

## 八位 Pseudo-Random Number Generator

文件编码: HA0085s

### 前言

Pseudo-Random number generator 在扩频通信、安全系统、编码及信号的调制解调等领域中均有广泛的应用。

构成 Pseudo-Random number generator 的最为普遍的硬件实现方式是利用线反馈式移位寄存器(LFSR)来实现。

事实上, Pseudo-Random number generator 随机数的产生并非真正随机无规律的, 若在运行过程中不中断对其装载新的初始数据, 那么, 在运行一定时间后, 数据的产生规律还是将会出现重复。利用这种方式来实现 Pseudo-Random number generator 主要是充分利用了移位寄存器的数据变换的长度来达到随机数的出现模式在相当长的执行时间后才出现重复的目的, 从而一定程度上达到产生随机随机数的目的。

本设计的目的就是在以上实现原理的基础上, 将线反馈式移位寄存器(LFSR)实现 Pseudo-Random number generator 的硬件转换逻辑与 HOLTEK 的软件指令运用相结合, 提供实现 8-bit Pseudo-Random number generator 的软件 SWIP。

本设计中 8-bit 随机数的产生步骤如下：

- (1)任取一个非 0 数作为随机数的初始值。
- (2)确定下一个随机数的 D0 位：  
如果初始值的 D1、D2、D3、D7 位中出现 1 的次数为奇数，则下一个随机数的 D0 位为 1；否则，（即初始值的 D1、D2、D3、D7 中出现 1 的次数为偶数），则下一个随机数的 D0 位为 0。
- (3)确定下一个随机数的 D1, D2, D3, D4, D5, D6, D7：  
将初始值的 D0, D1, D2, D3, D4, D5, D6 依次作为下一个随机数的 D1, D2, D3, D4, D5, D6, D7。
- (4)以(2)(3)产生的随机数为初始值，重复(2)(3)，再产生下一个随机数，如此循环，以至无穷。

按照上述方式产生的随机数具以下特征（用十进制表述）：

- (1)每次产生的随机数都不超出上述范围，即大于等于 1 且小于等于 255 的整数。
- (2)循环周期为 255，即：  
在任意截取的连续的 255 个随机数中，1 至 255（包含 1 和 255 本身）之间的每一个整数都出现、且只出现一次；  
任意截取的连续的 255 个随机数，与其左侧相邻的 255 个随机数及右侧相邻的 255 个随机数整体相同。
- (3)整个随机数序列越长，1 至 255（包含 1 和 255 本身）之间的每一个整数出现的机率将无限逼近同一个值： $1/255$ 。

## 所有功能说明

本软件 SWIP 设计是以 HT48R05A-1 的 MCU 为母体来进行的。

就该软件 SWIP 而言，设计中并未涉及具体的硬件电路，故该软件 SWIP 适用于 HOLTEK 任何系列的 MCU 母体。

本设计最终提供的 SWIP 中包括了以下 1 条宏指令：

```
pseudo_random_number_generator_8bit
```

### 应用格式

```
pseudo_random_number_generator_8bit
```

### 功能

产生一次随机数。

## 说明

执行该宏指令时，将以本软件 SWIP 中 public 的存储单元 r\_seed 中的数值为基准进行随机数的产生运作，并最终将产生的随机数保存于存储单元 r\_seed 中。故在执行该宏指令前若要设置存储单元 r\_seed 中的数值时，应注意该数值必须为非 0 值，否则该宏指令运行产生的结果将总是保持为 0，不符合随机数的产生要求。故对于 8-bit 存储单元 r\_seed 而言，其中存储的数值范围为 1~255（十进制）。

要在应用程序中使用该 SWIP，需进行以下操作：

- 将该 SWIP 中提供的“8-bit pseudo-random number generator\_macro.asm”文件 include 到应用主程序中。
- 将该 SWIP 中提供的“8-bit pseudo-random number generator\_IP.asm”文件加入到应用程序所在的 project 中一起编译。

进行了以上 2 步骤之后，就能在应用程序中使用该 SWIP 中所提供的宏指令。

以下为所有功能的详细列表。

IP Name (Label)	System Resources	Function Descriptions
8-bit pseudo-random number generator	Functions	8-bit pseudo-random number generator
	MCU	HT48R05A-1
	ROM	13 words in all
	RAM	3 bytes: "r_seed" (public), "left_shift_count", "tap_one_count"
	Stack	1 level used in all (call)
	I/O	None
	f <sub>sys</sub>	400kHz~8MHz
	Other MCU Resources	WDT
	User Interface	1. Include "8-bit pseudo-random number generator_macro.asm" 2. Edit 8-bit pseudo-random number generator IP.asm into project

以下为在主程序（main.asm）中使用该 SWIP 所提供宏指令的应用程序范例。

```

;;-----
;; BODY: HT48R05A-1
;;.....
include ht48r05a-1.inc
.LISTMACRO
.LISTINCLUDE
include "8-bit pseudo-random number generator_macro.asm"
;;.....
;; MASK OPTION
;;.....
main .SECTION 'DATA'
;;-----
MAIN .SECTION AT 0 'CODE'
JMP START
;;-----
start:

mov a,1                                ;预设初始值
mov r_seed,a                            ;

random_loop:
pseudo_random_number_generator_8bit ;呼叫 IP
jmp random_loop
;;-----

```

## 软件流程图

8-bit pseudo-random number generator\_ip.asm

### random\_8bit\_function

该子程序被宏指令 pseudo\_random\_number\_generator\_8bit 所调用。  
其流程如下：

