Abstraction in Cryptography

Ueli Maurer

Department of Computer Science
ETH Zurich
CH-8092 Zurich, Switzerland,
maurer@inf.ethz.ch

Abstract. Abstraction means to eliminate irrelevant details from consideration, thereby focusing only on the relevant aspects of a problem or context. Abstraction is of paramount importance in most scientific fields, especially in computer science and mathematics. The purpose of abstraction is to provide, at the same time, simpler definitions, higher generality of results, simpler proofs, improved elegance, and often better didactic suitability.

Abstraction can be a gradual process and need not be unique, but in many contexts, the highest achievable level of abstraction, once identified, appears natural and stable. For example, the abstract and natural concepts of a group or a field in algebra capture exactly what is required to prove many important results.

In the spirit of algebraic abstraction, we advocate the definition and use of higher levels of abstraction in cryptography, with the goal of identifying the highest possible level at which a definition or theorem should be stated and proved. Some questions one can ask are: What are abstractions of a system, a game, indistinguishability, a hybrid argument, a reduction, indifferentiability, or of (universal) composability? What are abstractions of efficient and negligible, and at which level of abstraction can computational and information-theoretic models be unified? And, of course: Can the abstract viewpoint lead to new concepts and results that are perhaps otherwise missed?