Human-readable Proof of the Related-Key Security of AES-128

Khoongming Khoo[1] Eugene Lee[2]
Thomas Peyrin[3] Siang Meng Sim[1,3]

1. DSO National Laboratories, Singapore
2. Raffles Institution, Singapore
3. Nanyang Technological University, Singapore

FSE 2018, 7 March 2018

Table of Contents

Table of Contents

Block Cipher AES

Advanced Encryption Standard (AES) is a 128-bit block cipher with 3 variants of key size:
128-bit key size — AES-128,
192-bit key size — AES-192,
256-bit key size — AES-256.

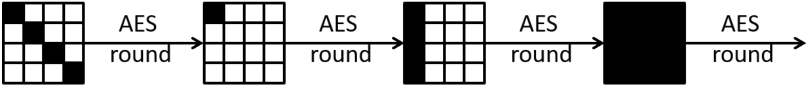
For more than a decade, it has been used world-wide and remains secure.

Block Cipher AES

One of the main features is its 8-bit Sbox with strong differential and linear properties.

Another feature is its simple ShiftRows and MixColumns operations: able to prove a minimum of 25 active Sboxes in 4-round of AES under single-key model.

Together, AES provides strong resistance against classical differential and linear cryptanalysis.



Related-key Model

In related-key model, attacker is allowed to insert differences in both the plaintext and key.

Related-key differential cryptanalysis is much harder to protect against.

AES-192 and AES-256 were shown to be vulnerable to related-key attacks [Biryukov *et al.*, ASIACRYPT 2009. Biryukov *et al.*, CRYPTO 2009].

Related-key Model

Analysing related-key differential is much more complex than single-key model due to the interaction between the differences in the internal state and key schedule.

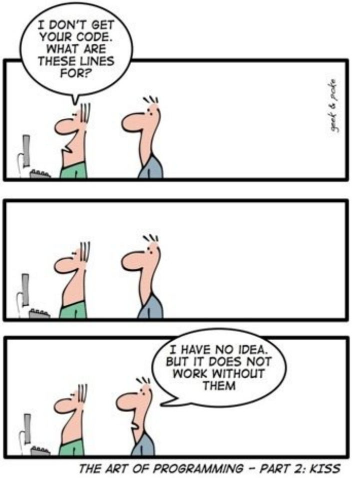
The resistance against differential cryptanalysis is directly related to the number of active Sboxes in the differential trail.

What is the minimum number of active Sboxes in AES−128 in related-key model?

Computer Assisted Tools

Although there are computer assisted tools to check the bounds, such tools have their drawbacks:

- have to review the entire code and trust the implementation,
- no really meaningful information for designers to understand the interactions between key schedule and internal state,
- does not tell us anything about how to design a good key schedule.



Contribution

Present the first human-readable proof on the minimal number of active Sboxes for 1/2/3/4 rounds of AES-128 in related-key model, without external computational help.

From the proof, we gain insight and design a more efficient key schedule with better related-key differential bounds.

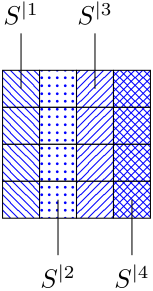
Table of Contents

Initialisation

The 128-bit plaintext is arranged into a 4×4 internal state S, where each cell is a byte.

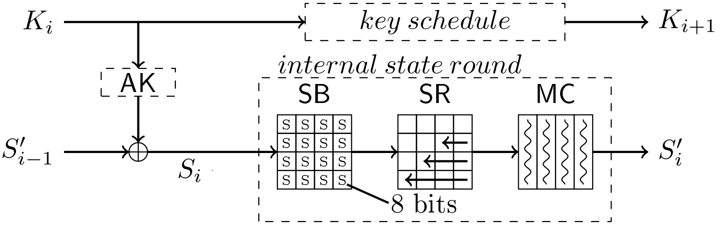
Similarly, the 128-bit key is arranged into a 4×4 key state K.

Notation



Denote $S^{|j}$ the j-th column of the internal state (resp. key state).

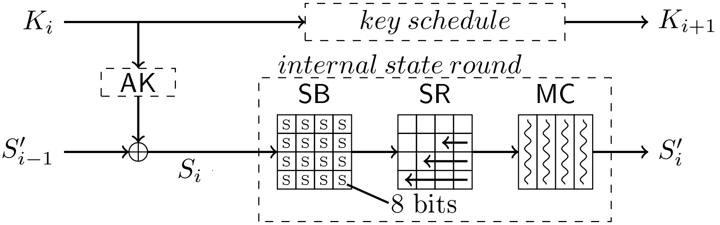
Adding Round Key



At round i,
AddRoundKey(AK) XOR the key state K_i to internal state S'_{i-1} to produce S_i.

The key state K_i is then updated by the key schedule (KS) to get the next key state K_{i+1} for the next round.

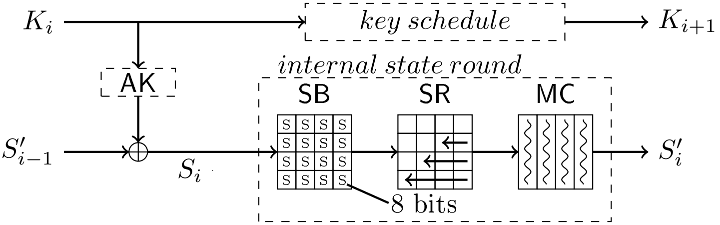
Internal State Round



SubBytes (SB) applies Sbox to each of the 16 bytes in the internal state.

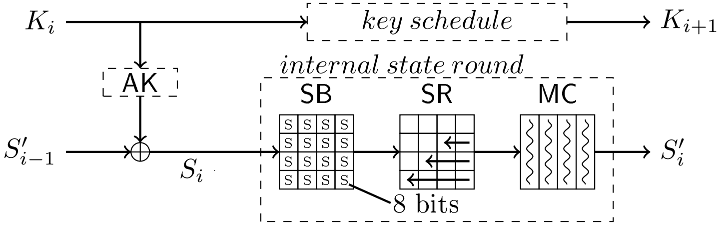
An Sbox is active if the byte in S_i has nonzero difference.

Internal State Round



ShiftRows (SR) rotates r-th row of the internal state by $(r-1)$-bytes to the left.

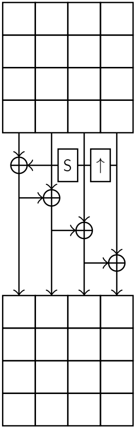
Internal State Round



MixColumns (MC) updates each column through multiplication by an MDS matrix to produce S'_i.

The MDS property ensures that the total number of nonzero differences in a column before and after MC is either 0 (if the column is empty) or at least 5 (if the column is nonzero/active).

Key Schedule



K_i

K_{i+1}

$K_{i+1}^{|1}$ is obtained by
taking the column $K_i^{|4}$,
upward rotating it by 1-byte,
applying Sboxes to every byte,
XORing it with round constant, and
XORing it with $K_i^{|1}$.

For $1 < c \leq 4$, $K_{i+1}^{|c} = K_i^{|c} \oplus K_{i+1}^{|c-1}$.

Table of Contents

Related-key Differential Bounds

Our proved bounds are in line with computer search results.

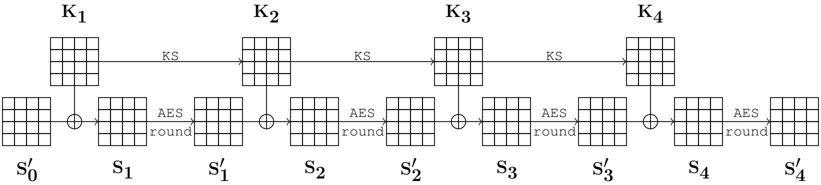
Rounds	**1**	**2**	**3**	**4**
computed-aided bounds (truncated differences)	0	1	3	9
our bounds (truncated differences)	0	1	3	9

Theorem

Any non-null related-key differential path for 4 consecutive rounds of AES−128 contains at least 9 active Sboxes.

The proof involves 11 lemmas, 2 corollaries and it's 15-page long!
In this talk, we present the outline of the proof.

4-round of AES-128



The number of active Sboxes in 4 consecutive rounds of AES-128:

$$N_{SB} = \sum_{x=1}^{4} \left(|S_x| + |K_x^{|4}| \right).$$

Older Version of the Proof

The number of active Sboxes in 4 consecutive rounds of AES-128:

$$N_{SB} = \sum_{x=1}^{4} \left(|S_x| + |K_x^{|4}| \right).$$

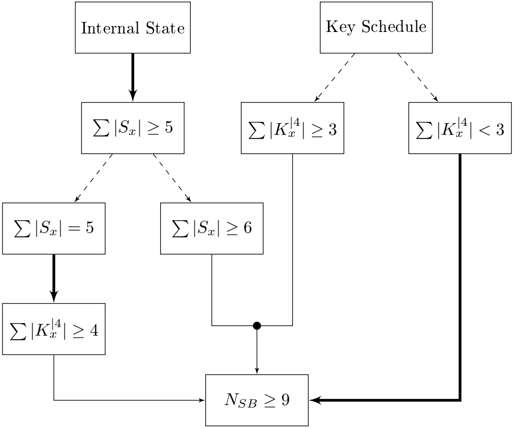
In earlier work, we proved that $\sum_{x=1}^{4} |S_x| \geq 5$.
Thus, if $\sum_{x=1}^{4} |K_x^{|4}| \geq 4$, the theorem is proven.

If $\sum_{x=1}^{4} |K_x^{|4}| < 3$, we can prove that $N_{SB} \geq 9$.

But for $\sum_{x=1}^{4} |K_x^{|4}| = 3$, we only achieve $N_{SB} \geq 8$. (Not tight!)

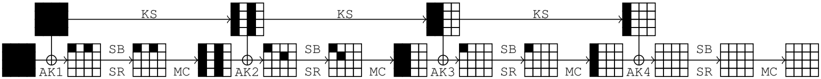
The number of active Sboxes in the internal state and key schedule are closely intertwined.

General Structure of the Proof



Thick arrows represent proven implication, thin arrows represent direct implication and hashed arrows represent subcases.

Tight Bound



The bound $N_{SB} \geq 9$ for 4-round of AES-128 is tight.

The internal state has $(2, 2, 1, 0)$ active Sboxes and $|K_1^{|4}| = 4$.

Table of Contents

New Key Schedule for AES−128

Our proofs provide an insight on the interplay between the internal state function and the key schedule.

From that, we propose a new fully linear key schedule that yields better bounds on the number of active Sboxes.

New Key Schedule for AES-128

Our new key schedule proposal is simple: it is basically a permutation on the key state byte positions. More precisely, the key state update function will simply:

- rotate by $(1, 0, 0, 2)$-byte positions to the right for $(1, 2, 3, 4)$-th row of the key state,
- rotate the entire key state by one position down.

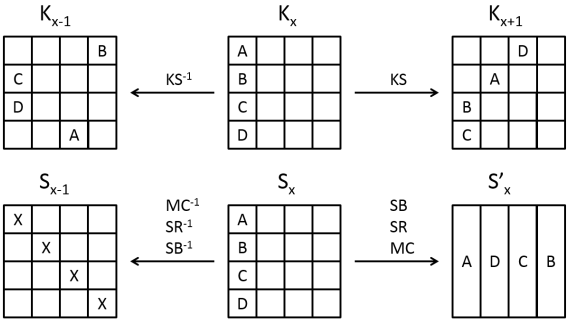
$$\begin{pmatrix} 0 & 4 & 8 & 12 \\ 1 & 5 & 9 & 13 \\ 2 & 6 & 10 & 14 \\ 3 & 7 & 11 & 15 \end{pmatrix} \longrightarrow \begin{pmatrix} 11 & 15 & 3 & 7 \\ 12 & 0 & 4 & 8 \\ 1 & 5 & 9 & 13 \\ 2 & 6 & 10 & 14 \end{pmatrix}$$

Design Rationale

- Efficient and easy to implement (no XOR or Sbox).
- No XOR, prevent manipulation of the number of active bytes in key state to match the internal state.
- Cycle of 16, every byte visits all the positions.
- Avoid overlapping and cancelling of active bytes in the internal state by the key state.

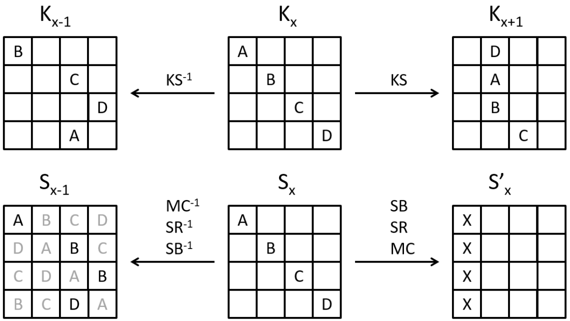
Design Rationale (Column)

If the difference comes from the key, it will not be cancelled in the previous or next round.



Design Rationale (Diagonal)

Similarly for the diagonal.



Observation

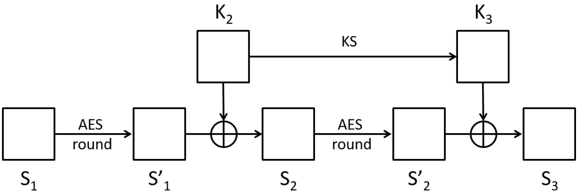
If the difference comes from the key, there is at least 6 active Sboxes in the previous/next two consecutive rounds.

Table of Contents

3 Rounds of AES with New Key Schedule

Recall that 3 rounds of AES-128 has at least 3 active Sboxes.

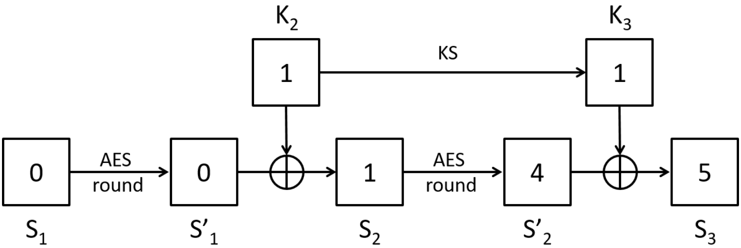
With the new key schedule, we can easily achieve more than 3 active Sboxes.



The number of active Sboxes in 3 consecutive rounds:

$$N_{SB} = \sum_{x=1}^{3} |S_x|.$$

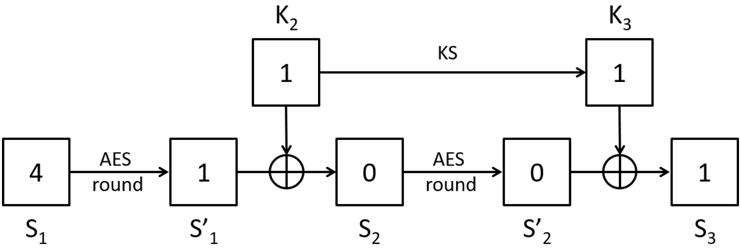
Subcase: $|S_1| = 0$



The difference in S_2 comes from K_2.

From the earlier observation, there are at least 6 active Sboxes.

Subcase: $|S_2| = 0$

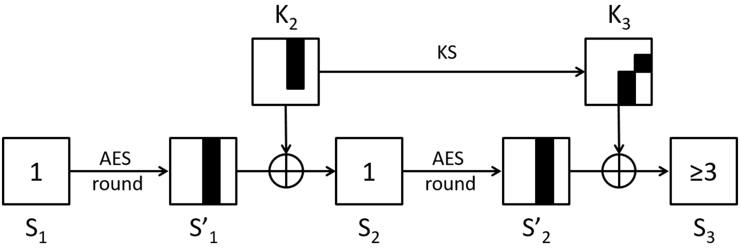


The difference in S_1' (resp. S_3) comes from K_2 (resp. K_3).

As there is no XOR in the key schedule, $|K_2| = |K_3|$.

$$|S_1| + |S_3| = |M^{-1}(S_1')| + |S_3| \geq 5.$$

Subcase: $|S_1| = |S_2| = 1$



For $|S_2| = 1$, there must be at least 3 active bytes in some column of K_2. Since at least one of these 3 active bytes will move to a different column in K_3, we have $|S_3| \geq 3$.

$$\therefore \sum_{x=1}^{3} |S_x| \geq 5.$$

Related-key Differential Bounds

Rounds	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
AES-128 key schedule (truncated differences)	0	1	3	9	11	13	15	21
our new key schedule (truncated differences)	0	1	5	10	14	18	21	25

Our candidate has better bounds than original AES even without using Sboxes in the KS.

Tweaking the New Key Schedule

Add a row of Sboxes in the KS:

- every active byte undergoes an Sbox every 4 rounds,
- easy to count the number of active Sboxes, directly adds to the bounds.

Dilemma for the attacker:

- low number of active bytes in KS will have low chance of cancelling the differences in the internal state,
- high number of active bytes in KS cannot be reduced because there is no XOR and no possible cancellation.

Table of Contents

Conclusion

- Present first human-readable proof on related-key security of AES-128.
- Prove that the minimum number of active Sboxes for 1/2/3/4 consecutive rounds of AES-128 under related-key model is 0/1/3/9.
- Propose a new key schedule that is more efficient and provide higher bounds.

Thank you. :)