Preimage attacks on HAVAL and MD5

Jean-Philippe Aumasson Willi Meier Florian Mendel

MD5

- 1991: publication
- 1993: **collision** attack (compression function)
- 2005: **collision** attack (hash function)
- 2005+: faster, chosen-prefix, meaningful **collisions**

No (second) preimage attack.

MD5

Our **preimage** attacks:

- **47**-step compression function
  - Cost: 2^{96} compressions and 2^{36} bytes
- **45**-step compression function
  - Cost: 2^{100} compressions and negligible memory
- **47**-step hash function
  - Cost: 2^{102} compressions and 2^{39} bytes

(full MD5 has 64 steps)

HAVAL

- 1992: publication
- 2003: **collision** attack (3-pass)
- 2006: **collision** attack (4- and 5-pass)
- 2008: **second-preimage** attack (3-pass)

No preimage attack.

3-pass HAVAL

Our **preimage** attacks:

- compression function
  - Cost: 2^{224} compressions and 2^{69} bytes
- compression function
  - Cost: 2^{224} compressions and 2^{69} bytes
- hash function
  - Cost: 2^{230} compressions and 2^{71} bytes

Further work

Extend attack to more than 47 steps?

Second preimages faster than preimages?

Build on collision-related results?