

Design Methodologies for Energy-Efficient Secure Cryptography Coprocessors

SNF Project Proposal – Part 2: Scientific Information

1 Summary

In the last few years several new forms of attacks to cryptographic algorithms have been developed, such as timing analysis and power analysis attacks. They exploit weaknesses of the hardware platform where the algorithm is implemented. The importance of the threat is proportional to the proliferation of security-sensitive devices: these include Smart Cards, nowadays in widespread use in Europe, and a great number of novel embedded devices, often portable and battery-operated.

Several solutions have been proposed and implemented against such attacks. Some are based on mathematical properties of specific cryptographic algorithms. Others rely on specific ways of writing the algorithm in software. Stronger techniques rely on special hardware implementation techniques. Yet, several problems remain: Firstly, none of the techniques is sufficiently robust in itself, and most of them need to be implemented at once, often with a significant impact on performance and, due to the higher number of instructions to execute, energy consumption. Secondly, most or all of the hardware implementation techniques proposed increase the power consumption per instruction of the devices, hence further worsening the energy situation. Unfortunately, both performance and energy are at a premium in most modern embedded systems and new solutions are needed.

No comprehensive comparison of the robustness and cost of the techniques to counter timing and power analysis attacks has been attempted (especially of different hardware implementation methodologies). Only recently researchers have introduced metrics of robustness for existing programmable devices. As a first step in the proposed project, we wish to explore more precisely the issue of security metrics. On one side, we wish to contrast quantitatively various implementation techniques. On the other, we need to study the possibility of carrying robustness information (intrinsically available at the lowest circuit level) toward higher levels of abstraction (gate level, architectural level, and even possibly software level). Although the problem appears difficult, we need to tackle it and obtain a priori metrics at least sufficient to guide us in subsequent phases.

Once the advantages and limitations of various hardware security countermeasures will be well quantified, our planned next step consists in elaborating novel techniques that combine the best robustness features and that are easily amenable to design automation. We will also explore new solutions, for instance exploiting some unorthodox techniques of logic synthesis. Again we will compare the different possibilities and concentrate on one or two options.

We will put in practice these options to conceive flexible tightly-coupled coprocessors for cryptographic applications, possibly based on a reconfigurable datapath. The advantages of the coprocessors will come on three fronts: (1) If the chosen design option will be one for which design automation is difficult, the coprocessor will be a way to limit the application of the unorthodox design option to a minimal part of the whole device requiring the secure implementation technique. (2) Similarly, if the chosen design option is intrinsically less energy efficient than typical hardware, the energy inefficiency will be limited to a minimum. (3) The coprocessor will improve significantly performance and, possibly, will bring a tangible energy-efficiency advantage to offset the additional cost of the secure implementation. We will pursue, as much as possible, general design methodologies and automatic design techniques rather than ad-hoc solutions.

We plan to demonstrate our results with the VLSI design of significant sections of a coprocessor in a typical embedded computing subsystem.

2 Research Plan

The increasing ubiquity of information technologies in all aspects of human life makes security issues one of the most critical aspects of system design: far from being a problem confined to a few specialists whose systems are exposed to potential threats, security now is of interest almost to everybody and it affects not only computer systems proper but the increasingly-wide spectrum of embedded systems. The use of (often mobile) devices adopted for critical functions such as banking, health care, and in general public administration services raises the criminal interest to access users' data. On the other hand, the proliferation of wireless technologies (not only portable phones but also *Personal Digital Assistants (PDAs)*, laptops, and novel personal devices) makes the privacy of the users and of their data more difficult to defend and opens systems to a larger spectrum of possible attacks. The emergence of solutions, such as ad-hoc networks—where all nodes need to participate as intermediaries to convey data, and private messages may be relayed by personal devices belonging to other users—adds to the already complex problem of security.

The increasing interest in breaking the security features of common devices has led to the development of a number of new types of attacks. Significant examples of advanced techniques are based on timing analysis, power analysis, eddy current measurements, or fault injection [Anderson01]. Countermeasures to power-based attacks are particularly challenging when mobile systems are considered: most solutions presented up to now for Systems-on-Chip (SoC) and Smart Cards [MooreApr02] actually lead to increased power consumption during all steps of the execution to achieve a smoother power consumption trace. This is obviously unacceptable in the case of mobile systems, where battery life is a basic design constraint, or in those cases where energy is obtained only from the environment and is therefore severely limited—e.g., in the case of contactless Smart Cards. Thus, it becomes mandatory to explore approaches that *satisfy both requirements of robustness toward power-analysis attacks and of low energy consumption*. More generally, the potential fragility of each countermeasure taken by itself and the rapid evolution in cryptographic algorithms suggest the need for *stronger design methodologies for robust cryptographic implementations at many levels (circuit level, software level, etc.)*.

We organise this document as follows: Firstly, in Section 2.1 we begin by introducing the main problem which drives the whole project, namely the possibility of attacks based on *Timing and Power Analyses (TA and PA)*, both in *Simple* and *Differential* form. In particular, we concentrate on the arguably strongest attack, *Differential Power Analysis (DPA)*. In Section 2.2, we state the goals that we believe are important when addressing solutions to TA and PA attacks. Section 2.3 is devoted to the state of the art; we discuss there several pieces of work, which either are immediately related to the achievement of robust implementation of cryptographic algorithms or, in our view, could be useful to improve current solutions to the problem. Section 2.4 discusses previous work of the applicants, especially where relevant to the present project. Sections 2.5 and 2.6 describe more in detail the project the steps we plan for our investigations, and establish a rough timeline for the project. Section 2.7 briefly addresses the significance of the project and summarises the scientific questions we wish to answer in the project.

2.1 The Problem: Timing and Power Analysis Attacks

There are many non-invasive attacks that pose a significant threat to cryptographic hardware, especially to Smart Cards. The most dangerous are the following:

- 1) *Timing Analysis (TA)* attacks, where information is leaked through the data-dependent execution duration of some operations (e.g., early completion in shift-and-add multipliers).
- 2) *Simple Power Analysis (SPA)* attacks, where information is leaked through the data-dependent power consumption of some operations in a single execution trace.

- 3) *Differential Power Analysis* (DPA) attacks, where information is leaked through correlation of several power-consumption traces—thus extracting minimal and critical data dependent information from them.
- 4) *Electromagnetic Analysis* (EMA) attacks, consisting of looking at the electromagnetic waves emitted by the active circuit. The EM signals collected can be used in a way very similar to a DPA attack. The main difference is that only small parts of the chip can be observed.
- 5) *Fault Injection*, for which, for instance, glitches on the master clock or on the power supply are injected to obtain a faulty behaviour of the circuit that could unveil secret information.
- 6) *Optical probing*, in which lasers are used to generate additional carriers and therefore a photocurrent that could switch some transistors to obtain a specific faulty behaviour of the chip that could unveil secret information.

In this project, only the first four methods will be considered, as they are the most dangerous. Timing attacks have to be considered simultaneously with DPA attacks, in order to avoid to have a better DPA-resistant circuit that is more sensitive to TA attacks. EMA attacks are similar to DPA attacks, as only the way to collect the waveforms is different. DPA was demonstrated in 1999 [KocherAug99]. It has been shown that it is possible to examine the power consumed by the circuit when processing data or executing instructions. For instance, by analysing the variation in power consumption and choosing the plain text to be processed, an attacker can discover the secret key hidden in the circuit. The attacker can analyse a single power trace (SPA) or can perform a statistical analysis of many collected power traces (DPA). In one of the most threatening scenarios, the attacker can statistically correlate the various traces to guess with a limited number of trials the secret key; for this, he or she needs only to know the algorithm being used and must be able to compare directly the power-consumption traces (i.e., align their starting point)—no knowledge or hypothesis on the algorithm implementation is needed. Several other variations to DPA attacks are possible.

2.2 Project Goals

Our final goal is to *enable the efficient design* of security-specific systems characterized by *robustness with respect to TA and PA attacks* as well as by *low-energy consumption*.

We aim at achieving not an individual circuit or system, but rather an *approach*, as far as possible platform- and technology-independent (although, obviously, specific platforms and technologies will be used to validate the concepts developed during the proposed research). In particular, this means exploring alternative solutions for the security-oriented subsystems, that may be fully based on specific hardware design techniques or involve dedicated hardware units together with software techniques exploiting them in a particular way. Ultimately, we plan to develop a *set of methodologies* aiming at the stated final goal. Our main goal requires research in three different areas: (1) Identification of metrics of robustness, (2) circuit design methodologies, and (3) coprocessor design methodologies.

2.2.1 Identification of Robustness Metrics

Today, robustness of cryptographic solutions is evaluated only in an “experimental” way—somehow “a posteriori”, considering mainly the computational complexity of the algorithm and the resulting timing and power trace. To evaluate design methodologies and alternative implementations, it is mandatory to develop metrics capable of providing the information on the TA- and PA-robustness at acceptable costs (in terms of processing complexity and time). Empirical metrics for security have been recently demonstrated and used to drive manual optimisations on standard off-the-shelf hardware [GebotysOct02] but we are aware of no attempts to develop analogous hardware design metrics. For instance, Spice-level simulations would provide fine-grained data but require very high processing times and could be performed only in the final stages of the design process; on the other hand, present gate-level or RT-level tools may be too coarse-grained or lack the type of detail required for the present purpose. A first part of the project will therefore concentrate on identification and validation of suitable models and metrics and consequent extension of existing CAD tools. It

should be noticed that achieving a general, abstract approach to a-priori robustness evaluation is obviously a problem of the greatest relevance but also of extreme complexity — the general problem is simply too ambitious to fit the present project, and we will restrict our activity to robustness metrics *pertaining to the specific aspects of PA and TA*.

2.2.2 Circuit Design Methodologies

There are already several approaches to design systems resistant to TA and PA attacks. A way to turn such approaches into design methodologies, rather than ad-hoc solutions, is to apply the above metrics to study systematically existing approaches. On one side, this should lead to the identification of fundamental design rules to achieve resistance and which can serve as the basis for design methodologies. On the other side, this can help envision novel solutions for the various sections of security-specific circuits.

For instance, TA and PA attacks are based on the fact that executed operations or instructions present execution times and power consumptions that are data-dependent. A very general goal is to find circuit implementations that minimize this effect; some circuit techniques, such a dual-rail approach (see Section 2.1.3.a), are known to display a moderate data-dependency in power consumption. Yet, practically all techniques to “flatten” the power-consumption profile invest “spurious” energy to hide the secrets and hence are not acceptable for most mobile systems. A specific goal is therefore to isolate critical operations and apply hierarchically different methodologies to different parts of the secure system and at different levels of abstraction. The challenge is to decide how much energy to spend for robustness and at which level of abstraction.

The classic design goal against TA and PA attacks consists in achieving the same power consumption and the same execution time for operations or instructions whatever the operands used during a particular execution. However, one could also look to the possibility of having variable execution time and power consumption but not in a data-dependent manner. If a given instruction with the same operands has some random data-independent variability, an attacker cannot find the processed data by looking at timing and/or power traces and, very importantly for differential attacks, won't be able to correlate multiple traces. Although it has been shown that simple applications of this technique are relatively easy to break [ClavierAug00], a comprehensive exploitation of its potentials at digital-design level has not been shown yet and we plan to explore this direction. An interesting approach could consist in considering the particular characteristics of the *operations* involved in cryptographic algorithms (in particular, of the specific arithmetic there adopted) and check whether power smoothing can be derived from such intrinsic factors.

An important consideration in circuit design is the availability or development of automated design tools; since our project focuses on methodologies rather than on individual solutions, we will carefully look into techniques that can exploit standard digital design flows and/or relying on robustness-oriented libraries—consisting of components of varying complexity and at different abstraction levels.

2.2.3 Secure Coprocessors

The complete design of cryptographic systems (e.g., a Smart Card) using secure hardware techniques is of course possible (and is in fact an accepted and implemented option in particular cases). An alternative option consists in the adoption of application-specific coprocessors that implement with dedicated hardware the most critical sections of the cryptographic algorithm and that are activated by the software program. This approach would allow reaching a balance between speed, manufacturing cost, design cost, and flexibility; only the most demanding segments of the encryption/decryption algorithms need be implemented by dedicated hardware, while their software-managed activation would grant a good measure of flexibility and adaptability to different algorithms (or to subsequent variations of given algorithms). A first basic problem is automatic extraction of the critical section from the overall algorithm: several proposals have been made in the literature (also by some of the present proponents) but figures of merit adopted for extraction have been area and performance. One

of our goals will be to adapt such techniques to drive the identification for security. We will need to use our a-priori high-level metrics to extraction operations to be performed in the coprocessor and to identify rules guiding invocation of the coprocessor by the software. While it is difficult to envision high-level, platform-independent solutions granting “smooth” power consumption in execution software, exploration of re-scheduling techniques leading to flat power profiles for a pre-determined platform could constitute an interesting complement to coprocessor design.

In summary, we will explore different aspects in the three domains to:

- Study systematically existing techniques to build systems and components with a high level of robustness to TA and PA attacks and conceive novel ones.
- Achieve systems whose low energy consumption and performance is not compromised by the need of obeying a security constraint.
- Develop design methodologies to achieve the goals of the two bullets above, rather than produce ad-hoc implementations in specific contexts or technologies.

2.3 State of the Art

The state of the art is organised as follows: Section 2.3.1 discusses several techniques that are either known effective against TA and PA, or that the applicants believe could be effectively used. Section 2.3.2 discusses in rather general terms the problem of achieving low power consumption: the field is very large but some specific background work fundamental for the present projects will be discussed. Although our aim is more focused on design methodologies rather than on specific implementations, we discuss briefly some of the most important implementations of energy-efficient cryptographic coprocessors in Section 2.3.3. Finally, Section 2.3.4 reviews some design methodologies that we see as the essential starting point to combine effectively and efficiently DPA-robust design ideas and low-power techniques in practical embedded processors customised with cryptographic coprocessors. In Section 2.3.5 we will briefly go back to our goals in the light of the discussed existing literature.

2.3.1 Design Solutions to Counter TA and PA Attacks

Since the original demonstration of the TA and PA attacks, several solutions have been investigated and, in many cases, applied. The following bullets review design techniques that are either known to be somehow effective to counter TA and PA attacks or that these authors believe to be applicable with success to design DPA-resistant systems.

It should be noted that many solutions have been developed in the software and mathematical domain to make the cryptographic computations secure to SPA and DPA, especially elliptic-curve cryptosystems. Many early techniques were introduced soon after TA- and PA attacks had been demonstrated [CoronAug99]. A recent paper [GoubinJan03] surveys most theoretical solutions and indicates that in some practical scenarios such countermeasures can in fact be defeated; in practice, this suggests that it is not possible to simply rely on one class of countermeasures but all areas should be addressed concurrently—provided they can be implemented sufficiently economically.

We will therefore focus here on hardware implementation solutions, whose automatic, and thus cheap, application will be the object of the present project.

a) Dual-Rail Design

A logic style called *dual-rail* consists in designing CMOS logic gates with two transistor networks, the first one generating the true output and the second one generating the complementary output. An example of such a logic style is, for instance, DCVSL logic [HellerFeb84]. It is based on precharged logic in which both outputs are precharged to “1” at the beginning of the operation. In the evaluation phase, one of the output is necessarily switched to “0” while the other output stays at “1”. As a consequence, for each computation,

one output signal is always switched to “0”, implying the same activity and the same power consumption for each computation. It is therefore more difficult to trace power consumption variation during the execution of a cryptographic algorithm. Recent research has shown some weaknesses of the basic DCVSL scheme and suggested improvements [TiriSep02].

All such logic styles directly impact on the number of transistors required to implement a given logic function. This number is roughly increased by a factor of two. Furthermore, the activity of each dual-rail logic gate is dramatically increased, as the gate is precharged and switches for each clock pulse. If the output of a non dual-rail logic gate stays at “0” during several clock pulses, there is no activity and therefore no dynamic power. If the same function is implemented in dual-rail logic, the gate switches at each clock pulse. Dynamic and differential schemes are certainly useful for the implementation of PA-resistant cryptographic hardware but cannot be used indiscriminately, especially in mobile power- and cost-sensitive environments.

b) Asynchronous Designs

An interesting approach is to adopt asynchronous logic for designing all the components of a SoC. While such an approach requires to master asynchronous circuit design—which is not yet an easy task due to the lack of appropriate CAD tools, it also brings very interesting features. It is recognized that asynchronous blocks (generally based on a dual rail circuit implementation) are very easy to reuse and easy to integrate in a complex heterogeneous integrated systems because they are locally controlled, they provide flexible and efficient interfacing mechanisms, they have a lower mean power consumption while providing maximum performance, and finally they generate lower electromagnetic noise and smaller currents peaks in the power supply [RenaudinMar01]. This last feature is recognized as very promising for cryptographic applications [KesselsApr00, AbrialJul01, MooreApr02].

Asynchronous circuits do not have a global clock, hence there is not a global timing signal to use as a reference and the analysis of power consumption is more difficult. In a DPA attack, an average power trace has to be established, but in asynchronous circuits, as operations or instructions execute in variable amount of time, there are some power waveform shift and overlap. In fact, it is hard to determine when an operation or instruction starts and stops. A variable execution time can result both from data-dependent operations (e.g., an addition can take time to complete or can absorb a larger power depending on the particular operands), but it can also result from the handshake signals from other asynchronous stages (in this case, it is data-independent). Therefore, the waveforms will not have exactly the same constant periodicity. The statistical analysis required for DPA will be much more difficult to compute. There are probably some possible techniques to re-synchronize the power traces to get the average one, but this could be quite difficult and the feasibility is still an open question. As mentioned, in asynchronous circuits the execution time is typically data-dependent (and should be avoided as much as possible [MooreApr02]), but can also be data-independent (and thus could be useful to confuse the attacker).

c) Synthesis Techniques to “Flatten” the Power Consumption Trace

Techniques to reduce the peaks in power consumption (and thus supply line bounce) have been around for a few years [BeniniJun97] and are essentially based on appropriately tuning the clock signal skew across the circuit: optimal skew for clusters of flip-flops “dilutes” the power consumption while still satisfying the timing constraints. More recent contributions [BlunnoSep02] have extended and optimised such techniques to reduce electromagnetic emissions and control the spectrum of the emitted radiation. These techniques are in principle independent of the logic implementation style of gates and flip-flops, and are applied during the logic synthesis step: they are good starting points to develop synthesis algorithms for cryptographic hardware. To our knowledge, the effectiveness of such high-level techniques for the purpose of PA-robustness has not been addressed yet; a comparison with other logic-style techniques to control the profile of the power consumption traces seems appropriate. Besides, synthesis techniques and special logic styles are not mutually exclusive and could possibly complement each other well.

2.3.2 Power Modelling and Low-power Design Techniques

Power consumption is today the major issue in the design of integrated circuits for portable and wireless devices. Design methodologies for both hardware and software and at different abstraction levels such as system, high-level language software, architecture, assembly code, logic design, basic cells, as well as layout, have nowadays to take into account the power consumption [Piguet01, Wolf01].

In hardware, the main goals of such design methods are supply voltage reduction, circuit activity reduction, as well as parasitic capacitance reduction. Many techniques have been presented in literature and their review goes beyond the scope of this survey; they include: gated clocks, pipelining, parallelism, very low supply voltage, multiple supply voltages, variable supply and transistor-threshold voltages, activity estimation and optimisation, low-power libraries, reduced voltage swing, asynchronous design, and adiabatic design [Chandrakasan98]. The choices among these techniques are strongly application-dependent and the very specific PA-robustness requirement dominates here the requirements; hence very peculiar methodologies might be required for cryptographic applications, inspired and yet original compared to established practices.

Considering instruction-level power modelling and optimisation, the work most relevant to the present research has concentrated on modelling power consumption per instruction and in profiling energy consumption in software programs [TiwariDec94, RussellOct98, SinhaJun01]. Such models have been used to improve the assembly code of an application either by binary transformations or by incorporating them in energy-aware research compilers. More recent work by one of the applicants has refined power consumption models so as to take into account more advanced architectures such as *Very Long Instruction Word (VLIW)* processors [Zaccaria03, SamiSep02, BonaJun02]. In our context, software aspects should be considered in relation to coprocessor design, insofar as bus and memory activities can be dominated by proper software design and compilation.

2.3.3 Cryptographic Coprocessors

As for most regular stream-based applications, a large amount of literature exists on any sort of coprocessors for various cryptographic algorithms. Typical goals for ASIC implementations are performance (e.g., [KuoMay02]), energy-efficiency (e.g., [GoodmanNov01]), robustness to side-attacks (e.g., [KesselsApr00], [AbrialJul01]), or reconfigurability (e.g., [SchaumontJun01], [GoodmanNov01]). Many of these approaches have been already discussed in previous sections; what seems important is to combine some of the research directions opened by these pieces of work and especially evolve them into appropriate design methodologies that go beyond specific implementations or cryptographic algorithms.

An important side of versatility in cryptographic coprocessors has not been much addressed so far: it is arguable that an increasing flexibility in embedded and mobile systems will be needed. This is not only justified by the introduction of new cryptographic algorithms, but in the need (or at least opportunity) to adapt the level of encoding (key length, type of algorithm, number of encrypting rounds, etc.) to environmental parameters such as available energy, available computing power, criticality of the information, application, etc. This emphasizes the growing importance of design methodologies (as opposed to ad-hoc designs) and of reconfigurable hardware in cryptographic coprocessors.

2.3.4 Automatic Design Methodologies for Tightly-Coupled Coprocessors

In the last decade, research in design methodologies for system-on-chip processors has been mainly revolving around the automatic synthesis of *Application Specific Instruction Processors (ASIPs)*. The goal has been to develop automatically processors, which are more cost effective for given applications or application domains. The synthesis of ASIPs involves the automatic generation of complete instruction sets for specific applications ([ImaiSep92,

Holmer93, VanPraet94, HuangJun95]. In that context, the goal is typically to cluster all the atomic operations required for an application into a complete instruction set which minimizes some important metric (e.g., execution time, program memory size, number of execution units).

More recently, the attention has shifted toward extending generic processors with units specialised for a given domain, rather than designing completely custom processors. These additional functional units or configurable datapaths can be thought as tightly-coupled fine-grained coprocessors. The goal of such processor extensions is typically to optimise performance in an application domain without incurring the area and energy cost of top-notch superscalar or multithreaded processors. Many readily extensible processors exist today both in academia (e.g., [LaRosaNov01], [CampiSep01]) and industry (e.g., [WangJun01], [HalfhillJun00], [FaraboschiJun00], [EyreJul00]). The important motivation toward specialisation of existing processors versus the design of complete ASIPs is to avoid the complexity of a complete processor and toolset development. Instead, an available and proven processor design (possibly including its implementation as a layout hard-macro) and its extensible toolset can be leveraged: design efforts must focus exclusively on the special application-domain specific datapath. This partitioning in a standard part (as large as possible) and a limited application specific part appears particularly appropriate in the context of this project, where potentially complex or unorthodox design techniques would be used for the coprocessor to make it secure. But we believe that it would be an extreme advantage to generate the required instruction-set extensions in an automated manner.

Authors who have attacked the problem of automatic instruction synthesis often concentrate on maximal reuse of the complex instructions and on a minimal number of instructions selected (e.g., [ChoiJun99]). The reuse goal is likely to favour the identification of small clusters of primitive operations; hence, heuristically, the search space is pruned by explicitly limiting the complexity of the special instructions. In [KastnerOct02] or [ArnoldApr01], the authors use approaches combining template matching (*instruction selection*, as it is called in compilers) and template generation (*identification*, in our parlance) for ASIPs. The main specificity of the approach described in [KastnerOct02] is that their clustering is based on the frequency of node types successions—e.g., multiplications followed by additions—rather than on frequency of execution of specific nodes; hence, simple pairs of operations appear the best candidates. Their work does not account for constraints on the number of inputs and outputs of the clusters, which is correspond to fundamental microarchitectural constraints. Work in reconfigurable computing is often more in line with the goal of clustering very large critical clusters (e.g., [RazdanNov94], [AlippiMar99], [KastrupApr99], [YeJun00]). Yet, identification algorithms are relatively simple and almost invariably target clusters producing a single result. Usually, clusters or subgraphs are somehow grown from their output nodes by adding predecessors until some constraints are violated. More formal approaches such as the one described in [AlippiMar99] guarantee a decomposition in maximal single-output subgraphs: unfortunately, the approach cannot be easily extended to multiple output subgraphs and the property of maximal size does not represent optimality under essential constraints such as the number of inputs. In [BaleaniMay02], the identification problem is addressed in a wider context of hardware/software partitioning. A simple clustering algorithm is used, called *clubbing*, to enforce limits on the input and output counts (to 3 and 2 respectively, in the examples) and to ensure deterministic functionality. Recent work by one of the applicants [VermaNov02, AtasuJun03] has introduced a stronger formalisation of the problem and new algorithms to solve it in realistic microarchitectural constraints.

In this project, we wish to improve algorithms for the synthesis of special instructions in two ways: (1) it should be possible to minimize also energy, rather than only cost or execution time alone, and (2) special instructions should include a part of the cryptographic application sufficiently large such that the implementation of such instruction using DPA-robust techniques will ultimately make the whole system DPA-robust. Currently, none of the existing instruction identification techniques can address either of these two aspects.

2.3.5 Summary of the Problems and Outlook

TA and PA attacks, in their many forms, represent today one of the most critical weaknesses of cryptographic implementations. Although many techniques to improve the security of the implemented algorithms have been introduced since the first demonstration of such attacks, none is fully secure. It seems unlikely that a single full solution to these form of attack will be find in any foreseeable time, whereas there is a growing need for cheap, very low power, highly secure implementations.

We believe that there is a need to work in a synergic way at various levels:

- Algorithmic level.
- Definition of metrics and models.
- Logic synthesis.
- Logic design style.

We do not plan to work on the first level but we will work jointly on the other three levels.

Essentially, in all areas, the main goals are:

1. Minimise data-dependent timing and/or power variability.
2. Exploit or create, whenever possible and appropriate, data-independent variability.

The first goal can build on a solid research tradition and often leverage existing results by reapplying them in a new form (e.g., instruction-level power modelling for smoothing rather than for minimal energy). The latter goal represents more an opportunity to be exploited whenever possible (e.g., using the irregular execution in asynchronous logic for uncritical code and thus shift power waveforms to make re-synchronization harder).

Unfortunately, typically the above goals increase significantly power consumption and often also reduce performance: they negatively impact two extremely critical design metrics in embedded and wireless systems. Also, the use of peculiar logic design styles may make it difficult to design full complex systems in an efficient VLSI design flow. The automatic or semiautomatic identification of tightly-coupled coprocessors may be key in (1) isolating minimal parts of the cryptographic code for secure implementation and (2) speeding up execution and reducing energy consumption.

References

- [AbrialJul01] André Abrial, Jacky Bouvier, Marc Renaudin, Patrice Senn, and Pascal Vivet. A new contactless Smart Card IC using an on-chip antenna and an asynchronous microcontroller. *IEEE Journal of Solid-State Circuits*, 36(7):1101-7, July 2001.
- [AlippiMar99] Cesare Alippi, William Fornaciari, Laura Pozzi, and Mariagiovanna Sami. A DAG based design approach for reconfigurable VLIW processors. In *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition*, pages 778-79, March 1999.
- [Anderson01] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, New York, 2001.
- [ArnoldApr01] Marnix Arnold and Henk Corporaal. Designing domain specific processors. In *Proceedings of the 9th International Workshop on Hardware/Software Codesign*, pages 61-66, Copenhagen, April 2001.
- [AtasuJun03] Kubilay Atasu, Laura Pozzi, and Paolo lenne. Automatic application-specific instruction-set extensions under microarchitectural constraints. In *Proceedings of the 40th Design Automation Conference, Anaheim, Calif., June 2003*. Submitted.
- [BaleaniMay02] Massimo Baleani, Frank Gennari, Yunjian Jiang, Yatish Pate, Robert K. Brayton, and Alberto Sangiovanni-Vincentelli. HW/SW partitioning and code generation of embedded control applications on a reconfigurable architecture platform. In *Proceedings of the 10th International Workshop on Hardware/Software Codesign*, pages 151-56, Estes Park, Colo., May 2002.
- [BeniniJun97] Luca Benini, Patrick Vuillod, Alessandro Bogliolo, and Giovanni De Micheli. Clock skew optimization for peak current reduction. *Journal of VLSI Signal Processing*, 16:117-30, June 1997.
- [BlunnoSep02] Ivan Blunno, Francesco Gregoretti, Roberto Passerone, D. Peretto, and Leonardo Maria Reyneri. Designing low electro magnetic emissions circuits through clock skew optimization. In *Proceedings of the 9th IEEE International Conference on Electronics, Circuits and Systems*, pages 417-20, Dubrovnik, Croatia, September 2002.
- [BonaJun02] Andrea Bona, Mariagiovanna Sami, Donatella Sciuto, Cristina Silvano, Vittorio Zaccaria, and Roberto Zafalon. Energy estimation and optimization of embedded VLIW processors based on instruction clustering. In *Proceedings of the 39th Design Automation Conference, New Orleans, La., June 2002*.

- [CampiSep01] Fabio Campi, Roberto Canegallo, and Roberto Guerrieri. IP-reusable 32-bit VLIW Risc core. In Proceedings of the European Solid State Circuits Conference, pages 456-59, Villach, Austria, September 2001.
- [Chandrakasan98] Anantha Chandrakasan and Robert Brodersen, editors. Low-Power CMOS Design. IEEE, New York, 1998.
- [ChoiJun99] Hoon Choi, Jong-Sun Kim, Chi-Won Yoon, In-Cheol Park, Seung Ho Hwang, and Chong-Min Kyung. Synthesis of application specific instructions for embedded DSP software. IEEE Transactions on Computers, 48(6):603-14, June 1999.
- [ClavierAug00] Christophe Clavier, Jean-Sebastien Coron, and Nora Dabbous. Differential power analysis in the presence of hardware countermeasures. In Çetin Kaya Koç and Christof Paar, editors, Cryptographic Hardware and Embedded Systems--CHES 2000, volume 1965 of Lecture Notes in Computer Science, pages 252-63. Springer, Berlin, August 2000.
- [CoronAug99] Jean-Sebastien Coron. Resistance against differential power analysis for elliptic curve cryptosystems. In Çetin Kaya Koç and Christof Paar, editors, Cryptographic Hardware and Embedded Systems--CHES '99, volume 1717 of Lecture Notes in Computer Science, pages 292-302. Springer, Berlin, August 1999.
- [EyreJul00] Jennifer Eyre and Jeff Bier. Infineon targets 3G with Carmel2000. Microprocessor Report, 17 July 2000.
- [FaraboschiJun00] Paolo Faraboschi, Geoffrey Brown, Joseph A. Fisher, Giuseppe Desoli, and Fred Homewood. Lx: A technology platform for customizable VLIW embedded processing. In Proceedings of the 27th Annual International Symposium on Computer Architecture, pages 203-13, Vancouver, June 2000.
- [GebotysOct02] Catherine H. Gebotys. Security-driven exploration of cryptography in DSP cores. In Proceedings of the 15th International Symposium on System Synthesis, pages 80-85, Kyoto, October 2002.
- [GoodmanNov01] James Goodman and Anantha P. Chandrakasan. An energy-efficient reconfigurable public-key cryptography processor. IEEE Journal of Solid-State Circuits, 36(11):1808-20, November 2001.
- [GoubinJan03] Louis Goubin. A refined power-analysis attack on elliptic curve cryptosystems. In Yvo G. Desmedt, editor, Public Key Cryptography--PKC 2003, volume 2567 of Lecture Notes in Computer Science, pages 199-211. Springer, Berlin, January 2003.
- [HalfhillJun00] Tom R. Halfhill. ARC Cores encourages ``plug-ins''. Microprocessor Report, 19 June 2000.
- [HellerFeb84] Lawrence G. Heller, William R. Griffin, James W. Davis, and Nandor G. Thoma. Cascode voltage switch logic: A differential CMOS logic family. In IEEE International Solid-State Circuits Conference, Digest of Technical Paper, pages 16-17, San Francisco, Calif., February 1984.
- [Holmer93] Bruce Kester Holmer. Automatic Design of Computer Instruction Sets. Ph.D. thesis, University of California, Berkeley, Calif., 1993.
- [HuangJun95] Ing-Jer Huang and Alvin M. Despain. Synthesis of application specific instruction sets. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, CAD-14(6):663-75, June 1995.
- [ImaiSep92] Masaharu Imai, Alauddin Alomary, Jun Sato, and Nobuyuki Hikichi. An integer programming approach to instruction implementation method selection problem. In Proceedings of the European Design Automation Conference, pages 106-11, Hamburg, September 1992.
- [KastnerOct02] Ryan Kastner, Adam Kaplan, Seda Ogrenci Memik, and Elaheh Bozorgzadeh. Instruction generation for hybrid reconfigurable systems. ACM Transactions on Design Automation of Embedded Systems (TODAES), 7(4), October 2002.
- [KastrupApr99] Bernardo Kastrup, Arjan Bink, and Jan Hoogerbrugge. ConClSe: A compiler-driven CPLD-based instruction set accelerator. In Proceedings of the 5th IEEE Symposium on Field-Programmable Custom Computing Machines, Napa Valley, Calif., April 1999.
- [KesselsApr00] Joep Kessels, Torsten Kramer, Gerrit den Besten, Ad Peeters, and Volker Timm. Applying asynchronous circuits in contactless Smart Cards. In Proceedings of the 6th International Symposium on Advanced Research in Asynchronous Circuits and Systems, pages 36-44, Eilat, Israel, April 2000.
- [KocherAug99] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael Wiener, editor, Advances in Cryptology--CRYPTO '99, volume 1666 of Lecture Notes in Computer Science, pages 398-412. Springer, Berlin, August 1999.
- [KuoMay02] Henry Kuo, Ingrid Verbauwhede, and Patrick Schaumont. A 2.29 Gbits/sec, 56 mW non-pipelined Rijndael AES encryption IC in a 1.8 V, 0.18 μ m CMOS technology. In Proceedings of the IEEE Custom Integrated Circuit Conference, pages 147-50, Orlando, Fla., May 2002.
- [LaRosaNov01] Alberto La Rosa, Luciano Lavagno, and Claudio Passerone. A software development tool chain for a reconfigurable processor. In Proceedings of the International Conference on Compilers, Architectures, and Synthesis for Embedded Systems, pages 93-98, Atlanta, Ga., November 2001.
- [MooreApr02] Simon Moore, Ross Anderson, Paul Cunningham, Robert Mullins, and George Taylor. Improving Smart Card security using self-timed circuits. In Proceedings of the 8th International Symposium on Advanced Research in Asynchronous Circuits and Systems, pages 211-18, Manchester, April 2002.
- [Piguet01] Christian Piguet. Low-power design of systems on chip. In Vojin G. Oklobdzija and Richard C. Dorf, editors, The Computer Engineering Handbook, chapter 18. CRC, 2001.
- [RazdanNov94] Rahul Razdan and Michael D. Smith. A high-performance microarchitecture with hardware-programmable functional units. In Proceedings of the 27th International Symposium on Microarchitecture, pages 172-80, San Jose, Calif., November 1994.
- [RenaudinMar01] Marc Renaudin and Christian Piguet. Asynchronous and locally synchronous low-power SOCs. In Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, pages 490-91, Munich, March 2001.

- [RussellOct98] Jeffry T. Russell and Margarida F. Jacome. Software power estimation and optimization for high performance, 32-bit embedded processors. In Proceedings of the International Conference on Computer Design, Austin, Tex., October 1998.
- [SamiSep02] Mariagiovanna Sami, Donatella Sciuto, Cristina Silvano, and Vittorio Zaccaria. An instruction-level energy model for embedded VLIW architectures. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, CAD-21(9):998-1010, September 2002.
- [SchaumontJun01] Patrick Schaumont, Ingrid Verbauwhede, Kurt Kreutzer, and Majid Sarrafzadeh. A quick safari through the reconfiguration jungle. In Proceedings of the 38th Design Automation Conference, pages 172-77, Las Vegas, Nev., June 2001.
- [SinhaJun01] Amit Sinha and Anantha P. Chandrakasan. JouleTrack: A web based tool for software energy profiling. In Proceedings of the 38th Design Automation Conference, pages 220-25, Las Vegas, Nev., June 2001.
- [TiriSep02] Kris Tiri, Moonmoon Akmal, and Ingrid Verbauwhede. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on Smart Cards. In Proceedings of the 28th European Solid-State Circuits Conference, pages 403-6, Florence, September 2002.
- [TiwariDec94] Vivek Tiwari, Sharad Malik, and Andrew Wolfe. Power analysis of embedded software: A first step towards software power minimization. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, VLSI-2(4):437-45, December 1994.
- [VanPraet94] Johan Van Praet, Gert Goossens, Dirk Lanneer, and Hugo De Man. Instruction set definition and instruction selection for ASIPs. In Proceedings of the 7th International Symposium on High-Level Synthesis, pages 11-16, 1994.
- [VermaNov02] Ajay Kumar Verma, Kubilay Atasu, Miljan Vuletic, Laura Pozzi, and Paolo lenne. Automatic application-specific instruction-set extensions under microarchitectural constraints. In Proceedings of the 1st Workshop on Application Specific Processors, Istanbul, November 2002.
- [WangJun01] Albert Wang, Earl Killian, Dror Maydan, and Chris Rowen. Hardware/software instruction set configurability for system-on-chip processors. In Proceedings of the 38th Design Automation Conference, pages 184-88, Las Vegas, Nev., June 2001.
- [Wolf01] Wayne Wolf. Computers as Components: Principles of Embedded Computer Systems Design. Morgan Kaufmann, San Mateo, Calif., 2001.
- [YeJun00] Zhi Alex Ye, Andreas Moshovos, Scott Hauck, and Prithviraj Banerjee. CHIMAERA: A high-performance architecture with a tightly-coupled reconfigurable functional unit. In Proceedings of the 27th Annual International Symposium on Computer Architecture, pages 225-35, Vancouver, June 2000.
- [Zaccaria03] Vittorio Zaccaria, Mariagiovanna Sami, Donatella Sciuto, and Cristina Silvano. Power Estimation and Optimization Methodologies for VLIW-based Embedded Systems. Kluwer Academic, Boston, Mass., 2003.

2.4 Research Fields of the Applicants

Paolo lenne is an Assistant Professor at the EPFL School of Computer and Communication Sciences, where he heads the *Laboratory of Processor Architecture (LAP)* and the *Centre for Advanced Digital Systems (CSDA)*.

The LAP has been created in 2000 and one of the main research topics addresses techniques for automatic processor specialisation. Early work at LAP dealt with the assessment of the potentials of specialisation through instruction-set extensions [PozziMar02, lenneDec01]; it was shown that significant speedups could be attained with limited hardware complexity. Development of an infrastructure for experimenting with VLIW processor specialisation has also been an important area of interest [MiddhaOct02]. Current work covers advanced techniques for the identification of complex instruction-set extensions under realistic microarchitectural constraints [VermaNov02, AtasuJun03]. As discussed in Section 2.2.4, these pieces of work constitute a starting point for the development of design methodologies under security constraints. Other current research activities are in the field of Networks-on-Chip and address low-power self-calibrating on-chip interconnects [WormOct02].

Before joining the EPFL, Paolo lenne was with Siemens Semiconductors AG (later Infineon Technologies AG) where he was responsible of the group developing SoC memory generators for all standard Infineon CMOS technologies. Active research in the unit addressed advanced memory architectures and generation and synthesis of datapath and arithmetic components [lennenJun98]. Previous research was in the area of specialised computer architectures, and in particular on accelerators for neural network algorithms [Viredaz02, lenneMar97, lenneDec94].

Prof. lenne has been member of the Program Committees of some international conferences, including the *IEEE International Conference of VLSI Design 2003*, the *Design Automation &*

Test in Europe Conference 2003, IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems 2002. He has been a reviewer for the *IEEE Transactions on Computers*, the *IEEE Journal of Solid-State Circuits*, the *Journal of System Architecture*, the *Journal of Parallel and Distributed Computing*, and several international conferences.

Mariagiovanna Sami is the Scientific Director of ALaRI (USI) and a full professor in Digital Systems Design at Politecnico di Milano (one of the partner Universities in the ALaRI scientific and training organization). She has been Chairperson of the Department of Electronics of Politecnico di Milano and is the Delegate of the Rector of Politecnico on ALaRI Steering Committee.

Prof. Sami got her Dr. Ing. Degree from Politecnico di Milano and subsequently her *Libera Docenza*, Computers, in 1971. Her research interests have focused always on the area of digital systems design, with particular reference to design and testing techniques, defect- and fault-tolerance of complex systems, and more recently to low-power design of embedded systems. In the past four years she has mainly concentrated on the last-named area, focusing on the problems of power estimation for complex CPUs and architectures and of CPU design optimization aimed at achieving low power consumption [Zaccaria03, SamiSep02, BonaJun02]. She has published over 200 papers in international scientific journals and in proceedings of international conferences and chapters of books, and is the co-author of the books “Fault-tolerance through Reconfiguration of VLSI and WSI Arrays” published by the MIT Press and “Power Estimation and Optimization Methodologies for VLIW-based Embedded Systems”, published by Kluwer Academic Press. She has filed an international patent concerning power-saving CPU architectures.

Prof. Sami has been a member of the Program Committees of a number of IEEE International Conferences, chaired several international conferences (in particular, IEEE conferences such as the 1983 *Fault-Tolerant Computing Symposium*, the 1993 *Defect and Fault Tolerance Symposium*, the 1999 *IJCNN*, etc.), as well as two NATO Advanced Study Institutes (on VLSI Testing in 1985, co-chaired with Prof. Lombardi then of the University of Colorado, and one in 1995 on Embedded Systems Design, co-chaired with Prof. De Micheli of Stanford University). Prof. Sami has been the Editor-in-chief (jointly with Prof. Lutz Richter of Zurich University) of the *Journal of System Architecture* (edited by North-Holland Elsevier) and has been a member of the Board of Editors of the *IEEE Transactions on Computers* and of *IEEE Design and Test*, as well as of the Advisory Board of *IEEE Computer*. She is a member of the Board of Editors of the *Journal of Electronic Testing—Theory and Applications* (JETTA) published by Kluwer International.

Christian Piguet (M.S. 1974, Ph. D. 1981) is Head of the Low-Power Section at CSEM, Neuchâtel, Switzerland. He is Professor at the Ecole Polytechnique Fédérale Lausanne (EPFL), Switzerland, and also lectures in VLSI and microprocessor design at the University of Neuchâtel, Switzerland and in the ALaRI master at the University of Lugano, Switzerland. He is also a lecturer for many postgraduates courses in low-power design.

At CSEM, he is involved in the design of low power integrated circuits in CMOS technology [Piguet01], including the design of very low-power microprocessors and DSPs, EEPROM memories and SRAM memories [MasgontySep01], low-power standard cell libraries [MasgontySep01b], gated clock [ArmSep00, Soudris02, Piguet02] and low-power techniques as well as asynchronous design [PiguetJul00, PiguetFeb01, PiguetMar01, RenaudinMar01, CuheJan02]. Some projects are focussed on very low supply voltage logic design, including SOI technologies, and the static power in very advanced technologies (0.13 micron and below). Multiple MOS Threshold Voltages, self-adjusting MOS Threshold Voltages and switches in the power lines, are known techniques, and some original techniques like weak inversion logic or new memory structures are currently studied. Applications in which these circuits are used are baseband, audio and image processing, Radio Data System, ad hoc networks.

Christian Piguet holds about 30 patents in digital design, microprocessors and watch systems. He is author and co-author of more than 150 publications in technical journals and of several books and book chapters in low-power digital design. He has served as reviewer

for many technical journals. He also served as Guest Editor for the July 96 JSSC Issue. He is member of steering and program committees of numerous conferences and has served as Program Chairman of PATMOS'95 in Oldenburg, Germany, co-chairman at FTFC'99 in Paris, Chairman of the ACiD'2001 Workshop in Neuchâtel, Co-Chair of VLSI-SOC 2001 in Montpellier and Co-Chair of ISLPED 2002 in Monterey.

References

- [ArmSep00] C. Arm, J.-M. Masgonty, and C. Piguet. Double-latch clocking scheme for low-power I.P. cores. In Proceedings of the International Workshop on Power and Timing Modeling, Optimization and Simulation--PATMOS 2000, Göttingen, Germany, September 2000.
- [AtasuJun03] Kubilay Atasu, Laura Pozzi, and Paolo lenne. Automatic application-specific instruction-set extensions under microarchitectural constraints. In Proceedings of the 40th Design Automation Conference, Anaheim, Calif., June 2003. Submitted.
- [BonaJun02] Andrea Bona, Mariagiovanna Sami, Donatella Sciuto, Cristina Silvano, Vittorio Zaccaria, and Roberto Zafalon. Energy estimation and optimization of embedded VLIW processors based on instruction clustering. In Proceedings of the 39th Design Automation Conference, New Orleans, La., June 2002.
- [CucheJan02] Cédric Cuche, Christian Piguet, and Vojin G. Oklobdzija. Design flow and CAD tools for asynchronous design of sequential library cells. In Proceedings of the ACiD-WG Workshop, Munich, January 2002.
- [lenneDec94] Paolo lenne and Marc A. Viredaz. Bit-serial multipliers and squarers. IEEE Transactions on Computers, C-43(12):1445-50, December 1994.
- [lenneMar97] Paolo lenne, Patrick Thiran, and Nikolaos Vassilas. Modified self-organizing feature map algorithms for efficient digital hardware implementation. IEEE Transactions on Neural Networks, NN-8(2):315-30, March 1997.
- [lenneJun98] Paolo lenne and Griesing Alexander. Practical experiences with standard-cell based datapath design tools--do we really need regular layouts? In Proceedings of the 35th Design Automation Conference, pages 396-401, San Francisco, Calif., June 1998.
- [lenneDec01] Paolo lenne, Laura Pozzi, and Miljan Vuletic. On the limits of processor specialisation by mapping dataflow sections on ad-hoc functional units. Technical Report 01/376, Swiss Federal Institute of Technology Lausanne (EPFL), Computer Science Department (DI), Lausanne, December 2001.
- [MasgontySep01] Jean-Marc Masgonty, Stefan Cserveny, and Christian Piguet. Low-power ROM and SRAM memories. In Proceedings of the International Workshop on Power and Timing Modeling, Optimization and Simulation, Yverdon, Switzerland, September 2001.
- [MasgontySep01b] Jean-Marc Masgonty, Stefan Cserveny, Claude Arm, Pierre-David Pfister, and Christian Piguet. Low-power low-voltage standard library cells with a limited number of cells. In Proceedings of the International Workshop on Power and Timing Modeling, Optimization and Simulation, Yverdon, Switzerland, September 2001.
- [MiddhaOct02] Bhuvan Middha, Varun Raj, Anup Gangwar, Anshul Kumar, M. Balakrishnan, and Paolo lenne. A Trimaran based framework for exploring the design space of VLIW ASIPs with coarse grain functional units. In Proceedings of the 15th International Symposium on System Synthesis, Kyoto, October 2002.
- [PiguetJul00] Christian Piguet. Robustness of asynchronous sequential standard cells in a synchronous environment. In Proceedings of the Workshop on Asynchronous INTERfaces--AINT'00, Delft, The Netherlands, July 2000.
- [Piguet01] Christian Piguet. Low-power design of systems on chip. In Vojin G. Oklobdzija and Richard C. Dorf, editors, The Computer Engineering Handbook, chapter 18. CRC, 2001.
- [PiguetFeb01] Christian Piguet. Design of dynamic asynchronous flip-flops and counters based on dynamic STG. In Proceedings of the ACiD-WG Workshop, Neuchâtel, Switzerland, February 2001.
- [PiguetMar01] Christian Piguet. Low-power issues for SoCs. In Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, pages 488-90, Munich, March 2001.
- [Piguet02] Christian Piguet. Low-power clock, interconnect and layout designs. In Dimitrios Soudris, Christian Piguet, and Costas Goutis, editors, Designing CMOS Circuits for Low Power, chapter 8, pages 143-70. Kluwer Academic, Boston, Mass., 2002.
- [PozziMar02] Laura Pozzi, Miljan Vuletic, and Paolo lenne. Automatic topology-based identification of instruction-set extensions for embedded processors. In Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, page 1138, Paris, March 2002.
- [RenaudinMar01] Marc Renaudin and Christian Piguet. Asynchronous and locally synchronous low-power SOCs. In Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, pages 490-91, Munich, March 2001.
- [SamiSep02] Mariagiovanna Sami, Donatella Sciuto, Cristina Silvano, and Vittorio Zaccaria. An instruction-level energy model for embedded VLIW architectures. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, CAD-21(9):998-1010, September 2002.
- [Soudris02] Dimitrios Soudris, Christian Piguet, and Costas Goutis, editors. Designing CMOS Circuits for Low Power. Kluwer Academic, Boston, Mass., 2002.
- [VermaNov02] Ajay Kumar Verma, Kubilay Atasu, Miljan Vuletic, Laura Pozzi, and Paolo lenne. Automatic application-specific instruction-set extensions under microarchitectural constraints. In Proceedings of the 1st Workshop on Application Specific Processors, Istanbul, November 2002.
- [Viredaz02] Marc A. Viredaz and Paolo lenne. MANTRA I: A systolic array for neural computation. In David Zhang and Sankar K. Pal, editors, Neural Networks and Systolic Array Design, volume 49 of

- Machine Perception and Artificial Intelligence, chapter 4, pages 71-92. World Scientific, Singapore, 2002.
- [WormOct02] Frédéric Worm, Paolo Ienne, Patrick Thiran, and Giovanni De Micheli. An adaptive low-power transmission scheme for on-chip networks. In Proceedings of the 15th International Symposium on System Synthesis, Kyoto, October 2002.
- [Zaccaria03] Vittorio Zaccaria, Mariagiovanna Sami, Donatella Sciuto, and Cristina Silvano. Power Estimation and Optimization Methodologies for VLIW-based Embedded Systems. Kluwer Academic, Boston, Mass., 2003.

2.5 Detailed Project Plan

To achieve our goal of enabling the efficient design of processor systems robust to TA and PA attacks and with low-energy consumption, we plan three steps: (1) Develop metrics of robustness to help identify critical software sections and to estimate the quality of hardware implementations. (2) Explore VLSI design methodologies to achieve high robustness at a low energy cost in cryptographic hardware, both using special circuit techniques or innovative logic synthesis methodologies. (3) Apply the robustness metrics to identify parts of the cryptographic algorithms best implemented in coprocessors and use the VLSI methodologies to realize secure and versatile implementations.

In the following, the *italic typeface* is used to indicate more speculative topics which may be only touched upon or investigated in more depth depending on the results obtained.

2.5.1 Robustness Metrics

To establish robustness metrics, we plan the following activities:

- **Explore metrics of hardware and software TA- and PA-criticality.** Algorithmic models of computation criticality are essential to (1) assess the impact of hardware/software partitioning on robustness and (2) develop algorithms to assign to hardware automatically or semi-automatically the critical code.
 - Collect and classify sources of TA- and PA-weaknesses described in literature; develop or collect software examples containing typical pathologies.
 - At hardware level, analyse the weaknesses of traditional designs at different levels of abstraction (e.g., transistor-level and gate-level) and develop algorithms to estimate the robustness at high abstraction levels.
 - At software level, develop and test algorithms to measure overall criticality of programs and/or assign a criticality index to variables, basic blocks, and/or operations; such algorithms might be implemented on some versatile compiler intermediate representation (e.g., SUIF or MachSUIF).
 - *Analyse the capabilities of such methods especially in relation with mathematical methods for robustness (e.g., randomised secret exponents or randomised projective homogeneous coordinates [GoubinJan03]); try to compensate their possible shortcomings with minimal manual annotations.*

2.5.2 VLSI Design Methodologies

On the VLSI design methodologies side, we plan to move along the following lines:

- **Compare implementation techniques with respect to information security and energy requirements. Develop novel and superior ones.** It is important to establish in a systematic way the advantages and disadvantages of known or usable techniques to achieve robustness with limited energy cost. Additional criteria to consider are the ease of automatic design, the ease of integration in standard CMOS synchronous logic, etc.
 - Traditional, energy-expensive, dual rail techniques should be considered for their simplicity. Possibilities of containing the power consumption should be explored.
 - Advanced quasi delay-insensitive techniques are also a natural option, but focus should be on (1) integrating a limited asynchronous implementation in a globally synchronous circuit—to reduce cost and energy—and (2)

understanding the possible intrinsic weakness due to data-dependent timings. The latter problem is probably emphasized by the integration of asynchronous logic in a globally synchronous environment (that is, the synchronous environment would make a good correlation of the traces possible and the asynchronous data-dependent timing could then easily leak the secrets).

- Complementarily, investigate the importance of shifts in power and timing waveforms of asynchronous architectures to defeat TA and PA attacks: to which extent such shifts prevent the correlation of these waveforms? Check robustness towards methods to resynchronize the waveforms or tolerate local correlation faults.
- Search for any other circuit techniques that present data-independent power consumption and execution time. They can be used to prevent information leaking in critical parts of the traces.
- Complementarily, search for novel circuit techniques that present different but data-independent power consumption and execution time for the same operations or instructions with the same operands. They can be used to make correlations between processed data and traces impossible or more difficult.
- **Compare special circuit techniques with special synthesis flows and standard circuit techniques.** An alternate strategy, which needs to be carefully contrasted with the one at the previous bullet, would be to use fully standard synchronous CMOS circuitry and modify logic synthesis techniques to reduce the power variations.
 - Adapt low-power and low-EM synthesis techniques to achieve “flattest” power consumption.

2.5.3 Methodologies for Secure Cryptographic Coprocessors

The ultimate goal of the project is in terms of overall hardware/software codesign methodologies. These are the planned activities:

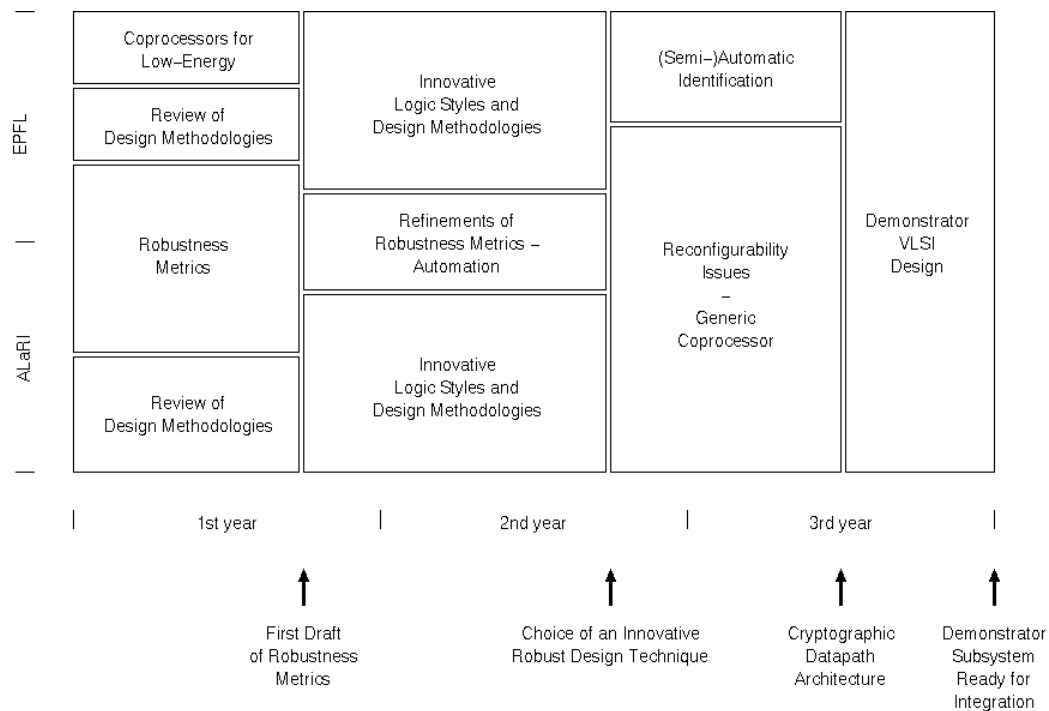
- **Understand the potentials of processor specialisation for low-energy.** The purpose of this topic is to (1) have a quantitative breakdown of the sources of consumption in a typical SoC processor subsystem and (2) assess the effectiveness of specialisation to address energy consumption.
 - Investigate specialisation potentials for representative cryptographic algorithms; focus on relatively simple, tightly coupled special functional units.
 - Assess their effectiveness both in terms of performance gain and reduced energy requirements; identify the sources of gain.
 - *If appropriate, derive new algorithms for automatic identification of special functional units which directly address energy reduction rather than performance improvement.*
- **Show automated or semiautomated flows to design secure low-power coprocessors.** The various conclusions of all phases of the project should converge in a set of methodologies to guide the designers. The level of automation of such techniques will largely depend on the individual results and achievements. Given the impossibility of solving the given security problem at a single level, the resulting methodologies should address a broad range of aspects.
 - *Exploit the novel metrics of robustness to improve automatic specialisation algorithms, at least to give reliable and easy-to-generate hints to developers on where to focus their attention.*
 - Research secure and flexible datapath structures for versatile low-power cryptographic applications.
 - Assess the suitability of explored implementation techniques to implement reconfigurable coprocessors. Reconfigurability could become critical in the future for mobile and embedded applications and it would be interesting to use a single datapath to implement various cryptographic algorithms and/or various levels of security.

2.6 Project Timetable

Two PhD students are planned for the project over a period of 3 years. One will work at EPFL and the other at ALaRI (USI). Each will profit of the specific strengths of the hosting institution: established competence in low-power and processor customisation at EPFL and in embedded system design and security at ALaRI.

The project outlined above is certainly an ambitious one and it will require much activity—not only in conception of innovative methodologies and design of original circuits and systems, but also in “experimental” phases involving development of suitable software tools (or extensions of existing toolsets) and extensive simulations. Actually, we should underscore that, to compensate for the relatively small man-power requested compared with the complexity of the task, we plan to foster a strong cooperation in this project not only with other researchers already operating within the cooperating institutions but also with master students (working for their practical MEng and MSc projects, at ALaRI and EPFL respectively) who will be involved in smaller sub-projects.

The three steps mentioned in Section 2.5 are logically in sequence, but will in practice largely overlap due to the need, for instance, of refining the metrics of criticality as a consequence of the detailed analysis of alternative implementation techniques. The figure indicate the planned development of the activities with an approximate share of the tasks between the two doctoral students:



The arrows at the bottom show four important milestones:

1. The first goal will be to understand to which extent robustness metrics are possible and how applicable they can be for automated design methodologies.
2. The second goal will be to add to the known robust logic styles and design methodologies both novel ideas and innovative ways to apply known methodologies. This will lead to the choice of one or two preferred robust design techniques
3. The third goal will be to determine a sufficiently flexible coprocessor architecture which is adapted to the design technique selected, on one hand, and to several cryptographic algorithms or security levels, on the other.

4. The achievements of the various phases of the project will be demonstrated with the VLSI design, potentially to be fully developed and manufactured at a later time, of significant sections of a generic/reconfigurable secure coprocessor.

2.7 Significance of the Research

At EPFL, the present project will be part of a larger effort to boost research in the area of Embedded Systems and Computer Engineering. The recently created *Centre for Advanced Digital Systems (CSDA)* across the School of Computer and Communication Sciences and the School of Engineering aims at fostering the interactions between Computer Science and Electrical Engineering. Among the first initiatives of the Centre, one could notice the plans for the creation of a specialisation in Computer Engineering in the MSc programmes, and the introduction of an advanced one-week yearly course in *Advanced Digital Systems Design*. The presence at EPFL of the NCCR MICS on ad-hoc networks is also particularly fitting, due to the complementarity of the present project with some of the MICS topics and the intrinsically accrued security needs of ad-hoc networks (see also Section 2.5.2).

At USI, the mission of ALaRI has been focused from the beginning on *embedded systems* and on design of application-specific digital systems; since its first year of existence, particular attention has been given to aspects of *security*, especially for *mobile systems*. Good results have been achieved in this area, particularly with respect to optimum implementation of cryptographic algorithms such as AES and Elliptic Curves and to design of innovative digital units dedicated to execution of relevant operations in cryptographic systems. Quality of the results achieved is proved by publications and by two patents filed on cryptography-related solutions.

2.5.1 Scientific Significance

To achieve the goals of the present project we raise the following fundamental questions:

1. Can one establish quantitative metrics of hardware TA and PA robustness? Can the properties they express be carried at higher abstraction levels (above transistor-level) to guide the design process (e.g., logic synthesis)?
2. Is it useful to extend the instruction-set of a standard processor to save energy? Is it a different problem than extending the instruction-set for performance? What are the appropriate algorithms to design such extensions automatically? What heuristics can be used to solve the problem efficiently?
3. Can one identify automatically sections of code that need to be isolated to achieve TA- and PA-robustness? What are the security-critical properties that trigger such clustering? How can these properties be combined with the techniques for low-power instruction-set extension?
4. Can one combine reconfigurable computing and secure implementation techniques? Is reconfigurability incompatible with security (e.g., because it will be impossible to guarantee “flat” consumption for every possible configuration)?

The questions at the first bullet have never been tackled systematically, to our knowledge. We do not hope for fully conclusive answers, but we wish to make some tangible steps toward an answer and show the importance of such effort—namely by using them to guide the design process.

The questions in the second bullet are still partly open and represent a new potential domain for generic embedded system optimisation. They are not specific to the cryptographic domain but cryptographic applications, thanks to their regularity, may be optimal candidates for such techniques. Clear answers can be expected from this project.

The questions concerning the identification of code sections requiring the application of robust design techniques have never been tackled, to our knowledge. It appears unlikely that fully automated decisions can be made, but the simple fact of investigating the issue could bring some new knowledge useful to design intrinsically robust cryptographic algorithms. Likely, more pragmatic, partly manual techniques will be applied to attain results of practical interest.

The last question is the most speculative: today both the field of TA- and PA-robust design and of reconfigurable hardware are active research domain in themselves. It is unclear whether the present project will advance sufficiently the state-of-the-art to address these questions, but attempts to answer the last bullet would mark a very significant achievement.

2.5.2 Industrial Significance

The proposed research addresses a very critical issue for economically very relevant domains such as wireless communications, Smart Cards, wireless PDAs, wireless ad-hoc networks. The need to avoid attacks on data transmitted from device to device is simply essential for many of these applications.

There are many emerging industrial applications requiring secure transmission, such as patient monitoring in hospitals, a proliferation of Smart Cards memorizing private information (especially in Europe), identification and control in office buildings and homes. For instance, hospitals are going to use extensively wireless technologies and will create significant markets for technologies dependent on secure transmission: Patients will wear small sensors to monitor vital functions and doctors will be able to monitor patients remotely and to control drug doses. Privacy protection is extremely important, as well as the security of authorizations to modify the amount or the frequency of the drug doses. Home surveillance systems will also soon have networks of wireless nodes, but the burglars should not be allowed to tamper with the information to and from the nodes that control and monitor windows and doors. Both examples demonstrate that secure transmissions are very important for most of the future wireless industrial systems.

Many wireless systems will be ad hoc networks—i.e., very small nodes that have to consume an extremely small amount of energy. Hence, the robustness of cryptographic algorithms to side-attacks cannot be considered independently from the tight low-power constraints of ad-hoc networks. From the industrial point of view, efficient and effective design methodologies for secure transmission consuming extremely small amounts of energy is one of the most critical elements for the success of ad-hoc wireless network products.

Several important semiconductor industries are present in Switzerland and can be interested in the results of the present project. Besides CSEM (in Neuchâtel), working on the WiseNet ad-hoc wireless sensor network research (to which one of the applicant participates), international companies active in SoC designs for communications include STMicroelectronics (with design centres in Lugano and Geneva), Motorola (with a design centre in wireless technologies in Geneva), and IBM ZRL (active in Zurich on research and advanced development on network processors).

Possible Referees

(in alphabetic order)

Prof. **Çetin Kaya Koç**
Oregon State University
Electrical & Computer Engineering
Corvallis, Oregon 97331
USA
E-Mail: koc@ece.orst.edu
<http://islab.oregonstate.edu/koc>

Dr. **Jeff Owen**
STMicroelectronics NV
Via Cantonale 16/E
6928 Manno
Switzerland
E-Mail: Jefferson.Owen@st.com

Prof. Dr.-Ing. **Christof Paar**
Ruhr-Universität Bochum
Department of Electrical Engineering and Information Technology
Communication Security Group
Gebaeude IC 4/131
Universitätsstrasse 150
44780 Bochum
Germany
E-Mail: cpaar@crypto.rub.de
http://www.crypto.ruhr-uni-bochum.de/MitarbeiterInnen/paar_eng.html

Prof. **Marc Renaudin**
TIMA-CIS
46, avenue Félix Vialet
38031 Grenoble Cedex
France
E-Mail: Marc.Renaudin@imag.fr
<http://tima.imag.fr/cis/people/renaudin.html>

Prof. **Ingrid Verbauwhede**
UCLA
Electrical Engineering Department
7440B Boelter Hall
P.O. Box 951594
Los Angeles, CA 90095-1594
USA
E-Mail: ingrid@ee.ucla.edu
<http://www.ee.ucla.edu/~ingrid/>