Examples of differential multicollisions for 13 and 14 rounds of AES-256

Alex Biryukov, Dmitry Khovratovich, Ivica Nikolić

University of Luxembourg

{alex.biryukov, dmitry.khovratovich, ivica.nikolic@uni.lu}

Here we present practical differential q-multicollisions for AES-256. In our paper [1] q-multicollisions are found with complexity $q \cdot 2^{67}$. We relax conditions on the plaintext difference Δ_P allowing some bytes to vary and find multicollisions for 13 and 14 round AES with complexity $q \cdot 2^{37}$. Even with the relaxation there is still a large complexity gap between our algorithm and the lower bound that we have proved in Lemma 1. Moreover we believe that in practice finding even two fixed-difference collisions for a good cipher would be very challenging.

The multicollision sets, presented in the tables below, are obtained using the technique described in our original paper. Our search algorithm for 13 and 14 rounds of AES-256 can be described as:

1. Build a differential trail for 14 rounds of AES-256. The trail specifies the admissible values of the active S-boxes in these rounds.
2. Using the triangulation algorithm produce one pair that satisfies all the conditions for the S-boxes in the rounds 3–7.
3. If this pair satisfies the conditions for the rounds 8-14 as well then goto step 4; else go to step 2.
4. Decrypt the pair through one round and print the 13 round example (decrypt the pair through two rounds and print the 14 round example).

Note that, since we use our triangulation algorithm, the S-boxes active in the rounds 3–7 do not increase the complexity of the search, because we always fix the right (admissible) values for them. Hence, the complexity of the above algorithm is fully determined only by the number of active S-boxes in the rounds 8-14 plus one active S-box in the key schedule in round 6 that our triangulation algorithm does not cover. Therefore, we have in total 6 active S-boxes. Five of these hold with probability 2^{-6} and one with probability 2^{-7}, hence the total complexity for finding one collision is 2^{37} executions of step 2. Since S-boxes get admissible values in rounds 3–14, the remaining one (two) rounds in the beginning can add only two bytes (eight bytes) variation to the difference, i.e. the rest of the bytes will still have the pre-fixed differences.

Our lower bound from Lemma 1 suggests that for 13 rounds of AES-256 one would expect to find this type of differential 5-multicollision, with fixed input difference in 14 bytes of the plaintext, and fixed output difference in the ciphertext, with complexity $2^{\frac{4 \cdot 112}{6}} = 2^{74.6}$ computations. Our search algorithm finds this multicollision set with $5 \cdot 2^{37}$ computations. For 14 rounds, with half of the plaintext difference fixed, and fully fixed difference in the ciphertext, the generic search would find differential 10-multicollisions with complexity $2^{\frac{9 \cdot 64}{11}} = 2^{52.3}$. Our algorithm finds this set with $10 \cdot 2^{37}$ computations.

The estimates for the generic multicollision search are given as lower bounds. Since we have highly structured and *fixed* differences in the plaintext and in the ciphertext, we expect that in practice finding each extra collision would cost about 2^{112} and 2^{64} time for 13 and 14 rounds of AES-256, respectively.

References

1. Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolić. Distinguisher and related-key attack on the full AES-256. In Shai Halevi, editor, *CRYPTO*, LNCS. Springer, 2009. to appear.

Table 1. Differential 5-multicollisions for 13 rounds of AES-256. The last row is the ciphertext difference for all of the five pairs.

$K_1 \oplus K_2$	0f070709 0e070709 0f070709 0e070709		
	371f1f21 00000000 371f1f21 00000000		
K_1	254a6373 cf362573 ef2cb535 6ae8f43a	K_2	2a4d647a c131227a e02bb23c 64eff333
	16a9ba79 a2c2fbed 7f00a01f 48ab1441		21b6a558 a2c2fbed 481fbf3e 48ab1441
P_1	243bc292 18fa5782 60236961 b3ec7d58	P_2	8724ddb3 18fa5782 793c7640 b3ec7d58
$P_1 \oplus P_2$	a3**1f1f21 00000000** 19**1f1f21 00000000**		
K_1	d6da793c adeb288e 7f8f4e9c f7f65854	K_2	d9dd7e35 a3ec2f87 70884995 f9f15f5d
	e4b93772 20fe8ecb 2491682d 1327930e		d3a62853 20fe8ecb 138e770c 1327930e
P_1	24159557 e524934a 1afebe7c 8acb180d	P_2	1e0a8a76 e524934a c1e1a15d 8acb180d
$P_1 \oplus P_2$	3a**1f1f21 00000000** db**1f1f21 00000000**		
K_1	e22f0568 1857d06d 2170bf42 dcef9e97	K_2	ed280261 1650d764 2e77b84b d2e8999e
	da3a3459 b8604fd7 a473efd7 939e628e		ed252b78 b8604fd7 936cf0f6 939e628e
P_1	93677864 20116bd1 e6889a49 9a0c3eaf	P_2	80786745 20116bd1 98978568 9a0c3eaf
$P_1 \oplus P_2$	13**1f1f21 00000000** 7e**1f1f21 00000000**		
K_1	1e16a0ac 0e8ccaeb f463fc3b 491381ed	K_2	1111a7a5 008bcde2 fb64fb32 471486e4
	3ad4dc1e ad3a6411 ef88c1d3 d81dc7a7		0dcbc33f ad3a6411 d897def2 d81dc7a7
P_1	8ff62851 a9a1784f f8f19558 f9de3c58	P_2	72e93770 a9a1784f feee8a79 f9de3c58
$P_1 \oplus P_2$	fd**1f1f21 00000000** 06**1f1f21 00000000**		
K_1	b35f91b2 450d32a0 074d95e5 260b39a8	K_2	bc5896bb 4b0a35a9 084a92ec 280c3ea1
	05fc10ec 1b5b7eea 4f504523 78bd9286		32e30fcd 1b5b7eea 784f5a02 78bd9286
P_1	78f7ad2f 5d12c822 71aaa425 538b0264	P_2	d3e8b20e 5d12c822 aab5bb04 538b0264
$P_1 \oplus P_2$	ab**1f1f21 00000000** db**1f1f21 00000000**		
$C_1 \oplus C_2$	01000000 01000000 01000000 01000000		

Table 2. Differential 10-multicollisions for 14 rounds of AES-256. The last row is the ciphertext difference for all of the ten pairs.

$K_1 \oplus K_2$	0f070709 0e070709 0f070709 0e070709		
	371f1f21 00000000 371f1f21 00000000		
K_1	254a6373 cf362573 ef2cb535 6ae8f43a	K_2	2a4d647a c131227a e02bb23c 64eff333
	16a9ba79 a2c2fbed 7f00a01f 48ab1441		21b6a558 a2c2fbed 481fbf3e 48ab1441
P_1	9b8ca2db 05ce0c9e 5f35ff8f 04791935	P_2	938bc4d2 0b6f0bb1 a0320686 0a881e85
$P_1 \oplus P_2$	08**07**66**09** **0e**a1**07**2f ff**07**f9**09** **0e**f1**07**b0		
K_1	dbbfaeb4 92388b3b 3708603d 1b0306c4	K_2	d4b8a9bd 9c3f8c32 380f6734 150401cd
	29f481aa 12c21882 d708dd52 e0b13282		1eeb9e8b 12c21882 e017c273 e0b13282
P_1	487a8f40 6e0356de 41da0ba3 3bc3c514	P_2	457d5e49 60ae51d0 15dd73aa 3524c25d
$P_1 \oplus P_2$	0d**07**d1**09** **0e**ad**07**0e 54**07**78**09** **0e**e7**07**49		
K_1	d6da793c adeb288e 7f8f4e9c f7f65854	K_2	d9dd7e35 a3ec2f87 70884995 f9f15f5d
	e4b93772 20fe8ecb 2491682d 1327930e		d3a62853 20fe8ecb 138e770c 1327930e
P_1	094bb6f6 a759cecf d41a31fd 319323c3	P_2	024c8aff a96ec91b 711dbcf4 3f2c2440
$P_1 \oplus P_2$	0b**07**3c**09** **0e**37**07**d4 a5**07**8d**09** **0e**bf**07**83		
K_1	e22f0568 1857d06d 2170bf42 dcef9e97	K_2	ed280261 1650d764 2e77b84b d2e8999e
	da3a3459 b8604fd7 a473efd7 939e628e		ed252b78 b8604fd7 936cf0f6 939e628e
P_1	5d7c9ca8 082f0f55 5f725130 f4666e5d	P_2	227b43a1 066b084f d6751039 fab9694e
$P_1 \oplus P_2$	7f**07**df**09** **0e**44**07**1a 89**07**41**09** **0e**df**07**13		
K_1	1e16a0ac 0e8ccaeb f463fc3b 491381ed	K_2	1111a7a5 008bcde2 fb64fb32 471486e4
	3ad4dc1e ad3a6411 ef88c1d3 d81dc7a7		0dcbc33f ad3a6411 d897def2 d81dc7a7
P_1	13e096fd 8fef8da5 979b2ccd 043cf04a	P_2	35e702f4 81368a9a e09c9bc4 0ac2f796
$P_1 \oplus P_2$	26**07**94**09** **0e**d9**07**3f 77**07**b7**09** **0e**fe**07**dc		
K_1	32bc86d4 69a1d814 766610ef 215a5a7b	K_2	3dbb81dd 67a6df1d 796117e6 2f5d5d72
	4d7933db eb334b0d ffa980c1 c888c7e3		7a662cfa eb334b0d c8b69fe0 c888c7e3
P_1	f2116489 3e44f43b 427d0b82 106e1616	P_2	c7164580 3089f3d7 787af28b 1ef4116a
$P_1 \oplus P_2$	35**07**21**09** **0e**cd**07**ec 3a**07**f9**09** **0e**9a**07**7c		
K_1	23af02e1 65dfae34 801e5598 c9d84572	K_2	2ca805e8 6bd8a93d 8f195291 c7df427b
	af15ae93 addc102d b985215d 8e2bbf62		980ab1b2 addc102d 8e9a3e7c 8e2bbf62
P_1	839adb14 fc39a4ef dd8b5835 d4055b3f	P_2	c79dde1d f2faa32e ec8cc93c da545cd7
$P_1 \oplus P_2$	44**07**05**09** **0e**c3**07**c1 31**07**91**09** **0e**51**07**e8		
K_1	66e16f1a fd4d0e90 db7d4985 bad4284f	K_2	69e66813 f34a0999 d47a4e8c b4d32f46
	caf7d6f6 19a1bc7e 467ef193 711e1300		fde8c9d7 19a1bc7e 7161eeb2 711e1300
P_1	2d310d6f a2a409cf e9f6f074 5167426f	P_2	2e360666 acd10eed 5ff1607d 5f3345e3
$P_1 \oplus P_2$	03**07**0b**09** **0e**75**07**22 b6**07**90**09** **0e**54**07**8c		
K_1	0b18834e 0810e179 4ef0d554 9b06ebfb	K_2	041f8447 0617e670 41f7d25d 9501ecf2
	73ee203f 98fd948a 53905aa3 647b6cc4		44f13f1e 98fd948a 648f4582 647b6cc4
P_1	c3738f78 9484d719 1180bb6e 9def69b4	P_2	cb74b471 9a94d017 5687fb67 93c26efa
$P_1 \oplus P_2$	08**07**3b**09** **0e**10**07**0e 47**07**40**09** **0e**2d**07**4e		
K_1	b35f91b2 450d32a0 074d95e5 260b39a8	K_2	bc5896bb 4b0a35a9 084a92ec 280c3ea1
	05fc10ec 1b5b7eea 4f504523 78bd9286		32e30fcd 1b5b7eea 784f5a02 78bd9286
P_1	6bca5047 12085de9 89a72bff f959571f	P_2	57cdf34e 1ca85a7a 30a0e7f6 f7fc50b3
$P_1 \oplus P_2$	3c**07**a3**09** **0e**a0**07**93 b9**07**cc**09** **0e**a5**07**ac		
$C_1 \oplus C_2$	01000000 01000000 01000000 01000000		

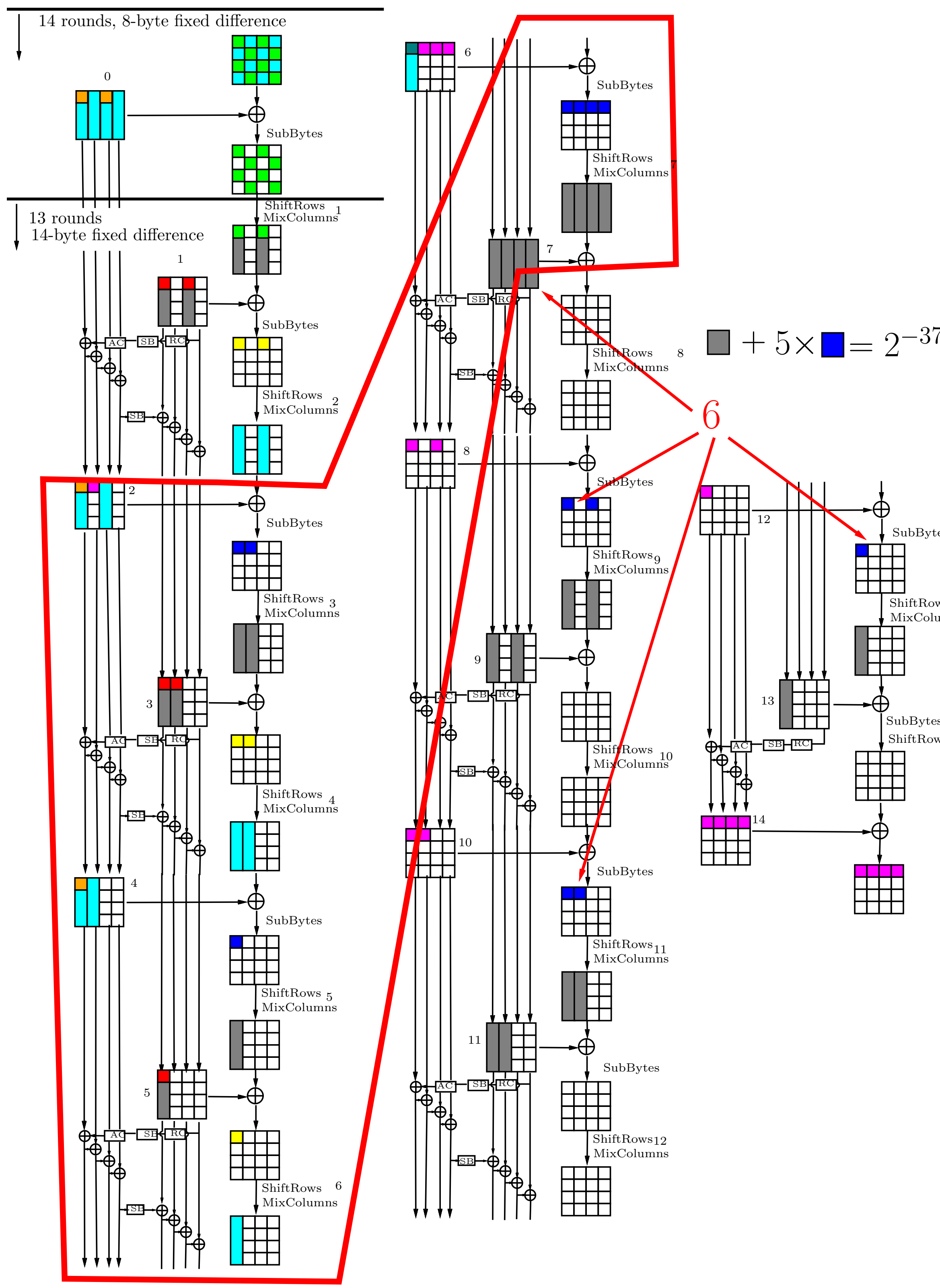

Fig. 1. Multicollision trail. Green bytes denote arbitrary differences, the other colors denote fixed differences.