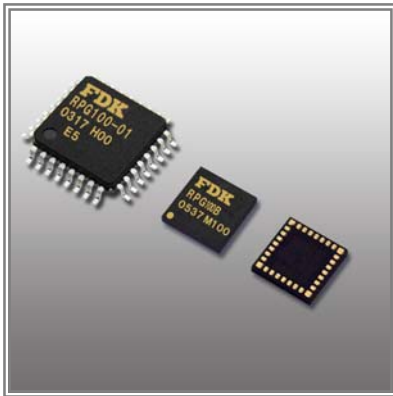


True Random Number Generation IC RPG100 / RPG100B



Features

- The TRNG generates high quality physical random numbers for various purposes in wide-ranging applications.
- Natural phenomenon in CMOS is used to generate true random numbers.
- The circuit is composed of only CMOS and no external components are needed.
- Two independent white noise sources are used as the sources of randomness to eliminate external noise interferences.
- The quality of the true random numbers (correspond to FIPS140-2 Change Notice 1 standard).
- A randomness statistical test circuit is equipped (conform to FIPS 140-2 Change Notice 1 standard).
- The random numbers are generated at a High speed (up to 32 x 16bits random numbers are stored internally; and they can also be read at a high-speed).

Applications

- Network security, E-Commerce, Cryptography, Authentication and Discrimination, Lottery, Game, Simulation, Graphics, Wireless LAN, Computer, Mobile equipments, FA

Specification

Serial random bits (bit/sec)	16bits random numbers	Quality of random numbers	Random bit generation Clock	Power supply voltage range	Supply current Ta=25°C	Operating temperature
250K *Synchronized with the random bits generation clock	Up to 32 x 16bits random numbers are held internally	Satisfies: FIPS140-2	250KHz	+3.0V to 3.6V	typ. 2.30mA (*1) typ. 0.13mA (*2) typ. 1uA (*3)	-40°C to 85°C

*1: Normal mode *2: Power save mode *3: Power save mode and CLK_R=fixed to L or H

Package and Dimensions

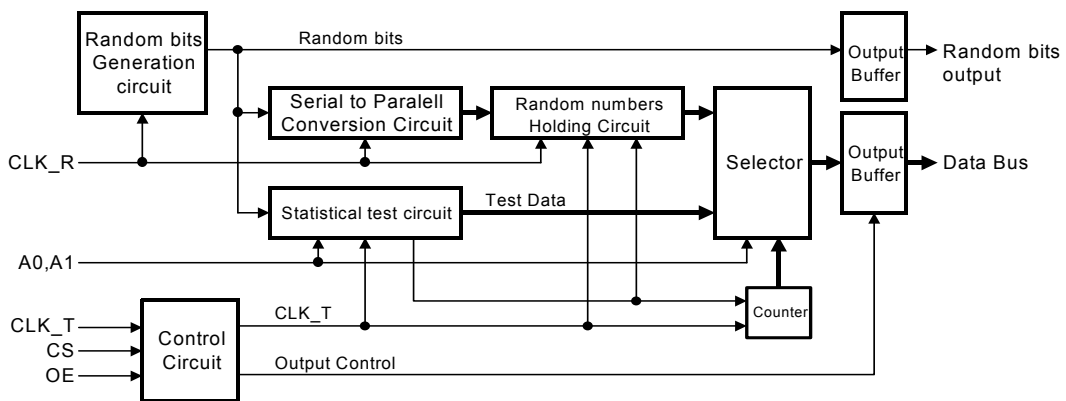
RPG100	RPG100B
Pb free 32 pins plastic LQFP	Pb free 32 pins plastic BCC

Unit: mm

Terminal Functions

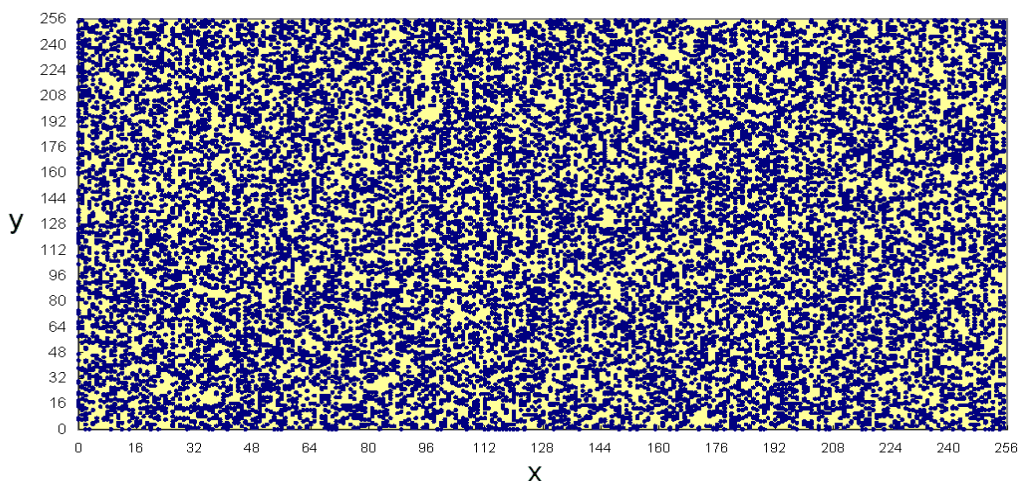
No.	Symbol	Name	I / O	No.	Symbol	Name	I / O
1	RVCC	Analog power supply	-	9	RST	Reset	I
2	RVSS	Analog GND	-	10	CLK_R	Random bit generation clock	I
3	TEST	Test	I	11	CLK_T	Shift clock	I
4	PSV	Power save	I	12,25	VSS	GND	-
5	A1	Address	I	13,25	VCC	Power supply	-
6	A0	Address	I	14	RNDS	Serial data output	O
7	OE	Output enable	I	15 to 24, 27 to 32	RND_D (15 : 0)	Data bus (Random bits / Verification data / Other internal test data)	O
8	CS	Chip select	I				

Block Diagram



<TEST RESULTS>

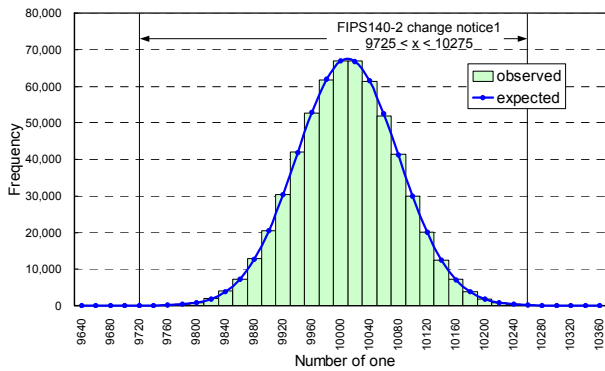
Two Dimensional Scatter Diagram of Random Numbers



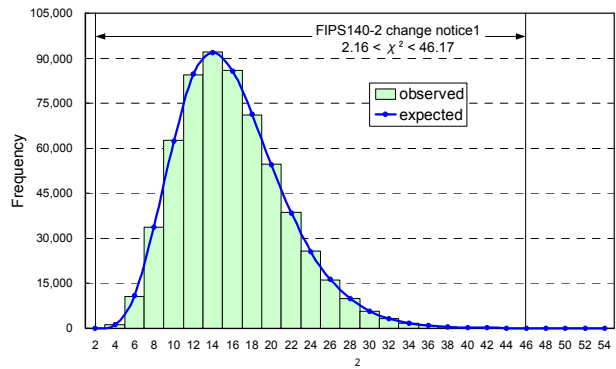
Random Number Test Results Based On FIPS140-2(change notice1)

(The number of tests considered : 600,000)

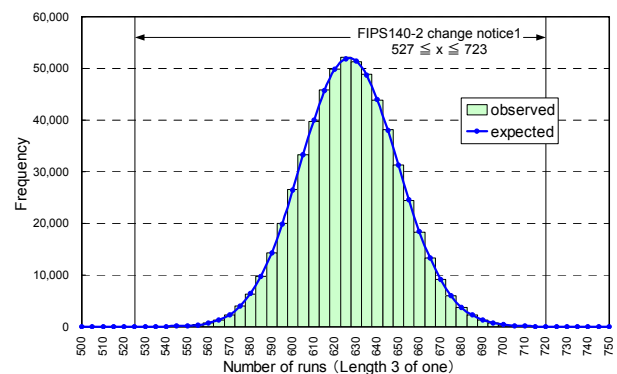
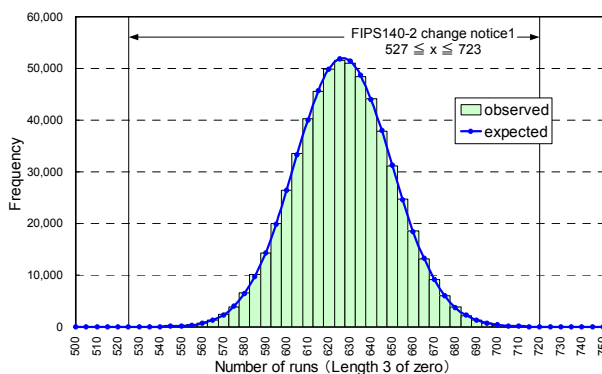
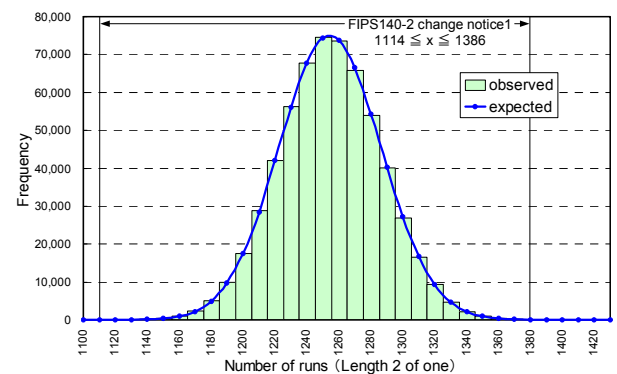
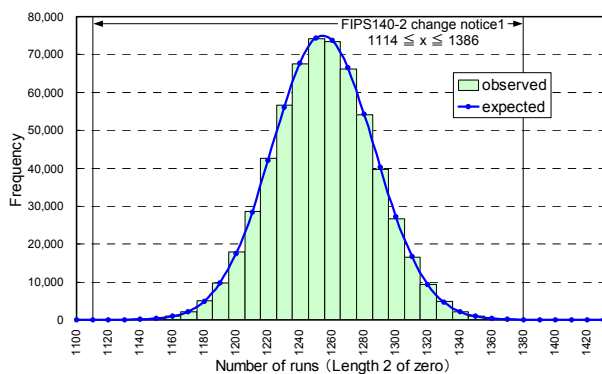
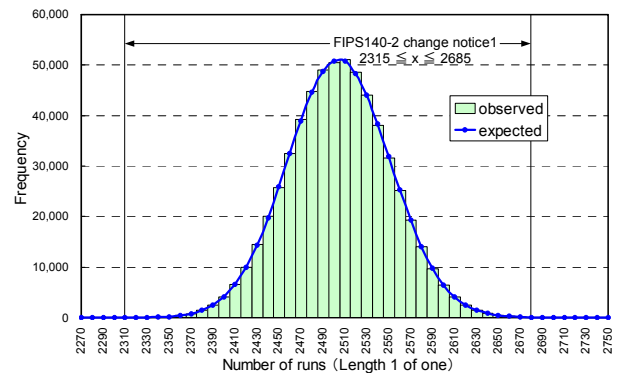
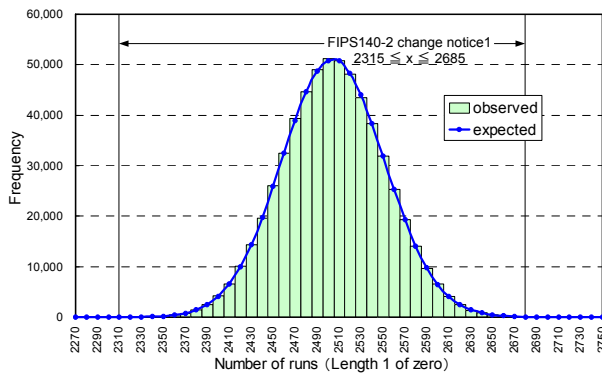
The monobit test

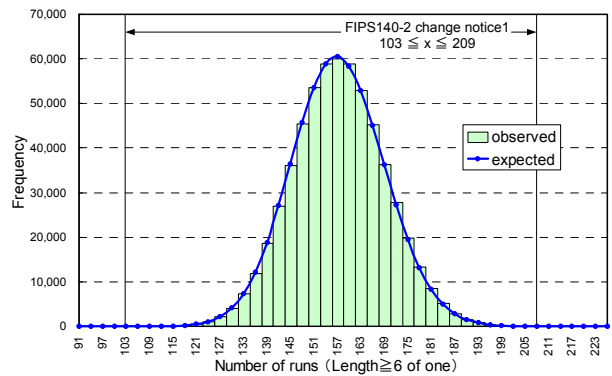
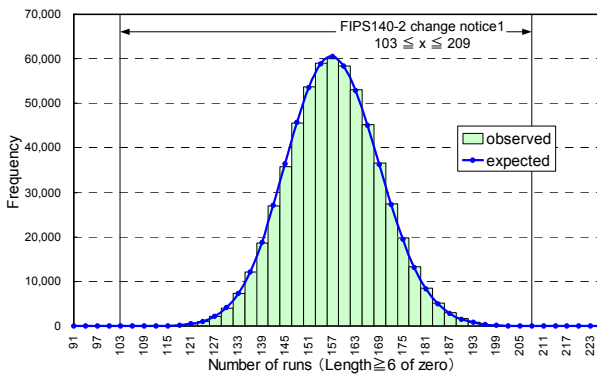
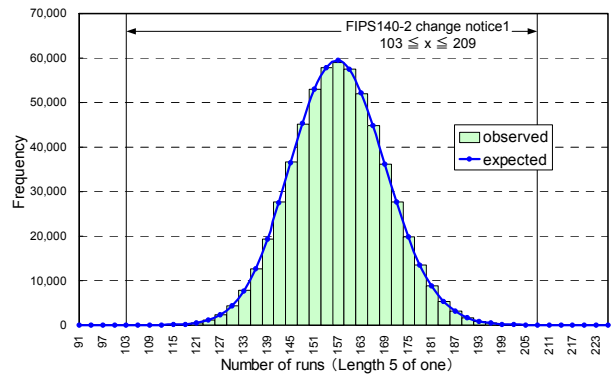
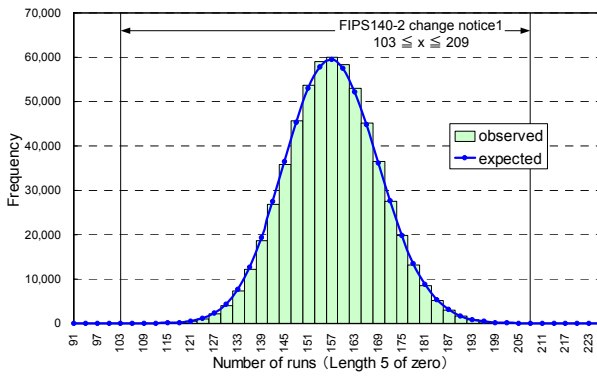
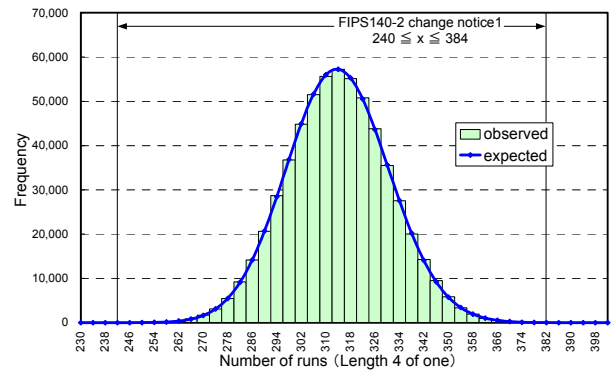
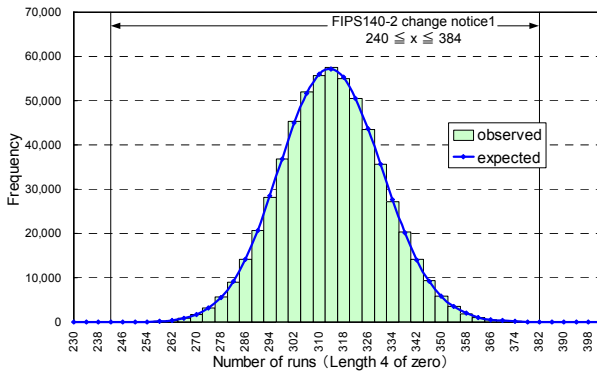


The poker test

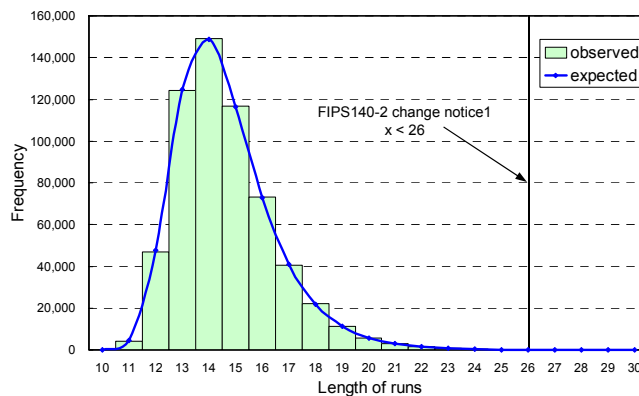


The runs test





The long runs test



■ The content of this catalog is subject to change without prior notice for further improvement. If you have any inquiries, please contact our sales department. Last update September 2005.