2018-00736 - Hardware security analysis and protection of post-quantum schemes (F/H)

Level of qualifications required: Graduate degree or equivalent
Function: PhD Position

Context
About Inria and the research team

Inria, the French National Institute for computer science and applied mathematics, promotes “scientific excellence for technology transfer and society”. Graduates from the world's top universities, Inria's 2,700 employees rise to the challenges of digital sciences. With its open, agile model, Inria is able to explore original approaches with its partners in industry and academia and provide an efficient response to the multidisciplinary and application challenges of the digital transformation. Inria is the source of many innovations that add value and create jobs.

The TAMIS team (https://team.inria.fr/tamis) at Inria Rennes - Bretagne Atlantique is among the largest security teams at Inria, including competences from hardware security to cryptography, and from vulnerability detection to malware analysis.

Assignment
Context

In recent years, there has been a substantial amount of research on quantum computers, which if built on a large-scale, would be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. Post-quantum cryptography (also called quantum-resistant cryptography) is considered to be the solution of this issue. It refers to all cryptosystems that are allegedly secure against both quantum and classical computers, and that can interoperate with existing communications protocols and networks.

Recently, NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers. NIST expects to perform multiple rounds of evaluation, over a period of three to five years. The goal of this process is to select a number of acceptable candidate cryptosystems for standardization.

At present, several post-quantum cryptosystems have been proposed:
- lattice-based,
- code-based,
- multivariate,
- hash-based signatures,
- and others.

However, for most of these proposals, further research is needed in order to gain more confidence in their security and to improve their performance.

Assignment

The selected student is expected to first perform a thorough hardware security analysis of proposed post-quantum secure schemes. This security analysis should be first focused on side-channel security in combination with algebraic attacks and may be extended to fault analysis and further hardware security threats.
Second, the student should propose suitable countermeasures for the found security threats and design efficient software implementations.

**Main activities**

Main activities
- research
- publishing in first rank conferences / journals
- presenting at workshops

**Skills**

Skills and profile
- Master degree in Computer Science or Computer Engineering is required.
- Programming skills.
- Knowledge of cryptography/ hardware Security (post-quantum security is a plus)
- Knowledge of side-channel analysis is a plus
- Fluent English required, both oral and written.
- Motivated to drive top-quality research

**Benefits package**

- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- Flexible working hours
- Sports facilities