Computational Soundness of Passively Secure Encryption in Presence of Active Adversaries

Sebastian Meiser

April 8, 2011

We investigate the impact on computational soundness when using passively secure encryption (IND-CPA) instead of actively secure encryption (IND-CCA2) in a scenario where active attacks are possible. Merely requiring an encryption scheme to be IND-CPA instead of being IND-CCA2 allows for using more efficient constructions.

Our main contribution is to show computational soundness of a Dolev-Yao model with public key encryption schemes only requiring IND-CPA secure encryption. This is achieved by adding the protocol assumption of *garbage free decryption*, stating that no ciphertext is decrypted that originates in the adversary.

Building on prior results (the CoSP framework by M.Backes, D.Hofheinz and D.Unruh), we show computational soundness of the applied π-calculus with public key encryptions and signatures. Moreover we show that we can transform every π-protocol P into a π-protocol P' such that the following property holds: If there is no trace in P' that raises the special event Bad, P has garbage free decryption. Finally, using this transformation, we show how to automatically check our new condition by using ProVerif.