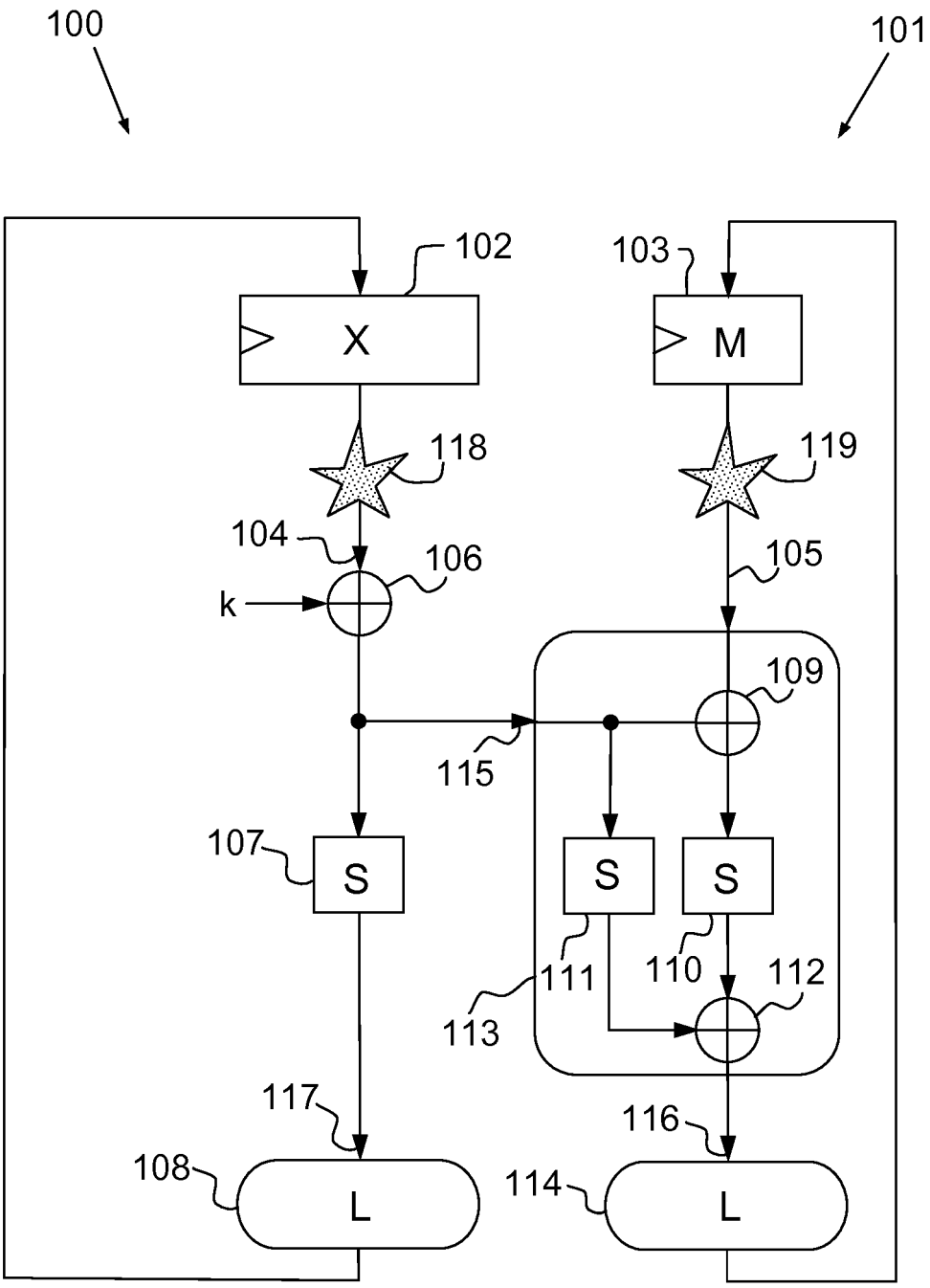
100
101
102
103
X
M
118
119
104
106
105
k
109
115
107
S
S
S
111
110
112
113
117
116
108
114
L
L

FIG.1

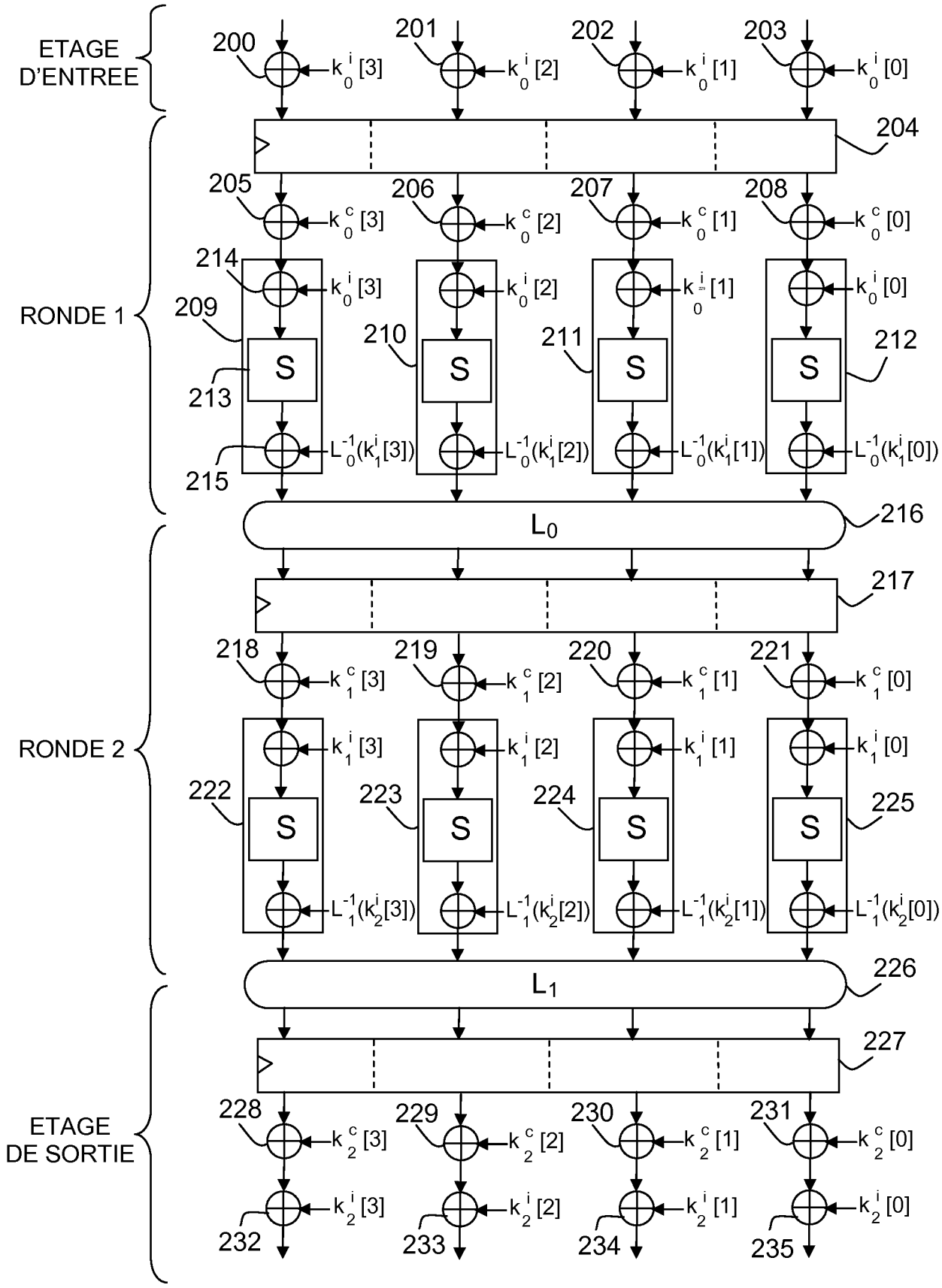
ETAGE D'ENTREE
RONDE 1
RONDE 2
ETAGE DE SORTIE
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
S
L_0
L_1
$k_0^i[3]$
$k_0^i[2]$
$k_0^i[1]$
$k_0^i[0]$
$k_0^c[3]$
$k_0^c[2]$
$k_0^c[1]$
$k_0^c[0]$
$L_0^{-1}(k_1^i[3])$
$L_0^{-1}(k_1^i[2])$
$L_0^{-1}(k_1^i[1])$
$L_0^{-1}(k_1^i[0])$
$k_1^i[3]$
$k_1^i[2]$
$k_1^i[1]$
$k_1^i[0]$
$k_1^c[3]$
$k_1^c[2]$
$k_1^c[1]$
$k_1^c[0]$
$L_1^{-1}(k_2^i[3])$
$L_1^{-1}(k_2^i[2])$
$L_1^{-1}(k_2^i[1])$
$L_1^{-1}(k_2^i[0])$
$k_2^c[3]$
$k_2^c[2]$
$k_2^c[1]$
$k_2^c[0]$
$k_2^i[3]$
$k_2^i[2]$
$k_2^i[1]$
$k_2^i[0]$

FIG.2

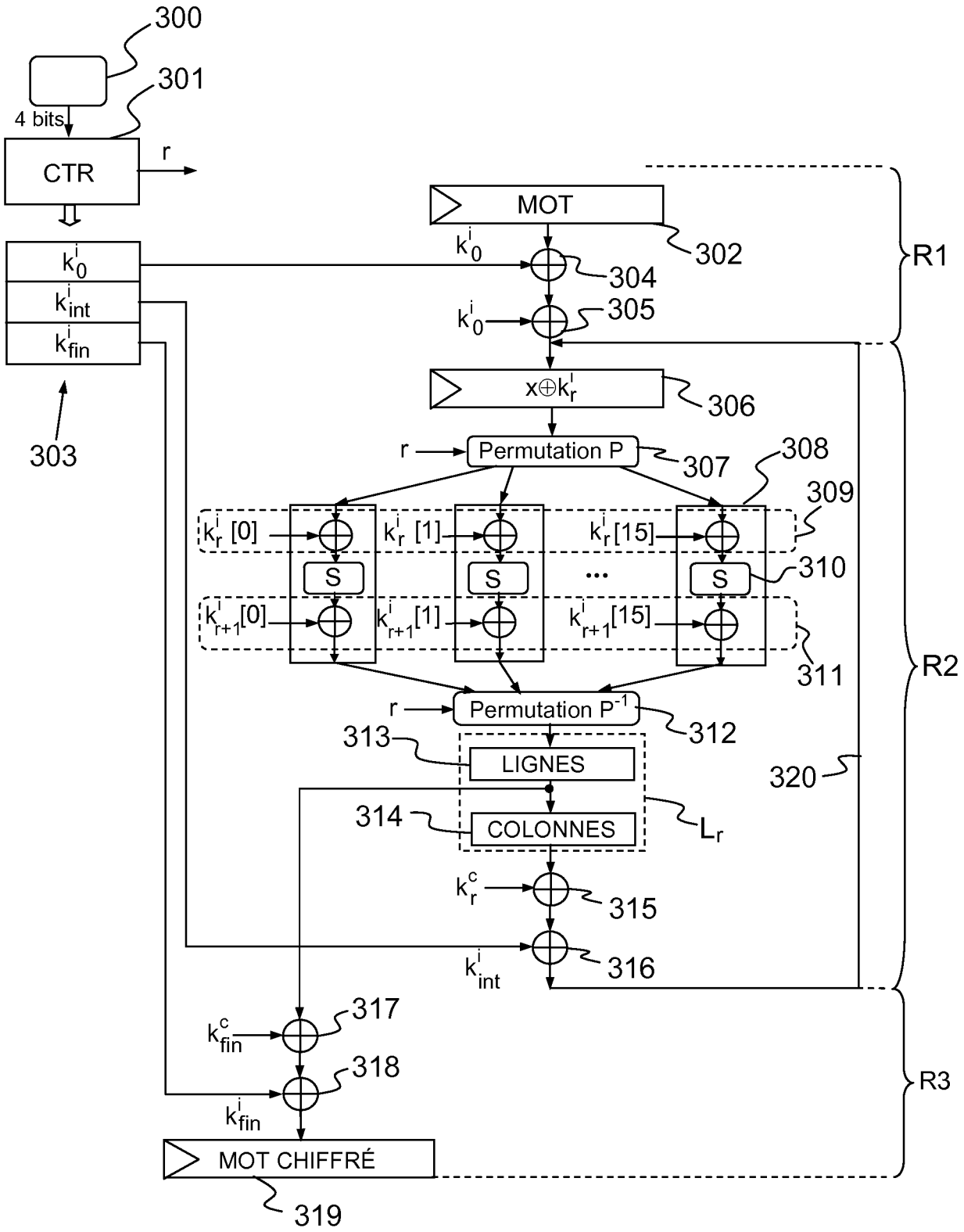
300
301
4 bits
CTR
r
303
MOT
302
304
305
306
Permutation P
307
308
309
S
310
311
Permutation P-1
312
313
LIGNES
314
COLONNES
Lr
315
316
317
318
MOT CHIFFRÉ
319
320
R1
R2
R3

FIG.3

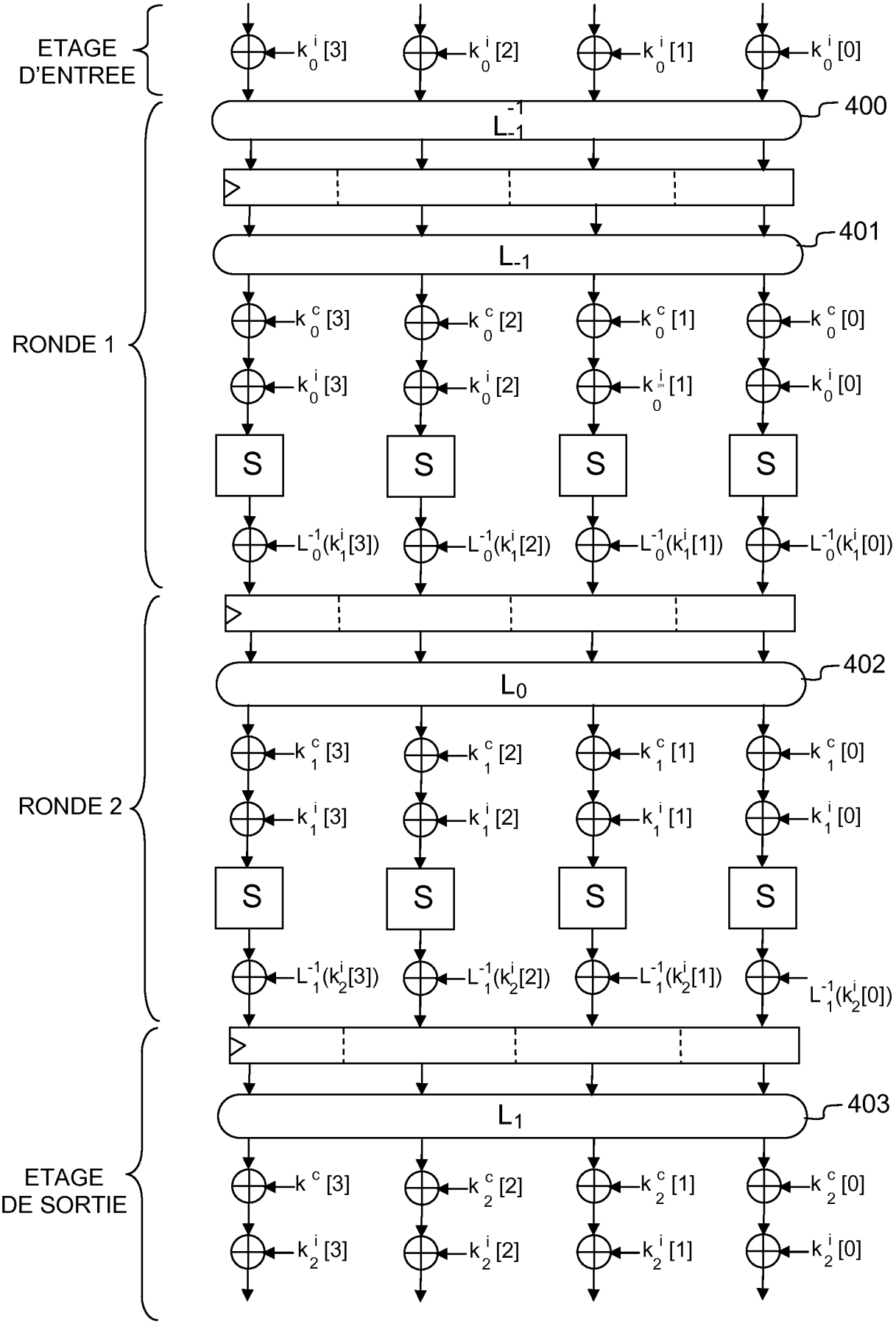
ETAGE D'ENTREE
RONDE 1
RONDE 2
ETAGE DE SORTIE
400
401
402
403
S

FIG.4