

32 位微控制器

RNG 应用说明

应用笔记

Rev1.0 2023 年 04 月

适用对象

产品系列	产品型号
HC32A136	HC32A136K8TB

声 明

- ★ 小华半导体有限公司（以下简称：“XHSC”）保留随时更改、更正、增强、修改小华半导体产品和/或本文档的权利，恕不另行通知。用户可在下单前获取最新相关信息。XHSC 产品依据购销基本合同中载明的销售条款和条件进行销售。
- ★ 客户应针对您的应用选择合适的 XHSC 产品，并设计、验证和测试您的应用，以确保您的应用满足相应标准以及任何安全、安保或其它要求。客户应对此独自承担全部责任。
- ★ XHSC 在此确认未以明示或暗示方式授予任何知识产权许可。
- ★ XHSC 产品的转售，若其条款与此处规定不同，XHSC 对此类产品的任何保修承诺无效。
- ★ 任何带有“®”或“™”标识的图形或字样是 XHSC 的商标。所有其他在 XHSC 产品上显示的产品或服务名称均为其各自所有者的财产。
- ★ 本通知中的信息取代并替换先前版本中的信息。

©2023 小华半导体有限公司 保留所有权利

目 录

适用对象	2
声 明	3
目 录	4
1 摘要	5
2 功能介绍	6
3 RNG 生成方式	7
3.1 上电第一次生成随机数	7
3.2 非上电第一次生成随机数	7
3.3 样例参考	7
4 随机数主要应用	8
5 总结	9
6 其他信息	10
版本修订记录	11

1 摘要

本篇应用笔记主要介绍小华半导体 MCU*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：

- 本应用笔记为小华半导体 MCU*的应用补充材料，不能代替参考手册，具体功能及寄存器的操作等相关事项请以参考手册为准。

注：*支持型号见“适用对象”章节。

2 功能介绍

小华半导体 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。

注：*支持型号见“适用对象”章节。

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 参考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

小华半导体（XHSC）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。

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。

在小华半导体 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。

注：*支持型号见“适用对象”章节。

5 总结

以上章节简要介绍了小华半导体 MCU*的 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。

注：*支持型号见“适用对象”章节。

6 其他信息

技术支持信息: <http://www.xhsc.com.cn>

版本修订记录

版本号	修订日期	修订内容
Rev1.0	2023/04/13	初版发布。

若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。

邮箱：support@xhsc.com.cn

电话：021-68667000-7355

地址：上海市浦东新区中科路 1867 号 A 座 10 层

