

# Uncorrelated Pseudo-Random Number Generator IP Cores

*Equidistributed pseudo-random number generators with extra-long periods*

## Key Features

- Efficient hardware implementations of various long-period pseudo-random number generators (PRNGs)
- PRNGs designs based on Combined Tausworthe Generators (CTGs), Well Equidistributed Long-period Linear (WELL), TT800, Mersenne Twister (MT) and SIMD-oriented Fast Mersenne Twister (SFMT) algorithms
- These PRNGs provides high-quality pseudo-random numbers with excellent equidistribution of the output values (up to 623 dimensions)
- Various period lengths available, ranging from  $2^{88}$  to  $2^{19937}$  and output bit widths ranging from 32 bits to 128 bits per instantiation
- User selectable seed value and multiple instantiations supported by jump-ahead seed calculation feature for long-period PRNGs

## Functional Description

Each PRNG core generates a sequence of uniformly distributed pseudo-random numbers. The seed values for the core sets the initial state of the PRNG. When clock enable is high the PRNG cores produce one output sample per clock cycle, except those based on the WELL algorithm, which generate one sample every two clock cycles. Generally, higher quality pseudo-random numbers, as measured by tests such as Diehard or testu01, are obtained from longer period PRNGs such as those based on the Mersenne twister (MT), SIMD-oriented fast Mersenne twister (SFMT) and WELL algorithms. The WELL algorithm has better bit mixing and equidistribution properties than other long-period PRNGs, but this comes at a cost of a lower pseudo-random number generation rate.

Figure 1 shows the top-level view of the system. Three system signals for the clock, clock enable and reset allow the user to control the pseudo-random number generation of the core. While clock enable is high, the core updates its internal state each clock cycle and produces pseudo-random numbers at the PRNG output pin. The bit width of the output depends on the particular PRNG algorithms chosen, and is detailed in Table 1. For the combined Tausworthe generators, reset brings the PRNG back to its initial state as set by the seed value. Longer period PRNGs have a larger internal state stored in memory and do not return to their initial state upon reset. Table 1 outlines the pin specifications for the UPRNG core.

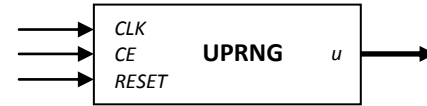


Figure 1: UPRNG core block diagram

Table 1: UPRNG core pin-out

Pin name	Pin type	Description
CLK	1-bit input	System clock input
CE	1-bit input	Active-high clock enable
RESET	1-bit input	Active-high synchronous reset
u	n-bit output	Uniform sample output port

## Implementation Performance

The UPRNG cores are suitable for FPGA devices and ASIC integration. Implementation results for the UPRNG cores on a Xilinx Virtex-5 LX 330 -2 (XC5VLX330-2) are listed in Table 2.

Table 2: Characteristics of the UPRNG cores on selected FPGA devices

PNG	Period	Sample bit width	Output rate (MSamp/s)	Slices	Memory blocks
CTG88	$\sim 3 \times 10^{26}$	32	715	30	-
CTG113	$\sim 1 \times 10^{34}$	32	701	37	-
CTG258	$\sim 4 \times 10^{77}$	64	638	85	-
WELL512	$\sim 1 \times 10^{154}$	32	205	52	-
TT800	$\sim 6 \times 10^{240}$	32	453	35	-
WELL1024	$\sim 1 \times 10^{308}$	32	193	61	-
MT19937	$\sim 4 \times 10^{6001}$	32	258	33	1
WELL19937	$\sim 4 \times 10^{6001}$	32	140	55	1
SFMT19937	$\sim 4 \times 10^{6001}$	128	330	278	-

## Deliverables

- Fully-commented and synthesizable Verilog source code or FPGA netlist
- Bit-true C and Matlab software models
- Instantiation example
- Self-checking test bench
- Product manual and detailed documentation
- Technical support

### Applications

Pseudo-random number generators find application in circuit testing, Monte-Carlo simulations and in the generation of non-uniform distributions. Monte-Carlo simulations specifically should use PRNGs such as the generators based on WELL, MT, or SFMT algorithms, since these PRNGs have very long periods and the necessary output correlations and equidistribution properties that are important for long running simulations.

Because the generated sequence of output values from this set of PRNGs can be predicted based on the seed value or can be determined by observing a small number of output values, these PRNGs are not suitable for cryptographic applications in their standard form. These IP cores can be made cryptographically secure using transforms on the output stream of the PRNG. Please contact Ukalta Engineering for further information when considering these PRNGs for cryptographic applications.

### Related Products

The PRNG cores can be used along with Ukalta's Gaussian noise generator IP cores (see datasheets **UGNG-31**, **UGNG-57** and **UGNG-71**) when evaluating the error rate performance of communication systems.

### Ordering Information

For purchasing or to obtain more detailed information on this or any of our other products or services, please contact Ukalta Engineering and we will be pleased to discuss how we can address your special requirements.

#### Ukalta Engineering Corporation

4344 Enterprise Square  
10230 Jasper Avenue NW  
Edmonton, Alberta, T5J 4P6  
Canada

Toll-free: +1 (866) 393 1524  
Phone: +1 (780) 701 1917  
Fax: +1 (866) 380 3755

Email: [contact@ukalta.com](mailto:contact@ukalta.com)  
Web: [www.ukalta.com](http://www.ukalta.com)