

▶ DMT-CBS-CE3D

大容量双界面安全芯片

芯片简介

目 录

1	芯片概述.....	2
2	芯片特性.....	2
3	芯片功能框图.....	3
4	芯片开发工具.....	3
5	芯片封装.....	4
6	平台和应用.....	5
7	应用领域.....	6
	版本说明.....	7
	法律声明.....	7
	联系我们(Contact Us).....	7

1 芯片概述

DMT-CBS-CE3D 金融安全芯片采用高安全、高性能、低功耗 CPU 内核，拥有 128KB EEPROM 用户数据存储空间容量配置。芯片适用 JAVA、GP 平台，通过金融和行业应用的 EAL4+、银联、国密认证，可实现“一芯多用，一芯通用，应用动态管理”，应用于金融支付、公共服务、公共交通和高安全认证增值服务等诸多领域。

2 芯片特性

■ CPU

- ◆ 32 位 ARMSC000
- ◆ 系统时钟：
 - 内部时钟：最大 30MHz (支持分频)
 - 外部时钟：1MHz~5MHz

■ 通信接口

- ◆ 接触 ISO/IEC 7816
 - T=0、T=1
 - 支持 PPS 协商
 - 支持多级速率（最高 97 速率）
- ◆ 非接触 ISO/IEC 14443 TypeA&B
 - 支持多级速率（最高 848Kbps）
- ◆ Mifare classic (1KB/4KB 可配)

■ 电特性

- ◆ 工作电压：1.62V~5.5V
- ◆ 最大工作电流：
- ◆ 小于 5mA @ (5V & 5MHz)
- ◆ 休眠电流：小于 200uA @ (5V & 1MHz)
- ◆ 工作温度：-25℃~+85℃
- ◆ ESD：接触式大于 4000V
- ◆ ESD：非接触式大于 6000V

■ 存储器

- ◆ ROM: 320KB
- ◆ **EEPROM: 128KB**
 - EEPROM 擦写次数 30 万次以上
 - EEPROM 数据保存时间 20 年以上
- ◆ RAM: 14KB
 - 10KB CPU RAM
 - 4KB 算法专用 RAM

■ 安全算法

- ◆ 国际算法：
 - 对称算法：DES、3DES、AES
 - 哈希算法：SHA1
 - 非对称算法：
 - RSA(2048bits)、ECC(512bit)
- ◆ 国产算法：
 - 对称算法：SSF33、SM1、SM4
 - 哈希算法：SM3
 - 非对称算法：SM2

■ 安全特性

- ◆ 硬件真随机数发生器、加解密协处理器
- ◆ 存储器访问控制单元、加解密设计、数据校验
- ◆ Active Shield、Active Fuse 安全机制

- ◆ 防 SPA/DPA 攻击设计、看门狗
- ◆ 电压、场强、频率、温度、光、Glitch 安全检测单元
- ◆ 金属屏蔽层

3 芯片功能框图

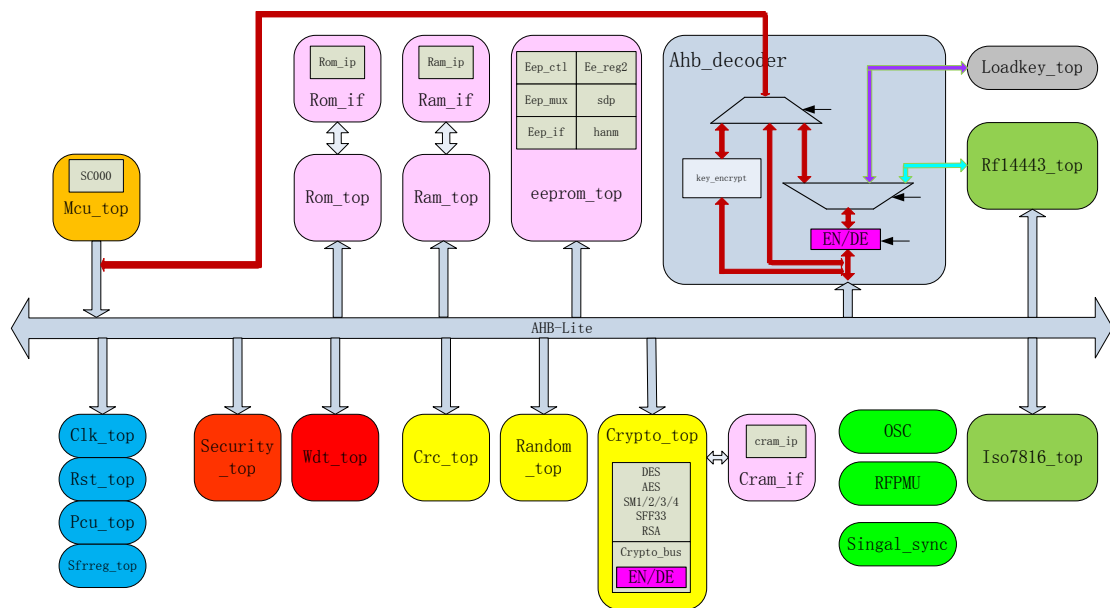


图 3-1: 功能框图

4 芯片开发工具

- 硬件开发环境（ULINK仿真器、FPGA开发板）
- 软件开发环境（IDE: Keil uVision 4）
- 芯片用户手册和开发环境指导文档
- 算法和驱动API库
- Demo COS和示例程序

5 芯片封装

6.1 产品形态

产品形态	封装形式
Wafer	12吋
Module	接触式模块、非接触式模块、双界面模块
Card	接触式智能卡、非接触式智能卡、双界面智能卡、异形卡

6.2 管脚定义

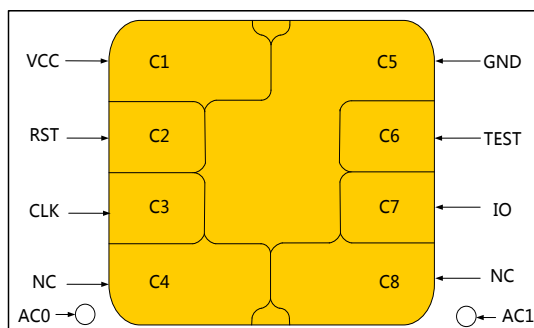


图 6-2 模块封装接线图

符号	功能
VCC	电压
RST	复位
CLK	时钟
NC	N/A
VSS/GND	接地
TEST	测试管脚
I/O	数据管脚
AC0	射频信号0
AC1	射频信号1

6 平台和应用

DMT-CBS-CE3D 芯片可搭载 DMTJRJCOS (JAVA 平台)，此平台完全遵循 JAVA CARD 和 GP 标准规范，由大唐微电子自主研发；通过银联卡嵌入式软件安全认证、Oracle 和 GP 组织的产品检测和评估；全面满足金融 IC 卡和其他高安全领域的应用要求。

- 满足多应用动态加载管理、支持多安全域管理；
- GP 版本：V2.1.1， JAVA 版本：V2.2.2；
- 金融及行业应用支持：

行业		应用
金融类	PBOC3.0 (支持双算法、兼容 PBOC2.0)	1. 借贷记； 2. 单币/双币电子现金； 3. QPBOC； 4. QPBOC 小额支付扩展应用； 5. UICS 应用 (含 ODA)； 6. PBOC 2.0 电子钱包/电子存折(ED/EP)； 7. PBOC 2.0 电子钱包/电子存折(ED/EP)扩展应用；
行业类		1. 居民健康卡应用； 2. 住建部应用； 3. 公安部 eID 应用； 4. 交通部应用； 5. 新一代社保应用； 6. 客户定制化行业增值应用；

7 应用领域

- 银行卡
- 多应用卡
- 医疗
- 移动支付
- 公共服务
- 认证鉴权
- 物联网

版本说明

版本号	发布日期	页数	章节或图表	更改说明
V1.0	2018.06.01	7		首次发布

法律声明

版权所有©大唐微电子技术有限公司 2018。保留一切权利。

未经大唐微电子技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制、翻译本芯片说明书内容的部分或全部，并不得以任何形式传播。

联系我们(Contact Us)

公司(Company): 大唐微电子技术有限公司(Datang Microelectronics)
地址(Address): 北京市海淀区永嘉北路6号
邮编(ZIP): 100094
电话(Telephone): +86(10)-58953111
传真(Fax): +86(10)-58953333
网址(Website): www.dmt.com.cn
邮箱(E-mail): market_fs@datang.com