PEACE OF MIND IN A DANGEROUS WORLD

XIP4001C: X25519

Curve25519 Key Exchange IP Core

Resource Sheet

2026-05-06

sales@xiphera.com

Introduction

This document details FPGA and ASIC resource requirements and performance of XIP4001C with the default configuration—for example, instantiation parameters, supported features, and selected bus interface—of XIP4001C.

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 XIP4001C on the TSMC 16nm FinFET Plus Low Leakage standard cell process. The results were obtained by synthesising XIP4001C with Synopsys® DC W-2024.09-SP2 using default settings.
Table 3 presents the total memories inside the XIP4001C.

[†]Quartus Prime Standard 24.1std.0, default compilation settings, industrial speedgrade.
[‡]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.
[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	$f_{\max}$
Altera® Cyclone® 10 LP†	720 LE, 1 M9K, 2 Mult. (9bit)	155.33 MHz
Altera® Agilex® 3 C‡	334 ALM, 2 M20K, 1 DSP	268.02 MHz
Altera® Cyclone® 10 GX‡	305 ALM, 2 M20K, 1 DSP	259.07 MHz
AMD® Spartan-7® §	472 LUT, 1 RAMB18, 1 DSP	214.22 MHz
AMD® Zynq-7000® §	472 LUT, 1 RAMB18, 1 DSP	193.39 MHz
Lattice® Avant® ¶	2054 LUT4, 1 EBR, 1 MULT18	181.78 MHz
Lattice® CertusPro-NX® ¶	1074 LUT4, 1 EBR, 2/1 MULT9/MULT18	175.65 MHz
Microchip® PolarFire® ‖	1412 4LUT, 1 LSRAM, 1 Math	274.50 MHz

Table 1: Resource usage and performance of XIP4001C on various FPGA families.

Total Gate Equivalent [1]	Total Cell Area [2] (µm²)	f_{target} [3]
3516	911	667 MHz

Table 2: Logic requirements and performance of XIP4001C on TSMC 16 nm FF+ process.

Type	Address depth	Data Width (bits)	Total (bits)
ROM	512	17	8704
Simple Dual Port	512	18	9216
			17920

Table 3: Memory requirements of XIP4001C.