Cryptology ePrint Archive: Report 2011/621

Adaptive Security of Concurrent Non-Malleable Zero-Knowledge

Zhenfu Cao, Zongyang Zhang , Yunlei Zhao

Abstract: A zero-knowledge protocol allows a prover to convince a verifier the correctness of a statement without disclosing any other information to the verifier. It is a basic tool and widely used in many other cryptographic applications. However, when stand-alone zero-knowledge protocols are used in complex environments, e.g., the Internet, the basic properties may not be sufficient. This is why researchers considered security of zero-knowledge protocols under concurrent composition and man-in-the-middle attacks. Moreover, it is more likely that an adversary might break computers that run the protocol and get internal information of the parties. It is thus very necessary to take account of the security of zero-knowledge protocols when adaptive corruptions are allowed.

Previous adaptively secure zero-knowledge protocols work either in a stand-alone setting, or in a concurrent setting with trusted setup assumptions. In this paper, we study adaptive security of zero-knowledge protocols under both concurrent self composition and man-in-the-middle attacks in the plain model (i.e., without any set-up assumptions). We provide a construction of adaptively secure concurrent non-malleable zero-knowledge proof/argument for every language in NP.

Category / Keywords: foundations / Zero-knowledge protocol, concurrent non-malleability, adaptive corruption, commitment schemes

Date: received 18 Nov 2011, last revised 21 Nov 2011

Contact author: zongyang zhang at gmail com