



(12) 发明专利

(10) 授权公告号 CN 112965926 B

(45) 授权公告日 2024. 04. 30

(21) 申请号 202110244211.X

CN 111832090 A, 2020.10.27

(22) 申请日 2021.03.05

CN 111881488 A, 2020.11.03

(65) 同一申请的已公布的文献号

WO 2009051952 A2, 2009.04.23

申请公布号 CN 112965926 A

CN 111917967 A, 2020.11.10

(43) 申请公布日 2021.06.15

CN 103500154 A, 2014.01.08

(73) 专利权人 张玉禄

US 2007235539 A1, 2007.10.11

地址 100102 北京市朝阳区利泽西园一区

CN 102136082 A, 2011.07.27

110楼608号

JP 2007011453 A, 2007.01.18

(72) 发明人 张玉禄

CN 106326966 A, 2017.01.11

(74) 专利代理机构 北京弘权知识产权代理有限公司

CN 101981885 A, 2011.02.23

公司 11363

US 2009144456 A1, 2009.06.04

专利代理师 逯长明 许伟群

WO 2017148221 A1, 2017.09.08

(51) Int. Cl.

CN 2864830 Y, 2007.01.31

G06F 13/40 (2006.01)

JP 2008217116 A, 2008.09.18

G06F 13/42 (2006.01)

CN 208675215 U, 2019.03.29

(56) 对比文件

汪永琳; 丁一. 一种3线制半双工SPI接口设计. 半导体技术. 2010, (05), 全文.

CN 111488305 A, 2020.08.04

审查员 马晓北

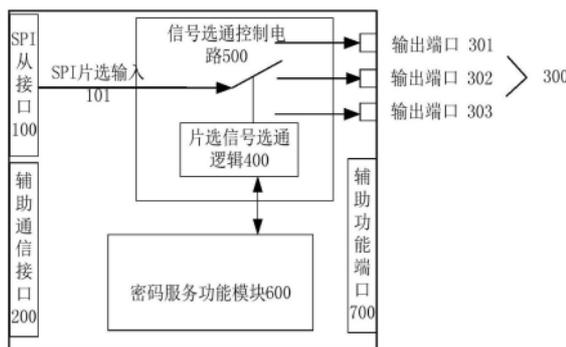
权利要求书2页 说明书8页 附图5页

(54) 发明名称

一种SPI接口安全芯片及SPI接口电子装置

(57) 摘要

本申请公开了一种SPI接口安全芯片及SPI接口电子装置,安全芯片支持SPI从接口, SPI片选输入端口可与安全芯片其他一个或多个输出端口分时选通或者空置,选通路径由内部逻辑状态控制。安全SPI接口电子装置是指具有密码服务功能的SPI设备。具体实现方法是,通过SIP封装方式,将本发明公开的SPI接口安全芯片与普通SPI设备合封在一起。合封打线方法是:安全芯片的SPI接口信号全都引出到对应管脚,普通SPI设备的SPI时钟信号、数据信号也都引出到对应管脚,但普通SPI接口电子装置的SPI片选信号不引出到芯片相应管脚上,而是与本发明的安全芯片对应的输出端口相连接,由安全芯片控制。利用具有该电路结构的安全芯片能简化普通电子装置的安全升级、显著降低升级成本。



1. 一种SPI接口安全芯片,其特征在于,所述安全芯片包括:
至少一个SPI从接口(100),所述SPI从接口(100)包含SPI片选信号输入端口;
与任意一个SPI从接口(100)相连接的信号选通控制电路(500);所述信号选通控制电路(500)设有一个或多个输出端口(300);
片选信号选通逻辑(400),与所述信号选通控制电路(500)连接,被配置为根据所述SPI从接口(100)输入的指令或预设指令控制所述信号选通控制电路(500)分时选通至对应的输出端口(300)或者空置;
密码服务功能模块(600),被配置为通过所述SPI从接口(100)对外提供密码服务;
所述SPI从接口负责SPI主设备与SPI从设备之间的通信,所述SPI片选信号输入端口用于输入SPI片选输入信号,SPI片选信号输入端口与片选信号输出端口(300)连接,以使SPI主设备与片选信号输出端口(300)连接的SPI从设备器件建立通信;所述SPI从设备器件与安全芯片共用时钟信号和数据信号线。
2. 根据权利要求1所述的安全芯片,其特征在于,所述SPI从接口(100)支持1/2/4/8数据线中的任意一种或多种组合。
3. 根据权利要求1所述的安全芯片,其特征在于,所述SPI从接口(100)支持时钟上升沿采样和下降沿采样中的至少一种。
4. 根据权利要求1所述的安全芯片,其特征在于,所述安全芯片还包括:
辅助通信接口(200),所述辅助通信接口(200)为usb、uart、iic、gpio、7816、SWP、1Wire中至少一种,被配置为安全芯片提供数据交换功能。
5. 根据权利要求1所述的安全芯片,其特征在于,所述安全芯片还包括:
辅助功能端口(700),被配置为提供电源、接地、时钟服务。
6. 根据权利要求1所述的安全芯片,其特征在于,所述密码服务功能模块(600)包括:
CPU、算法协处理器、内部存储器、防护传感器、噪声源、电源管理模块、时钟产生电路以及上电复位电路之中的一种或多种。
7. 一种安全SPI闪存电子装置,其特征在于,所述电子装置包括:
普通SPI闪存(30);
如权利要求1至6中任意一项所述的安全芯片(10),所述安全芯片(10)与所述普通SPI闪存(30)以采用封装方式合封;
SPI通信接口,所述SPI通信接口包括时钟端口(41),数据端口(42)和片选信号端口(43);其中,所述安全芯片(10)和普通SPI闪存(30)分别共用时钟端口(41)、数据端口(42);所述片选信号端口(43)与所述安全芯片(10)的片选信号输入端口连接;
所述安全芯片(10)的输出端连接至所述普通SPI闪存(30)的片选信号输入端;所述安全芯片(10)被配置为根据输入的命令,判断是否将片选信号接入普通SPI闪存(30)。
8. 根据权利要求7所述的电子装置,其特征在于,所述普通SPI闪存(30)的存储介质为Norflash或Nandflash。
9. 一种安全SPI接口复合电子装置,其特征在于,所述电子装置包括:
普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器之中的一种或者任意组合;

如权利要求1至6中任意一项所述的安全芯片,所述安全芯片与所述普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中的一种或者任意组合均采用封装方式合封;

SPI通信接口,所述SPI通信接口包括时钟端口(41),数据端口(42)和片选信号端口(43);其中,所述安全芯片和普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中的任意一种均共用时钟端口(41)、数据端口(42);所述片选信号端口(43)与所述安全芯片的片选信号输入端口连接;

所述安全芯片的片选信号输出端口(300)连接至所述普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中任意一种的片选信号输入端;所述安全芯片被配置为根据输入的命令,判断是否将片选信号接入普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组以及SPI接口A/D转换器。

10.根据权利要求9所述的电子装置,其特征在于,所述普通SPI闪存的存储介质为Norflash或Nandflash。

一种SPI接口安全芯片及SPI接口电子装置

技术领域

[0001] 本申请实施例涉及电子装置数据加密、敏感信息保护技术领域,特别涉及一种SPI接口安全芯片及带有该种安全芯片的安全SPI闪存电子装置及安全SPI接口复合电子装置。

背景技术

[0002] 目前,我们信息化网络中分布了各种电子装置,这些电子装置都在面临通过增加密码模块实现安全改造的局面。通过在电子装置中添加密码模块是安全升级的主要方法,在现有技术中,密码模块与主控单元的连接方式多种多样,比如通过usb接口、spi控制接口、iic接口、uart、iis接口、7816、甚至是高速的pcie、sata等接口。

[0003] 然而,上述在电子装置中添加密码模块来实现电子装置安全升级的方法普遍存在一些实际的问题,例如由于主控芯片与SPI接口器件的连接方式固定且唯一,当需要进行安全升级时,必须要重新设计PCB印制电路以提供附加的密码模块相关电路接入,当主控芯片没有多余的接口时甚至需要更换主控芯片,这不仅导致了安全升级工程量大,还极大增加了升级成本。

[0004] 以安全SPI闪存电子装置为例,现有的电子装置通常由普通SPI闪存直接接到SPI各接口,如果要想对该电子装置进行安全升级,必须要采用多余接口外接密码模块来实现,当不存在其他接口时,必须要重新设计电路板,显然占用了大量工作量及升级成本。

发明内容

[0005] 本申请提供了一种SPI接口安全芯片及SPI接口电子装置,利用具有该电路结构的安全芯片可非常简便的实现普通电子装置的安全升级,对现有电子装置的电路影响非常小。

[0006] 第一方面,本申请提供了一种SPI接口安全芯片,包括:

[0007] 至少一个SPI从接口,所述SPI从接口包含SPI片选信号输入端口;

[0008] 与任意一个SPI从接口相连接的信号选通控制电路;所述信号选通控制电路设有一个或多个输出端口;

[0009] 片选信号选通逻辑,与所述信号选通控制电路连接,被配置为根据所述SPI从接口输入的指令或预设指令控制所述信号选通控制电路分时选通至对应的输出端口;

[0010] 密码服务功能模块,被配置为通过所述SPI从接口对外提供密码服务。

[0011] 在一些实施例中,所述SPI从接口支持1/2/4/8数据线中的任意一种或多种组合。

[0012] 在一些实施例中,所述SPI从接口支持时钟上升沿采样和下降沿采样中的至少一种。

[0013] 在一些实施例中,所述安全芯片还包括:

[0014] 辅助通信接口,所述辅助通信接口为usb、uart、iic、gpio、7816、SWP、1Wire中至少一种,被配置为安全芯片提供数据交换功能。

[0015] 在一些实施例中,所述安全芯片还包括:

[0016] 辅助功能端口,被配置为提供电源、接地、时钟服务。

[0017] 在一些实施例中,所述密码服务功能模块包括:

[0018] CPU、算法协处理器、内部存储器、防护传感器、噪声源、电源管理模块、时钟产生电路以及上电复位电路之中的一种或多种。

[0019] 对于通信接口资源紧张的电子装置,本申请提供可以在不更换主控芯片的情况下,仅需用所述安全芯片接管现有SPI接口,便可实现安全升级,提供密码服务功能,同时还可扩展多个SPI设备,分时复用SPI接口通信。

[0020] 第二方面,本申请提供了一种安全SPI闪存电子装置,包括:

[0021] 普通SPI闪存;

[0022] 本申请第一方面所述的安全芯片,所述安全芯片与所述普通SPI闪存以采用封装方式合封;

[0023] SPI通信接口,所述SPI通信接口包括时钟端口,数据端口和片选信号端口;其中,所述安全芯片和普通SPI闪存分别共用时钟端口,数据端口;所述片选信号端口与所述安全芯片连接;

[0024] 所述安全芯片的输出端连接至所述普通SPI闪存的片选信号输入端;所述安全芯片被配置为根据输入的命令,判断是否将片选信号接入普通SPI闪存。

[0025] 第三方面,本申请还提供了一种安全SPI接口复合电子装置,包括:

[0026] 普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器之中的一种或者任意组合;

[0027] 本申请第一方面所述的安全芯片,所述安全芯片与所述普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中的一种或者任意组合均采用封装方式合封;

[0028] SPI通信接口,所述SPI通信接口包括时钟端口,数据端口和片选信号端口;其中,所述安全芯片和普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中的任意一种均共用时钟端口、数据端口;所述片选信号端口与所述安全芯片连接;

[0029] 所述安全芯片的输出端连接至所述普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中任意一种的片选信号输入端;所述安全芯片被配置为根据输入的命令,判断是否将片选信号接入普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组以及SPI接口A/D转换器。

[0030] 现有电子装置在不改变PCB印制电路板的情况下,仅需将普通SPI接口设备更换为本申请中的安全SPI闪存电子装置或安全SPI接口复合电子装置即可实现安全升级。使得现有电子装置的安全改造简单易行、成本可控、性能优异,为电子装置的安全改造提供有力支持,促进产业发展。

附图说明

- [0031] 图1为普通SPI总线信号连接示意图；
- [0032] 图2为扩展SPI总线信号连接示意图；
- [0033] 图3为SPI接口使能后数据传输示意图；
- [0034] 图4为接收方在时钟上升沿沿采样数据线上的数据时序示意图；
- [0035] 图5为接收方在时钟下降沿沿采样数据线上的数据时序示意图；
- [0036] 图6为接收方在时钟上升沿和下降沿均采样数据线上的数据时序示意图；
- [0037] 图7为2线SPI接口按照MSB传输模式信号线与数据位的关系图；
- [0038] 图8为4线SPI接口按照MSB传输模式信号线与数据位的关系图；
- [0039] 图9为8线SPI接口按照MSB传输模式信号线与数据位的关系图；
- [0040] 图10为本申请一种SPI接口安全芯片的结构示意图；
- [0041] 图11为片选信号路径选通后输出信号与片选信号的跟随逻辑图；
- [0042] 图12为一般电子装置中主控芯片与SPI从器件的连接方式图；
- [0043] 图13为图10所述安全芯片在一种实施例下的应用实例图；
- [0044] 图14为本申请中多组命令实现选通路径切换命令的一种实施例时序图；
- [0045] 图15为本申请一种安全SPI闪存电子装置的结构示意图；
- [0046] 图16为图15所示电子装置在一种应用下的内部状态转换图；
- [0047] 图17为本申请一种安全SPI接口复合电子装置的结构示意图。

具体实施方式

[0048] 下面,结合附图以及具体实施方式,对本发明做进一步描述:

[0049] 需要说明的是,SPI是串行外设接口(Serial Peripheral Interface)的缩写,是Motorola公司推出的一种同步串行接口技术,包含SCK(时钟)、CS_n(片选)、MISO(主入从出数据线)、MOSI(主出从入数据线)等信号线,是一种全双工、同步的通信总线,为标准SPI,又称作SPI 1线模式。

[0050] 如图1所示出的,为普通SPI总线信号连接示意图;

[0051] 传输数据时,SPI主设备与SPI从设备之间可采用图中的形式,其中,时钟信号SCK,来自SPI主设备,单向,为片选和数据信号的时序参考源;片选信号CS,来自SPI主设备,单向。SPI主设备可有多个CS,一个片选CS信号对应一个从设备。片选使能时,表示对应的从设备被主设备选择。数据线MOSI用于传输数据,来自主设备,单向。数据线MISO用于传输数据,来自从设备,单向。该总线为全双工,主设备在发送数据的同时也会收到来自从设备发送的数据,主设备在接收数据的同时也会发送数据到从设备。

[0052] 而在本申请实施例中提出的SPI接口是在标准SPI的基础上增加数据线而形成的总线形式,其通信模式从全双工改为半双工,数据线为2/4/8线可选。选用2线、4线、8线模式通信时,将大大提高数据传输能力,因此在实际应用中,根据实际需求,SPI接口支持1/2/4/8数据线可以采用任意一种或几种的任意组合。

[0053] 另外,在实现SPI功能的硬件配置上,目前凡是对性能有一定要求的电子装置,都要求其主控单元具有较高的主频和数据处理能力,与此性能相匹配,此类主控单元基本都支持高速SPI程序存储器读写接口,以便快速读出指令代码;此类SPI程序读写接口时钟频

率最高可达100MHz以上。

[0054] 相对应的,由图2所示出的SPI总线信号连接示意图中,此时SPI从设备具有多个,并且每个片选CS信号对应一个从设备;其中,时钟信号SCK,来自多通道SPI主设备,单向,为片选和数据信号的时序参考源;片选信号CS,来自SPI主设备,单向。SPI主设备可有多个CS,一个片选CS信号对应一个从设备。片选使能时,表示对应的从设备被主设备选通。数据线MOSI/D0用于传输数据,双方向。数据线MISO/D1用于传输数据,双方向。数据线D2-D7均用于传输数据,双方向。该总线为半双工,每次通信时数据线都是相同方向,具体方向由主从双方协商决定。

[0055] 当采用2/4/8线数据线通信时,其数据线与所传输的数据位之间的关系分别如图7、图8和图9所示。

[0056] 进一步的,为了提高数据传输效率,在一些实施例中,SPI接口支持时钟上升沿采样和下降沿采样中一种或两种。图3为SPI接口使能后数据传输示意图。

[0057] 具体的,如图4所示出的为接收方在时钟上升沿采样数据线上的数据时序示意图,此种情况要求传输的数据在时钟上升沿到来之前必须稳定;其中接收方即可以是主设备也可以是从设备。

[0058] 还可以如图5所示出的为接收方在时钟下降沿采样数据线上的数据时序示意图,此种情况要求传输的数据在时钟下降沿到来之前必须稳定;

[0059] 还可以如图6所示出的为接收方在时钟上升沿和下降沿均采样数据线上的数据时序示意图,此种情况要求传输的数据在任何一个时钟沿到来之前都必须稳定。双沿采样可有效提高数据传输效率,在相同时钟频率的情况下,数据传输效率提高一倍。

[0060] 在本实施例中,普通SPI闪存(SPI闪存存储器,SPI flash memory,简称SPI闪存)是采用SPI作为通信接口的闪存存储器,具有接口信号少、芯片面积小、不同容量命令相互兼容等特点,广泛应用于现有的电子设备中,主要用来存储控制程序及数据等信息。目前SPI闪存存储器普遍支持1/2/4/8线数据通信模式的一种或者几种。闪存(flash)又分为Norflash和Nandflash等类型。

[0061] 实施例一

[0062] 参见图10,为本申请一种SPI接口安全芯片的结构示意图;

[0063] 由图10可知,本申请实施例提供了一种SPI接口安全芯片,包括:

[0064] 至少一个SPI从接口100,所述SPI从接口100包含SPI片选信号输入端口;

[0065] 与任意一个SPI从接口100相连接的信号选通控制电路500;所述信号选通控制电路500设有一个或多个输出端口300;其中信号选通控制电路500负责SPI片选信号选通的实现,SPI从接口100输入的片选信号101可与芯片其他多个输出端口信号301/302/303分时选通,一旦与某个输出端口选通,则被选通的输出端口逻辑信号与输入的片选信号保持实时跟随,两者逻辑值保持一致;此外,SPI从接口还可保持空置状态,即不与任何一个输出端口选通,此时只有安全芯片可以通信,其他器件都处于非选通状态,确保SPI接口数据线不会发生冲突。信号跟随时序图如图11所示。

[0066] 选通路径可以在多个输出端口信号之间切换,具体选通路径由芯片内部控制逻辑400状态决定,该控制逻辑状态可通过芯片通信接口发送命令设置,也可按照预置的顺序切换。片选信号选通逻辑400,与所述信号选通控制电路500连接,被配置为根据所述SPI从接

口100输入的指令或预设指令控制所述信号选通控制电路500分时选通至对应的输出端口300。

[0067] 密码服务功能模块600,被配置为通过所述SPI从接口100对外提供密码服务。不限于包括CPU、算法协处理器、内部存储器、防护传感器、噪声源、电源管理模块、时钟产生电路以及上电复位电路;这些模块可组成一个SOC芯片。使得本申请的安全芯片可通过SPI接口或者其他通信接口对外提供密码服务。

[0068] 此外,在一些实施例中,所述安全芯片还包括:

[0069] 辅助通信接口200,所述辅助通信接口200为usb、uart、iic、gpio、7816、SWP、1Wire中至少一种,被配置为安全芯片提供数据交换功能。

[0070] 辅助功能端口700,可以是提供电源、接地、时钟等功能的端口。

[0071] 由上述技术方案可知,使用上述安全芯片,可实现在安全芯片与多个SPI接口器件之间分时、共用SPI接口总线,在不增加SPI接口资源的情况下,便可增加密码模块并能实现SPI从设备的扩展。具体的,上述安全芯片的使用方法如图12所示进行说明:

[0072] 普通电子装置其SPI接口连接方式类似图12所示,使用本发明所述安全芯片对此类电子装置进行安全升级,在使用时其连接方式如图13所示。各个SPI接口电子器件的片选信号交由安全芯片10接管,原有SPI接口器件1的时钟信号和数据信号线与主控芯片20保持原来的连接关系,同时还可以增添SPI接口器件2和器件3;安全芯片10上电默认选通一路SPI片选信号或者选通安全芯片自身。此时电子装置的主控芯片20可与默认选通SPI器件进行数据交互,实现对默认SPI器件的访问;同时安全芯片10监听SPI总线上传输的数据,并解析是否属于通道切换命令。

[0073] 安全芯片10若监听到选通路径切换指令(或者按照预置的规则),则按照切换指令意图改变内部状态,将SPI片选输入信号与对应的输出端口信号连通,选通对应的路径。此时电子装置主控芯片20与被选通SPI器件建立新的通信,可对选通SPI器件进行访问;安全芯片10保持对SPI接口数据的监听,但不会发送数据到SPI数据总线上。

[0074] 若安全芯片10收到关闭其他路径的相关命令(或者按照预置的规则),则改变内部状态,使其他SPI元器件的片选信号都处于禁止状态,此时安全芯片10与主控芯片20之间建立数据通信通道,安全芯片10可作为密码模块为电子装置提供密码服务。

[0075] 电子装置根据需要发送相关指令(或者按照预置的顺序),在安全芯片10和多个SPI元器件之间随时切换,分时复用SPI总线,实现对不同元器件的访问。

[0076] 为避免SPI通信数据误识别为切换命令,命令长度可适当增加或由连续多组命令拼接实现。具体示例图如图14所示。

[0077] 由上述技术方案可知,本申请提供了一种SPI接口安全芯片,包括至少一个SPI从接口,所述SPI从接口包含SPI片选信号输入端口;与任意一个SPI从接口相连接的信号选通控制电路;所述信号选通控制电路设有一个或多个输出端口;片选信号选通逻辑,与所述信号选通控制电路连接,被配置为根据所述SPI从接口输入的指令或预设指令控制所述信号选通控制电路分时选通至对应的输出端口;密码服务功能模块,被配置为通过所述SPI从接口对外提供密码服务。本申请提供的安全芯片,在不更换主控芯片的情况下,仅需用所述安全芯片接管现有SPI接口,便可实现安全升级,提供密码服务功能,同时还可扩展多个SPI设备,分时复用SPI接口通信,极大地减少了安全升级的成本。

[0078] 实施例二

[0079] 参见图15,为本申请提供的一种安全SPI闪存电子装置的结构示意图;

[0080] 由图15可知,对应于上述安全芯片,本申请还提供了一种安全SPI闪存电子装置,所述电子装置包括:

[0081] 普通SPI闪存30;

[0082] 前述实施例提供的安全芯片10,所述安全芯片10与所述普通SPI闪存30以采用封装方式合封;

[0083] SPI通信接口,所述SPI通信接口包括时钟端口41,数据端口42和片选信号端口43;其中,所述安全芯片10和普通SPI闪存30分别共用时钟端口41,数据端口42;所述片选信号端口43与所述安全芯片10连接;

[0084] 所述安全芯片10的输出端连接至所述普通SPI闪存30的片选信号输入端;所述安全芯片10被配置为根据输入的命令,判断是否将片选信号接入普通SPI闪存30。

[0085] 其中,安全SPI闪存是指具有密码服务功能的SPI闪存。该装置实现安全SPI闪存操作时,其SPI通信接口信号与普通闪存的SPI通信接口信号保持一致。安全SPI闪存电子装置在保持普通SPI闪存功能的同时还能提供密码服务功能,可解决现有提供密码服务的电子装置改造工程量、结构复杂、成本高、难实现等问题。

[0086] 所述电子装置具体的实现方法为:将安全芯片10与普通SPI闪存30通过SIP封装方式合封在一起,对外提供与普通SPI闪存30相同的SPI通信接口,该接口包括用于接收时钟信号的时钟端口41、用于连接数据总线的的数据端口42、用于接收片选信号的片选信号端口43。SIP封装具体连线方案为,安全芯片10的时钟信号11与闪存的SPI接口时钟信号31均连接时钟端口41,安全芯片数据总线12和闪存数据总线32均与数据端口42连接,安全芯片的SPI片选信号13与合封后的安全SPI闪存片选信号端口43相连,普通SPI闪存30的片选信号33与安全芯片相应的输出端口14相连,由安全芯片10控制是否将安全芯片的SPI片选信号13直连过来。安全芯片10通过判断SPI接口上传输的命令决定是否接管普通SPI闪存30的片选信号33,使得两者分时复用SPI接口总线。这样,在SPI接口不增加信号线的情况下,既保留了原有的闪存功能,又添加了密码服务模块。现有使用SPI闪存的电子装置,若要进行安全升级改造,由于共用了同一套完全相同的SPI通信接口,只需将普通SPI闪存更换为所述安全SPI闪存即可,其PCB印制电路板以及其他电路均不须改动。

[0087] 本发明的安全SPI闪存电子装置支持的命令包括如下几类:

[0088]

序号	命令类别	功能说明
1	普通 SPI 闪存命令	命令码及时序与普通 SPI 闪存完全一致,负责对普通 SPI 闪存的读、写、控制等访问操作。
2	开启密码服务命令	开启密码服务命令负责选通安全芯片,使普通 SPI 闪存处于禁止状态,安全芯片占用 SPI 总线。 为避免将通信数据识别为该命令,该命令码长度应当增加或者由多组命令码组合而成。
3	关闭密码服务命令	关闭密码服务命令负责选通普通 SPI 闪存,使普通 SPI 闪存由 SPI 接口直接控制,普通 SPI 闪存占用 SPI 总线。 为避免将通信数据识别为该命令,该命令码长度应当增加或者由多组命令码组合而成。
4	密码服务相关命令	负责提供密码服务相关功能,包括数字签名、签名验证、数据加解密、获取随机数、数据写入、数据读出等功能。

[0089] 本发明所述安全SPI闪存内部状态及切换方式如图16所示,安全SPI闪存内部状态在禁止密码服务S1、开启密码服务S2之间切换,分别由启动密码服务命令C1和关闭密码服务命令C2设置。

[0090] 本申请提供的电子装置实现密码服务功能的具体方法如下:

[0091] 上电后安全SPI闪存默认处于状态S1,安全芯片将输入的片选信号透传给普通SPI闪存芯片,通过SPI接口可对SPI闪存执行读、写、控制等操作。此时,安全芯片仅仅监听SPI接口上传的所有数据,不发送数据到SPI接口上。

[0092] 当SPI接口出现启用密码服务的命令C1时,安全芯片和普通SPI闪存均会接收到这一组命令数据,SPI闪存会认为非法指令而忽略该数据,安全芯片则能正确解析为开启密码服务的命令,根据指令设置,关闭SPI片选信号透传功能,将SPI闪存的片选信号设置为无效状态,切换到S2开启密码服务状态。此时,安全SPI闪存可通过SPI接口提供密码服务功能。

[0093] 当SPI接口出现关闭密码服务命令C2时,安全芯片将识别出关闭密码服务功能的命令,并切换到S1禁止密码服务的状态,开启普通SPI闪存片选信号透传功能,再次将普通SPI闪存的片选信号与SPI接口片选输入信号直接相连,此时安全芯片内部可继续进行密码运算等工作,但不再往SPI接口上发送数据,直到再次开启密码服务功能。

[0094] 按照上述流程,安全SPI闪存可通过SPI接口提供普通闪存功能和安全芯片的密码服务功能。

[0095] 由上述技术方案可知,本申请提供了一种安全SPI闪存电子装置,包括:普通SPI闪存;安全芯片,所述安全芯片与所述普通SPI闪存以采用封装方式合封;SPI通信接口,所述SPI通信接口包括时钟端口,数据端口和片选信号端口;其中,所述安全芯片和普通SPI闪存分别共用时钟端口,数据端口;所述片选信号端口与所述安全芯片连接;所述安全芯片的输出端连接至所述普通SPI闪存的片选信号输入端;所述安全芯片被配置为根据输入的命令,判断是否将片选信号接入普通SPI闪存。

[0096] 现有电子装置在不改变PCB印制电路板的情况下,仅需将普通SPI闪存更换为安全SPI闪存即可实现安全升级。使得现有电子装置的安全改造简单易行、成本可控、性能优异,为电子装置的安全改造提供有力支持,促进产业发展。

[0097] 实施例三

[0098] 参见图17,为本申请提供的一种安全SPI接口复合电子装置的结构示意图;

[0099] 与实施例二的不同之处在于,所述电子装置包括:

[0100] 普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中的一种或者任意组合;

[0101] 所述安全芯片与所述普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中的一种或者任意组合均采用封装方式合封;

[0102] 所述安全芯片和普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中的任意一种均共用时钟端口41、数据端口42;

[0103] 所述安全芯片的输出端连接至所述普通SPI闪存、SPI接口Wifi通信模组、SPI接口

蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中任意一种的片选信号输入端；所述安全芯片被配置为根据输入的命令，判断是否将片选信号接入普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组以及SPI接口A/D转换器。

[0104] 在本实施例中，由于采用了上述实施例一中所述的安全芯片，使得该安全芯片可与多个SPI接口设备一并封装至同一个电子装置内，需要说明的是，附图17中仅以三个接口设备为例进行说明，实际可以是任意其它个数，图中的SPI接口设备1-n可以是普通SPI闪存、SPI接口Wifi通信模组、SPI接口蓝牙通信模组、SPI接口指纹模组、SPI接口触控模组、SPI接口实时时钟模组、SPI接口显示控制模块、SPI接口电池管理模组、SPI接口A/D转换器中的任意一种。

[0105] 采用上述电子装置，即可以完成对不同SPI接口设备的分时选通，或者切换至空置状态等操作，更适用于多种场景需求。

[0106] 本实施例中电子装置的实现方法、使用流程及效果可参见实施例二中的描述，在此不再赘述。

[0107] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本发明的其它实施方案。本申请旨在涵盖本发明的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本发明的一般性原理并包括本发明未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本发明的真正范围和精神由下面的权利要求指出。

[0108] 应当理解的是，本发明并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本发明的范围仅由所附的权利要求来限制。



图1

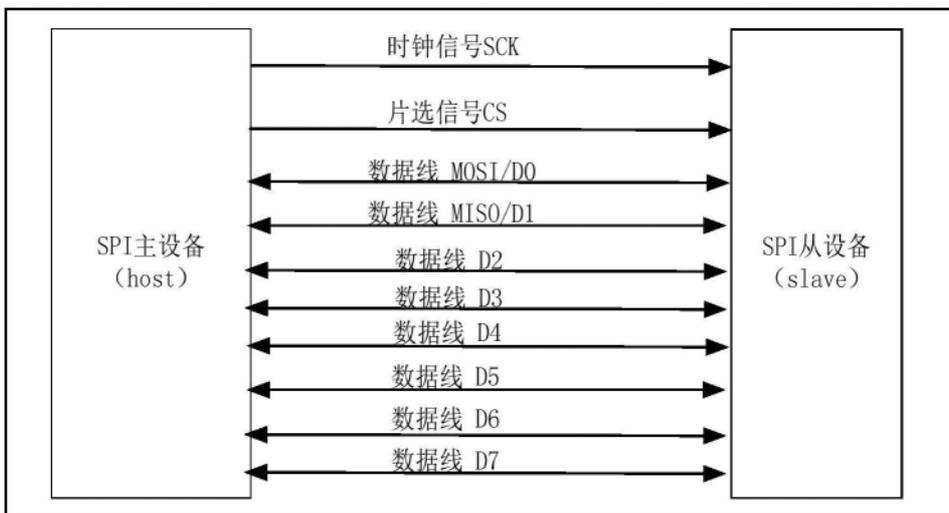


图2

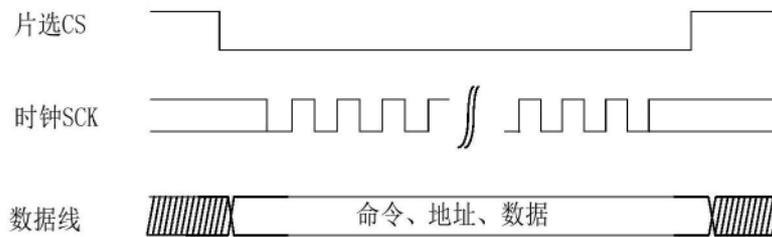


图3

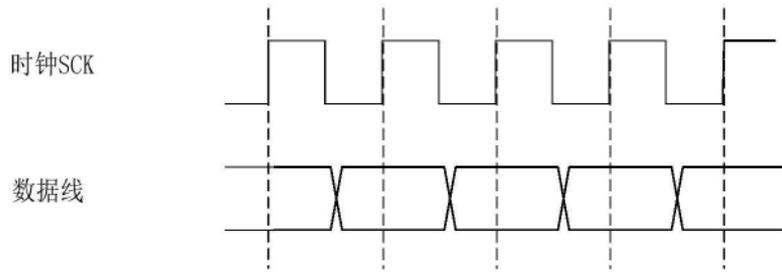


图4

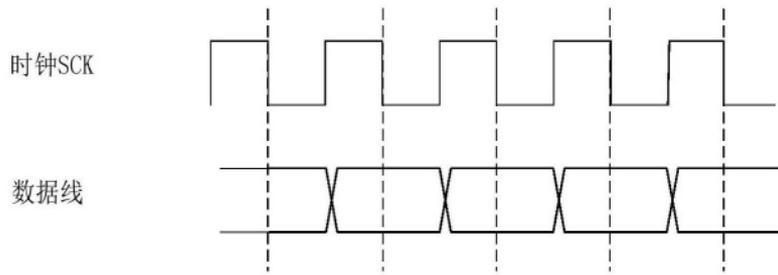


图5

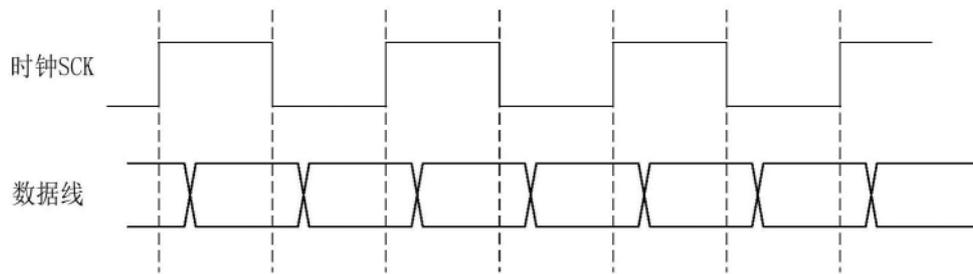


图6

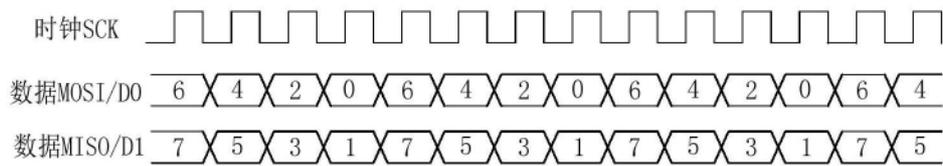


图7

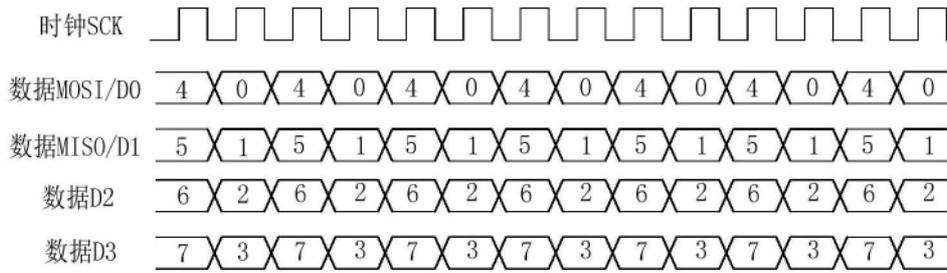


图8

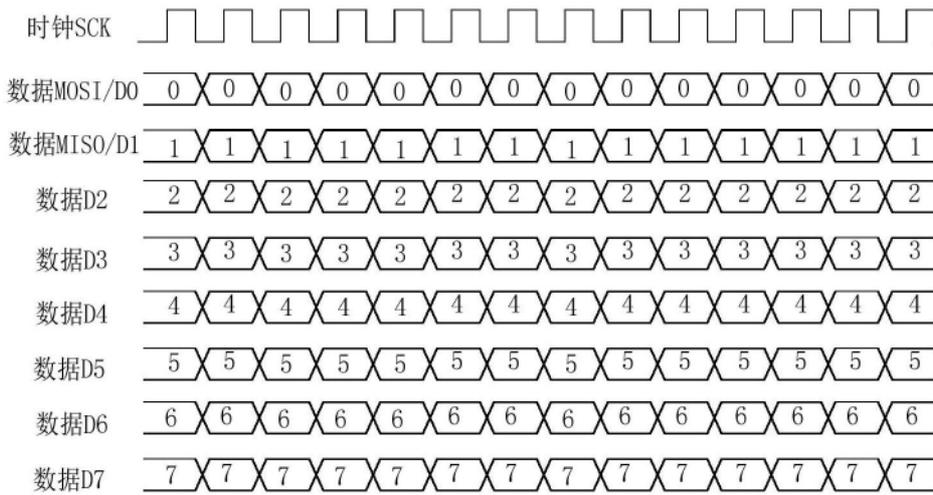


图9

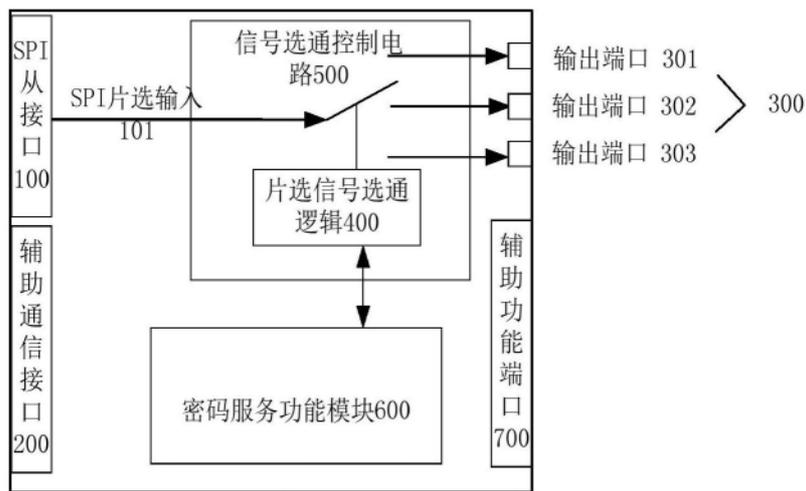


图10

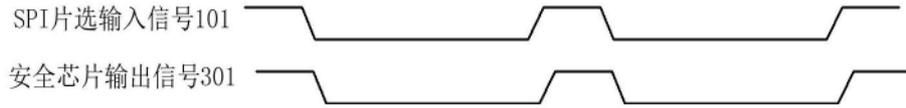


图11



图12

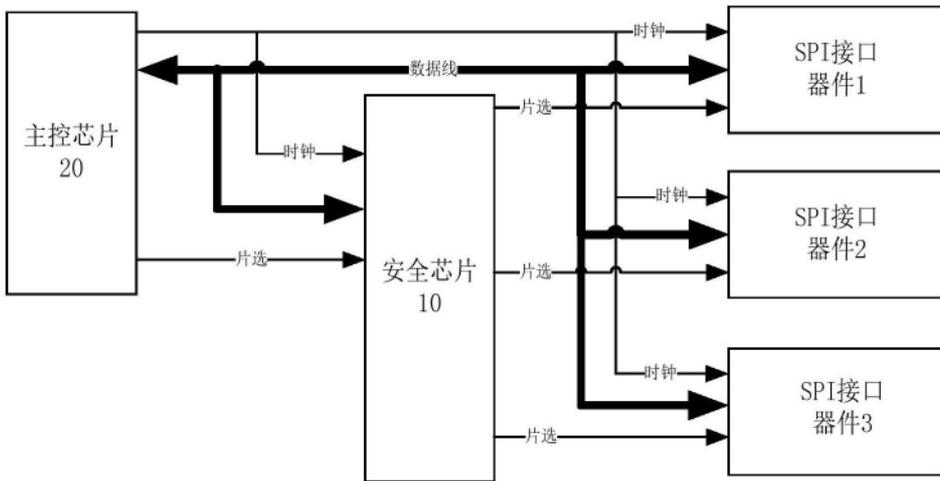


图13

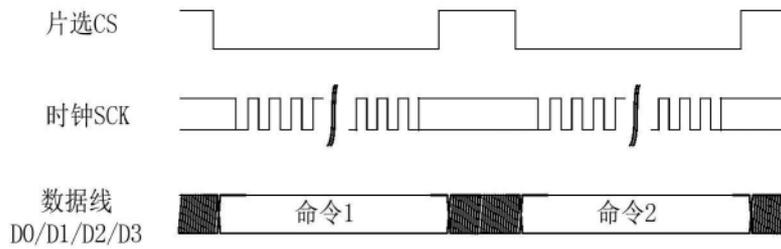


图14

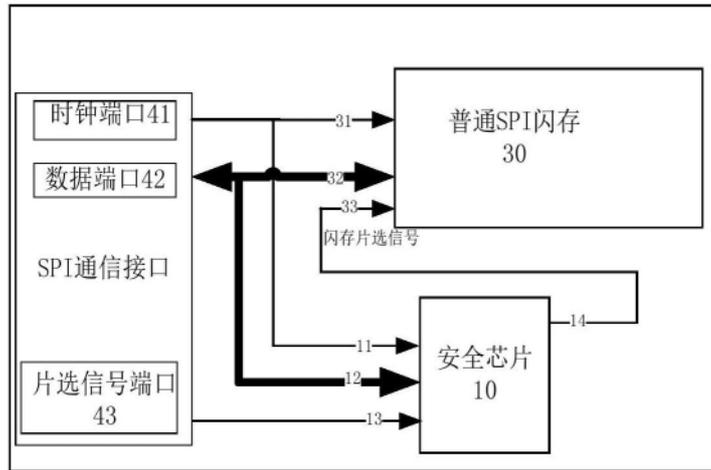


图15

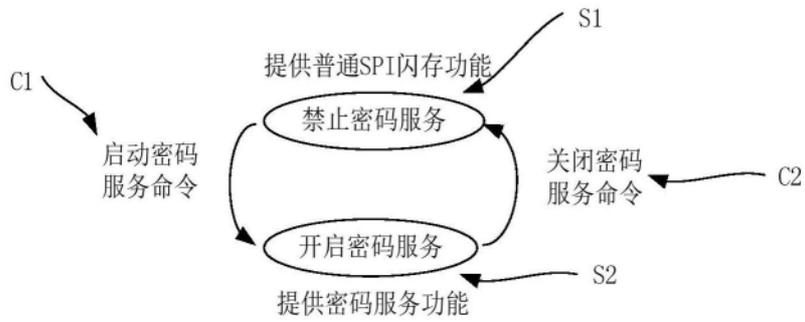


图16

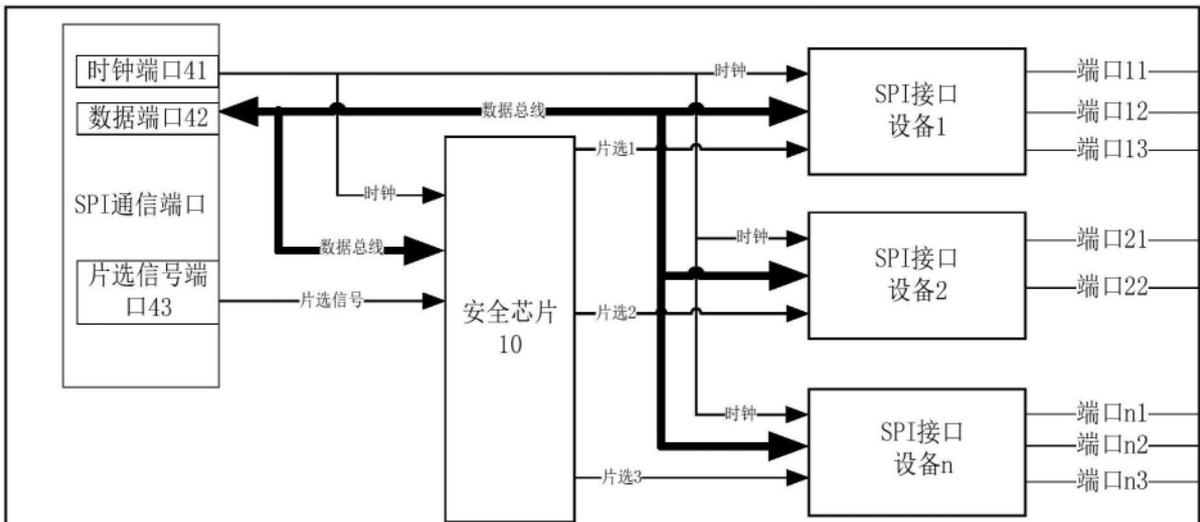


图17