The Super-Sbox Cryptanalysis

Improved Attacks for AES-like Permutations

Henri Gilbert and Thomas Peyrin

Orange Labs and Ingenico

FSE 2010 - Seoul - Korea
(February 9, 2010)

Outline

Introduction

Previous cryptanalysis techniques for AES-like permutations

The Super-Sbox cryptanalysis

Results

Outline

Introduction

Previous cryptanalysis techniques for AES-like permutations

The Super-Sbox cryptanalysis

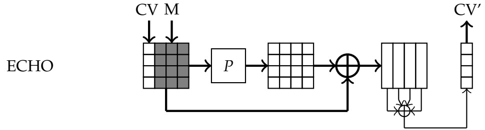
Results

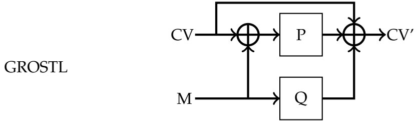
The SHA−3 competition and the current status of AES

- SHA−3 competition launched in October 2008 with 51 accepted submissions (among 64). Second round brought this number to 14 only. Among them, **many AES-based or AES-related candidates:**
  - ECHO
  - FUGUE
  - Grøstl
  - SHAvite−3
- Because of a somewhat too light key schedule, AES-256 has been recently attacked in the related key model [CRYPTO-09], while AES-128 remains unharmed.

Block ciphers and hash functions

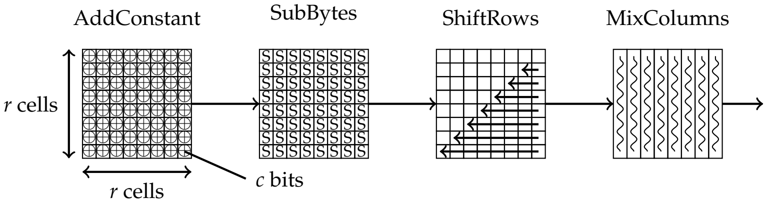
The new AES-256 attacks may impact the AES-based hash functions using a key schedule, but some of them basically use fixed key permutations (for example ECHO or Grøstl).





- **What is the security of an AES-like permutation for a hash function utilization (known-key model [ASIACRYPT-07]) ?**
- **What is the impact of the attacks on the security of the whole compression function ?**

What is an AES-like permutation ?



$$MixColumns \circ ShiftRows \circ SubBytes \circ AddConstant(C).$$

- **AddConstant:** in knwon-key model, just add a round-dependent constant (breaks natural symmetry of the three other functions)
- **SubBytes:** application of a c-bit Sbox (only non-linear part)
- **ShiftRows:** rotate column position of all cells in a row, according to its row position
- **MixColumns:** linear diffusion layer.

Outline

Introduction

Previous cryptanalysis techniques for AES-like permutations

The Super-Sbox cryptanalysis

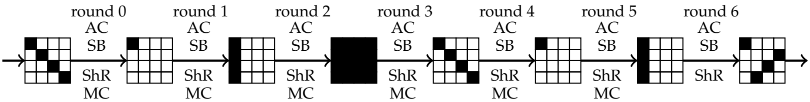
Results

Truncated differences

- Originally introduced by Knudsen for block ciphers [FSE-94]
- Later applied to hash functions (collision attack on Grindahl) [ASIACRYPT-07]
- **Idea:** consider byte-differences, without considering their actual value (active or inactive).
- **Only the truncated differences propagation through MixColumns behave probabilistically. Per column:**

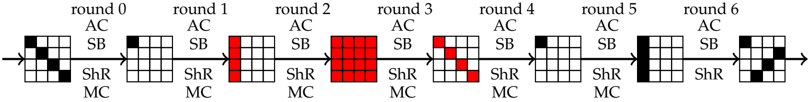
$$\text{nb active input cells} + \text{nb active output cells} \geq r + 1.$$

$$P \simeq 2^{-xc} \text{ for } x \neq r \text{ inactive output cells.}$$



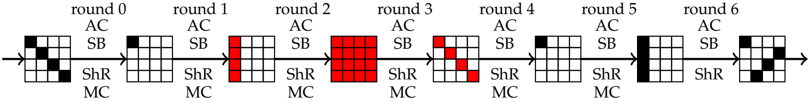
Controlled and uncontrolled rounds

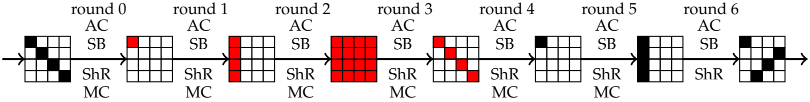
- **Idea:** use the freedom degrees in the middle of the differential path (Mendel et al. [FSE-09]).
- The path is divided into two different kind of steps:
  - **The controlled rounds:** the part where the freedom degrees are used (usually in the middle of the path). On average, finding a solution for the controlled rounds should cost only a few operations.
  - **The uncontrolled rounds:** the part where all the events are verified probabilistically (left and right part of the path) because no more freedom degree is available. Determine the complexity of the overall attack.



Rebound Attack and Start-from-the-middle

- **Rebound attack:** allows to get 2 controlled rounds [FSE-09]. Requires 2^{rc} memory. It broke compression functions of many SHA-3 candidates.
- **Start-from-the-middle:** use more complicated techniques to get up to 3 controlled rounds in the case of low weight differential paths [SAC-09]. Requires 2^{rc} memory.

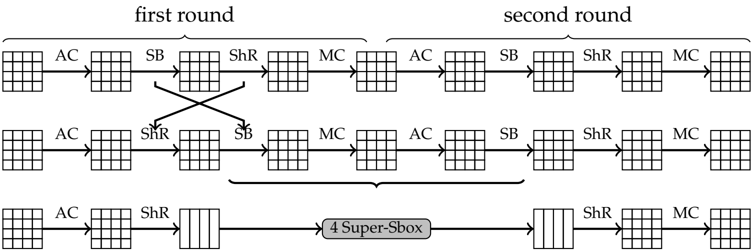




Outline

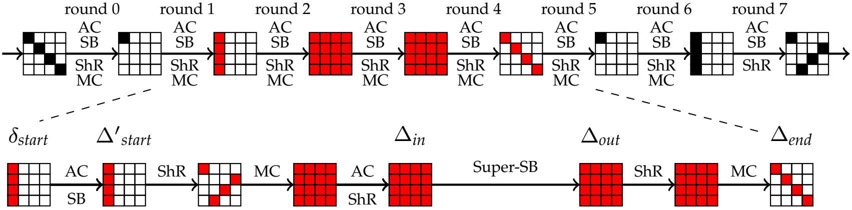
The Super-Sbox view

- Introduced by Daemen and Rijmen (e.g. [SCN-06]) to simplify the analysis of AES differential properties and not for cryptanalysis purposes.
- **Idea:** one can view two rounds of an AES-like permutation as a layer of big 2^{rc}-bit Sboxes preceded and followed by simple affine transformations. We call those **Super-Sboxes**



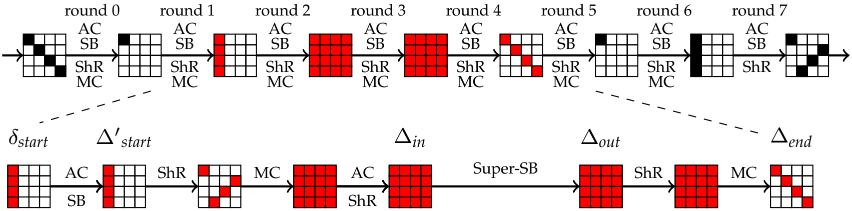
The controlled rounds in the Super-Sbox view

- **One can get 3 controlled rounds, even for high weight differential paths.**
- **Forward:** start with a random (not truncated) difference δ'_{start} at the beginning of round 2 (such that we obtain a compatible truncated difference Δ_{start} when inverting *SB* and *AC*). Then, pass *ShR*, *MC*, *AC* and *ShR* to obtain the aimed input difference Δ_{in} on the *r* Super-Sboxes.
- **Backward:** start with a random (not truncated) difference Δ_{end} at the end of round 4, and invert *MC* and *ShR* in order to obtain the aimed output difference Δ_{out} on the *r* Super-Sboxes.
- **Problem:** need the ability to find for each of the *r* columns, a value that maps Δ_{in} to Δ_{out} ... seems hard.



The controlled rounds

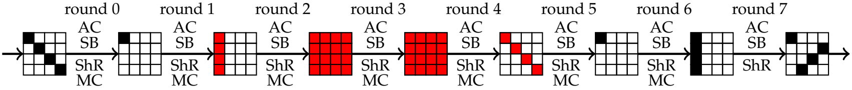
- **Idea:** pay a big price (2^{rc} operations and memory), but get many solutions (2^{rc}) once you paid.
- **1st step:** Fix a random Δ'_{start} difference value, which gives a fixed random Δ_{in}. For each of the r Super-Sboxes, exhaust all 2^{rc} possible actual values, then sort the results in r tables according to the output difference obtained.
- **2nd step:** try 2^{rc} distinct Δ_{end} differences. Then, for each Δ_{out} obtained by computing backward, check if for all the r columns the appropriate 2^{rc}-bit difference is present in the corresponding table. On average, one solution is found per Δ_{end} try.
- **The average complexity for finding one internal state pair verifying the controlled rounds is** 1**.**



The uncontrolled rounds

Eight-round path:

- On the left side, one has one $4 \mapsto 1$ MixColumns transition to control (round 1): $P \simeq 2^{-(r-1)c}$
- On the right side, one has one $4 \mapsto 1$ MixColumns transition to control (round 5): $P \simeq 2^{-(r-1)c}$
- Total complexity for finding a solution for the whole path: $2^{2(r-1)c}$ operations.



One has also to check that we have enough freedom degrees, such that a valid pair can be found.

Outline

Introduction

Previous cryptanalysis techniques for AES-like permutations

The Super-Sbox cryptanalysis

Results

Limited-birthday distinguishers

What is the generic complexity for mapping i fixed-difference bits to j fixed-difference bits through a random permutation E ?

Wlog, assume that $i \geq j$ and let $n := r^2 c$. Due to the birthday paradox, each structure of 2^{n-i} input values obtained by fixing the value of the i fixed-difference bits allows to get fixed-difference on $2(n-i)$ output bits:

- if $j \leq 2(n-i)$, then one can select $2^{j/2}$ input values from one single structure and this suffices to achieve a collision on the j target positions. The attack complexity is about $2^{j/2}$.
- if $j > 2(n-i)$, then about $2^{j-2(n-i)}$ structures have to be used to obtain a collision on the j prescribed positions. Overall, the complexity of the attack is about $2^{n-i} \times 2^{j-2(n-i)} = 2^{i+j-n}$.

Same reasoning for the $n-j$ free difference bits on the output and attacking E^{-1}:

- if $i \leq 2(n-j)$, then the attack complexity is about $2^{i/2}$.
- if $i > 2(n-j)$, then the attack complexity is about 2^{i+j-n}.

Final complexity: $\max\{2^{j/2}, 2^{i+j-n}\}$.

Results on AES, ECHO and Grøstl

Table: Results on the underlying permutation

target	rounds	computational complexity	memory requirements	type	source
AES	7	2^{24}	2^{16}	known-key-distinguisher	[SAC-09]
	8	2^{48}	2^{32}	known-key-distinguisher	this paper
Grøstl-256 permutation	7	2^{56}		distinguisher	[SAC-09]
	8	2^{112}	2^{64}	distinguisher	this paper
ECHO internal permutation	7	2^{384}	2^{64}	distinguisher	[SAC-09]
	8	2^{768}	2^{512}	distinguisher	this paper

Table: Results on the compression function

target	rounds	computational complexity	memory requirements	type	source
Grøstl-256 comp. function	6	2^{120}	2^{64}	semi-free-start collision	[FSE-09]
	6	2^{64}	2^{64}	semi-free-start collision	[SAC-09]
	7	2^{120}	2^{64}	semi-free-start collision	this paper
	7	2^{56}		distinguisher	[SAC-09]
	8	2^{112}	2^{64}	distinguisher	this paper
ECHO comp. function	none	none		none	—

Future work

- Try to find **better differential paths** for `ECHO` and `Grøstl` (**see Rump session !**)
- Try to apply the technique on `SHAvite-3`
- Control the key as well ! Is it conceivable to use a **"chosen key(s)" model** ? Would we be able to attack more rounds in this very optimistic model ?