FIG. 1

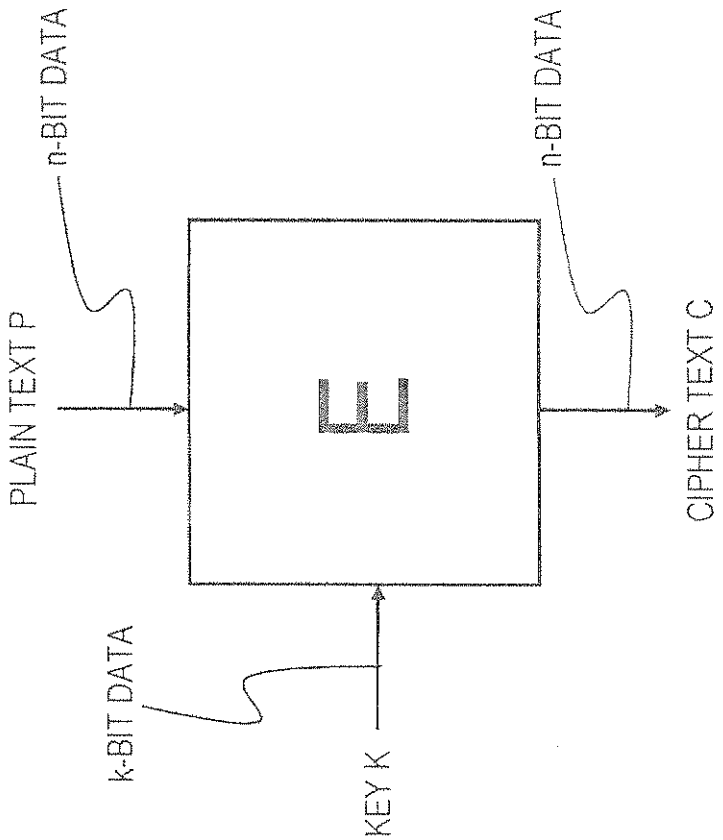

n-BIT DATA
PLAIN TEXT P
E
n-BIT DATA
CIPHER TEXT C
k-BIT DATA
KEY K

FIG. 2

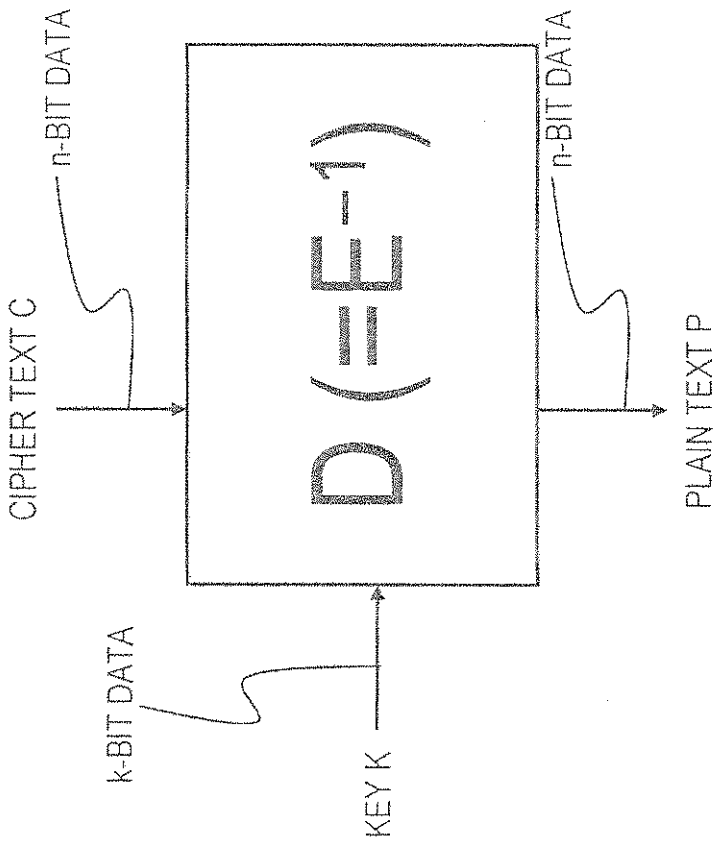

n-BIT DATA
CIPHER TEXT C
$D_K(\cdot)$
n-BIT DATA
PLAIN TEXT P
k-BIT DATA
KEY K

FIG. 3

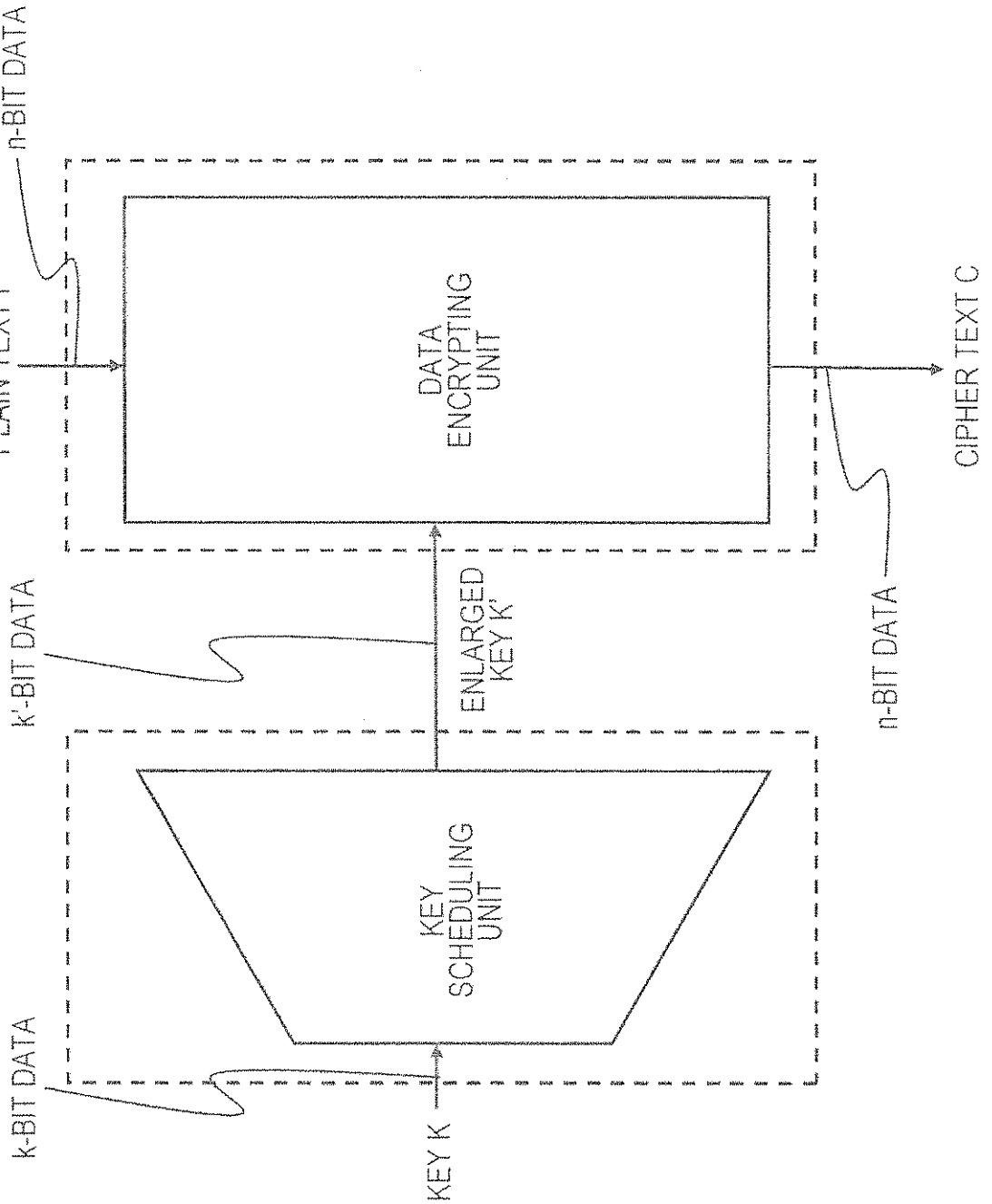

n-BIT DATA
PLAIN TEXT P
DATA ENCRYPTING UNIT
CIPHER TEXT C
k'-BIT DATA
ENLARGED KEY K'
n-BIT DATA
KEY SCHEDULING UNIT
k-BIT DATA
KEY K

FIG. 4

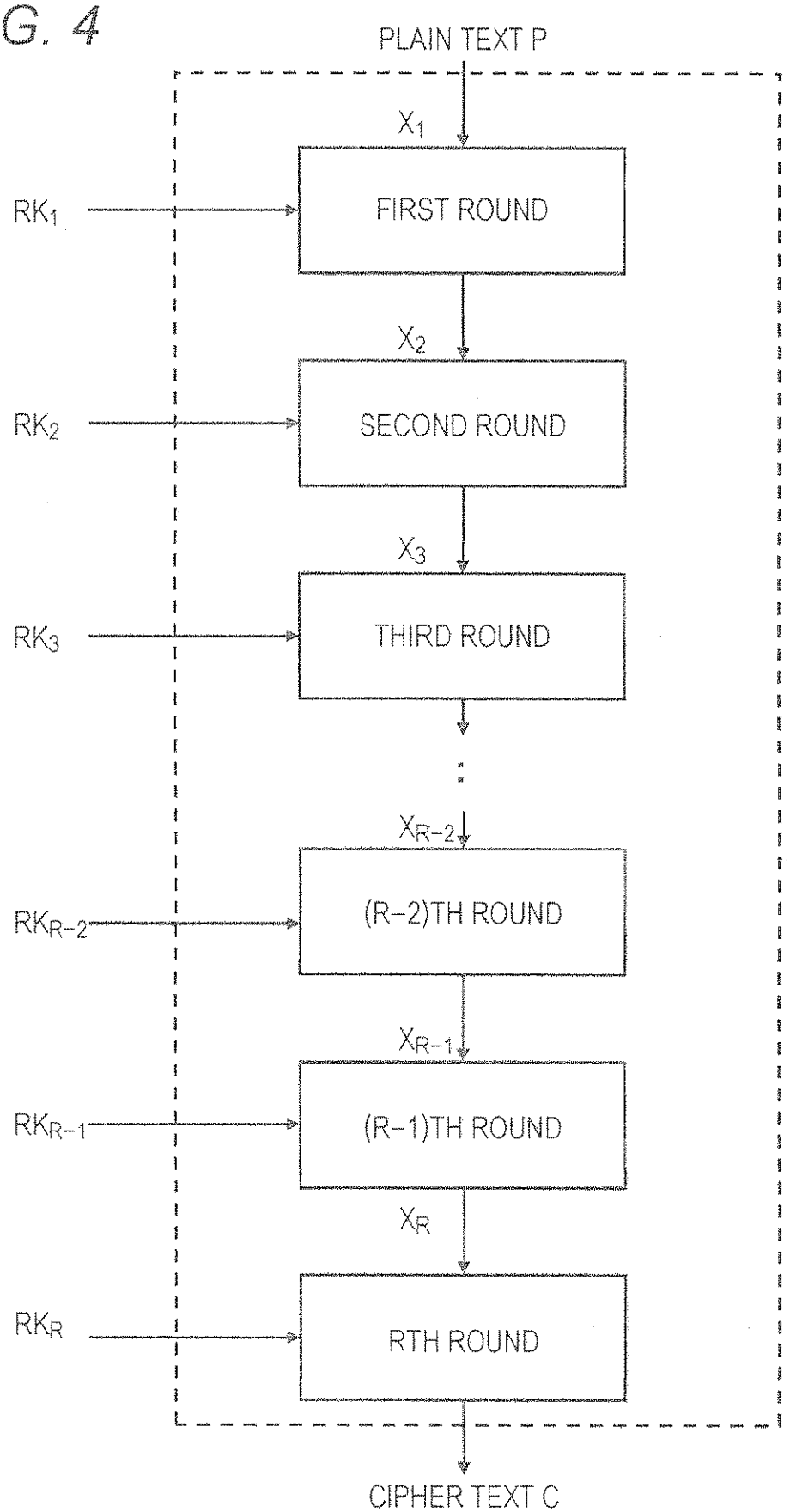

PLAIN TEXT P
X1
FIRST ROUND
RK1
X2
SECOND ROUND
RK2
X3
THIRD ROUND
RK3
XR-2
(R-2)TH ROUND
RKR-2
XR-1
(R-1)TH ROUND
RKR-1
XR
RTH ROUND
RKR
CIPHER TEXT C

FIG. 5

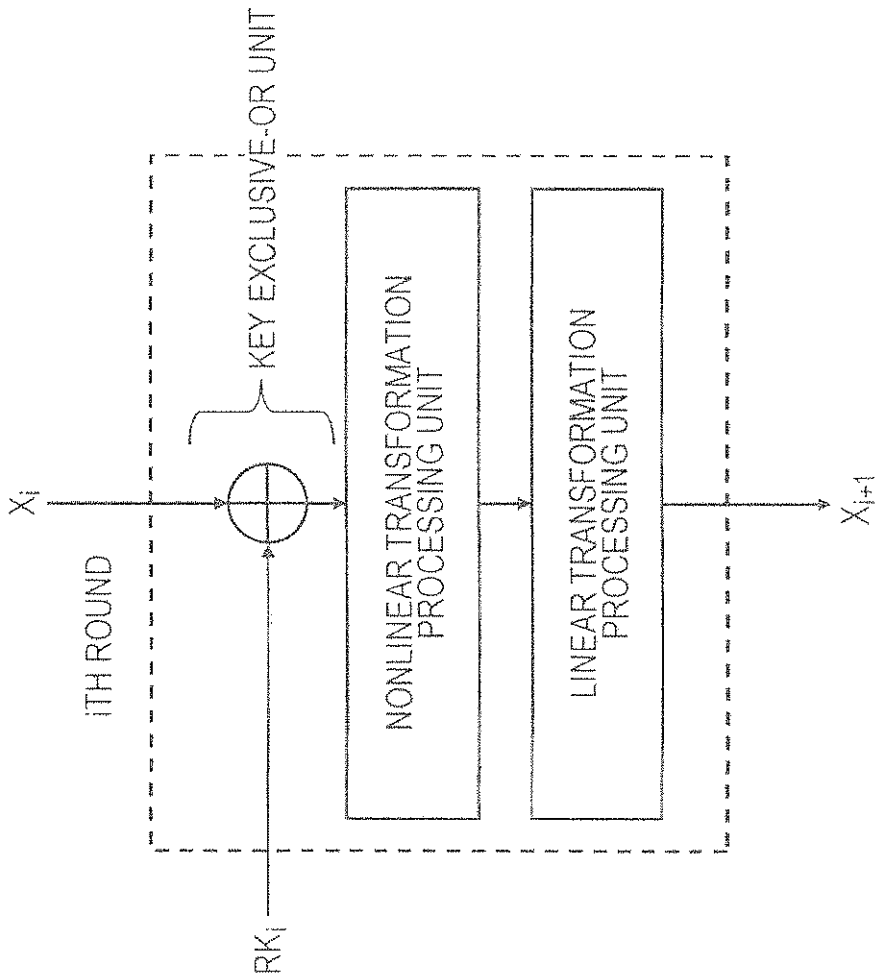

X_i
iTH ROUND
KEY EXCLUSIVE-OR UNIT
NONLINEAR TRANSFORMATION PROCESSING UNIT
LINEAR TRANSFORMATION PROCESSING UNIT
X_{i+1}
RK_i

FIG. 6

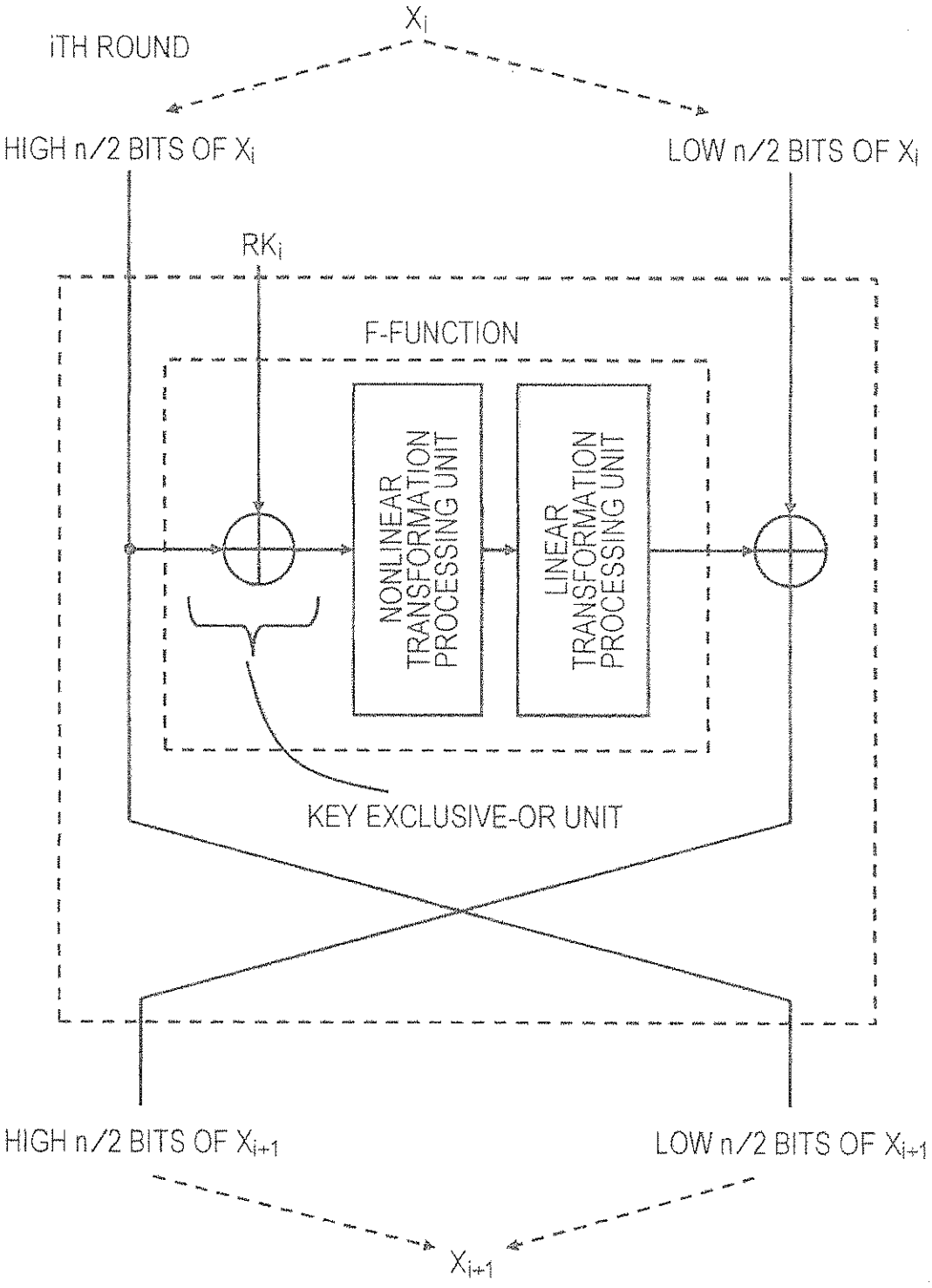

iTH ROUND
X_i
HIGH n/2 BITS OF X_i
LOW n/2 BITS OF X_i
RK_i
F-FUNCTION
NONLINEAR TRANSFORMATION PROCESSING UNIT
LINEAR TRANSFORMATION PROCESSING UNIT
KEY EXCLUSIVE-OR UNIT
HIGH n/2 BITS OF X_{i+1}
LOW n/2 BITS OF X_{i+1}
X_{i+1}

FIG. 7

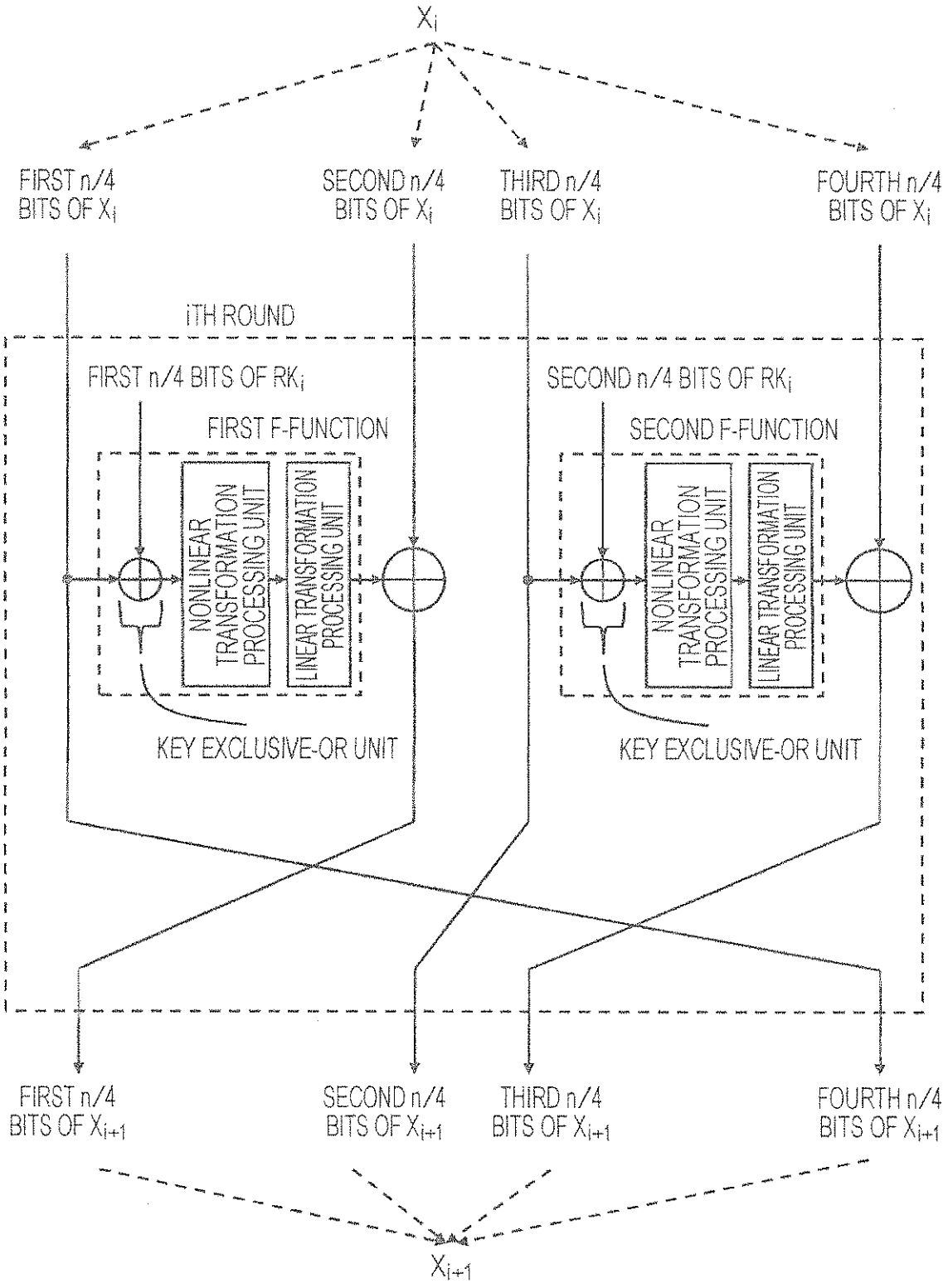

X_i
FIRST n/4 BITS OF X_i
SECOND n/4 BITS OF X_i
THIRD n/4 BITS OF X_i
FOURTH n/4 BITS OF X_i
iTH ROUND
FIRST n/4 BITS OF RK_i
FIRST F-FUNCTION
NONLINEAR TRANSFORMATION PROCESSING UNIT
LINEAR TRANSFORMATION PROCESSING UNIT
KEY EXCLUSIVE-OR UNIT
SECOND n/4 BITS OF RK_i
SECOND F-FUNCTION
NONLINEAR TRANSFORMATION PROCESSING UNIT
LINEAR TRANSFORMATION PROCESSING UNIT
KEY EXCLUSIVE-OR UNIT
FIRST n/4 BITS OF X_{i+1}
SECOND n/4 BITS OF X_{i+1}
THIRD n/4 BITS OF X_{i+1}
FOURTH n/4 BITS OF X_{i+1}
X_{i+1}

FIG. 8

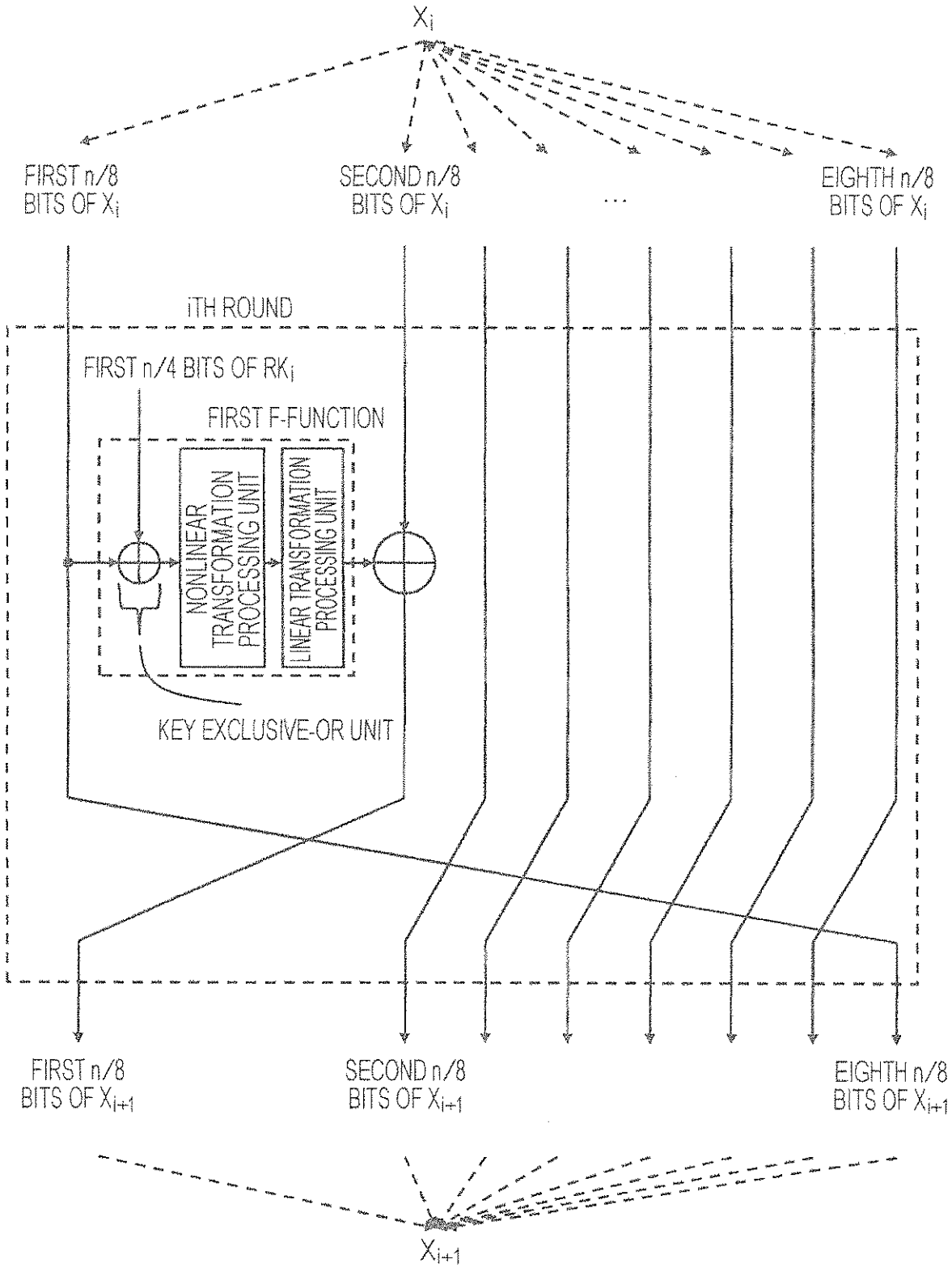

X_i
FIRST n/8 BITS OF X_i
SECOND n/8 BITS OF X_i
...
EIGHTH n/8 BITS OF X_i
iTH ROUND
FIRST n/4 BITS OF RK_i
FIRST F-FUNCTION
NONLINEAR TRANSFORMATION PROCESSING UNIT
LINEAR TRANSFORMATION PROCESSING UNIT
KEY EXCLUSIVE-OR UNIT
FIRST n/8 BITS OF X_{i+1}
SECOND n/8 BITS OF X_{i+1}
EIGHTH n/8 BITS OF X_{i+1}
X_{i+1}

FIG. 9

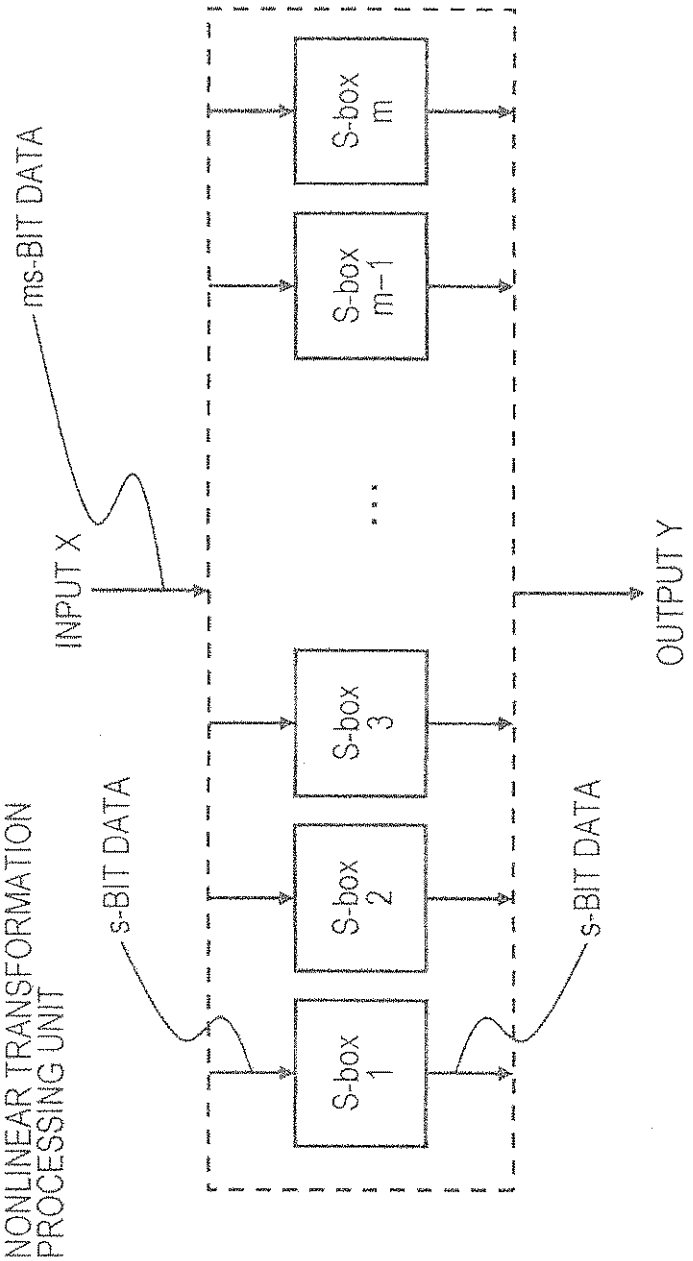

NONLINEAR TRANSFORMATION PROCESSING UNIT
INPUT X
ms-BIT DATA
s-BIT DATA
s-BIT DATA
OUTPUT Y
S-box 1
S-box 2
S-box 3
S-box m-1
S-box m

FIG. 10

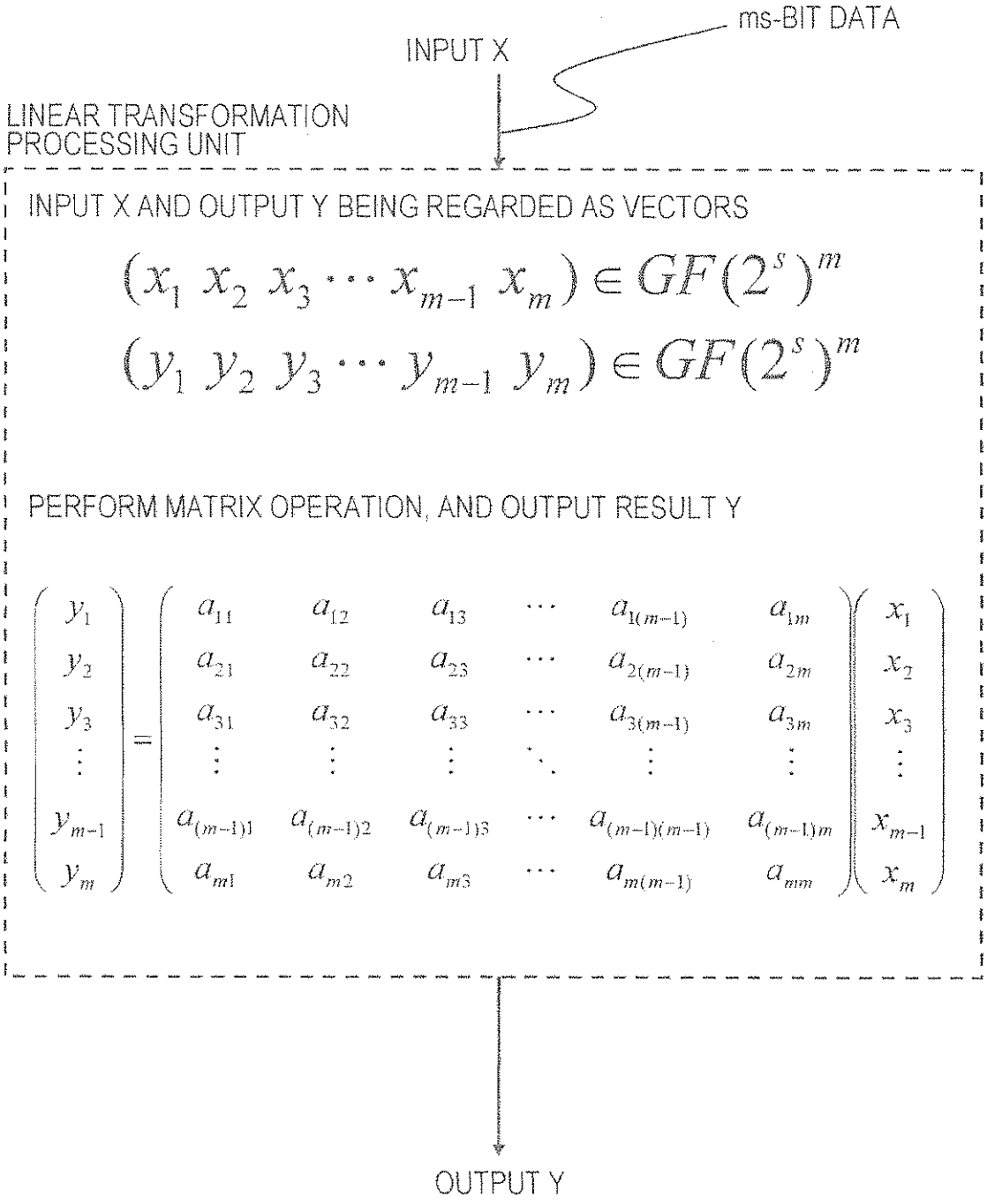

ms-BIT DATA
INPUT X
LINEAR TRANSFORMATION PROCESSING UNIT
INPUT X AND OUTPUT Y BEING REGARDED AS VECTORS
$(x_1\ x_2\ x_3 \cdots x_{m-1}\ x_m) \in GF(2^s)^m$
$(y_1\ y_2\ y_3 \cdots y_{m-1}\ y_m) \in GF(2^s)^m$
PERFORM MATRIX OPERATION, AND OUTPUT RESULT Y
$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_{m-1} \\ y_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1(m-1)} & a_{1m} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2(m-1)} & a_{2m} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3(m-1)} & a_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{(m-1)1} & a_{(m-1)2} & a_{(m-1)3} & \cdots & a_{(m-1)(m-1)} & a_{(m-1)m} \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{m(m-1)} & a_{mm} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{m-1} \\ x_m \end{pmatrix}$
OUTPUT Y

FIG. 11

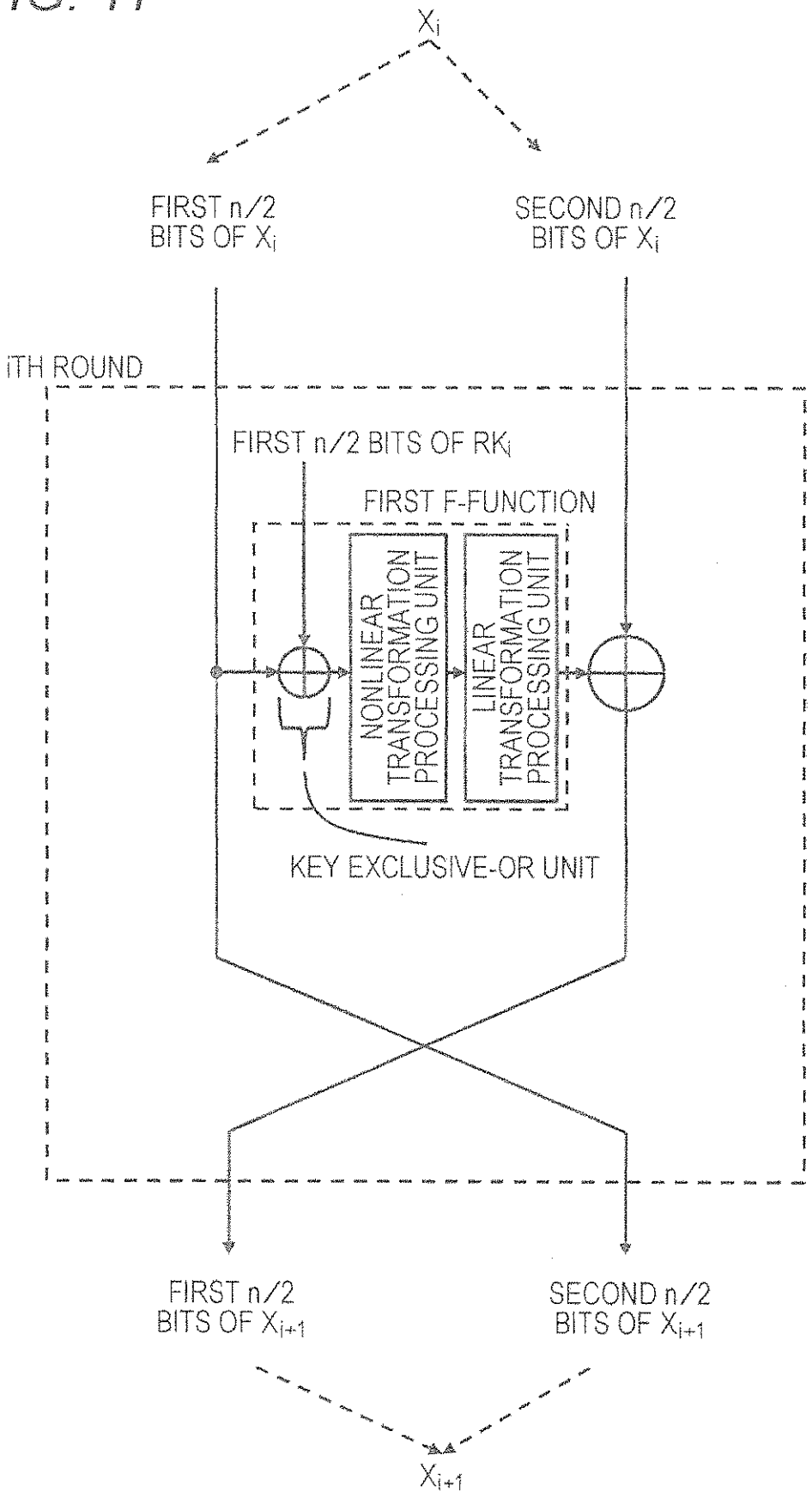

X_i
FIRST n/2 BITS OF X_i
SECOND n/2 BITS OF X_i
iTH ROUND
FIRST n/2 BITS OF RK_i
FIRST F-FUNCTION
NONLINEAR TRANSFORMATION PROCESSING UNIT
LINEAR TRANSFORMATION PROCESSING UNIT
KEY EXCLUSIVE-OR UNIT
FIRST n/2 BITS OF X_{i+1}
SECOND n/2 BITS OF X_{i+1}
X_{i+1}

FIG. 12

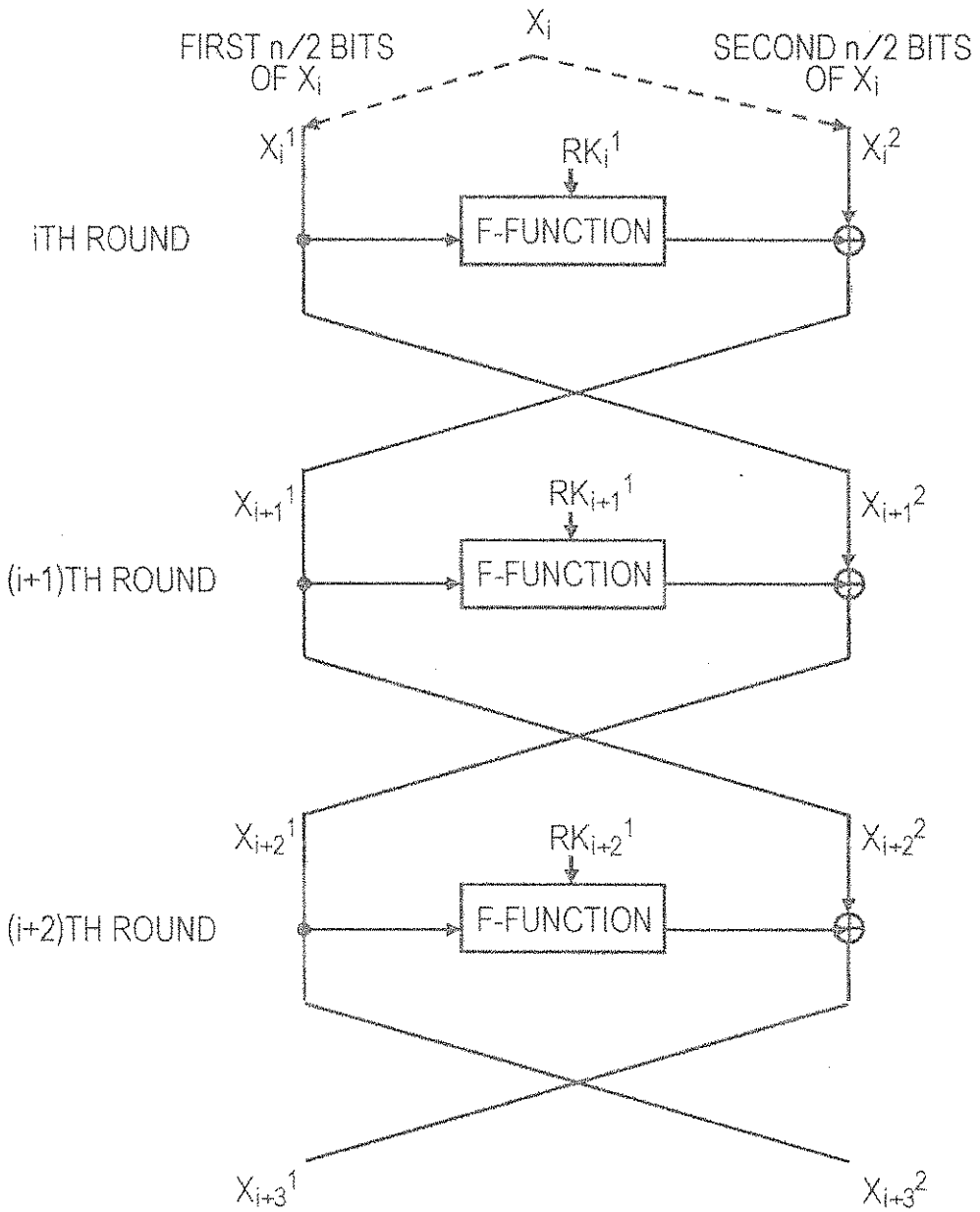

X_i
FIRST n/2 BITS OF X_i
SECOND n/2 BITS OF X_i
X_i^1
RK_i^1
X_i^2
iTH ROUND
F-FUNCTION
X_{i+1}^1
RK_{i+1}^1
X_{i+1}^2
(i+1)TH ROUND
F-FUNCTION
X_{i+2}^1
RK_{i+2}^1
X_{i+2}^2
(i+2)TH ROUND
F-FUNCTION
X_{i+3}^1
X_{i+3}^2

FIG. 13

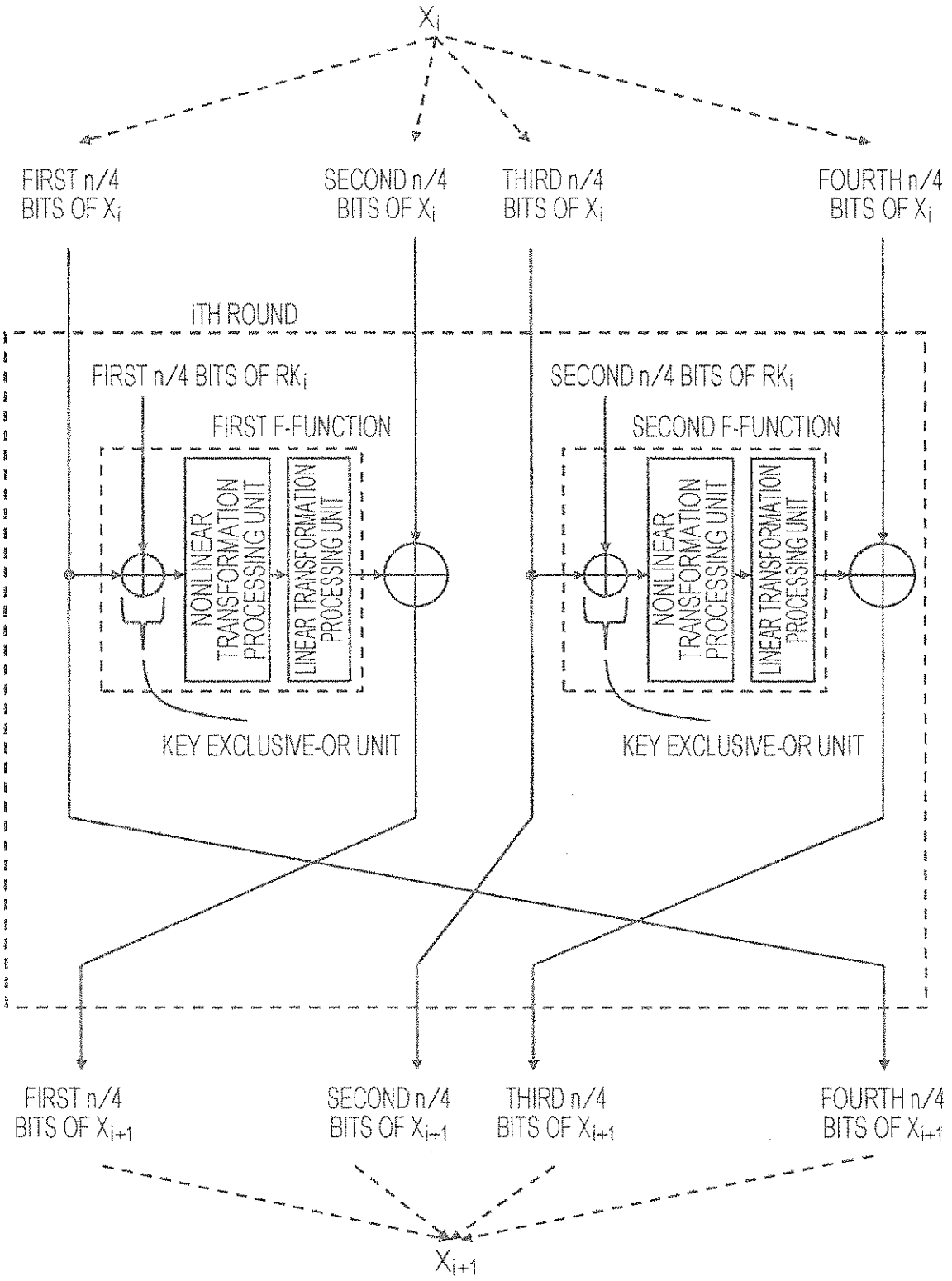

X_i
FIRST n/4 BITS OF X_i
SECOND n/4 BITS OF X_i
THIRD n/4 BITS OF X_i
FOURTH n/4 BITS OF X_i
iTH ROUND
FIRST n/4 BITS OF RK_i
FIRST F-FUNCTION
NONLINEAR TRANSFORMATION PROCESSING UNIT
LINEAR TRANSFORMATION PROCESSING UNIT
KEY EXCLUSIVE-OR UNIT
SECOND n/4 BITS OF RK_i
SECOND F-FUNCTION
NONLINEAR TRANSFORMATION PROCESSING UNIT
LINEAR TRANSFORMATION PROCESSING UNIT
KEY EXCLUSIVE-OR UNIT
FIRST n/4 BITS OF X_{i+1}
SECOND n/4 BITS OF X_{i+1}
THIRD n/4 BITS OF X_{i+1}
FOURTH n/4 BITS OF X_{i+1}
X_{i+1}

FIG. 14

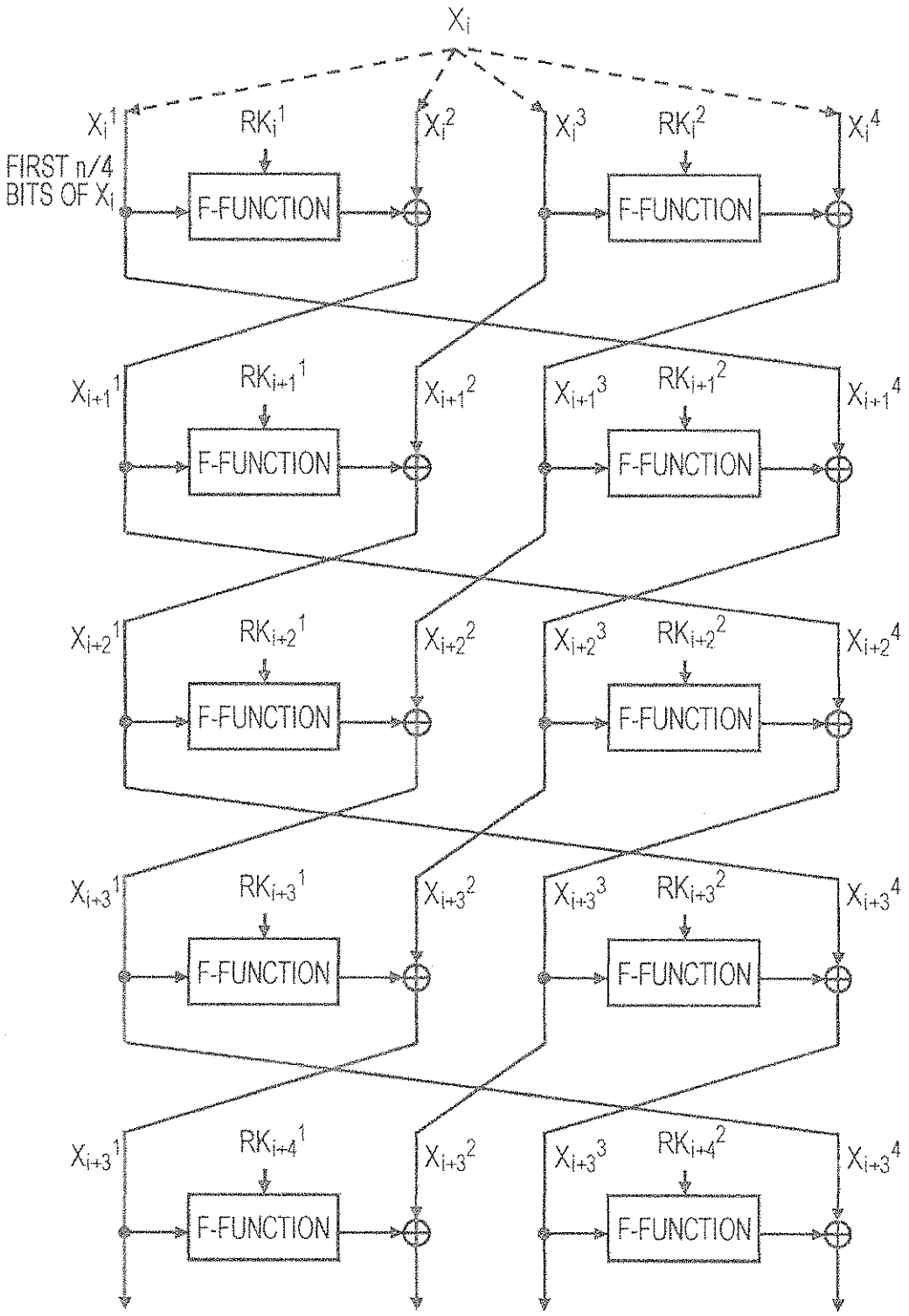

X_i
X_i^1
RK_i^1
X_i^2
X_i^3
RK_i^2
X_i^4
FIRST n/4 BITS OF X_i
F-FUNCTION
F-FUNCTION
X_{i+1}^1
RK_{i+1}^1
X_{i+1}^2
X_{i+1}^3
RK_{i+1}^2
X_{i+1}^4
F-FUNCTION
F-FUNCTION
X_{i+2}^1
RK_{i+2}^1
X_{i+2}^2
X_{i+2}^3
RK_{i+2}^2
X_{i+2}^4
F-FUNCTION
F-FUNCTION
X_{i+3}^1
RK_{i+3}^1
X_{i+3}^2
X_{i+3}^3
RK_{i+3}^2
X_{i+3}^4
F-FUNCTION
F-FUNCTION
X_{i+3}^1
RK_{i+4}^1
X_{i+3}^2
X_{i+3}^3
RK_{i+4}^2
X_{i+3}^4
F-FUNCTION
F-FUNCTION

FIG. 15

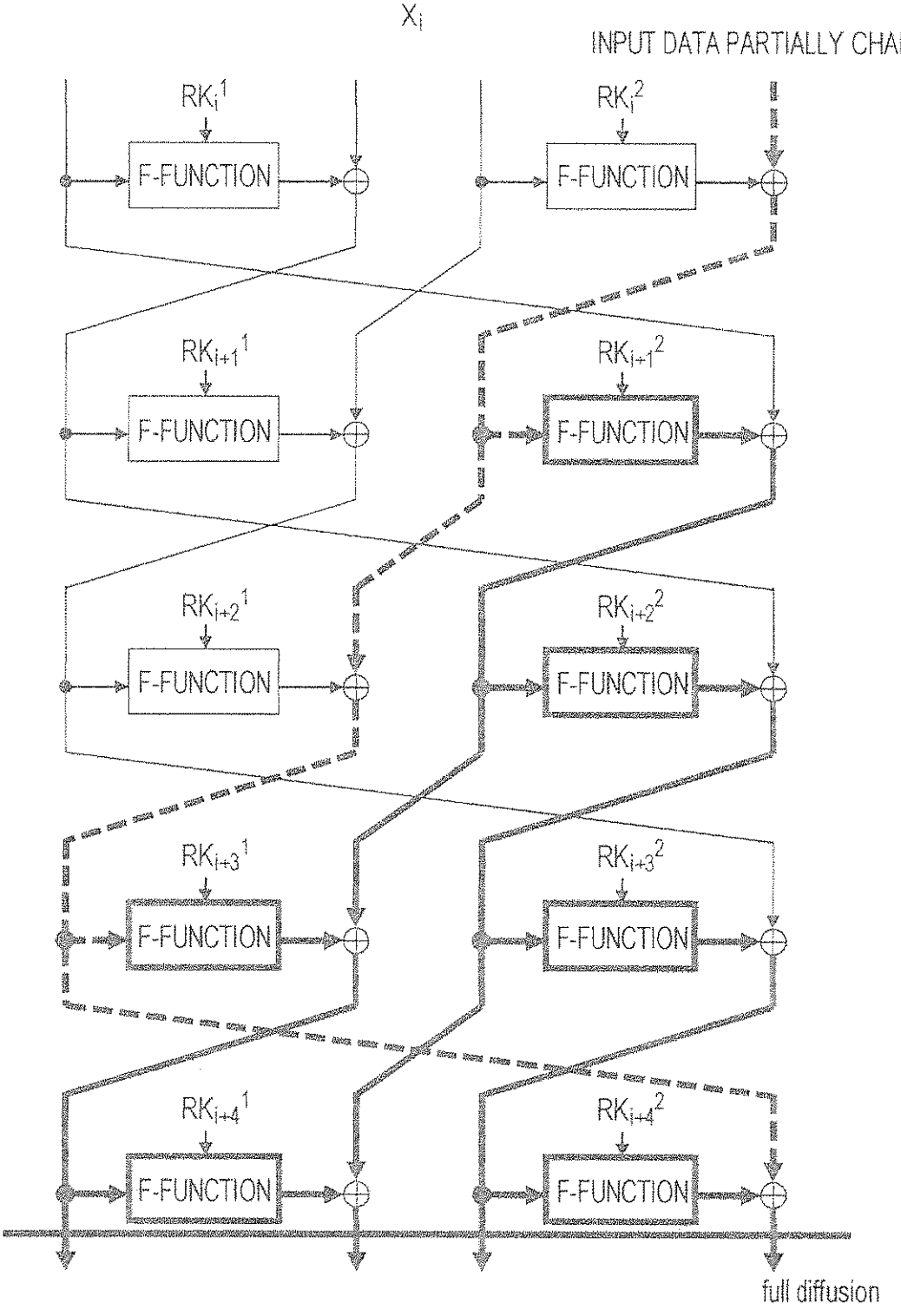

X_i
INPUT DATA PARTIALLY CHANGED
RK_i^1
F-FUNCTION
RK_i^2
F-FUNCTION
RK_{i+1}^1
F-FUNCTION
RK_{i+1}^2
F-FUNCTION
RK_{i+2}^1
F-FUNCTION
RK_{i+2}^2
F-FUNCTION
RK_{i+3}^1
F-FUNCTION
RK_{i+3}^2
F-FUNCTION
RK_{i+4}^1
F-FUNCTION
RK_{i+4}^2
F-FUNCTION
full diffusion

FIG. 16

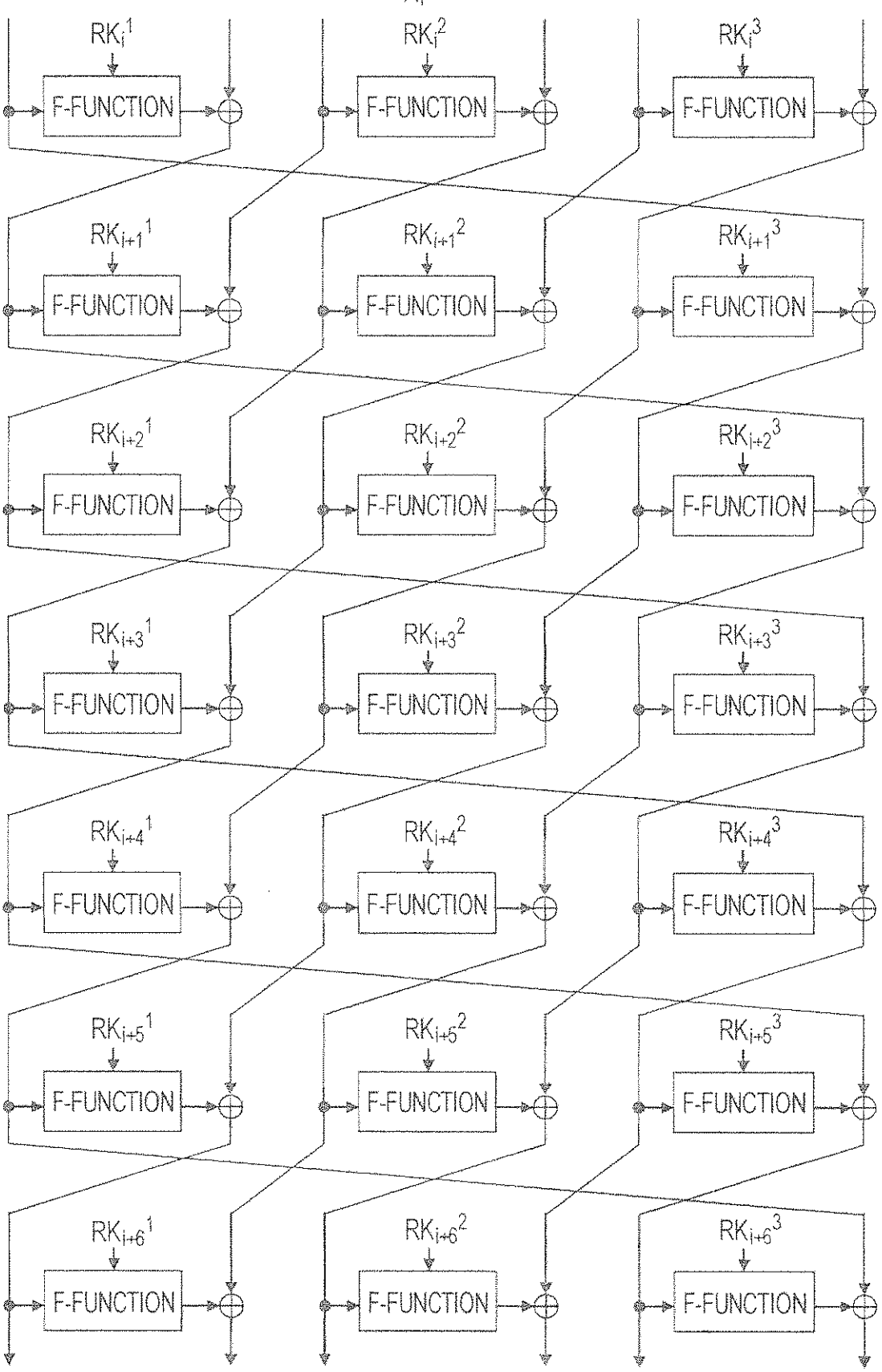

X_i
RK_i^1
RK_i^2
RK_i^3
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3
RK_{i+4}^1
RK_{i+4}^2
RK_{i+4}^3
RK_{i+5}^1
RK_{i+5}^2
RK_{i+5}^3
RK_{i+6}^1
RK_{i+6}^2
RK_{i+6}^3
F-FUNCTION

FIG. 17

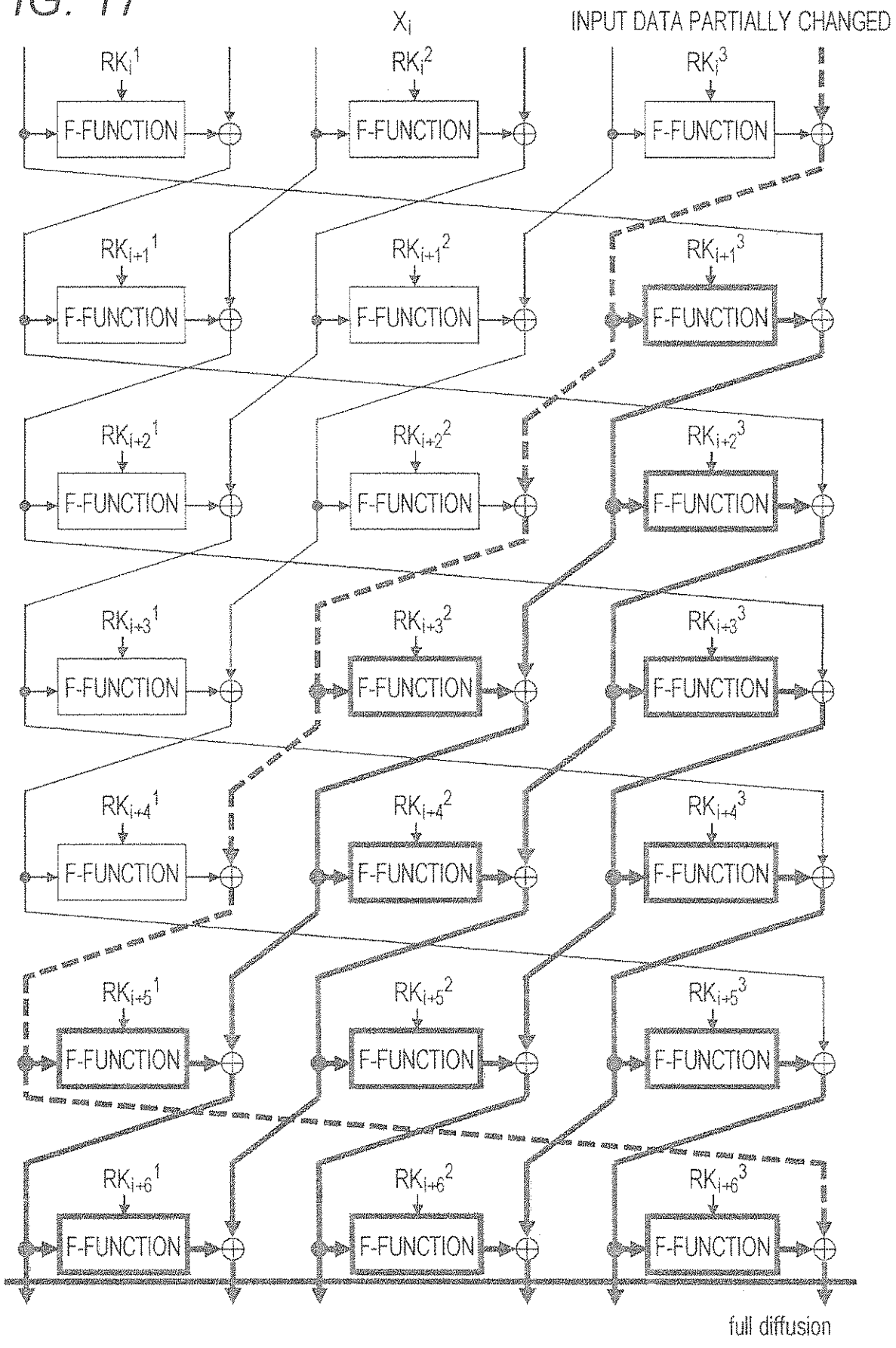

X_i
INPUT DATA PARTIALLY CHANGED
RK_i^1
RK_i^2
RK_i^3
F-FUNCTION
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3
RK_{i+4}^1
RK_{i+4}^2
RK_{i+4}^3
RK_{i+5}^1
RK_{i+5}^2
RK_{i+5}^3
RK_{i+6}^1
RK_{i+6}^2
RK_{i+6}^3
full diffusion

FIG. 18

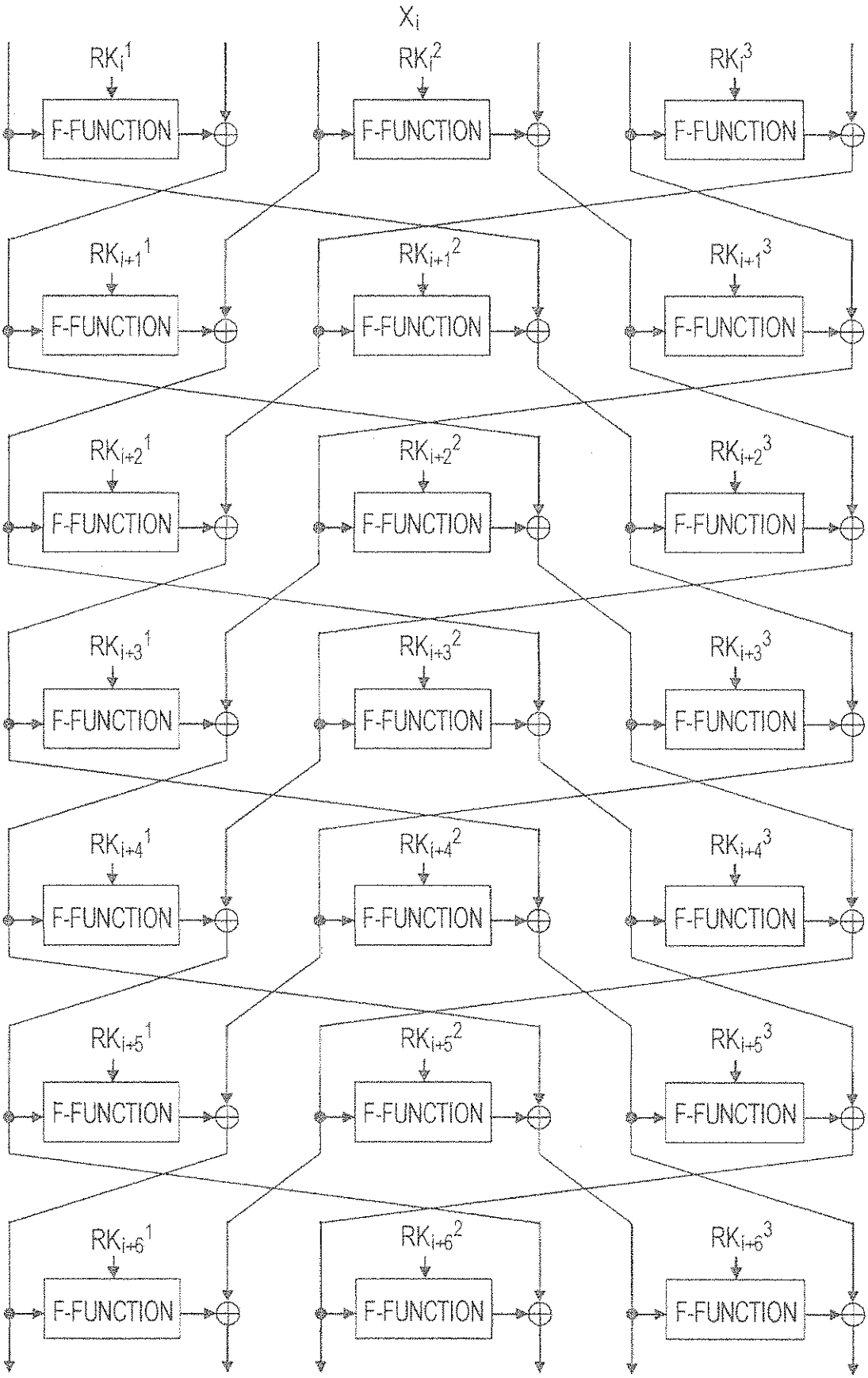

X_i
RK_i^1
RK_i^2
RK_i^3
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3
RK_{i+4}^1
RK_{i+4}^2
RK_{i+4}^3
RK_{i+5}^1
RK_{i+5}^2
RK_{i+5}^3
RK_{i+6}^1
RK_{i+6}^2
RK_{i+6}^3
F-FUNCTION

FIG. 19

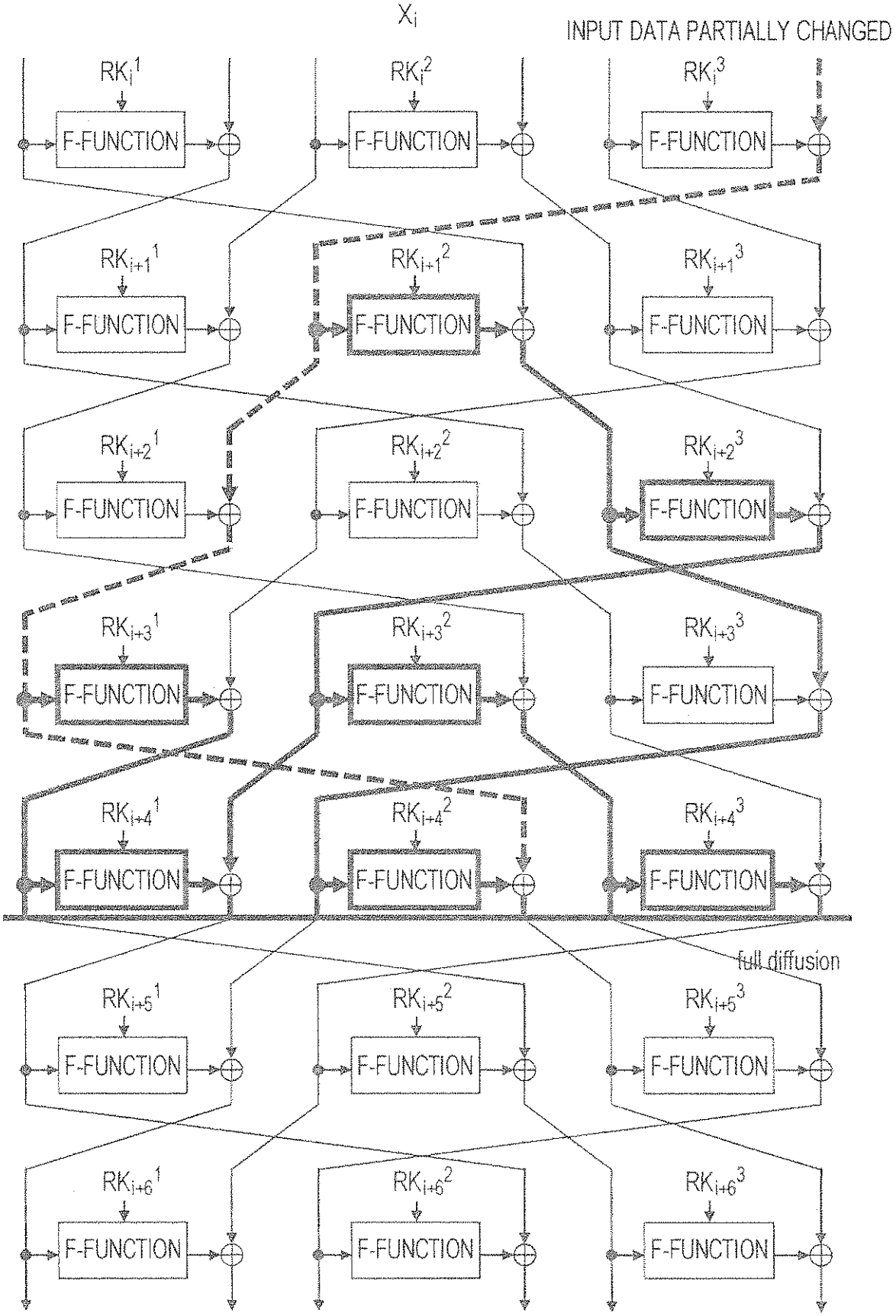

X_i
INPUT DATA PARTIALLY CHANGED
RK_i^1
RK_i^2
RK_i^3
F-FUNCTION
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3
RK_{i+4}^1
RK_{i+4}^2
RK_{i+4}^3
full diffusion
RK_{i+5}^1
RK_{i+5}^2
RK_{i+5}^3
RK_{i+6}^1
RK_{i+6}^2
RK_{i+6}^3

FIG. 20

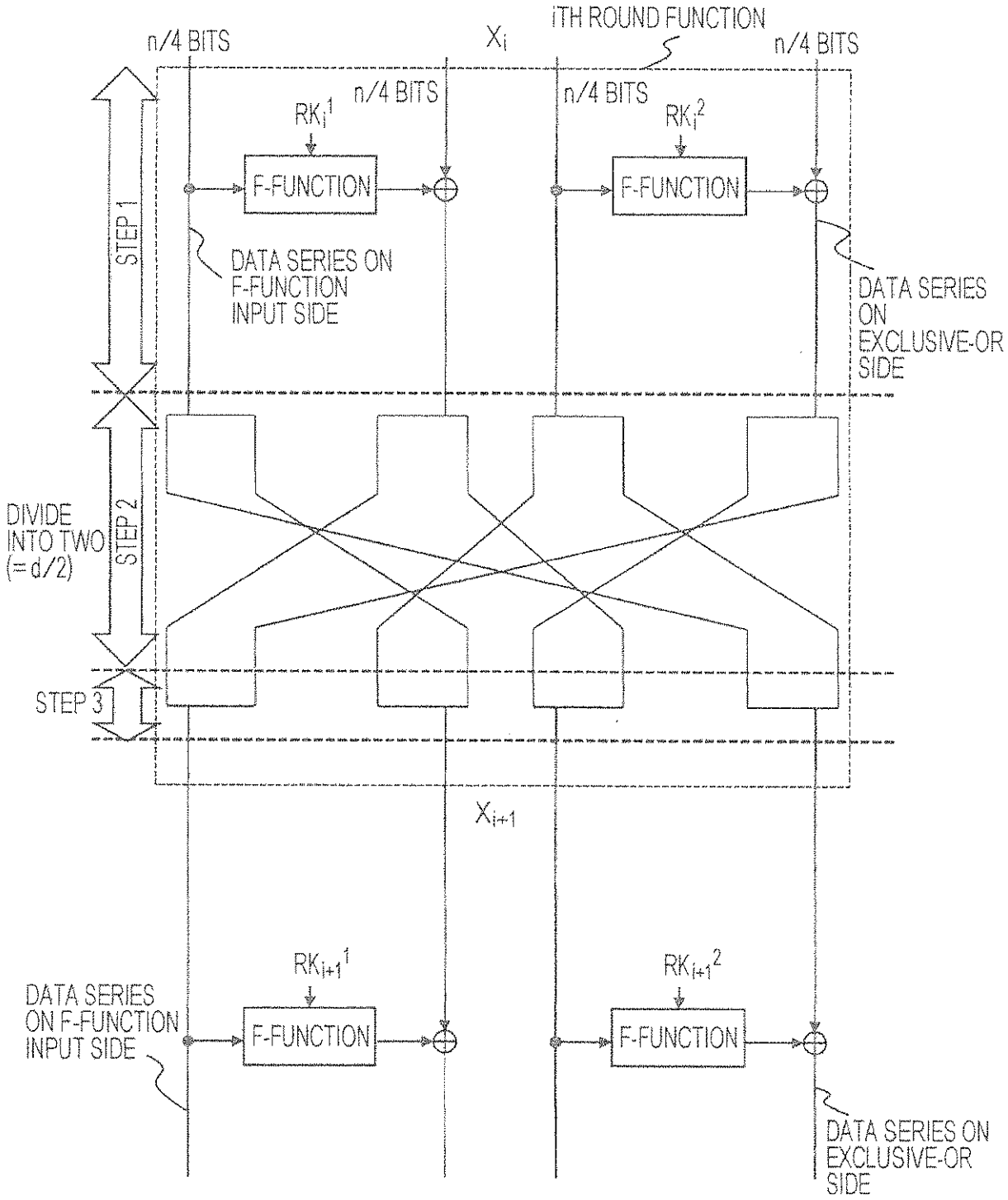

n/4 BITS
Xi
iTH ROUND FUNCTION
n/4 BITS
n/4 BITS
n/4 BITS
RKi1
RKi2
F-FUNCTION
F-FUNCTION
STEP 1
DATA SERIES ON F-FUNCTION INPUT SIDE
DATA SERIES ON EXCLUSIVE-OR SIDE
DIVIDE INTO TWO (=d/2)
STEP 2
STEP 3
Xi+1
RKi+11
RKi+12
DATA SERIES ON F-FUNCTION INPUT SIDE
F-FUNCTION
F-FUNCTION
DATA SERIES ON EXCLUSIVE-OR SIDE

FIG. 21

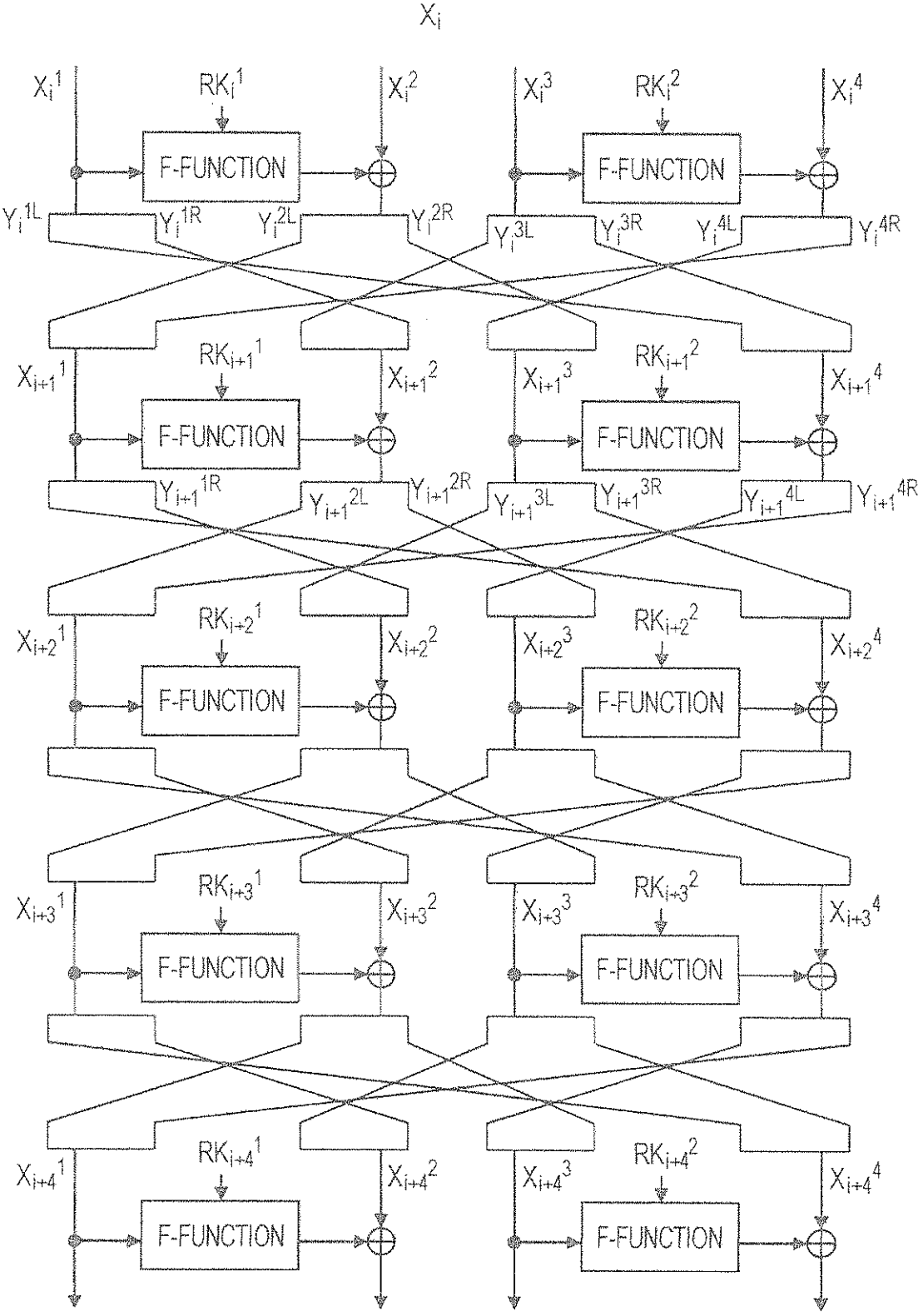

Xi
Xi1
RKi1
Xi2
Xi3
RKi2
Xi4
F-FUNCTION
Yi1L
Yi1R
Yi2L
Yi2R
Yi3L
Yi3R
Yi4L
Yi4R
Xi+11
RKi+11
Xi+12
Xi+13
RKi+12
Xi+14
Yi+11R
Yi+12L
Yi+12R
Yi+13L
Yi+13R
Yi+14L
Yi+14R
Xi+21
RKi+21
Xi+22
Xi+23
RKi+22
Xi+24
Xi+31
RKi+31
Xi+32
Xi+33
RKi+32
Xi+34
Xi+41
RKi+41
Xi+42
Xi+43
RKi+42
Xi+44

FIG. 22

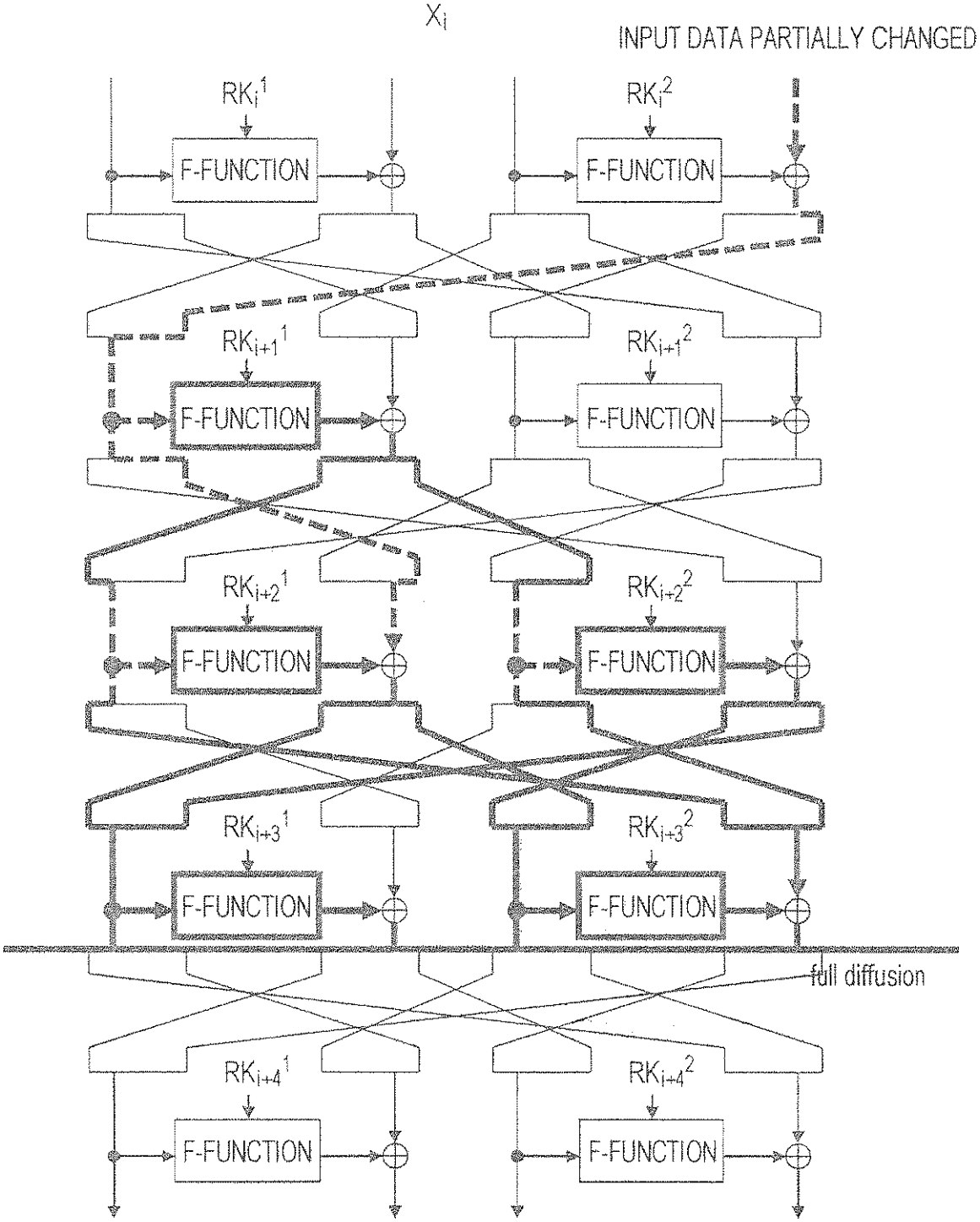

X_i
INPUT DATA PARTIALLY CHANGED
RK_i^1
RK_i^2
F-FUNCTION
F-FUNCTION
RK_{i+1}^1
RK_{i+1}^2
F-FUNCTION
F-FUNCTION
RK_{i+2}^1
RK_{i+2}^2
F-FUNCTION
F-FUNCTION
RK_{i+3}^1
RK_{i+3}^2
F-FUNCTION
F-FUNCTION
full diffusion
RK_{i+4}^1
RK_{i+4}^2
F-FUNCTION
F-FUNCTION

FIG. 23

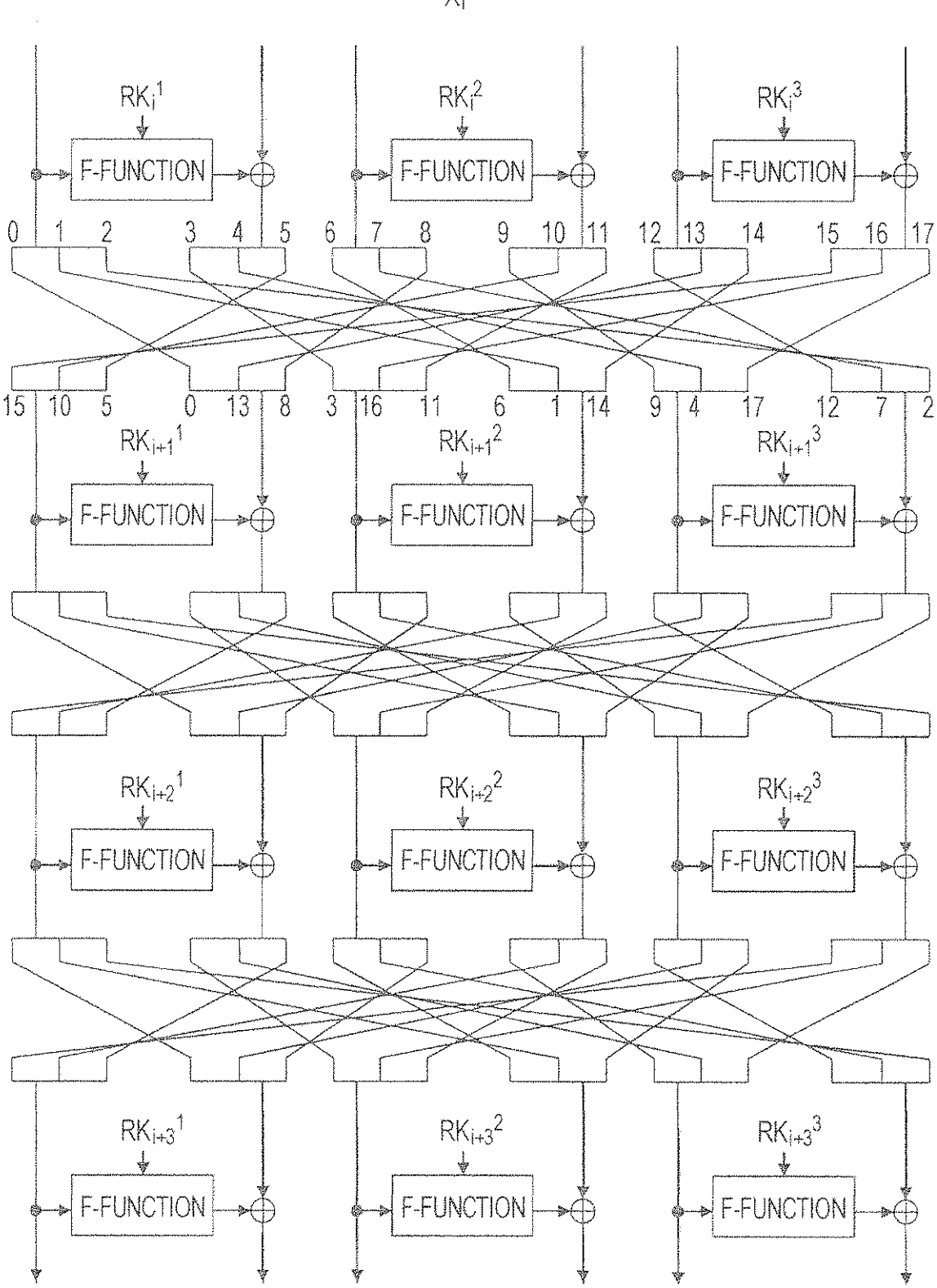

X_i
RK_i^1
RK_i^2
RK_i^3
F-FUNCTION
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
15 10 5 0 13 8 3 16 11 6 1 14 9 4 17 12 7 2
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3

FIG. 24

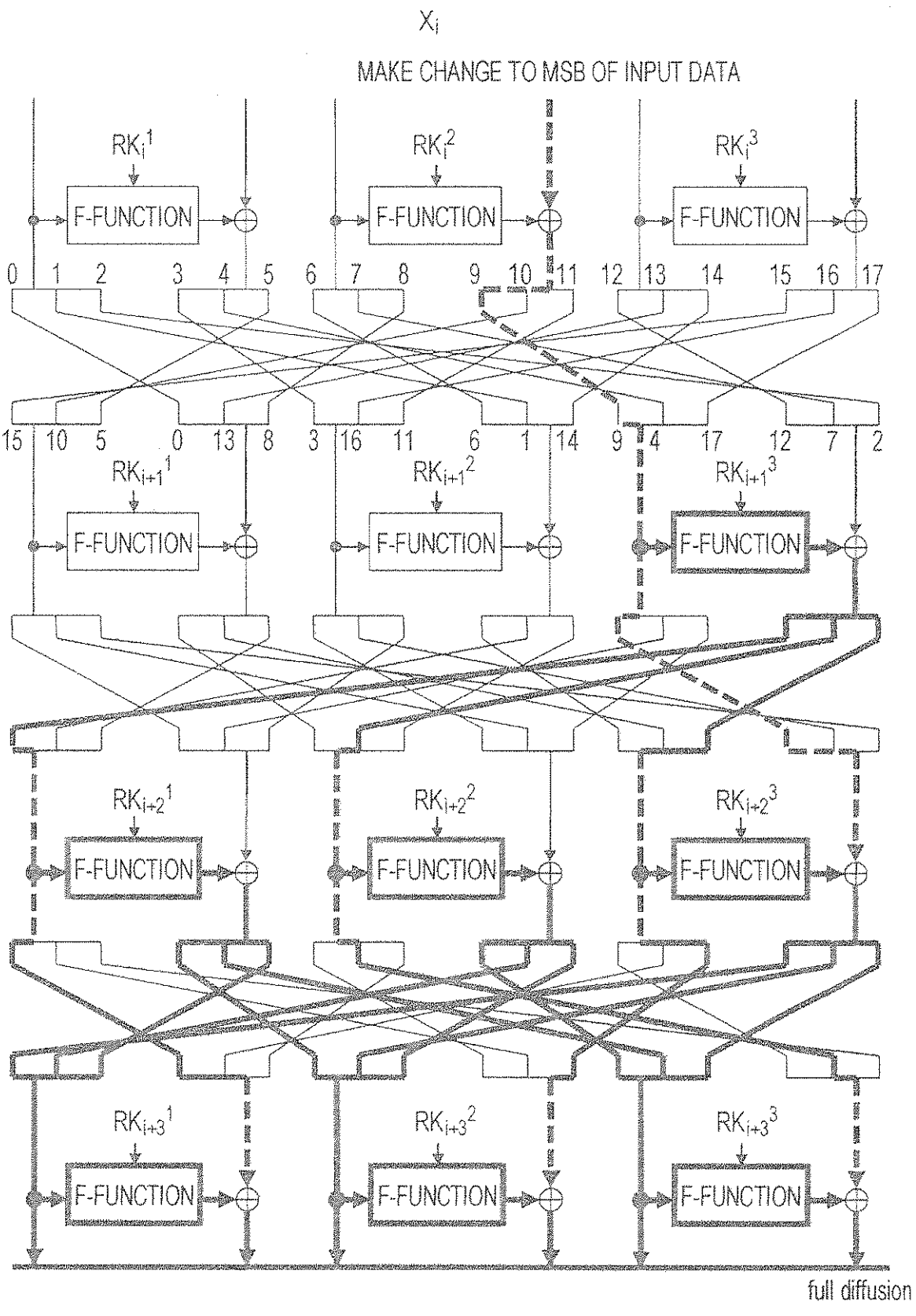

X_i
MAKE CHANGE TO MSB OF INPUT DATA
RK_i^1
RK_i^2
RK_i^3
F-FUNCTION
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
15 10 5 0 13 8 3 16 11 6 1 14 9 4 17 12 7 2
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3
full diffusion

FIG. 25

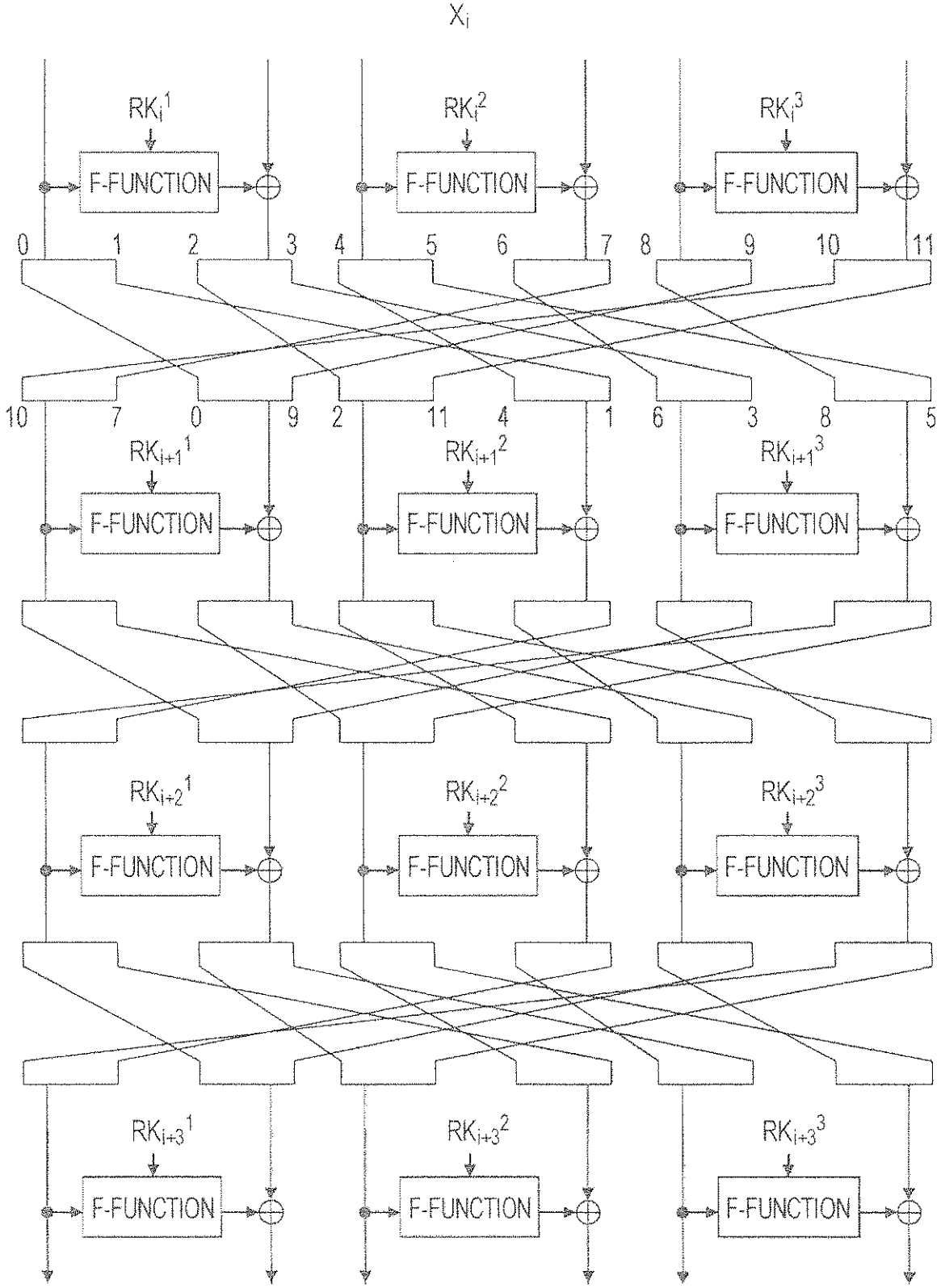

Xi
RKi1
RKi2
RKi3
F-FUNCTION
0 1 2 3 4 5 6 7 8 9 10 11
10 7 0 9 2 11 4 1 6 3 8 5
RKi+11
RKi+12
RKi+13
RKi+21
RKi+22
RKi+23
RKi+31
RKi+32
RKi+33

FIG. 26

RELATIONS AMONG n-BIT DATA DIVISION NUMBER d, d/n-BIT DATA DIVISION NUMBER p, AND NUMBER OF full-diffusion ROUNDS

d \ p	2	3	4	5	6	7	8	9	10	11	12
4	4	–	–	–	–	–	–	–	–	–	–
6	5	4	–	–	–	–	–	–	–	–	–
8	5	5	4	–	–	–	–	–	–	–	–
10	6	5	5	4	–	–	–	–	–	–	–
12	6	5	5	5	4	–	–	–	–	–	–
14	6	5	5	5	5	4	–	–	–	–	–
16	6	5	5	5	5	5	4	–	–	–	–
18	7	5	5	5	5	5	5	4	–	–	–
20	7	6	5	5	5	5	5	5	4	–	–
22	7	6	5	5	5	5	5	5	5	4	–
24	7	6	5	5	5	5	5	5	5	5	4

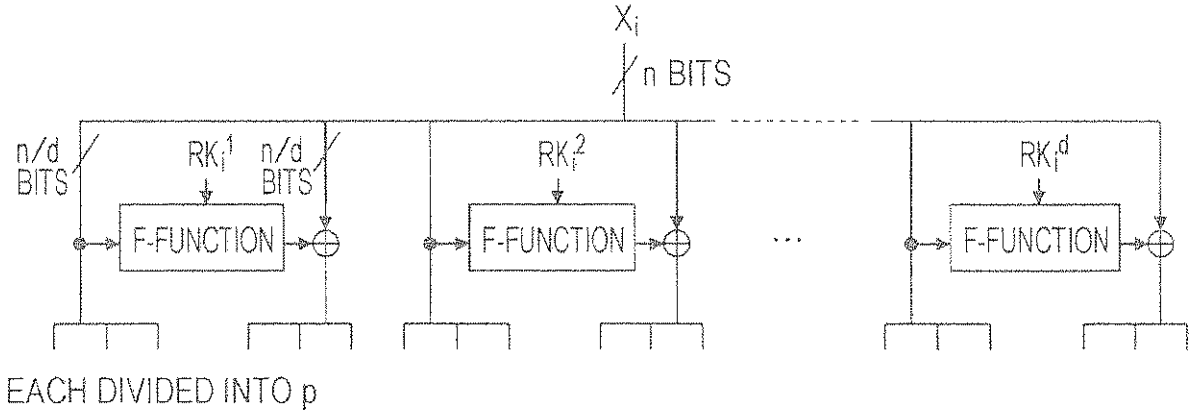


FIG. 27

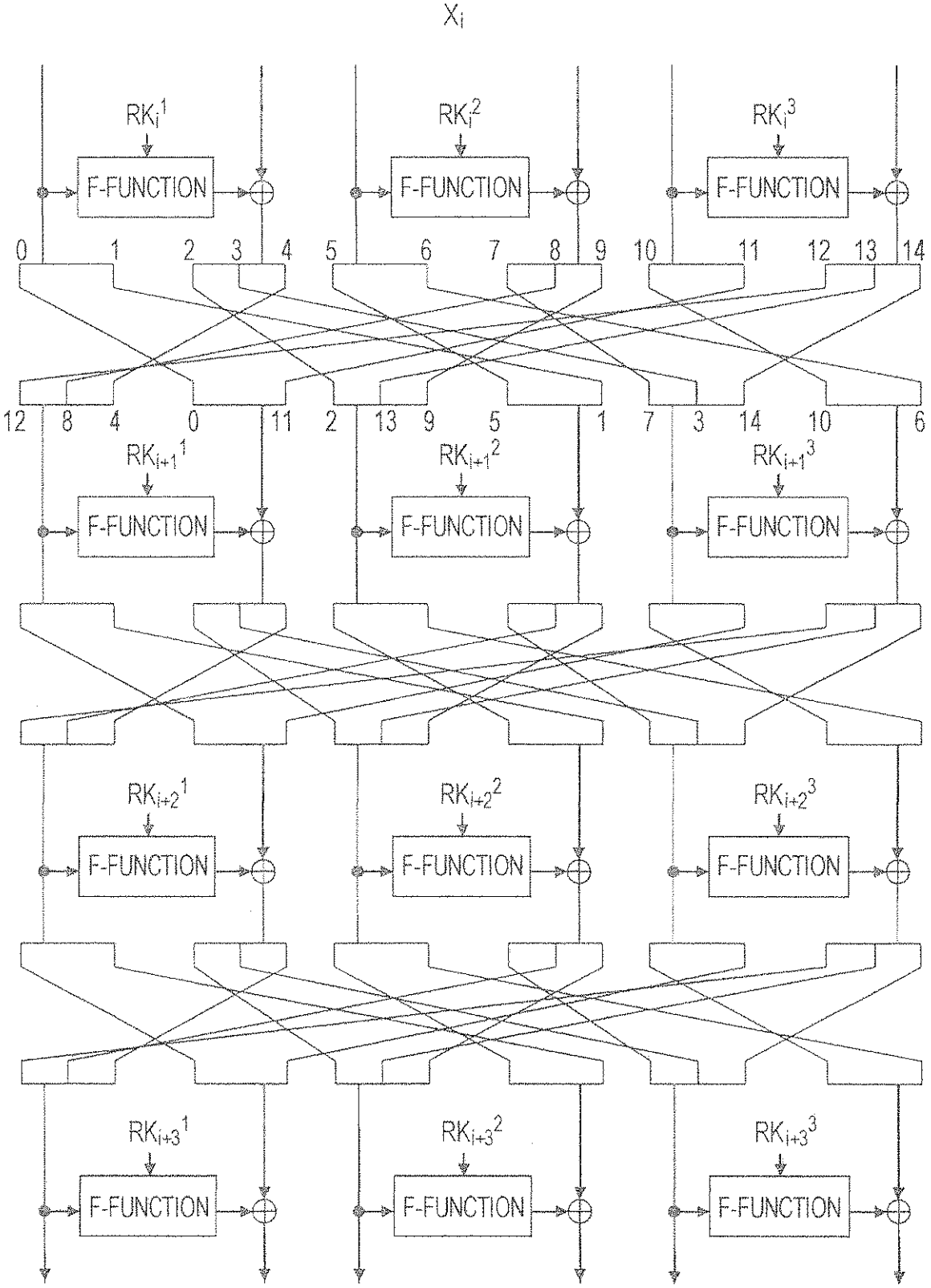

Xi
RKi1
RKi2
RKi3
F-FUNCTION
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
12 8 4 0 11 2 13 9 5 1 7 3 14 10 6
RKi+11
RKi+12
RKi+13
RKi+21
RKi+22
RKi+23
RKi+31
RKi+32
RKi+33

FIG. 28

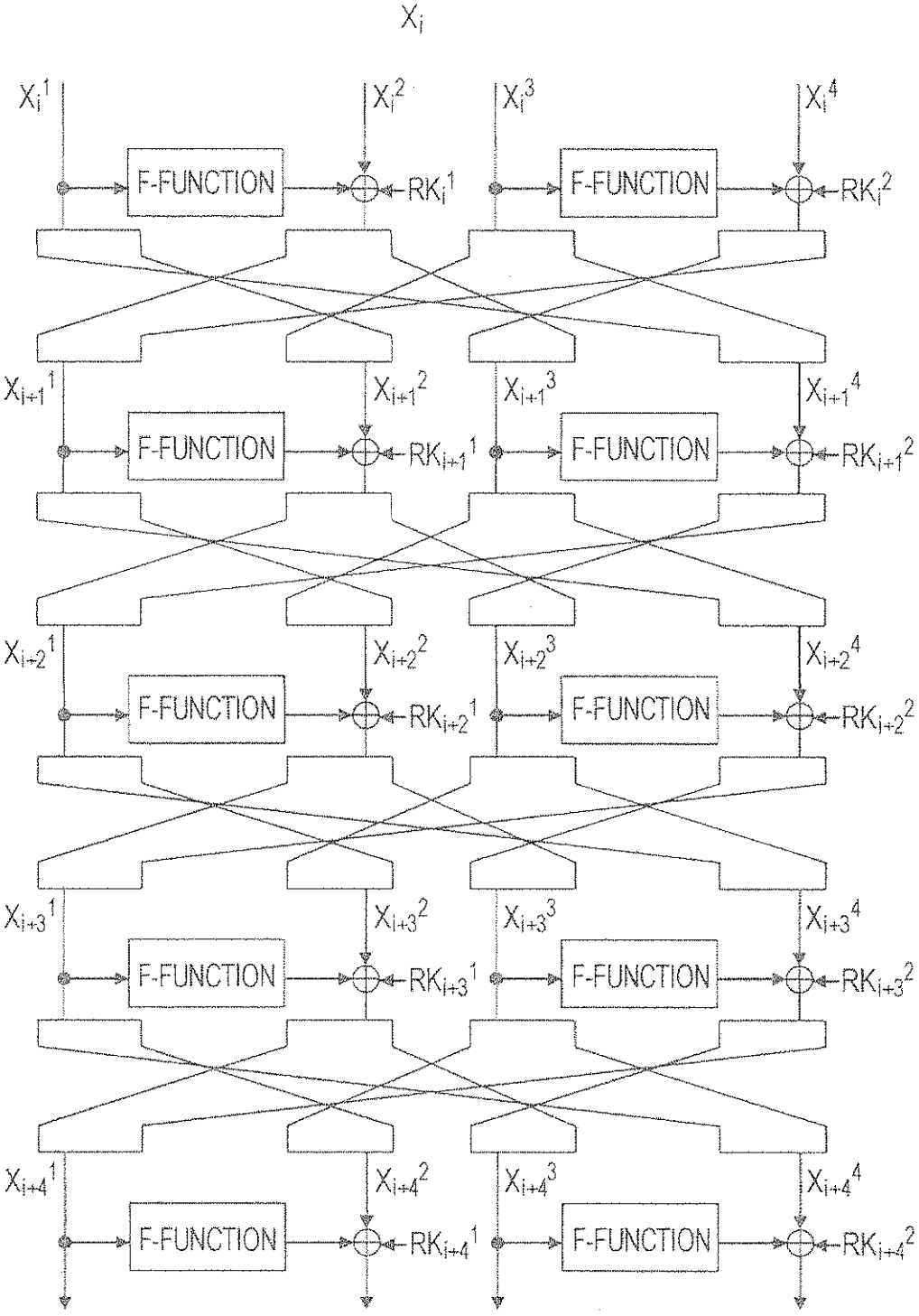

X_i
X_i^1
X_i^2
X_i^3
X_i^4
F-FUNCTION
RK_i^1
F-FUNCTION
RK_i^2
X_{i+1}^1
X_{i+1}^2
X_{i+1}^3
X_{i+1}^4
F-FUNCTION
RK_{i+1}^1
F-FUNCTION
RK_{i+1}^2
X_{i+2}^1
X_{i+2}^2
X_{i+2}^3
X_{i+2}^4
F-FUNCTION
RK_{i+2}^1
F-FUNCTION
RK_{i+2}^2
X_{i+3}^1
X_{i+3}^2
X_{i+3}^3
X_{i+3}^4
F-FUNCTION
RK_{i+3}^1
F-FUNCTION
RK_{i+3}^2
X_{i+4}^1
X_{i+4}^2
X_{i+4}^3
X_{i+4}^4
F-FUNCTION
RK_{i+4}^1
F-FUNCTION
RK_{i+4}^2

FIG. 29

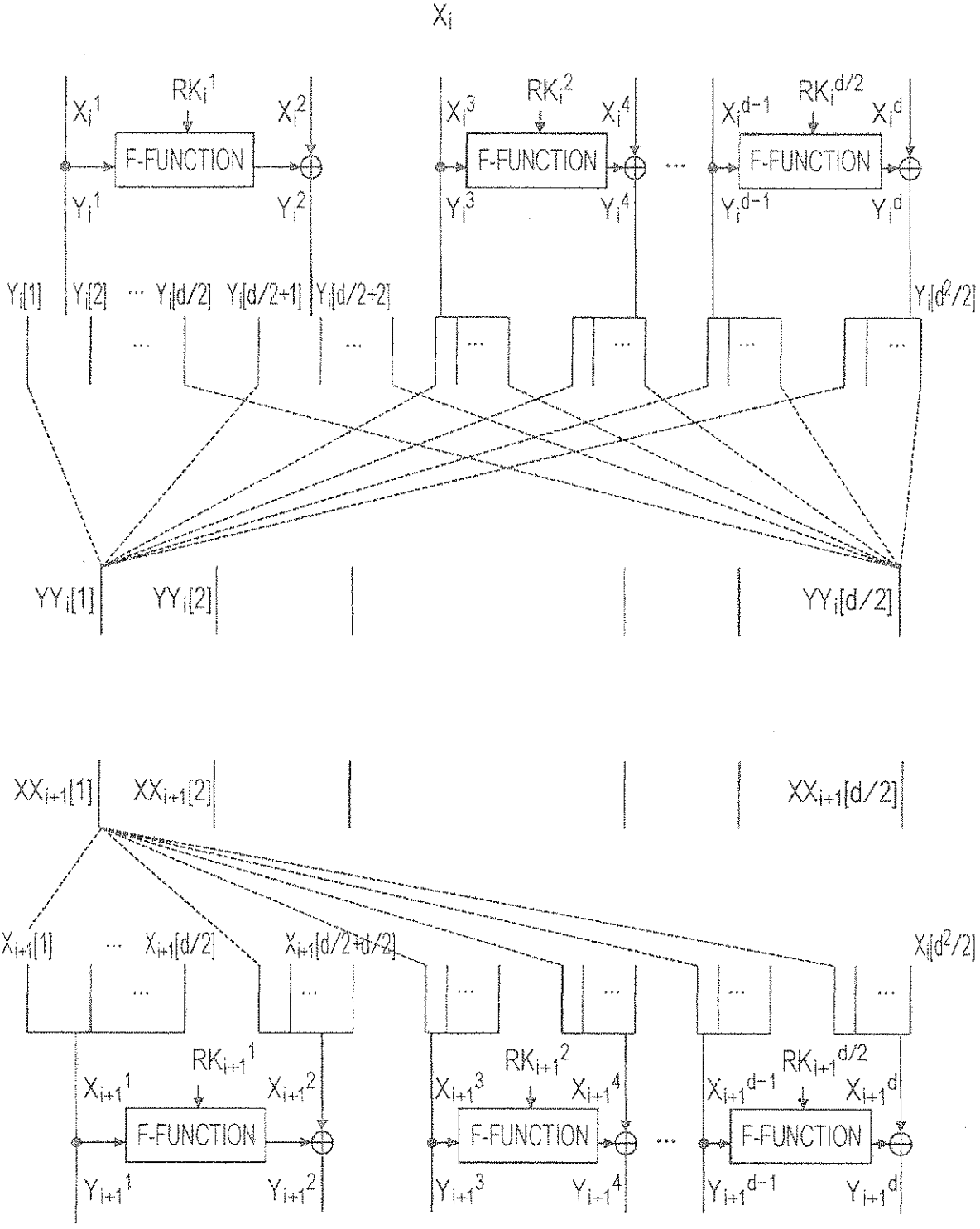

Xi
Xi1
RKi1
Xi2
F-FUNCTION
Yi1
Yi2
Xi3
RKi2
Xi4
F-FUNCTION
Yi3
Yi4
Xid-1
RKid/2
Xid
F-FUNCTION
Yid-1
Yid
Yi[1]
Yi[2]
Yi[d/2]
Yi[d/2+1]
Yi[d/2+2]
Yi[d2/2]
YYi[1]
YYi[2]
YYi[d/2]
XXi+1[1]
XXi+1[2]
XXi+1[d/2]
Xi+1[1]
Xi+1[d/2]
Xi+1[d/2+d/2]
Xi+1[d2/2]
RKi+11
Xi+11
Xi+12
F-FUNCTION
Yi+11
Yi+12
RKi+12
Xi+13
Xi+14
F-FUNCTION
Yi+13
Yi+14
RKi+1d/2
Xi+1d-1
Xi+1d
F-FUNCTION
Yi+1d-1
Yi+1d

FIG. 30

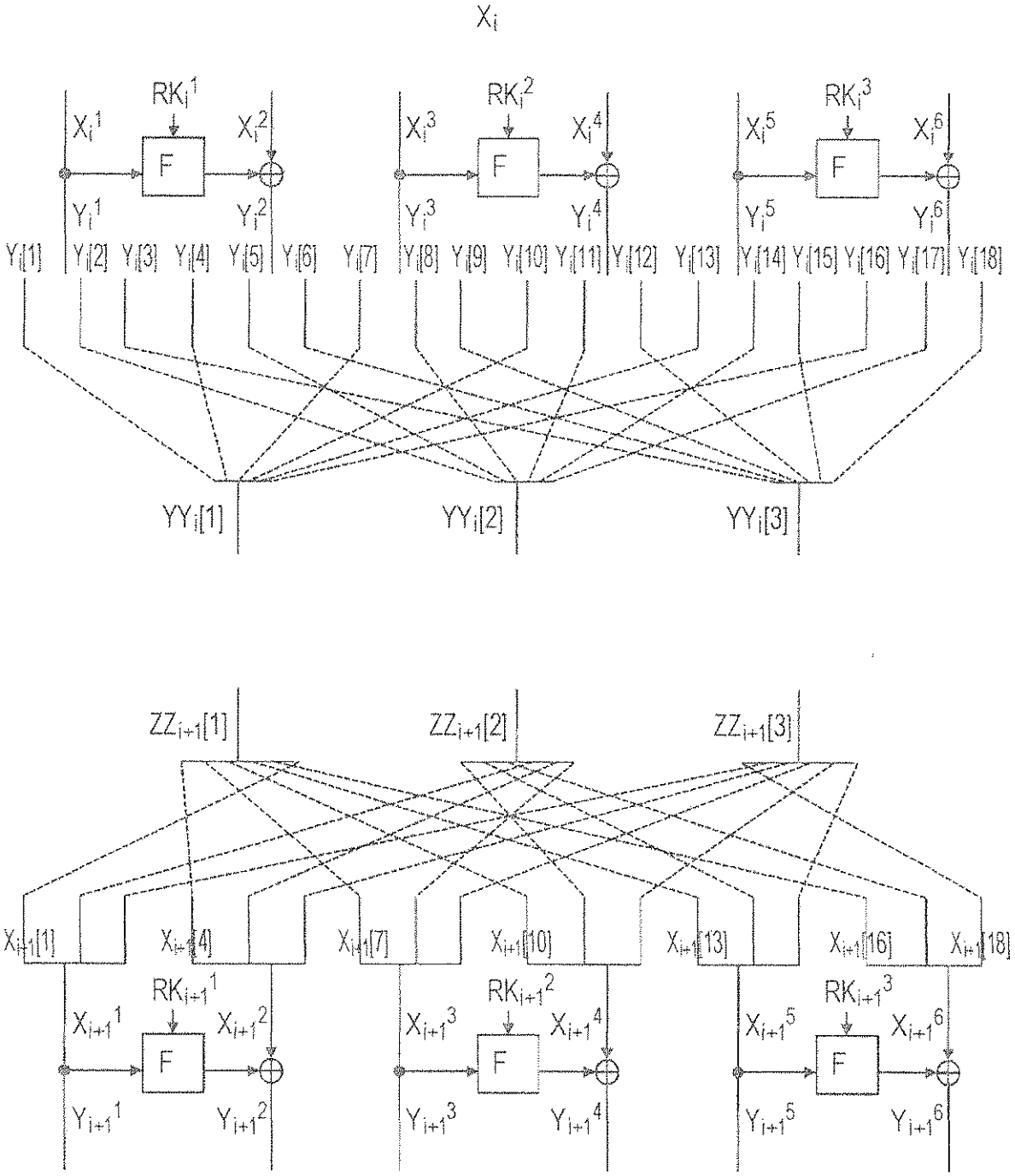

X_i
RK_i^1
RK_i^2
RK_i^3
F
$Y_i[1]$ $Y_i[2]$ $Y_i[3]$ $Y_i[4]$ $Y_i[5]$ $Y_i[6]$ $Y_i[7]$ $Y_i[8]$ $Y_i[9]$ $Y_i[10]$ $Y_i[11]$ $Y_i[12]$ $Y_i[13]$ $Y_i[14]$ $Y_i[15]$ $Y_i[16]$ $Y_i[17]$ $Y_i[18]$
$YY_i[1]$ $YY_i[2]$ $YY_i[3]$
$ZZ_{i+1}[1]$ $ZZ_{i+1}[2]$ $ZZ_{i+1}[3]$
$X_{i+1}[1]$ $X_{i+1}[4]$ $X_{i+1}[7]$ $X_{i+1}[10]$ $X_{i+1}[13]$ $X_{i+1}[16]$ $X_{i+1}[18]$
RK_{i+1}^1 RK_{i+1}^2 RK_{i+1}^3
Y_{i+1}^1 Y_{i+1}^2 Y_{i+1}^3 Y_{i+1}^4 Y_{i+1}^5 Y_{i+1}^6

FIG. 31

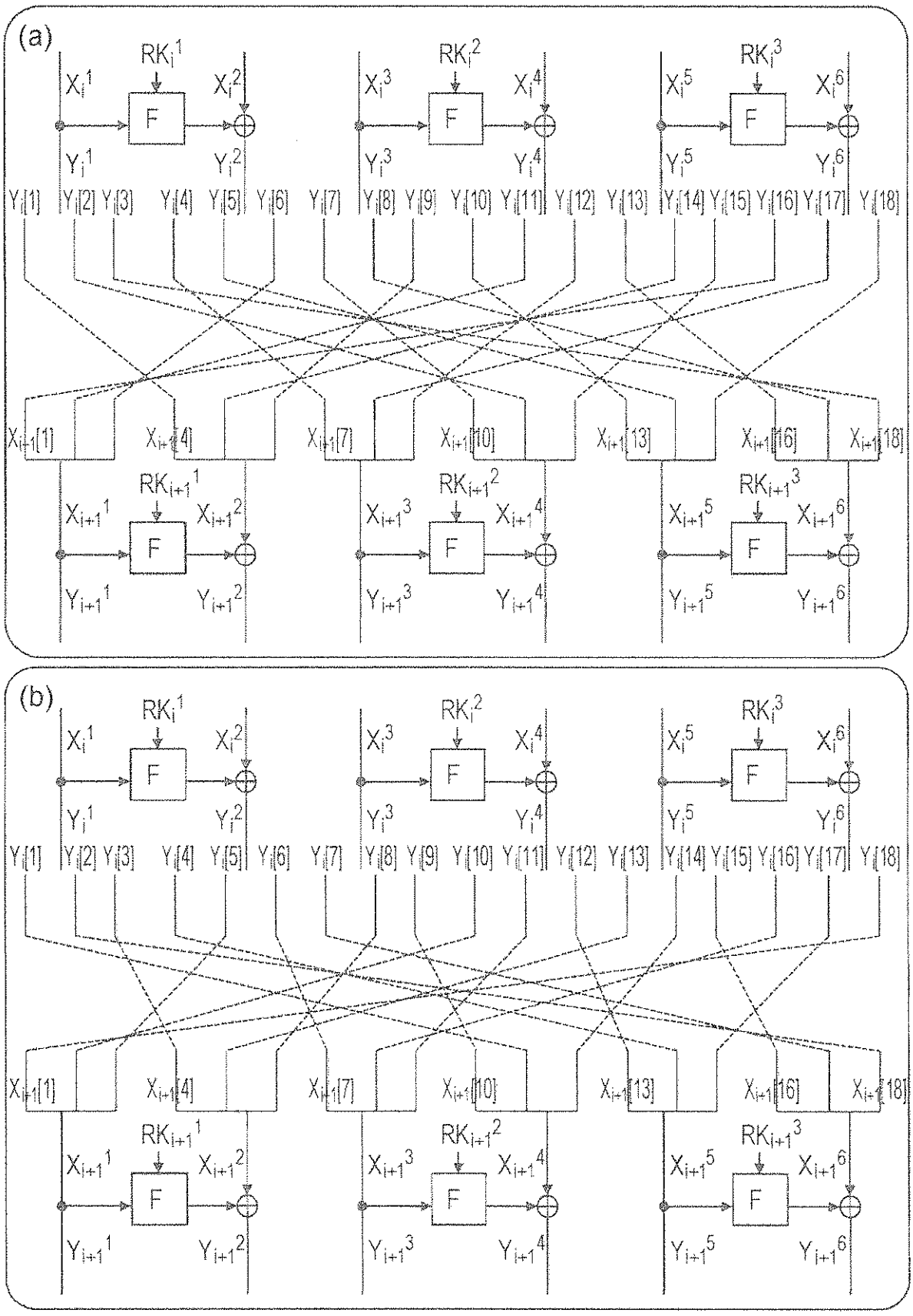

(a)
RKi1
RKi2
RKi3
Xi1
Xi2
Xi3
Xi4
Xi5
Xi6
F
Yi1
Yi2
Yi3
Yi4
Yi5
Yi6
Yi[1] Yi[2] Yi[3] Yi[4] Yi[5] Yi[6] Yi[7] Yi[8] Yi[9] Yi[10] Yi[11] Yi[12] Yi[13] Yi[14] Yi[15] Yi[16] Yi[17] Yi[18]
Xi+1[1] Xi+1[4] Xi+1[7] Xi+1[10] Xi+1[13] Xi+1[16] Xi+1[18]
RKi+11
RKi+12
RKi+13
Xi+11
Xi+12
Xi+13
Xi+14
Xi+15
Xi+16
Yi+11
Yi+12
Yi+13
Yi+14
Yi+15
Yi+16
(b)
RKi1
RKi2
RKi3
Xi1
Xi2
Xi3
Xi4
Xi5
Xi6
F
Yi1
Yi2
Yi3
Yi4
Yi5
Yi6
Yi[1] Yi[2] Yi[3] Yi[4] Yi[5] Yi[6] Yi[7] Yi[8] Yi[9] Yi[10] Yi[11] Yi[12] Yi[13] Yi[14] Yi[15] Yi[16] Yi[17] Yi[18]
Xi+1[1] Xi+1[4] Xi+1[7] Xi+1[10] Xi+1[13] Xi+1[16] Xi+1[18]
RKi+11
RKi+12
RKi+13
Xi+11
Xi+12
Xi+13
Xi+14
Xi+15
Xi+16
Yi+11
Yi+12
Yi+13
Yi+14
Yi+15
Yi+16

FIG. 32

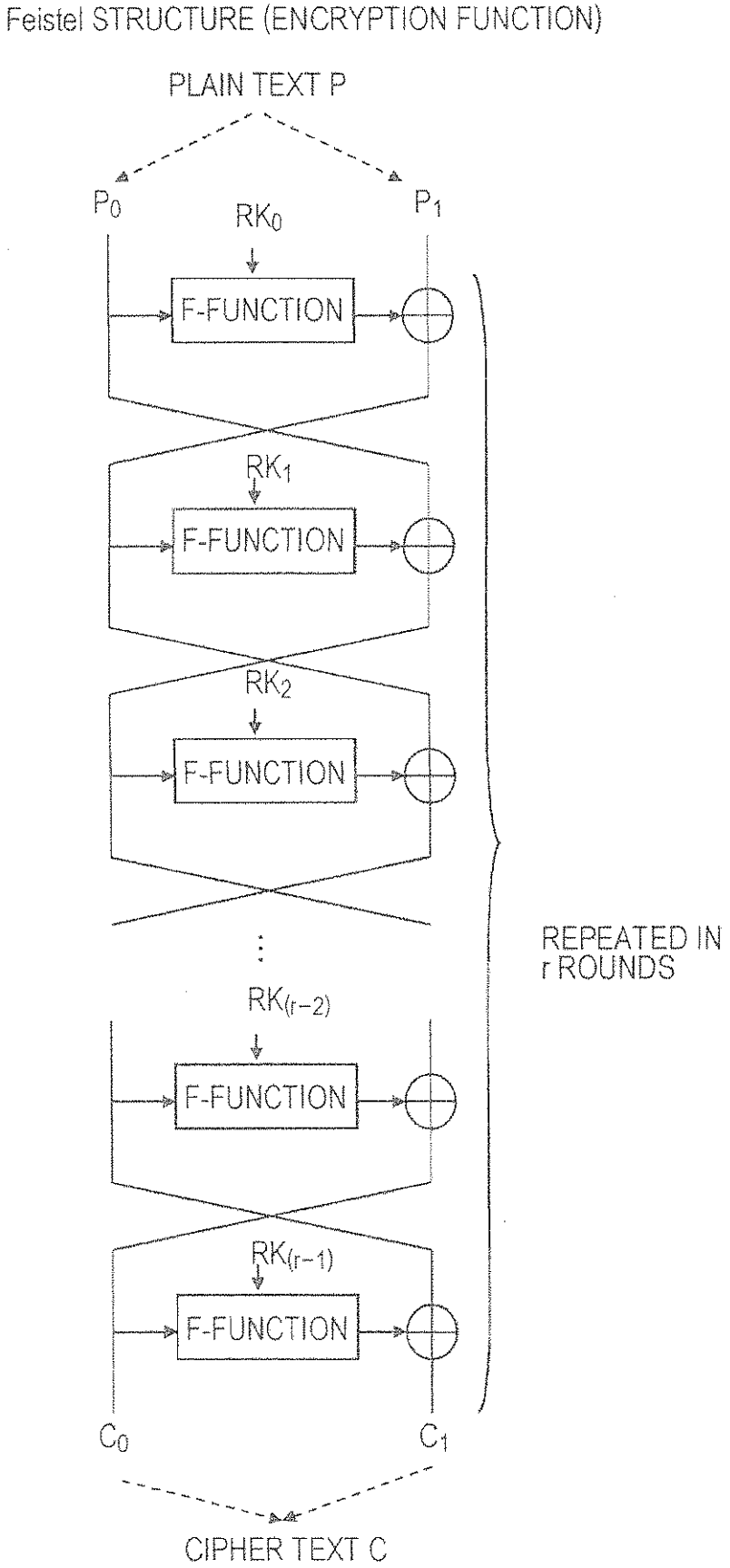

Feistel STRUCTURE (ENCRYPTION FUNCTION)
PLAIN TEXT P
P0
P1
RK0
F-FUNCTION
RK1
F-FUNCTION
RK2
F-FUNCTION
RK(r−2)
F-FUNCTION
RK(r−1)
F-FUNCTION
REPEATED IN r ROUNDS
C0
C1
CIPHER TEXT C

FIG. 33

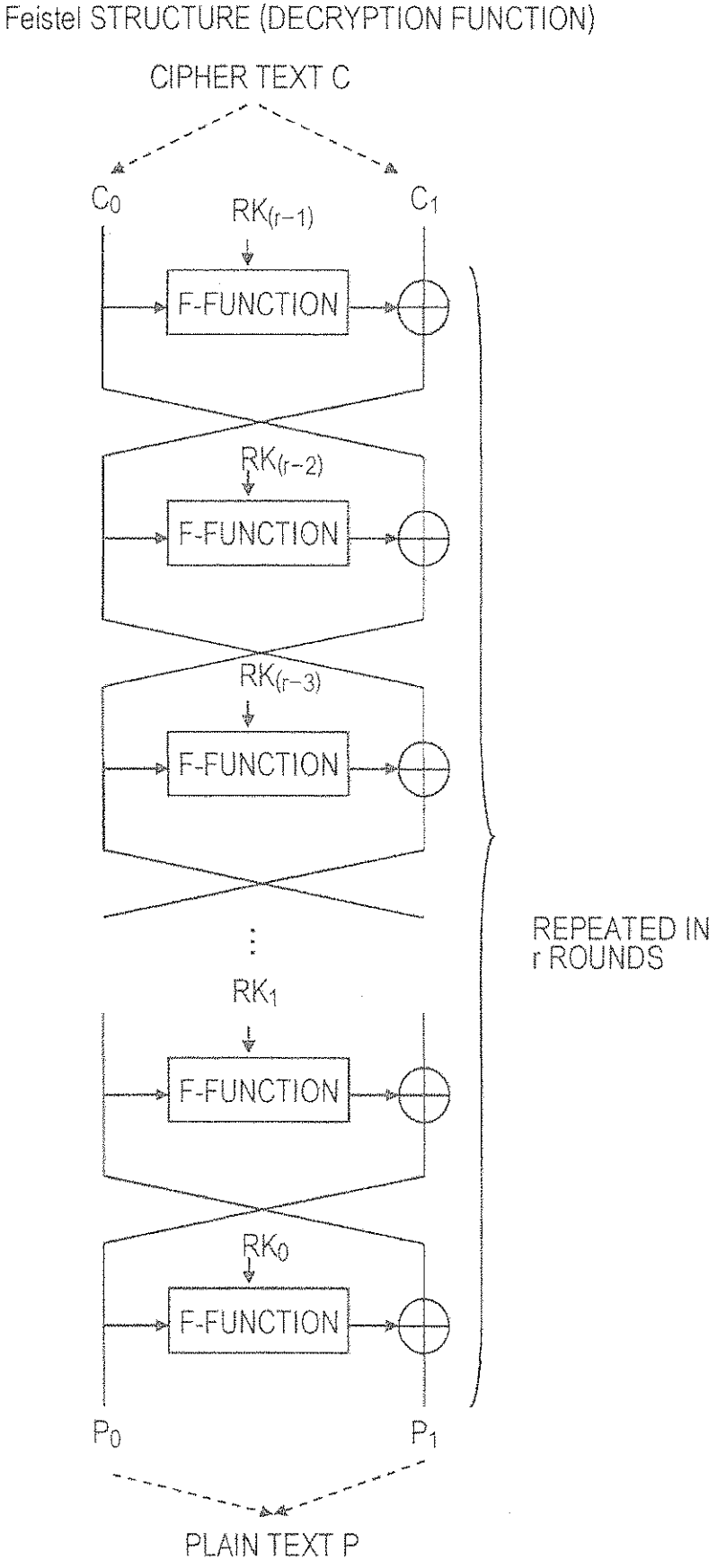

Feistel STRUCTURE (DECRYPTION FUNCTION)
CIPHER TEXT C
C0
C1
RK(r-1)
F-FUNCTION
RK(r-2)
F-FUNCTION
RK(r-3)
F-FUNCTION
RK1
F-FUNCTION
RK0
F-FUNCTION
REPEATED IN r ROUNDS
P0
P1
PLAIN TEXT P

FIG. 34

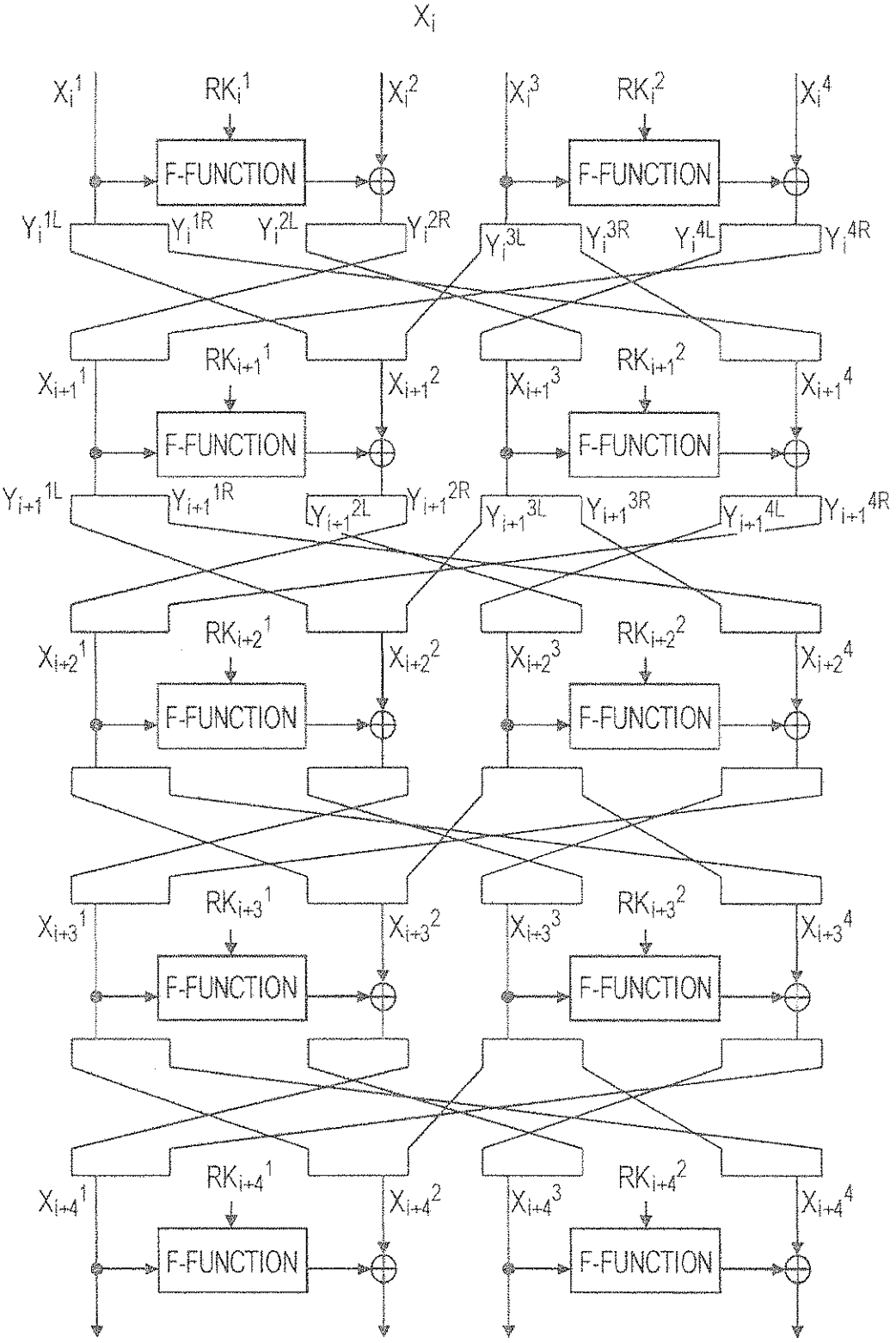

X_i
X_i^1
RK_i^1
X_i^2
X_i^3
RK_i^2
X_i^4
F-FUNCTION
F-FUNCTION
Y_i^{1L}
Y_i^{1R}
Y_i^{2L}
Y_i^{2R}
Y_i^{3L}
Y_i^{3R}
Y_i^{4L}
Y_i^{4R}
RK_{i+1}^1
X_{i+1}^1
X_{i+1}^2
RK_{i+1}^2
X_{i+1}^3
X_{i+1}^4
F-FUNCTION
F-FUNCTION
Y_{i+1}^{1L}
Y_{i+1}^{1R}
Y_{i+1}^{2L}
Y_{i+1}^{2R}
Y_{i+1}^{3L}
Y_{i+1}^{3R}
Y_{i+1}^{4L}
Y_{i+1}^{4R}
RK_{i+2}^1
X_{i+2}^1
X_{i+2}^2
RK_{i+2}^2
X_{i+2}^3
X_{i+2}^4
F-FUNCTION
F-FUNCTION
RK_{i+3}^1
X_{i+3}^1
X_{i+3}^2
RK_{i+3}^2
X_{i+3}^3
X_{i+3}^4
F-FUNCTION
F-FUNCTION
RK_{i+4}^1
X_{i+4}^1
X_{i+4}^2
RK_{i+4}^2
X_{i+4}^3
X_{i+4}^4
F-FUNCTION
F-FUNCTION

FIG. 35

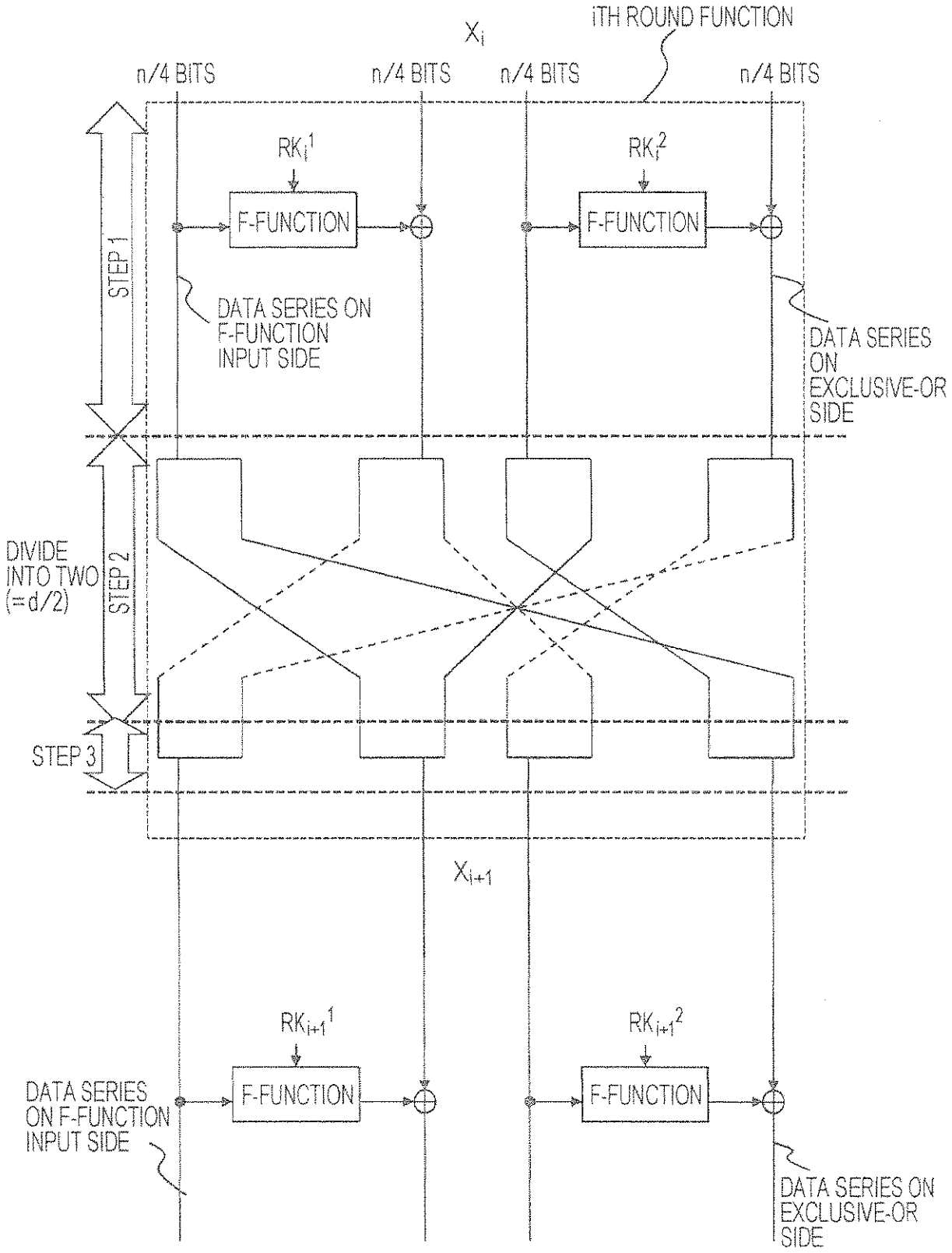

X_i
iTH ROUND FUNCTION
n/4 BITS
n/4 BITS
n/4 BITS
n/4 BITS
RK_i^1
RK_i^2
F-FUNCTION
F-FUNCTION
STEP 1
DATA SERIES ON F-FUNCTION INPUT SIDE
DATA SERIES ON EXCLUSIVE-OR SIDE
DIVIDE INTO TWO (=d/2)
STEP 2
STEP 3
X_{i+1}
RK_{i+1}^1
RK_{i+1}^2
F-FUNCTION
F-FUNCTION
DATA SERIES ON F-FUNCTION INPUT SIDE
DATA SERIES ON EXCLUSIVE-OR SIDE

FIG. 36

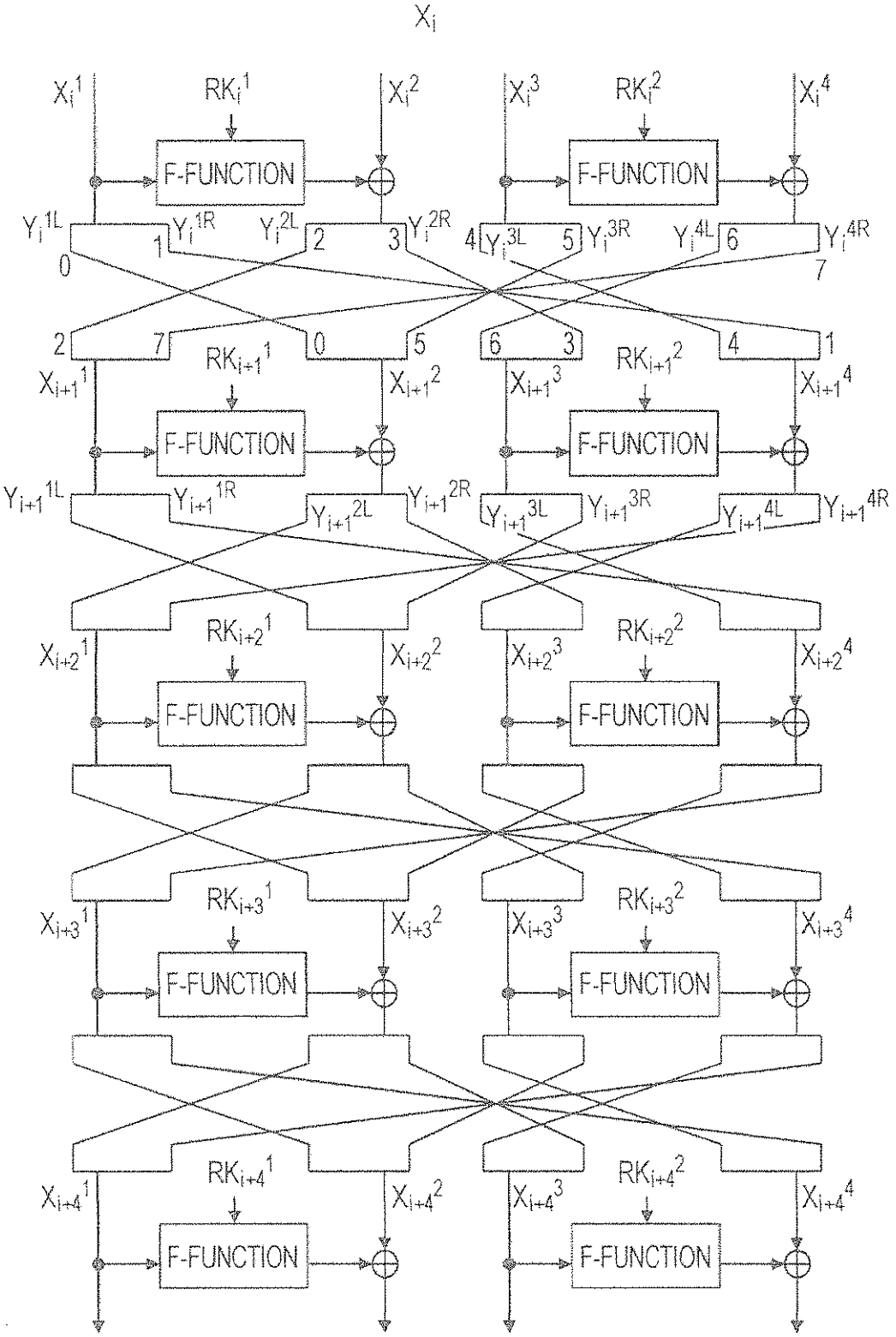

X_i
X_i^1
RK_i^1
X_i^2
X_i^3
RK_i^2
X_i^4
F-FUNCTION
Y_i^{1L}
Y_i^{1R}
Y_i^{2L}
Y_i^{2R}
Y_i^{3L}
Y_i^{3R}
Y_i^{4L}
Y_i^{4R}
0
1
2
3
4
5
6
7
RK_{i+1}^1
X_{i+1}^1
X_{i+1}^2
RK_{i+1}^2
X_{i+1}^3
X_{i+1}^4
Y_{i+1}^{1L}
Y_{i+1}^{1R}
Y_{i+1}^{2L}
Y_{i+1}^{2R}
Y_{i+1}^{3L}
Y_{i+1}^{3R}
Y_{i+1}^{4L}
Y_{i+1}^{4R}
RK_{i+2}^1
X_{i+2}^1
X_{i+2}^2
RK_{i+2}^2
X_{i+2}^3
X_{i+2}^4
RK_{i+3}^1
X_{i+3}^1
X_{i+3}^2
RK_{i+3}^2
X_{i+3}^3
X_{i+3}^4
RK_{i+4}^1
X_{i+4}^1
X_{i+4}^2
RK_{i+4}^2
X_{i+4}^3
X_{i+4}^4

FIG. 37

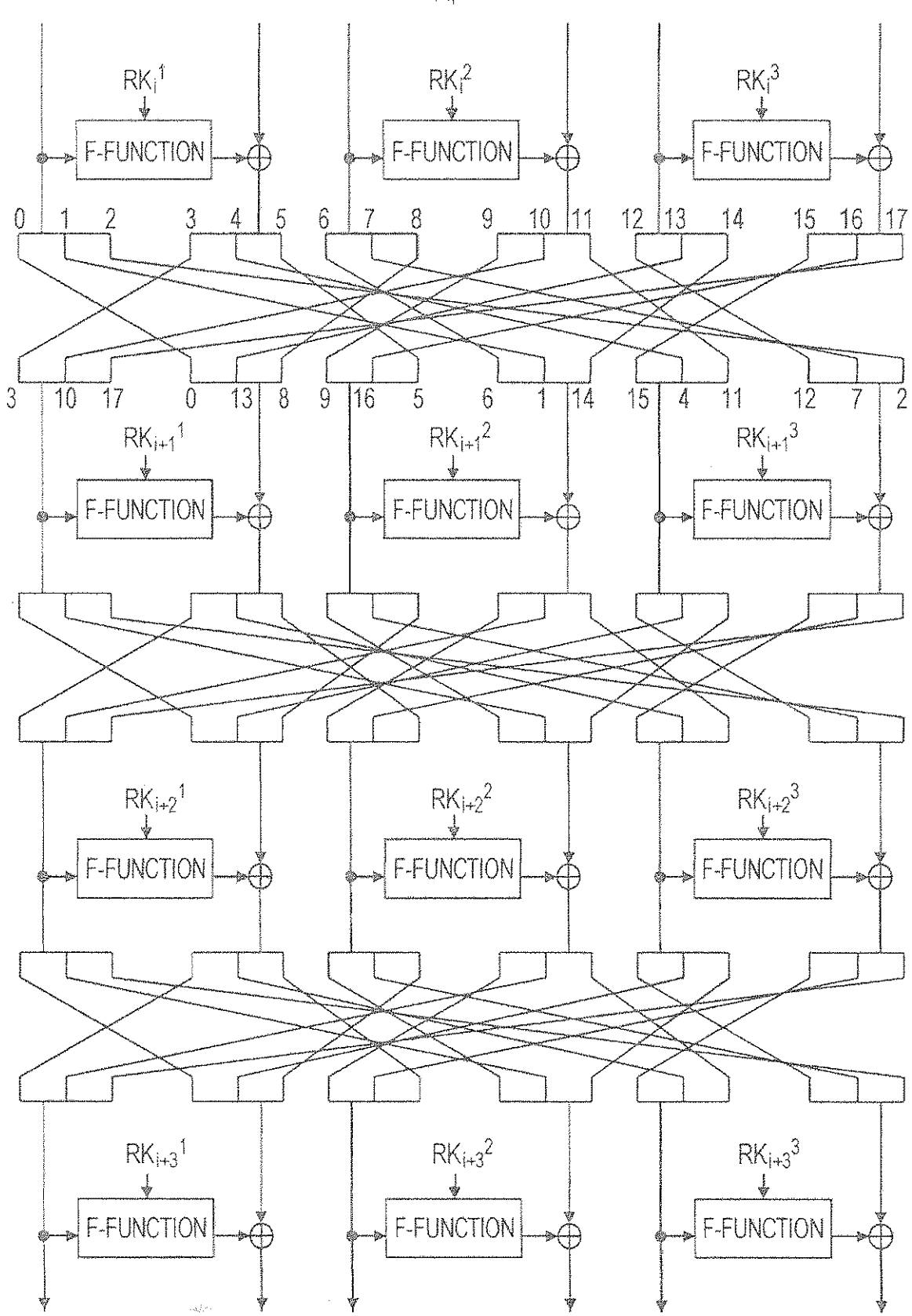

X_i
RK_i^1
RK_i^2
RK_i^3
F-FUNCTION
F-FUNCTION
F-FUNCTION
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
3 10 17 0 13 8 9 16 5 6 1 14 15 4 11 12 7 2
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
F-FUNCTION
F-FUNCTION
F-FUNCTION
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
F-FUNCTION
F-FUNCTION
F-FUNCTION
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3
F-FUNCTION
F-FUNCTION
F-FUNCTION

FIG. 38

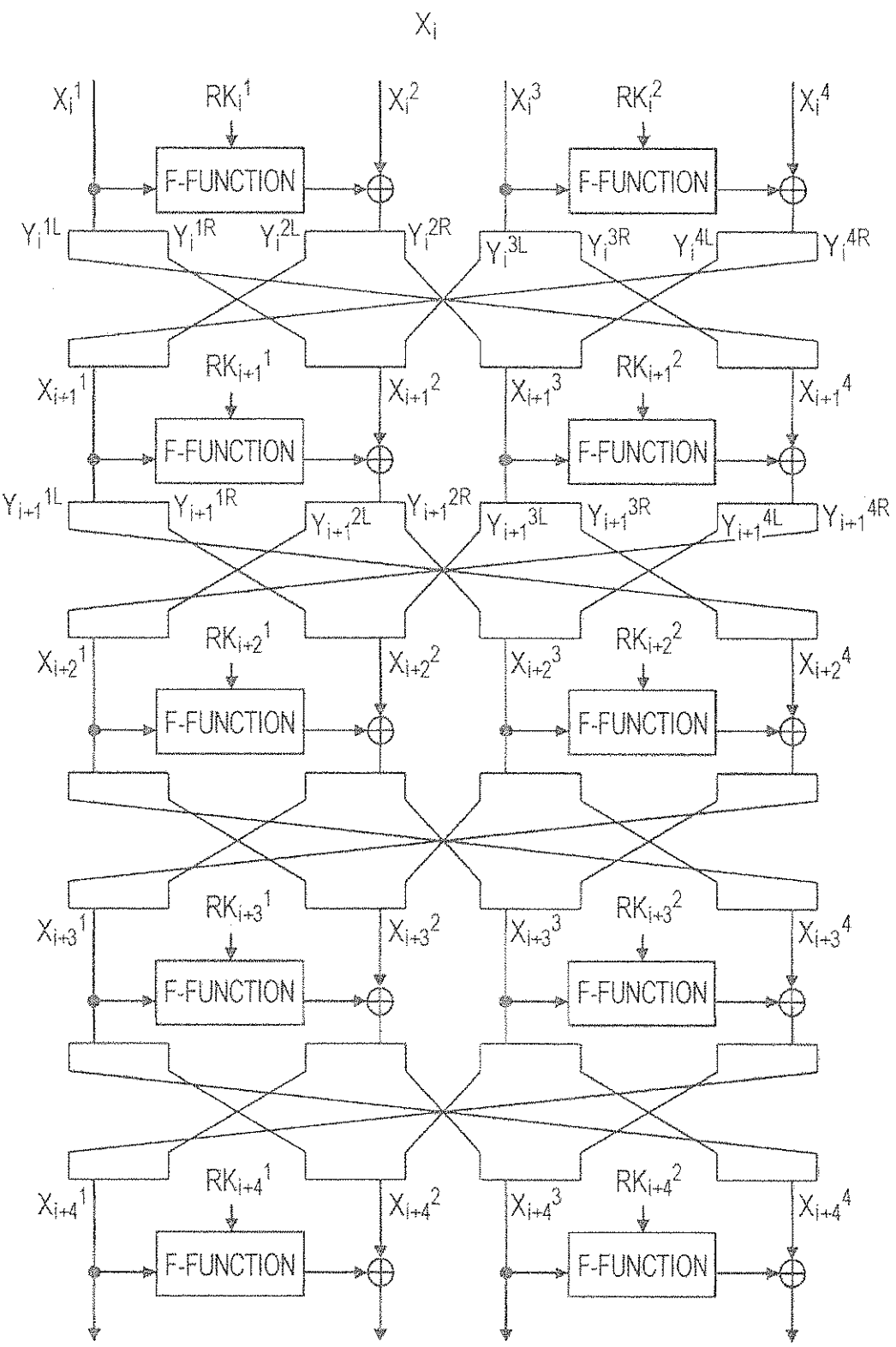

X_i
X_i^1
RK_i^1
X_i^2
X_i^3
RK_i^2
X_i^4
F-FUNCTION
F-FUNCTION
Y_i^{1L}
Y_i^{1R}
Y_i^{2L}
Y_i^{2R}
Y_i^{3L}
Y_i^{3R}
Y_i^{4L}
Y_i^{4R}
RK_{i+1}^1
RK_{i+1}^2
X_{i+1}^1
X_{i+1}^2
X_{i+1}^3
X_{i+1}^4
F-FUNCTION
F-FUNCTION
Y_{i+1}^{1L}
Y_{i+1}^{1R}
Y_{i+1}^{2L}
Y_{i+1}^{2R}
Y_{i+1}^{3L}
Y_{i+1}^{3R}
Y_{i+1}^{4L}
Y_{i+1}^{4R}
RK_{i+2}^1
RK_{i+2}^2
X_{i+2}^1
X_{i+2}^2
X_{i+2}^3
X_{i+2}^4
F-FUNCTION
F-FUNCTION
RK_{i+3}^1
RK_{i+3}^2
X_{i+3}^1
X_{i+3}^2
X_{i+3}^3
X_{i+3}^4
F-FUNCTION
F-FUNCTION
RK_{i+4}^1
RK_{i+4}^2
X_{i+4}^1
X_{i+4}^2
X_{i+4}^3
X_{i+4}^4
F-FUNCTION
F-FUNCTION

FIG. 39

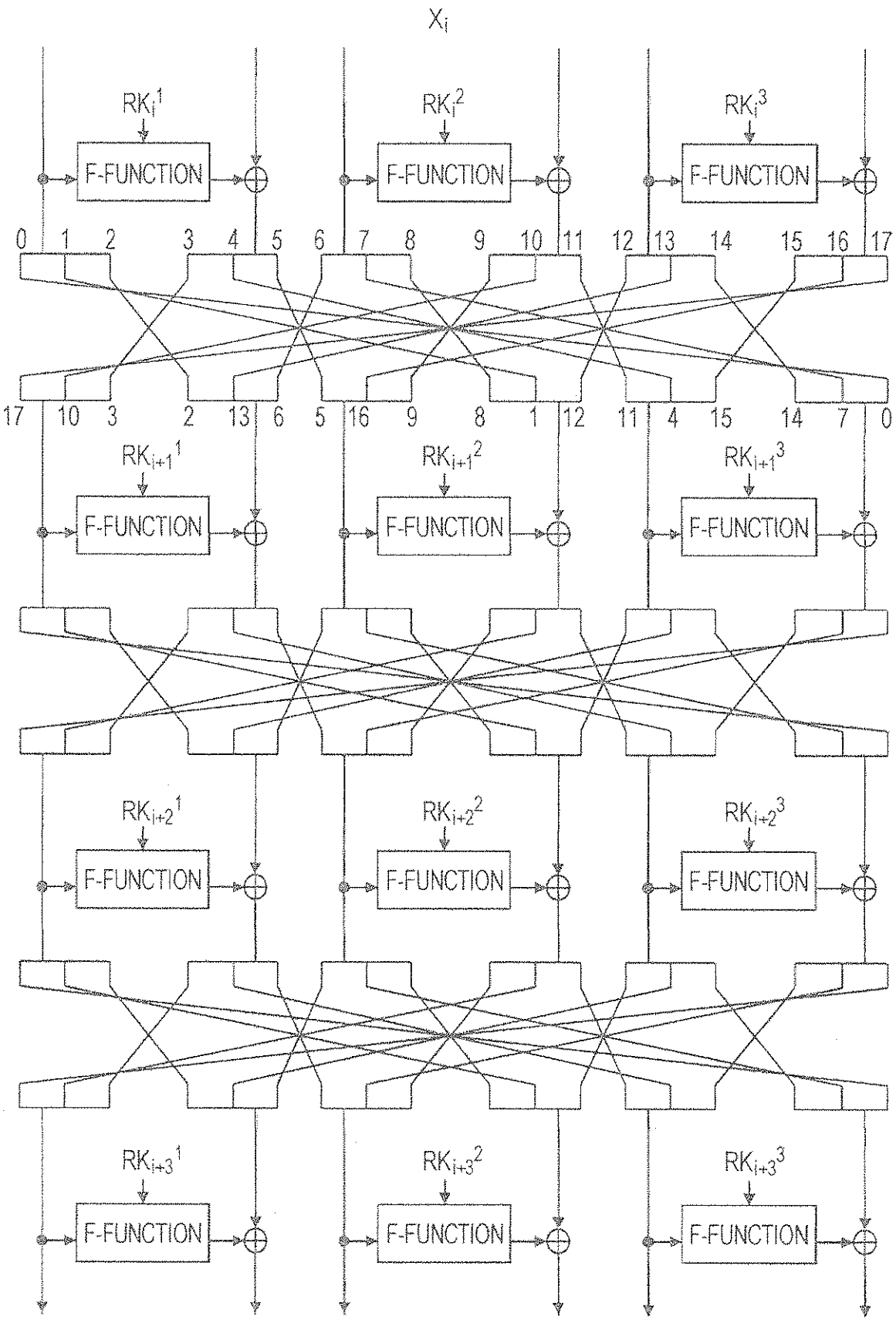
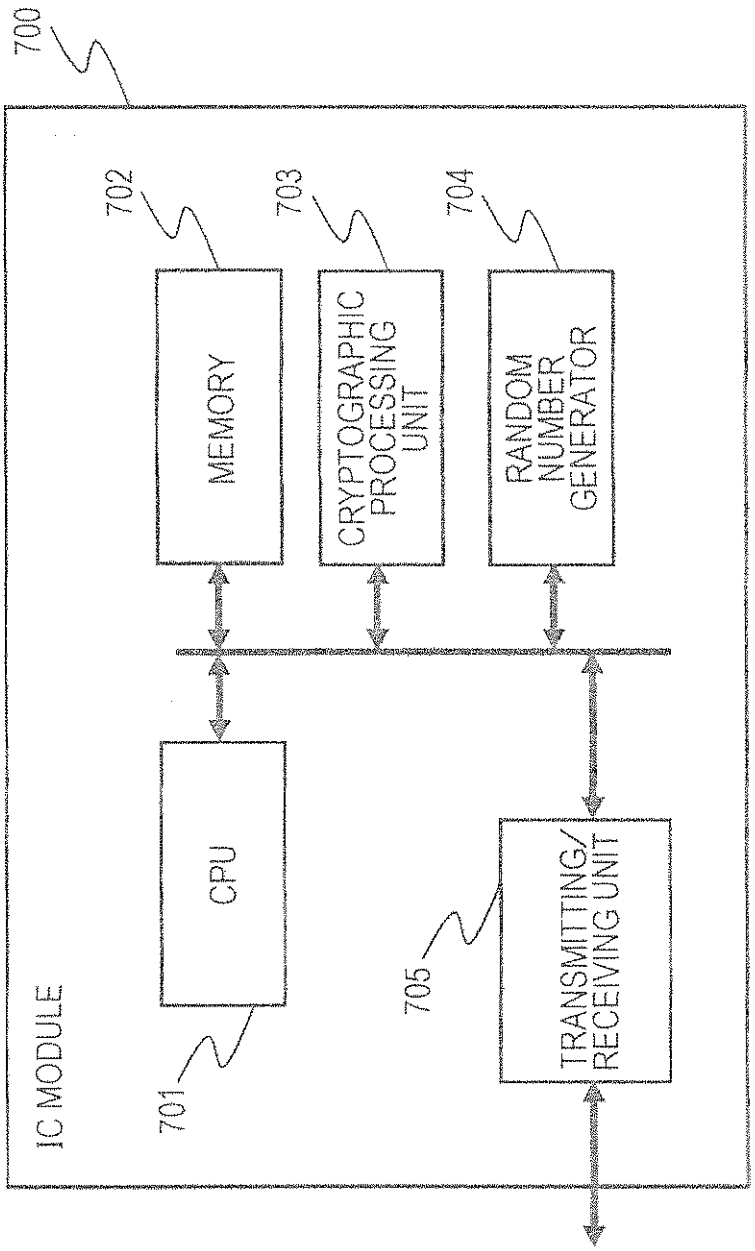

X_i
RK_i^1
RK_i^2
RK_i^3
F-FUNCTION
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
17 10 3 2 13 6 5 16 9 8 1 12 11 4 15 14 7 0
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3

FIG. 40


700
IC MODULE
MEMORY
CRYPTOGRAPHIC PROCESSING UNIT
RANDOM NUMBER GENERATOR
CPU
TRANSMITTING/ RECEIVING UNIT
701
702
703
704
705