XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP3324B: HKDF/HMAC/SHA-512

SHA-512 IP Core with Extended Functionalities

Resource Sheet

2026-05-06

sales@xiphera.com

Introduction

This document details FPGA and ASIC resource requirements and performance of XIP3324B with the default configuration—for example, instantiation parameters, supported features, and selected bus interface—of XIP3324B.

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.

FPGA Family	Resources	$f_{\max}$
Altera® Cyclone® 10 GX[†]	2527 ALM, 6 M20K	188.47 MHz
Altera® Agilex® 5[†]	2695 ALM, 6 M20K	145.16 MHz
AMD® Zynq® MPSoC[‡]	2696 LUT, 2 RAMB36	262.47 MHz
AMD® Versal® Prime[‡]	3504 LUT, 2 RAMB36	359.07 MHz
Lattice® CertusPro-NX® [§]	6010 LUT4, 6 EBR	85.24 MHz
Lattice® Avant® [§]	6261 LUT4, 2 EBR	108.07 MHz
Microchip® PolarFire® [¶]	5149 4LUT, 6/8 uSRAM/LSRAM	165.70 MHz

Table 1: Resource usage and performance of XIP3324B on various FPGA families.

[†]Quartus Prime Pro 25.1.0, 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.

ASIC Resources and Performance

Table 2 describes the logic requirements of XIP3324B on the TSMC 16nm FinFET Plus Low Leakage standard cell process. The results were obtained by synthesising XIP3324B with Synopsys® DC T-2022.03 using default settings.

Total Gate Equivalent [1]	Total Cell Area [2] (µm²)	f_{target} [3]
27022	7004	750 MHz

Table 2: Logic requirements and performance of XIP3324B on TSMC 16 nm FF+ process.

Table 3 presents the total memories inside the XIP3324B.

Type	Address depth	Data Width (bits)	Total (bits)
Simple Dual Port	18	65	1170
Simple Dual Port	32	68	2176
			3346

Table 3: Memory requirements of XIP3324B.

Throughput and Latency

SHA512

The latency of SHA512 computation depends on the length of the message. Computation of one iteration takes 86 clock cycles after the last block for that message block has been written for SHA512. Because reading the resulting hash value takes in minimum 8 clock cycles and the latency for initiating and finalizing a hash computation is 3 clocks cycles, the effective minimum latency of a SHA512 computation (for an at most 64-bit message) is 97 clock cycles.

HMAC-SHA512

The minimum latency for HMAC-SHA512 is 338 clock cycles after the message has been written until the authentication tag has been computed because it requires in minimum four iterations of SHA512. The minimum latency taking into account the initial latency and reading the tag is 370 clock cycles. The asymptotic throughput (bits per clock cycle) is:

$$\frac{1024 \cdot P}{252 + 86 \cdot P} \frac{\text{b}}{\text{cc}} \approx 11.9 \frac{\text{b}}{\text{cc}}, \quad \text{where } P \text{ is the number of 1024-bit message blocks.}$$

HKDF-SHA512

Assuming that input keying material (with SHA padding) fits into one SHA512 block, then the latency for HKDF-extract is the minimum latency for HMAC. The throughput can be calculated by multiplying the bits per clock cycle with the operating frequency.

[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.