

Figure 1
Prior Art

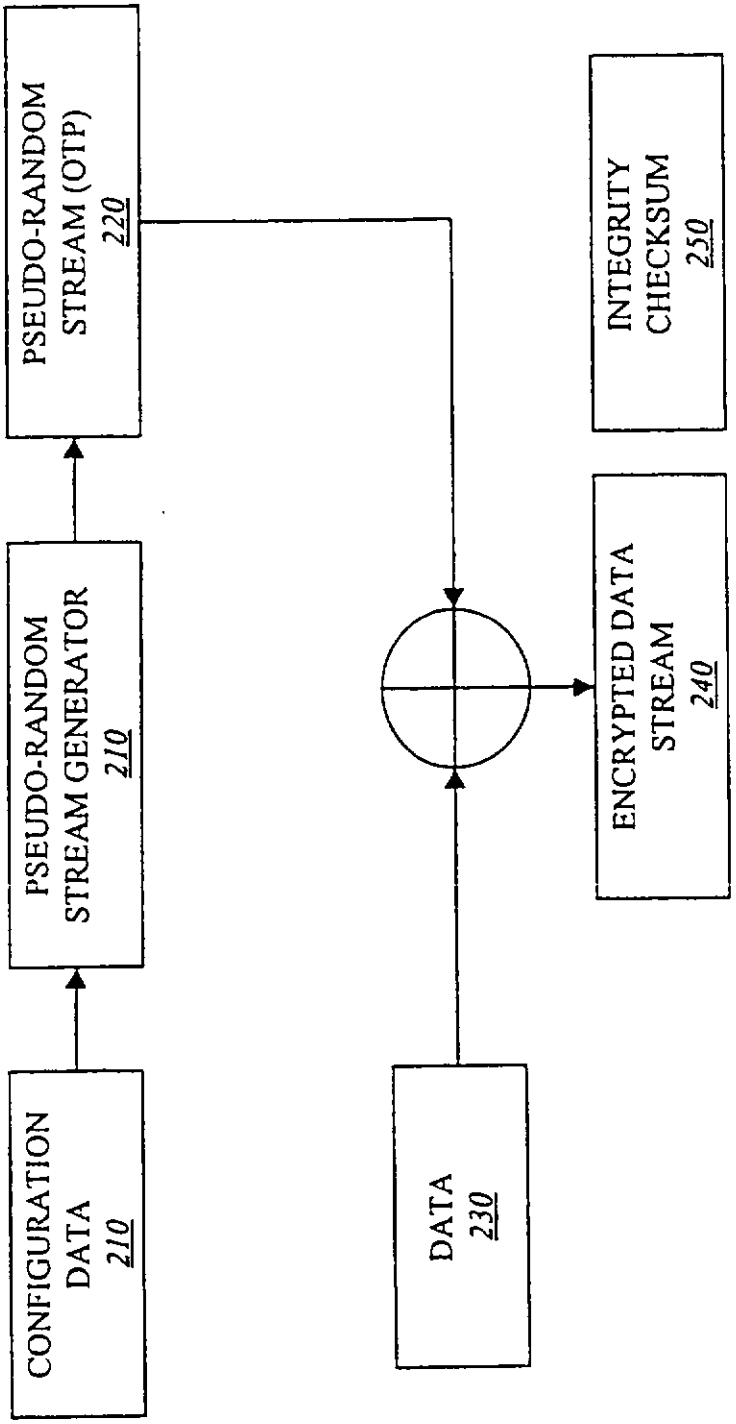


Figure 2
Prior Art

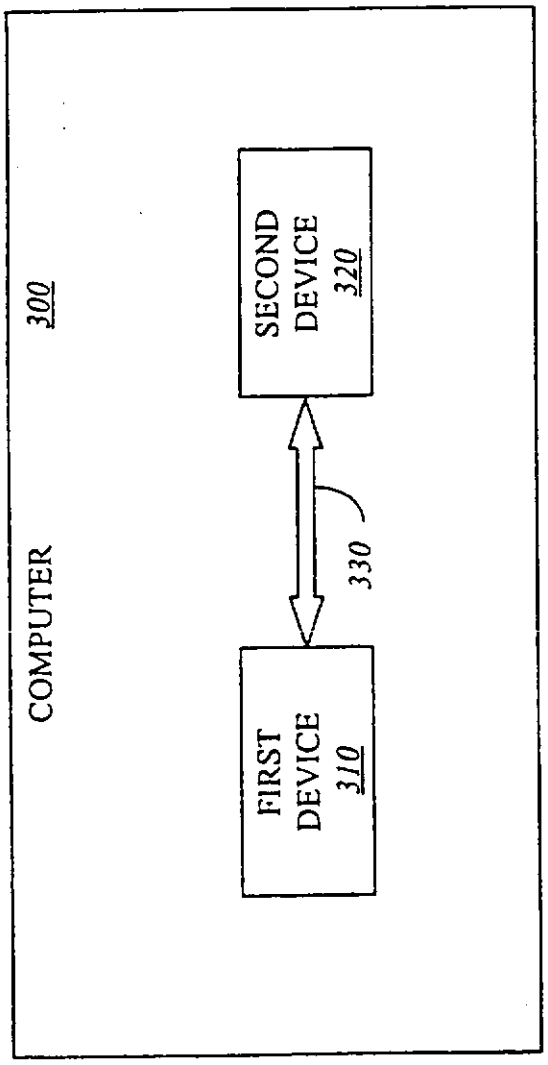


Figure 3

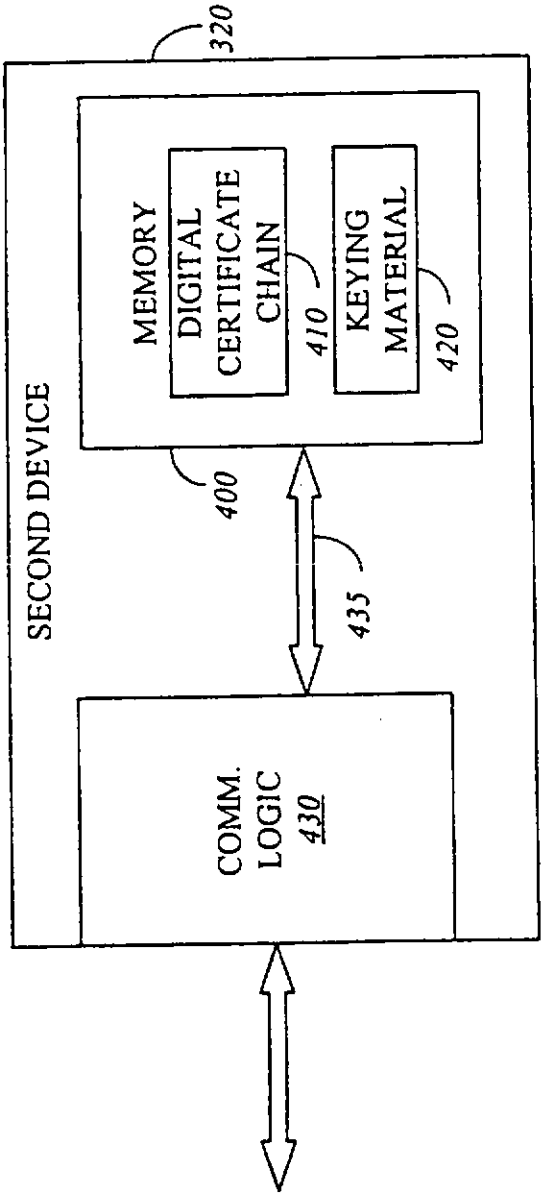


Figure 4A

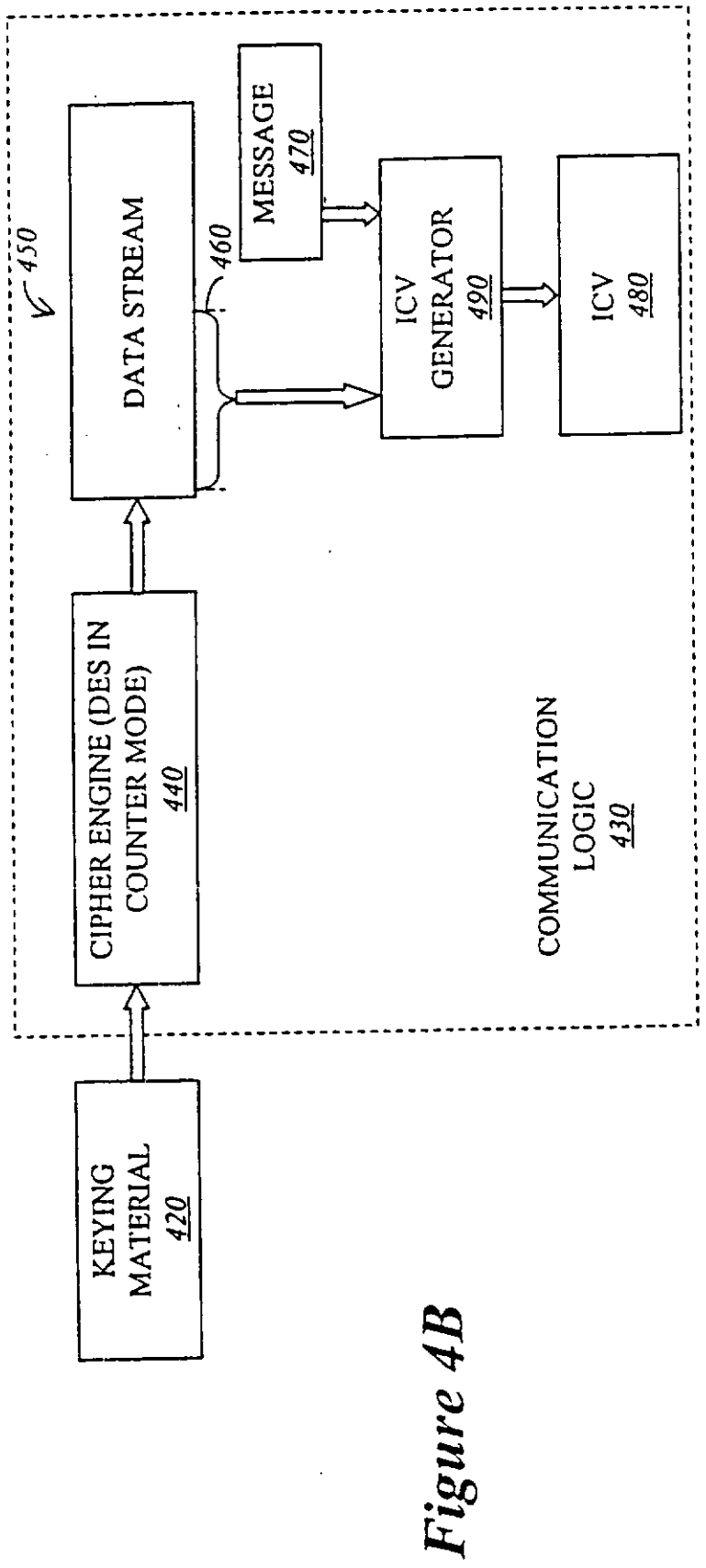


Figure 4B

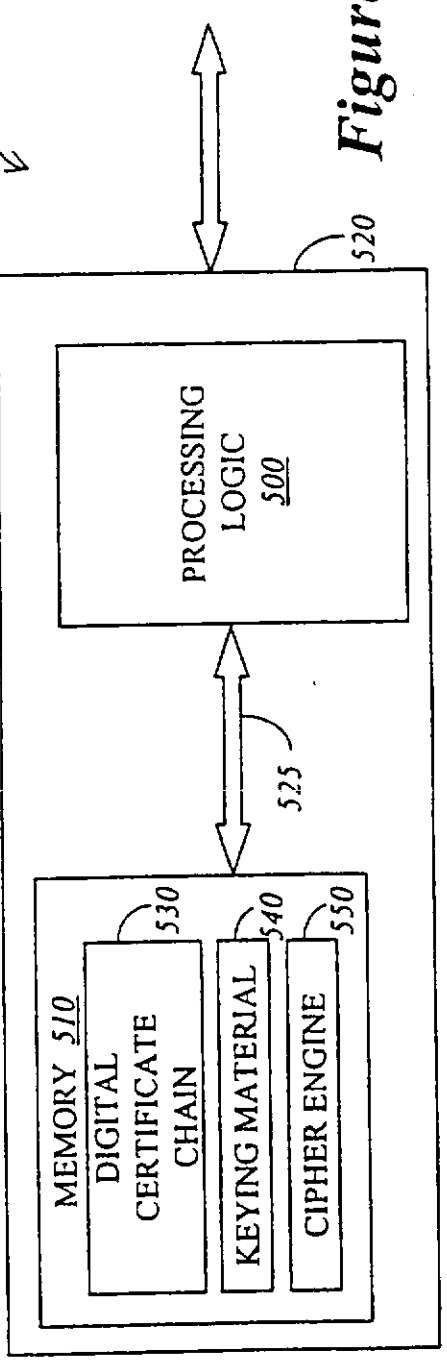


Figure 5

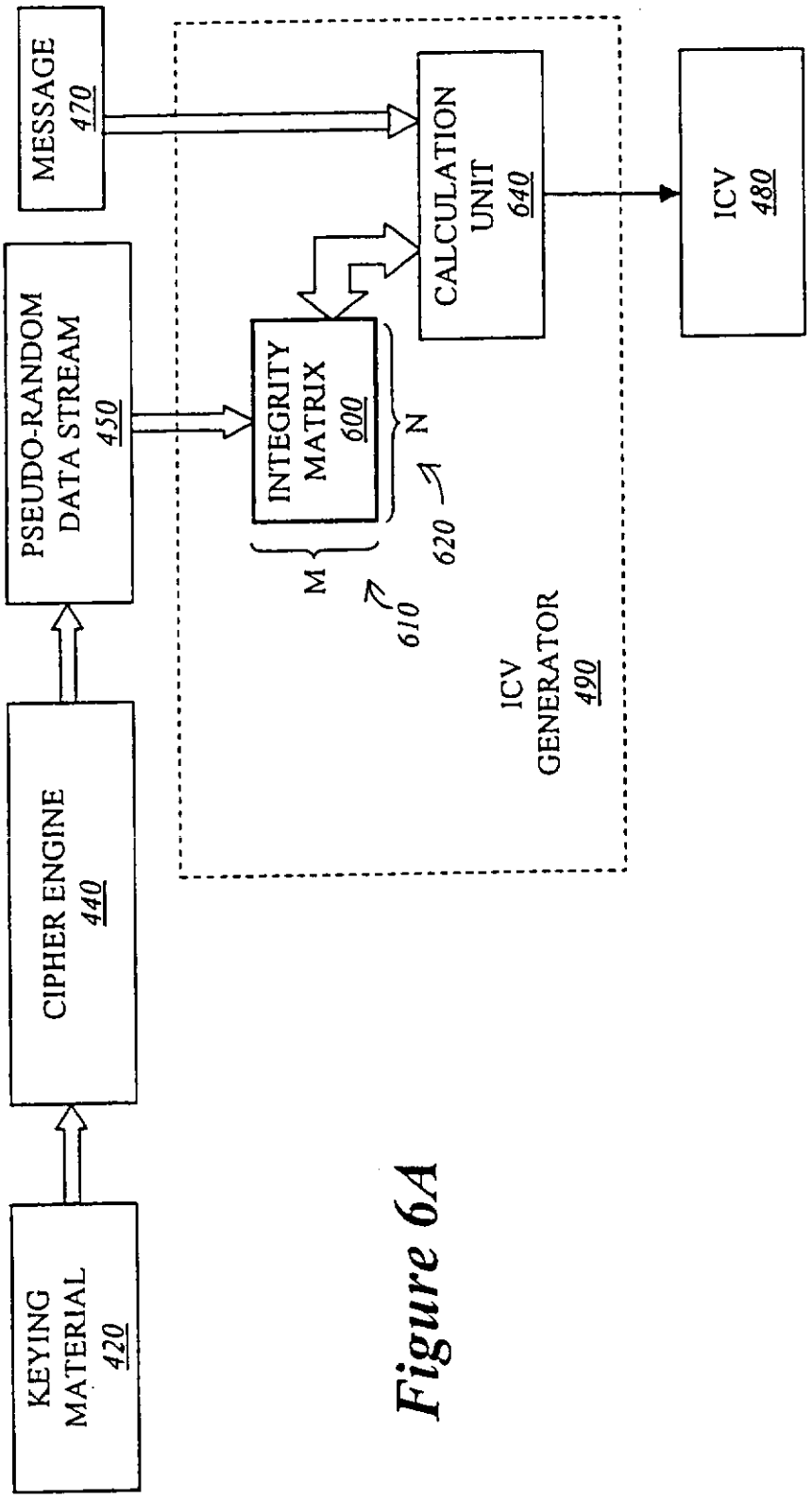

KEYING MATERIAL 420
CIPHER ENGINE 440
PSEUDO-RANDOM DATA STREAM 450
MESSAGE 470
ICV 480
ICV GENERATOR 490
INTEGRITY MATRIX 600
CALCULATION UNIT 640
M
N
610
620

Figure 6A

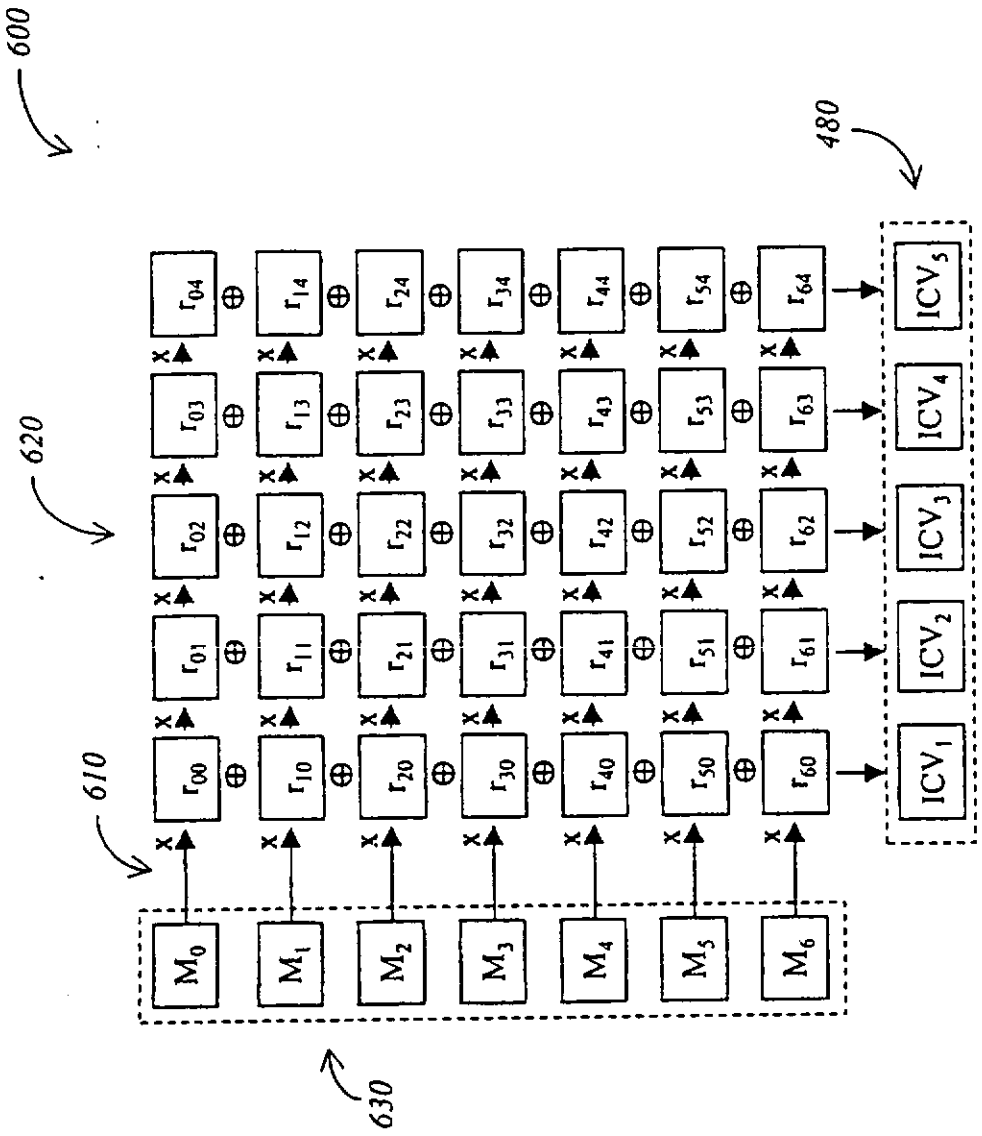

600
480
620
610
630
r_{04} r_{14} r_{24} r_{34} r_{44} r_{54} r_{64}
r_{03} r_{13} r_{23} r_{33} r_{43} r_{53} r_{63}
r_{02} r_{12} r_{22} r_{32} r_{42} r_{52} r_{62}
r_{01} r_{11} r_{21} r_{31} r_{41} r_{51} r_{61}
r_{00} r_{10} r_{20} r_{30} r_{40} r_{50} r_{60}
M_0 M_1 M_2 M_3 M_4 M_5 M_6
ICV_5 ICV_4 ICV_3 ICV_2 ICV_1

Figure 6B

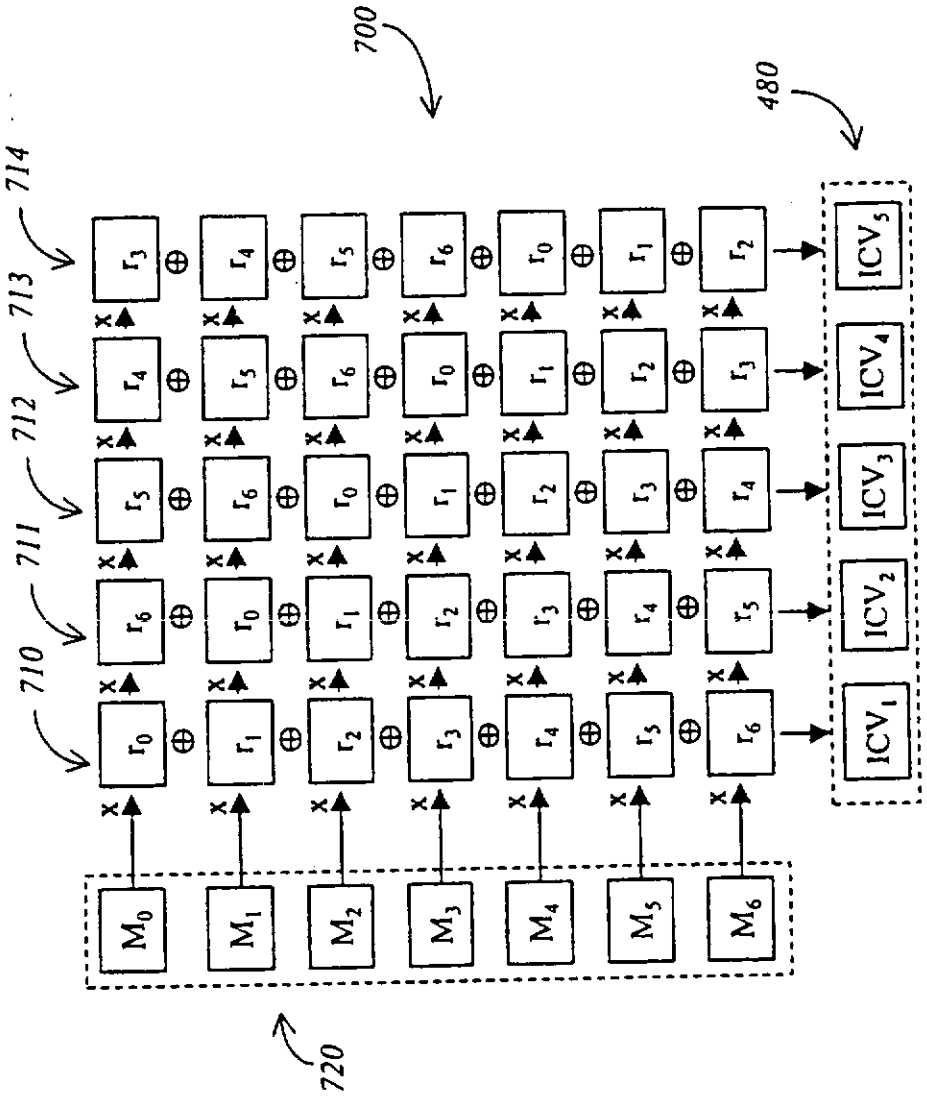

700
480
714
713
712
711
710
720
r_3 r_4 r_5 r_6 r_0 r_1 r_2 ICV_5
r_4 r_5 r_6 r_0 r_1 r_2 r_3 ICV_4
r_5 r_6 r_0 r_1 r_2 r_3 r_4 ICV_3
r_6 r_0 r_1 r_2 r_3 r_4 r_5 ICV_2
r_0 r_1 r_2 r_3 r_4 r_5 r_6 ICV_1
M_0 M_1 M_2 M_3 M_4 M_5 M_6

Figure 7

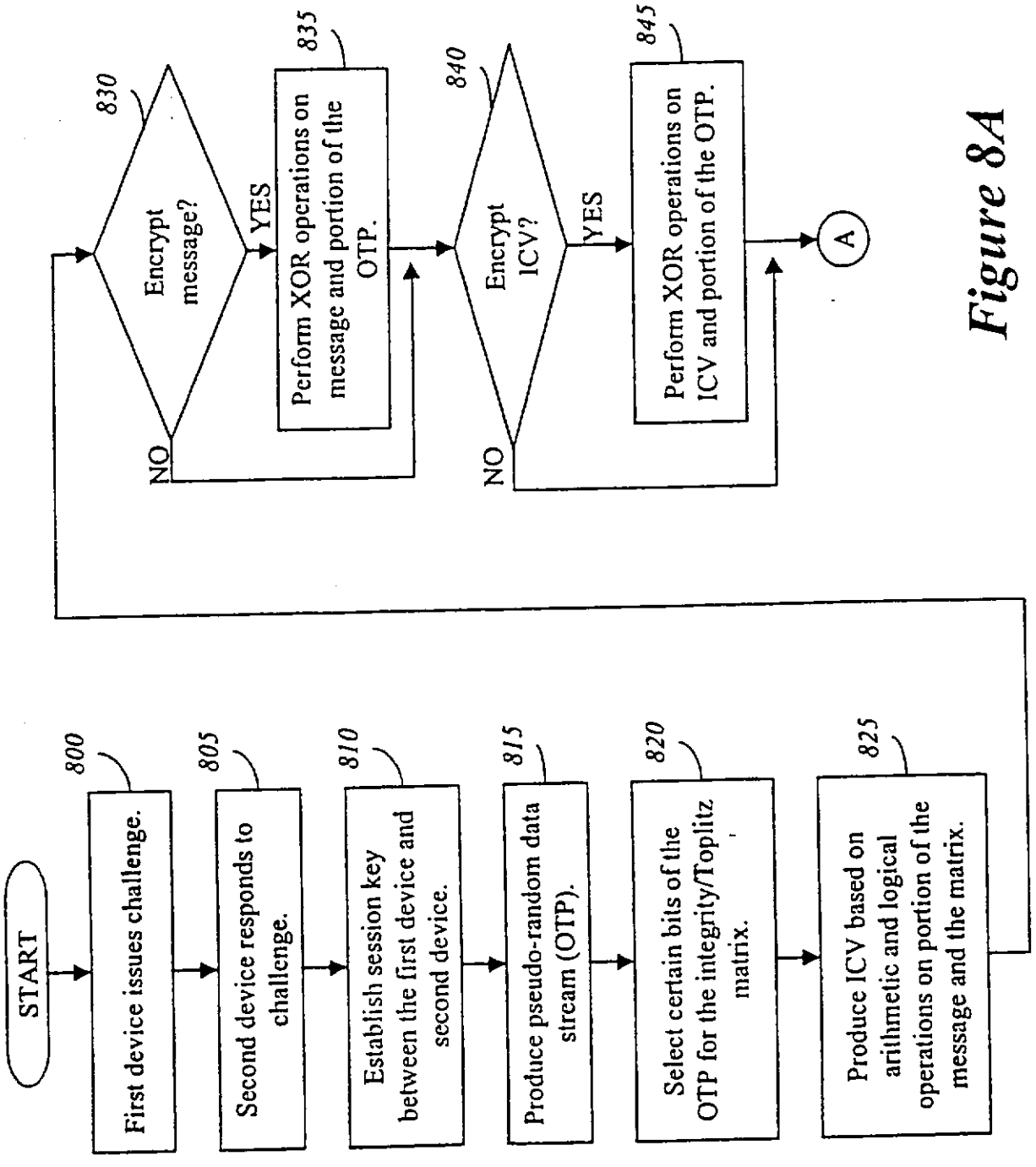
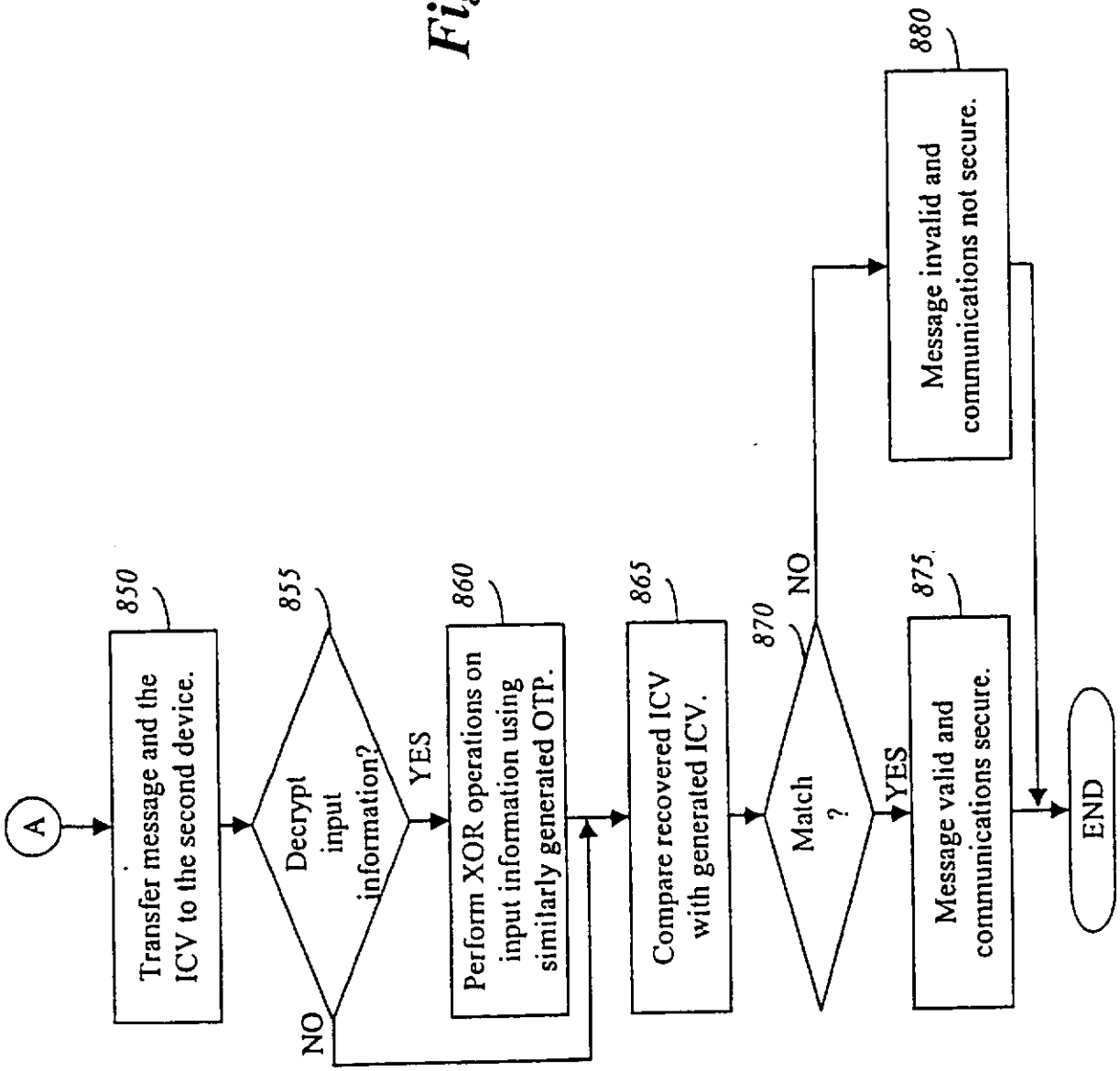

START
800
First device issues challenge.
805
Second device responds to challenge.
810
Establish session key between the first device and second device.
815
Produce pseudo-random data stream (OTP).
820
Select certain bits of the OTP for the integrity/Toplitz matrix.
825
Produce ICV based on arithmetic and logical operations on portion of the message and the matrix.
830
Encrypt message?
YES
NO
835
Perform XOR operations on message and portion of the OTP.
840
Encrypt ICV?
YES
NO
845
Perform XOR operations on ICV and portion of the OTP.
A

Figure 8A

Figure 8B


A
850
Transfer message and the ICV to the second device.
855
Decrypt input information?
YES
NO
860
Perform XOR operations on input information using similarly generated OTP.
865
Compare recovered ICV with generated ICV.
870
Match ?
NO
YES
875
Message valid and communications secure.
880
Message invalid and communications not secure.
END