AES MixColumn with 92 XOR gates

Alexander Maximov

Ericsson Research, Lund, Sweden
alexander.maximov@ericsson.com

Abstract. In this short report we present a short linear program for AES MixColumn with 92 XOR gates and depth 6.

Keywords: AES · MixColumn · Short Linear Program

1 Introduction

The part MixColumn of AES encryption round, applied to the AES state $\{r_{i,j}\}$ for $0 \leq i, j \leq 3$, is the following column-wise matrix multiplication.

$$\begin{bmatrix} r'_{0,j} \\ r'_{1,j} \\ r'_{2,j} \\ r'_{3,j} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} r_{0,j} \\ r_{1,j} \\ r_{2,j} \\ r_{3,j} \end{bmatrix}, 0 \leq j \leq 3.$$

The classical circuit of MixColumn needs 108 2-input XOR gates and can be implemented as follows: for each $0 \leq j \leq 3$ do: $t_0 = r_0 + r_1$, $t_1 = r_1 + r_2$, $t_2 = r_2 + r_3$, $t_3 = r_3 + r_0$, and then $r'_0 = 2t_0 + t_2 + r_1$, $r'_1 = 2t_1 + t_3 + r_2$, $r'_2 = 2t_2 + t_0 + r_3$, $r'_3 = 2t_3 + t_1 + r_0$, where multiplication $2t_i$ is the multiplication by x in the Rijndael field and can be implemented with three 2-input XOR gates.

Previous results. There were several improvements to the classical circuit. In CHES 2017 a new circuit of MixColum with 103 XOR gates was presented in [JMPS17]. Later on, an improved version with 97 gates was given in [KLSW17]. Recently, there was a new paper published on IACR ePrint [EJMY19] where in Appendix F the authors presented MixColumn with 95 gates. A similar result with 95 gates was independently found in the recent paper [BFI19], which is also accepted in the conference IWSEC-2019. In the previous version of this report, we found a circuit with 94 gates, and yet in another recent paper [TP19] a circuit with 94 gates was also found, independently.

Our results. In this updated short report we improve all mentioned previous results and present a short linear program for AES MixColumn with 92 gates and depth 6. At our best knowledge it is the smallest as of today.

2 Results

This work was mainly based on the parts of the algorithm given by Boyar et al [BP10], as well as our own techniques presented in [EM19]. We wrote a search program that combines Boyar's algorithm to compute the shortest distance, and our ideas for metrics and the search tree. In our simulations we used up to 50000 leaves of the search tree with 150 leaves being extended from each leaf.

Surprisingly, we were achieving best results when we tried to *minimize* the Euclidean norm metric. As it was mentioned in [EM19], the norm metric (ν) is not stable. When the norm is maximized, the algorithm tends to accept a gate that reduces distances (δ_i) to targets "unevenly", i.e., it is a greedy approach. When the norm is minimized, the distances are reduced more evenly, thus giving more chances for shared gates on the final steps of the search. However, which approach is better (to maximize or to minimize the norm) is still unclear – for different input matrices different approaches work better.

In the previous version of this report we made a conjecture that there exists a circuit with 92 gates, and now we found it. For this to happen, we made two tweaks in our SLP program as follows. We have chosen and fixed the first 16 gates `t0..t15` ourselves – these 16 gates did appear in every 94-gates solution that we found earlier. This tweak is not really necessary but it helps to speed up simulations. The second tweak was to prohibit one specific gate `x15^x31` to appear in the solution (alternatively, we could prohibit `x7^x23`) – in previous 94-gates circuits we have seen a redundancy of 2 gates where `x15^x31` was involved, thus we made an assumption that removing that specific gate would also remove the redundancy.

Note that when applying Boyar's metric the SLP algorithm favors a lot to pick the gate `x15^x31` (and also `x7^x23`), but it is now clear that such a decision does not lead to a smaller circuit. We believe that the found circuit of AES MixColumn with 92 gates is a good test and study case for further improvements of SLP algorithms.

In the circuit below, x is the 32-bit input value, and y is the 32-bit output value.

```
t0 = x0 ^ x8
t1 = x16 ^ x24
t2 = x1 ^ x9
t3 = x17 ^ x25
t4 = x2 ^ x10
t5 = x18 ^ x26
t6 = x3 ^ x11
t7 = x19 ^ x27
t8 = x4 ^ x12
t9 = x20 ^ x28
t10 = x5 ^ x13
t11 = x21 ^ x29
t12 = x6 ^ x14
t13 = x22 ^ x30
t14 = x23 ^ x31
t15 = x7 ^ x15
t16 = x8 ^ t1
y0 = t15 ^ t16
t17 = x7 ^ x23
t18 = x24 ^ t0
y16 = t14 ^ t18
t19 = t1 ^ y16
y24 = t17 ^ t19
t20 = x27 ^ t14
t21 = t0 ^ y0
y8 = t17 ^ t21
t22 = t5 ^ t20
y19 = t6 ^ t22
t23 = x11 ^ t15
t24 = t7 ^ t23
y3 = t4 ^ t24
t25 = x2 ^ x18
t26 = t17 ^ t25
t27 = t9 ^ t23
t28 = t8 ^ t20
t29 = x10 ^ t2
y2 = t5 ^ t29
t30 = x26 ^ t3
y18 = t4 ^ t30
t31 = x9 ^ x25
t32 = t25 ^ t31
y10 = t30 ^ t32
y26 = t29 ^ t32
t33 = x1 ^ t18
t34 = x30 ^ t11
y22 = t12 ^ t34
t35 = x14 ^ t13
y6 = t10 ^ t35
t36 = x5 ^ x21
t37 = x30 ^ t17
t38 = x17 ^ t16
t39 = x13 ^ t8
y5 = t11 ^ t39
t40 = x12 ^ t36
y21 = t10 ^ t41
t41 = x29 ^ t9
t42 = x28 ^ t40
y13 = t41 ^ t42
y29 = t39 ^ t42
t43 = x15 ^ t12
y7 = t14 ^ t43
t44 = x14 ^ t37
y31 = t43 ^ t44
t45 = x31 ^ t13
y15 = t44 ^ t45
y23 = t15 ^ t45
t46 = t12 ^ t36
y14 = y6 ^ t46
t47 = t31 ^ t33
y17 = t19 ^ t47
t48 = t6 ^ y3
y11 = t26 ^ t48
t49 = t2 ^ t38
y25 = y24 ^ t49
t50 = t7 ^ y19
y27 = t26 ^ t50
t51 = x22 ^ t46
y30 = t11 ^ t51
t52 = x19 ^ t28
y20 = x28 ^ t52
t53 = x3 ^ t27
y4 = x12 ^ t53
t54 = t3 ^ t33
y9 = y8 ^ t54
t55 = t21 ^ t31
y1 = t38 ^ t55
t56 = x4 ^ t17
t57 = x19 ^ t56
y12 = t27 ^ t57
t58 = x3 ^ t28
t59 = t17 ^ t58
y28 = x20 ^ t59
```

Listing 1: MixColumn with 92 gates

The study of the above circuit reveals that after adding the first 66 gates the total distance is 26, i.e., it already shows a 92 gates solution in case no more shared gates. The vector of distances is:

`D = [0 0 0 0 2 2 2 2 | 0 0 0 0 0 2 0 2 | 2 3 2 3 0 0 0 0 | 0 2 0 2 0 0 0 0 ]`

which indicates that there could, potentially, be more shared gates. We leave this for further research.

References

[BFI19] Subhadeep Banik, Yuki Funabiki, and Takanori Isobe. More results on shortest linear programs. Cryptology ePrint Archive, Report 2019/856, 2019. https://eprint.iacr.org/2019/856.

[BP10] Joan Boyar and René Peralta. A New Combinational Logic Minimization Technique with Applications to Cryptology. In Paola Festa, editor, *Experimental Algorithms*, pages 178–189, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[EJMY19] Patrik Ekdahl, Thomas Johansson, Alexander Maximov, and Jing Yang. A new SNOW stream cipher called SNOW-V. Cryptology ePrint Archive, Report 2018/1143 version 20190603:135044, June 3, 2019. https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2018/1143&version=20190603:135044&file=1143.pdf.

[EM19] Patrik Ekdahl and Alexander Maximov. New Circuit Minimization Techniques for Smaller and Faster AES SBoxes. Cryptology ePrint Archive, Report 2019/802, 2019. https://eprint.iacr.org/2019/802.

[JMPS17] Jmy Jean, Amir Moradi, Thomas Peyrin, and Pascal Sasdrich. Bit-Sliding: A Generic Technique for Bit-Serial Implementations of SPN-based Primitives. In *Cryptographic Hardware and Embedded Systems CHES 2017*, volume 10529 of *Lecture Notes in Computer Science*, pages 687–707. Springer, 2017.

[KLSW17] Thorsten Kranz, Gregor Leander, Ko Stoffelen, and Friedrich Wiemer. Shorter Linear Straight-Line Programs for MDS Matrices. *IACR Transactions on Symmetric Cryptology*, 2017(4):188–211, Dec. 2017.

[TP19] Quan Quan Tan and Thomas Peyrin. Improved heuristics for short linear programs. Cryptology ePrint Archive, Report 2019/847, 2019. https://eprint.iacr.org/2019/847.