FDK

物理乱数生成器

ＲＰＧ１００／ＲＰＧ１００Ｆ
データシート

REV.08

目　　次

１．概　　要

ＲＰＧ１００／ＲＰＧ１００Ｆは外付け部品無しに、高速で物理的にランダムビット及び乱数を出力するＩＣです。ランダムビットは、ランダムビット生成クロックに同期し連続で出力されます。また、乱数は高速のシフトクロックにより読み出すことが可能です。内部には乱数生成器の検定回路が内蔵されており、乱数の検定を容易に行なえます。

２．機　　能

項　　目	説　　明
ﾗﾝﾀﾞﾑﾋﾞｯﾄ出力	ﾗﾝﾀﾞﾑﾋﾞｯﾄ生成ｸﾛｯｸに同期したｼﾘｱﾙの連続ﾗﾝﾀﾞﾑﾋﾞｯﾄを、ｼﾘｱﾙ出力端子から出力します。
乱数出力	ｼﾘｱﾙの連続ﾗﾝﾀﾞﾑﾋﾞｯﾄが 16bit の乱数に変換され、内部に保持されます。保持された乱数はｼﾌﾄｸﾛｯｸにより読み出すことが可能であり、ﾃﾞｰﾀﾊﾞｽから出力されます。
乱数の検定 及び 検定ﾃﾞｰﾀ出力	FIPS 140-2(Change Notice1)Statistical random number generator tests における乱数の検定ができます。また、検定ﾃﾞｰﾀと判定を読み出すことも可能です。検定をｽﾀｰﾄすると内部に保持された全ての乱数はｸﾘｱされ、検定を行なった新しい乱数が保持されます。検定結果を参照して、これらの乱数を使用することができます。

３．仕　　様

3-1.絶対最大定格

(VSS=RVSS=0V)

項　　目	記号	定　　格	単位
電源電圧	VCC	VSS-0.5 ～ +4.0	V
	RVCC	RVSS-0.5 ～ +4.0	V
入力電圧	Vi	VSS-0.5 ～ VCC+0.5	V
出力電圧	Vo	VSS-0.5 ～ VCC+0.5	V
出力電流	Io	±14	mA
許容損失	Pd	300	mW
保存温度	Tstg	-55 ～ 125	℃

3-2.推奨動作条件

(VSS=RVSS=0V)

項　　目	記号	MIN	TYP	MAX	単位
電源電圧	VCC	3.0	3.3	3.6	V
	RVCC	3.0	3.3	3.6	V
Ｈﾚﾍﾞﾙ入力電圧	VIH	VCC×0.8	-	VCC	V
Ｌﾚﾍﾞﾙ入力電圧	VIL	VSS	-	VCC×0.2	V
CLK_R 周波数	f_R	245	250	255	KHz
CLK_R ﾃﾞｭｰﾃｨｰ	-	-	50	-	%
ｸﾛｯｸ入力禁止時間	t_{RT}	50	-	-	nS
Ｈﾚﾍﾞﾙﾎｰﾙﾄﾞ時間	t_{TH}	50	-	-	nS
Ｌﾚﾍﾞﾙﾎｰﾙﾄﾞ時間	t_{TL}	50	-	-	nS
ｽﾀｰﾄﾊﾟﾙｽ幅	t_{WT}	50	-	-	nS
動作温度	Ta	-40	-	85	℃

3-3.直流特性

(VCC=RVCC=3.3±0.3V,VSS=RVSS=0V,Ta=25°C)

項　　目	記号	条　件	MIN	TYP	MAX	単位
電源電流	ICC	CLK_R=250KHz	-	2.3	-	mA
		PSV=H	-	0.13	-	mA
		PSV=H CLK_R=停止	-	1	5	uA
Hﾚﾍﾞﾙ出力電圧	VOH	IOH=-4mA	VCC-0.5	-	VCC	V
Lﾚﾍﾞﾙ出力電圧	VOL	IOL=4mA	VSS	-	0.4	V

3-4.交流特性

(VCC=RVCC=3.3±0.3V,VSS=RVSS=0V,Ta=25°C)

項　　目	記号	条　件	MIN	TYP	MAX	単位
ﾃﾞｰﾀ出力遅延時間 1	t_{TS}	負荷 50pF	-	-	20	nS
ﾃﾞｰﾀ出力遅延時間 2	t_{TD}	負荷 50pF	-	-	50	nS
ﾃﾞｰﾀ出力遅延時間 3	t_{TA}	負荷 50pF	-	-	25	nS
出力ｲﾈｰﾌﾞﾙ時間	t_{ZD}	負荷 50pF	-	-	18	nS
出力ﾃﾞｨｽｴｰﾌﾞﾙ時間 (ﾄﾞﾗｲﾌﾞ OFF 時間)	t_{DZ}		-	-	6	nS
ｱﾄﾞﾚｽｾｯﾄｱｯﾌﾟ時間	t_{SA}		20	-	-	nS
ｱﾄﾞﾚｽﾎｰﾙﾄﾞ時間	t_{HA}		50	-	-	nS
ﾁｯﾌﾟｾﾚｸﾄｾｯﾄｱｯﾌﾟ時間	t_{SC}		20	-	-	nS
ﾁｯﾌﾟｾﾚｸﾄﾎｰﾙﾄﾞ時間	t_{HC}		50	-	-	nS

3-5.ﾗﾝﾀﾞﾑﾋﾞｯﾄ＆乱数仕様

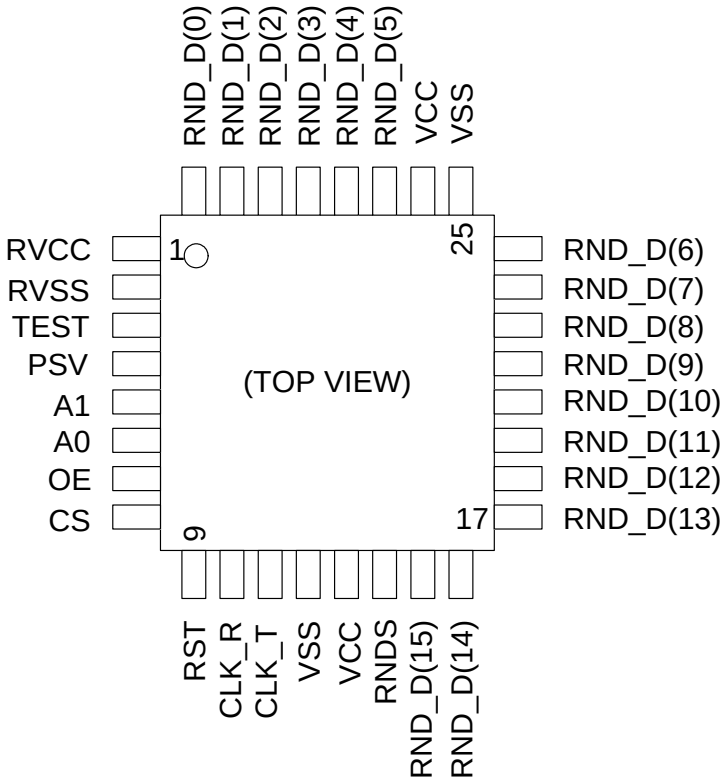
項　　目	仕　　様
ランダム源	半導体内部の雑音
最大乱数保持数	最大 16bit×32
ﾗﾝﾀﾞﾑﾋﾞｯﾄ品位	FIPS 140-2(Change Notice1)Statistical random number generator tests 相当

3-6.パッケージ仕様

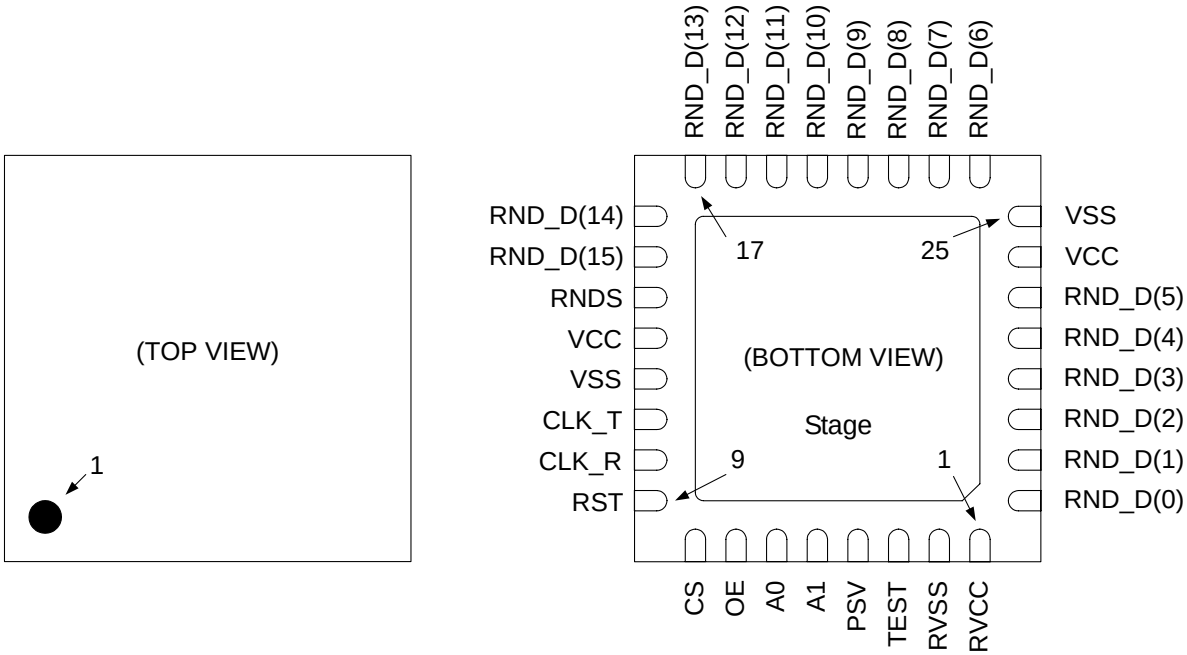
項　　目	RPG100	RPG100F
ﾊﾟｯｹｰｼﾞ形状	ﾌﾟﾗｽﾁｯｸ LQFP	ﾌﾟﾗｽﾁｯｸ QFN
ﾊﾟｯｹｰｼﾞ寸法(ﾘｰﾄﾞ含む)	9mm×9mm	5mm×5mm
ﾋﾟﾝ数	32ﾋﾟﾝ	32ﾋﾟﾝ
ﾘｰﾄﾞﾋﾟｯﾁ	0.8mm	0.5mm

3-7.ピン配置

＜ＲＰＧ１００ ＬＱＦＰパッケージ＞



＜ＲＰＧ１００Ｆ ＱＦＮパッケージ＞



※Stage 部は電気的に接続されておりませんので、GND への接続は不要です。
尚、直下に信号パターンを配置しないようお願いします。

４．端子機能説明

端子記号	端子名	I/O	機能説明
OE	ｱｳﾄﾌﾟｯﾄｲﾈｰﾌﾞﾙ	I	ﾃﾞｰﾀﾊﾞｽ出力制御信号
CS	ﾁｯﾌﾟｾﾚｸﾄ	I	ﾁｯﾌﾟ動作制御信号
CLK_R	ﾗﾝﾀﾞﾑﾋﾞｯﾄ生成ｸﾛｯｸ	I	ｸﾛｯｸの立ち上がりでﾗﾝﾀﾞﾑﾋﾞｯﾄ生成
CLK_T	ｼﾌﾄｸﾛｯｸ	I	乱数出力時のｼﾌﾄｸﾛｯｸ、検定ﾃﾞｰﾀ読出し時のﾃﾞｰﾀ選択ｸﾛｯｸ及び検定ｽﾀｰﾄ時のｽﾀｰﾄﾊﾟﾙｽ
A1,A0	ｱﾄﾞﾚｽ	I	ﾃﾞｰﾀﾊﾞｽへの出力ﾃﾞｰﾀ選択及び検定ｽﾀｰﾄｲﾈｰﾌﾞﾙｱﾄﾞﾚｽ
PSV	ﾊﾟﾜｰｾｰﾌﾞ	I	‘Ｈ’の時ﾊﾟﾜｰｾｰﾌﾞ（8-2 項参照）
RNDS	ｼﾘｱﾙﾃﾞｰﾀ出力	O	ﾗﾝﾀﾞﾑﾋﾞｯﾄ生成ｸﾛｯｸに同期したﾗﾝﾀﾞﾑﾋﾞｯﾄが出力され、乱数生成動作状態ﾌﾗｸﾞが‘Ｌ’の時使用可ﾊﾟﾜｰｾｰﾌﾞ時出力は‘Ｌ’
RND_D(15～00)	ﾃﾞｰﾀﾊﾞｽ	O	乱数及び各種ﾃﾞｰﾀが出力され、保持された乱数は乱数生成動作状態ﾌﾗｸﾞが‘Ｌ’の時使用可
TEST	ﾃｽﾄ	I	VSS と同電位へ接続
RST	ﾘｾｯﾄ	I	‘Ｌ’の時ﾘｾｯﾄ、電源投入時に‘Ｌ’を入力して下さい
VCC	電源		
RVCC	ｱﾅﾛｸﾞ電源		VCC と同電位へ接続
VSS	GND		
RVSS	ｱﾅﾛｸﾞ GND		VSS と同電位へ接続

（真理値表）　×:H or L

CS	OE	ﾁｯﾌﾟ動作	ﾃﾞｰﾀﾊﾞｽ	ｼﾘｱﾙﾃﾞｰﾀ出力
H	×	不　可	ﾊｲｲﾝﾋﾟｰﾀﾞﾝｽ	出　力
L	L	可	ﾃﾞｰﾀ出力	出　力
L	H	可	ﾊｲｲﾝﾋﾟｰﾀﾞﾝｽ	出　力

A1	A0	ﾃﾞｰﾀﾊﾞｽ出力ﾃﾞｰﾀ	ｼﾌﾄｸﾛｯｸ	ｼﾘｱﾙﾃﾞｰﾀ出力
0	0	乱　数	乱数ｼﾌﾄｸﾛｯｸ	出　力
0	1	動作状態ﾃﾞｰﾀ	乱数ｼﾌﾄｸﾛｯｸ	出　力
1	0	検定状態ﾃﾞｰﾀ	検定ｽﾀｰﾄﾊﾟﾙｽ	出　力
1	1	検定ﾃﾞｰﾀ	検定ﾃﾞｰﾀ選択ｸﾛｯｸ	出　力

５．出力データ説明

5-1.乱　数

出力ﾋﾞｯﾄ	出力データ説明
b15～b00	16bit 乱数であり乱数保持数まで連続で読出し可

5-2.動作状態ﾃﾞｰﾀ

出力ﾋﾞｯﾄ	出力データ説明
b05～b00	乱数保持数
b06	乱数保持の有無（H:保持有り、L:保持無し）
b07	初期設定ﾌﾗｸﾞ（H:初期設定終了、L:初期設定中） ﾘｾｯﾄ解除後 512 ｸﾛｯｸ(CLK_R)間‘Ｌ’となりﾗﾝﾀﾞﾑﾋﾞｯﾄ出力は無効
b08	検定状態（H:検定中、L:検定終了）
b09	乱数生成動作状態ﾌﾗｸﾞ（H:異常動作、L:正常動作） ﾗﾝﾀﾞﾑﾋﾞｯﾄ生成回路が正常動作時‘Ｌ’　但し、初期設定中は‘Ｈ’
b15～b10	‘Ｌ’固定

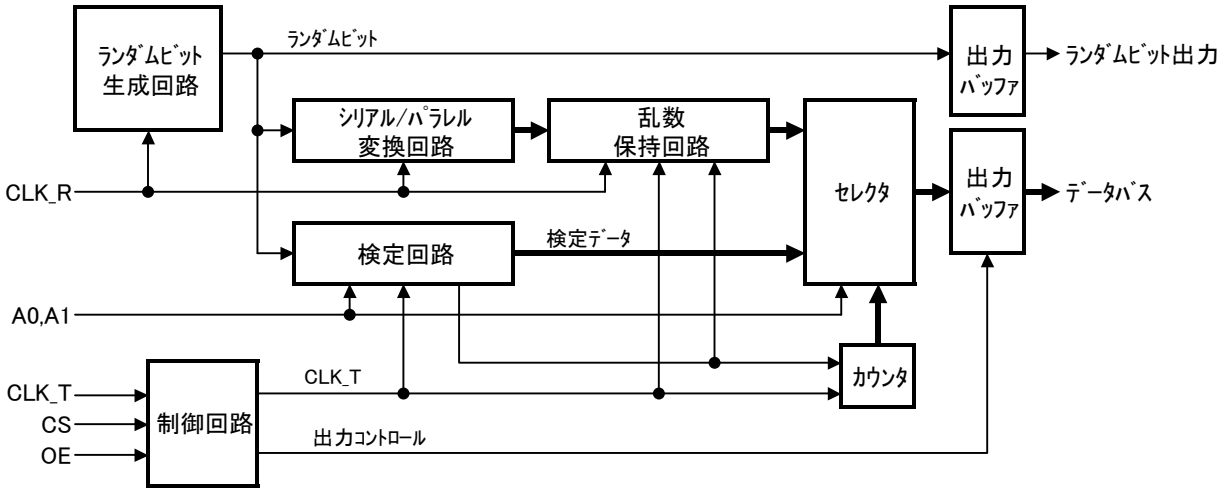
5-3.検定状態ﾃﾞｰﾀ　＊ﾀｲﾐﾝｸﾞﾁｬｰﾄ 7-3,7-4 参照

出力ﾋﾞｯﾄ	出力データ説明
B05～b00	検定ﾃﾞｰﾀ選択ｱﾄﾞﾚｽ
b06	検定用ﾗﾝﾀﾞﾑﾋﾞｯﾄ範囲
b07	検定状態 （H:検定中、L:検定終了）
b08	検定結果 （H:検定不合格、L:検定合格） ＊検定ﾃﾞｰﾀ 00(b15)と同じ
B12～b09	ﾃｽﾄ用ﾃﾞｰﾀ
B15～b13	ﾃｽﾄ用ﾃﾞｰﾀ

5-4.検定ﾃﾞｰﾀ　＊ﾀｲﾐﾝｸﾞﾁｬｰﾄ 7-3,7-4 参照

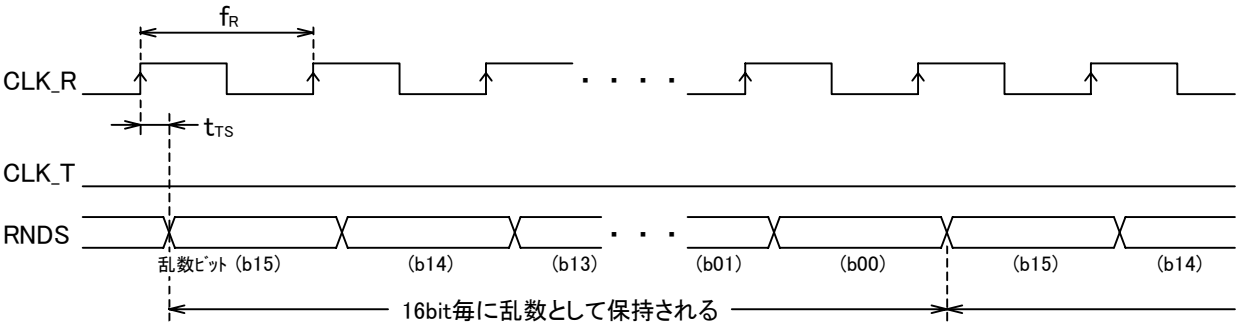
検定ﾃﾞｰﾀ選択ｱﾄﾞﾚｽ (検定ﾃﾞｰﾀ)	出力ﾋﾞｯﾄ	出力データ説明			
00 (ﾃﾞｰﾀ 00)	b15～b00	検定結果 (H:不合格) (L:合　格)	b00:ﾃﾞｰﾀ 02 判定	b08:ﾃﾞｰﾀ 10 判定	
			b01:ﾃﾞｰﾀ 03 判定	b09:ﾃﾞｰﾀ 11 判定	
			b02:ﾃﾞｰﾀ 04 判定	b10:ﾃﾞｰﾀ 12 判定	
			b03:ﾃﾞｰﾀ 05 判定	b11:ﾃﾞｰﾀ 13 判定	
			b04:ﾃﾞｰﾀ 06 判定	b12:ﾃﾞｰﾀ 14 判定	
			b05:ﾃﾞｰﾀ 07 判定	b13:ﾃﾞｰﾀ 15 判定	
			b06:ﾃﾞｰﾀ 08 判定	b14:ﾃﾞｰﾀ 16,17 判定	
			b07:ﾃﾞｰﾀ 09 判定	b15:総合判定	
01 (ﾃﾞｰﾀ 01)	b15～b00	検定総ﾗﾝﾀﾞﾑﾋﾞｯﾄ数			
02 (ﾃﾞｰﾀ 02)	b15～b00	FIPS 140-2(Change Notice1) Statistical random number generator tests	The monobit test ﾃﾞｰﾀ (‘H’ﾋﾞｯﾄ数)		
03 (ﾃﾞｰﾀ 03)	b15～b00		The long runs test ﾃﾞｰﾀ (最長連続ﾋﾞｯﾄ数)		
04 (ﾃﾞｰﾀ 04)	b15～b00		The runs test ﾃﾞｰﾀ	‘L’連続ﾋﾞｯﾄ長‘1’度数	
05 (ﾃﾞｰﾀ 05)	b15～b00			‘H’連続ﾋﾞｯﾄ長‘1’度数	
06 (ﾃﾞｰﾀ 06)	b15～b00			‘L’連続ﾋﾞｯﾄ長‘2’度数	
07 (ﾃﾞｰﾀ 07)	b15～b00			‘H’連続ﾋﾞｯﾄ長‘2’度数	
08 (ﾃﾞｰﾀ 08)	b15～b00			‘L’連続ﾋﾞｯﾄ長‘3’度数	
09 (ﾃﾞｰﾀ 09)	b15～b00			‘H’連続ﾋﾞｯﾄ長‘3’度数	
10 (ﾃﾞｰﾀ 10)	b15～b00			‘L’連続ﾋﾞｯﾄ長‘4’度数	
11 (ﾃﾞｰﾀ 11)	b15～b00			‘H’連続ﾋﾞｯﾄ長‘4’度数	
12 (ﾃﾞｰﾀ 12)	b15～b00			‘L’連続ﾋﾞｯﾄ長‘5’度数	
13 (ﾃﾞｰﾀ 13)	b15～b00			‘H’連続ﾋﾞｯﾄ長‘5’度数	
14 (ﾃﾞｰﾀ 14)	b15～b00			‘L’連続ﾋﾞｯﾄ長‘6’以上度数	
15 (ﾃﾞｰﾀ 15)	b15～b00			‘H’連続ﾋﾞｯﾄ長‘6’以上度数	
16 (ﾃﾞｰﾀ 16)	b15～b00		The poker test ﾃﾞｰﾀ	計算値 （Σ[f(i)]²）	下位ﾃﾞｰﾀ
17 (ﾃﾞｰﾀ 17)	b15～b00			* f(i)はﾃﾞｰﾀ 18～33	上位ﾃﾞｰﾀ
18 (ﾃﾞｰﾀ 18)	b15～b00			4bit 値“00”度数	
19 (ﾃﾞｰﾀ 19)	b15～b00			4bit 値“01”度数	
20 (ﾃﾞｰﾀ 20)	b15～b00			4bit 値“02”度数	
21 (ﾃﾞｰﾀ 21)	b15～b00			4bit 値“03”度数	
22 (ﾃﾞｰﾀ 22)	b15～b00			4bit 値“04”度数	
23 (ﾃﾞｰﾀ 23)	b15～b00			4bit 値“05”度数	
24 (ﾃﾞｰﾀ 24)	b15～b00			4bit 値“06”度数	
25 (ﾃﾞｰﾀ 25)	b15～b00			4bit 値“07”度数	
26 (ﾃﾞｰﾀ 26)	b15～b00			4bit 値“08”度数	
27 (ﾃﾞｰﾀ 27)	b15～b00			4bit 値“09”度数	
28 (ﾃﾞｰﾀ 28)	b15～b00			4bit 値“10”度数	
29 (ﾃﾞｰﾀ 29)	b15～b00			4bit 値“11”度数	
30 (ﾃﾞｰﾀ 30)	b15～b00			4bit 値“12”度数	
31 (ﾃﾞｰﾀ 31)	b15～b00			4bit 値“13”度数	
32 (ﾃﾞｰﾀ 32)	b15～b00			4bit 値“14”度数	
33 (ﾃﾞｰﾀ 33)	b15～b00			4bit 値“15”度数	

6．ブロック図

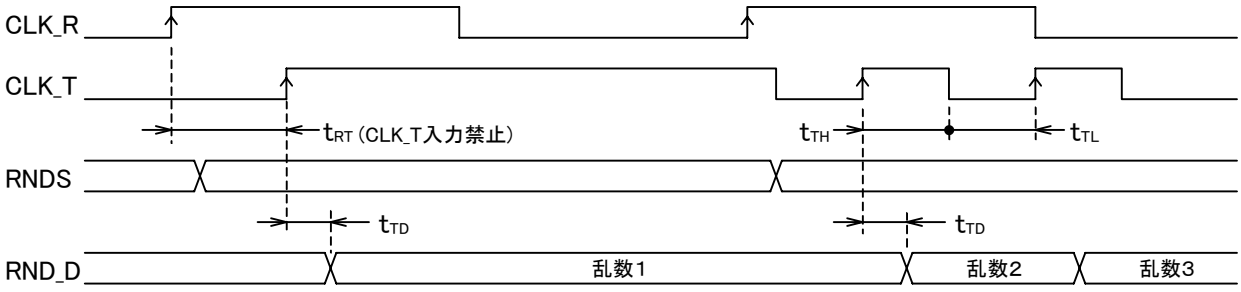


7．タイミングチャート

7-1. ﾗﾝﾀﾞﾑﾋﾞｯﾄ出力 (RST=H,PSV=TEST=L)



7-2. 乱数出力 (RST=H,TEST=OE=CS=A0=A1=L) ＊乱数保持数まで連続出力可



データバス使用時の注意点

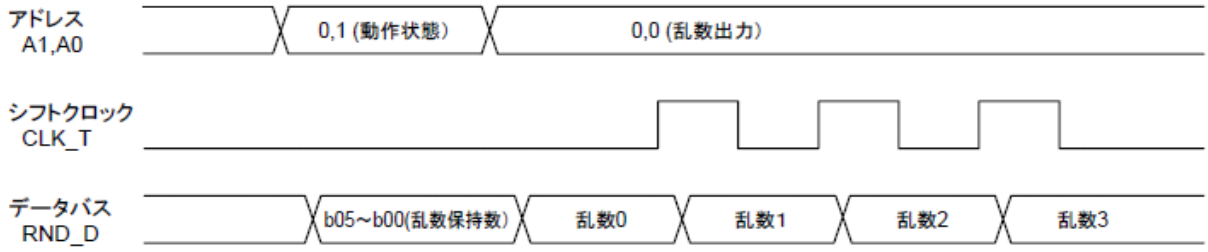
パラレル乱数は、CLK_R によって IC 内部にある 32 段のレジスタに保持され、16 ビット単位でデータバス RND_D へ出力できます。

内部レジスタにどれだけの段数を保持しているかはアドレス A1=0、A0=1 をセットすることにより、データバス RND_D の b05～b00 に保持数として出力されます。この保持数を元にシフトクロック CLK_T によってパラレル乱数出力のレジスタ段をシフトさせ、データバス RND_D 上へパラレル乱数を出力することができます。

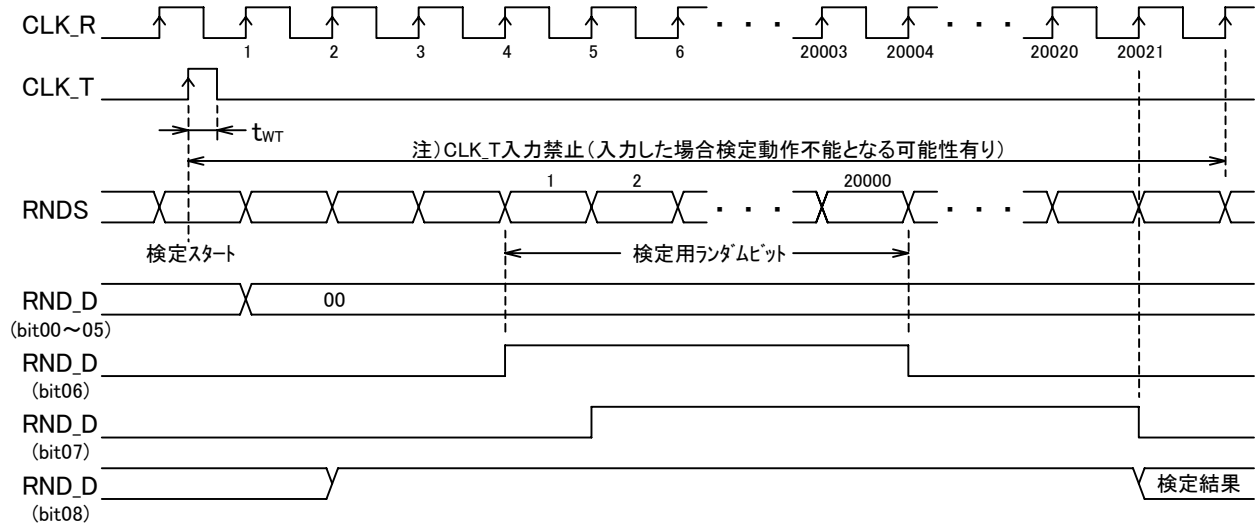
乱数の保持数を確認し内部レジスタに乱数データが保持されている場合、次にアドレスを乱数出力 A1=0、A0=0 へ切り替えます。この時データバス RND_D にはレジスタに保持されている最初の乱数が出力されていますので、このデータも使用して下さい。

内部レジスタをシフトさせ保持している乱数を全て出力するには、先に確認した保持数より「-1」した回数分のシフトクロック CLK_T を入力します。誤って先に確認した保持数と同じシフトクロック CLK_T を入力しますと、乱数データの入っていない ‘ 0000000000000000 ’ のデータを取得してしまいますので、ご注意願います。

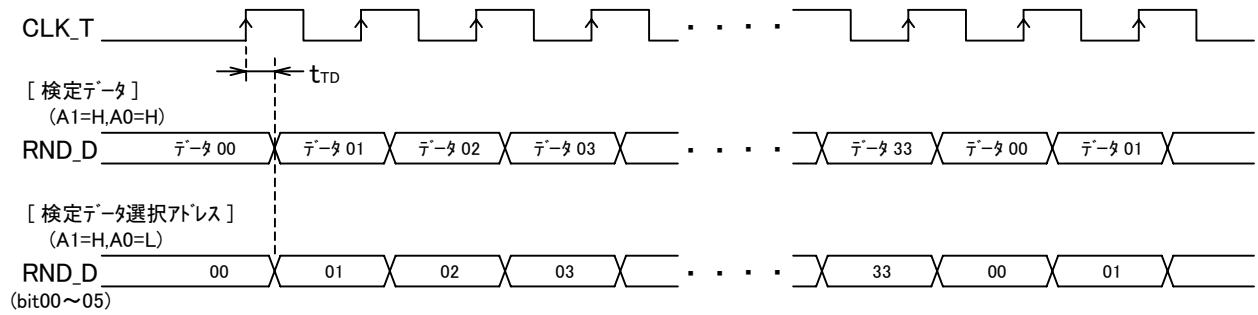
パラレル乱数保持数確認～データバスの乱数取得 (RST=H,TEST=OE=CE=L)



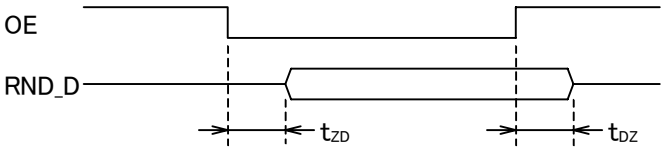
7-3. 検　定 (RST=A1=H,PSV=TEST=OE=CS=A0=L)



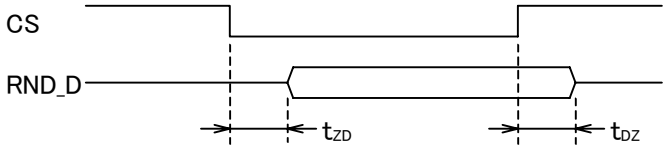
7-4. 検定データ出力 (RST=H,TEST=OE=CS=L)



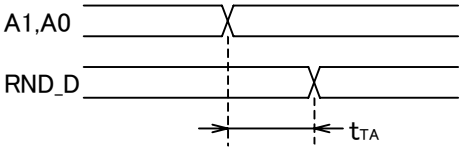
7-5. 出力ｲﾈｰﾌﾞﾙ/ﾃﾞｨｽｴｰﾌﾞﾙ時間 1 (CS=L)



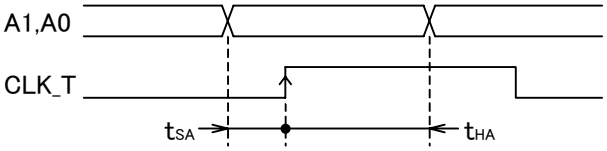
7-6. 出力ｲﾈｰﾌﾞﾙ/ﾃﾞｨｽｴｰﾌﾞﾙ時間 2 (OE=L)



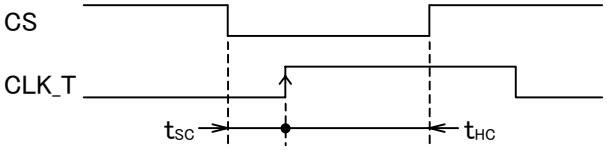
7-7. ﾃﾞｰﾀ出力遅延時間 3 (CS=OE=L)



7-8. ｱﾄﾞﾚｽｾｯﾄｱｯﾌﾟ/ﾎｰﾙﾄﾞ時間



7-9. ﾁｯﾌﾟｾﾚｸﾄｾｯﾄｱｯﾌﾟ/ﾎｰﾙﾄﾞ時間



８．参考資料

8-1. FIPS 140-2 (Change Notice1) Statistical random number generator tests

(1) The monobit test

連続するﾗﾝﾀﾞﾑな 20,000bit 中‘Ｈ’の数がＸのとき、9,725 < Ｘ < 10,275 であれば pass。

(2) The long runs test

連続するﾗﾝﾀﾞﾑな 20,000bit 中‘Ｈ’or‘Ｌ’の最長連続ﾋﾞｯﾄ数がＸのとき、Ｘ < 26 であれば pass。

(3) The runs test

連続するﾗﾝﾀﾞﾑな 20,000bit において、ｉを‘Ｈ’or‘Ｌ’の連続する bit 長としＸｉをその度数とする。但し、i≧6 の場合 i=6 としｉの範囲は 1≦i≦6 とする。Ｘｉの度数計算を‘Ｈ’と‘Ｌ’で行い両方ともＸｉが下表であれば pass。

連続 bit 長	度　数
1	2,315 ≦ Ｘ1 ≦ 2,685
2	1,114 ≦ Ｘ2 ≦ 1,386
3	527 ≦ Ｘ3 ≦ 723
4	240 ≦ Ｘ4 ≦ 384
5	103 ≦ Ｘ5 ≦ 209
6≦	103 ≦ Ｘ6 ≦ 209

(4) The poker test

連続するﾗﾝﾀﾞﾑな 20,000bit を 4bit 毎に 5,000 に区切る。その値 i(0～15)の度数を f(i)とし、下記で判定する。

$$X=(16/5000)*\left(\sum_{i=0}^{15}[f(i)]^2\right)-5000$$

2.16 < Ｘ <46.17 であれば pass。

式を変形すると

$$1{,}563{,}175 < \sum_{i=0}^{15}[f(i)]^2 < 1{,}576{,}928$$

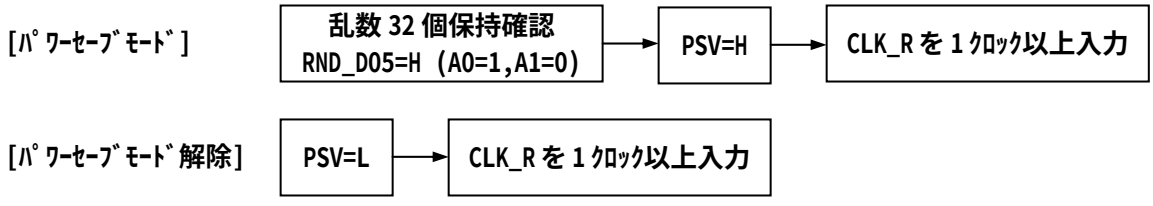
この式で判定する。

8-2. パワーセーブ(PSV)使用時の注意点

ﾊﾟﾜｰｾｰﾌﾞは内部のﾗﾝﾀﾞﾑﾋﾞｯﾄ生成回路を停止させ、電源電流を少なくする機能です。ﾊﾟﾜｰｾｰﾌﾞﾓｰﾄﾞにすると内部のﾗﾝﾀﾞﾑﾋﾞｯﾄ生成回路が停止する為、ﾊﾟﾜｰｾｰﾌﾞを使用するには以下の注意が必要です。

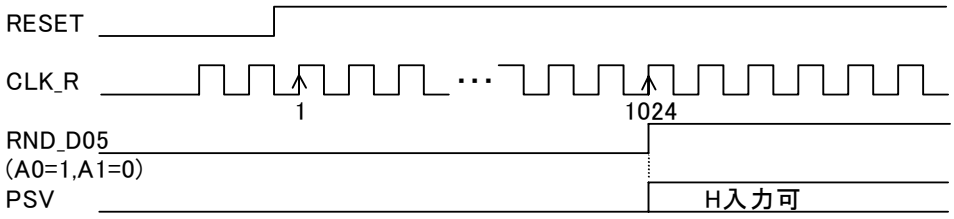
(1) パワーセーブモード及びモード解除

ﾊﾟﾜｰｾｰﾌﾞﾓｰﾄﾞ及びﾓｰﾄﾞ解除は以下のｼｰｹﾝｽによって実行されます。



(2) リセット解除後のＰＳＶ入力

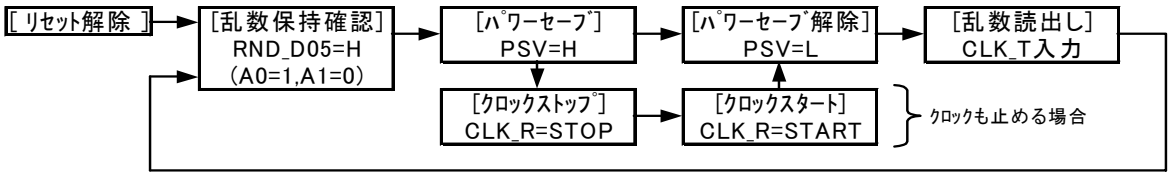
ﾘｾｯﾄ解除後 1024 ｸﾛｯｸ(CLK_R)の区間は初期設定及び乱数保持(16bit×32)期間であり、この区間で PSV=H とするとﾗﾝﾀﾞﾑﾋﾞｯﾄ生成が止まり保持乱数が ”0” となってしまうので、ﾊﾟﾜｰｾｰﾌﾞﾓｰﾄﾞは 1024 ｸﾛｯｸ入力後に実施して下さい。



(3) パワーセーブ時の乱数読出し(A1=0 での CLK_T 入力)

乱数を読み出すと、読み出された分だけ自動的に乱数が追加されるようになっていますが、PSV=H ではﾗﾝﾀﾞﾑﾋﾞｯﾄ生成が止まっている為下記ｼｰｹﾝｽ以外で乱数を読み出すと、 ”0” が保持される可能性がありますので、下記ｼｰｹﾝｽ以外での乱数読出しは避けて下さい。

［シーケンス１］



［シーケンス２］