UNIVERSITÄT KONSTANZ

Hashfunktion und Blockchain

Fachseminar Zahlentheorie
Prof. Dr. Salma Kuhlmann

14. Juli 2021

Autor: Rebecca Köchling Mayán
Betreuer: Michele Serra

Abstract

In diesem Vortrag geht es um Hashfunktionen. Zuerst werden Grundlagen aus der Informationstheorie eingeführt. Mittels Modularer Hashfunktionen wird die Bedeutung des Aufbaus von Hashfunktionen veranschaulicht und bedeutende Merkmale zur Kollisionsreduktion aufgezeigt. Der Schwerpunkt des Vortrags liegt auf kryptografischen Hashfunktionen. Dazu werden elementare Sicherheitsanforderungen wie die Kollisionsresistenz und Urbildresistenz betrachtet. Infolgedessen wird mittels des Merkle-Meta-Verfahrens eine zentrale Konstruktion von kollisionsresistenten Hashfunktionen vorgestellt. Schließlich wird die Sicherheit der digitalen Signatur in Kombination mit Hashfunktion verdeutlicht. Den Abschluss bildet die Vorstellung der Blockchain Technologie und dessen fundamentale Anwendung von Hashfunktionen in der Blockchain.