XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP6110B: ML-KEM KYBER-512/768/1024

Balanced Post-Quantum Key Encapsulation IP Core

Product Brief
ver. 1.0
October 17, 2023

sales@xiphera.com

Introduction

XIP6110B from Xiphera is an Intellectual Property (IP) core for ML-KEM (previously known as CRYSTALS-Kyber) [2] post-quantum Key Encapsulation Mechanism (KEM). It supports key generation, encapsulation, and decapsulation operations for all ML-KEM variants Kyber-512, Kyber-768, and Kyber-1024. XIP6110B is optimized for a good balance between speed and resource requirements.

XIP6110B is a member of xQlave® product family of secure and efficient IP cores for post-quantum cryptography (PQC) algorithms.

Key Features

- **Small Resource Requirements:** XIP6110B fits into about 8000 LUTs and additionally uses only a few multipliers/DSP blocks and internal memory block in a typical AMD® FPGA implementation.
- **Fast Performance:** XIP6110B is capable of computing a few thousand key generation, encapsulation, or decapsulation operations in a second in a typical AMD® FPGA implementation.
- **Secure Architecture:** The execution time of XIP6110B is independent of the secret values and, consequently, provides full protection against timing-based side-channel attacks. XIP6110B has been implemented only in digital logic without any software components.
- **Easy Integration:** The simple 64-bit interface of XIP6110B supports easy integration to various systems.
- **Compliance:** XIP6110B is compliant with ML-KEM specifications 3.0 (Oct. 1, 2020) [2] which is the version that was selected as a candidate to be standardized by NIST [1]. Xiphera commits to update XIP6110B when the standardization proceeds to newer versions.

Functionality

XIP6110B can be used for key generation, encapsulation, and decapsulation operations of all ML-KEM variants Kyber-512, Kyber-768, and Kyber-1024[1]. ML-KEM was selected as the primary algorithm for post-quantum key encapsulation by the NIST [1] and, hence, it is expected to be very widely used in multiple different protocols in the coming years.

The main optimization objective for XIP6110B has been on achieving a good balance between resource requirements and performance as well as in providing a versatile support for all operations of all ML-KEM variants with a single IP core.

XIP6110B also includes protections against side-channel attacks, the most important of which is that the operation latency does not depend on any secret values. Because ML-KEM uses rejection sampling to obtain certain non-secret values (most importantly, the public key), the actual latency varies slightly between different execution runs. However, because the secret values are obtained in fully constant time by XIP6110B, the variance in the operation latencies does not induce any weaknesses against side-channel attacks.

XIP6110B implements the ML-KEM operations defined in [2], but key generation and encapsulation require random bytes as inputs. Hence, XIP6110B requires an external random number generator (for example, XIP8001B) for generating high-quality random bytes.

Block Diagram

The internal high-level block diagram of XIP6110B is depicted in Figure 1.

Interfaces

The external interfaces of XIP6110B are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP6110B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP6110B, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

FPGA Resources and Performance

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

Device	Resources	f_{MAX}
Xilinx® Zynq® MPSoC*	8622 LUT, 4/3 RAMB36/18, 6 DSP	230.10 MHz
Xilinx® Kintex® UltraScale+*	8570 LUT, 4/3 RAMB36/18, 6 DSP	351.37 MHz

Table 1: Resource usage and performance of XIP6110B on representative AMD® FPGA families.

[1] "90s" variants of ML-KEM, which are based on AES and SHA-2, that are also defined in [2] are not supported.
*Vivado 2022.1, default compilation settings, industrial speedgrade.

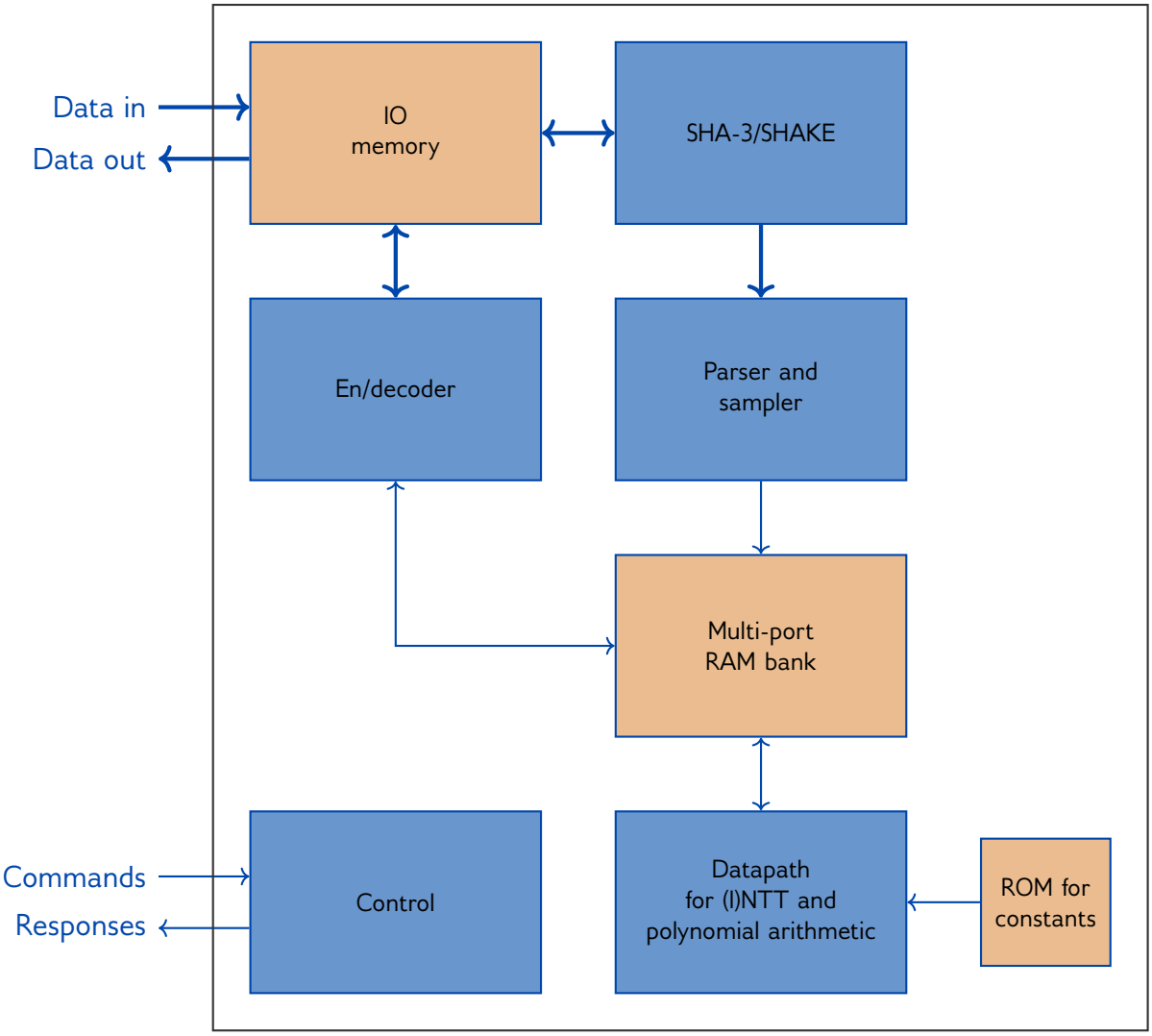

Figure 1: Internal high-level block diagram of XIP6110B

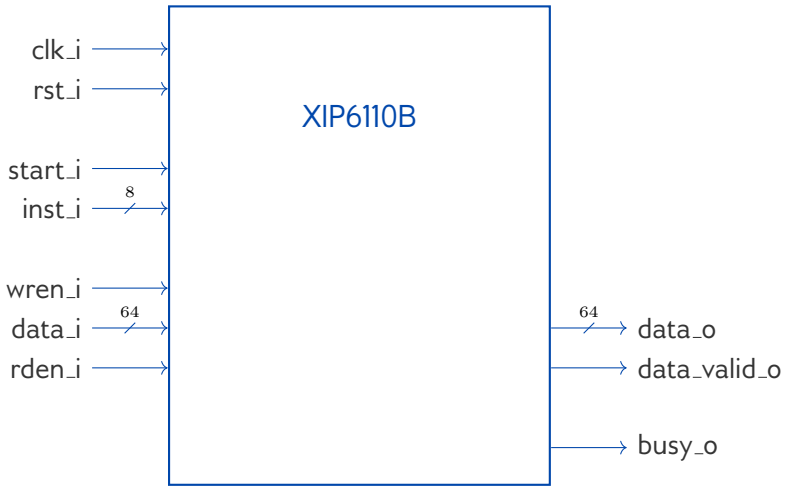

Figure 2: External interfaces of XIP6110B

Example Use Cases

ML-KEM can be expected to be used for key exchange in various security protocols in the coming years. Therefore, XIP6110B will have several applications in protecting critical systems. There are already drafts about how Kyber will be used in security protocols: for example, IPsec IKEv2 [4] and TLS 1.3 [3].

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP6110B 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] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber: Algorithm specifications and supporting documentation. Ver. 3.0, October 2020.

[3] Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in TLS 1.3. Internet-Draft draft-ietf-tls-hybrid-design-06, Internet Engineering Task Force, February 2023. Work in Progress.

[4] C. Tjhai, M. Tomlinson, G. Bartlett, Scott Fluhrer, Daniel Van Geest, Oscar Garcia-Morchon, and Valery Smyslov. Multiple Key Exchanges in IKEv2. Internet-Draft draft-ietf-ipsecme-ikev2-multiple-ke-12, Internet Engineering Task Force, December 2022. Work in Progress.