AES	SPN	S-AES
128-bit	block	16-bit
128-bit	key	16-bit
10	rounds	2
8×8	S-box	4×4
F_{2^8}	field	F_{16}
$x^8 + x^4 + x^3 + x + 1$	modulus	$x^4 + x + 1$
2^8		

S-box input 0101 → inverse in F_{16} → 1011

$x^3 + x + 1$

$x^2 + 1$

$x^5 + x^3 + x^2$

$x^3 + x + 1$

$x^5 + x^2 + x + 1$

x

$x^4 + x + 1 \;\big|\; x^5 + x^2 + x + 1$

$x^5 + x^2 + x$

1

affine transformation

multiply: $(y^3 + y^2 + 1)(y^3 + y + 1)$ — add: $+ (y^3 + 1) \bmod (y^4 + 1)$

inverse mod $(y^4 + 1)$ — not irreducible

$y^6 + y^4 + y^3$

$y^5 + y^3 + y^2$

$y^3 + y + 1$

$y^6 + y^5 + y^4 + y^3 + y^2 + y + 1$

$y^6 + y^5 + y^4 + y^3 + y^2 + y + 1$

$y^3 + 1$

$y^6 + y^5 + y^4 \quad + y^2 + y$

$y^2 + y + 1$

$y^3 + 1 \;\big|\; y^6 + y^5 + y^4 + y^2 + y$

$y^6 \quad + y^3$

$y^5 + y^4 + y^2 + y$

$y^5 \quad + y^2$

$y^4 + y^3 + y$

$y^4 \quad + y$

$y^3 + 1$

1

output of S-box 0001

S-box is nonlinear

Inversion $y = b_2$

$xy = 1$

The S-box lookup table

	input	output	
0	00000	1001	9
1	00001	0100	4
2	00010	1010	A
3	00011	1011	B
4	00100	1101	D
5	00101	0001	1
6	00110	1000	8
7	00111	0101	5
8	10000	0110	6
9	10001	0010	2
A	10010	0000	0
B	10011	0011	3
C	11100	1100	C
D	11101	1110	E
E	11110	1111	F
F	11111	0111	7