Cryptographic Agents: Towards a Unified Theory of Computing on Encrypted Data[1]

Shashank Agrawal
University of Illinois, Urbana-Champaign
Shweta Agrawal
Indian Institute of Technology, Delhi
Manoj Prabhakaran
University of Illinois, Urbana-Champaign

Abstract

We provide a new framework of *cryptographic agents* that unifies various modern "cryptographic objects" — identity-based encryption, fully-homomorphic encryption, functional encryption, and various forms of obfuscation – similar to how the Universal Composition framework unifies various multi-party computation tasks like commitment, coin-tossing and zero-knowledge proofs. These cryptographic objects can all be cleanly modeled as "*schemata*" in our framework. Highlights of our framework include the following:

- We use a new *indistinguishability preserving* (IND-PRE) definition of security that interpolates indistinguishability and simulation style definitions, which (often) sidesteps the known impossibilities for the latter. IND-PRE-security is parameterized by the choice of the "test" family, such that by choosing different test families, one can obtain different levels of security for the same primitive (including various standard definitions in the literature).
- We present a notion of *reduction* from one schema to another and a powerful *composition theorem* with respect to IND-PRE security. We show that obfuscation is a "complete" schema under this notion, under standard cryptographic assumptions. We also provide a stricter notion of reduction that composes even when security is only with respect to certain restricted test families of importance.
- Last but not the least, our framework can be used to model abstractions like the generic group model and the random oracle model, letting one translate a general class of constructions in these heuristic models to constructions based on *standard model assumptions.*

We also illustrate how our framework can be applied to specific primitives like obfuscation and functional encryption. We relate our definitions to existing definitions and also give new constructions and reductions between different primitives.

[1] To appear in Eurocrypt 2015.