Cryptology ePrint Archive: Report 2013/025

The IITM Model: a Simple and Expressive Model for Universal Composability

Ralf Kuesters and Max Tuengerthal

Abstract: The universal composability paradigm allows for the modular design and analysis of cryptographic protocols. It has been widely and successfully used in cryptography. However, devising a coherent yet simple and expressive model for universal composability is, as the history of such models shows, highly non-trivial. For example, several partly severe problems have been pointed out in the literature for the UC model.

In this work, we propose a coherent model for universal composability, called the IITM model (``Inexhaustible Interactive Turing Machine''). A main feature of the model is that it is stated without a priori fixing irrelevant details, such as a specific way of addressing of machines by session and party identifiers, a specific modeling of corruption, or a specific protocol hierarchy. In addition, we employ a very general notion of runtime. All reasonable protocols and ideal functionalities should be expressible based on this notion in a direct and natural way, and without tweaks, such as (artificial) padding of messages or (artificially) adding extra messages.

Not least because of these features, the model is simple and expressive. Also the general results that we prove, such as composition theorems, hold independently of how such details are fixed for concrete applications.

Being inspired by other models for universal composability, in particular the UC model and because of the flexibility and expressivity of the IITM model, conceptually, results formulated in these models directly carry over to the IITM model.

Category / Keywords: foundations / cryptographic protocols, universal composability, modular security analysis

Date: received 18 Jan 2013

Contact author: kuesters at uni-trier de