

AES Masked State

AES Masks State

Key Masked State

Key Masks State

m0	m1	m2	m3
m4	m5	m6	m7
m8	m9	m10	m11
m12	m13	m14	m15

m0	m1	m2	m3
m4	m5	m6	m7
m8	m9	m10	m11
m12	m13	m14	m15

r0	r1	r2	r3
r4	r5	r6	r7
r8	r9	r10	r11
r12	r13	r14	r15

r0	r1	r2	r3
r4	r5	r6	r7
r8	r9	r10	r11
r12	r13	r14	r15

m0 + r0	m1 + r1	m2 + r2	m3 + r3
m4 + r4	m5 + r5	m6 + r6	m7 + r7
m8 + r8	m9 + r9	m10 + r10	m11 + r11
m12 + r12	m13 + r13	m14 + r14	m15 + r15

m0 + r0	m1 + r1	m2 + r2	m3 + r3
m4 + r4	m5 + r5	m6 + r6	m7 + r7
m8 + r8	m9 + r9	m10 + r10	m11 + r11
m12 + r12	m13 + r13	m14 + r14	m15 + r15

AddRoundKey

rmult aes

rmult key

rin	rin	rin	rin
rin	rin	rin	rin
rin	rin	rin	rin
rin	rin	rin	rin

rin

SubBytes

rout	rout	rout	rout
rout	rout	rout	rout
rout	rout	rout	rout
rout	rout	rout	rout

rout

m0 + r0	m1 + r1	m2 + r2	m3 + r3
m4 + r4	m5 + r5	m6 + r6	m7 + r7
m8 + r8	m9 + r9	m10 + r10	m11 + r11
m12 + r12	m13 + r13	m14 + r14	m15 + r15

m0 + r0	m1 + r1	m2 + r2	m3 + r3
m4 + r4	m5 + r5	m6 + r6	m7 + r7
m8 + r8	m9 + r9	m10 + r10	m11 + r11
m12 + r12	m13 + r13	m14 + r14	m15 + r15

ShiftRows/MixColumns

m0	m1	m2	m3
m4	m5	m6	m7
m8	m9	m10	m11
m12	m13	m14	m15

m0	m1	m2	m3
m4	m5	m6	m7
m8	m9	m10	m11
m12	m13	m14	m15