AN LSI RANDOM NUMBER GENERATOR (RNG)

R. C. Fairfield, R. L. Mortenson, & K. B. Coulthart

AT&T Bell Laboratories
25 Lindsley Drive
Morristown, New Jersey 07960

INTRODUCTION

This paper describes a CMOS digital LSI device which generates a random bit stream based on the frequency instability of a free running oscillator. The output of the device is a truly random binary number; not pseudo random.

The device was developed to be used, principally, in cryptographic systems as a source for cryptographic keys and/or initial values. Some cryptographic systems rely on pseudo random generator schemes as a source of keys and initial values but a cryptographically secure system demands the use of truly random numbers.

DESIGN OBJECTIVES

At the outset of the device development four design objectives were established.

(1) The fundamental source of the random binary number had to be based on a natural statistical or probabilistic phenomenon.

(2) A completely digital IC was desired.

(3) The device should operate in a microprocessor controlled environment. That is, a microprocessor compatible interface had to be provided.

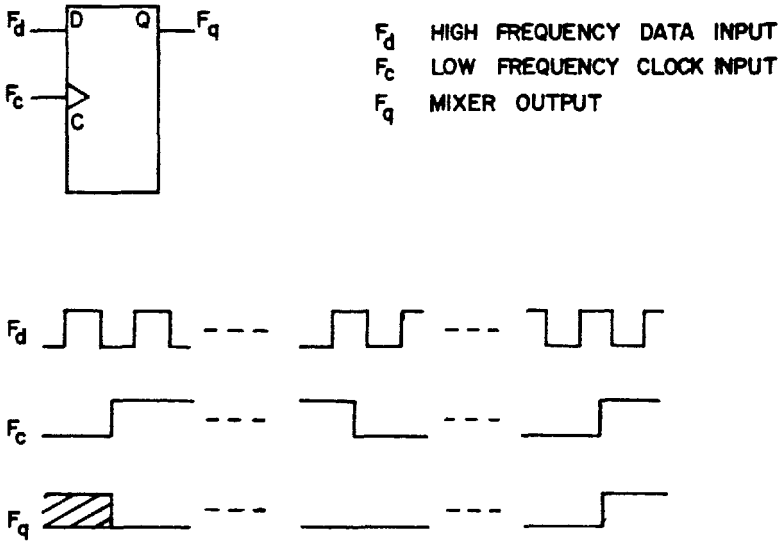
(4) Means to run periodic checks of the circuitry had to be provided.

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, pp. 203-230, 1985.

IMPLEMENTATION

The fundamental probabilistic phenomena utilized on the device is the frequency instability of a free running oscillator. The use of this phenomena to generate truly random numbers is not new. The RAND Corporation used this phenomena to generate a table of a million random digits which it published in 1955 [1].

In the device under discussion here, a random bit stream is generated by digitally mixing two independent square waves in a positive-edge-triggered D-type flip-flop. In the implementation, a low frequency wave is used to clock the flip-flop and in so doing sample a high frequency wave which is applied to the flip-flop input data lead. The circuit is shown in Figure 1.



DIGITAL MIXER

Figure 1

The IC contains two on-chip oscillators. One produces a high frequency nonadjustable 8 MHz square wave which can be used as the sampled signal at the data input. The second oscillator frequency is adjustable with external resistors and capacitors and can be used as the sampling signal applied to the clock lead of the mixer. The data

and clock signals can also be supplied from off chip sources. It is not recommended that the 8 MHz on-chip oscillator be used. Weak coupling or interaction between the two oscillators has been observed and this may affect the randomness of the number produced. The use of an off chip high frequency square wave oscillator, preferably crystal controlled, will substantially reduce any possibility of coupling. The use of an RC controlled oscillator for the sampling signal is favored over an LC or crystal controlled oscillator in this application because of the inherently lower Q of the frequency determining circuits. The result is higher noise and poorer spectral purity and thus larger period variations in the output waveform [2], [3].

If the high frequency signal has a 50% duty cycle and the low frequency clock has significant cycle to cycle period variation, each successively generated bit is independent and has equal probability of being a "one" or a "zero". What is meant by significant is defined below. Of course, neither of these conditions hold in general. Thus, deterministic circuitry must be used to eliminate bias caused by less than ideal signals.

If the high frequency sampled square wave has something other than a 50% duty cycle there will be a bias toward either "one" or "zero" bits at the sampling D-type flip-flop output. This bias can be effectively removed if groups of samples are passed through an exclusive-or chain. Figure 2 shows an implementation which generates a single random bit by taking the exclusive-or sum of four stored bits. The data rate is reduced by four since bits are not reused. This circuit is implemented on the IC with the left most or first flip-flop performing the digital mixing of the two applied square waves. The bias correction achieved by such a circuit is given by the following. If the duty cycle of the high frequency square wave is p, the probability of obtaining a "one" as a sample is p while the probability of obtaining a "zero" is 1-p. However, if n independent samples obtained from a biased signal are passed through an exclusive-or chain, the probability that the bit at the output of the chain is "one" is given by

$$P_x(1) = 0.5 - 2^{n-1}(p-0.5)^n$$

while the probability that the bit is a "zero" is given by

$$P_x(0) = 0.5 + 2^{n-1}(p-0.5)^n$$

Thus if the duty cycle of the high frequency square wave is 55% and the exclusive-or operation is performed over four samples, the probability of obtaining a "one" out of the exclusive-or chain is

$$P_x(1) = 0.49995$$

while the probability of obtaining a "zero" is

$$P_x(0) = 0.50005$$

In the above equations it can be seen that as n goes to infinity the probability approaches 0.5.

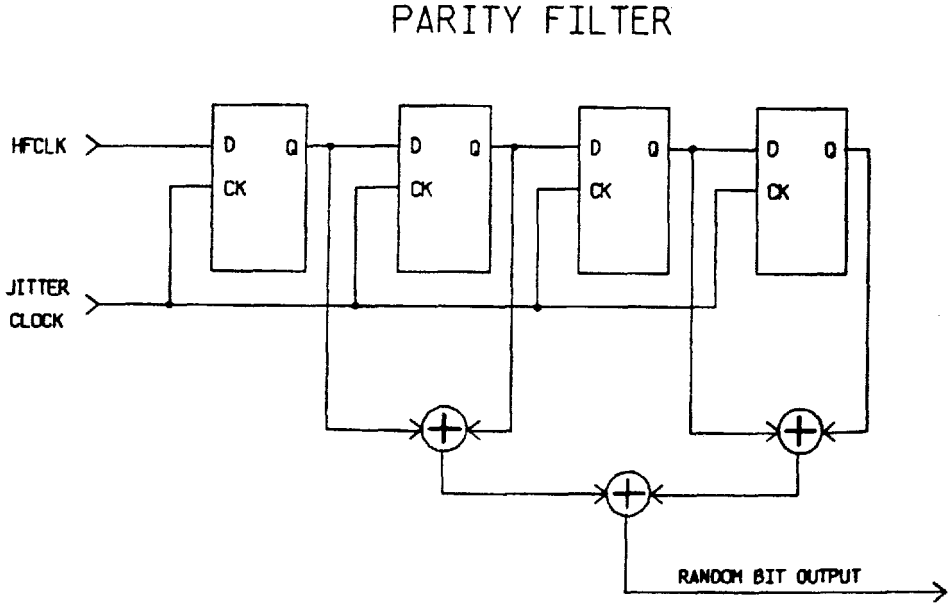


Figure 2

The second bias or difficulty which arises stems from insufficient phase jitter or frequency fluctuations on the clock input. As previously stated, if the low frequency clock has significant cycle to cycle period variation, each successively generated sample is independent and an individual cannot accurately predict the state of a sample knowing the state of the preceding sample and the mean frequencies of the two signals generating them. Figure 3 and Table 1 show the probability of guessing a bit in sequence knowing the expected periods of the high and low frequency oscillators, the standard deviation of the low frequency oscillator's

period variations, plus the state of the previous bit.

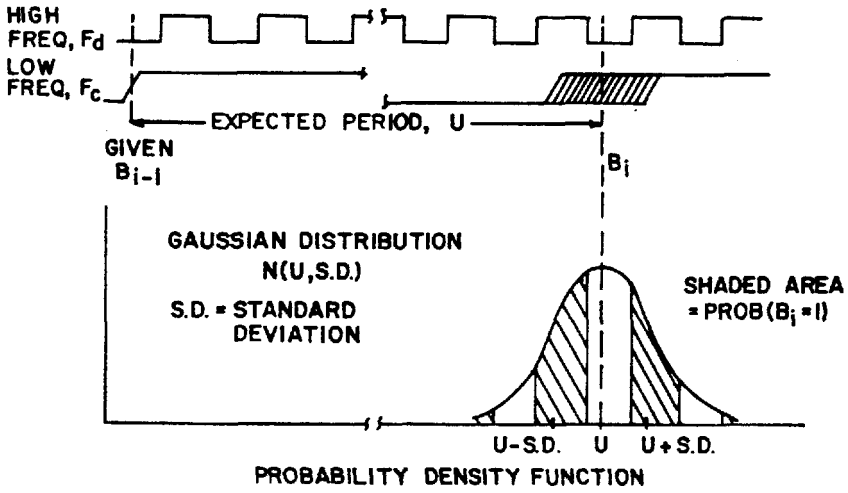


Figure 3

2 x S.D./Td	PROB[Bi|Bi-1]
**********	**********
2.00	0.50000+
1.50	0.500006
1.25	0.500180
1.00	0.502891
0.75	0.525041
0.50	0.617052
0.25	0.797871
0.20	0.837035
0.10	0.913442

S.D. = standard deviation of the low frequency period variation.

Td = period of the high frequency oscillator.

Table 1

It is clear from Table 1 that if twice the standard deviation of the low frequency period variation is but a fraction of the high frequency oscillator period there is significant bit to bit correlation and individual bits can be guessed from the state of preceding bits. On the other hand, if the ratio of twice the standard deviation of the

low frequency period variation to the high frequency oscillator period is greater than 1.5 there is little bit to bit correlation.

In general one does not get cycle to cycle period variations from the D-type flip-flop clock such that the variations span 1.5 or more cycles of the data input signal. Thus, there will be sample to sample correlation between bits out of the flip-flop and knowing one sample and the mean frequencies of the input signals one can predict the state of the next sample with some degree of accuracy. As with the duty cycle bias the sample to sample correlation may be effectively removed through the use of exclusive-or circuits. The correlation correction is achieved as samples generated many clock cycles apart are exclusive-ored together. The circuit in Figure 4, which appears on the IC and is fed from the output of the parity filter shown in Figure 2, performs this task.

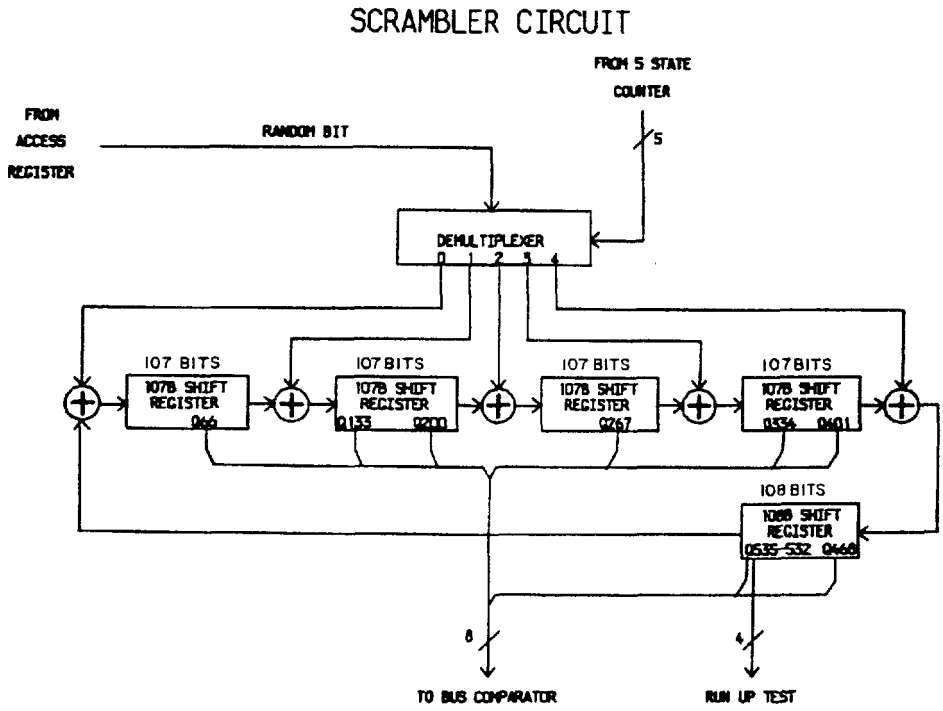


Figure 4

The magnitude of the correlation correction stems from the Gaussian distribution model which can be used for the low frequency oscillator period variations. The Gaussian distribution has the property that a

change in the random variable (the period) yields a like change in the standard deviation. This linear property has been experimentally verified in the case of the on-chip oscillator. If we consider samples taken ten cycles apart, as opposed to successive samples, the standard deviation of the tenth clock edge with respect to the first clock edge is tenfold the standard deviation between successive clock edges. Thus, samples taken many cycles apart have low correlation and the lower the correlation of the samples passing through an exclusive-or network, the lower the probability of predicting the state of the exclusive-or output with any degree of certainty. The spacing of the first five register samples which are exclusive-ored in the circuit of Figure 4 is shown in Table 2.

SCRAMBLER REGISTER CONTENT AFTER 2680 SAMPLES

REGISTER NUMBER	CONTENT
1	307+736+1700+2129+2558
2	413+842+1271+2235+2664
3	90+519+948+1377+1806
4	625+1054+1483+1912+2341
5	196+1160+1589+2018+2447
6	302+731+1695+2124+2553
7	408+837+1266+2230+2659
8	85+514+943+1372+1801
9	620+1049+1478+1907+2336
10	191+1155+1584+2013+2442
11	297+726+1690+2119+2548
12	403+832+1261+2225+2654
13	80+509+938+1367+1796
14	615+1044+1473+1902+2331
15	186+1150+1579+2008+2437
16	292+721+1685+2114+2543
-	-
107	308+737+1166+2130+2559
-	-

The symbol + stands for an exclusive-or operation.

Table 2

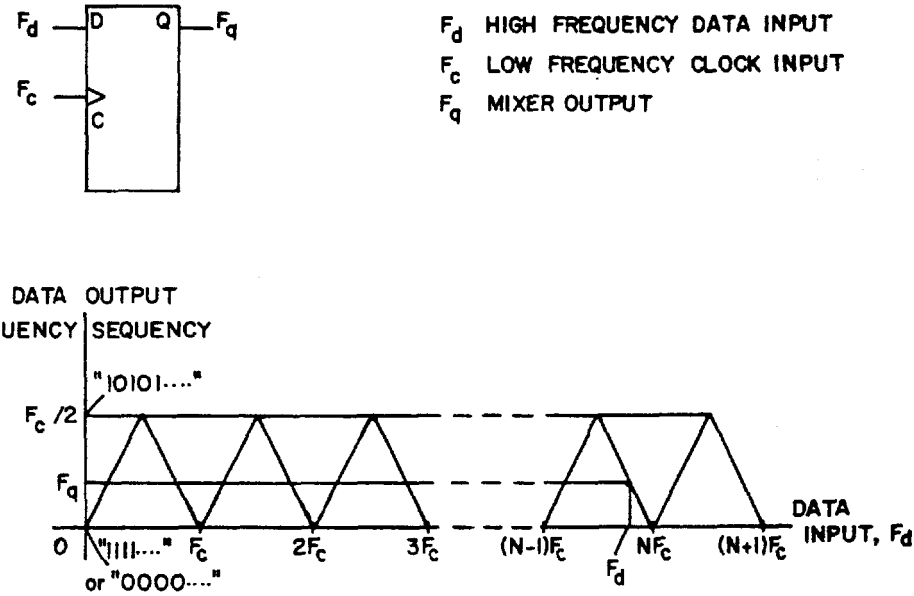
The table should be read as follows: After 2680 samples have been input to the scrambler, the content of scrambler register one is the exclusive-or sum of the 307th, 736th, 1700th, 2129th, & 2558th samples. As is evident from Table 2, the registers in the scrambler contain the exclusive-or sum of samples generated 429 or 964 clock cycles apart or the exclusive-or sum of independent samples. Also upon examination of registers 1 and 107 it is apparent that pairs of successively generated bits do tend to accumulate in pairs of registers. However, this pair accumulation is not complete in that one pair of bits in registers 1 and 107 are samples which are generated 534 clock cycles apart. Samples generated 534 cycles apart are independent. Looking down the register contents we see that the closest correlation exists between registers spaced five apart since they contain pairs of samples all of which are generated five clock cycles apart.

One item to note is that as signals feed into the scrambler and are exclusive-ored with other samples, the duty cycle bias correction is enhanced. Actually, the parity filter shown in Figure 2 is not necessary and if it were removed from the IC, the generation and accumulation of a random number in the scrambler circuit would occur four times faster.

EXPERIMENTAL RESULTS

The effects of frequency instabilities on the digital mixing operation is best illustrated through the digital mixer transfer function shown in Figure 5. At the output of the mixer it is most appropriate to speak of output sequency as opposed to the output frequency. One can speak of the mixer output frequency only in the sense of the fixed number of transitions which occur in a given period for, in general, the transitions are not evenly spaced in time. Thus, we speak of output sequency or the output patterns generated. As evident from Figure 5, the transfer function of the digital mixer is a periodic function with period equal to the frequency of the clock input. The output sequency varies from: a steady string of "ones" or "zeros" when the data lead frequency is an integral multiple of the clock; to the most rapidly varying sequence of alternating "ones" and "zeroes" which occurs when twice the data lead frequency is an odd integral multiple of the clock frequency. At other data lead

frequencies, different patterns are generated.



MIXER TRANSFER FUNCTION

Figure 5

In the presence of clock lead frequency or period fluctuations, the digital mixer output sequency fluctuates. In the current application one would like the frequency fluctuations to be large enough to cover all possible output patterns. Of course, this in general will not occur. To determine what will occur one must know the extent of the fluctuations of the oscillators being used. Two types of parameters are generally of interest in describing oscillators: the short term or instantaneous frequency variations and the long term frequency drift. Figure 6 shows the experimentally measured (short term) fluctuations of the on-chip RC oscillator at two different frequencies. Figure 7 shows the effects of the measured low frequency period variations on the output sequency given a data lead frequency in the vicinity of 8.1 MHz. In Figure 7, the mixer transfer characteristics for the experimentally measured clock oscillator frequencies are plotted about the high frequency data lead operating point. The solid lines represent the mixer characteristic with the clock frequency set to its nominal value minus the standard deviation and the dashed lines

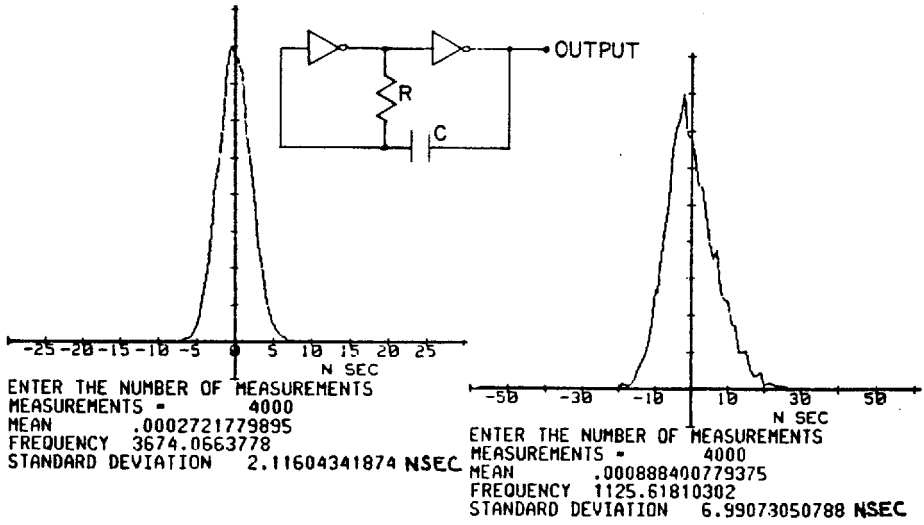


FIGURE 6 LOW FREQUENCY OSCILLATOR CHARACTERISTICS

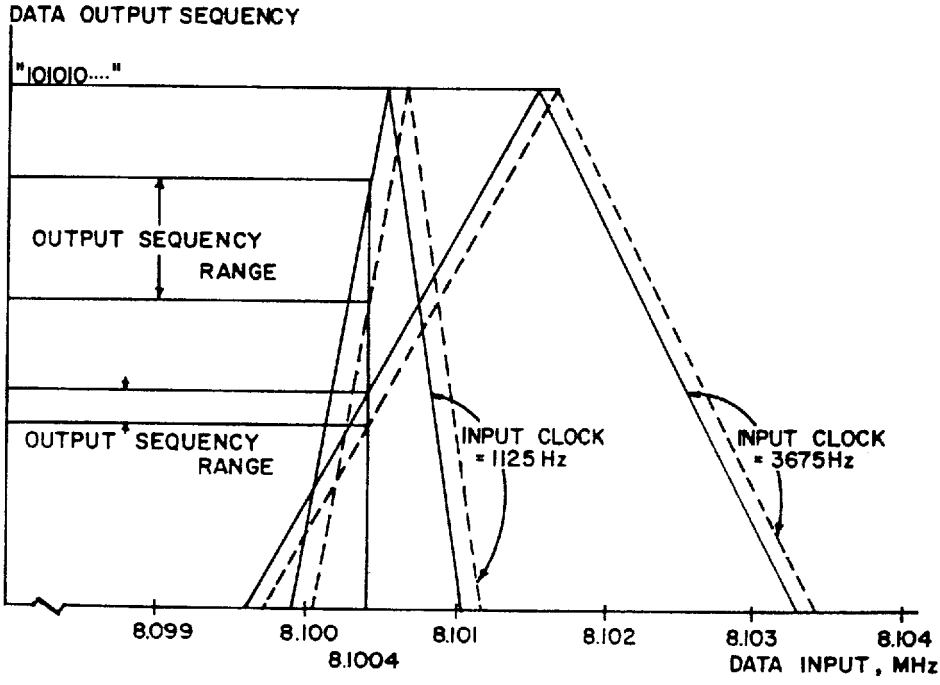


FIGURE 7 MIXER RESPONSE TO FREQUENCY INSTABILITY

represent the characteristic for the clock set to its nominal value plus the standard deviation. For a completely stable high frequency, only a portion of the possible output patterns are covered by the frequency variations. For the 3.674 KHz signal, approximately 7% of the possible patterns will be generated while for the 1.125 KHz signal, approximately 23% of the patterns will be generated. This, of course, indicates that the lower clock frequency is more desirable for the generation of the random number. Figure 8 shows the long term drift of the on-chip RC oscillator mean frequency when operating about 1.125 KHz.

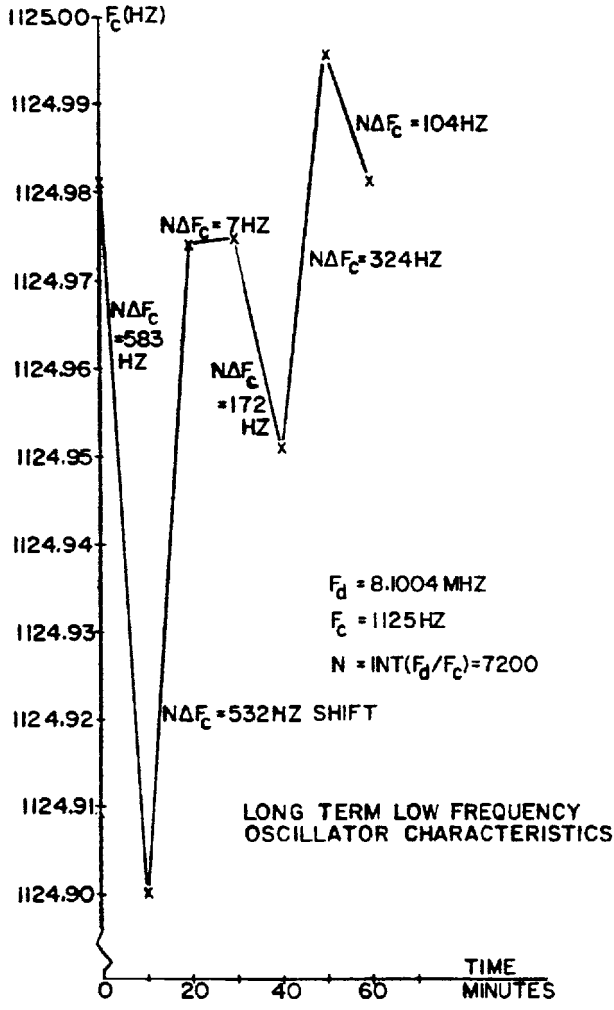


Figure 8

This variation translates to an almost 700 Hz shift in the transfer function about the 8.1 MHz clock. Thus, over a long period of time (hours) one can expect the operating point to be uniformly distributed over all possible patterns.

Figure 9 shows the power spectrum of the data coming out of the IC's D-type flip-flop mixer.

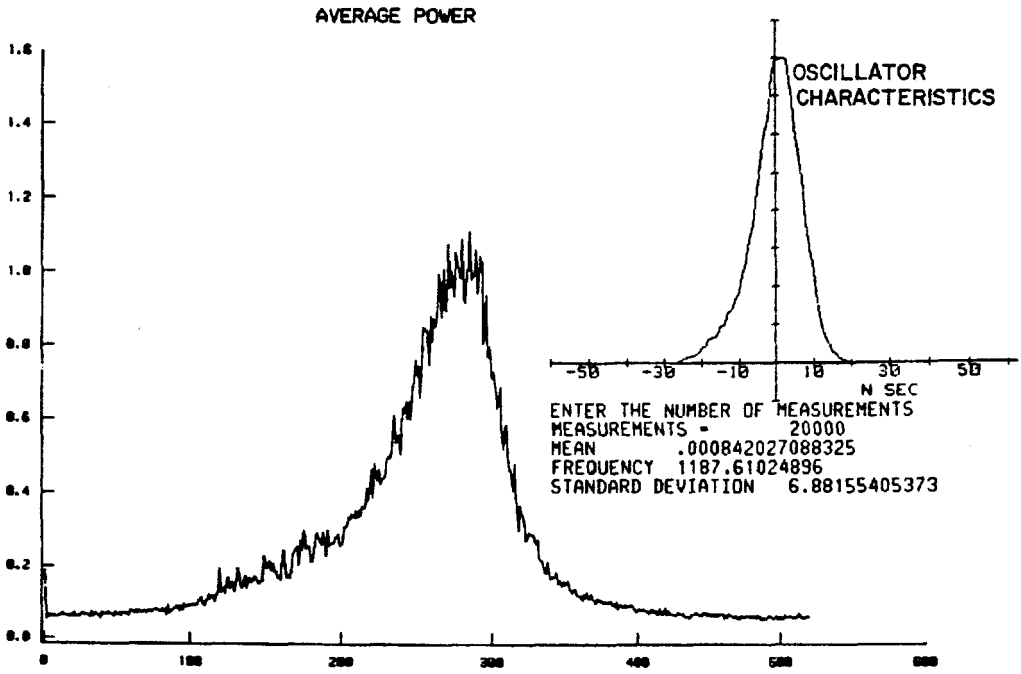


Figure 9

Data was broken up into blocks of 1024 nonoverlapping samples and the power spectrum was estimated and averaged over a file of approximately a quarter of a million points. One sees that the power is confined to a band of frequences (sequencies) about some mean. Figure 10 shows the power spectrum after exclusive-oring adjacent samples and scrambling groups of five bits as the scrambler circuit of Figure 4 would. One sees that after scrambling the energy is uniformly spread over all frequencies as it should be for a truly random bit stream.

Figure 11 shows the power spectrum of a second set of D-type flip-flop mixer samples. This time the spectrum is centered about a different mean frequency and the deviation from the mean is smaller. Also, one sees a d.c. term indicating a local bias (within 1024

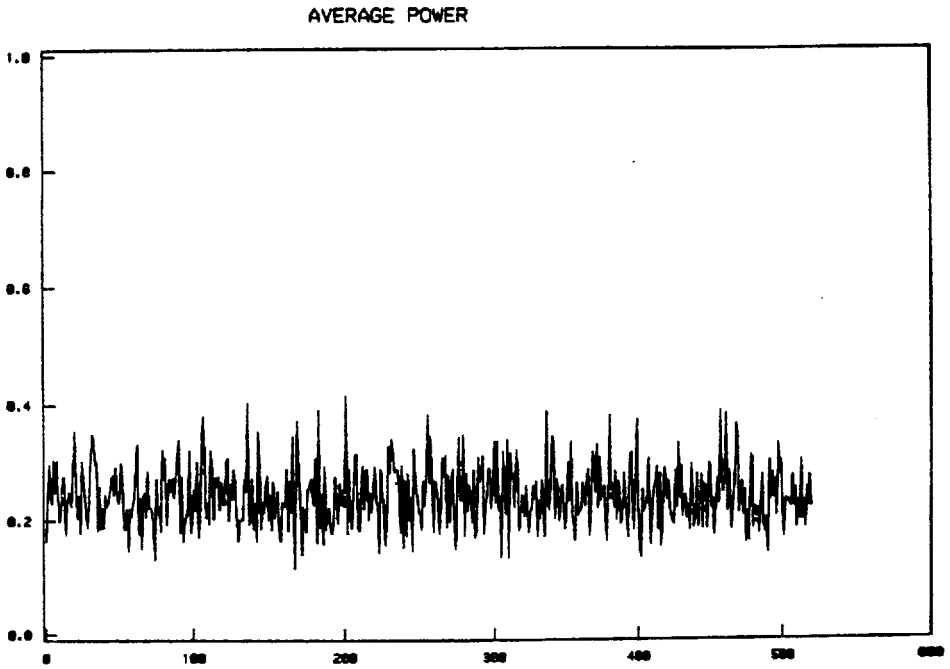


FIGURE 10

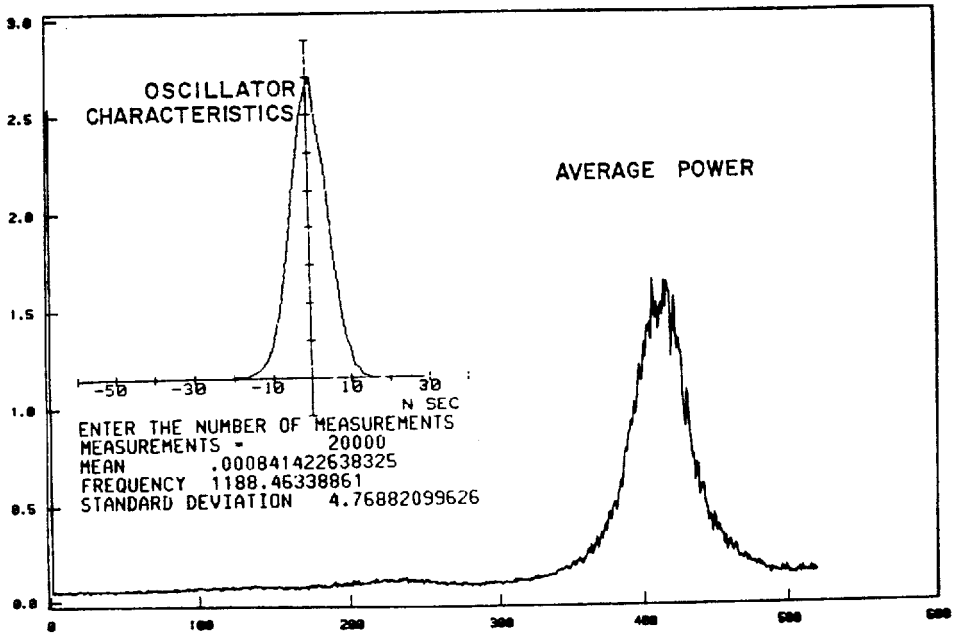


FIGURE 11

samples) in the data toward either a "one" or a "zero". Figure 12 shows the data after adjacent bits are exclusive-ored and scrambled. Note, a d.c. component is still present. This component is removed with additional scrambling of bits. In actual IC operation, each register in the scrambler will contain the exclusive-or sum of a minimum of nine samples before the user can remove a random number from the device. This amount of scrambling removes the d.c. component seen in Figure 12. Figure 13 shows the effect of scrambling five bits without first exclusive-oring adjacent terms. Note that there is no d.c. term in this spectrum. This indicates that the IC would perform better if adjacent bits were not exclusive-ored before they were fed into the scrambler.

RNG INTEGRATED CIRCUIT FEATURES

1. 8 bit bidirectional Data Bus.
2. Separate Read (RD~), Write (WR~) and Chip Select (CS~) inputs. Note: The ~ is used here and in the following text to designate the complement or inverse of a signal.
3. 3 bit input Address Bus.
4. Generation of a 536 bit random number accessible in sixty-seven, eight bit bytes.
5. Elementary randomness check via internal 4 bit "run-up" test, during which time a random number is accumulating in the scrambler. External access to statistics generated, i.e., not just a pass fail test. "Run-up" test limits programmed through the host processor. This test may be used to verify the internal circuitry.
6. Internal verification that the data generated and stored in the RNG is the same as the data appearing on the data bus during a microprocessor read of the device.
7. Use of on-chip oscillators or external signals.
8. Output flags, Data Ready and Alarm, may be read from the data bus or on independent output pins. This enables either processor interrupt or processor polled systems to be configured.

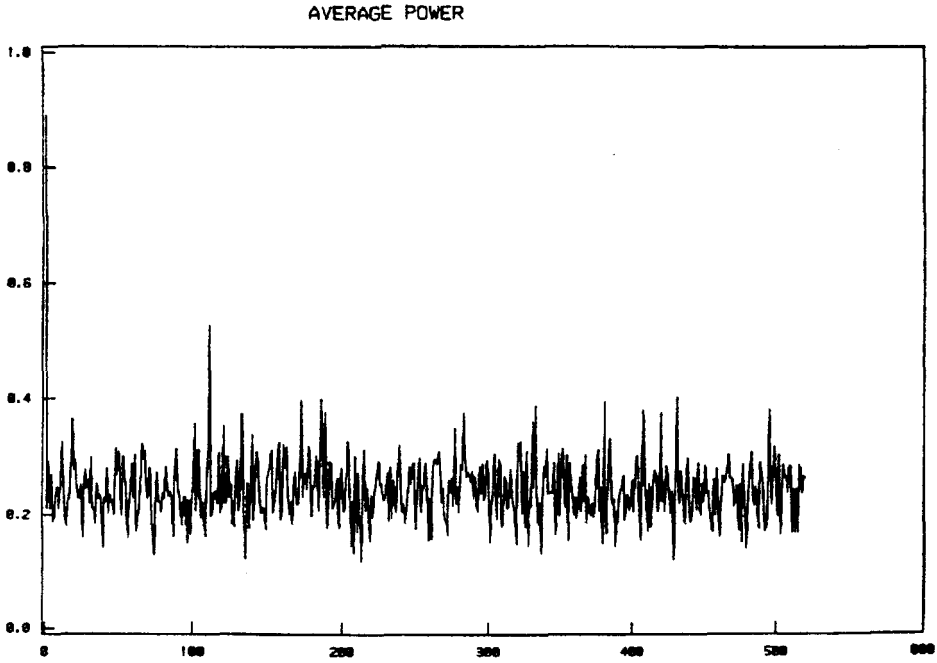


FIGURE 12

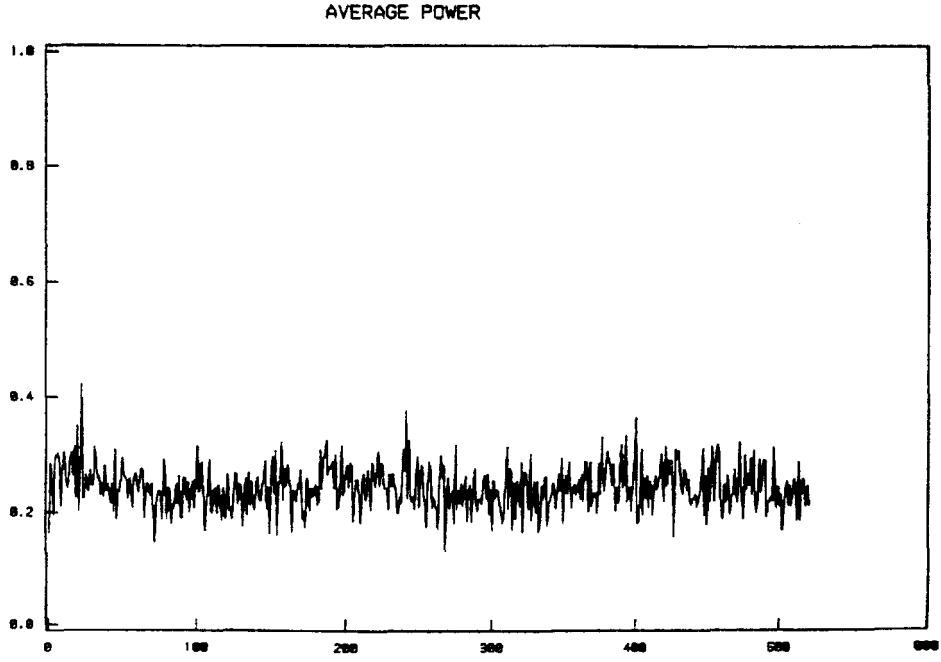


FIGURE 13

RNG OPERATION

The block diagram of the RNG is shown in Figure 14. The device is configured to appear as a standard microprocessor peripheral. There are eight internal registers for control and/or status reporting. All of these registers may be read. The Upper and Lower Limit Registers, used in a "run-up" test, plus the Status/Command Register control device operation and must be written to, by the host processor, before proper operation can begin.

Following device initialization by the controlling processor, random number generation is initiated with a master reset pulse. Ensuing this master reset, random bits are generated and fill the 536 bit (67 byte) Random Data Byte Register. Following the initial fill, a "run-up" test (described below) is executed on the last four bits in the shift register. If the test passes, the Data Ready flag goes active and the host processor can address the Random Data Byte Register to read the 67 bytes. At the end of the sixty-seventh read pulse, the device automatically behaves as if a new master reset pulse was received. If the "run-up" test fails, the Data Ready flag remains inactive, the Alarm flag goes active and any attempt to read the random data bytes is inhibited. The alarm condition remains active until a Master Reset is issued. Access to the Random Data Byte Register continues to be denied until a "run-up" test is passed.

During any read operation of the random data bytes, the number output to the data bus is checked against the number stored in the shift register and a Bus Error flag goes active if there is any discrepancy. This flag state may be read directly from the Status/Command Register or on the output Alarm pin; it indicates a catastrophic condition due to hardware failure.

RUN-UP AND SELF TEST

During a run-up test the last four bits in the shift register are compared to the output from a 4 bit Pattern Counter. If both bit patterns match, an Event Counter is incremented. At the end of one thousand non-overlapping four bit tests on a fixed pattern, the result accumulated in the Event Counter is compared to the contents of the Upper and Lower limit registers. If the event count is outside the stored limits the test fails. It takes approximately 20 seconds to

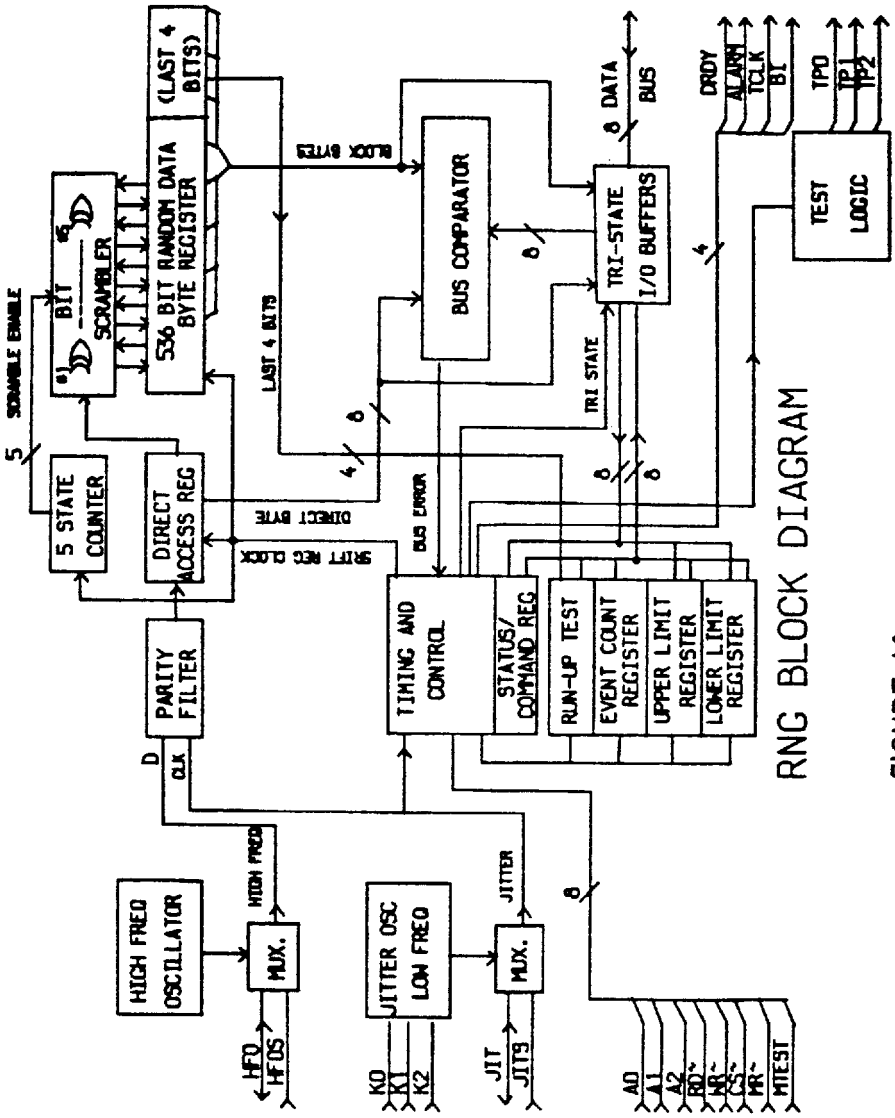

RNG BLOCK DIAGRAM
SCRAMBLE ENABLE
5
5 STATE COUNTER
BIT SCRAMBLER
536 BIT RANDOM DATA BYTE REGISTER
(LAST 4 BITS)
BLOCK BYTES
LAST 4 BITS
DIRECT ACCESS REG
DIRECT BYTE
SHIFT REG CLOCK
BUS COMPARATOR
BUS ERROR
TRI STATE
TRI-STATE I/O BUFFERS
8 DATA BUS
DRDY
ALARM
TCLK
BT
TPO
TP1
TP2
TEST LOGIC
TIMING AND CONTROL
STATUS/ COMMAND REG
RUN-UP TEST
EVENT COUNT REGISTER
UPPER LIMIT REGISTER
LOWER LIMIT REGISTER
PARITY FILTER
D
CLK
HIGH FREQ OSCILLATOR
MUX.
HIGH FREQ
HFO
HFOS
JITTER OSC LOW FREQ
JITTER
K0
K1
K2
JIT
JITS
A0
A1
A2
RD~
WR~
CS~
HR~
MTEST

FIGURE 14

execute a "run-up" test with the low frequency jitter oscillator set to 1 KHz. If a different frequency is used, be it from the internal or an external source, the testing time may be computed by multiplying the Jitter oscillator period by 20,096. At the end of a "run-up" test, every scrambler register location will be the exclusive-or sum of either nine or ten data bits coming from the parity filter.

If the random bits are independent with P(1)=P(0)=0.5 the probability of any 4 bit pattern is simply 0.0625 and the expected event count for 1000 samples is 62.5. The event count has a binomial distribution with a standard deviation of 7.65. Using the normal approximation to the binomial distribution, the probability of a test failing can readily be computed. For example, if the limits are set at plus and minus twice the standard deviation, the probability of the test failing is 0.0456 (taken from a table of values of the Standard Normal Distribution Function). At plus and minus three times the standard deviation, the probability of the test failing is 0.0026. In the device structure, the upper and lower limits are entered and appear in registers as hex integers. This test will distort the random numbers coming out of the device by eliminating patterns having very low probability. To prevent this, the upper limit register can be loaded with FF (255) and the lower limit register with 00. With these limits, the test will never fail. The run-up test may be used to completely test the deterministic circuitry by using the "Alarm Test" circuitry explained in the next section.

At this point it is worth talking about oscillator failure and its detection. If the low frequency oscillator were to fail, device operation would halt since that oscillator is used to clock the entire chip. The Data Ready flag would never go active. If the high frequency oscillator were to fail either high or low, the output of the parity filter would be all zeroes. Hence, to check for a high frequency failure the run-up test may be used with the limits set to 01 and FE (254). A master reset must be issued before running the test in order to set the scrambler register to zero. If the oscillator were stuck, any of the 16 possible patterns would fail. The chance of a fully operating device failing under these conditions is

$$1 - 6.22 \times 10^{-16}, (8\sigma)$$

Therefore, it may be a good idea to normally operate the device in this manner.

REGISTERS

There are eight addressable registers. Figure 15 defines data port output during a register read operation.

RANDOM NUMBER GENERATOR READ OPERATION

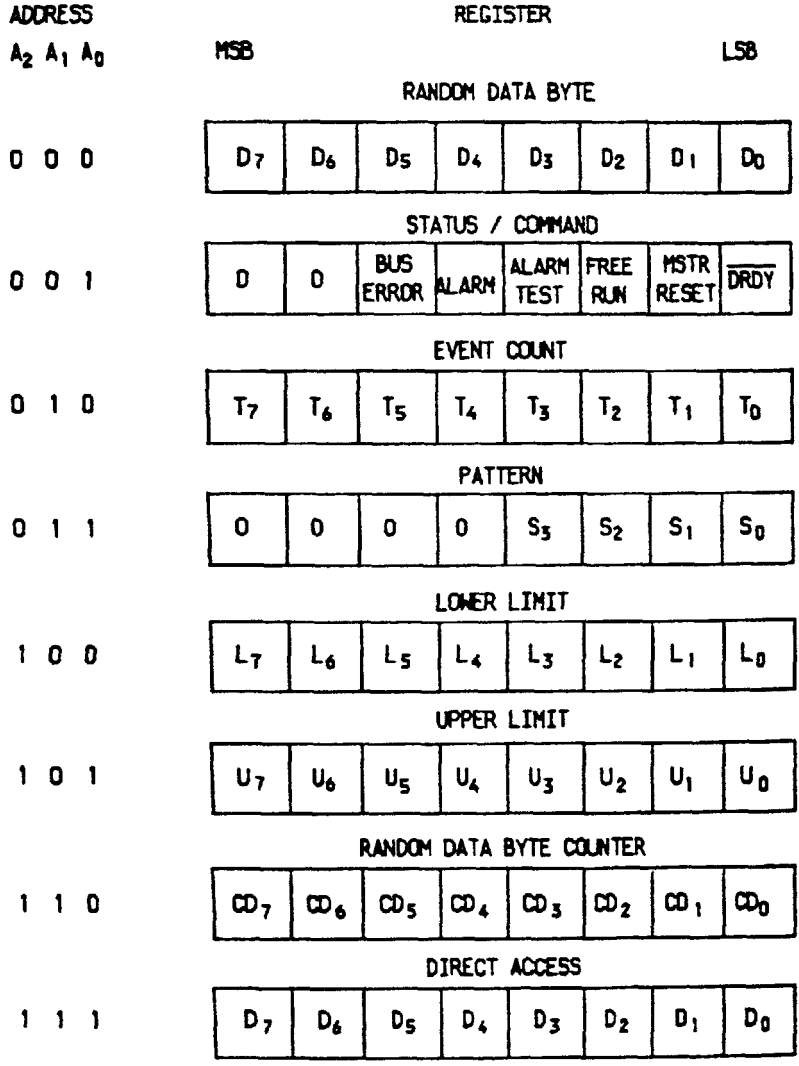


Figure 15

Figure 16 defines data port input during a write operation.

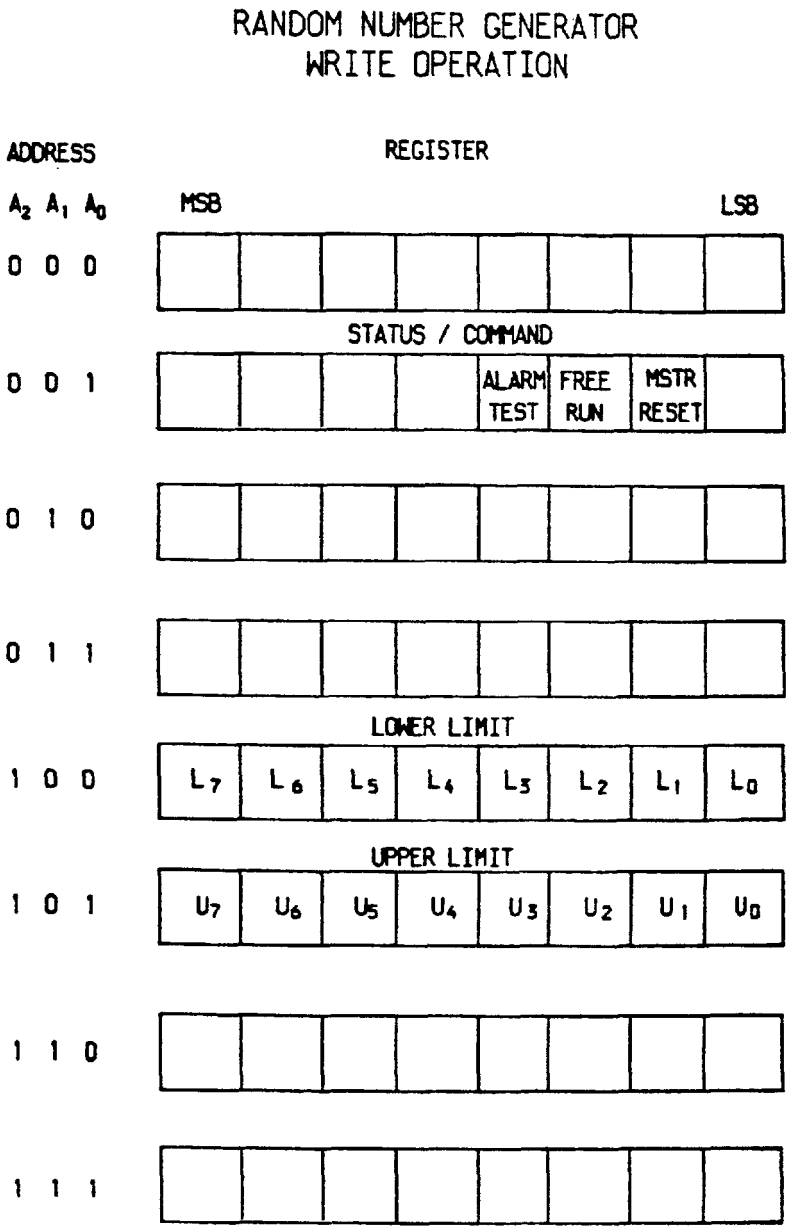


Figure 16

1. Address 0 selects the read only Random Data Byte Register. Sixty-seven read pulses empties the shift register. After emptying the shift register the "run-up" test cycle begins again. If less than 67 read pulses are input, the device will remain inactive waiting for the remaining pulses unless a Master Reset is issued. Addressable register 6 is a down counter and keeps track of the number of random bytes remaining in the shift register.

2. Address 1 selects the read/write Status/Command Register and must be written to, before certain device operations can begin.

   A. Bit 0 of the Status/Command Register is a read only, active low, Data Ready flag (DRDY~) used to indicate a "run-up" test has passed and a 67 byte random number is stored in the Random Data Byte Register (Address 0). This flag remains active until: all 67 random data bytes have been read, a bus error is detected, or a Master Reset is issued. This information is also available on the Data Ready output pin.

   B. Bit 1 of the Status/Command Register is a read/write, active high, Master Reset command. If active, a Master Reset condition exists until this bit is cleared by pulsing the external Master Reset pin or by writing a "0" to this bit. A master reset clears the scrambler.

   C. Bit 2 of the Status/Command Register is a read/write, active high, Free Run command (FR). In the inactive state, the device executes a single "run-up" test and halts operation. If the test passes, the Data Ready flag goes active and all 67 random data bytes must be read (or a Master Reset issued) before a second "run-up" test is begun. If Bit 2 is set active, the device continually executes "run-up" tests. The Data Ready flag will go active after the first "run-up" test passes and remain active until a failure. Once this flag has gone active, data can be read from the Random Byte Register. During the reading of the Random Byte Register, "run-up" tests temporarily cease. That is, with the first read pulse accessing the Random Byte Register, the current "run-up" test halts. After the sixty-seventh read pulse which

empties the Random Byte Register, "run-up" tests start anew. When a failure occurs the Alarm flag goes active, the Data Ready flag goes inactive, and any attempt to read from the Random Byte Register is inhibited. An Alarm condition can only be cleared by a Master Reset. Bit 2 can be set at any time during chip operation. An external Master Reset pulse clears bit 2, but an internal Master Reset has no affect.

D. Bit 3 of the Status/Command Register is a read/write, active high, Alarm Test command (ALRMT). If active, a known sequence of zeros and ones is automatically loaded into the Random Byte Register producing known pattern counts for the "run-up" test. The counts which are generated are given in Table 3.

Alarm Test Register Data							
Pattern (Hex)	Event Count (Hex)	Random Data Byte Register					
		Byte Number	Byte (Hex)	Byte Number	Byte (Hex)	Byte Number	Byte (Hex)
		1	71	23	E8	45	C9
0	A0	2	F0	24	A1	46	61
1	21	3	EC	25	C8	47	B0
2	4E	4	A1	26	73	48	E0
3	25	5	58	27	B0	49	A1
4	55	6	73	28	E8	50	C9
5	3B	7	F0	29	A1	51	61
6	15	8	EC	30	C8	52	B0
7	4E	9	A1	31	73	53	A2
8	28	10	58	32	B0	54	A1
9	52	11	73	33	E0	55	C9
A	42	12	F0	34	A1	56	61
B	38	13	E8	35	C8	57	B0
C	1D	14	A1	36	73	58	A2
D	3F	15	58	37	B0	59	A1
E	47	16	73	38	E0	60	C9
F	2A	17	B0	39	A1	61	41
		18	E8	40	C8	62	B0
		19	A1	41	61	63	A2
		20	58	42	B0	64	A9
		21	73	43	E0	65	C9
		22	B0	44	A1	66	41
						67	B0

Table 3

This test is used to check the "run-up" and alarm circuitry. It can also be used to produce a known pattern

in the Random Byte Register which can be read out if desired. This pattern is also listed in Table 3. In order for this test to operate correctly the device must be first cleared with the internal Master Reset command (set bit 1). Then, on a subsequent write cycle, the internal master reset command bit must be cleared simultaneously with the Alarm Test bit being set. Bit 3 is cleared with an external Master Reset (internal Master Reset has no affect).

E. Bit 4 of the Status/Command Register is a read only, active high, Alarm flag (ALRM). If active, a "run-up" test has failed. An active Alarm flag will inhibit device operation and can only be cleared by a Master Reset. This information is also indicated by an active Alarm flag pin.

F. Bit 5 of the Status/Command Register is a read only, active high, Bus Error flag (BE). If active, there has been a discrepancy between the data in the Random Data Byte Register and the data appearing on the eight bit bidirectional Data Bus during a read of the register. An active Bus Error flag will inhibit device operation and can only be cleared by a Master Reset. This information is also indicated by an active Alarm flag pin.

G. Bits 6 and 7 of the Status/Command Register are unused and always low.

3. Address 2 selects the read only Event Count Register. This register stores the hex event count from the most recently completed "run-up" test. This is an eight bit register and the maximum count it can display is decimal 255. A reading less than 255 (hex FF) indicates the actual event count obtained during the last "run-up" test while a reading of 255 indicates an event count of 255 or more.

4. Address 3 selects the read only Pattern Register. This register stores the 4 bit hex pattern associated with the most recently completed "run-up" test. At the completion of every successful "run-up test, the pattern counter is incremented. If the "run-up" test fails, the pattern is not changed and the test is repeated following a Master Reset. Master Reset does not affect this counter. In power up this counter assumes an arbitrary

state and increments from there.

5. Address 4 selects the read/write Lower Limit Register. This register stores the hex lower limit associated with the "run-up" test and must be written to before proper operation of the device can begin.

6. Address 5 selects the read/write Upper Limit Register. This register stores the hex upper limit associated with the "run-up" test and must be written to before proper operation of the device can begin.

7. Address 6 selects the read only Random Data Byte Counter Register. This down counter register keeps track of the number of random bytes left in the shift register (Address 0). Following an active Data Ready signal, this register is preset to hex 43 (67 decimal). After the 67 random data bytes have been read, this register is at hex 0 and remains there until the next active Data Ready signal.

8. Address 7 selects the read only Direct Access Register. This register along with the TCLK pin allows the user to continually monitor the random data byte at the input to the scrambler. The random data is latched into this register on the rising edge of the TCLK signal and it can be read after this edge. If the internal random bit generator is used at 1KHz, the TCLK period is approximately 32 milliseconds. Using a different jitter frequency or an external source, the TCLK period may be computed by multiplying the Jitter oscillator period by 32.

   Data read from this register has not been subjected to the bit scrambler and may have high bit to bit correlation. Thus, this data should not be used in place of data obtained from the Random Byte register as a random number but should only be used for device monitoring and/or testing.

PIN DESCRIPTION

Figure 17 shows the RNG pin configuration.

1. VDD This is the +5 volt power supply input.
2. GND Ground.

3. MR~ Master Reset is used to clear the RNG when the Chip Select line is active. The control bits in the Status/Command Register (Address 1) are all set inactive, the Event Count Register is set to zero, the scrambler is cleared, and a test sequence is begun on the rising edge of the reset pulse. The Pattern Register (Address 3), Lower Limit Register (Address 4), and Upper Limit Register (Address 5) are unaffected.

RANDOM NUMBER GENERATOR
PIN DIAGRAM

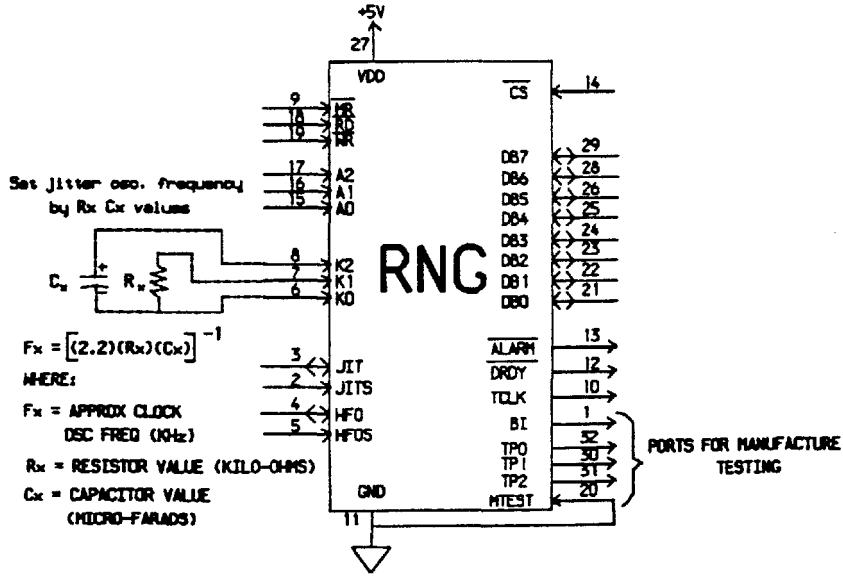


Figure 17

4. RD~ Read is an active low input used with the Chip Select, the Address Bus, and the Data Bus to read one of the eight internal registers. The data appears on the bus following the falling edge of the pulse and remains on the bus as long as RD~ is low. The Write input should be held inactive during a Read pulse.

5. WR~ Write is an active low input used with the Chip Select, the Address Bus, and the Data Bus to write to one of three internal registers. The data is latched into the addressed register on

the rising edge of the Write pulse. The Read input should be held inactive during a Write pulse.

6. A2 - A0 The Address Bus input is used to select an internal register for a read or write operation.

7. DB7 - DB0 The Data Bus, an eight bit bidirectional port, is used to read data from or write data to the internal registers. The output buffers driving the eight bit bus are in a high impedance state if either CS~ or RD~ are inactive.

8. CS~ Chip Select is an active low input. When active MR~, RD~, and WR~ are enabled; when inactive these inputs are disabled.

9. ALARM~ Alarm flag is an active low output used to indicate either a "run-up" test failure or a bus error. Both of these conditions may also be read from the Status/Command Register (Address 1). An active Alarm flag may only be cleared by a Master Reset.

10. DRDY~ Data Ready flag is an active low output used to indicate a "run-up" test has passed and a 67 byte random number is stored in the Random Data Byte Register. This flag may also be read from the Status/Command Register (Address 1). Following the rising edge of the sixty-seventh RD~ pulse, with the Random Data Register addressed (Address 0), the DRDY~ flag goes inactive.

11. TCLK Test Clock is an output used with the Direct Access Register to monitor the random data at the input to the Random Data Byte Register. The random data is latched into the Direct Access on the rising edge of the TCLK signal and it can be read after this edge. Using the internal random bit generator (with jitter osc. set to 1KHz), the TCLK period is approximately 32 milliseconds. Using a different oscillator frequency or an external source, the TCLK period may be computed by multiplying the Jitter oscillator (JIT) Register period by 32.

12. HFOS This pin controls a switch that determines the high frequency source for the chip: when HFOS is "0", the internal high frequency oscillator is used (about 8MHz); when HFOS is 1, an external oscillator is expected at the HFO pin. It is recommended that an external high frequency square wave be used for critical applications (possibly the system clock).

13. HFO This pin is bi-directional and serves two purposes: when HFOS is "0", HFO serves as an output for viewing the internal high frequency oscillator; when HFOS is 1, HFO serves as an input for an external high frequency oscillator.

14. JITS This pin controls a switch that determines the jitter input source for the chip: when JITS is "0", the internal jitter oscillator is used; when JITS is 1, an external oscillator is expected at the JIT pin.

15. JIT This pin is bi-directional and serves two purposes: when JITS is "0", JIT serves as an output for viewing the internal jitter oscillator when JITS is 1, JIT serves as an input for an external jitter oscillator.

16. BI This pin monitors the output of the first sampling D-type flip-flop at the front end of the parity filter. HFO is the data into the positive-edge-triggered flip-flop and JIT is the clock.

17. K0, K1, K2 These leads are used to attach the external resistor and capacitor which control the frequency of oscillation of the on-chip jitter oscillator. The frequency of oscillation is approximately given by

$$f \approx 1/(2.2RC)$$

The resistor is connected between K0 and K1 while the capacitor is connected between K0 and K2.

18. TEST PINS used for manufacture purposes: MTEST This pin should always be grounded when in normal use. This is only used for manufacturing tests. TP0,TP1,TP2 These are only used for manufacturing tests and should remain floating since they are outputs.

CONCLUSIONS

An LSI CMOS random number generator which generates a truly random binary number has been described. The fundamental mechanism generating the random bit stream is based on a previously documented physical phenomenon and this paper has tried to quantify the magnitude of the parameters governing device performance. Statistical tests

have been run on device output and no problems have been observed for sampling oscillator frequencies (Fc) below 2 KHz. Although it takes almost 20 seconds to generate a 67 byte number when a 1000 Hz sampling clock is used, the generation can be done in the background after power-up or during a session so that keys and/or initial values are available on request. This is the first integrated device of its type that we are aware of and it should solve the problem of generating cryptographic keys and/or initial values in cryptographic systems.

REFERENCES

[1] The RAND Corporation, "A Million Random Digits with 100,000 Normal Deviates", The Free Press, New York.

[2] Motorola Data Book, "Phase-Locked Loop Systems", Motorola Semiconductor Products Inc., second edition, August, 1973.

[3] Asad A. Abidi and Robert G. Meyer, "Noise in Relaxation Oscillators", IEEE Journal of Solid-State Circuits, Vol. SC-18, No 6, December 1983.