PhD Position
Symmetric primitives of low multiplicative complexity, side-channel attacks and masking

SECTOR: Higher Education Institution

LOCATION: France, Grenoble

RESEARCHER PROFILE:
☐ First stage researcher,

INSTITUTION: Univ. Grenoble Alpes, University of Innovation

One of the major research-intensive French universities, Univ. Grenoble Alpes enjoys an international reputation in many scientific fields, as confirmed by international rankings. It benefits from the implementation of major European instruments (ESRF, ILL, EMBL, IRAM, EMFL*). The vibrant ecosystem, grounded on a close interaction between research, education and companies, has earned Grenoble to be ranked as the 5th most innovative city in the world. Surrounded by mountains, the campus benefits from a natural environment and a high quality of life and work environment. With 7000 foreign students and the annual visit of more than 8000 researchers from all over the world, Univ. Grenoble Alps is an internationally engaged university.

A personalized Welcome Center for international students, PhDs and researchers facilitates your arrival and installation.

In 2016, Univ. Grenoble Alpes was labeled “Initiative of Excellence”. This label aims at the emergence of around ten French world class research universities. By joining Univ. Grenoble Alpes, you have the opportunity to conduct world-class research, and to contribute to the social and economic challenges of the 21st century ("sustainable planet and society", "health, well-being and technology", "understanding and supporting innovation: culture, technology, organizations", "Digital technology").

* ESRF (European Synchrotron Radiation Facility), ILL (Institut Laue-Langevin), IRAM (International Institute for Radio Astronomy), EMBL (European Molecular Biology Laboratory), EMFL (European Magnetic Field Laboratory)

Key figures:
- + 50,000 students including 7,000 international students
- 3,700 PhD students, 45% international
- 5,500 faculty members
- 180 different nationalities
- 1st city in France where it feels good to study and 5th city where it feels good to work
- ISSO: International Students & Scholars Office affiliated to EURAXESS
SUBJECT TITLE: Symmetric primitives of low multiplicative complexity, side-channel attacks and masking

RESEARCH FIELD: Computer Science, Mathematics

SCIENTIFIC DEPARTMENT (LABORATORY'S NAME): Laboratoire Jean Kuntzmann

DOCTORAL SCHOOL'S: Mathématiques, Sciences et Technologies de l'Information, Informatique

SUPERVISOR'S NAME: Jean-Guillaume Dumas

SUBJECT DESCRIPTION:

A first objective of this thesis will be to design, analyze and implement (both in low-level software and hardware) block ciphers with low multiplicative complexity, that is, algorithms whose implementation requires few finite field multiplications (e.g. few AND gates for an implementation over GF(2)).

Such primitives play an important role in the security of embedded systems, as the overhead in protecting them against side-channel attacks such as DPA is relatively low. This is especially true when the deployed countermeasures such as masking are used at very high order, e.g. 32.

So far, quite a few algorithms have been proposed in this setting, such as Zorro, Fantomas, Mysterion, or LowMC. However, some (e.g. Zorro) have now been broken, and others (e.g. LowMC) base their security on statistical arguments.

In this thesis, we wish to study new constructions based on algebraic geometry codes. A first approach consists in exploiting codes of large dimension and high minimum distance built over small fields, such as GF(16). This would allow defining a block cipher with a classical SPN structure requiring few rounds, and globally few accesses to a 4-bit S-box of low multiplicative complexity. An important challenge will be to find efficient implementations of the relevant matrix-vector multiplication, where the matrix is dense and of large dimension, but possibly possessing some structure. Another challenge will be to couple the resulting round function with a minimal key derivation algorithm, while avoiding the typical weaknesses of this kind of approach, such as invariant subspace attacks.

A second approach will be to study alternative instantiations of the paradigm followed by the LowMC ciphers. Namely, we wish to replace the randomly drawn diffusion matrices by ones coming from binary Goppa codes. This would allow to get rid of the statistical argument currently used to analyze the security of LowMC. Even then, the peculiar structure of the incomplete round function of this cipher family would still present an interesting challenge in finding strong wide-trail arguments.

Another part of this thesis will focus more closely on masking algorithms themselves, especially ones of low complexity. Some recent work introduced algorithms with remarkably low multiplicative or randomness complexity. Yet these require complex matrix conditions to be safely instantiated, with a side effect that the cardinality of the field over which the masking scheme is built increases sharply with the masking order. An interesting question is whether this phenomenon is intrinsic to the approach, or if a less costly alternative could be designed. A related challenge would be to build a scheme that would be easier to instantiate by relaxing its associated matrix conditions.

Finally, cryptography as a whole being a very active field, a major part of the thesis will focus on studying newly proposed block ciphers, masking schemes, primitive implementations, with the view of analyzing (and possibly attacking) them, and more generally of interacting with the scientific community.

Selected references:
Student profile:
The candidate should have a strong background in mathematics and/or computer science, and should ideally have
followed at least one course in cryptography or coding theory. Good programming skills in a low-level programming
language such as C are expected, while some knowledge of assembly (x86, ARM) would be a plus.

ELIGIBILITY CRITERIA
Applicants must hold a Master's degree (or be about to earn one) or have a university degree equivalent to a
European Master's (5-year duration).

Applicants will have to send an application letter in English and attach:
- Their last diploma
- Their CV
- A short presentation of their scientific project (2 to 3 pages max)
- Letters of recommendation are welcome.

Address to send their application: cyberalps-pilotage@univ-grenoble-alpes.fr, jean-
guillaume.dumas@univ-grenoble-alpes.fr, pierre.karpman@univ-grenoble-alpes.fr,
paolo.maistri@imag.fr.

SELECTION PROCESS
Application deadline: 2018-06-22 at 17:00 (CEST)
Applications will be evaluated through a three-step process:

1. Eligibility check of applications in 2018-06-25
2. 1st round of selection: the applications will be evaluated by a Review Board on June 29, 2018. Results will be
given on July 2, 2018.
3. 2nd round of selection: shortlisted candidates will be invited for an interview session in Grenoble on July 6,
   2018. (if necessary)

TYPE of CONTRACT: temporary-3 years of doctoral contract
JOB STATUS: Full time
HOURS PER WEEK: 35
OFFER STARTING DATE: 2018-10-01
APPLICATION DEADLINE: 2018-06-22
Salary: between 1768.55 € and 2100 € brut per month (depending on complementary activity or not)