XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP6110B: ML-KEM 512/768/1024

Balanced Post-Quantum Key Encapsulation IP Core

Resource Sheet

2026-05-06

sales@xiphera.com

Introduction

This document details FPGA and ASIC resource requirements and performance of XIP6110B with the default configuration—for example, instantiation parameters, supported features, and selected bus interface—of XIP6110B.

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[†]	5917 ALM, 11 M20K, 3 DSP	150.40 MHz
Altera® Agilex® 5[†]	6270 ALM, 13 M20K, 3 DSP	127.68 MHz
AMD® Zynq® MPSoC[‡]	8646 LUT, 4/3 RAMB36/18, 6 DSP	236.46 MHz
AMD® Versal® Prime[‡]	8898 LUT, 6/1 RAMB36/18, 6 DSP	294.38 MHz
Lattice® Avant® [§]	12978 LUT4, 9 EBR, 4 MULT18	131.37 MHz
Lattice® CertusPro-NX® [§]	13497 LUT4, 11 EBR, 10/5 MULT9/MULT18	97.53 MHz
Microchip® PolarFire® [¶]	14974 4LUT, 6 LSRAM, 7 Math	121.36 MHz

Table 1: Resource usage and performance of XIP6110B 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 XIP6110B on the TSMC 16nm FinFET Plus Low Leakage standard cell process. The results were obtained by synthesising XIP6110B with Synopsys® DC T-2022.03 using default settings.

Total Gate Equivalent [1]	Total Cell Area [2] (µm²)	f_{target} [3]
53435	13850	750 MHz

Table 2: Logic requirements and performance of XIP6110B on TSMC 16 nm FF+ process.

Table 3 presents the total memories inside the XIP6110B.

Type	Address depth	Data Width (bits)	Total (bits)
ROM	256	12	3072
SPRAM	1024	64	65536
True Dual Port	4096	12	49152
True Dual Port	4096	12	49152
			166912

Table 3: Memory requirements of XIP6110B.

Throughput and Latency

The average latencies of different instructions are collected into Table 4. They are calculated from 100 randomly chosen test vectors for each instruction.

Latencies of some of the instructions vary between test vectors because those instructions perform rejection samplings internally. Although these latencies are not strictly speaking constant, they are still fully independent of any secret values processed during the instruction and, therefore, they are “constant time” in respect to side channel attacks and fully immune to all timing attacks. It is also noteworthy that the variations in latencies are small (typically within some tens of clock cycles) as shown by the standard deviations and minimum/maximum values listed in Table 4.

[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-KEM-512	ML-KEM-768	ML-KEM-1024
KeyGen	13790	27332	40205
Encaps	20085	35295	49299
Decaps	28676	47654	63388
Check-ek	1314	1965	2616
Check-dk	391	562	733

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