XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP8103H: PRNG

High-Speed AES-based Pseudorandom Number Generator

Product brief
ver. 1.0
October 28, 2024

info@xiphera.com

Introduction

XIP8103H from Xiphera is a Pseudorandom Number Generator (PRNG) Alteralectual Property (IP) core. XIP8103H is based on Counter (CTR) operation mode of a 256-bit Advanced Encryption Standard (AES) and uses a high-speed AES-CTR implementation as an integral building block.

XIP8103H has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP8103H does not rely on any FPGA manufacturer-specific features.

Key Features

- **High Performance:** XIP8103H can achieve over 16.18 Gbps throughput, while consuming only about 36855 Lookup Tables (4LUTs) in a typical Lattice® FPGA implementation.
- **Iersatility:** XIP8103H 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:** XIP8103H is compliant with the NIST SP800-90A specification [1]. XIP8103H 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 XIP8103H 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 seeded with a *full-entropy seed* its outputs provide as much randomness, or security, as the seed it was seeded with.

XIP8103H is a CTR_DRBG, which means that the deterministic function producing the pseudorandom outputs is AES in Counter operation mode. XIP8103H uses AES with a 256-bit key, and is designed to be compliant with the NIST SP800-90A [1]. Combining XIP8103H 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 XIP8103H is depicted in Figure 1. The block diagram consists of a control component, an internal state, ROM block for the known-answer tests and a high-speed AES IP core in Counter (CTR) mode.

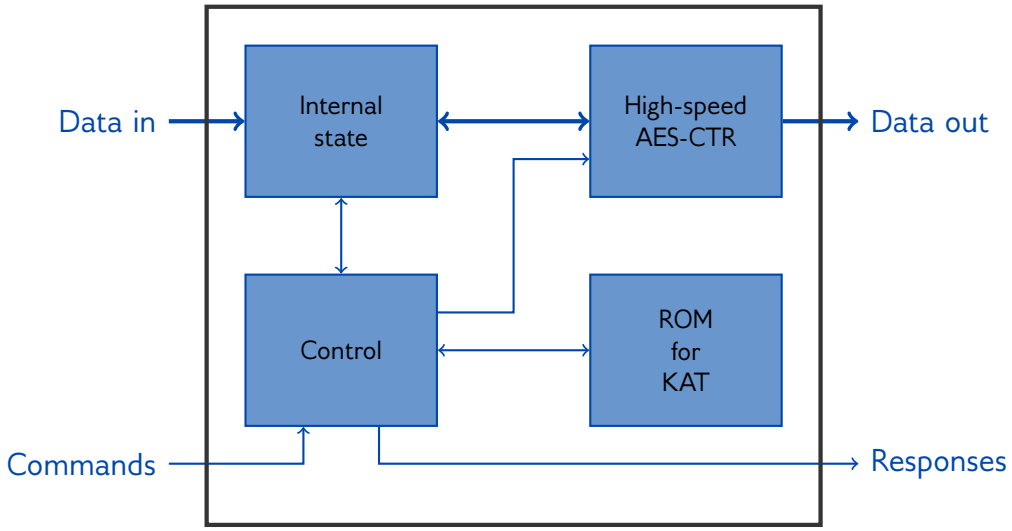

Figure 1: Internal high-level block diagram of XIP8103H

Interfaces

The external interface of XIP8103H is depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP8103H. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP8103H, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

FPGA Resources and Performance

Table 1 presents the Lattice® FPGA resource requirements for representative implementations on different Lattice® FPGA architectures. On request, the resource estimates can also be supplied

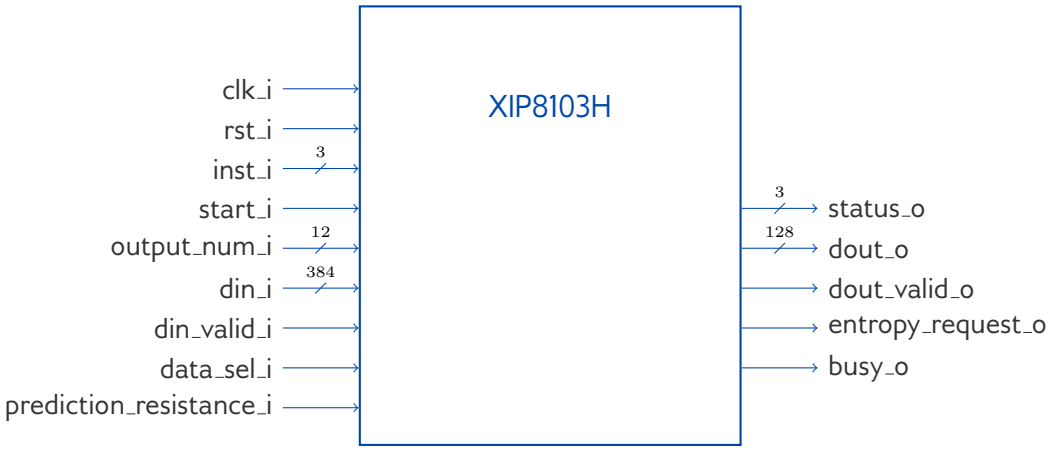

Figure 2: Interface diagram of XIP8103H.

for ASIC and other Lattice® FPGA families. For in-depth perfomance figures please request and consult the datasheet.

Device	Resources	f_{MAX}	Max. throughput*
Lattice® ECP5® §	36855 LUT4 , 2/1 MULT18/ALU54	127.84 MHz	16.18 Gbps
Lattice® CertusPro-NX® ¶	33285 LUT4	137.70 MHz	17.43 Gbps

Table 1: Resource usage and performance of XIP8103H on representative Lattice® FPGA families.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP8103H 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.

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 Alteralectual 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.

§Diamond 3.12.0, default compilation settings, industrial speedgrade.

¶Radiant 2022.1.0, default compilation settings, industrial speedgrade.

*$\text{Throughput} = \frac{128\text{bits}*4096}{4096+47 \text{ clock cycles}} * f_{\text{MAX}}$

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.