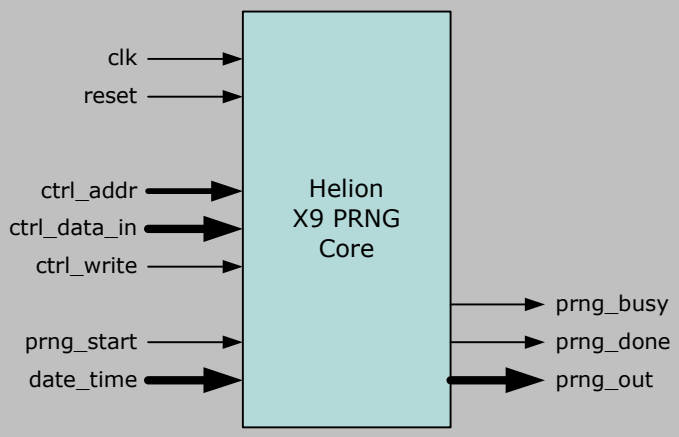
Helion Technology

FULL DATASHEET – ANSI X9 Random Number Generator for Xilinx FPGA



Features

- Implements ANSI X9.17 and X9.31 Pseudorandom Number Generators
- Supports either Triple-DES or AES encryption algorithms
- Supports 2-Key and 3-Key Triple-DES
- Supports AES with 128/192/256 bit key sizes.
- Supports ECB mode operation of underlying block cipher
- Simple external interface
- Ideally suited to acceleration of cryptographic Key and IV generation
- Highly optimised for use in Xilinx FPGA technology

Deliverables

- Target specific netlist or fully synthesisable RTL VHDL/Verilog
- VHDL/Verilog simulation model and testbench
- Comprehensive user documentation

Overview

The Helion Pseudorandom Number Generator (PRNG) Core family is built on Helion's mature and well proven Triple-DES and AES block cipher cores, and has been designed especially for use in Xilinx FPGA.

The core implements the ANSI X9.17 and ANSI X9.31 standard PRNG algorithms which are used in a variety of security applications to generate cryptographic Keys and Initialisation Vectors. Applications include implementations of ANSI X9 standard financial security protocols, and the Digital Signature Standard (DSS) described in FIPS PUB 186-2.

The core may be supplied in either Triple-DES or AES versions. The Triple-DES version supports both 2-Key and 3-Key Triple-DES operation, whilst the AES version supports all three AES key sizes (128/192/256), as recommended by NIST for use in ANSI X9.31.

Helion Technology Limited
Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England

Functional Description

Operation of the Helion PRNG core is very simple. First the core is initialised by the host writing the key and seed values to the control interface. For the AES version the host should also indicate the required key length by selecting either a 128, 192 or 256 bit key.

Once initialisation of the core is complete, the host asserts the start input each time it requires generation of a new pseudorandom number. In the same cycle as start is asserted the current host date/time input is latched for use internal to the core. When the core is in the process of generating a number it asserts the busy output, during which time host writes to the control interface are disabled.

Once generation is complete the core indicates that the pseudorandom number output is valid by asserting the done output. Note that each pseudorandom number generated will be 64-bits in length for the 3DES core, or 128-bits in length for the AES core, this reflecting the native blocksize of the underlying encryption algorithm.

The PRNG core also offers direct access to the underlying block cipher in ECB mode to provide basic encryption acceleration and to ease FIPS compliance testing.

Logic Utilisation and Performance

The tables below show typical logic area and performance figures for the two versions of the PRNG core, covering three of the most popular Xilinx device families. Please note that these cores are also available in versions supporting all other Xilinx FPGA families (both old and new), and that area and performance figures are available from Helion on request for any device types or speed grades not listed below.

	PRNG core - 3DES version		
technology	Spartan3 -5	Spartan6 -2	Virtex6 -3
logic resource	441 slices	147 slices	149 slices
max clock	152 MHz	237 MHz	467 MHz
random bit rate	64 Mbps	99 Mbps	197 Mbps

	PRNG core – AES version		
technology	Spartan3 -5	Spartan6 -2	Virtex6 -3
logic resource	562 slices 3 RAMB16	253 slices	279 slices
max clock	161 MHz	202 MHz	358 MHz
random bit rate	136 Mbps	170 Mbps	303 Mbps

About Helion

Founded in 1992, Helion is a well established British company based in Cambridge, England, offering a range of product-proven Data Security IP cores backed up by highly experienced and professional design service capabilities. Being members of the Xilinx AllianceCORE IP program and a certified Xilinx Alliance Partner, Helion takes its Xilinx implementations very seriously indeed. Both of the PRNG cores have been designed from the ground up to be highly optimal in Xilinx FPGA and are not simply based on a generic ASIC designs like much of the competition.

More Information

For more detailed information on this or any of our other products and services, please contact Helion and we will be pleased to discuss how we can assist with your individual requirements.

Helion Technology Limited
Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England

tel: +44 (0)1223 500 924 email: info@heliontech.com
fax: +44 (0)1223 500 923 web: www.heliontech.com