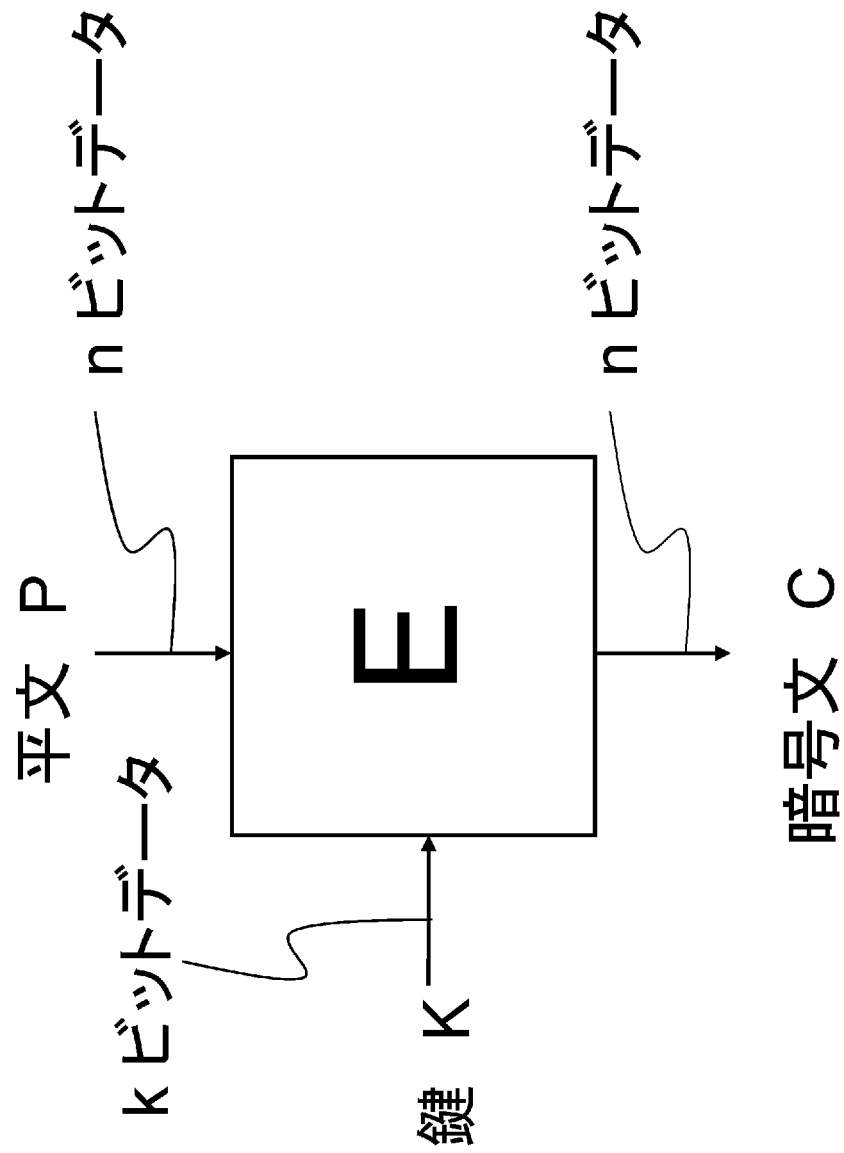
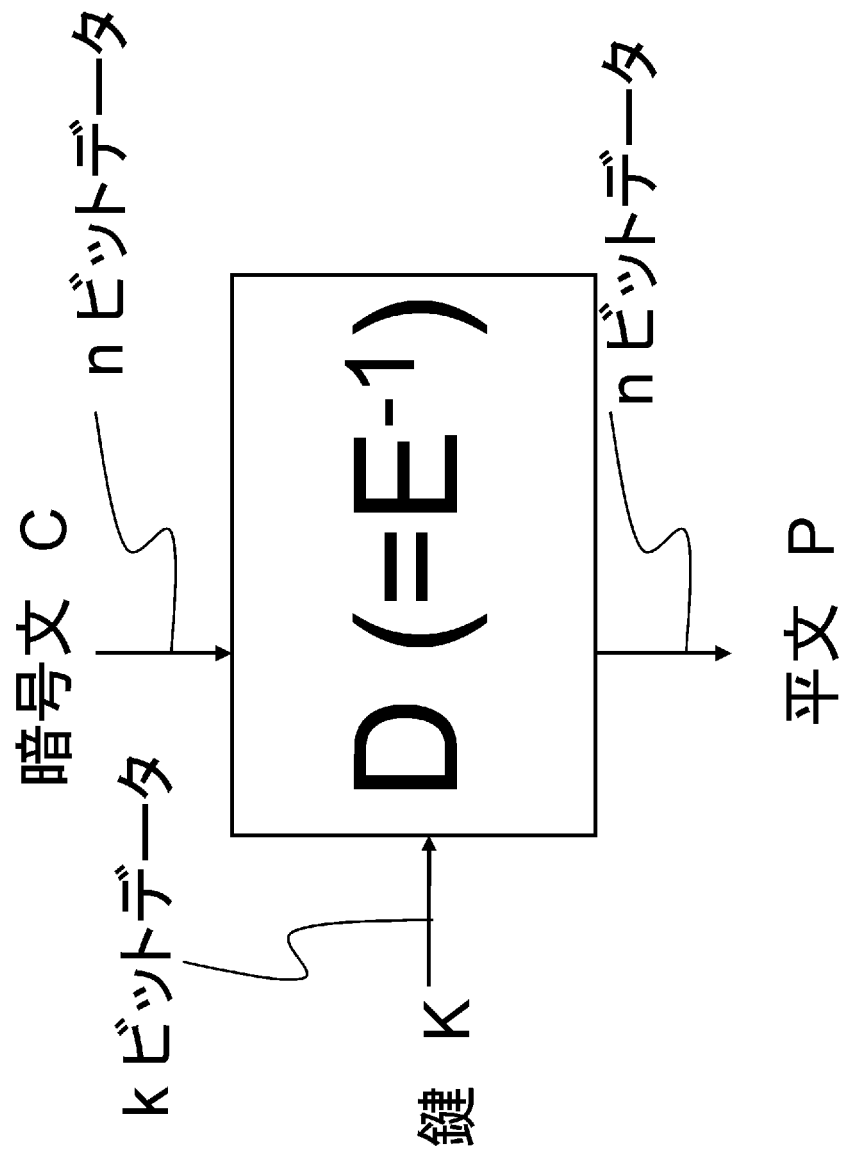


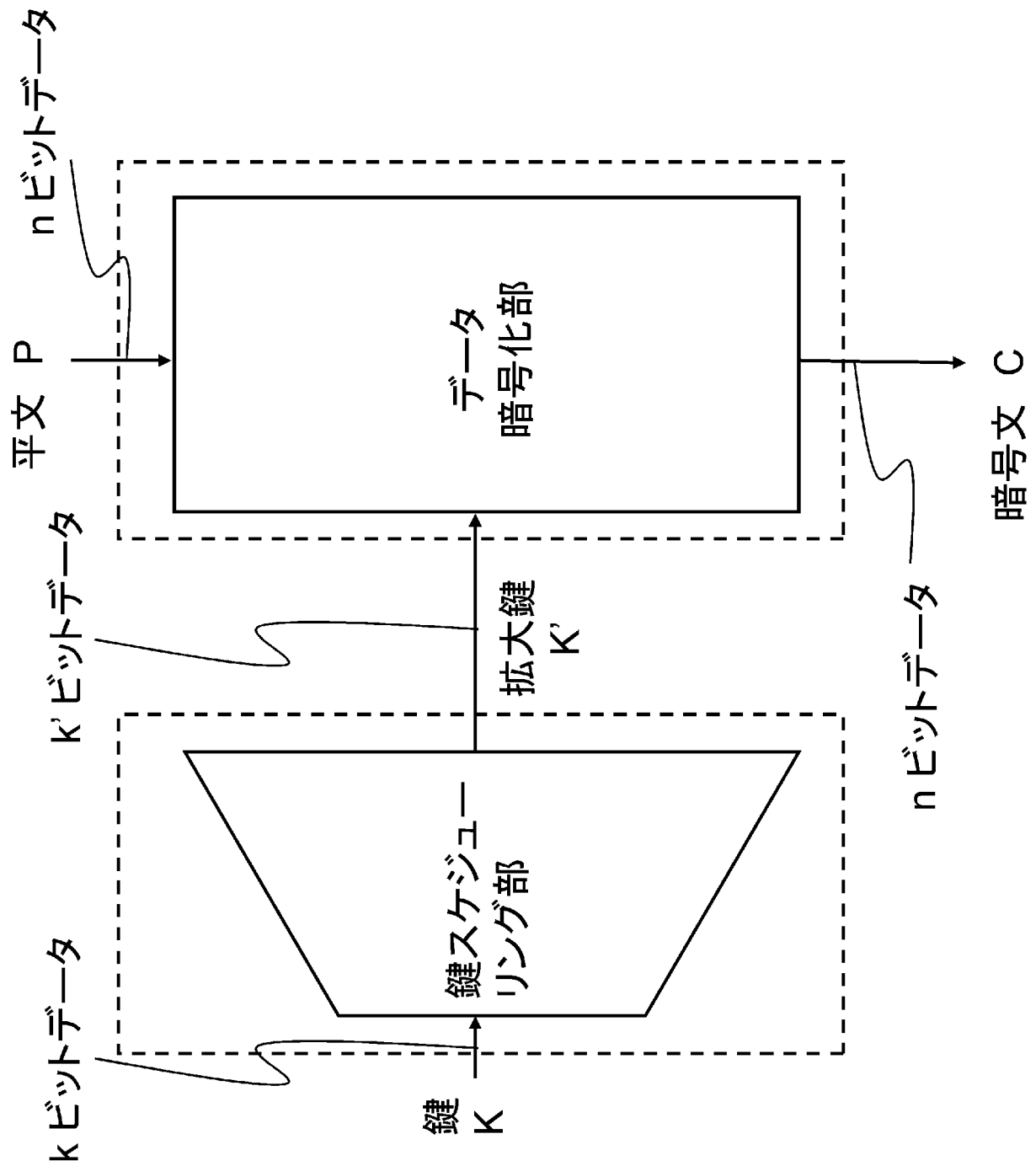
[図1]



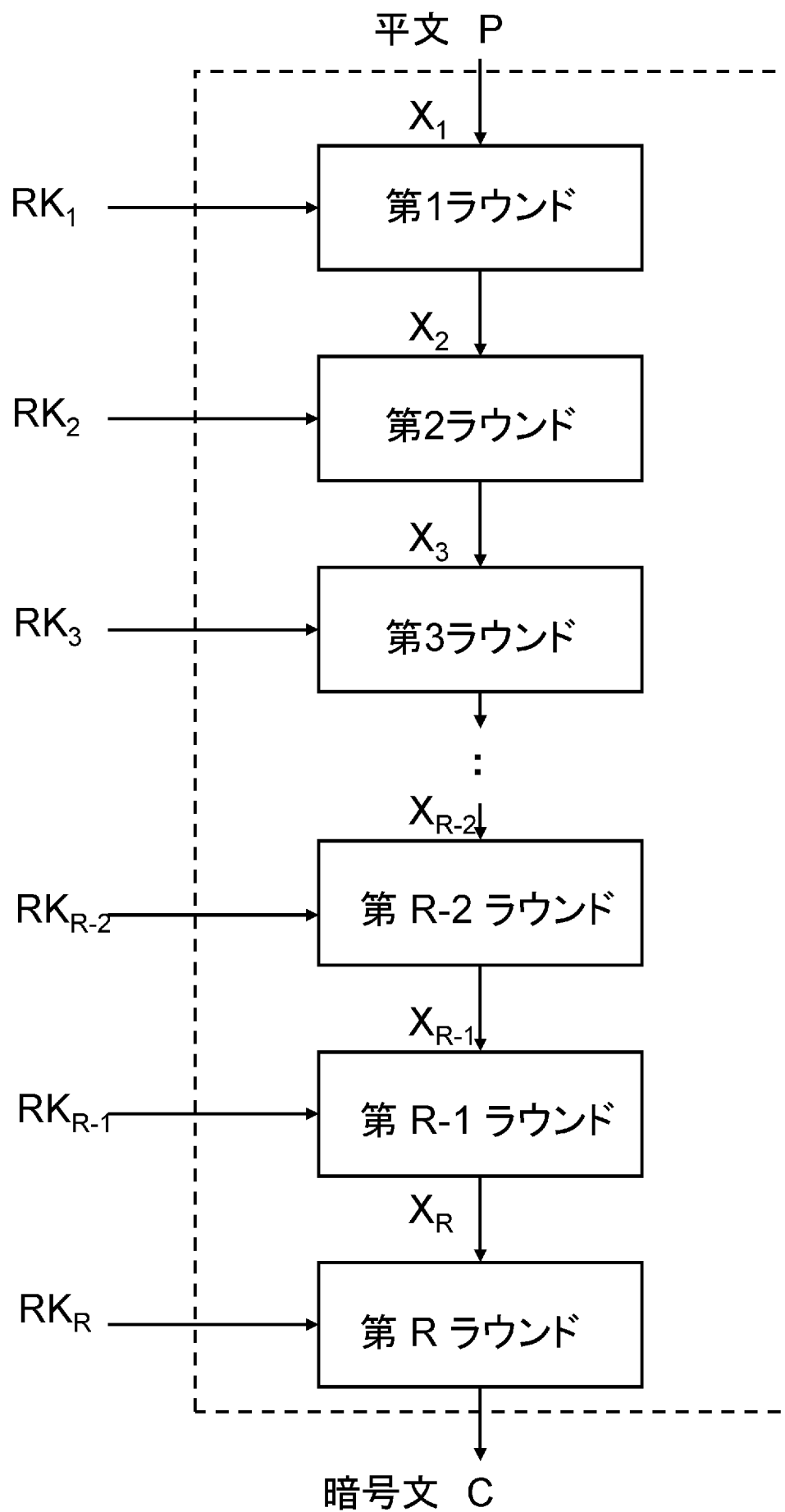
[図2]



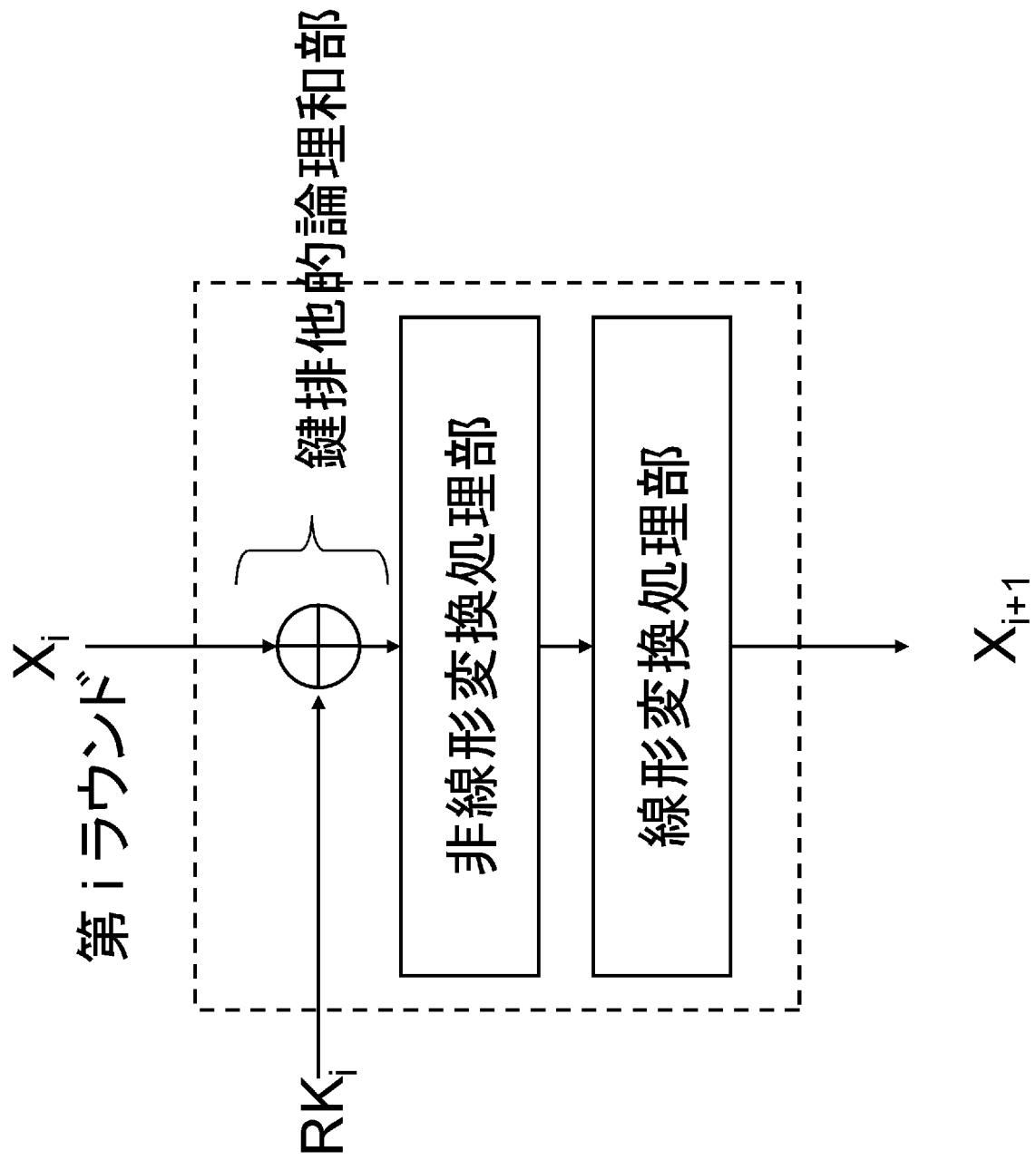
[図3]



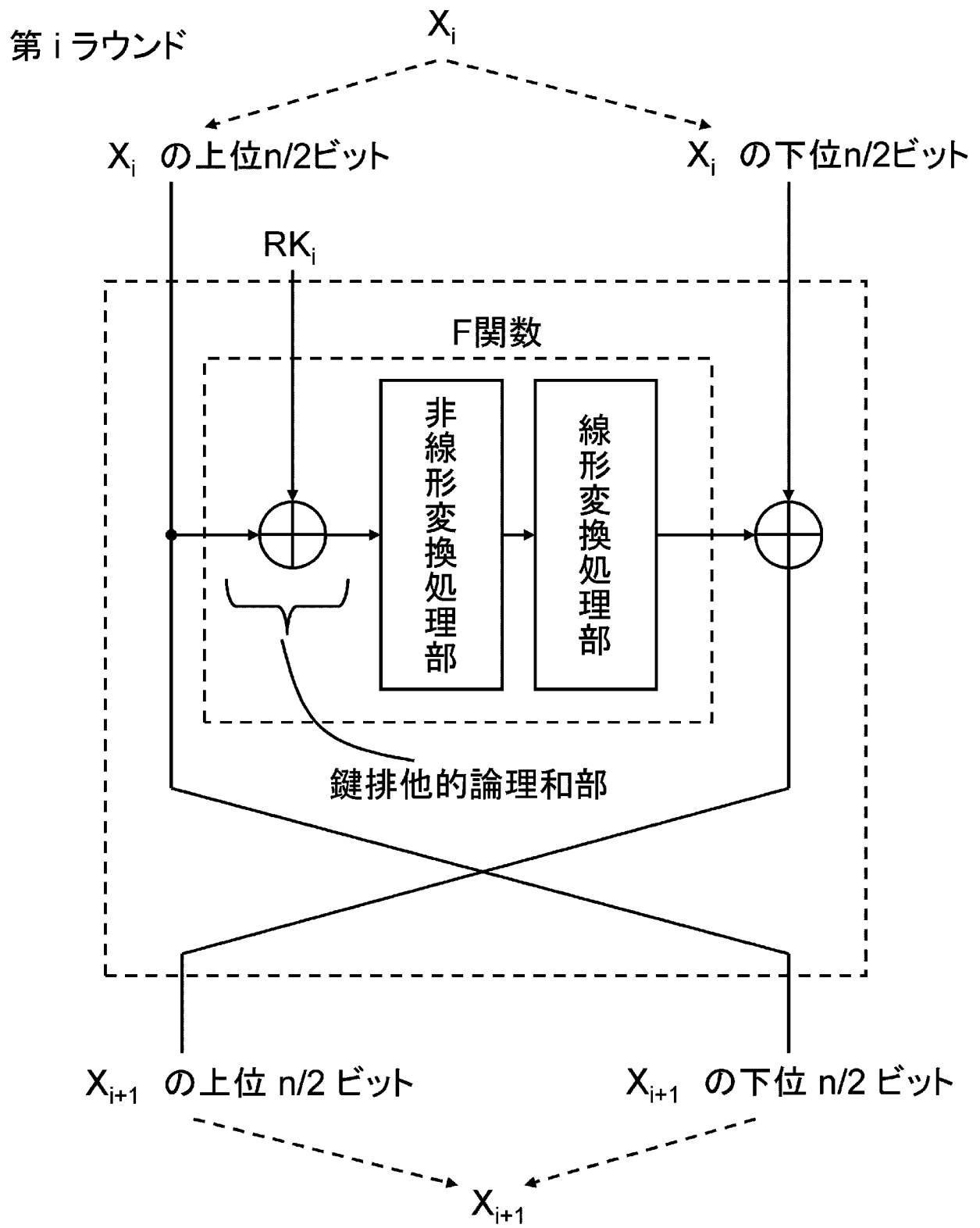
[図4]



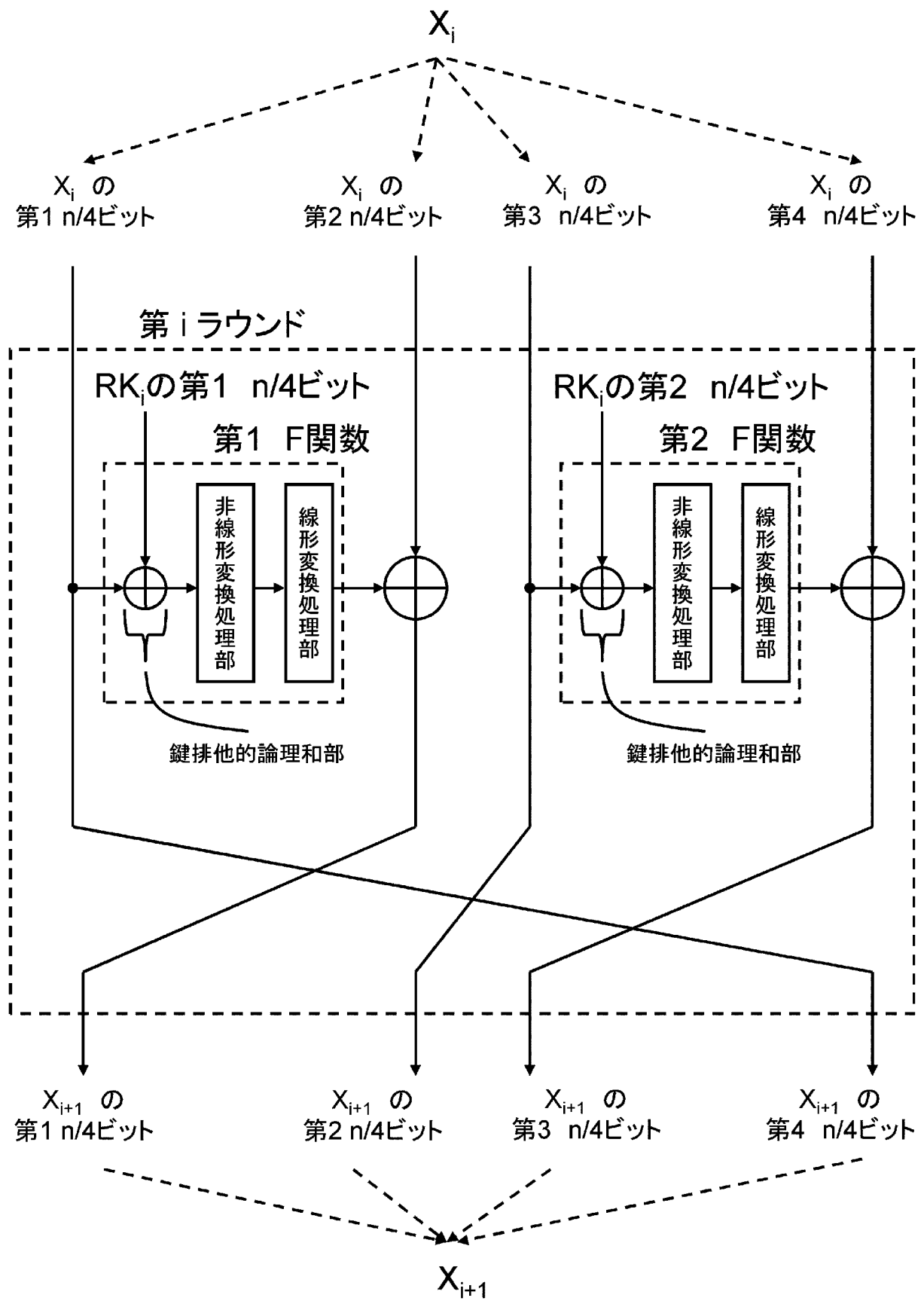
[図5]



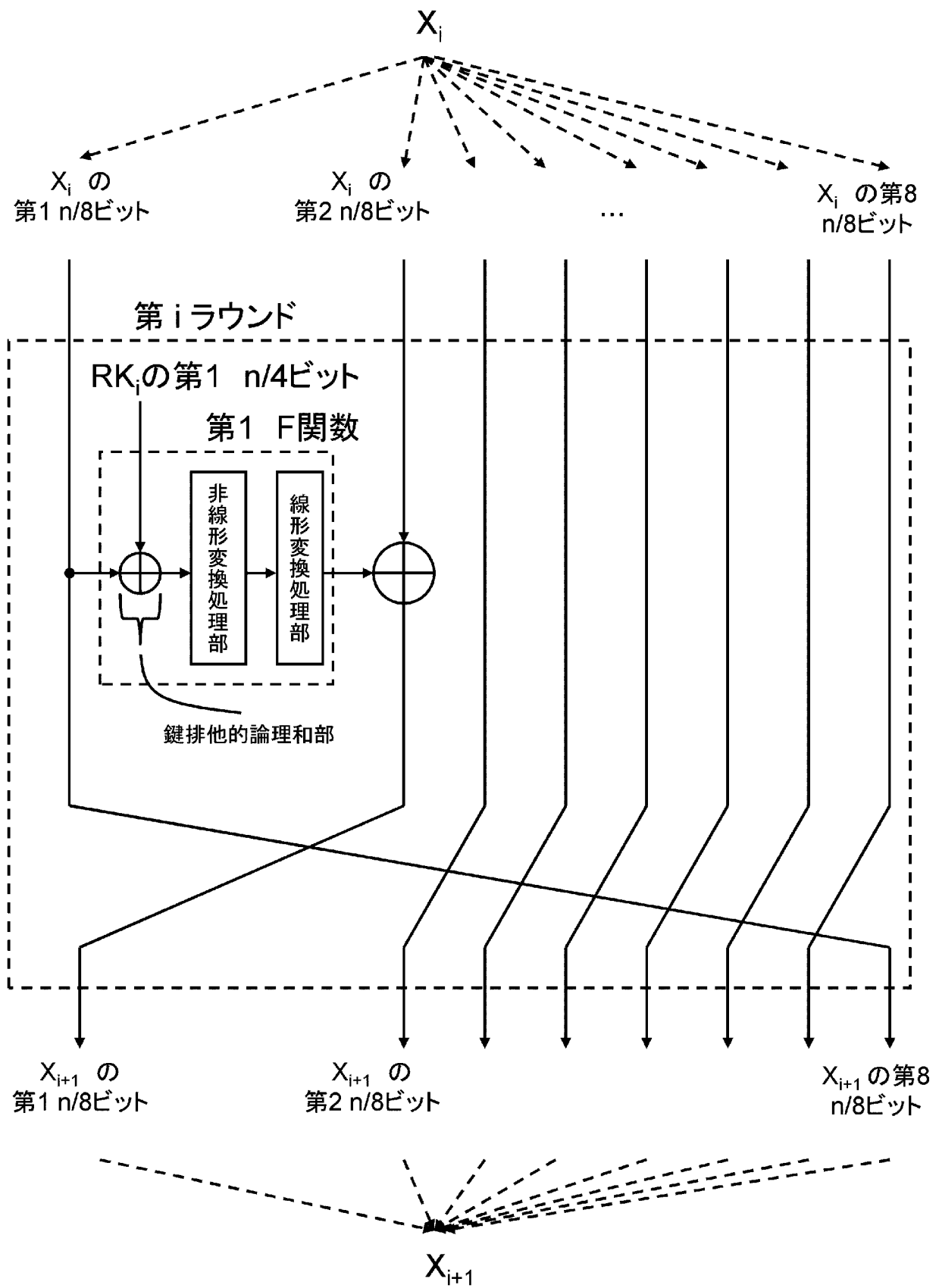
[図6]



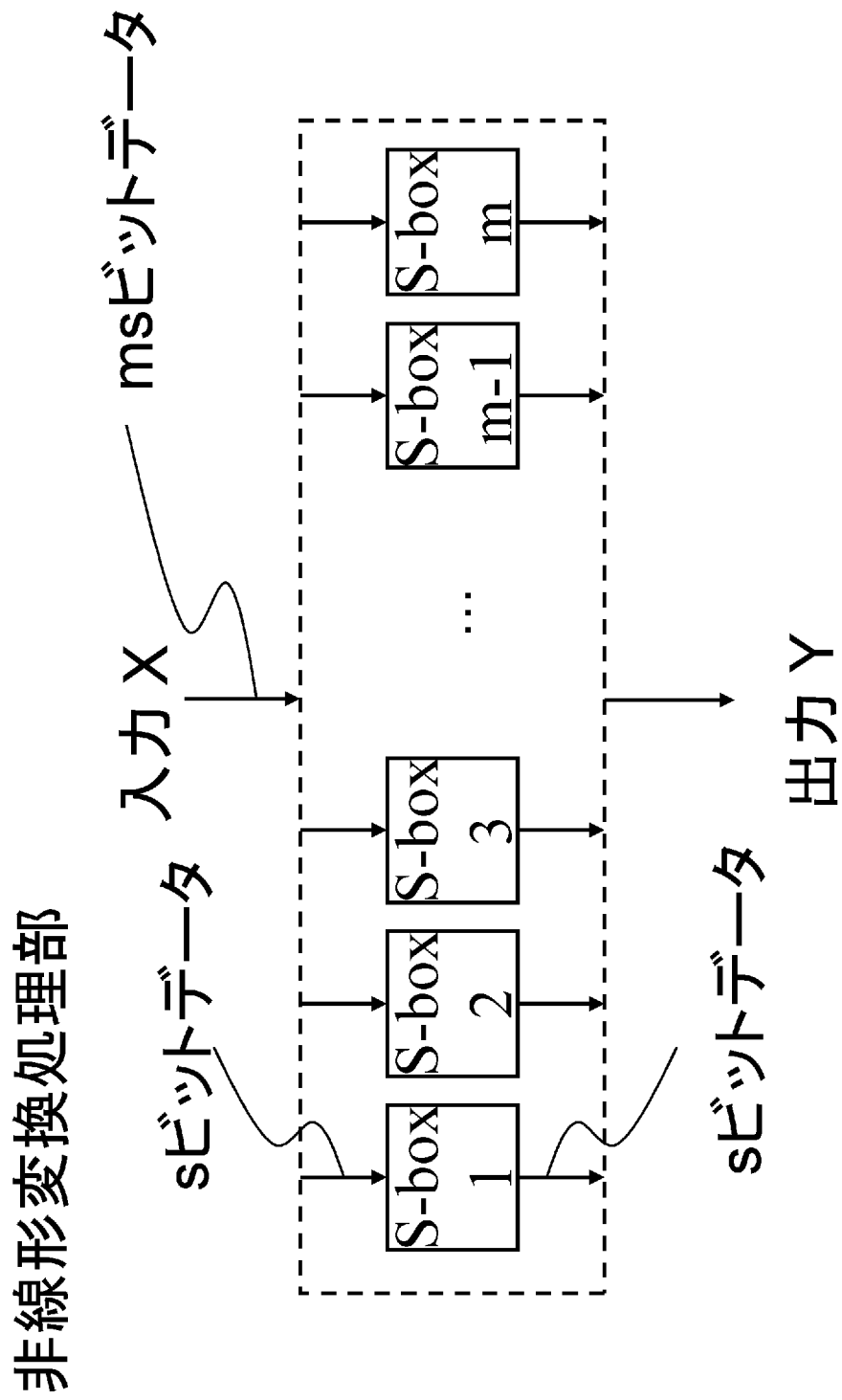
[図7]



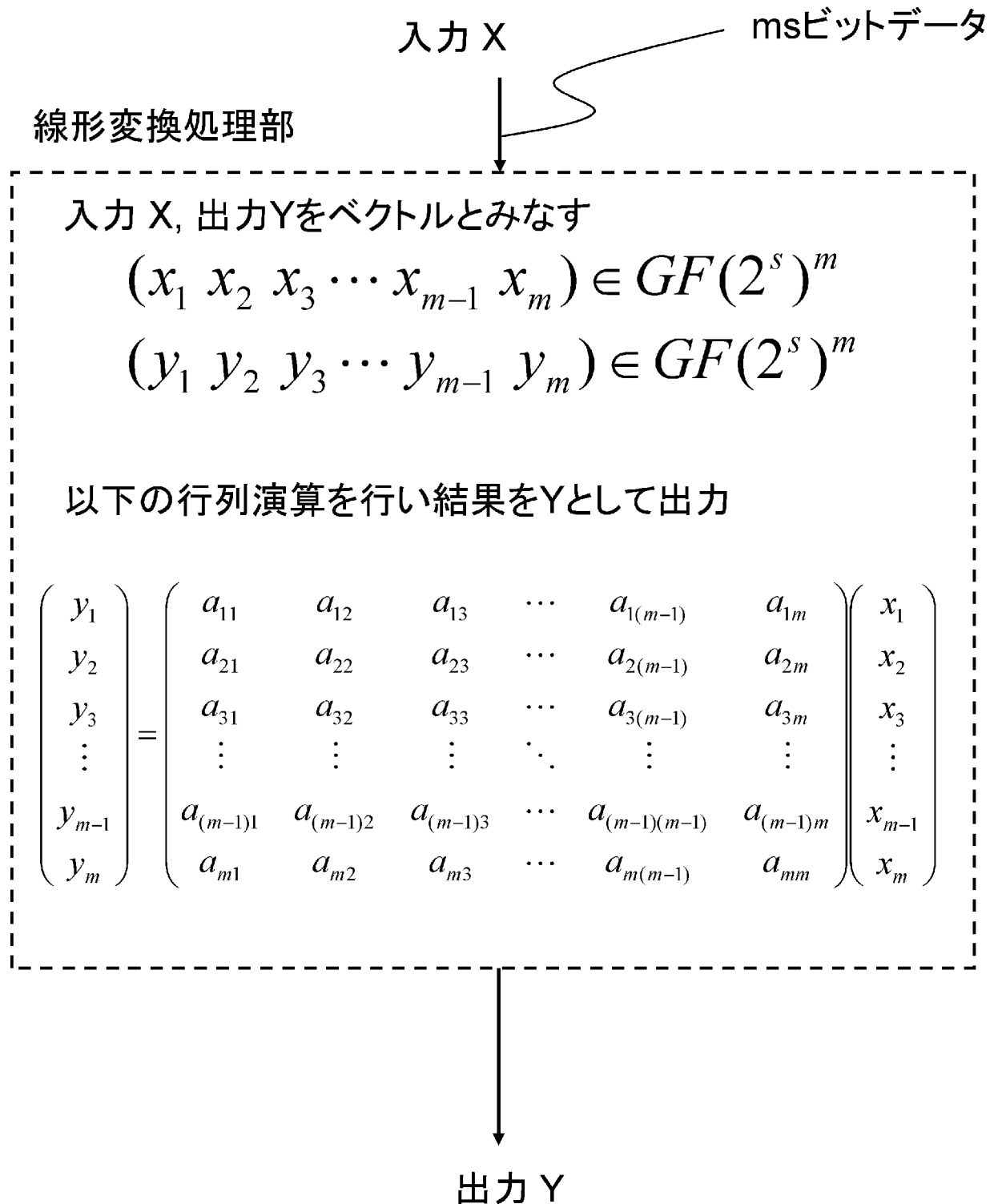
[図8]



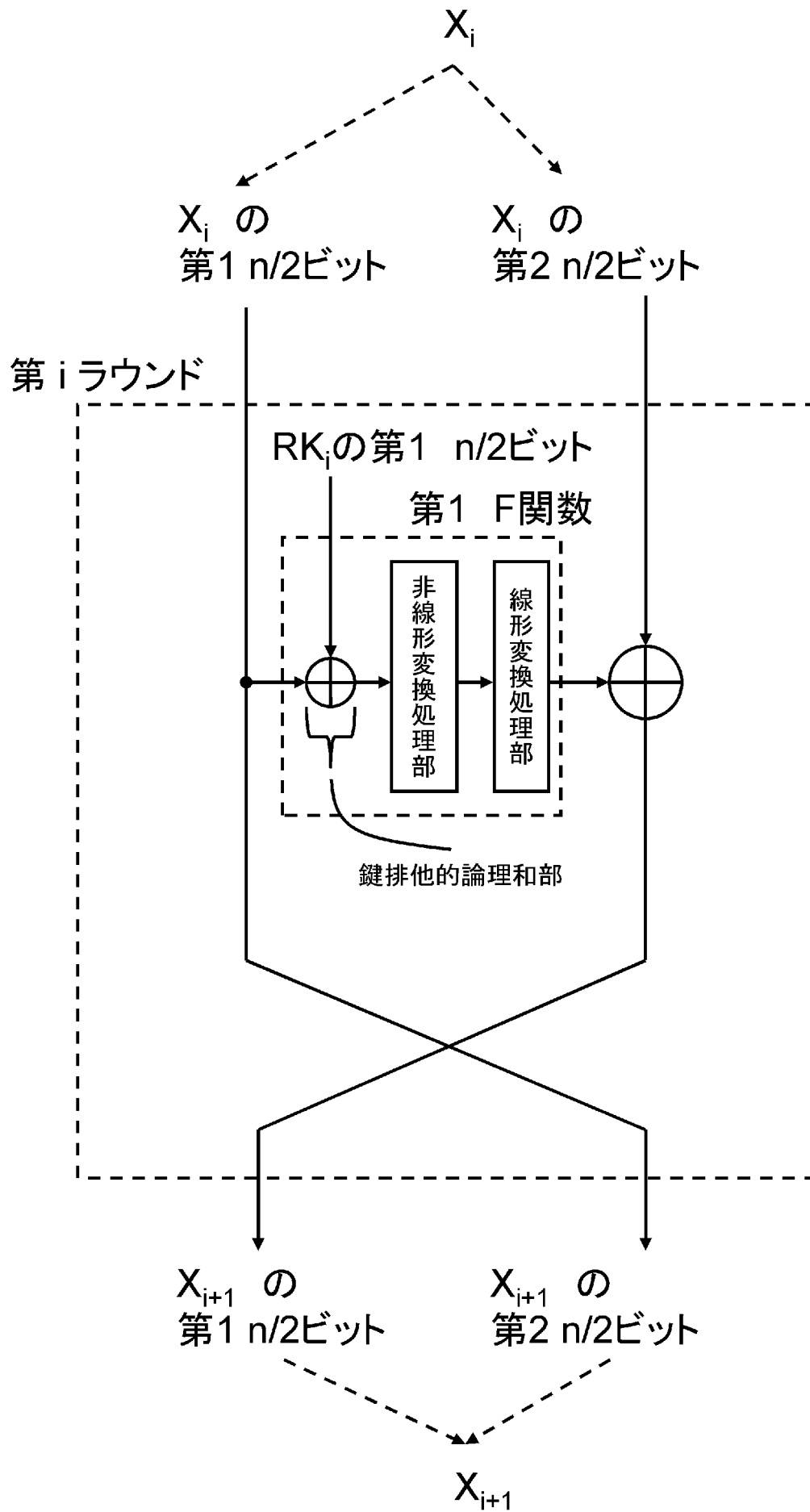
[図9]



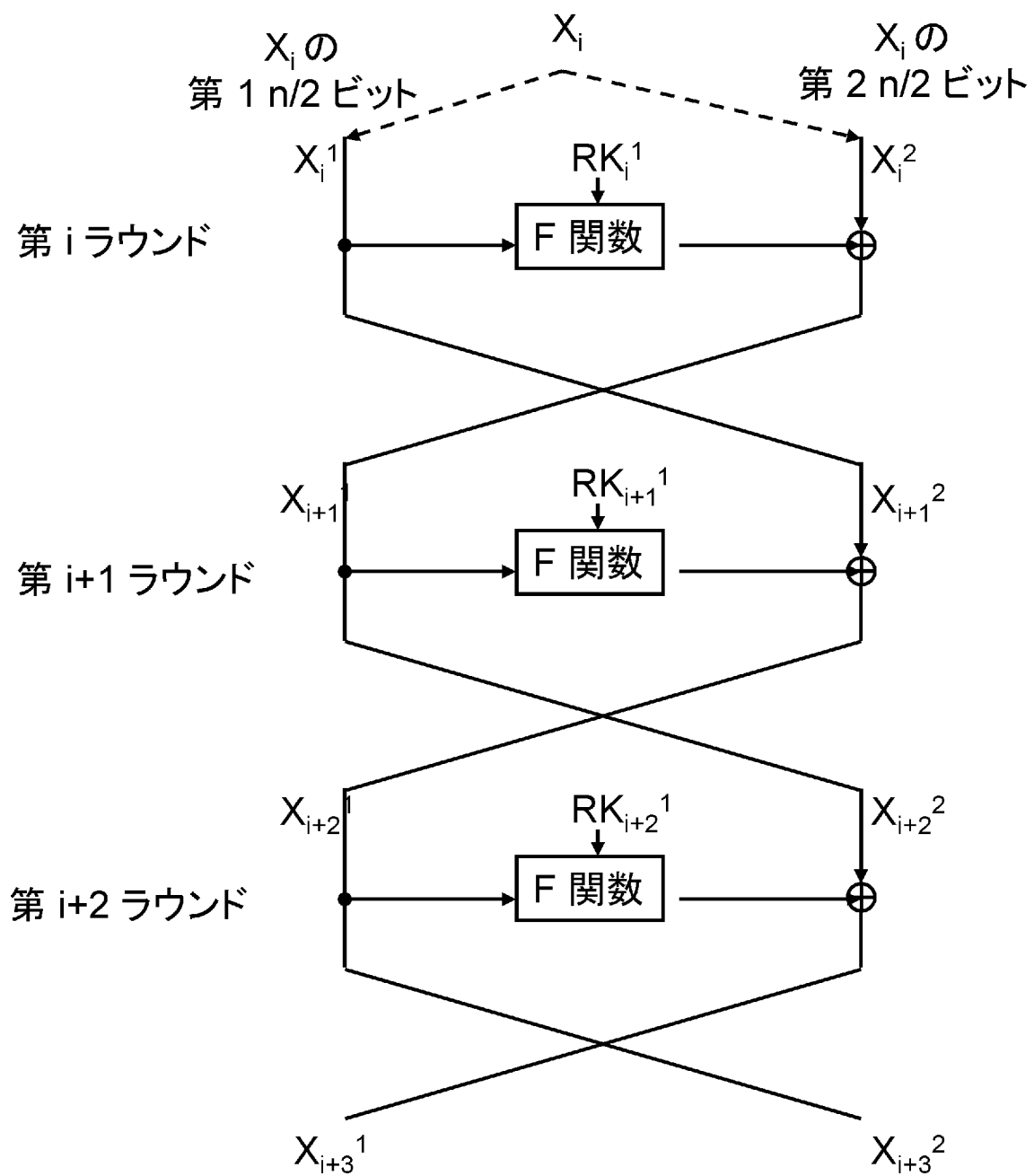
[図10]



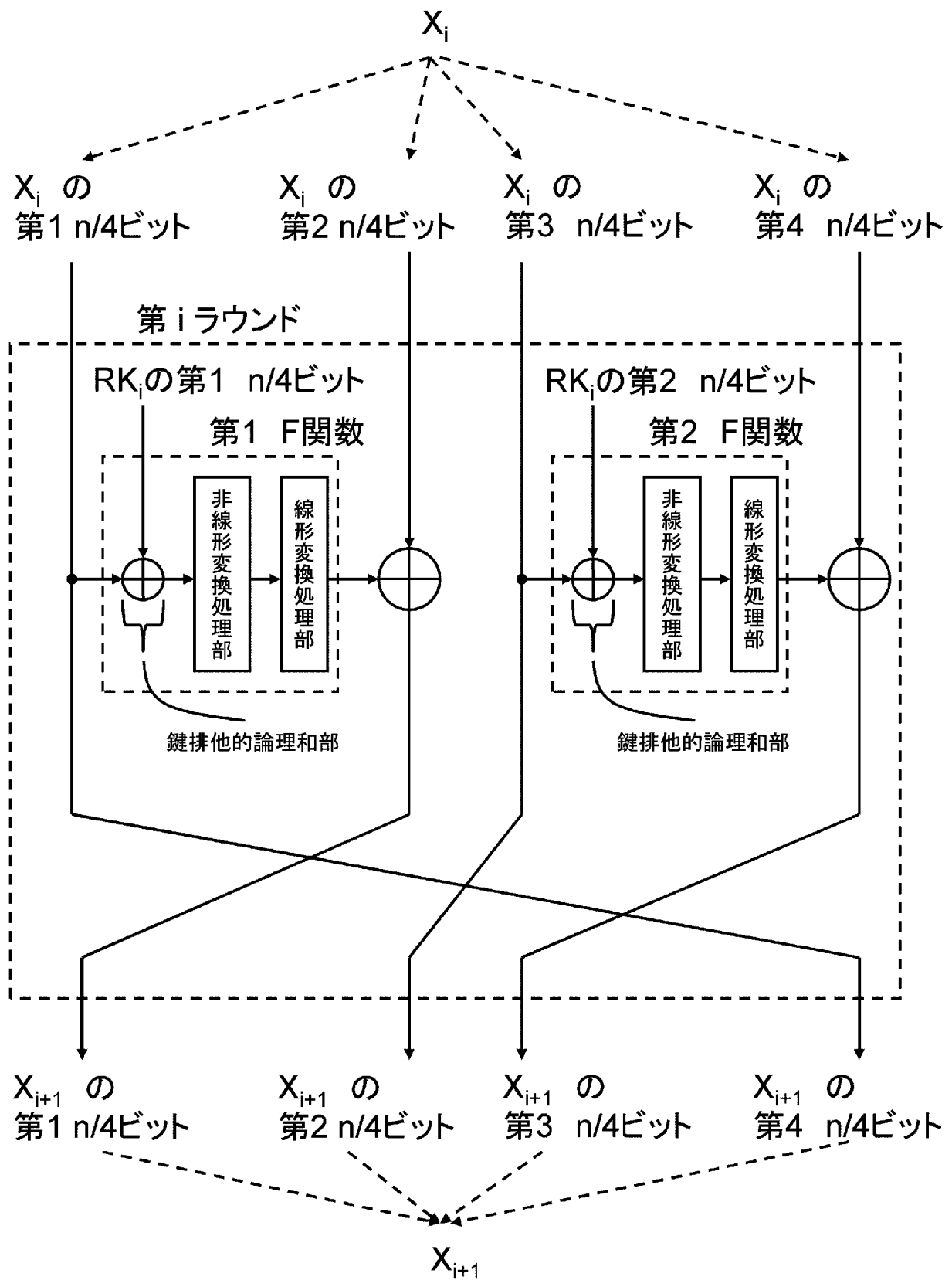
[図11]



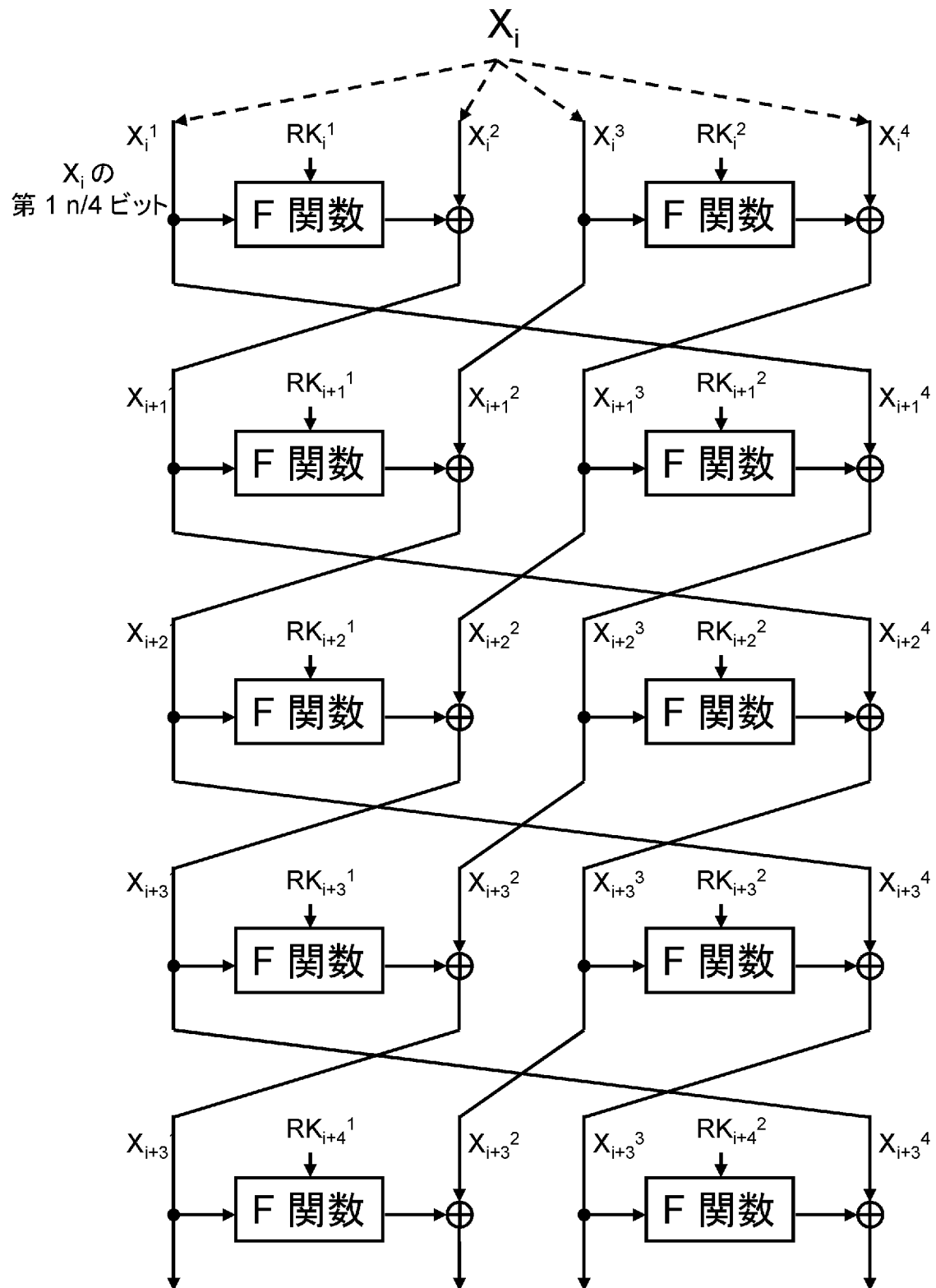
[図12]



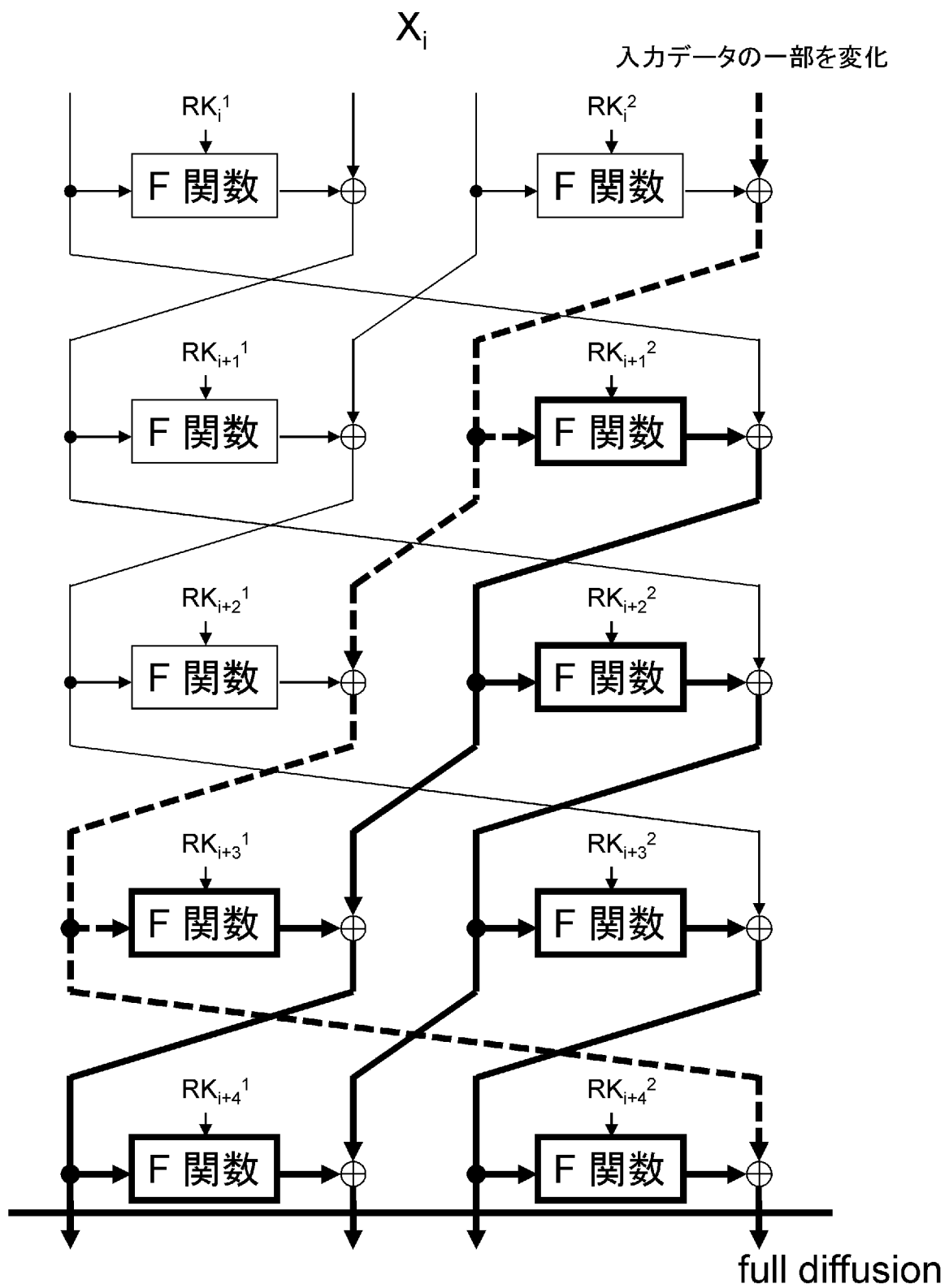
[図13]



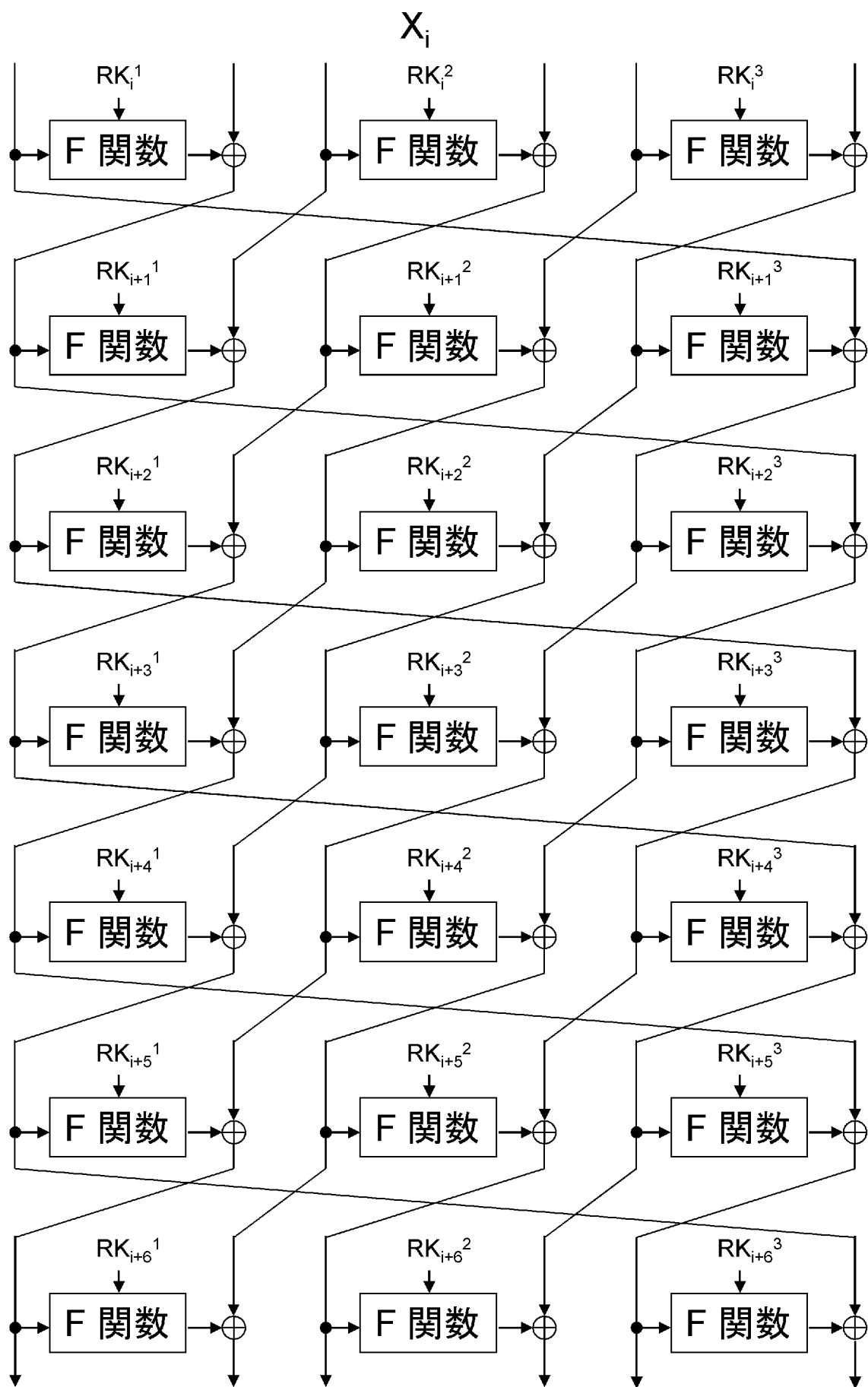
[図14]



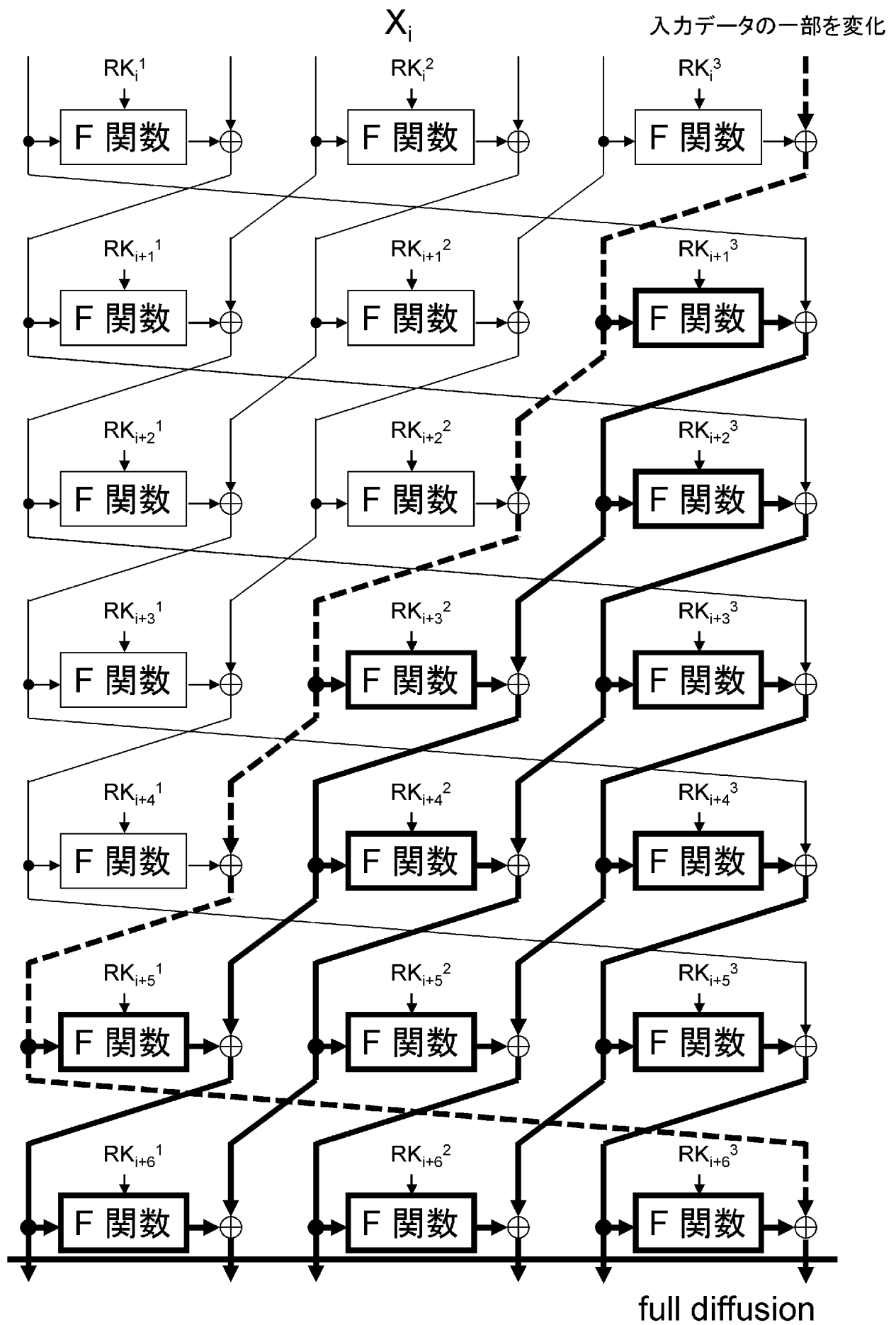
[図15]



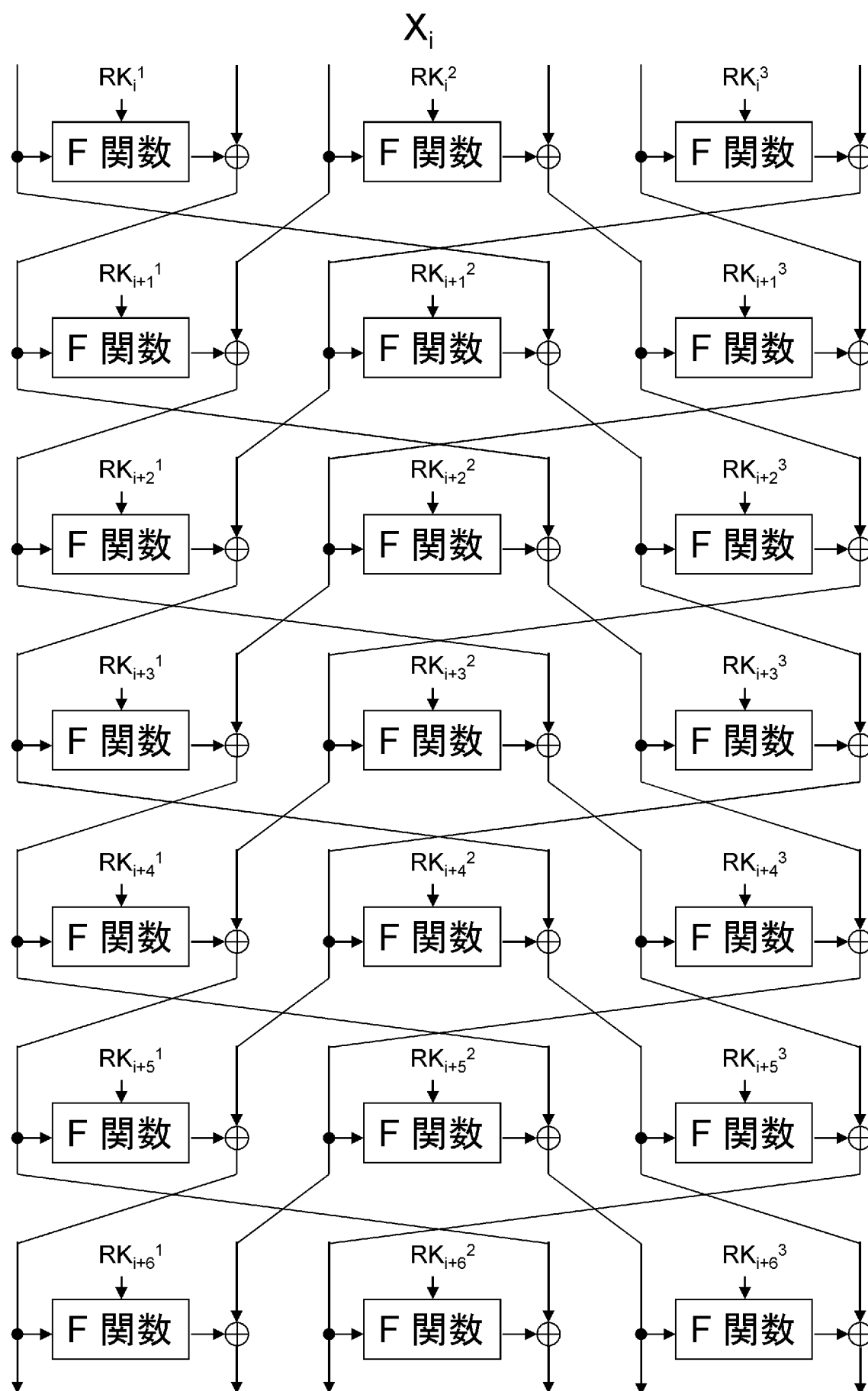
[図16]



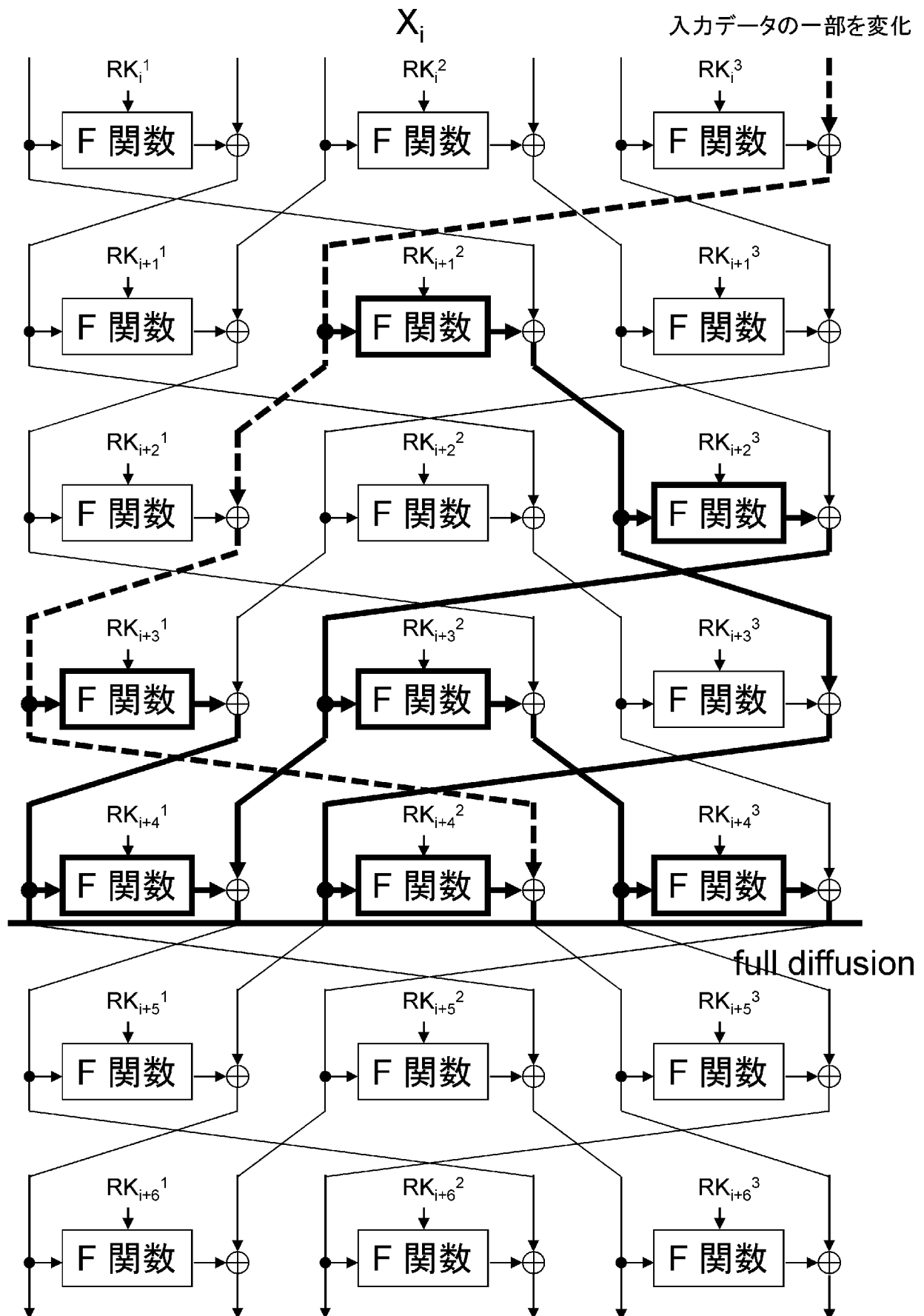
[図17]



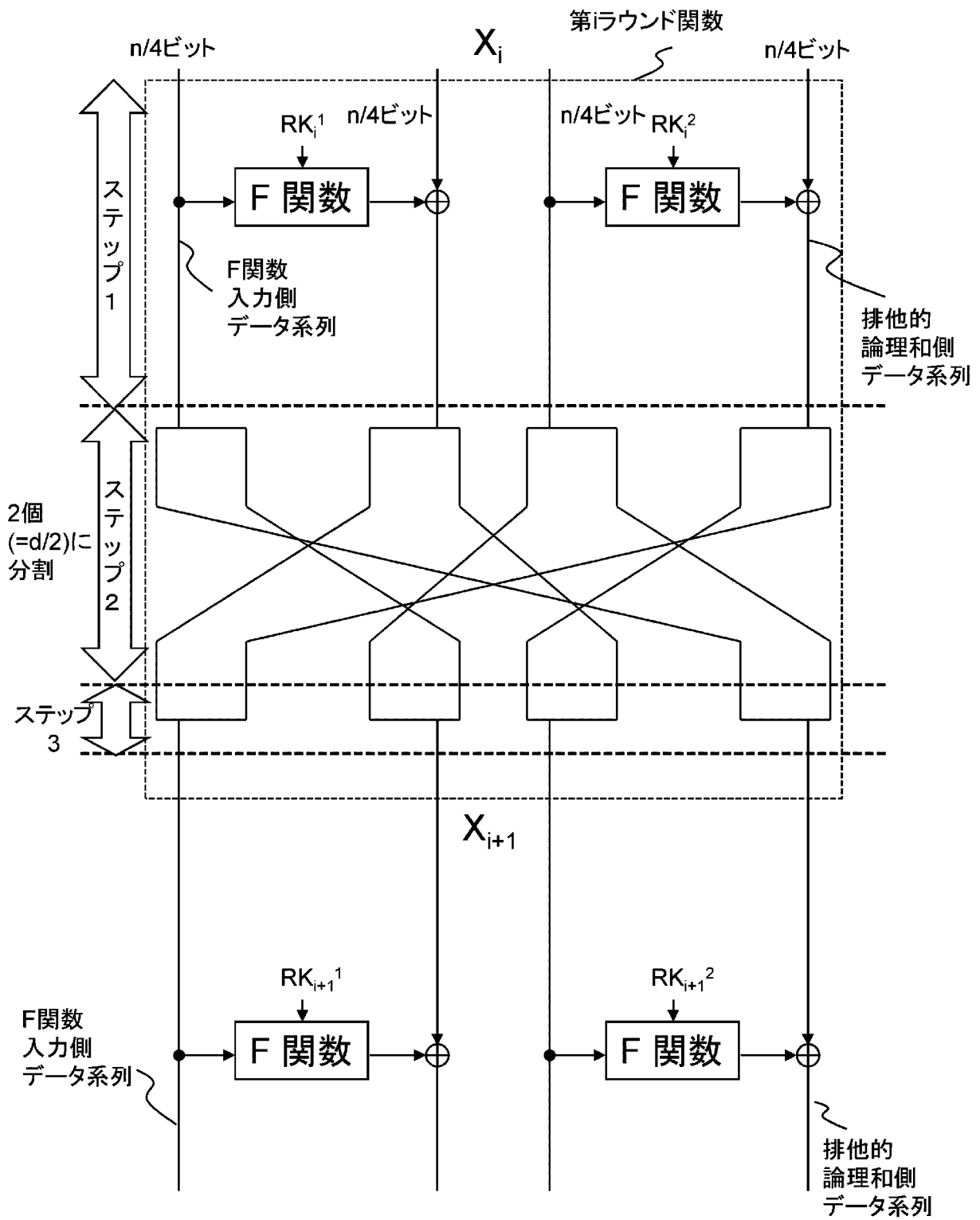
[図18]



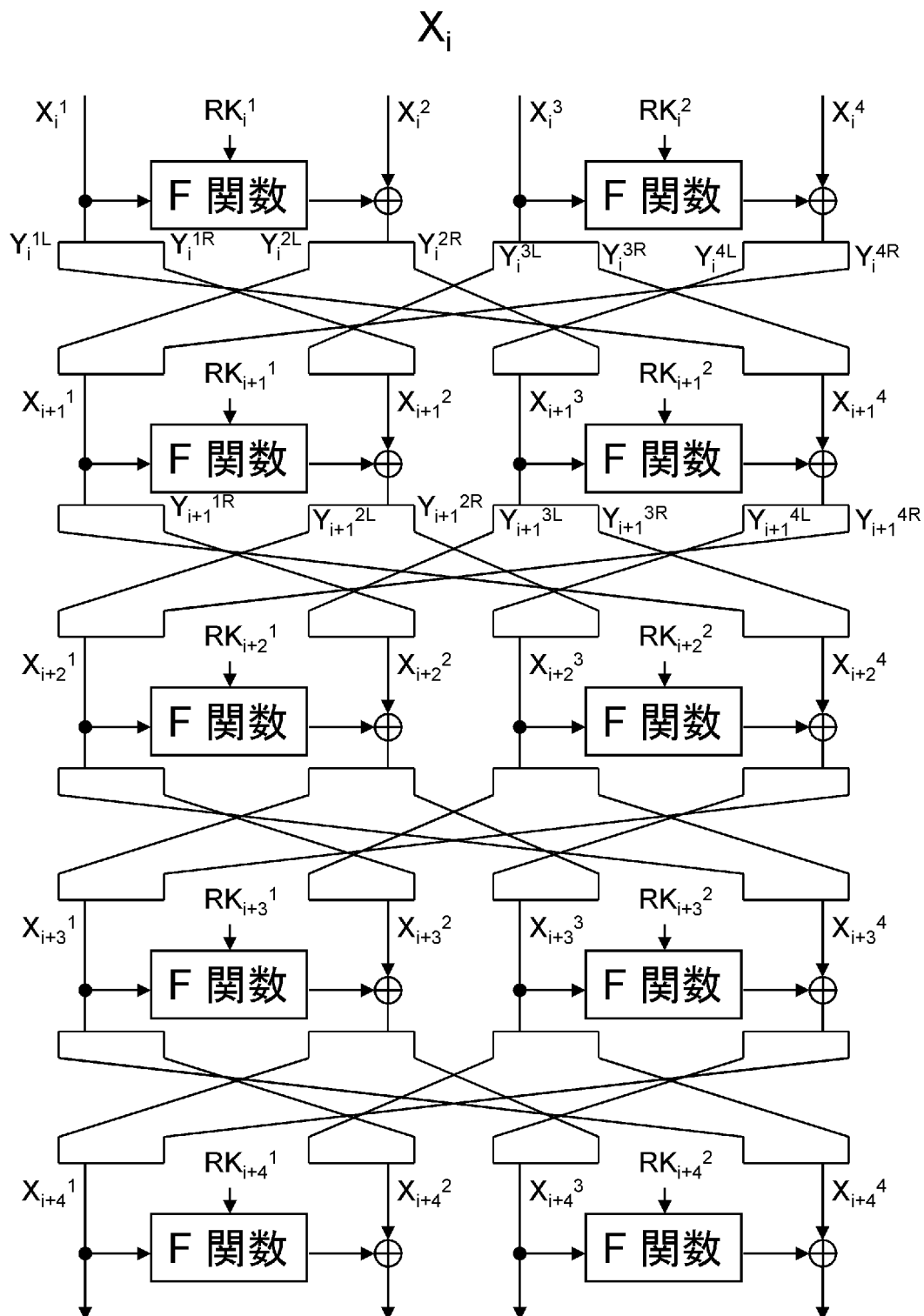
[図19]



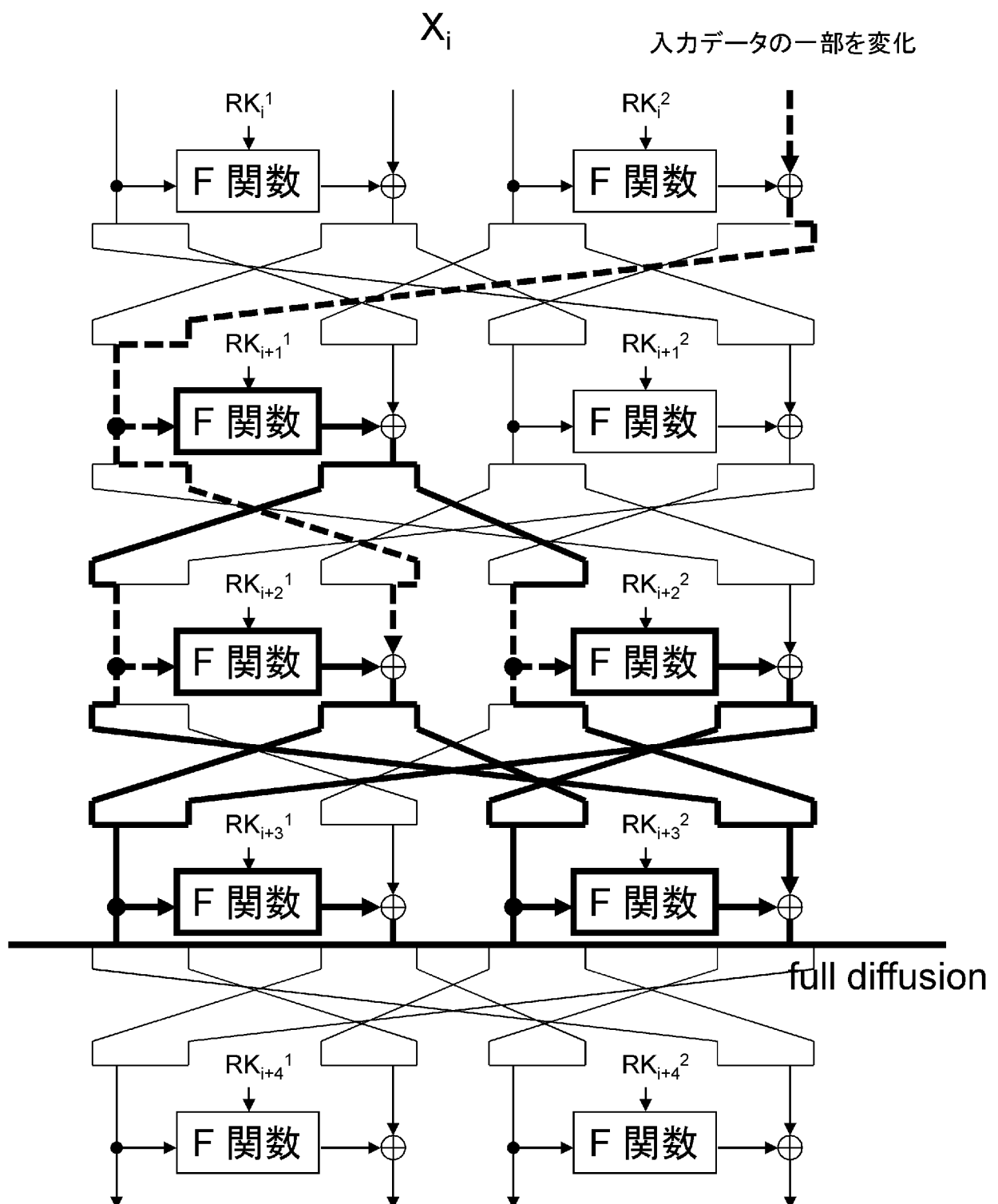
[図20]



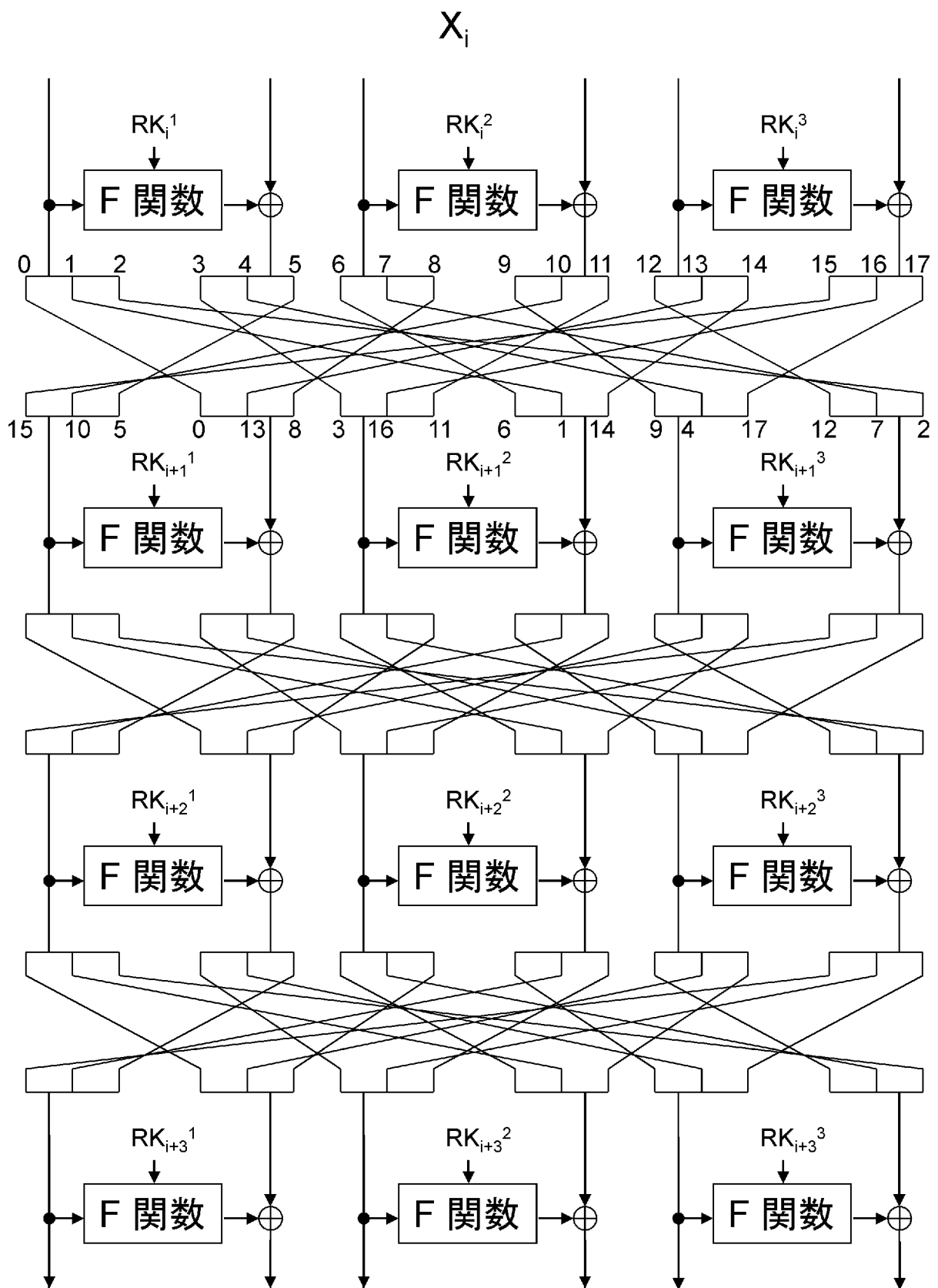
[図21]



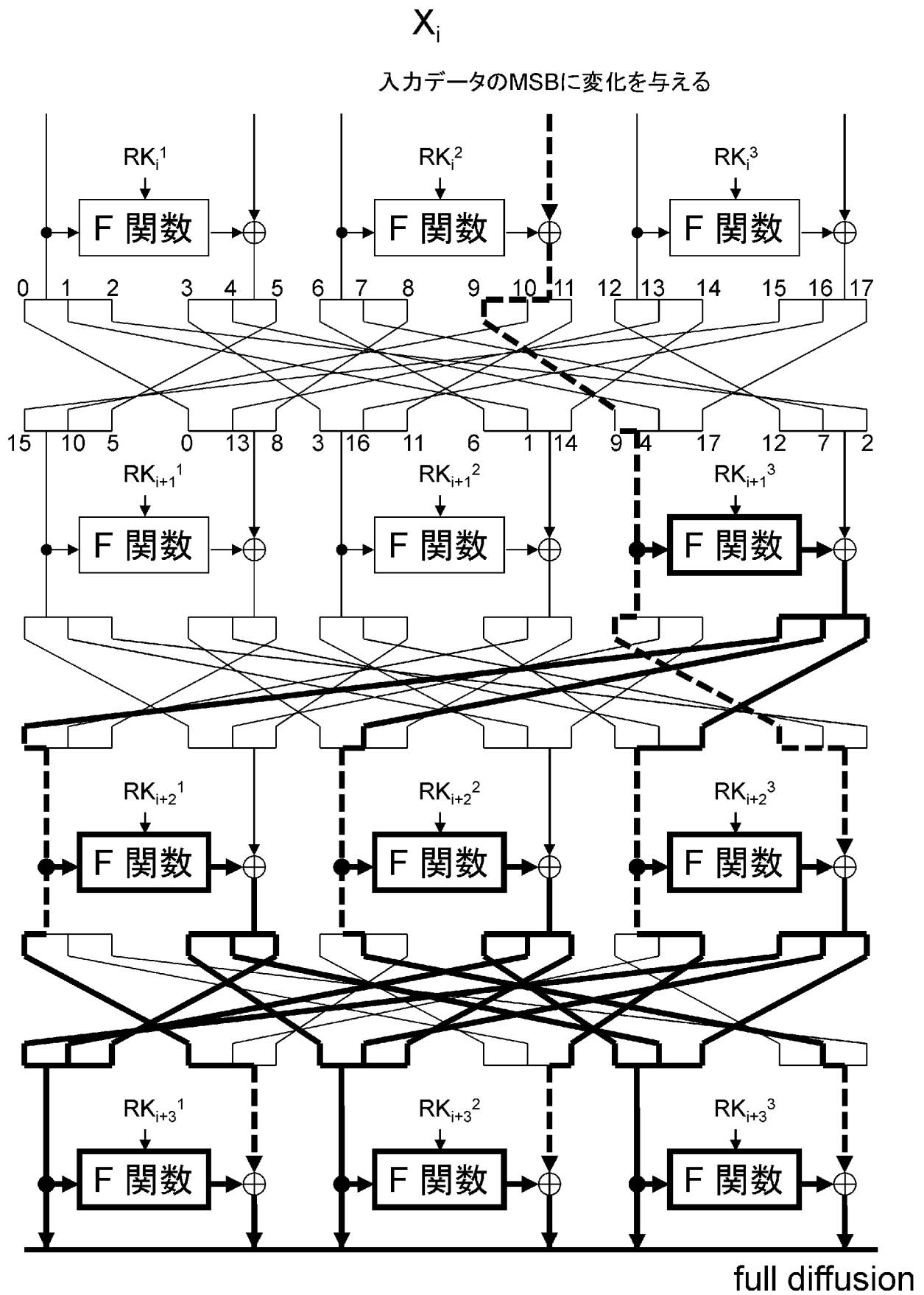
[図22]



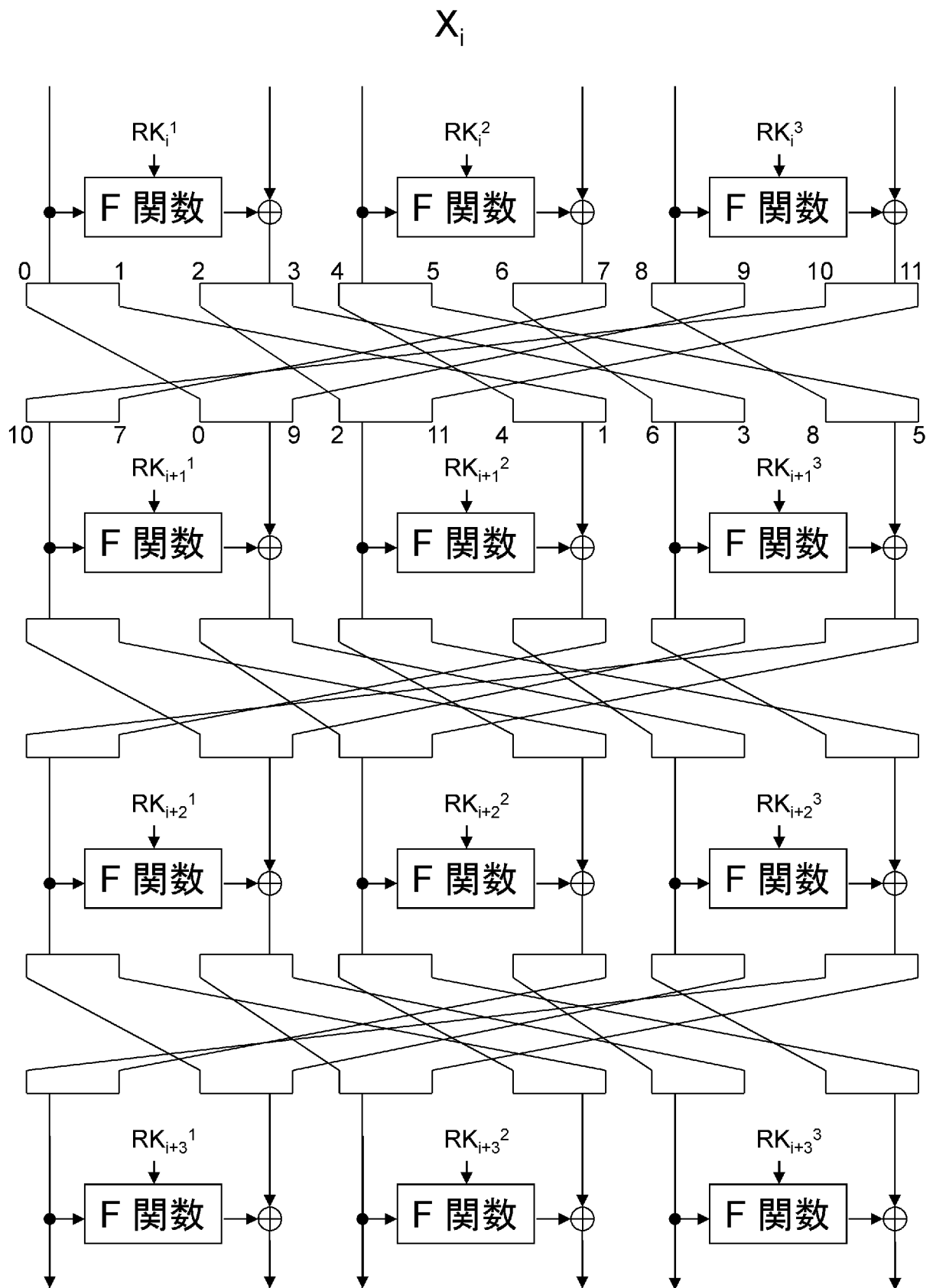
[図23]



[図24]



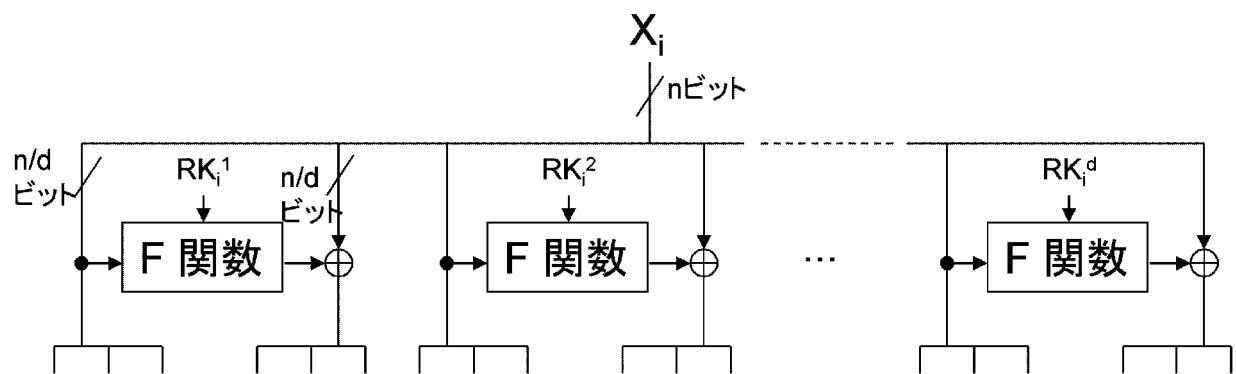
[図25]



[図26]

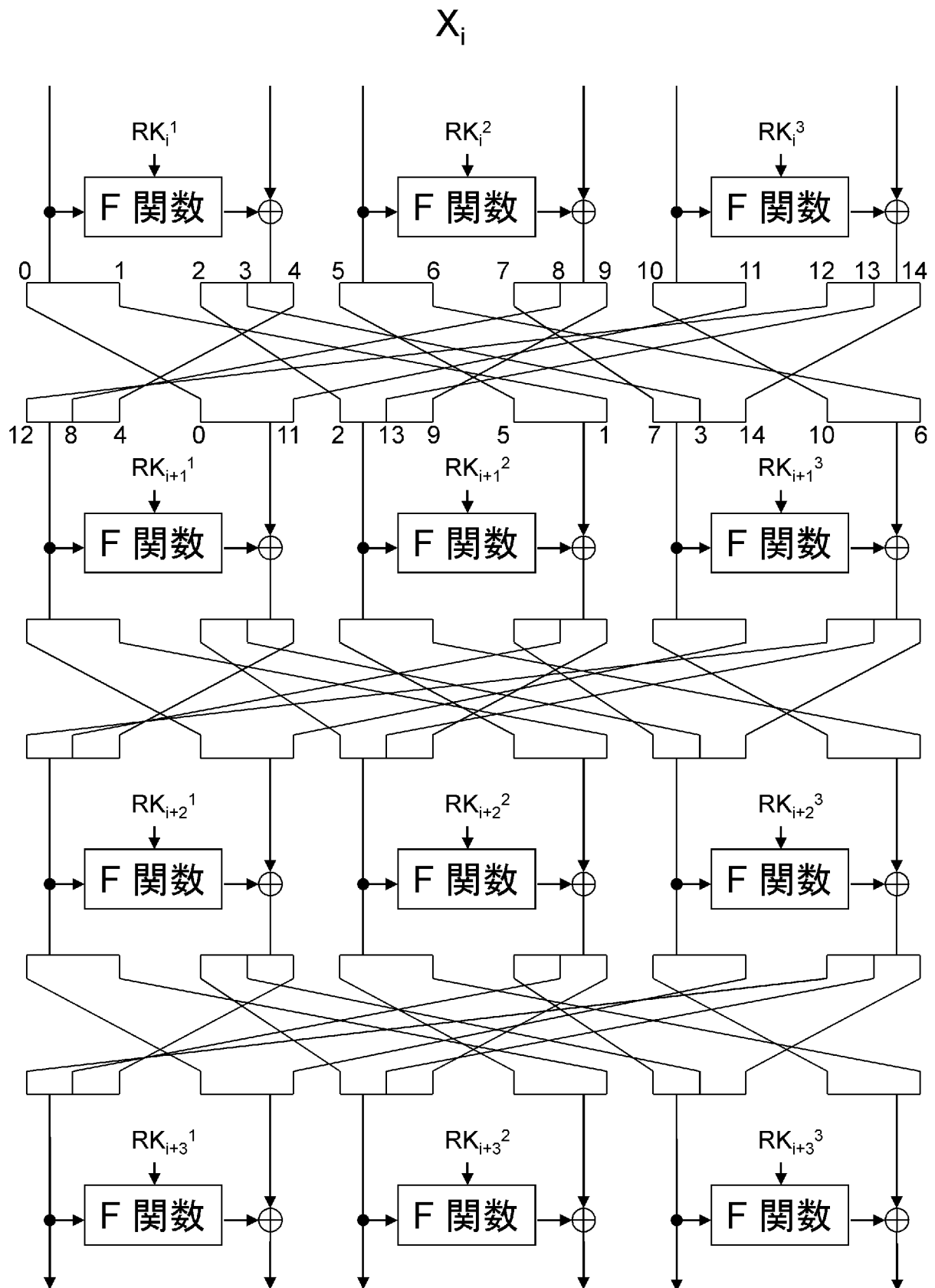
$n$  ビットデータ分割数  $d$ ,  $d/n$  ビットデータ分割数  $p$  と  
full diffusion ラウンド数の関係

| $d \backslash p$ | 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  |

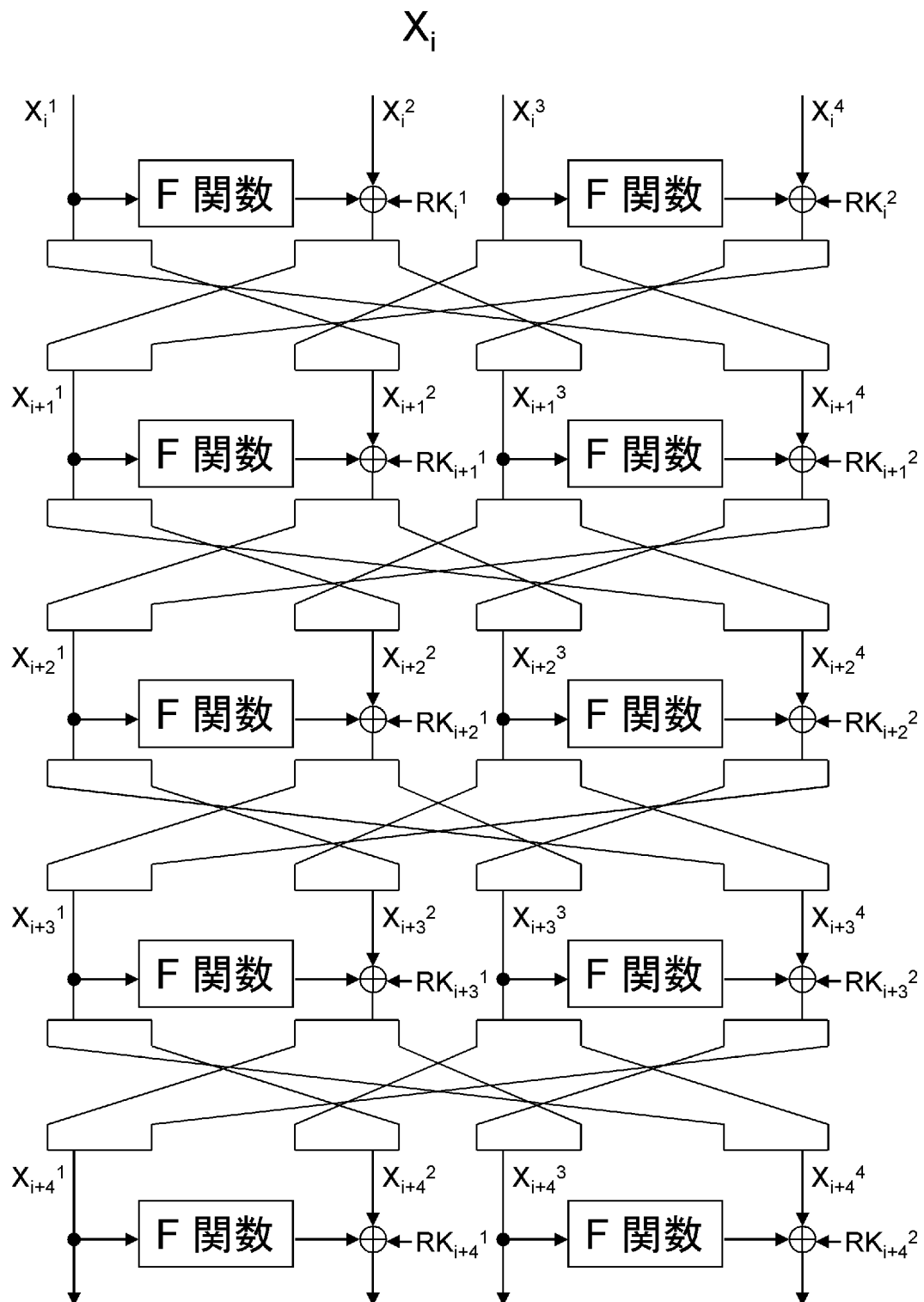


それぞれ  $p$  個に分割

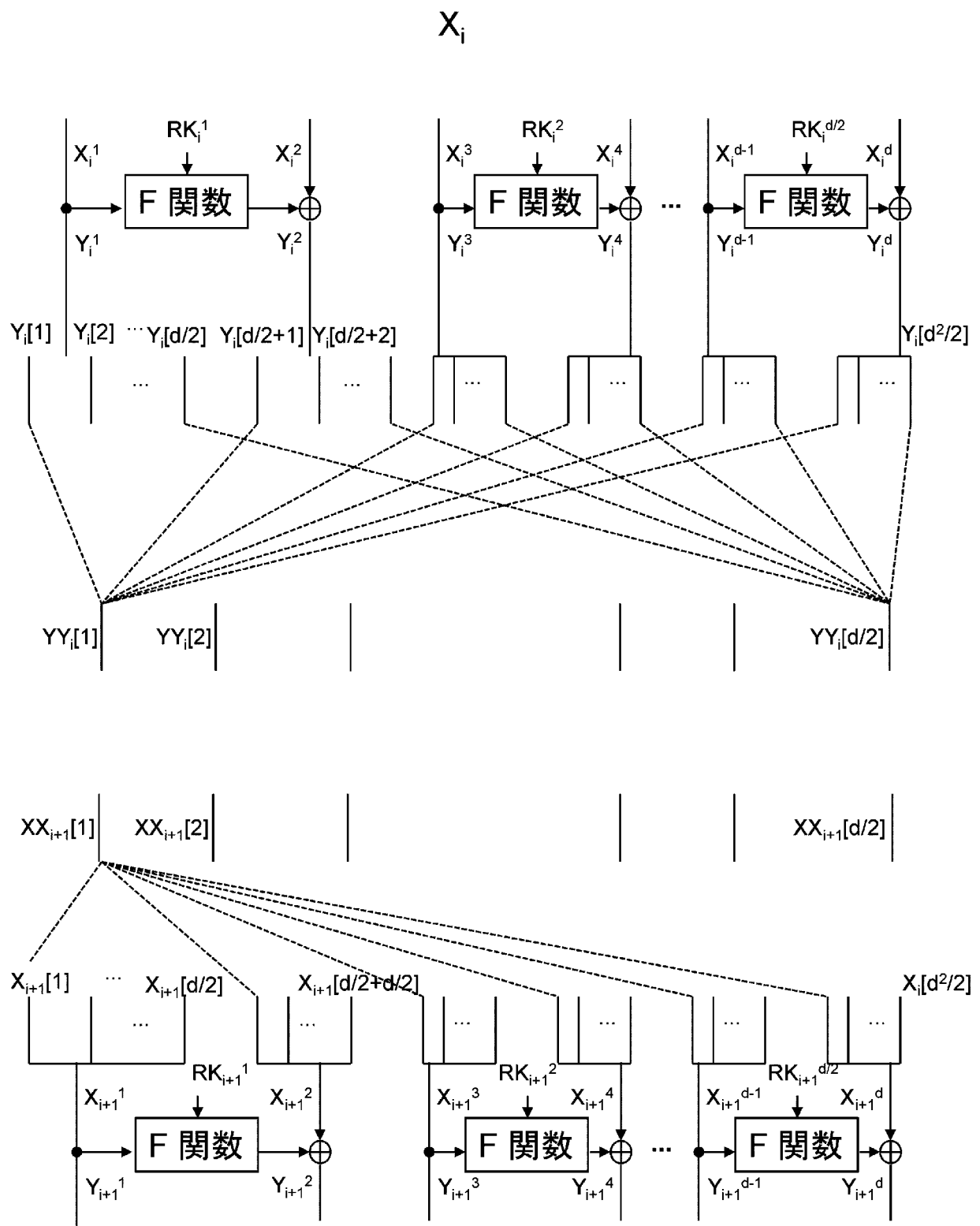
[図27]



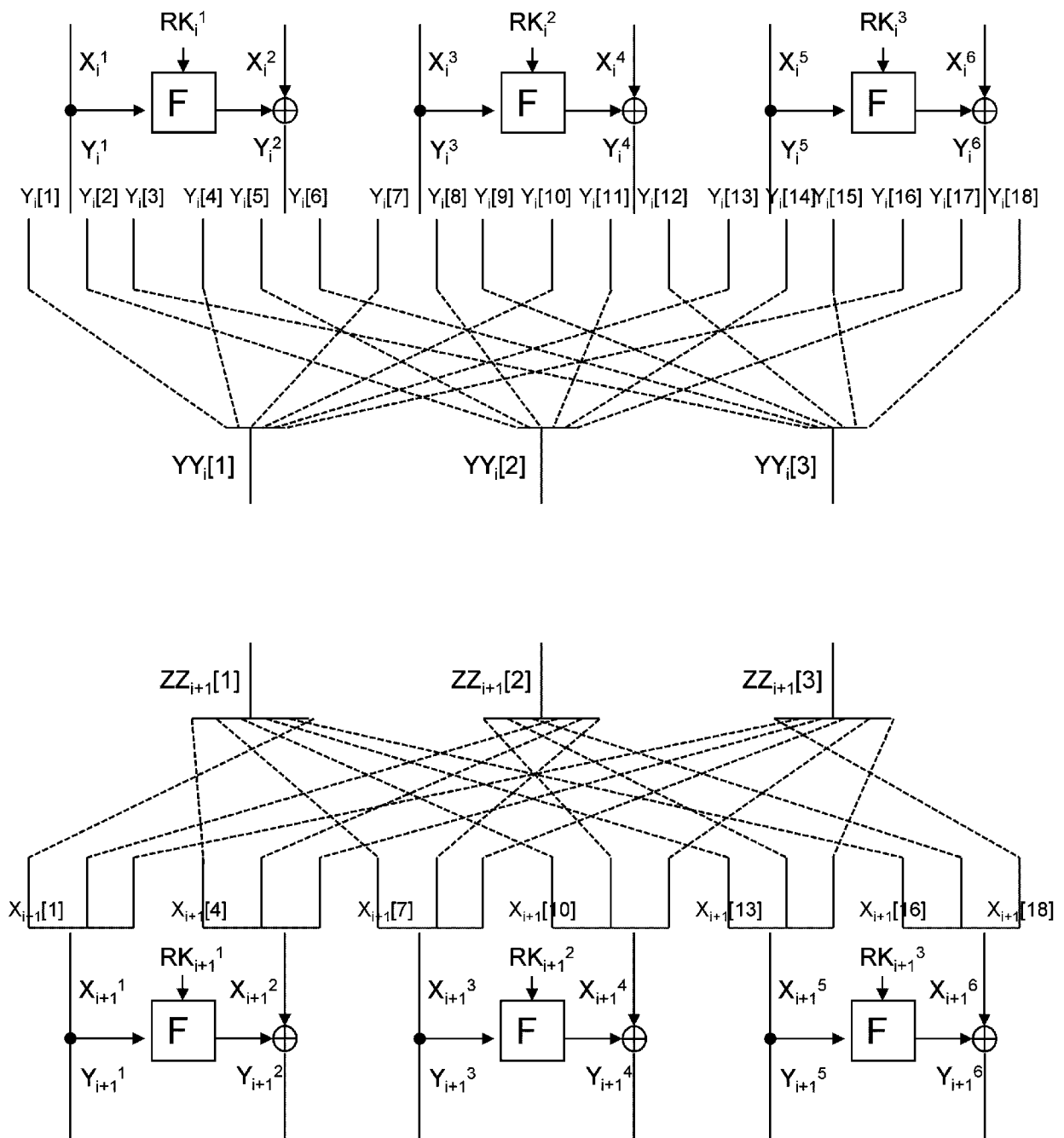
[図28]



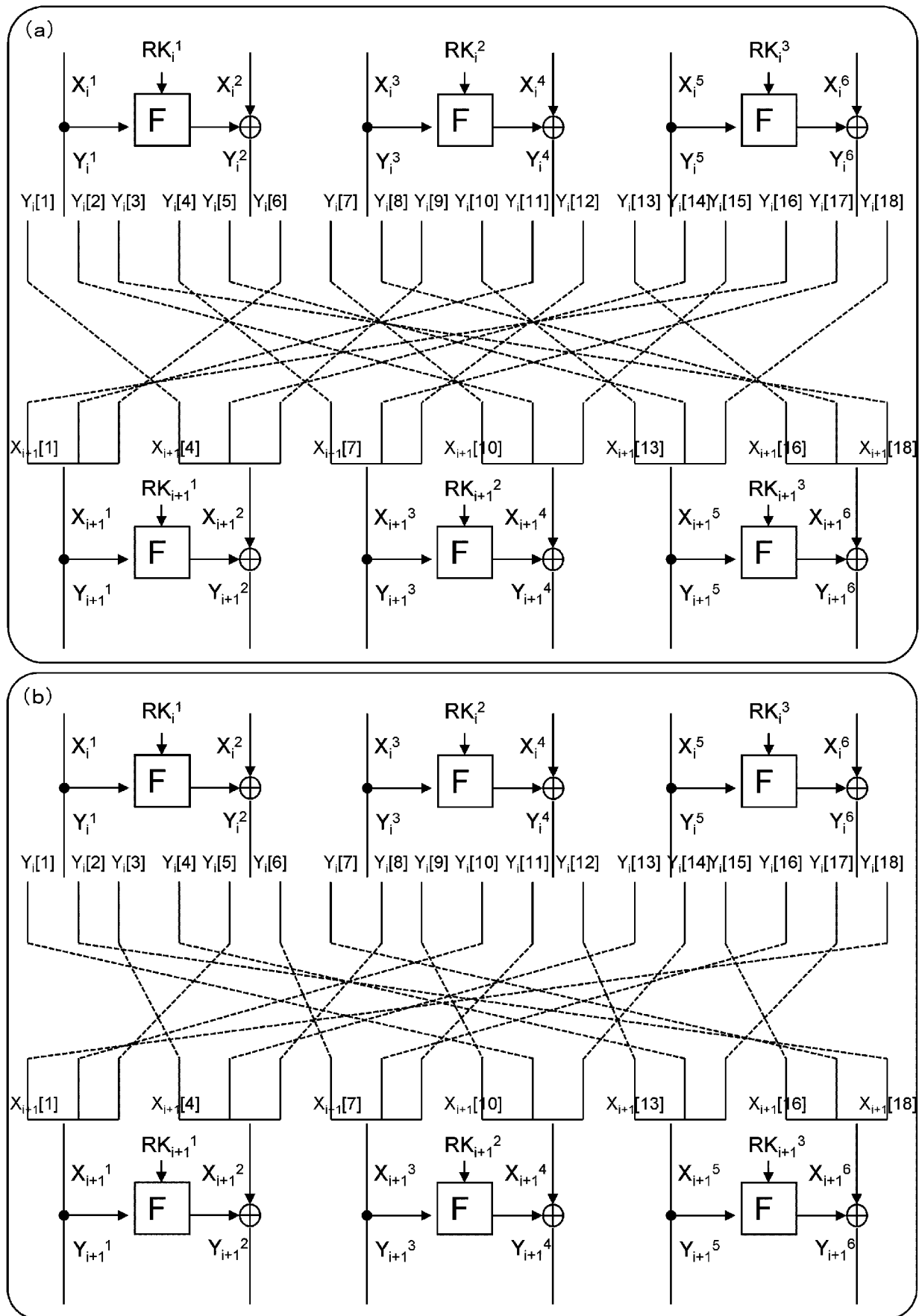
[図29]



[図30]

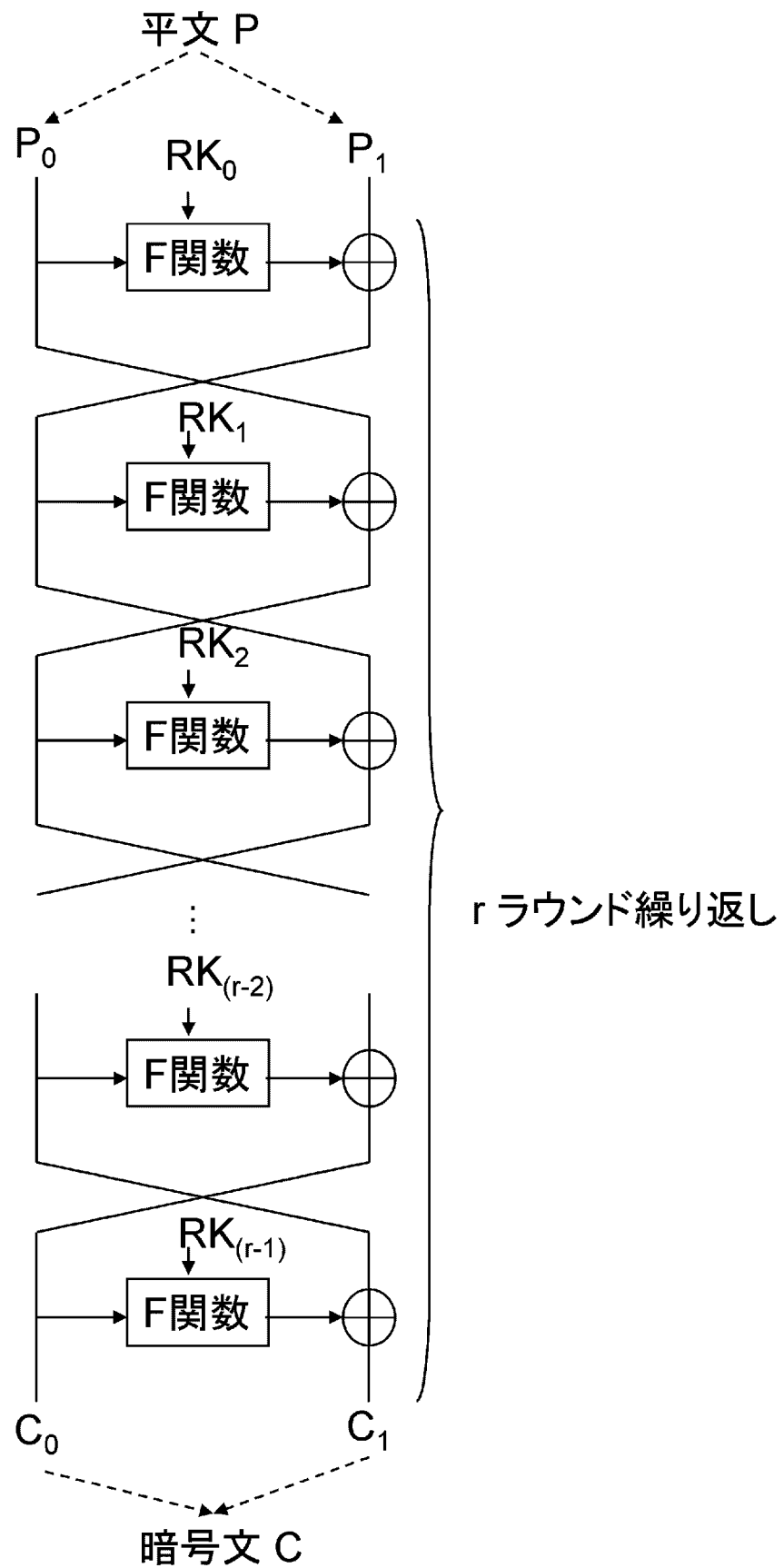
 $X_i$ 

[図31]



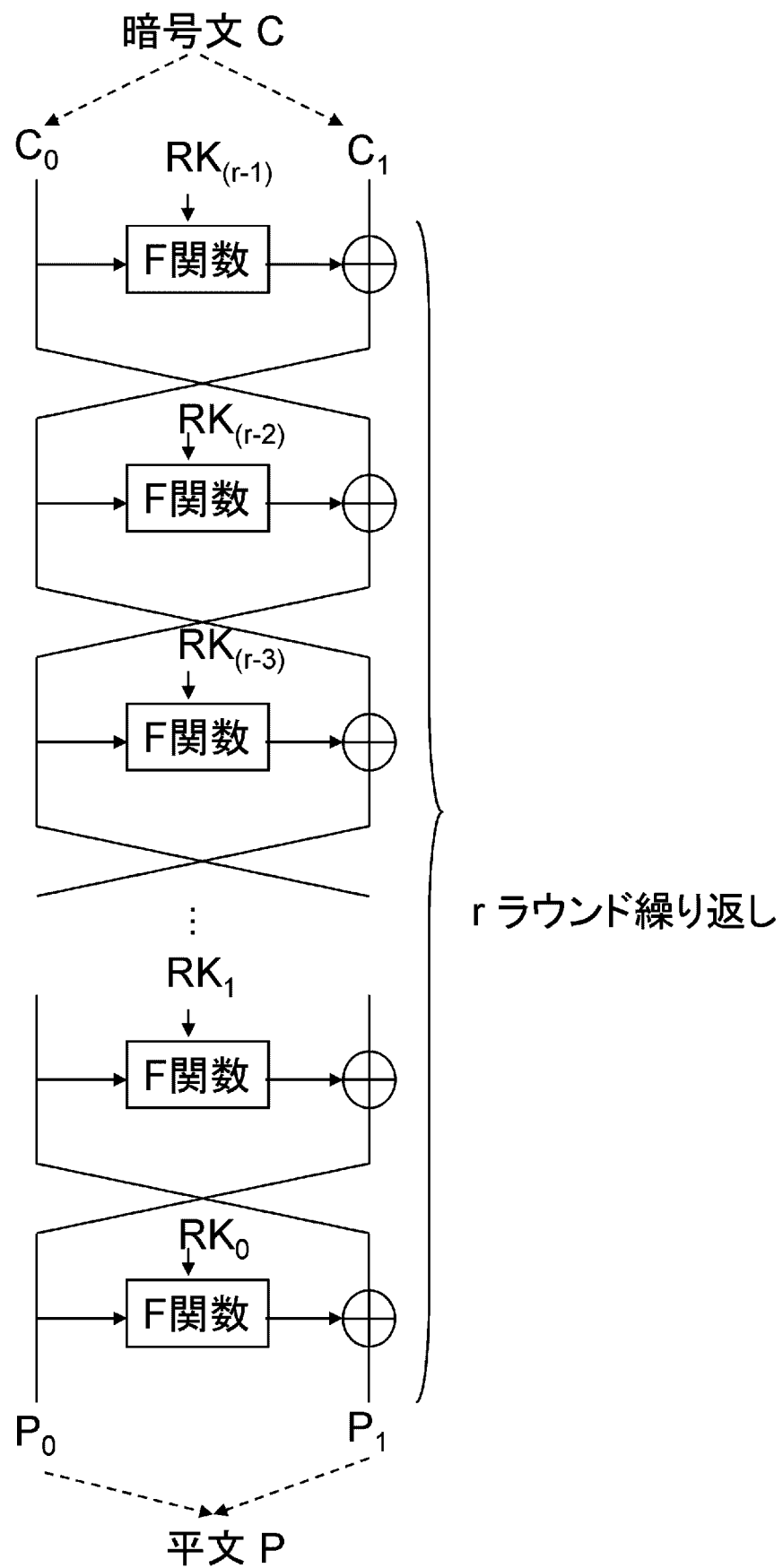
[図32]

## Feistel 構造(暗号化関数)

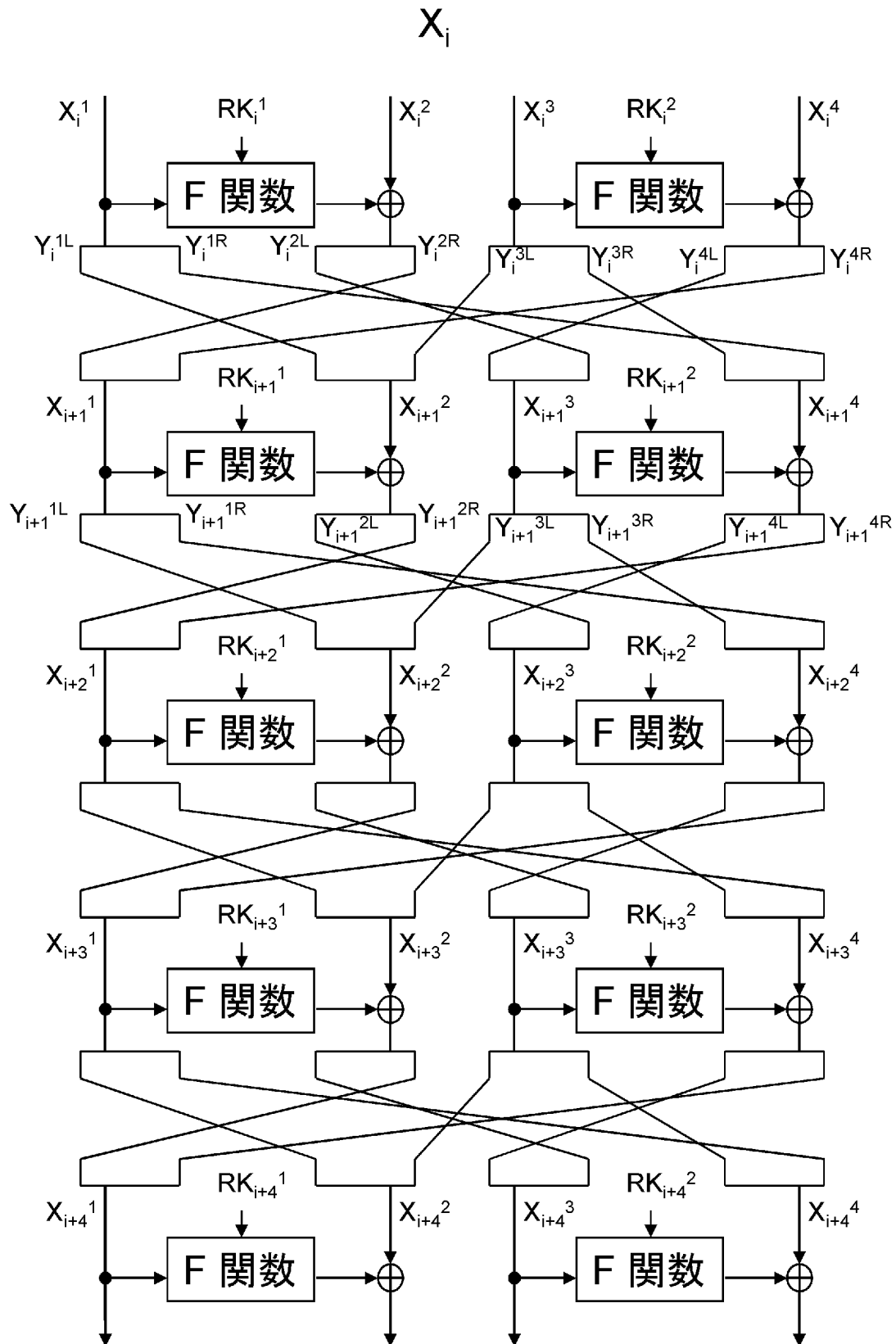


[図33]

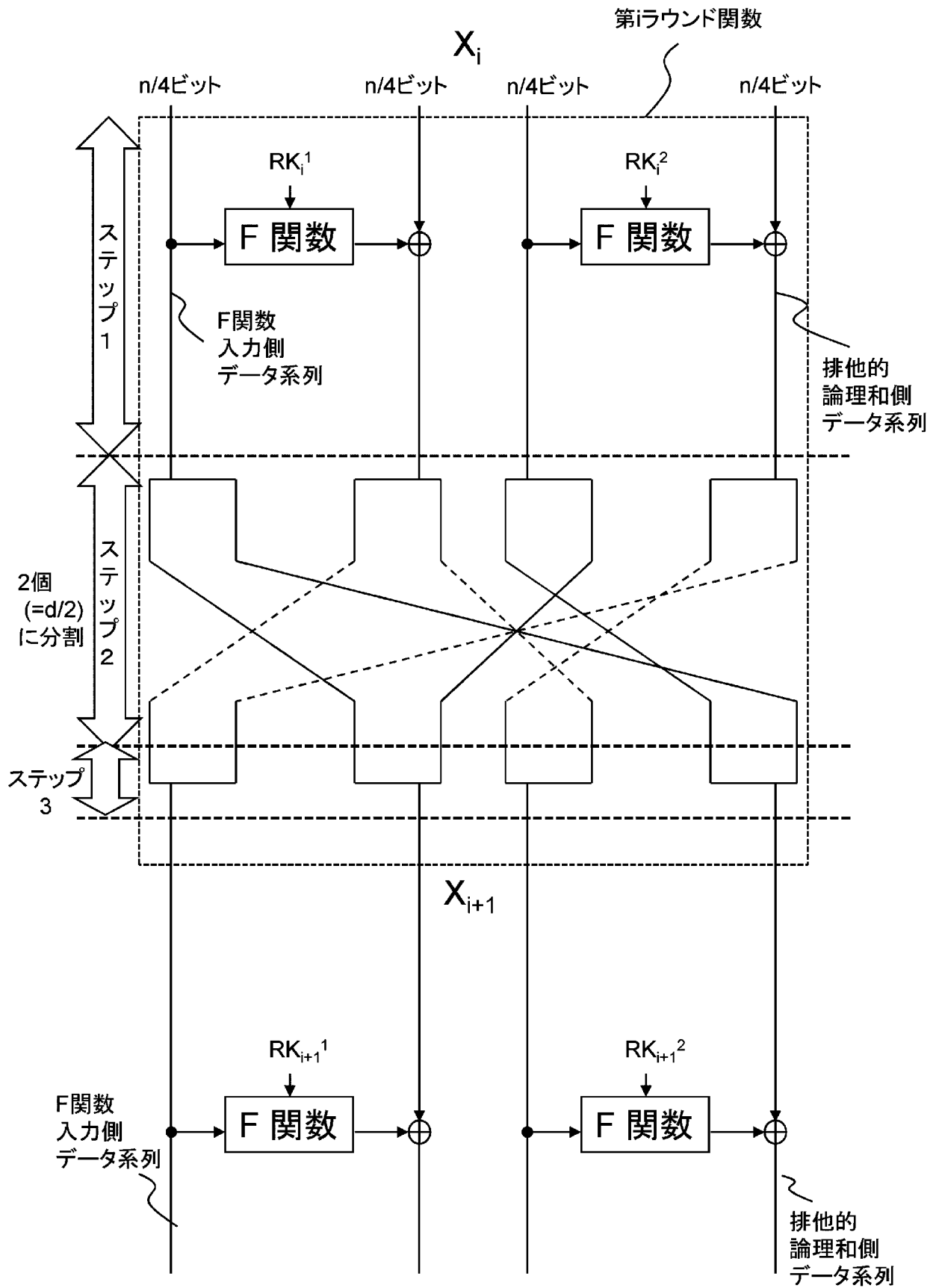
## Feistel 構造(復号関数)



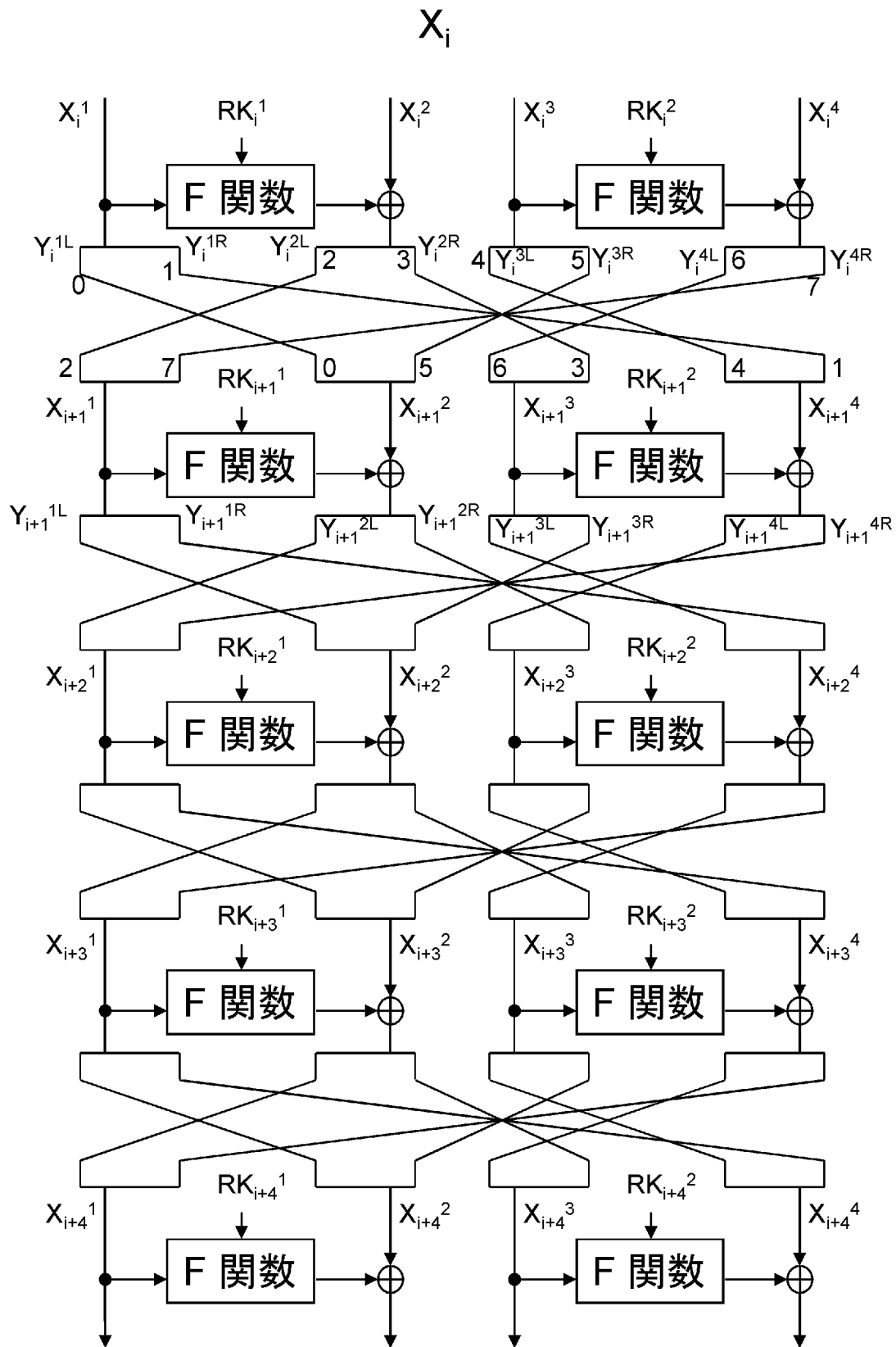
[図34]



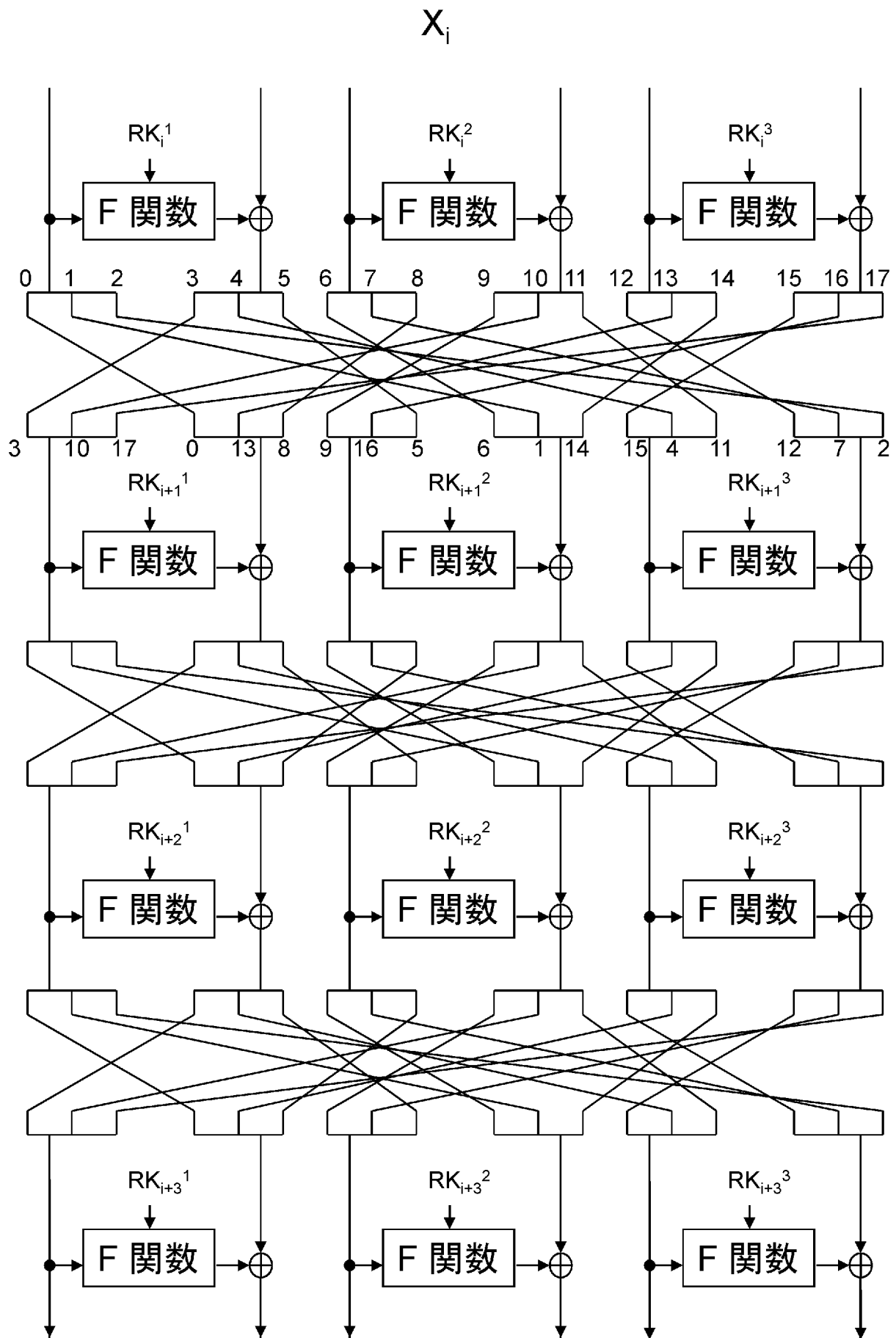
[図35]



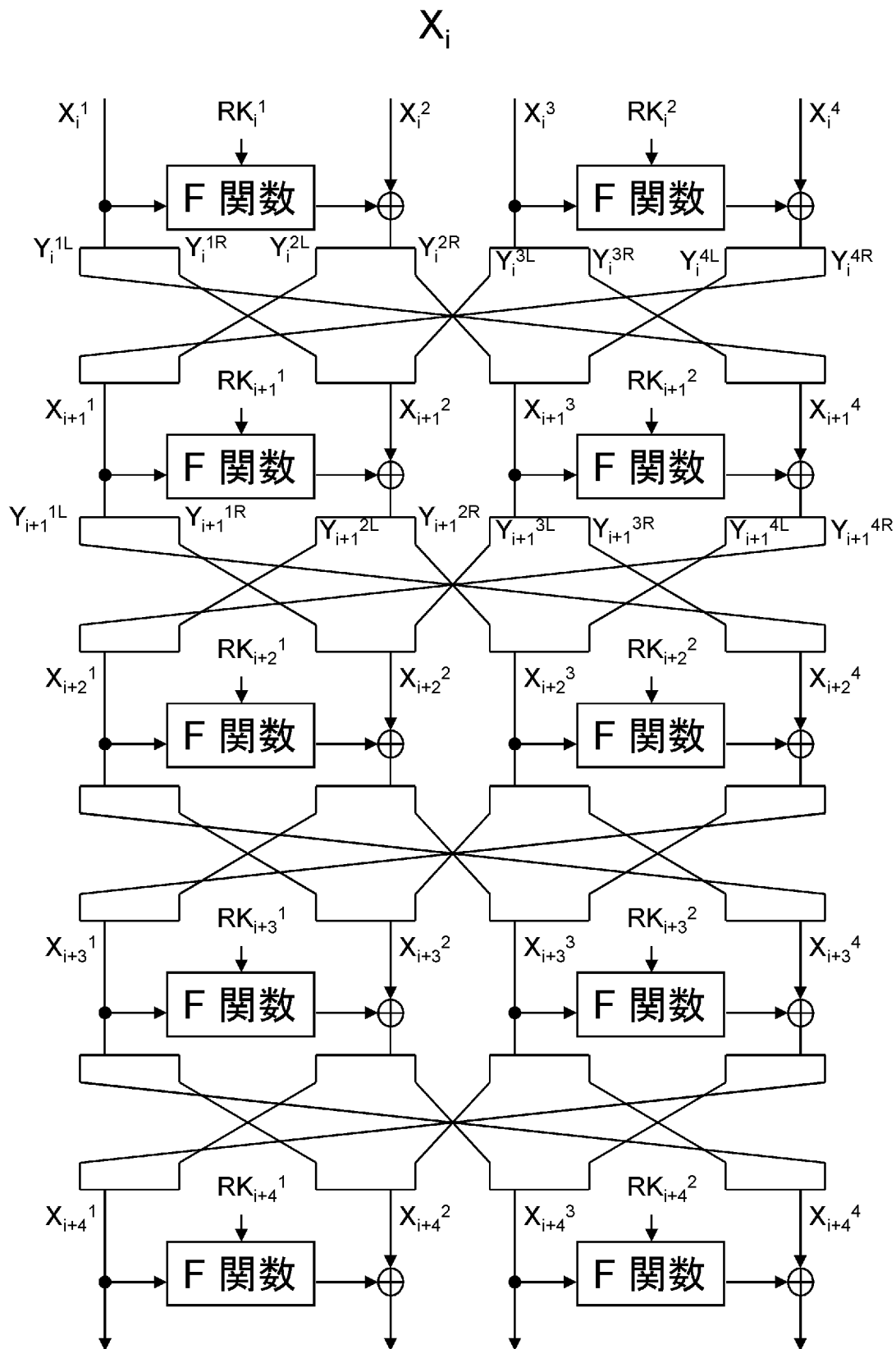
[図36]



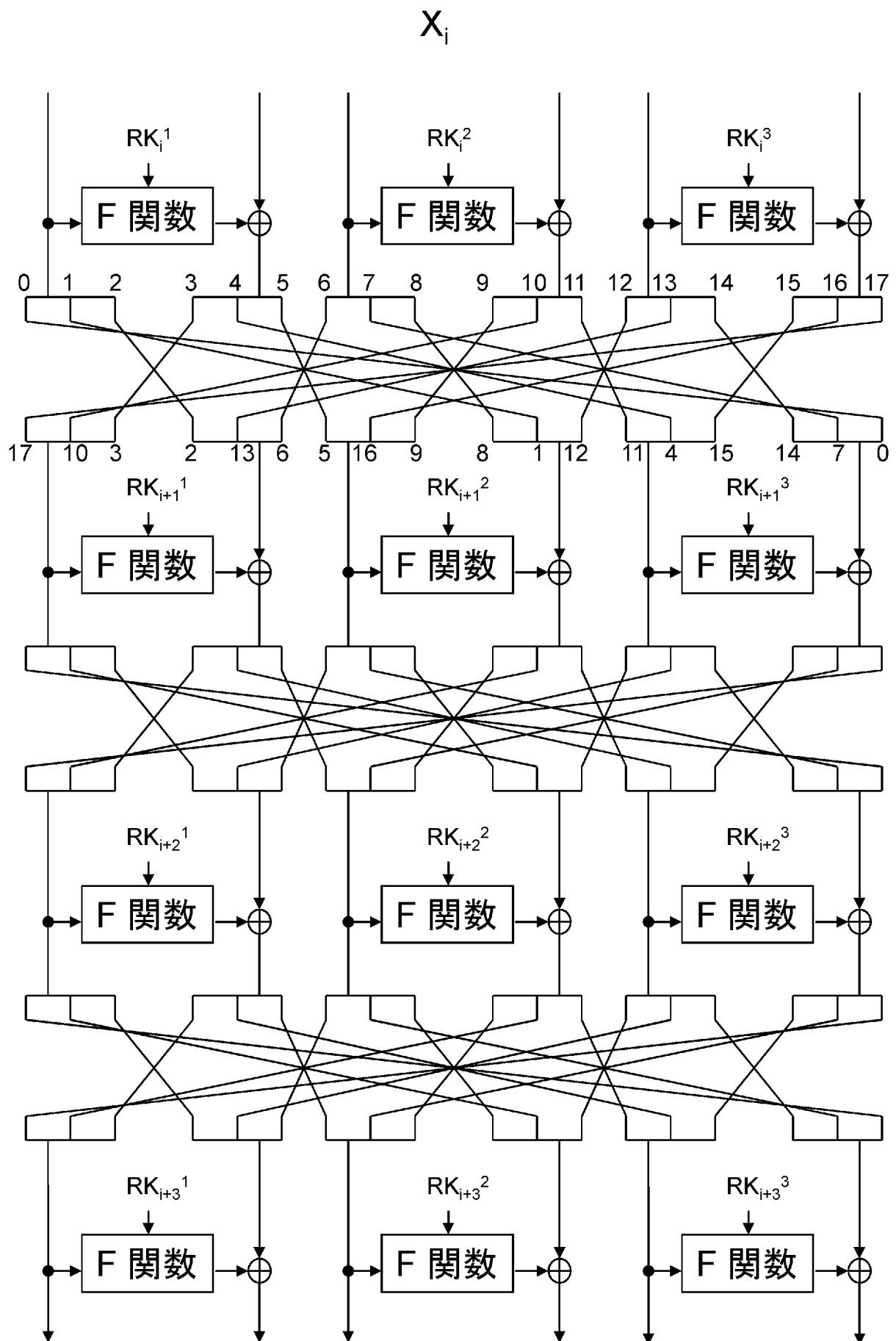
[図37]



[図38]



[図39]



[図40]

