Final report:

Cryptographic Processor and Side-channel Attacks

Dr. Santosh Ghosh
ESAT - COSIC, KU Leuven,
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium.
Email: Santosh.Ghosh@gmail.com

Belspo Postdoctoral Fellowship for Non-EU Members Joined on Nov 21, 2011
Promotor: Prof. Ingrid Verbauwhede, ESAT/ COSIC, KU Leuven.

1. Background

With the rise of the Internet as a global information infrastructure and the increasing adoption of connected devices, information that used to take a considerable effort to retrieve is now readily available. This information infrastructure will keep expanding and will become more pervasive: we will evolve from a few devices per user to thousands of devices, large and small (up to the nano-scale) that are integrated into the environment and into our bodies and that interact in many complex ways. In addition our dependence on this infrastructure will grow, hence it becomes increasingly important to understand and manage the risks coming with this new infrastructure. This includes unauthorized access to services and information, privacy violations, denial of service attacks, and various kind of malware. With legal protection proving too slow and cumbersome to act as an effective deterrent in the fast-moving world of information technology, prevention of attacks by technological means has become more important than ever.

This technology depends on the quality and strength of the cryptographic algorithms which are used to set up secure and reliable communications and to provide privacy, authentication and other security goals in this ICT environment of the future. The security of today's most popular algorithms for public key cryptography (PKC) such as RSA, DSA and ECDSA highly relies on the strength and the hardness of the underlying mathematical problems. While the hard problems are intractable using today's computers, they are practically solvable using large quantum computers. As a result, in case quantum computers appear, it will bring a disaster to today's information security infrastructure. In order to prevent such potential risks, it is important to study cryptographic schemes that are provably secure in the era of quantum computers.

This research focuses on the design of compact, low-power hardware implementations of post-quantum PKCs. This study is motivated by the following two observations:

- research progress in post-quantum secure cryptographical algorithms
- increasing need for compact cryptographic cores in constrained devices.

This study is also an important part of the group's larger research framework, namely, efficient and secure implementations of public key cryptography for ubiquitous devices [1] [2]. We believe post-quantum PKCs are not only necessary but also have a great potential in embedded devices.

On the other hand, the physical security of a cryptographic algorithm depends on several

different issues which are mainly based on the unwanted leakage elimination from a cryptographic device. These leakages are power consumption, timing information, electromagnetic radiations, scan-out of design-for-test (DFT) structure, etc. These, information sometimes make a complex algorithm to be easily vulnerable.

2. Challenges and Objectives

This research focuses on the compact implementation of todays and post-quantum cryptographic schemes. Our goal is to investigate the implementation aspects of them. The objectives of this study include mainly three parts:

- **Efficient arithmetic:** Implementation of conventional PKC schemes (e.g. ECC and RSA), optimization of the arithmetic is the key step to achieve a high performance-cost ratio. There are a lot of options to improve performance of present days advanced PKC and pairing algorithms. However, studies on efficient arithmetic for the post-quantum schemes are rare in literature.
- **Low area implementation:** Strong cryptography is needed in not only for powerful computing devices such as personal computers, but also in resource-constrained devices. These small devices range from smart cards to passive RFID tags. ECC has been shown feasible on passive RFID tags [1], while the use of pairing as well as post-quantum PKCs on such constrained devices remains a great challenge.
- **Side-channel Security:** Theoretically sound cryptographic algorithms and protocols can be attacked at the implementation level [3][4]. In addition to the direct communication channels considered in typical cryptographic models, attackers may exploit several side-channels that may accidentally leak sensitive information (such as plaintext or secret keys); these channels include timing information, power consumption, electromagnetic and thermal radiation, scan-out etc. This study will focus on the vulnerability analysis and the design of countermeasures for the selected cryptographic schemes.

3. Methodology and Design approach

To obtain a compact side-channel secure implementation of an advanced public key cryptographic algorithm requires several design steps. The following steps have been identified for the research:

- **Complexity analysis and scheme selection:** This step analyzes the computational complexity of both proposed cryptographic schemes, and selects the most suitable one for compact implementation.
- **Arithmetic optimization:** This step searches for efficient arithmetic to realize the selected cryptographic scheme.
- **Hardware/Software co-design:** This step explores different architectures to reduce the area and power consumption. We provide a solution that consists of a dedicated hardware co-processor to implement the arithmetic instructions. It comes with a small micro-controller to the side that interfaces with other components and that provides flexibility.

- **Verification on FPGA**: In this step a prototype functional verification on an FPGA platform is made.
- **Side-channel Analysis and Countermeasures:** This step analyzes the physical security of the implementation and searches for possible countermeasures.
- **Further optimizations:** Based on the results of previous steps, this steps searches for further optimization in area, power and security. This may involve several design iterations.

4. Scientific Results

Here, we describe the scientific results which are obtained during this fellowship period. These results are the most important things which we achieved through this fund. Next, this fellowship gave Dr. Ghosh the opportunity to work at COSIC, a world famous research group in the field of cryptography and implementation aspects of cryptography. It provides him the opportunity to interact with many different researchers from many different scientific backgrounds and also to guide and supervise more junior students.

4.1 Compact Crypto-processors

The primary focus of this research was on secure and efficient implementations of *Current and New generation Public Key Cryptography (PKC).* For the current PKC, it made a significant progress in the implementation aspects of Elliptic curve and Pairing on FPGA platforms. The issue of efficient implementations as well as secure architecture design against Side-channel Attacks (SCA) have been targeted. In this regard, following two publications are achieved.

I. **Santosh Ghosh,** Ingrid Verbauwhede, and Dipanwita Roychowdhury. Core based architecture to speed up optimal Ate pairing on FPGA platform. **Pairing 2012, LNCS 7708, pp. 141-159,** Cologne, Germany, May 16-18, 2012.

Brief Description: This work presents an efficient implementation of optimal-ate pairing over Barreto-Naehrig curves. It exploits the highly optimized IP cores available for modern FPGAs. The in-built independencies of underlying operations of the pairing computation are fully utilized in order to run an optimized pipeline datapath with reduced number of stall cycles. The memory architecture based on IP cores are efficiently used for generating pipeline operands and storing intermediate results which reduces the use of registers in the design too. The pipelined datapath together with said memory architecture helps to reduce clock cycle count more than 50% of the pairing computation. A dedicated inversion unit is also incorporated into the design for reducing further cycle count. The final design, on a Virtex-6 FPGA, computes an optimal-ate pairing having 126-bit security in 0.375 ms which is a 32% speedup from state of the art result.

II. **Santosh Ghosh,** Amit Kumar, Amitabh Das, and Ingrid Verbauwhede. On the side-channel resistance of a unified binary Huff elliptic curve implementation on FPGA. Submitted to CHES 2013.

Brief Description: Unified formula for computing elliptic curve point addition and doubling are considered to be resistant against simple side-channel attack. A new elliptic curve formula known as unified binary Huff curve in this regard has appeared into the literature in 2011. This paper is devoted to analysing the applicability of this elliptic curve in practice. We demonstrate that the unified binary Huff curve is not actually secure against side-channel attacks. Even though both point operations are executed by the same sequence of finite field operations, due to processing of different coordinates, they demand different amounts of power. This paper pinpoints to the fact that the point doubling with unified Huff formula produces zero output in some intermediate finite field operations, which are non-zero in point addition. These zero (non-zero) values for point doubling (point addition) are further used as multiplicands in the unified formula. Results of the multiplications are also zero (non-zero). The power consumption of the multiplier circuit having zero and non-zero data are significantly different and they are visually observable through their power consumption graphs. We show the actual power consumption graphs of those operations on a SASEBO-G board which proves our claim and successfully demonstrates the vulnerability of the unified huff formula against simple power analysis. Apart from the side-channel resistance analysis, this paper also provides an efficient architecture and an optimal countermeasure of binary Huff curve.

On the other hand, the research on next generation post-quantum PKC achieved an important progress in the realization of the McEliece scheme, which is a Code-based Post Quantum PKC algorithm. The feasibility of a 128-bit secure McEliece cryptosystem on FPGA is shown for the first time by this research. The results of this research are accepted for publication in one of the top IEEE journals in Computer Science and Electrical Engineering.

I. **Santosh Ghosh** and Ingrid Verbauwhede. BLAKE-512 based 128-bit CCA2 secure timing attack resistant McEliece cryptoprocessor. [Accepted] IEEE Trans. on Computers, [now available online] http://ieeexplore.ieee.org, Vol. PP, Issue 99.

Brief Description: The most popular asymmetric key algorithms like RSA, Elliptic Curve, and Pairing are easily broken once fully functional quantum computer appears. The algorithms which can survive against the computation power of a quantum computer are known as post-quantum public key algorithms. McEliece is the oldest post-quantum public key encryption scheme (PKS) based on the hardness of decoding a general linear code which is known to be NP-Complete. In this regard, our research contributes the followings:

- It proposes hardware architecture for a 128-bit secure McEliece cryptosystem.
- It integrates BLAKE-512 hash algorithm with original McEliece scheme for providing CCA2 security based on a Kobara-Imai scheme.
- Suitable countermeasures are incorporated in the current design in order to overcome existing side-channel leakages of McEliece cryptosystem.
- To design an efficient and timing-attack resistant architecture, this paper introduces a binary-XGCD algorithm for Goppa field based on binary-GCD and its variant for computing error locator polynomials in Reed-Solomon decoding.
- The proposed architecture performs on a Virtex-6 FPGA encryption and decryption in 4.74 μs and 0.92 ms, respectively.

II. **Santosh Ghosh,** Jeroen Delvaux, Leif Uhsadel, and Ingrid Verbauwhede. A speed area optimized embedded co-processor for McEliece cryptosystem. IEEE ASAP 2012, Delft, The Netherlands, July 9-11, 2012.

Brief Description: This paper describes the systematic design methods of an embedded co-processor for a post quantum secure McEliece cryptosystem. A hardware/software co-design has been targeted for the realization of McEliece in practice on low-cost embedded platforms. Design optimizations take place when choosing system parameters, algorithm transformations, architecture choices, and arithmetic primitives. The final architecture consists of an 8-bit PicoBlaze soft-core for flexibility and several parallel acceleration units for throughput optimization. A prototype of the coprocessor is implemented on a Spartan-3an xc3s1400an FPGA, using less than 30% of its resources. On this FPGA, one McEliece decryption of an 80-bit security level takes less than 100K clock cycles corresponding to only 1 ms at a clock frequency of 92 MHz. This is 10 times faster and 3.8 times smaller than the existing design.

4.2 Physical Attacks

The secondary focus of the research was on *secure design for testability*. VLSI circuits are in general tested through the IEEE standard test infrastructure JTAG. JTAG is also sometimes used to update the internal firmware. This test structure uses scan-chains for providing inputs to the circuit and for taking outputs from the circuit. However, in case of cryptographic circuit scan-chains could be exploited for breaking the security. The current research outcomes some new ideas and shows several experimental results in the direction for standardizing a secure JTAG infrastructure. The related publications are as follows:

I. Amitabh Das, Baris Ege, **Santosh Ghosh,** and Ingrid Verbauwhede. Differential scan attack on AES with X-Tolerant and X-Masked test response compactor. DSD 2012, IEEE, Turkey, 2012.

Brief Description: Scan-chains are test infrastructures included in a circuit for providing high fault coverage. However, they can be exploited by an attacker as a side-channel in the case of a cryptographic application like AES. Test Compression and thereafter X-tolerance and X-masking over it, which reduce test effort without compromising on testability, can help in counteracting scan-based attacks. This work focuses on the security issues of an AES-circuit containing test compression with X-masking and X-tolerance logic. With experimental results, we show the weakness of such an AES circuit against our modified differential scan-attack. Finally, the paper outlines two suitable countermeasures to prevent such attacks.

II. Jean Da Rolt, Amitabh Das, **Santosh Ghosh,** Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre, and Ingrid Verbauwhede. Scan attacks on side-channel and fault attack resistant public-key implementations. Journal of Cryptographic Engineering, Vol. 2, No. 3, 19 pages, 2012.

Brief Description: Cryptographic devices are the targets of side-channel attacks, which exploit physical characteristics (e.g. power consumption) to compromise the system's security. Several side-channel attacks and countermeasures have been proposed in the literature in the past decade. However, countermeasures are usually designed to resist attacks for a single side-channel. Few papers study the effectiveness of a particular countermeasure which was developed for one specific side-channel attack on *another* attack which was not the target of the countermeasure. In this paper, we present scan-

based side-channel attacks on public key cryptographic hardware implementations in the presence countermeasures for power analysis and fault attacks. These aspects were not considered in any of the previous work on scan attacks. We have also considered the effect of Design for Test structures such as test compression and X-masking in our work to illustrate the effectiveness of our proposed scan attack on practical implementations. Experimental results showing the requirement of the number of messages/points and retrieval time are presented to evaluate the complexity of the attacks. Results show that algorithmic countermeasures for Simple Power Analysis and Fault attack are not immune against our differential scan-attacks, whereas the algorithmic countermeasures against Differential Power Analysis are secure against such scan-attacks.

III. Amitabh Das, Jean Da Rolt, **Santosh Ghosh,** Stefaan Seys, Sophie Dupuis, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre, and Ingrid Verbauwhede. Secure JTAG implementation using Schnorr protocol. [Accepted] Journal of Electronic Testing: Theory and Applications, Springer, 2013.

Brief Description: JTAG (Joint Test Access Group) is a powerful tool for the embedded system development environments. The features of JTAG, however, can be exploited by malicious users as a backdoor for launching attacks, an approach which now constitutes a major threat in the domain of device hacking. To deny unauthenticated users access to the features of JTAG port, this paper proposes a novel JTAG security mechanism. The proposed solution uses authentication based on credentials to achieve improved security and usability over existing solutions. Our approach is easily applicable to all standard JTAG environments because its structure is designed to be independent from the application environment. Further, the approach has lower implementation cost than encryption/decryption-based solutions since only hash and XOR calculations are employed in its authentication protocol. The security of the proposed mechanism has been verified through analysis against all forms of expected attacks, and its functionality is demonstrated with a real-life implementation.

IV. Amitabh Das, Baris Ege, **Santosh Ghosh,** and Ingrid Verbauwhede. Security of industrial test compression schemes. [Submitted] IEEE Trans. on CAD.

Brief Description: Test compression is widely used for reducing test time and cost of a VLSI circuit. It is also claimed to provide security against scan-based side-channel attacks. This paper pursues the legitimacy of this claim and presents scan attack vulnerabilities of test compression schemes used in commercial EDA tools. A publicly available AES design is used and test compression structures provided by Synopsys, Cadence and Mentor Graphics DFT tools are inserted into the design. The differential scan attacks presented in this paper suggest that the tools using X-masking are vulnerable against such attacks. The other test choice, the use of X-tolerant logic, however, leaks limited information about the secret key, with the best case success rate of 49.14% for a random scan design. On the other hand, time compaction seems to be the strongest choice with the best case success rate of 3.55%. In addition, similar attacks are also performed on existing scan attack countermeasures proposed in literature, thus experimentally evaluating their practical security. Finally, a suitable countermeasure is proposed and compared to the previously proposed countermeasures.

5. Teaching Activities

During this period Dr. Ghosh taught a group of undergraduate students VLSI systems design on FPGA platforms.

Supervision: As a post-doctoral fellow Dr. Ghosh has provided significant effort to guide the PhD student Mr. Amitabh Das at COSIC/ESAT, KU Leuven during this fellowship period. The research toward his PhD is related to secure design for testability. In this area the joint publications are mentioned before.

In the last summer, June – August, 2012 Dr. Ghosh has supervised Mr. Amit Kumar, a visiting researcher from Indian Institute of Technology Kharagpur, India. During Amit's visit at COSIC/ESAT, KU Leuven the implementation and security issues of a new Elliptic curve called Binary Huff curve have been studied. The vulnerability of unified binary Huff curve has been addressed and proposed a suitable countermeasure against Side-channel attacks (SCA). A crypto-processor has been designed for computing proposed SCA secure Huff curve algorithm which provides the best performance among all other existing unified elliptic curve processors. One paper has been submitted on this topic.

6. Research Collaborations

6.1 Collaboration with IIT Kharagpur

After joining the COSIC research group through this BELSPO post-doctoral fellowship, Dr. Ghosh has been instrumental in maintaining the research collaboration with IIT Kharagpur. The work published in Pairing 2012 (mentioned before) is a joint work with Prof. Dipanwita Roychowdhury from IIT Kharagpur, who was one of his PhD supervisors.

A joint workshop has been organized by Dr. Debdeep Mukhopadhyay, another one of his PhD Supervisors, and Prof. Ingrid Verbauwhede at IIT Kharagpur during March 2012. A team of three researchers had traveled from Leuven to Kharagpur to teach theory and practical classes in the workshop.

Another person Mr. Sujor Sinha Roy from IIT Kharagpur has joined COSIC as a pre-doctoral student on September 24, 2012. One other person, Ayan Mallik may also come during the coming summer as a visiting researcher; he is currently pursuing BTech at IIT Kharagpur.

6.2 Collaboration with Other Universities and Visits.

During this fellowship period Dr. Ghosh has attended "2nd Bar-Ilan Winter School on Cryptography" conducted by Bar-Ilan University at Tel Aviv, Israel during Feb 19-22, 2012. Main focus of the school was to provide an in depth coverage of lattices and their role in cryptographic constructions. In this school, he met several experts in this area of research and understood the technical advancement necessary for applying next generation public key cryptography in practice.

Dr. Ghosh has presented technical papers at two international conferences during this fellowship period. One is "Pairing 2012" which was conducted at Cologne, Germany during

May 16-18, 2012. The other one is "IEEE ASAP 2012" at Delft, The Netherlands during July 9-11, 2012.

Two collaborative researches have been initiated with ETH Zurich, Switzerland. One of which targets the implementation of a 128-bit secure pairing for low cost and low power embedded platforms. The other one aims at the practical Hardware Trojan detection on 130nm AES chip.

7. Acknowledgement

The fellowship has been acknowledged in all above publications by following way:

- Santosh Ghosh is a Postdoctoral Fellow at KU Leuven funded by the IAP Programme P6/26 BCRYPT of Belgian Science Policy (Belspo).

- This work was supported in part by the Research Council KU Leuven: GOA TENSE (GOA/11/007), by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy) and by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II.

References

[1] Y. K. Lee, L. Batina, K. Sakiyama, and I. Verbauwhede, "Elliptic Curve Based Security Processor for RFID," IEEE Transactions on Computers 57(11), 2008.
[2] J. Fan, L. Batina, and I. Verbauwhede, "Light-weight implementation options for curve-based cryptography: HECC is also ready for RFID," RISC 2009, 2009.
[3] P. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems". CRYPTO 1996.
[4] P. Kocher, J. Jaffe, B. Jun. "Differential Power Analysis". CRYPTO 1999.
[5] R.J. McEliece, "A public-key cryptosystem based on algebraic coding theory," JPL DSN Progress Report, pp. 114–116, 1978.
[6] H. Niederreiter, "Knapsack-Type Cryptosystems and Algebraic Coding Theory," Problems of Control and Information Theory 15, pp. 159–166, 1986.
[7] S. Ghosh, D. Roychowdhury, A. Das, "High Speed Cryptoprocessor for ηT Pairing on 128-bit Secure Supersingular Elliptic Curves over Characteristic Two Fields," CHES 2011. LNCS, vol. 6917, pp. 442–458. Springer, Heidelberg (2011).