Cryptology ePrint Archive: Report 2013/062

Symbolic Universal Composability

Florian Böhl and Dominique Unruh

Abstract: We introduce a variant of the Universal Composability framework (UC; Canetti, FOCS 2001) that uses symbolic cryptography. Two salient properties of the UC framework are secure composition and the possibility of easily defining security by giving an ideal functionality as specification. These advantages are now also available in a symbolic modeling of cryptography, allowing for a modular analysis of complex protocols.

We furthermore introduce a new technique for modular design of protocols that uses UC but avoids the need for powerful cryptographic primitives that often comes with UC protocols; this "virtual primitives" approach is unique to the symbolic setting and has no counterpart in the original computational UC framework.

Category / Keywords: universal composability, symbolic cryptography, virtual primitives

Date: received 6 Feb 2013, last revised 6 Feb 2013

Contact author: florian boehl at kit edu