



YC31xx TRNG 应用说明

V1.0

Yichip Microelectronics

©2014

Revision History

Version	Date	Author	Description
V1.0	2020-2-19	Fanglingxue	Initial version

Confidentiality Level:

confidential

目录

1	文档说明	4
1.1	编写目的	4
1.2	适用范围	4
1.3	文件说明	4
2	函数说明	5
2.1	TRNG_Init.....	5
2.2	TRNG_Get.....	5
2.3	GetTRNGData_8bit.....	5
2.4	GetTRNGData	6
2.5	Disable_Trng	6
3	示例代码:	6
4	备注	7
4.1	TRand	7
4.2	RAND_Rand.....	7
4.3	RAND_RandCheck	8
4.4	RAND_Init	8

1 文档说明

1.1 编写目的

为使用 TRNG 相关 demo 及 demo 中相关 API 提供指南

1.2 适用范围

3121 系列芯片

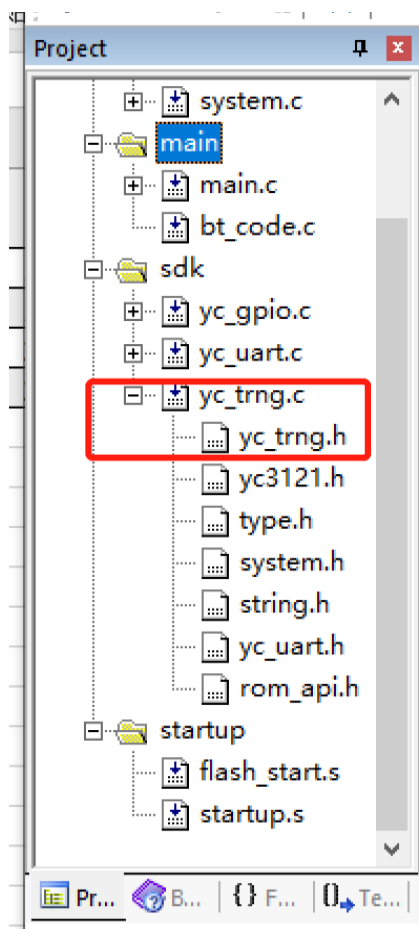
1.3 文件说明

TRNG Demo 路径

TRNG 库文件为如下图

ModuleDemo\RNG

Librarier\sdk



2 函数说明

2.1 TRNG_Init

函数原型: void TRNG_Init(void)

函数说明: trng 初始化

参数	方向	说明
None	None	None

返回值	说明
None	None

2.2 TRNG_Get

函数原型: void TRNG_Get(volatile unsigned long *rand)

函数说明: 得到 trng 真随机数

参数	方向	说明
rand	OUT	得到的随机数存放单元

返回值	说明
None	None

2.3 GetTRNGData_8bit

函数原型: uint8_t GetTRNGData_8bit(void)

函数说明: 获取 8bit trng 数据

参数	方向	说明
None	None	None

返回值	说明
uint8_t num	trng 数据

2.4 GetTRNGData

函数原型：int GetTRNGData(void)

函数说明：获得 trng 数据，供 GetTRNGData_8bit 函数调用

参数	方向	说明
None	None	None

返回值	说明
int num	trng 数据

2.5 Disable_Trng

函数原型：void Disable_Trng(void)

函数说明：失能 trng 模块

参数	方向	说明
None	None	None

返回值	说明
None	None

3 示例代码：

```
int main(void)
{
    unsigned long Buf[4];

    UART_Configuration();

    MyPrintf("YcChip 3121 RNG polling Demo V1.0.\n");

    TRNG_Init();
```

```

while(1)
{
    TRNG_Get(Buf);
    MyPrintf("Rng : %08X %08X %08X %08X \r\n",Buf[0],Buf[1],Buf[2],Buf[3]);
}
}

```

4 备注

Rand 是调用 Trng 模块使用的

4.1 TRand

函数原型：static uint32_t TRand(void *buf, uint32_t bytes)

函数说明：得到随机数，调用 trng.c 中 GetTRNFDat 函数

参数	方向	说明
buf	OUT	得到的随机数存放单元
bytes	IN	得到的随机数长度

返回值	说明
uint32_t	0: FAIL Other: len (SUCCESS)

4.2 RAND_Rand

函数原型：uint32_t RAND_Rand(void *rand, uint32_t bytes)

函数说明：得到随机数调用 TRand 函数

参数	方向	说明
rand	OUT	得到的随机数存放单元
bytes	IN	得到的随机数长度

返回值	说明
uint32_t	0: FAIL Other: len (SUCCESS)

4.3 RAND_RandCheck

函数原型：uint32_t RAND_RandCheck(void *rand, uint32_t bytes)

函数说明：检查数据是否符合要求

参数	方向	说明
rand	IN	得检查的数据存放单元
bytes	IN	数据长度 16 < bytes < 784

返回值	说明
uint32_t	0: SUCCESS 1: FAIL

4.4 RAND_Init

函数原型：uint32_t RAND_Init(void)

函数说明：rand 初始化，调用 trng 初始化函数

参数	方向	说明
None	None	None

返回值	说明
uint32_t num	成功时返回 0