Diffie–Hellman-Problem
Unter welchen Voraussetzungen ist das Diffie–Hellman-Problem besonders schwer zu lösen?

6. Juli 2021

SEMINAR ZAHLENTHEORIE AN DER UNIVERSITÄT KONSTANZ BEI
PROF. DR. SALMA KUHLMANN
AUTORIN: TAMARA EDINBOROUGH
DATUM DES VORTRAGS: 07.07.2021

SUPERVISOR
MICHELE SERRA

Abstract

Dieser Vortrag thematisiert das Diffie–Hellman-Problem und setzt sich mit der Leitfrage auseinander unter welchen Voraussetzungen dieses Problem besonders schwer zu lösen ist. Dazu gehen wir auf ein paar Grundlagen der Kryptographie, wie z.B. die Einwegfunktionen, ein. Außerdem definieren wir das diskrete Logarithmus Problem, welches in vielen Kryptoverfahren für das Ver- und Entschlüsseln von Nachrichten genutzt wird. Danach schauen wir uns das Diffie–Hellman-Verfahren an und betrachten wie das diskrete Logarithmus Problem bei diesem Verfahren implementiert wird. Wir definieren anschließend das Diffie–Hellman-Problem und untersuchen die Leitfrage, indem wir uns eine Behauptung überlegen, aufstellen und überprüfen. Insbesondere wird dabei der Satz von Lagrange thematisiert. Zum Schluss beantworten wir die Leitfrage und schauen uns noch einmal die Einwegfunktionen an.