

# Physical Random number generator

RPG100/RPG100F

data sheet

REV.08

---



---

## Contents

---



---

1. Outline
2. Functions
3. Specifications
  - 3-1. Absolute maximum ratings
  - 3-2. Recommended operation conditions
  - 3-3. DC characteristics
  - 3-4. AC characteristics
  - 3-5. Random numbers specifications
  - 3-6. Package specifications
  - 3-7. Pin layout
4. Terminal function explanation
5. Output data explanation
  - 5-1. Parallel random numbers
  - 5-2. Action state data
  - 5-3. Statistical test state data
  - 5-4. Statistical test data
6. Block diagram
7. Timing chart
  - 7-1. Serial random bits output
  - 7-2. Parallel random numbers output
  - 7-3. Statistical test of randomness
  - 7-4. Statistical test data output
  - 7-5. Output enable/disable time
8. References

1. The contents of this document are subject to change without prior notice as a result of product improvement or discontinuation of production. Therefore, please be sure to check with our sales representatives about the contents before your ordering.
2. Product specifications described in this document are for reference only. Upon the actual use, please obtain specification sheets separately to check the contents.
3. When intending to use our products in the equipments or devices which require especially high reliability and the defects of which might directly cause damage to human life or property, such as nuclear control equipment, aerospace equipment, medical equipment, transportation equipment, disaster prevention equipment, or other safety devices, please do not fail to consult with our sales representatives in advance.  
FDK CORPORATION shall not be liable for any claim or damage caused by improper use of our products that deviates from the conditions or environments for use described in this document.
4. FDK CORPORATION shall not be liable for any infringement or dispute arising in connection with the effect of our or third party's intellectual property rights or other rights during your use of our products or information described in this document. No license to use the rights mentioned above shall be granted without our consent.
5. For products which are controlled items subject to the Foreign Exchange and Foreign Trade Law of Japan, the export license according to the law is required for export.

## 1. Outline

RPG100/RPG100F is an IC that generates physical random bit stream and random numbers at high speeds and no external components are required. Each random bit is output with the random bit generation clock continuously and each random number can be read with the high-speed shift clock. Statistical random number generator tests circuit is built into the chip and statistical tests for randomness can easily be obtained.

## 2. Functions

| Item                                                 | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Random bit output                                    | Continuous serial random bits, which are synchronized with the random bit generation clock, are output from serial data output terminal.                                                                                                                                                                                                                                                                                                                   |
| Random number output                                 | Serial random bit stream is converted to 16 bits random numbers and are stored internally. The stored random numbers, which can be read with a shift clock, are output from data bus.                                                                                                                                                                                                                                                                      |
| Statistical test for randomness and test data output | A statistical test for randomness [FIPS1402 (Change Notice1) Statistical random number generator tests] can be obtained. The test data and the judgment of the statistical test can be read. All internally stored random numbers are cleared when the statistical test is started and random numbers by which the statistical test for randomness was executed are newly stored. These random numbers can be used referring to the judgement of the test. |

## 3. Specifications

## 3-1. Absolute maximum ratings

(VSS=RVSS=0V)

| Item                | Symbol | Rating          | Unit |
|---------------------|--------|-----------------|------|
| Supply voltage      | VCC    | VSS-0.5~+4.0    | V    |
|                     | RVCC   | RVSS-0.5~+4.0   | V    |
| Input voltage       | Vi     | VSS-0.5~VCC+0.5 | V    |
| Output voltage      | Vo     | VSS-0.5~VCC+0.5 | V    |
| Output current      | Io     | ±14             | mA   |
| Power dissipation   | Pd     | 300             | mW   |
| Storage temperature | Tstg   | -55~ 125        | °C   |

## 3-2. Recommended operation conditions

(VSS=RVSS=0V)

| Item                          | Symbol | MIN     | TYP | MAX     | Unit |
|-------------------------------|--------|---------|-----|---------|------|
| Supply voltage                | VCC    | 3.0     | 3.3 | 3.6     | V    |
|                               | RVCC   | 3.0     | 3.3 | 3.6     | V    |
| H level input voltage         | VIH    | VCC×0.8 | -   | VCC     | V    |
| L level input voltage         | VIL    | VSS     | -   | VCC×0.2 | V    |
| CLK_R frequency               | fR     | 245     | 250 | 255     | KHz  |
| CLK_R duty                    | -      | - 5     | 0 - |         | %    |
| Clock input interdiction time | tRT    | 50      | -   | -       | nS   |
| Hold time of H level          | tTH    | 50      | -   | -       | nS   |
| Hold time of L level          | tTL    | 50      | -   | -       | nS   |
| Width of start pulse          | tWT    | 50      | -   | -       | nS   |
| Operating temperature         | Ta     | -40     | -   | 85      | °C   |

## 3-3. DC characteristics

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

| Item                   | Symbol | Condition           | MIN     | TYP  | MAX | Unit |
|------------------------|--------|---------------------|---------|------|-----|------|
| Supply current         | ICC    | CLK_R=250KHz        | -       | 2.3  | -   | mA   |
|                        |        | PSV=H               | - 0.    | 13 - |     | mA   |
|                        |        | PSV=H<br>CLK_R=STOP | - 1     |      | 5   | uA   |
| H level output voltage | VOH    | IOH=4mA             | VCC-0.5 | -    | VCC | V    |
| L level output voltage | VOL    | IOL=4mA             | VSS     | -    | 0.4 | V    |

## 3-4. AC characteristics

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

| Item                                    | Symbol          | Condition | MIN | TYP | MAX | Unit |
|-----------------------------------------|-----------------|-----------|-----|-----|-----|------|
| Data output delay time 1                | t <sub>rs</sub> | Load 50pF | -   | -   | 20  | nS   |
| Data output delay time 2                | t <sub>TD</sub> | Load 50pF | -   | -   | 50  | nS   |
| Data output delay time 3                | t <sub>TA</sub> | Load 50pF | -   | -   | 25  | nS   |
| Output enable time                      | t <sub>zD</sub> | Load 50pF | -   | -   | 18  | nS   |
| Output disable time<br>(Drive OFF time) | t <sub>DZ</sub> |           | -   | -   | 6   | nS   |
| Address setup time                      | t <sub>SA</sub> |           | 20  | -   | -   | nS   |
| Address hold time                       | t <sub>HA</sub> |           | 50  | -   | -   | nS   |
| Chip select setup time                  | t <sub>SC</sub> |           | 20  | -   | -   | nS   |
| Chip select hold time                   | t <sub>HC</sub> |           | 50  | -   | -   | nS   |

## 3-5. Random bit &amp; Random number specifications

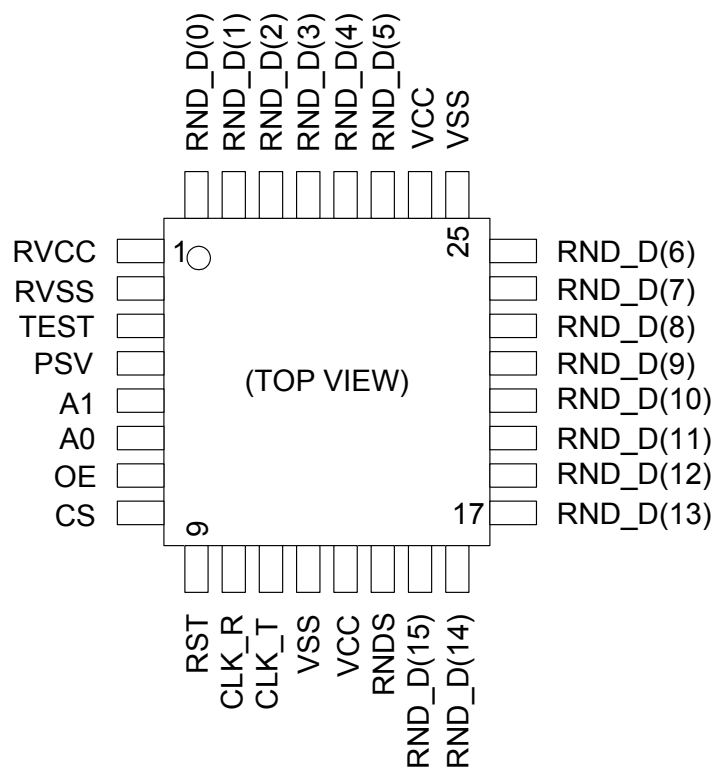
| Item S                                  | pecification                                                                       |
|-----------------------------------------|------------------------------------------------------------------------------------|
| Source of randomness                    | Noise in semiconductors                                                            |
| Stored maximum number of random numbers | Max 16bit×32                                                                       |
| Quality of the random bit stream        | FIPS 140-2(Change Notice1) Statistical random number generator tests corresponding |

## 3-6. Package specifications

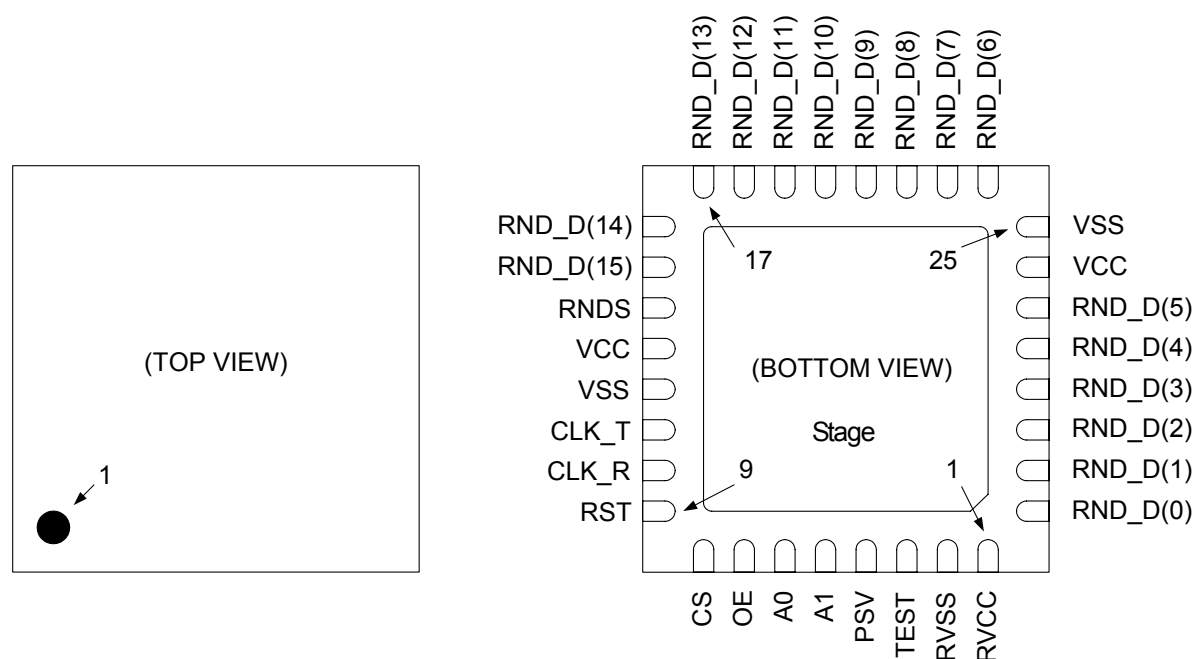
| Item RP                      | G100         | RPG100F     |
|------------------------------|--------------|-------------|
| Package dimensional standard | Plastic LQFP | Plastic QFN |
| Size of package with leads   | 9mm×9mm      | 5mm×5mm     |
| Number of pins               | 32 pins      | 32 pins     |
| Lead pitch                   | 0.8mm        | 0.5mm       |

## 3-7. Pin layout

## &lt;RPG100 LQFP Package&gt;



## &lt;RPG100F QFN Package&gt;



## Note

Stage is open circuit, connection to GND is unnecessary.  
 Please do not lay the PCB signal patterns under the Stage.

## 4. Terminal function explanation

| Terminal symbol | Terminal name               | I/O | Function explanation                                                                                                                                                                                                  |
|-----------------|-----------------------------|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OE              | Output enable               | I   | Data bus output control signal.                                                                                                                                                                                       |
| CS              | Chip select                 | I   | Chip enable/disable control signal.                                                                                                                                                                                   |
| CLK_R           | Random bit generation clock | I   | Random bits are generated with the rising edge of the clock.                                                                                                                                                          |
| CLK_T           | Shift clock                 | I   | Shift clock to random numbers output, data selection clock when statistical test data is read and start pulse when statistical test is started.                                                                       |
| A1,A0           | Address                     | I   | Output data selection to data bus and enabling address to start statistical test.                                                                                                                                     |
| PSV             | Power saving                | I   | If 'H' powersaving is enabled (8-2 reference)                                                                                                                                                                         |
| RNDS            | Serial data output          | O   | Random bits that synchronize with the random bits generation clock are output. When the random bits generation state flag is 'L' the valid random bits can be used. If the power saving is enabled the output is 'L'. |
| RND_D (15~00)   | Data bus                    | O   | Random numbers and various data are output. When the random bits generation state flag is 'L', valid stored random numbers can be used.                                                                               |
| TEST            | Test                        | I   | Connect to the same potential as VSS.                                                                                                                                                                                 |
| RST             | Reset                       | I   | When 'L' reset occurs.<br>Input a 'L' level signal at power-on.                                                                                                                                                       |
| VCC             | Power supply                |     |                                                                                                                                                                                                                       |
| RVCC            | Analog power supply         |     | Connect to the same potential as VCC.                                                                                                                                                                                 |
| VSS             | GND                         |     |                                                                                                                                                                                                                       |
| RVSS            | Analog GND                  |     | Connect to the same potential as VSS.                                                                                                                                                                                 |

(Truth tables)

X : H or L

| CS | OE | Chip control | Data bus       | Serial data output |
|----|----|--------------|----------------|--------------------|
| H  | X  | Disable      | High impedance | Output             |
| L  | L  | Enable       | Data output    | Output             |
| L  | H  | enable       | High impedance | Output             |

| A1 | A0 | Data in the data bus        | Shift clock function                  | Serial data output |
|----|----|-----------------------------|---------------------------------------|--------------------|
| 0  | 0  | Random number               | Random numbers shift clock            | Output             |
| 0  | 1  | Action state data           | Random numbers shift clock            | Output             |
| 1  | 0  | Statistical test state data | Start pulse to Statistical test       | Output             |
| 1  | 1  | Statistical test data       | Statistical test data selection clock | Output             |

## 5. Output data explanation

## 5-1. Random number

| Output bit | Output data explanation                                                                   |
|------------|-------------------------------------------------------------------------------------------|
| b15~b00    | 16 bits random number can be read continuously up to the number of random numbers stored. |

## 5-2. Action state data

| Output bit | Output data explanation                                                                                                                                                                                     |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| b05~b00    | Number of random numbers stored.                                                                                                                                                                            |
| b06        | Presence of stored random numbers (H: Presence, L: Absence).                                                                                                                                                |
| b07        | Initialization flag (H: Initialized end, L: Initializing). After releasing reset the output becomes 'L' until 512 CLK_R counts and the random bits output are invalid.                                      |
| b08        | Statistical test state (H: Testing, L: Test end).                                                                                                                                                           |
| b09        | Random bits generation state flag (H: Abnormal operation, L: Normal operation). When the random bits generation circuit is in normal operation mode the flag is 'L'. But the flag is 'H' when Initializing. |
| b15~b10    | 'L' fixation.                                                                                                                                                                                               |

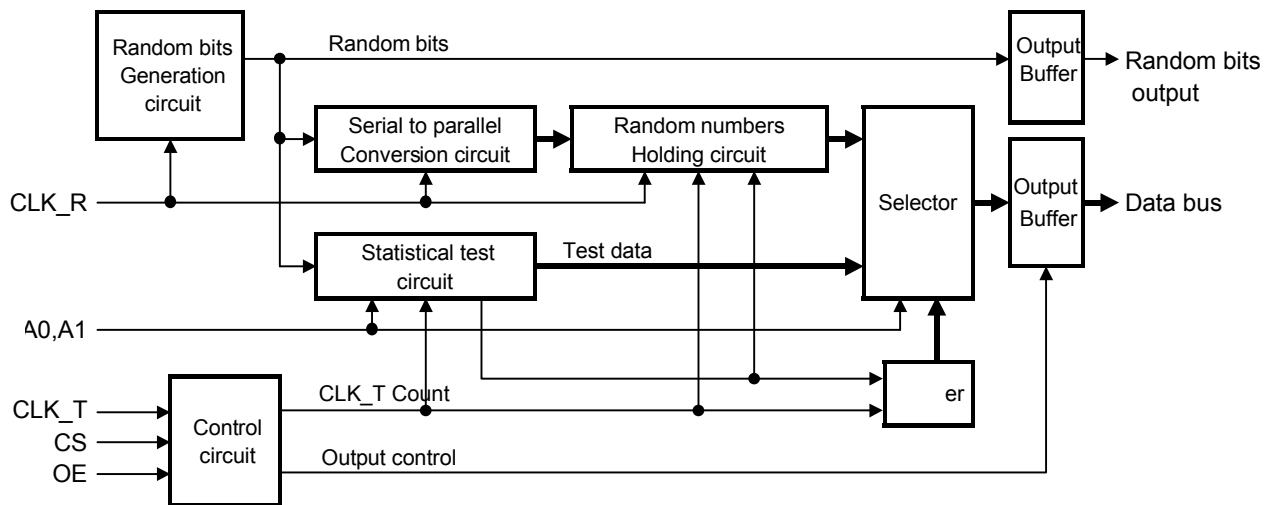
## 5-3. Statistical test state data \* timing chart 7-3 and 7-4 references.

| Output bit | Output data explanation                                                                |
|------------|----------------------------------------------------------------------------------------|
| b05~b00    | Statistical test data selection address.                                               |
| b06        | Region of random bits for statistical test.                                            |
| b07        | Statistical test state (H: Testing, L: Test end).                                      |
| b08        | Statistical test result (H: Fail, L: Pass).<br>* Same as statistical test data00(b15). |
| b12~b09    | Data for test.                                                                         |
| b15~b13    | Data for test.                                                                         |

## 5-4. Statistical test data \* timing chart 7-3 and 7-4 references.

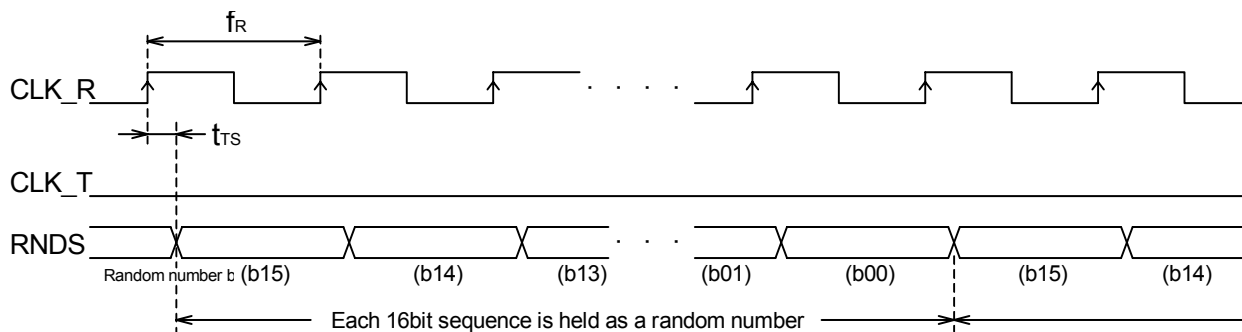
| Statistical test data selection address (Test data) | Output bits | Output data explanation                                              |                                                            |                                        |
|-----------------------------------------------------|-------------|----------------------------------------------------------------------|------------------------------------------------------------|----------------------------------------|
| 00 (Data 00)                                        | b15~b00     | Statistical test result (H:Fail) (L:Pass)                            | b00:Data 02 judgment                                       | b08:Data 10 judgment                   |
|                                                     |             |                                                                      | b01:Data 03 judgment                                       | b09:Data 11 judgment                   |
|                                                     |             |                                                                      | b02:Data 04 judgment                                       | b10:Data 12 judgment                   |
|                                                     |             |                                                                      | b03:Data 05 judgment                                       | b11:Data 13 judgment                   |
|                                                     |             |                                                                      | b04:Data 06 judgment                                       | b12:Data 14 judgment                   |
|                                                     |             |                                                                      | b05:Data 07 judgment                                       | b13:Data 15 judgment                   |
|                                                     |             |                                                                      | b06:Data 08 judgment                                       | b14:Data 16,17 judgment                |
|                                                     |             |                                                                      | b07:Data 09 judgment                                       | b15:Total judgment                     |
| 01 (Data 01)                                        | b15~b00     | The total number of random bits for statistical test                 |                                                            |                                        |
| 02 (Data 02)                                        | b15~b00     | FIPS 140-2(Change Notice1) Statistical random number generator tests | The monobit test data (Number of 'H' bits)                 |                                        |
| 03 (Data 03)                                        | b15~b00     |                                                                      | The longrun test data (Maximum number of consecutive bits) |                                        |
| 04 (Data 04)                                        | b15~b00     |                                                                      | The run test data                                          | Number of continuous 'L' bit length1   |
| 05 (Data 05)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'H' bit length1   |
| 06 (Data 06)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'L' bit length2   |
| 07 (Data 07)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'H' bit length2   |
| 08 (Data 08)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'L' bit length3   |
| 09 (Data 09)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'H' bit length3   |
| 10 (Data 10)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'L' bit length4   |
| 11 (Data 11)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'H' bit length4   |
| 12 (Data 12)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'L' bit length5   |
| 13 (Data 13)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'H' bit length5   |
| 14 (Data 14)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'L' bit length6 ≤ |
| 15 (Data 15)                                        | b15~b00     |                                                                      |                                                            | Number of continuous 'H' bit length6 ≤ |
| 16 (Data 16)                                        | b15~b00     |                                                                      | The poker test data                                        | Calculated value $(\sum [f(i)]^2) / n$ |
| 17 (Data 17)                                        | b15~b00     |                                                                      |                                                            | * f(i) is Data 18-33.                  |
| 18 (Data 18)                                        | b15~b00     |                                                                      |                                                            | Low bits                               |
| 19 (Data 19)                                        | b15~b00     |                                                                      |                                                            | High bits                              |
| 20 (Data 20)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '00'             |
| 21 (Data 21)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '01'             |
| 22 (Data 22)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '02'             |
| 23 (Data 23)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '03'             |
| 24 (Data 24)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '04'             |
| 25 (Data 25)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '05'             |
| 26 (Data 26)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '06'             |
| 27 (Data 27)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '07'             |
| 28 (Data 28)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '08'             |
| 29 (Data 29)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '09'             |
| 30 (Data 30)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '10'             |
| 31 (Data 31)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '11'             |
| 32 (Data 32)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '12'             |
| 33 (Data 33)                                        | b15~b00     |                                                                      |                                                            | Number of 4bits value '13'             |
|                                                     |             |                                                                      |                                                            | Number of 4bits value '14'             |
|                                                     |             |                                                                      |                                                            | Number of 4bits value '15'             |

## 6. Block diagram



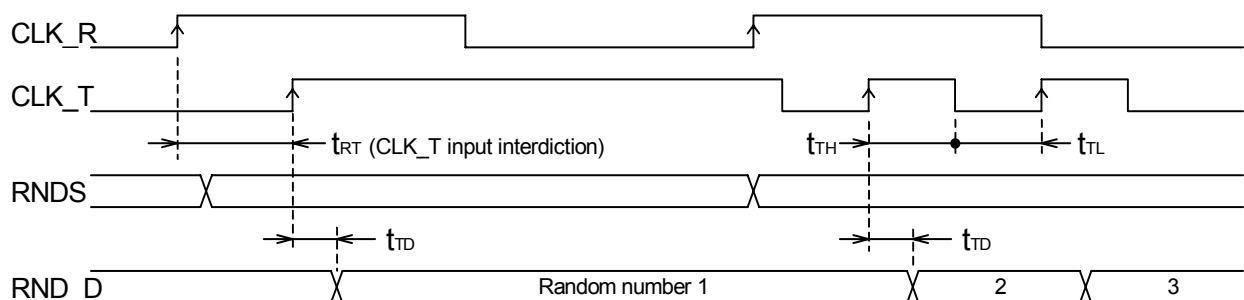
## 7. Timing chart

## 7-1. Random bits output (RST=H,PSV=TEST=L)



## 7-2. Random numbers output (RST=H,TEST=OE=CS=A0=A1=L)

\*Possible to read continuously up to the number of random numbers stored



## Note: Data Bus use

This IC can store 32 steps 16bit random number and you can read them continuously up to the number of stored. You can check the number of 16bit random number stored, and get them by reading and shifting register with CLK\_T. If you want to check the number of 16bit random number stored, please set address A1=0, A0=1, and read output b05 - b00 of RND\_D.

And if register stores 16bit random number, please change address A1=0, A0=0 to read them.

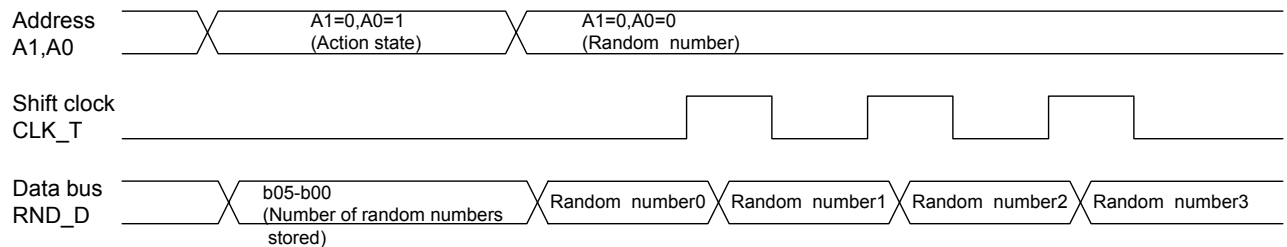
Then the first 16bit random nuber is comming to output of RND\_D with changing address.

If you want to read all random numbers stored please input CLK\_T with "the number of 16bit random number stored - 1" times

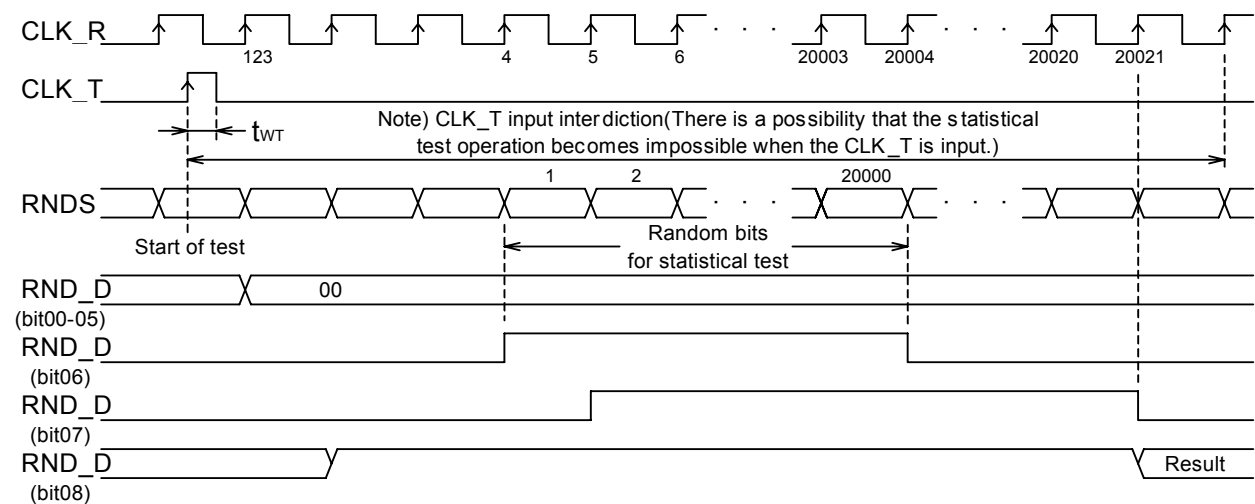
Please note that if you input CLK\_T with same as the number of 16bit random number stored, the last output of RND\_D is '0000000000000000' and this is not random number.

Checking the number of 16bit random number stored and output them.

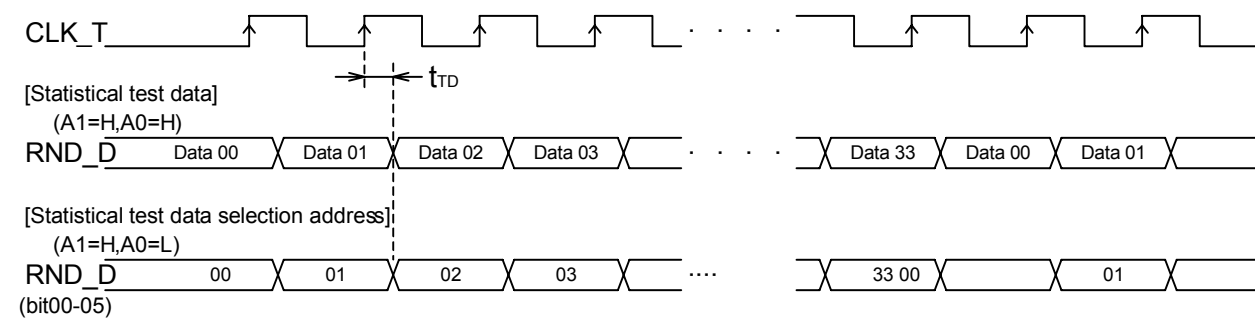
(RST=H, TEST=OE=CE=L)



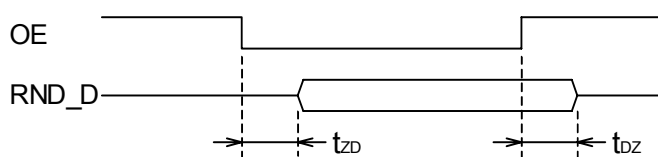
### 7-3. Statistical test ( RST=A1=H, PSV=TEST=OE=CS=A0=L )



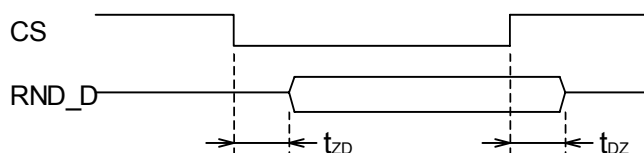
### 7-4. Statistical test data output ( RST=H, TEST=OE=CS=L )



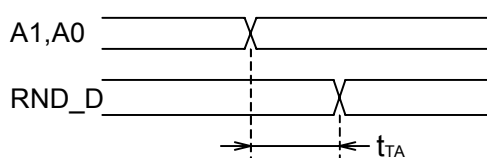
## 7-5. Output enable / disable time 1(CS=L)



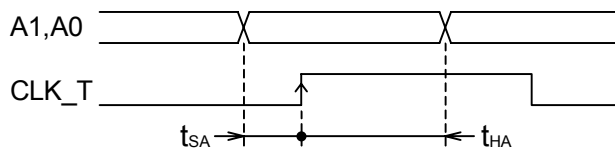
## 7-6. Output enable / disable time 2(OE=L)



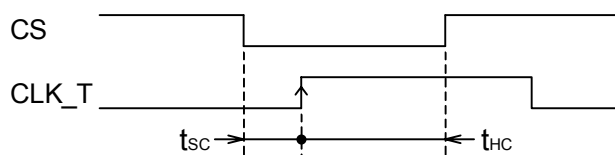
## 7-7. Data output delay time 3 (CS=OE=L)



## 7-8. Address setup / hold time



## 7-9. Chip select setup / hold time



## 8. Reference material

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

## (1) The monobit test

X denotes the number of 'H' bits in a 20,000 random bits stream. The test is passed if  $9,725 < X < 10,275$ .

## (2) The long runs test

X denotes the maximum number of consecutive bits of either all 'H' or all 'L' in a 20,000 random bits stream. The test is passed if  $X < 26$ .

## (3) The runs test

$X_i$  denotes the number of consecutive bits of same kind of length  $i$  ( $1 \leq i \leq 6$ ) in a 20,000 random bits stream. If  $i \geq 6$  considered to be of  $i = 6$ . The test is passed if the  $X_i$  lies within the specified required intervals in the table given below. This must hold for both H's and L's.

| Length of Run | Required Interval         |
|---------------|---------------------------|
| 1 2,          | $315 \leq X_1 \leq 2,685$ |
| 2 1,          | $114 \leq X_2 \leq 1,386$ |
| 3 5           | $27 \leq X_3 \leq 723$    |
| 4 2           | $40 \leq X_4 \leq 384$    |
| 5 1           | $03 \leq X_5 \leq 209$    |
| 6 ≤ 1         | $03 \leq X_6 \leq 209$    |

## (4) The poker test

Divide the 20,000 random bits stream into 5,000 consecutive four bits segments. Let  $f(i)$  be the number of occurrences of the  $i$ th ( $0 \leq i \leq 15$ ) type of four bits segment.

Evaluate the following:

$$X = (1/5000) \cdot \left( \sum_{i=0}^{15} [f(i)]^2 \right) - 5000$$

The test is passed if  $2.16 < X < 46.17$ .

Let modify the inequality

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

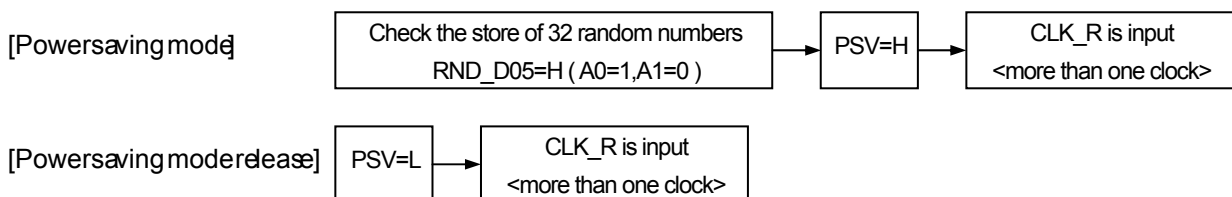
The poker test is judged from this inequality

## 8-2. Notes when power saving (PSV) is used

The power saving is a function to stop the internal random bit generation circuit operation, and to reduce the power supply current. The following attention is necessary to use the power saving so that an internal random bit generation circuit stops when changing to the power saving mode.

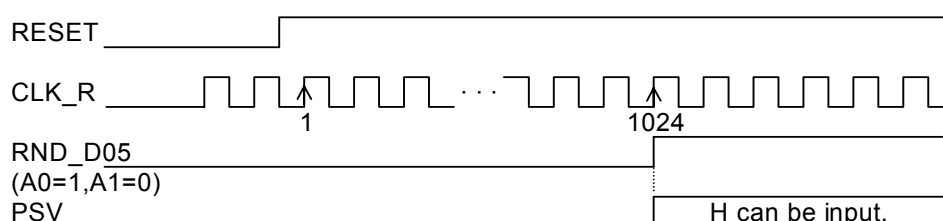
## (1) Power saving mode and mode release

The power saving mode and the mode release are executed by the following sequences.



## (2) PSV input after releasing reset

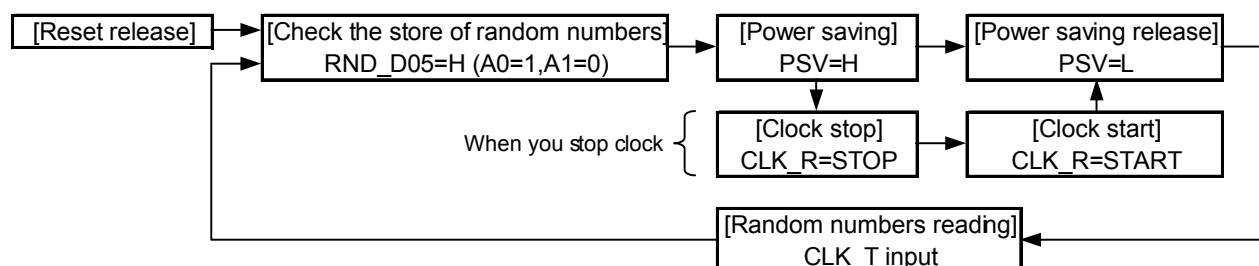
After releasing reset, the first section of 1024 clocks (CLK\_R) period is used for initialization and to store first 32 (16bit×32) random numbers. If PSV=H in this section, the random bit generation stops, and the stored random numbers become "0". Please execute the power saving mode after inputting 1024 clocks.



## (3) Random numbers reading when power saving (CLK\_T input with A1=0)

When random numbers are read, random numbers are automatically added only as for the read amount. There is a possibility that "0" is stored because the random bit generation stops at PSV=H when random numbers are read other than the undermentioned sequences. Please avoid the reading of random numbers other than the undermentioned sequences.

## [Sequence 1]



## [Sequence 2]

