AES_encrypt>MixColumns (Calls: 294975, Time: 170.152 s)

Generated 02-abr-2024 22:21:22 using performance time.
Subfunction in file D:\UPIBI\Proyecto de titulacion\software\AES\AES_encrypt.m
Copy to new window for comparing multiple runs

Parents (calling functions)

Function Name	Function Type	Calls
AES_encrypt	Function	294975

Lines that take the most time

Line Number	Code	Calls	Total Time (s)	% Time	Time Plot
186	`if mul_str(i,d) == "mul1"`	18878400	45.349	26.7%	
189	`aux(d,j,i) =mul.(mul_str(i,d))(state(d,j…`	9439200	42.779	25.1%	
200	`,aux(4,1,i)));`	4719600	36.260	21.3%	
199	`temp(i) = bitxor(bitxor(aux(1,1,i),aux(2…`	4719600	20.607	12.1%	
182	`aux = zeros(4,4,4);`	294975	4.010	2.4%	
All other lines			21.146	12.4%	
Totals			170.152	100%	

Children (called functions)

No children

Code Analyzer results

No Code Analyzer messages.

Coverage results

Show coverage for parent folder

Total lines in function	66
Non-code lines (comments, blank lines)	43
Code lines (lines that can run)	23
Code lines that did run	23
Code lines that did not run	0
Coverage (did run/can run)	100.00 %

Function listing

```
Time     Calls    Line
                  139  function state = MixColumns(state)
                  140  %UNTITLED Summary of this function goes here
                  141  %   Detailed explanation goes here
                  142
   3.305  294975  143  mul.mul2 = [0,32,64,96,128,160,192,224,27,59,91,123,155,187,219,251;...
```

```
                144              2,34,66,98,130,162,194,226,25,57,89,121,153,185,217,249;...
                145              4,36,68,100,132,164,196,228,31,63,95,127,159,191,223,255;...
                146              6,38,70,102,134,166,198,230,29,61,93,125,157,189,221,253;...
                147              8,40,72,104,136,168,200,232,19,51,83,115,147,179,211,243;...
                148              10,42,74,106,138,170,202,234,17,49,81,113,145,177,209,241;...
                149              12,44,76,108,140,172,204,236,23,55,87,119,151,183,215,247;...
                150              14,46,78,110,142,174,206,238,21,53,85,117,149,181,213,245;...
                151              16,48,80,112,144,176,208,240,11,43,75,107,139,171,203,235;...
                152              18,50,82,114,146,178,210,242,9,41,73,105,137,169,201,233;...
                153              20,52,84,116,148,180,212,244,15,47,79,111,143,175,207,239;...
                154              22,54,86,118,150,182,214,246,13,45,77,109,141,173,205,237;...
                155              24,56,88,120,152,184,216,248,3,35,67,99,131,163,195,227;...
                156              26,58,90,122,154,186,218,250,1,33,65,97,129,161,193,225;...
                157              28,60,92,124,156,188,220,252,7,39,71,103,135,167,199,231;...
                158              30,62,94,126,158,190,222,254,5,37,69,101,133,165,197,229];
                159
1.583    294975 160   mul.mul3 = [0,48,96,80,192,240,160,144,155,171,251,203,91,107,59,11;...
                161              3,51,99,83,195,243,163,147,152,168,248,200,88,104,56,8;...
                162              6,54,102,86,198,246,166,150,157,173,253,205,93,109,61,13;...
                163              5,53,101,85,197,245,165,149,158,174,254,206,94,110,62,14;...
                164              12,60,108,92,204,252,172,156,151,167,247,199,87,103,55,7;...
                165              15,63,111,95,207,255,175,159,148,164,244,196,84,100,52,4;...
                166              10,58,106,90,202,250,170,154,145,161,241,193,81,97,49,1;...
                167              9,57,105,89,201,249,169,153,146,162,242,194,82,98,50,2;...
                168              24,40,120,72,216,232,184,136,131,179,227,211,67,115,35,19;...
                169              27,43,123,75,219,235,187,139,128,176,224,208,64,112,32,16;...
                170              30,46,126,78,222,238,190,142,133,181,229,213,69,117,37,21;...
                171              29,45,125,77,221,237,189,141,134,182,230,214,70,118,38,22;...
                172              20,36,116,68,212,228,180,132,143,191,239,223,79,127,47,31;...
                173              23,39,119,71,215,231,183,135,140,188,236,220,76,124,44,28;...
                174              18,34,114,66,210,226,178,130,137,185,233,217,73,121,41,25;...
                175              17,33,113,65,209,225,177,129,138,186,234,218,74,122,42,26];
                176
0.039    294975 177   mul_str = ["mul2","mul3","mul1","mul1";...
                178              "mul1","mul2","mul3","mul1";...
                179              "mul1","mul1","mul2","mul3";...
                180              "mul3","mul1","mul1","mul2"];
                181
4.010    294975 182   aux = zeros(4,4,4);
0.047    294975 183   for i = 1:4
0.150   1179900 184       for j = 1:4
0.446   4719600 185           for d=1:4
45.349 18878400 186               if mul_str(i,d) == "mul1"
1.018    9439200 187                   aux(d,j,i) = state(d,j);
0.852    9439200 188               else
42.779   9439200 189                   aux(d,j,i) =mul.(mul_str(i,d))(state(d,j)+1);
```

1.689	18878400	190	end
1.921	18878400	191	end
0.478	4719600	192	end
0.160	1179900	193	end
		194	
2.774	294975	195	aux = reshape(aux,4,1,16);
0.483	294975	196	temp = zeros(1,16);
		197	
0.043	294975	198	for i = 1:16
56.867	4719600	199	temp(i) = bitxor(bitxor(aux(1,1,i),aux(2,1,i)),bitxor(aux(3,1,i)...
	4719600	200	,aux(4,1,i)));
0.582	4719600	201	end
2.117	294975	202	state = reshape(temp,4,[])';
		203	
2.516	294975	204	end

Local functions in this file are not included in this listing.