PEACE OF MIND IN A DANGEROUS WORLD

XIP41X3C: NIST P-224/P-256/P-384/P-521 ECDH+ECDSA

Compact ECC IP Cores supporting ECDH and ECDSA on NIST P-224/P-256/P-384/P-521

Resource Sheet

2026-05-06

sales@xiphera.com

Introduction

This document details FPGA and ASIC resource requirements and performance of XIP41X3C with the default configuration—for example, instantiation parameters, supported features, and selected bus interface—of XIP41X3C.

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 XIP41X3C on the TSMC 16nm FinFET Plus Low Leakage standard cell process. The results were obtained by synthesising XIP41X3C with Synopsys® DC T-2022.03 using default settings.

[†]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	$f_{\max}$
XIP4113C		
Altera® Agilex® 3 C†	785 ALM, 7 M20K, 1 DSP	170.24 MHz
Altera® Cyclone® 10 GX†	734 ALM, 7 M20K, 1 DSP	155.16 MHz
AMD® Zynq-7000® ‡	987 LUT, 2/1 RAMB36/18, 1 DSP	96.67 MHz
AMD® Spartan-7® ‡	972 LUT, 2/1 RAMB36/18, 1 DSP	121.64 MHz
Lattice® CertusPro-NX® §	4182 LUT4, 4 EBR, 2/1 MULT9/MULT18	94.27 MHz
Lattice® Avant® §	8910 LUT4, 3 EBR, 1 MULT18	136.48 MHz
Microchip® PolarFire® ¶	5291 4LUT, 1/2 uSRAM/LSRAM, 1 Math	192.34 MHz
XIP4123C		
Altera® Cyclone® 10 GX†	739 ALM, 7 M20K, 1 DSP	156.81 MHz
Altera® Agilex® 3 C†	783 ALM, 7 M20K, 1 DSP	162.89 MHz
AMD® Spartan-7® ‡	972 LUT, 2/1 RAMB36/18, 1 DSP	121.64 MHz
AMD® Zynq-7000® ‡	987 LUT, 2/1 RAMB36/18, 1 DSP	96.67 MHz
Lattice® Avant® §	8883 LUT4, 3 EBR, 1 MULT18	143.21 MHz
Lattice® CertusPro-NX® §	4275 LUT4, 4 EBR, 2/1 MULT9/MULT18	101.15 MHz
Microchip® PolarFire® ¶	5411 4LUT, 1/2 uSRAM/LSRAM, 1 Math	182.98 MHz
XIP4133C		
Altera® Cyclone® 10 GX†	739 ALM, 7 M20K, 1 DSP	156.74 MHz
Altera® Agilex® 3 C†	783 ALM, 7 M20K, 1 DSP	162.89 MHz
AMD® Spartan-7® ‡	972 LUT, 2/1 RAMB36/18, 1 DSP	121.64 MHz
AMD® Zynq-7000® ‡	987 LUT, 2/1 RAMB36/18, 1 DSP	96.67 MHz
Lattice® Avant® §	8878 LUT4, 3 EBR, 1 MULT18	139.47 MHz
Lattice® CertusPro-NX® §	4419 LUT4, 4 EBR, 2/1 MULT9/MULT18	105.43 MHz
Microchip® PolarFire® ¶	5604 4LUT, 1/2 uSRAM/LSRAM, 1 Math	174.55 MHz
XIP4143C		
Altera® Agilex® 3 C†	831 ALM, 9 M20K, 1 DSP	166.94 MHz
Altera® Cyclone® 10 GX†	770 ALM, 9 M20K, 1 DSP	163.83 MHz
AMD® Zynq-7000® ‡	981 LUT, 3 RAMB36, 1 DSP	89.73 MHz
AMD® Spartan-7® ‡	1004 LUT, 3 RAMB36, 1 DSP	111.77 MHz
Lattice® Avant® §	8907 LUT4, 4 EBR, 1 MULT18	133.21 MHz
Lattice® CertusPro-NX® §	4342 LUT4, 6 EBR, 2/1 MULT9/MULT18	101.67 MHz
Microchip® PolarFire® ¶	5735 4LUT, 1/4 uSRAM/LSRAM, 1 Math	177.90 MHz

Table 1: Resource usage and performance of XIP41X3C on various FPGA families.

Core version	Total Gate Equivalent [1]	Total Cell Area [2] (µm²)	f_{target} [3]
XIP4113C	9173	2378	400 MHz
XIP4123C	9357	2425	400 MHz
XIP4133C	9530	2470	400 MHz
XIP4143C	9551	2476	400 MHz

Table 2: Logic requirements and performance of XIP41X3C on TSMC 16 nm FF+ process.

Table 3 presents the total memories inside the XIP41X3C.

Type	Address depth	Data Width (bits)	Total (bits)
XIP4113C-XIP4133C			
ROM	256	16	4096
ROM	256	16	4096
ROM	2048	29	59392
SPRAM	1024	16	16384
SPRAM	1024	16	16384
			100352
XIP4143C			
ROM	256	16	4096
ROM	256	16	4096
ROM	2048	29	59392
SPRAM	2048	16	32768
SPRAM	2048	16	32768
			133120

Table 3: Memory requirements of XIP41X3C.

Operation	XIP4113C	XIP4123C	XIP4133C	XIP4143C
EC-KeyGen	2 748k	4 308k	10 816k	21 955k
EC-DH	2 750k	4 310k	10 820k	21 960k
ECDSA-Sign	3 370k	5 126k	13 250k	27 588k
ECDSA-Verify	3 215k[1]	4 823k[1]	12 605k[1]	26 566k[1]

[1] The latency is an average from 10 random test vectors, as the operation is not constant.

Table 4: Approximate latencies of XIP41X3C in clock cycles

Throughput and Latency

Table 4 collects the latencies of operations supported by XIP41X3C. The time for an operation can be obtained by dividing the latency with the clock frequency. For example, a computation of EC-KeyGen for XIP4123C takes 21.5 ms with a 200 MHz clock.