Cryptology ePrint Archive: Report 2011/682

UC framework for anonymous communication

István Vajda

Abstract: In this research report we present an UC framework for the general task of anonymous communication. Definition of the ideal and the real models are carried out in the BPW (Backes-Pfitzmann-Waidner) formalism. It is shown how this approach relates to and extends earlier proposals [10],[15]. We consider also the adaptive adversary. An example is given for a wireless application.

Category / Keywords: cryptographic protocols / anonymity, cryptanalysis

Date: received 16 Dec 2011

Contact author: vajda at hit bme hu