Classification of the accepted SHA-3 candidates

Ewan Fleischmann Christian Forler Michael Gorski

Sirrix AG

Bauhaus-Universität Weimar

The First SHA-3 Candidate Conference, KU Leuven

February 28, 2009

Outline

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.

Feistel Network

Balanced Feistel Network

Hash function can be depict as a Feistel network.

- Unbalanced Feistel Network
- Balanced Feistel Network

Characteristic	**#Candidates**	**#Theoretically broken**
Unbalanced Feistel Network	11	1
Balanced Feistel Network	4	2
	15	3

Wide Pipe Design

Wide Pipe

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

Number of candidates:	22
Number of theoretically broken candidates:	11

Message Expansion

Key Schedule / Message Expansion

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

```
Number of candidates:                          25
Number of theoretically broken candidates:      6
```

Maximum Distance Separable Matrix

Maximum Distance Separable Matrix

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

Characteristic	**#Candidates**	**#Theoretically broken**
1.5×1.5	1	1
2×2, 4×4	1	0
4×4	6	2
4×4, 8×8	3	0
8×8	4	2
8×8, 16×16	1	1
16×16	1	0
TRS Codes	1	0
	18	6

Output Transformation

Output Transformation

Non trivial function that transforms the "final" chaining value.

```
Number of candidates:                          18
Number of theoretically broken candidates:      8
```

S-Box

S-Box

The compression function contains substitution boxes.

Characteristic	#Candidates	#Theoretically broken
3×3	1	0
4×4	3	1
4×3	1	0
5×5	1	0
8×8	24	12
8×32	1	1
8×1016	1	0
	33	14

Feedback Shift Register

Feedback Shift Register

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

```
Number of candidates:                          9
Number of theoretically broken candidates:     6
```

Overview

Attribute	#Candidates	Theoretically broken
Feistel Network	15	3 (20%)
Message Expansion	25	6 (24%)
MDS Matrix	18	6 (33.3%)
S-Box	32	14 (43.7%)
Output Transformation	18	8 (44.4%)
Wide Pipe	22	12 (54.5%)
Feedback Shift Register	9	6 (66.6%)

Combination

AES Design

4×4 MDS matrix $+$ 8×8 S-box $\Rightarrow$ Using AES as building block.

Number of candidates:	6
Number of theoretically broken candidates:	2

Attack Overview

Statistic

- Theoretically unbroken candidates (unharmed) : 29
- Theoretically broken candidates (harmed): 22
  - Collision Attacks: 18
  - (2nd) Preimage Attacks: 16
  - Practical attacks: 10 (six collision examples)
  - Conceded broken: 9

Speed Classification (32-Bit)

32-Bit Speed Classification Table

Speed (cpb)	Class	256 Bit	512 Bit
$x < \frac{1}{2}$ SHA-2	AA	8 (5)	15 (8)
$\frac{1}{2} \cdot$ SHA-2 $\leq x < \frac{3}{4} \cdot$ SHA-2	A	8 (3)	4 (3)
$\frac{3}{4} \cdot$ SHA-2 $\leq x < \cdot$ SHA-2	B	6 (1)	4 (-)
SHA-2 $\leq x < \frac{5}{4} \cdot$ SHA-2	C	6 (1)	6 (2)
$\frac{5}{4} \cdot$ SHA-2 $\leq x \leq 2 \cdot$ SHA-2	D	5 (3)	6 (-)
$x > 2 \cdot$ SHA-2	E	11 (6)	11 (6)

Speed Classification (64-Bit)

64-Bit Speed Classification Table

Speed (cpb)	Class	256 Bit	512 Bit
$x < \frac{1}{2}$ SHA-2	AA	7 (5)	6 (4)
$\frac{1}{2} \cdot$ SHA-2 $\leq x < \frac{3}{4} \cdot$ SHA-2	A	8 (2)	0 (-)
$\frac{3}{4} \cdot$ SHA-2 $\leq x <$ $\cdot$ SHA-2	B	6 (2)	7 (3)
SHA-2 $\leq x < \frac{5}{4} \cdot$ SHA-2	C	2 (-)	3 (-)
$\frac{5}{4} \cdot$ SHA-2 $\leq x \leq 2 \cdot$ SHA-2	D	10 (2)	5 (2)
$x > 2 \cdot$ SHA-2	E	11 (8)	23 (10)

The End.

Questions?