(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112165443 B
(45)授权公告日 2023.06.02

(21)申请号 202010764000.4

(22)申请日 2020.08.01

(65)同一申请的已公布的文献号
申请公布号 CN 112165443 A

(43)申请公布日 2021.01.01

(73)专利权人 广东电网有限责任公司广州供电局
地址 510620 广东省广州市天河区天河南二路2号

(72)发明人 衷宇清 王浩 林泽兵 吴刚 王敏 陈立业

(74)专利代理机构 广州三辰专利事务所(普通合伙) 44227
专利代理师 陈惠珊

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/08(2006.01)
H04L 9/14(2006.01)

(56)对比文件
CN 104809407 A,2015.07.29
US 2018109508 A1,2018.04.19
CN 111259370 A,2020.06.09

审查员 蒋联娇

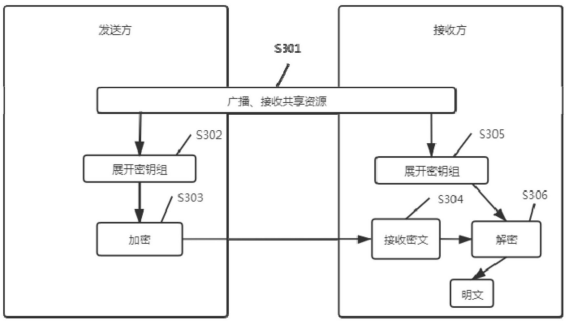
权利要求书3页 说明书4页 附图2页

(54)发明名称

一种多密钥信息加密解密方法、装置及存储介质

(57)摘要

本发明提供一种多密钥信息加密解密方法、装置及存储介质，通过固定长度的源密钥与盐函数进行合并，生成可选取的多个密钥组合，发送方、接收方均利用报文分段形成的序号与密钥组合中的密钥进行一一映射，对比传统单密钥加密方法，防止攻击方通过分析各数据报文段密文之间关系破解密钥，有效止损被破解密钥之后造成信息泄漏的安全风险，同时确保双方对信息加密、解密的唯一性，保障信息传递的稳定性。



CN 112165443 B

1.一种多密钥信息加密方法,包括待加密信息以及共享资源,所述共享资源包括固定长度的源密钥、盐函数,以及将所述源密钥与所述盐函数合并的展开算法,其特征在于,还包括以下步骤:

步骤S101:根据所述源密钥、盐函数、展开算法生成多个密钥组;

步骤S102:所述待加密信息根据报文进行分段,并生成分段序号;

步骤S103:所述待加密信息根据所述分段序号选取所述密钥组中相应的密钥进行加密;

其中,所述步骤S101具体包括:

步骤S111:源密钥即由发送方生成的一定长度的随机数,作为之后展开密钥组的初始值;

步骤S112:所述盐函数为一一映射函数,且其输入输出值均为正整数,进行运算时,所述盐函数根据所述分段序号对所述源密钥进行有序加盐处理,自变量N从1开始,直到累加至与所述分段序号对应的某一数值;

步骤S113:所述展开算法采取相加或固定位置插入方式将所述源密钥与盐函数合并,根据盐函数的自变量不同生成相应的合并值;

步骤S114:对所述合并值进行单向散列变换,得到一定长度的不可逆推的密钥,根据所述盐函数中自变量N的不同产生一一对应的密钥组,所述密钥组中密钥的序号为自变量N的值。

2.一种多密钥信息解密方法,包括待解密信息以及共享资源,所述共享资源包括固定长度的源密钥、盐函数,以及将所述源密钥与所述盐函数合并的展开算法,其特征在于,还包括以下步骤:

步骤S201:接收方根据与发送方相同的所述源密钥、盐函数、展开算法生成多个同步密钥组;

步骤S202:接收从发送方处广播的数据报文段;

步骤S203:所述待解密信息根据报文进行分段,并生成分段序号;

步骤S204:所述待解密信息根据所述分段序号选取所述同步密钥组中相应的密钥进行解密;

其中,所述步骤S201具体包括:

步骤S211:源密钥即由发送方生成的一定长度的随机数,作为之后展开密钥组的初始值;

步骤S212:所述盐函数为一一映射函数,且其输入输出值均为正整数,进行运算时,所述盐函数根据所述分段序号对所述源密钥进行有序加盐处理,自变量N从1开始,直到累加至与所述分段序号对应的某一数值;

步骤S213:所述展开算法采取相加或固定位置插入方式将所述源密钥与盐函数合并,根据盐函数的自变量不同生成相应的合并值;

步骤S214:对所述合并值进行单向散列变换,得到一定长度的不可逆推的密钥,根据所述盐函数中自变量N的不同产生一一对应的密钥组,所述密钥组中密钥的序号为自变量N的值。

3.一种多密钥信息传送方法,包括待传送信息以及共享资源,所述共享资源包括固定

长度的源密钥、盐函数，以及将所述源密钥与所述盐函数合并的展开算法，其特征在于，还包括以下步骤：

步骤S301：发送方广播所述共享资源，接收方接收并储存所述共享资源；

步骤S302：所述发送方、接收方同步根据所述源密钥、盐函数、展开算法生成多个密钥组；

步骤S303：所述发送方根据所述待传送信息的报文进行分段，并生成分段序号，所述待传送信息根据所述分段序号选取所述密钥组中相应的密钥进行加密；

步骤S304：所述发送方广播加密后的加密信息，所述接收方接收所述加密信息；

步骤S305：接收方根据所述共享资源，同步生成与发送方相同的第二密钥组；

步骤S306：所述接收方根据所述加密信息的报文分段序号，选取所述第二密钥组中的相应密钥进行解密，得到明文数据报文；

其中，所述步骤S302具体包括：

步骤S321：源密钥即由发送方生成的一定长度的随机数，作为之后展开密钥组的初始值；

步骤S322：所述盐函数为一一映射函数，且其输入输出值均为正整数，进行运算时，所述盐函数根据所述分段序号对所述源密钥进行有序加盐处理，自变量N从1开始，直到累加至与所述分段序号对应的某一数值；

步骤S323：所述展开算法采取相加或固定位置插入方式将所述源密钥与盐函数合并，根据盐函数的自变量不同生成相应的合并值；

步骤S324：对所述合并值进行单向散列变换，得到一定长度的不可逆推的密钥，根据所述盐函数中自变量N的不同产生一一对应的密钥组，所述密钥组中密钥的序号为自变量N的值；

所述步骤S305具体包括：

步骤S351：源密钥即由发送方生成的一定长度的随机数，作为之后展开密钥组的初始值；

步骤S352：所述盐函数为一一映射函数，且其输入输出值均为正整数，进行运算时，所述盐函数根据所述分段序号对所述源密钥进行有序加盐处理，自变量N从1开始，直到累加至与所述分段序号对应的某一数值；

步骤S353：所述展开算法采取相加或固定位置插入方式将所述源密钥与盐函数合并，根据盐函数的自变量不同生成相应的合并值；

步骤S354：对所述合并值进行单向散列变换，得到一定长度的不可逆推的密钥，根据盐函数中自变量N的不同产生一一对应的第二密钥组，所述第二密钥组中密钥的序号为自变量N的值。

4.一种信息加密装置，其特征在于，所述装置包括存储器、处理器及发送器，所述存储器上存储有可在所述处理器上运行的多密钥信息加密程序，所述多密钥信息加密程序被所述处理器执行时实现如权利要求1所述的多密钥信息加密方法的步骤，所述发送器发送所述共享资源及加密后的密文。

5.一种信息解密装置，其特征在于，所述装置包括存储器、处理器及接收器，所述存储器上存储有可在所述处理器上运行的多密钥信息解密程序，所述接收器接收所述共享资源

及待解密信息,所述多密钥信息解密程序被所述处理器执行时实现如权利要求2中所述的多密钥信息解密方法的步骤,所述待解密信息经所述多密钥信息解密方法最终得到明文数据报文。

6.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有机器可运行指令,所述机器可运行指令在被处理器调用和运行时,所述机器可运行指令促使所述处理器运行权利要求1至3任一项所述的方法。

一种多密钥信息加密解密方法、装置及存储介质

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种多密钥信息加密解密方法、装置及存储介质。

背景技术

[0002] 信息加密技术是为了在不安全的传输环境中实现信息的安全传输，但是加密后攻击方同样有各种方法截获并破解传递的信息。不公开的加密算法容易出现各种漏洞并不能保证安全，所以当前的加密算法大多都是公开的，当前的信息加密的安全性主要取决于密钥的安全。

[0003] 密码破解技术就是在不知道密钥和明文的情况下，通过对密文进行分析取得密钥，并最终恢复明文。当前数据加密主要靠单密钥进行加密，如果攻击方采用各种方法对其进行破解之后，接下来所有的信息对攻击方来说都是透明的。

[0004] 当前国内外对密码学方面主要研究更加复杂和安全的加密算法，由以往的DES到3DES再到AES。虽然加密算法的安全性越来越高，但是加密和破解是一对相互对立共同发展的过程，以往被人认为极其安全的加密算法在运算能力日益强大的计算机面前也逐一被破解，因此急需开发更为安全的信息加密解密方法。

发明内容

[0005] 鉴于现有技术存在的上述不足，本发明提供一种多秘钥信息加密解密方法、装置及存储介质。

[0006] 为达到上述信息安全加密，本发明的采用如下技术方案：

[0007] 一种多密钥信息加密方法，包括待加密信息以及共享资源，所述共享资源包括固定长度的源密钥、盐函数，以及将所述源密钥与所述盐函数合并的展开算法，还包括以下步骤：

[0008] 步骤S101:根据所述源密钥、盐函数、展开算法生成多个密钥组；

[0009] 步骤S102:所述待加密信息根据报文进行分段，并生成第一分段序号；

[0010] 步骤S103:所述待加密信息根据所述第一分段序号选取所述密钥组中相应的密钥进行加密。

[0011] 进一步地，所述一种多密钥信息加密方法还包括步骤S104:所述盐函数为一一映射函数，且其输入输出值均为正整数，进行运算时，所述盐函数根据所述第一分段序号对所述源密钥进行有序加盐处理，自变量N从1开始，直到累加至与所述第一分段序号对应的某一数值。

[0012] 进一步地，所述一种多密钥信息加密方法还包括步骤S105:所述展开算法采取相加或固定位置插入方式将所述源密钥与盐函数合并，根据盐函数的自变量不同生成相应的合并值。

[0013] 进一步地，所述一种多密钥信息加密方法还包括步骤S106:对所述合并值进行单

向散列变换，得到一定长度的不可逆推的密钥。

[0014] 为达到上述信息安全解密，本发明还提供如下技术方案：

[0015] 一种多密钥信息解密方法，包括待解密信息以及共享资源，所述共享资源包括固定长度的源密钥、盐函数，以及将所述源密钥与所述盐函数合并的展开算法，还包括以下步骤：

[0016] 步骤S201：接收方根据与发送方相同的所述源密钥、盐函数、展开算法生成多个同步密钥组；

[0017] 步骤S202：接收从发送方处广播的数据报文段；

[0018] 步骤S203：所述待解密信息根据报文进行分段，并生成第二分段序号；

[0019] 步骤S204：所述待解密信息根据所述第二分段序号选取所述密钥组中相应的密钥进行解密。

[0020] 为达到上述信息安全传送，本发明还提供如下技术方案：

[0021] 一种多密钥信息传送方法，包括待传送信息以及共享资源，所述共享资源包括固定长度的源密钥、盐函数，以及将所述源密钥与所述盐函数合并的展开算法，还包括以下步骤：

[0022] 步骤S301：发送方广播所述共享资源，接收方接收并储存所述共享资源；

[0023] 步骤S302：所述发送方、接收方同步根据所述源密钥、盐函数、展开算法生成多个密钥组；

[0024] 步骤S303：所述发送方根据所述待传送信息的报文进行分段，并生成分段序号，所述待传送信息根据所述分段序号选取所述密钥组中相应的密钥进行加密；

[0025] 步骤S304：所述发送方广播加密后的加密信息，所述接收方接收所述加密信息；

[0026] 步骤S305：接收方根据所述共享资源，同步生成与接收方相同的第二密钥组；

[0027] 步骤S306：所述接收方根据所述加密信息的报文分段序号，选取所述第二密钥组中的相应密钥进行解密，得到明文数据报文。

[0028] 为提供上述信息进行加密的装置，本发明还提供如下技术方案：

[0029] 一种信息加密装置，所述装置包括存储器、处理器及发送器，所述存储器上存储有可在所述处理器上运行的多密钥信息加密程序，所述多密钥信息加密程序被所述处理器执行时实现如上述记载的多密钥信息加密方法的步骤，所述发送器发送所述共享资源及加密后的密文。

[0030] 为提供上述信息进行解密的装置，本发明还提供如下技术方案：

[0031] 一种信息解密装置，所述装置包括存储器、处理器及接收器，所述存储器上存储有可在所述处理器上运行的多密钥信息解密程序，所述接收器接收所述共享资源及待解密信息，所述多密钥信息解密程序被所述处理器执行时实现如上述记载的多密钥信息解密方法的步骤，所述待解密信息经所述多密钥信息解密方法最终得到明文数据报文。

[0032] 为提供上述方法可执行的计算机可读存储介质，本发明还提供如下技术方案：

[0033] 一种计算机可读存储介质，所述计算机可读存储介质存储有机器可运行指令，所述可运行指令在被处理器调用和运行时，所述可运行指令促使所述处理器运行上述任一项加密解密及传送方法。

[0034] 本发明的一种多密钥信息加密解密方法、装置及存储介质具有以下有益效果：

[0035] 1、通过固定长度的源密钥与盐函数进行合并，生成多个可选取的多密钥组合，对比传统单密钥加密方法，防止攻击方通过分析各数据报文段密文之间关系破解密钥，有效止损被破解密钥之后造成信息泄漏的安全风险；

[0036] 2、发送方、接收方均利用报文分段形成的序号，并通过序号与密钥一一映射关系，确保双方对信息加密、解密的唯一性，保障信息传递的稳定性；

[0037] 3、对密钥进行单向散列变换，密钥组中的各个密钥相互之间无法推出，进一步提高信息传输时的安全和稳定。

附图说明

[0038] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，并不构成对本发明的不当限定，在附图中：

[0039] 图1为本发明多密钥信息加密流程示意图；

[0040] 图2为本发明展开密钥组过程流程示意图；

[0041] 图3为本发明多密钥信息解密流程示意图；

[0042] 图4为本发明多密钥信息传送流程示意图。

具体实施方式

[0043] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0044] 如图1所示为本发明一种多密钥信息加密方法，包括待加密信息以及共享资源，所述共享资源包括固定长度的源密钥、盐函数，以及将所述源密钥与所述盐函数合并的展开算法，还包括以下步骤：

[0045] 步骤S101:根据所述源密钥、盐函数、展开算法生成多个密钥组；

[0046] 步骤S102:所述待加密信息根据报文进行分段，并生成第一分段序号；

[0047] 步骤S103:所述待加密信息根据所述第一分段序号选取所述密钥组中相应的密钥进行加密。

[0048] 如图2所示为步骤S101具体展开密钥组过程，其中具体步骤如下：

[0049] 步骤S111:源密钥即由发送方生成的一定长度的随机数，作为之后展开密钥组的初始值。

[0050] 步骤S112:盐函数为一种输入和输出皆为正整数的一对一关系映射函数，其输入的值确定了唯一的输出值，且根据输出值仅能找到唯一的输入值与其对应，盐函数负责对源密钥进行有序的加盐处理。进行运算时，自变量N从1开始，直到累加至某一数值。

[0051] 步骤S113:展开算法是将固定的源密钥与盐函数合并形成合并值，需要注意的是，必须保证生成的合并值与盐函数的自变量N同样为一对一关系映射，该合并过程可以采取相加和固定位置插入等方式。

[0052] 步骤S114:合并值是将源密钥和盐函数按照展开算法进行运算组合后的结果。根据盐函数的自变量不同生成相应的合并值。

[0053] 步骤S115:对合并值进行单向散列变换,得到一定长度的不可逆推的密钥。

[0054] 步骤S116:最终根据自变量N的不同产生一一对应的密钥组,其中密钥的序号为生成步骤中其盐函数F(N)中的自变量N的值,并且密钥组中的密钥因为经过了单向散列变换所以互相之间无法推出。

[0055] 如图3所示为本发明多密钥信息解密步骤,步骤S201:接收方根据与发送方相同的所述源密钥、盐函数、展开算法生成多个同步密钥组;步骤S202:接收从发送方处广播的数据报文段;步骤S203:所述待解密信息根据报文进行分段,并生成第二分段序号;步骤S204:所述待解密信息根据所述第二分段序号选取所述密钥组中相应的密钥进行解密。

[0056] 如图4所示为本发明一种多密钥信息传送方法,包括待传送信息以及共享资源,所述共享资源包括固定长度的源密钥、盐函数,以及将所述源密钥与所述盐函数合并的展开算法,还包括以下步骤:

[0057] 步骤S301:发送方广播所述共享资源,接收方接收并储存所述共享资源;

[0058] 步骤S302:所述发送方、接收方同步根据所述源密钥、盐函数、展开算法生成多个第一密钥组;

[0059] 步骤S303:所述发送方根据所述待传送信息的报文进行分段,并生成分段序号,所述待传送信息根据所述分段序号选取所述密钥组中相应的密钥进行加密;

[0060] 步骤S304:所述发送方广播加密后的加密信息,所述接收方接收所述加密信息;

[0061] 步骤S305:接收方根据所述共享资源,同步生成与接收方相同的第二密钥组;

[0062] 步骤S306:所述接收方根据所述加密信息的报文分段序号,选取所述第二密钥组中的相应密钥进行解密,得到明文数据报文。

[0063] 本发明还提供一种信息加密装置,所述装置包括存储器、处理器及发送器,所述存储器上存储有可在所述处理器上运行的多密钥信息加密程序,所述多密钥信息加密程序被所述处理器执行时实现如上述记载的多密钥信息加密方法的步骤,所述发送器发送所述共享资源及加密后的密文。

[0064] 本发明还提供一种信息解密装置,所述装置包括存储器、处理器及接收器,所述存储器上存储有可在所述处理器上运行的多密钥信息解密程序,所述接收器接收所述共享资源及待解密信息,所述多密钥信息解密程序被所述处理器执行时实现如上述记载的多密钥信息解密方法的步骤,所述待解密信息经所述多密钥信息解密方法最终得到明文数据报文。

[0065] 本发明还提供一种计算机可读存储介质,所述计算机可读存储介质存储有机器可运行指令,所述可运行指令在被处理器调用和运行时,所述可运行指令促使所述处理器运行上述任一项加密解密及传送方法。

[0066] 以上所述,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本领域技术的技术人员在本发明公开的技术范围内,可轻易想到的变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以所述权利要求的保护范围为准。

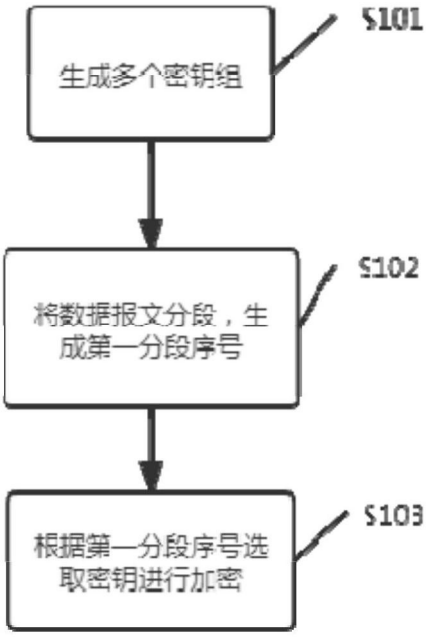

S101
生成多个密钥组
S102
将数据报文分段，生成第一分段序号
S103
根据第一分段序号选取密钥进行加密

图1

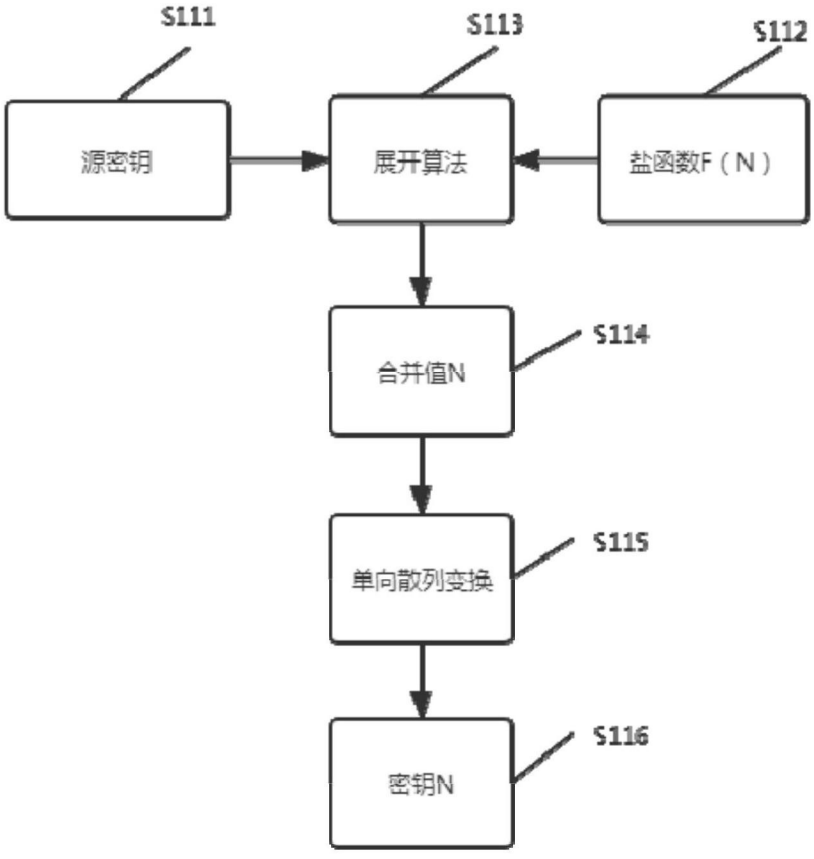

S111
源密钥
S113
展开算法
S112
盐函数F（N）
S114
合并值N
S115
单向散列变换
S116
密钥N

图2

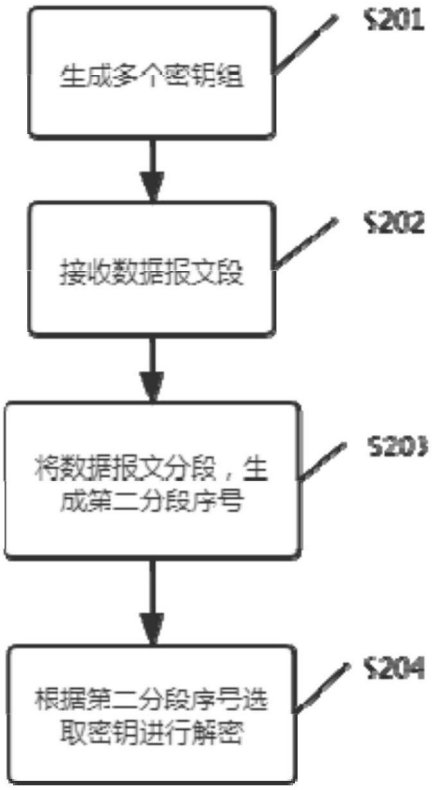

S201
生成多个密钥组
S202
接收数据报文段
S203
将数据报文分段，生成第二分段序号
S204
根据第二分段序号选取密钥进行解密

图3

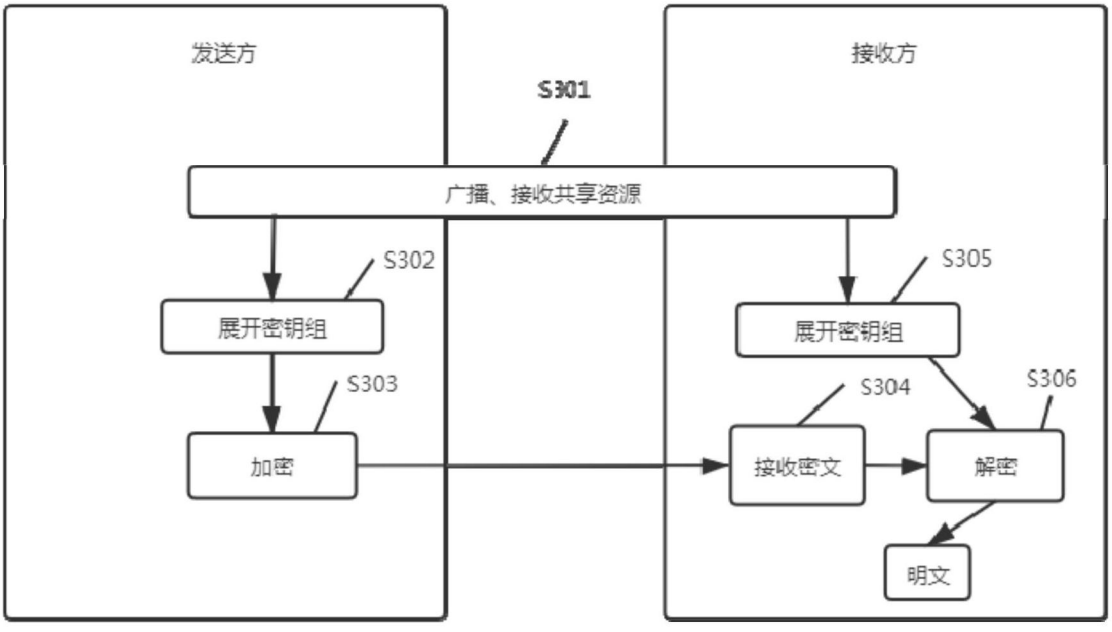

发送方
接收方
S301
广播、接收共享资源
S302
展开密钥组
S303
加密
S305
展开密钥组
S304
接收密文
S306
解密
明文

图4