technische universität
dortmund

Bachelor Thesis

Hash-Funktions

Marco Bellmann

May 8, 2023

Reviewers:
Professor Coja-Oghlan
Arnab Chatterjee

Technische Universität Dortmund
Fakultät für Informatik
LEHRSTUHL 2 (LS 2)
https://eac.cs.tu-dortmund.de//

Inhaltsverzeichnis

Kapitel 1

Introduction

1. Introduction
2. about hashfunctions
3. about md5
4. about collisions
5. goals and motivation
6. notation explained
7. Definition of md5
8. impelmentation of md5
   (a) padding (difficulties, missing by stevens)
   (b) processing
   (c) md5compress
   (d) representation
   (e) potential for improvement
   (f) difficulties
9. attack of md5

Kapitel 2

Implementation of MD5

Stevens starts with Wangs attack, which trys to finde to pairs of blocks: (B_0, B_0') and (B_1, B_1') that $IHV = IHV'$, with the goal to create two massages M and M', with the same hash value:

$$IHV_0 \xrightarrow[M_{(1)}]{} \cdots \xrightarrow[M_k]{} IHV_k \xrightarrow[B_0]{} IHV_{k+1} \xrightarrow[B_1]{} IHV_{k+2} \xrightarrow[M_{k+1}]{} \cdots \xrightarrow[M_N]{} IHV_N$$

$$==\neq==$$

$$IHV_0 \xrightarrow[M_{(1)}]{} \cdots \xrightarrow[M_k]{} IHV_k \xrightarrow[B_0]{} IHV'_{k+1} \xrightarrow[B_1]{} IHV'_{k+2} \xrightarrow[M_{k+1}]{} \cdots \xrightarrow[M_N]{} IHV_N$$

Anhang A

Weitere Informationen

Abbildungsverzeichnis

Algorithmenverzeichnis

Literaturverzeichnis

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst habe und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet sowie Zitate kenntlich gemacht habe.

Dortmund, den 8. Mai 2023

Muster Mustermann