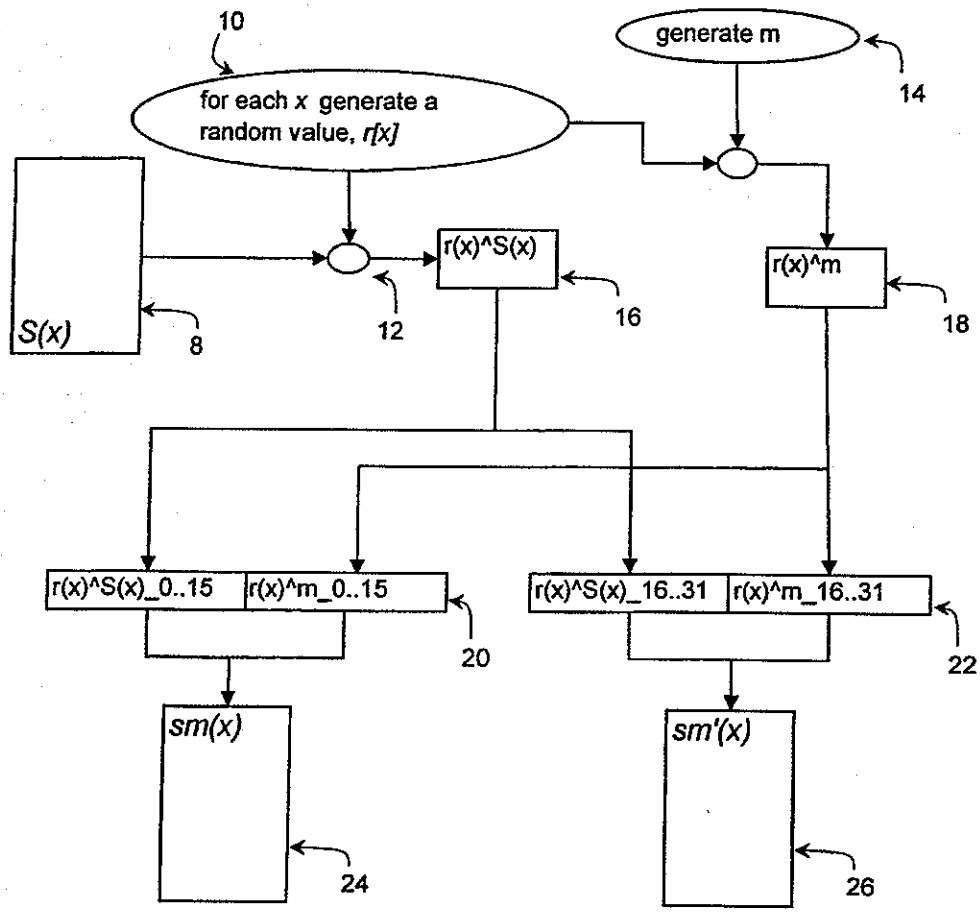
10
for each x generate a random value, r[x]
generate m
14
S(x)
8
12
r(x)^S(x)
16
r(x)^m
18
r(x)^S(x)_0..15
r(x)^m_0..15
20
r(x)^S(x)_16..31
r(x)^m_16..31
22
sm(x)
24
sm'(x)
26

FIGURE 1

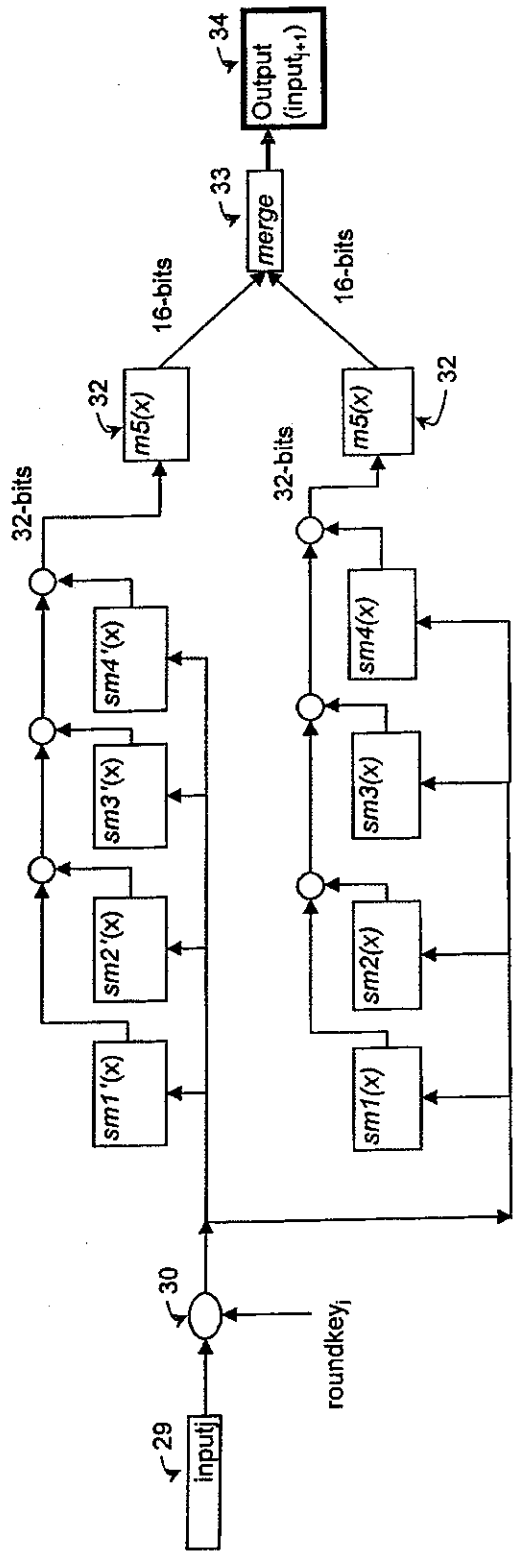
29
inputj
30
roundkeyj
32-bits
sm1'(x)
sm2'(x)
sm3'(x)
sm4'(x)
32
m5(x)
16-bits
32-bits
sm1(x)
sm2(x)
sm3(x)
sm4(x)
32
m5(x)
16-bits
33
merge
34
Output
(inputj+1)

Figure 2

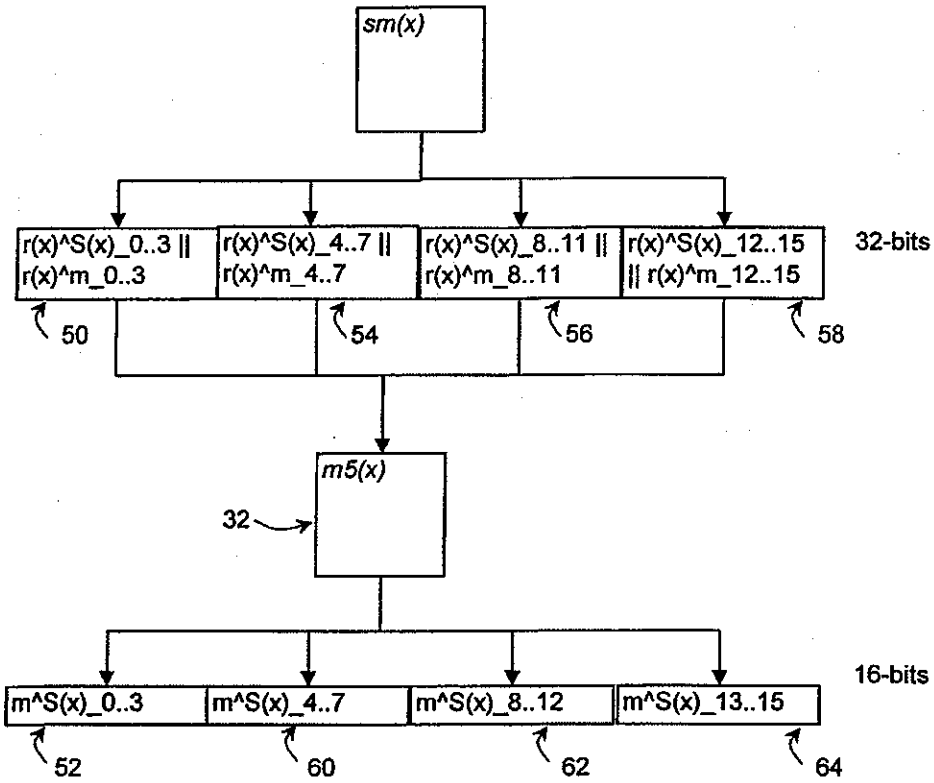
sm(x)
r(x)^S(x)_0..3 || r(x)^m_0..3
r(x)^S(x)_4..7 || r(x)^m_4..7
r(x)^S(x)_8..11 || r(x)^m_8..11
r(x)^S(x)_12..15 || r(x)^m_12..15
32-bits
50
54
56
58
m5(x)
32
m^S(x)_0..3
m^S(x)_4..7
m^S(x)_8..12
m^S(x)_13..15
16-bits
52
60
62
64

Figure 3

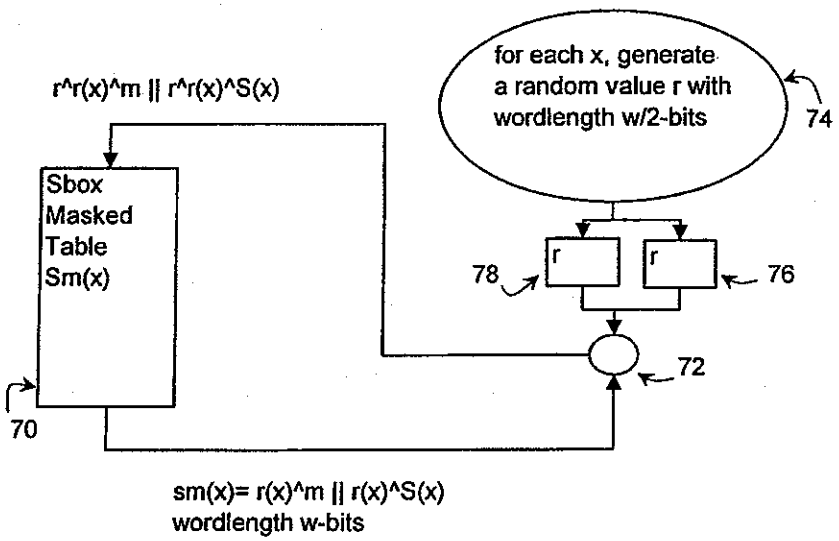
r^r(x)^m || r^r(x)^S(x)
for each x, generate a random value r with wordlength w/2-bits
74
Sbox Masked Table Sm(x)
r
r
78
76
72
70
sm(x)= r(x)^m || r(x)^S(x)
wordlength w-bits

Figure 4

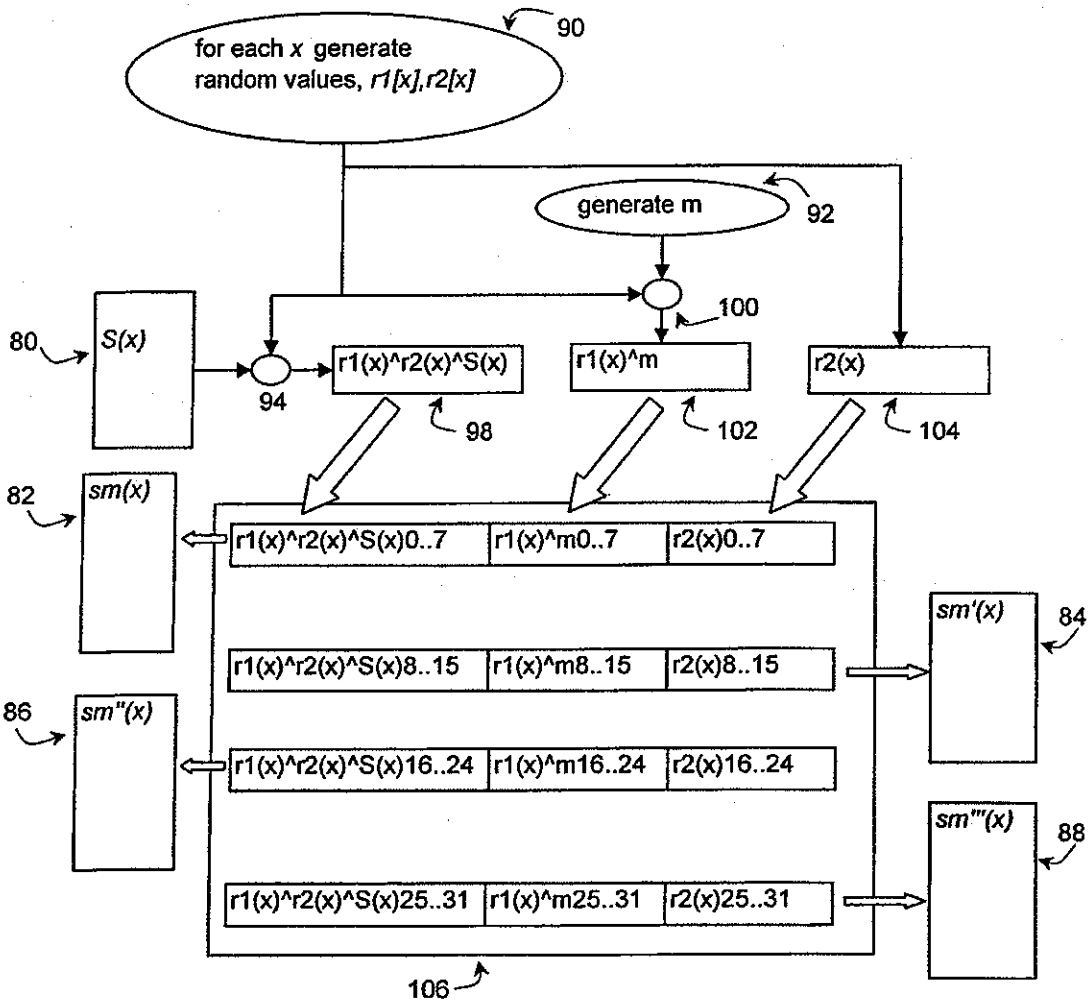
for each x generate
random values, r1[x],r2[x]
90
generate m
92
100
80
S(x)
94
r1(x)^r2(x)^S(x)
r1(x)^m
r2(x)
98
102
104
82
sm(x)
r1(x)^r2(x)^S(x)0..7
r1(x)^m0..7
r2(x)0..7
sm'(x)
84
r1(x)^r2(x)^S(x)8..15
r1(x)^m8..15
r2(x)8..15
86
sm''(x)
r1(x)^r2(x)^S(x)16..24
r1(x)^m16..24
r2(x)16..24
sm'''(x)
88
r1(x)^r2(x)^S(x)25..31
r1(x)^m25..31
r2(x)25..31
106

Figure 5

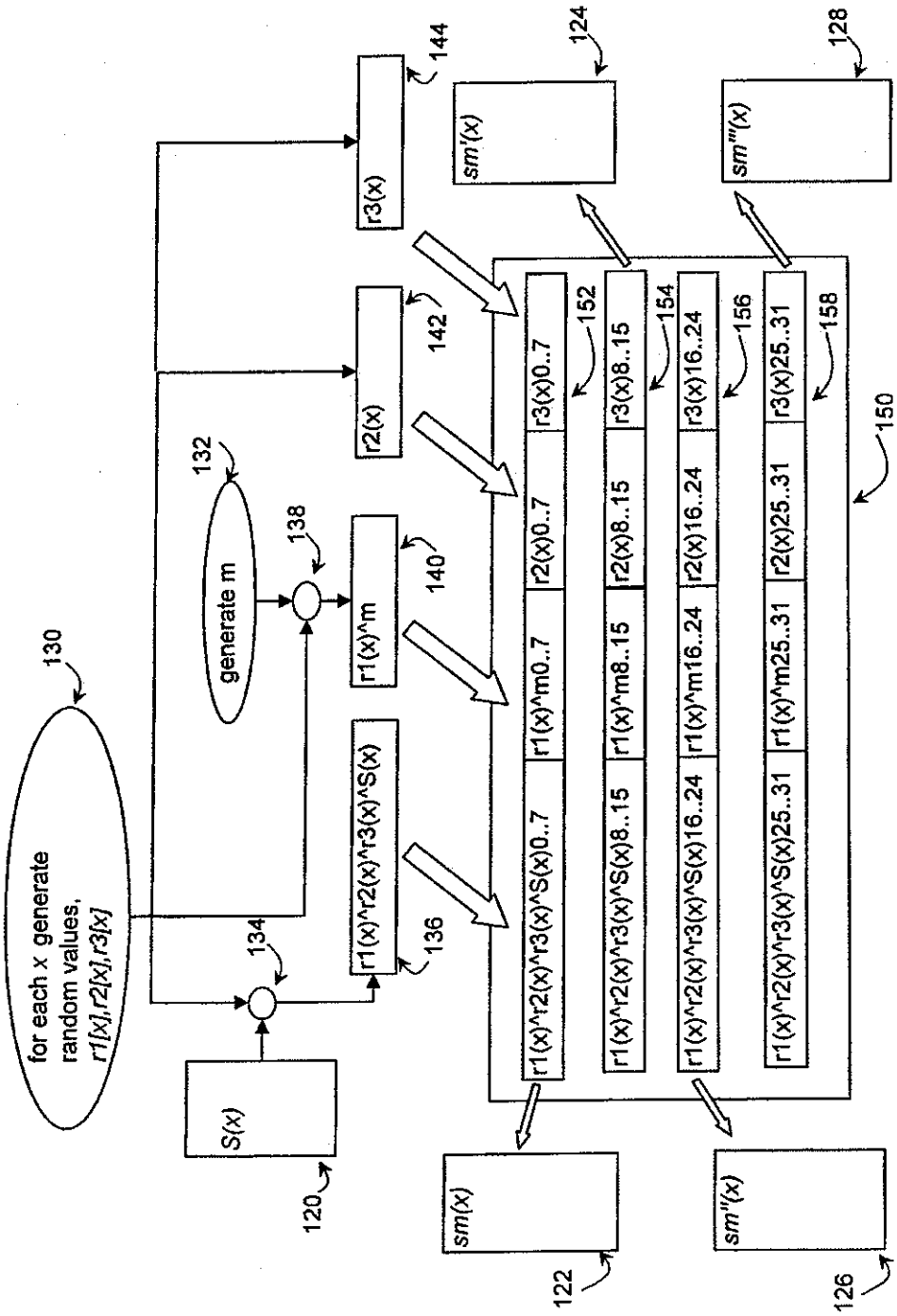
for each x generate random values, r1[x],r2[x],r3[x]
130
generate m
132
S(x)
120
134
138
r1(x)^m
140
r1(x)^r2(x)^r3(x)^S(x)
136
r2(x)
142
r3(x)
144
sm(x)
122
sm'(x)
124
sm''(x)
126
sm'''(x)
128
r1(x)^r2(x)^r3(x)^S(x)0..7
r1(x)^m0..7
r2(x)0..7
r3(x)0..7
152
r1(x)^r2(x)^r3(x)^S(x)8..15
r1(x)^m8..15
r2(x)8..15
r3(x)8..15
154
r1(x)^r2(x)^r3(x)^S(x)16..24
r1(x)^m16..24
r2(x)16..24
r3(x)16..24
156
r1(x)^r2(x)^r3(x)^S(x)25..31
r1(x)^m25..31
r2(x)25..31
r3(x)25..31
158
150

Figure 6