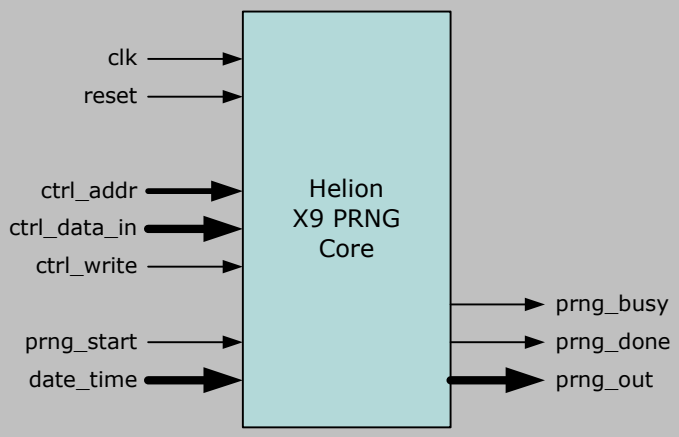
Helion Technology

FULL DATASHEET – ANSI X9 Random Number Generator for 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.
- Offers optional access to 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 each individual 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 each different FPGA technology.

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-bit), 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 address mapped control interface. For the AES version, the host should also indicate the required AES key length to either 128, 192 or 256 bits.

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.

As an option, 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

Helion has a long history in high-end FPGA design, and we therefore take great care when implementing our IP cores. As a result they have been designed from the ground up to be highly optimal for each individual FPGA technology - they are not simply based on a synthesised generic RTL ASIC design. The Helion PRNG core makes use of the architectural features available in each FPGA technology to achieve the highest performance combined with the most efficient logic resource utilisation.

The latest logic area, performance figures, and datasheets for the Helion PRNG core in a range of different technologies are available at http://www.heliontech.com/random.htm. Please feel free to contact us should you require further details.

About Helion

Helion is a long established British company based in Cambridge, England, offering a range of product-proven Data Security silicon IP cores backed up by our highly experienced and professional design service capabilities. Although we specialise in providing the highest performance data encryption and authentication IP, our interest does not stop there. Unlike broadline IP vendors who try to supply a very diverse range of solutions, being specialists we can offer much more than just the IP core itself.

For instance, we are pleased to be able to supply up-front expert advice on any security applications which might take advantage of our technology. Many of our customers are adding data security into their existing systems for the first time, and are looking for a little assistance with how best to achieve this. We are pleased to help with suitable advice and support where necessary, and pride ourselves in our highly personal approach.

The quality of our IP is however the main reason our customers keep coming back for more. We passionately believe that if you are buying IP, it should have been designed with the ultimate in care, crafted to achieve the ultimate performance in each target technology, and thoroughly tested to ensure compliance with any associated standards. All this comes as standard with IP from Helion.

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