



ANSI X9.17/X9.31 Pseudorandom Number Generator

April 20, 2006

Product Specification



Helion Technology

Ash House, Breckenwood Road, Fulbourn, Cambridge CB1 5DQ, England
Phone: +44 1223 500 924
Fax: +44 1223 500 923
E-mail: helioncores@heliontech.com
URL: www.heliontech.com

AllianceCORE™ Facts	
Provided with Core	
Documentation	User Guide
Design File Formats	Xilinx netlist
Constraints Files	.ucf
Verification	VHDL or Verilog test bench; VHDL or Verilog Simulation models
Instantiation templates	VHDL ,Verilog
Reference designs & application notes	
Additional Items	Example ModelSim scripts
Simulation Tool Used	
ModelSim PE 5.8d	
Support	
Support provided by Helion Technology Limited	

Features

- Implements ANSI X9.17 and ANSI X9.31 Pseudorandom Number Generators
- TripleDES and AES versions available
- Supports 2-Key and 3-Key TripleDES
- Supports AES 128, 192, and 256-bit key sizes
- Provides pseudorandom number generation at rates up to 200 Mbits/sec
- Compact high performance design
- Specially designed for and highly efficient in Xilinx FPGA
- Simple external interface
- Mature and product proven IP
- Available under terms of the SignOnce IP License

Table 1: Example Implementation Statistics – TripleDES version

Family	Example Device	Fmax ¹ (MHz)	Slices	IOB ²	GCLK	BRAM	MULT	DCM/DLL	MGT	PPC	Design Tools
Spartan-3™	XC3S1000-5	153	438	170	1	0	0	0	N/A	N/A	ISE 8.1.01i
Spartan-3E™	XC3S1200E-5	158	438	170	1	0	0	0	N/A	N/A	ISE 8.1.01i
Virtex-II Pro™	XC2VP7-7	244	438	170	1	0	0	0	0	0	ISE 8.1.01i
Virtex-4™	XC4VLX25-11	256	438	170	1	0	0	0	0	0	ISE 8.1.01i

Notes:

- 1) Fmax is quoted assuming all core inputs are sourced from flip-flops, and all core outputs drive flip-flops; this has been done to best represent real applications where the core is typically embedded within a larger system.
- 2) Assuming all core I/Os and clocks are routed off-chip

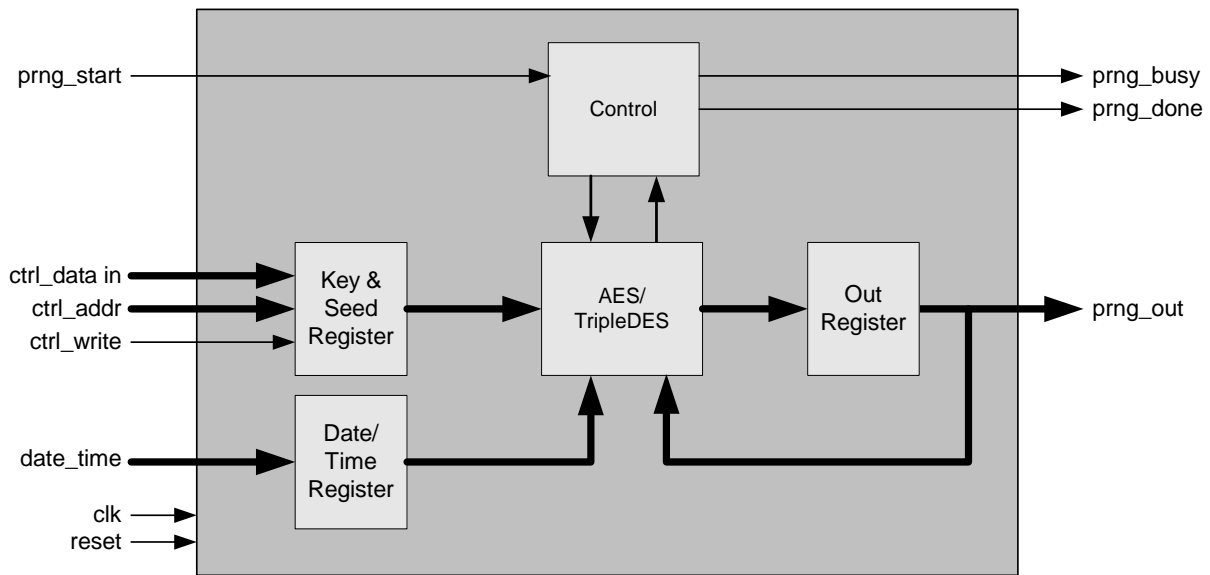


Figure 1: ANSI PRNG Block Diagram

Applications

The core is intended for any security application that requires a standard PRNG function for the generation of cryptographic Keys and IVs using strong encryption. Both ANSI X9.17 and ANSI X9.31 PRNGs are defined as part of the ANSI X9 standards which are used to secure financial transactions. The core may also be used for pseudorandom number generation as part of an implementation of the Digital Signature Standard described in NIST FIPS PUB 186-2.

General Description

The Helion PRNG core implements two of the most widely used pseudorandom number generators which may be used to produce encryption keys and IVs for use in hardware implementations of a variety of security protocols. Based on a strong encryption algorithm, and utilising two random inputs - a user supplied random seed value and the current system date/time - the core produces random numbers which meet the requirements of the ANSI X9 standards as recommended by NIST.

Functional Description

Control

The control block is responsible for interfacing with the external user application and overall control of the main PRNG datapath.

AES/TripleDES Encryptor

At the heart of the PRNG is either a TripleDES or AES core which provide the strong encryption on which the PRNG calculation is founded.

Key Register

This write-only register is programmed by the host to provide the encryption key used by the PRNG. It may only be programmed by the host when the PRNG core is idle.

Seed Register

This write-only register is programmed by the host to provide the random seed value used by the PRNG. This value is updated internally for use in the next operation unless it is re-seeded by the host between PRNG operations. The seed may only be programmed by the host when the PRNG core is idle.

Date/Time Register

This register contains the host system date/time at the point at which the core was started. This provides a second random input to the PRNG calculation.

Output Register

This register contains the final PRNG output value.

Core Modifications

The PRNG core may be supplied either in TripleDES or AES versions. The Triple DES version supports both two-key and three-key operation to meet the PRNG requirements for both ANSI X9.17 and ANSI X9.31. The AES version supports all three AES key sizes specified for the ANSI X9.31 PRNG.

Table 2: Example Implementation Statistics – AES version

Family	Example Device	Fmax ¹ (MHz)	Slices	IOB ²	GCLK	BRAM	MULT	DCM/ DLL	MGT	PPC	Design Tools
Spartan-3™	XC3S1000-5	162	556	298	1	3	0	0	N/A	N/A	ISE 8.1.01i
Spartan-3ET™	XC3S1200E-5	170	570	298	1	3	0	0	N/A	N/A	ISE 8.1.01i
Virtex-II Pro™	XC2VP7-7	263	559	298	1	3	0	0	0	0	ISE 8.1.01i
Virtex-4™	XC4VLX25-11	250	565	298	1	3	0	0	0	0	ISE 8.1.01i

Notes:

1. Fmax is quoted assuming all core inputs are sourced from flip-flops, and all core outputs drive flip-flops; this has been done to best represent real applications where the core is typically embedded within a larger system.
2. Assuming all core I/Os and clocks are routed off-chip

Tables 2 shows typical figures for the AES version of the PRNG core.

Core Data Throughput Capability

The maximum PRNG output rate is directly proportional to the master clock frequency used in the implementation. It also depends on the data throughput of the encryption algorithm as follows;

$$\text{2-Key or 3-Key TripleDES output rate (Mbps)} = (64/151) * \text{Fclk}$$

$$\text{AES-128 output rate (Mbps)} = (128/151) * \text{Fclk}$$

$$\text{AES-192 output rate (Mbps)} = (128/175) * \text{Fclk}$$

$$\text{AES-256 output rate (Mbps)} = (128/199) * \text{Fclk}$$

Helion can also provide higher throughput versions of both AES and TripleDES versions of the PRNG core upon request, please contact us for details.

Core I/O Signals

The core signal I/O have not been fixed to specific device pins to provide flexibility for interfacing with user logic. Descriptions of all signal I/O are provided in Table 3.

Table 3: Core I/O Signals.

Signal	Width	Signal Direction	Description
clk	1	Input	master clock input
reset	1	Input	asynchronous reset; 1 = reset
prng_start	1	Input	PRNG start pulse
prng_done	1	Output	PRNG done pulse
prng_busy	1	Output	PRNG busy
ctrl_data_in	32	Input	control data word in
ctrl_addr	4	Input	control address
ctrl_write	1	Input	control data write enable
date_time	64/128	Input	current date/time
prng_out	64/128	Output	PRNG output value

NOTE: The width of the date_time and prng_out I/O signals are dependent on the block size of the underlying encryption algorithm used by the PRNG e.g. 64-bit for TripleDES, 128-bit for AES.

Verification Methods

The Helion PRNG core has been thoroughly verified under simulation. In addition, it has been fully proven in real Xilinx hardware, and has been deployed by our customers within real products out in the field.

Recommended Design Experience

Users should be familiar with HDL methodology and Xilinx design flows including VHDL/Verilog component instantiation, synthesis, implementation and simulation.

Ordering Information

This product is available directly from Xilinx AllianceCORE member Helion Technology under the terms of the SignOnce IP License. Please contact Helion Technology for pricing and additional information about this product. Contact information for them is on the front page of this datasheet. To learn more about the SignOnce IP License program, contact Helion Technology or visit the web:

Email: commonlicense@xilinx.com
URL: www.xilinx.com/ipcenter/signonce

Export

Strong encryption technology such as Triple-DES and AES are governed internationally by export regulations. Immediate export is permitted to the following countries;

Austria	Australia	Belgium
Canada	Cyprus	Czech Republic
Denmark	Estonia	Finland
France	Germany	Greece
Hungary	Ireland	Italy
Japan	Latvia	Lithuania
Luxembourg	Malta	New Zealand
The Netherlands	Norway	Poland
Portugal	Slovakia	Slovenia
Spain	Sweden	Switzerland
United Kingdom	United States	

Please contact Helion to discuss delivery to other destinations; approval is subject to the applicable export licenses being granted. Please note that licensees are responsible for complying with the applicable requirements for re-export of electronics containing Triple-DES and AES technology.

Related Information

“ANSI X9.17 - 1985 Appendix C”

“ANSI X9.31 – 1998 Appendix A.2.4”

“NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms”, January 31st, 2005.

“FIPS PUB 186-2 Digital Signature Standard (DSS)”, January 27th, 2000.

Xilinx Programmable Logic

For information on Xilinx programmable logic or development system software, contact your local Xilinx sales office, or:

Xilinx, Inc.
2100 Logic Drive
San Jose, CA 95124
Phone: +1 408-559-7778
Fax: +1 408-559-7114
URL: www.xilinx.com