XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

# XIP6220B: ML-DSA-44/65/87

## Balanced Post-Quantum Digital Signature IP Core

Product Brief
ver. 1.0.2
August 28, 2024

sales@xiphera.com

## Introduction

XIP6220B from Xiphera is an Intellectual Property (IP) core for ML-DSA (previously known as CRYSTALS-Dilithium) [2] post-quantum digital signature algorithm. It currently supports signature verification operation for all three ML-DSA variants ML-DSA-44, ML-DSA-65, and ML-DSA-87 as defined in the draft standard [2] from August 2023. Support for key generation and signature generation will be added within a relatively short time frame after NIST finalises the standard. XIP6220B is optimized for a good balance between speed and resource requirements.

XIP6220B is a member of xQlave® product family of secure and efficient IP cores for post-quantum cryptography (PQC) algorithms.

## Key Features

- **Small Resource Requirements:** XIP6220B fits into about a few thousands of ALMs and additionally uses only a few multipliers/DSP blocks and internal memory block in a typical Altera® FPGA implementation.
- **Fast Performance:** XIP6220B is capable of computing a few thousand signature verification operations in a second in a typical Altera® FPGA implementation.
- **Easy Integration:** The simple 64-bit interface of XIP6220B supports easy integration to various systems.
- **Compliance:** XIP6220B is compliant with ML-DSA Initial Public Draft of the NIST standard FIPS 204 (Aug. 28, 2023) [2]. Xiphera commits to update XIP6220B when the standardization proceeds to newer versions.

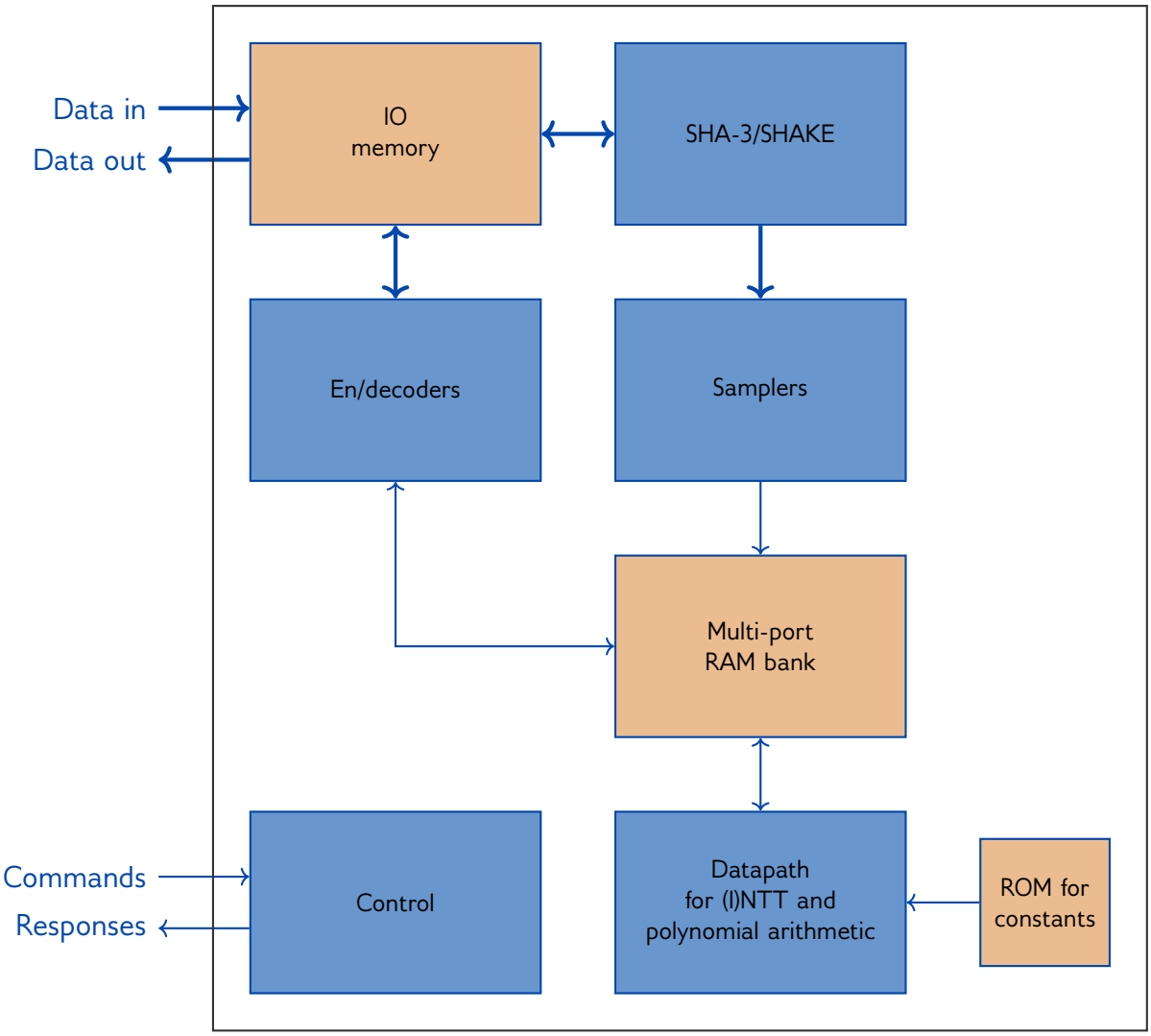


Figure 1: Internal high-level block diagram of XIP6220B

## Functionality

XIP6220B can be used for signature verification operations of all ML-DSA variants ML-DSA-44, ML-DSA-65, and ML-DSA-87. ML-DSA was selected as the primary algorithm for post-quantum digital signature algorithm by NIST [1] and, hence, it is expected to be very widely used in multiple different protocols in the coming years. Support for key generation and signature generation will be available in future versions of XIP6220B.

The main optimization objective for XIP6220B has been on achieving a good balance between resource requirements and performance as well as in providing versatile support for all operations of all ML-DSA variants with a single IP core.

As XIP6220B supports digital signature verifications, there are no side-channel threats against it.

## Block Diagram

The internal high-level block diagram of XIP6220B is depicted in Figure 1.

## Interfaces

The external interfaces of XIP6220B are depicted in Figure 2.

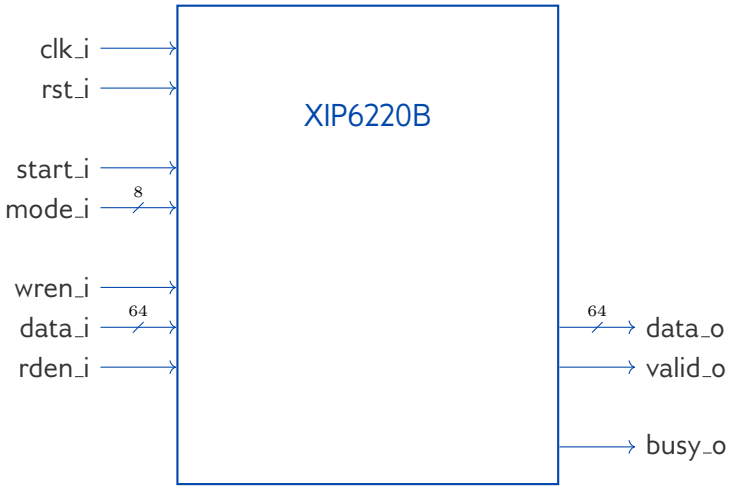


Figure 2: External interfaces of XIP6220B

## altera® FPGA Resources and Performance

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

| Device | Resources | $f_{\max}$ |
|---|---|---|
| Altera Arria 10 | 7888 ALM, 17 M20K, 1 DSP | 256.67 MHz |
| Altera Cyclone 10 GX | 7888 ALM, 17 M20K, 1 DSP | 244.26 MHz |
| Altera Agilex | 8931 ALM, 19 M20K, 1 DSP | 382.41 MHz |

Table 1: Resource usage and performance of XIP6220B on representative altera® FPGA families.

## Example Use Cases

ML-DSA can be expected to be used as the digital signature algorithm in various security systems and protocols in the coming years. Therefore, XIP6220B will have several applications in protecting critical systems. There are already drafts about how ML-DSA will be used in security protocols: for example, X.509 certificates [4], hybrid signatures for PKI [5], and PGP [3].

## Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP6220B 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] Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone. Status report on the third round of the NIST post-quantum cryptography standardization process. Technical Report NIST IR 8413-upd1, National Institute of Standards & Technology, Gaithersburg, MD, United States, July 2022.

[2] NIST Computer Security Division. FIPS PUB 204 (draft), Module-Lattice-Based Digital Signature Standard. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, August 2023.

[3] Stavros Kousidis, Johannes Roth, Falko Strenzke, and Aron Wussler. Post-Quantum Cryptography in OpenPGP. Internet-Draft draft-ietf-openpgp-pqc-02, Internet Engineering Task Force, March 2024. Work in Progress.

[4] Jake Massimo, Panos Kampanakis, Sean Turner, and Bas Westerbaan. Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA. Internet-Draft draft-ietf-lamps-dilithium-certificates-03, Internet Engineering Task Force, February 2024. Work in Progress.

[5] Mike Ounsworth, John Gray, Massimiliano Pala, and Jan Klaußner. Composite ML-DSA for use in Internet PKI. Internet-Draft draft-ounsworth-pq-composite-sigs-13, Internet Engineering Task Force, March 2024. Work in Progress.