A New Security Analysis of AES-128

Alex Biryukov and Ivica Nikolić

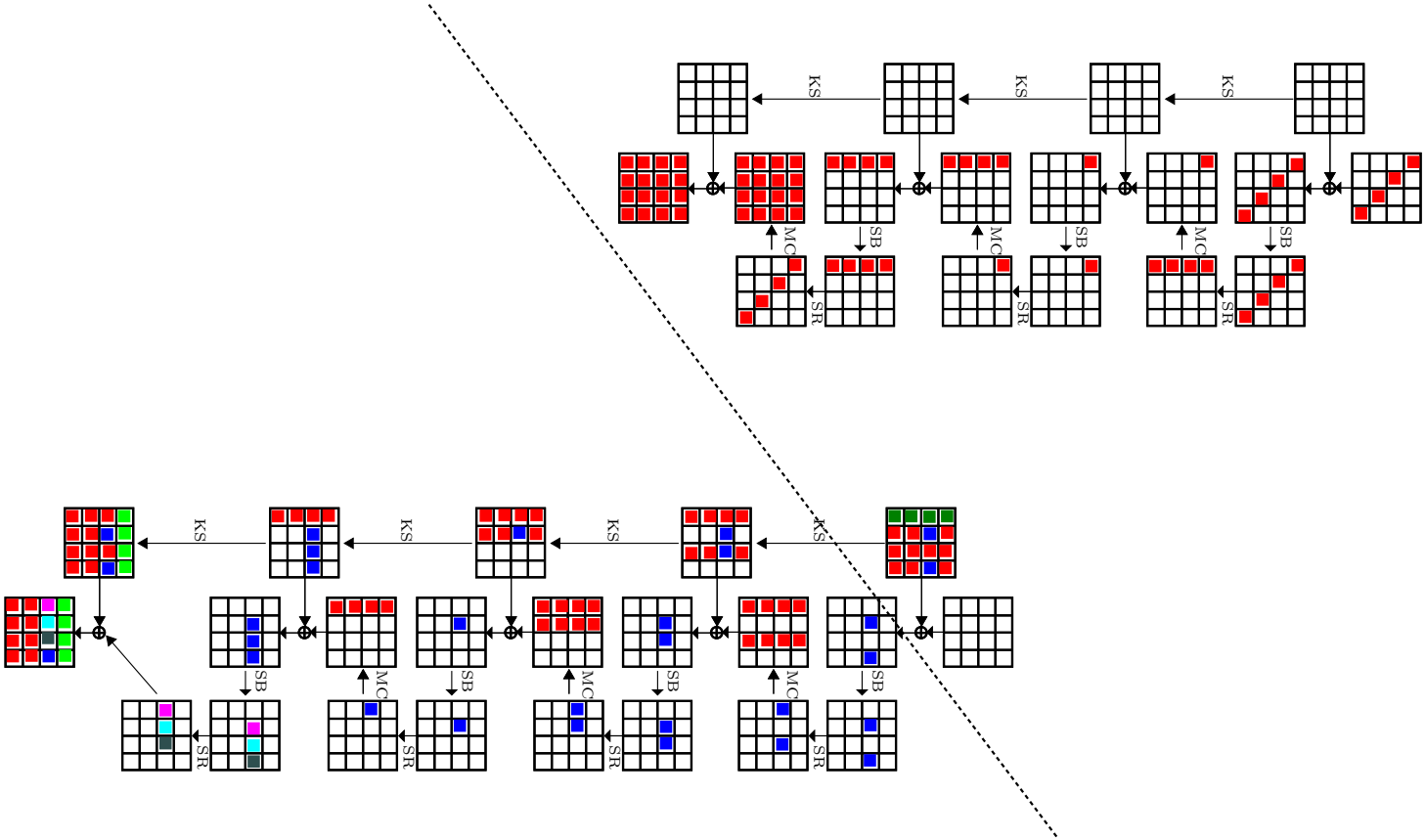
University of Luxembourg

18 Aug 2009

Summary of the Previous Attacks

Attack	Rounds	Data	Workload	Memory
Square attack [DR98]	6	2^{32}	2^{72}	2^{32}
RK-boomerang attack[B04]	6	2^{71}	2^{71}	2^{33}
Collisions [GM00]	7	2^{32}	2^{128}	2^{80}
Partial sum [FKLSSWW00]	7	$2^{128} - 2^{119}$	2^{120}	2^{64}
Known key [KR07]	7	2^{56}	2^{56}	–
Known key [MPRS09]	7	2^{24}	2^{24}	–

Boomerang Attack on AES-128

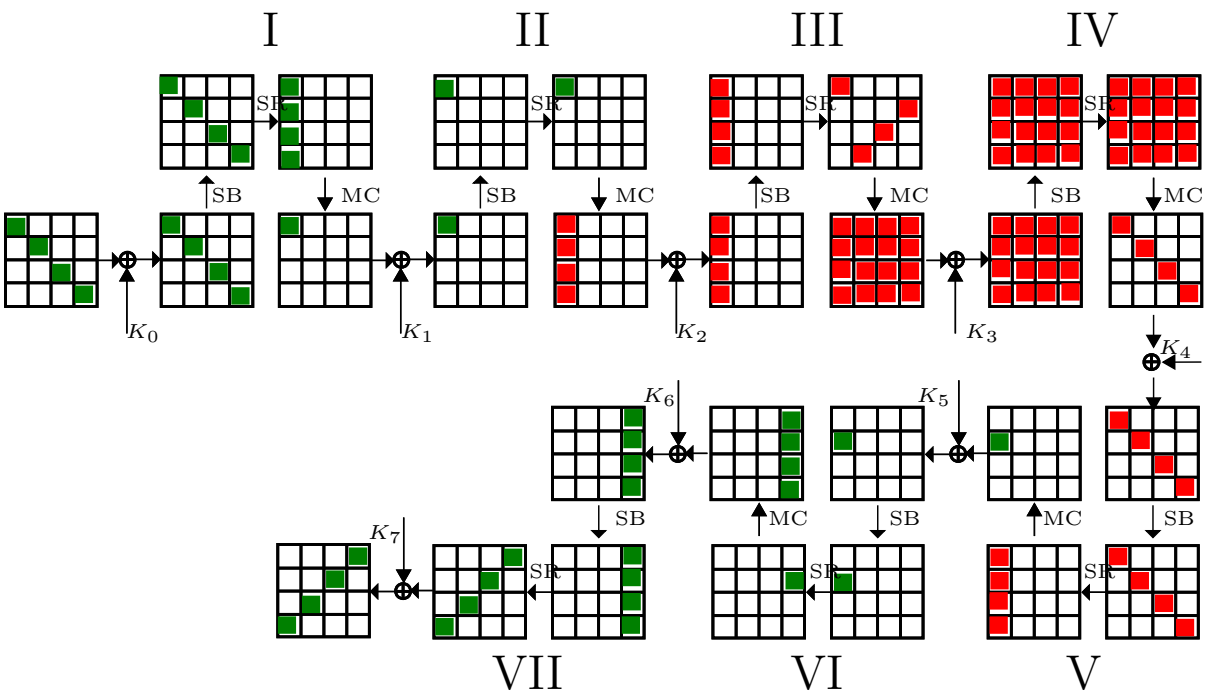


The best attack on 7 rounds of AES-128 in the secret key model

Known Key Distinguisher on AES-128

7-round differential with rebound attack (complexity 2^{44}):

$$4 \to 1 \to 4 \to 16 \to 4 \to 1 \to 4 \to 4$$



Chosen Key Distinguisher on AES-128

Take the 7-round differential and using the key freedom:

- Fix the active S-boxes in one additional round $\Longrightarrow$ improve the complexity of 7-round differential (complexity 2^{22})
- Add one additional full state difference round $\Longrightarrow$ obtain 8-round differential (complexity 2^{44})

$$4 \rightarrow 1 \rightarrow 4 \rightarrow 16 \rightarrow 16 \rightarrow 4 \rightarrow 1 \rightarrow 4 \rightarrow 4$$

This is the first attack on 8-rounds of AES-128 (but it is in the open key model)

Summary of our Attacks

Attack	Rounds	Data	Workload	Memory
RK-boomerang attack	7	2^{97}	2^{97}	2^{35}
Known key disting.	7	2^{44}	2^{44}	–
Chosen key disting.	7	2^{22}	2^{22}	–
Chosen key disting.	8	2^{44}	2^{44}	–

Paper

The paper will appear on e-print soon.