Analysis of LASH (Work in Progress)

Scott Contini, Krystian Matusiewicz
Josef Pieprzyk, Ron Steinfeld

Macquarie University

Guo Jian, Huaxiong Wang

Nanyang Technological Institute, Singapore

August 2007

Introduction

- LASH is a lattice-based cryptographic hash function proposed at Second NIST Workshop by Bentahar, Page, Silverman, Saarinen and Smart.
- Modification of Goldreich et al construction aimed at resisting 'faster than generic' collision and preimage attacks
  - Miyaguchi-Preneel feedforward
  - 'Large Pipe' wide state design (output length $= 1/2$ state length)
  - Final Compression function truncates 4 LS bits per byte
- With security parameter x, LASH-x produces hash of length x bit
- Until now, no 'faster than generic' attacks known

Summary of Our Results for LASH-x

- 'Long message' collision attack with asymptotic time and memory complexity $O(2^{0.364 \cdot x})$
  - Uses cycling with precomputed table lookup for forcing some output bytes to zero in each iteration
  - Time/Memory tradeoff with precomp. memory $O(2^c)$ and time $O(2^{x/2-3c/8})$
  - Exploits $IV = 0$ and zero fixed-point of compression function
- Implications:
  - Collisions in **LASH**-160 with order 2^{58} **time/memory**
  - Implementation with 2^{24} memory and 1 day on 2.4 GHz PC produced 'half collision' (hashes matching on last 80 bits)

Long Message 'Half Collision' for LASH-160

First Message									
$l = 3380367992$									
first nonzero block:									
16	14	2e	87	6b	cd	8e	00	ff	01
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	
hash:									
f7	22	11	a5	61	b1	d1	15	ff	0b
22	17	eb	62	9a	d7	b8	ff	0f	00

Second Message									
$l = 1380208632$									
first nonzero block:									
1e	9c	59	fe	f2	94	d5	ff	00	02
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	
hash:									
f2	56	e8	70	6b	8a	94	6f	b9	76
22	17	eb	62	9a	d7	b8	ff	0f	00

Figure 1: Two long messages that match on the last 10 bytes of the hash.

Summary of Our Results for LASH-x

- Compression function of LASH is not a PRF (when keyed via half the input bits)
  - Overwhelming distinguishing advantage with just 2 queries
- Collisions in *final* compression function of LASH-x:
  - Exploit truncation of 4 LS bits per byte in final compression function
  - Variant of Wagner's Generalized birthday attack: collisions using $O(2^{0.248x})$ time and memory
    - For **LASH-160**: About 2^{44} **time and** 2^{48} **bytes memory** suffice
  - Lattice attacks on **LASH-160**:
    - SVP: Collision on **120 output bits** in order 2^{36} **time** (computation in progress)
    - CVP+cycling: Collision on **ALL 160 output bits** in order 2^{70} **time**.