Improved Cryptanalysis of `ECHO` & `Grøstl`

FSE 2010 Rump Session - Seoul - Korea

Thomas Peyrin

Ingenico

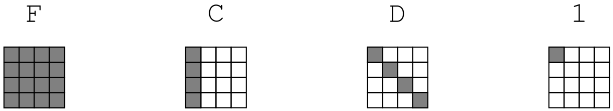
February 9th, 2010

The AES-based functions in the SHA−3 competition

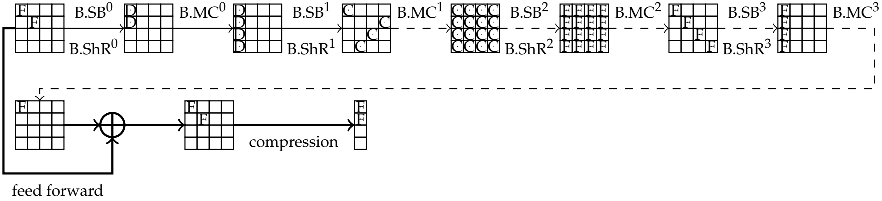
- We already know how to use **freedom degrees** very efficiently:
  - Rebound attack [MRST09]
  - Start-from-the-middle attack [MPRS09]
  - Super-Sbox attack [GP10,MRST10]
- But what about the **differential paths** ?
  - Usually very good security arguments (bounds, minimal number of active Sboxes, etc.)
  - Truncated differential paths seem the best technique so far [K94,P07] ...
  - ... but let's try to improve them a little bit.

ECHO

Consider 4 different types of truncated differential states

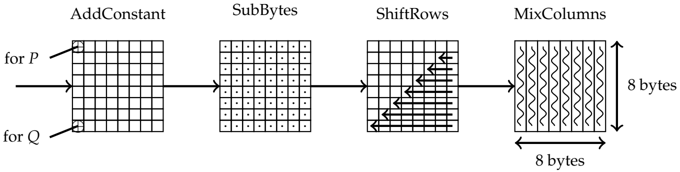


Increase the granularity of the previous known paths

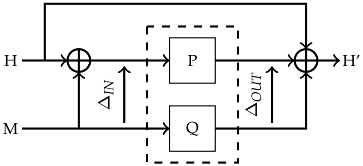


Grøstl

Grostl compression function is made of two parallels permutations P and Q



Idea: Do not look at differences between input pairs, but between P and Q



Results on ECHO and Grøstl

Table: Results on ECHO compression function

target	rounds	computational complexity	memory requirements	type
ECHO-SP-256 comp. function	3/8	2^{64}	2^{64}	semi-free-start collision
	3/8	2^{64}	2^{64}	**distinguisher**
ECHO-256 comp. function	3/8	2^{64}	2^{64}	semi-free-start collision
	4/8	2^{64}	2^{64}	**distinguisher**
ECHO-SP-512 comp. function	3/10	2^{64}	2^{64}	semi-free-start collision
	4/10	2^{64}	2^{64}	**distinguisher**
ECHO-512 comp. function	3/10	2^{96}	2^{64}	semi-free-start collision
	6/10	2^{96}	2^{64}	**distinguisher**

Table: Results on Grøstl compression function

target	rounds	computational complexity	memory requirements	type	section
Grøstl-256 comp. function	7/10	2^{56}		distinguisher	[MPRS09]
	8/10	2^{112}	2^{64}	distinguisher	[GP10,MRST10]
	9/10	2^{80}	2^{64}	**distinguisher**	**new**
	10/10	2^{192}	2^{64}	**distinguisher**	**new**
Grøstl-512 comp. function	7/14	2^{152}	2^{64}	semi-free-start collision	[MRST10]
	11/14	2^{640}	2^{64}	**distinguisher**	**new**