(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114070552 B
(45)授权公告日 2022.11.08

(21)申请号 202111261664.X

(22)申请日 2021.10.28

(65)同一申请的已公布的文献号
申请公布号 CN 114070552 A

(43)申请公布日 2022.02.18

(73)专利权人 国核自仪系统工程有限公司
地址 200241 上海市闵行区江川东路428号

(72)发明人 朱怀宇

(74)专利代理机构 上海弼兴律师事务所 31283
专利代理师 林嵩

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

审查员 朱少华

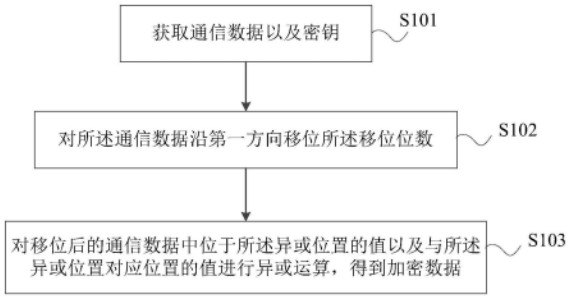
权利要求书2页 说明书8页 附图7页

(54)发明名称

数据加密方法及装置、数据解密方法及装置、设备及介质

(57)摘要

本发明公开了一种数据加密方法及装置、数据解密方法及装置、设备及介质。其中，数据加密方法包括以下步骤：获取通信数据以及密钥；对所述通信数据沿第一方向移位所述移位位数；对移位后的通信数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到加密数据；其中，所述加密数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与移位后的通信数据中位于对应位置的值相同。本发明提供的数据加密方法和数据解密方法利用软件和硬件均可实现，实现方式简单可靠可以应用在各种场合。具体地，在利用硬件实现时，可以利用FPGA的移位寄存器实现移位操作，利用FPGA的异或门实现异或运算。



CN 114070552 B

1.一种数据加密方法,其特征在于,包括以下步骤:

获取通信数据以及密钥;其中,所述密钥用于表征移位位数和异或位置;所述密钥还用于表征第一方向和与所述异或位置对应的位置;

对所述通信数据沿所述第一方向移位所述移位位数;

对移位后的通信数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算,得到加密数据;其中,所述加密数据中位于所述异或位置的值为进行异或运算的结果,位于其它位置的值与移位后的通信数据中位于对应位置的值相同。

2.如权利要求1所述的数据加密方法,其特征在于,所述密钥还用于表征加密次数,在执行所述移位和所述异或运算的步骤之后,且在得到加密数据的步骤之前,还包括以下步骤:将运算次数加一;

所述得到加密数据的步骤具体包括:

若所述运算次数达到所述加密次数,则得到加密数据;

若所述运算次数未达到所述加密次数,则得到第一中间数据,将所述通信数据更新为所述第一中间数据,继续执行所述移位和所述异或运算的步骤。

3.一种数据加密装置,其特征在于,包括:

第一获取模块,用于获取通信数据以及密钥;其中,所述密钥用于表征移位位数和异或位置;所述密钥还用于表征第一方向和与所述异或位置对应的位置;

第一移位模块,用于对所述通信数据沿所述第一方向移位所述移位位数;

第一异或模块,用于对移位后的通信数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算,得到加密数据;其中,所述加密数据中位于所述异或位置的值为进行异或运算的结果,位于其它位置的值与移位后的通信数据中位于对应位置的值相同。

4.一种数据解密方法,其特征在于,包括以下步骤:

获取加密数据以及密钥;其中,所述密钥用于表征移位位数和异或位置;所述密钥还用于表征第一方向和与所述异或位置对应的位置;

对所述加密数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算,得到第二中间数据;其中,所述第二中间数据中位于所述异或位置的值为进行异或运算的结果,位于其它位置的值与所述加密数据中位于对应位置的值相同;

对所述第二中间数据沿与所述第一方向相反的方向移位所述移位位数,得到解密数据。

5.如权利要求4所述的数据解密方法,其特征在于,所述密钥还用于表征解密次数,在执行所述异或运算和所述移位的步骤之后,且在得到解密数据的步骤之前,还包括以下步骤:将运算次数加一;

所述得到解密数据的步骤具体包括:

若所述运算次数达到所述解密次数,则得到解密数据;

若所述运算次数未达到所述解密次数,则将所述加密数据更新为移位后的第二中间数据,继续执行所述异或运算和所述移位的步骤。

6.一种数据解密装置,其特征在于,包括:

第二获取模块,用于获取加密数据以及密钥;其中,所述密钥用于表征移位位数和异或

位置;所述密钥还用于表征第一方向和与所述异或位置对应的位置;

第二异或模块,用于对所述加密数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算,得到第二中间数据;其中,所述第二中间数据中位于所述异或位置的值为进行异或运算的结果,位于其它位置的值与所述加密数据中位于对应位置的值相同;

第二移位模块,用于对所述中间数据沿与所述第一方向相反的方向移位所述移位位数,得到解密数据。

7.一种电子设备,包括存储器、处理器以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计算机程序时实现权利要求1或2所述的数据加密方法或者权利要求4或5所述的数据解密方法。

8.一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,所述计算机程序被处理器执行时实现权利要求1或2所述的数据加密方法或者权利要求4或5所述的数据解密方法。

数据加密方法及装置、数据解密方法及装置、设备及介质

技术领域

[0001] 本发明涉及通信技术领域，特别涉及一种数据加密方法及装置、数据解密方法及装置、电子设备及存储介质。

背景技术

[0002] 在数字化仪控系统中，远程接收数据和远程操控的应用场合越来越广泛。在信息安全的大时代背景下，特别是一些特殊应用场合，通信数据加密成为首要需求。DES(Data Encryption Standard，数据加密标准)、AES(Advanced Encryption Standard，高级加密标准)等加密算法在软件层通信比较广泛，但是硬件实现比较繁琐。

发明内容

[0003] 本发明要解决的技术问题是为了克服现有技术中的加密算法在硬件实现比较繁琐的缺陷，提供一种数据加密方法及装置、数据解密方法及装置、设备及介质。

[0004] 本发明是通过下述技术方案来解决上述技术问题：

[0005] 本发明的第一方面提供一种数据加密方法，包括以下步骤：

[0006] 获取通信数据以及密钥；其中，所述密钥用于表征移位位数和异或位置；

[0007] 对所述通信数据沿第一方向移位所述移位位数；

[0008] 对移位后的通信数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到加密数据；其中，所述加密数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与移位后的通信数据中位于对应位置的值相同。

[0009] 可选地，所述密钥还用于表征加密次数，在执行所述移位和所述异或运算的步骤之后，且在得到加密数据的步骤之前，还包括以下步骤：将运算次数加一；

[0010] 所述得到加密数据的步骤具体包括：

[0011] 若所述运算次数达到所述加密次数，则得到加密数据；

[0012] 若所述运算次数未达到所述加密次数，则得到第一中间数据，将所述通信数据更新为所述第一中间数据，继续执行所述移位和所述异或运算的步骤。

[0013] 可选地，所述密钥还用于表征第一方向，和/或，所述密钥还用于表征与所述异或位置对应的位置。

[0014] 本发明的第二方面提供一种数据加密装置，包括：

[0015] 第一获取模块，用于获取通信数据以及密钥；其中，所述密钥用于表征移位位数和异或位置；

[0016] 第一移位模块，用于对所述通信数据沿第一方向移位所述移位位数；

[0017] 第一异或模块，用于对移位后的通信数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到加密数据；其中，所述加密数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与移位后的通信数据中位于对应位置的值相同。

[0018] 本发明的第三方面提供一种数据解密方法,包括以下步骤:

[0019] 获取加密数据以及密钥;其中,所述密钥用于表征移位位数和异或位置;

[0020] 对所述加密数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算,得到第二中间数据;其中,所述第二中间数据中位于所述异或位置的值为进行异或运算的结果,位于其它位置的值与所述加密数据中位于对应位置的值相同;

[0021] 对所述第二中间数据沿与第一方向相反的方向移位所述移位位数,得到解密数据。

[0022] 可选地,所述密钥还用于表征解密次数,在执行所述异或运算和所述移位的步骤之后,且在得到解密数据的步骤之前,还包括以下步骤:将运算次数加一;

[0023] 所述得到解密数据的步骤具体包括:

[0024] 若所述运算次数达到所述解密次数,则得到解密数据;

[0025] 若所述运算次数未达到所述解密次数,则将所述加密数据更新为移位后的第二中间数据,继续执行所述异或运算和所述移位的步骤。

[0026] 可选地,所述密钥还用于表征第一方向,和/或,所述密钥还用于表征与所述异或位置对应的位置。

[0027] 本发明的第四方面提供一种数据解密装置,包括:

[0028] 第二获取模块,用于获取加密数据以及密钥;其中,所述密钥用于表征移位位数和异或位置;

[0029] 第二异或模块,用于对所述加密数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算,得到第二中间数据;其中,所述第二中间数据中位于所述异或位置的值为进行异或运算的结果,位于其它位置的值与所述加密数据中位于对应位置的值相同;

[0030] 第二移位模块,用于对所述中间数据沿与第一方向相反的方向移位所述移位位数,得到解密数据。

[0031] 本发明的第五方面提供一种电子设备,包括存储器、处理器以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计算机程序时实现第一方面所述的数据加密方法或者第三方面所述的数据解密方法。

[0032] 本发明的第六方面提供一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序被处理器执行时实现第一方面所述的数据加密方法或者第三方面所述的数据解密方法。

[0033] 本发明的积极进步效果在于:本发明提供的数据加密方法和数据解密方法利用软件和硬件均可实现,实现方式简单可靠,可以应用在各种场合。具体地,在利用硬件实现时,可以使用基于FPGA(Field Programmable Gate Array,现场可编程逻辑门阵列)的硬件设备,具体利用FPGA的移位寄存器实现移位操作,以及利用FPGA的异或门实现异或运算。

附图说明

[0034] 图1为本发明实施例提供的一种上位机通信方法的流程示意图。

[0035] 图2为本发明实施例提供的一种下位机通信方法的流程示意图。

[0036] 图3为本发明实施例1提供的一种数据加密方法的流程图。

[0037] 图4为本发明实施例1提供的另一种数据加密方法的流程图。

[0038] 图5为本发明实施例1提供的一种密钥的数据格式示意图。

[0039] 图6为本发明实施例1提供的一种数据加密方法的操作示意图。

[0040] 图7为本发明实施例1提供的一种数据加密装置的结构框图。

[0041] 图8为本发明实施例2提供的一种数据解密方法的流程图。

[0042] 图9为本发明实施例2提供的另一种数据解密方法的流程图。

[0043] 图10为本发明实施例2提供的一种数据解密方法的操作示意图。

[0044] 图11为本发明实施例2提供的一种数据解密装置的结构框图。

[0045] 图12为本发明实施例3提供的一种电子设备的结构示意图。

具体实施方式

[0046] 下面通过实施例的方式进一步说明本发明，但并不因此将本发明限制在所述的实施例范围之中。

[0047] 图1用于示出上位机通信方法的具体流程，图2用于示出下位机通信方法的具体流程。参考图1和图2，上位机与下位机之间的通信过程包括：上位机向下位机发送链接请求，若下位机收到链接请求，则向上位机发送链接响应。若上位机收到链接响应，则向下位机发送密钥，否则重新向下位机发送链接请求。若下位机收到密钥，则向上位机发送密钥响应。若上位机收到密钥响应，可以确定下位机和上位机使用的密钥相同，此时可以向下位机发送加密数据，否则重新向下位机发送密钥。若下位机收到加密数据，则向上位机发送数据响应。其中，下位机可以利用接收的密钥对加密数据进行解密。若上位机收到数据响应，则通过查看定时器判断是否到达预设时间，若到达，则向下位机发送新密钥，若未到达，则继续向下位机发送密钥数据。若下位机收到新密钥，则向上位机发送密钥响应，若下位机没有收到新密钥，则使用旧密钥对加密数据进行解密。

[0048] 其中，若上位机向下位机重发M次密钥之后仍然收不到密钥响应，则停止向下位机发送密钥，一段时间后重新向下位机发送链接请求。若上位机向下位机重发N次加密数据之后仍然收不到数据响应，则停止向下位机发送密钥数据，一段时间后重新向下位机发送链接请求。其中，M和N的值可以根据实际情况进行设置。在一个具体的例子中，M和N的值均为3。

[0049] 在具体实施中，上位机和下位机的通信数据包可以包括同步字、数据类型、通信数据、数据区CRC(Cyclic Redundancy Check，循环冗余校验)以及包CRC。其中，同步字用于上位机和下位机之间的数据同步。数据类型可以包括链接请求、链接响应、密钥、密钥响应、读写命令、读写响应等。通信数据为上位机发送的有效数据。数据区CRC为加密前的数据区的CRC结果，可以和加密方法一起决定收到数据的合法性，若上位机和下位机密钥不统一，则下位机的数据区的CRC校验码是错误的，需要丢弃此通信数据包。包CRC为整个通信数据包的CRC结果，用于判断通信过程中数据是否被损坏。

[0050] 实施例1

[0051] 本实施例提供的数据加密方法可以由数据加密装置执行，该数据加密装置可以通过软件和/或硬件的方式实现，该数据加密装置可以为电子设备的部分或全部。其中，本实施例中的电子设备可以为个人计算机(Personal Computer，PC)，例如台式机、一体机、笔记

本电脑、平板电脑等，还可以为手机、可穿戴设备、掌上电脑(Personal Digital Assistant,PDA)等终端设备。在一些例子中，本实施例中的电子设备也可以称为上位机。下面以上位机为执行主体介绍本实施例提供的数据加密方法。

[0052] 本实施例提供一种数据加密方法，如图3所示，包括以下步骤S101～S103：

[0053] 步骤S101、获取通信数据以及密钥；其中，所述密钥用于表征移位位数和异或位置。所述异或位置可以为一个，也可以为多个。

[0054] 在具体实施中，密钥的数据格式以及数据位数可以根据实际情况进行设置。例如可以为二进制格式，数据位数为32位。

[0055] 步骤S102、对所述通信数据沿第一方向移位所述移位位数。

[0056] 在可选的一种实施方式中，所述密钥还用于表征第一方向。在可选的其它实施方式中，通信双方还可以通过其它方式约定第一方向。

[0057] 步骤S103、对移位后的通信数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到加密数据。

[0058] 其中，所述加密数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与移位后的通信数据中位于对应位置的值相同。

[0059] 在可选的一种实施方式中，所述密钥还用于表征与所述异或位置对应的位置。在可选的其它实施方式中，通信双方还可以通过其它方式约定与所述异或位置对应的位置。例如可以统一约定所述异或位置左边一位的位置为与所述异或位置对应的位置，或者统一约定所述异或位置右边两位的位置为与所述异或位置对应的位置。

[0060] 本实施例还提供一种数据加密方法，如图4所示，包括以下步骤S201～S206：

[0061] 步骤S201、获取通信数据以及密钥。

[0062] 其中，所述密钥用于表征移位位数、异或位置以及加密次数。图5用于示出一种密钥的数据格式示意图。在如图5所示的例子中，密钥的位数共32位，其中，第0～7位用于表征移位位数，第8～23位用于表征异或位置，第24～31位用于表征加密次数。

[0063] 步骤S202、对所述通信数据沿第一方向移位所述移位位数。

[0064] 步骤S203、对移位后的通信数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算。对移位后的通信数据中位于除异或位置以外的值保持不变。

[0065] 步骤S204、将运算次数加一。

[0066] 步骤S205、判断所述运算次数是否达到所述加密次数，若是，则执行步骤S206；若否，则得到第一中间数据，将所述通信数据更新为所述第一中间数据，继续执行步骤S202～S204。其中，所述第一中间数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与移位后的通信数据中位于对应位置的值相同。

[0067] 需要说明的是，运算次数的初始值为零，若运算次数达到加密次数，则将运算次数清零。

[0068] 步骤S206、得到加密数据。其中，所述加密数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与移位后的通信数据中位于对应位置的值相同。

[0069] 本实施方式中，一次加密操作包括一次移位和一次异或运算，执行所述加密次数的加密操作得到加密数据。

[0070] 图6用于示出一种数据加密方法的操作示意图。如图6所示，通信数据包括32位，根

据密钥可以确定第一方向为向左、移位位数为K、异或位置包括第0位、第7位、第15位、第23位以及第30位、异或位置对应的位置分别为第1位、第8位、第16位、第24位以及第31位、加密次数为X。对通信数据向左移位K位后，分别对第0位的值和第1位的值、第7位的值和第8位的值、第15位的值和第16位的值、第23位的值和第24位的值以及第30位的值和第31位的值进行异或运算，得到第一中间数据。其中，第一中间数据中位于第0、7、15、23、30位的值分别为对应位置进行异或运算的结果，位于第1～6、8～14、16～22、24～29、30位的值与移位后的通信数据中位于第1～6、8～14、16～22、24～29、30位的值相同。此时运算次数加一，若运算次数未达到加密次数，则将通信数据更新为第一中间数据，继续进行与之前相同的移位和异或运算，直至运算次数达到加密次数，得到最终的加密数据。

[0071] 本实施例提供的数据加密方法中，上位机根据密钥对通信数据进行加密，得到加密数据，从而向下位机发送加密数据，实现上位机和下位机的加密通信。上位机利用软件和硬件均可实现数据加密方法，实现方式简单可靠，可以应用在各种场合。具体地，上位机在利用硬件实现数据加密方法时，可以使用基于FPGA的硬件设备，具体利用FPGA的移位寄存器实现移位操作，利用FPGA的异或门实现异或运算。其中，可以根据密钥表征的异或位置的数量确定参与异或运算的异或门的数量，还可以根据密钥表征的加密次数确定包括移位寄存器和异或门的加密电路的叠加次数。

[0072] 本实施例还提供一种数据加密装置70，如图7所示，包括第一获取模块71、第一移位模块72以及第一异或模块73。

[0073] 第一获取模块71用于获取通信数据以及密钥；其中，所述密钥用于表征移位位数和异或位置。

[0074] 第一移位模块72用于对所述通信数据沿第一方向移位所述移位位数。

[0075] 第一异或模块73用于对移位后的通信数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到加密数据；其中，所述加密数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与移位后的通信数据中位于对应位置的值相同。

[0076] 需要说明的是，本实施例中的数据加密装置具体可以是单独的芯片、芯片模组或电子设备，也可以是集成于电子设备内的芯片或者芯片模组。

[0077] 关于本实施例中描述的数据加密装置包含的各个模块，其可以是软件模块，也可以是硬件模块，或者也可以部分是软件模块，部分是硬件模块。

[0078] 实施例2

[0079] 在实施例1的基础上，本实施例提供一种与数据加密方法对应的数据解密方法，该数据解密方法可以由数据解密装置执行，该数据解密装置可以通过软件和/或硬件的方式实现，该数据解密装置可以为电子设备的部分或全部。其中，本实施例中的电子设备可以为个人计算机，例如台式机、一体机、笔记本电脑、平板电脑等，还可以为手机、可穿戴设备、掌上电脑等终端设备。在一些例子中，本实施例中的电子设备也可以称为下位机。下面以下位机为执行主体介绍本实施例提供的数据解密方法。

[0080] 如图8所示，本实施例提供的数据解密方法包括以下步骤S301～S303：

[0081] 步骤S301、获取加密数据以及密钥。在具体实施中，下位机获取上位机发送的加密数据以及密钥。

[0082] 其中，所述密钥用于表征移位位数和异或位置。所述异或位置可以为一个，也可以为多个。

[0083] 步骤S302、对所述加密数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到第二中间数据。其中，所述第二中间数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与所述加密数据中位于对应位置的值相同。

[0084] 在可选的一种实施方式中，所述密钥还用于表征与所述异或位置对应的位置。在可选的其它实施方式中，通信双方还可以通过其它方式约定与所述异或位置对应的位置。例如可以约定所述异或位置左边一位的位置为与所述异或位置对应的位置，或者约定所述异或位置右边两位的位置为与所述异或位置对应的位置。

[0085] 步骤S303、对所述第二中间数据沿与第一方向相反的方向移位所述移位位数，得到解密数据。

[0086] 在可选的一种实施方式中，所述密钥还用于表征第一方向。在可选的其它实施方式中，通信双方还可以通过其它方式约定第一方向。

[0087] 本实施例还提供一种数据解密方法，如图9所示，包括以下步骤S401～S406：

[0088] 步骤S401、获取加密数据以及密钥。其中，所述密钥用于表征移位位数、异或位置以及解密次数。需要说明的是，所述解密次数与实施例1中数据加密方法中的加密次数相同。

[0089] 步骤S402、对所述加密数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到第二中间数据。其中，所述第二中间数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与所述加密数据中位于对应位置的值相同。

[0090] 步骤S403、对所述第二中间数据沿与第一方向相反的方向移位所述移位位数。

[0091] 步骤S404、将运算次数加一。

[0092] 步骤S405、判断所述运算次数是否达到所述解密次数，若是，则执行步骤S406；若否，则将所述加密数据更新为移位后的第二中间数据，继续执行步骤S402～S404。其中，所述第二中间数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与移位后的通信数据中位于对应位置的值相同。

[0093] 需要说明的是，运算次数的初始值为零，若运算次数达到解密次数，则将运算次数清零。

[0094] 步骤S406、得到解密数据。

[0095] 本实施方式中，一次解密操作包括一次异或运算和一次反向移位，执行所述解密次数的解密操作得到解密数据。

[0096] 图10用于示出一种数据解密方法的操作示意图。如图10所示，加密数据包括32位，根据密钥可以确定第一方向为向左、异或位置包括第0位、第7位、第15位、第23位以及第30位、异或位置对应的位置分别为第1位、第8位、第16位、第24位以及第31位、移位位数为K、解密次数为X。分别对加密数据中第0位的值和第1位的值、第7位的值和第8位的值、第15位的值和第16位的值、第23位的值和第24位的值以及第30位的值和第31位的值进行异或运算，得到第二中间数据。其中，第二中间数据中位于第0、7、15、23、30位的值分别为对应位置进行异或运算的结果，位于第1～6、8～14、16～22、24～29、30位的值与加密数据中位于第1～6、8～14、16～22、24～29、30位的值相同。对第二中间数据向右移位K位后，此时运算次数加

一，若运算次数未达到解密次数，则将加密数据更新为移位后的第二中间数据，继续进行与之前相同的异或运算和移位，直至运算次数达到解密次数，得到最终的解密数据。

[0097] 本实施例提供的数据解密方法中，下位机接收上位机发送的加密数据，根据密钥对加密数据进行解密，从而得到解密数据。下位机利用软件和硬件均可实现数据解密方法，实现方式简单可靠，可以应用在各种场合。具体地，下位机在利用硬件实现数据解密方法时，可以使用基于FPGA的硬件设备，具体利用FPGA的异或门实现异或运算，利用FPGA的移位寄存器实现移位操作。

[0098] 本实施例还提供一种数据解密装置80，如图11所示，包括第二获取模块81、第二异或模块82以及第二移位模块83。

[0099] 第二获取模块81用于获取加密数据以及密钥；其中，所述密钥用于表征移位位数和异或位置。

[0100] 第二异或模块82用于对所述加密数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到第二中间数据；其中，所述第二中间数据中位于所述异或位置的值为进行异或运算的结果，位于其它位置的值与所述加密数据中位于对应位置的值相同。

[0101] 第二移位模块83用于对所述中间数据沿与第一方向相反的方向移位所述移位位数，得到解密数据。

[0102] 需要说明的是，本实施例中的数据解密装置具体可以是单独的芯片、芯片模组或电子设备，也可以是集成于电子设备内的芯片或者芯片模组。

[0103] 关于本实施例中描述的数据解密装置包含的各个模块，其可以是软件模块，也可以是硬件模块，或者也可以部分是软件模块，部分是硬件模块。

[0104] 实施例3

[0105] 图12为本实施例提供的一种电子设备的结构示意图。所述电子设备包括至少一个处理器以及与所述至少一个处理器通信连接的存储器。其中，所述存储器存储有可被所述至少一个处理器运行的计算机程序，所述计算机程序被所述至少一个处理器执行，以使所述至少一个处理器能够执行实施例1的数据加密方法或者实施例2的数据解密方法。本实施例提供的电子设备可以为个人计算机，例如台式机、一体机、笔记本电脑、平板电脑等，还可以为手机、可穿戴设备、掌上电脑等终端设备。图12显示的电子设备3仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0106] 电子设备3的组件可以包括但不限于：上述至少一个处理器4、上述至少一个存储器5、连接不同系统组件(包括存储器5和处理器4)的总线6。

[0107] 总线6包括数据总线、地址总线和控制总线。

[0108] 存储器5可以包括易失性存储器，例如随机存取存储器(RAM)51和/或高速缓存存储器52，还可以进一步包括只读存储器(ROM)53。

[0109] 存储器5还可以包括具有一组(至少一个)程序模块54的程序/实用工具55，这样的程序模块54包括但不限于：操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

[0110] 处理器4通过运行存储在存储器5中的计算机程序，从而执行各种功能应用以及数据处理，例如上述数据加密方法或者数据解密方法。

[0111] 电子设备3也可以与一个或多个外部设备7(例如键盘、指向设备等)通信。这种通信可以通过输入/输出(I/O)接口8进行。并且,电子设备3还可以通过网络适配器9与一个或者多个网络(例如局域网(LAN),广域网(WAN)和/或公共网络,例如因特网)通信。如图12所示,网络适配器9通过总线6与电子设备3的其它模块通信。应当明白,尽管图12中未示出,可以结合电子设备3使用其它硬件和/或软件模块,包括但不限于:微代码、设备驱动器、冗余处理器、外部磁盘驱动阵列、RAID(磁盘阵列)系统、磁带驱动器以及数据备份存储系统等。

[0112] 应当注意,尽管在上文详细描述中提及了电子设备的若干单元/模块或子单元/模块,但是这种划分仅仅是示例性的并非强制性的。实际上,根据本发明的实施方式,上文描述的两个或更多单元/模块的特征和功能可以在一个单元/模块中具体化。反之,上文描述的一个单元/模块的特征和功能可以进一步划分为由多个单元/模块来具体化。

[0113] 实施例4

[0114] 本实施例提供一种存储有计算机程序的计算机可读存储介质,所述计算机程序被处理器执行时实现实施例1中的数据加密方法或者实施例2中的数据解密方法。

[0115] 其中,可读存储介质可以采用的更具体可以包括但不限于:便携式盘、硬盘、随机存取存储器、只读存储器、可擦拭可编程只读存储器、光存储器件、磁存储器件或上述的任意合适的组合。

[0116] 在可能的实施方式中,本发明还可以实现为一种程序产品的形式,其包括程序代码,当所述程序产品在电子设备上运行时,所述程序代码用于使所述电子设备执行实现实施例1中的数据加密方法或者实施例2中的数据解密方法。

[0117] 其中,可以以一种或多种程序设计语言的任意组合来编写用于执行本发明的程序代码,所述程序代码可以完全地在电子设备上执行、部分地在电子设备上执行、作为一个独立的软件包执行、部分在电子设备上部分在远程设备上执行或完全在远程设备上执行。

[0118] 虽然以上描述了本发明的具体实施方式,但是本领域的技术人员应当理解,这仅是举例说明,本发明的保护范围是由所附权利要求书限定的。本领域的技术人员在不背离本发明的原理和实质的前提下,可以对这些实施方式做出多种变更或修改,但这些变更和修改均落入本发明的保护范围。

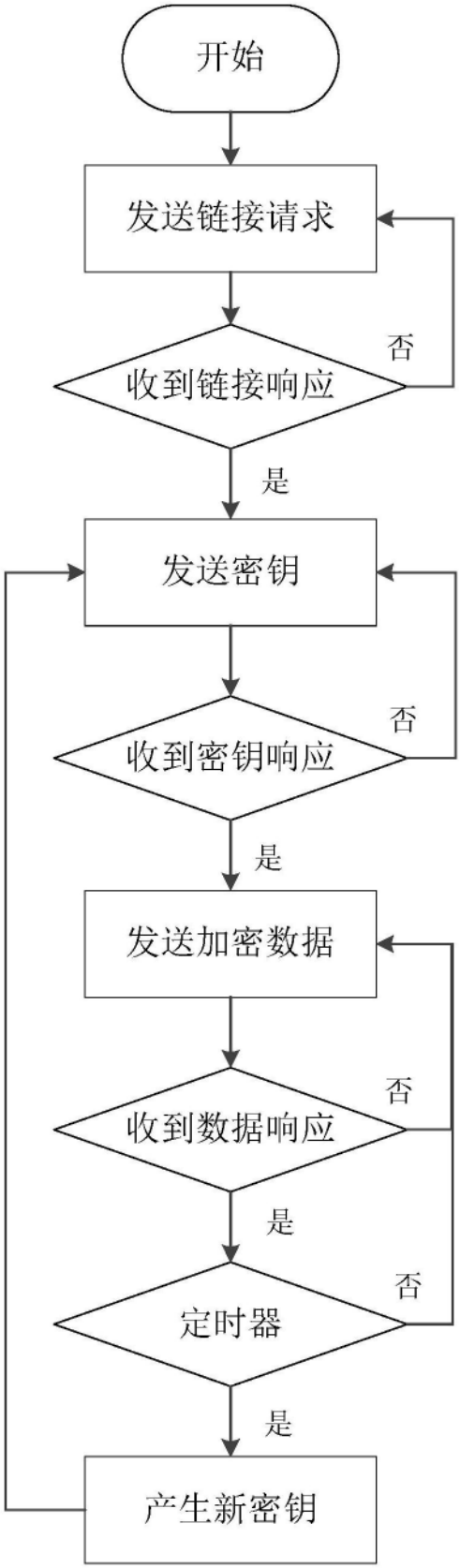

开始
发送链接请求
否
收到链接响应
是
发送密钥
否
收到密钥响应
是
发送加密数据
否
收到数据响应
是
否
定时器
是
产生新密钥

图1

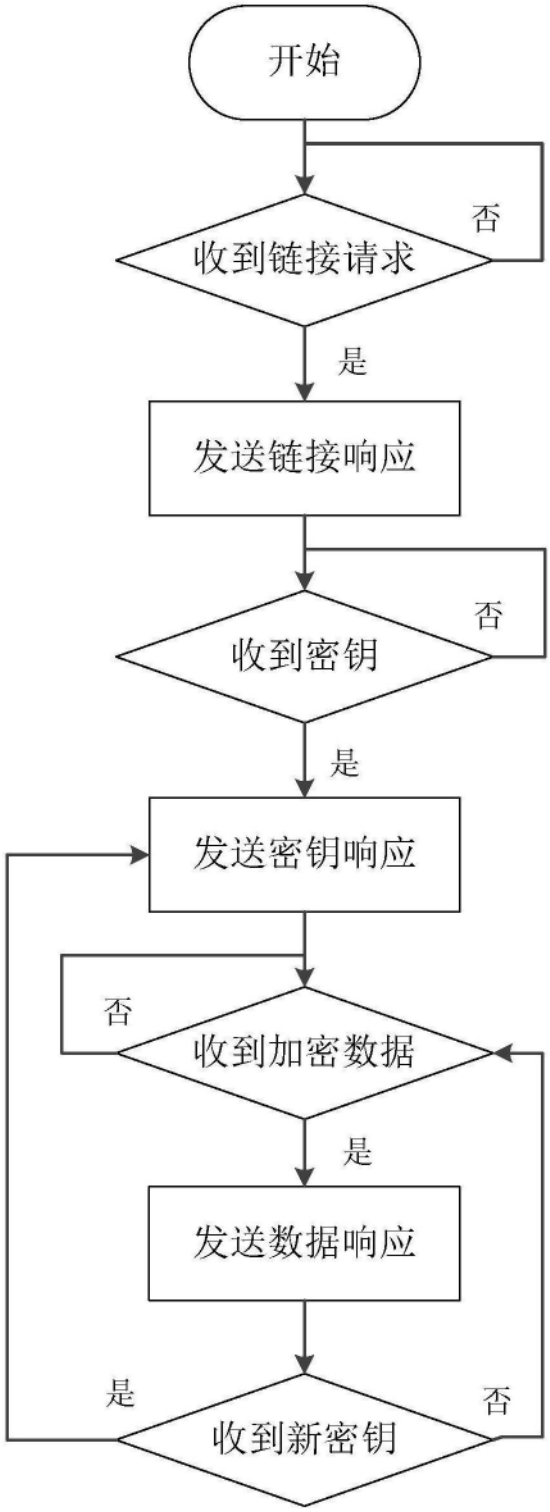


图2

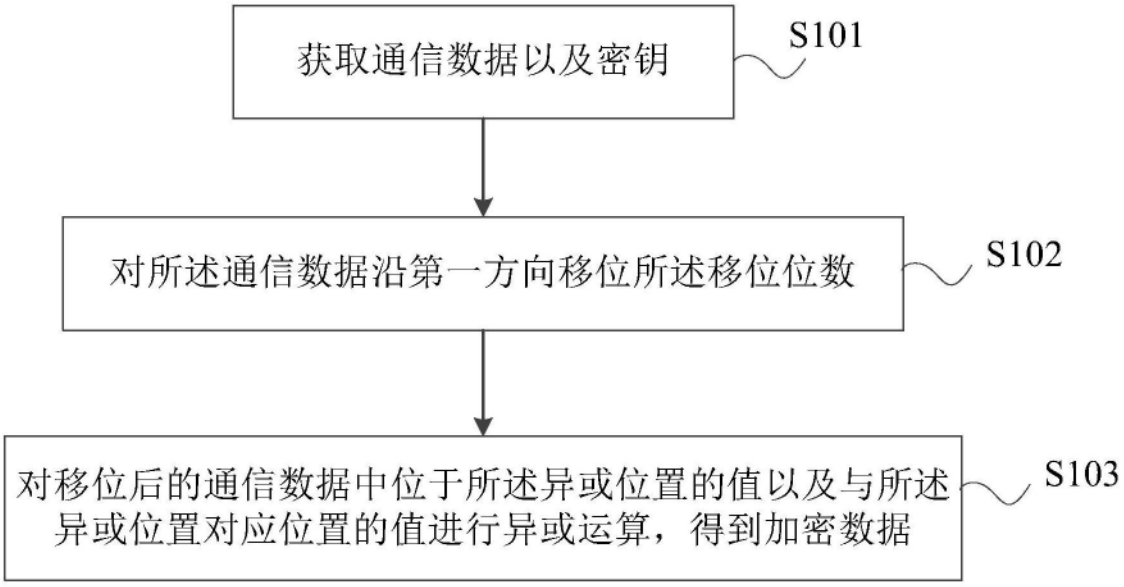

获取通信数据以及密钥
S101
对所述通信数据沿第一方向移位所述移位位数
S102
对移位后的通信数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到加密数据
S103

图3

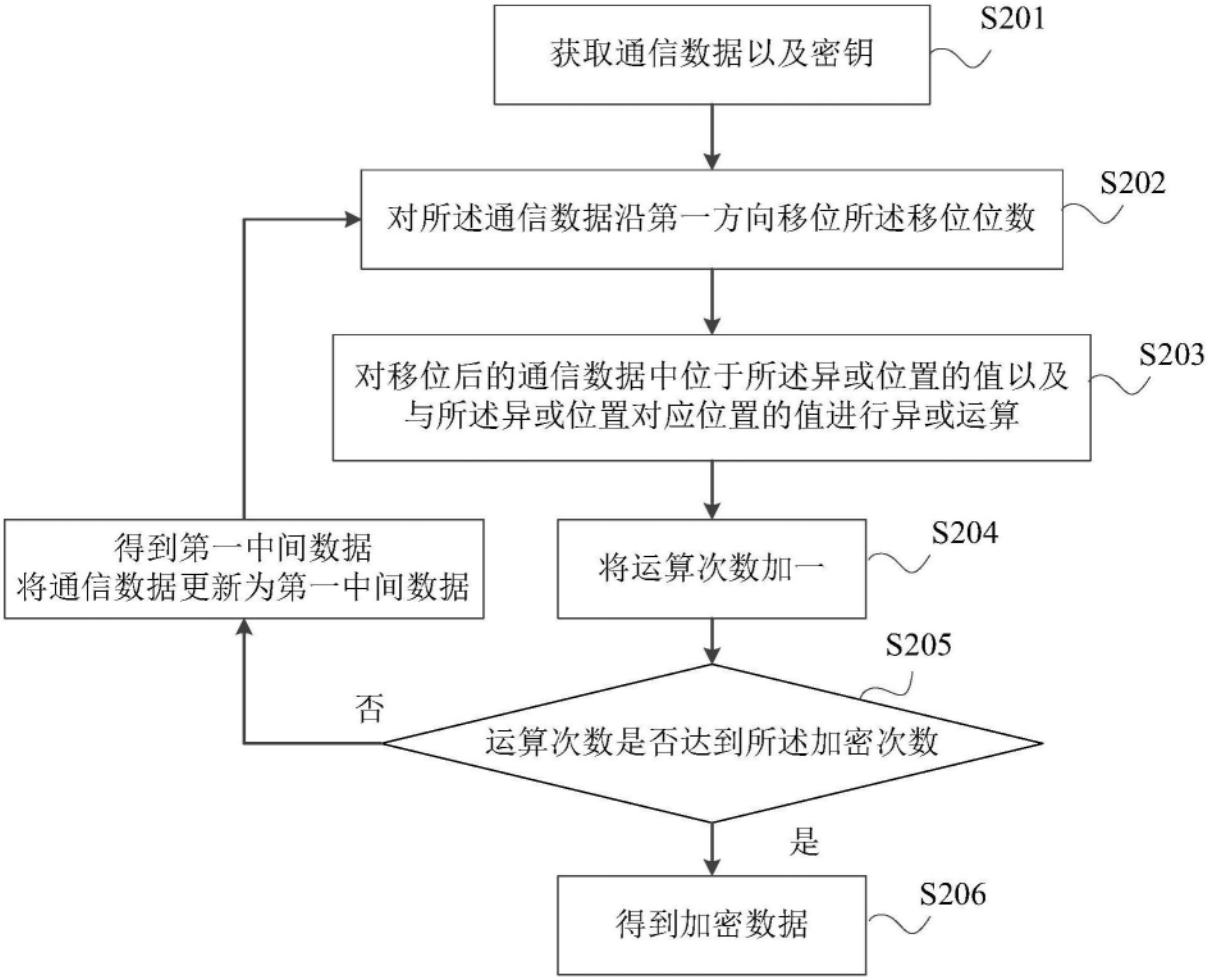

获取通信数据以及密钥
S201
对所述通信数据沿第一方向移位所述移位位数
S202
对移位后的通信数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算
S203
将运算次数加一
S204
运算次数是否达到所述加密次数
S205
否
是
得到第一中间数据
将通信数据更新为第一中间数据
得到加密数据
S206

图4

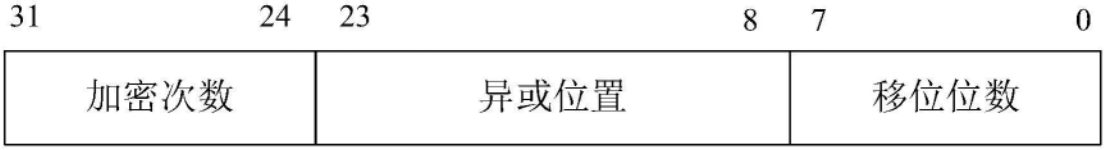

31
24
23
8
7
0
加密次数
异或位置
移位位数

图5

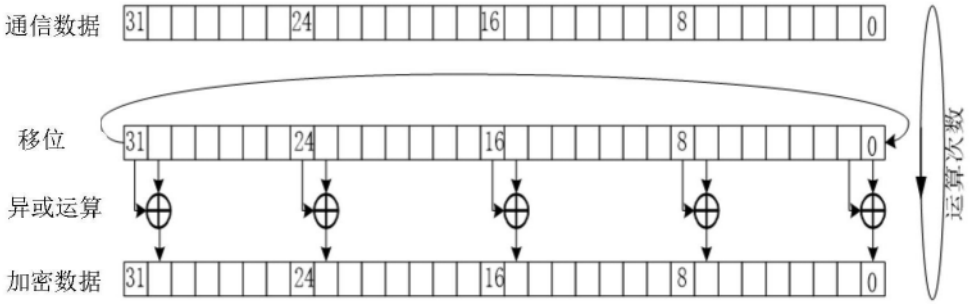

通信数据
移位
异或运算
加密数据
31
24
16
8
0
运算次数

图6

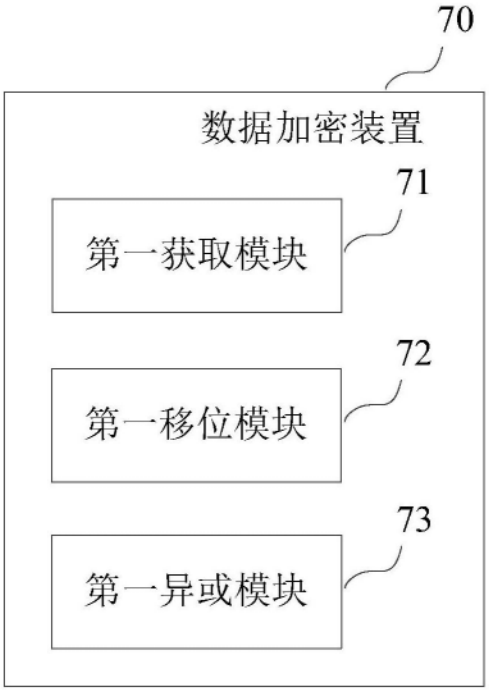

70
数据加密装置
71
第一获取模块
72
第一移位模块
73
第一异或模块

图7

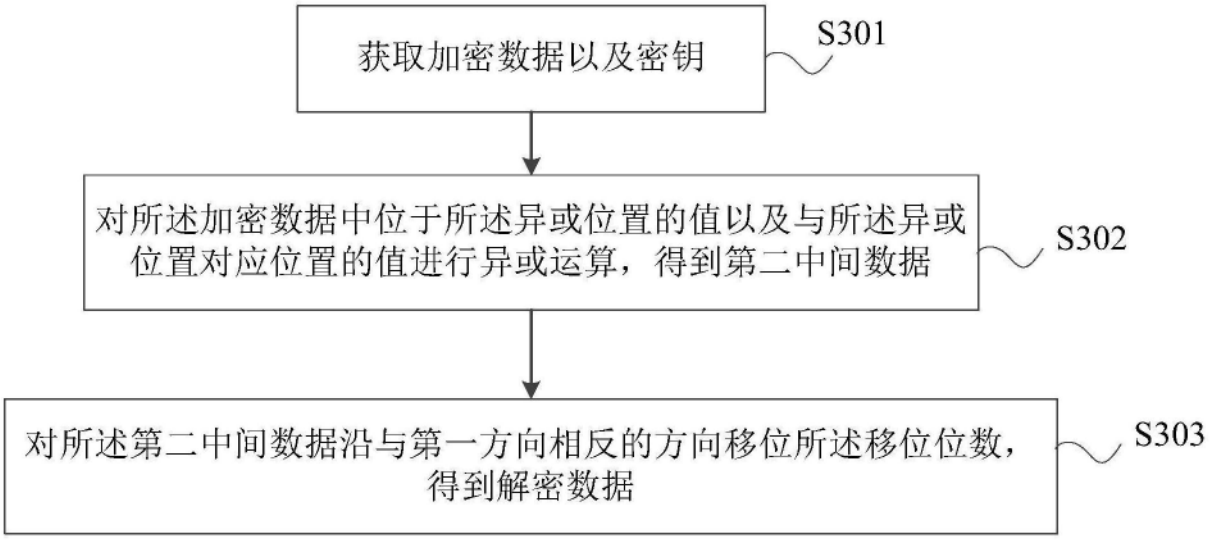

获取加密数据以及密钥
S301
对所述加密数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到第二中间数据
S302
对所述第二中间数据沿与第一方向相反的方向移位所述移位位数，得到解密数据
S303

图8

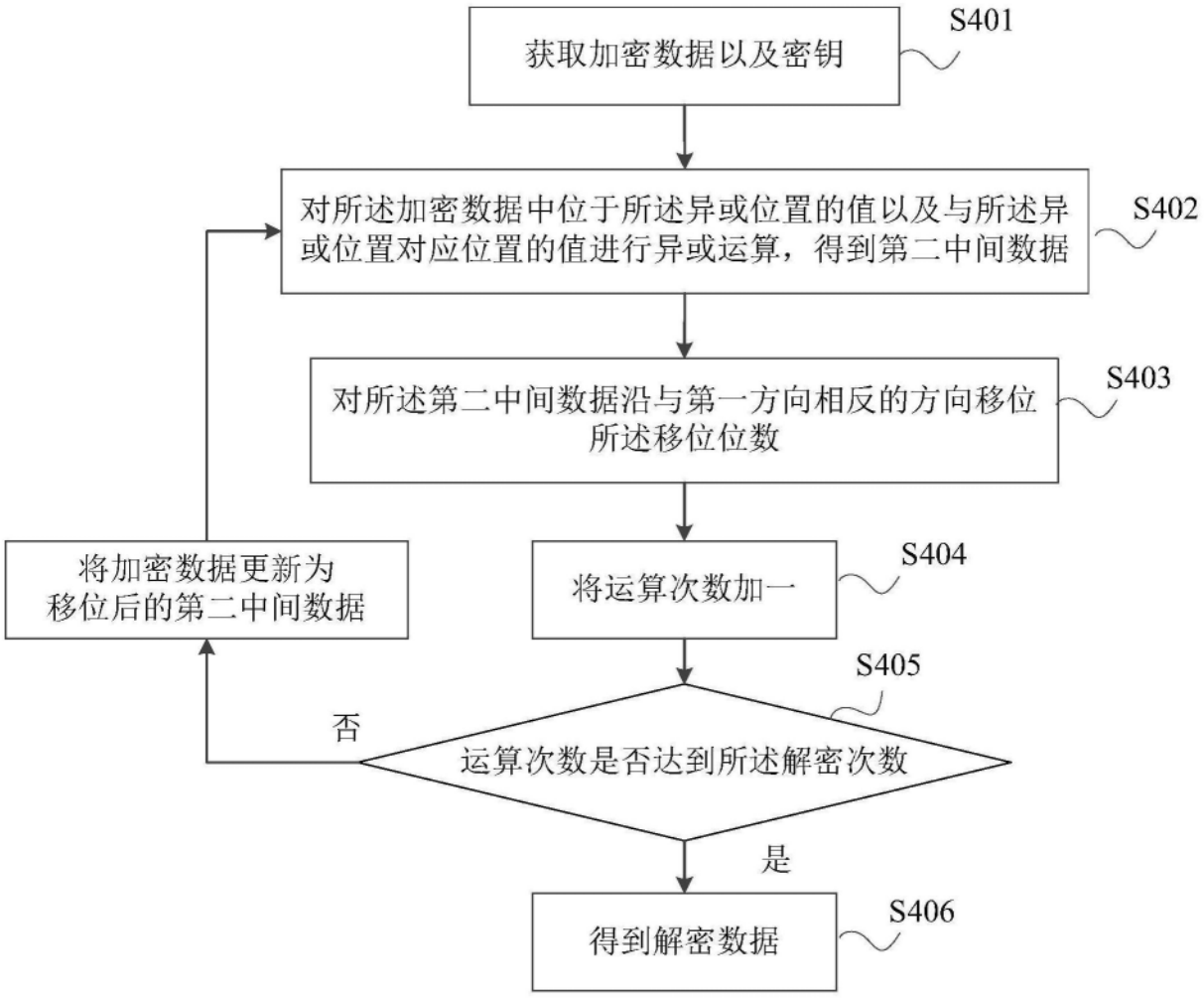

获取加密数据以及密钥
S401
对所述加密数据中位于所述异或位置的值以及与所述异或位置对应位置的值进行异或运算，得到第二中间数据
S402
对所述第二中间数据沿与第一方向相反的方向移位所述移位位数
S403
将运算次数加一
S404
运算次数是否达到所述解密次数
S405
否
是
将加密数据更新为移位后的第二中间数据
得到解密数据
S406

图9

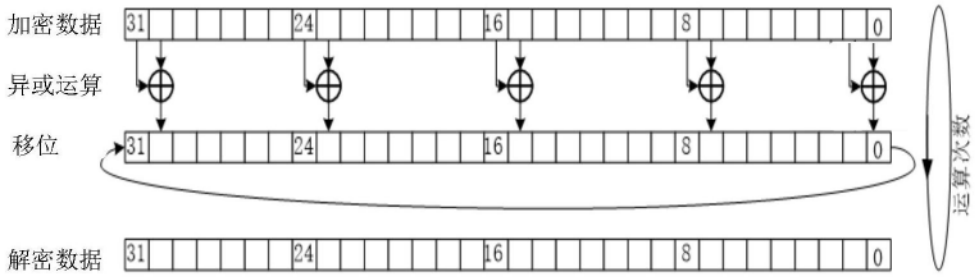

加密数据
异或运算
移位
解密数据
31
24
16
8
0
运算次数

图10

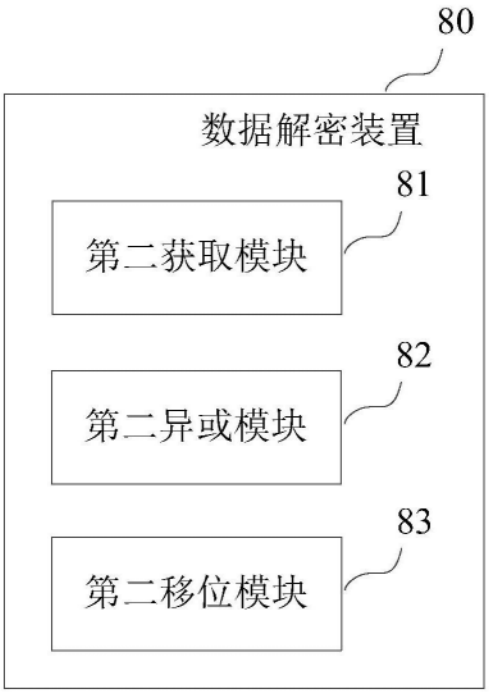

80
数据解密装置
81
第二获取模块
82
第二异或模块
83
第二移位模块

图11

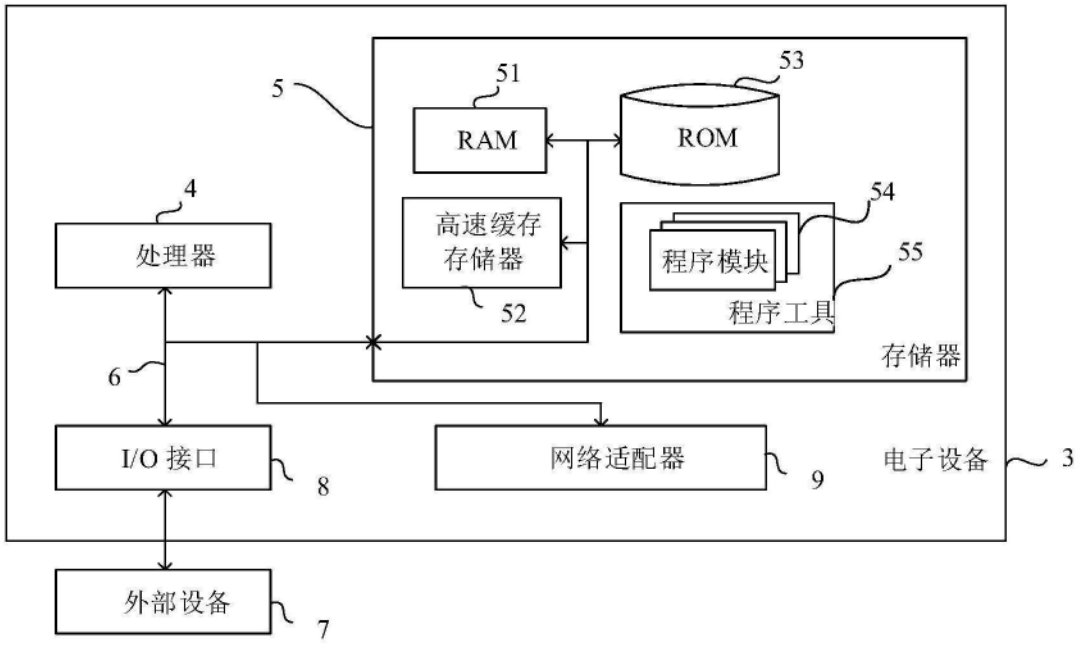

5
51
RAM
53
ROM
4
处理器
高速缓存
存储器
52
54
程序模块
55
程序工具
存储器
6
I/O 接口
8
网络适配器
9
电子设备
3
外部设备
7

图12