(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 108123793 A
(43)申请公布日 2018.06.05

(21)申请号 201711375890.4

(22)申请日 2017.12.19

(71)申请人 杭州中天微系统有限公司
地址 310012 浙江省杭州市西湖区西斗门路3号天堂软件园A幢15楼

(72)发明人 杨军 奚嘉琦 杨指望 蔡蕊

(74)专利代理机构 北京汇泽知识产权代理有限公司 11228
代理人 张瑾

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 29/06(2006.01)

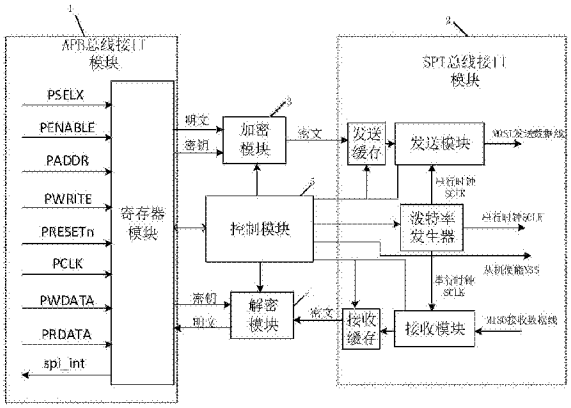
权利要求书1页 说明书5页 附图5页

(54)发明名称

基于APB总线的SPI通信装置

(57)摘要

本发明提供一种基于APB总线的SPI通信装置。所述装置包括:APB总线接口模块、SPI总线接口模块、加密模块、解密模块和控制模块,加密模块通过所述APB总线接口模块接收主机传来的明文数据和密钥,被使能时根据所述明文数据和密钥生成密文数据,将所述密文数据通过所述SPI总线接口模块发送到从机;解密模块通过所述SPI总线接口模块接收从机传来的密文数据,并通过所述APB总线接口模块接收主机传来的密钥,被使能时根据所述密文数据和密钥生成明文数据,将所述明文数据通过所述APB总线接口模块发送到主机。本发明能够提高数据传输的安全性。



CN 108123793 A

1.一种基于APB总线的SPI通信装置，用于实现主机和从机之间的SPI通信，其特征在于，包括：

APB总线接口模块，与主机的APB总线连接；

SPI总线接口模块，与从机的SPI总线连接；

加密模块，通过所述APB总线接口模块接收主机传来的明文数据和密钥，被使能时根据所述明文数据和密钥生成密文数据，将所述密文数据通过所述SPI总线接口模块发送到从机；

解密模块，通过所述SPI总线接口模块接收从机传来的密文数据，并通过所述APB总线接口模块接收主机传来的密钥，被使能时根据所述密文数据和密钥生成明文数据，将所述明文数据通过所述APB总线接口模块发送到主机；

控制模块，通过所述APB总线接口模块接收主机传来的控制指令，根据所述控制指令对所述加密模块、解密模块和SPI总线接口模块进行控制，并通过所述APB总线接口模块向主机反馈状态信号。

2.根据权利要求1所述的装置，其特征在于，所述装置还包括：第一2选1多路选择器，所述第一2选1多路选择器输入所述APB总线接口模块传来的明文数据及所述加密模块输出的密文数据，在所述控制模块的控制下选通输出所述明文数据或者密文数据。

3.根据权利要求1或2所述的装置，其特征在于，所述装置还包括：第二2选1多路选择器，所述第二2选1多路选择器输入所述SPI总线接口模块传来的密文数据及所述解密模块输出的明文数据，在所述控制模块的控制下选通输出所述明文数据或者密文数据。

4.根据权利要求1所述的装置，其特征在于，所述加密模块由加法器和SR寄存器构成。

5.根据权利要求1所述的装置，其特征在于，所述解密模块由加法器和DSR寄存器构成。

6.根据权利要求1所述的装置，其特征在于，所述明文数据和密文数据的宽度为8位、16位、32位或者64位。

7.根据权利要求1所述的装置，其特征在于，所述密钥的宽度为32位、64位、128位或者256位。

8.根据权利要求1所述的装置，其特征在于，所述从机为具有SPI总线的存储器。

9.根据权利要求1所述的装置，其特征在于，所述APB总线接口模块包括中断请求信号线以及AMBA协议定义的APB总线。

10.根据权利要求1所述的装置，其特征在于，所述SPI总线接口模块包括数据接收信号线、数据发送信号线、串行时钟信号线以及从机使能信号线。

基于APB总线的SPI通信装置

技术领域

[0001] 本发明涉及嵌入式系统技术领域，尤其涉及一种基于APB总线的SPI通信装置。

背景技术

[0002] SPI(Serial Peripheral Interface，串行外设接口)是目前广泛使用的一种通用串行数据接口，应用范围极其广泛，例如计算机外设、工业控制等场合。SPI既可以接收外围设备的串行数据输入，并转换成计算机内部所需的并行数据，也可以把计算机内部的并行数据转换成串行数据，并发送给外围设备。对于串10行数据传输速率要求不高的设备，使用SPI进行串行通信是一种性价比较高的设计方案。

[0003] 传统的SPI通信装置一般由主机侧总线接口部分、SPI总线接口模块和控制模块组成，其中SPI总线接口模块包括发送模块、接收模块和波特率发生器，发送模块和接收模块可以是双缓冲结构，主机侧总线接口部分可以采用APB总15线结构，如图1所示。

[0004] 传统的SPI通信装置只能传输明文数据，对于一些安全性高的通信领域，如信息安全卡、军事领域等，上述装置不能满足安全通信的使用要求。因此有必要提出一种更加安全的SPI通信装置。

发明内容

[0005] 本发明提供的基于APB总线的SPI通信装置，能够对传输的数据进行加密和解密，传输密文数据，提高了数据传输的安全性。

[0006] 本发明提供一种基于APB总线的SPI通信装置，用于实现主机和从机之间的SPI通信，包括：

[0007] APB总线接口模块，与主机的APB总线连接；

[0008] SPI总线接口模块，与从机的SPI总线连接；

[0009] 加密模块，通过所述APB总线接口模块接收主机传来的明文数据和密钥，被使能时根据所述明文数据和密钥生成密文数据，将所述密文数据通过所述SPI总线接口模块发送到从机；

[0010] 解密模块，通过所述SPI总线接口模块接收从机传来的密文数据，并通过所述APB总线接口模块接收主机传来的密钥，被使能时根据所述密文数据和密钥生成明文数据，将所述明文数据通过所述APB总线接口模块发送到主机；

[0011] 控制模块，通过所述APB总线接口模块接收主机传来的控制指令，根据所述控制指令对所述加密模块、解密模块和SPI总线接口模块进行控制，并通过所述APB总线接口模块向主机反馈状态信号。

[0012] 可选地，所述装置还包括：第一2选1多路选择器，所述第一2选1多路选择器输入所述APB总线接口模块传来的明文数据及所述加密模块输出的密文数据，在所述控制模块的控制下选通输出所述明文数据或者密文数据。

[0013] 可选地，所述装置还包括：第二2选1多路选择器，所述第二2选1多路选择器输入所

述SPI总线接口模块传来的密文数据及所述解密模块输出的明文数据，在所述控制模块的控制下选通输出所述明文数据或者密文数据。

[0014] 可选地，所述加密模块由加法器和SR寄存器构成。

[0015] 可选地，所述解密模块由加法器和DSR寄存器构成。

[0016] 可选地，所述明文数据和密文数据的宽度为8位、16位、32位或者64位。

[0017] 可选地，所述密钥的宽度为32位、64位、128位或者256位。

[0018] 可选地，所述从机为具有SPI总线的存储器。

[0019] 可选地，所述APB总线接口模块包括中断请求信号线以及AMBA协议定义的APB总线。

[0020] 可选地，所述SPI总线接口模块包括数据接收信号线、数据发送信号线、串行时钟信号线以及从机使能信号线。

[0021] 本发明提供的基于APB总线的SPI通信装置，包括APB总线接口模块、SPI总线接口模块、加密模块、解密模块和控制模块，当主机向从机写入数据时，通过加密模块对传输的明文数据进行加密，当主机读取从机中存储的加密数据时，通过解密模块对加密数据进行解密，与现有技术相比，本发明能够在SPI通信时通过硬件对传输数据加密和解密，传输密文数据，提高了数据传输的安全性。同时本发明硬件资源简单，易于实现。

附图说明

[0022] 图1为传统的基于APB总线的SPI通信装置的结构示意图；

[0023] 图2为本发明的基于APB总线的SPI通信装置的一个实施例的结构示意图；

[0024] 图3为本发明的基于APB总线的SPI通信装置的另一个实施例的结构示意图；

[0025] 图4为APB总线写数据的时序图；

[0026] 图5为APB总线读数据的时序图；

[0027] 图6为CPHA＝1时SPI传输数据的时序图；

[0028] 图7为CPHA＝0时SPI传输数据的时序图；

[0029] 图8为加密模块设计的原理图；

[0030] 图9为解密模块设计的原理图。

具体实施方式

[0031] 为使本发明实施例的目的、技术方案和优点更加清楚，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。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他实施例，都属于本发明保护的范围。

[0032] 本发明实施例提供一种基于APB总线的SPI通信装置，用于实现主机和从机之间的SPI通信，如图2所示，所述装置包括：APB总线接口模块1、SPI总线接口模块2、加密模块3、解密模块4和控制模块5，其中，

[0033] APB总线接口模块1，与主机的APB总线连接，负责与APB主机通信；

[0034] SPI总线接口模块2，与从机的SPI总线连接，负责与SPI从机通信；

[0035] 加密模块3，通过APB总线接口模块1接收主机传来的明文数据和密钥，加密模块3

受控制模块5的使能控制，当加密模块3被控制模块5使能时，根据明文数据和密钥生成密文数据，将密文数据通过SPI总线接口模块2发送到从机；

[0036] 解密模块4，通过SPI总线接口模块2接收从机传来的密文数据，并通过APB总线接口模块1接收主机传来的密钥，解密模块4受控制模块5的使能控制，当解密模块4被控制模块5使能时，根据密文数据和密钥生成明文数据，将明文数据通过APB总线接口模块1发送到主机；

[0037] 控制模块5，通过APB总线接口模块1接收主机传来的控制指令，通过控制指令对加密模块3、解密模块4和SPI总线接口模块2进行控制，并通过APB总线接口模块1将控制模块5的状态信号反馈到主机上。

[0038] 在本发明中，从机只是作为存储器，包括具有SPI总线的存储芯片，主机向从机写入数据，或者，主机读取从机中存储的数据。

[0039] 本发明实施例提供的基于APB总线的SPI通信装置，当主机向从机写入数据时，通过加密模块对传输的明文数据进行加密，当主机读取从机中存储的加密数据时，通过解密模块对加密数据进行解密，与现有技术相比，本发明能够在SPI通信时通过硬件对传输数据加密和解密，传输密文数据，提高了数据传输的安全性。同时本发明硬件资源简单，易于实现。

[0040] 进一步地，如图3所示，所述基于APB总线的SPI通信装置包括两个2选1多路选择器6和7，两个多路选择器为8位，多路选择器6配合加密模块3工作，多路选择器7配合解密模块4工作。

[0041] 多路选择器6的输入端输入APB总线接口模块1传来的明文数据及加密模块3输出的密文数据，在控制模块5的控制下选通输出所述明文数据或者密文数据。如果使能加密模块3，则由控制模块5控制选通输出密文数据到SPI总线接口模块2；如果不使能加密模块3，则密钥无效，则由控制模块5控制选通输出明文数据到SPI总线接口模块2。

[0042] 多路选择器7的输入端输入SPI总线接口模块2传来的密文数据及解密模块4输出的明文数据，在控制模块5的控制下选通输出所述明文数据或者密文数据。如果使能解密模块4，则由控制模块5控制选通输出解密后的明文数据到APB总线接口模块1；如果不使能解密模块4，则密钥无效，则由控制模块5控制选通输出接收到的密文数据到APB总线接口模块1。

[0043] 下面具体介绍一下本发明实施例提供的基于APB总线的SPI通信装置的工作原理。

[0044] APB总线侧：

[0045] APB总线接口模块1拥有一根中断请求信号线以及APB总线定义的所有信号线，中断请求信号spi_int当没有中断请求时保持低电平，当发生中断请求时保持高电平。

[0046] 空闲时选通信号(PSEL)与使能信号(PENABLE)均为低，数据(PDATA)与地址(PADDR)无效。

[0047] 发生一次APB写操作时，时序图如图4所示，在准备周期主机将数据(PWDATA)，地址(PADDR)准备好，同时置位选通信号(PSEL)，在使能周期置位使能信号(PENABLE)。这些信号必须保持到使能周期末的上升沿，在此上升沿，数据将根据地址写入相应寄存器。

[0048] 发生一次APB读操作时，时序图如图5所示，在准备周期主机将地址(PADDR)准备好，同时置位选通信号(PSEL)，在使能周期置位使能信号(PENABLE)，同时APB总线接口模块

根据地址将数据(PRDATA)准备好。这些信号必须保持到使能周期末的上升沿，在此上升沿，主机将读走数据。

[0049] SPI总线侧：

[0050] SPI总线接口模块2拥有接收MISO(主输入从输出)与发送MOSI(主输出从输入)两根信号线、串行时钟信号线SCLK以及从机使能信号线NSS，由主机控制，支持与其他SPI从机通信。SPI通信有4种不同的模式，通过CPOL(时钟极性)和CPHA(时钟相位)来控制其通信模式。其中时钟极性CPOL是用来配置SCLK的电平处于哪种状态时是空闲态或者有效态，时钟相位CPHA是用来配置数据采样是在第几个边沿。具体的通信格式如图6和7所示。

[0051] 发送数据时，由波特率发生器产生串行时钟SCLK，发送模块监测使能信号线NSS拉低，根据时钟极性和时钟相位，将并行数据以上文所述通信格式从MOSI发送数据线上串行发送出去。

[0052] 接收数据时，由波特率发生器产生串行时钟SCLK，接收模块监测使能信号线NSS拉低，根据时钟极性和时钟相位，采样一次接收数据线RXD。完成数据采样后将并行数据放到接收缓存中。

[0053] 下面进行加密模块3和解密模块4的设计举例，该例子采用硬件比特流加密法，仅表示模块的可实现性，在具体实现时并不限于这一种方式。

[0054] 加密模块3根据明文数据和密钥生成密文数据，明文数据和密文数据的宽度相等，可以采用8位、16位、32位或者64位，密钥宽度为32位、64位、128位或者256位。

[0055] 以8位明文数据为例说明加密模块3的工作过程。8位明文数据其中1位的加密原理图如图8所示。

[0056] 当密钥为32位时，n＝4，图8示电路包括4个SR寄存器和2个加法器，4个SR寄存器的初始化值为密钥中的4位(明文数据的第1位对应密钥1-4位，明文数据的第2位对应密钥5-8位，……，以此类推，明文数据的第8位对应密钥29-32位)；

[0057] 当密钥为64位时，n＝8，图8示电路包括8个SR寄存器和2个加法器，8个SR寄存器的初始化值为密钥中的8位(明文数据的第1位对应密钥1-8位，明文数据的第2位对应密钥9-16位，……以此类推)；

[0058] 当密钥为128位时，n＝16，图8示电路包括16个SR寄存器和2个加法器，16个SR寄存器的初始化值为密钥中的16位(明文数据的第1位对应密钥1-16位，明文数据第2位对应密钥17-32位，……，以此类推)；

[0059] 当密钥为256位时，n＝32，图8示电路包括32个SR寄存器和2个加法器，32个SR寄存器的初始化值为密钥中的32位(明文数据的第1位对应密钥1-32位，明文数据的第2位对应密钥33-64位，……，以此类推)；

[0060] 对1位明文数据加密时，输出密文Y＝X+SR0，并写回SRn-1。SRn-2＝SRn-1+Y，其余SR0～SRn-3均为SR(i-1)＝SR(i)，i取1至n-2。

[0061] 8组该电路一起构成加密模块3，在一个时钟周期完成一次一个8位数据的加密。

[0062] 解密模块4根据密文数据和密钥生成明文数据，同样以8位密文数据为例说明解密模块4的工作过程。8位密文数据其中1位的解密原理图如图9所示。

[0063] 当密钥为32位时，n＝4，图9所示电路包括4个DSR寄存器和2个加法器，4个DSR寄存器的初始化值为密钥中的4位(密文数据的第1位对应密钥1-4位，密文数据的第2位对应密

钥5-8位,……,以此类推,密文数据的第8位对应密钥29-32位);

[0064] 当密钥为64位时,n=8,图9所示电路包括8个DSR寄存器和2个加法器,8个DSR寄存器的初始化值为密钥中的8位(密文数据的第1位对应密钥1-8位,密文数据的第2位对应密钥9-16位,……以此类推);

[0065] 当密钥为128位时,n=16,图9所示电路包括16个DSR寄存器和2个加法器,16个DSR寄存器的初始化值为密钥中的16位(密文数据的第1位对应密钥1-16位,密文数据第2位对应密钥17-32位,……,以此类推);

[0066] 当密钥为256位时,n=32,图9所示电路包括32个DSR寄存器和2个加法器,32个DSR寄存器的初始化值为密钥中的32位(密文数据的第1位对应密钥1-32位,密文数据的第2位对应密钥33-64位,……,以此类推);

[0067] 对1位密文数据解密时,输出明文Y=X+DSR0,同时X写入DSRn-1,DSRn-2=DSRn-1+X,其余DSR0～DSRn-3均为DSR(i-1)=DSR(i),i取1至n-2。

[0068] 8组该电路一起构成解密模块4,在一个时钟周期完成一次一个8位数据的解密。

[0069] 通过上述加密模块和解密模块,能够实现在主机和从机之间进行SPI通信时,传输密文数据,提高了数据传输的安全性。

[0070] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的程序可存储于一计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)或随机存储记忆体(Random Access Memory,RAM)等。

[0071] 以上所述,仅为本发明的具体实施方式,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,可轻易想到的变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应该以权利要求的保护范围为准。

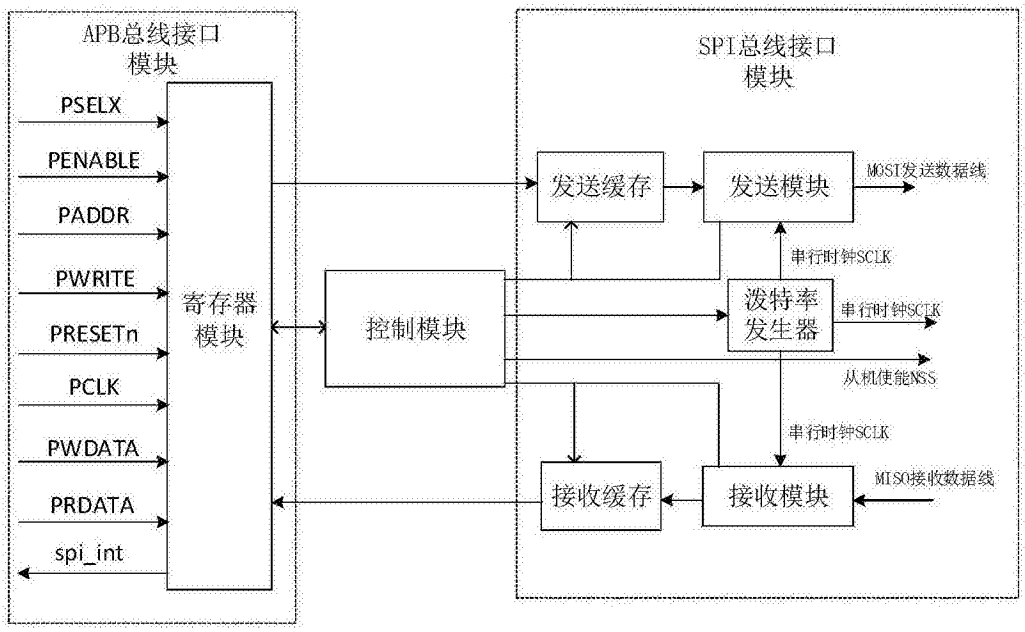

APB总线接口
模块
PSELX
PENABLE
PADDR
PWRITE
PRESETn
PCLK
PWDATA
PRDATA
spi_int
寄存器
模块
控制模块
SPI总线接口
模块
发送缓存
发送模块
MOSI发送数据线
串行时钟SCLK
波特率
发生器
串行时钟SCLK
从机使能NSS
串行时钟SCLK
接收缓存
接收模块
MISO接收数据线

图1

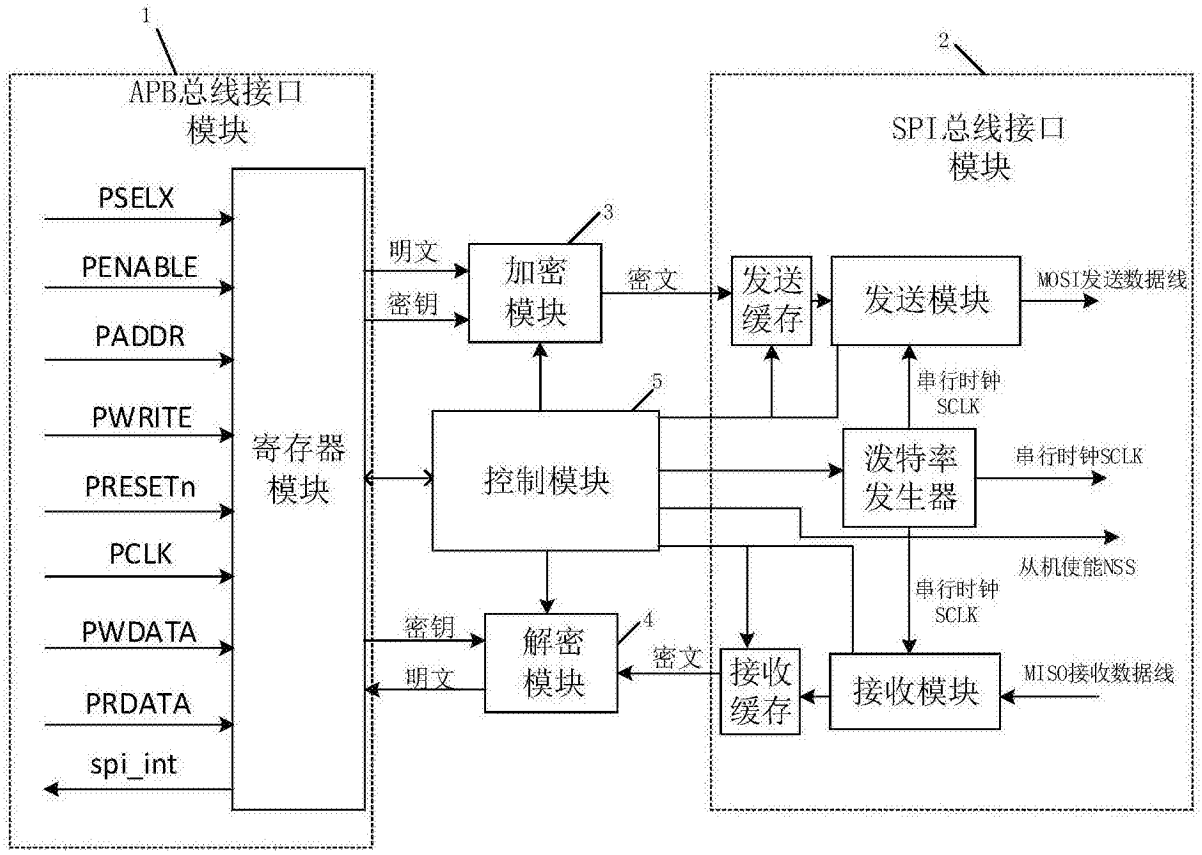

1
APB总线接口
模块
PSELX
PENABLE
PADDR
PWRITE
PRESETn
PCLK
PWDATA
PRDATA
spi_int
寄存器
模块
2
SPI总线接口
模块
3
明文
密钥
加密
模块
密文
发送
缓存
发送模块
MOSI发送数据线
串行时钟
SCLK
5
控制模块
波特率
发生器
串行时钟SCLK
从机使能NSS
串行时钟
SCLK
密钥
明文
4
解密
模块
密文
接收
缓存
接收模块
MISO接收数据线

图2

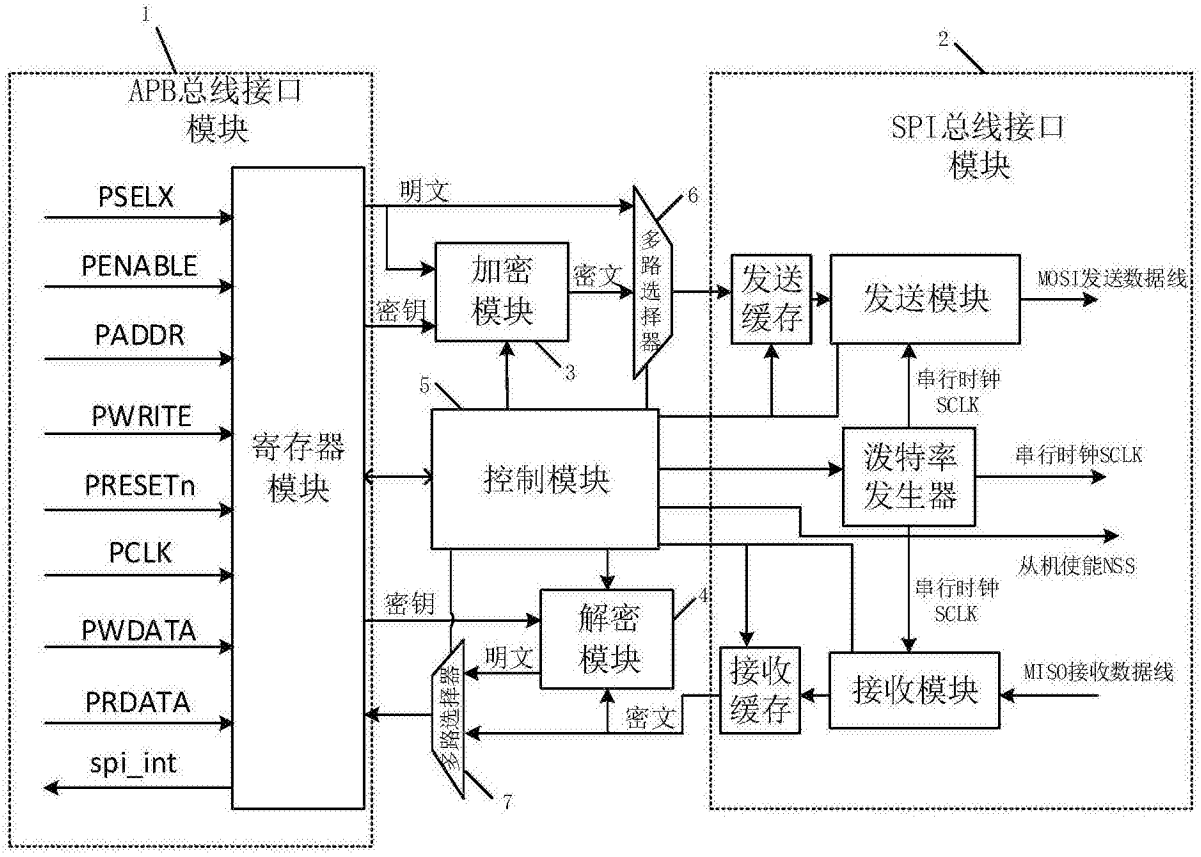

1
APB总线接口
模块
2
SPI总线接口
模块
PSELX
PENABLE
PADDR
PWRITE
PRESETn
PCLK
PWDATA
PRDATA
spi_int
寄存器
模块
明文
密钥
加密
模块
密文
3
多路选择器
6
发送
缓存
发送模块
MOSI发送数据线
串行时钟
SCLK
5
控制模块
波特率
发生器
串行时钟SCLK
从机使能NSS
串行时钟
SCLK
密钥
解密
模块
4
明文
密文
多路选择器
7
接收
缓存
接收模块
MISO接收数据线

图3

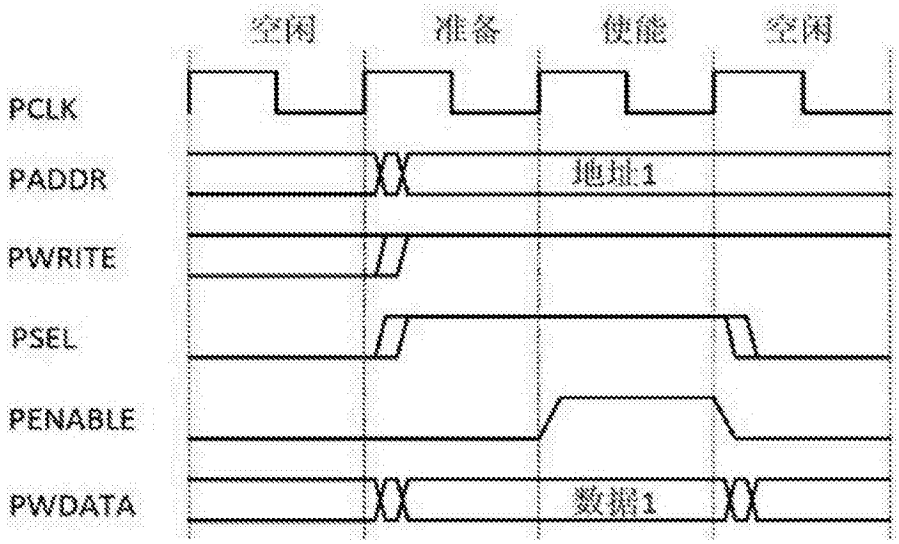

空闲
准备
使能
空闲
PCLK
PADDR
地址1
PWRITE
PSEL
PENABLE
PWDATA
数据1

图4

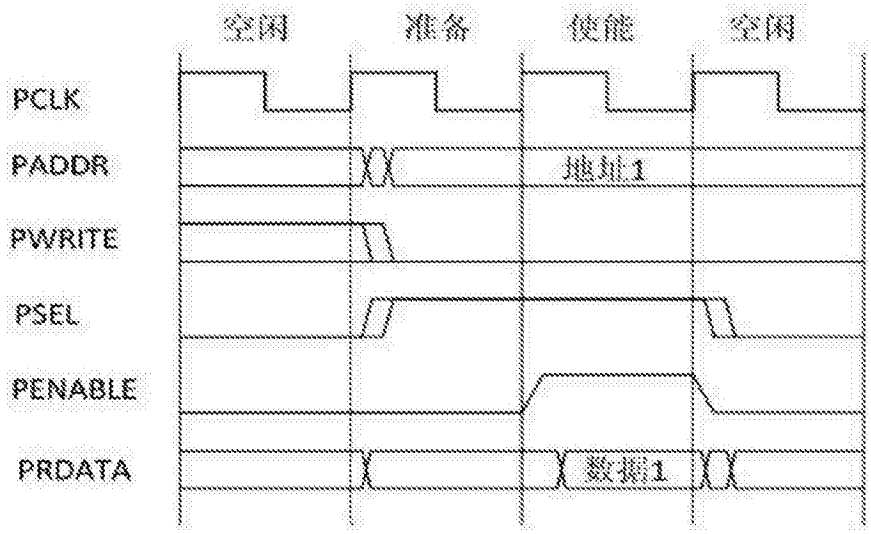

空闲
准备
使能
空闲
PCLK
PADDR
地址1
PWRITE
PSEL
PENABLE
PRDATA
数据1

图5

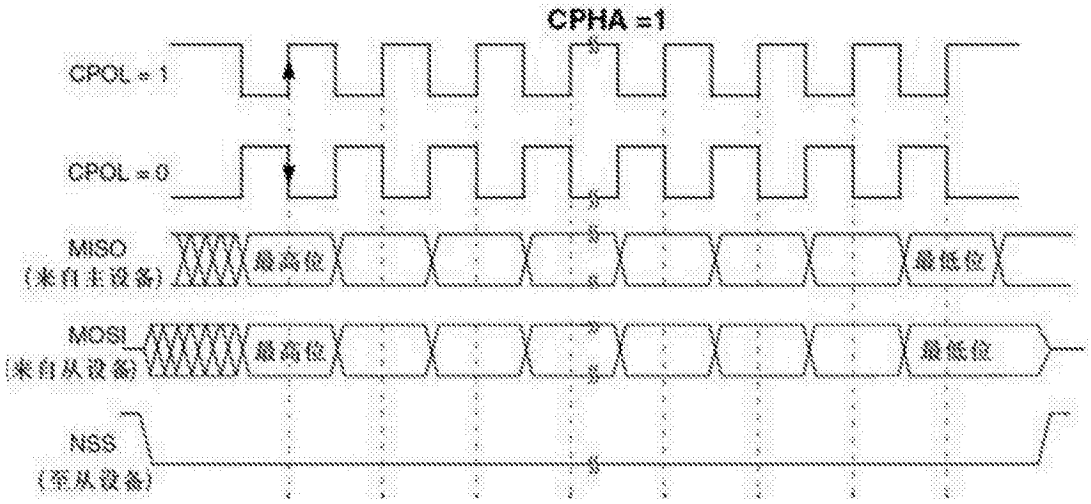

CPHA =1
CPOL = 1
CPOL = 0
MISO
(来自主设备)
最高位
最低位
MOSI
(来自从设备)
最高位
最低位
NSS
(至从设备)

图6

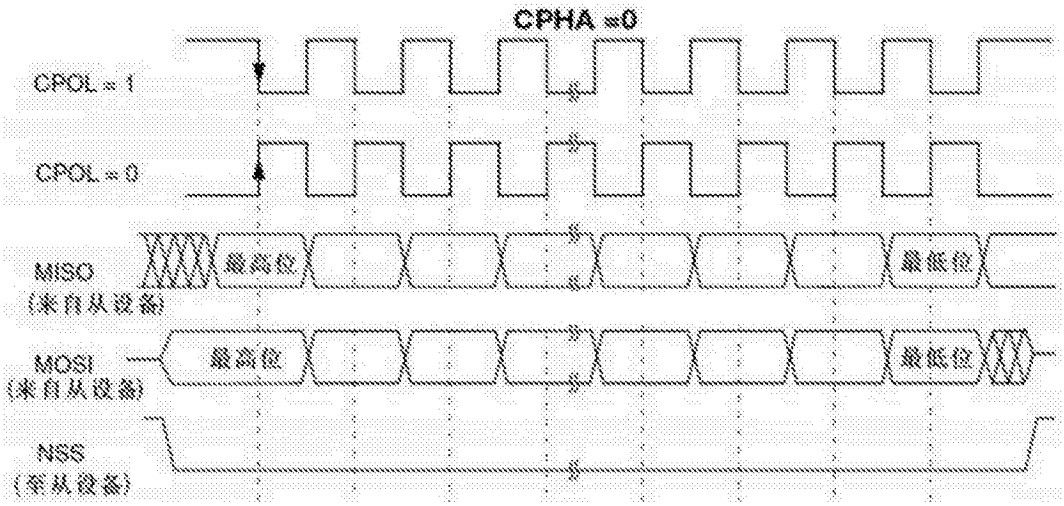

CPHA =0
CPOL = 1
CPOL = 0
MISO
(来自从设备)
MOSI
(来自从设备)
NSS
(至从设备)
最高位
最低位

图7

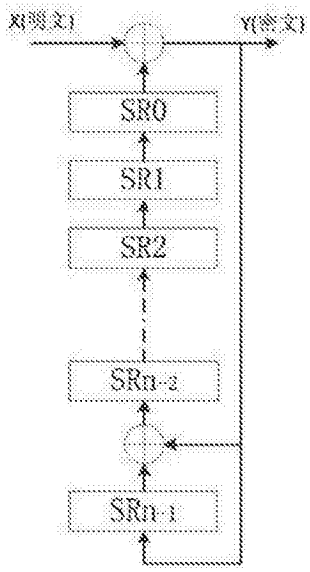

X(明文)
Y(密文)
SR0
SR1
SR2
SRn-2
SRn-1

图8

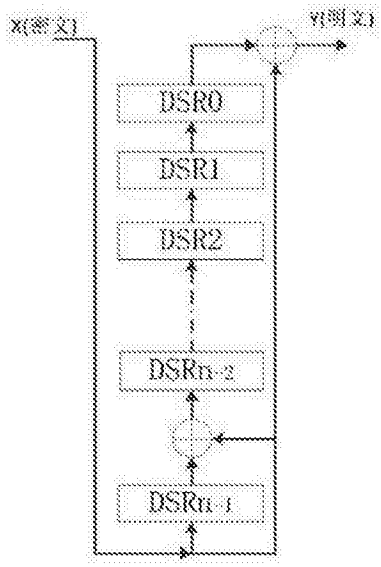


图9