XCIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP8001B: TRNG

True Random Number Generator IP Core

Product Brief
ver. 1.3
July 4, 2022

sales@xiphera.com

Introduction

XIP8001B from Xiphera is a True Random Number Generator (TRNG) Intellectual Property (IP) core designed in generic and portable VHDL. XIP8001B has been designed for easy integration with FPGA- and ASIC-based designs, and consequently its design methodology is vendor-agnostic, and the functionality of XIP8001B does not rely on any FPGA manufacturer-specific features. XIP8001B includes the NIST SP 800-90B specified startup tests and online health tests.

The output of the entropy source (the so-called "raw bits") in XIP8001B have been successfully tested with PractRand [6], gjrand [2], TestU01 [7], NIST SP 800-22 [3] statistical test suite and the `dieharder` [1] test suite. XIP8001B includes a NIST SP 800-90B [4] compliant AES-CBC-MAC -based entropy extractor, thus making XIP8001B suitable for use in a crypto module targeting a FIPS 140-3 [5] certification.

Key Features

- **Compact Size:** The entire design requires only 1387 Adaptive Lookup Modules (ALMs) (Intel® Cyclone® 10 GX) and 1-2 internal memory blocks[1] in a typical FPGA implementation.
- **Autonomous Operation:** The entropy source used by XIP8001B functions independently from the rest of the FPGA logic; for example no FPGA internal clock signals are required for the entropy source to function.
- **Parameterizability:** XIP8001B has a number of parameterizable features, including the width of the `dout` output, the sizes (width and depth) of the internal buffers, and the threshold values for the health tests.

[1] The memory block consumption depends on the size of the internal and output buffer as well as on the FPGA architecture.

- **Security Features:** XIP8001B has a number of additional security features, including a zeroize function to erase (set to '0') all the bits in the internal buffer.
- **Standard Compliance:** The core has been designed to comply with NIST SP 800-90B, thus making its use in a crypto module targeting a FIPS 140-3 certification possible.
- **Passing Statistical Tests:** The output of the entropy source in XIP8001B passes PractRand, gjrand, TestU01, the NIST SP 800-22 statistical test suite, and the `dieharder` test suite.

Functionality

The internal block diagram of XIP8001B is depicted in Figure 1. When enabled, the entropy source generates a continuous stream of random bits (the so-called "raw bits"), which are monitored by the NIST SP 800-90B compliant online health tests. The internal "raw bits" are only written to internal buffer if they pass the online health tests. The entropy extractor is based on NIST SP 800-90B compliant AES-CBC-MAC design, whose output is written to the output buffer[2]. The random bits generated by XIP8001B can be read by the external FPGA design on the `dout` output.

Block Diagram

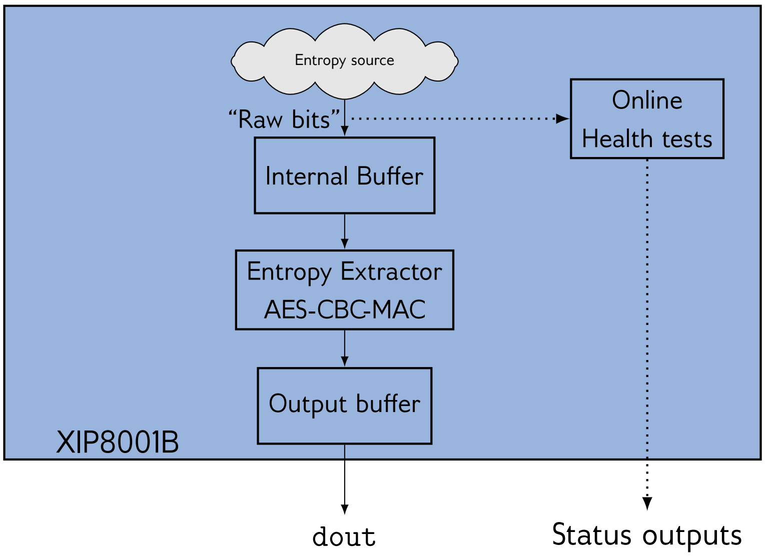

Figure 1: Internal high-level block diagram of XIP8001B

Interfaces

The external interfaces of XIP8001B are depicted in Figure 2.

To facilitate the integration of XIP8001B with the rest of the customer's design, all input and output signals of XIP8001B are synchronized to the clock signal `clk`.

[2] The output buffer is designed as a FIFO with a default word width of 32 bits.

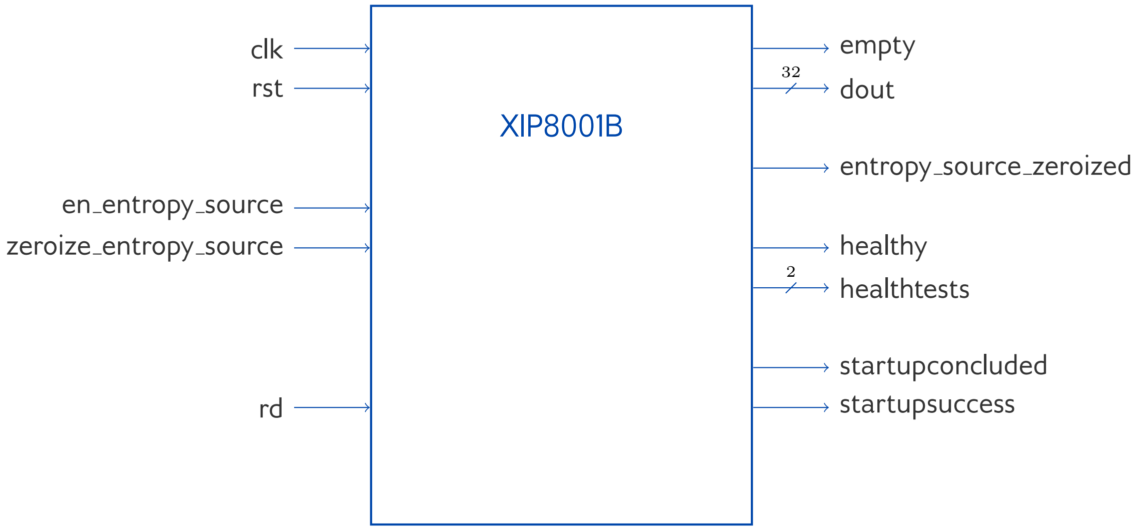

Figure 2: External interfaces of XIP8001B

This Product Brief describes a high-level overview of the functionality and capabilities of XIP8001B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP8001B, example simulation waveforms, parameterization of the online health tests, and the FPGA resource requirements of your targeted FPGA family.

FPGA Resources and Performance

Table 1 presents the FPGA resource requirements for representative low-cost and high-end FPGA implementations from two leading FPGA manufacturers. On request, the resource estimates can also be supplied for other FPGA families.

Device	Resources	Output bit rate [*]
Intel® Cyclone® 10 GX[†]	1387 ALM, 2 M20K	$2.34 Mbps$
Intel® Arria® 10 GX[†]	1387 ALM, 2 M20K	$2.56 Mbps$
Xilinx® Kintex® UltraScale+[‡]	1426 LUT, 1 RAMB18	$4.28 Mbps$
Xilinx® Zynq® MPSoC[‡]	1453 LUT, 1 RAMB18	$4.11 Mbps$
Lattice® ECP5® [‡]	2737 4LUTs, 3 EBR	$2.79 Mbps$

Table 1: Resource usage and performance of XIP8001B on representative FPGA families.

Example Use Cases

The output of XIP8001B can be used to supply the required number of random bits for a multitude of applications, including key derivation (for example, with Xiphera IP cores XIP3322B and XIP3327C), generating initialization vectors for symmetric key algorithms (for example, Xiphera Advanced Encryption Standard (AES) IP cores XIP1101B, XIP1101H, XIP1111B, XIP1111H, and XIP1113H), and

[*] Hardware validated. Varies sligthly with deployment options.
[†] Quartus® Prime Pro 21.1.0, default compilation settings, industrial speedgrade.
[‡] Vivado 2020.2, default compilation settings, industrial speedgrade.

as an input to a Pseudo Random Number Generator (PRNG)[3].

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP8001B can be shipped in a number of formats, including netlist, source code, or encrypted source code. Additionally, a comprehensive VHDL testbench and a detailed datasheet are included.

About Xiphera

Xiphera specializes in secure and efficient implementations of standardized cryptographic algorithms on Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs). Our product portfolio includes individual cryptographic Intellectual Property (IP) cores, as well as comprehensive security solutions built from a combination of individual IP cores.

Xiphera is a Finnish company operating under the laws of the Republic of Finland, and is fully owned by Finnish citizens and institutional investors.

Contact

Xiphera Oy
Otakaari 5
FIN-02150 Espoo
Finland
sales@xiphera.com
+358 20 730 5252

References

[1] Dieharder: A Random Number Test Suite, Version 3.31.1. `http://webhome.phy.duke.edu/~rgb/General/dieharder.php`.

[2] gjrand: random numbers website. `http://gjrand.sourceforge.net/`.

[3] SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Technical report, Gaithersburg, MD, United States, 2010.

[4] SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2018.

[5] FIPS PUB 140-3, Security Requirements for Cryptographic Modules. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2019.

[6] Chris Doty-Humphrey. Practically random: C++ library of statistical tests for RNGs. `http://pracrand.sourceforge.net/`.

[3] Known as Deterministic Random Bit Generator (DRBG) in NIST terminology

[7] Pierre L'Ecuyer and Richard Simard. Testu01: Ac library for empirical testing of random number generators. http://simul.iro.umontreal.ca/testu01/tu01.html.