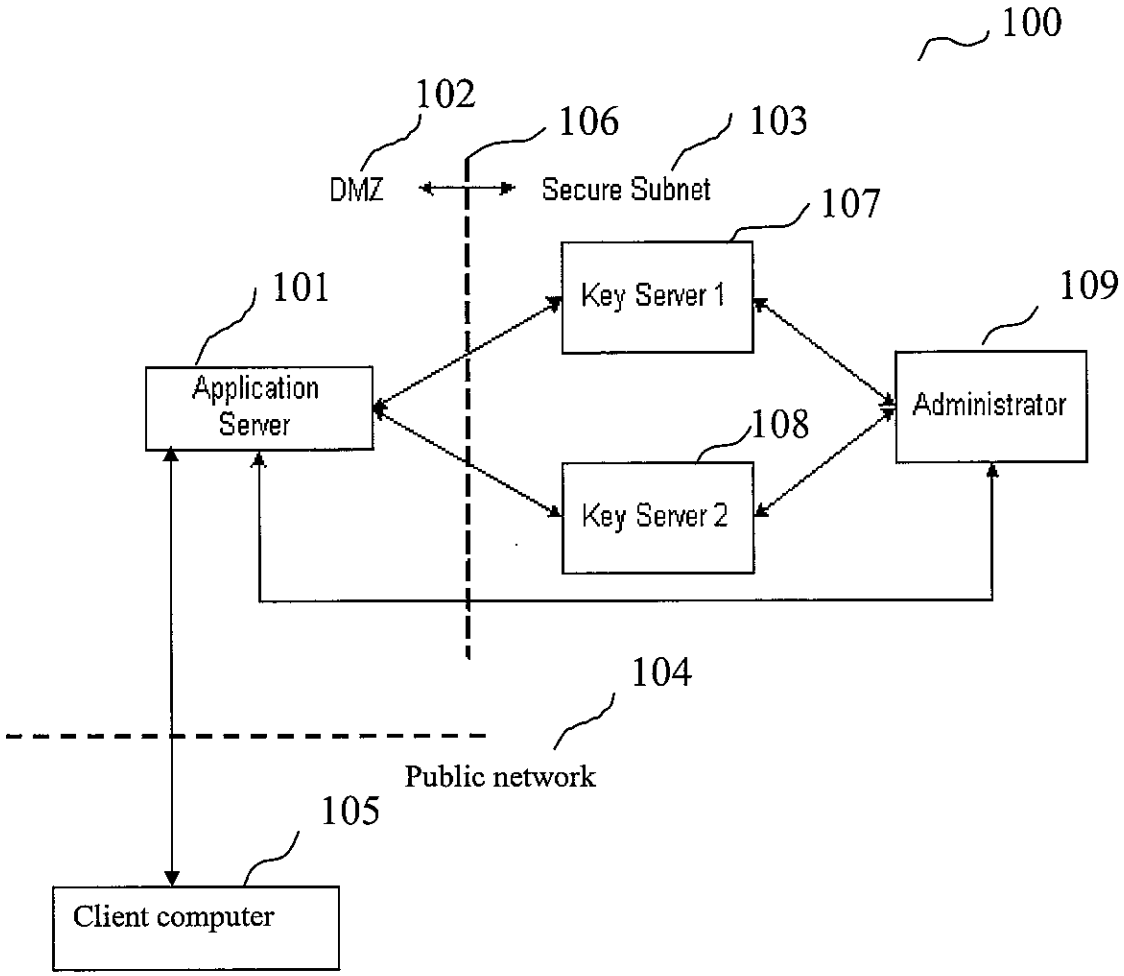

100
102
106
103
DMZ
Secure Subnet
107
101
Key Server 1
109
Application Server
Administrator
108
Key Server 2
104
Public network
105
Client computer

Fig. 1

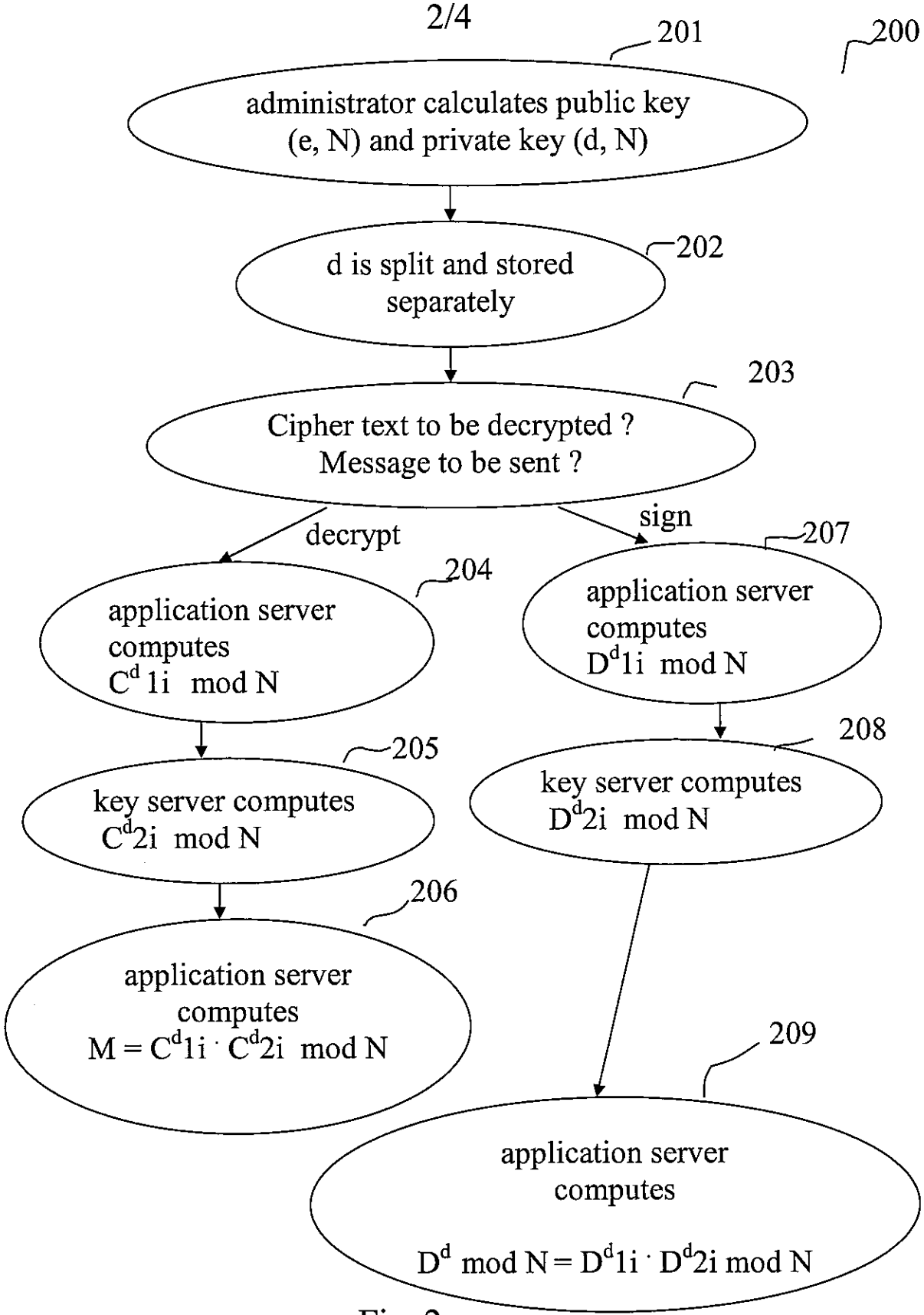

200
201
administrator calculates public key (e, N) and private key (d, N)
202
d is split and stored separately
203
Cipher text to be decrypted ? Message to be sent ?
decrypt
sign
204
application server computes $C^d 1i \mod N$
205
key server computes $C^d 2i \mod N$
206
application server computes $M = C^d 1i \cdot C^d 2i \mod N$
207
application server computes $D^d 1i \mod N$
208
key server computes $D^d 2i \mod N$
209
application server computes $D^d \mod N = D^d 1i \cdot D^d 2i \mod N$

Fig. 2

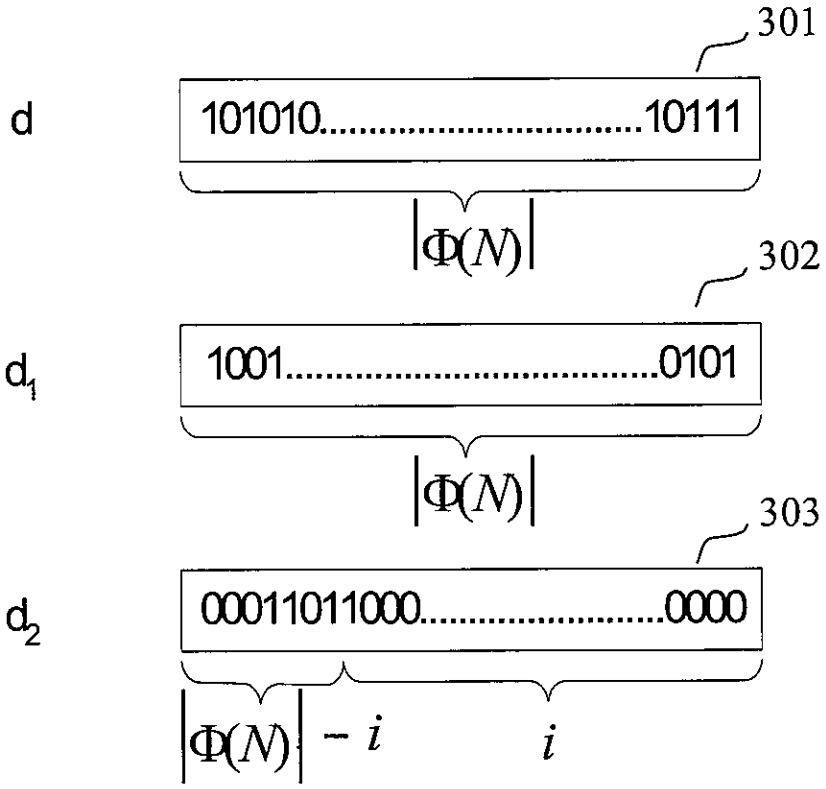

301
d
101010.....10111
$|\Phi(N)|$
302
d_1
1001.....0101
$|\Phi(N)|$
303
d_2
00011011000.....0000
$|\Phi(N)| - i$
i

Fig. 3

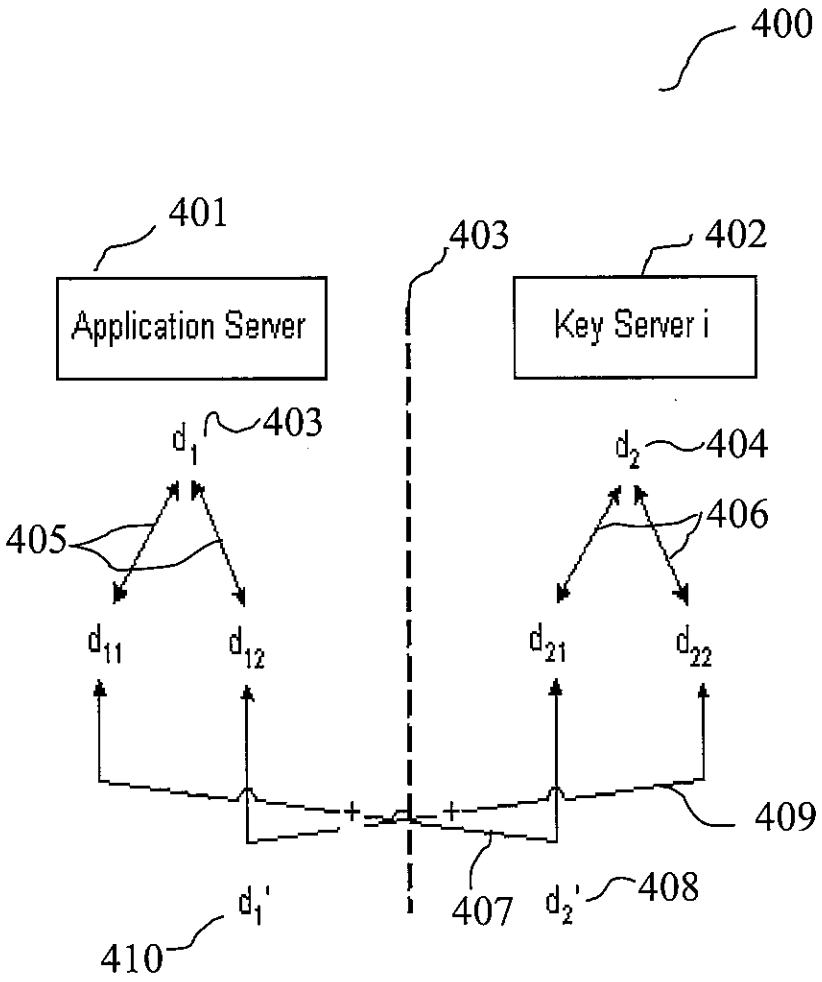

400
401
403
402
Application Server
Key Server i
d_1
403
d_2
404
405
406
d_{11}
d_{12}
d_{21}
d_{22}
409
d_1'
407
d_2'
408
410

Fig. 4