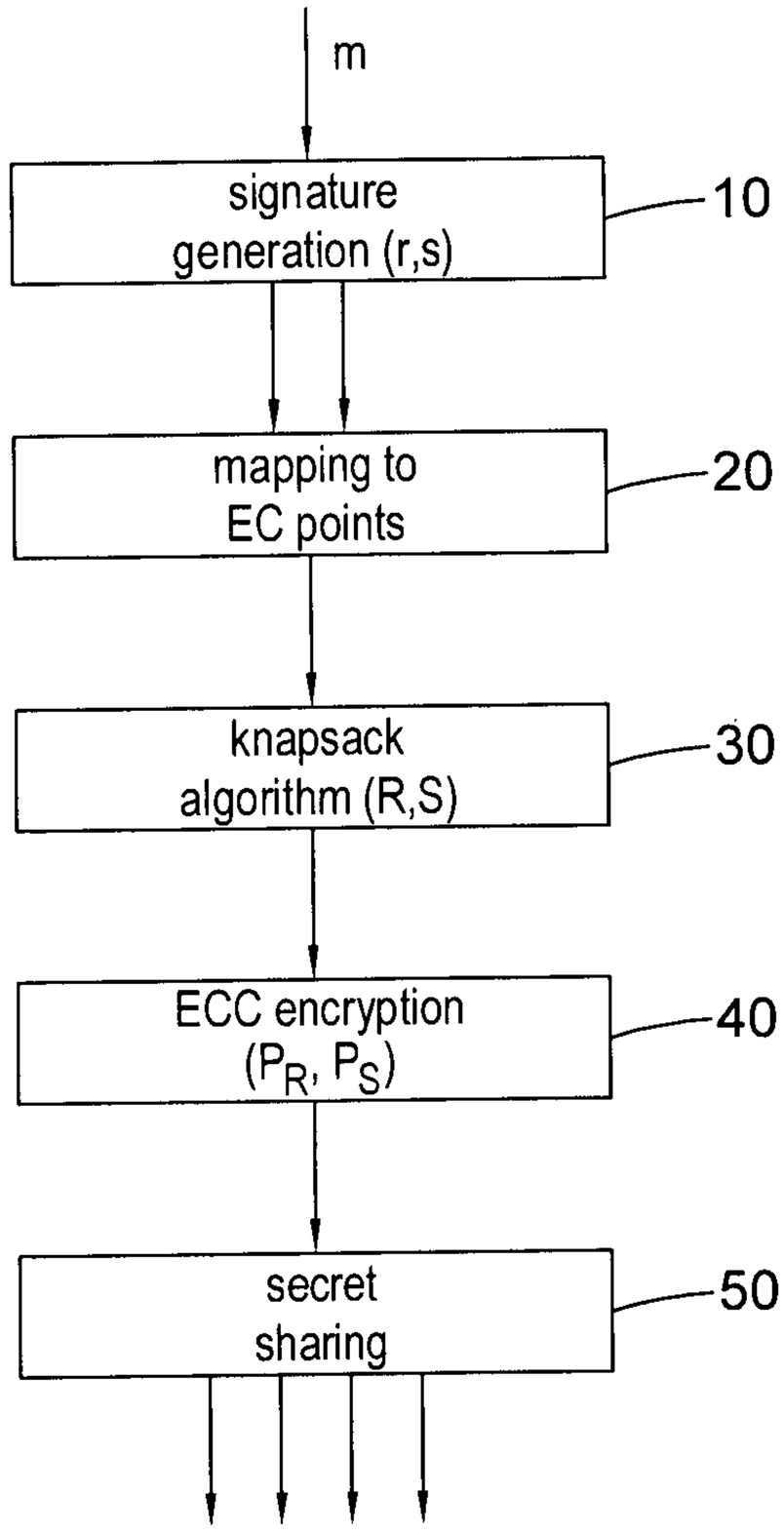

m
signature generation (r,s)
10
mapping to EC points
20
knapsack algorithm (R,S)
30
ECC encryption ($P_R$, $P_S$)
40
secret sharing
50

Fig. 1

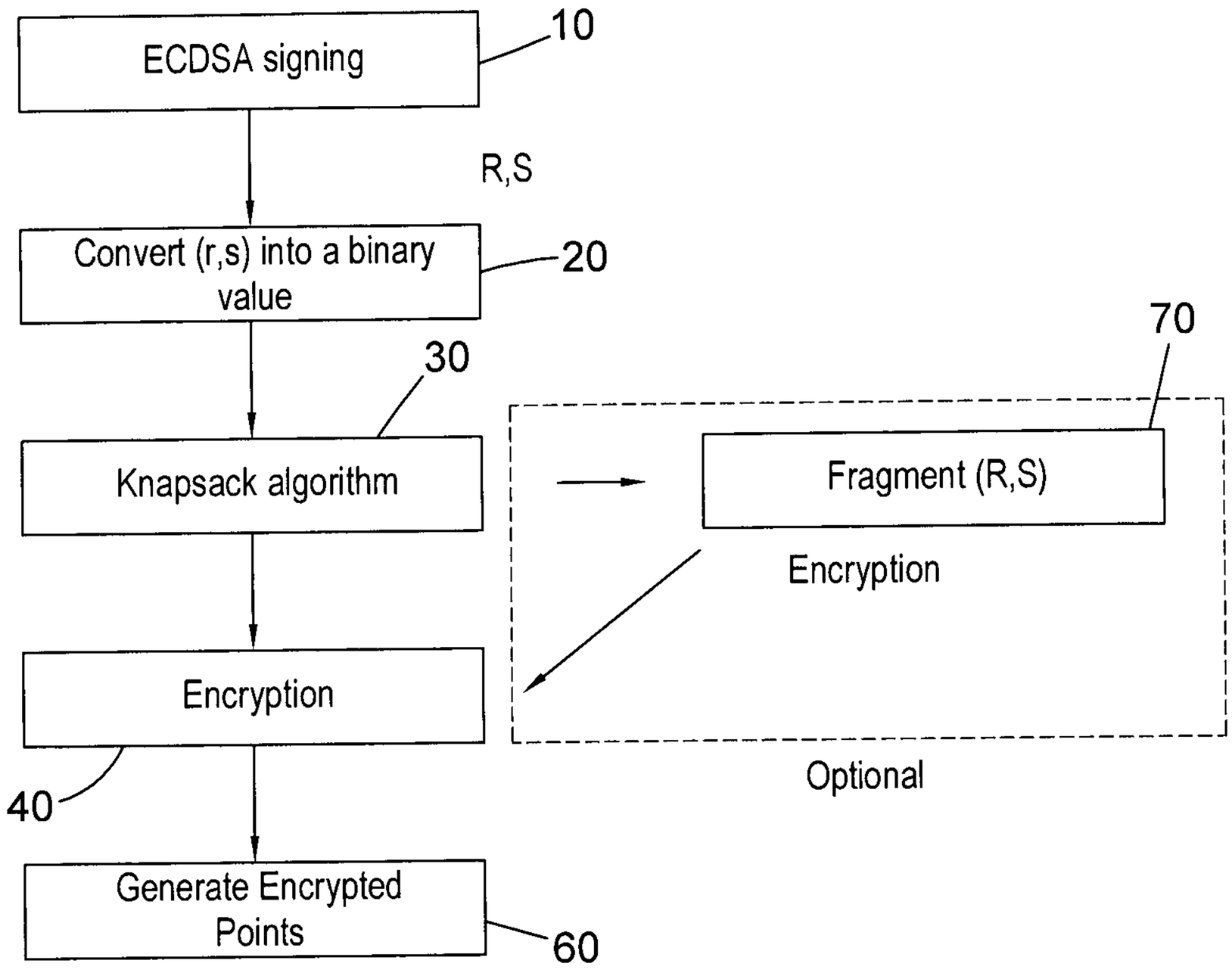

ECDSA signing
10
R,S
Convert (r,s) into a binary value
20
30
Knapsack algorithm
70
Fragment (R,S)
Encryption
Encryption
Optional
40
Generate Encrypted Points
60

Fig. 2

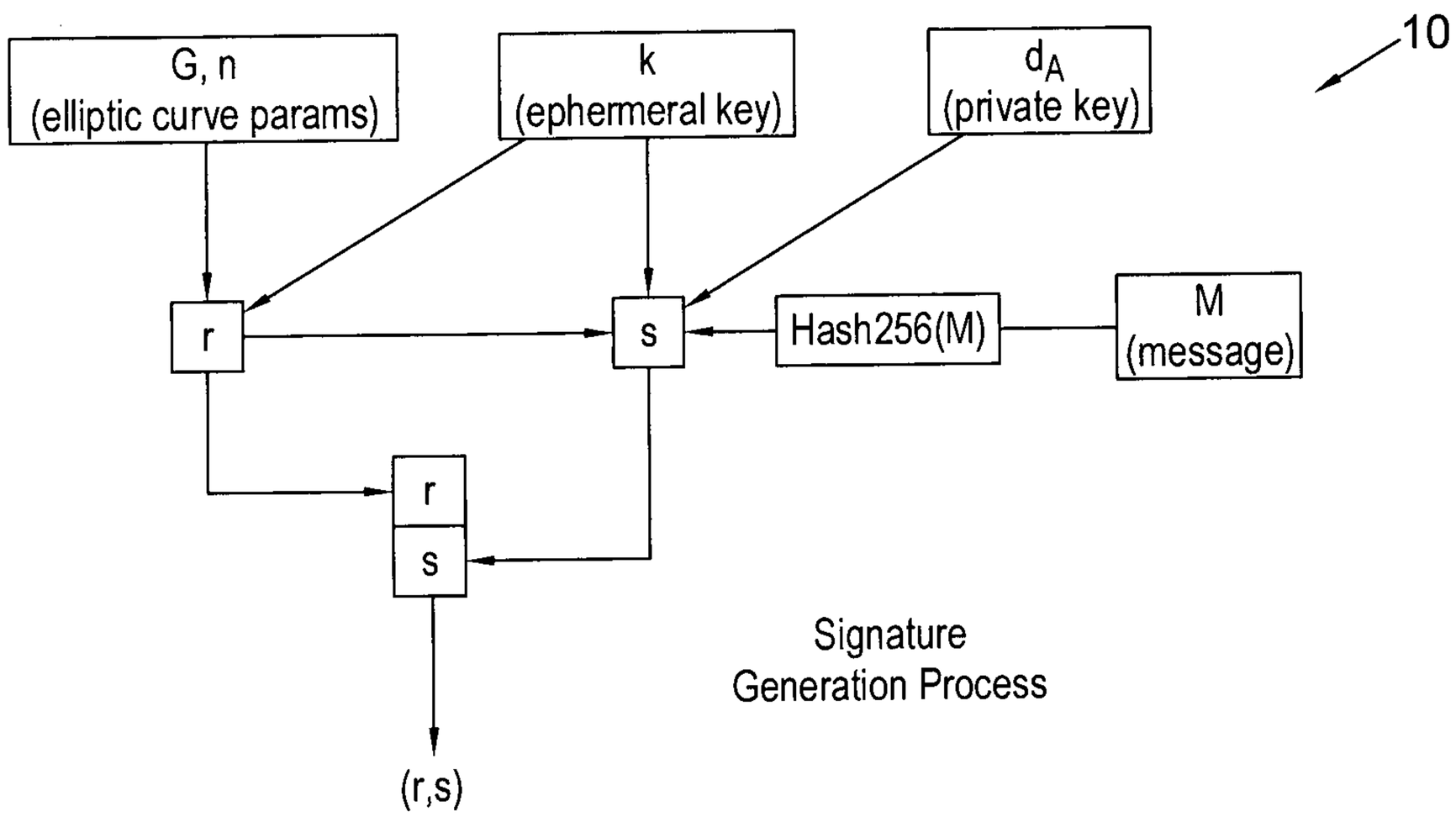

G, n
(elliptic curve params)
k
(ephermeral key)
$d_A$
(private key)
10
r
s
Hash256(M)
M
(message)
r
s
(r,s)
Signature
Generation Process

Fig. 3

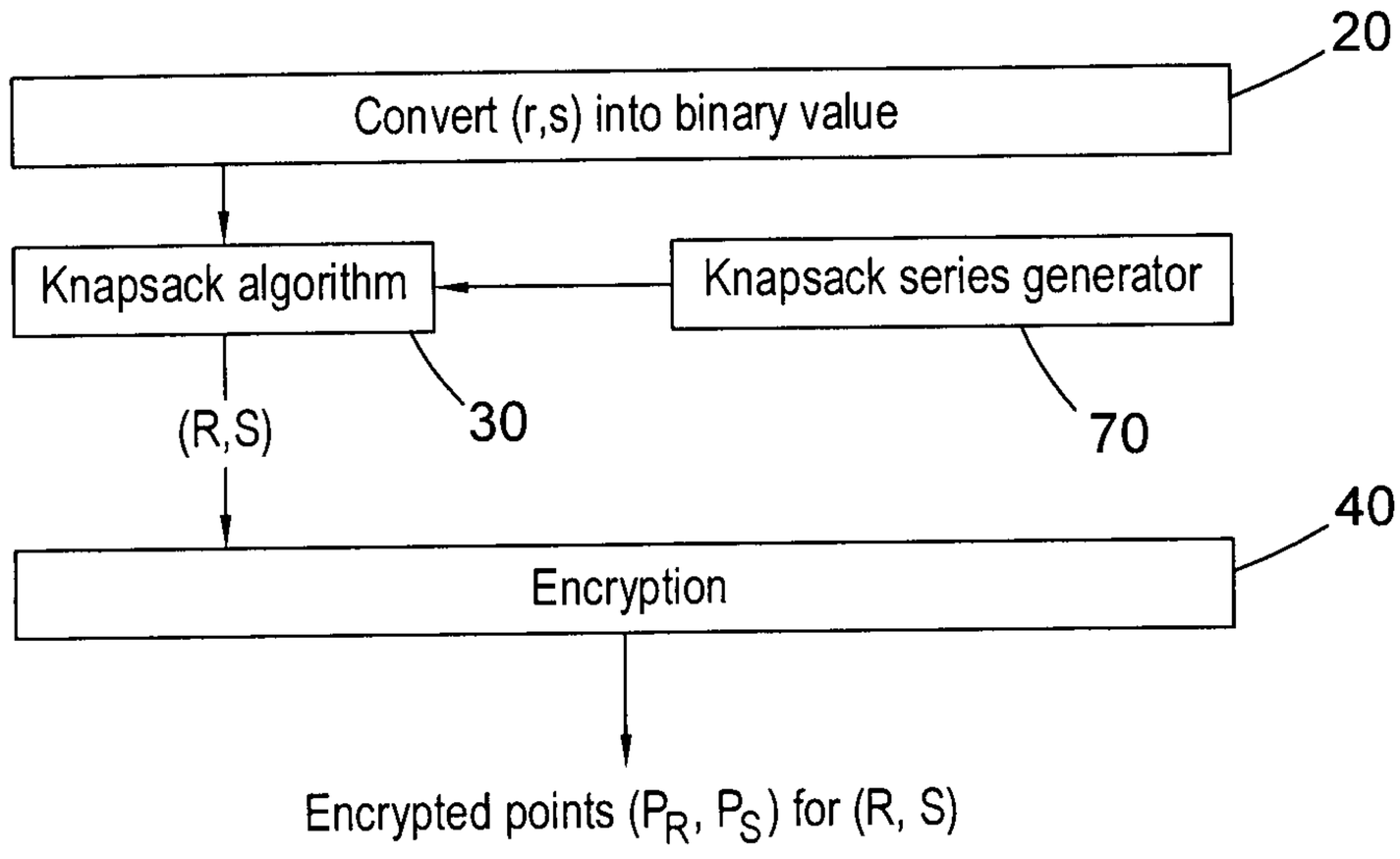

20
Convert (r,s) into binary value
Knapsack algorithm
Knapsack series generator
(R,S)
30
70
40
Encryption
Encrypted points ($P_R$, $P_S$) for (R, S)

Fig. 4

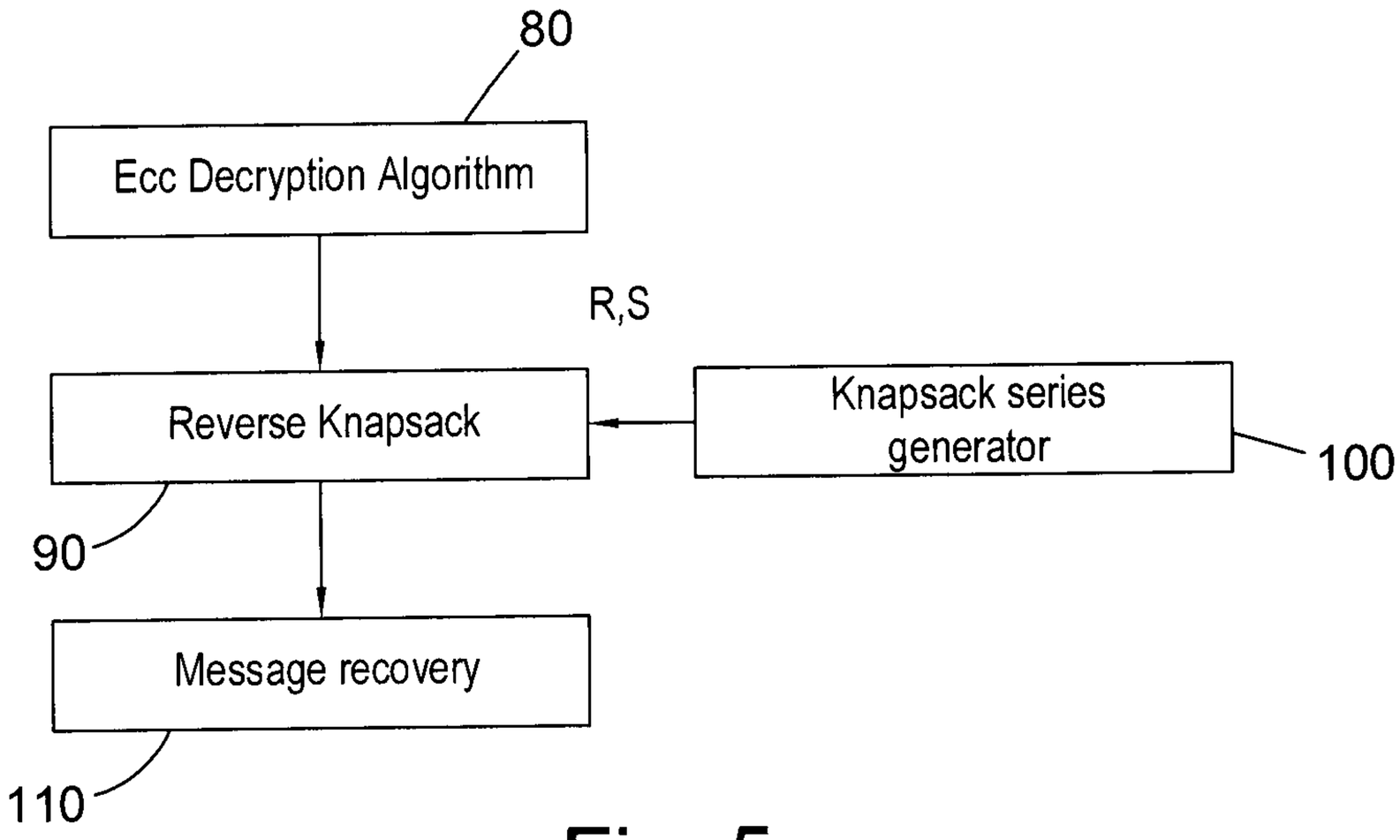

80
Ecc Decryption Algorithm
R,S
Reverse Knapsack
Knapsack series generator
100
90
Message recovery
110

Fig. 5

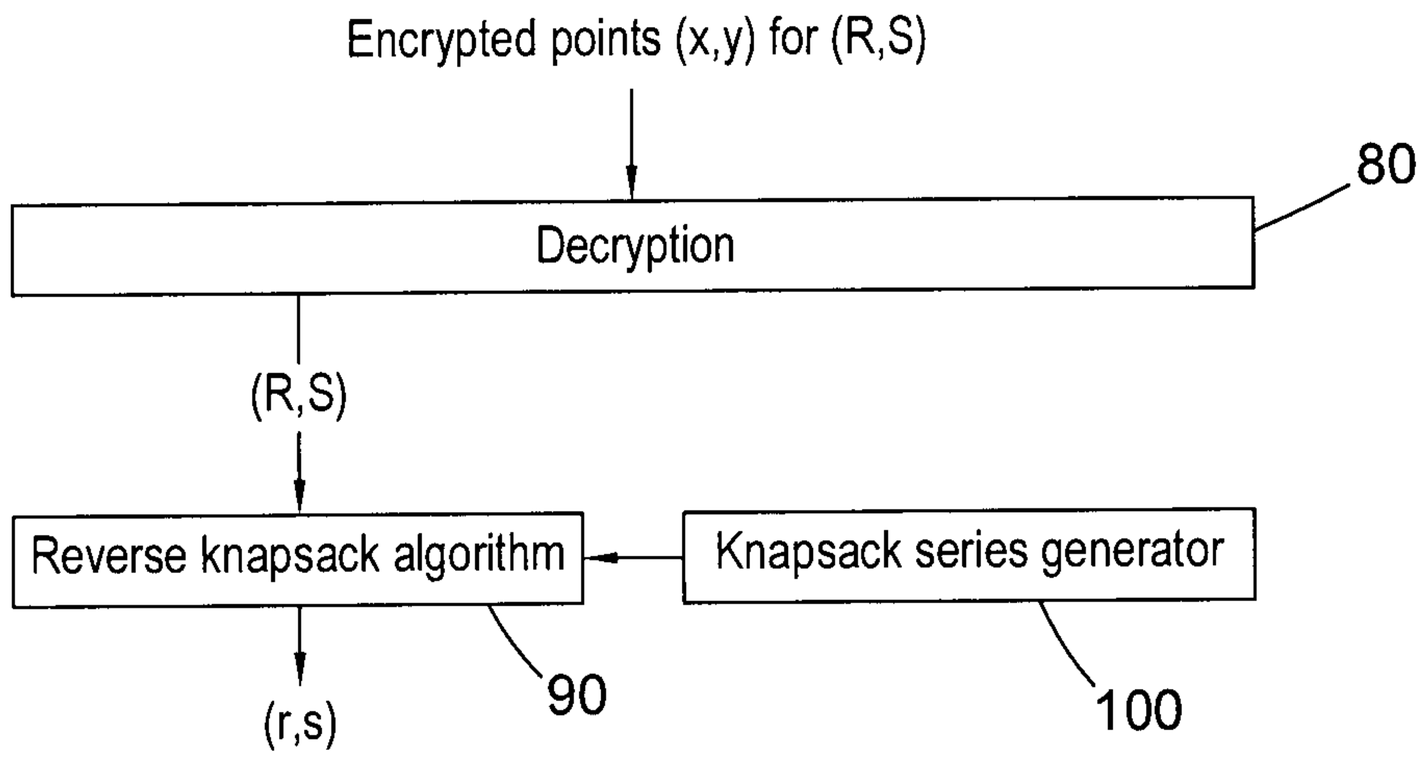

Encrypted points (x,y) for (R,S)
Decryption
80
(R,S)
Reverse knapsack algorithm
Knapsack series generator
(r,s)
90
100

Fig. 6

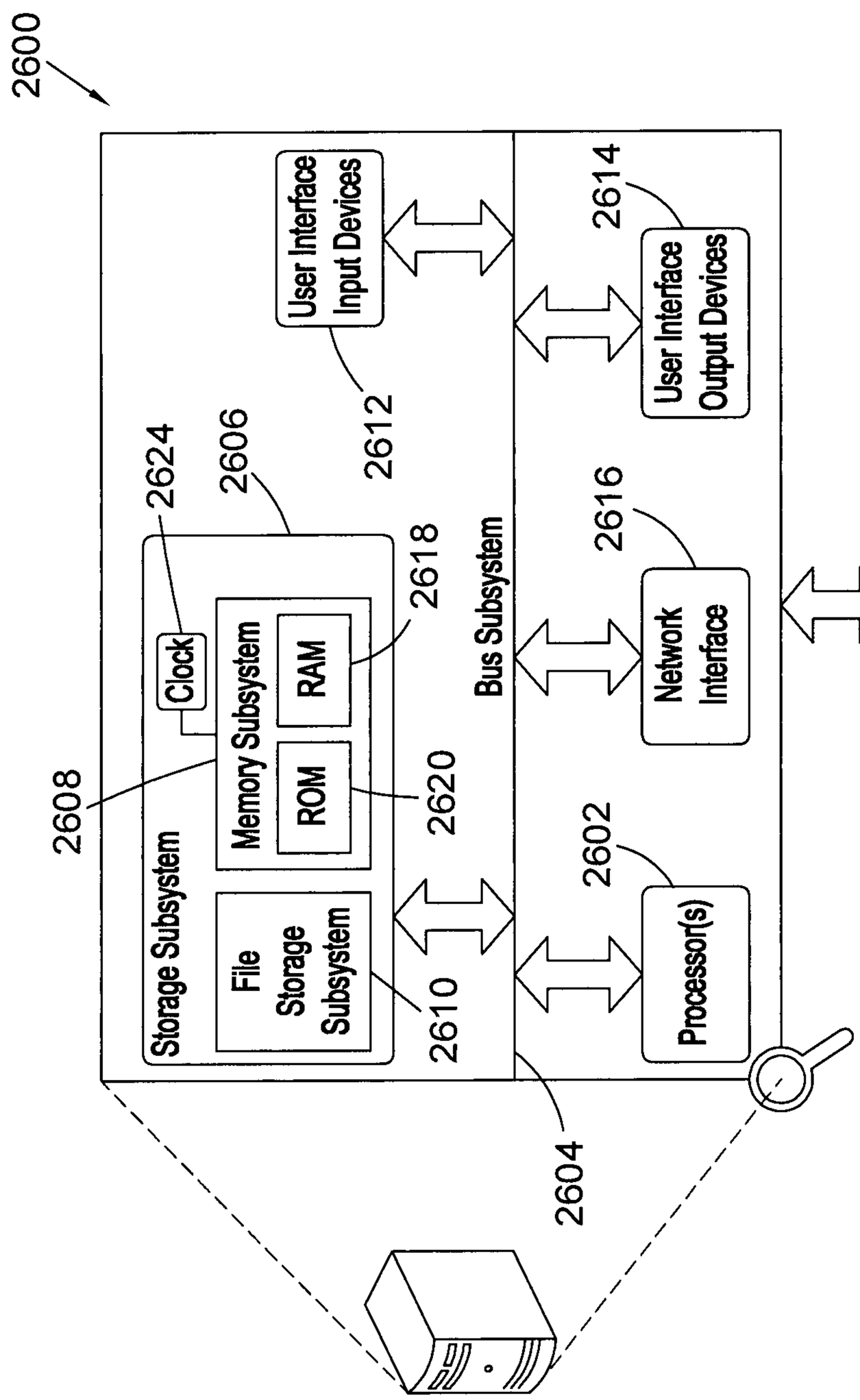

2600
2624
2606
2612
2618
2614
2616
2608
2620
2602
2610
2604
Clock
Memory Subsystem
RAM
ROM
User Interface Input Devices
User Interface Output Devices
Network Interface
Bus Subsystem
Storage Subsystem
File Storage Subsystem
Processor(s)

Fig. 7