(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 109787750 A
(43)申请公布日 2019.05.21

(21)申请号 201910184808.2

(22)申请日 2019.03.12

(71)申请人 广州合众互联信息技术有限公司
地址 510000 广东省广州市白云区丛云路0765号C栋305室

(72)发明人 聂品

(74)专利代理机构 深圳市华盈知识产权代理事务所(普通合伙) 44543
代理人 周婵

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)

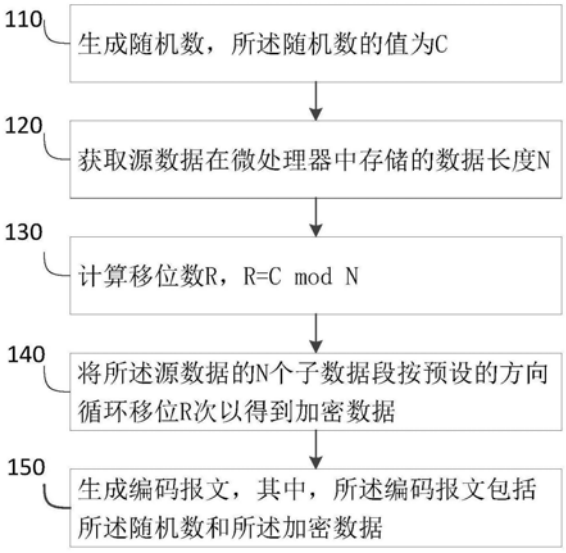
权利要求书2页 说明书7页 附图3页

(54)发明名称

通信报文的编解码方法、装置、设备和存储介质

(57)摘要

本发明实施例公开了一种通信报文的编码方法,包括:生成随机数,所述随机数的值为C;获取源数据在微处理器中存储的数据长度N;计算移位数R,R=C mod N;将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据;生成编码报文,其中,所述编码报文包括所述随机数和所述加密数据。相应地,本发明还公开解码方法、装置、设备和存储介质。本发明可应用于低位数微处理器,使得低位数微处理器的通信能够得到有效加密,避免遭受外部攻击和窃听。



CN 109787750 A

1.一种通信报文的编码方法,其特征在于,包括:

生成随机数,所述随机数的值为C;

获取源数据在微处理器中存储的数据长度N;

计算移位数R,R=C mod N;

将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据;

生成编码报文,其中,所述编码报文包括所述随机数和所述加密数据。

2.根据权利要求1所述的通信报文的编码方法,其特征在于,所述微处理器的位数为8。

3.根据权利要求1所述的通信报文的编码方法,其特征在于,所述方法还包括:生成用于指示循环移位方向的方向值;

所述将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据,具体包括:将所述源数据的N个子数据段按照所述方向值指示的方向循环移位R次以得到加密数据;

所述编码报文还包括所述方向值。

4.根据权利要求3所述的通信报文的编码方法,其特征在于,所述随机数的位数为M,所述微处理器的位数为S,所述方向值的位数为Y,S=Y+M。

5.根据权利要求4所述的通信报文的编码方法,其特征在于,Y=1。

6.一种通信报文的编码装置,其特征在于,包括:

第一生成模块,用于生成随机数,所述随机数的值为C;

获取模块,用于获取源数据在微处理器中存储的数据长度N;

第一计算模块,用于计算移位数R,R=C mod N;

正移位模块,用于将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据;

第二生成模块,用于生成编码报文,其中,所述编码报文包括所述随机数和所述加密数据。

7.一种通信报文的解码方法,其特征在于,包括:

读取编码报文中的随机数和加密数据;其中,所述随机数的值为C,所述加密数据在微处理器中存储的数据长度为N;

计算移位数R,R=C mod N;

将所述加密数据的N个子数据段按预设的反方向循环移位R次以得到源数据。

8.一种通信报文的解码装置,其特征在于,包括:

读取模块,用于读取编码报文中的随机数和加密数据;其中,所述随机数的值为C,所述加密数据在微处理器中存储的数据长度为N;

第二计算模块,用于计算移位数R,R=C mod N;

反移位模块,用于将所述加密数据的N个子数据段按预设的反方向循环移位R次以得到源数据。

9.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1-5和7任一项所述的方法的步骤。

10.一种设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现如权利要求1-5和7任一项所述的方法的

步骤。

通信报文的编解码方法、装置、设备和存储介质

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种通信报文的编解码方法、装置、设备和存储介质。

背景技术

[0002] 现有技术中有各种安全加密算法，用于对传输数据进行加密，以确保传输的信息不会被窃取。但目前的各种加密算法要求高位处理器处理，例如64位处理器，加密过程相当复杂。而在诸多通信设备中，例如物联网监控设备和无线遥测传感器中，一般应用低位数的微处理器，微处理器计算能力非常有限，无法使用上述加密过程复杂的加密算法，因此，大多数低位数的微处理器的无线射频通讯仍然是明文传输，没有安全机制，容易受到外部攻击和窃听。

发明内容

[0003] 本发明实施例提供一种逆变器的通信报文的编解码方法、装置、设备和存储介质，可应用于低位数微处理器，使得低位数微处理器的通信能够得到有效加密，避免遭受外部攻击和窃听。

[0004] 第一方面，本发明实施例提供一种通信报文的编码方法，包括：

[0005] 生成随机数，所述随机数的值为C；

[0006] 获取源数据在微处理器中存储的数据长度N；

[0007] 计算移位数R，R＝C mod N；

[0008] 将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据；

[0009] 生成编码报文，其中，所述编码报文包括所述随机数和所述加密数据。

[0010] 可选的，所述微处理器的位数为8。

[0011] 可选的，所述方法还包括：生成用于指示循环移位方向的方向值；

[0012] 所述将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据，具体包括：将所述源数据的N个子数据段按照所述方向值指示的方向循环移位R次以得到加密数据；

[0013] 所述编码报文还包括所述方向值。

[0014] 可选的，所述随机数的位数为M，所述微处理器的位数为S，所述方向值的位数为Y，S＝Y+M。

[0015] 可选的，Y＝1。

[0016] 第二方面，本发明实施例还提供一种通信报文的编码装置，包括：

[0017] 第一生成模块，用于生成随机数，所述随机数的值为C；

[0018] 获取模块，用于获取源数据在微处理器中存储的数据长度N；

[0019] 第一计算模块，用于计算移位数R，R＝C mod N；

[0020] 正移位模块，用于将所述源数据的N个子数据段按预设的方向循环移位R次以得到

加密数据；

[0021] 第二生成模块，用于生成编码报文，其中，所述编码报文包括所述随机数和所述加密数据。

[0022] 第三方面，本发明实施例还提供一种通信报文的解码方法，包括：

[0023] 读取编码报文中的随机数和加密数据；其中，所述随机数的值为C，所述加密数据在微处理器中存储的数据长度为N；

[0024] 计算移位数R，R＝C mod N；

[0025] 将所述加密数据的N个子数据段按预设的反方向循环移位R次以得到源数据。

[0026] 第四方面，本发明实施例还提供一种通信报文的解码装置，包括：

[0027] 读取模块，用于读取编码报文中的随机数和加密数据；其中，所述随机数的值为C，所述加密数据在微处理器中存储的数据长度为N；

[0028] 第二计算模块，用于计算移位数R，R＝C mod N；

[0029] 反移位模块，用于将所述加密数据的N个子数据段按预设的反方向循环移位R次以得到源数据。

[0030] 第五方面，本发明实施例提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现本发明任意实施例提供的方法的步骤。

[0031] 第六方，本发明实施例提供一种设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现本发明任意实施例提供的方法的步骤。

[0032] 实施本发明实施例，具有如下有益效果：

[0033] 本发明实施例的技术方案，生成随机数打包于编码报文中，采用循环移位的策略，在计算循环移位次数时，随机数作为除数，源数据的数据长度作为被除数，除数与被除数都是变量，使得对源数据进行循环移位的方法具有有效的加密性，而且无需复杂运算，具有简单高效的优点，适于低位数微处理器运行，因此可应用于低位数微处理器，使得低位数微处理器的通信能够得到有效加密，避免遭受外部攻击和窃听。

附图说明

[0034] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本发明的其它特征、目的和优点将会变得更明显：

[0035] 图1是本发明实施例提供的通信报文的编码方法的流程图；

[0036] 图2是本发明实施例提供的编码方法中的移位循环的示意图；

[0037] 图3是本发明实施例提供的通信报文的解码方法的流程图；

[0038] 图4是本发明实施例提供的通信报文的编码装置的结构示意图；

[0039] 图5是本发明实施例提供的通信报文的解码装置的结构示意图；

[0040] 图6是本发明实施例提供的一种设备的结构示意图。

具体实施方式

[0041] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此处所描述的具体实施例用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描

述,附图中仅示出了与本发明相关的部分而非全部结构。

[0042] 此外,在说明书和权利要求书中的术语第一、第二、第三等仅用于区别相同技术特征的描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量,也不一定描述次序或时间顺序。在合适的情况下术语是可以互换的。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。

[0043] 图1是本发明实施例提供的一种通信报文的编码方法的流程图。该实施例可以适用于在微处理器中对通信报文进行编码。具体地,一种通信报文的编码方法,包括:

[0044] 步骤110、生成随机数,所述随机数的值为C;

[0045] 具体地,可以在通信报文中生成nouce字段,其中承载随机数。

[0046] 步骤120、获取源数据在微处理器中存储的数据长度N;

[0047] 具体地,数据长度N为源数据占用微处理器寻址位宽的数量。以8位微处理器为例,一次执行寻址指令的数据带宽为8位,即单字节,则数据长度为源数据的字节数量。

[0048] 步骤130、计算移位数R,R=C mod N;

[0049] 具体地,mod指取余运算,不同的计算机语言对取余可能有不同的表达,例如在C语言中,R的取值代码为C%N。

[0050] 步骤140、将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据;

[0051] 具体地,源数据的子数据段,指的是按照微处理器的寻址位宽对源数据进行划分的子数据段,例如,将源数据按照8位字串数据类型存储(如字符数组char[]或字符链表char*)在8位微处理器中,则每一字节数据为一个子数据段。

[0052] 预设的方向可以是预先设置好,在编码过程中只要默认执行的方向,也可以是预先设定了获取方式和解读方式的方向。例如,可以在nouce字段中承载方向信息。

[0053] 参照图2,图2是本编码方法中的循环移位的示意图。源数据存储在寄存器上N个字节空间中,可看作如图2所示的数据段字节环,其逻辑结构上首位相连,可实现循环移位,例如向右循环移位两次,则每一子数据段均向右移位两次,在寄存器上,原来数据1会移至原来存储数据3的位置,在上述N个字节空间中,首个字节空间存储的数据为数据N-1。

[0054] 步骤150、生成编码报文,其中,所述编码报文包括所述随机数和所述加密数据。

[0055] 具体地,该编码报文包括上述nouce字段和加密数据。

[0056] 作为一种优选的实施方式,nouce字段承载方向信息,即预先设定了获取方向信息的方式和解读方向的方式。

[0057] 该优选实施方式具体为:所述方法还包括:生成用于指示循环移位方向的方向值;所述将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据,具体包括:将所述源数据的N个子数据段按照所述方向值指示的方向循环移位R次以得到加密数据;

[0058] 所述编码报文还包括所述方向值。

[0059] 例如,在编码报文中的nouce字段用几位数来承载方向信息,其中部分取值用于指向向左移位,部分取值用于指向向右移位。优选地,nouce字段由方向值和随机数组成,且占用处理器一次寻址位宽。即若所述随机数的位数为M,所述微处理器的位数为S,所述方向值的位数为Y,则S=Y+M。充分利用微处理器寄存器的寻址位宽长度,优化编码报文的结构。

[0060] 更为优选地,方向值占用1位,随机数占用剩余位。可以是0表示左移位,1表示右移

位,也可以相反取值。

[0061] 在8位微处理器中的一种优选的实施方式是:

[0062] 先将源数据按照8位字串数据类型存储(如字符数组char[]或字符链表char*),前后相连形成N字节环(N表示数据段长度),以便循环移位;

[0063] 在生成的编码报文中设置nouce字段(一个字节),该字节第一位0表示反向(左)移位,1表示正向(右)移位,后续七位为随机数C(0-127之间);

[0064] 将上一步的随机数除以不定长数据段的长度N,取余数R=C%N;

[0065] 把源数据按照nouce字段指示的方向循位移动R个字节,即获得源数据对应的加密数据,完成加密。

[0066] 编码报文的数据结构可以如下所示:

[0067]

报文头/包头	设备类型/报文类型	设备ID/设备地址	起始地址/寄存器	nouce(单字节)	数据长度(非必要)	加密数据(N字节)	报文尾/包尾

[0068] 其中nouce字段的格式可以如下:

[0069]

方向值(0-左,1-右,1位)	随机数C(0-127之间,7位)

[0070] 综上所述,本发明实施例的技术方案,生成随机数打包于编码报文中,采用循环移位的策略,在计算循环移位次数时,随机数作为除数,源数据的数据长度作为被除数,除数与被除数都是变量,使得对源数据进行循环移位的方法具有有效的加密性,而且无需复杂运算,具有简单高效的优点,适于低位数微处理器运行,因此可应用于低位数微处理器,使得低位数微处理器的通信能够得到有效加密,避免遭受外部攻击和窃听。

[0071] 相应地本发明还提供一种解密方法即解码方法,如图3所示。该方法包括:

[0072] 步骤310、读取编码报文中的随机数和加密数据;其中,所述随机数的值为C,所述加密数据在微处理器中存储的数据长度为N;

[0073] 步骤320、计算移位数R,R=C mod N;

[0074] 步骤330、将所述加密数据的N个子数据段按预设的反方向循环移位R次以得到源数据。

[0075] 该解码方法与上述各实施例提供的编码方法对应。进一步地,有如下可选的具体实施方式:

[0076] 可选的,所述微处理器的位数为8。

[0077] 可选的,该解码方法还包括:读取编码报文中的用于指示循环移位方向的方向值;所述将所述加密数据的N个子数据段按预设的反方向循环移位R次以得到源数据,具体包括:将所述加密数据的N个子数据段按照所述方向值指示的反方向循环移位R次以得到源数据。

[0078] 可选的,所述随机数的位数为M,所述微处理器的位数为S,所述方向值的位数为Y,S=Y+M。

[0079] 可选的,Y＝1。

[0080] 本发明提供的解码方法实施例,与编码方法实施例对应,具备相应的有益效果。

[0081] 本发明实施例还提供一种通信报文的编码装置,如图4所示,包括:

[0082] 第一生成模块410,用于生成随机数,所述随机数的值为C;

[0083] 获取模块420,用于获取源数据在微处理器中存储的数据长度N;

[0084] 第一计算模块430,用于计算移位数R,R＝C mod N;

[0085] 正移位模块440,用于将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据;

[0086] 第二生成模块450,用于生成编码报文,其中,所述编码报文包括所述随机数和所述加密数据。

[0087] 可选的,所述微处理器的位数为8。

[0088] 可选的,所述编码装置还包括:第三生成模块,用于生成用于指示循环移位方向的方向值;

[0089] 则所述正移位模块具体用于:将所述源数据的N个子数据段按照所述方向值指示的方向循环移位R次以得到加密数据;

[0090] 所述编码报文还包括所述方向值。

[0091] 可选的,所述随机数的位数为M,所述微处理器的位数为S,所述方向值的位数为Y,S＝Y+M。

[0092] 可选的,Y＝1。

[0093] 本发明提供的编码装置实施例,可用于实现本发明提供的编码方法实施例,具备相应的有益效果。

[0094] 本发明实施例还提供一种通信报文的解码装置,如图5所示,包括:

[0095] 读取模块510,用于读取编码报文中的随机数和加密数据;其中,所述随机数的值为C,所述加密数据在微处理器中存储的数据长度为N;

[0096] 第二计算模块520,用于计算移位数R,R＝C mod N;

[0097] 反移位模块530,用于将所述加密数据的N个子数据段按预设的反方向循环移位R次以得到源数据。

[0098] 可选的,所述微处理器的位数为8。

[0099] 可选的,该解码装置还包括:第二读取模块,用于读取编码报文中的用于指示循环移位方向的方向值;所述反移位模块具体用于:将所述加密数据的N个子数据段按照所述方向值指示的反方向循环移位R次以得到源数据。

[0100] 可选的,所述随机数的位数为M,所述微处理器的位数为S,所述方向值的位数为Y,S＝Y+M。

[0101] 可选的,Y＝1。

[0102] 本发明提供的解码装置实施例,可用于实现本发明提供的解码方法实施例,具备相应的有益效果。

[0103] 此外,本发明实施例还提供了一种计算机可读存储介质,其上存储有计算机程序,该程序被处理器执行时实现如上所述方法的步骤。

[0104] 本实施例中,所述编码装置或解码装置装置集成的模块/单元如果以软件功能单

元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实现上述实施例方法中的全部或部分流程，也可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括：能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random AccessMemory)、电载波信号、电信信号以及软件分发介质等。需要说明的是，所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括电载波信号和电信信号。

[0105] 图6为本发明实施例提供的设备的示意图。本发明实施例提供的设备，包括存储器610、处理器620及存储在存储器610上并可在处理器620上运行的计算机程序，所述处理器620执行所述计算机程序时实现上述各个通信报文的编码方法或解码方法实施例中的步骤，例如图1所示的生成随机数，所述随机数的值为C；获取源数据在微处理器中存储的数据长度N；计算移位数R，R＝Cmod N；将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据；生成编码报文，其中，所述编码报文包括所述随机数和所述加密数据。或者，图3所示的：读取编码报文中的随机数和加密数据；其中，所述随机数的值为C，所述加密数据在微处理器中存储的数据长度为N；计算移位数R，R＝C mod N；将所述加密数据的N个子数据段按预设的反方向循环移位R次以得到源数据。或者，所述处理器620执行所述计算机程序时实现上述各编码装置或解码装置实施例中各模块/单元的功能，例如图4所示的第一生成模块410、获取模块420、第一计算模430、正移位模块440和第二生成模块450；或者，图5所示的读取模块510、第二计算模块520和反移位模块530。

[0106] 示例性的，所述计算机程序可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器中，并由所述处理器执行，以完成本发明。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述所述计算机程序在所述设备远程备份升级装置中的执行过程。例如，所述计算机程序可以被分割成设置模块410、计算模块420和补偿模块430。

[0107] 所述设备可以是计算机设备。所述设备可包括，但不仅限于，处理器、存储器。本领域技术人员可以理解，所述示意图4仅仅是所述设备的示例，并不构成对设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述设备还可以包括输入输出设备、网络接入设备、总线等。

[0108] 所述处理器可以是中央处理单元(Central Processing Unit，CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor，DSP)、专用集成电路(Application Specific Integrated Circuit，ASIC)、现成可编程门阵列(Field-Programmable Gate Array，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等，所述处理器是所述设备的控制中心，利用各种接口和线路连接整个设备的各个部分。

[0109] 所述存储器可用于存储所述计算机程序和/或模块，所述处理器通过运行或执行

存储在所述存储器内的计算机程序和/或模块，以及调用存储在存储器内的数据，实现所述设备的各种功能。所述存储器可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等；存储数据区可存储根据手机的使用所创建的数据(比如音频数据、电话本等)等。此外，存储器可以包括高速随机存取存储器，还可以包括非易失性存储器，例如硬盘、内存、插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)、至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

[0110] 在本发明实施例中，应该理解到，所揭露的编解码装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性或其它的形式。

[0111] 本领域的技术人员能够理解，尽管在此的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0112] 注意，上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员会理解，本发明不限于这里所述的特定实施例，对本领域技术人员来说能够进行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此，虽然通过以上实施例对本发明进行了较为详细的说明，但是本发明不仅仅限于以上实施例，在不脱离本发明构思的情况下，还可以包括更多其他等效实施例，而本发明的范围由所附的权利要求范围决定。

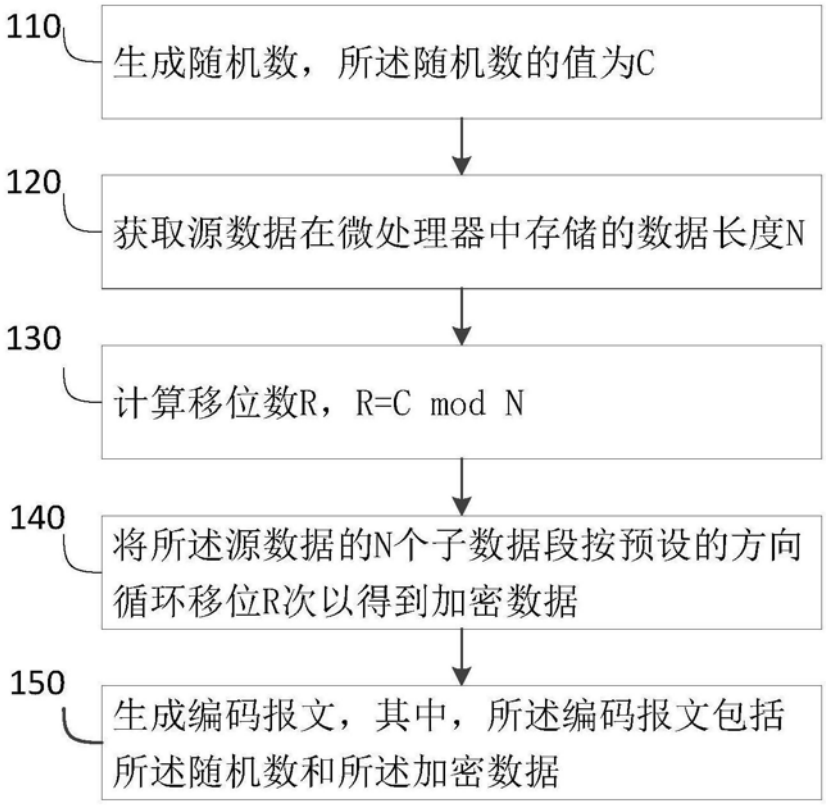

110
生成随机数，所述随机数的值为C
120
获取源数据在微处理器中存储的数据长度N
130
计算移位数R，R=C mod N
140
将所述源数据的N个子数据段按预设的方向循环移位R次以得到加密数据
150
生成编码报文，其中，所述编码报文包括所述随机数和所述加密数据

图1


数据1|数据2|数据3|数据4|数据5|数据6|数据7|数据8|数据...|数据N|

图2

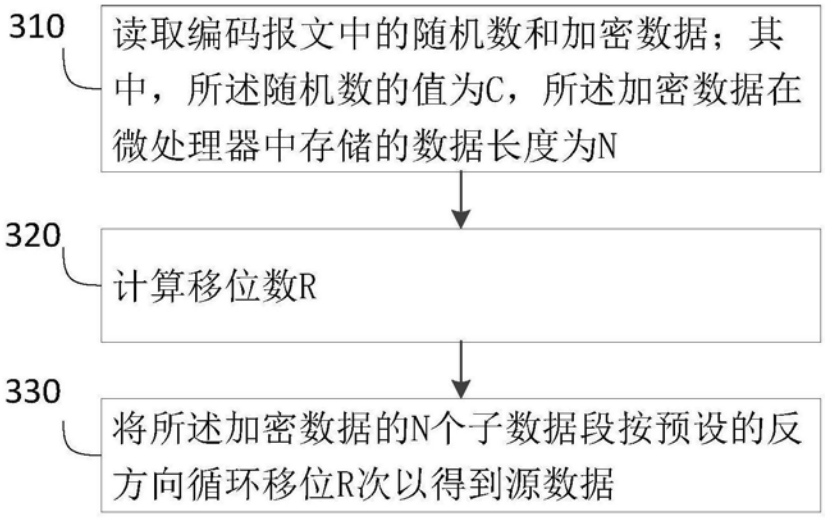

310
读取编码报文中的随机数和加密数据；其中，所述随机数的值为C，所述加密数据在微处理器中存储的数据长度为N
320
计算移位数R
330
将所述加密数据的N个子数据段按预设的反方向循环移位R次以得到源数据

图3

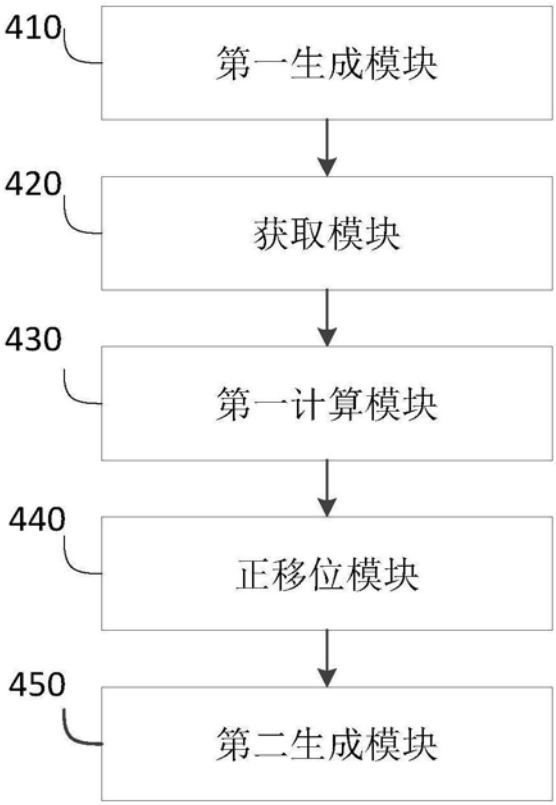

410
第一生成模块
420
获取模块
430
第一计算模块
440
正移位模块
450
第二生成模块

图4

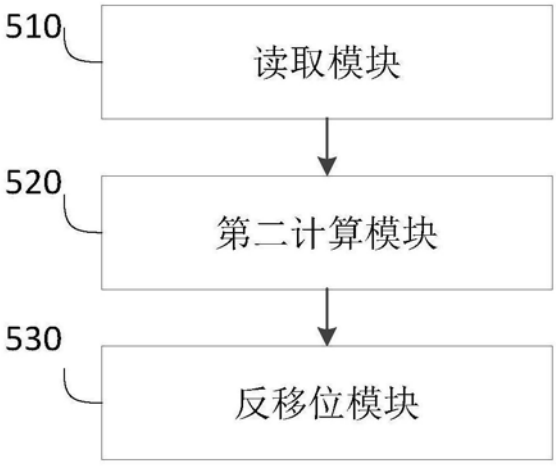


图5

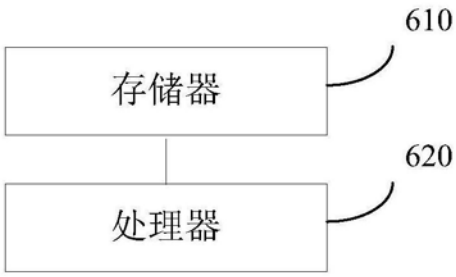


图6