(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112751663 B
(45)授权公告日 2022.12.23

(21)申请号 202011641668.6

(22)申请日 2020.12.31

(65)同一申请的已公布的文献号
申请公布号 CN 112751663 A

(43)申请公布日 2021.05.04

(73)专利权人 南方电网科学研究院有限责任公司
地址 510663 广东省广州市萝岗区科学城科翔路11号J1栋3、4、5楼及J3栋3楼
专利权人 中国南方电网有限责任公司

(72)发明人 肖勇 崔超 赵云 林伟斌 王浩林

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 贾小慧

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

(56)对比文件
CN 103812641 A,2014.05.21
CN 108206735 A,2018.06.26
US 2016182542 A1,2016.06.23
US 2018262525 A1,2018.09.13

审查员 牛威

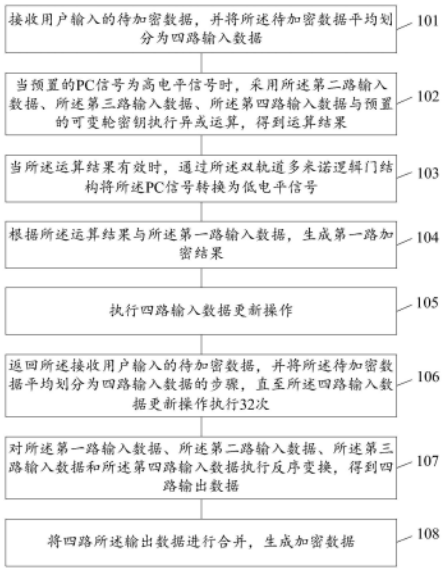
权利要求书2页 说明书8页 附图6页

(54)发明名称

一种数据加密方法和装置

(57)摘要

本发明公开了一种数据加密方法和装置，涉及双轨道多米诺逻辑门结构，方法包括：接收输入的待加密数据，并将待加密数据划分为四路输入数据；当预置的PC信号为高电平信号时，采用第二路输入数据、第三路输入数据、第四路输入数据与可变轮密钥执行异或运算，得到运算结果；当运算结果有效时，通过双轨道多米诺逻辑门结构将PC信号转换为低电平信号；根据运算结果与第一路输入数据，生成第一路加密结果；执行四路输入数据更新操作；重复执行32次上述操作后，对四路输入数据执行反序变换，得到四路输出数据并合并生成加密数据。该方法提高了加密过程的速度，同时由于多米诺逻辑门结构的加入，降低加密功耗，提高加密安全性。



CN 112751663 B

1.一种数据加密方法,其特征在于,涉及双轨道多米诺逻辑门结构,所述方法包括:

接收用户输入的待加密数据,并将所述待加密数据平均划分为四路输入数据;其中,所述四路输入数据包括第一路输入数据、第二路输入数据、第三路输入数据和第四路输入数据;

当预置的PC信号为高电平信号时,采用所述第二路输入数据、所述第三路输入数据、所述第四路输入数据与预置的可变轮密钥执行异或运算,得到运算结果;

当所述运算结果有效时,通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号;

根据所述运算结果与所述第一路输入数据,生成第一路加密结果;

执行四路输入数据更新操作;

返回所述接收用户输入的待加密数据,并将所述待加密数据平均划分为四路输入数据的步骤,直至所述四路输入数据更新操作执行32次;

对所述第一路输入数据、所述第二路输入数据、所述第三路输入数据和所述第四路输入数据执行反序变换,得到四路输出数据;

将四路所述输出数据进行合并,生成加密数据。

2.根据权利要求1所述的一种数据加密方法,其特征在于,在所述执行四路输入数据更新操作的步骤之后,所述方法还包括:

从预置的轮密钥组中选择与所述可变轮密钥不同的轮密钥作为新的可变轮密钥。

3.根据权利要求1所述的一种数据加密方法,其特征在于,所述根据所述运算结果与所述第一路输入数据,生成第一路加密结果的步骤包括:

采用预置的可逆变换算法对所述运算结果执行合成置换操作,生成中间结果;

采用所述中间结果与所述第一路输入数据执行异或运算,生成第一路加密结果。

4.根据权利要求1所述的方法,其特征在于,所述执行四路输入数据更新操作的步骤包括:

采用所述第二路输入数据更新所述第一路输入数据;

采用所述第三路输入数据更新所述第二路输入数据;

采用所述第四路输入数据更新所述第三路输入数据;

采用所述第一路加密结果更新所述第四路输入数据。

5.根据权利要求1所述的一种数据加密方法,其特征在于,在所述当所述运算结果有效时,通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号的步骤之后,所述方法还包括:

返回所述低电平信号到上一级的双轨道多米诺逻辑门结构,使得所述上一级的双轨道多米诺逻辑门结构所对应的运算结果有效。

6.一种数据加密装置,其特征在于,涉及双轨道多米诺逻辑门结构,所述装置包括:

输入数据划分模块,用于接收用户输入的待加密数据,并将所述待加密数据平均划分为四路输入数据;其中,所述四路输入数据包括第一路输入数据、第二路输入数据、第三路输入数据和第四路输入数据;

运算结果生成模块,用于当预置的PC信号为高电平信号时,采用所述第二路输入数据、所述第三路输入数据、所述第四路输入数据与预置的可变轮密钥执行异或运算,得到运算

结果；

低电平信号转换模块，用于当所述运算结果有效时，通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号；

第一路加密结果生成模块，用于根据所述运算结果与所述第一路输入数据，生成第一路加密结果；

数据更新模块，用于执行四路输入数据更新操作；

重复执行模块，用于返回所述接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据的步骤，直至所述四路输入数据更新操作执行32次；

四路输出数据生成模块，用于对所述第一路输入数据、所述第二路输入数据、所述第三路输入数据和所述第四路输入数据执行反序变换，得到四路输出数据；

加密数据生成模块，用于将四路所述输出数据进行合并，生成加密数据。

7.根据权利要求6所述的一种数据加密装置，其特征在于，所述装置还包括：

轮密钥重选模块，用于从预置的轮密钥组中选择与所述可变轮密钥不同的轮密钥作为新的可变轮密钥。

8.根据权利要求6所述的一种数据加密装置，其特征在于，所述第一路加密结果生成模块包括：

中间结果生成子模块，用于采用预置的可逆变换算法对所述运算结果执行合成置换操作，生成中间结果；

第一路加密结果生成子模块，用于采用所述中间结果与所述第一路输入数据执行异或运算，生成第一路加密结果。

9.根据权利要求6所述的装置，其特征在于，所述数据更新模块包括：

第一路输入数据更新子模块，用于采用所述第二路输入数据更新所述第一路输入数据；

第二路输入数据更新子模块，用于采用所述第三路输入数据更新所述第二路输入数据；

第三路输入数据更新子模块，用于采用所述第四路输入数据更新所述第三路输入数据；

第四路输入数据更新子模块，用于采用所述第一路加密结果更新所述第四路输入数据。

10.根据权利要求6所述的一种数据加密装置，其特征在于，所述装置还包括：

信号返回模块，用于返回所述低电平信号到上一级的双轨道多米诺逻辑门结构，使得所述上一级的双轨道多米诺逻辑门结构所对应的运算结果有效。

一种数据加密方法和装置

技术领域

[0001] 本发明涉及数据加密技术领域，尤其涉及一种数据加密方法和装置。

背景技术

[0002] 当今是信息科技高速发展的时代，互联网正迅速成为各行各业的载体，推动着行业的进步，而物联网作为提高互联网应用的基础媒介以及先驱，大大提高着行业生产和人们生活的效率。它的应用被称为继计算机、互联网之后世界信息产业发展的第三次浪潮，因此，物联网的安全性问题也备受人们关注。

[0003] 集成电路制造工艺的飞速发展，片上系统SoC应运而生。SoC极大地缩小了系统体积，提高了系统的性能；SoC以其集成度高、体积小、功耗少、可靠性好、产品问世周期短等优点得到了越来越广泛地应用。然而在目前市场有些产品采用软件加密方式，导致数据加密速度慢、周期长，同时还有一些产品加密完全由硬件完成，虽然速度较快，但芯片面积较大、功耗较高，无法满足物联网产品的低功耗要求。同时，几乎市场上绝大多数产品都将密钥保存在非易失性存储器中，从而很容易受到侵入式攻击，导致密钥被复制窃取。这些问题严重制约着物联网的普及和发展，对物联网产品带来极大的安全隐患。

发明内容

[0004] 本发明提供了一种数据加密方法和装置，解决了现有的数据加密方法由于软件缺陷所导致的加密速度较慢，硬件加密所导致的功耗较高以及密钥保存方式导致出现安全隐患的技术问题。

[0005] 本发明提供的一种数据加密方法，涉及双轨道多米诺逻辑门结构，所述方法包括：

[0006] 接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据；其中，所述四路输入数据包括第一路输入数据、第二路输入数据、第三路输入数据和第四路输入数据；

[0007] 当预置的PC信号为高电平信号时，采用所述第二路输入数据、所述第三路输入数据、所述第四路输入数据与预置的可变轮密钥执行异或运算，得到运算结果；

[0008] 当所述运算结果有效时，通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号；

[0009] 根据所述运算结果与所述第一路输入数据，生成第一路加密结果；

[0010] 执行四路输入数据更新操作；

[0011] 返回所述接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据的步骤，直至所述四路输入数据更新操作执行32次；

[0012] 对所述第一路输入数据、所述第二路输入数据、所述第三路输入数据和所述第四路输入数据执行反序变换，得到四路输出数据；

[0013] 将四路所述输出数据进行合并，生成加密数据。

[0014] 可选地，在所述执行四路输入数据更新操作的步骤之后，所述方法还包括：

[0015] 从预置的轮密钥组中选择与所述可变轮密钥不同的轮密钥作为新的可变轮密钥。

[0016] 可选地，所述根据所述运算结果与所述第一路输入数据，生成第一路加密结果的步骤包括：

[0017] 采用预置的可逆变换算法对所述运算结果执行合成置换操作，生成中间结果；

[0018] 采用所述中间结果与所述第一路输入数据执行异或运算，生成第一路加密结果。

[0019] 可选地，所述执行四路输入数据更新操作的步骤包括：

[0020] 采用所述第二路输入数据更新所述第一路输入数据；

[0021] 采用所述第三路输入数据更新所述第二路输入数据；

[0022] 采用所述第四路输入数据更新所述第三路输入数据；

[0023] 采用所述第一路加密结果更新所述第四路输入数据。

[0024] 可选地，在所述当所述运算结果有效时，通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号的步骤之后，所述方法还包括：

[0025] 返回所述低电平信号到上一级的双轨道多米诺逻辑门结构，使得所述上一级的双轨道多米诺逻辑门结构所对应的运算结果有效。

[0026] 本发明还提供了一种数据加密装置，涉及双轨道多米诺逻辑门结构，所述装置包括：

[0027] 输入数据划分模块，用于接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据；其中，所述四路输入数据包括第一路输入数据、第二路输入数据、第三路输入数据和第四路输入数据；

[0028] 运算结果生成模块，用于当预置的PC信号为高电平信号时，采用所述第二路输入数据、所述第三路输入数据、所述第四路输入数据与预置的可变轮密钥执行异或运算，得到运算结果；

[0029] 低电平信号转换模块，用于当所述运算结果有效时，通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号；

[0030] 第一路加密结果生成模块，用于根据所述运算结果与所述第一路输入数据，生成第一路加密结果；

[0031] 数据更新模块，用于执行四路输入数据更新操作；

[0032] 重复执行模块，用于返回所述接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据的步骤，直至所述四路输入数据更新操作执行32次；

[0033] 四路输出数据生成模块，用于对所述第一路输入数据、所述第二路输入数据、所述第三路输入数据和所述第四路输入数据执行反序变换，得到四路输出数据；

[0034] 加密数据生成模块，用于将四路所述输出数据进行合并，生成加密数据。

[0035] 可选地，所述装置还包括：

[0036] 轮密钥重选模块，用于从预置的轮密钥组中选择与所述可变轮密钥不同的轮密钥作为新的可变轮密钥。

[0037] 可选地，所述第一路加密结果生成模块包括：

[0038] 中间结果生成子模块，用于采用预置的可逆变换算法对所述运算结果执行合成置换操作，生成中间结果；

[0039] 第一路加密结果生成子模块，用于采用所述中间结果与所述第一路输入数据执行

异或运算,生成第一路加密结果。

[0040] 可选地,所述数据更新模块包括:

[0041] 第一路输入数据更新子模块,用于采用所述第二路输入数据更新所述第一路输入数据;

[0042] 第二路输入数据更新子模块,用于采用所述第三路输入数据更新所述第二路输入数据;

[0043] 第三路输入数据更新子模块,用于采用所述第四路输入数据更新所述第三路输入数据;

[0044] 第四路输入数据更新子模块,用于采用所述第一路加密结果更新所述第四路输入数据。

[0045] 可选地,所述装置还包括:

[0046] 信号返回模块,用于返回所述低电平信号到上一级的双轨道多米诺逻辑门结构,使得所述上一级的双轨道多米诺逻辑门结构所对应的运算结果有效。

[0047] 从以上技术方案可以看出,本发明具有以下优点:

[0048] 本发明通过接收用户输入的待加密数据并划分为四路数据,将除第一路数据以外的三路数据与预置的可变轮密钥执行异或运算,得到运算结果;当运算结果有效时,通过双轨道多米诺逻辑门结构将PC信号转换为低电平信号,再根据运算结果与第一路输入数据的异或操作,生成第一路加密结果,执行四路输入数据更新操作,重复31次后,对四路数据执行反序变换,以得到四路输出数据;最后合并四路输出数据以生成加密数据。该方法提高了加密过程的速度,同时由于多米诺逻辑门结构的加入,降低加密功耗,提高加密安全性。

附图说明

[0049] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动性的前提下,还可以根据这些附图获得其它的附图。

[0050] 图1为本发明实施例提供的一种数据加密方法的步骤流程图;

[0051] 图2为本发明实施例中的双轨道多米诺逻辑门的异或结构示意图;

[0052] 图3为本发明实施例中的双轨道多米诺逻辑门的与门结构示意图;

[0053] 图4为本发明可选实施例提供的一种数据加密方法的步骤流程图;

[0054] 图5为本发明实施例提供的一种数据加密装置的数据流程图;

[0055] 图6为本发明实施例提供的一种数据加密装置的结构框图。

具体实施方式

[0056] 随着无线区域网标准的推广应用,我国自主设计了SM4对称分组密码算法,该算法加解密速度快,硬件实现简单以及具备一定的安全性,多适用于制作密码芯片,现已大量运用于对金融领域、物联网等重要数据的保护。因此单纯从研究密码算法的结构而判断密码算法的安全性已经远远不够,我们必须还从密码算法的实现角度来考虑运行的速度和功耗设计,这样可以大幅度的改善芯片的质量。因此本发明实施例提供了一种数据加密方法和

装置，用于解决现有的数据加密方法由于软件缺陷所导致的加密速度较慢，硬件加密所导致的功耗较高以及密钥保存方式导致出现安全隐患的技术问题。

[0057] 为使得本发明的发明目的、特征、优点能够更加的明显和易懂，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，下面所描述的实施例仅仅是本发明一部分实施例，而非全部的实施例。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它实施例，都属于本发明保护的范围。

[0058] 请参阅图1，图1为本发明实施例提供的一种数据加密方法的步骤流程图。

[0059] 本发明提供的一种数据加密方法，涉及双轨道多米诺逻辑门结构，所述方法包括：

[0060] 步骤101，接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据；

[0061] 其中，所述四路输入数据包括第一路输入数据、第二路输入数据、第三路输入数据和第四路输入数据；

[0062] 步骤102，当预置的PC信号为高电平信号时，采用所述第二路输入数据、所述第三路输入数据、所述第四路输入数据与预置的可变轮密钥执行异或运算，得到运算结果；

[0063] 步骤103，当所述运算结果有效时，通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号；

[0064] 在本发明实施例中，多米诺逻辑门指的是一类在动态逻辑门之间插入静态反向器以避免动态逻辑门直接级联时，产生过早放电的动态电路。由于电路状态变化在级联的各级间依次传播，像多米诺骨牌，所以才被称为多米诺逻辑。而双轨道多米诺逻辑门，指的是在多米诺逻辑门上采用同步双路的形式的设计，以降低硬件资源损耗和功耗。

[0065] 请参阅图2，图2示出了本发明实施例中的双轨道多米诺逻辑门的异或结构示意图，其中包括多个场效应管，PC表示预充电信号，q_t和a_f表示输出信号。当PC信号为0时，输出端q_t和q_f都是为0信号，表示输出信号无效；当PC信号为1时，输出端q_t和q_f都是为1信号，表示输出信号有效。

[0066] 请参阅图3，图3示出了本发明实施例中的双轨道多米诺逻辑门的与门结构示意图，其中包括多个场效应管，PC表示预充电信号，q_t和a_f表示输出信号。当PC信号为0时，输出端q_t和q_f都是为0信号，表示输出信号无效；当PC信号为1时，输出端q_t和q_f都是为1信号，表示输出信号有效。

[0067] 步骤104，根据所述运算结果与所述第一路输入数据，生成第一路加密结果；

[0068] 步骤105，执行四路输入数据更新操作；

[0069] 步骤106，返回所述接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据的步骤，直至所述四路输入数据更新操作执行32次；

[0070] 步骤107，对所述第一路输入数据、所述第二路输入数据、所述第三路输入数据和所述第四路输入数据执行反序变换，得到四路输出数据；

[0071] 所述反序变换指的是根据字节流中保存的对象状态及描述信息，通过反序列化重建对象。例如密文C＝(Y0,Y1,Y2,Y3)＝R(X32.X33,X34,X35)＝(X35, X34,X33,X32)。

[0072] 步骤108，将四路所述输出数据进行合并，生成加密数据。

[0073] 在本发明实施例中，通过接收用户输入的待加密数据并划分为四路数据，将除第

一路数据以外的三路数据与预置的可变轮密钥执行异或运算，得到运算结果；当运算结果有效时，通过双轨道多米诺逻辑门结构将PC信号转换为低电平信号，再根据运算结果与第一路输入数据的异或操作，生成第一路加密结果，执行四路输入数据更新操作，重复31次后，对四路数据执行反序变换，以得到四路输出数据；最后合并四路输出数据以生成加密数据。该方法提高了加密过程的速度，同时由于多米诺逻辑门结构的加入，降低加密功耗，提高加密安全性。

[0074] 请参阅图4，图4为本发明实施例提供的一种数据加密方法的步骤流程图。

[0075] 本发明提供的一种数据加密方法，涉及双轨道多米诺逻辑门结构，所述方法包括：

[0076] 步骤401，接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据；其中，所述四路输入数据包括第一路输入数据、第二路输入数据、第三路输入数据和第四路输入数据；

[0077] 在本发明实施例中，每一轮的数据加密的逻辑门均由信号PC控制，当电路中第一次开始工作时，所有的PC信号必须复位为零一段时间为电路预先充电，然后PC信号转换为高电平，等待有效数据的计算。

[0078] 步骤402，当预置的PC信号为高电平信号时，采用所述第二路输入数据、所述第三路输入数据、所述第四路输入数据与预置的可变轮密钥执行异或运算，得到运算结果；

[0079] 在具体实现中，以第二路输入数据X1、第三路输入数据X2和第四路输入数据X3为例，运算结果X可以通过以下公式进行计算：

[0080] $$X=X1\oplus X2\oplus X3\oplus rki$$

[0081] 其中，rki指的是第i轮的可变轮密钥。

[0082] 步骤403，当所述运算结果有效时，通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号；

[0083] 在本发明实施例中，若运算结果有效时，通过双轨道多米诺逻辑门结构件 PC信号转换为低电平信号，以启动加密进程，对第一路输入数据进行加密。

[0084] 步骤404，返回所述低电平信号到上一级的双轨道多米诺逻辑门结构，使得所述上一级的双轨道多米诺逻辑门结构所对应的运算结果有效。

[0085] 在具体实现中，在多个数据需要进行流水线加密时，需要对上一轮电路进行预充电，此时可以将低电平信号返回到上一级双轨道多米诺逻辑门结果，以保证上一级的双轨道多米诺逻辑门结构所对应的运算结果有效。

[0086] 步骤405，根据所述运算结果与所述第一路输入数据，生成第一路加密结果；

[0087] 进一步地，所述步骤405可以包括以下子步骤：

[0088] 采用预置的可逆变换算法对所述运算结果执行合成置换操作，生成中间结果；

[0089] 采用所述中间结果与所述第一路输入数据执行异或运算，生成第一路加密结果。

[0090] 在本发明的一个示例中，采用可逆变换算法对运算结果执行合成置换操作，以得到中间结果，采用中间结果与第一路输入数据进行异或运算，生成第一路加密结果。

[0091] 其中，可逆变换算法指的是可逆线性变换(invertible linear transformation)亦称非退化线性变换，或满秩线性变换，是一种特殊的线性变换，设V是数域P上的线性空间，σ是V的线性变换，若存在V的变换τ，使στ＝τσ＝I，其中I为单位变换，则σ称为可逆线性变换，τ称为σ的逆变换，V上的可逆线性变换σ的逆变换仍为V的线性变换，且是惟一的，记为

σ^{-1}。

[0092] 合成置换操作指的是可逆变换，由一个非线性变换r和线性变换L复合而成的，即T(a)＝L(r(a))，a为运算结果。

[0093] 步骤406，执行四路输入数据更新操作；

[0094] 在本发明实施例中，所述步骤406可以包括以下子步骤：

[0095] 采用所述第二路输入数据更新所述第一路输入数据；

[0096] 采用所述第三路输入数据更新所述第二路输入数据；

[0097] 采用所述第四路输入数据更新所述第三路输入数据；

[0098] 采用所述第一路加密结果更新所述第四路输入数据。

[0099] 可选地，在所述步骤406之后，所述方法还包括：

[0100] 从预置的轮密钥组中选择与所述可变轮密钥不同的轮密钥作为新的可变轮密钥。

[0101] 在本发明实施例中，加密密钥的长度为128比特，表示为MK＝(MK0,MK1,MK2,MK3)，其中MKi为32位，可变轮密钥表示为(rk0,rk1,……, rk31)，其中rki为32位。可以通过密钥扩展方法：设$(K0, K1, K2, K3)=(MK0 \oplus FK0, MK1 \oplus FK1, MK2 \oplus FK2, MK3 \oplus FK3)$，以得到$rki=Ki+4=Ki \oplus T'(Ki+1 \oplus Ki+2 \oplus Ki+3 \oplus CKi)$。

[0102] 步骤407，返回所述接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据的步骤，直至所述四路输入数据更新操作执行32次；

[0103] 步骤408，对所述第一路输入数据、所述第二路输入数据、所述第三路输入数据和所述第四路输入数据执行反序变换，得到四路输出数据；

[0104] 步骤409，将四路所述输出数据进行合并，生成加密数据。

[0105] 在本发明实施例中，通过接收用户输入的待加密数据并划分为四路数据，将除第一路数据以外的三路数据与预置的可变轮密钥执行异或运算，得到运算结果；当运算结果有效时，通过双轨道多米诺逻辑门结构将PC信号转换为低电平信号，再根据运算结果与第一路输入数据的异或操作，生成第一路加密结果，执行四路输入数据更新操作，重复31次后，对四路数据执行反序变换，以得到四路输出数据；最后合并四路输出数据以生成加密数据。该方法提高了加密过程的速度，同时由于多米诺逻辑门结构的加入，降低加密功耗，提高加密安全性。

[0106] 请参阅图5，图5示出了本发明实施例的一种数据加密装置的数据流程图。

[0107] 通过输入128bit的待加密数据Plaintext X，划分为四路输入数据X0、X1、X2和X3，在进入到$Round_1$后，通过X1、X2、X3与rk1进行异或操作，得到运算结果后通过detect电路(即双路多米诺逻辑门结果)输出PC信号，并执行合成置换操作T后，与X0进行异或操作，生成第一路加密数据，再对每一路输入数据进行更新，将X0作为X4并进行移位，以此类推，直到32轮数据加密过程完成，将四路数据进行反序变化、合并后输出128bit的加密数据Ciphertext Y。

[0108] 请参阅图6，图6示出了本发明实施例的一种数据加密装置的结构框图。

[0109] 本发明还提供了一种数据加密装置，涉及双轨道多米诺逻辑门结构，所述装置包括：

[0110] 输入数据划分模块601，用于接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据；其中，所述四路输入数据包括第一路输入数据、第二路输入数据、第三路输入数据和第四路输入数据；

[0111] 运算结果生成模块602，用于当预置的PC信号为高电平信号时，采用所述第二路输入数据、所述第三路输入数据、所述第四路输入数据与预置的可变轮密钥执行异或运算，得到运算结果；

[0112] 低电平信号转换模块603，用于当所述运算结果有效时，通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号；

[0113] 第一路加密结果生成模块604，用于根据所述运算结果与所述第一路输入数据，生成第一路加密结果；

[0114] 数据更新模块605，用于执行四路输入数据更新操作；

[0115] 重复执行模块606，用于返回所述接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据的步骤，直至所述四路输入数据更新操作执行32次；

[0116] 四路输出数据生成模块607，用于对所述第一路输入数据、所述第二路输入数据、所述第三路输入数据和所述第四路输入数据执行反序变换，得到四路输出数据；

[0117] 加密数据生成模块608，用于将四路所述输出数据进行合并，生成加密数据。

[0118] 可选地，所述装置还包括：

[0119] 轮密钥重选模块，用于从预置的轮密钥组中选择与所述可变轮密钥不同的轮密钥作为新的可变轮密钥。

[0120] 可选地，所述第一路加密结果生成模块604包括：

[0121] 中间结果生成子模块，用于采用预置的可逆变换算法对所述运算结果执行合成置换操作，生成中间结果；

[0122] 第一路加密结果生成子模块，用于采用所述中间结果与所述第一路输入数据执行异或运算，生成第一路加密结果。

[0123] 可选地，所述数据更新模块605包括：

[0124] 第一路输入数据更新子模块，用于采用所述第二路输入数据更新所述第一路输入数据；

[0125] 第二路输入数据更新子模块，用于采用所述第三路输入数据更新所述第二路输入数据；

[0126] 第三路输入数据更新子模块，用于采用所述第四路输入数据更新所述第三路输入数据；

[0127] 第四路输入数据更新子模块，用于采用所述第一路加密结果更新所述第四路输入数据。

[0128] 可选地，所述装置还包括：

[0129] 信号返回模块，用于返回所述低电平信号到上一级的双轨道多米诺逻辑门结构，使得所述上一级的双轨道多米诺逻辑门结构所对应的运算结果有效。

[0130] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的装置的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0131] 在本发明所提供的几个实施例中，应该理解到，所揭露的装置和方法，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，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0132] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0133] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0134] 以上所述，以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

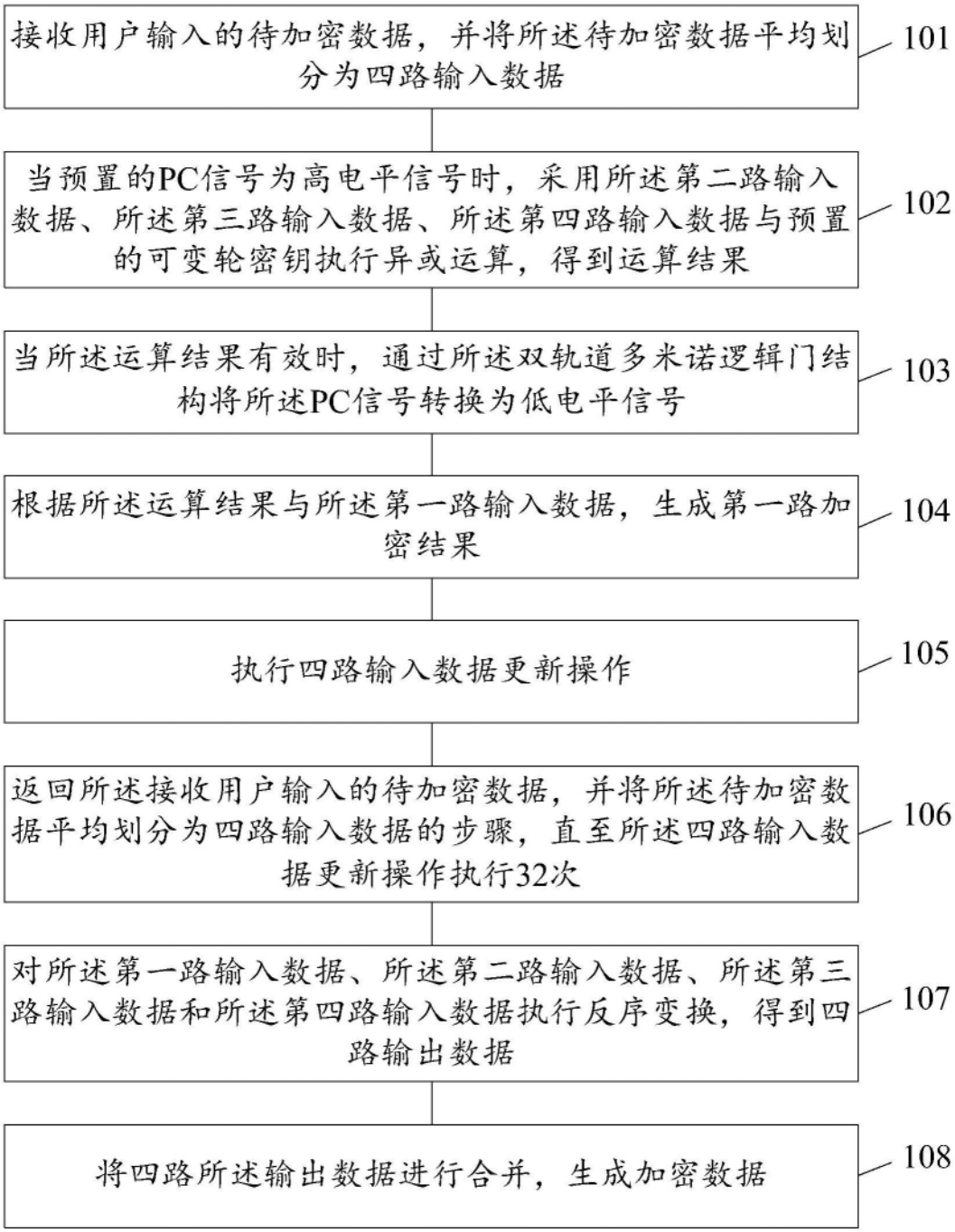

接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据
101
当预置的PC信号为高电平信号时，采用所述第二路输入数据、所述第三路输入数据、所述第四路输入数据与预置的可变轮密钥执行异或运算，得到运算结果
102
当所述运算结果有效时，通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号
103
根据所述运算结果与所述第一路输入数据，生成第一路加密结果
104
执行四路输入数据更新操作
105
返回所述接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据的步骤，直至所述四路输入数据更新操作执行32次
106
对所述第一路输入数据、所述第二路输入数据、所述第三路输入数据和所述第四路输入数据执行反序变换，得到四路输出数据
107
将四路所述输出数据进行合并，生成加密数据
108

图1

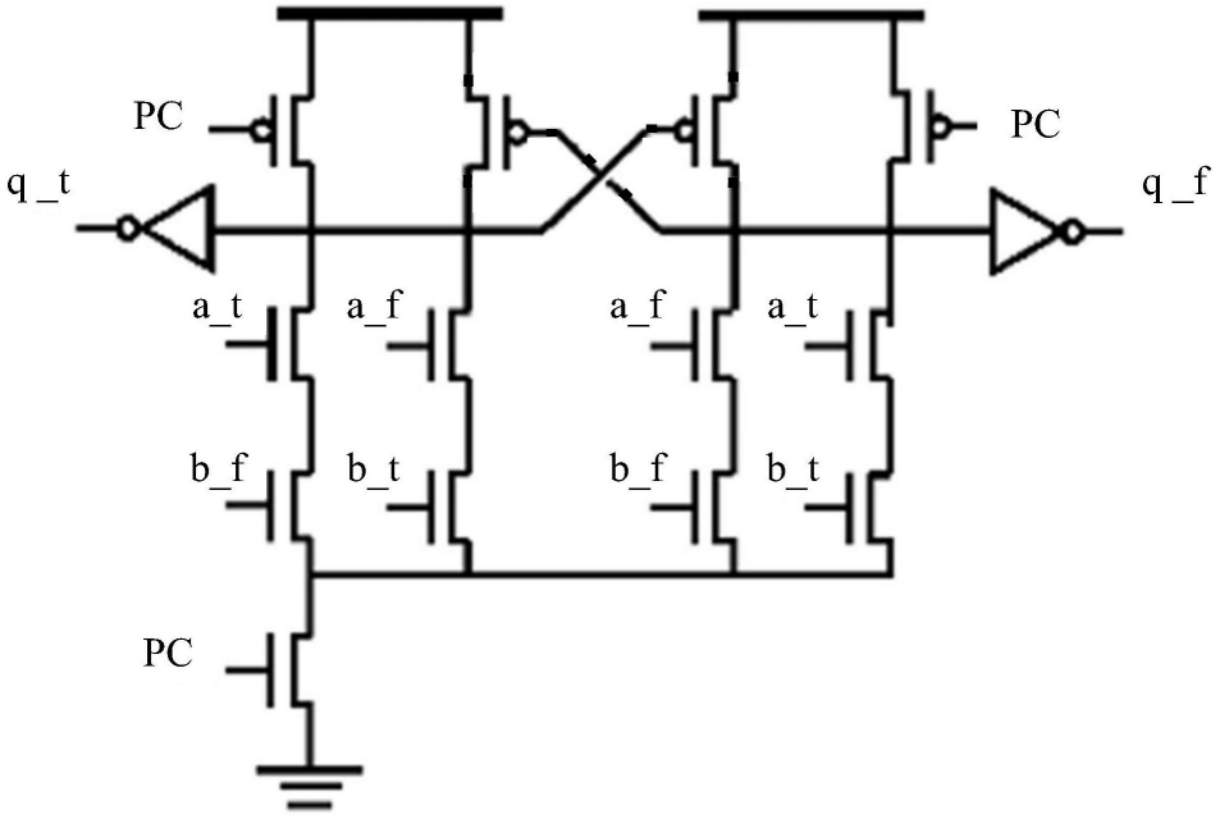


图2

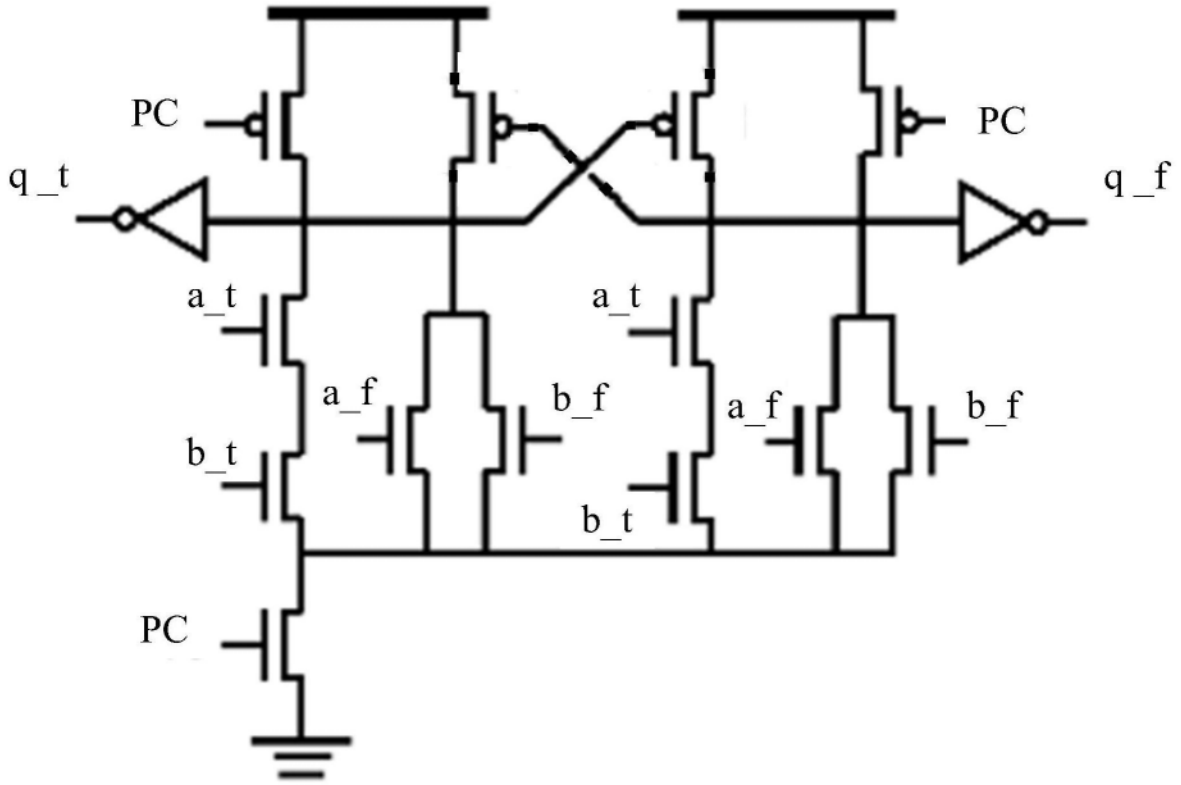


图3

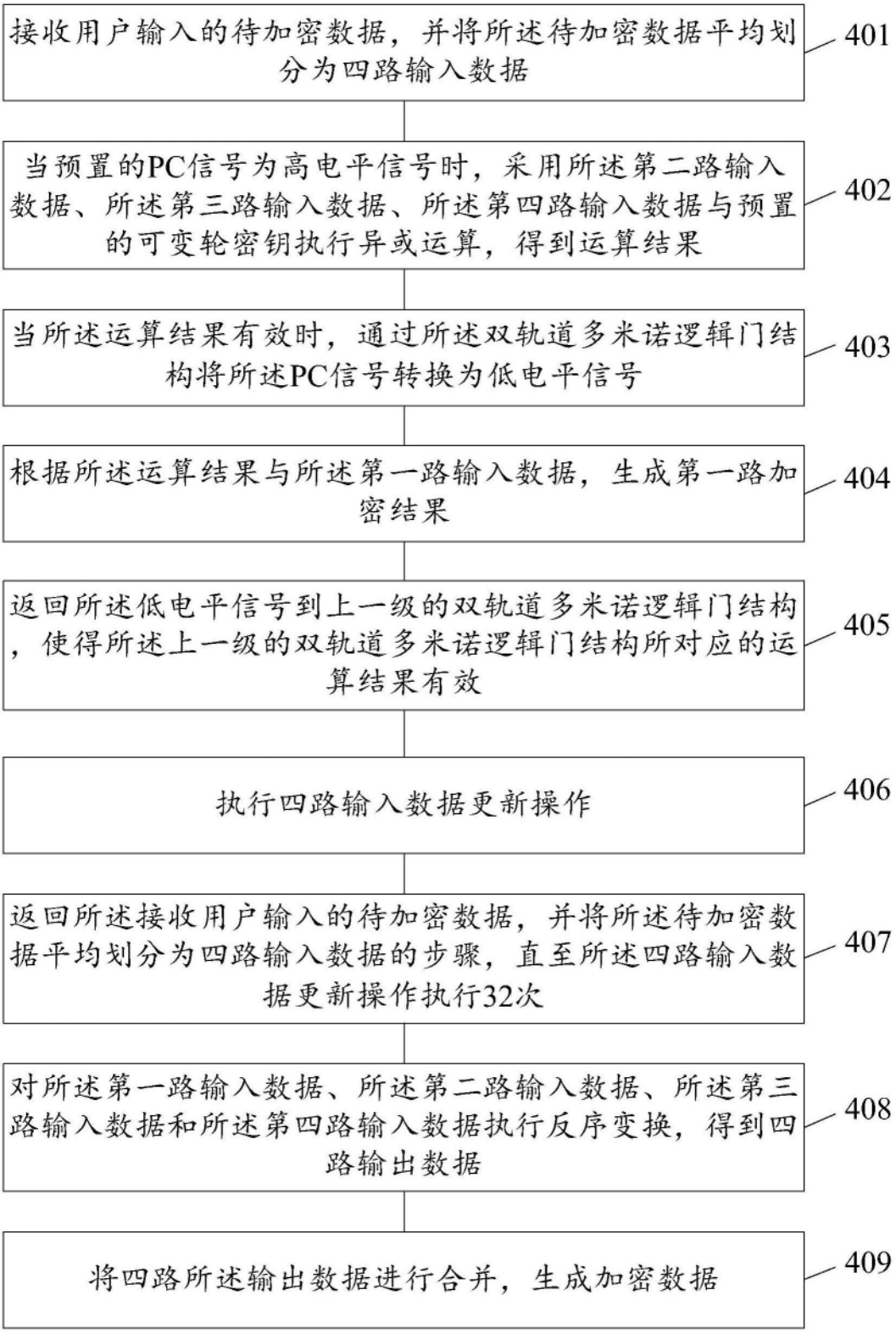

接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据
401
当预置的PC信号为高电平信号时，采用所述第二路输入数据、所述第三路输入数据、所述第四路输入数据与预置的可变轮密钥执行异或运算，得到运算结果
402
当所述运算结果有效时，通过所述双轨道多米诺逻辑门结构将所述PC信号转换为低电平信号
403
根据所述运算结果与所述第一路输入数据，生成第一路加密结果
404
返回所述低电平信号到上一级的双轨道多米诺逻辑门结构，使得所述上一级的双轨道多米诺逻辑门结构所对应的运算结果有效
405
执行四路输入数据更新操作
406
返回所述接收用户输入的待加密数据，并将所述待加密数据平均划分为四路输入数据的步骤，直至所述四路输入数据更新操作执行32次
407
对所述第一路输入数据、所述第二路输入数据、所述第三路输入数据和所述第四路输入数据执行反序变换，得到四路输出数据
408
将四路所述输出数据进行合并，生成加密数据
409

图4

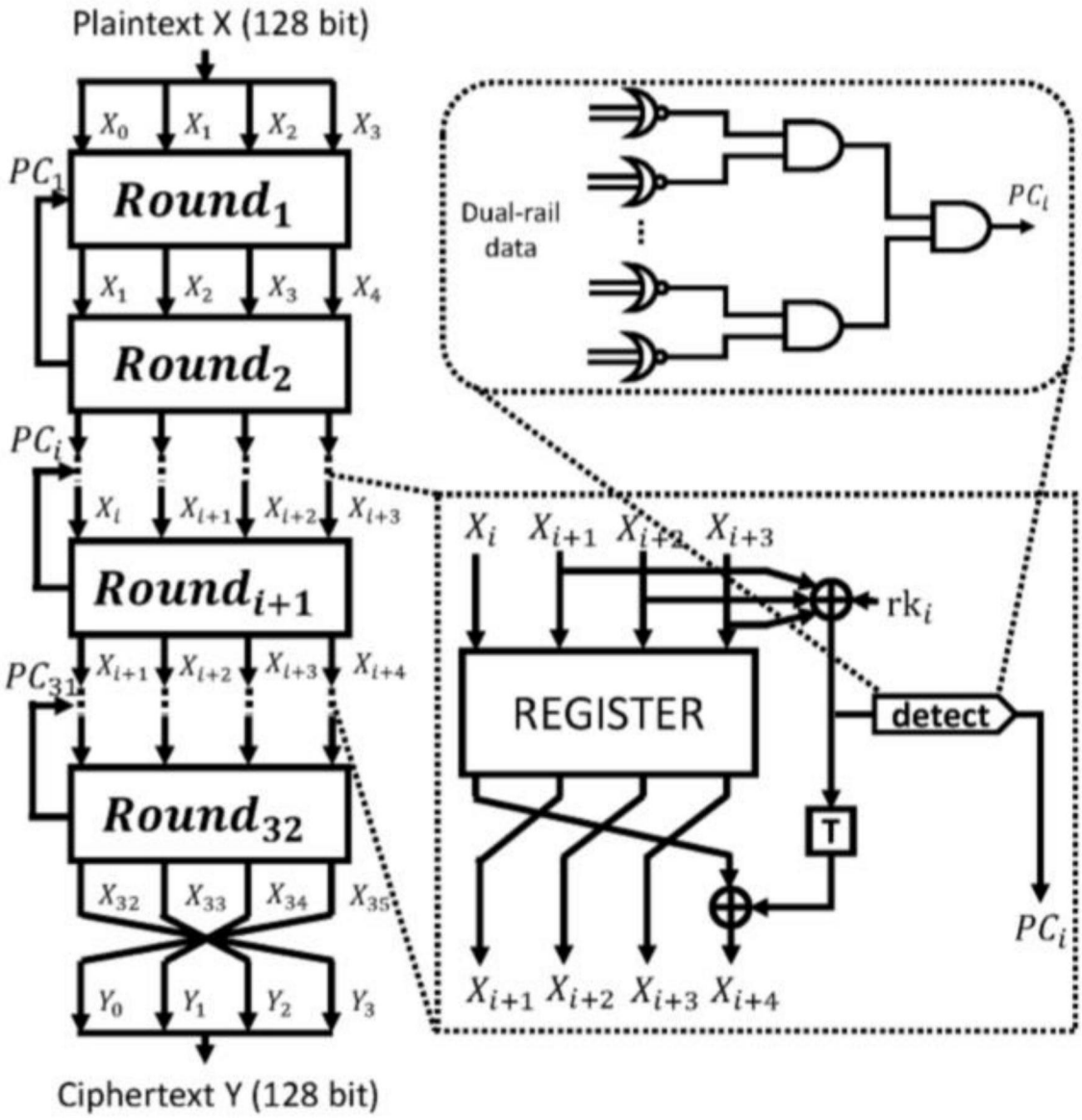

Plaintext X (128 bit)
X_0 X_1 X_2 X_3
PC_1
$Round_1$
X_1 X_2 X_3 X_4
$Round_2$
PC_i
X_i X_{i+1} X_{i+2} X_{i+3}
$Round_{i+1}$
PC_{31}
X_{i+1} X_{i+2} X_{i+3} X_{i+4}
$Round_{32}$
X_{32} X_{33} X_{34} X_{35}
Y_0 Y_1 Y_2 Y_3
Ciphertext Y (128 bit)
Dual-rail data
PC_i
X_i X_{i+1} X_{i+2} X_{i+3}
rk_i
REGISTER
detect
T
PC_i
X_{i+1} X_{i+2} X_{i+3} X_{i+4}

图5

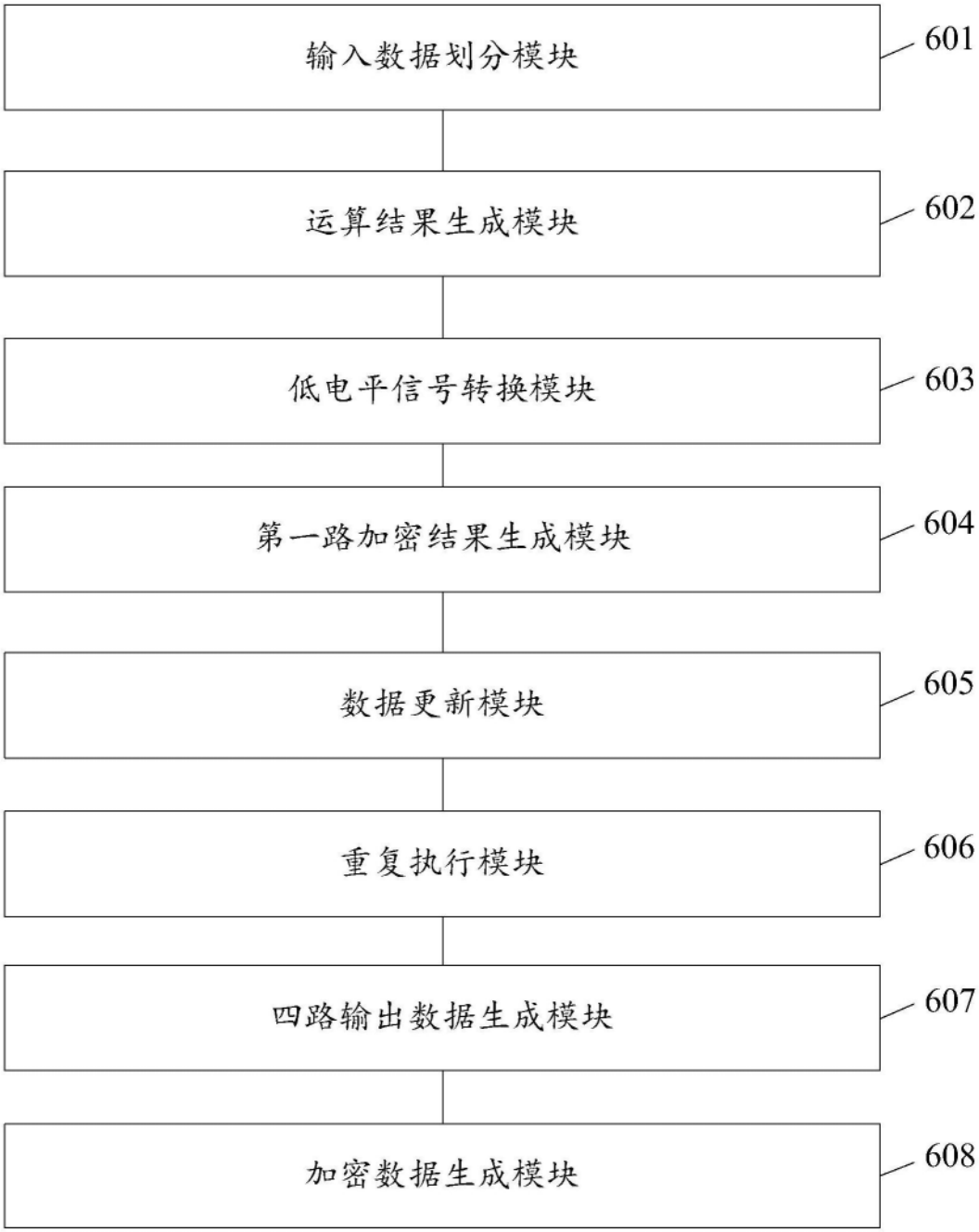

输入数据划分模块
601
运算结果生成模块
602
低电平信号转换模块
603
第一路加密结果生成模块
604
数据更新模块
605
重复执行模块
606
四路输出数据生成模块
607
加密数据生成模块
608

图6