An On-chip Security Monitoring Solution For System Clock For Low Cost Devices

Frank Vater
Innovations for High
Performance Microelectronics
Im Technologiepark 25
15236 Frankfurt (Oder),
Germany
vater@ihp-microelectronics.com

Steffen Peter
Innovations for High
Performance Microelectronics
Im Technologiepark 25
15236 Frankfurt (Oder),
Germany
peter@ihp-microelectronics.com

Peter Langendörfer
Innovations for High
Performance Microelectronics
Im Technologiepark 25
15236 Frankfurt (Oder),
Germany
langend@ihp-microelectronics.com

ABSTRACT

In this paper we present a new approach for a clock watchdog. This is an essential component to prevent secret key extraction from security hardware by side channel attacks based on clock manipulation. Our proposed circuit detects both too fast and too slow clock speeds and is implemented using only standard digital elements. We also introduce a post-fabrication configuration mechanism by using additional fusebits. In a 0.25μm technology the circuit has an area less than $12{,}500\mu m^2$ and consumes 2 mA, so that an application in very constrained devices, such as wireless sensor nodes, is feasible.

1. INTRODUCTION

In recent years wireless sensor networks (WSN) have gained a lot of attention especially for supporting environmental monitoring and military applications. We envision that WSN will play an important role in the area of homeland security. Here they will be used to secure sensitive infrastructures such as supply network systems and large industrial plants. On one hand, the sensor nodes need to be very cost efficient due to the large area that need to be covered. On the other hand, the WSN needs to provide a high level of security and dependability to fulfill their task reliably.

In order to design the correct level of security into a system, the presumed attacker needs to be profiled. In the area of homeland security we assume that potential attackers are professionals. This means the attackers are willing to take a risk, are familiar with applied cryptographic mean, and have considerable financial resources. Given this attacker model, sensor nodes need to be highly tamper resistant. Full tamper resistant devices are very expensive which contradicts the low cost approach of sensor nodes.

In this paper we introduce an innovative approach to strengthen sensor nodes equipped with crypto hardware against side channel attacks. The solution discussed in this paper focuses on monitoring the clock frequency. By this means, attacks based on power analysis as well as attacks that exploit glitches can be prevented. Our watch dog can be realized in pure CMOS technology. Resulting in a number of important benefits.

First, the design process itself is simplified in comparison to other approaches using analog technology to monitor the clock frequency. Second, production cost is kept low, and third our solution can be directly integrated into any crypto hardware.

2. BACKGROUND

At this time, low cost cryptographic cores already offer strong encryption, but they are only weakly protected against side channel attacks. Such attacks can be used to extract secret information [5] from the system. In particular, the internal private key is in the focus of an attacker. In the area of WSN a physical attack is simple to perform since the attacker can walk by and grab some nodes. The “best” case for the attacker is if the key is hardwired, that is the key will never change in the lifetime of the sensor node. This provides the attacker with sufficient time to retrieve the sensitive data and to misuse it. An easy way to get key information is to use a side channel attack, whereby e.g. the key can be extracted by observing the power consumption.

To prevent side channel attacks, tamper proof hardware has been proposed in [6]. The PCI-Card is resistant against clock signal manipulation, temperature and voltage fluctuations, and device opening. However this approach is very expensive, large, and requires a lot of energy and additional backup batteries. Our goal is to develop components which have a similar functionality against side channel attacks but which are much cheaper than current solutions. In this paper we discuss a solution for one of these problems.

Basically, two different manipulations of the clock are conceivable: slowing down or acceleration. The first approach particularly supports side channel attacks. In [7] a side channel attack is described which was significantly more successful at reduced clock frequencies. To increase the observ-

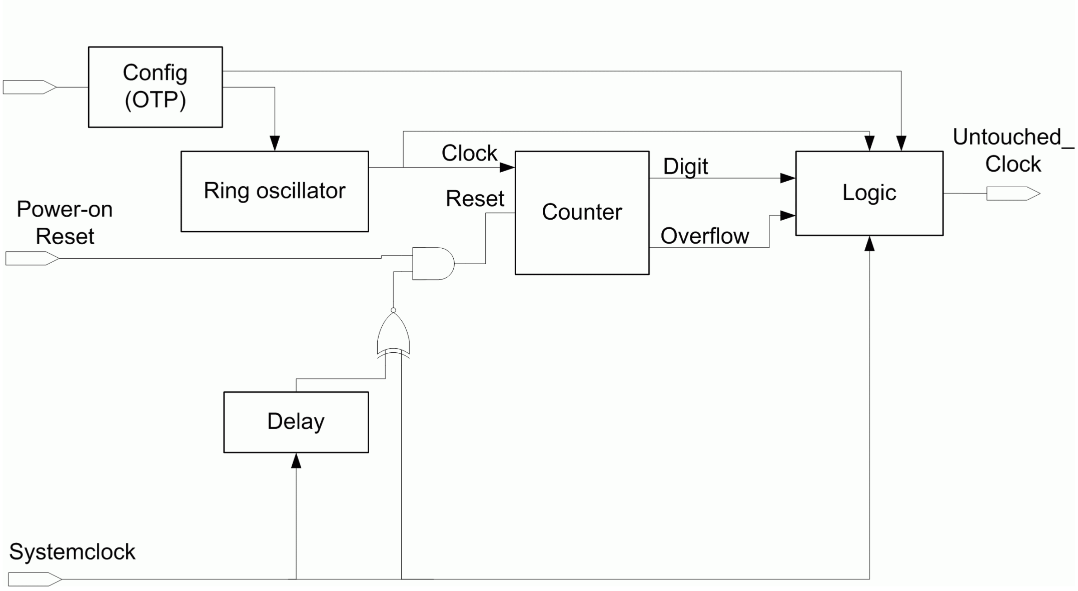

Figure 1: Structure of the clock watchdog

ability in an attack, the clock signal is reduced, so that the power consumption in every clock cycle is clearly separated from that in the preceding clock cycle. The on-chip power rings function as very small capacitors which blur the current and power consumption, so that at high frequencies it is much harder, if not impossible, to extract any information from the observed side channels. This is why reducing the clock frequency is required for many side channel attacks.

The second group of attacks uses a high clock frequency which is out of range or glitches on the clock signal. In [4] the authors described this kind of attack, called "fault injection". ASIC's state should become undefined, which allows to get key details [3]. A glitch attack is straightforward and one of the most practical threats [2]. To prevent such attacks, typically a Phase Looked Loop (PLL) is used as internal clock reference. A PLL can be used to detect missing or extra pulses or a too fast or too slow clock as described in [6]. In [8] a clock watchdog was introduced. It was also realized in pure CMOS technology, but was not able to reliably detect increased clock frequencies. So, attacks based on glitches could still be executed. The design we propose in this paper not only remedies this problem but can also be tuned after fabrication.

3. CLOCK WATCHDOG

The clock watchdog circuit introduced in this section pursues a straightforward idea: The clock watchdog interacts as a stopwatch for each half cycle of the system clock. For that purpose we have a small, fast oscillator that continuously increases a counter. If the system clock edge comes too early, i.e. before the counter reached its lower threshold, an error signal will be generated. The same happens if the upper threshold of the counter is reached before the next edge of the system clock has arrived. In some parts (ring oscillator and counter) the system is similar to a digital PLL.

3.1 Design

Fig. 1 shows the block diagram of the clock watchdog. In view of the basic idea it obviously needs a ring oscillator, a counter, and a comparison logic unit. Additionally we need a delay element for the reset impulse of the counter register. The configuration register, made of fuse bits, allows a post-fabrication adjustment of the circuit.

As additional component in an ASIC, the clock watchdog requires the following inputs: system clock and system reset. Furthermore a memory like interface enables the access to the fuse bit register for adjusting the circuit (configuration space). There is only one output, an indicator signal which will set to "1" if the system clock was modified. In such a situation the connected main circuit (e.g. a cryptographic unit) should stop computation, prevent any register and memory writing operation or even delete the stored keys.

3.2 Oscillator

As mentioned earlier, we need an internal reference clock based on an oscillator. Since it is our goal to have a technology-independent low cost circuit, we focused our research on ring oscillators based on inverter chains. However such straightforward ring oscillators may cause serious problems when it comes to physical fabrication of the circuit.

To get a feeling for the variation in the frequency we measured a number of fabricated ring oscillators in the applied 0.25 μm technology. Figure 2 shows measurement results. Due to variations in production process, the frequency of the ring oscillator differs ±10% around 87.4MHz. To increase the maximum yield the oscillator was extended with a configuration unit.

Figure 3 shows a standard ring oscillator (bases on inverters) plus additionally a buffer line, a multiplexer, and a fuse bit to allow for variation in the frequency. After fabrication, the circuit is set to the slowest supported oscillator frequency,

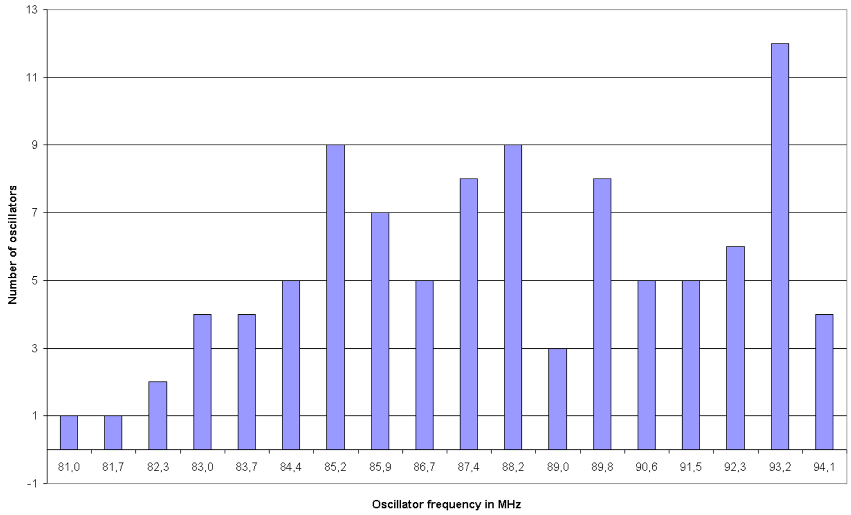

Figure 2: Measured variation in frequency of fabricated ring oscillators

i.e. all additional elements are active. The fusebit output is ’1’. We use this output as input for the select signal of a multiplexer that controls the path length. In the default case (select=’1’) the input S_1 is selected, which means that the long path is chosen. By blowing the fuse bit, the multiplexer increase the frequency because the shorter timing path (input S_2) is selected.

The fusebits are set irreversibly, so that resetting to ’1’ is impossible. This configuration system does not require any other security mechanism. Indeed, unauthorized disabling of fuse bits can increase the clock frequency. However, by careful design of the maximum settable frequency (all fuse bits blown), the ASIC can still work properly and at least will not allow a successful clock glitch attack. Usually the goal of an attacker would be to either reduce the speed of the ring oscillator or to increase the frequency significantly - both cases are not jeopardized by the additional configuration functions.

Figure 3 shows an exemplary simplified configuration unit. The depicted two configuration elements allow three different frequencies. After fabrication the elements that for the addition of 1ns and 2ns are enabled in the loop so that the extra delay is about 3ns. A calibration step measures the current frequency and, if necessary one or two fuse bits can be disabled in order to decrease the delay thus reaching the requested frequency. In practice the configuration unit will have several elements with different timing.

3.3 Counter

The counter is increased every clock cycle of the internal ring oscillator. It consists of an adder, a sum register (n bit width) and a 1-bit-register, indicating whether the sum register has an overflow.

The most interesting element of the counter unit is the logic required for resetting the counter on every edge of the system clock. A delay element (also based on inverters) and a few logic elements are used to generate a reset impulse for the counter registers. The delay time is the minimum specified time for a reset of the used flip-flops. This value can be found in digital library description of the relevant technology.

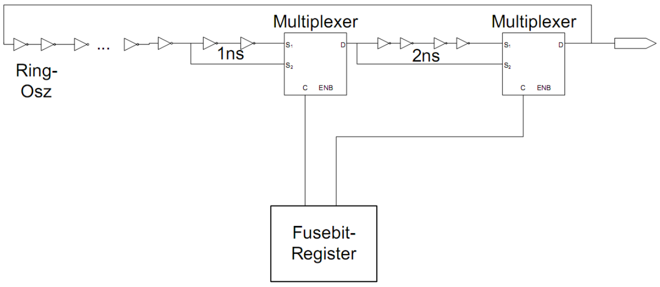

Figure 3: Ring oscillator with 2-step calibration unit. Each calibration unit consists of an additional buffer line, a multiplexer and one time programmable register for selecting the multiplexer input

The input for the delay element is provided by the system clock signal. The output will be combined (XNOR) with system clock so that a reset impulse is generated at both the rising and the falling system clock. For the applied 0.25 μm technology, a time of 0.13 ns is specified.

After reset, the counter register will be incremented with every rising edge of the internal oscillator clock until the next edge on the system clock resets the counter again.

3.4 Comparison Logic

The comparison logic unit observes the counter and the system clock signal. The output of the logic unit is a signal which indicates whether or not the system clock was manipulated. The unit comprises two smaller units. One propagates the overflow signal of the counter, and the second compares the counter register value.

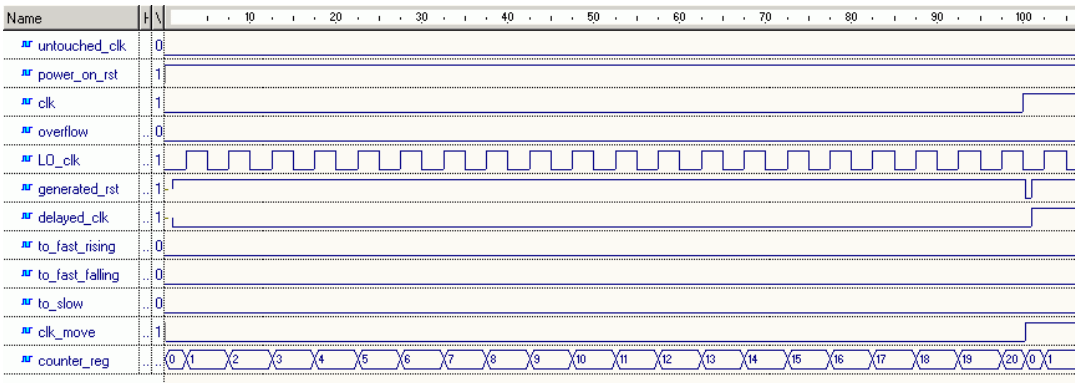

Figure 4: Simulation of clock watchdog for a allowed frequency. The signal "untouched_clk" is low.

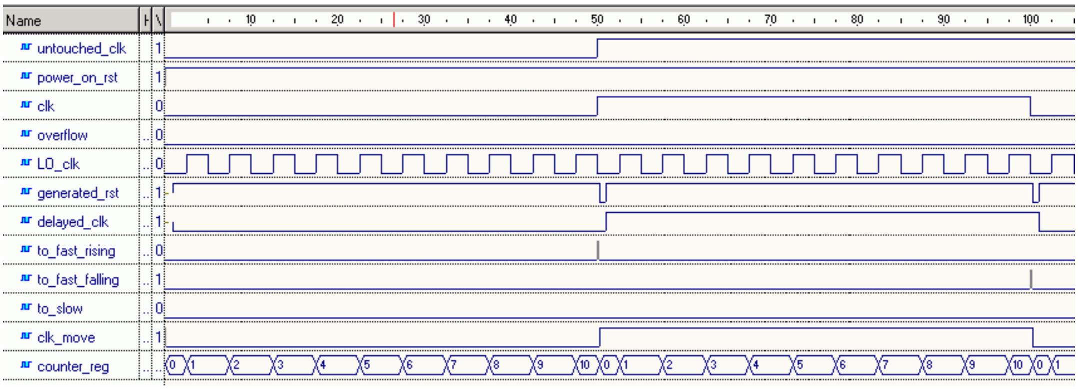

Figure 5: Simulation of the clock watchdog for a too high frequency. At the rising edge of the system clock the signal "untouched_clk" goes on high.

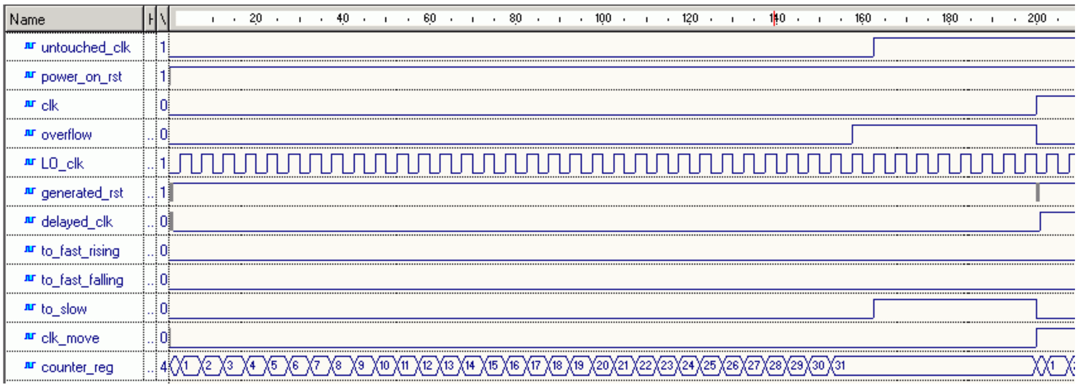

Figure 6: Simulation of the clock watchdog for a too slow frequency. At the rising edge of the internal clock and the register "overflow"=1 the signal "untouched_clk" goes high.

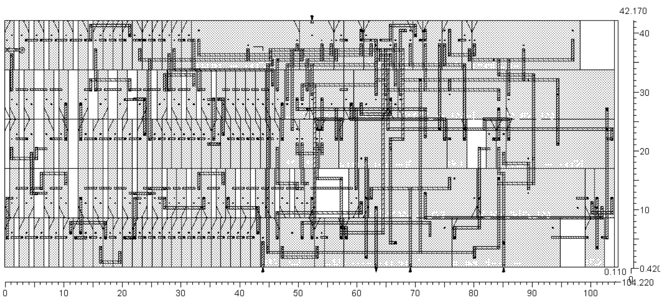

Figure 7: Prototyping layout of clock watchdog. On the left side the oscillator is placed, on the right side logic and registers

The first component is responsible for recognizing a slowed clock. At each rising edge of the internal oscillator clock the overflow register of the counter will be checked. If the overflow register is set, it indicates that the system clock is overdue. This is a clear signal for a manipulated clock. In case clock that is too slow, it is important that the circuit generates an alert immediately after an overdue clock has been detected. An attacker should not even get the chance to exploit the result of a single stopped clock cycle. It has been shown [7] that already half a clock period which is longer than necessary improves the results of a side channel attack significantly.

The second component compares the value of the counter register at each edge (rising and falling) of the system clock. The value must be in a pre-defined range. The pre-defined value has a minimum and a maximum (also called "operation window"). Due to fabrication variations and run-time effects such as temperature and voltage sensitivity, applying only one value would not reasonably work in practice.

As an example we consider that valid counter register values are in the range from 16 to 32. The internal oscillator frequency is 200 MHz and the expected system clock frequency is 4.5 MHz. At 4.5 MHz system clock the period time is 220 ns and consequently a half period has a length of 110ns. Due to the fact that the internal oscillator runs at 200 MHz, the counter reaches the value "22" for a perfect un-manipulated clock. In the operation window 16 to 32, we allow frequencies from 3.1 to 6.3 MHz. If at the next clock event the counter register contains a value smaller than 16 it indicates that the system clock is too fast. Immediately after recognizing a too fast clock, the clock watchdog sets the alert signal. A too slow clock will be recognized in the moment that the counter overflow bit is set. In contrast to the configuration register, in the oscillator the counter thresholds cannot be set after fabrication. The configuration in the oscillator can be considered as a calibration unit, while the counter threshold is an additional element to cover runtime fluctuations.

3.5 Simulation

We initially implemented the concept in VHDL and verified the idea in various simulations: first behavioral simulation, than post-synthesis simulation and finally simulation after layout. The final simulation includes gates and wires, resistance and capacitances so that all delays are considered. Therefor we applied the following tools: Cadence SimVision, Synopsys DesignVison, Cadence Encounter and Synopsys PrimePower.

In the following, we describe a simulated design with an allowed period range from 160ns to 320ns. Figure 4 shows a simulation for a non-tampered clock for a half clock period. The power-on reset sets the system into the initial state. Then the internal oscillator clock starts incrementing the counter register. At the time of a rising edge of the system clock, the counter value is "20". This is in the specified range from 16 to 31. The signal "generated_rst" set the counter register to zero and the clock watchdog starts again for the high level of the system clock.

An example where the system clock has been reduced (clock too slow) is shown in Fig. 6. The counter reaches its maximum value of "31" before the system clock triggers again. Consequently the overflow register is set to "1" and via the signal "to_slow" the output signal "untouched_clk" is set to "1". One can clearly see that the clock watchdog could successfully detect the tampered clock. Considered that the ASIC stops the computation and register write operations the attacker will not gain any advantage from manipulation of the clock.

Figure 5 shows an example where the system clock speed was significantly increased. It can be seen that the counter does not reach the necessary value of "16" at the rising edge of the system clock. The comparison logic detects the tampered clock and immediately sets the signal "untouched_clk" which eventually effects the computation on the ASIC. If in such a case the register write operations is disabled and the computation unit stops processing, it is unlikely that an attacker can extract valuable information.

3.6 Discussion of the Implementation

We implemented and simulated the design for a 0.25μm CMOS digital library. Fig. 7 shows the automatically generated layout. The density has the value of 85%. For an optimized, small layout the design should be placed by hand. In this case a density of almost 100% is possible, since the design is not very complex, manual placement is feasible. We are planning an integration of the clock watchdog in one of our next cryptographic ASICs.

In our design the oscillator is the largest component of the system. It requires an area of $10,000\ \mu\mathrm{m}^2$ and a current of 2 mA for a 200 MHz system. The remaining components (logic, register) require $2,500\mu\mathrm{m}^2$ with a power consumption of 280 μţW.

An external quartz oscillator typically requires about 28mA, which is fourteen times more than the integrated clock watchdog. Furthermore an external component would also significantly increase the costs per chip and is usually not as secure as an internal solution. A low power quartz oscillator costs $\approx$ 3 Euro in high quantities [1]. The internal clock watchdog costs a fraction of a cent, which is roughly 1000 times cheaper than the external solution.

Beside the size and energy consumption the advantage of this clock watchdog is that it can recognize a manipulated clock signal immediately. Already a single too slow or too fast half clock period results in an alert. A glitch on the system clock is detectable, if it is longer than the delay of the reset in the counter unit. In our example this propagation delay is 0.13ns.

Beside the detection of accelerated clock manipulations the major improvement of the proposed circuit, compared to [8], is its configurability. However, due to this extension more than simple digital library elements are required a fusebit element has to be integrated.

The digital design is quite straightforward. Typically a ring oscillator is designed, fabricated and tested during the evaluation of a new digital library to get performance data. Finally, the internal oscillator with a high frequency (typ. 10x faster than the observing frequency) will be extended with multiplexers and fuse bits for the calibration.

Currently, a power saving mode (reduction of the clock frequency in idle mode) is not yet supported. But it is conceivable to solve this problem by integrating a second clock watchdog for a lower frequency or by adding a second counter and comparing unit.

A further advantage of our design is the valid counter window, which helps to avoid a false alarm caused by voltage or temperature fluctuations. It would be a further improvement of the circuit if the window could be configured after fabrication.

In any case, a clock watchdog alone is not sufficient to consider a circuit as resistant against side channel attacks. Additional mechanisms and algorithms have to be developed and implemented to secure the designs. In the low cost sector of very constrained devices, this is a challenging task. It is our goal to implement a set of security mechanisms that need less than 20% additional area of the protected cryptographic core.

4. CONCLUSIONS

In this paper we have discussed a new approach to monitor the clock frequency of a sensor node equipped with specialized crypto-hardware. It reliably detects reduced clock frequencies, which could otherwise be used in differential power analysis attacks. Our proposed design also detects increased clock frequencies which help in attacks which exploit glitches. The solution is also extremely small, i.e. it needs only $12,500\ \mu\text{m}^2$.

A major benefit of our solution compared to traditional ones is that it can be realized using a standard CMOS technology. This reduces cost during the design process, since digital designers can handle the issue, and during fabrication, since just one process needs to be used. The second benefit is that it can be manufactured together with the crypto-hardware on a single chip. This prevents attackers from manipulating the connection between the clock watchdog and the crypto-hardware.

As a final point, our solution allows to fine tune the supervised clock frequencies after fabrication of the clock watchdog. Making it so that deviations due to the manufacturing process can be remedied, thereby helping to improve the go-reliability of our clock watch dog and to increase the yield.

5. REFERENCES

[1] http://www.farnell.com/datasheets/90978.pdf.

[2] H. Bar-El. Known attacks against smartcards. 2003. White paper available at: ”www.hbarel.com”.

[3] C. H. Kim and J.-J. Quisquater. Fault attacks for CRT based RSA: new attacks, new results, and new countermeasures. In *Workshop in Information Security Theory and Practices: Smart cards, Mobile and Ubiquitous computing systems - WISTP 2007*, pages 215–228. Springer-Verlag, 2007.

[4] O. Kömmerling and M. G. Kuhn. Design principles for tamper-resistant smartcard processors. In *Proceedings of the USENIX Workshop on Smartcard Technology, Chicago, 10–11 May, 1999.*, pages 9–20, 1999.

[5] S. Mangard, M. Aigner, and S. Dominikus. A highly regular and scalable aes hardware architecture. *IEEE Trans. Comput.*, 52(4):483–491, 2003.

[6] S. Smith and S. Weingart. Building a high-performance, programmable secure coprocessor. *IBM Research Report*, February 1998.

[7] F. Vater. Entwicklung von Designkonzepten zur Verbesserung der Seitenattacken-Resistenz von Krypto-Beschleunigern. Master's thesis, BTU Cottbus, Germany, April 2007.

[8] F. Vater, S. Peter, and P. Langendörfer. Combinatorial logic circuitry as means to protect low cost devices against side channel attacks. In D. Sauveron, C. Markantonakis, A. Bilas, and J.-J. Quisquater, editors, *WISTP*, volume 4462 of *Lecture Notes in Computer Science*, pages 244–253. Springer, 2007.