Reyhane Falanji – Linköping University

Title: Provable Entity Accountability for Protocols with Modifiable Signed Messages

Abstract: In this study, we focus on formal analysis of protocols that utilise chameleon signatures. These protocols allow a modifier to modify a signed data, while keeping the same signature valid on the new data. Even though chameleon signatures provide unforgeability, non-repudiation and non-frameability for the signer on the signature, it is not trivial whether the same properties hold for protocols that rely on chameleon signatures. Moreover, chameleon signatures provide no guarantee for another entity that is involved in the process (i.e., the modifier). In this paper, we provide definitions of the mentioned properties for symbolic verification, and formally verify the mentioned properties for both parties of a protocol that relies on chameleon signatures.