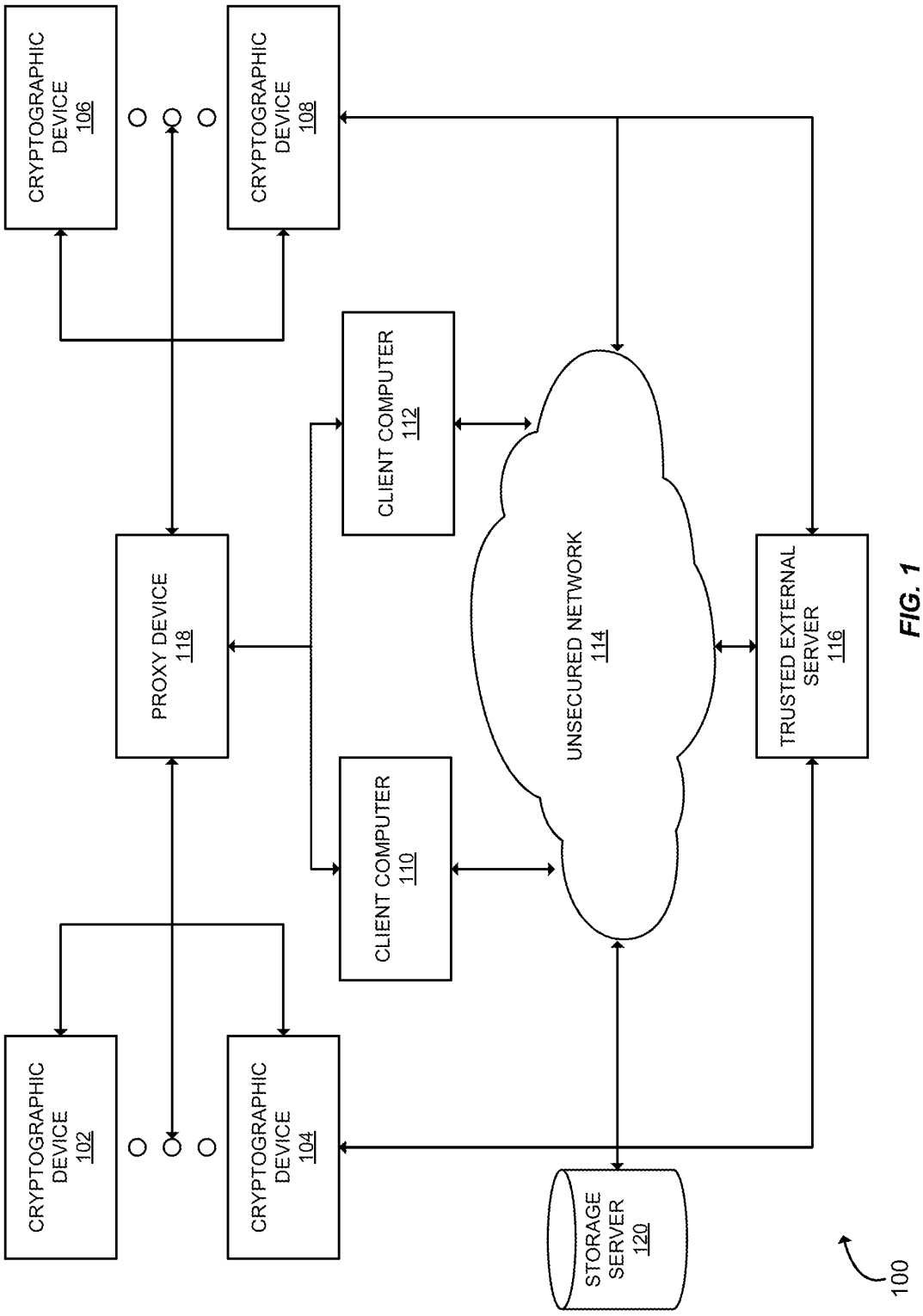

CRYPTOGRAPHIC DEVICE 106
CRYPTOGRAPHIC DEVICE 108
CLIENT COMPUTER 112
PROXY DEVICE 118
UNSECURED NETWORK 114
TRUSTED EXTERNAL SERVER 116
CLIENT COMPUTER 110
CRYPTOGRAPHIC DEVICE 102
CRYPTOGRAPHIC DEVICE 104
STORAGE SERVER 120
100

FIG. 1

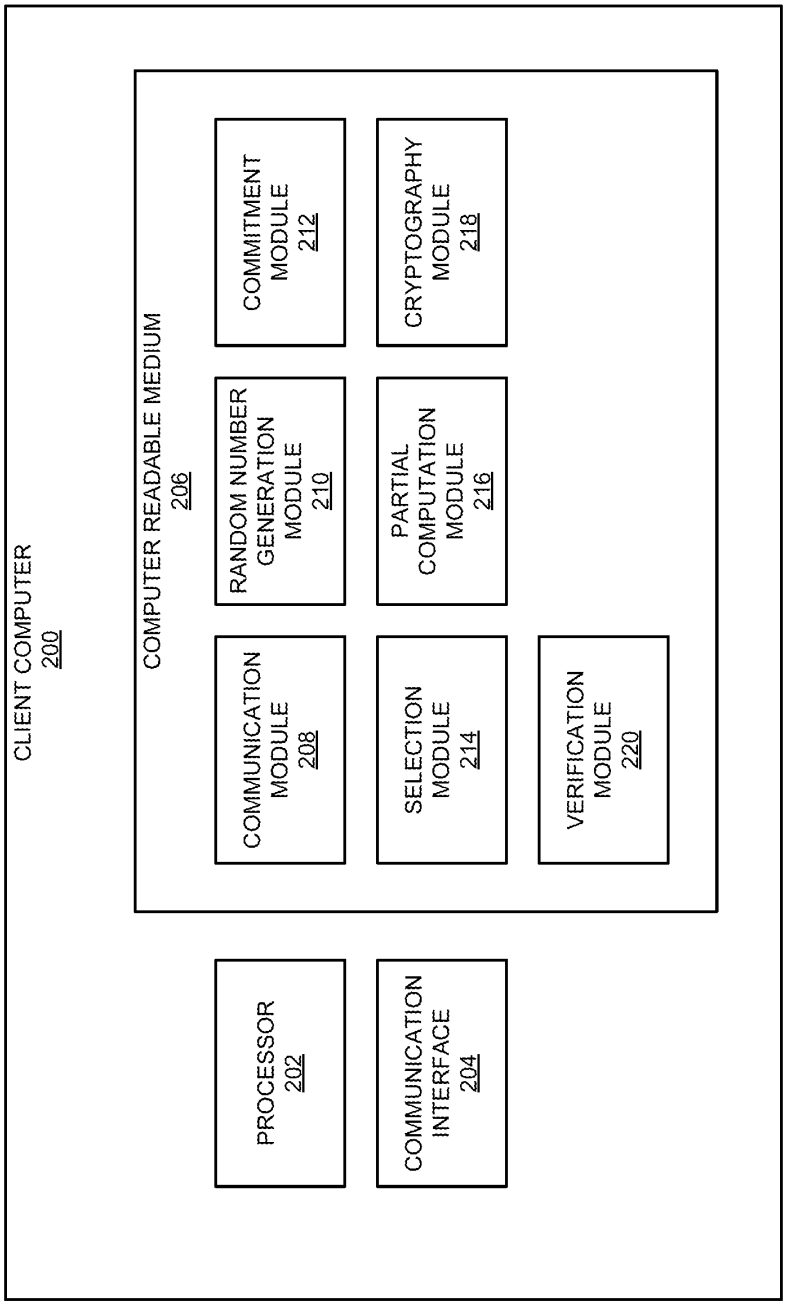

CLIENT COMPUTER
200
COMPUTER READABLE MEDIUM
206
COMMUNICATION MODULE
208
RANDOM NUMBER GENERATION MODULE
210
COMMITMENT MODULE
212
SELECTION MODULE
214
PARTIAL COMPUTATION MODULE
216
CRYPTOGRAPHY MODULE
218
VERIFICATION MODULE
220
PROCESSOR
202
COMMUNICATION INTERFACE
204

FIG. 2

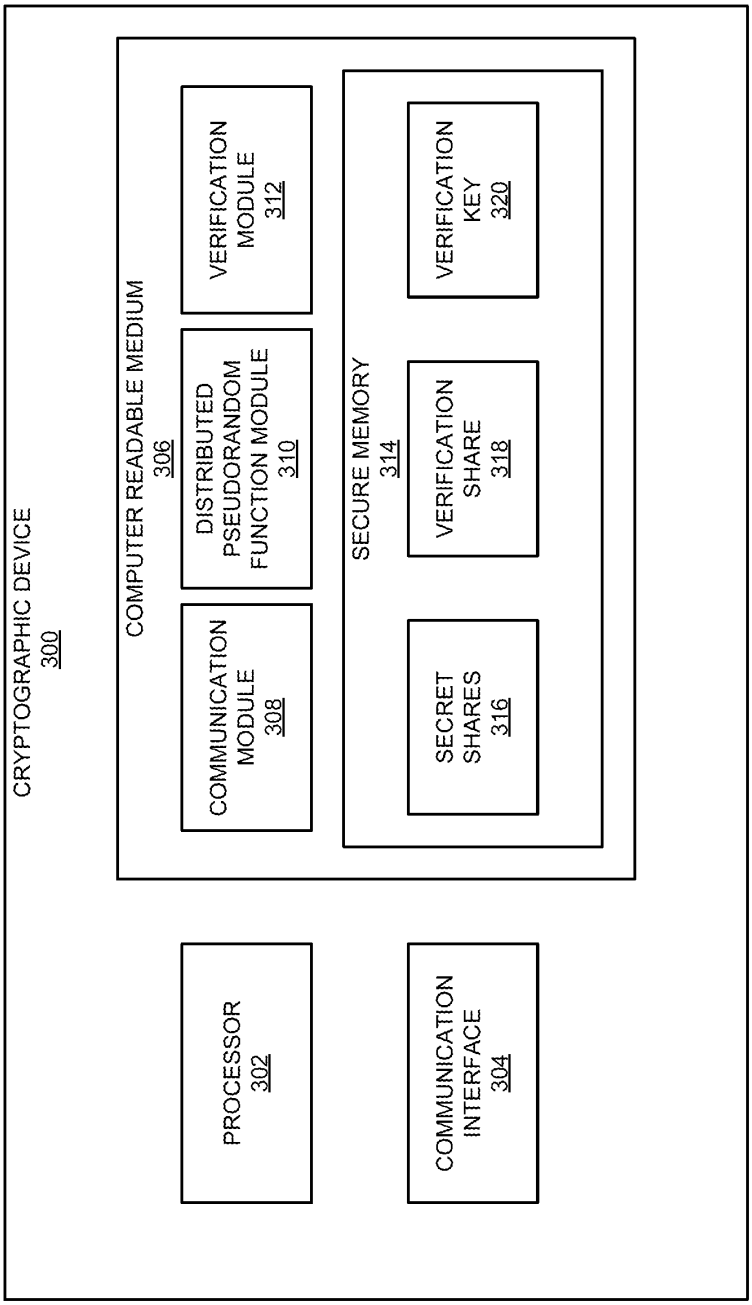

CRYPTOGRAPHIC DEVICE
300
PROCESSOR
302
COMMUNICATION
INTERFACE
304
COMPUTER READABLE MEDIUM
306
COMMUNICATION
MODULE
308
DISTRIBUTED
PSEUDORANDOM
FUNCTION MODULE
310
VERIFICATION
MODULE
312
SECURE MEMORY
314
SECRET
SHARES
316
VERIFICATION
SHARE
318
VERIFICATION
KEY
320

FIG. 3

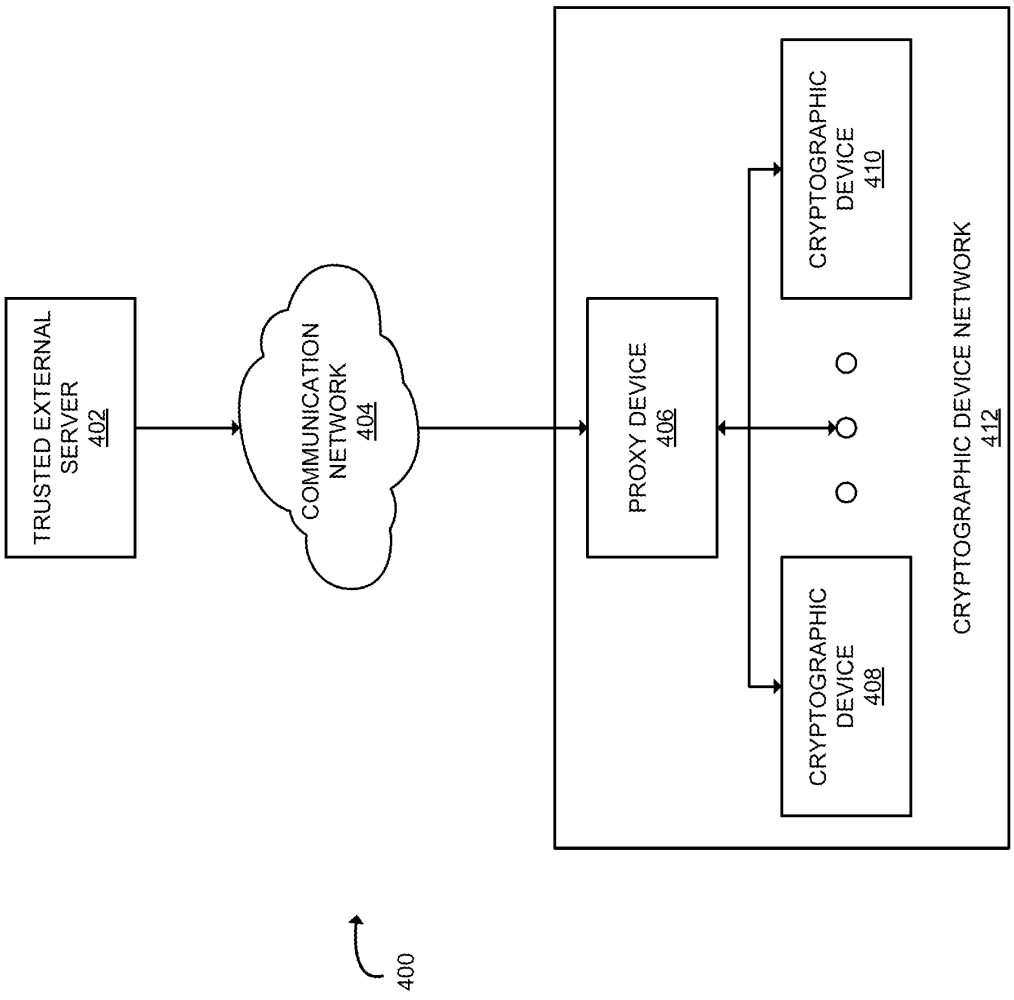

TRUSTED EXTERNAL SERVER 402
COMMUNICATION NETWORK 404
PROXY DEVICE 406
CRYPTOGRAPHIC DEVICE 410
CRYPTOGRAPHIC DEVICE 408
CRYPTOGRAPHIC DEVICE NETWORK 412
400

FIG. 4

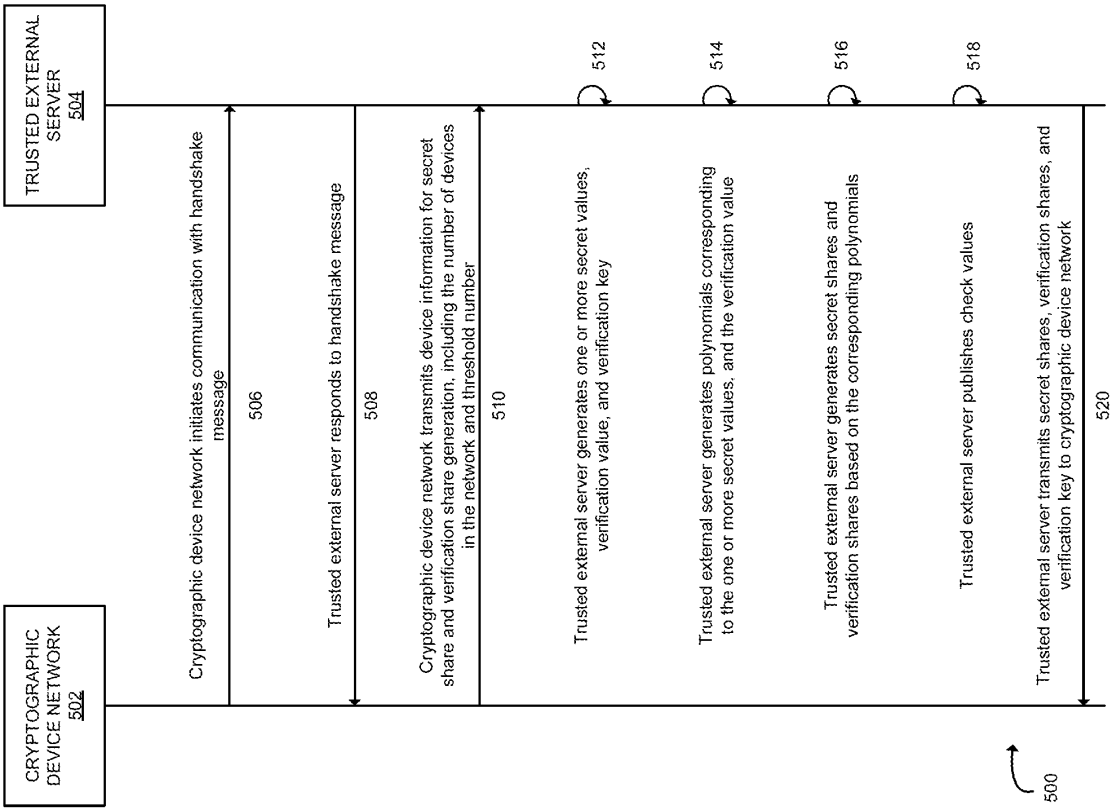

CRYPTOGRAPHIC DEVICE NETWORK 502
TRUSTED EXTERNAL SERVER 504
Cryptographic device network initiates communication with handshake message
506
Trusted external server responds to handshake message
508
Cryptographic device network transmits device information for secret share and verification share generation, including the number of devices in the network and threshold number
510
Trusted external server generates one or more secret values, verification value, and verification key
512
Trusted external server generates polynomials corresponding to the one or more secret values, and the verification value
514
Trusted external server generates secret shares and verification shares based on the corresponding polynomials
516
Trusted external server publishes check values
518
Trusted external server transmits secret shares, verification shares, and verification key to cryptographic device network
520
500

FIG. 5

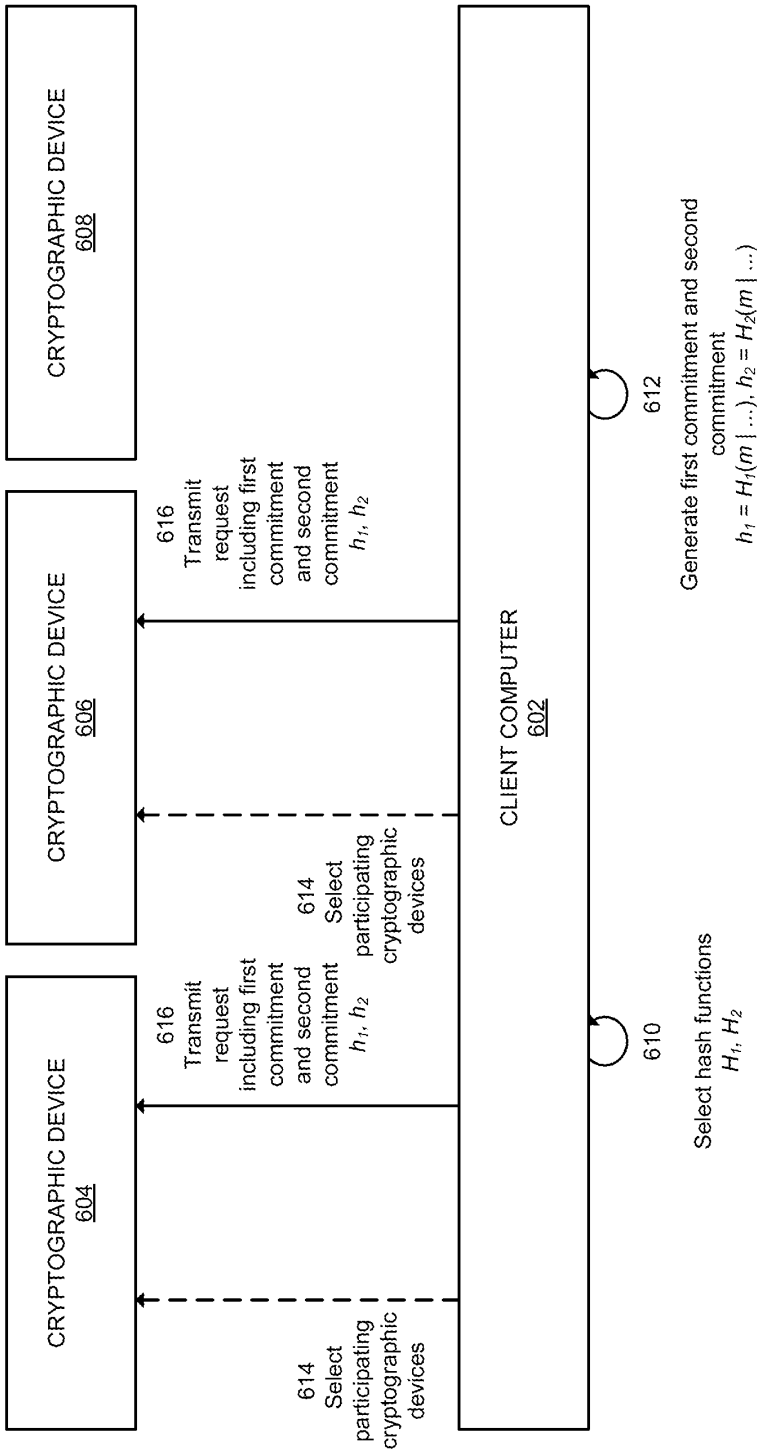

CRYPTOGRAPHIC DEVICE
604
CRYPTOGRAPHIC DEVICE
606
CRYPTOGRAPHIC DEVICE
608
CLIENT COMPUTER
602
610
Select hash functions
H_1, H_2
612
Generate first commitment and second commitment
$h_1 = H_1(m \mid \ldots), h_2 = H_2(m \mid \ldots)$
614
Select participating cryptographic devices
616
Transmit request including first commitment and second commitment
h_1, h_2
614
Select participating cryptographic devices
616
Transmit request including first commitment and second commitment
h_1, h_2

FIG. 6A

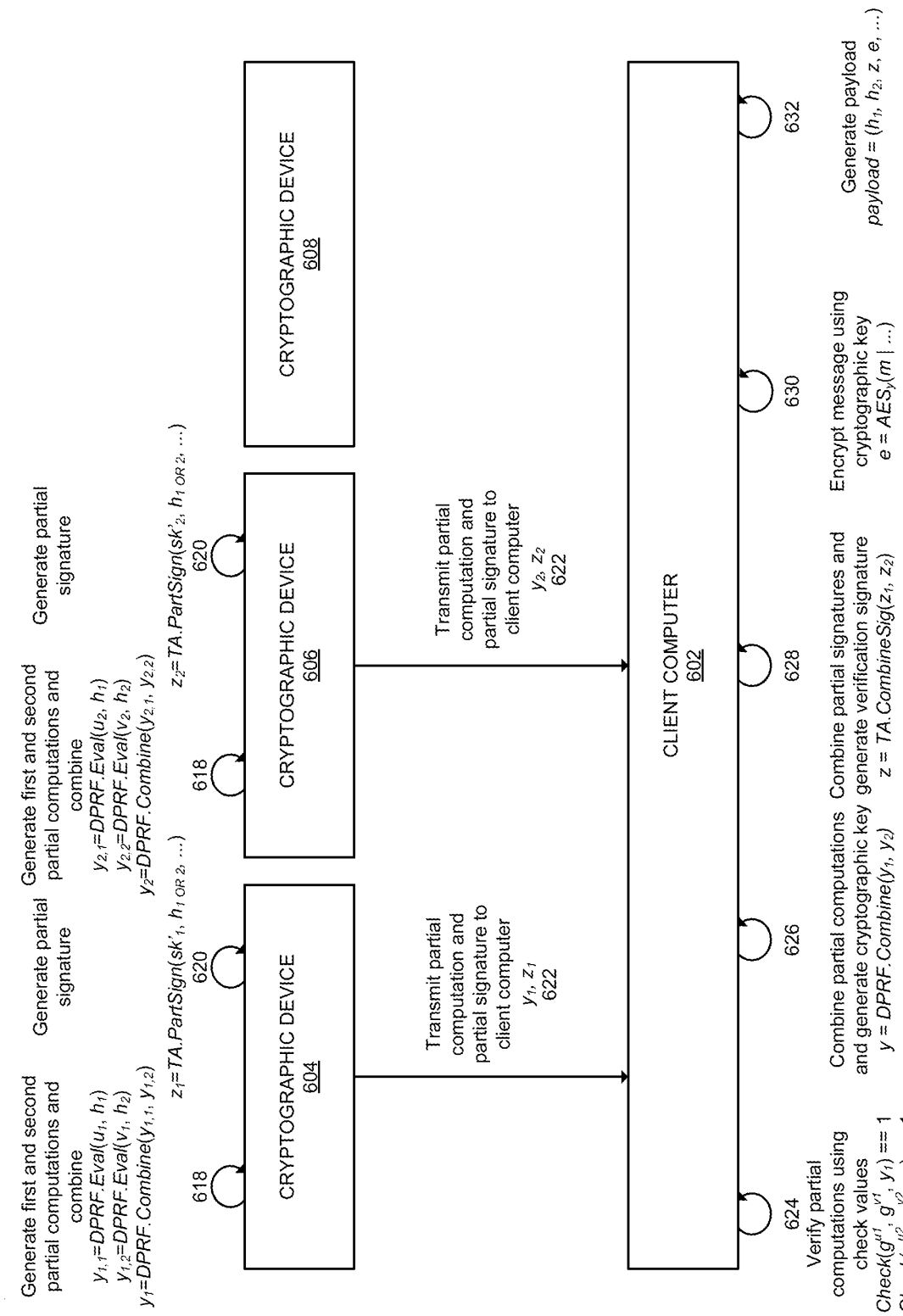

CRYPTOGRAPHIC DEVICE
604
CRYPTOGRAPHIC DEVICE
606
CRYPTOGRAPHIC DEVICE
608
CLIENT COMPUTER
602
Generate first and second partial computations and combine
$y_{1,1}$=DPRF.Eval(u_1, h_1)
$y_{1,2}$=DPRF.Eval(v_1, h_2)
y_1=DPRF.Combine($y_{1,1}$, $y_{1,2}$)
618
Generate partial signature
z_1=TA.PartSign(sk'_1, $h_{1\ OR\ 2}$, ...)
620
Generate first and second partial computations and combine
$y_{2,1}$=DPRF.Eval(u_2, h_1)
$y_{2,2}$=DPRF.Eval(v_2, h_2)
y_2=DPRF.Combine($y_{2,1}$, $y_{2,2}$)
618
Generate partial signature
z_2=TA.PartSign(sk'_2, $h_{1\ OR\ 2}$, ...)
620
Transmit partial computation and partial signature to client computer
y_1, z_1
622
Transmit partial computation and partial signature to client computer
y_2, z_2
622
624
Verify partial computations using check values
Check(g^{u1}, g^{v1}, y_1) == 1
Check(g^{u2}, g^{v2}, y_2) == 1
626
Combine partial computations and generate cryptographic key
y = DPRF.Combine(y_1, y_2)
628
Combine partial signatures and generate verification signature
z = TA.CombineSig(z_1, z_2)
630
Encrypt message using cryptographic key
e = AES_y(m | ...)
632
Generate payload
payload = (h_1, h_2, z, e, ...)

FIG. 6B

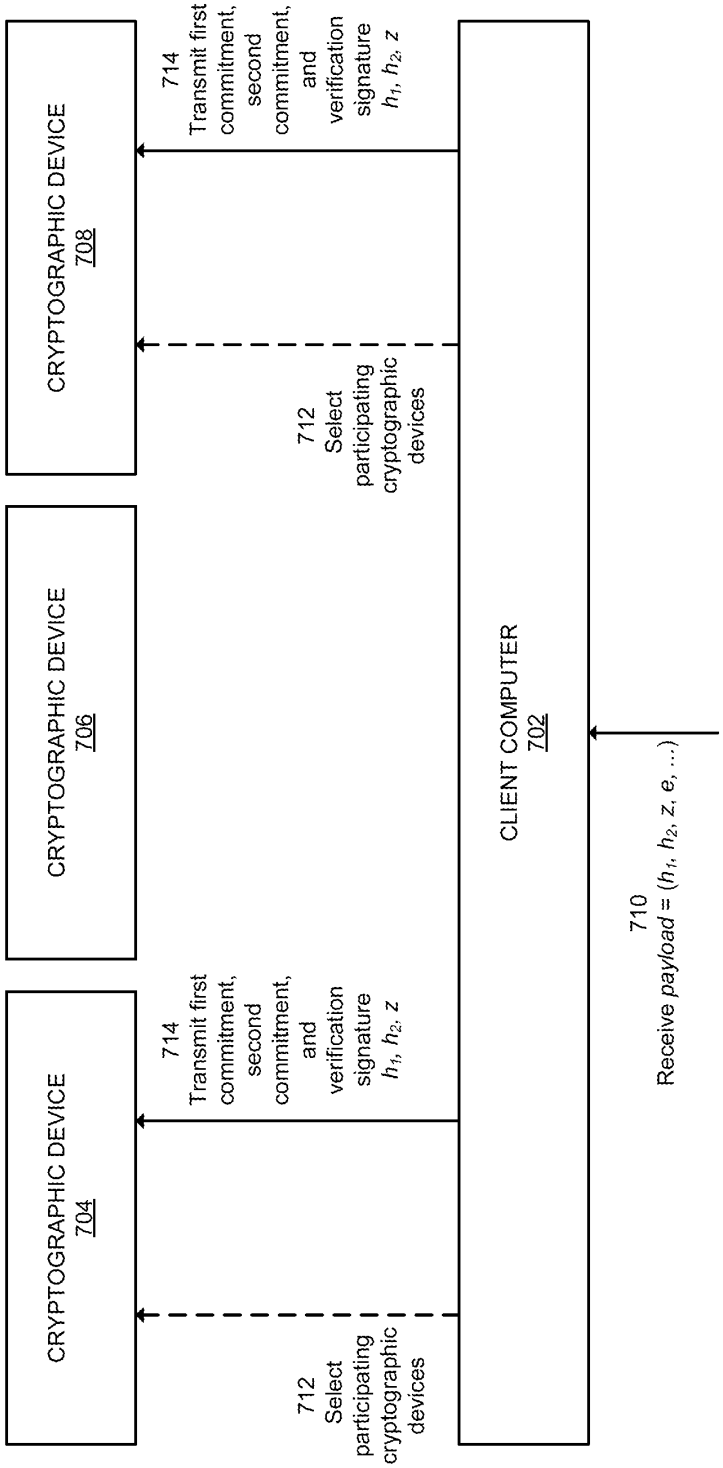

CRYPTOGRAPHIC DEVICE
704
CRYPTOGRAPHIC DEVICE
706
CRYPTOGRAPHIC DEVICE
708
CLIENT COMPUTER
702
710
Receive payload = (h1, h2, z, e, ...)
712
Select participating cryptographic devices
714
Transmit first commitment, second commitment, and verification signature h1, h2, z

FIG. 7A

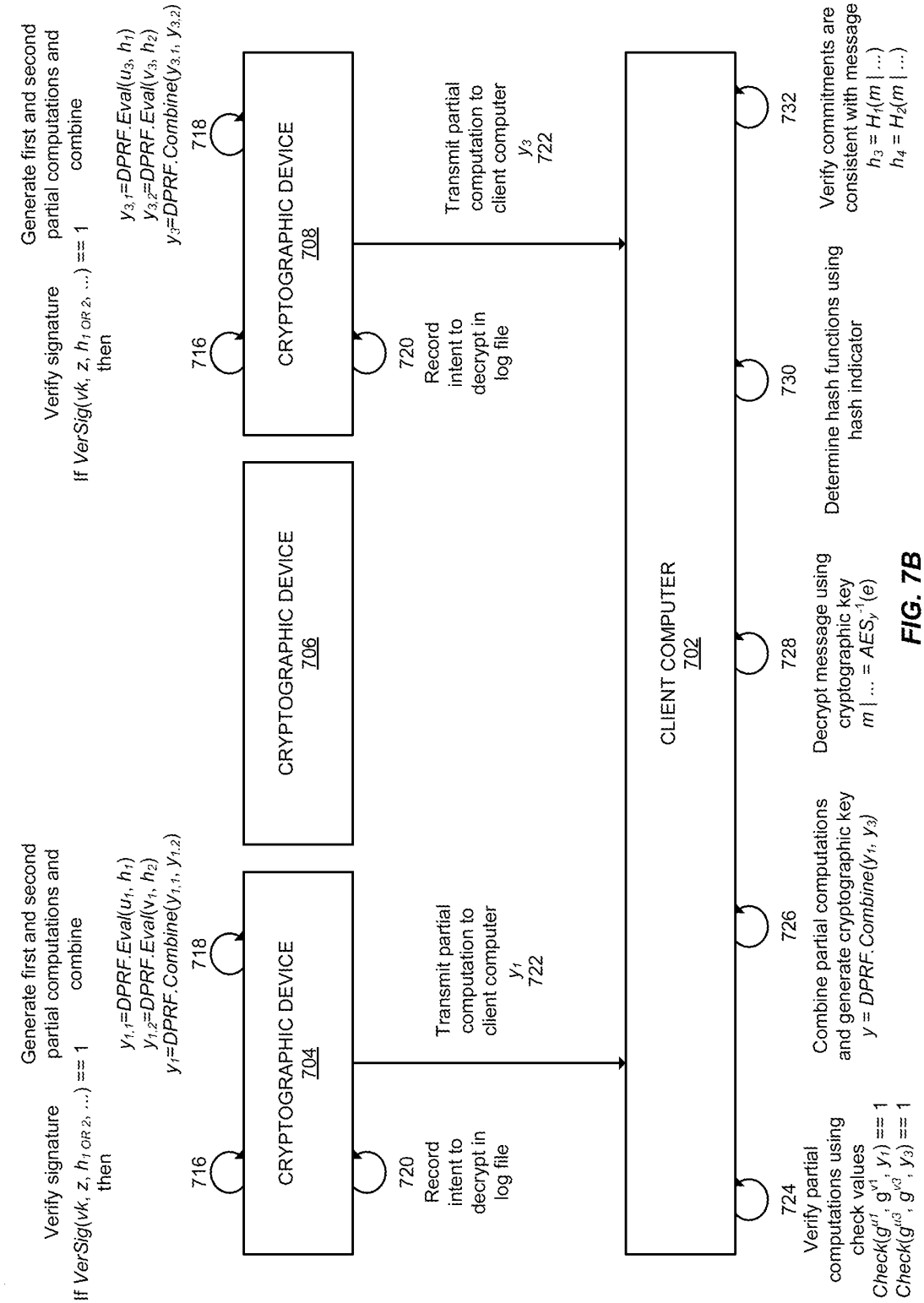

CRYPTOGRAPHIC DEVICE 704
CRYPTOGRAPHIC DEVICE 706
CRYPTOGRAPHIC DEVICE 708
CLIENT COMPUTER 702
716
Verify signature
If VerSig(vk, z, h1 OR 2, ...) == 1
then
718
Generate first and second partial computations and combine
y1,1=DPRF.Eval(u1, h1)
y1,2=DPRF.Eval(v1, h2)
y1=DPRF.Combine(y1,1, y1,2)
y3,1=DPRF.Eval(u3, h1)
y3,2=DPRF.Eval(v3, h2)
y3=DPRF.Combine(y3,1, y3,2)
720
Record intent to decrypt in log file
Transmit partial computation to client computer
y1
722
Transmit partial computation to client computer
y3
722
724
Verify partial computations using check values
Check(g^r1, g^v1, y1) == 1
Check(g^r3, g^v3, y3) == 1
726
Combine partial computations and generate cryptographic key
y = DPRF.Combine(y1, y3)
728
Decrypt message using cryptographic key
m | ... = AES_y^-1(e)
730
Determine hash functions using hash indicator
732
Verify commitments are consistent with message
h3 = H1(m | ...)
h4 = H2(m | ...)

FIG. 7B

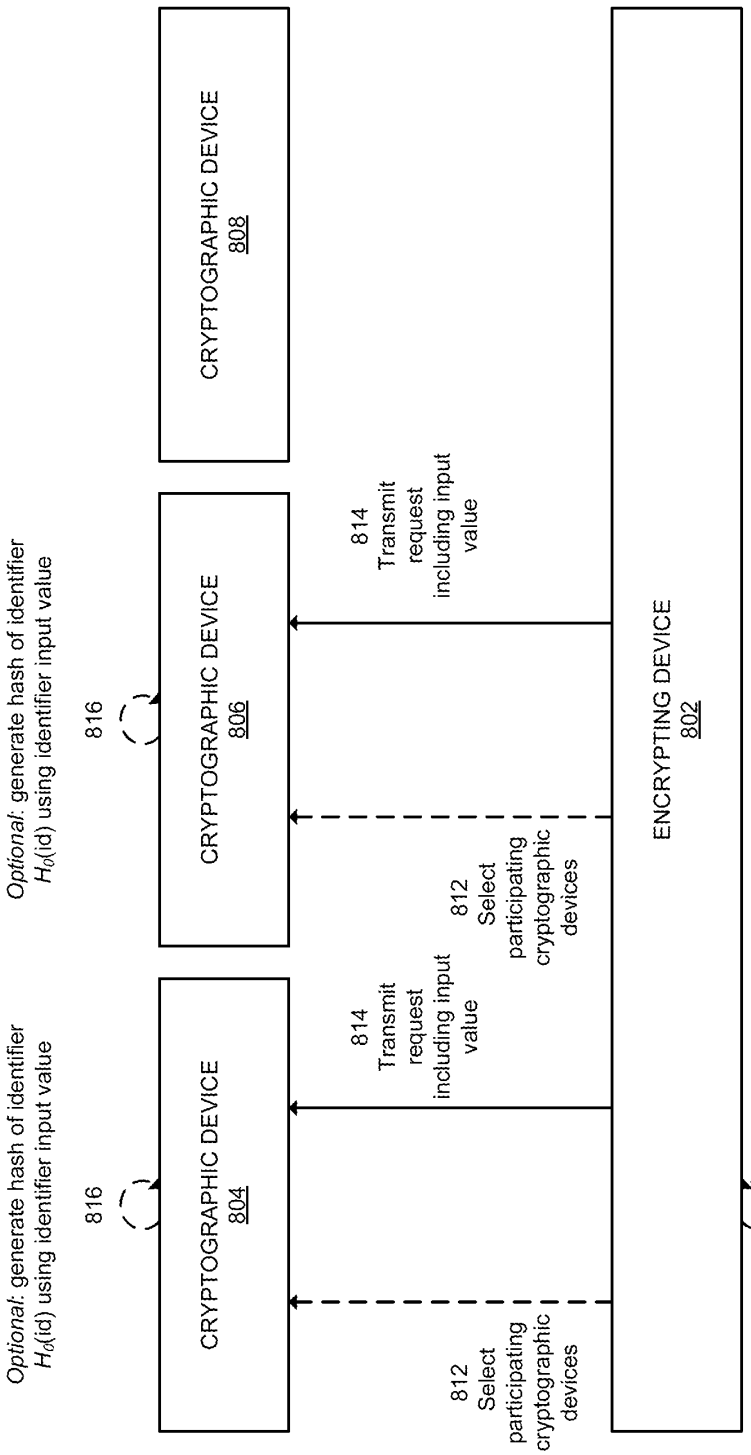

CRYPTOGRAPHIC DEVICE
804
CRYPTOGRAPHIC DEVICE
806
CRYPTOGRAPHIC DEVICE
808
ENCRYPTING DEVICE
802
Optional: generate hash of identifier
H_0(id) using identifier input value
816
Optional: generate hash of identifier
H_0(id) using identifier input value
816
814
Transmit
request
including input
value
814
Transmit
request
including input
value
812
Select
participating
cryptographic
devices
812
Select
participating
cryptographic
devices
Optional: generate input value by
hashing client computer identifier:
H_0(id)
810

FIG. 8A

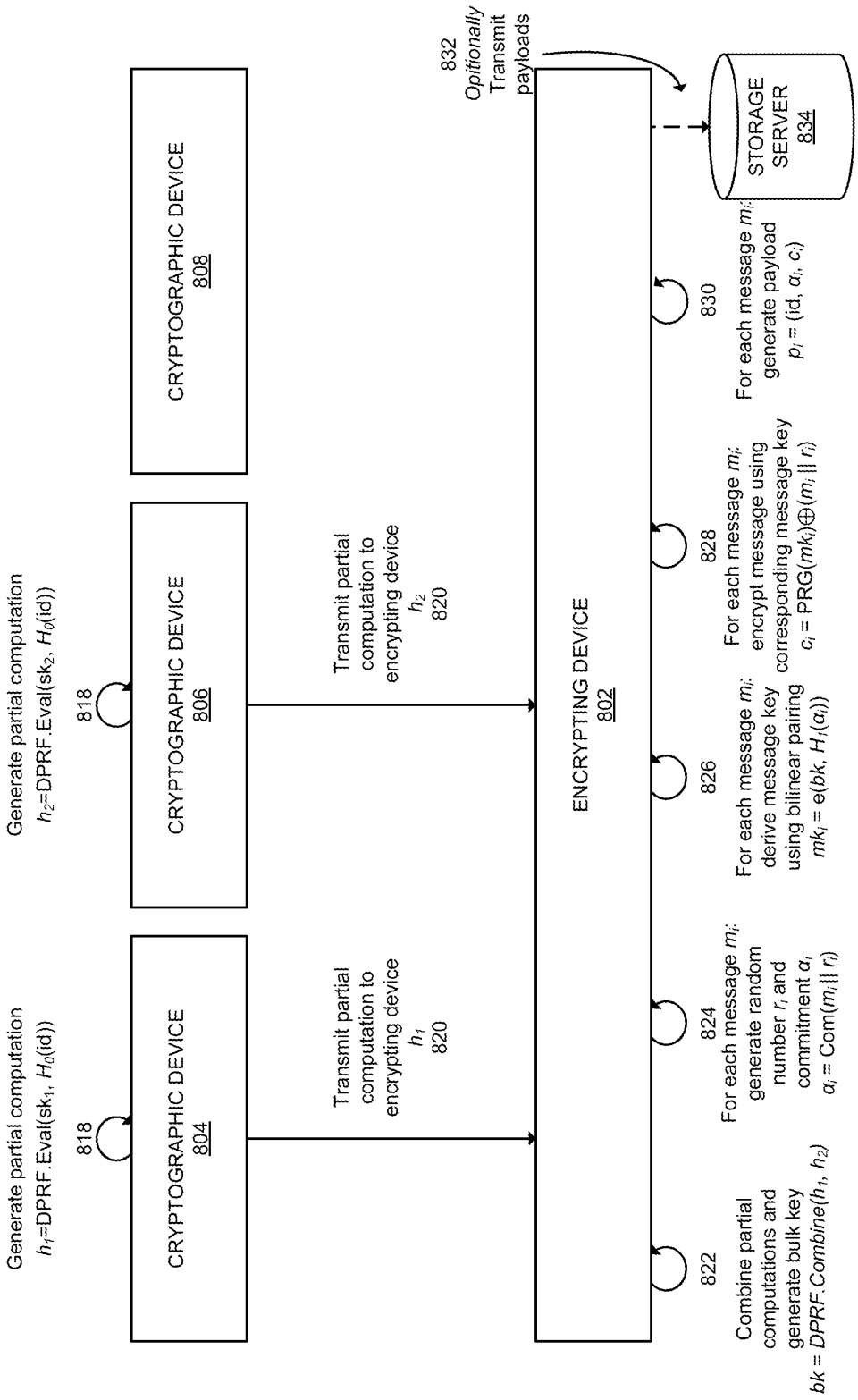

CRYPTOGRAPHIC DEVICE 804
CRYPTOGRAPHIC DEVICE 806
CRYPTOGRAPHIC DEVICE 808
ENCRYPTING DEVICE 802
STORAGE SERVER 834
Generate partial computation h_1=DPRF.Eval(sk_1, H_0(id))
818
Generate partial computation h_2=DPRF.Eval(sk_2, H_0(id))
818
Transmit partial computation to encrypting device h_1 820
Transmit partial computation to encrypting device h_2 820
822 Combine partial computations and generate bulk key bk = DPRF.Combine(h_1, h_2)
824 For each message m_i: generate random number r_i and commitment α_i α_i = Com(m_i || r_i)
826 For each message m_i: derive message key using bilinear pairing mk_i = e(bk, $H_1(\alpha_i)$)
828 For each message m_i: encrypt message using corresponding message key c_i = PRG(mk_i)⊕(m_i || r_i)
830 For each message m_i: generate payload p_i = (id, α_i, c_i)
832 Optionally Transmit payloads

FIG. 8B

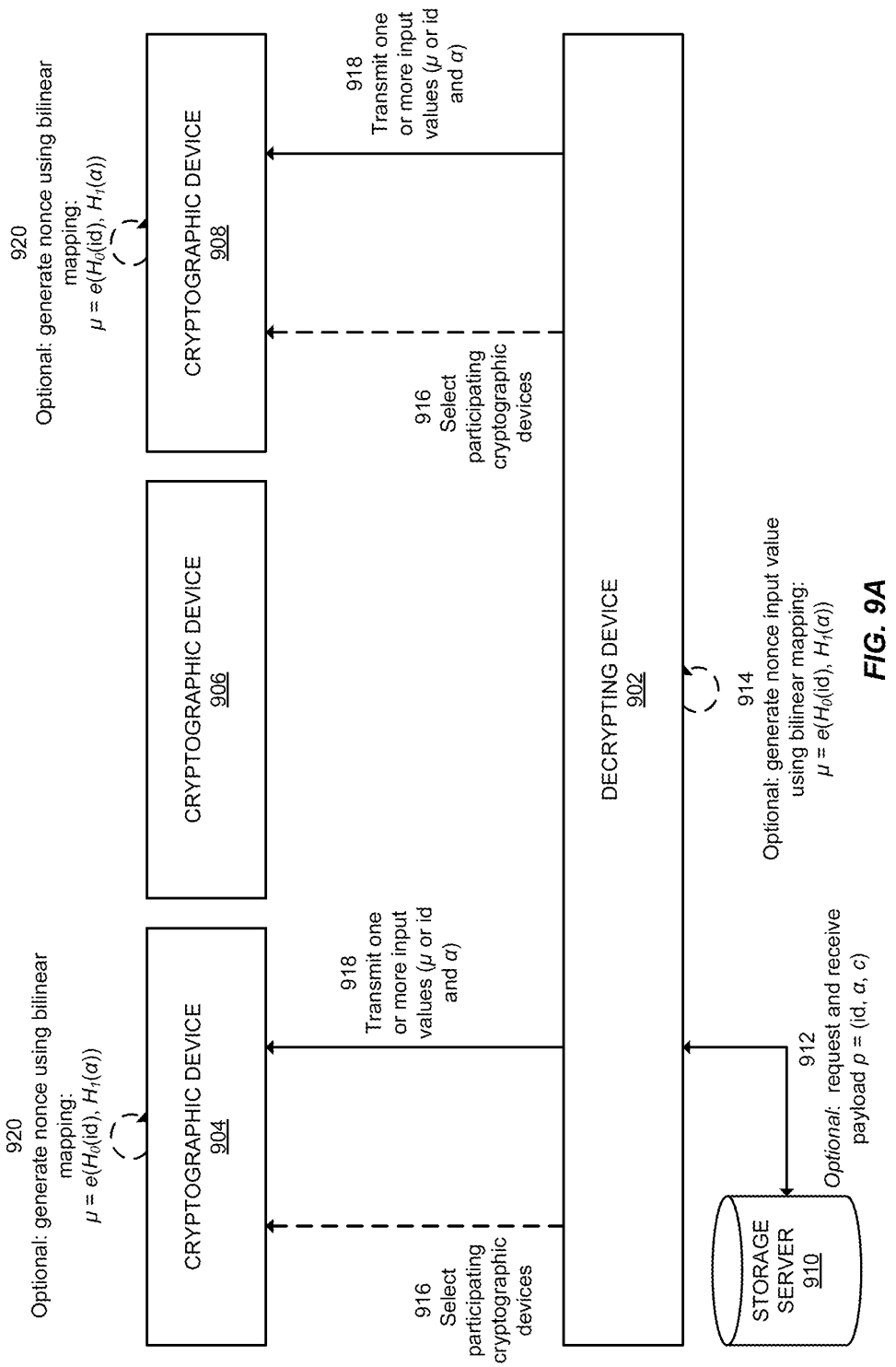

CRYPTOGRAPHIC DEVICE 904
CRYPTOGRAPHIC DEVICE 906
CRYPTOGRAPHIC DEVICE 908
DECRYPTING DEVICE 902
STORAGE SERVER 910
920 Optional: generate nonce using bilinear mapping: $\mu = e(H_0(\mathrm{id}), H_1(\alpha))$
916 Select participating cryptographic devices
918 Transmit one or more input values (μ or id and α)
912 Optional: request and receive payload $\rho = (\mathrm{id}, a, c)$
914 Optional: generate nonce input value using bilinear mapping: $\mu = e(H_0(\mathrm{id}), H_1(\alpha))$

FIG. 9A

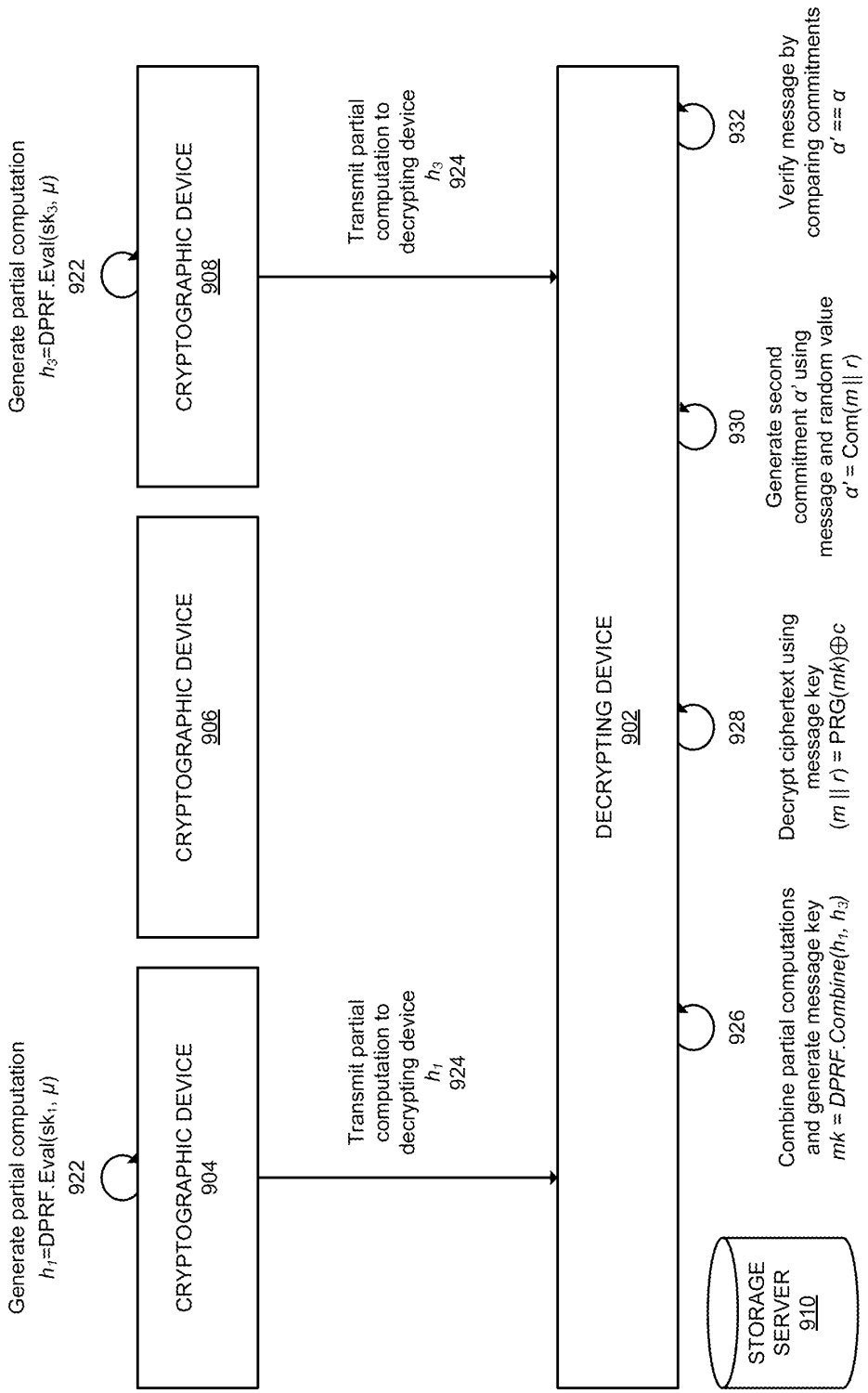

Generate partial computation
h_1=DPRF.Eval(sk_1, μ)
922
CRYPTOGRAPHIC DEVICE
904
Transmit partial computation to decrypting device
h_1
924
Generate partial computation
h_3=DPRF.Eval(sk_3, μ)
922
CRYPTOGRAPHIC DEVICE
908
Transmit partial computation to decrypting device
h_3
924
CRYPTOGRAPHIC DEVICE
906
DECRYPTING DEVICE
902
926
Combine partial computations and generate message key
mk = DPRF.Combine(h_1, h_3)
928
Decrypt ciphertext using message key
$(m \,||\, r)$ = PRG(mk)⊕c
930
Generate second commitment α' using message and random value
α' = Com($m \,||\, r$)
932
Verify message by comparing commitments
$\alpha' == \alpha$
STORAGE SERVER
910

FIG. 9B

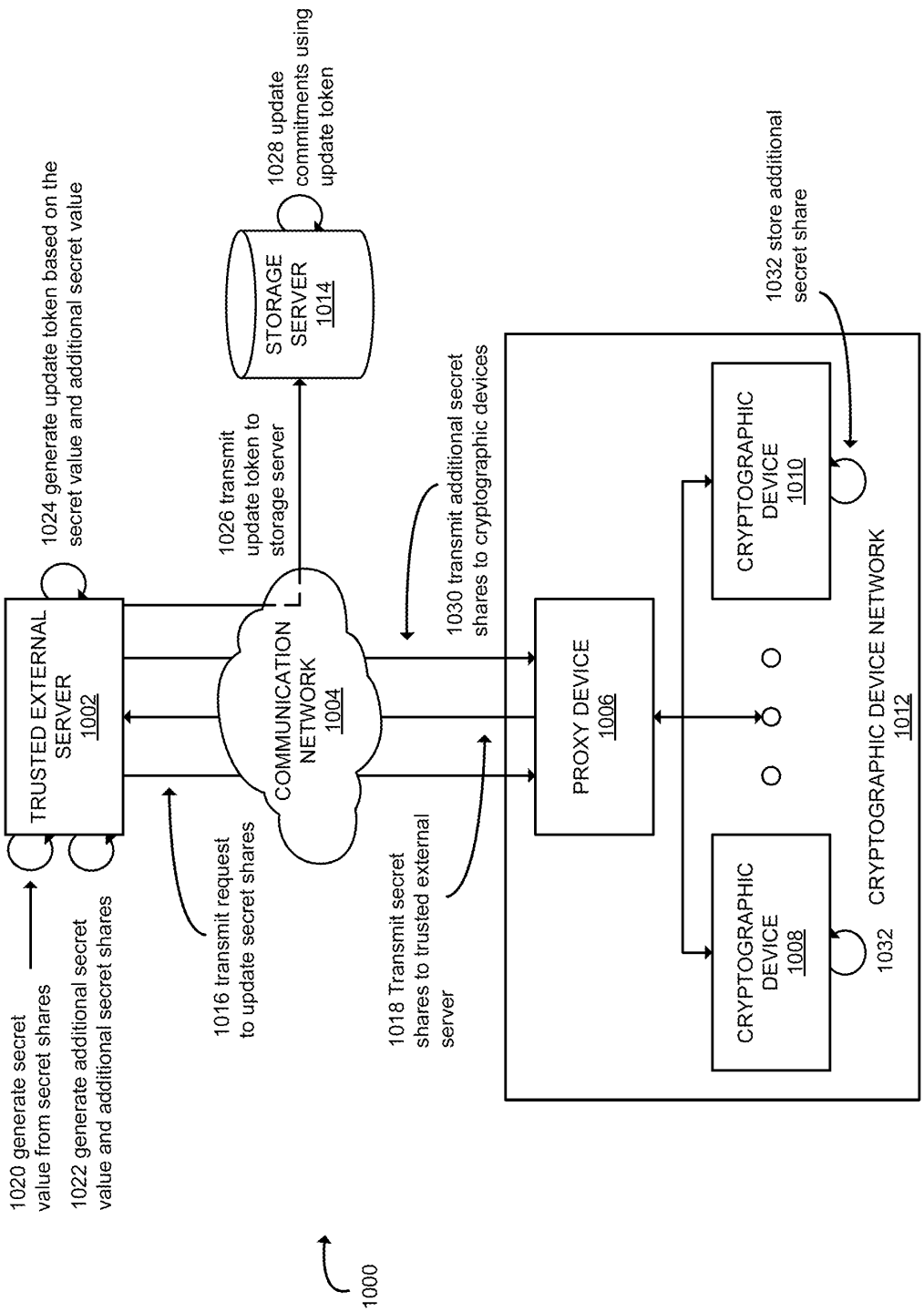

1000
TRUSTED EXTERNAL SERVER 1002
COMMUNICATION NETWORK 1004
STORAGE SERVER 1014
PROXY DEVICE 1006
CRYPTOGRAPHIC DEVICE 1008
CRYPTOGRAPHIC DEVICE 1010
CRYPTOGRAPHIC DEVICE NETWORK 1012
1020 generate secret value from secret shares
1022 generate additional secret value and additional secret shares
1024 generate update token based on the secret value and additional secret value
1026 transmit update token to storage server
1028 update commitments using update token
1030 transmit additional secret shares to cryptographic devices
1032 store additional secret share
1016 transmit request to update secret shares
1018 Transmit secret shares to trusted external server

FIG. 10

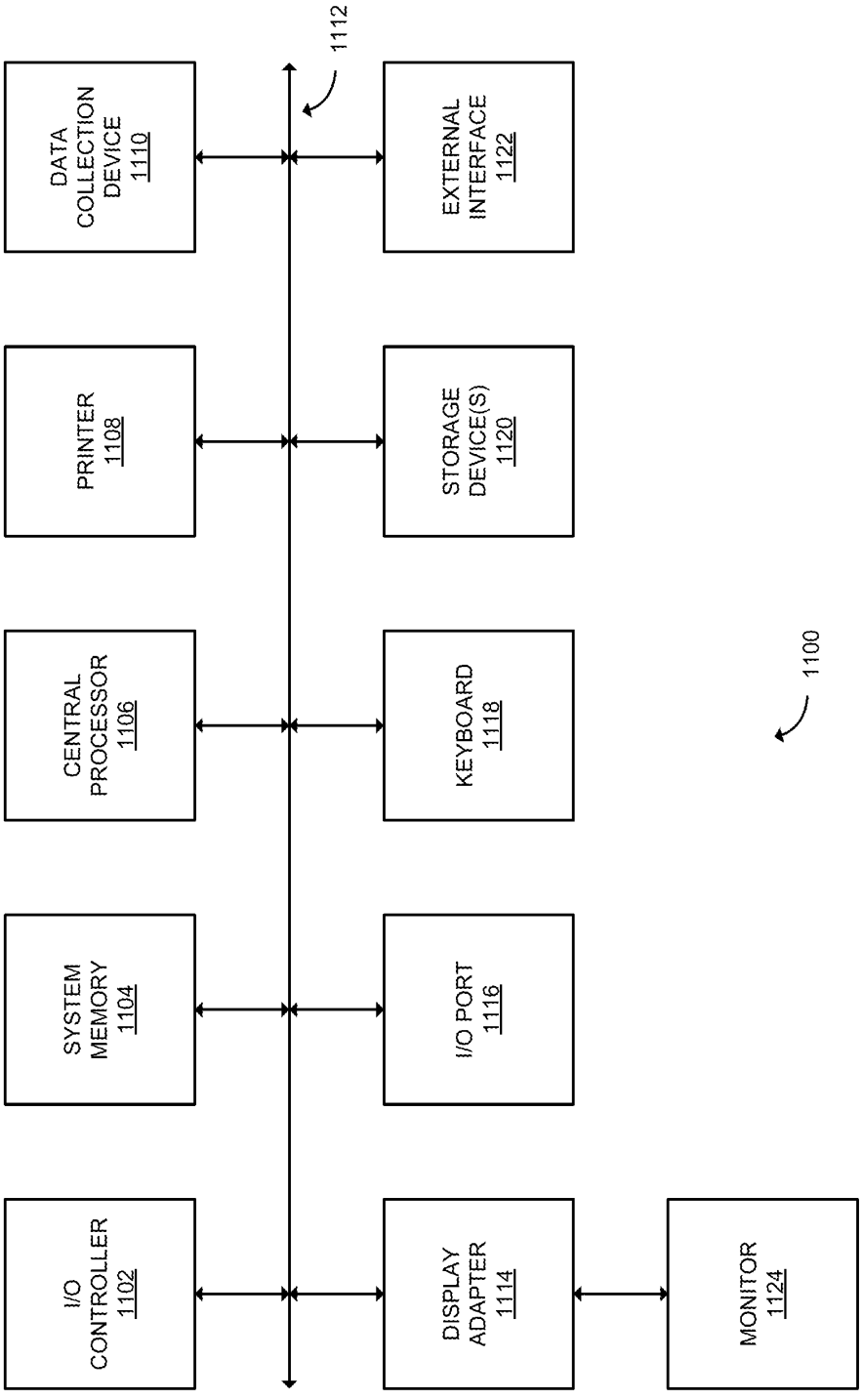

1112
DATA COLLECTION DEVICE 1110
EXTERNAL INTERFACE 1122
PRINTER 1108
STORAGE DEVICE(S) 1120
CENTRAL PROCESSOR 1106
KEYBOARD 1118
1100
SYSTEM MEMORY 1104
I/O PORT 1116
I/O CONTROLLER 1102
DISPLAY ADAPTER 1114
MONITOR 1124

FIG. 11