Security and Privacy by Typing in Cryptographic Systems

Matteo Maffei

Abstract

The security of modern distributed systems is an important and complex challenge, which has attracted the interest of a growing research community over the last decade. The cryptographic protocols used to securely transmit data over an untrusted network, and even more so their software implementations, are extraordinarily difficult to design and to prove secure, as witnessed by the continuously growing list of discovered vulnerabilities. The complexity of cryptographic systems stem from several factors and has significantly increased over the years. First of all, while early academic protocols mostly consisted of simple combinations of signature and encryption schemes, modern ones rely on much more sophisticated, and arguably fascinating, cryptographic primitives, such as zero-knowledge proofs and secure multiparty computations. Secondly, the security and privacy properties required by modern applications go well beyond the well-understood secrecy and authenticity properties, covering, e.g., indistinguishability relations and differential privacy.

Language-based techniques, and type systems in particular, lived up to the challenge, constituting a solid and expressive framework for the verification and design of cryptographic systems. While early academic cryptographic protocols required relatively simple type and effect systems, modern cryptography called for more powerful techniques, such as refinement types, union and intersection types, linear types, and relational refinements.

The goal of this talk is to guide the audience through the literature on type theory for cryptographic applications, giving a consolidated view of the research development in this field and establishing bridges with various subdisciplines of interest to the logic, semantics, and verification community (e.g., type theory, SMT solving, linear logic, proof-carrying authorization, relational verification, and concurrent programming), with the final goal of fostering cross-fertilizing research ideas.