Low Data Complexity Attacks on AES

Orr Dunkelman

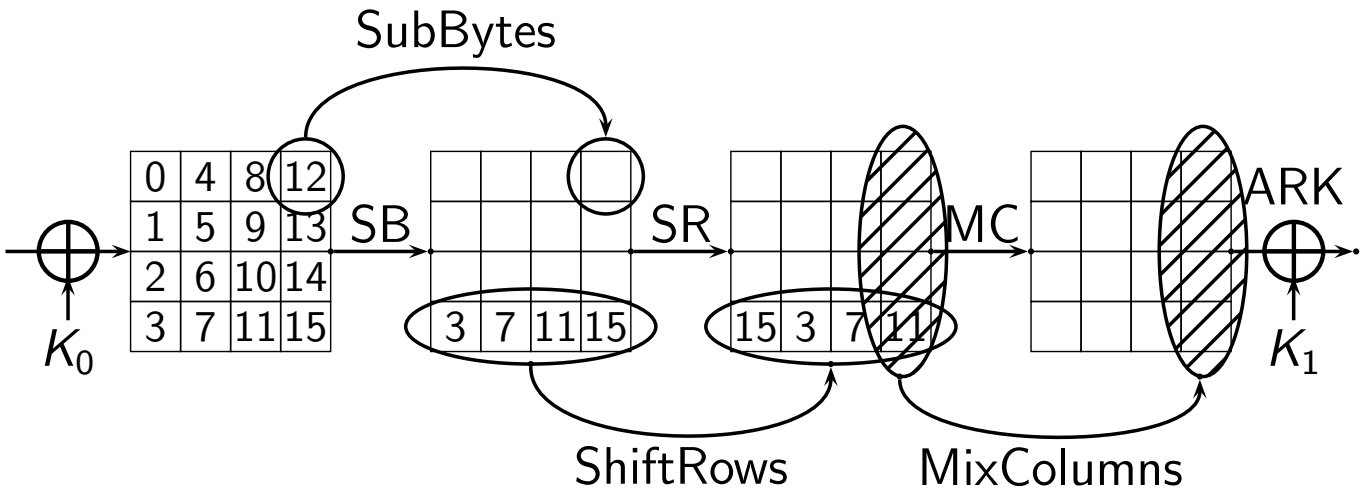
Joint work with Nathan Keller
Faculty of Mathematics and Computer Science
Weizmann Institute of Science

9 February, 2010

מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE

A Cryptographic Challenge

Consider one full round of AES:



Why?

- A LEX variant (one that leak the entire state every 4 rounds).
- A sub-routine in other attacks (in case of KP attacks).
- ALPHA MAC?
- Hash functions? (Vortex-0.0)

Why?

- A LEX variant (one that leak the entire state every 4 rounds).
- A sub-routine in other attacks (in case of KP attacks).
- ALPHA MAC?
- Hash functions? (Vortex-0.0)
- Practicing the art of running after bits.

So How Far Can You Go with 1 KP on AES-128

- Seems easy ah?

So How Far Can You Go with 1 KP on AES-128

- Seems easy ah?
- Our best attack takes 2^{48} using (heavily) the key schedule.
- We asked some people doing algebraic attacks, and they could not do better.
- We have strong evidence to believe that it is impossible to go below 2^{32}.

How Far Can You Go With 1 KP on AES-128

- Consider 2 full rounds of AES with 1 KP.
- Not so easy, ah?

How Far Can You Go With 1 KP on AES-128

- Consider 2 full rounds of AES with 1 KP.
- Not so easy, ah?
- Our best attack takes 2^{96} using (heavily) the key schedule.

Some More Results

Attack Type	Number of Rounds	Complexity		Independent Keys
		Data	Time	
MitM	1	1 KP	2^{48}	
Diff.	1	2 KP	2^{16}	
MitM	2	1 KP	2^{96}	
Diff.	2	2 KP	2^{48}	
Diff.	2	3 KP	2^{32}	
Diff.	3	2 CP	2^{28}	✓
Diff.	3	9 KP	2^{40}	✓
Diff.	4	5 CP	2^{64}	✓
Diff. MitM	4	11 CP	2^{40}	✓
Diff. MitM	4	$2^{49.3}$ KP	$2^{49.3}$	✓
Diff. MitM	4	$2^{33.2}$ KP	2^{80}	✓
Diff. MitM	4	$2^{17.7}$ KP	2^{120}	✓

Side Effects

AES Proposal: Rijndael

"In order to make the cipher and its inverse more similar in structure, the linear mixing layer of the last round is different from the mixing layer in the other rounds. It can be shown that this does not improve or reduce the security of the cipher in any way. This is similar to the absence of the swap operation in the last round of the DES."

Side Effects (cont.)

- If the last rounds MixColumns is dropped, our 1-round attack with 1 KP is improved to 2^{16}!
- Other attacks improve as well.
- Hence, the lack of MixColumns in the last round does affect security.
- Note that breaking the symmetry may help against slide attacks.

For more information: See
http://eprint.iacr.org/2010/041.

Questions?

Thank you for your attention.