Feasible Attack on the 13-round AES-256

Alex Biryukov and Dmitry Khovratovich

University of Luxembourg

alex.biryukov@uni.lu, dmitry.khovratovich@uni.lu

Abstract. In this note we present the first attack with feasible complexity on the 13-round AES-256. The attack runs in the related-subkey scenario with four related keys, in 2^{76} time, data, and memory.

1 Introduction

The year 2009 saw significant improvements in the cryptanalysis of Advanced Encryption Standard. The following results were presented: practical distinguisher for AES-256 in the chosen-key model[3], boomerang attacks on the full-round AES-192 and AES-256 [2], practical complexity attacks on AES-256 with up to 10 rounds [1].

In this paper we consider related-key boomerang attacks in the secret-key model and exploit the related-key weaknesses in AES, that were extensively described in previous works.

We advance to the following results. First, we provide the first attack on a 13-round AES-256 with complexity feasible in the real world. The best feasible attack so far was given on a 10-round version and hypothesized on a 11-round version. Our attack has 2^{76} time and data complexity, which is also significantly lower than $2^{99.5}$ complexity of the attack on the full 14-round AES-256.

Attack	Rounds	# keys	Data	Time	Memory	Source
Partial sums	9	256	2^{85}	2^{226}	2^{32}	[4]
Related-key differential	10	2	2^{44}	2^{45}	2^{33}	[1]
Related-key differential	11	2	2^{70}	2^{70}	2^{33}	[1]
Related-key boomerang	13	4	2^{76}	2^{76}	2^{76}	This paper
Related-key differential	14	2^{35}	2^{131}	2^{131}	2^{65}	[3]
Related-key boomerang	14	4	$2^{99.5}$	$2^{99.5}$	2^{77}	[2]

Table 1. Best attacks on AES-256 in the secret-key model.

2 Attack on AES-256

In this section we present a related key boomerang attack on AES-256.

2.1 The trail

The boomerang trail is depicted in Figure 2, and the actual values are listed in Tables 3 and 2. It consists of two subtrails: the first one covers rounds 1–8, and the second one covers rounds 8–13. The switching state is the state A^8 (internal state after the SubBytes in round 8) and a special key state K_S, which is the concatenation of the last four columns of K^4 and the first four columns of K^5. Although there is an active S-box in the first round of the key schedule, we do not impose conditions on it. As a result, the difference in column 0 of K^0 is partly unknown.

Related keys We define the relation between four keys as follows (see Figure 1 for the illustration). For a secret key K_A, which the attacker tries to find, compute its second subkey K_A^1 and apply the difference ΔK^1 to get a subkey K_B^1, from which the key K_B is computed. The switch into the keys K_C, K_D happens between the 3rd and the 4th subkeys in order to minimize the number of active S-boxes in the key-schedule using the *Ladder switch* idea described above. We compute subkeys K^3 and K^4 for both K_A and K_B. We add the difference ∇K^3 to K_A^3 and compute the upper half (four columns) of K_C^3. Then we add the difference ∇K^4 to K_A^4 and compute the lower half (four columns) of K_C^4. From these eight consecutive columns we compute the full K_C. The key K_D is computed from K_B in the same way.

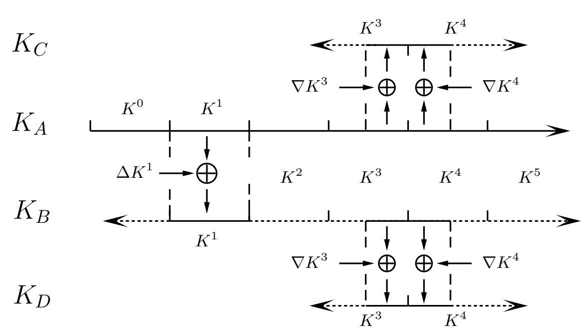


Fig. 1. Computing K_B, K_C, and K_D from K_A.

Finally, we point out that difference between K_C and K_D can be computed in the backward direction deterministically since we apply the *Feistel trick*. The secret key K_A, and the three keys K_B, K_C, K_D computed from K_A as described above form a proper related key quartet. Moreover, due to a slow diffusion in the backward direction, as a bonus we can compute some values in ∇K^i even for $i = 0, 1, 2, 3$ (Table 2). Hence given the byte value $k^l_{i,j}$ for K_A we can partly compute K_B, K_C and K_D.

Internal state The plaintext difference is specified in 7 bytes. We require that all the active S-boxes in the internal state should output the difference `0x1f` so that the active S-boxes are passed with probability 2^{-6}. The only exception is the first round where the input differences in four of seven active bytes are not specified.

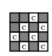
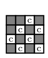
Let us start a boomerang attack with a random pair of plaintexts that fit the trail after two rounds. Active S-boxes in rounds 3–7 are passed with probability 2^{-6} each so the overall probability is 2^{-18}.

We switch the internal state in round 8 with the *Ladder switch* technique: the row 1 is switched before the application of S-boxes, and the other rows are switched after the S-box layer. As a result, we do not pay for the active S-boxes at all in this round.

The second part of the boomerang trail is quite simple. Three S-boxes in rounds 10–13 contribute to the probability, which is thus equal to 2^{-18}. Finally, a right pair after the second round produces a boomerang quartet with probability $2^{-18-18-18-18} = 2^{-72}$.

2.2 The attack

Repeat the following steps four times.

1. Prepare a structure of 2^{72} plaintexts each  .
2. Encrypt it on keys K_A and K_B and keep the resulting sets S_A and S_B in memory.
3. XOR Δ_C to all the ciphertexts in S_A and decrypt the resulting ciphertexts with K_C. Denote the new set of plaintexts by S_C.
4. Repeat previous step for the set S_B and the key K_D. Denote the set of plaintexts by S_D.
5. Compose from S_C and S_D all the possible pairs of plaintexts which are equal in 56 bits  .
6. For every remaining pair check if the difference in $p_{0,0}$ is equal on both sides of the boomerang quartet (8-bit filter). Note that $\nabla k^0_{1,7} = 0$ so $\Delta k^0_{0,0}$ should be equal for both key pairs (K_A, K_B) and (K_C, K_D).
7. For every remaining quartet try all 2^{28} values for ΔB^1 (2^{14} for each related-key pair):
   - Compute both ΔA^1. Check if ΔA^1 is admissible for ΔP (one-bit condition for each of 16 positions).

– Given ΔA^1 and ΔP, every plaintext row i proposes two candidates for each of the two key bytes in both related-key pairs. Since the ∇ difference is equal in all the row bytes, this is an 8-bit equation on the key bytes. Therefore, this is a 4-bit filter for each row, or a 16-bit filter in total. As a result, we get a four-bit filter on the quartets and leave with the only possible combination of ΔB^1.

8. Each remaining quartet proposes an 8-byte key candidate for K_A and, independently, a 4-byte key candidate for K_C.

Finally, choose the key candidate that is proposed by four quartets.

Each structure has all possible values in 9 bytes, and constant values in the other bytes. Of 2^{72} texts per structure we can compose 2^{144} ordered pairs. Of these pairs $2^{144-8\cdot 9} = 2^{72}$ pass the first round. Thus we expect one right quartet per structure, or four right quartets in total.

Let us compute the number of candidate quartets. We can compose 2^{146} quartets from the initial structures, of which 2^{80} quartets come out of step 6. Then we apply a 4-bit filter so that there remains 2^{76} candidates, each proposing a 12-byte key candidate. It is highly likely that only the right quartets propose the same candidate. We also point out, that each quartet propose two candidates for $k^0_{1,7}$, which defines $\Delta p_{0,0}$. The most time-consuming filtering part is the processing of 2^{80} candidate quartets, which is equivalent to about 2^{74} AES encryptions.

Therefore, we recover 71 key bits with 2^{74} chosen plaintexts and ciphertexts, and time equivalent to 2^{76} encryptions. The remaining key bits can be found using our partial knowledge of the key and using slightly different key relations.

References

1. Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds, available at `http://eprint.iacr.org/2009/374.pdf`. In *EUROCRYPT'10, to appear*, 2010.
2. Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In *ASIACRYPT'09*, volume 5912 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2009.
3. Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolić. Distinguisher and related-key attack on the full AES-256. In *CRYPTO'09*, volume 5677 of *LNCS*, pages 231–249. Springer, 2009.
4. Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In *FSE'00*, volume 1978 of *LNCS*, pages 213–230. Springer, 2000.

ΔK^i					
0	? 00 00 00 3e 3e 3e 3e ? 01 01 01 ? 1f 1f 1f ? 00 00 00 1f 1f 1f 1f ? 00 00 00 21 21 21 21	1	00 00 00 00 3e 00 3e 00 00 01 00 01 1f 00 1f 00 00 00 00 00 1f 00 1f 00 00 00 00 00 21 00 21 00	2	00 00 00 00 3e 3e 00 00 00 01 01 00 1f 1f 00 00 00 00 00 00 1f 1f 00 00 00 00 00 00 21 21 00 00
3	00 00 00 00 3e 00 00 00 00 01 00 00 1f 00 00 00 00 00 00 00 1f 00 00 00 00 00 00 00 21 00 00 00	4	01 01 01 01 ? ? ? ? 00 00 00 00 1f 1f 1f 1f 00 00 00 00 1f 1f 1f 1f 00 00 00 00 21 21 21 21		

∇K^i					
0	X X X X ? ? ? 00 Y Y Y Y 01 01 01 00 Z Z Z Z 01 01 01 00 T T T T 03 03 03 00	1	X ab X 00 ? ? 00 00 Y 00 Y 00 01 01 00 00 Z 00 Z 00 01 01 00 00 T 00 T 00 03 03 00 00	2	X X 00 00 ? 00 00 00 Y Y 00 00 01 00 00 00 Z Z 00 00 01 00 00 00 T T 00 00 03 00 00 00
3	X ab ab ab 02 02 02 02 Y 00 00 00 01 01 01 01 Z 00 00 00 01 01 01 01 T 00 00 00 03 03 03 03	4	ab 00 ab 00 02 00 02 00 00 00 00 00 01 00 01 00 00 00 00 00 01 00 01 00 00 00 00 00 03 00 03 00	5	ab ab 00 00 02 02 00 00 00 00 00 00 01 01 00 00 00 00 00 00 01 01 00 00 00 00 00 00 03 03 00 00
6	ab 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00	7	ab ab ab ab ? ? ? ? 00 00 00 00 01 01 01 01 00 00 00 00 01 01 01 01 00 00 00 00 03 03 03 03		

Table 2. Subkey difference in the 13-round trail.

ΔP	? ? 3e ? ? 1f ? 1f 1f ? 1f ? ? 21 ? 21	ΔA^1	00 ? 00 ? ? 00 ? 00 00 ? 00 ? ? 00 ? 00	ΔA^2	00 00 00 00 00 1f 00 1f 00 00 00 00 00 00 00 00	ΔA^3 ΔA^5 ΔA^7	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
ΔA^4	00 00 00 00 00 1f 1f 00 00 00 00 00 00 00 00 00	ΔA^6	00 00 00 00 00 1f 00 00 00 00 00 00 00 00 00 00	ΔA^8	00 00 00 00 00 ? ? ? 00 00 00 00 00 00 00 00	∇A^9 ∇A^{11} ∇A^{13}	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
∇A^8	01 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00	∇A^{10}	01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00	∇A^{12}	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ΔC	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Table 3. Internal state difference in the 13-round trail.

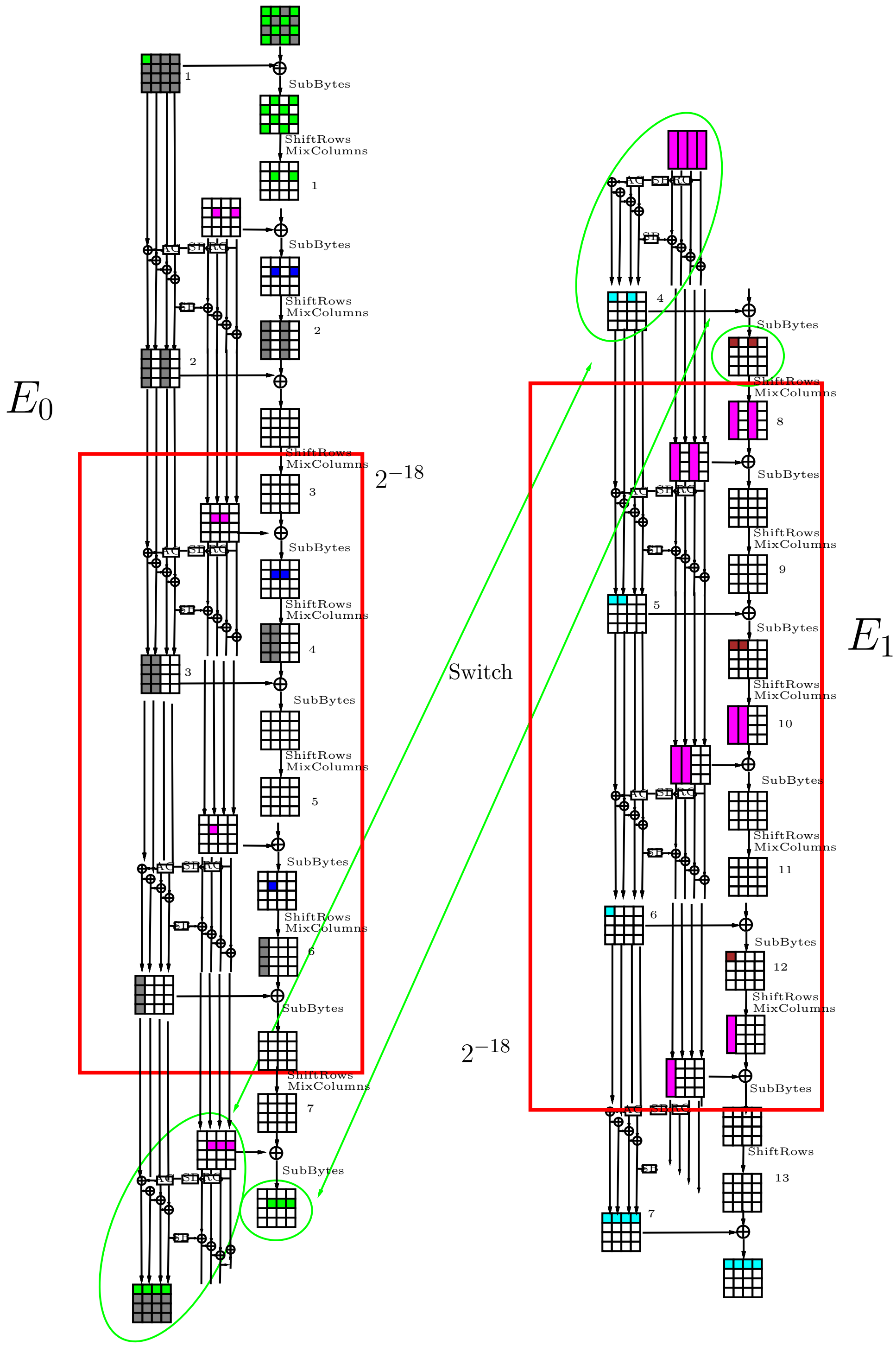


Fig. 2. AES-256 E_0 and E_1 trails. Green ovals show an overlap between the two trails where the switch happens.