
102
104
VIDEO SOURCE DEVICE
VIDEO SINK DEVICE
106

FIG. 1

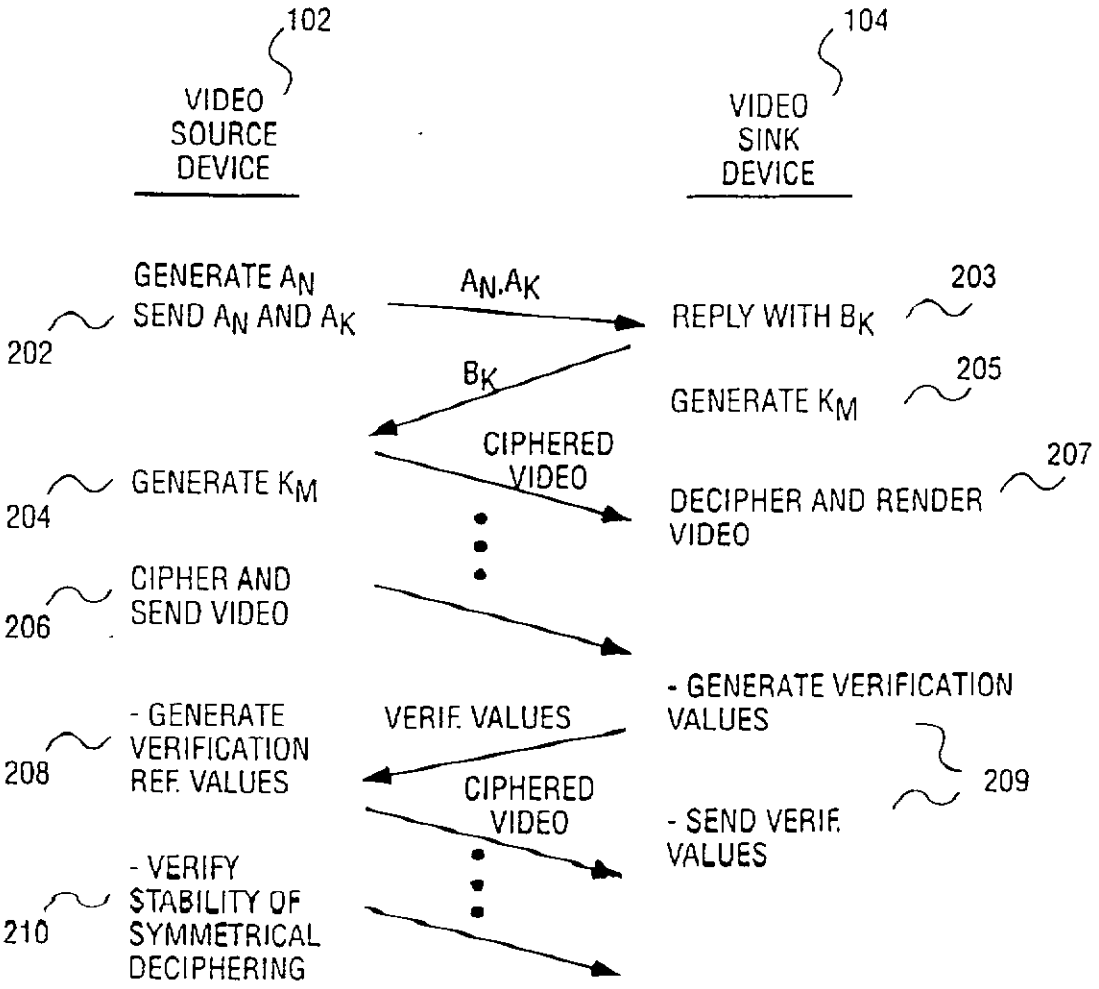

102
104
VIDEO SOURCE DEVICE
VIDEO SINK DEVICE
GENERATE A_N
SEND A_N AND A_K
202
A_N.A_K
203
REPLY WITH B_K
B_K
GENERATE K_M
205
CIPHERED VIDEO
207
GENERATE K_M
204
DECIPHER AND RENDER VIDEO
CIPHER AND SEND VIDEO
206
- GENERATE VERIFICATION VALUES
209
VERIF. VALUES
- GENERATE VERIFICATION REF. VALUES
208
CIPHERED VIDEO
- SEND VERIF. VALUES
- VERIFY STABILITY OF SYMMETRICAL DECIPHERING
210

FIG. 2

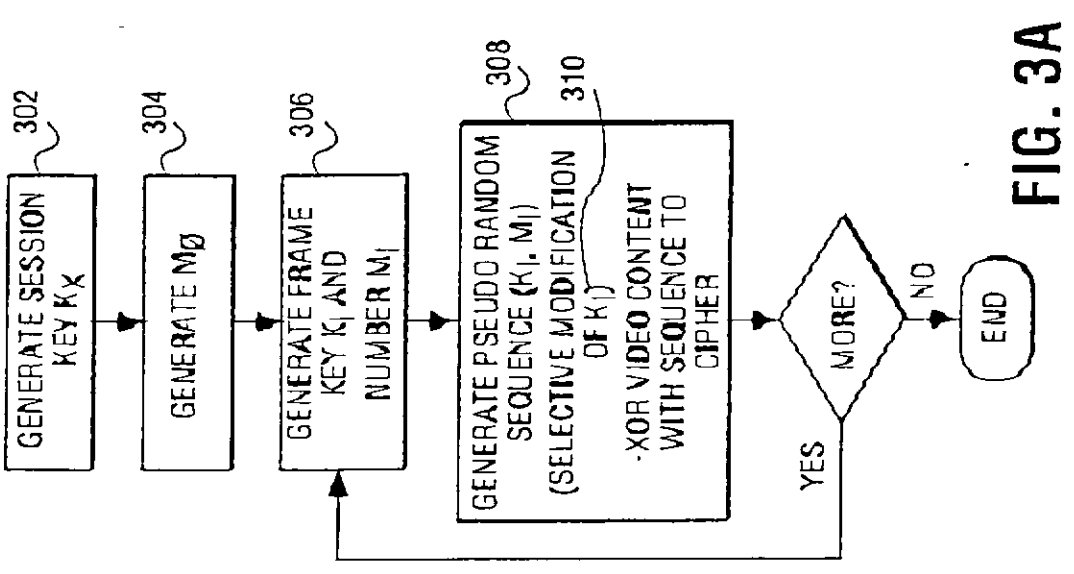

GENERATE SESSION KEY K_X
302
GENERATE $M_\emptyset$
304
GENERATE FRAME KEY K_I AND NUMBER M_I
306
GENERATE PSEUDO RANDOM SEQUENCE (K_I, M_I) (SELECTIVE MODIFICATION OF K_I)
308
310
-XOR VIDEO CONTENT WITH SEQUENCE TO CIPHER
MORE?
YES
NO
END

FIG. 3A

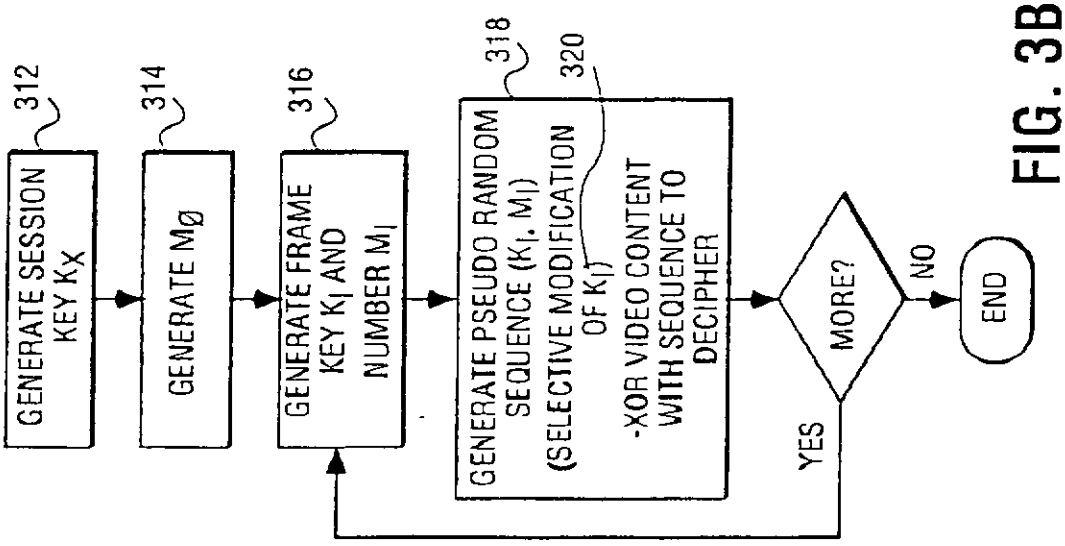

GENERATE SESSION KEY K_X
312
GENERATE $M_\emptyset$
314
GENERATE FRAME KEY K_I AND NUMBER M_I
316
GENERATE PSEUDO RANDOM SEQUENCE (K_I, M_I) (SELECTIVE MODIFICATION OF K_I)
318
320
-XOR VIDEO CONTENT WITH SEQUENCE TO DECIPHER
MORE?
YES
NO
END

FIG. 3B

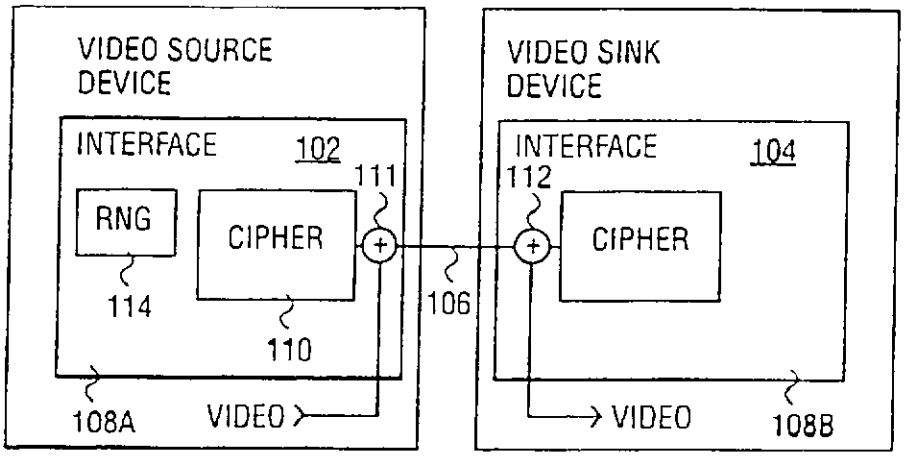

VIDEO SOURCE DEVICE
INTERFACE
102
RNG
CIPHER
111
114
110
106
108A
VIDEO
VIDEO SINK DEVICE
INTERFACE
104
112
CIPHER
VIDEO
108B

FIG. 4

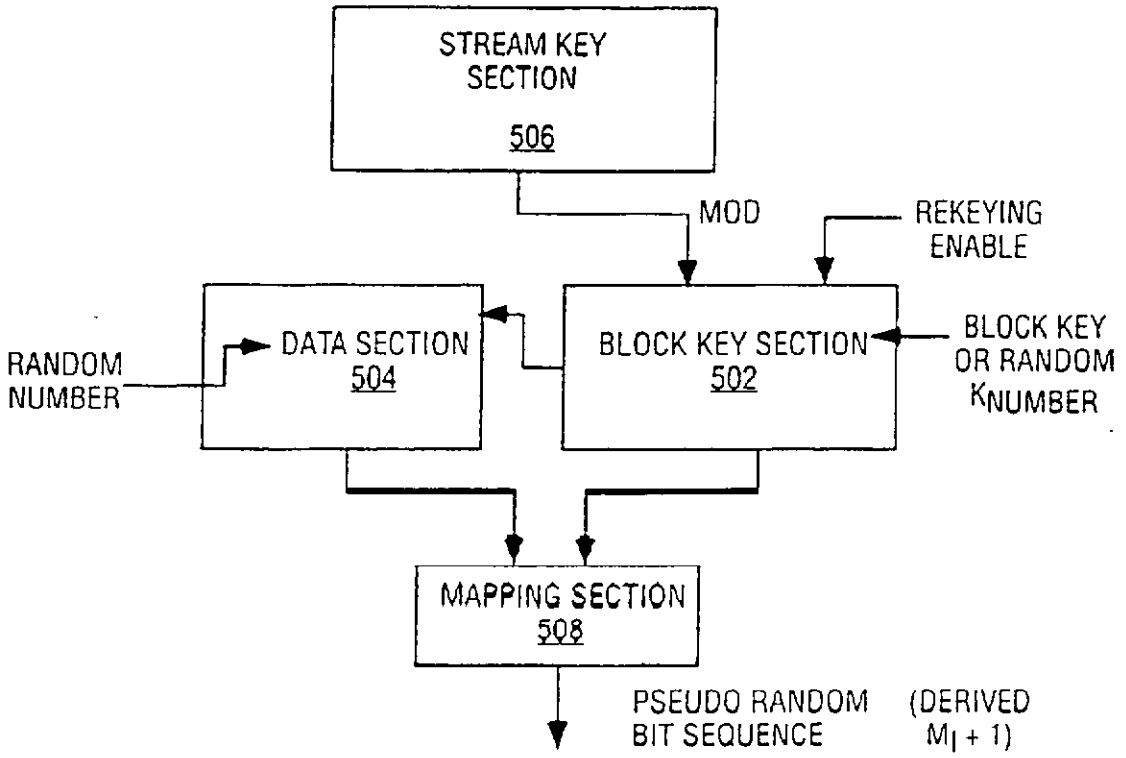

STREAM KEY SECTION
506
MOD
REKEYING ENABLE
RANDOM NUMBER
DATA SECTION
504
BLOCK KEY SECTION
502
BLOCK KEY OR RANDOM KNUMBER
MAPPING SECTION
508
PSEUDO RANDOM BIT SEQUENCE
(DERIVED $M_I + 1$)

FIG. 5

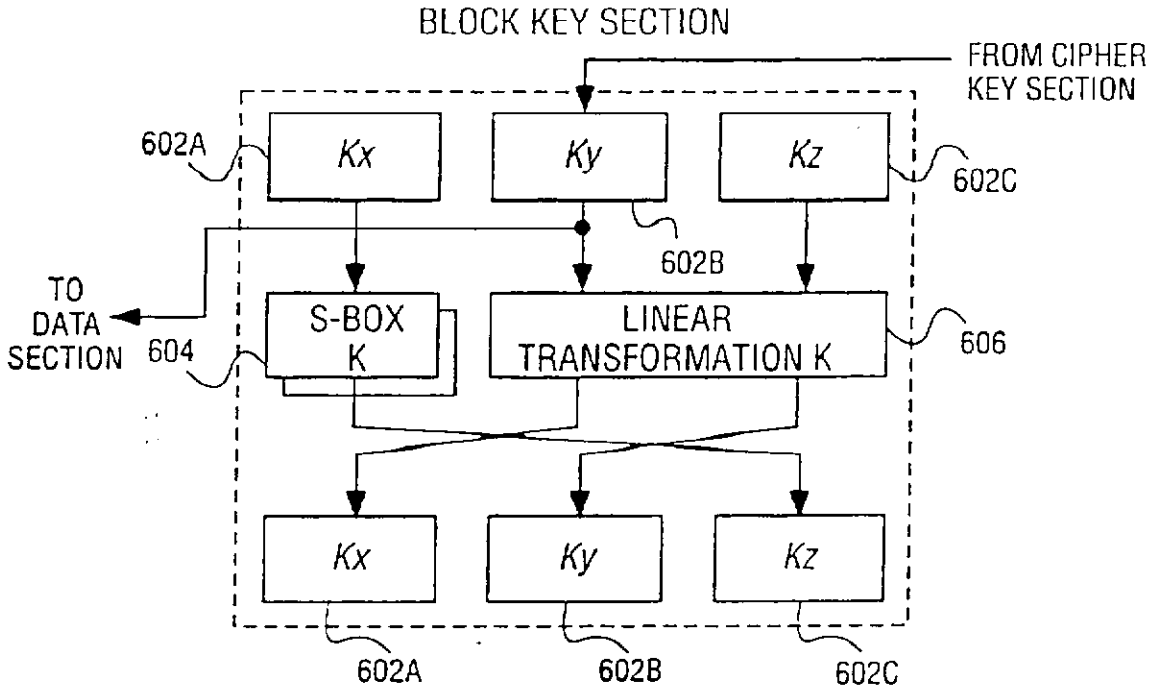

BLOCK KEY SECTION
FROM CIPHER KEY SECTION
602A
Kx
Ky
Kz
602C
602B
TO DATA SECTION
604
S-BOX K
LINEAR TRANSFORMATION K
606
Kx
Ky
Kz
602A
602B
602C

FIG. 6

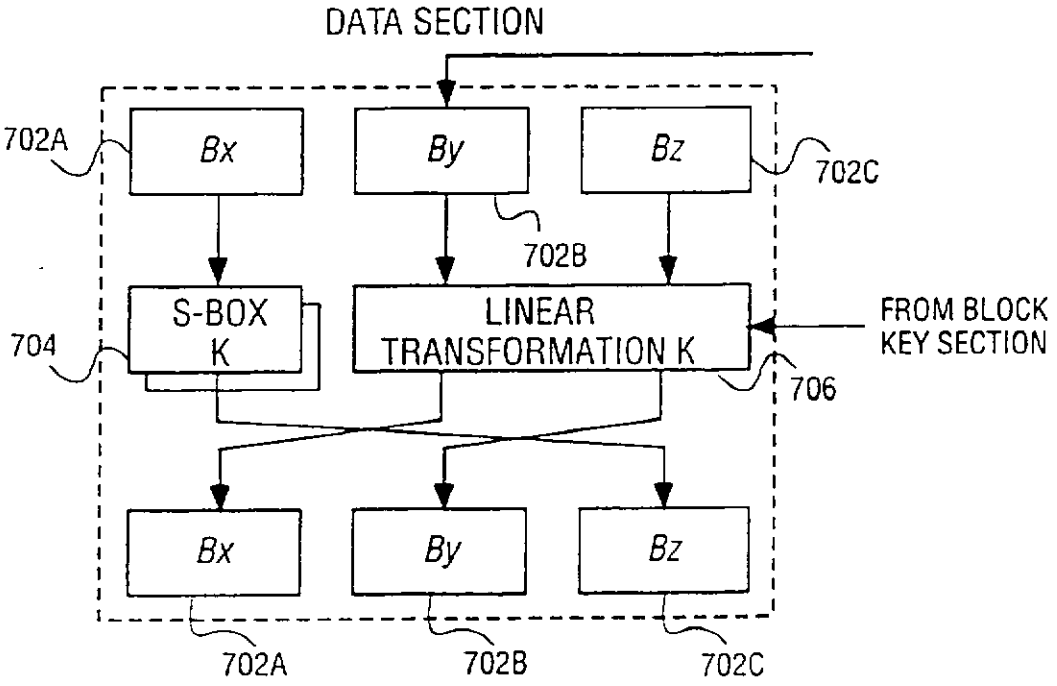

DATA SECTION
702A
Bx
By
Bz
702C
702B
704
S-BOX K
LINEAR TRANSFORMATION K
FROM BLOCK KEY SECTION
706
Bx
By
Bz
702A
702B
702C

FIG. 7

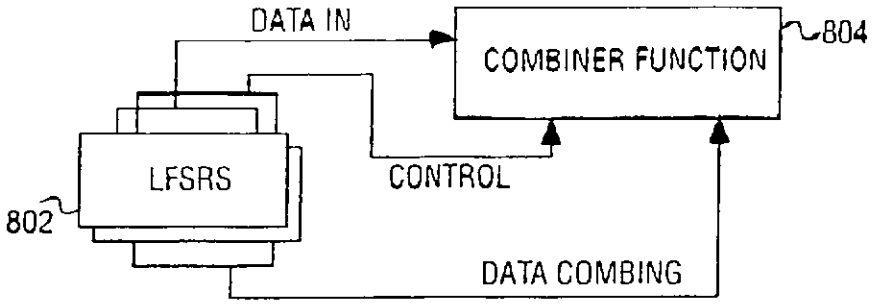


FIG. 8A

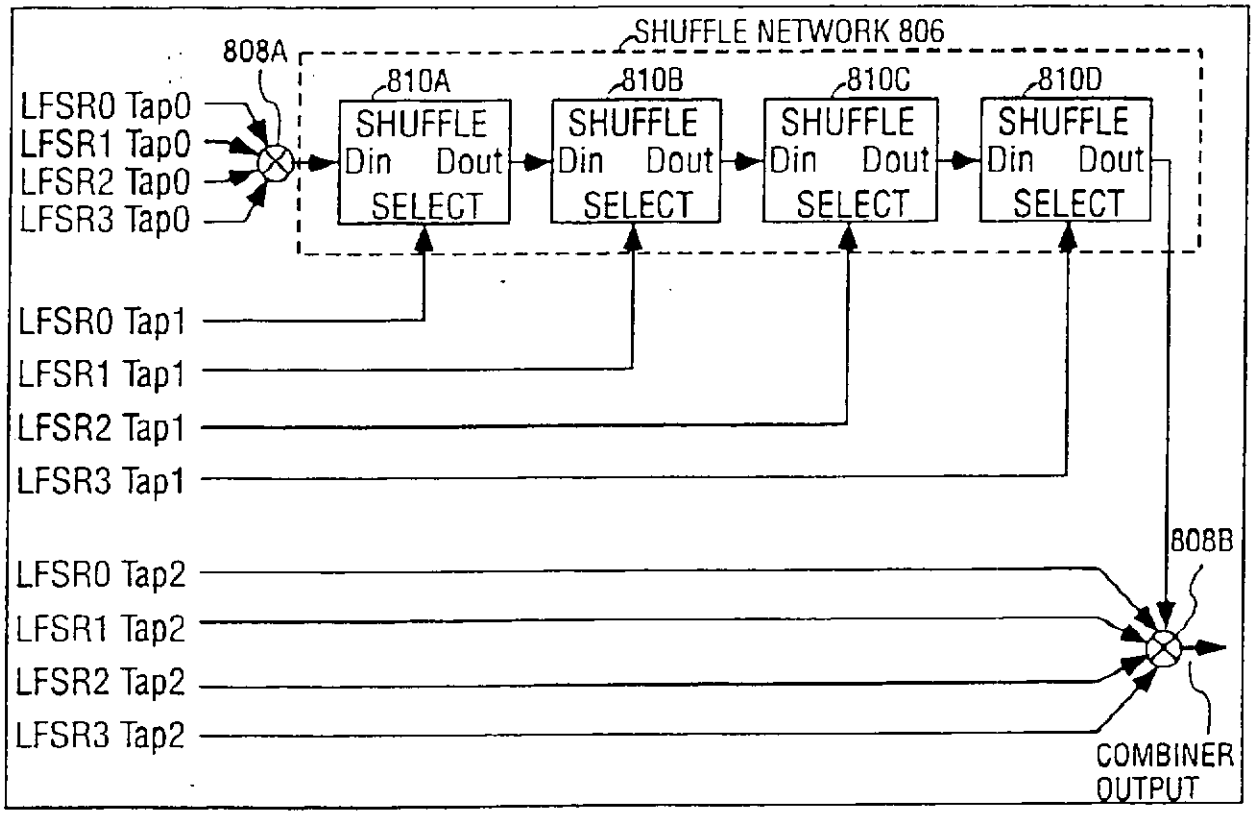


FIG. 8B

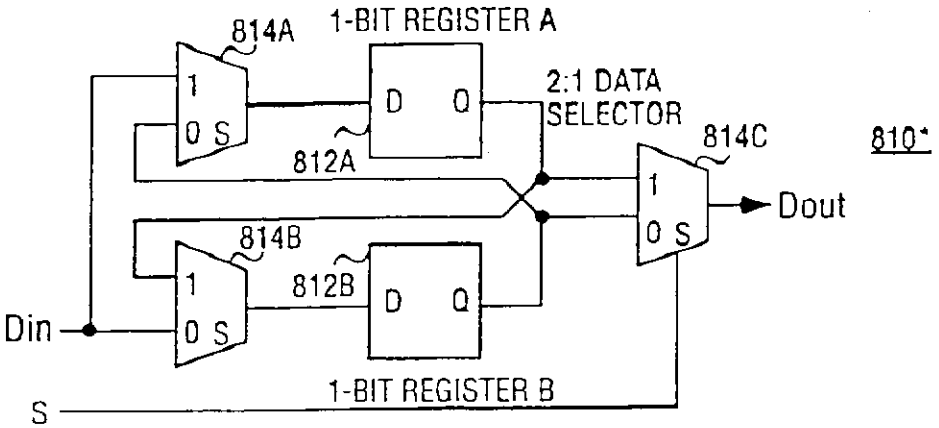


FIG. 8C