Cryptology ePrint Archive: Report 2011/564

Private-key Symbolic Encryption

N. Ahmed and C.D. Jensen and E. Zenner

Abstract: Symbolic encryption, in the style of Dolev-Yao models, is ubiquitous in formal security analysis aiming at the automated verification of network protocols. The naive use of symbolic encryption, however, may unnecessarily require an expensive construction: an arbitrary-length encryption scheme that is private and non-malleable in an adaptive CCA-CPA setting. Most of the time, such assumptions remain hidden and rather symbolic encryption is instantiated with a seemingly ``good'' cryptographic encryption, such as AES in the CBC configuration. As an illustration of this problem, we first report new attacks on ECB and CBC based implementations of the well-known Needham-Schroeder and Denning-Sacco protocols. We then present a few symbolic encryption schemes along with their cryptographic semantics, and prove the hierarchical relations between the proposed schemes from both cryptographic and formal perspectives. These symbolic schemes can be seamlessly used in many existing formal security models.

Category / Keywords: Symbolic Encryption, Hidden Assumptions, Formal Security Model

Date: received 18 Oct 2011, last revised 18 Oct 2011

Contact author: naah at imm dtu dk