HDSC 华大半导体 HUADA SEMICONDUCTOR

32 位微控制器

HC32L130 / HC32L136 / HC32F030 系列的 AES 模块

适用对象

系列	产品型号
HC32L130	HC32L130E8PA HC32L130F8UA HC32L130J8TA
HC32L136	HC32L136J8TA HC32L136K8TA
HC32F030	HC32F030E8PA HC32F030F8UA HC32F030F8TA HC32F030J8TA HC32F030K8TA

目　录

1 摘要

本篇应用笔记主要介绍 HC32L130 / HC32L136 / HC32F030 系列 AES 模块的使用。

本应用笔记主要包括：

- 寄存器操作
- 加密
- 解密
- 注意事项
- 异常机制
- 性能

注意：

— 本应用笔记为 HC32L130 / HC32L136 / HC32F030 系列的应用补充材料，不能代替用户手册，具体功能及寄存器的操作等相关事项请以用户手册为准。

2 功能介绍

通过本篇可以了解到 HC32L130 / HC32L136 / HC32F030 系列 MCU 的 AES 模块的应用。

- 执行 AES 算法标准的加密流程和解密流程，其执行结果完全符合《FIPS PUB 197》对算法原理的描述；
- 仅支持 128 位密钥。

3 AES 模块

3.1 寄存器操作

数据寄存器由四个 32 位的寄存器组成 128 位数据。

用于在模块运算前存放需要被加密的明文或者需要被解密的密文，并且运算完成后存放加密后的密文或者解密后的明文。

加密运算		解密运算	
运算前	运算后	运算前	运算后
128 位明文	128 位密文	128 位密文	128 位明文

四个 32 位寄存器连接在一起组成一个 128 位的数据，读写操作时需要分别对四个寄存器进行操作。数据寄存器对应的操作顺序如下：

数据举例： 0x00112233445566778899AABBCCDDEEFF

Data0	0x33221100
Data1	0x77665544
Data2	0xBBAA9988
Data3	0xFFEEDDCC

密钥寄存器由 4 个 32 位的寄存器组成，存放输入的初始密钥。

写操作时需要分别对 4 个 32 位的寄存器进行操作。对应的操作顺序如下：

数据举例： 0x000102030405060708090A0B0C0D0E0F

Key0	0x03020100
Key1	0x07060504
Key2	0x0B0A0908
Key3	0x0F0E0D0C

- 对于数据和密钥寄存器的写入只能在本模块没有处于运算状态时（即 CR.Start = 0 时）才能进行，否则硬件将自动忽略对本寄存器的写操作。
- 对于数据和密钥寄存器的读取只能在本模块没有处于运算状态时（即 CR.Start = 0 时）才能进行，否则对本寄存器的读取将得到全 0。

3.2 加密

- 将待加密的 128 位数据写入数据寄存器（DATA）中。
- 将加密密钥写入密钥寄存器（KEY）中。
- 将 CR.Mode 设置为 0。
- 向控制寄存器中的 CR.Start 写入 1，启动模块进行运算。
- 等待 CR.Start 的值恢复位 0，模块运算结束。
- CR.Mode CR.Start 可同时进行配置。
- 读取数据寄存器（DATA），获得 128 位密文。

3.3 解密

- 将待解密的 128 位数据写入数据寄存器（DATA）中。
- 将解密密钥写入密钥寄存器（KEY）中。
- 将 CR.Mode 设置为 1。
- 向控制寄存器中的 CR.Start 写入 1，启动模块进行运算。
- CR.Mode CR.Start 可同时进行配置。
- 等待 CR.Start 的值恢复位 0，模块运算结束。

3.4 注意事项

- 上电后，时钟 hclk 必须在复位脱离前稳定有效，并且在后续运行中持续稳定。
- 在 AES 加解密过程中，数据寄存器会改变，如果下次运算的被操作数据就是本次运算的结果，那么就无需重新写入数据了。
- 密钥仅支持 128 位，密钥写入偏移地址 0x20-0x2C。
- 判断模块运算结束的方法：不断读取 CR.Start，如果其值变为 0，则表示运算结束。

3.5 异常机制

- 只支持 32 位访问，其它位宽的访问返回硬件异常(HardFault)。
- 数据和密钥访问偏移大于 0x0F 的地址，返回硬件异常(HardFault)。

3.6 性能

本模块从启动一次运算（CR.Start 写入 1）到该次运算结束（CR.Start 恢复到 0）所需时间。

加密	216 cycles
解密	286 cycles

4 参考样例及驱动

通过上述介绍，配合本系列的用户手册，我们对本系列 MCU 的 AES 模块功能及操作方法有了进一步的掌握。

华大半导体（HDSC）官方同时提供了该模块的应用样例及驱动库，用户可通过打开样例的工程进一步直观地熟悉该模块以及驱动库的应用，在实际开发中也可以直接参考样例和使用驱动库来快速实现对该模块的操作。

- 样例参考：~/HC32L130_DDL/example/aes
- 驱动库参考：~/HC32L130_DDL/driver/…/aes

5 总结

以上章节简要介绍了 HC32L130 / HC32L136 / HC32F030 系列的 AES 模块，详细说明了 AES 模块的使用。用户在实际的应用开发过程中，如果需要更深一步了解该模块的使用方法及操作事项，应以相应的用户手册为准。本篇中提到的样例及驱动库，既可以作为用户进一步的实验与学习，也可以在实际开发中直接应用。

6 其他信息

技术支持信息： www.hdsc.com.cn

7 版本信息 & 联系方式

日期	版本	修改记录
2018/6/20	Rev1.0	初版发布。
2018/9/3	Rev1.1	更新支持的产品型号。

如果您在购买与使用过程中有任何意见或建议，请随时与我们联系。

Email：mcu@hdsc.com.cn

网址：www.hdsc.com.cn

通信地址：上海市张江高科园区碧波路 572 弄 39 号

邮编：201203