# Cryptology ePrint Archive: Report 2011/335

**New look at impossibility result on Dolev-Yao models with hashes**

*István Vajda*

**Abstract:** Backes, Pfitzmann and Waidner showed in [7] that for protocols with hashes Dolev-Yao style models do not have cryptographically sound realization in the sense of BRSIM/UC in the standard model of cryptography. They proved that random oracle model provides a cryptographically sound realization. Canetti [9] introduced the notion of oracle hashing “towards realizing random oracles”. Based on these two approaches, we propose a random hash primitive, which already makes possible cryptographically sound realization in the sense of BRSIM/UC in the standard model of cryptography.

**Category / Keywords:** cryptographic protocols / cryptanalysis, hash functions

**Date:** received 20 Jun 2011

**Contact author:** vajda at hit bme hu