

32 位微控制器

HC32L130 / HC32L136 / HC32F030 系列的 RNG 应用说明

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	3
2	功能介绍	3
	RNG 生成方式	
	3.1 上电第一次生成随机数	
	3.2 非上电第一次生成随机数	4
	3.3 样例参考	4
4	随机数主要应用	5
5	总结	5
6	其他信息	5
7	版本信息 & 联系方式	6



1 摘要

本篇应用笔记主要介绍 HC32L130 / HC32L136 / HC32F030 系列的随机数发生器 RNG (Random Number Generator)的操作流程及应用。

本应用笔记主要包括:

- RNG 简介
- RNG生成方式
- RNG应用说明

注意:

一本应用笔记为 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

本系列 MCU 的 RNG 可以生成 64 位随机数,可使用内部模拟随机源。对于内部随机数的生成方式可进行软件配置,生成的 64 位随机数分别存储在 DATA0 和 DATA1 寄存器中。

应用笔记 Page 3 of 6



3 RNG生成方式

如果需要自己配置随机数的生成方式,可参考该系列 MCU 用户手册中的软件操作流程进行。本例主要讲解如何使用驱动库进行随机数的生成。

3.1 上电第一次生成随机数

- 1. 打开随机数外设时钟使能;
- 2. 使用随机数初始化函数进行第一次随机数的生成;
- 3. 获取 64 位随机数。

3.2 非上电第一次生成随机数

- 1. 打开随机数外设时钟使能;
- 2. 使用随机数初始化函数进行第一次随机数的生成;
- 3. 使用随机数生成函数进行非上电第一次随机数生成;
- 4. 获取 64 位随机数。

3.3 样例参考

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/rng
- ➤ 驱动库参考: ~/HC32L130 DDL/driver/.../rng

应用笔记 Page 4 of 6



4 随机数主要应用

随机数在密码学中非常重要,保密通信中大量运用的会话密钥的生成即需要真随机数的参与。如果一个随机数生成算法是有缺陷的,那么会话密钥可以直接被推算出来。若果真发生这种事故,那么任何加密算法都失去了意义。

在该系列 MCU 中,生成的随机数可配合 AES 模块用于密钥生成或使用到安全相关的软件算法中,来增加安全性。

5 总结

以上章节简要介绍了 HC32L130 / HC32L136 / HC32F030 系列 RNG 的操作流程及样例参考, 用户在实际应用开发中可根据实际情况参考本例进行 RNG 的生成和使用。

6 其他信息

技术支持信息: www.hdsc.com.cn

应用笔记 Page 5 of 6



7 版本信息 & 联系方式

日期	版本	修改记录
2018/6/19	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



应用笔记 AN0060004C