XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP3322B: HKDF/HMAC/SHA-256

SHA-256 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 XIP3322B with the default configuration—for example, instantiation parameters, supported features, and selected bus interface—of XIP3322B.

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[†]	1262 ALM, 3 M20K	242.07 MHz
Altera® Agilex® 5[†]	1298 ALM, 3 M20K	179.99 MHz
AMD® Zynq® MPSoC[‡]	1379 LUT, 1 RAMB36	335.12 MHz
AMD® Versal® Prime[‡]	1858 LUT, 1 RAMB36	395.73 MHz
Lattice® Avant® [§]	2883 LUT4, 1 EBR	128.30 MHz
Lattice® CertusPro-NX® [§]	2940 LUT4, 2 EBR	109.77 MHz
Microchip® PolarFire® [¶]	2762 4LUT, 3/4 uSRAM/LSRAM	187.20 MHz

Table 1: Resource usage and performance of XIP3322B 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 XIP3322B on the TSMC 16nm FinFET Plus Low Leakage standard cell process. The results were obtained by synthesising XIP3322B with Synopsys® DC T-2022.03 using default settings.

Total Gate Equivalent [1]	Total Cell Area [2] (µm²)	f_{target} [3]
12827	3325	750 MHz

Table 2: Logic requirements and performance of XIP3322B on TSMC 16 nm FF+ process.

Table 3 presents the total memories inside the XIP3322B.

Type	Address depth	Data Width (bits)	Total (bits)
Simple Dual Port	18	33	594
Simple Dual Port	32	35	1120
			1714

Table 3: Memory requirements of XIP3322B.

Throughput and Latency

SHA256

The latency of computation depends on the length of the message. Computation of one iteration takes 72 clock cycles after the last block for that message block has been written for SHA256. An iteration is computed for each 512-bit block of the message for SHA256. 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 SHA256 computation (for an at most 64-bit message) is 83 clock cycles.

HMAC-SHA256

The minimum latency for HMAC-SHA256 is 275 clock cycles after the message has been written until the authentication tag has been computed because it requires in minimum four iterations of SHA256. The minimum latency taking into account the initial latency and reading the tag is 306 clock cycles. The asymptotic throughput (bits per clock cycle) is:

$$\frac{512 \cdot P}{234 + 72 \cdot P} \frac{\text{b}}{\text{cc}} \approx 7,\overline{1} \frac{\text{b}}{\text{cc}}, \quad \text{where } P \text{ is the number of 512-bit message blocks.}$$

HKDF-SHA256

Assuming that input keying material (with SHA padding) fits into one SHA256 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.