

硬件随机数实验

1 RNG简介

RNG，随机数发生器，用于生成随机数的程序或者硬件

随机数相关介绍

特性：产生的后面的那个数与前面那个数毫无关系

真随机数

完全随机，毫无规律（STM32的部分型号上具备真随机数发生器）

伪随机数

伪随机数是用确定性的算法计算出的随机数序列。并非真正的随机

应用场景

验证码、密码学、概率学、统计学、游戏

2 RNG框图介绍

模拟电路

LFSR

时钟检查器和故障检测器

3个RNG寄存器

3 RNG相关寄存器介绍

RNG控制寄存器RNG_CR

用于使能随机数发生器和中断

RNG状态寄存器RNG_SR

用于显示RNG当前的一些状态

RNG数据寄存器RNG_DR

用于存储32位随机数值

4 RNG相关HAL库驱动介绍

HAL_RNG_Init

HAL_RNG_MspInit

__HAL_RCC_RNG_CLK_ENABLE

HAL_RCCEx_PeriphCLKConfig

HAL_RNG_GenerateRandomNumber

判断DRDY位并读取随机数

__HAL_RNG_GET_FLAG

获取RNG相关标记

5 RNG基本驱动步骤

1. 使能RNG时钟

__HAL_RCC_RNG_CLK_ENABLE

2. 初始化（使能）随机数发生器

HAL_RNG_Init

HAL_RNG_MspInit

HAL_RCCEx_PeriphCLKConfig

3. 判断DRDY位，读取随机数值

HAL_RNG_GenerateRandomNumber

6 编程实战

驱动RNG，使用串口打印随机数