University Pierre et Marie Curie (UPMC)  
France

Acceleration of integer factorization by the Elliptic Curve Method (ECM) algorithm on FPGA

- **Deadline:** April 30, 2018  
- **Career levels:** Assistant Researcher, PostDoc  
- **Keywords:** Computer architecture, Design Space Exploration, Safety and Security

Context: ECM is an integer factorization method based on elliptic curves whose complexity depends only on the smallest prime factor of the computed integer. This method allows to find factors up to a hundred bits. In addition to its own interest, it is also used as a sub-method for larger numbers (QS and NFS). FPGAs being good hardware accelerators for algorithms requiring a high computing power, an FPGA hardware implementation of the ECM could be a step forward for factorization methods.

Description: The purpose of this study is to determine which are the most efficient implementations of the ECM algorithm on FPGA in order to quickly select composite numbers. It will involve synthesis and simulation on the latest generations of FPGA available from the main vendors (Xilinx, Altera). In this context, we envisage the following lines of research:

- Exploration of feasible hardware implementations of basic arithmetic blocks, in the environment developed by LIP6. Exploration of feasible hardware implementations of arithmetic operations in any finite field using, for example, Montgomery algorithms, cellular automata, etc. Choice of curves (Edwards, Montgomery, etc.) whose computational complexity of the group law is weaker, without excluding other axes including more theoretical aspects. The implementation performance will be evaluated according to the number of points or curves calculated per time unit and will be compared to an already available CPU reference implementation, such as GMP-ECM.

Required skills: The candidate must have obtained a PhD in the field of hardware architectures possibly in security. He should have the mathematical concepts related to cryptography (algebra, finite fields etc.) as well as good programming skills. An experience of implementation on FPGA is highly recommended.

Terms: The offer corresponds to a one-year fixed-term contract that may be renewed if the project is extended and is to be filled immediately. The salary is about 1900 € net per month to be modulated according to the experience of the candidate. The work will take place in the premises of LIP6, 4 place Jussieu, Paris 5th.

Contact: Roselyne.Chotin-Avot@lip6.fr, +33 (0)1.44.27.65.28