(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111147230 A
(43)申请公布日 2020.05.12

(21)申请号 201911414897.1

(22)申请日 2019.12.31

(71)申请人 东方红卫星移动通信有限公司
地址 401135 重庆市渝北区龙兴镇两江大道618号

(72)发明人 覃丽娟

(74)专利代理机构 重庆启恒腾元专利代理事务所(普通合伙) 50232
代理人 万建

(51)Int.Cl.
H04L 9/06(2006.01)
H04B 7/185(2006.01)

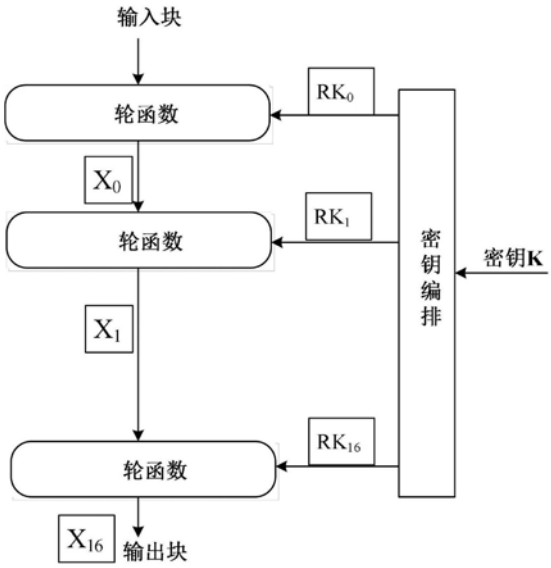
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种基于低轨卫星物联网轻量级星间的信息加密传输方法

(57)摘要

本发明公开了一种基于低轨卫星物联网轻量级星间的信息加密传输方法,应用于低轨卫星之间以及中继站与低轨卫星之间,单次传输过程包括发送端和接收端,主要包括以下步骤:S1:发送端获取明文分组;S2:在发送端,明文分组执行加密算法,经过轮函数的多轮运算得到密文,并将密文发送至接收端;S3:接收端接受密文,在接收端密文经过多轮轮函数的逆运算得到明文分组,完成解密。本发明具有结构简单、易于实现、算法安全强度高,适用广的优点。



CN 111147230 A

1.一种基于低轨卫星物联网轻量级星间的信息加密传输方法，其特征在于：应用于低轨卫星之间以及中继站与低轨卫星之间，单次传输过程包括发送端和接收端，主要包括以下步骤：

S1:发送端获取明文分组；

S2:在发送端，明文分组执行加密算法，经过轮函数的多轮运算得到密文，并将密文发送至接收端；

S3:接收端接受密文，在接收端密文经过多轮轮函数的逆运算得到明文分组，完成解密。

2.根据权利要求1所述的一种基于低轨卫星物联网轻量级星间的信息加密传输方法，其特征在于，步骤S1到步骤S3中的具体运算步骤如下:

A1:发送端执行密码扩展算法，将128、192和256bit的主密钥$K_{(128)}$、$K_{(192)}$和$K_{(256)}$扩展生成轮函数所需的白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}；

A2:发送端将明文分组P与256bit的白化密钥RK_0异或得到X_0；

A3:对步骤A2得到的结果进行轮函数运算，轮函数包括非线性变换S盒替换SB、线性变换LT以及轮密钥异或运算AK；

A4:发送端生成密文C，$C=X_{16}$；

A5:接收端执行密码扩展算法，将128、192和256比特主密钥$K_{(128)}$、$K_{(192)}$和$K_{(256)}$扩展生成轮函数所需的白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}；

A6:接收端收到密文C,与第16轮的轮密钥RK_{16}异或，得到X_0'；

A7:对步骤A6进行轮函数逆运算，轮函数逆运算包括非线性变换的S盒替换的逆运算SB^{-1}、线性变换的逆运算LT^{-1}以及轮密钥异或运算的逆运算AK^{-1}；

A8:接收端解密获得明文P，$P=X_{16}$。

3.根据权利要求1所述的一种基于低轨卫星物联网轻量级星间的信息加密传输方法，其特征在于，在加密阶段进行轮函数运算以及解密阶段的轮函数逆运算的轮数均为16轮。

4.根据权利要求2所述的一种基于低轨卫星物联网轻量级星间的信息加密传输方法，其特征在于，在步骤A1和A5中，执行密码扩展算法的步骤包括

B1:将主密钥变换成256bit的种子密钥SK；

B2:利用非线性反馈移位寄存器结构，将种子密钥SK扩展生成白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}。

5.根据权利要求4所述的一种基于低轨卫星物联网轻量级星间的信息加密传输方法，步骤B1中，在进行种子秘钥变化时，采用以下公式:

$$SK=\begin{cases} K_{(128)}\|K_{(128)} & \text{当主密钥为128bit} \\ K_{(192)}\|K_{(192)} & \text{当主密钥为192bit} \\ K_{(256)} & \text{当主密钥为256bit} \end{cases}$$

6.根据权利要求5所述的一种基于低轨卫星物联网轻量级星间的信息加密传输方法，其特征在于，步骤B2中，在生成白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}时，将256bit种子密钥

SK分为8个32bit的字，记为SK→(k-4,k-3,k-2,k-1,k0,k1,k2,k3)。根据算分轮数长度16，利用以下方式生成ki：

$$k_i=\begin{cases}k_i & \text{当i<4}\\ P_0\left(SW\left(k_{i-8}\oplus k_{i-6}\oplus k_{i-3}\oplus k_{i-1}\oplus RC_{i/4}\right)\right) & \text{当}i\%4=0,i\geq 4\\ P_0\left(SW\left(k_{i-8}\oplus k_{i-6}\oplus k_{i-3}\oplus k_{i-1}\right)\right) & \text{当}i\%4\neq 0,i\geq 4\end{cases}$$

7.根据权利要求6所述的一种基于低轨卫星物联网轻量级星间的信息加密传输方法，其特征在于，步骤A2-A4中对于明文分组P，加密算法获得密文C运算如下：

$$X_0=P\oplus RK_0$$

$X_i=AKoLToSB(X_{i-1})$，i＝1，...Nr

$C=X_{16}$

其中，RK_0为白化密钥，RK_1、RK_2、…、RK_{16}为轮密钥，每个轮密钥为256bit，由主密码通过密钥扩展算法生成。第i轮的输入为X_{i-1}，经过SB，LT，AK后的状态值分别标志为Y_{i-1}，W_{i-1}和X_i，即：

$Y_{i-1}=SB(X_{i-1})$

$W_{i-1}=LT(Y_{i-1})$

$X_i=AK(W_{i-1})$。

8.根据权利要求7所述的一种基于低轨卫星物联网轻量级星间的信息加密传输方法，其特征在于，步骤A6-A8中，在进行解密获得明文P的运算如下：

$$X_0=C\oplus RK_{16}$$

$X_i=AK^{-1}oLT^{-1}oSB^{-1}(X_{i-1})$，i＝1，...，16

$P=X_{16}$

令经过逆运算LT^{-1}、SB^{-1}和AK^{-1}后的状态值分别记为Y_{i-1}，W_{i-1}和X_i，即：

$Y_{i-1}=LT^{-1}(X_{i-1})$

$W_{i-1}=SB^{-1}(Y_{i-1})$

$X_i=AK^{-1}(W_{i-1})$。

一种基于低轨卫星物联网轻量级星间的信息加密传输方法

技术领域

[0001] 本发明涉及空间互联网信息安全技术领域，尤其涉及一种基于低轨卫星物联网轻量级星间的信息加密传输方法。

背景技术

[0002] 随着卫星通信的发展，卫星物联网信息安全性的问题愈来愈显得突出，现有的空间网络安全方案存在缺乏对星际骨干网组网安全的考虑、缺乏对星际骨干网的节点特别是中继站的双向认证以及密钥管理和认证效率不高，密码计算复杂度较高等问题。

[0003] 卫星物联网的通信安全通常需要加扰技术保障卫星通信数据的机密性，目前加扰技术主要基于分组密码算法的加密，分组密码算法作为一类基础的密码算法，不仅用于保护网络通信的私密性，防止敏感信息被窃听，被泄露；也是设计消息认证码的关键技术，用于保证消息的完整性，进行消息源认证，防止消息被篡改等，自第一个分组密码算法标准DES提出以来，经过近四十年的发展，在各个国际密码组织的支持下，分组密码的分析与设计发展迅速，美国国家标准技术所(NIST)推出了AES算法代替DES算法，随后，欧洲、日本等发达国家都推出了一些分组密码算法，建议在一些重要领域作为标准使用，AES算法广泛的应用于计算机网络通信，其安全性受到国际密码领域的广泛研究与国际社会的普遍关注。

[0004] 尽管目前的安全性评估结果显示AES算法还未发现安全隐患，但是由于物联网等相关技术的进步，人们发现传统的加密算法已经在资源受限的环境中无法得到广泛的应用特别是卫星，为解决现有的空间网络安全方案密码计算复杂度较高的问题，对资源消耗较少、实现效率较高的轻量级密码算法设计得到了广泛的关注。

发明内容

[0005] 针对上述现有技术的不足，本专利申请所要解决的技术问题是：如何提供一种结构简单、易于实现、算法安全强度高，适用广的基于低轨卫星物联网轻量级星间的信息加密传输方法。

[0006] 为了实现上述目的，本发明采用了如下技术方案：

[0007] 一种基于低轨卫星物联网轻量级星间的信息加密传输方法，应用于低轨卫星之间以及中继站与低轨卫星之间，单次传输过程包括发送端和接收端，主要包括以下步骤：

[0008] S1:发送端获取明文分组；

[0009] S2:在发送端，明文分组执行加密算法，经过轮函数的多轮运算得到密文，并将密文发送至接收端；

[0010] S3:接收端接受密文，在接收端密文经过多轮轮函数的逆运算得到明文分组，完成解密。

[0011] 优化的，步骤S1到步骤S3中的具体运算步骤如下:

[0012] A1:发送端执行密码扩展算法，将128、192和256bit的主密钥$K_{(128)}$、$K_{(192)}$和$K_{(256)}$扩展生成轮函数所需的白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}；

[0013] A2:发送端将明文分组P与256bit的白化密钥RK_0异或得到X_0;

[0014] A3:对步骤A2得到的结果进行轮函数运算,轮函数包括非线性变换S盒替换SB、线性变换LT以及轮密钥异或运算AK;

[0015] A4:发送端生成密文C,C=X_{16};

[0016] A5:接收端执行密码扩展算法,将128、192和256比特主密钥$K_{(128)}$、$K_{(192)}$和$K_{(256)}$扩展生成轮函数所需的白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16};

[0017] A6:接收端收到密文C,与第16轮的轮密钥RK_{16}异或,得到X_0';

[0018] A7:对步骤A6进行轮函数逆运算,轮函数逆运算包括非线性变换的S盒替换的逆运算SB^{-1}、线性变换的逆运算LT^{-1}以及轮密钥异或运算的逆运算AK^{-1};

[0019] A8:接收端解密获得明文P,P=X_{16}。

[0020] 优化的,在加密阶段进行轮函数运算以及解密阶段的轮函数逆运算的轮数均为16轮。

[0021] 优化的,在步骤A1和A5中,执行密码扩展算法的步骤包括

[0022] B1:将主密钥变换成256bit的种子密钥SK;

[0023] B2:利用非线性反馈移位寄存器结构,将种子密钥SK扩展生成白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}。

[0024] 优化的,步骤B1中,在进行种子秘钥变化时,采用以下公式:

[0025] $$SK=\begin{cases} K_{(128)}\|K_{(128)} & \text{当主密钥为128bit} \\ K_{(192)}\|K_{(192)} & \text{当主密钥为192bit} \\ K_{(256)} & \text{当主密钥为256bit} \end{cases}$$

[0026] 优化的,步骤B2中,在生成白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}时,将256bit种子密钥SK分为8个32bit的字,记为SK→(k_{-4},k_{-3},k_{-2},k_{-1},k_0,k_1,k_2,k_3)。根据算分轮数长度16,利用以下方式生成k_i:

[0027] $$k_i=\begin{cases} k_i & \text{当i<4} \\ P_0\left(SW\left(k_{i-8}\oplus k_{i-6}\oplus k_{i-3}\oplus k_{i-1}\oplus RC_{i/4}\right)\right) & \text{当}i\%4=0, i\geq 4 \\ P_0\left(SW\left(k_{i-8}\oplus k_{i-6}\oplus k_{i-3}\oplus k_{i-1}\right)\right) & \text{当}i\%4\neq 0, i\geq 4 \end{cases}$$

[0028] 优化的,步骤A2-A4中对于明文分组P,加密算法获得密文C运算如下:

[0029] $$X_0=P\oplus RK_0$$

[0030] X_i=AKoLToSB(X_{i-1}),i=1,...Nr

[0031] C=X_{16}

[0032] 其中,RK_0为白化密钥,RK_1、RK_2、…、RK_{16}为轮密钥,每个轮密钥为256bit,由主密码通过密钥扩展算法生成。第i轮的输入为X_{i-1},经过SB,LT,AK后的状态值分别标志为Y_{i-1},W_{i-1}和X_i,即:

[0033] Y_{i-1}=SB(X_{i-1})

[0034] W_{i-1}=LT(Y_{i-1})

[0035] $X_i = AK(W_{i-1})$。

[0036] 优化的，步骤A6-A8中，在进行解密获得明文P的运算如下：

[0037] $$X_0 = C \oplus RK_{16}$$

[0038] $X_i = AK^{-1} \circ LT^{-1} \circ SB^{-1}(X_{i-1})$，i＝1，...，16

[0039] $P = X_{16}$

[0040] 令经过逆运算LT^{-1}、SB^{-1}和AK^{-1}后的状态值分别记为Y_{i-1}，W_{i-1}和X_i，即：

[0041] $Y_{i-1} = LT^{-1}(X_{i-1})$

[0042] $W_{i-1} = SB^{-1}(Y_{i-1})$

[0043] $X_i = AK^{-1}(W_{i-1})$。

[0044] 有益效果：

[0045] (1)本发明的一种低轨卫星物联网轻量级星上密码设计方法，算法整体结构上采用SPN结构，该结构包括混淆层和扩散层，其中混淆层由非线性的S盒替换实现，扩散层为可逆的线性变换分组。该结构用混淆层和扩散层构造轮函数，并迭代轮函数多次，从而增强密码的混淆性与扩散性，使密码的输出和输入之间的依赖关系更加复杂。

[0046] (2)本发明的一种低轨卫星物联网轻量级星上密码设计方法，在扩散层方面，使用两层P置换来实现快速线性扩散。两层P置换的结合增强了算法的线性扩散强度。P置换参数的选择综合考虑了异或项数、移位间距、逆置换P^{-1}项数等情况。

[0047] (3)本发明的一种低轨卫星物联网轻量级星上密码设计方法，密钥生成算法采用基于字的非线性反馈移位寄存器。非线性反馈函数由抽头项的异或、非线性函数S盒替换和线性置换P_0构成，能够有效抵抗相关密钥攻击。

附图说明：

[0048] 图1为本发明公开的基于低轨卫星物联网轻量级星间的信息加密传输方法的步骤图。

[0049] 图2为图1中所述基于低轨卫星物联网轻量级星间的信息加密传输方法的轮函数运算框架示意图。

具体实施方式

[0050] 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。

[0051] 参照图1-图2，一种基于低轨卫星物联网轻量级星间的信息加密传输方法，应用于低轨卫星之间以及中继站与低轨卫星之间，单次传输过程包括发送端和接收端，主要包括以下步骤：

[0052] S1:发送端获取明文分组；

[0053] S2:在发送端，明文分组执行加密算法，经过轮函数的多轮运算得到密文，并将密文发送至接收端；

[0054] S3:接收端接受密文，在接收端密文经过多轮轮函数的逆运算得到明文分组，完成解密。

[0055] 本实施例中，步骤S1到步骤S3中的具体运算步骤如下：

[0056] A1：发送端执行密码扩展算法，将128、192和256bit的主密钥$K_{(128)}$、$K_{(192)}$和$K_{(256)}$扩展生成轮函数所需的白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}；

[0057] A2：发送端将明文分组P与256bit的白化密钥RK_0异或得到X_0；

[0058] A3：对步骤A2得到的结果进行轮函数运算，轮函数包括非线性变换S盒替换SB、线性变换LT以及轮密钥异或运算AK；

[0059] A4：发送端生成密文C，C＝X_{16}；

[0060] A5：接收端执行密码扩展算法，将128、192和256比特主密钥$K_{(128)}$、$K_{(192)}$和$K_{(256)}$扩展生成轮函数所需的白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}；

[0061] A6：接收端收到密文C，与第16轮的轮密钥RK_{16}异或，得到X_0'；

[0062] A7：对步骤A6进行轮函数逆运算，轮函数逆运算包括非线性变换的S盒替换的逆运算SB^{-1}、线性变换的逆运算LT^{-1}以及轮密钥异或运算的逆运算AK^{-1}；

[0063] A8：接收端解密获得明文P，P＝X_{16}。

[0064] 本实施例中，在加密阶段进行轮函数运算以及解密阶段的轮函数逆运算的轮数均为16轮。

[0065] 本实施例中，在步骤A1和A5中，执行密码扩展算法的步骤包括

[0066] B1：将主密钥变换成256bit的种子密钥SK；

[0067] B2：利用非线性反馈移位寄存器结构，将种子密钥SK扩展生成白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}。

[0068] 本实施例中，步骤B1中，在进行种子秘钥变化时，采用以下公式：

[0069] $$SK=\begin{cases}K_{(128)}\|K_{(128)} & \text{当主密钥为128bit}\\ K_{(192)}\|K_{(192)} & \text{当主密钥为192bit}\\ K_{(256)} & \text{当主密钥为256bit}\end{cases}$$

[0070] 本实施例中，步骤B2中，在生成白化密钥RK_0和轮密钥RK_1、RK_2、…、RK_{16}时，将256bit种子密钥SK分为8个32bit的字，记为SK→$(k_{-4},k_{-3},k_{-2},k_{-1},k_0,k_1,k_2,k_3)$。根据算分轮数长度16，利用以下方式生成$k_i$：

[0071] $$k_i=\begin{cases}k_i & \text{当i<4}\\ P_0\left(SW\left(k_{i-8}\oplus k_{i-6}\oplus k_{i-3}\oplus k_{i-1}\oplus RC_{i/4}\right)\right) & \text{当}i\%4=0,i\geq 4\\ P_0\left(SW\left(k_{i-8}\oplus k_{i-6}\oplus k_{i-3}\oplus k_{i-1}\right)\right) & \text{当}i\%4\neq 0,i\geq 4\end{cases}$$

[0072] 优化的，步骤A2-A4中对于明文分组P，加密算法获得密文C运算如下：

[0073] $$X_0=P\oplus RK_0$$

[0074] X_i＝AKoLToSB(X_{i-1})，i＝1，...Nr

[0075] C＝X_{16}

[0076] 其中，RK_0为白化密钥，RK_1、RK_2、…、RK_{16}为轮密钥，每个轮密钥为256bit，由主密码通过密钥扩展算法生成。第i轮的输入为X_{i-1}，经过SB，LT，AK后的状态值分别标志为Y_{i-1}，W_{i-1}

和X_i，即：

[0077] $Y_{i-1}=SB(X_{i-1})$

[0078] $W_{i-1}=LT(Y_{i-1})$

[0079] $X_i=AK(W_{i-1})$。

[0080] 本实施例中，步骤A6-A8中，在进行解密获得明文P的运算如下：

[0081] $$X_0 = C \oplus RK_{16}$$

[0082] $X_i=AK^{-1}oLT^{-1}oSB^{-1}(X_{i-1})$，i＝1，...，16

[0083] $P=X_{16}$

[0084] 令经过逆运算LT^{-1}、SB^{-1}和AK^{-1}后的状态值分别记为Y_{i-1}，W_{i-1}和X_i，即：

[0085] $Y_{i-1}=LT^{-1}(X_{i-1})$

[0086] $W_{i-1}=SB^{-1}(Y_{i-1})$

[0087] $X_i=AK^{-1}(W_{i-1})$。

[0088] 有益效果：

[0089] (1)本发明的一种低轨卫星物联网轻量级星上密码设计方法，算法整体结构上采用SPN结构，该结构包括混淆层和扩散层，其中混淆层由非线性的S盒替换实现，扩散层为可逆的线性变换分组。该结构用混淆层和扩散层构造轮函数，并迭代轮函数多次，从而增强密码的混淆性与扩散性，使密码的输出和输入之间的依赖关系更加复杂。

[0090] (2)本发明的一种低轨卫星物联网轻量级星上密码设计方法，在扩散层方面，使用两层P置换来实现快速线性扩散。两层P置换的结合增强了算法的线性扩散强度。P置换参数的选择综合考虑了异或项数、移位间距、逆置换P^{-1}项数等情况。

[0091] (3)本发明的一种低轨卫星物联网轻量级星上密码设计方法，密钥生成算法采用基于字的非线性反馈移位寄存器。非线性反馈函数由抽头项的异或、非线性函数S盒替换和线性置换P_0构成，能够有效抵抗相关密钥攻击。

[0092] 本方案针对现有的空间网络安全方案存在密码计算复杂度较高等问题，提出一种轻量级星上密码设计方法，该算法采用代替置换网络(SPN)结构，混淆层由非线性的S盒替换实现，采用域$\left(F_{2^8}\right)$上的模逆运算构造S盒，以便获得好的差分、线性分布；扩散层由可逆的线性变换分组实现，使用两层P置换来实现快速线性扩散，第一层P置换P_0作用于每个64bit的字，打破了状态中的字节结构，使得算法能够抵抗积分攻击、碰撞攻击、中间相遇攻击等基于字节属性的积分类攻击；第二层P置换P_1作用于整个256bit的状态。S盒和P置换的结合，使算法能够抵抗差分攻击、线性攻击、不可能差分攻击等密码学攻击方法，在降低密码计算复杂度的同时，提高低轨卫星物联网通信的安全性。

[0093] 以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，根据本发明的技术方案及其发明构思加以等同替换或改变，都应涵盖在本发明的保护范围之内。

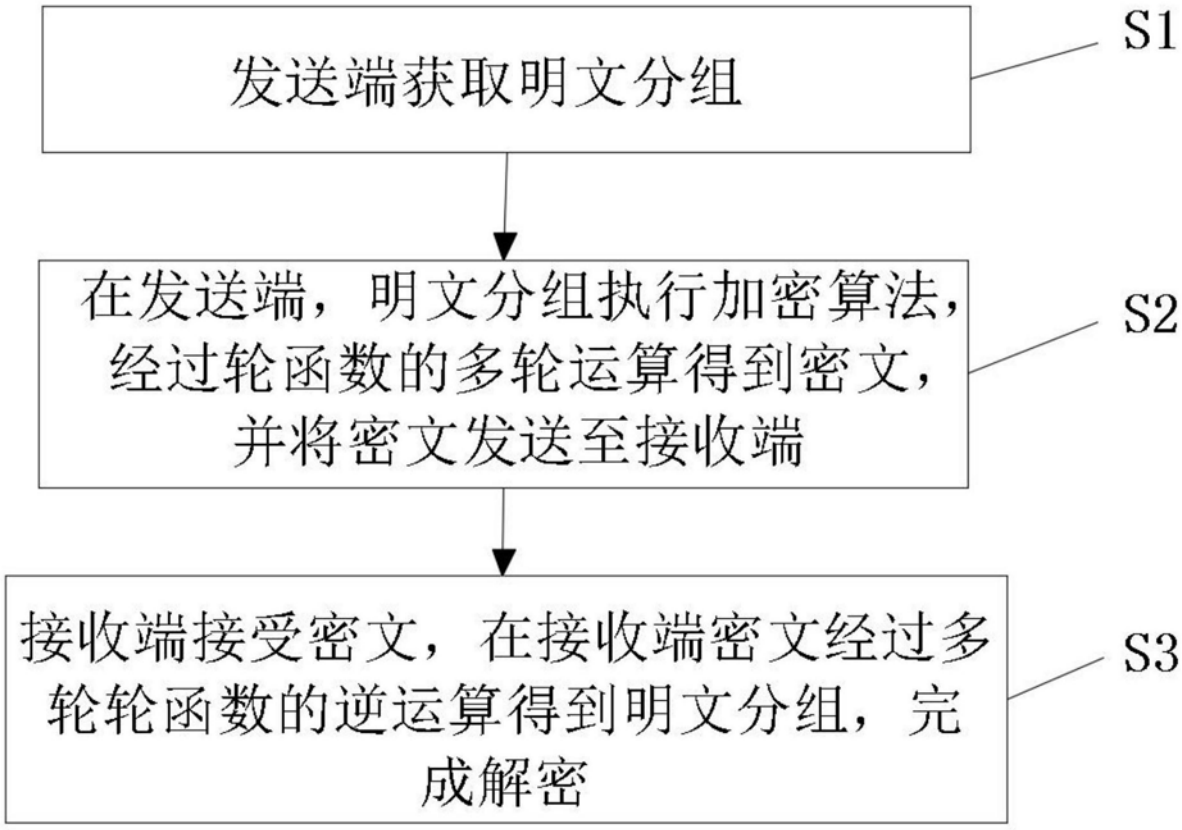

发送端获取明文分组
S1
在发送端，明文分组执行加密算法，经过轮函数的多轮运算得到密文，并将密文发送至接收端
S2
接收端接受密文，在接收端密文经过多轮轮函数的逆运算得到明文分组，完成解密
S3

图1

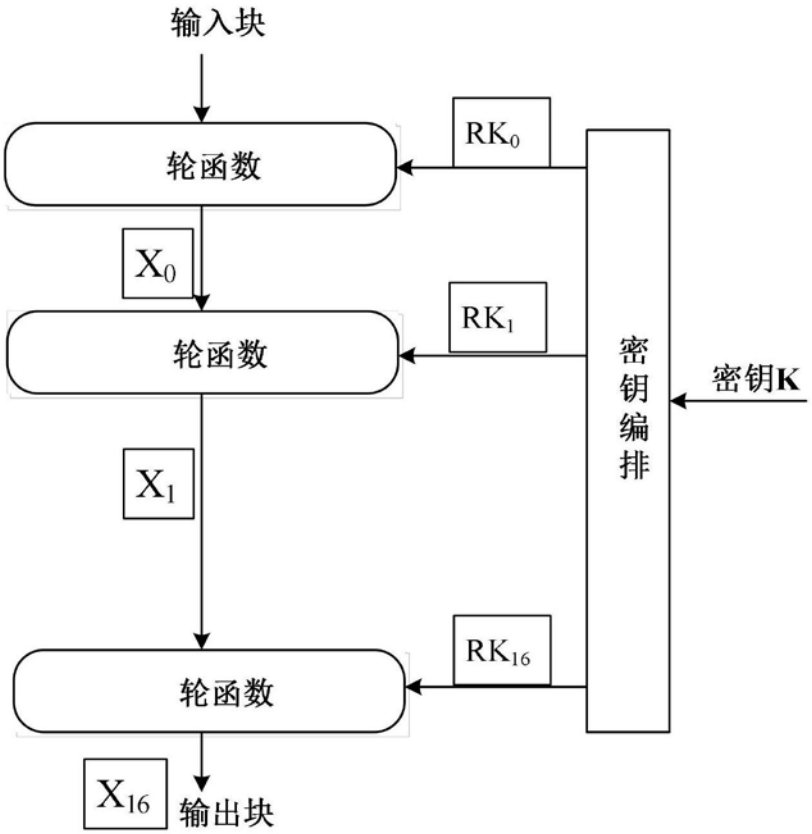


图2