XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

# XIP41X3C: NIST P-256/P-384 ECDH+ECDSA

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

Product Brief
ver. 1.0
May 5, 2023

sales@xiphera.com

## Introduction

XIP41x3C from Xiphera are a family of compact Intellectual Property (IP) cores implementing Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) on NIST prime curves [1]. ECDH and ECDSA on NIST prime curves are widely used in various cryptographic protocols and systems.

The XIP41x3C family currently includes two IP cores:

- **XIP4123C** for ECDH and ECDSA on the NIST P-256 elliptic curve and
- **XIP4133C** for ECDH and ECDSA on the NIST P-384 elliptic curve.

These two curves are the most commonly used NIST curves today. XIP41x3C has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP41x3C does not rely on any FPGA manufacturer-specific features.

## Key Features

- **Minimal Resource Requirements:** XIP41x3C require for example 1118 LUTs in Xilinx Artix-7® and use only 1-2 multipliers/DSP blocks and 1-3 internal memory block in a typical FPGA implementation.
- **Secure Architecture:** The execution time of XIP41x3C is independent of the secret values and, consequently, provides full protection against timing-based side-channel attacks. Additionally, the pattern of operations during computations is independent of the secrets. XIP41x3C have two interfaces which can be used for separating access to security-critical values.

- **Standard Compliance:** XIP41x3C are compliant with FIPS 186-4 [1] and SP 800-56A [2]. XIP41x3C can be used as a part of numerous public-key systems and protocols including IKEv2 [4, 6, 3] and TLS 1.3 (RFC 8446) [5].
- **Easy Integration:** The 16-bit interface of XIP41x3C supports easy integration to various systems.

## Functionality

XIP41x3C can be used for elliptic curve key generation, computation of Diffie-Hellman shared secrets as well as for ECDSA signature generation and verification. Hence, they are very versatile IP cores that can be used in a variety of cryptographic protocols and systems. The NIST prime curves are arguably still the most used elliptic curves and it is common for practical systems using ECC to support P-256 and/or P-384.

The main optimization objective for XIP41x3C has been on reducing the resource requirements and XIP41x3C require only very few resources considering the complexity of the operations that they support. They also include various security checks for the input values that prevent accidental misuses that could compromise the security of the cryptosystem. These include validations that the input points are in fact a valid point on the curve and in-built prevention of accidential misuse of values that should be used only once (ECDSA nonces). XIP41x3C also include protections against side-channel attacks, the most important of which is the fully constant-time operation of all operations that use secret values.

XIP41x3C implements the main elliptic curve operations. XIP41x3C requires an external random number generator (for example, XIP8001B) and ECDSA also requires an external hash function.

## Block Diagram

The internal high-level block diagram of XIP41x3C is depicted in Figure 1.

## Interfaces

The external interfaces of XIP41x3C are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP41x3C. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP41x3C, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

## FPGA Resources and Performance

Tables 1 presents the FPGA resource requirements for representative implementations on different FPGA architectures. On request, the resource estimates can also be supplied for other FPGA families.

*Quartus® Prime Lite 20.1.1, default compilation settings, industrial speedgrade.
†Vivado 2021.2, default compilation settings, industrial speedgrade.
‡Radiant 2022.1.0, default compilation settings, synthesised with Synplify.
§Diamond 3.12.0, default compilation settings, synthesised with Synplify.

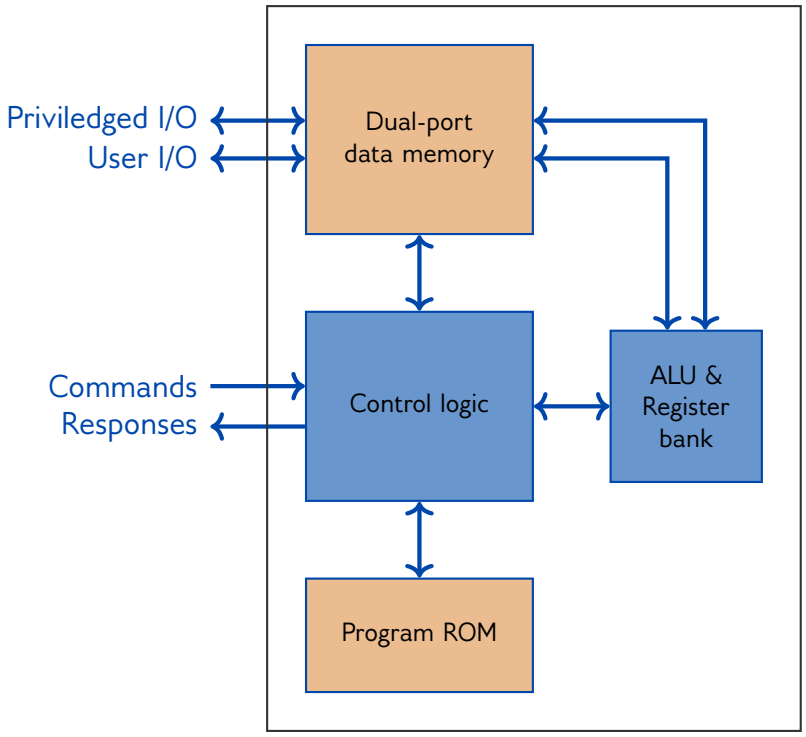


Figure 1: Internal high-level block diagram of XIP41x3C

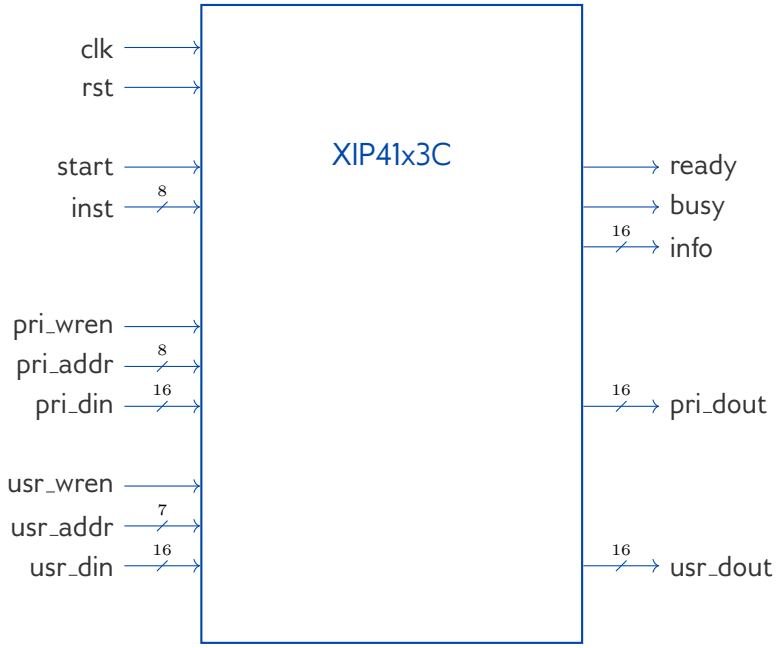


Figure 2: External interfaces of XIP41x3C

## Example Use Cases

XIP41x3C have several applications, as ECC on NIST prime curves are popular asymmetric cryptography schemes that are used in a number of standardized communications protocols, including IPSEC, MACSEC and TLS (Transport Layer Security) versions 1.2 and 1.3.

[¶]Libero 2022.1.0.10, default compilation settings, industrial speedgrade.

| Device | Resources | $f_{MAX}$ |
|---|---|---|
| **XIP4123C** | | |
| Intel® Cyclone® 10 LP* | 4727 LE, 2 M9K , 2 Mult. (9bit) | 80.61 MHz |
| Intel® Cyclone® V SX SoC* | 1549 ALM, 2 M10K , 1 DSP | 132.33 MHz |
| Xilinx® Spartan-7® † | 1119 LUT, 2/1 RAMB36/18 , 1 DSP | 105.09 MHz |
| Xilinx® Artix-7® † | 1118 LUT, 2/1 RAMB36/18 , 1 DSP | 105.64 MHz |
| Xilinx® Zynq-7000® † | 1130 LUT, 2/1 RAMB36/18 , 1 DSP | 87.28 MHz |
| Lattice® CertusPro-NX® ‡ | 4498 LUT4, 1 EBR, 2/1 MULT9/MULT18 | 74.27 MHz |
| Lattice® ECP5® § | 4481 LUT4, 1 EBR, 1 MULT18 | 80.37 MHz |
| Microchip® PolarFire® ¶ | 4778 4LUTs, 1/1 uSRAM/LSRAM, 1 Math | 67.45 MHz |
| **XIP4133C** | | |
| Intel® Cyclone® 10 LP* | 4941 LE, 2 M9K , 2 Mult. (9bit) | 77.72 MHz |
| Intel® Cyclone® V SX SoC* | 1571 ALM, 2 M10K , 1 DSP | 122.37 MHz |
| Xilinx® Spartan-7® † | 1185 LUT, 2/1 RAMB36/18 , 1 DSP | 111.32 MHz |
| Xilinx® Artix-7® † | 1185 LUT, 2/1 RAMB36/18 , 1 DSP | 117.94 MHz |
| Xilinx® Zynq-7000® † | 1204 LUT, 2/1 RAMB36/18 , 1 DSP | 94.11 MHz |
| Lattice® CertusPro-NX® ‡ | 4559 LUT4, 1 EBR, 2/1 MULT9/MULT18 | 73.26 MHz |
| Lattice® ECP5® § | 4608 LUT4, 1 EBR, 1 MULT18 | 75.94 MHz |
| Microchip® PolarFire® ¶ | 4835 4LUTs, 1/1 uSRAM/LSRAM, 1 Math | 85.06 MHz |

Table 1: Resource usage and performance of both variants of the XIP41x3C on representative FPGA families.

## Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP41x3C can be shipped in a number of formats, including netlist, source code, or encrypted source code. Additionally, a comprehensive VHDL testbench and a detailed datasheet are included.

## About Xiphera

Xiphera specializes in secure and efficient implementations of standardized cryptographic algorithms on Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs). Our product portfolio includes individual cryptographic Intellectual Property (IP) cores, as well as comprehensive security solutions built from a combination of individual IP cores.

Xiphera is a Finnish company operating under the laws of the Republic of Finland, and is fully owned by Finnish citizens and institutional investors.

## Contact

Xiphera Oy
Tekniikantie 12
FIN-02150 Espoo
Finland
sales@xiphera.com
+358 20 730 5252

## References

[1] FIPS PUB 186-4 Digital Signature Standard (DSS). Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2013.

[2] SP 800-56A Rev.3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2018.

[3] David E. Fu and Jerome Solinas. IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA). RFC 4754, January 2007.

[4] Charlie Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306, December 2005.

[5] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018.

[6] Jerome Solinas and David E. Fu. Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2. RFC 5903, June 2010.