

Summary

Tring is a true random number generator (TRNG) that exploits the drift of analog components with temperature, operating voltage, chemistry and quantum effects in order to generate true random numbers. It can generate up to 1 byte per second of true random data.

Tring is firmware for the PIC10F200 microcontroller and is available as a firmware download from www.hexwax.com. Individual devices are programmed in-circuit using the TEAclipper programming clip.

Applications

- Gaming machines
- Encryption key generation
- Random number seed generation
- Stochastic algorithms

Features

- SPI interface
- Invertible sleep control for power saving
- Ultra low cost, low component count
- Based on the PIC10F200 processor
- Available in SOT-23 and DIL packages
- SOT-23 package smaller than 3mm x 2mm
- Industrial and extended temperature ranges
- 2.0V to 5.5V supply
- nanoWatt power when not selected

Functional Diagram

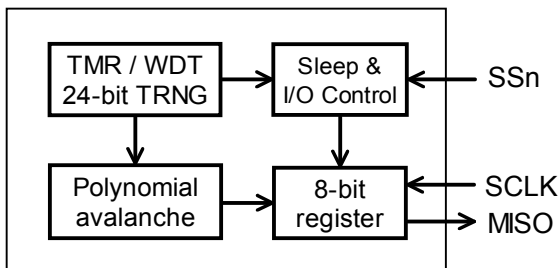
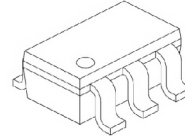
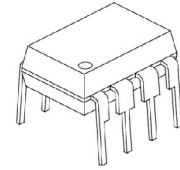


Figure 1 - Functional diagram

Mechanical Specifications



SOT-23



DIL

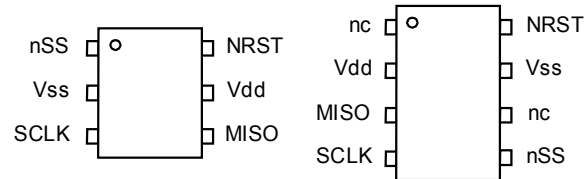


Table 1. Pinout Table

Name	Description
SSn	Slave select (chip select), active low TEAclipper programming pin 2
SCLK	SPI clock input TEAclipper programming pin 3
NRST	Reset, active low, 22K pullup recommended TEAclipper programming pin 4
MISO	SPI data master in / slave out
Vdd	2.0V – 5.5V supply
Vss	Power supply ground

Electrical Specifications

Table 2. Electrical Specifications

Voltage on Vdd (Normal use)	2.0 – 5.5 VDC
Voltage on Vdd during programming	4.5 – 5.5 VDC
Typical supply current, active	175µA Vdd = 2V 630µA Vdd = 5V
Maximum supply current, active	275µA Vdd = 2V 1100µA Vdd = 5V
Typical supply current, sleep	100nA Vdd = 2V 350nA Vdd = 5V
Maximum supply current, sleep	1200nA Vdd = 2V 2400nA Vdd = 5V
Operating Temperature, Industrial	–40°C to 85°C
Operating Temperature, Extended	–40°C to 125°C*

*Higher maximum current figures may apply.

Random Number Generation

The true random number generator exploits the fact that the RC circuit in the watchdog timer is subject to substantial drift with temperature, operating voltage and age. Each random bit is generated by running a calibrated 1MHz timer is run for a period of 18ms, as measured by the watchdog timer. At the end of this period, the least significant bit of the timer is essentially random, being sensitive to 0.005% variations in the watchdog timer period.

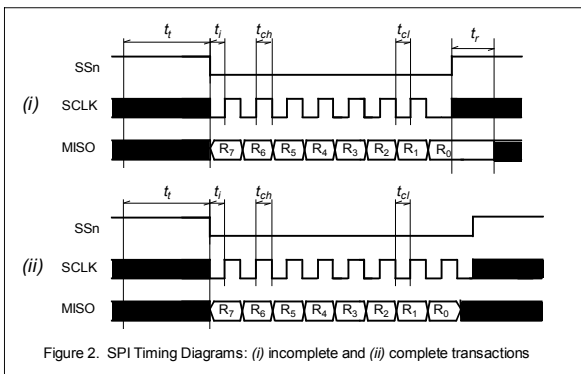
To counter any absolute to temporal distribution bias, 24 such bits are generated. These are then fed into a high-avalanche polynomial ring to derive an 8-bit true random value.

The entire process may take up to 1 second. On power-up, and after each random number is output, a new random number is immediately generated. *Tring* then enters a nanoWatt sleep state until its SPI slave select line SSn is selected and the new random number is clocked out.

SPI Interface

The SPI interface should clock out random numbers no sooner than one second after either the last random number output or power-up event.

Referring to figure 3, SSn transitions from high to low and then the host clocks in up to eight bits of data on MISO. If all 8 bits are output, MISO will immediately enter a high-impedance state regardless of the state of SSn. If SSn goes high before the eighth bit has been output, MISO will release the line within a time t_r .



The *NRST* input is an active low reset. During normal operation and programming it should be connected to Vdd via a 22K pull-up. As with all microcontroller circuits, a 100nF decoupling capacitor is recommended across, and as close as possible to, the Vss and Vdd pins.

The SPI interface on *Tring* is implemented in firmware rather than hardware, placing strict limitations on the speed of communications. Refer to table 3 for timing details.

Name	Value	Description
t_t	1 s	Minimum time since power-up or last random number output
f_{clk}	40 kHz	Maximum clock frequency [$=1/(t_{cl}+t_{ch})$]
t_{ch}, t_{cl}	12.5 μ s	Minimum clock high / low time
t_i	20 μ s	Minimum initialization time
t_r	20 μ s	Maximum MISO release time

Refer to figure 2 for interpretation of these values

Slave Select / Sleep

SSn must be held low continuously for an entire transaction to complete successfully. It may, however, be taken high at any time.

When SSn is high and the next random number has been generated, *Tring* will enter a low power sleep state. MISO will enter a high impedance state within a time t_r . For minimum power consumption, SCLK and MISO should be biased high or low when not in use to avoid unnecessary waking.

Firmware Delivery

The *Tring* firmware is available as an encrypted firmware download from www.hexwax.com. To download it you will need a TEAclipper/PIC HV and a TEAclipper/USB adapter.

To load the firmware onto the TEAclipper, start the HexWax Explorer firmware and log in. Then download the *Tring* firmware pack from the hexwax.com products section. When download completes, a *Tring* folder will appear in the Local Files section of HexWax Explorer. In this folder is the *Tring.wax* file which contains the firmware.

You will need *Tring* license credits in order to decrypt the *Tring.wax* file. Contact hexwax.com for details of payment options and how to obtain free samples.

Once you have license credits, select the *Tring.wax* file and insert a TEAclipper/PIC HV into the TEAclipper/USB adapter. Press the *Charge Now...* button. Referring to figure 3, select how many licenses you wish to load onto the TEAclipper. Finally press OK to obtain a decryption key and to charge the TEAclipper with the decrypted firmware.

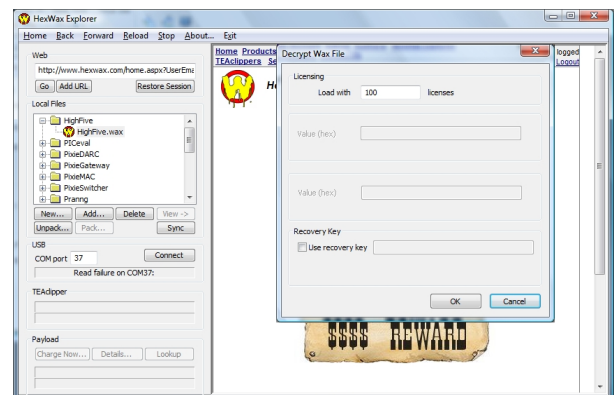


Figure 3: Decrypting the *Tring.wax* file

Programming Tring

Tring may be programmed in-circuit provided the programming signals are protected against contention. In particular, note that the *NRST* line is subject to a voltage of 13V during programming. The recommended circuit is shown in figure 4.

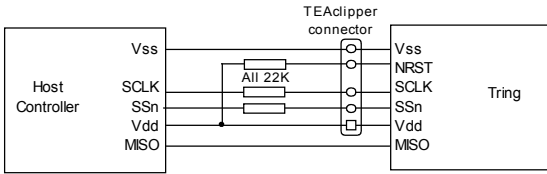


Figure 4. Recommended connection to permit in-circuit programming

Tring is programmed into the microcontroller simply by inserting the TEAclipper into its connector. The circuit must be powered and the TEAclipper must be held in place until the LEDs stop flashing and the green LED glows steadily. Since the programming time is very fast, no programming socket is required for the TEAclipper. It may be leaned against five plate-through holes as depicted in figure 5.

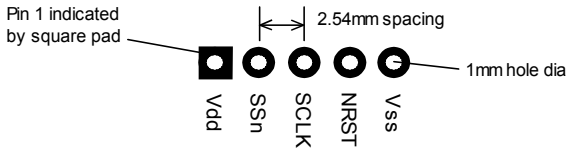


Figure 5. Recommended plate-through connector design

The TEAclipper requires a minimum supply to the Tring of 4.5V during programming. If the target board cannot tolerate a *Vdd* of 5V, then a supply of 5V may be temporarily applied in an isolated fashion as shown in figure 6. (The host *Vdd* should be powered as normal during programming.)

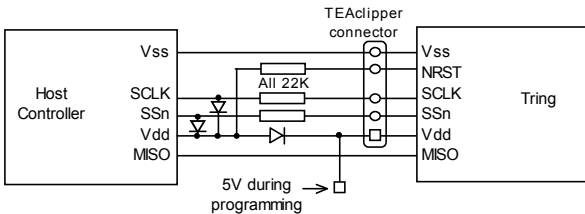


Figure 6. Recommended connection to permit in-circuit 5V programming host controller cannot tolerate *Vdd* of 5V.

Evaluation Guide

The circuit in figure 7 was used during development and testing of this product and is recommended for evaluation. The test Host Controller firmware *TringHost* is provided in the firmware pack in both compiled hex format and in C.

Note that the *NRST* input is connected to an I/O pin on the host. This allows the evaluator to experiment with its use; doing so does, however, require the use of a protection diode. Note also that the circuit is identical to the SerialStore evaluation circuit.

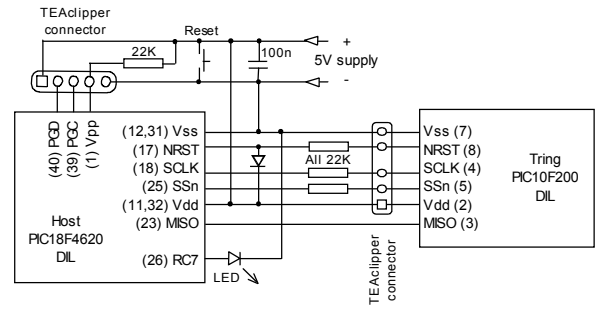


Figure 7. Recommended evaluation circuit

The TEAclipper Evaluation Board contains a PIC10F202 microcontroller originally intended for TEAleaf evaluation. PIC10F202 devices are compatible except for the location of the oscillator calibration bit. So long as you don't mind de-calibrating the oscillator, it may also be used for evaluating Tring. (See Table 4 for a labeling key.) There is also a ZIF socket to allow you to implement the host controller on a variety of processors, including the 18F4620 shown in figure 7.

Tring Pin Name	Evaluation Board Label	TEAclipper Connection
MOSI	PGD	PGD
SCLK	PGC	PGC
NRST	nRST	Vpp
SSn	Dat	-
Vdd	Vdd	Vdd
Vss	Vss	Vss

Program the 18F4620 with the *TringHost.hex* firmware and the PIC10F202 with the *Tring.wax* firmware. The host firmware *TringHost.hex* waits one second, reads in the random byte and then displays it as flashes on the LED. It is displayed as two hex digits as shown in table 5.

# of flashes	Hex Digit	# of flashes	Hex Digit
16	0	8	8
1	1	9	9
2	2	10	A
3	3	11	B
4	4	12	C
5	5	13	D
6	6	14	E
7	7	15	F

If the SPI signals interfere with the programming process, press the Reset button to hold the host in the reset state while programming the Tring.

Contact Information



Firmware Factory Ltd
2 Marshall St, 3rd Floor
London W1F 9BB, UK
sales@firmwarefactory.com
support@firmwarefactory.com