AESE

AES single round encryption.

Advanced SIMD
(FEAT_AES)

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	1	0	0	1	1	1	0	0	0	1	0	1	0	0	0	0	0	1	0	0	1	0			Rn				Rd		

D

> **AESE** **<Vd>**.16B, **<Vn>**.16B

```
integer d = UInt(Rd);
integer n = UInt(Rn);
if !IsFeatureImplemented(FEAT_AES) then UNDEFINED;
```

Assembler Symbols

<Vd>   Is the name of the SIMD&FP source and destination register, encoded in the "Rd" field.

<Vn>   Is the name of the second SIMD&FP source register, encoded in the "Rn" field.

Operation

```
AArch64.CheckFPAdvSIMDEnabled();

bits(128) operand1 = V[d, 128];
bits(128) operand2 = V[n, 128];
bits(128) result;
result = operand1 EOR operand2;
result = AESSubBytes(AESShiftRows(result));

V[d, 128] = result;
```

Operational information

If PSTATE.DIT is 1:

- The execution time of this instruction is independent of:
  - The values of the data supplied in any of its registers.
  - The values of the NZCV flags.
- The response of this instruction to asynchronous exceptions does not vary based on:
  - The values of the data supplied in any of its registers.
  - The values of the NZCV flags.