PEACE OF MIND IN A DANGEROUS WORLD

XIP6220B: ML-DSA-44/65/87

Balanced Post-Quantum Digital Signature IP Core

Resource Sheet

2026-05-06

sales@xiphera.com

Introduction

This document details FPGA and ASIC resource requirements and performance of XIP6220B with the default configuration—for example, instantiation parameters, supported features, and selected bus interface—of XIP6220B.

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® Agilex® 5†	10011 ALM, 22 M20K, 1 DSP	223.71 MHz
Altera® Cyclone® 10 GX†	8842 ALM, 20 M20K, 1 DSP	228.10 MHz
AMD® Versal® Prime‡	13604 LUT, 7/1 RAMB36/18, 1 DSP	400.00 MHz
AMD® Zynq® MPSoC‡	13026 LUT, 7/1 RAMB36/18, 2 DSP	342.35 MHz
Lattice® Avant® §	25229 LUT4, 11 EBR, 2 MULT18	132.75 MHz
Lattice® CertusPro-NX® §	25750 LUT4, 22 EBR, 8/4 MULT9/MULT18	119.15 MHz
Microchip® PolarFire® ¶	27235 4LUT, 4/18 uSRAM/LSRAM, 4 Math	99.00 MHz

Table 1: Resource usage and performance of XIP6220B 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 XIP6220B on the TSMC 16nm FinFET Plus Low Leakage standard cell process. The results were obtained by synthesising XIP6220B with Synopsys® DC T-2022.03 using default settings.

Total Gate Equivalent [1]	Total Cell Area [2] (µm²)	f_{target} [3]
69984	18140	750 MHz

Table 2: Logic requirements and performance of XIP6220B on TSMC 16 nm FF+ process.

Table 3 presents the total memories inside the XIP6220B.

Type	Address depth	Data Width (bits)	Total (bits)
ROM	524	23	12052
Simple Dual Port	2048	64	131072
True Dual Port	256	2	512
True Dual Port	4096	23	94208
True Dual Port	4096	23	94208
			332052

Table 3: Memory requirements of XIP6220B.

Throughput and Latency

Computation latencies of XIP6220B in clock cycles for KeyGen, Sign, and Verify for all parameter sets of ML-DSA are collected in Table 4. It shows latency results for 100 randomly selected test cases for each operation. It gives the average (mean) values of these 100 vectors. The latencies for Verify are for successful verifications (PASSED), and the latencies for unsuccessful verifications (FAILED) may be significantly shorter in some cases.

[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.

Operation	ML-DSA-44	ML-DSA-65	ML-DSA-87
KeyGen	36465	60245	92556
Sign	262793	472919	617039
Verify	42065	66757	102475
Memory-Clear	4110	4110	4110

Table 4: Latencies (in clock cycles) collected from 100 random vectors for each operation.