TRNG Module

IP 概述

主要特点如下：

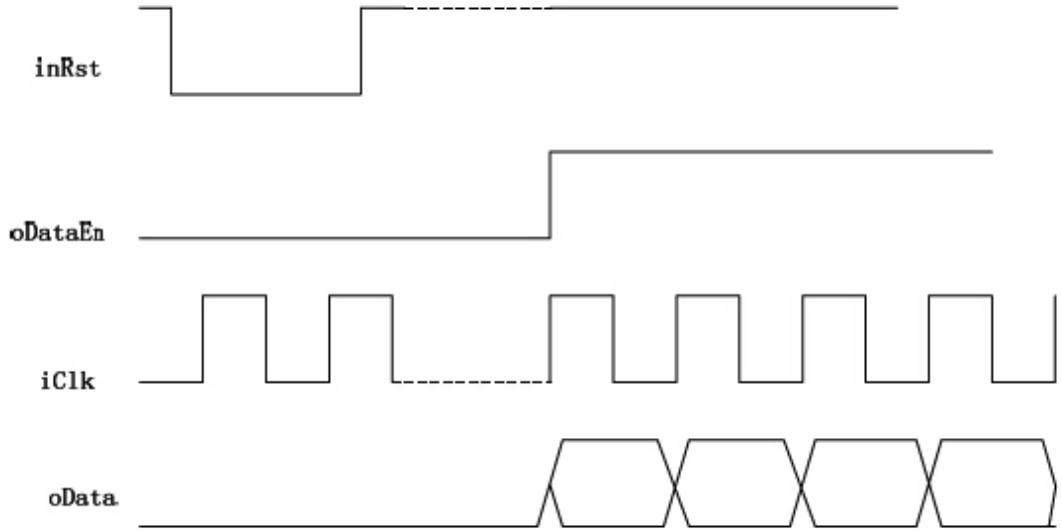
- 采用 SMIC 0.18um logic 1P6M 工艺，基于国家标准 RNG4 算法技术设计，并通过国家密码管理局商用密码检测中心的检测。
- 单一供电电源：1.8V
- 典型版图面积约：465um x 413um
- 典型速率 20Mbps,可扩展更高速率输出。

接口定义

真随机数生成算法 IP 核输入输出端口如图所示

端口名称	定义及说明
iClk	输入，时钟信号，不高于 20MHz
inRst	输入，复位信号，低电平复位
oDataEn	输出，随机数输出使能指示
oData	输出，随机数输出信号
VDD	电源，1.8V
VSS	地

接口时序



IP 核接口时序图

1) oDataEn 上电复位等待时间，在 20Mhz 时，典型情况下等待约 300ms 后变成高电平。

2) 随机数的输出 oData 在输入时钟信号的上升沿发生变化。

在可测试性设计时:(1)可使用 CPU 采样等类似的方法输出测试;(2)如果直接输出随机数进行测试，需要将该 IP 的所有信号都在芯片的引脚上引出。

电气特性

参数	符号	Min	Typ	Max	单位	备注
工作电压	VDD	1.6	1.8	2	V	
地	VSS	--	0	--	V	
版图面积	--	--	--	--	mm2	约为0.2
功耗	--	--	--	10	mW	25℃，1.8V

温度范围	--	－40	25	110	℃	
输出摆率	--			0.1＋4*CL	ns	CL单位pF

附：基于 NIST 随机数测试标准的测试报告

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
8	5	10	10	12	12	12	11	6	14	0.595549	0.9900	frequency
7	12	10	11	12	10	11	5	13	9	0.798139	0.9900	block-frequency
10	5	8	8	13	8	11	18	10	9	0.262249	0.9900	cumulative-sums
10	8	7	15	13	12	8	12	10	5	0.494392	0.9900	cumulative-sums
7	11	14	9	10	12	9	12	7	9	0.867692	0.9900	runs
4	6	13	16	11	9	11	3	14	13	0.042808	1.0000	longest-run
11	14	12	10	7	10	6	10	9	11	0.851383	0.9900	rank
13	13	10	14	8	10	8	9	8	7	0.779188	0.9800	fft
14	9	10	8	10	13	8	7	8	13	0.779188	0.9800	overlapping-templat
8	10	10	9	11	12	11	12	9	8	0.991468	0.9800	universal
9	15	7	9	8	10	7	11	12	12	0.759756	0.9900	apen