88-XOR Implementation of the AES MixColumns Matrix

Jérémy Jean

ANSSI, Paris, France

Jeremy.Jean@ssi.gouv.fr

We give in this short note a circuit implementing the matrix-vector product with the 32x32 binary matrix of the AES MixColumns using 88 XOR gates. Previously known circuits minimizing this metric have been published in the past years and achieved 94 XOR in [TP19], 92 XOR in [Max19], 91 XOR in [LXZZ21], and 89 XOR in [SYL25]. As far as we can tell, a circuit with 88 XOR was previously unknown.

Acknowledgements. This result has been found with the help of AI, most specifically models from OpenAI under codex.

References

[LXZZ21] Da Lin, Zejun Xiang, Xiangyong Zeng, and Shasha Zhang. A framework to optimize implementations of matrices. In Kenneth G. Paterson, editor, *Topics in Cryptology – CT-RSA 2021*, pages 609–632, Cham, 2021. Springer International Publishing.

[Max19] Alexander Maximov. AES MixColumn with 92 XOR gates. Cryptology ePrint Archive, Paper 2019/833, 2019.

[SYL25] Yao Sun, Runhe Yang, and Ting Li. Revisit the boyar-peralta algorithm to solve the shortest linear program problem. Cryptology ePrint Archive, Paper 2025/1493, 2025.

[TP19] Quan Quan Tan and Thomas Peyrin. Improved heuristics for short linear programs. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020(1):203–230, Nov. 2019.

Algorithm 1 An 88-XOR circuit for the AES MixColumns

Inputs: A 32-bit vector $x = (x_0, x_1, \ldots, x_{31})$
Outputs: A 32-bit vector $y = (y_0, y_1, \ldots, y_{31})$

1: $t_0 \leftarrow x_7 \oplus x_{23}$
2: $t_1 \leftarrow x_{15} \oplus x_{23}$
3: $t_2 \leftarrow x_7 \oplus x_{31}$
4: $t_3 \leftarrow x_0 \oplus t_1$
5: $t_4 \leftarrow x_{16} \oplus x_{24}$
6: $t_5 \leftarrow t_4 \oplus t_0$
7: $y_8 \leftarrow t_4 \oplus t_3$
8: $t_6 \leftarrow x_8 \oplus t_5$
9: $t_7 \leftarrow t_6 \oplus y_8$
10: $y_0 \leftarrow t_6 \oplus t_1$
11: $t_8 \leftarrow x_{16} \oplus t_2$
12: $t_9 \leftarrow y_0 \oplus t_8$
13: $y_{16} \leftarrow t_3 \oplus t_9$
14: $y_{24} \leftarrow t_5 \oplus y_{16}$
15: $t_{10} \leftarrow x_1 \oplus x_9$
16: $t_{11} \leftarrow x_9 \oplus x_{17}$
17: $t_{12} \leftarrow x_{25} \oplus t_{10}$
18: $t_{13} \leftarrow x_{17} \oplus t_{12}$
19: $t_{14} \leftarrow t_5 \oplus t_2$
20: $y_{17} \leftarrow t_{12} \oplus t_{14}$
21: $t_{15} \leftarrow x_1 \oplus t_7$
22: $y_1 \leftarrow t_{13} \oplus t_{15}$
23: $t_{16} \leftarrow t_9 \oplus t_{11}$
24: $y_9 \leftarrow t_{16} \oplus y_{17}$
25: $y_{25} \leftarrow t_{15} \oplus t_{16}$
26: $t_{17} \leftarrow x_2 \oplus x_{10}$
27: $t_{18} \leftarrow x_{10} \oplus x_{18}$
28: $t_{19} \leftarrow t_{13} \oplus t_{17}$
29: $t_{20} \leftarrow x_{18} \oplus t_{11}$
30: $t_{21} \leftarrow x_{26} \oplus t_{10}$
31: $t_{22} \leftarrow x_2 \oplus x_{26}$
32: $t_{23} \leftarrow t_{17} \oplus t_0$
33: $y_2 \leftarrow t_{18} \oplus t_{21}$
34: $y_{10} \leftarrow t_{20} \oplus t_{22}$
35: $y_{18} \leftarrow t_{19} \oplus t_{21}$
36: $y_{26} \leftarrow t_{19} \oplus t_{20}$
37: $t_{24} \leftarrow x_{19} \oplus t_1$
38: $t_{25} \leftarrow x_{11} \oplus t_{22}$
39: $t_{26} \leftarrow x_3 \oplus x_{27}$
40: $t_{27} \leftarrow x_{11} \oplus t_{24}$
41: $t_{28} \leftarrow x_3 \oplus x_{19}$
42: $t_{29} \leftarrow t_{18} \oplus t_{26}$
43: $t_{30} \leftarrow t_2 \oplus t_{25}$
44: $t_{31} \leftarrow t_{23} \oplus t_{27}$
45: $y_3 \leftarrow x_{27} \oplus t_{31}$
46: $y_{11} \leftarrow t_{24} \oplus t_{29}$
47: $t_{32} \leftarrow t_{29} \oplus t_{30}$
48: $y_{19} \leftarrow t_{23} \oplus t_{32}$
49: $y_{27} \leftarrow t_{28} \oplus t_{30}$
50: $t_{33} \leftarrow x_{12} \oplus x_{28}$
51: $t_{34} \leftarrow x_{20} \oplus t_{27}$
52: $t_{35} \leftarrow t_{28} \oplus t_0$
53: $t_{36} \leftarrow x_{12} \oplus x_{20}$
54: $t_{37} \leftarrow t_{33} \oplus t_{35}$
55: $t_{38} \leftarrow x_4 \oplus t_2$
56: $t_{39} \leftarrow x_4 \oplus x_{28}$
57: $t_{40} \leftarrow t_{26} \oplus t_{38}$
58: $y_4 \leftarrow t_{34} \oplus t_{37}$
59: $y_{12} \leftarrow t_{39} \oplus t_{34}$
60: $y_{20} \leftarrow t_{37} \oplus t_{40}$
61: $y_{28} \leftarrow t_{36} \oplus t_{40}$
62: $t_{41} \leftarrow x_{13} \oplus x_{29}$
63: $t_{42} \leftarrow x_{21} \oplus t_{39}$
64: $t_{43} \leftarrow x_{21} \oplus x_{29}$
65: $t_{44} \leftarrow x_5 \oplus t_{36}$
66: $t_{45} \leftarrow t_{33} \oplus t_{41}$
67: $t_{46} \leftarrow x_5 \oplus x_{13}$
68: $y_5 \leftarrow t_{42} \oplus t_{45}$
69: $y_{13} \leftarrow t_{43} \oplus t_{44}$
70: $y_{21} \leftarrow t_{44} \oplus t_{45}$
71: $y_{29} \leftarrow t_{42} \oplus t_{46}$
72: $t_{47} \leftarrow x_6 \oplus x_{22}$
73: $t_{48} \leftarrow t_{41} \oplus t_{47}$
74: $t_{49} \leftarrow x_{14} \oplus t_{46}$
75: $t_{50} \leftarrow x_{22} \oplus x_{30}$
76: $t_{51} \leftarrow x_{30} \oplus t_{43}$
77: $t_{52} \leftarrow x_6 \oplus x_{14}$
78: $y_6 \leftarrow t_{49} \oplus t_{50}$
79: $y_{14} \leftarrow t_{48} \oplus t_{51}$
80: $y_{22} \leftarrow t_{51} \oplus t_{52}$
81: $y_{30} \leftarrow t_{48} \oplus t_{49}$
82: $t_{53} \leftarrow x_{15} \oplus t_{50}$
83: $t_{54} \leftarrow x_{31} \oplus t_{52}$
84: $t_{55} \leftarrow t_{47} \oplus t_0$
85: $y_7 \leftarrow t_1 \oplus t_{54}$
86: $y_{15} \leftarrow t_{54} \oplus t_{55}$
87: $y_{23} \leftarrow t_{53} \oplus t_2$
88: $y_{31} \leftarrow t_{53} \oplus t_{55}$
89: **return** y