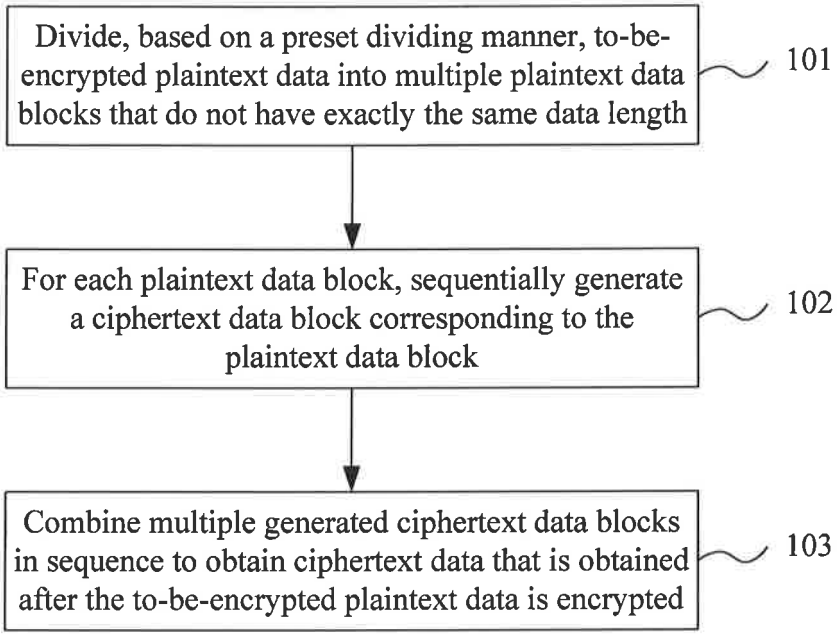
Divide, based on a preset dividing manner, to-be-encrypted plaintext data into multiple plaintext data blocks that do not have exactly the same data length
101
For each plaintext data block, sequentially generate a ciphertext data block corresponding to the plaintext data block
102
Combine multiple generated ciphertext data blocks in sequence to obtain ciphertext data that is obtained after the to-be-encrypted plaintext data is encrypted
103

FIG. 1

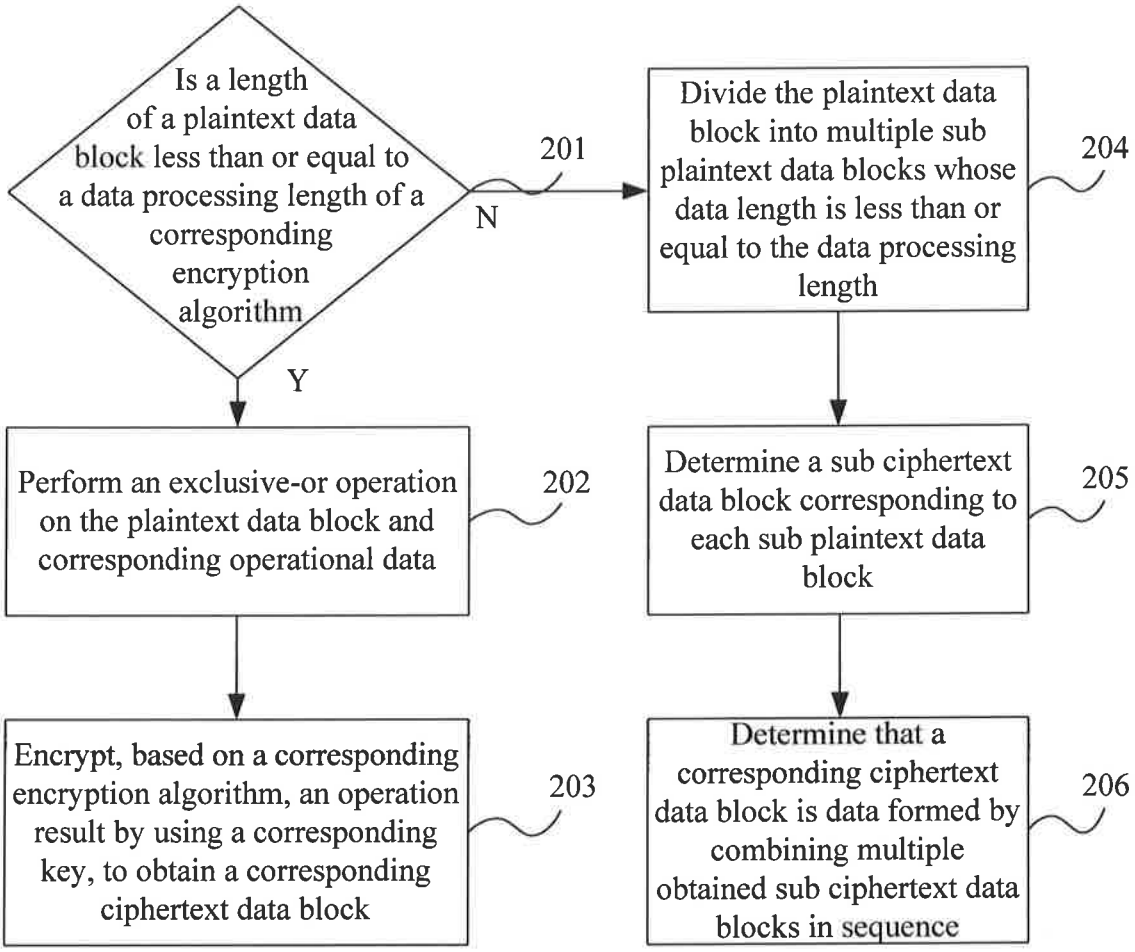
Is a length of a plaintext data block less than or equal to a data processing length of a corresponding encryption algorithm
201
N
Y
Divide the plaintext data block into multiple sub plaintext data blocks whose data length is less than or equal to the data processing length
204
Perform an exclusive-or operation on the plaintext data block and corresponding operational data
202
Determine a sub ciphertext data block corresponding to each sub plaintext data block
205
Encrypt, based on a corresponding encryption algorithm, an operation result by using a corresponding key, to obtain a corresponding ciphertext data block
203
Determine that a corresponding ciphertext data block is data formed by combining multiple obtained sub ciphertext data blocks in sequence
206

FIG. 2

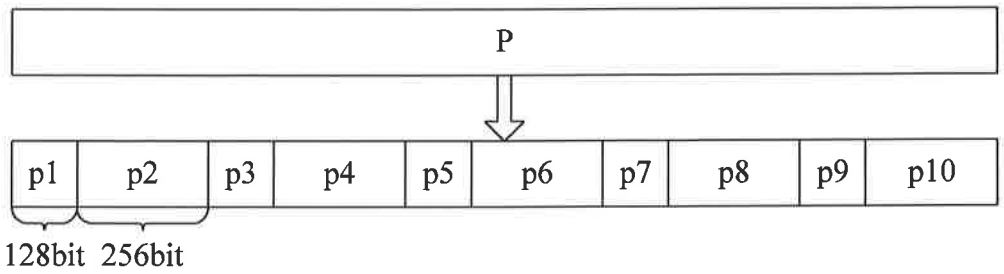

FIG. 3

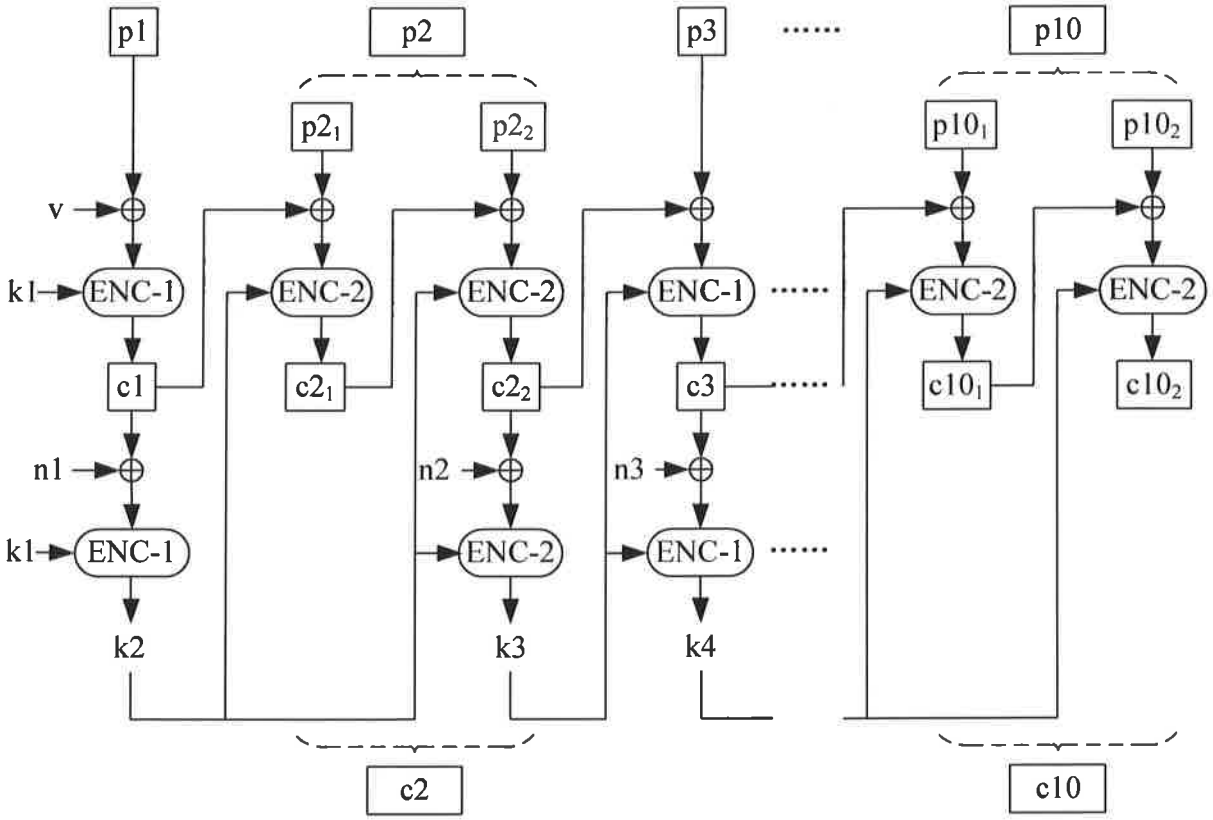

FIG. 4

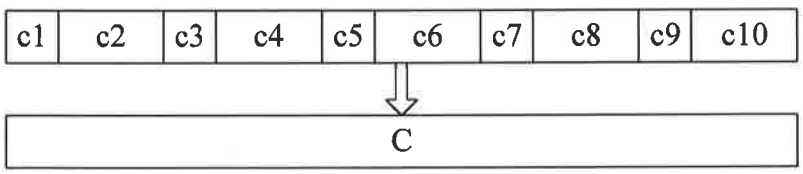

FIG. 5

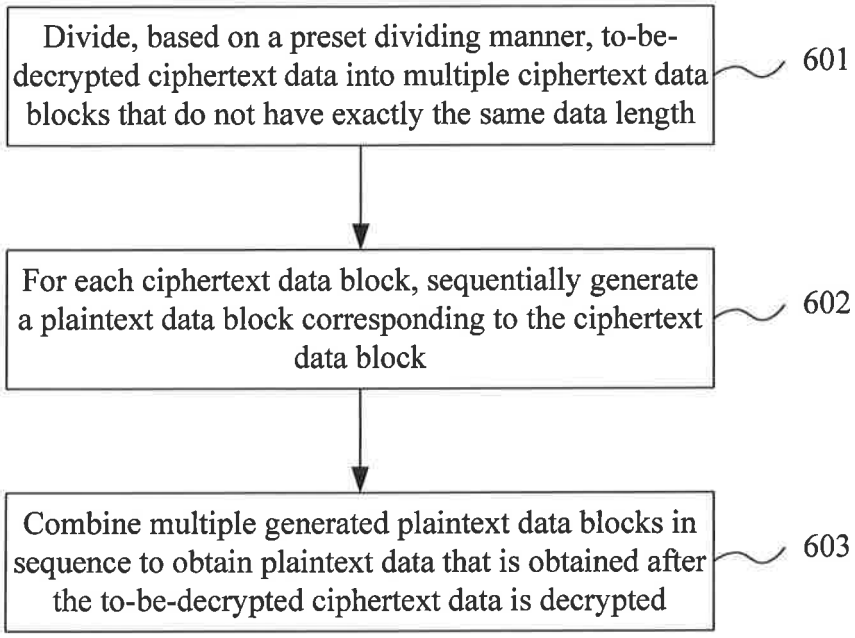
Divide, based on a preset dividing manner, to-be-decrypted ciphertext data into multiple ciphertext data blocks that do not have exactly the same data length
601
For each ciphertext data block, sequentially generate a plaintext data block corresponding to the ciphertext data block
602
Combine multiple generated plaintext data blocks in sequence to obtain plaintext data that is obtained after the to-be-decrypted ciphertext data is decrypted
603

FIG. 6

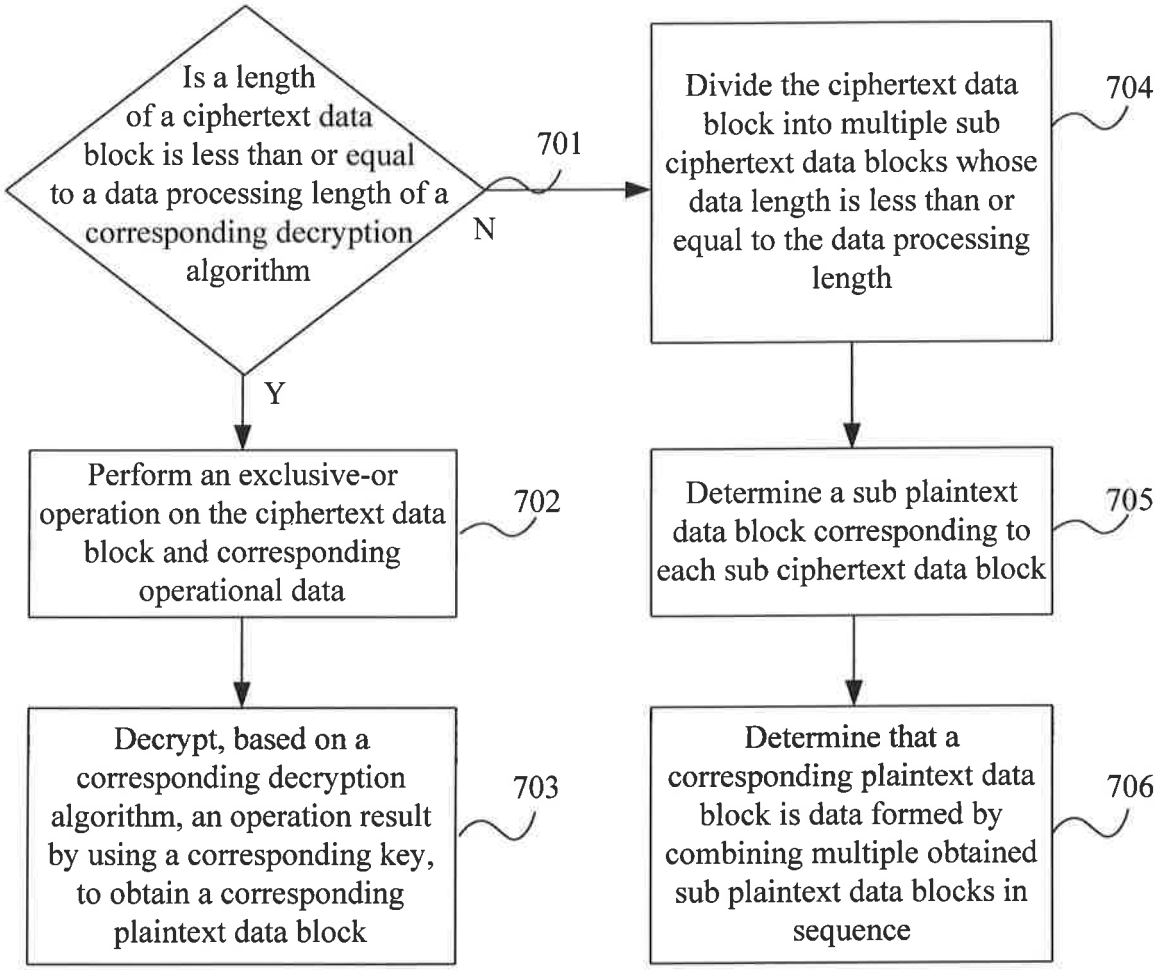
Is a length of a ciphertext data block is less than or equal to a data processing length of a corresponding decryption algorithm
701
N
Y
Divide the ciphertext data block into multiple sub ciphertext data blocks whose data length is less than or equal to the data processing length
704
Perform an exclusive-or operation on the ciphertext data block and corresponding operational data
702
Decrypt, based on a corresponding decryption algorithm, an operation result by using a corresponding key, to obtain a corresponding plaintext data block
703
Determine a sub plaintext data block corresponding to each sub ciphertext data block
705
Determine that a corresponding plaintext data block is data formed by combining multiple obtained sub plaintext data blocks in sequence
706

FIG. 7

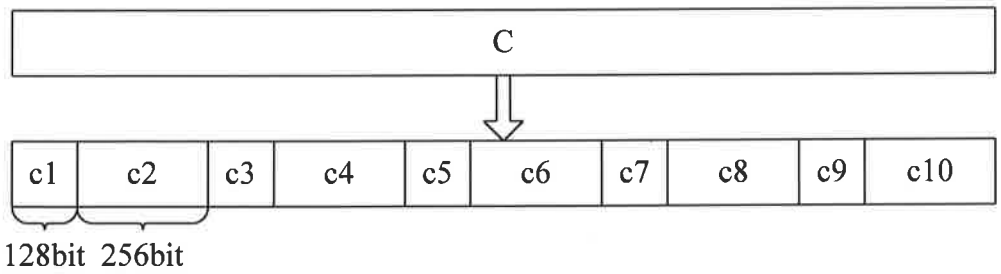
C
c1
c2
c3
c4
c5
c6
c7
c8
c9
c10
128bit
256bit

FIG. 8

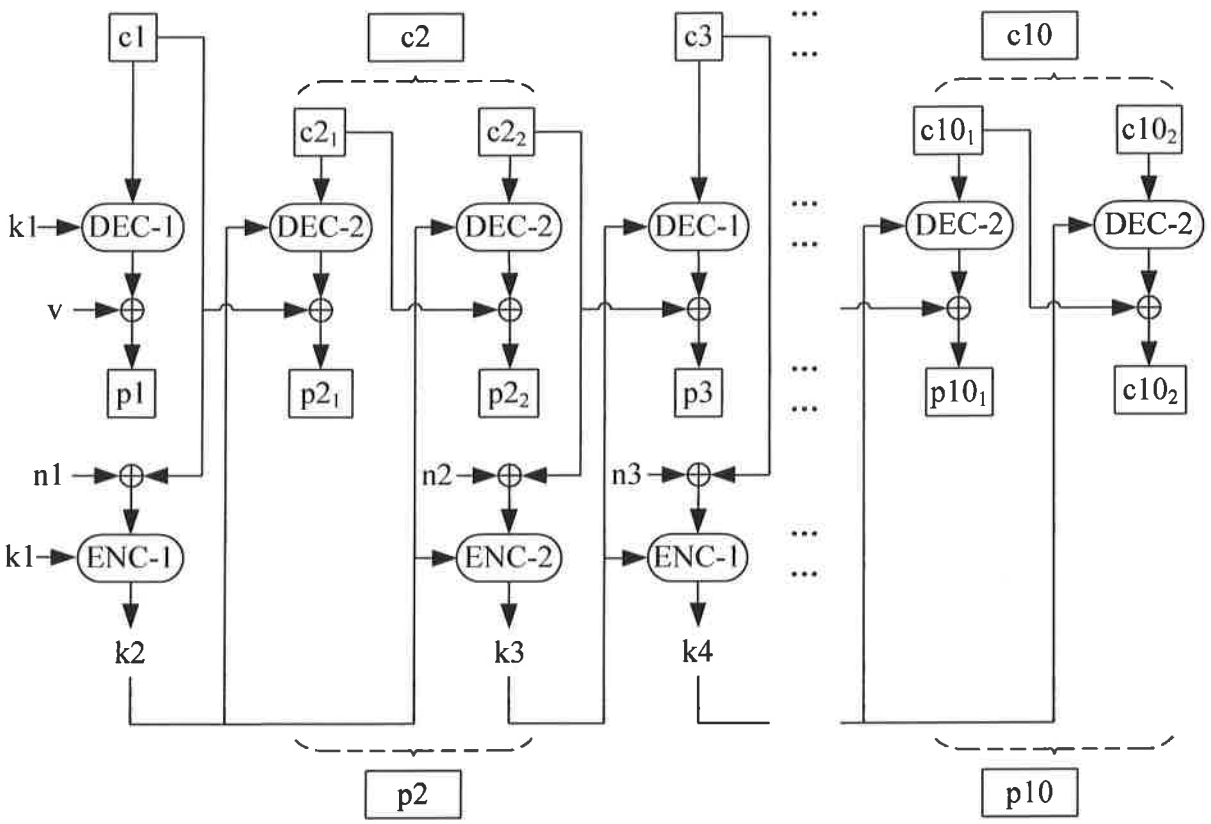
c1
c2
c3
c10
$c2_1$
$c2_2$
$c10_1$
$c10_2$
k1
DEC-1
DEC-2
DEC-2
DEC-1
DEC-2
DEC-2
v
p1
$p2_1$
$p2_2$
p3
$p10_1$
$c10_2$
n1
n2
n3
k1
ENC-1
ENC-2
ENC-1
k2
k3
k4
p2
p10

FIG. 9

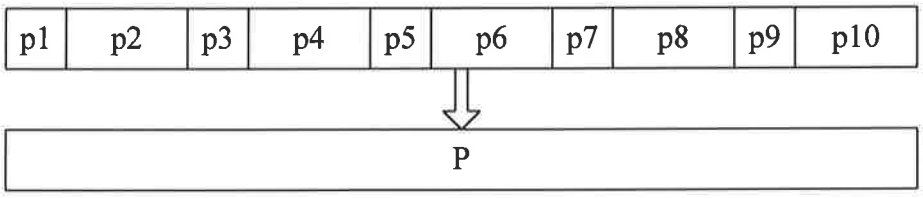
p1
p2
p3
p4
p5
p6
p7
p8
p9
p10
P

FIG. 10

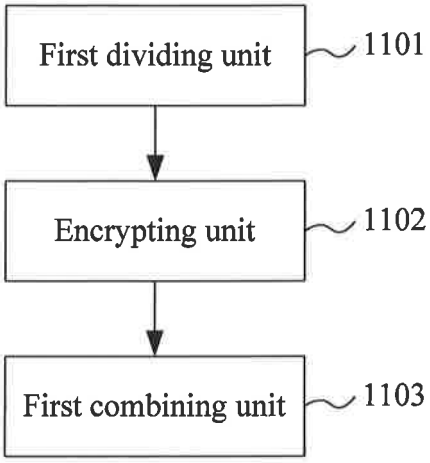
First dividing unit
1101
Encrypting unit
1102
First combining unit
1103

FIG. 11

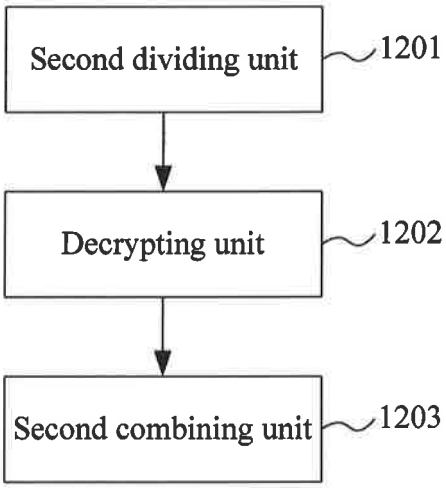
Second dividing unit
1201
Decrypting unit
1202
Second combining unit
1203

FIG. 12