XCIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP8103B: PRNG

Balanced AES-based Pseudorandom Number Generator

Product brief
ver. 1.0
December 19, 2023

info@xiphera.com

Introduction

XIP8103B from Xiphera is a Pseudorandom Number Generator (PRNG) Intellectual Property (IP) core. XIP8103B is based on Counter (CTR) operation mode of a 256-bit Advanced Encryption Standard (AES) and uses an AES-CTR implementation as an integral building block. XIP8103B has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP8103B does not rely on any FPGA manufacturer-specific features.

Key Features

- **Balanced Between Speed and Resource Requirements:** XIP8103B can achieve over 2 Gbps throughput, while consuming only about 4100 Lookup Tables (LUTs) in a typical FPGA implementation.

- **Versatility:** XIP8103B supports the forward prediction resistance mode, which can be set on and off between output generation, as well as the use of personalization strings and additional inputs for instantiation and reseeding.

- **Standard Compliance:** XIP8103B is compliant with the NIST SP800-90A specification [1]. XIP8103B can be combined with Xiphera's NIST SP800-90B [3] compliant XIP8001B to form a NIST SP800-90C compliant [2] Random Bit Generator (RBG).

- **Easy integration** with AXI4-lite and AXI stream interfaces.

Functionality

The main functionality of XIP8103B is to produce pseudorandom numbers. Pseudorandom numbers are numbers which look completely random but which are generated deterministically from a seed. If the seed is known, all outputs of the PRNG can be computed. If the PRNG is properly seed with a *full-entropy seed* its outputs provide as much randomness, or security, as the seed it was seeded with.

XIP8103B is a CTR_DRBG, which means that the deterministic function producing the pseudorandom outputs is AES in Counter operation mode. XIP8103B uses AES with a 256-bit key, and is designed to be compliant with the NIST SP800-90A [1]. Combining XIP8103B with a TRNG compliant with NIST SP800-90B [3], gives a NIST SP800-90C compliant random number generator which is optimal for cryptographic security.

Block Diagram

The internal high-level block diagram of XIP8103B is depicted in Figure 1. The block diagram consists of a control component, an internal state, ROM block for the known-answer tests and an AES IP core in CTR mode.

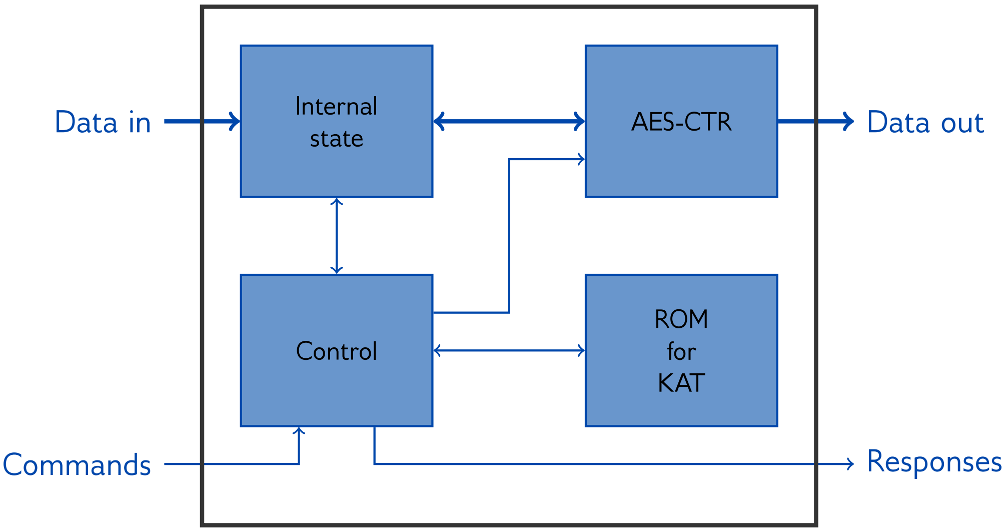

Figure 1: Internal high-level block diagram of XIP8103B

Interfaces

The external interface of XIP8103B is depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP8103B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP8103B, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

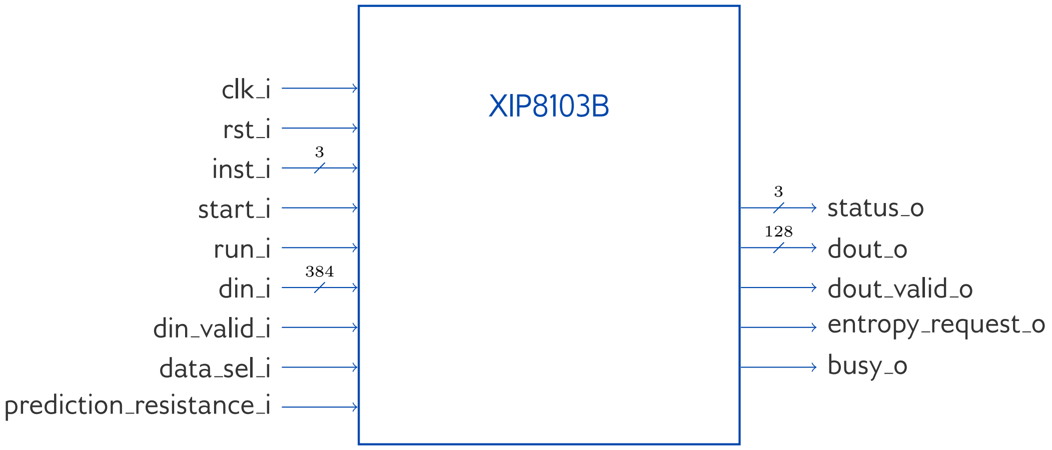

Figure 2: Interface diagram of XIP8103B.

FPGA Resources and Performance

Table 1 presents the FPGA resource requirements for representative implementations on different FPGA architectures. On request, the resource estimates can also be supplied for other FPGA families. For in-depth perfomance figures please request and consult the datasheet.

Device	Resources	f_{MAX}	Max. throughput*
Intel® Arria® 10 GX†	3674 ALM, 4 M20K	283.61 MHz	1.65 Gbps
Intel® Agilex® F†	3829 ALM, 4 M20K	473.93 MHz	2.76 Gbps
Intel® Cyclone® 10 GX†	3674 ALM, 4 M20K	276.85 MHz	1.61 Gbps
AMD® Kintex® UltraScale+‡	4307 LUT, 1 RAMB18	407.50 MHz	2.37 Gbps
AMD® Zynq® MPSoC‡	4332 LUT, 1 RAMB18	334.22 MHz	1.94 Gbps
Lattice® CertusPro-NX® §	6204 LUT4, 4 EBR	134.37 MHz	781.80 Mbps
Lattice® ECP5® ¶	5862 LUT4, 4 EBR	120.98 MHz	703.87 Mbps
Microchip® PolarFire® ‖	6189 4LUTs, 11 uSRAM	85.19 MHz	495.67 Mbps

Table 1: Resource usage and performance of XIP8103B on representative FPGA families.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP8103B can be shipped in a number of formats, including netlist, source code, or encrypted source code. Additionally, synthesis scripts, a comprehensive testbench, and a detailed datasheet including an integration guide are included.

*Throughput $= \frac{128\text{bits}}{22\text{ clock cycles}} * f_{\text{MAX}}$

†Quartus® Prime Pro 22.4.0, default compilation settings, industrial speedgrade.

‡Vivado 2022.1, default compilation settings, industrial speedgrade.

§Radiant 2022.1.0, default compilation settings, synthesised with Synplify.

¶Diamond 3.12.0, default compilation settings, synthesised with Synplify.

‖Libero 2022.1.0.10, default compilation settings, industrial speedgrade.

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 fully in-house designed 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
Tekniikantie 12
FIN-02150 Espoo
Finland
sales@xiphera.com
+358 20 730 5252

References

[1] SP 800-90A Rev.1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2015.

[2] SP 800-90C (Second Draft) Recommendation for Random Bit Generator (RBG) Constructions. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2016.

[3] 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.