Computational Soundness of Malleable Zero-Knowledge Proofs

Michael Backes
Saarland University
MPI-SWS

Esfandiar Mohammadi
Saarland University

Non-interactive zero-knowledge proofs (NIZKP) are deployed in many modern privacy preserving cryptographic protocols. Recent work shows how to abstract zero-knowledge proofs in a computationally sound Dolev-Yao style symbolic model, which is amenable to automated verification techniques (Backes & Unruh, CSF '08). The computational soundness proof for this abstraction, however, requires a cryptographic zero-knowledge proof to satisfy very strong properties, called extraction zero-knowledge (EZK). This property states that a simulated proof is indistinguishable from a real proof even if the attacker has access to an extraction oracle for any but the challenge proof. All known NIZKP satisfying EZK are far too inefficient, and thus impractical for real-world protocols.

We present a computationally sound Dolev-Yao style abstraction of zero-knowledge proofs merely requiring the zero-knowledge property (instead of EZK). This relaxation, however, leads to a symbolic model in which the NIZKP are malleable. More precisely, our symbolic model allows the attacker to reuse any secret that has been used in a previously received zero-knowledge proof. This is formalized by introducing an additional knowledge relation that characterizes the secrets the attacker can use in the zero-knowledge proofs that it constructs.

This symbolic abstraction of non-interactive malleable zero-knowledge proofs allows for much more efficient cryptographic realizations, yet providing a sufficiently expressive model for the automated verification of cryptographic protocols that use NIZKP.