TUNDRA

RBG 1210

RANDOM BIT GENERATOR

- Operational speeds up to 20,000 bits/second
- Each value is independent of all other values
- No seed value required
- No hardware/software algorithms required
- Based on Johnson Noise phenomenon
- Single 12 Volt supply
- TTL compatible I/O
- Shielded package

APPLICATIONS

- Encryption Systems
- Statistical Analysis
- Password Generation
- Seed Generator
- Fair Selection
- Monte Carlo Analysis
- Natural Phenomenon Simulation

The RBG 1210 Random Bit Generator produces truly random bits. Based on the naturally occurring random phenomenon, Johnson noise, the RBG 1210 requires no initial starting value or seed. Furthermore, each new value is completely independent of all previous values. Unlike digital logic circuits or software based algorithms, the RBG 1210 is not pseudo-random; there is no repeating pattern, giving an infinite cycle size. This makes the RBG 1210 ideal for applications where purely random bits are required.

TTL compatible STROBE and OUTPUT signal pins are provided to allow the RBG 1210 to be easily connected into any digital system.

Table 3-1 : Pin Descriptions

Pin	Function
1	Gnd
2	STROBE
3	OUTPUT
4	+12V

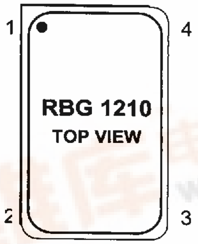

Figure 3-1 : RBG 1210 Random Bit Generator

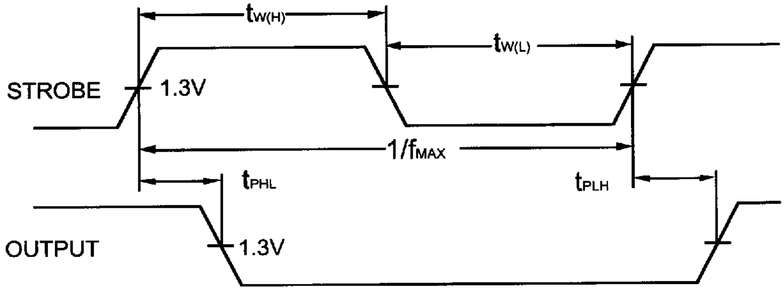

Figure 3-2 : Timing Diagram

Table 3-2 : AC Characteristics (V_{CC} = 0° to 70°C)

Symbol	Parameter	Test Conditions	Limits			Units
			Min	Typ	Max	
f_{MAX}	Maximum strobe frequency	C_L = 15pF	1	-	20	kHz
t_{PLH}	Strobe to output delay		-	13	25	nS
t_{PHL}			-	25	40	nS
$t_{W(H)}$	Strobe width		25	-	-	nS
$t_{W(L)}$	Supply voltage		25	-	-	nS

Table 3-3 : DC Characteristics (V_{CC} = 0° to 70°C)

Symbol	Parameter	Test Conditions	Limits			Units
			Min	Typ	Max	
I_{CC}	Supply current	V_{CC} = 12V	-	-	30	mA
I_{IH}	Input current @ max input voltage	V_{IH} = 7V	-	-	0.2	mA
	High level input current	V_{IH} = 2.7V	-	-	40	μA
I_{IL}	Low level input current	V_{IL} = 0.4V	-	-	–0.8	mA
I_{OS}	Output short circuit current	V_{CC} = 12V	-	-	–100	mA
V_{CC}	Supply voltage		10.5	12.0	16	V
V_{OH}	High level output voltage	I_{OH} = –400μA	2.7	3.5	-	V
V_{OL}	Low level output voltage	V_{IH} = 2V, I_{OL} = 8mA	-	0.4	0.5	V

FUNCTIONAL DESCRIPTION

The RBG 1210 uses a new and different approach to produce random bits which are neither predictable, nor repeatable, unlike computer generated pseudo random numbers, which are both. True randomness occurs naturally in electronic circuits, as evidenced by the background hissing sound heard from radio and audio equipment. Normally, amplifier circuits are carefully designed to minimize this problem. However, in the CA1210 RBG, such amplifier noise has been captured and purposely designed in.

Mathematically, this can be represented as follows. With reference to the noise equivalent circuit of an amplifier shown in Figure 3-3, the total input referred noise density is given by:

$$e_t = \sqrt{e^2 + r^2 + \langle iR \rangle^2} \qquad \left(\frac{V}{\sqrt{Hz}}\right)$$

where: R is the equivalent source resistance (Ohms),

r is the thermal noise of the input resistor $\left(\frac{V}{\sqrt{Hz}}\right)$,

e is the input noise voltage density $\left(\frac{V}{\sqrt{Hz}}\right)$ and

i is the input noise current density $\left(\frac{A}{\sqrt{Hz}}\right)$.

Also $r = \sqrt{4kTR}$

where: k is the Boltzmann constant ($1.38X10^{-23}$ joules/°K) and T is the temperature of the resistor (°K).

The input resistor value is chosen to maximize the contribution of the resistor thermal noise relative to the voltage and current sources. This ensures a wideband noise source with equal noise densities at all frequencies. Thermal noise is due to the random motion of free electrons in the resistor

Figure 3-4 shows a block diagram of the RBG 1210, which consists of a noisy amplifier and an analog to digital converter (A/D). The noise from an input resistor is amplified to about 50mV$_{RMS}$. This white noise signal is then converted to a stream of binary levels by an A/D converter. This A/D is designed to equalize the probability of 1s and 0s, and negate the effects of component parametric tolerances and power supply voltage variations. The output is a standard TTL (transistor-transistor logic) level signal that is latched on the rising edge of the strobe signal.

To produce longer random numbers, one RBG 1210 may be read several times and the resulting bit stream saved until the desired number length has been obtained. A second approach is to connect several RBG 1210s in parallel to produce wider numbers. The serial approach is more cost effective (since only one RBG 1210 is required), while the parallel approach offers a substantial speed advantage, as no delay is incurred after reading each bit.

The NM 810 RNG Random Number Generator is an implementation of the latter approach, with eight RBG 1210s in parallel and a PC XT/AT bus interface. Random bytes are input to the computer through an I/O (Input/Output) port. Any data type (integer, floating point etc.) can then be easily constructed in software by using successive random bytes and arranging them according to the desired internal data format.

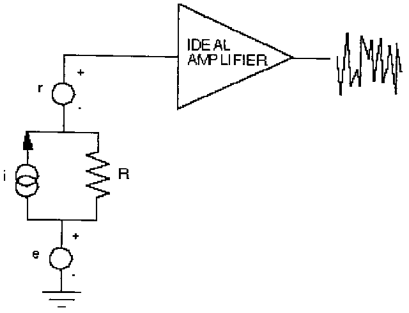

Figure 3-3 : Equivalent Circuit of an Amplifier

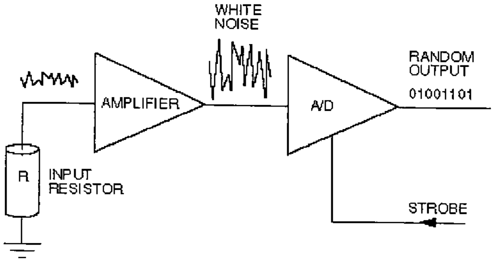

Figure 3-4 : RBG 1210 Block Diagram

TESTING FOR RANDOMNESS

The RBG 1210 Random Bit Generator has been successfully tested for true randomness against an extensive set of recognized tests which include; Chi squared, KS test, frequency test, serial test, poker test, coupon collector test, run test, collision test and picturing randomness. These tests results are available from Tundra Semiconductor Corporation.