Zero Knowledge Proofs

Max Ostermann

28.05.2019

1 Abstract

Diese Ausarbeitung ist eine Einführung in Zero Knowledge Proofs. Zuerst wird die Motivation und die Idee hinter Zero Knowledge Proofs anhand von Alibabas Höhle erläutert. Danach werde ich die grundlegenden Definitionen von Vollständigkeit, Korrektheit und Zero-Knowledge sowie den generellen Beweisablauf erklären. Es Folgen einige Protokolle und das Protokoll des quadratischen Restes wird beispielsweise durchgerechnet. Im Rahmen dieses Beispiels wird auch der Begriff der Simulierbarkeit, sowohl für Black-Box-, als auch Honest-Verifier Simulatoren sowie parallele und simultan Abläufe näher betrachtet. Als letzter Protokolltyp werden Non-interactive Zero Knowledge Proofs anhand der Fiat-Shamir Heuristik betrachtet. Abschließend beschäftige ich mich noch mit den modernen Anwendungsmöglichkeiten der Beweisprotokolle, untersuche gleichzeitig die Schwächen gegenüber Angriffen und wie sich diese möglicherweise vermeiden lassen.