(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114584297 A
(43)申请公布日 2022.06.03

(21)申请号 202210196739.9

(22)申请日 2022.03.01

(71)申请人 广东工业大学
地址 510062 广东省广州市越秀区东风东路729号

(72)发明人 蔡述庭 张启航 蒲佳铭 熊晓明

(74)专利代理机构 广东广信君达律师事务所 44329
专利代理师 熊冰

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

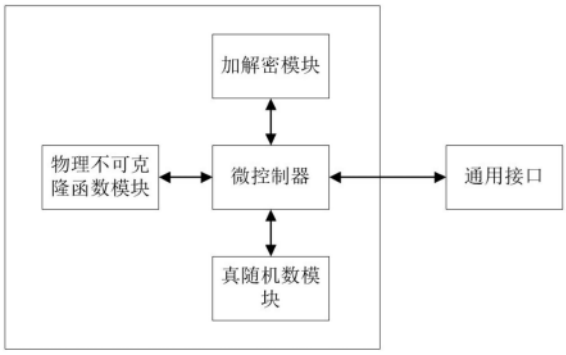
权利要求书2页 说明书4页 附图4页

(54)发明名称

一种基于物理不可克隆技术的加解密系统及加解密方法

(57)摘要

本发明公开了一种基于物理不可克隆技术的加解密系统及加解密方法，系统包括微控制器、PUF模块、加解密模块、真随机数发生器模块；所述微控制器通过总线与加解密模块、PUF模块和真随机数发生器模块连接。所述PUF模块包括循环移位模块、延时模块、自调整模块；延时模块包括多路延时路径和延时路径后的仲裁器，且每路结构相同；通过对多条延时路径后的仲裁器的仲裁结果进行异或操作，形成XOR型PUF。本发明通过PUF模块生成硬件唯一ID作为加解密模块密钥，通过XOR型PUF的实现和自调整模块的加入，有效提高了传统仲裁器PUF的稳定性和唯一性，具有加解密速度快、使用过程简单、能够有效保护信息安全等优点。



CN 114584297 A

1.一种基于物理不可克隆技术的加解密系统,其特征在于,包括微控制器、PUF模块、加解密模块、真随机数发生器模块;所述微控制器通过总线与加解密模块、PUF模块和真随机数发生器模块连接,进行数据传输和运行控制。

2.根据权利要求1所述的一种基于物理不可克隆技术的加解密系统,其特征在于,所述PUF模块包括延时模块;

所述延时模块包括延时路径和延时路径后的仲裁器;

所述延时路径的输入为系统运行后自动产生的跳变信号,信号在延时路径中的传输路径受到真随机数发生器模块产生的触发激励的影响,仲裁器根据接收到的两路信号到达先后输出结果,经过次运算形成硬件唯一ID。

3.根据权利要求2所述的一种基于物理不可克隆技术的加解密系统,其特征在于,所述延时路径包含n个节点,每个节点包括两个二选一多路选择器,选择信号由n位触发激励提供,选择信号决定当前节点信号平行传输还是交叉传输到下一个节点;

所述仲裁器接收最后一个节点的二选一多路选择器信号输出,判断仲裁结果并输出。

4.根据权利要求3所述的一种基于物理不可克隆技术的加解密系统,其特征在于,所述延时模块包括多路延时路径和延时路径后的仲裁器,且每路结构相同;通过对仲裁器的仲裁结果进行异或操作,形成XOR型PUF;多路延时路径中相同位置节点采用相同的控制信号。

5.根据权利要求4所述的一种基于物理不可克隆技术的加解密系统,其特征在于,所述PUF模块还包括有循环移位模块,该循环移位模块与延时模块连接,对触发激励信号进行循环移位,从而起到提供不同的激励的目的,使PUF模块生成的相应数据最后拼接成64位数据为止。

6.根据权利要求5所述的一种基于物理不可克隆技术的加解密系统,其特征在于,所述循环移位模块为循环移位寄存器。

7.根据权利要求5或6所述的一种基于物理不可克隆技术的加解密系统,其特征在于,所述PUF模块还包括有自调整模块,该自调整模块与对应延时模块连接,用于增加PUF模块输出数据的唯一性和随机性。

8.根据权利要求7所述的一种基于物理不可克隆技术的加解密系统,其特征在于,所述自调整模块由i个节点组成,每个节点包含两个二选一选择器;节点间两条路径只有一条具有缓冲器,自调整模块的控制信号控制相应节点选择是否要把缓冲器加入信号的传输路径。

9.一种基于物理不可克隆技术的加解密系统的加密方法,其特征在于,包括以下步骤:

S1、初始化加解密系统,自调整模块控制信号置0;

S2、从通用接口接收待加密信息,传输至微控制器并存储;

S3、真随机数模块产生随机数,存储在微控制器中,作为PUF模块的触发激励;

S4、PUF模块分析响应结果,对自调整模块的延时路径进行调整优化;

S5、PUF模块生成硬件唯一ID并作为加密算法的密钥传输至微控制器并存储;

S6、加解密模块读取待加密信息和密钥进行加密运算,得到加密信息;

S7、加密信息返回微控制器后,通过通用接口传出并存储。

10.一种基于物理不可克隆技术的加解密系统的解密方法,其特征在于,包括以下步骤:

A1、初始化加解密系统，自调整模块控制信号置0；

A2、从通用接口接收待解密信息，传输至微控制器并存储；

A3、真随机数模块产生随机数，存储在微控制器中，作为PUF模块的触发激励；

A4、PUF模块分析响应结果，对自调整模块的延时路径进行调整优化；

A5、PUF模块生成硬件硬件唯一ID并作为解密算法的密钥传输至微控制器并存储；

A6、加解密模块读取待解密信息和密钥进行解密运算，得到原始信息；

A7、原始信息返回微控制器后，通过通用接口传出并存储。

一种基于物理不可克隆技术的加解密系统及加解密方法

技术领域

[0001] 本发明涉及物联网信息安全的技术领域，尤其涉及到一种基于物理不可克隆技术的加解密系统及加解密方法。

背景技术

[0002] 随着信息时代的飞速发展，信息攻击手段逐渐升级，传统的安全保护方案不足以抵抗先进的攻击技术。物联网设备需要考虑更多的抗攻击策略，以提高设备信息的安全性。

[0003] 在目前主流的安全加密芯片中，通常采用ROM储存密钥的方案来机型密钥管理，并通过总线或者通用接口来读取密钥数据。该密钥管理方案存在安全漏洞，密钥数据可能通过侵入式攻击被获取，数据安全得不到保证。

发明内容

[0004] 本发明的目的在于克服现有技术的不足，提供一种能保证信息安全的基于物理不可克隆技术的加解密系统。

[0005] 为实现上述目的，本发明所提供的技术方案为：

[0006] 一种基于物理不可克隆技术的加解密系统及加解密方法，包括微控制器、PUF模块、加解密模块、真随机数发生器模块；所述微控制器通过总线与加解密模块、PUF模块和真随机数发生器模块连接，进行数据传输和运行控制。

[0007] 进一步地，所述PUF模块包括延时模块；

[0008] 所述延时模块包括延时路径和延时路径后的仲裁器；

[0009] 所述延时路径的输入为系统运行后自动产生的跳变信号，信号在延时路径中的传输路径受到真随机数发生器模块产生的触发激励的影响，仲裁器根据接收到的两路信号到达先后输出结果，经过次运算形成硬件唯一ID。

[0010] 进一步地，所述延时路径包含n个节点，每个节点包括两个二选一多路选择器，选择信号由n位触发激励提供，选择信号决定当前节点信号平行传输还是交叉传输到下一个节点；

[0011] 所述仲裁器接收最后一个节点的二选一多路选择器信号输出，判断仲裁结果并输出。

[0012] 进一步地，所述延时模块包括多路延时路径和延时路径后的仲裁器，且每路结构相同；通过对仲裁器的仲裁结果进行异或操作，形成XOR型PUF；多路延时路径中相同位置节点采用相同的控制信号。

[0013] 进一步地，所述PUF模块还包括有循环移位模块，该循环移位模块与延时模块连接，对触发激励信号进行循环移位，从而起到提供不同的激励的目的，使PUF模块生成的相应数据最后拼接成64位数据为止。

[0014] 进一步地，所述循环移位模块为循环移位寄存器。

[0015] 进一步地，所述PUF模块还包括有自调整模块，该自调整模块与对应延时模块连

接,用于增加PUF模块输出数据的唯一性和随机性。

[0016] 进一步地,所述自调整模块由i个节点组成,每个节点包含两个二选一选择器;节点间两条路径只有一条具有缓冲器,自调整模块的控制信号控制相应节点选择是否要把缓冲器加入信号的传输路径。

[0017] 进一步地,所述加解密模块采用国密算法SM4进行加解密。

[0018] 为实现上述目的,本发明另外提供一种基于物理不可克隆技术的加解密系统的加密方法,包括以下步骤:

[0019] S1、初始化加解密系统,自调整模块控制信号置0;

[0020] S2、从通用接口接收待加密信息,传输至微控制器并存储;

[0021] S3、真随机数模块产生随机数,存储在微控制器中,作为PUF模块的触发激励;

[0022] S4、PUF模块分析响应结果,对自调整模块的延时路径进行调整优化;

[0023] S5、PUF模块生成硬件唯一ID并作为加密算法的密钥传输至微控制器并存储;

[0024] S6、加解密模块读取待加密信息和密钥进行加密运算,得到加密信息;

[0025] S7、加密信息返回微控制器后,通过通用接口传出并存储。

[0026] 为实现上述目的,本发明另外提供一种基于物理不可克隆技术的加解密系统的解密方法,包括以下步骤:

[0027] A1、初始化加解密系统,自调整模块控制信号置0;

[0028] A2、从通用接口接收待解密信息,传输至微控制器并存储;

[0029] A3、真随机数模块产生随机数,存储在微控制器中,作为PUF模块的触发激励;

[0030] A4、PUF模块分析响应结果,对自调整模块的延时路径进行调整优化;

[0031] A5、PUF模块生成硬件硬件唯一ID并作为解密算法的密钥传输至微控制器并存储;

[0032] A6、加解密模块读取待解密信息和密钥进行解密运算,得到原始信息;

[0033] A7、原始信息返回微控制器后,通过通用接口传出并存储。

[0034] 与现有技术相比,本方案原理及优点如下:

[0035] 本发明提供一种基于物理不可克隆技术的加解密系统,该系统通过PUF模块生成硬件唯一ID作为加解密模块密钥,利用了国密SM4算法对信息进行加解密,通过通用接口完成数据的输入输出,通过XOR型PUF的实现和自调整模块的加入,有效提高了传统仲裁器PUF的稳定性和唯一性,所述系统加解密速度快,使用过程简单,能够有效保护信息安全。

附图说明

[0036] 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服务作简单地介绍,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的前提下,还可以根据这些附图获得其他的附图。

[0037] 图1为本发明一种基于物理不可克隆技术的加解密系统的结构框图;

[0038] 图2为本发明一种基于物理不可克隆技术的加解密系统中PUF模块的结构示意图;

[0039] 图3为本发明一种基于物理不可克隆技术的加解密系统中仲裁器型PUF模块的结构示意图;

[0040] 图4为添加自调整模块(路径)的多路XOR型PUF的结构示意图;

[0041] 图5为基于物理不可克隆技术的加解密方法的加密流程示意图；

[0042] 图6为基于物理不可克隆技术的加解密方法的解密流程示意图。

具体实施方式

[0043] 下面结合具体实施例对本发明作进一步说明：

[0044] 如图1所示，本实施例所述的一种基于物理不可克隆技术的加解密系统，包括微控制器、物理不可克隆函数模块(PUF模块)、加解密模块、真随机数发生器模块；所述微控制器通过总线与加解密模块、PUF模块和真随机数发生器模块连接，进行数据传输和运行控制。待加解密信息通过通用接口，如GPIO，I2C等，传入加解密系统，发送至所述微控制器并存储。

[0045] 具体地，如图2所示，所述PUF模块包括循环移位模块、延时模块、自调整模块；

[0046] 其中，延时模块包括多路延时路径和延时路径后的仲裁器，且每路结构相同。

[0047] 延时路径的输入为系统运行后自动产生的跳变信号，信号在延时路径中的传输路径受到真随机数发生器模块产生的触发激励的影响，仲裁器根据接收到的两路信号到达先后输出结果，经过次运算形成硬件唯一ID。

[0048] 具体地，如图3所示，每条延时路径包含n个节点，每个节点包括两个二选一多路选择器，选择信号由n位触发激励提供，选择信号决定当前节点信号平行传输还是交叉传输到下一个节点；仲裁器接收最后一个节点的二选一多路选择器信号输出，判断仲裁结果并输出。

[0049] 通过对多条延时路径后的仲裁器的仲裁结果进行异或操作，形成XOR型PUF，提高PUF输出的稳定性，可根据系统性能和要求选择2路，4路或8路PUF等结构。多路延时路径中相同位置节点采用相同的控制信号。

[0050] 具体地，为了降低硬件模块与CPU的通信频率，本实施例增加了与延时模块连接的循环移位模块，该循环移位模块具体为循环移位寄存器，其对触发激励信号进行循环移位，从而起到提供不同的激励的目的，使PUF模块生成的相应数据最后拼接成64位数据为止。

[0051] 具体地，如图4所示，自调整模块与对应延时模块连接，用于增加PUF模块输出数据的唯一性和随机性。自调整模块也是延时路径，由i个节点组成，每个节点包含两个二选一选择器。节点间两条路径只有一条具有缓冲器(buff)，自调整模块的控制信号控制相应节点选择是否要把缓冲器加入信号的传输路径。

[0052] 具体地，加解密模块采用国密算法SM4进行加解密。

[0053] 如图5所示，基于物理不可克隆技术的加解密系统的加密方法，包括以下步骤：

[0054] S1、初始化加解密系统，自调整模块控制信号置0；

[0055] S2、从通用接口接收待加密信息，传输至微控制器并存储；

[0056] S3、真随机数模块产生随机数，存储在微控制器中，作为PUF模块的触发激励；

[0057] S4、PUF模块分析响应结果，对自调整模块的延时路径进行调整优化；

[0058] S5、PUF模块生成硬件唯一ID并作为加密算法的密钥传输至微控制器并存储；

[0059] S6、加解密模块读取待加密信息和密钥进行加密运算，得到加密信息；

[0060] S7、加密信息返回微控制器后，通过通用接口传出并存储。

[0061] 如图6所示，基于物理不可克隆技术的加解密系统的解密方法，包括以下步骤：

[0062] A1、初始化加解密系统，自调整模块控制信号置0；

[0063] A2、从通用接口接收待解密信息，传输至微控制器并存储；

[0064] A3、真随机数模块产生随机数，存储在微控制器中，作为PUF模块的触发激励；

[0065] A4、PUF模块分析响应结果，对自调整模块的延时路径进行调整优化；

[0066] A5、PUF模块生成硬件硬件唯一ID并作为解密算法的密钥传输至微控制器并存储；

[0067] A6、加解密模块读取待解密信息和密钥进行解密运算，得到原始信息；

[0068] A7、原始信息返回微控制器后，通过通用接口传出并存储。

[0069] 本实施例提供一种基于物理不可克隆技术的加解密系统，该系统通过PUF模块生成硬件唯一ID作为加解密模块密钥，利用了国密SM4算法对信息进行加解密，通过通用接口完成数据的输入输出。

[0070] 衡量PUF电路优劣主要有两个指标：稳定性和唯一性。稳定性通过片内海明距离来体现，理想的片内海明距离是0％。唯一性通过片间海明距离体现，理想的片间海明距离是50％。实验通过例化8个PUF模块，测试稳定性和唯一性。当采用传统的仲裁器PUF时，平均片内海明距离为13.23％，平均片间海明距离为36.3％；当采用本实施例所述系统，采用2路XOR型PUF，并添加自调整模块后，平均片内海明距离为1.1％，平均片间海明距离为43.3％。

[0071] 对比传统仲裁器型PUF，通过XOR型PUF的实现和自调整模块的加入，有效提高了传统仲裁器PUF的稳定性和唯一性。

[0072] 本实施例所述系统加解密速度快，使用过程简单，能够有效保护信息安全。

[0073] 以上所述之实施例子只为本发明之较佳实施例，并非以此限制本发明的实施范围，故凡依本发明之形状、原理所作的变化，均应涵盖在本发明的保护范围内。

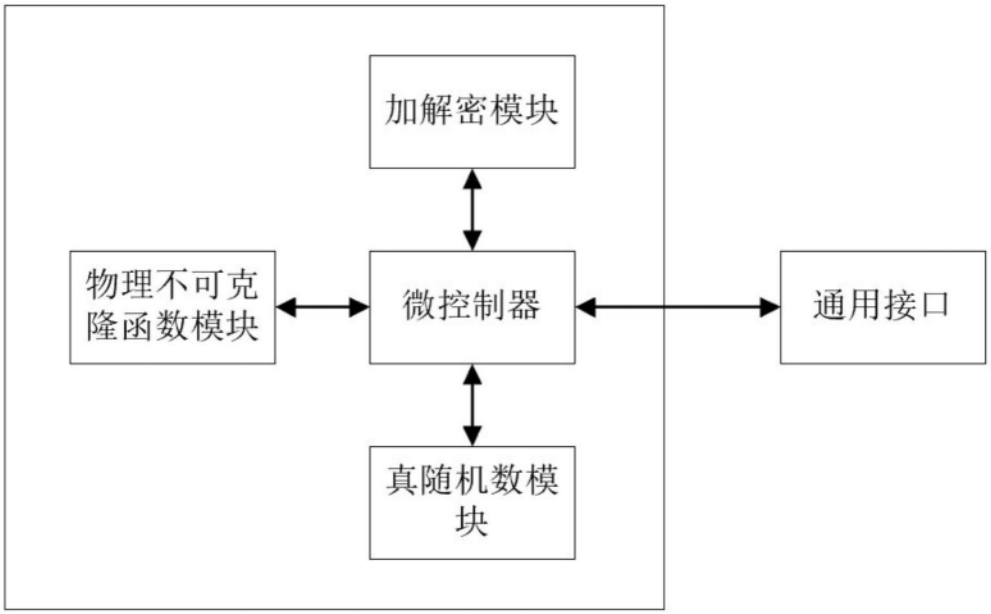

加解密模块
物理不可克隆函数模块
微控制器
通用接口
真随机数模块

图1

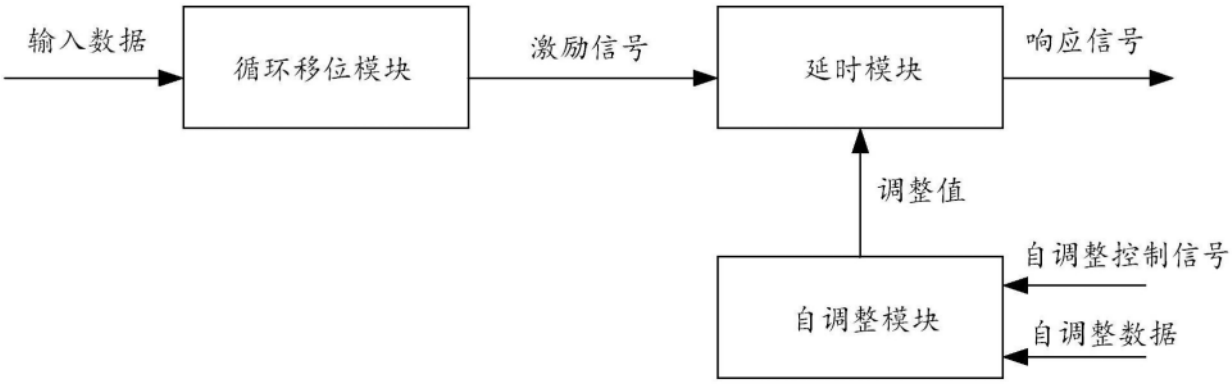

输入数据
循环移位模块
激励信号
延时模块
响应信号
调整值
自调整控制信号
自调整模块
自调整数据

图2

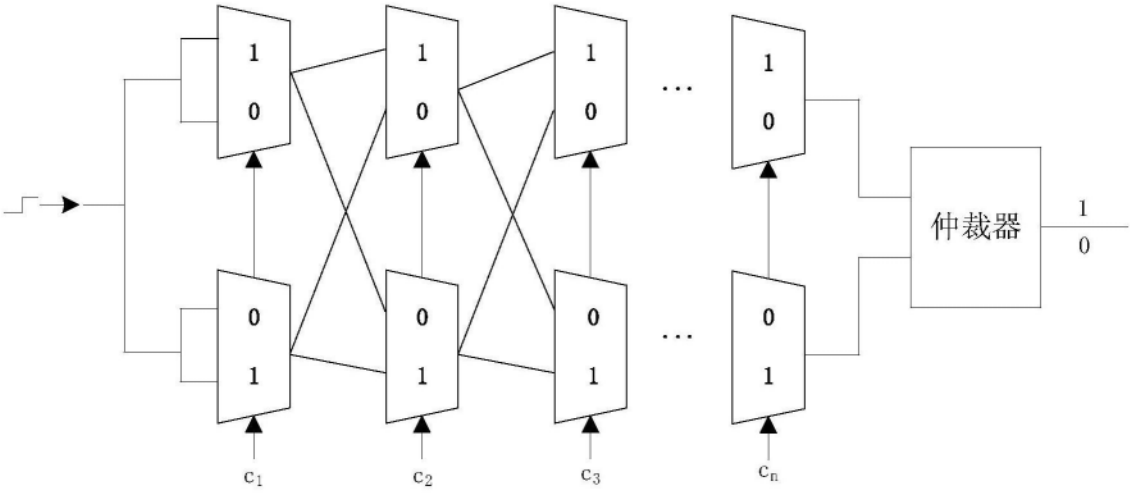

仲裁器
1
0
c1
c2
c3
cn

图3

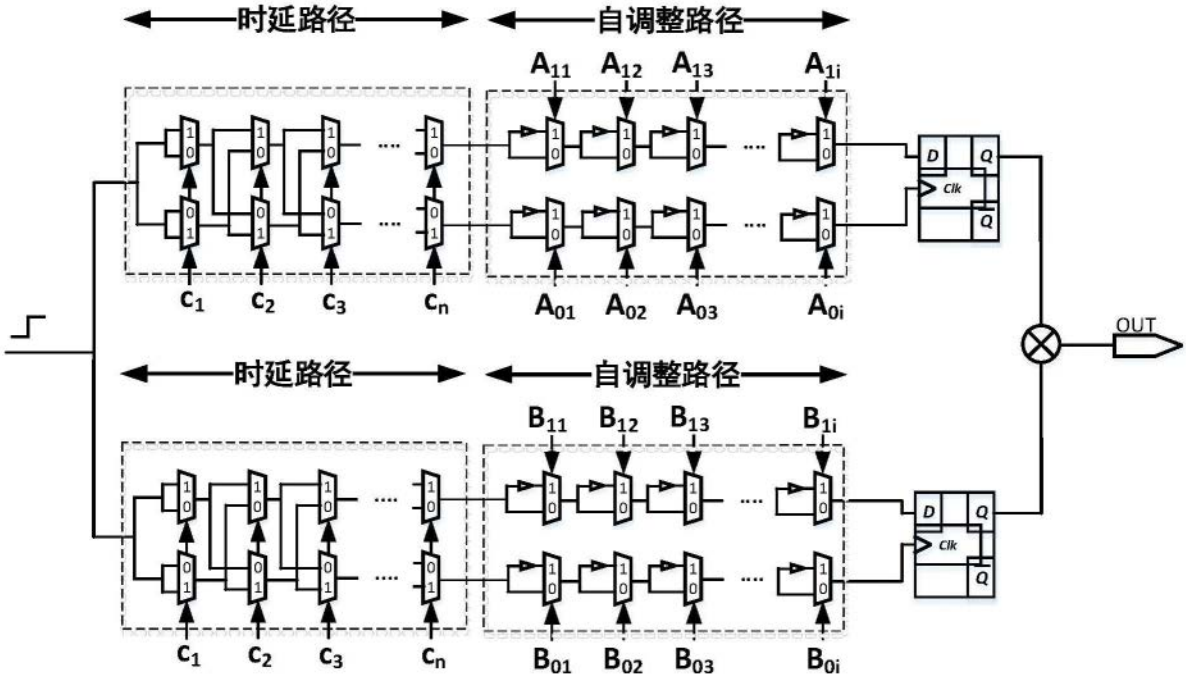

时延路径
自调整路径
A11 A12 A13 A1i
A01 A02 A03 A0i
B11 B12 B13 B1i
B01 B02 B03 B0i
c1 c2 c3 cn
D Q Clk
OUT

图4

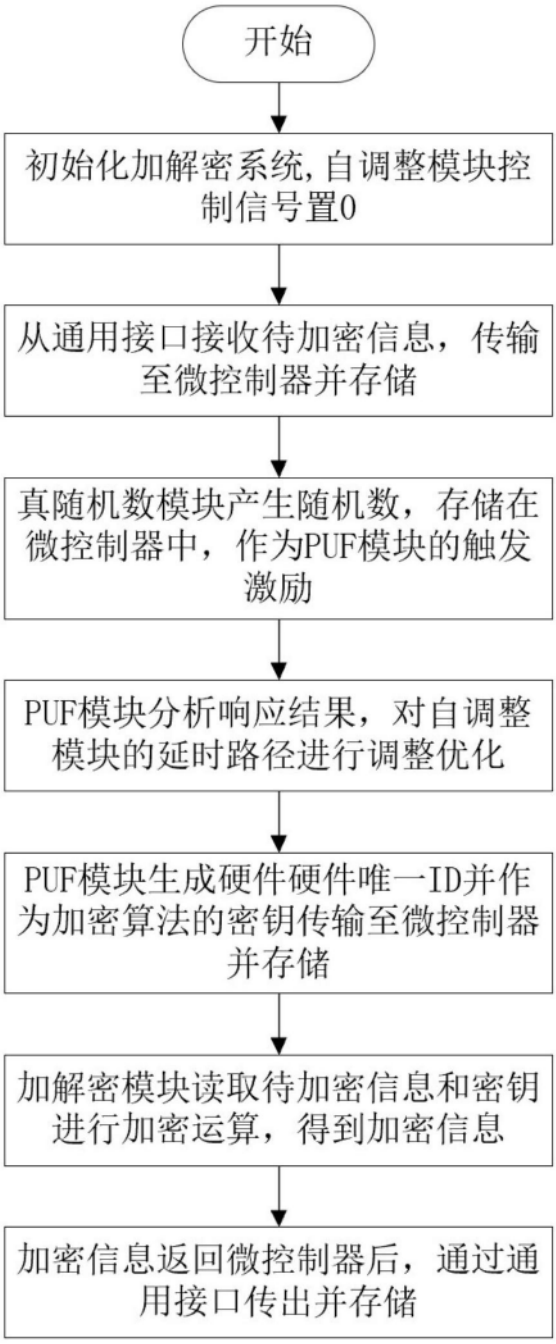

开始
初始化加解密系统,自调整模块控制信号置0
从通用接口接收待加密信息，传输至微控制器并存储
真随机数模块产生随机数，存储在微控制器中，作为PUF模块的触发激励
PUF模块分析响应结果，对自调整模块的延时路径进行调整优化
PUF模块生成硬件硬件唯一ID并作为加密算法的密钥传输至微控制器并存储
加解密模块读取待加密信息和密钥进行加密运算，得到加密信息
加密信息返回微控制器后，通过通用接口传出并存储

图5

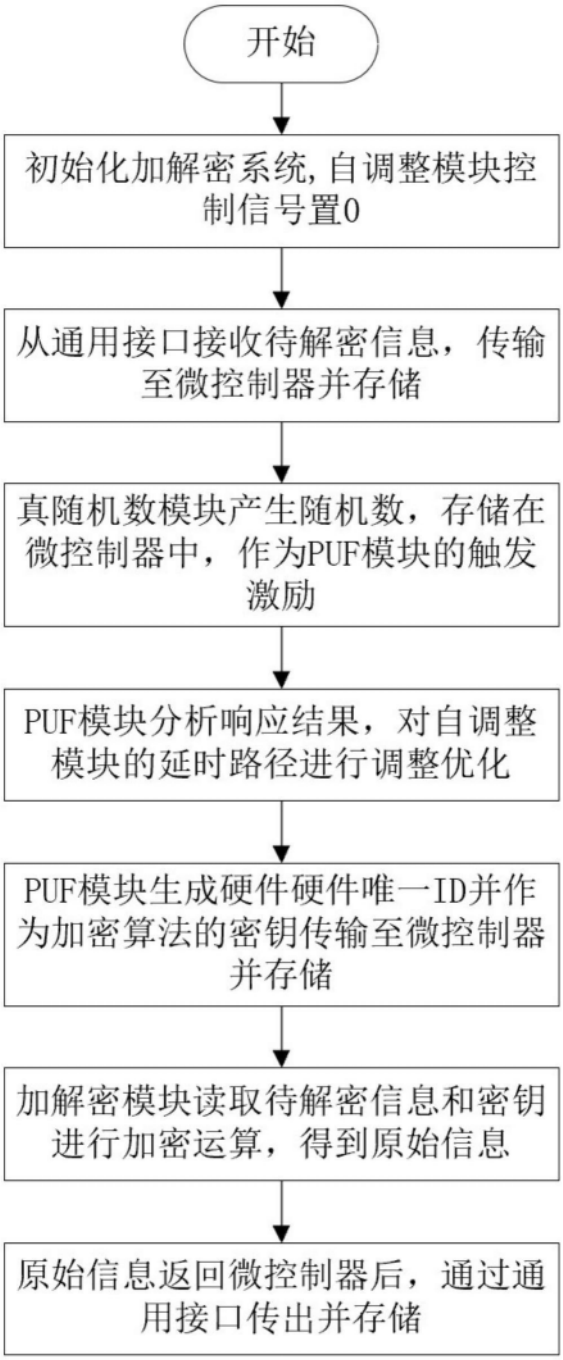

开始
初始化加解密系统,自调整模块控制信号置0
从通用接口接收待解密信息，传输至微控制器并存储
真随机数模块产生随机数，存储在微控制器中，作为PUF模块的触发激励
PUF模块分析响应结果，对自调整模块的延时路径进行调整优化
PUF模块生成硬件硬件唯一ID并作为加密算法的密钥传输至微控制器并存储
加解密模块读取待解密信息和密钥进行加密运算，得到原始信息
原始信息返回微控制器后，通过通用接口传出并存储

图6