Algorithmic aspects of coding and cryptology

Contract type: Public service fixed-term contract
Level of qualifications required: PhD or equivalent
Fonction: Post-Doctoral Research Visit

Assignment
Research on cryptology or coding

Main activities
The research work within the project-team is mostly devoted to the design and analysis of cryptographic algorithms, in the classical or in the quantum setting. It is especially motivated by the fact that the current situation of cryptography is rather fragile: for instance, the security of the available primitives has been so much threatened by the recent progress in cryptanalysis that no stream ciphers and only a few hash functions are nowadays considered to be secure. The most widely used public-key cryptosystems are also threatened by the possible invention of a large quantum computer.

Research topics:
Symmetric cryptology: We focus on stream ciphers, block ciphers and hash functions. Our work considers all aspects of the field, from practical (new attacks, concrete specifications of new systems) to more theoretical ones (study of the algebraic structure of underlying mathematical objects, definition of optimal objects).

Code-based cryptography: Cryptographic primitives which exploit some problems coming from coding theory provide a good alternative to the commonly used systems based on number theory. They are usually named post-quantum cryptosystems since they would not become obsolete with the coming up of the quantum computer. We investigate the security of these systems, their practical implementation and the design of fast cryptographic primitives based on codes.

Reverse engineering of communication systems: When a communication is eavesdropped, some raw data, not necessarily encrypted, are observed out of a noisy channel. Then, to access the information, the whole communication system has first to be disassembled and every constituent reconstructed. We study this reverse engineering problem. Most notably, we investigate the problem of recovering the specifications of the involved scramblers and error-correcting codes.

Quantum information theory: The main obstacle towards the development of quantum computing is decoherence, a consequence of the interaction of the computer with a noisy environment. We investigate approaches to quantum error-correction as a way to fight against this effect, and we study more
particularly some families of quantum error-correcting codes which generalise the best classical codes available today. Our research also covers quantum cryptography where we study the security of efficient protocols for key distribution, in collaboration with experimental groups. More generally, we investigate how quantum theory severely constrains the action of honest and malicious parties in cryptographic scenarios.

Skills
Expertise in one of our research areas: symmetric cryptology, code-based asymmetric cryptography, quantum algorithms, coding theory, quantum cryptography, discrete mathematics

Benefits package
- Subsidised catering service
- Partially-reimbursed public transport

Remuneration
- Location: Paris 12ème
- Gross Salary per month: 2 653€ brut/mensuel

Security and defense procedure:
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).

Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.