

Many cryptographic operations require a source of random numbers primarily in the creation of cipher keys. This core generates pseudo random based on initial seed values from the host. It is also capable of adding entropy by mixing in noise received from an external analog-source random number generator. A unique feature of the CLP-01 is a secure mode of operation which makes the core largely tamper proof, offering another layer of protection against attempts to compromise the operation of the random number generator. This simplifies the design of high security applications such as NIST FIPS 140-2 level 4 hardware security modules.

Key Features:

- Area: 23K ASIC gates
- High entropy operation – over 128 bits
- High speed operation – 380 Mbps at 200 MHz core clock
- Initial seed provided from embedded processor or host core logic
- Automatic re-seeding
- Support for mixing of true analog-source RNG input
- Provides a security mode to prevent internal registers from being modified
- Test bench provided

Applications:

- WiMax applications such as 802.16
- IPSec designs in gateways and enterprise routers
- WLAN applications such as 802.11i
- Digital Rights Management
- Military communications systems

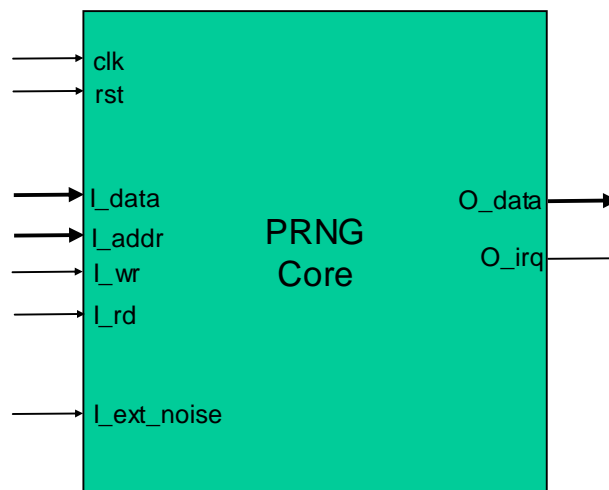


Figure 1 CLP-01 Block Diagram

Pin Description

Signal Name	Width	Description
<i>System clock domain</i>		
clk	1	System clock
rst	1	Asynchronous system reset. Active high.
I_data	32	Write data bus. Single cycle access to all control and configuration registers.
I_addr	6	Address bus. Allows access to all internal control and configuration registers.
I_wr	1	Write signal. Active high.
I_rd	1	Read signal. Active high.
O_data	32	Read data bus. Single cycle access to all control, configuration and output registers.
O_irq	1	Interrupt line. Indicates PRN is available.
I_ext_noise	1	External noise input

General Description

The CLP-01 is a hardware implementation of a random number generator. It is commonly used to generate keys for cryptographic applications or to provide initialization vectors for packet-based security protocols. At the heart of the CLP-01 is the CLP-03 AES core used in a special mode with an optional external noise source. The CLP-03 is a fully proven core in volume silicon production. The CLP-01 has been proven in FPGA form and comes with a complete test bench and in depth user documentation. Elliptic's talented and helpful support staff is also available to simplify the integration of the core into the target ASIC or FPGA.

The CLP-01 PRNG is intended to be integrated into an embedded processor based SoC, or to be driven by a Finite State Machine. Inputs to the core include:

- A memory-mapped set of registers that configure the core
- Two 128-bit registers used for seeding purposes
- An optional input from an external analog noise source
- A register which when written to, engages secure mode to prevent tampering by preventing modification of internal configuration and control registers.

The CLP-01 provides a 128 bit random number accessed via the host interface. A 128-bit random number is available every 69 clock cycles (equivalent to 1.9 bits per clock).

The CLP-01 is available in soft IP form, either as a netlist or HDL Source. The deliverables available are:

Netlist Licenses:

- Post synthesis netlist
- Testbench
- Sample simulation script
- Documentation

HDL Source Licenses:

- Verilog 2001 HDL
- Testbench
- Sample synthesis script
- Documentation

An FPGA load can be made available under license or through the Elliptic evaluation card – the EVAL-01 for evaluation purposes. For more information on pricing and a full data sheet, please contact:

Elliptic Semiconductor Inc.
62 Steacie Drive, Suite 201
Ottawa, ON
Canada
K2K 2A9

Phone: +1 613 254-5456
Fax: +1 613 254-7260
Email: info@ellipticsemi.com