Framework for reasoning about cryptographic protocols with randomization

**Laboratory, institution and university** LSV, ENS Cachan and LORIA, Nancy universités The internship will be located at Nancy or at ENS Cachan depending on the choice of the candidate.

**Team or project of the Lab** Team SecSI at LSV and team Cassis at Loria

**Name and email address of the advisor** Rohit Chadha, chadha@lsv.ens-cachan.fr and Steve Kremer, Steve.Kremer@inria.fr.

**Indemnisation** The internship is supported by the European grant ProSecure (ERC Starting Grant).

**Context.** Cryptographic protocols are distributed programs which use cryptographic primitives to secure communication over untrusted networks (such as the Internet). They are designed to achieve security properties such as confidentiality, authentication or anonymity. Due to the complexity of cryptographic primitives, the inherent concurrency and the untrusted nature of networks, their design has often proved to be error-prone. In order to tackle this problem, formal methods have been designed to detect errors in cryptographic protocols and proved very successful.

One successful approach is to model the cryptographic protocols in process calculi, and prove that the protocols behave like ideal protocols. Process calculi are ‘programming languages’ for distributed programs; and have a **non-deterministic construct** to model concurrency. For cryptographic protocols, applied pi-calculus [AF01] has been designed to take into account cryptographic operations. The cryptographic primitives in this framework are modeled as equational theories. While applied pi-calculus has been very successful, it cannot reason about cryptographic protocols (such as anonymity protocols and oblivious transfers) that explicitly use randomization techniques to achieve its goal. In order to achieve this, probabilistic applied pi-calculus has been proposed [GLPT07] where a probabilistic operator has been added to handle randomization. In order to give a semantics of the probabilistic applied pi-calculus, nondeterministic choices have to be resolved in presence of probabilistic choices. Usually, nondeterministic choices in probabilistic systems is resolved in the presence of schedulers. However, for security, the schedulers have to be restricted [GD07, CP10]. However, the framework in [GLPT07] suffers in that this restriction is no placed on the scheduler.

**Objectives of the internship.** The objective of the internship is to develop a framework to reason about cryptographic protocols that employ
randomization as a key technique to achieve its security goals. The framework will take probabilistic applied pi-calculus as the starting version and restrict the set of schedulers to the correct set. While this restriction has been studied in abstract models including process calculi [GD07, CP10], it has never been studied within the context of cryptographic process calculi. This internship will develop this framework, resulting in proof methods for cryptographic protocols with randomization. We expect the framework to be able to reason about protocols such as oblivious transfers and dining cryptographic protocols.

**Expected skills.** We are looking for candidates with good skills in Foundations of Computer Science (logic, process calculus, . . . ) and probabilities. Some knowledge in security is an asset but is not mandatory. The candidate will assimilate this knowledge during the internship.

**References**


