Z32HCD2/2S
芯片简介

国民技术股份有限公司

版本历史

版本	日期	作者	备注
V1.0	2014-02-18		发布
V1.1	2015-08-27		更新

文档说明

权利申明

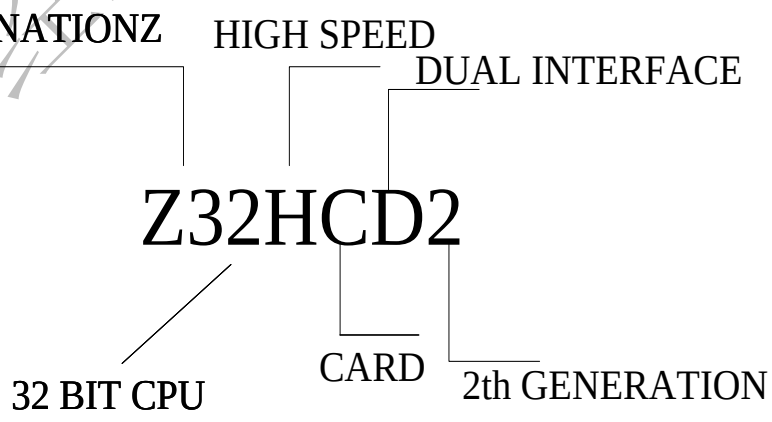
第一部分 系统概述

1 概述

Z32HCD2/2S 是国民技术第二代双界面智能卡芯片。该芯片主要应用于金融 IC 卡、居民健康卡、金融社保卡等高端智能卡领域。芯片采用 32 位 ARM 安全处理器，集成有 8KB+3KB SRAM、40KB/80KBEEPROM、256KB/320KBROM 及硬件算法协处理器和真随机数发生器。硬件算法协处理器提供性能优异的 SM1、SM2、SM3、SM4、SM7、SSF33、DES/3DES、RSA、ECC、SHA-1/SHA-256 安全算法。在通讯接口上，该芯片具有 ISO/IEC 7816 接触、ISO/IEC 14443 非接触(TypeA/B)以及 GPIO 接口。在安全性上，芯片具备主动防护层、被动防护层、光温传感器、胶粘逻辑等高安全性防护措施，满足银联芯片安全认证、国密型号（二级）、CC EAL5+等认证的要求

Z32HCD2/2S 芯片采用 0.13um 工艺，相对于第一代产品 Z32H256CPR(D040)在系统时钟、算法性能、安全性、Java 执行效率、系统功耗及控制方面有显著地提升，接口和存储资源也更为丰富。

1.1 命名规则



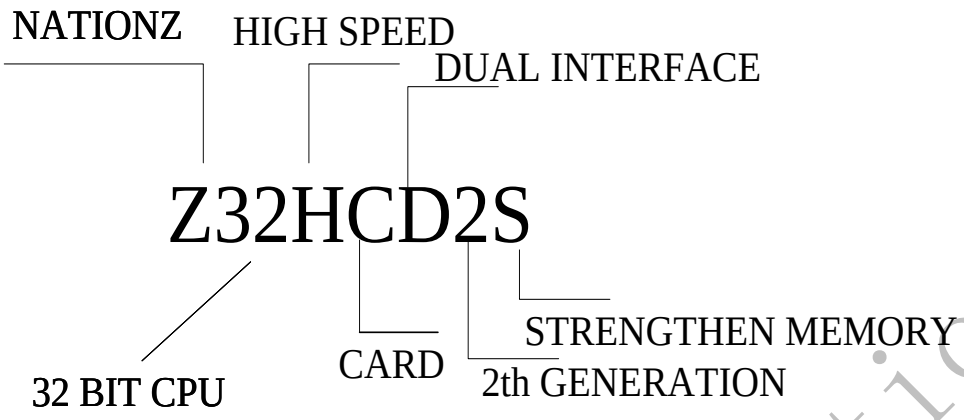


表 1-1 命名规则

Z32HCD2/2S	
Z	国民技术安全芯片名称代号
32	32 位 CPU
H	高速
C	智能卡
D	支持双界面
2	第二代
S	容量增强

1.2 系统框图

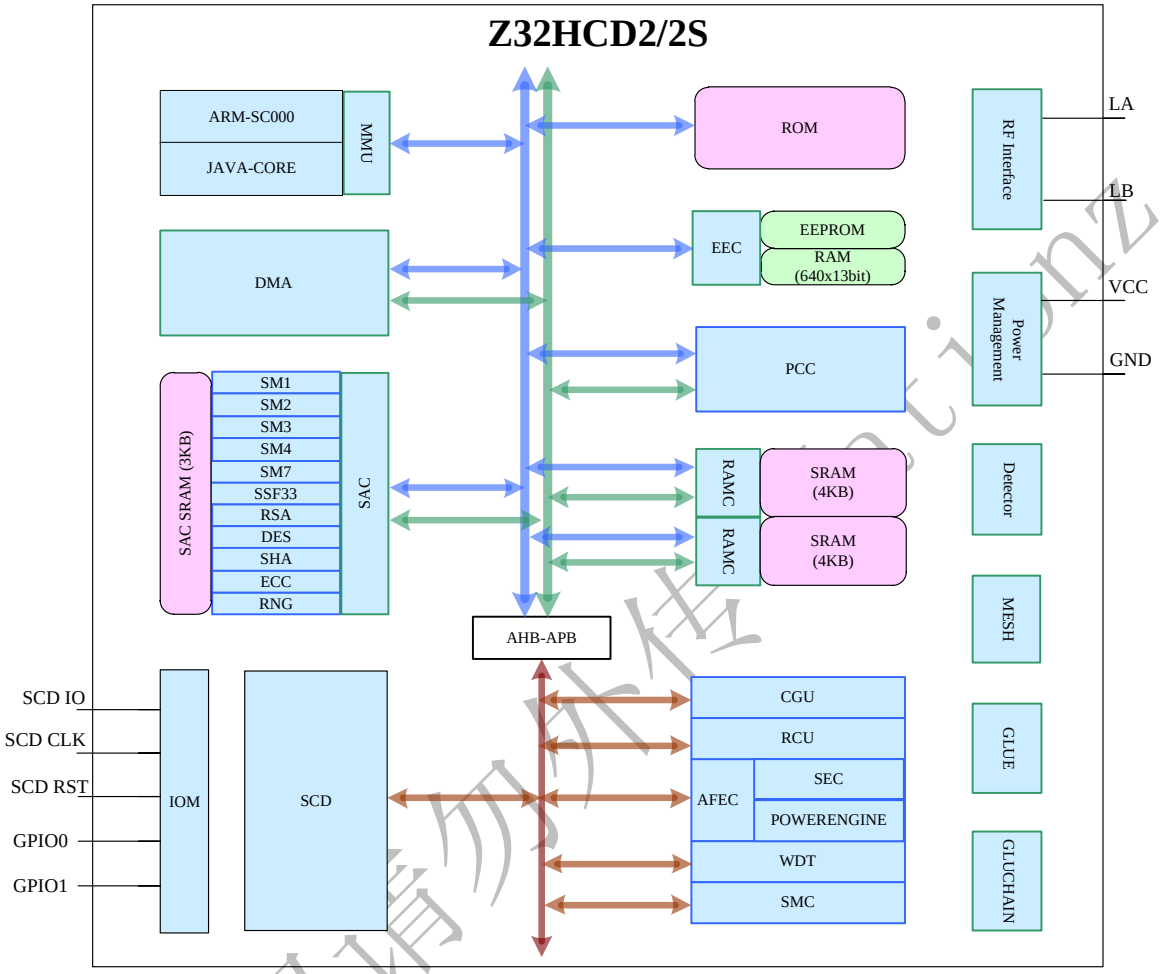


图 1-1Z32HCD2/2S 芯片总体框图

1.3 系统组件

1.3.1 CPU 核

Z32HCD2/2S 采用 32 位高性能、高安全、低功耗的 ARM SC000 处理器，其仿真器支持 ULINK 在线调试，可有效缩短客户开发周期。

1.3.2 系统控制

Z32HCD2/2S 支持多用户、多应用场景，并提供物理地址隔离功能来保护客

户知识产权。芯片支持 4 级中断优先级，支持中断现场硬件自动保护功能。芯片在非接模式下可根据磁场强弱自动调整芯片负载功耗以满足不同场景的刷卡需求。

1.3.3 存储介质

Z32HCD2/2S 具有 SRAM、EEPROM、ROM 三种存储介质。系统支持在 SRAM 执行程序，支持多种 EEPROM 编程模式。在 50M 系统时钟下，ROM 读性能可达 20ns/次，SRAM 读写性能可达 20ns/次。

1.3.4 智能卡接口

Z32HCD2/2S 具备接触、非接触接口。接触式接口支持 ISO/IEC 7816 T=0/1 协议，波特率最高可达 800Kbps@10MHz 通信时钟；非接触接口支持 ISO/IEC 14443 TypeA/B 协议，支持 106Kbps~848Kbps 波特率；支持 2 组独立的 GPIO。

1.3.5 算法协处理器

Z32HCD2/2S 具有丰富的算法协处理器资源，涵盖常用的对称、非对称和哈希算法。国民技术提供算法库给客户配套使用，可有效缩短客户的开发时间，提高应用的整体性能。对称算法支持 DES/3DES、SM1、SM4、SM7、SSF33，非对称算法支持 RSA、ECC、SM2，哈希算法支持 SHA-1、SHA-256、SM3。

1.4 外观与封装

卡封装 Pin 位置排布如下图所示：

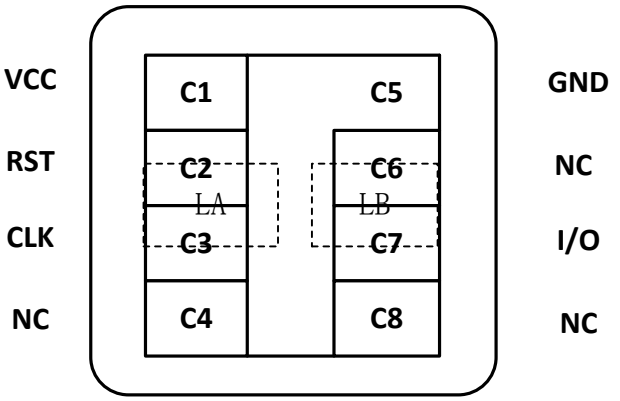


图 1-2 卡封装 Pin 映射图

卡封装 Pin 功能定义示于表 1-2

表 1-2 卡封装 Pin 说明表

管脚编号	管脚名称	管脚描述	管脚方向
C1	VCC	电源	输入
C2	RST	复位	输入
C3	CLK	时钟	输入
C4	NC	---	---
C5	GND	接地	输入
C6	NC	---	---
C7	IO	智能卡设备接口数据线	双向
C8	NC	---	---
LA	---	天线连接点	---
LB	---	天线连接点	---

2 系统特性

2.1 基本特性

2.1.1 CPU 特性

- 32bit 高性能、低功耗安全处理器，3 级流水线
- 总线结构：32 位 AMBA 总线

- 系统大小端：大端
- 中断系统：支持 32 个外部中断源，4 级中断优先级
- 指令集：支持 Thumb 指令集
- 乘法器：支持硬件乘法器
- 低功耗模式：自动打盹模式、休眠模式、IDLE 模式
- 支持 Java 协处理器

2.1.2 用户管理

- 多用户：支持将 ROM 及 EEPROM 划分为 4 个用户
- 用户分类：1 个特权级用户， 3 个普通用户
- 用户权限分级：特权用户和普通用户拥有不同的访问权限

2.1.3 系统时钟

- 接触模式：最高 50MHZ，支持 1~32 分频
- 非接模式：最高 50MHZ，支持 1~32 分频
- 模块时钟独立：CPU、总线、算法协处理器工作时钟频率可独立配置

2.1.4 工作模式

- 接触模式

接触系统工作，非接系统不工作

- 非接模式

非接系统工作，接触系统不工作

- 双界面模式

接触和非接系统可单独工作

对接触和非接系统同时供电，只启动接触系统

2.1.5 存储单元

- ROM

容量 256KB（客户可用 240KB）/320KB（客户可用 304KB）

用于程序、函数库、常量数据的存储

- EEPROM

容量 40KB/80KB

页面大小 128B

数据保持时间 20 年

重复擦写次数 50 万次

Page 擦除时间 1.0ms

Page 编程时间 2.0ms

用于程序、数据的存储

- SRAM

总容量 11KB：算法 SRAM 3KB，通用 SRAM 8KB

用于程序变量存储

其中 256KB ROM 版本固定搭配 40KB EEPROM，320KB ROM 版本固定搭配 80KB EEPROM

通信接口

- ISO/IEC 7816 从接口

  接口支持 Class A/B 类型，自适应

  接口接收 FIFO 为 9 级深度

  支持最大速率为 500Kbps@5Mhz 通信时钟

- ISO/IEC14443 接口

  支持 ISO/IEC 14443 TypeA/B 射频协议，协议类型可配

  支持 106Kbps~848Kbps 波特率

  正常工作场强范围 1A/m~7.5A/m

2.1.6 GPIO 接口

支持 4 个 GPIO 接口，其中 2 个与 ISO/IEC 7816 接口复用

2 个独立 GPIO，支持外部中断和低功耗唤醒

2.1.7 其他特性

- TIMER

  核内 SysTick Timer，支持 24 位递减计数

  核外 1 组独立 Timer,支持 10 位计数，步长可配

  非接和接触接口 Timer，支持 FWT 和 ETU 计数

- WDT

  支持 17/20/23/26 位计数

2.1.8 工作环境

表 2-1Z32HCD2/2S 工作环境表

符号	描述	最小值	最大值	条件
To	工作温度（℃）	-25	85	
TS	存储温度（℃）	-40	125	
Vesd(HBM)	静电限值（kV）		±6	VCC、GND、CLK、RST、SIO、GPIO0、GPIO1
			±4	LA、LB
Vesd(CDM)	静电限值(V)		±500	所有管脚
Ilu	Latch-up 电流值（mA）		±200	Vin>VCC

2.2 安全特性

2.2.1 加密算法

Z32HCD2/2S 的算法包括 SM1、SM2、SM3、SM4、SM7、SSF33、RSA(位宽可配置，最高支持 2048 位)、ECC、SHA-1/SHA-256、DES/3DES。

2.2.2 随机数发生器

- 真随机数发生器
- 随机性满足经国家密码管理局审批的《随机性检测规范》要求

2.2.3 安全检测

- 高低电压安全检测
- 高低频率安全检测
- 温度异常检测
- 光检测
- 场强检测

2.2.4 安全防护

- 总线加密
- 时钟加扰
- 存储加密
- 存储区访问控制
- 时钟和复位信号脉冲过滤
- 安全优化布线
- 每一芯片唯一序列号
- 内部上电复位
- 被动防护层
- 主动防护层
- 胶粘逻辑
- 不可逆自毁
- 测试模式不可逆

2.3 芯片应用

2.3.1 应用领域

- 金融 IC 卡
- 居民健康卡
- 金融社保卡
- 公交卡
- 门禁卡