technische universität
dortmund

Faculty for Computer scinece

Bachelor's Thesis

Collsisions in Hash-Funktions

Marco Bellmann

First Reviewer:
Prof. Dr. Coja-Oghlan

Second Reviewer:
Msc. Arnab Chatterjee

Dortmund, August 2023

Inhaltsverzeichnis

Kapitel 1

Introduction

1.1 May Contains

1. about hashfunctions
2. about md5
3. Definition of md5
4. impelmentation of md5
    (a) padding (missing in Stevens code)
    (b) md5compress
    (c) potential for improvement
5. collisions for md5
    (a) Blocks N & M
    (b) 00, 01, 10, 11
    (c) MMM
6. conclusion
7. SHA1
8. why not in SHA1
9. notation helper

Motivation

This thesis is about a deeper look on MD5. We take a closer look at the Master thesis of M. Stevens: a fast collisions finding algorithm [1]. The goal is to work out a more clear and understandable code, which is not necessarily faster, to reevaluate the code on modern systems and the difference to SHA1.

Nodes

Bsp für Stevens Werte für Q_t mit $t = 3$:
Bit Conds for $Q_t|t = 3$:

4. the old bit Conds
3. the new bit Conds
2. the val to set the ones (or with $0x017841c0$)
1. the val to set the zeros (and with 0xfe87bc3f)

1.&	11111110	10000111	10111100	00111111	$0xfe87bc3f$
2.$\|$	00000001	01111000	01000001	11000000	$0x017841c0$
3.	....	.1111...	.1....01	11......	
4.	....	....0...	....0...	.0......	

the & flips the 0 correct, the $\|$ flips the 1 correct

Stevens	Wang	Definition
$RL\left(X, Y\right)$	$ROTL^{Y}\left(X\right)$	cyclic left shift X by Y (usually mod 31)
$RR\left(X, Y\right)$	-	cyclic right shift X by Y
$RC\left(t\right)$	$S\left(t\right)$	rotation Constant of t
Block 1, Block 2	Block N, Block M	pair of first blocks for collisions finding
Block 0, Block 1	Block N, Block M	same pair but im Code

1.2 Notation helper

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 25. Mai 2023

Muster Mustermann