits *side-channels*, which transmit information of the secret components of the cryptosystem. In passive hardware cryptanalysis, attacks measure parameters of the implementation, such as execution delay of a cryptographic algorithm, power consumption and EM radiation, while in active hardware cryptanalysis, attacks are implemented through injections of hardware faults that cause faulty computations and result to leakage of secret key information. Active attacks, also known as the Bellcore active attacks, target implementations of RSA using Chinese Remainder Theorem or Montgommery arithmetic, Schnorr's scheme and the Fiat-Shamir identification scheme.

In this paper, we focus on the Fiat-Shamir identification scheme, which is widely used in environments with resource-limited clients, such as smart-cards. We provide a proof that the Bellcore attack on Fiat-Shamir systems is incomplete and we demonstrate that, there exist configurations of Fiat-Shamir systems that can defend against the Bellcore attack. Finally, we introduce a new active (hardware) attack and we prove that it is effective against all possible Fiat-Shamir configurations. This new attack is not only successful, but efficient and realistic for typical resource-limited environments like smart cards.

Keywords: Side-channel attacks, active attacks, Bellcore attack, hardware faults, Fiat-Shamir identification scheme.

1 Introduction

Side-channel cryptanalysis [13][14] has introduced a new class of (hardware) attacks, which are applied to implementations of cryptographic algorithms and exploit a *side-channel* that transmits information of the secret components of an algorithm. These attacks are classified as active and passive, depending on the implementation of the side-channel. Passive hardware attacks target some measurable parameter of the implementation, such as power consumption [16] [17], time delay of the execution of a cryptographic algorithm [15] [10] and lately electromagnetic radiation [1] [12] [18]. In contrast, active hardware attacks insert faults in data of cryptographic calculations [6] [7] [8]; such attacks can be realized, for example, by operating a cryptosystem in extreme conditions or by destroying gates [2] [3].

Active hardware attacks were introduced with the development of the well-known Bellcore attack [8] [9], which targets the implementations of RSA using Chinese Remainder Theorem, RSA using Montgommery arithmetic, Schnorr's scheme and the Fiat-Shamir identification scheme. These theoretical attacks were verified through simulation as well [4]; furthermore, practical experiments have been carried for the case of RSA/CRT [5]. Simulations have shown that all theoretical active attacks are complete, with the exception of the Fiat-Shamir identification scheme, where there is indication that, in general, there may be system configurations, where the Bellcore attack is not successful.

In this paper, we focus on the Fiat-Shamir identification scheme. The scheme is widely used in environments with resource-limited clients, such as smart-cards, whose population is increasing at a dramatic rate. We have proven that the Bellcore attack is not successful, in general, on systems implementing the Fiat-Shamir scheme, because it is based on an assumption which is not always true: one can construct a full-rank $\ell \times \ell$ matrix over $\mathbb{Z}_2$. Taking advantage of the conditions under which this assumption does not hold, we describe Precautious Fiat-Shamir, a version of the original Fiat-Shamir scheme, which successfully defends against the Bellcore attack; however, the scheme is weak against alternative active attacks which are extensions of the original one, as we describe with an attack that requires the same resources (as the Bellcore attack) in order to obtain secret information [4]. This extended attack leads to a need for increased computational and memory resources to impersonate a legitimate user. Thus, it is ineffective and unrealistic when targeted to resource-limited environments, such as smart-cards. Considering that active attacks target systems with limited resources, we introduce a new active attack model, which is not only successful but efficient and realistic for these environments as well.

The paper is organized as follows. Section 2 describes the Fiat-Shamir identification scheme, the fault insertion model and the Bellcore attack. Section 3 introduces a configuration of the Fiat-Shamir protocol, called Precautious Fiat-Shamir scheme, which defends against the attack, and proves its correctness. Section 4 introduces an extension of the Bellcore attack, which is successful against Precautious Fiat-Shamir. Finally, we introduce our new active attack model, which is successful and efficient in limited resource environments.

2 Background

The Fiat-Shamir identification scheme [11] is a zero-knowledge authentication scheme, where one party, say Alice, authenticates her identity to another, say Bob, using an asymmetric method based on a public key. The scheme works as follows. Alice has an n-bit modulus N, where N is the product of two large prime numbers, and a set of invertible elements $s_1, s_2, \ldots, s_\ell \pmod N$. Alice's public key is the set $PK_\ell = \{u_i \mid u_i = s_i^2 \pmod N \text{ and } 1 \leq i \leq \ell\}$. Alice proves her identity to Bob using the following communication protocol:

1. Alice and Bob agree on the security parameter, ℓ;
2. Alice chooses a random number $r \in \mathbb{Z}_N^*$, calculates $r^2 \bmod N$ and sends this number to Bob;
3. Bob chooses a random subset $S \subseteq \{1, \ldots, \ell\}$ and sends S to Alice;
4. Alice computes $y = r \cdot \prod_{i \in S} s_i \bmod N$ and sends y to Bob;
5. Bob verifies Alice's identity by checking that the following holds:

$$y^2 = r^2 \cdot \prod_{i \in S} u_i \pmod N$$

The security of the scheme is based on the hypothesis that computation of square roots is a hard problem over $\mathbb{Z}_N$ (this is believed to be equivalent to factoring N).

2.1 Bellcore attack on Fiat-Shamir Identification Scheme

Bellcore attack [8], introduced by Boneh, De Millo and Lipton and revised in [9], is a theoretical active attack model that exploits erroneous cryptographic computations. The attack models derive secret keys for various cryptographic protocols. In the case of Fiat-Shamir identification scheme, Bob can derive Alice's secret elements, $s_1, \ldots, s_\ell \pmod N$. The attack assumes that it is possible to introduce transient bit flips during Alice's computations. Specifically, Bob introduces bit flips in r, during Step 3 of the communication protocol described above, while Alice waits for Bob to send the subset S. Then, Alice's computation in Step 4 is made with an incorrect value of r. This leads to Bob's ability to calculate Alice's secret elements. Bellcore attack on Fiat-Shamir identification scheme is summarized in the following theorem:

Theorem 1. *Let N be an n-bit modulus and ℓ the predetermined security parameter of the Fiat-Shamir protocol. Given ℓ erroneous executions of the protocol one can recover the secret $s_1, \ldots, s_\ell$ in the time it takes to perform $O(n\ell + \ell^2)$ modular multiplications.*

Proof 1. (summarized) A bit-flip at bit position i, $i \in \{0, 1, \ldots, n-1\}$, in r changes its original value by adding the value E, where $E = \pm 2^i$; the sign of the change depends on whether the bit-flip caused a 0-to-1 or a 1-to-0 change.

When the bit-flip occurs, Alice calculates (and sends Bob) an incorrect value of y, denoted as $\hat{y}$, during Step 4 of the protocol:

$$\hat{y} = (r + E) \cdot \prod_{i \in S} s_i$$

From this, Bob can compute

$$T(S) = \prod_{i \in S} s_i = \frac{2E \cdot \hat{y}}{\frac{\hat{y}^2}{\prod_{i \in S} u_i} - r^2 + E^2} \bmod N$$

Bob validates the correctness of his bit-flip guess by checking that

$$T^2(S) = \prod_{i \in S} u_i$$

Since we have a method to compute $T(S)$ for various sets S, we need an algorithm to derive each $s_1, s_2, \ldots s_\ell$. If Alice accepts singleton sets, then the algorithm is trivial: Bob can choose $S = \{k\}$ and then, $T(S) = s_k$. Thus, Bob needs only ℓ iterations to collect all ℓ possible s_i's.

However, if Alice does not accept singleton sets, Bob can follow the following algorithm. Bob can map each set S to its characteristic binary vector $U \in \{0,1\}^\ell$, i.e. $U(i) = 1$ if $i \in S$. Now, if Bob can construct an $\ell \times \ell$ full rank matrix over $\mathbb{Z}_2$, then Bob can derive each s_i. For example, in order to determine s_1, Bob constructs elements $a_1, a_2, \ldots, a_\ell \in \{0,1\}$, so that

$$a_1 U_1 + \ldots + a_\ell U_\ell = (1, 0, 0, \ldots, 0) \pmod 2$$

This is efficient, because vectors $U_1, \ldots, U_\ell$ are linearly independent over $\mathbb{Z}_2$. When computations are made over the integers, we have:

$$a_1 U_1 + \ldots + a_\ell U_\ell = (2b_1 + 1, 2b_2, 2b_3, \ldots, 2b_\ell)$$

for some known $b_1, \ldots, b_\ell$. Then, Bob calculates s_1 as:

$$s_1 = \frac{T_1^{a_1} \cdots T_l^{a_\ell}}{u_1^{b_1} \cdots u_\ell^{b_\ell}} \pmod N$$

The overall complexity of the algorithm is $O(n\ell + \ell^2)$ modular multiplications [9].

3 Defense against Bellcore attack

Bellcore attack identifies that the Fiat-Shamir identification scheme breaks very easily when $|S| = 1$, i.e., when Alice accepts singleton index sets, and assumes that it is reasonable for Alice to deny to accept such singleton S sets. However, it presents the attack described above, which derives Alice's secret elements even when Alice accepts index sets S with $|S| \geq 2$.

The ability to have Alice deny singleton S sets motivated our work: we introduce the concept that Alice may be able to judge and/or decide what sets S to accept. So, in the following, we evaluate Bellcore attack under the assumption that Alice accepts specific sizes for the index sets S. Our evaluation originates from the claim in the proof of Theorem 1. that a full rank matrix can be always constructed over $\mathbb{Z}_2$.

Assuming that Alice accepts only specific sizes for S, in the following, we denote the set of acceptable (by Alice) sizes for the index set as $G = \{n_1,\ n_2,\ \ldots,\ n_k\}$.

Using this notation, one can easily verify that, for even ℓ and $\{2, \ell - 1\} \subseteq G$, the following matrix B_e of characteristic vectors constitutes a full rank matrix over $\mathbb{Z}_2$:

$$B_e = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{\ell-1} \\ b_{le} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \ldots & 0 & 1 \\ 0 & 1 & \ldots & 0 & 1 \\ & & \ddots & & \\ 0 & 0 & \ldots & 1 & 1 \\ 1 & 1 & \ldots & 1 & \mathbf{0} \end{bmatrix}$$

Accordingly, for odd ℓ and $\{2, \ell\} \subseteq G$ the matrix B_o of characteristic vectors constitutes a full rank matrix over $\mathbb{Z}_2$:

$$B_o = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{\ell-1} \\ b_{lo} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 & 1 \\ 0 & 1 & \dots & 0 & 1 \\ & & \ddots & & \\ 0 & 0 & \dots & 1 & 1 \\ 1 & 1 & \dots & 1 & \mathbf{1} \end{bmatrix}$$

Thus, in conclusion, Bellcore attack is effective under these assumptions, because one can always construct a full rank matrix.

However, it is possible to choose G in such a way, so that it is impossible to construct a full-rank matrix; this renders Bellcore attack ineffective. As an example, consider the case where $l = 3$ and $G = \{2\}$; in this case $\{2, \ell\} \nsubseteq G$. For this example, there are only three possible vectors: $(1, 0, 1), (0, 1, 1)$ and $(1, 1, 0)$. Furthermore, over $\mathbb{Z}_2$, $(1, 0, 1) + (0, 1, 1) = (1, 1, 0)$. Hence, the "only" possible $\ell \times \ell$ matrix

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

has rank 2 and not 3 as required for Bellcore attack to be effective. Thus, Bellcore attack is not effective in the case of the example.

The analysis above indicates that there exists a relationship between the Hamming weight of the characteristic vectors, $w(u) = \sum u_i$ and the rank of the matrix they can formulate. In the following, we establish this relationship. For our analyses we denote as $V_2(\ell)$ the set of vectors of $\mathbb{Z}_2^\ell$ with even Hamming weight.

In [19], we prove the next two propositions that we will use in our analysis:

Proposition 1. For every $a, b \in \mathbb{Z}_2^n$ the Hamming weight of their sum is:

- **even**, if $w(a), w(b)$ are both even or both odd;
- **odd**, otherwise.

Proposition 2. $V_2(\ell)$ is a subspace of $\mathbb{Z}_2^\ell$. Its dimension is $dim(V_2(\ell)) = \ell - 1$.

3.1 The "Precautious Fiat-Shamir Identification Scheme"

We define a variation of the original Fiat-Shamir identification scheme, which changes slightly the third step (Step 3) of the communication protocol used in the Fiat-Shamir scheme. The new scheme is defined as follows:

Definition 1. A Fiat-Shamir Identification Scheme augmented with a set G of even numbers is called *precautious*, if Alice accepts on the third step only S, such that $|S| \in G$.

By definition, if it could be $G = \{1, 2, \dots, \ell\}$, then the scheme is the original Fiat-Shamir identification scheme. If $G \subset \{1, 2, \dots, \ell\}$, we argue that the scheme offers equivalent security as the original one. The security of the scheme is solely based on the difficulty of factoring a product over $\mathbb{Z}_N$ and on the diffusion effect of the random number r. The original scheme's security is not based on the exact number of factors of a given product. The defined Precautious Fiat-Shamir scheme does not disclose any selection of an individual s_i, but rather limits the total number of factors of a protocol reply y. Furthermore, there is no known work, where the total number of factors of a number over $\mathbb{Z}_N$ provides any evidence of the factors themselves.

The Precautious Fiat-Shamir identification scheme provides good defense characteristics against Bellcore attack, as proven in the following theorem:

Theorem 2. If Alice implements Precautious Fiat-Shamir Identification Scheme, then Bellcore attack is not effective.

Proof 2. Bellcore attack is effective when one can construct an $\ell \times \ell$ full rank matrix which has as columns (or rows) elements of $V_2(\ell)$.

According to Proposition 2., $V_2(\ell)$ has dimension $\ell - 1$. Thus, any ℓ vectors from $V_2(\ell)$ are linearly dependent, and use of any such ℓ vectors as rows (or columns) in an $\ell \times \ell$ matrix, results to a matrix rank at most $\ell - 1$.

4 A New Attack on the Precautious Fiat-Shamir Scheme

4.1 Strength of the Precautious Fiat-Shamir Scheme

We proved that the Bellcore attack is unsuccessful, since a device that judges the nature of challenges can defend against it. The new set of acceptable challenges, $V_2(\ell)$, is approximately half of $\mathbb{Z}_2^\ell$. Thus, the probability of impersonation is reduced by a factor of two and becomes $2^{-\ell+1}$. However, with this slight modification, the Bellcore attack can not derive Alice's secret elements, $s_1, \ldots, s_\ell$.

Since the set G contains even numbers, the set of acceptable challenges will be a subset of $V_2(\ell)$. Following the methodology of the Bellcore attack, one could give challenges such as their characteristics vectors to be linear independent. By Proposition 2., such a set of vectors exists and $\ell - 1$ erroneous executions of the protocol will suffice to impersonate Alice. Thus, a simple adaptation of the Bellcore attack to the new space, $V_2(\ell)$, is enough to impersonate Alice.

In Section 3, we provided a configuration for the implementation of the Fiat-Shamir scheme, with $\ell = 3$ and $G = \{2\}$, which defended against the Bellcore attack. Here, we apply the extended attack to this example and demonstrate its success.

In this case, $\ell = 3$ and $G = \{2\}$, thus $G_S = 3$. Alice can produce three products in total: s_1s_2, s_1s_3, s_2s_3. Without loss of generality, we assume that, after two erroneous protocol invocations, the first step of the extended Bellcore attack has derived s_1s_2 and s_1s_3. Then, in the second step, we compute the remaining product as follows. As the characteristic vectors $(1,1,0)$ and $(1,0,1)$ are linearly independent, we can express: $(0,1,1) = a_1(1,1,0) + a_2(1,0,1)$; so, $a_1 = a_2 = 1$. Respectively, we can compute $b_1 = 1$, $b_2 = 0$, $b_3 = 0$. So, we derive s_2s_3:

$$\frac{(s_1s_2)^{a_1}(s_1s_3)^{a_2}}{u_1^{b_1}u_2^{b_2}u_3^{b_3}} \pmod N == \frac{s_1^2s_2s_3}{u_1} \pmod N = s_2s_3 \pmod N$$

So, after two erroneous protocol invocations, we have all possible replies that Alice can produce (recall that it is Alice who controls the random number r in the first step of the protocol). Thus, we can impersonate Alice successfully, although she implements the Precautious Fiat-Shamir identification scheme.

The impersonation information collected using this attack is not always useful for practical implementations. In the case a smart card is the object of the attack, the new, fraudelent smart card, will need to either compute in real-time the correct responses using the collected information, or precompute all possible replies. The former approach introduces a detectable timing overhead for performing the extra modular multiplications. Such time increases can be a strong indication of a fraudelent smart card. The latter approach is not feasible, since the size of all possible replies is exponential with respect to ℓ; a smart card has very limited memory resources and thus a careful selection of ℓ can protect against this attack.

4.2 A new attack on the Fiat-Shamir identification scheme

In the previous section, we showed that the Fiat-Shamir Identification Scheme can defend against known active attacks, if properly implemented. In this section, we propose a new theoretical active attack model which is successful against both the classical and precautious Fiat-Shamir schemes. This model allows Bob to derive Alice's secret elements in polynomial time, in all cases.

4.2.1 Fault model

We assume that single transient bit flips can occur during the computation of the reply, in Step 4 of the Fiat-Shamir identification scheme. Furthermore, we assume that an error can be introduced in any s_i, before Alice starts the computation of the reply $r \prod_{i \in S} s_i$, in Step 4 of the protocol. Thus, Bob (the attacker) needs to solve both time and space isolation problems, because he cannot control in time this step of the protocol. In this context, our assumption of the fault model is stronger than the corresponding assumption of Bellcore's attack, because we need exact synchronization with the device that acts as Alice (i.e., the probability of introducing an error is smaller). In contrast, Bellcore attack needs to solve only the space isolation problem.

Similarly to Bellcore attack, our model is effective for multiple bit flips, with increased complexity.

4.2.2 Revised Theoretical Active Attack

Using the predefined fault model, our attack is percepted in the following theorem.

Theorem 3. Let N be an n-bit modulus and ℓ the predetermined security parameter of the Fiat-Shamir protocol. Given ℓ erroneous executions of the protocol one can recover the secret $s_1, \ldots, s_\ell$ in the time it takes to perform $\mathrm{O}(n\ell^2)$ modular multiplications.

Proof 3. Assume that a single bit flip occurs during a protocol invocation, in Step 4. Bob can detect that an error indeed occurred in Step 5 of the protocol. Without loss of generality, let us assume that the error occurred in s_j. Then, we derive s_j as follows.

Since a single bit flip occurred, s_j was changed in Step 4 to $s_j \pm 2^i$, for some $0 \leq i \leq n-1$. After such a protocol invocation, Bob has collected the following numbers (during the corresponding protocol steps):

Step 2:

$$r_1^2 \pmod N$$

Step 4:

$$\hat{y} = r_1(s_j \pm 2^i) \prod_{k \in S - s_j} s_k \pmod N$$

The following simple operations allow Bob to derive s_j, if Bob knows that the error indeed occurred in s_j.

$$\begin{aligned}
C_1 &= \frac{\hat{y}^2}{r_1^2} \pmod N = && (1)\\
&= (s_j \pm 2^i)^2 \prod_{k \in S - s_k} s_k^2 \pmod N && (2)\\
C &= \frac{C_1}{\prod_{i \in S} u_i} \pmod N = && (3)\\
&= \frac{u_j + 2^{2i} \pm 2^{i+1} s_j}{u_j} \pmod N && (4)\\
s_j &= \pm \frac{u_j(C-1) - 2^{2i}}{2^{i+1}} \pmod N && (5)
\end{aligned}$$

During this calculation, we perform three multiplications in equations 2 and 4. In equation 5, we must perform $\mathrm{O}(n)$ tries (modular multiplications) to find the correct s_j, by determining the correct error position i. Thus, the complexity to compute s_j is $\mathrm{O}(n)$.

Considering that Bob does not know a priori in which s_j the error occurred, he must try all $|S|$ possible s_j's to derive the correct one. Thus, the total complexity for deriving one s_j is $\mathrm{O}(n\ell)$.

Given ℓ erroneous protocol invocations, so that errors occur in every $s_1, \ldots, s_\ell$, we can derive all secret elements of Alice in the time it takes to perform $\mathrm{O}(n\ell^2)$ modular exponentations.

5 Conclusions

The Bellcore attack against systems implementing the Fiat-Shamir scheme is based on the assumption that the construction of a full rank $\ell \times \ell$ matrix over $\mathbb{Z}_2$ is always possible, where ℓ is the number of Alice's secret elements. The construction of such a full rank matrix is not always possible, leading to alternative system configurations, as the described *Precautious Fiat-Shamir Identification Scheme*, which render the original attack unsuccessful. As we have shown, the original fault model of the Bellcore attack can lead to successful attacks on Precautious Fiat-Shamir, which, theoretically, derive enough information to impersonate Alice. However, these attacks are very demanding in terms of computational power and memory resources, rendering these attacks impractical in resource-limited environments, such as smart-cards. Considering these limitations of the extended attack, we have introduced a novel active attack model, which enables successful attacks in all environments and known Fiat-Shamir system configurations.

References

[1] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The EM Side-Channel(s). In *Cryptographic Hardware and Embedded Systems - CHES 2002, LNCS 2523*, pages 29–45. Springer-Verlag, 2002.

[2] R. Anderson and M. Kuhn. Tamper Resistance – a Cautionary Note. In *Proceedings of the Second USENIX Workshop on Electronic Commerce*, November 1996.

[3] R. Anderson and M. Kuhn. Low Cost Attacks on Tamper Resistance Devices. In *Security Protocol Workshop '97, LNCS 1361*, pages 125–136. Springer-Verlag, 1997.

[4] E.P. Antoniadis, D.N. Serpanos, A. Traganitis, and A.G. Voyiatzis. Software Simulation of Active Attacks on Cryptographic Systems. Technical Report TR-CSD-2001-01, Department of Computer Science, University of Crete, 2001.

[5] Christian Aumüller, Peter Bier, Wieland Fischer, Peter Hofreiter, and Jean-Pierre Seifert. Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures. In *Cryptographic Hardware and Embedded Systems, CHES 2002*, pages 260–275. Springer-Verlag, 2002.

[6] F. Bao, R. Deng, Y. Han, A.D. Narasimhalu, and T. Ngair. Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults. In *Security Protocol Workshop '97, LNCS 1361.* Springer-Verlag, 1997.

[7] E. Biham and A. Shamir. Differential Fault Analysis of Secret Key Cryptosystems. In *Advances in Cryptology-Crypto '97, LNCS 1294*, pages 513–525. Springer-Verlag, 1997.

[8] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In *Advances in Cryptology - EUROCRYPT '97, LNCS 1233*, pages 37–51. Springer-Verlag, 1997.

[9] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of eliminating errors in cryptographic computations. *Journal of Cryptology*, 14(2):101–119, 2001.

[10] J.-F. Dhem, F. Koeune, P.-A. Leroux, Mestré, J.-J. Quisquater, and J.-L. Willems. A Practical Implementation of the Timing Attack. Technical Report CG-1998/1, UCL Crypto Group, DICE, Université Catholique de Louvain, Belgium, 1998.

[11] A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. In *Advances in Cryptology - CRYPTO '86, LNCS 263*, pages 186–194. Springer-Verlag, 1987.

[12] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In *Cryptographic Hardware and Embedded Systems - CHES 2001, LNCS 2162*, pages 251–261. Springer-Verlag, 2001.

[13] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Side Channel Cryptanalysis of Product Ciphers. In *Computer Security - ESORICS 98, LNCS 1485*, pages 97–110. Springer-Verlag, 1998.

[14] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Side channel cryptanalysis of product ciphers. *Journal of Computer Security*, 8(2–3):141–158, 2000.

[15] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems. In *Advances in Cryptology - Crypto '96, LNCS 1109*, pages 104–113. Springer-Verlag, 1996.

[16] P. Kocher, J. Jaffe, and J. Benjamin. Differential Power Analysis. In *Advances in Cryptology - Crypto '99, LNCS 1666*, pages 388–397. Springer-Verlag, 1999.

[17] T.S. Messerges, E.A. Dabbish, and R.H. Sloan. Investigations of Power Analysis Attacks on Smartcards. In *Proceedings of the First USENIX Workshop on Smartcard Technology*, May 1999.

[18] Jean-Jacques Quisquater and David Samyde. ElectroMagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards. In *Smart Card Programming and Security, E-smart 2001, LNCS 2140*, pages 200–210. Springer-Verlag, 2001.

[19] A.G. Voyiatzis and D.N. Serpanos. Active Hardware Attacks and Proactive Countermeasures. In *Proceedings of the 7th IEEE Symposium on Computers and Communications (ISCC'02)*, pages 361–366, July 2002.