Universal Composability: A Comparison of Different Models

Daniel Rausch
University of Stuttgart

29th Crypto Day, 6/7 September 2018

Universal composability models enable modular security proofs: one can first analyze a small part of a protocol in isolation, prove its security, and then re-use this result in the context of the whole protocol. Furthermore, security guarantees obtained in a universal composability model are particularly strong as they hold true in every (polynomial time) environment, where arbitrary other protocols can run concurrently and where some parties might be corrupted.

Nowadays, universally composable security proofs are mostly based on the so-called UC model [2] proposed by Canetti. This model, however, is quite complex and includes several technical details that protocol designers have to take care of. Even worse, some of the core theorems do not formally hold true. Thus, protocol designers resort to doing their proofs based on an abstract "idea" of how they think the UC model should work. Clearly, this is unsatisfying as it remains unclear whether security guarantees and composability properties still hold true for such proofs.

Ideally, one would like to have a formally sound and expressive model that, at the same time, is easy to use without being cluttered by technical details. This would allow protocol designers to obtain valid security results with composability guarantees by basing their proofs on that model.

Fortunately, such a model exists, namely the so-called IITM model (with responsive environments) [4, 1]. In this talk, we discuss this model and compare it to other prominent models for universal composability, namely the UC model and GNUC model [3].

References

[1] J. Camenisch, R. R. Enderlein, S. Krenn, R. Küsters, and D. Rausch. Universal Composition with Responsive Environments. In *Advances in Cryptology - ASIACRYPT 2016*.

[2] R. Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. Technical Report 2000/067, Cryptology ePrint Archive, 2000. Available at `http://eprint.iacr.org/2000/067`.

[3] D. Hofheinz and V. Shoup. GNUC: A New Universal Composability Framework. *J. Cryptology*, 28(3):423–508, 2015.

[4] R. Küsters and M. Tuengerthal. The IITM Model: a Simple and Expressive Model for Universal Composability. Technical Report 2013/025, Cryptology ePrint Archive, 2013. Available at `http://eprint.iacr.org/2013/025`.

crypto day matters 29 (2018)
Beiträge vom 29. Krypto-Tag, 06.-07.09.2018, Bosch, Renningen.
doi:10.18420/cdm-2018-29-23