

Many cryptographic operations require a source of random numbers primarily in the creation of cipher keys. This core is derived from the CLP-01 and adds a noise source that may be used to seed the random number stream as well as provide an ongoing source of entropy. The noise source does not depend on process specific circuitry and is therefore very portable across different fabrication source. The CLP-21 offers a tamper resistant or secure mode of operation which makes it difficult to compromise.

Key Features:

- Area: 45K ASIC gates
- High entropy operation – over 128 bits
- High speed operation – 380 Mbps at 200 MHz core clock
- Initial seed provided from internal noise source
- Automatic re-seeding
- Features 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

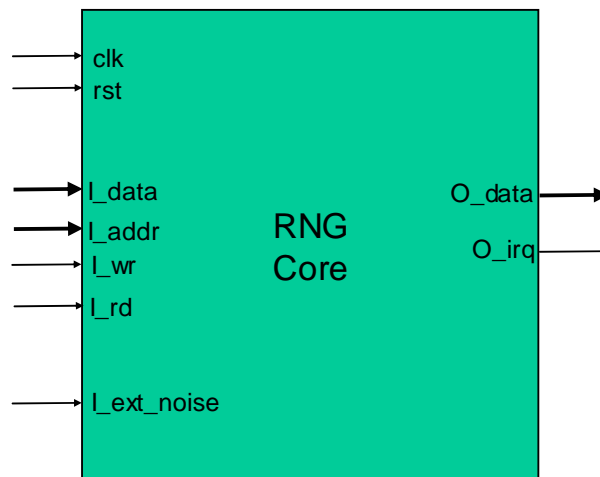


Figure 1 CLP-21 Pinout

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	8	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 random number is available.
I_ext_noise	1	External noise input

General Description

The CLP-21 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-21 is a pseudo-random number generator (also known as a deterministic bit generator) which is supplemented by an on-chip noise source to seed and re-seed the generator. The block diagram shown in Figure 2 on the next page illustrates the major functional components of the CLP-21.

Elliptic's talented and helpful support staff are also available to simplify the integration of the core into the target ASIC or FPGA. Guidelines for synthesis and layout of the core are provided in order to maximize entropy added from the noise source.

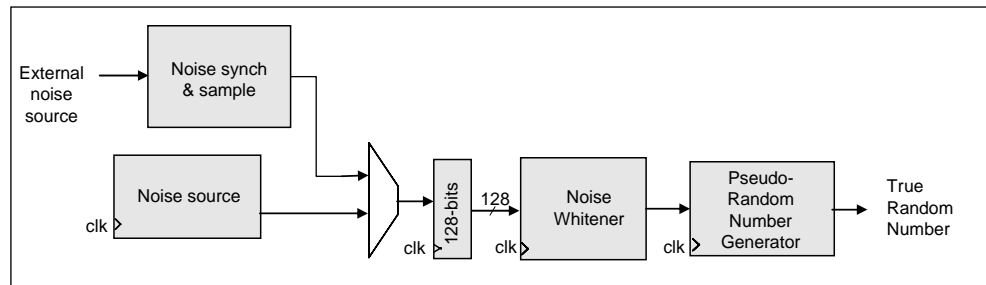


Figure 2 CLP-21 Functional Blocks

The CLP-21 RNG is intended to be integrated into an embedded processor based SoC
Inputs to the core include:

- A memory-mapped set of registers that configure the core
- An input from an external analog noise source
- A register which, when written to, engages secure mode to prevent tampering

The CLP-21 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-21 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 HDL
- Testbench
- Sample synthesis script
- Documentation

The CLP-21 is available for use in an FPGA and it can also be made available for evaluation under license through the Elliptic evaluation cards – either the EVAL-01 or EVAL-02 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, K2K 2A9

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