Cryptographic Types for Homomorphic Encryptions

Cédric Fournet
Microsoft Research

Jérémy Planul
MSR–INRIA Joint Centre

Tamara Rezk
INRIA Sophia Antipolis-Méditerranée

April 13, 2011

Abstract

We develop a flexible information-flow type system for a variety of encryptions primitives, reflecting their diverse functional and security features. We provide a uniform framework for understanding their properties, and for automatically checking their usage in cryptographic programs and compilers.

Depending on the relative security levels of keys, plaintexts, and ciphertexts, we propose different typing rules, relying on standard cryptographic assumptions such as CPA or CCA2, and enabling the selective re-use of keys for protecting different types of payloads. We also formally support useful additional features, such as re-encryption and homomorphic operations.

Our main security result is that any well-typed program that uses a mix of these encryption primitives is computationally non-interferent against any active probabilistic polynomial-time adversary, both as regards confidentiality and integrity.

We illustrate our approach on several classic schemes, such as ElGamal, and Paillier encryption. We develop two larger applications of cryptographic verification by typing: (1) private search on data streams; and (2) the bootstrapping construction of Gentry's fully-homomorphic encryption. We also report on a prototype typechecker used for verifying our sample programs.