国民技术
nationz technologies

Z32HUB 芯片简介

V1.0

声明

国民技术股份有限公司（以下简称国民技术）保有在不事先通知而修改这份文档的权利。国民技术认为提供的信息是准确可信的。尽管这样，国民技术对文档中可能出现的错误不承担任何责任。在购买前请联系国民技术获取该器件说明的最新版本。对于使用该器件引起的专利纠纷及第三方侵权国民技术不承担任何责任。另外，国民技术的产品不建议应用于生命相关的设备和系统，在使用该器件中因为设备或系统运转失灵而导致的损失国民技术不承担任何责任。国民技术对本手册拥有版权等知识产权，受法律保护。未经国民技术许可，任何单位及个人不得以任何方式或理由对本手册进行使用、复制、修改、抄录、传播等。

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南区粤兴三道9号华中科技大学产学研基地A座2-7层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

注意

这是国民技术不便于披露的文件，它包含一些保密的信息。在没有签订任何保密协议前或者在国民技术单方面要求的情况下请归还于国民技术。任何非国民技术委托人不得使用或者参考该文件。

如果你得到了这份文件，请注意：

- 不得公开文档内容
- 不得转载全部或部分文档内容
- 不得修改全部或部分文档内容

在以下情况这份文件必须销毁

- 国民技术已经提供更新的版本
- 未签订保密协议或者保密协议已经过期
- 受委托人离职

致我们的客户：

我们一直在不断的改进我们的产品及说明文档的品质。我们努力保证这份文档的说明是准确的，但也可能存在一些我们未曾发现的失误。如果您发现了文档中有任何疑问或错失的地方请及时联系我们。您的理解及支持将使得这份文档更加完善。

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南区粤兴三道9号华中科技大学产学研基地A座2-7层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

Z32HUB 芯片简介

概述

Z32HUB 是一款带有硬件 USB2.0 Full Speed 的高性能 32 位 USB KEY 芯片，带有 1 路 SPI 主接口、1 路 UART 接口、特别定制化耳机接口和丰富的 GPIO。集成了 32 位 ARM 高性能安全核、16KB 核外 RAM 和 320KB 内置 FLASH，内置 SM1/SM3/SM4 算法运算单元、带 3KB 专用 RAM 的 64 位公钥密码引擎（ECC/SM2/RSA1024/RSA2048）、DES/3DES 算法运算单元、AES 算法运算单元、SHA1/SHA256/SHA384/SHA512 算法运算单元和真随机数发生电路。Z32HUB 芯片采用高安全设计，提供电压、温度、频率、光照异常检测，内部错误实时侦测模块进行实时错误侦测，独特的版图设计保护信号层不受攻击，独特功耗处理技术防止功耗和电磁辐射分析。

功能框图

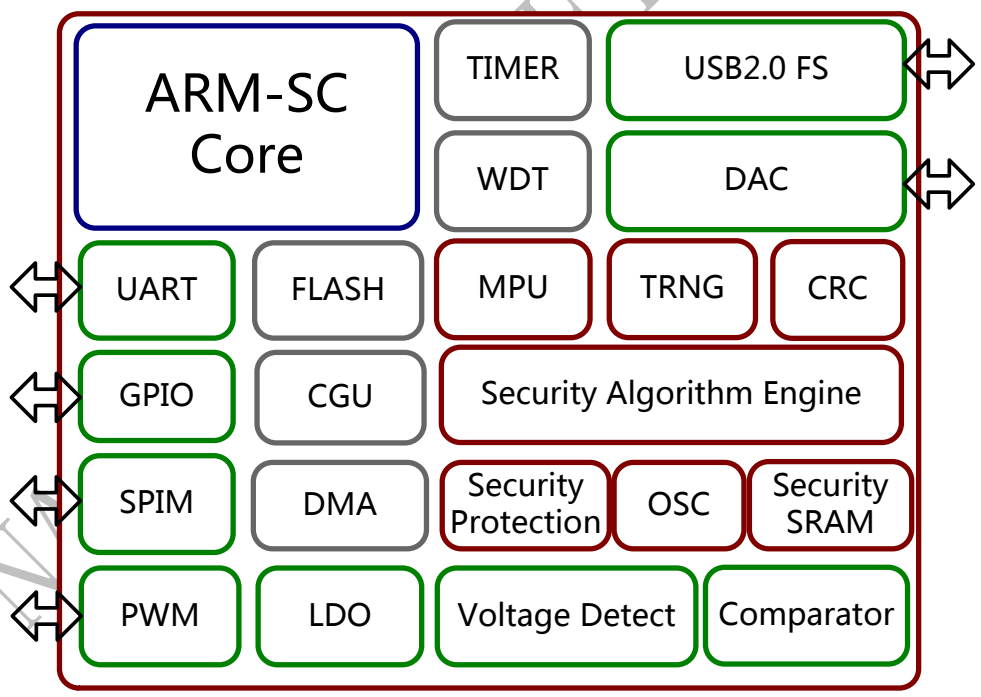

图 1 Z32HUB 功能框图

关键特性

处理器系统

- 采用 32 位高性能 ARM 安全核，大端对齐，支持 Thumb/Thumb-2 指令集；

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南区粤兴三道9号华中科技大学产学研基地A座2-7层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

- 支持 4K Bytes ICACHE；
- 支持中断：支持中断嵌套，中断优先级可配置；
- 系统时钟源来自 OSC 60MHz，支持分频；
- 低功耗模式支持：Idle 模式、Sleep 模式；
- 支持 2 路 32 位 Timer；
- 支持 1 路看门狗定时器；
- 支持 DMA 数据传输；

存储单元

- 片上集成 320K Bytes 嵌入式 Flash，页面大小 512Bytes，最小擦写次数 10 万次@25°C；
- 片上集成 19K Bytes SRAM（16K Bytes XRAM + 3K Bytes ARAM）；
- 支持存储保护单元（MPU），实现安全访问控制和多用户分区管理；

安全组件

- 64 位高速硬件公钥算法引擎，支持 RSA1024、RSA2048、ECC、SM2 算法运算
- DES 算法单元
- SM1 算法单元
- SM3 算法单元
- SM4 算法单元
- SHA 算法单元
- AES 算法单元
- 真随机数发生器
- CRC 校验单元：满足 ISO/IEC 3309 标准，支持多项式 $X^{16}+X^{15}+X^{2}+X^{0}$；
- 安全检测与防护单元
  - 光照异常检测单元
  - 电压异常检测单元
  - 温度异常检测单元
  - 频率异常检测单元
  - 模块实时错误侦测单元（GLUE）
  - 主动防护层检测单元（MESH）；
- 存储器加密机制
- 唯一芯片序列号
  - 每颗芯片都具有唯一序列号

通讯接口

- USB2.0 全速设备接口
  - 遵循 USB2.0 FS 协议规范；
  - 支持 1 个控制端点、3 个中断端点（IN/IN/OUT）、2 个 BULK（IN/OUT）；
  - 支持无晶振工作模式；
- SPI 主接口（SPIM）
  - 1 路 SPI 主接口；

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南区粤兴三道9号华中科技大学产学研基地A座2-7层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

- 时钟速率可配，最高时钟支持 15MHZ；
- 支持 Quad 、Dual 、Standard SPI 模式；

- UART 接口
  - 1 路 UART 接口；
  - 时钟源可选择外部晶振和内部 OSC；
  - 典型波特率支持 115200bps；
- PWM 接口
  - 1 路 PWM 接口；
- GPIO
  - 支持 22 个可复用 GPIO 接口，所有 IO 都支持上、下拉可配置；
  - 10 个中断/唤醒 IO；
  - IO 驱动能力不小于 4mA，其中 2 个 IO 驱动能力不少于 12mA；

模拟模块

- 对外供电（VDD33）：
  - 支持输出 3.3V（+/-10%），驱动能力 50mA；
  - 支持限流保护；
  - 支持短路保护；
- DAC 模块
  - 最高输出信号频率为 400KHz；
  - 10 位 DAC；
  - 量化电平支持配置为 3V、2.4V、1.8V；

电气特性

- 支持工作电源输入范围：2.7V~5.5V；
- Power Down 模式功耗：1uA；
- Sleep 模式功耗：130uA；
- 典型工作模式：20mA@60MHz；2mA @2.5MHz；
- ESD：±4KV（HBM）；
- 工作温度：-25℃～85℃；
- 存储温度：-40℃～125℃；

芯片封装

- 封装形式：QFN32

安全认证

- 国家密码管理局安全芯片密码检测二级认证
- 国家信息安全测评中心 EAL4+认证
- FIPS 140-2 CAVP 认证

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南区粤兴三道9号华中科技大学产学研基地A座2-7层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

- USB IF 认证
- 银检 USBKEY 测试

产品应用

- 耳机 KEY；
- 蓝牙 KEY；
- 二代 KEY；
- 标准 KEY；
- 安全加密模块

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南区粤兴三道9号华中科技大学产学研基地A座2-7层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057