



(12)发明专利

(10)授权公告号 CN 105071933 B

(45)授权公告日 2018.02.06

(21)申请号 201510563255.3

CN 203859823 U, 2014.10.01,

(22)申请日 2015.09.07

CN 204392484 U, 2015.06.10,

(65)同一申请的已公布的文献号

CN 103051444 A, 2013.04.17,

申请公布号 CN 105071933 A

CN 102196425 A, 2011.09.21,

US 2015222619 A1, 2015.08.06,

(43)申请公布日 2015.11.18

审查员 张俊锋

(73)专利权人 安徽问天量子科技股份有限公司

地址 241003 安徽省芜湖市高新区漳河路
12号

(72)发明人 刘梦婕 尹凯 黄敦锋 刘云
苗春华

(51)Int. Cl.

H04L 9/08(2006.01)

H04M 7/00(2006.01)

(56)对比文件

CN 204967836 U, 2016.01.13,

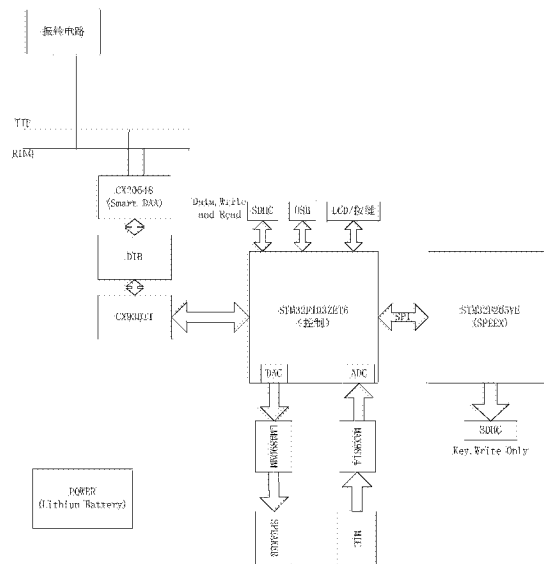
权利要求书1页 说明书3页 附图3页

(54)发明名称

应用于PSTN公网的量子数据终端

(57)摘要

本发明公开了一种应用于PSTN公网的量子数据终端,模数转换模块输入端与电话线连接;数字隔离模块输出端与对数字信号调制解调模块的输入端连接;数字信号调制解调模块通过UART接口与控制MCU连接;还包括用于语音播放的RECIEVE模块、用于语音采样的MIC模块和两个放大模块;其中一个放大模块用于音频放大,另一个放大模块用于将麦克风采集的信号放大;控制MCU通过DAC依次与其中一个放大模块和RECIEVE模块串接;控制MCU通过ADC依次与另一个放大模块和MIC模块串接。本发明可在普通PSTN上实现流畅清晰的保密通话和保密数据的传输,且对密钥SD卡多重保护,提高用户使用安全性。



1. 一种应用于PSTN公网的量子数据终端,包括控制MCU和与控制MCU电连接的语音处理MCU;其特征在于:还包括分别与语音处理MCU连接的SRAM和密钥SD卡;SRAM和密钥SD卡均用于存储密钥;还包括通过USB接口与控制MCU连接的充电口;还包括用于将模拟信号转为数字信号的模数转换模块、数字隔离模块和用于对数字信号进行调制与解调的数字信号调制解调模块;模数转换模块输入端与电话线连接;数字隔离模块输出端与数字信号调制解调模块的输入端连接;数字信号调制解调模块通过UART接口与控制MCU连接;

还包括用于语音播放的RECIEVE模块、用于语音采样的MIC模块和两个放大模块;其中一个放大模块用于音频放大,另一个放大模块用于将麦克风采集的信号放大;控制MCU通过DAC依次与其中一个放大模块和RECIEVE模块串接;控制MCU通过ADC依次与另一个放大模块和MIC模块串接;

还包括分别与控制MCU连接的用于读写存储待加密传输的用户文件的SD卡接口、用于拷贝密钥、充电或者作为访问用户文件传输卡的扩展USB接口和用于显示和操作保密终端的LCD按键。

2. 根据权利要求1所述的应用于PSTN公网的量子数据终端,其特征在于:所述控制MCU为STM32F103VE系列处理器。

3. 根据权利要求1或2所述的应用于PSTN公网的量子数据终端,其特征在于:所述语音处理MCU为STM32F205RE系列处理器。

4. 根据权利要求3所述的应用于PSTN公网的量子数据终端,其特征在于:SRAM并且用过密钥删除,掉电密钥删除。

5. 根据权利要求4所述的应用于PSTN公网的量子数据终端,其特征在于:所述与语音处理MCU连接的SRAM和密钥SD卡在密钥粉碎上用硬件擦除方式,将用过的存储区域擦掉,并写上新的伪随机数,用过的密钥不可还原。

6. 根据权利要求5所述的应用于PSTN公网的量子数据终端,其特征在于:外部USB口不能访问密钥SD卡,且在提供给对外的访问接口中删除读操作,SD卡只能写不能读。

7. 根据权利要求6所述的应用于PSTN公网的量子数据终端,其特征在于:开放给用户的文件传输卡和密钥SD卡均为SDHC卡。

应用于PSTN公网的量子数据终端

技术领域

[0001] 本发明涉及一种量子数据终端,尤其涉及一种应用于PSTN公网的量子数据终端。

背景技术

[0002] 目前的PSTN网络在客户终端一般是模拟接入,在经过运营商的配线箱和交换机后则被转换成数字信号,其中模数、数模转化存在失真。这也是本发明采用数字加密而不是模拟加密的原因之一。为了实现在模拟线路中进行数字信号传输,需要进行数字信号的调制和解调。这对调制、解调模块的设计和选择上提出了较高的要求。现有基于PSTN公网的量子数据终端中存在:1) 体积较大,不适用于外出携带;2) 和其他电话设备匹配差,音质一般;3) 对密钥SD卡的保护较差,SD卡可方便取出,在普通电脑上访问;4) 使用专业音频压缩芯片,成本较高,安全性降低。

发明内容

[0003] 本发明的目的是提供一种应用于PSTN公网的量子数据终端,应用于PSTN公网的量子数据终端基于PSTN公网,可在普通PSTN上实现流畅清晰的保密通话和保密数据的传输,且对密钥SD卡实现多重保护,提高用户使用安全性。

[0004] 为实现上述技术目的,本发明采取的技术方案为:应用于PSTN公网的量子数据终端,包括控制MCU和与控制MCU电连接的语音处理MCU;其特征在于:还包括分别与语音处理MCU连接的SRAM和密钥SD卡;SRAM和密钥SD卡均用于存储密钥;还包括通过USB接口与控制MCU连接的充电口;还包括用于将模拟信号转为数字信号的模数转换模块、数字隔离模块和用于对数字信号进行调制与解调的数字信号调制解调模块;模数转换模块输入端与电话线连接;数字隔离模块输出端与数字信号调制解调模块的输入端连接;数字信号调制解调模块通过UART接口与控制MCU连接;

[0005] 还包括用于语音播放的RECIEVE模块、用于语音采样的MIC模块和两个放大模块;其中一个放大模块用于音频放大,另一个放大模块用于将麦克风采集的信号放大;控制MCU通过DAC依次与其中一个放大模块和RECIEVE模块串接;控制MCU通过ADC依次与另一个放大模块和MIC模块串接;

[0006] 还包括分别与控制MCU连接的用于读写存储待加密传输的用户文件的SD卡接口用于拷贝密钥、充电或者作为访问用户文件传输卡的扩展USB接口和用于显示和操作保密终端的LCD按键。

[0007] 保密终端支持文件传输,开放一个SD口供用户使用,可以把需要传输的内容拷贝到这张文件传输卡上。

[0008] 作为本发明进一步改进的技术方案,所述控制MCU为STM32F103VE系列处理器。

[0009] 作为本发明进一步改进的技术方案,所述语音处理MCU为STM32F205RE系列处理器;

[0010] 作为本发明进一步改进的技术方案,SRAM并且用过密钥删除,掉电密钥删除。

[0011] 作为本发明进一步改进的技术方案,所述与语音处理MCU连接的SRAM和密钥SD卡在密钥粉碎上用硬件擦除方式,将用过的存储区域擦掉,并写上新的伪随机数,用过的密钥不可还原。

[0012] 作为本发明进一步改进的技术方案,外部USB口不能访问密钥SD卡,且在提供给对外的访问接口中无读操作,SD卡只能写不能读。

[0013] 作为本发明进一步改进的技术方案,开放给用户的文件传输卡和密钥SD卡均为SDHC卡。

[0014] 本发明选用了工业级的Modem模块作为数据调制解调的核心,在保证系统功能实现和稳定性的同时,大大降低了开发难度,利于产品的快速成型。Modem模块在选型上选择可以支持语音、传真、数据发送等多种功能的模块,对于数字文件的保密传输支持包括文档、图片等类型文件的加密传输。Modem模块与后端MCU通过全双工UART连接,操作简单。采用“一次一密”对称加密方式,可实时从QKD上取密钥对通话和文件进行加密传输,也可以在密钥存储区域(RAM、SD卡)预先存储密钥,用于外出或无QKD场所使用。总之,本发明基于PSTN公网,可在普通PSTN上实现流畅清晰的保密通话和保密数据的传输,且对密钥SD卡实现多重保护,提高用户使用安全性。

[0015] 说明书附图

[0016] 图1为本发明的结构示意图。

[0017] 图2为CODEC软件处理流程示意图。

[0018] 图3上位机软件写密钥SD卡的流程示意图。

具体实施方式

[0019] 实施例1

[0020] 参见图1、图2和图3,本应用于PSTN公网的量子数据终端,包括控制MCU和与控制MCU电连接的语音处理MCU;还包括分别与语音处理MCU连接的SRAM和密钥SD卡;SRAM和密钥SD卡均用于存储密钥;还包括通过USB接口与控制MCU连接的充电口;还包括用于将模拟信号转为数字信号的模数转换模块、数字隔离模块和用于对数字信号进行调制与解调的数字信号调制解调模块;模数转换模块输入端与电话线连接;数字隔离模块输出端与数字信号调制解调模块的输入端连接;数字信号调制解调模块通过UART接口与控制MCU连接;还包括用于语音播放的RECIEVE模块、用于语音采样的MIC模块和两个放大模块;其中一个放大模块用于音频放大,另一个放大模块用于将麦克风采集的信号放大;控制MCU通过DAC依次与其中一个放大模块和RECIEVE模块串接;控制MCU通过ADC依次与另一个放大模块和MIC模块串接;还包括分别与控制MCU连接的用于读写存储待加密传输的用户文件的SD卡接口用于拷贝密钥、充电或者作为访问用户文件传输卡的扩展USB接口和用于显示和操作保密终端的LCD与按键。保密终端支持文件传输,开放一个SD口供用户使用,可以把需要传输的内容拷贝到这张文件传输卡上。

[0021] 作为优选方案,所述控制MCU为STM32F103VE系列处理器。所述语音处理MCU为STM32F205RE系列处理器。SRAM用过密钥删除,掉电密钥删除。所述与语音处理MCU连接的SRAM和密钥SD卡在密钥粉碎上用硬件擦除方式,将用过的存储区域数据擦掉,并写上新的伪随机数,用过的密钥不可还原。外部USB口不能访问密钥SD卡,对外的访问接口无读操作,

SD卡只能写不能读。开放给用户的文件传输卡和密钥SD卡均为SDHC卡。

[0022] 本应用于PSTN公网的量子数据终端有两颗MCU,如图1所示,一颗做控制用,一颗做语音处理用。主控单元是系统运行的核心管理器,需要负责系统资源的调配、通路及存储器的读写、用户接口信息的检测与处理、信息的显示。本发明实现多压缩码率可选,经实测可在5000bps码率下可清晰通话且失真率较低,可以进行简单人声身份验证。即使在通信环境很差情况下,也可支持3000bps码率下的清晰通话。

[0023] 对于保密产品,密钥的安全性是保密产品安全的关键。由于采用“一次一密”加密技术,只要能够保证用过的密钥及时擦除粉碎,未用的密钥被盗不产生危害,只要将与其配对机器上未用的密钥丢弃即可,从而保证保密产品的安全性。

[0024] 对于量子数据终端,本发明支持两种密钥存储方式,SRAM和SD卡存储。SRAM掉电密钥删除,保证了密钥的安全性。

[0025] 另外,对于长期在外用户,本发明还支持SD卡密钥存储方式,最大支持到8G密钥。对于SD卡密钥用户,用以下方式保证密钥的安全性:

[0026] 1) 在密钥粉碎上,本发明用硬件擦除方式,将用过的存储区域数据擦掉,并写上新的伪随机数,用过的密钥不可还原;

[0027] 2) 外部USB口访问不到密钥SD卡,对外的访问接口中无读操作,SD卡只能写不能读;

[0028] 3) 结构上将密钥SD卡固定在机壳内,密钥卡只能通过破坏机壳才能盗走,机壳一旦被破坏一定人为可以发现。

[0029] 密钥存储SD卡在普通电脑上不可见,只可以用我公司开发的专用上位机软件进行多重身份验证后才可以写密钥,且密钥内容单向不可读,只可以写。保证了密钥SD卡的安全。

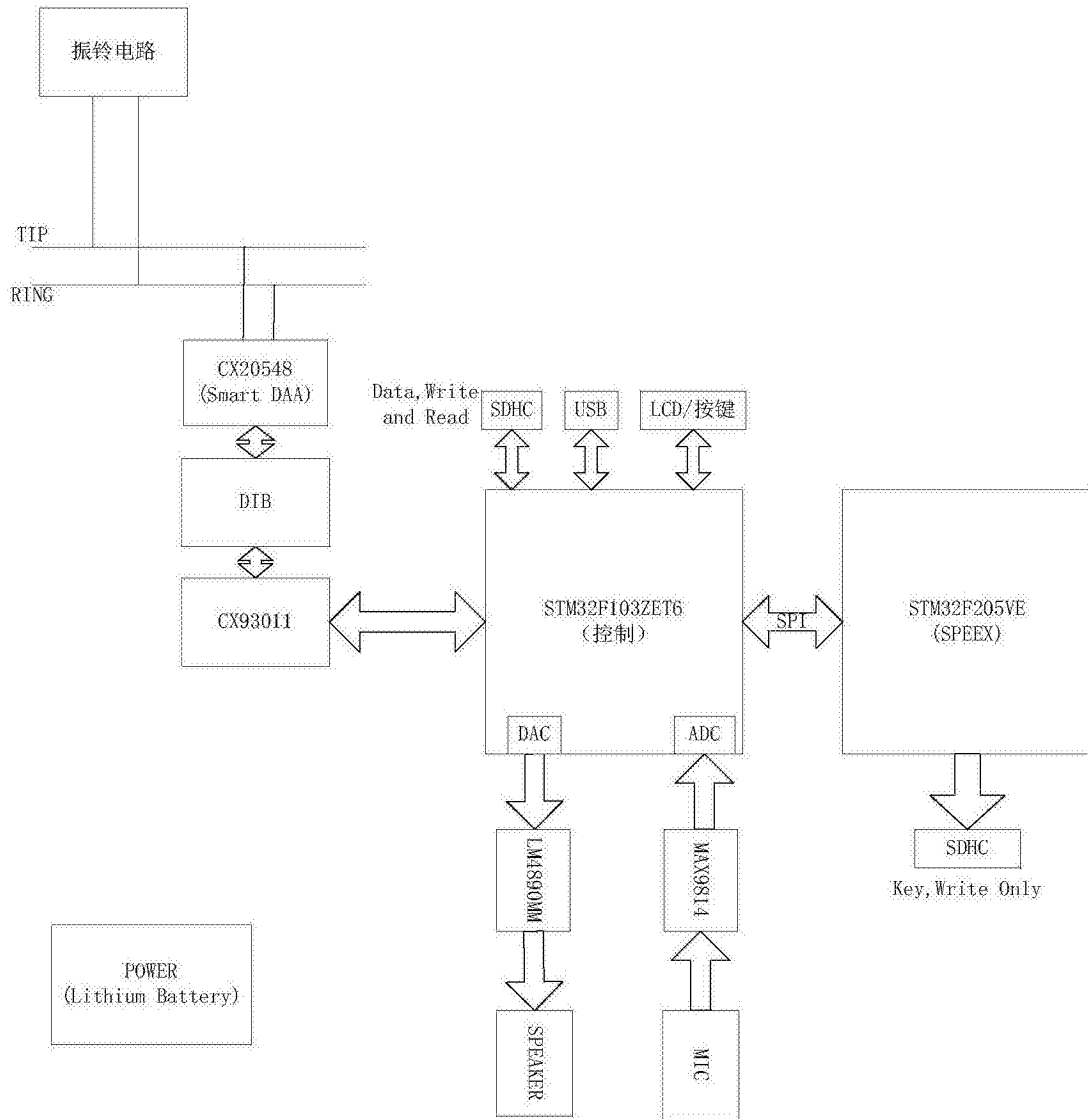


图1

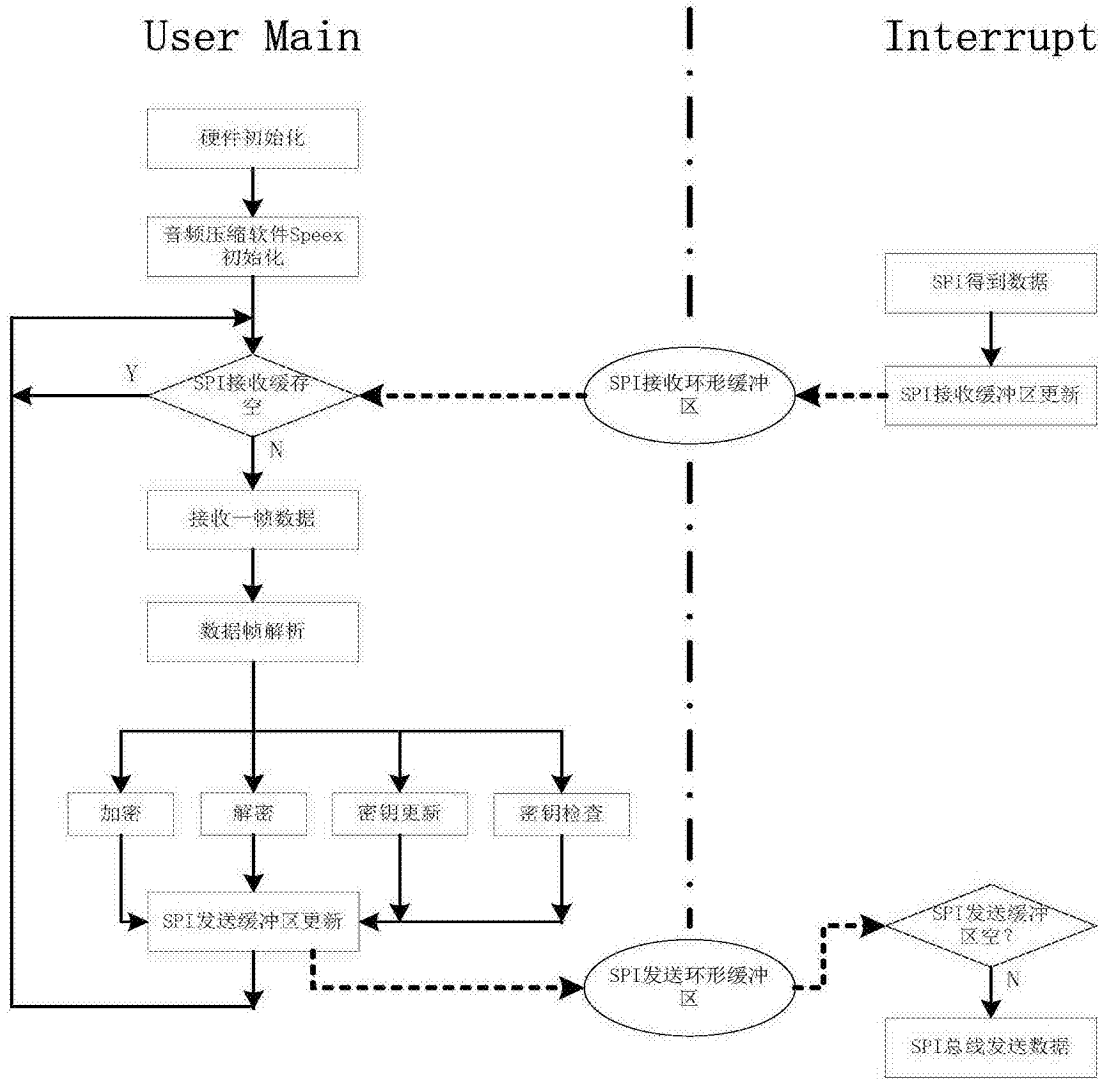


图2

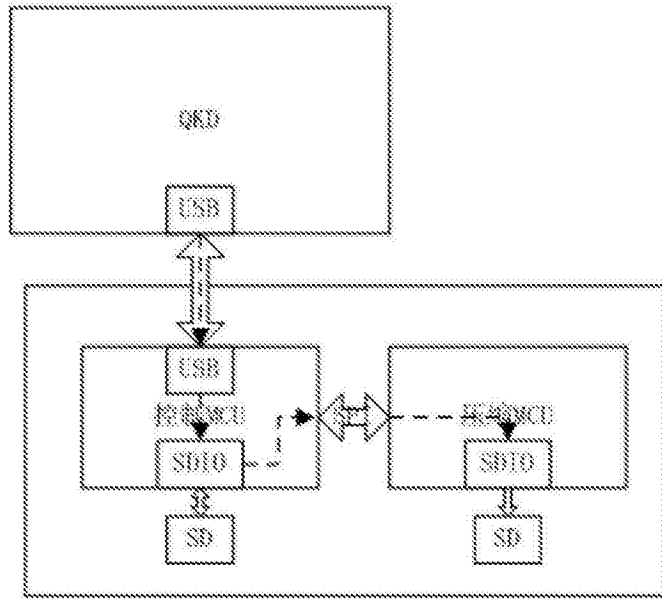


图3