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

Contents

Chapter 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

1. padding
2. procseesing
3. md5 sum
4. output

Figure 1.1: MD5 algo

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.

1.2 MD5

Massage Digest Algorithm 5 is a .. to , from ..., in ...
MD5 is usually seen as 4 steps as seen in fig md5

Notes

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)

Notation

Stevens	Wang	Definition
$RL(X,Y)$	$ROTL^{Y}(X)$	cyclic left shift X by Y (mod 31)
$RR(X,Y)$	-	cyclic right shift X by Y (mod 31)
$RC(t)$	$S(t)$	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.&	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

1.3 Notation helper

$RR(X,Y) \equiv X\textcircled{\scriptsize RR}Y$

Chapter 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:

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

$$==\neq==$$

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

Chapter 3

MD5-Attack

3.1 Bit Conditions

We need the bit Conditions to avoid a carry, so a manipulation in step t stays in step t and does not propagate beyond the 31st bit.

We calculate the bit conditions by using the Add difference. We calculate an δ for each f_t, Q_t, T_t and R_t to calculate the Add-Difference for Q_{t+1}. Additional we need the rotation constant RC for each t. In general we begin with the f_t:

1. $t \in \{0, 1, 2, 3\}$:
   $Q_t = 0$ since here is no influence by an message and no calculation of f, there is nothing to change:

2. $t = 4$
   $\Delta T_4 = -2^{31}$, because we must not have a carry, we *lock* the last bit. Since $RL(T_4, RC_4) = RL(-2^{31}, 7) = -2^6$ and $\delta Q_4 = 0 \Rightarrow \delta Q_5 = -2^6$

t	$RC(t)$
0	7
1	12
2	17
3	22
4	7
5	12
6	17
7	22
8	7
9	12
10	17
11	22
12	7
13	12
14	17
15	22

An MD5 hash is created by taking a string of an any length and encoding it into a 128-bit fingerprint. Encoding the same string using the MD5 algorithm will always result in the same 128-bit hash output. MD5 hashes are commonly used with smaller strings when storing passwords, credit card numbers or other sensitive data in databases such as the popular MySQL. This tool provides a quick and easy way to encode an MD5 hash from a simple string of up to 256 characters in length.

$$m_t = RR\left(Q_{t+1} - Q_t, RC_t\right) - f_t\left(Q_t, Q_{t-1}, Q_{t-2}\right) - Q_{t-3} - AC$$

Appendix A

Tables

```
+—+
|abc|
+—+
```

Appendix B

Code

a +=a;

List of Figures

Algorithmenverzeichnis

Bibliography

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 May 26, 2023

Muster Mustermann