PhD Thesis Position at CAIRN-IRISA Lannion

Title: Hardware Arithmetic Units and Crypto-Processor for Hyperelliptic Curves Cryptography

Funding: Project H-A-H (`http://h-a-h.inria.fr/`) supported by Labex CominLabs, Labex Lebesgue and Région Bretagne. The PhD student will be an employee of CNRS during the period.

Period: October 2014 to September 2017 (36 months, no extension will be granted)

Location: Lannion (22) in CAIRN team from IRISA laboratory

Advisors: Dr. Arnaud TISSERAND (HDR) and Dr. Nicolas VEYRAT-CHARVILLON

Doctoral School: MATISSE (PhD registration field: computer science)

Keywords: Public key cryptography, security, side channel attacks, arithmetic algorithms, representations of numbers, protections, countermeasures, hardware implementation, integrated circuits, FPGA

Collaboration: This thesis is part of the H-A-H (`http://h-a-h.inria.fr/`) **joint multidisciplinary project** between the CAIRN team from IRISA laboratory in **computer science** and **microelectronics**, and the GAR team from IRMAR laboratory in **mathematics**.

Context and Motivations

Efficient and robust public key cryptography (PKC) is of major importance for information security and privacy (e.g. generation of secret keys for symmetric cryptographic sessions and digital signatures).

Until recently, PKC in the industry was almost exclusively dominated by RSA. Over the past few years, curve based cryptography has gained enormous popularity. It has been recently shown that hyperelliptic curves provide the most efficient support for PKC. This is due to the fact that it allows to work on smaller base fields. As the complexity of the base field arithmetic is usually quadratic in its size, very interesting improvements can be expected. Currently, there are very few hardware implementations of hyperelliptic curves cryptography (HECC).

Hardware crypto-processors provide a very fast way for encrypting/signing messages. But hardware devices may leak some information (variations of the power consumption, computation delay, electromagnetic radiations, etc.) that can be exploited in side-channel attacks. Protection systems have to be adapted and deployed over the circuit according to the required security level.

The H-A-H project deals with both theoretical and hardware implementation aspects of efficient and secure hardware implementation of advanced hyperelliptic curve cryptography with a special focus at the arithmetic level(s).

PhD Objectives

- **State of Art Analysis:** The first objective is to analyze the previous relevant works, algorithms, implementations and attacks on HECC. Some new methods were recently successfully introduced and relaunched the interest of hyperelliptic curves, a second objective is then to understand them.
- **Efficient and Secure Arithmetic Units for HECC:** We will develop a library of efficient and secure arithmetic units (or accelerators) in hardware for advanced HECC. In this context efficiency means: high speed but low energy (and power consumption), silicon area and memory footprint.

The security will evaluated at two levels: selection of the cryptosystem parameters accordingly to the theoretical attacks protection, and protection against SCAs at various levels: computations algorithms, representation of numbers, architecture, circuit level counter-measures.

- **Hardware implementation of HECC crypto-processor:** Hardware implementations of HECC systems are very rare and the very few publicly available use very basic algorithms and do not consider protections aspects. We will reuse some parts of a crypto-processor developed at CAIRN-IRISA for elliptic curve cryptography, and its programming tools, to build a extended version with new HECC capabilities based on the proposed algorithmic and arithmetic solutions.
- **Performances/Cost/Energy Evaluation for Various Parameters:** We will propose accurate measurement methods to evaluate the trade-offs between performances (speed, internal code size, silicon cost and energy) and security (robustness against passive and active attacks). Some other parameters may be used such as the flexibility (possible implementation of various high-level primitives or not).
- **Security against Side-Channel Attacks Evaluation:** One of our goal is to theoretically study and practically measure the impact of various protection schemes on the performances (speed, silicon cost and power consumption). The originality of the work lies in new mathematical and arithmetic approaches for optimizing and protecting cryptographic building blocks. We will perform an intensive security evaluation against physical attacks (SCAs types) using the attack equipment available at CAIRN-IRISA.

The PhD student will participate in the H-A-H project activities: publications, presentations, internal meetings, organization of events. Regular internal project meetings will be organized (one time in Lannion, one time in Rennes). The PhD student will be in charge of the preparation and organization of the meetings with the PhD student at IRMAR laboratory.

As a member of the CAIRN-IRISA team, the PhD student will also have access to the activities of the team (e.g. internal seminars, security seminars).

Application Process

Important: applications must respect this process (non-conform applications will not be considered).

The applicant must hold (at most in July 2014) a **Master degree** in computer science, or in digital microelectronics, or in mathematics. Good skills are mandatory in at least 2 of the 3 following topics: 1) digital circuit and FPGA design, 2) applied cryptography, 3) computer arithmetic.

Email to **Arnaud TISSERAND**[1] the **complete** application file including (only PDF documents):

- Clear indication to the PhD thesis title (see above)
- Complete name, permanent coordinates and CV of the applicant
- Detailed motivation letter of the applicant with the skills corresponding to **this** PhD thesis
- Complete description of the applicant relevant Degree (list of followed classes/courses, grades and ranking if possible)
- Complete name and coordinates of the responsible of the Degree
- If possible recommendation letter(s) from previous advisor(s) (e.g. Master Thesis) or Degree responsible (with clear and complete name and coordinates of the author(s) of the letter who may be contacted)

Applications will be analyzed. For relevant applications, a visio-conference meeting may be organized to verify the skills and motivations of the applicant.

[1] mailto:arnaud.tisserand@irisa.fr