XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP4200H: ECC ACCELERATOR

High-Speed Elliptic Curve Cryptography Accelerator for ECDH and ECDSA

Resource Sheet

2026-05-06

sales@xiphera.com

Introduction

This document details FPGA and ASIC resource requirements and performance of XIP4200H with the default configuration—for example, instantiation parameters, supported features, and selected bus interface—of XIP4200H.

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 XIP4200H on the TSMC 16nm FinFET Plus Low Leakage standard cell process. The results were obtained by synthesising XIP4200H with Synopsys® DC T-2022.03 using default settings.
Table 3 presents the total memories inside the XIP4200H.

[†]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® Agilex® 7 F†	24256 ALM, 18 M20K, 48 DSP	168.29 MHz
Altera® Cyclone® 10 GX†	21905 ALM, 18 M20K, 49 DSP	93.77 MHz
AMD® Zynq® MPSoC‡	8964 LUT, 4 RAMB36, 47 DSP	266.60 MHz
AMD® Versal® Prime‡	10291 LUT, 4 RAMB36, 47 DSP	370.23 MHz
Lattice® CertusPro-NX® §	18777 LUT4, 8 EBR, 175/87 MULT9/MULT18	79.86 MHz
Lattice® Avant® §	24078 LUT4 , 87 MULT18	83.04 MHz
Microchip® PolarFire® ¶	21710 4LUT, 8 LSRAM, 88 Math	145.31 MHz

Table 1: Resource usage and performance of XIP4200H on various FPGA families.

Total Gate Equivalent [1]	Total Cell Area [2] (µm²)	f_{target} [3]
228485	59223	1.0 GHz

Table 2: Logic requirements and performance of XIP4200H on TSMC 16 nm FF+ process.

Type	Address depth	Data Width (bits)	Total (bits)
ROM	1024	128	131072
ROM	2048	32	65536
True Dual Port	512	32	16384
True Dual Port	512	32	16384
True Dual Port	512	32	16384
True Dual Port	512	32	16384
			262144

Table 3: Memory requirements of XIP4200H.

Throughput and Latency

Table 4 collects the latencies of operations supported by XIP4200H. The time for an operation can be obtained by dividing the latency with the clock frequency. For example, if XIP4200H is clocked with a 200 MHz clock, a key generation on P-256 takes 854 μs, which equals to about 1170 operations in a second. The latencies in Table 4 represent successful operations and the latency of a failed operation may be different from the given one. For example, KEYGEN operation terminates quickly if the provided scalar is not in the interval $[1, q-1]$. Notice that these differences in latencies do not have an effect on the side-channel properties.

Context	KEYGEN	SIGN	VERIFY[1]	Fast-DH[2]	Secure-DH[3]
CTX_NIST_P192	170898	186347	252446	197558	284151
CTX_NIST_P224	173500	191005	292291	227220	330049
CTX_NIST_P256	170726	189615	322843	254213	370574
CTX_NIST_P384	257236	300082	687817	530947	769220
CTX_NIST_P521	871671	980962	1689763	1266249	1832275

Context	CTX_NIST*	ECDSA_KEY	DH_KEY	DH_RAND_KEY	DH_RERAND_KEY
CTX_NIST_P192	159	168	82	239	162
CTX_NIST_P224	159	168	82	239	162
CTX_NIST_P256	159	168	82	239	162
CTX_NIST_P384	159	184	84	250	164
CTX_NIST_P521	159	216	88	272	168

Context	CHECK_POINT	CHECK_SCALAR
CTX_NIST_P192	519	139
CTX_NIST_P224	519	139
CTX_NIST_P256	519	139
CTX_NIST_P384	681	147
CTX_NIST_P521	1115	163

[1] The latency is an average of 10 randomly generated successful verifications rounded to the nearest integer.
[2] Fast-DH is DH where the key has been set with DH_KEY.
[3] Secure-DH is DH where the key has been set with DH_RAND_KEY (and DH_RERAND_KEY).

Table 4: Latencies of XIP4200H