How good are some 2^{nd} round SHA3 hashes when their compression functions are weak? (Work in progress)

Charles Bouillaguet, Pierre-Alain Fouque, Praveen Gauravaram[*]
and Gaëtan Leurent

ENS, France and DTU, Denmark[*]

17th August 2010

It is a folklore that some attacks on compression functions do not weaken hash functions.

It is a folklore that some attacks on compression functions do not weaken hash functions.

When can we say that even after doing some strong attack on the compression function, the above belief on the hash function security would still hold?

On some SHA3 hash functions

1. Nearly all SHA3 designers who have had distinguishers, symmetries, fixed points, partial fixed point etc.. sort of analysis on their compression functions claimed that they do not lead to attacks on hash functions.
2. Some designers (e.g SIMD, SHABAL) even proved the indifferentiability security of their hash function when the compression function has efficient distinguishers.

Are these hash functions still indifferentiable if their compression functions are easily invertible (pseudo preimage attacks)?

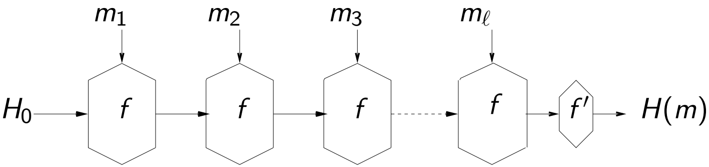
On some SHA3 hash functions

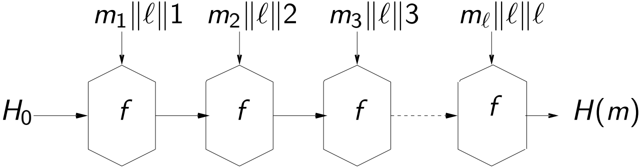
1. Nearly all SHA3 designers who have had distinguishers, symmetries, fixed points, partial fixed point etc.. sort of analysis on their compression functions claimed that they do not lead to attacks on hash functions.
2. Some designers (e.g SIMD, SHABAL) even proved the indifferentiability security of their hash function when the compression function has efficient distinguishers.

Are these hash functions still indifferentiable if their compression functions are easily invertible (pseudo preimage attacks)?

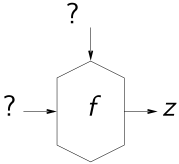
Many second round SHA3 hash functions use a wide-pipe or a pfMD or their special instantiation for the iteration.

Wide-pipe and pfMD



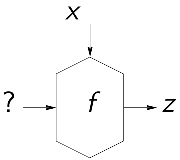


Invertible queries to compression functions

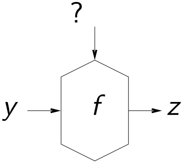


Weak backward query

[We consider]



Strong backward query



Bridging query

Strong inversion queries

[Liskov-SAC'06,Hoch-Shamir-ICALP'08]

Indifferentiability results

Mode	pfMD	wide pipe
Bridging	no	no
Strong backward	no	yes* [SHABAL team]
Weak backward	yes	yes* [SHABAL team]

1. Generalisation of indifferentiability of Sponge hash construction[Bertoni *et al.*-Eurocrypt'08].
2. Wide-pipe of a weak compression function such as Rabin's 78 scheme seems to remain indifferentiable [SHABAL team].

Thank you!!!!