Pioneer Journal of Computer Science and Engineering Technology

Volume 6, Issues 1&2, Pages 19-39 (September & December 2013)

ISSN: 2231-184X

PROVABLY SECURE ON-DEMAND ROUTING PROTOCOLS

István Vajda

Received July 16, 2013

Abstract

We present techniques for proving the security of on-demand routing protocols in the sense of secure emulation of an ideal process. We give the first security proof for an on-demand routing protocol. The proof is given in the Backes-Pfitzmann-Waidner's [M. Backes, B. Pfitzmann and M. Waidner, A universally composable cryptographic library. IACR Cryptology ePrint Archive, Report 2003/015, http://eprint.iacr.org/, January 2003; M. Backes and B. Pfitzmann, A General Composition Theorem for Secure Reactive Systems, Theory of Cryptograpy Conference (TCC 2004), LNCS 2951 (2004), 336-354 and B. Pfitzmann and M. Waidner, A model for asynchronous reactive systems and its application to secure message transmission, In Proc. 22nd IEEE Symposium on Security and Privacy (2001), 184-200] proof framework as well as we show the corresponding steps of assessment also in Canetti's Universal Composability (UC) [R. Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols, Cryptology ePrint Archive: Report 2000/067] proof framework, providing the first publication working in both frameworks in parallel.

Keywords and phrases: provable security, composable cryptographic library, universal composability, on-demand routing protocols.