1 芯片概述

Z8IDA 芯片是基于 EEPROM 工艺的安全芯片，它内嵌一个安全 8 位 MCU 核 NZ8051-SC，支持 DES、AES、SHA、ECC、RSA 等国际标准算法，SM2、SM3、SM4 等国密算法，真随机数发生器 RNG。通信接口支持标准速率 I^2C 从接口和 ISO7816 从接口 SCD，内嵌 32KB EEPROM 和 8KB SRAM，用户可将自定义程序下载到芯片运行，实现防抄板、设备认证、数据加解密等功能。

2 芯片资源

2.1 CPU 核

Z8IDA 芯片主频 12M，完全兼容 51 指令，每个机器周期 1 个时钟周期，而 Intel8051 每个机器周期 12 个系统时钟周期

中断结构：具有 5 个中断源，2 个优先级

位寻址功能

定时器：2 个 16 位可编程定时器/计数器

看门狗定时电路

低功耗模式：支持低功耗 PD 模式

核内 256 字节 iRAM

2.2 存储介质

Z8IDA 具有 8K SRAM（5K 通用，3K 算法专用）和 32K EEPROM 两种存储介质。其中 EEPROM 支持在线编程（程序改写 EEP，直接调用编程接口即可）。

数据保持时间 20 年

重复擦写次数 50 万次

编程时间：2ms

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

2.3 通讯接口

Z8IDA 具备智能卡接触式接口，支持 ISO/IEC 7816 T=0/1 协议，波特率最高可达 625Kbps@5MHz 通信时钟；

Z8IDA I^2C 从接口最高速率可达到 150Kbps（Demo 代码可以提供）

2.4 算法模块

Z8IDA 硬件支持大数运算，能够快速实现多种加解密算法。支持的算法有 DES、AES、国密 SM2、SM3、SM4、2048bit 以内的 RSA、512bit 以内的 ECC、SHA1、SHA256 和随机数 RNG。原厂提供算法库，用户开发只需调用函数接口。

常用算法性能：

DES 加解密 16 字节时间：7ms（含通信时间）

RSA 加解密 128 字节时间：112ms（含通信时间）

2.5 高强度安全

2.5.1 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

2.5.2 安全防护

- 总线加密
- 时钟加扰
- 存储加密

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057