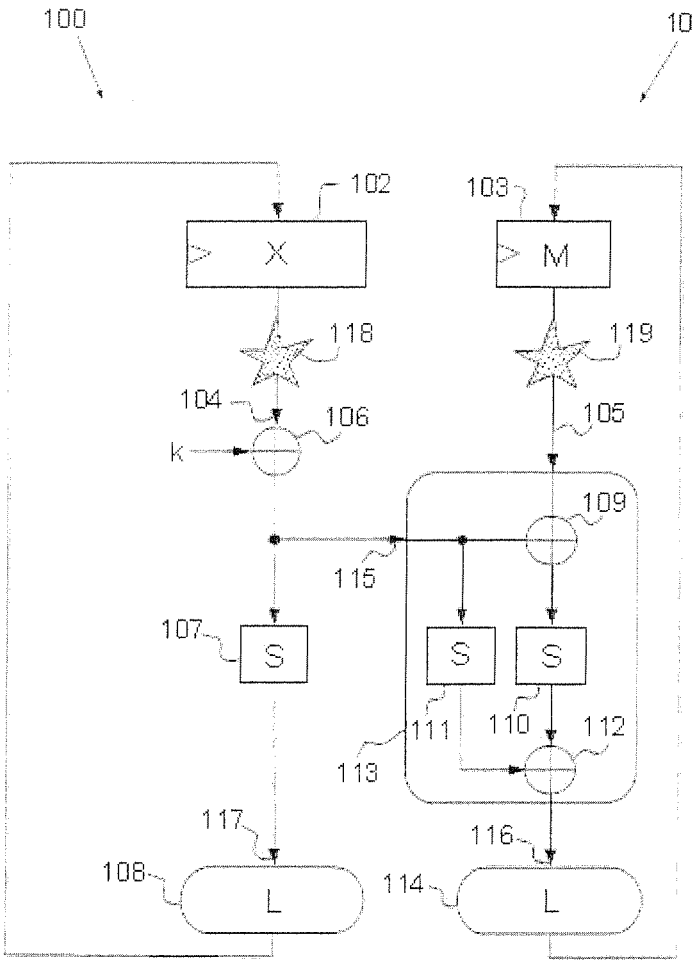
100
101
102
103
X
M
118
119
104
106
105
k
109
115
107
S
S
S
111
110
112
113
117
116
108
L
114
L

FIG.1

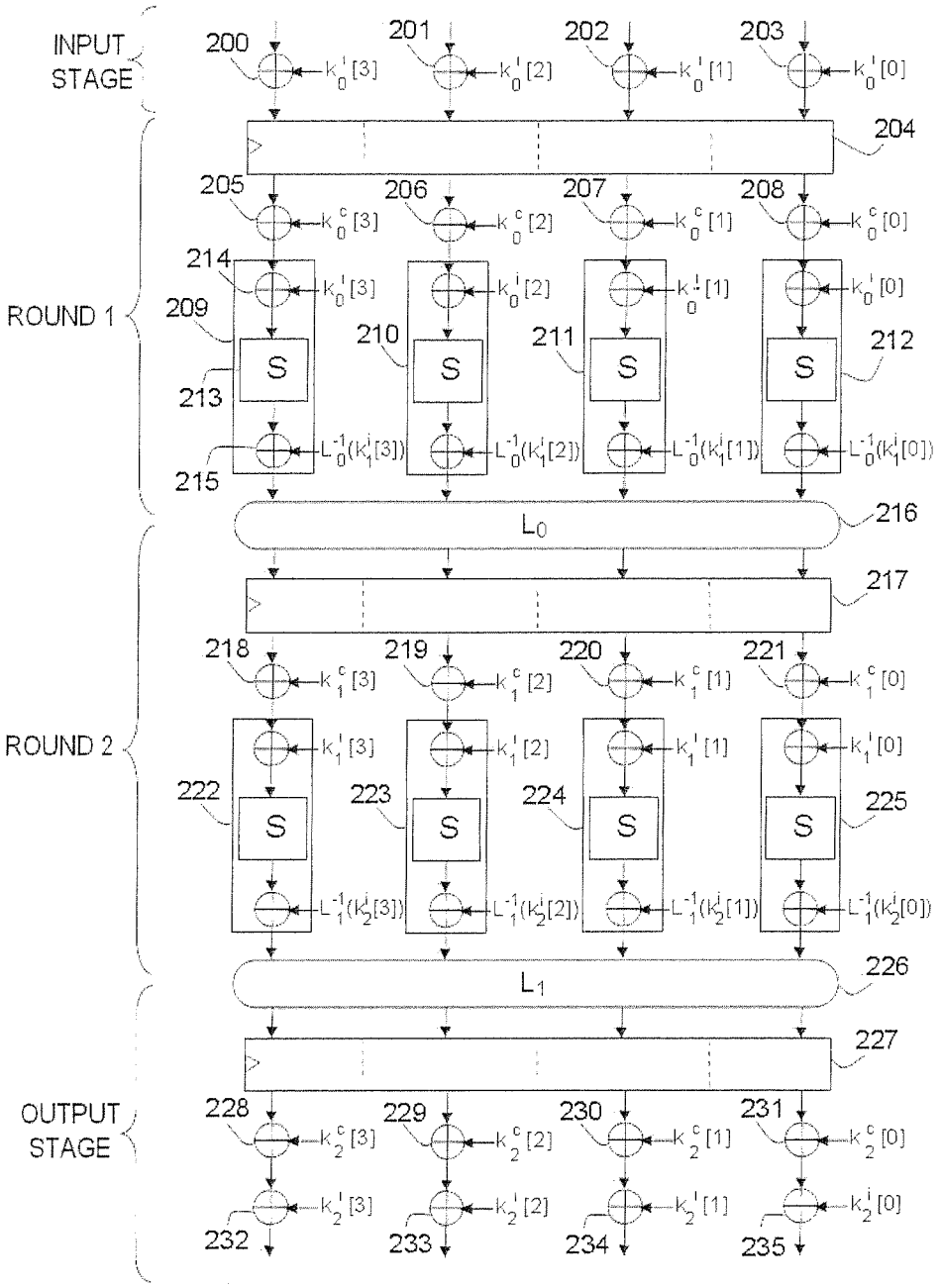
INPUT STAGE
ROUND 1
ROUND 2
OUTPUT STAGE
200
201
202
203
204
205
206
207
208
214
209
210
211
212
213
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
S
L0
L1

FIG.2

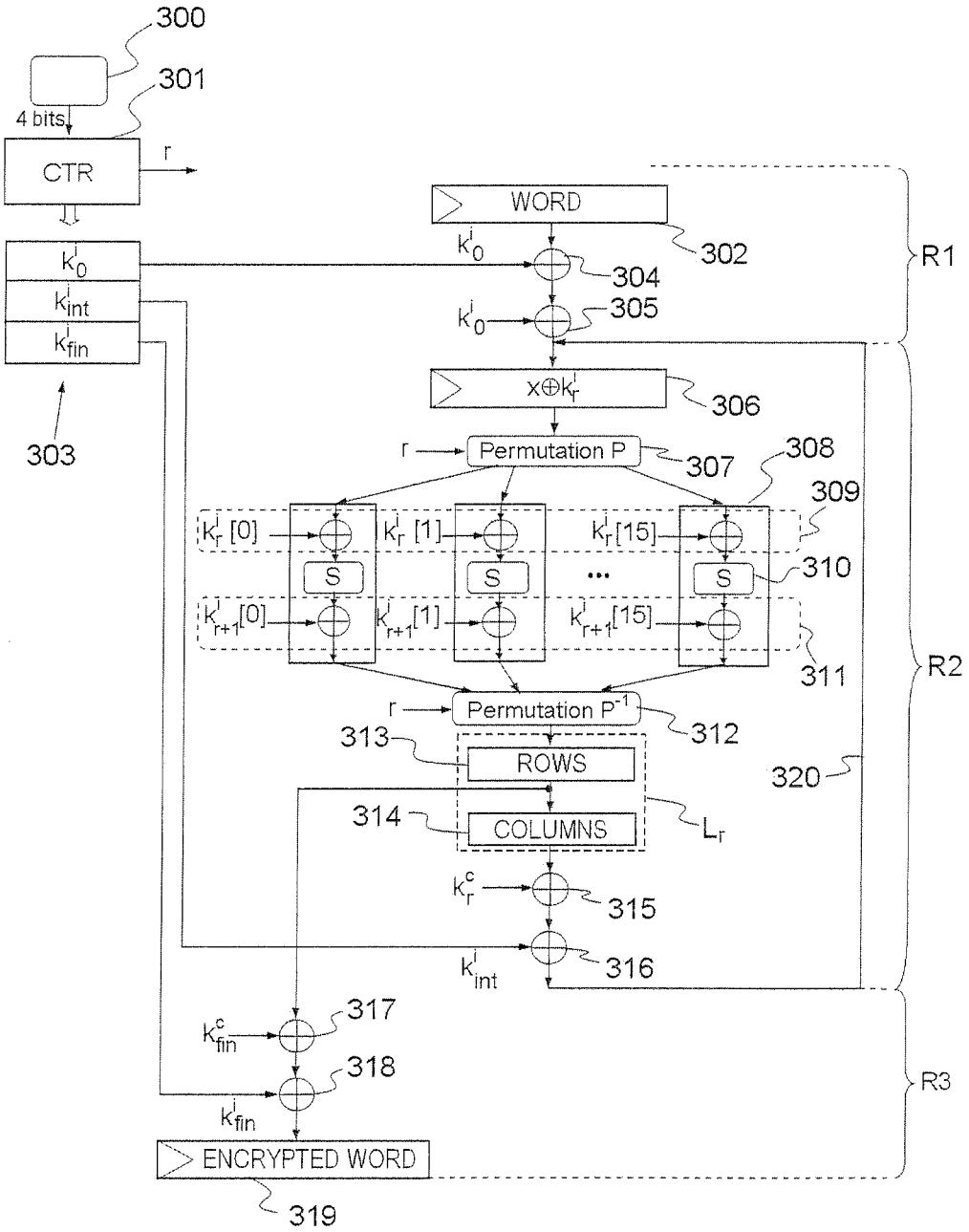
300
301
4 bits
CTR
r
303
WORD
302
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
Permutation P
Permutation P-1
ROWS
COLUMNS
S
R1
R2
R3
ENCRYPTED WORD

FIG.3

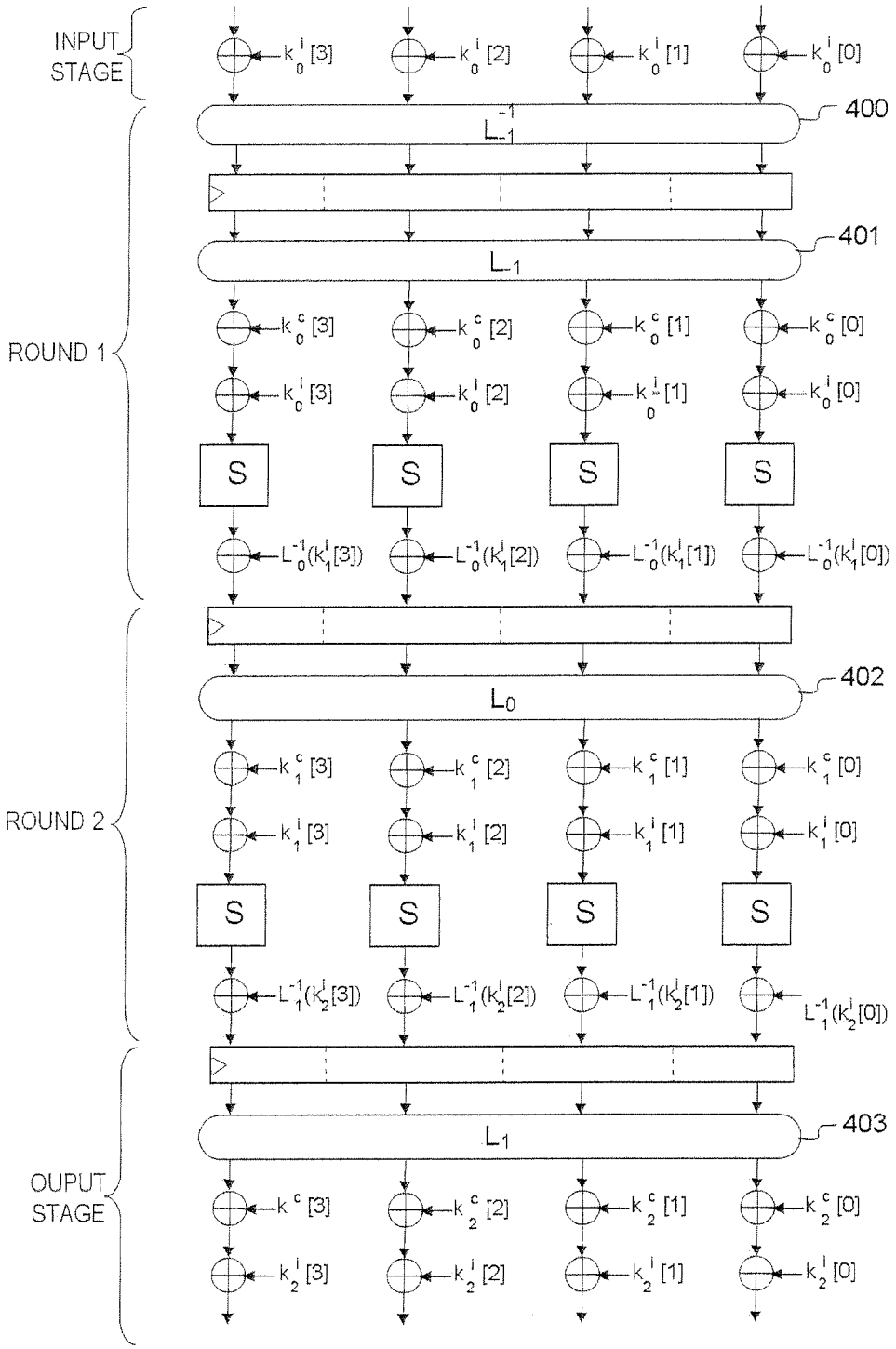

FIG.4