

CLAIMS

What is claimed is:

1. A data encryption method, comprising:

dividing, based on a preset dividing manner, to-be-encrypted plaintext data into multiple
5 plaintext data blocks that do not have exactly the same data length;

for each plaintext data block, sequentially determining that an encryption algorithm
corresponding to the plaintext data block is an encryption algorithm corresponding to a preset
length interval within which a data length of the plaintext data block falls; and generating,
based on the encryption algorithm corresponding to the plaintext data block and by using a
10 key corresponding to the plaintext data block, a ciphertext data block corresponding to the
plaintext data block, wherein a larger value in the preset length interval indicates lower
security strength of the encryption algorithm corresponding to the preset length interval; and

combining multiple generated ciphertext data blocks according to a sequence of the
multiple plaintext data blocks that are obtained by means of the dividing, to obtain ciphertext
15 data that is obtained after the to-be-encrypted plaintext data is encrypted,

wherein, when the plaintext data block is the first plaintext data block among the
multiple plaintext data blocks, the key corresponding to the plaintext data block is a preset
initial key; and

when the plaintext data block is not the first plaintext data block among the multiple
20 plaintext data blocks, the key corresponding to the plaintext data block is generated according
to a ciphertext data block corresponding to a previous plaintext data block of the plaintext
data block, based on an encryption algorithm corresponding to the previous plaintext data
block, and by using a key corresponding to the previous plaintext data block.

2. The method according to claim 1, wherein the preset length interval specifically
25 comprises two intervals: one preset length interval is a length interval less than or equal to a
specified length, and the other preset length interval is a length interval greater than the
specified length.

~~3. The method according to claim 1, wherein, when the plaintext data block is the first~~

plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is a preset initial key; and

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is generated according to a ciphertext data block corresponding to a previous plaintext data block of the plaintext data block, based on an encryption algorithm corresponding to the previous plaintext data block, and by using a key corresponding to the previous plaintext data block.

43. The method according to any one of claims 1 to 32, wherein the generating, based on the encryption algorithm corresponding to the plaintext data block and by using a key corresponding to the plaintext data block, a ciphertext data block corresponding to the plaintext data block specifically comprises:

when the data length of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the plaintext data block, performing an exclusive-or operation on the plaintext data block and operational data corresponding to the plaintext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain the ciphertext data block corresponding to the plaintext data block; and

when the data length of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the plaintext data block, dividing the plaintext data block into multiple sub plaintext data blocks whose data length is less than or equal to the data processing length; for each sub plaintext data block, sequentially performing an exclusive-or operation on the sub plaintext data block and operational data corresponding to the sub plaintext data block, to obtain an operation result, and encrypting the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain a sub ciphertext data block corresponding to the sub plaintext data block; and combining multiple obtained sub ciphertext data blocks according to a sequence of the multiple sub plaintext data blocks that are obtained by means of the dividing, to obtain the ciphertext data block corresponding to the plaintext data block.

54. The method according to claim 43, wherein, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the operational data corresponding to the plaintext data block is preset initial data; and

when the plaintext data block is not the first plaintext data block among the multiple
5 plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is the ciphertext data block corresponding to the previous plaintext data block; and if the data length of the previous plaintext data block of the plaintext data block is
10 greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block.

65. The method according to claim 43, wherein, when the sub plaintext data block is the
15 first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is the operational data corresponding to the plaintext data block; and

when the sub plaintext data block is not the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data
20 corresponding to the sub plaintext data block is a sub ciphertext data block corresponding to a previous sub plaintext data block of the sub plaintext data block.

76. The method according to claim 43, wherein the key corresponding to the plaintext data block is generated specifically in the following manner:

when the plaintext data block is not the first plaintext data block among the multiple
25 plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, performing an exclusive-or operation on the ciphertext data block corresponding to the previous plaintext data block and a preset parameter value corresponding to the previous plaintext data block, to obtain an operation
30 result; and encrypting the operation result based on the encryption algorithm corresponding to

the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block; and

if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, performing an exclusive-or operation on a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block and the preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block.

87. The method according to claim 45 or 6-7, wherein the specified sub plaintext data block among the multiple sub plaintext data blocks is specifically the first sub plaintext data block among the multiple sub plaintext data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.

98. A data decryption method, comprising:
dividing, 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;

for each ciphertext data block, sequentially determining that a decryption algorithm corresponding to the ciphertext data block is a decryption algorithm corresponding to a preset length interval within which a data length of the ciphertext data block falls; and generating, based on the decryption algorithm corresponding to the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block, wherein a larger value in the preset length interval indicates lower security strength of an encryption algorithm corresponding to the decryption algorithm corresponding to the preset length interval; and

combining multiple decrypted plaintext data blocks according to a sequence of the multiple ciphertext data blocks that are obtained by means of the dividing, to obtain plaintext data that is obtained after the to-be-decrypted ciphertext data is decrypted,

wherein, when the ciphertext data block is the first ciphertext data block among the

multiple ciphertext data blocks, the key corresponding to the ciphertext data block is a preset initial key; and

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is generated according to a previous ciphertext data block of the ciphertext data block, based on an encryption algorithm corresponding to a decryption algorithm corresponding to the previous ciphertext data block, and by using a key corresponding to the previous ciphertext data block.

109. The method according to claim 89, wherein the preset length interval specifically comprises two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

~~11. The method according to claim 9, wherein, when the ciphertext data block is the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is a preset initial key; and~~

~~when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is generated according to a previous ciphertext data block of the ciphertext data block, based on an encryption algorithm corresponding to a decryption algorithm corresponding to the previous ciphertext data block, and by using a key corresponding to the previous ciphertext data block.~~

110. The method according to any one of claims 89 to 91, wherein the generating, based on the decryption algorithm corresponding to the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block specifically comprises:

when the data length of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the ciphertext data block, decrypting the ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result; and performing an exclusive-or operation on the decryption result and operational data corresponding to the ciphertext data block, to obtain the plaintext data block corresponding to the ciphertext data block; and

when the data length of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the ciphertext data block, dividing the ciphertext data block into multiple sub ciphertext data blocks whose data length is less than or equal to the data processing length; for each sub ciphertext data block, sequentially decrypting the sub ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result, and performing an exclusive-or operation on the decryption result and operational data corresponding to the sub ciphertext data block, to obtain a sub plaintext data block corresponding to the sub ciphertext data block; and combining multiple obtained sub plaintext data blocks according to a sequence of the multiple sub ciphertext data blocks that are obtained by means of the dividing, to obtain the plaintext data block corresponding to the ciphertext data block.

1311. The method according to claim 1210, wherein, when the ciphertext data block is the first ciphertext data block among the multiple ciphertext data blocks, the operational data corresponding to the ciphertext data block is preset initial data; and

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is the previous ciphertext data block; and if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block.

1412. The method according to claim 1210, wherein, when the sub ciphertext data block is the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is the operational data corresponding to the ciphertext data block; and

when the sub ciphertext data block is not the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data

corresponding to the sub ciphertext data block is a previous sub ciphertext data block of the sub ciphertext data block.

1513. The method according to claim 1210, wherein the key corresponding to the ciphertext data block is generated specifically in the following manner:

5 when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, performing an exclusive-or operation on the previous ciphertext data block and a preset parameter value corresponding to the previous
10 ciphertext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block; and

15 if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, performing an exclusive-or operation on a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block and the preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypting the operation result based on the encryption
20 algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block.

1614. The method according to claim 1311 or 1513, wherein the specified sub ciphertext data block among the multiple sub ciphertext data blocks is specifically the first sub
25 ciphertext data block among the multiple sub ciphertext data blocks or the last sub ciphertext data block among the multiple sub ciphertext data blocks.

1715. A data encryption apparatus, comprising:

30 a first dividing unit, configured to 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;

an encrypting unit, configured to sequentially determine, for each plaintext data block, that an encryption algorithm corresponding to the plaintext data block is an encryption algorithm corresponding to a preset length interval within which a data length of the plaintext data block falls; and generate, based on the encryption algorithm corresponding to the
5 plaintext data block and by using a key corresponding to the plaintext data block, a ciphertext data block corresponding to the plaintext data block, wherein a larger value in the preset length interval indicates lower security strength of the encryption algorithm corresponding to the preset length interval; and

a first combining unit, configured to combine multiple generated ciphertext data blocks
10 according to a sequence of the multiple plaintext data blocks that are obtained by means of the dividing, to obtain ciphertext data that is obtained after the to-be-encrypted plaintext data is encrypted,

wherein, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is a preset
15 initial key; and

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is generated according to a ciphertext data block corresponding to a previous plaintext data block of the plaintext data block, based on an encryption algorithm corresponding to the previous plaintext data
20 block, and by using a key corresponding to the previous plaintext data block.

1816. The apparatus according to claim 1715, wherein the preset length interval specifically comprises two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

~~19. The apparatus according to claim 17, wherein, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is a preset initial key; and~~
25

~~when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is generated according to a ciphertext data block corresponding to a previous plaintext data block of the plaintext
30~~

~~data block, based on an encryption algorithm corresponding to the previous plaintext data block, and by using a key corresponding to the previous plaintext data block.~~

2017. The apparatus according to any one of claims 17-15 to 1916, wherein the encrypting unit is specifically configured to: when the data length of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the plaintext data block, perform an exclusive-or operation on the plaintext data block and operational data corresponding to the plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain the ciphertext data block corresponding to the plaintext data block; and

when the data length of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the plaintext data block, divide the plaintext data block into multiple sub plaintext data blocks whose data length is less than or equal to the data processing length; for each sub plaintext data block, sequentially perform an exclusive-or operation on the sub plaintext data block and operational data corresponding to the sub plaintext data block, to obtain an operation result, and encrypt the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain a sub ciphertext data block corresponding to the sub plaintext data block; and combine multiple obtained sub ciphertext data blocks according to a sequence of the multiple sub plaintext data blocks that are obtained by means of the dividing, to obtain the ciphertext data block corresponding to the plaintext data block.

2+18. The apparatus according to claim 2017, wherein, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the operational data corresponding to the plaintext data block is preset initial data; and

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is the ciphertext data block corresponding to the previous plaintext data block; and if the data length of the previous plaintext data block of the plaintext data block is

greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block.

5 | 2219. The apparatus according to claim 2017, wherein, when the sub plaintext data block is the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is the operational data corresponding to the plaintext data block; and

when the sub plaintext data block is not the first sub plaintext data block among the
10 multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is a sub ciphertext data block corresponding to a previous sub plaintext data block of the sub plaintext data block.

| 2320. The apparatus according to claim 2017, wherein the encrypting unit is specifically configured to: when the plaintext data block is not the first plaintext data block among the
15 multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, perform an exclusive-or operation on the ciphertext data block corresponding to the previous plaintext data block and a preset parameter value corresponding to the previous plaintext data block, to obtain an
20 operation result; and encrypt the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block; and

if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous
25 plaintext data block, perform an exclusive-or operation on a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block and the preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the previous plaintext data block
30 and by using the key corresponding to the previous plaintext data block, to obtain the key

corresponding to the plaintext data block.

2421. The apparatus according to claim 2418 or 2320, wherein the specified sub plaintext data block among the multiple sub plaintext data blocks is specifically the first sub plaintext data block among the multiple sub plaintext data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.

2522. A data decryption apparatus, comprising:

a second dividing unit, configured to 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;

a decrypting unit, configured to sequentially determine, for each ciphertext data block, that a decryption algorithm corresponding to the ciphertext data block is a decryption algorithm corresponding to a preset length interval within which a data length of the ciphertext data block falls; and generate, based on the decryption algorithm corresponding to the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block, wherein a larger value in the preset length interval indicates lower security strength of an encryption algorithm corresponding to the decryption algorithm corresponding to the preset length interval; and

a second combining unit, configured to combine multiple decrypted plaintext data blocks according to a sequence of the multiple ciphertext data blocks that are obtained by means of the dividing, to obtain plaintext data that is obtained after the to-be-decrypted ciphertext data is decrypted,

wherein, when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is a preset initial key; and

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is generated according to a previous ciphertext data block of the ciphertext data block, based on an encryption algorithm corresponding to a decryption algorithm corresponding to the previous ciphertext data block, and by using a key corresponding to the previous ciphertext data block.

2623. The apparatus according to claim 2522, wherein the preset length interval

specifically comprises two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

~~27. The apparatus according to claim 25, wherein, when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is a preset initial key; and~~

~~when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is generated according to a previous ciphertext data block of the ciphertext data block, based on an encryption algorithm corresponding to a decryption algorithm corresponding to the previous ciphertext data block, and by using a key corresponding to the previous ciphertext data block.~~

~~28~~24. The apparatus according to any one of claims ~~25-22~~ 25-22 to ~~27~~23, wherein the decrypting unit is specifically configured to: when the data length of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the ciphertext data block, decrypt the ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result; and perform an exclusive-or operation on the decryption result and operational data corresponding to the ciphertext data block, to obtain the plaintext data block corresponding to the ciphertext data block; and

when the data length of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the ciphertext data block, divide the ciphertext data block into multiple sub ciphertext data blocks whose data length is less than or equal to the data processing length; for each sub ciphertext data block, sequentially decrypt the sub ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result, and perform an exclusive-or operation on the decryption result and operational data corresponding to the sub ciphertext data block, to obtain a sub plaintext data block corresponding to the sub ciphertext data block; and combine multiple obtained sub plaintext data blocks according to a sequence of the multiple sub ciphertext data blocks that are obtained by means of the dividing, to obtain the plaintext data block corresponding to the

ciphertext data block.

2925. The apparatus according to claim 2824, wherein, when the ciphertext data block is the first ciphertext data block among the multiple ciphertext data blocks, the operational data corresponding to the ciphertext data block is preset initial data; and

5 when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is the previous ciphertext data block; and if the data length of the
10 previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block.

3026. The apparatus according to claim 2824, wherein, when the sub ciphertext data
15 block is the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is the operational data corresponding to the ciphertext data block; and

when the sub ciphertext data block is not the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data
20 corresponding to the sub ciphertext data block is a previous sub ciphertext data block of the sub ciphertext data block.

3127. The apparatus according to claim 2824, wherein the decrypting unit is specifically configured to: when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the
25 ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, perform an exclusive-or operation on the previous ciphertext data block and a preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the decryption algorithm
30 corresponding to the previous ciphertext data block and by using the key corresponding to the

previous ciphertext data block, to obtain the key corresponding to the ciphertext data block;
and

5 if the data length of the previous ciphertext data block of the ciphertext data block is
greater than the data processing length of the decryption algorithm corresponding to the
previous ciphertext data block, perform an exclusive-or operation on a specified sub
ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext
data block and the preset parameter value corresponding to the previous ciphertext data block,
to obtain an operation result; and encrypt the operation result based on the encryption
algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext
10 data block and by using the key corresponding to the previous ciphertext data block, to obtain
the key corresponding to the ciphertext data block.

3228. The apparatus according to claim 29-25 or 3427, wherein the specified sub
plaintext data block among the multiple sub plaintext data blocks is specifically the first sub
plaintext data block among the multiple sub plaintext data blocks or the last sub plaintext data
15 block among the multiple sub plaintext data blocks.