PEACE OF MIND IN A DANGEROUS WORLD

XIP4200H: ECC ACCELERATOR

High-Speed Elliptic Curve Cryptography Accelerator for ECDH and ECDSA

Product Brief
ver. 1.1.1
October 8, 2024

sales@xiphera.com

Introduction

XIP4200H from Xiphera is an Intellectual Property (IP) core implementing Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA). This IP core demonstrates a capability of executing over a thousand operations per second when deployed on a modern Field-Programmable Gate Array (FPGA) or Application-Specific Integrated Circuit (ASIC). The IP core comprehensively covers all NIST P curves, namely P-192, P-224, P-256, P-384, and P-521, within a singular IP core instance. It also facilitates the utilization of user-specified elliptic curves. The IP core includes hardened protections against multiple-trace side-channel attacks.

XIP4200H has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP4200H does not rely on any FPGA manufacturer-specific features.

Key Features

- **High Speed:** XIP4200H is optimized for high speed. For example, a key generation on NIST P-256 requires approximately 180k clock cycles, and XIP4200H can compute over a thousand operations per second on modern high-speed Microchip® FPGAs.

- **Iersatile Curve Support:** XIP4200H natively supports all NIST P curves [2] within a single IP core instance. Customer-specified curves can be added into the set of supported curves.

- **Secure Architecture:** Execution time and pattern of operations are independent of the secret values providing full protection against timing-based side-channel attacks. XIP4200H includes hardened protections against multi-trace side-channel attacks (for example, DPA). XIP4200H is fully RTL-based with no embedded software or CPU components.

- **Standard Compliance:** XIP4200H is compliant with FIPS 186-5 [3] and SP 800-56A [1]. XIP4200H can be used as a part of numerous public-key systems and protocols including IKEv2 [5] [8] [4] and TLS 1.3 [7].
- **Easy Integration:** The simple 32-bit interface supports easy system integration.

Functionality

XIP4200H can be used for elliptic curve key generation, computation of Diffe-Hellman shared secrets as well as for ECDSA signature generation and verification [3]. It is a very versatile IP core that can be used in a variety of cryptographic protocols and systems. XIP4200H supports all NIST P curves [2]: P-192, P-224, P-256, P-384, and P-521. NIST P curves are the most widely used elliptic curves and systems using ECC commonly support P-256 and/or P-384. It is possible to prepare customer-specific sets of supported curves including even customer-specified elliptic curves. Xiphera will also be extending the set of natively supported curves in future versions of XIP4200H (for example, Brainpool curves [**?**] as well as Curve25519 and Curve448 [6]).

The main optimization objective for XIP4200H is high performance. It supports high-speed computation of elliptic curve cryptography operations typically used in practical protocols and systems including key generation, digital signature signing and verification, and calculation of Diffie–Hellman shared secret. It includes various security checks for the input values to prevent accidental or deliberate misuse that could compromise the security of the cryptosystem. These include validating that the input points are valid points on the curve and prevention of accidential misuse of values that should be used only once (ECDSA nonces).

XIP4200H includes advanced protections against side-channel attacks. Most importantly, all operations in XIP4200H are fully constant time and follow regular patterns of sub-operations. The only exception is the ECDSA verification which does not utilize any secret values and, thus, cannot be a target for side-channel attacks. XIP4200H also allows to randomize long-term keys (in particular, the ECDSA signing key) so that each calculation using the same key happens in a different randomized form. Also the temporary values during elliptic curve operations are randomized. These protections provide very high security even against side-channel attacks utilizing multiple measurements with the same key, which are sometimes called multi-trace or DPA attacks.

XIP4200H implements the main elliptic curve operations and requires an external random number generator (e.g. XIP8001B). Use of ECDSA also requires an external hash function.

Block Diagram

The internal high-level block diagram of XIP4200H is depicted in Figure 1.

Interfaces

The external interfaces of XIP4200H are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP4200H. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP4200H, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

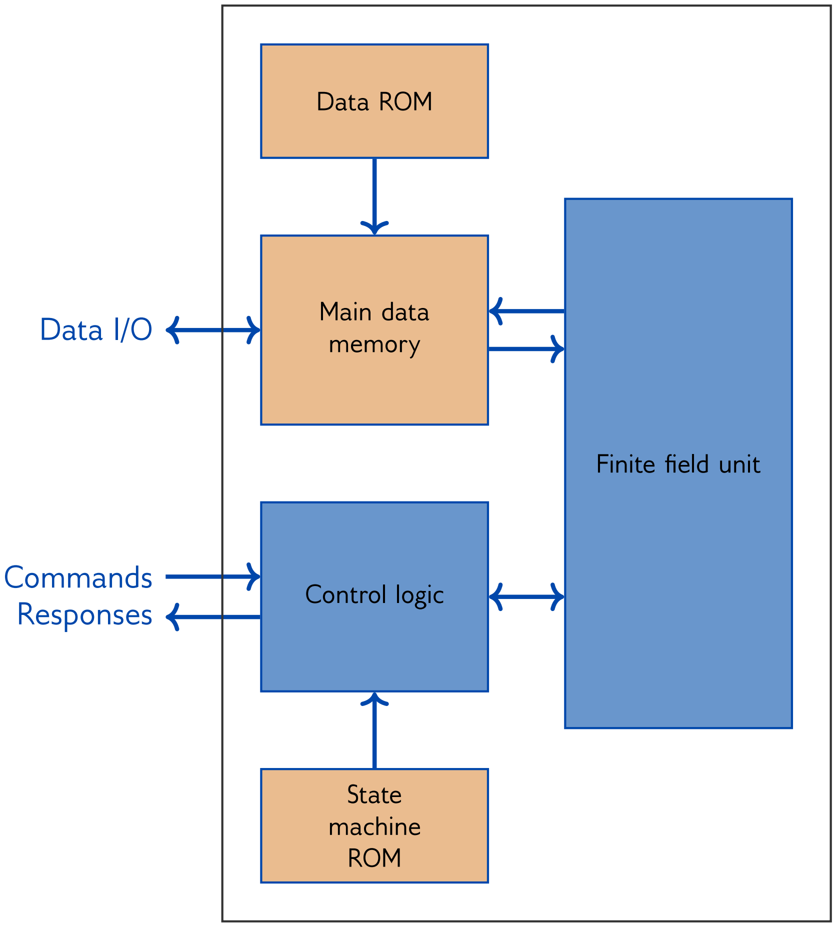

Figure 1: Internal high-level block diagram of XIP4200H

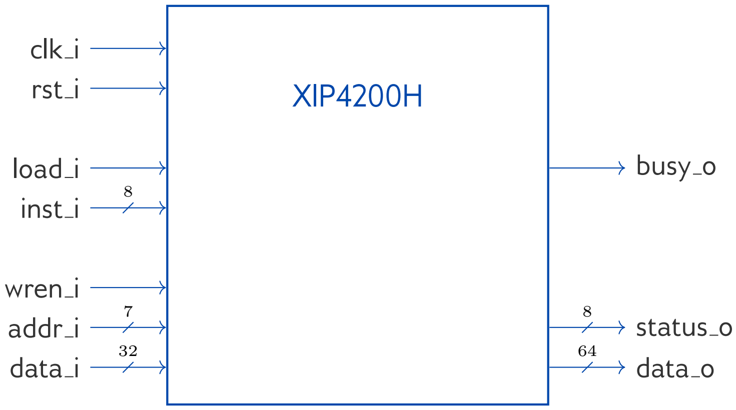

Figure 2: External interfaces of XIP4200H

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.

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

Device	Resources	$f_{\max}$
Microchip® PolarFire® [¶]	109746 4LUT, 1/8 uSRAM/LSRAM, 90 Math	75.28 MHz

Table 1: Resource usage and performance of both variants of the XIP4200H on representative FPGA families.

Example Use Cases

XIP4200H has 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.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP4200H can be shipped in a number of formats, including netlist, source code, or encrypted source code. Additionally, synthesis scripts, a comprehensive testbench, and a detailed datasheet including an integration guide 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 fully in-house designed 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] 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.

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

[3] NIST Computer Security Division. FIPS PUB 186-5 Digital Signature Standard (DSS). FIPS Publication 186-5, National Institute of Standards & Technology, Gaithersburg, MD, United States, February 2023.

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

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

[6] Adam Langley, Mike Hamburg, and Sean Turner. Elliptic Curves for Security. RFC 7748, January 2016.

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

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