Active Hardware Attacks and Proactive Countermeasures*

Artemios G. Voyiatzis and Dimitrios N. Serpanos
Department of Electrical and Computer Engineering
University of Patras
GR-26500 Patras
Greece
{bogart,serpanos}@ee.upatras.gr

Abstract

Active hardware attacks succeed in deriving cryptographic secrets from target devices. They were originally proposed for systems implementing RSA, Fiat-Shamir scheme, and Schnorr's scheme.Common targets for these attacks are systems used for client authentication in order to access services, e.g., pay-per view TV, video distribution and cellular telephony. These client systems hold secrets, typically cryptographic keys, owned by the service provider, and often implement the Fiat-Shamir identification scheme. Given the strength of active attacks and the increasingly wide deployment of client systems, it is desirable to design proactive countermeasures for them.

In this paper we focus on the Fiat-Shamir scheme. We prove that the conventional active attack can be easily avoided through appropriate system and protocol configuration; we denote this configuration as the Precautious Fiat-Shamir Scheme. We argue that proactive countermeasures against active attacks are feasible and lead to systems that are inherently resistant to active attacks by careful protocol design, rather than ad hoc solutions.

1. Introduction

Advances in cryptanalysis have introduced a new class of attacks, designated as *side-channel cryptanalysis* (originally proposed in [11]).These hardware attacks are applied to implementations of cryptographic algorithms, and take advantage of a *side-channel*, which transmits information of the secret components of an algorithm. Hardware attacks are classified as active or passive. Differentiation among them lies in realization of the side-channel. In passive attacks the channel is some measurable implementation parameter, such as power consumption [13] [15], execution delay of a cryptographic algorithm [12] [8] and lately electromagnetic radiation [17] [10] [16]. In active attacks, the channel is fault insertion in data of cryptographic calculations [4] [5] [6] and can be realized, for example, by operation in extreme conditions and gate destruction [1] [2].

The Bellcore attack [6] [7], is an active hardware attack targeting implementations of RSA using Chinese Remainder Theorem or Montgomery arithmetic, Schnorr's scheme and Fiat-Shamir identification scheme. These theoretical attacks have been verified through simulation [3]. Simulation has shown that all theoretical active attacks are complete, with the exclusion of the Fiat-Shamir scheme, where there is indication that, in general, there may be system configurations, where the Bellcore attack is not successful.

In this paper, we introduce the concept of proactive countermeasures for active hardware attacks. Specifically, we demonstrate that a device can implement a cryptographic protocol in a fashion that prevents leakage of secret information, even in the presence of faulty computations. In our work, we focus on the Fiat-Shamir scheme, due to its popularity. We prove that the Bellcore attack is based on an assumption that is not always true: one can always construct a full-rank $\ell \times \ell$ matrix over $\mathbb{Z}_2$. Using this fact, we prove that a careful implementation (or configuration) of the scheme can protect secrets from leaking out of a device.

The paper is organized as follows. Section 2 describes the Fiat-Shamir identification scheme 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, but realistically infeasible in resource-limited environments, such as smart-cards. Finally, we analyze the concept of proactive countermeasures for active hardware attacks, and argue, based on the development of Precautious Fiat-Shamir, that such countermeasures are feasible and lead to systems that

*This work was done with partial support from Telcordia Technologies (formerly Bellcore).

Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02)
1530-1346/02 $17.00 © 2002 IEEE

are inherently resistant to active attacks by careful protocol design, rather than by ad hoc solutions.

2. Background

2.1. Fiat-Shamir Identification Scheme

The Fiat-Shamir identification scheme [9] 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 a n-bit modulus N, where N is the product of two large prime numbers, and a set of invertible elements $s_1, s_2, \ldots, s_\ell \bmod N$. Alice's public key is the set $PK_\ell = \{u_i \mid u_i = s_i^2 \bmod N \text{ and } 1 \leq i \leq \ell\}$. Alice proves her identity to Bob using the following communication protocol:

1. Alice and Bob agree on a security parameter, $t \leq \ell$;
2. Alice picks a random number $r \in \mathbb{Z}_N^*$, calculates $r^2 \bmod N$ and sends the result to Bob;
3. Bob chooses a random subset $S \subseteq \{1, \ldots, t\}$ 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: $y^2 = r^2 \cdot \prod_{i \in S} u_i \bmod N$

The security of the scheme is based on the hypothesis that computation of square roots is a hard problem over $\mathbb{Z}_N$.

2.2. The Bellcore attack on Fiat-Shamir Identification Scheme

The Bellcore attack [6] [7], 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 using Bellcore attack can derive Alice's secret elements, $s_1, \ldots, s_\ell \bmod N$. 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, as we describe briefly below.

It is interesting to note that, in this case, the attacker solves the time isolation problem, which constitutes a significant difficulty in the implementation of active attacks. Specifically, the attacker (Bob) does not need exact synchronization with the device that acts as Alice, because the attacker can delay transmission of the subset S arbitrarily. So, the attacker needs to solve only the space isolation problem, i.e., he needs to locate the correct memory location that stores r, in order to introduce the transient bit flip. For shake of simplicity, we assume in the following that a single bit flip occurs. The Bellcore attack on Fiat-Shamir identification scheme is summarized in the following theorem:

Theorem 1 (Bellcore attack) *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 $\mathrm{O}(n\ell + \ell^2)$ modular multiplications.*

Proof 1 (summarized) *A bit-flip in r at position i,changes its value by $E = \pm 2^i$; the sign denotes 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 $T^2(S) = \prod_{i \in S} u_i$ This step requires $\mathrm{O}(n + \ell)$ modular multiplications, since Bob must try all possible bit error positions, as to detect the position where the bit flip occured. Thus, for ℓ different sets S, $\mathrm{O}(n\ell + \ell^2)$ modular multiplications are required.

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

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

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:

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

The calculation of s_1 requires $\mathrm{O}(\ell)$ modular multiplications, and thus, the calculation of all $s_1, s_2, \ldots, s_\ell$ requires a total $\mathrm{O}(\ell^2)$ modular multiplications. Overall, the entire algorithm requires $\mathrm{O}(n\ell + \ell^2)$ modular multiplications.

3. Defense against Bellcore attack

The original proof of the Bellcore attack [6] 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, we evaluate the 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 $\mathbb{Z}_2$.

3.1. Preliminary results

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 $\mathbb{Z}_2$:

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

In conclusion, the Bellcore attack is effective, under these assumptions since 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 $\{2, \ell\} \not\subseteq G$. 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. So, the Bellcore attack is not effective in this case.

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. First, we prove two propositions.

Proposition 1 *$\forall a, b \in \mathbb{Z}_2^n$, $w(a \oplus b)$ is* **even***, if $w(a), w(b)$ are both even or both odd and* **odd***, otherwise.*

Proof 2 *The sum of two binary vectors a, b is the exclusive-OR (xor) of a, b. So, the Hamming weight of $a \oplus b$ is:*

$$\begin{aligned} w(a \oplus b) &= \sum_{i=1}^{n} \left(a_i b_i^{'} + a_i^{'} b_i\right) = \\ &= \sum_{i=1}^{n} \Big(a_i(1 - b_i) + (1 - a_i) b_i\Big) = \\ &= w(a) + w(b) - 2 \sum_{i=1}^{n} a_i b_i \end{aligned}$$

Since $2 \sum_{i=1}^{n} a_i b_i$ is even, $w(a \oplus b)$ depends only on $w(a)$ and $w(b)$. If they are both even or both odd, then their sum is even and so is $w(a \oplus b)$. If this is not the case, then their sum is odd and so is $w(a \oplus b)$.

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

Proof 3 *The space of $\mathbb{Z}_2^\ell$ is defined as $< \mathbb{Z}_2^\ell, \mathbb{Z}_2, \oplus, \cdot >$, where $\oplus$ denotes the exclusive-OR operation. $V_2(\ell)$ is a subspace, since for each $u, v \in V_2(\ell)$:*

- $(0, \ldots, 0) \in V_2(\ell)$*;*
- $u \oplus v \in V_2(\ell)$*, by proposition 1;*
- $0 \cdot u = (0, \ldots, 0)$ *and* $1 \cdot u = u$ *are in* $V_2(\ell)$*.*

The set of vectors $b_1,\ b_2,\ \ldots,\ b_{\ell-1}$, that is the $\ell-1$ first rows of B_e and B_o, are linearly independent:

$$\begin{aligned}\mathbf{b_1} &= (1,0,0,\ldots,0,1)\\ \mathbf{b_2} &= (0,1,0,\ldots,0,1)\\ \mathbf{b_3} &= (0,0,1,\ldots,0,1)\\ &\vdots\\ \mathbf{b_{\ell-1}} &= (0,0,0,\ldots,1,1)\end{aligned}$$

Considering a vector $\mathbf{a}=(a_1,a_2,\ldots,a_\ell)$ of $V_2(\ell)$, one can express this vector as a linear combination of b_i's:

$$\mathbf{a} = a_1\mathbf{b_1} + a_2\mathbf{b_2} + \ldots + a_{\ell-1}\mathbf{b_{\ell-1}}$$

Although the sum includes only $(\ell-1)$ vectors $\mathbf{b_i}$, $1\le i<\ell$, and the value a_ℓ is not used in the calculation, the sum results in a correct value for a_ℓ:

- *if $a_\ell = 1$ then $w((a_1,a_2,\ldots,a_{\ell-1}))$ is odd. Given that $\mathbf{b_i}(\ell)=1$ for every $\mathbf{b_i}$, $1\le i<\ell$, the sum adds an odd number of 1's in the last (ℓ-th) position. Thus, $a_\ell=1$, as required.*
- *if $a_\ell = 0$, then $w((a_1,a_2,\ldots,a_{\ell-1}))$ is even. Given that $\mathbf{b_i}(\ell)=1$ for every $\mathbf{b_i}$, $1\le i<\ell$, the sum adds an even number of 1's in the last (ℓ-th) position. Thus, $a_\ell=0$, as required.*

Thus, in conclusion, the set $\{\mathbf{b_1},\mathbf{b_2},\ldots,\mathbf{b_{\ell-1}}\}$ contains $\ell-1$ linearly independent vectors, which span $V_2(\ell)$. By definition, these vectors form a basis of the subspace and its dimension is $\ell-1$.

3.2. The "Precautious Fiat-Shamir 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 (Precautious Fiat-Shamir Scheme) *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 $G=\{1,2,\ldots,\ell\}$, then the scheme is the original Fiat-Shamir identification scheme. If $G\subset\{1,2,\ldots,\ell\}$, 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 (Defense against Bellcore attack) *If Alice implements Precautious Fiat-Shamir Identification Scheme, then Bellcore attack is not effective.*

Proof 4 *Bellcore attack is effective when one can construct an $\ell\times\ell$ full rank matrix using 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. Strength of Precautious Fiat-Shamir

4.1. Extension of the Bellcore attack

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 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 an implementation configuration for the Fiat-Shamir scheme,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:

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

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

4.2. Issues in impersonation of smart cards

We consider the case where a smart card acts as Alice in the Precautious Fiat-Shamir Scheme. Assume that Bob has already initiated the extended Bellcore attack successfully. So, Bob is in possesion of pairwise products $s_i s_j$ of Alice's secret keys. Bob's next task is to construct a smart card that can be authenticated as Alice.

One way to achieve this, is to program a new smart card, so that it can produce any possible reply in real time, given the $\ell - 1$ linear independent vectors. An authenticating device can detect such an impersonating smart card by measuring the response time between a challenge and its response (Step 4 of the Fiat-Shamir scheme, as described in Section 2). In impersonating smart cards, this response time is quite long, because there is need for additional operations, specifically modular multiplications. For example, consider the case where $\ell = 9$ and the challenge is $S = \{1, 2, 3, 6, 7, 9\}$. Given the vectors of Proposition 2, an impersonator needs to perform one extra modular multiplication, relatively to a legitimate card's operations. As modular multiplication is quite time-consuming in a smart card, especially when not equipped with a cryptographic coprocessor, such long time delays can be a serious indication of a malicious card's presence.

Alternatively, Bob can precompute all possible responses and load them to the smart card. This is equivalent to producing all vectors of $V_2(\ell)$, given the $\ell - 1$ linear independent vectors of Proposition 2. Given that ℓ is usually small, one can argue that it is feasible to compute them, although the size of $V_2(\ell)$ is exponential to ℓ. However, smart cards have limited memory resources, and thus, it is not feasible to store all these responses with the appropriate choice of ℓ (in conventional smart cards, Bob would fail for $\ell \geq 5$).

In conclusion, the fact that Bob cannot possess each secret key of Alice, $s_1, s_2, \ldots, s_\ell$, but possesses pairwise key products, places sigificant obstacles for a realistic impersonation in smart card environments. For successful attacks, it is clearly desirable that the attacker obtains every s_i.

5. Proactive Countermeasures

In Section 4, we showed that the Fiat-Shamir Identification Scheme can defend against known active attacks, if properly implemented. In this section, we consider the problem of developing countermeasures for active attacks.

Up to date, there is no published practical implementation of active attacks for any algorithm or protocol. However, this should not discourage the development of appropriate countermeasures, because there are claims that the pay-TV hacking community has been using such techniques for some time [1] [2].

A common approach to defeat active attacks is double computation, i.e. devices compute twice and compare all encrypted information before they transmit it. In resource-limited environments, such as smart card systems, this is not efficient, because it doubles the protocol execution time. Furthermore, in multi-round authentication schemes, double computation is not feasible, because the device uses random number(s) in computations and thus, there can be no comparison between results, even in correct computations [6].

Other approaches include result verification, protection of memory with parity bits and blinding or random padding [4]. Result verification is not always feasible and depends on the size of the keys and the nature of the underlying mathematical problem [4] [14]. Protecting memory with parity bits defeated differential fault analysis [5], but resulted in a more efficient and realistic attack [2]. Among these approaches, the only successful and practical ones are blinding and random padding, as demonstrated for RSA systems [4]. Importantly, these methods belong to the category of *proactive countermeasures*.

Considering the effectiveness of Precautious Fiat-Shamir and the success of other proactive countermeasures (blinding and random padding), it becomes clear that cryptosystems can be designed with embedded proactive countermeasures. Proactive countermeasures are any technique incorporated to a cryptosystem that proactively protects secret key leakage, in case of side-channel attacks. However, there are two significant requirements for the implementation of such countermeasures: *(i)* they must not introduce performance penalty (as double computations do), and *(ii)* they must not degrade the security level of the cryptosystem (as parity bits did in the case of differential fault analysis).

6. Conclusions-Future work

The Bellcore attack against systems implementing the Fiat-Shamir identification 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. We have proven formally that, the construction of such a full rank matrix is not always possible. We have introduced the *Precautious Fiat-Shamir Identification Scheme*, a modification of the original scheme, which renders the attack unsuccessful. Considering the properties of Precautious Fiat-Shamir and the effectiveness of alternative proactive countermeasures, we argue that proactive coun-

termeasures against active hardware attacks are feasible and lead to systems that are inherently resistant to active attacks by careful protocol design, rather than ad hoc solutions.

References

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

[2] 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.

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

[4] F. Bao, R. Deng, Y. Han, A. 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.

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

[6] D. Boneh, R. DeMillo, and R. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In *EUROCRYPT '97, LNCS 1233*, pages 37–51. Springer-Verlag, 1997.

[7] D. Boneh, R. DeMillo, and R. Lipton. On the importance of eliminating errors in cryptographic computations. *Journal of Cryptology*, 14(2):101–119, 2001.

[8] 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.

[9] U. Feige, A. Fiat, and A. Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94, 1988.

[10] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic Analysis: Concrete Results. In *CHES 2001, LNCS 2162*, pages 251–261. Springer-Verlag, 2001.

[11] J. Kelsey, B. Schneier, D. Wagner, and C. Hall. Side Channel Cryptanalysis of Product Ciphers. In *ESORICS 98, LNCS 1485*, pages 97–110. Springer-Verlag, 1998.

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

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

[14] A. Lenstra. Memo on RSA Signature Generation in the Presense of Faults. Manuscript available from author, arjen.lenstra@citicorp.com.

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

[16] J.-J. Quisquater and D. Samyde. ElectroMagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards. In *E-smart 2001, LNCS 2140*, pages 200–210. Springer-Verlag, 2001.

[17] J. R. Rao and P. Rohatgi. EMpowering Side-Channel Attacks. Cryptology ePrint Archive, Report 2001/037, 2001. `http://eprint.iacr.org/`.