Types for complexity analysis, with applications to security

proposed by Patrick Baillot (LIP, ENS Lyon)

Contact:
patrick.baillot@ens-lyon.fr
http://perso.ens-lyon.fr/patrick.baillot/

Location: LIP, ENS Lyon, Équipe Plume (Preuves et langages),

Description:
This internship deals with the problem of automatically analysing the time complexity of higher-order programs. A particular motivation for that is the analysis of cryptographic schemes. Indeed some tools like EasyCrypt [BGHB11, eas] allow to analyse formally a cryptographic scheme, to establish that it is secure, assuming that a certain computational problem is hard. However such tools currently do not handle in a satisfactory way the complexity analysis of the constructed adversaries. There is thus a need to develop analysis techniques that would fit well in this approach.

The recent work [BBDL15] tackles this problem for a lambda-calculus with references and primitive recursion. This language is expressive enough to represent some non-trivial cryptographic reductions. This work performs complexity analysis by means of a dedicated rich type system, following the methodology introduced by [DLG11]. Roughly speaking the types are parameterized and in this way carry information about the sizes of the values handled during the computation. Then from a type derivation one can obtain a complexity bound on the runtime of the program. The techniques underlying this approach come from linear logic and type systems theory.

In this internship we propose to bring this research line further, in one of the following possible directions:
- Enhancement of the programming language: it is important to have an expressive programming language, in order to be able to analyse interesting cryptographic reductions. In this direction one could investigate to which extent the analysis can be extended to a programming language with more programming features (eg pattern matching) or data-types (eg trees). This will be guided by a study of motivating examples of reductions from the cryptography literature.
- Type system: currently the analysis provides types with an (expected) accurate information on the size of values, but which in practice might be difficult to understand and to use. Concretely the types are parameterized by first-order functions which are themselves defined by mutual equations. In this direction we propose to explore methods to overapproximate these types, in order to gain in readability/usability even if loosing on accuracy. For instance one could consider types parameterized by a given algebra of first-order functions (for instance polynomials).

The prerequisites for this internship are a good knowledge of lambda-calculus and type systems. Some notions of cryptography are also useful, but can be acquired by reading some references, if needed.

This work fits in a collaboration between Patrick Baillot (ENS Lyon), Gilles Barthe (Madrid) and Ugo Dal Lago (Bologna, Italy). It is also a topic of the ANR project ELICA.

Références


