PEACE OF MIND IN A DANGEROUS WORLD

XIP2113H : CHACHA20-POLY1305

High-Speed IP Core for ChaCha20-Poly1305 Authenticated Encryption

Resource Sheet

2026-05-06

sales@xiphera.com

Introduction

This document details FPGA and ASIC resource requirements and performance of XIP2113H with the default configuration—for example, instantiation parameters, supported features, and selected bus interface—of XIP2113H.

FPGA Resources and Performance

Table 1 presents the FPGA resource requirements for different FPGA architectures. Upon request, resource requirements can also be provided for other FPGA manufacturers, families, and specific part numbers. The results were obtained using default synthesis and P&R (placement and routing) settings in the FPGA design software.

ASIC Resources and Performance

Table 2 describes the logic requirements of XIP2113H on the TSMC 16nm FinFET Plus Low Leakage standard cell process. The results were obtained by synthesising XIP2113H with Synopsys® DC W-2024.09-SP2 using default settings.
Table 3 presents the total memories inside the XIP2113H.

[†]Quartus Prime Pro 25.1.0, default compilation settings, industrial speedgrade.
[‡]Quartus Prime Pro 24.2.0, default compilation settings, industrial speedgrade.
[§]Vivado 2024.2, default compilation settings, industrial speedgrade.
[¶]Radiant 2024.2.1, default compilation settings, industrial speedgrade.
[‖]Libero 2024.2.0.13, default compilation settings, industrial speedgrade.
[1]Equivalent to the total cell area normalised to the area of a representative NAND2 gate.
[2]Excluding IO pins and memories listed in Table 3.
[3]Target frequency. Does not account for routing delays.

FPGA Family	Resources	$f_{\max}$	Throughput
Altera® Cyclone® 10 GX†	13638 ALM, 8 M20K, 25 DSP	134.75 MHz	17.25 Gbps
Altera® Agilex® 7 F‡	14949 ALM, 8 M20K, 25 DSP	236.46 MHz	30.27 Gbps
AMD® Zynq® MPSoC§	24344 LUT , 100 DSP	305.44 MHz	39.10 Gbps
AMD® Versal® Prime§	25357 LUT , 75 DSP	362.84 MHz	46.44 Gbps
Lattice® CertusPro-NX® ¶	51337 LUT4, 8 EBR, 200/100 MULT9/MULT18	94.99 MHz	12.16 Gbps
Lattice® Avant® ¶	42855 LUT4 , 50 MULT18	104.92 MHz	13.43 Gbps
Microchip® PolarFire® ‖	37614 4LUT, 24 uSRAM, 100 Math	143.76 MHz	18.40 Gbps

Table 1: Resource usage and performance of XIP2113H on various FPGA families.

Total Gate Equivalent [1]	Total Cell Area [2] (µm²)	f_{target} [3]
279426	72427	1.0 GHz

Table 2: Logic requirements and performance of XIP2113H on TSMC 16 nm FF+ process.

Type	Address depth	Data Width (bits)	Total (bits)
SPRAM	16	134	2144
SPRAM	16	134	2144
			4288

Table 3: Memory requirements of XIP2113H.

Throughput and Latency

The latency of XIP2113H depends on the length of the message. After a certain initial latency, XIP2113H is able to process one 128-bit data block in a clock cycle. However, as mentioned, XIP2113H includes logic to automatically optimize this initial latency for short messages.

XIP2113H also supports a high frequency version which utilizes a deeper internal pipeline and achieves higher maximum clock frequencies. This version has longer latencies but achieve higher throughputs for long messages. Contact Xiphera for additional information.

Because XIP2113H can process one 128-bit data block per clock cycle, the peak throughput can be calculated as $128 \cdot f$ bits/s, where f is the clock frequency. The peak throughput is an accurate estimate for the actual throughput for long messages.