Constructive Cryptography – A Primer

Ueli Maurer

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

Abstract. A central paradigm in any constructive discipline is the decomposition of a complex system into simpler component systems or modules, which each may consist of yet simpler modules, and so on. This paradigm, sometimes called step-wise refinement, is useful only if the composition of modules is well-defined and preserves the relevant properties of the modules. For example, in software design, the composition operation must preserve correctness of the modules, i.e., a system consisting of correct modules must itself be correct.

In cryptography, the modules are cryptographic schemes (e.g. an encryption scheme or a message authentication code, MAC) or protocols (e.g. a zero-knowledge proof), and the composition must preserve the security of the modules. Surprisingly, for the traditional, game-based cryptographic security definitions, this composition property is unclear or at best highly non-trivial. Recall that a game-based security definition states that an adversary with certain capabilities (e.g. access to a MAC oracle) cannot win a certain game (e.g. forge a MAC) with non-negligible probability. One consequence of the lack of composability is that cryptographic protocols are often complex and lack modularity.

We propose *constructive cryptography* as a new paradigm, where the security definition of cryptographic schemes is radically different (though in many cases can be proved to be equivalent). For example, a message authentication scheme is defined to be secure if it *constructs* an authenticated communication channel from an insecure communication channel and a secret key, for a well-defined, simulation-based notion of "construct" and for well-defined definitions of an insecure and an authenticated channel. Similarly, a symmetric encryption scheme is defined to be secure if it constructs a secure communication channel from an authenticated communication channel and a secret key. The general composition property of this theory implies that the combination of a secure MAC and secure encryption scheme constructs a secure channel from an insecure channel and two secret keys (which can be constructed from a single secret key using a pseudo-random generator).

The security of public-key cryptosystems and digital signature schemes can be seen similarly in the constructive cryptography paradigm. In addition to making composition clear, the constructive cryptography approach has many other benefits. For example, it allows to investigate the intrinsic limitations of cryptography.

R. Sion (Ed.): FC 2010, LNCS 6052, p. 1, 2010.