

Classification of the accepted SHA-3 candidates

Ewan Fleischmann Christian Forler Michael Gorski

Sirrix AG security technologies

Bauhaus-Universität Weimar

Symmetric Cryptography - Schloss Dagstuhl

January 12, 2009

Roadmap

- 1 Introduction
- 2 Design
- 3 Attacks
- 4 Speed

History

- Aug 2004: Wang et al. published MD5 attack.
- Feb 2005: Wang et al. published SHA-1 attack.
- Nov 2007: NIST announced SHA-3 contest.
- Oct 2008: Deadline for SHA-3 candidates submission.
- Dec 2008: NIST announced 51 round one candidates.

Classification

Why?!?

- 51 first round candidates!
- Fun and curiosity. ;-)
- Allows comparison.
 - Speed.
 - Security.
 - Complexity.

Other takers

- SHA-3 Zoo list of all candidates and attacks.
- Niels Ferguson also started a SHA-3 classification.

Balanced Feistel Network

Balanced Feistel Network (BFN)

Hash function can be depicted as a balanced feistel network.

Number of candidates:	4
Number of academically broken candidates:	2

Unbalanced feistel network

Unbalanced Feistel Network (UFN)

Hash function can be depicted as an unbalanced feistel network.

Number of candidates:	11
Number of academically broken candidates:	1

Wide Pipe Design

Wide Pipe (WP)

The internal state of the hash function is larger than the message digest.

Number of candidates: 22

Number of academically broken candidates: 12

Message Expansion

Key Schedule / Message Expansion (KEY)

Hash function contains (key schedule or) a message expansion algorithm.

Number of candidates: 25

Number of academically broken candidates: 8

Maximum Distance Separable Matrix

Maximum Distance Separable Matrix (MDS)

Maximum Distance Separable (MDS) matrices are used as a building block of the compression/hash function.

Number of candidates:	17
Number of academically broken candidates:	6

Output Transformation

Output Transformation (OUT)

Non trivial function that transforms the “final” chaining value.

Number of candidates:	18
Number of academically broken candidates:	8

S-Box

S-Box (SBOX)

The compression function contains substitution boxes.

Number of candidates:	33
Number of academically broken candidates:	15

Feedback Shift Register

Feedback Shift Register (FSR)

The compression function is/uses a (N)LFSRs.

Number of candidates:	8
Number of academically broken candidates:	5

Overview

Attribute	#candidates (academically broken)
S-Box	33 (15)
Message Expansion	25 (8)
Wide Pipe	22 (12)
Output Transformation	18 (8)
MDS Matrix	17 (6)
Unbalanced Feistel Network	11 (1)
Feedback Shift Register	8 (5)
Balanced Feistel Network	4 (2)

Combination

AES Design

MDS + SBOX + !FSR \Rightarrow AES based design.

Number of candidates: 15

Number of academically broken candidates: 4

Attack Overview

Statistic

- Academically unbroken candidates (unharmed) : 29
- Academically broken candidates (harmed): 22
 - Collision Attacks: 18
 - (2nd) Preimages Attacks: 16
 - Practical attacks: 10 (six collision examples)
 - Conceded broken: 8

Speed Classification

Speed classification table

Speed (cpb)	Class
$x < \frac{1}{2} \text{ SHA-2}$	AA
$\frac{1}{2} \cdot \text{SHA-2} \leq x < \frac{3}{4} \cdot \text{SHA-2}$	A
$\frac{3}{4} \cdot \text{SHA-2} \leq x < \cdot \text{SHA-2}$	B
$\text{SHA-2} \leq x < \frac{5}{4} \cdot \text{SHA-2}$	C
$\frac{5}{4} \cdot \text{SHA-2} \leq x \leq 2 \cdot \text{SHA-2}$	D
$x > 2 \cdot \text{SHA-2}$	E

256-Bit Message Digest on 32-Bit System

Conditions

- Target Platform: Intel Core 2 Duo
- Reference Value: SHA-256 (openssl): 29.3 cpb
- Speed Range: 8.3 cpb (EnRUPT*) - 324 cpb (FSB)

Top 5 (“unbroken” candidates only)

Place	Candidate	Speed	Class
1.	EnRUPT*	8.3 cpb	AA
2.	BMW*	8.6 cpb	AA
3.	Edon-R*	9,1 cpb	AA
4.	SIMD	12 cpb	AA
5.	TIB3	12.9 cpb	AA

* harmed

512-Bit Message Digest on 32-Bit System

Conditions

- Target Platform: Intel Core 2 Duo
- Reference Value: SHA-512 (openssl): 55.2 cpb
- Speed Range: 4.9 cpb (TIB3) - 507 cpb (FSB)

Top 5 (“unbroken” candidates only)

Place	Candidate	Speed	Class
1.	TIB3	4.9 cpb	AA
2.	EnRUPT*	5.1 cpb	AA
3.	BMW*	13.3 cpb	AA
4.	Edon-R*	13.7 cpb	AA
5.	Lux, ARIRANG	14.9 cpb	AA

* harmed

256-Bit Message Digest on 64-Bit System

Conditions

- Target Platform: Intel Core 2 Duo
- Reference Value: SHA-256 (openssl): 20.1 cpb
- Speed Range: 4.4 cpb (MeshHash**) - 454.6 cpb (Spectral Hash*)

Top 5 (“unbroken” candidates only)

Place	Candidate	Speed	Class
1.	Edon-R*	5.9 cpb	AA
2.	Skein, TIB3	7.6 cpb	AA
3.	BMW*	7.8 cpb	AA
4.	SHAMATA	8 cpb	AA
5.	EnRUPT*	8.3 cpb	AA

* harmed, ** broken

512-Bit Message Digest on 64-Bit System

Conditions

- Target Platform: Intel Core 2 Duo
- Reference Value: SHA-512 (openssl): 13.1 cpb
- Speed Range: 2.9 cpb (Edon-R*) - 454.6 cpb (Spectral Hash*)

Top 5 (“unbroken” candidates only)

Place	Candidate	Speed	Class
1.	Edon-R*	2.9 cpb	AA
2.	BMW*	4 cpb	AA
3.	EnRUPT*	5.1 cpb	AA
4.	Skein, TIB3	6.3 cpb	AA
5.	SHAMATA	11 cpb	B

* harmed

Questions?

Questions?

- New attributes?

Questions?

- New attributes?
- Old attributes?

Questions?

- New attributes?
- Old attributes?
- Speed classes?