XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP7410B: SECURE BOOT

A Quantum-Resistant nQrux® Secure Boot IP core

Product Brief
ver. 1.0.0
September 5, 2024

sales@xiphera.com

Introduction

nQrux® Secure Boot (XIP7410B) is an Intellectual Property (IP) core from Xiphera, enabling quantum-secure authenticated boot. nQrux® is Xiphera's product family for Hardware Trust Engines. XIP7410B allows verifying the authenticity and integrity of binary images that are loaded into a processor during the boot sequence. The protection is based on a hybrid digital signature scheme using ECDSA [1] and ML-DSA [2]. The ML-DSA signatures are designed to withstand attacks utilizing quantum computers and the ECDSA signatures are established digital signatures which provide fallback security if a cryptanalytic attack is discovered against the quantum-secure ML-DSA algorithm.

XIP7410B has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP7410B does not rely on any FPGA manufacturer-specific features.

Key Features

- **Enabler for trusted computing:** Authenticated boot creates trust in a computing platform by providing cryptographic authenticity and integrity guarantees for programs that are executed in the system.
- **Secure architecture:** The architecture of XIP7410B is purely based on digital logic and is implemented without any hidden software components, offering first-grade security as well as easier validation and certification. The solution is not susceptible to side-channel attacks.
- **Hybrid security:** Simultaneous use of ECDSA and ML-DSA protects against both classical and quantum attacks.
- **Easy integration:** The simple 32-bit interface supports easy system integration.

Functionality

XIP7410B offers means to protect the boot sequence. In authenticated boot, the binary images of programs that are loaded into a processor during boot have been digitally signed using secure cryptographic digital signature algorithms. These signatures are then verified in XIP7410B using trusted copies of the signer's public key. Only if the verification is successful, a binary image is allowed to be executed in the target processor. In order to run their own program in the processor, an adversary would need to be able to forge the digital signatures attached to the binary image and this is impossible assuming the security of the cryptographic digital signature schemes.

XIP7410B combines the use of ML-DSA quantum-secure digital signatures [2] and ECDSA elliptic curve digital signatures [1]. ML-DSA ensures that this hybrid structure is quantum-secure in the sense that even adversaries who could utilize large-scale quantum computers in the attack are not able to break the security. ECDSA serves as a backup against the unlikely case that a cryptographic weakness is found from the relatively new ML-DSA.

XIP7410B supports different means to provide the public keys used in verification. Either the keys or their hash values are written directly from a secure source to XIP7410B via the Key Storage Memory (KSM) interface. If the hashes are written, then the actual keys can be later written from Non-Volatile Memory (NVM) interface together with the protected binary image (binary image and signatures) and the hashes are used for ensuring their integrity. There is an option to write the binary image through XIP7410B to the processor (CPU interface).

XIP7410B does not utilize any cryptographic secrets during the authentication process and, consequently, side-channel attacks are not a threat.

Xiphera also provides the software tools for creating protected binary images so that they can be verified using XIP7410B.

Block Diagram

The internal high-level block diagram of XIP7410B is depicted in Figure 1.

Interfaces

The external interfaces of XIP7410B are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP7410B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP7410B, example simulation waveforms, and resource requirements.

Example Use Cases

Boot image authentication can be used to build trust in a computing system. XIP7410B can be the trust anchor that verifies authenticity of programs (importantly, the boot image) that are loaded and executed in the system. This way only programs that pass the authentication are allowed to be executed in the system. These trusted programs may then be used for deriving trust to further components and the entire system.

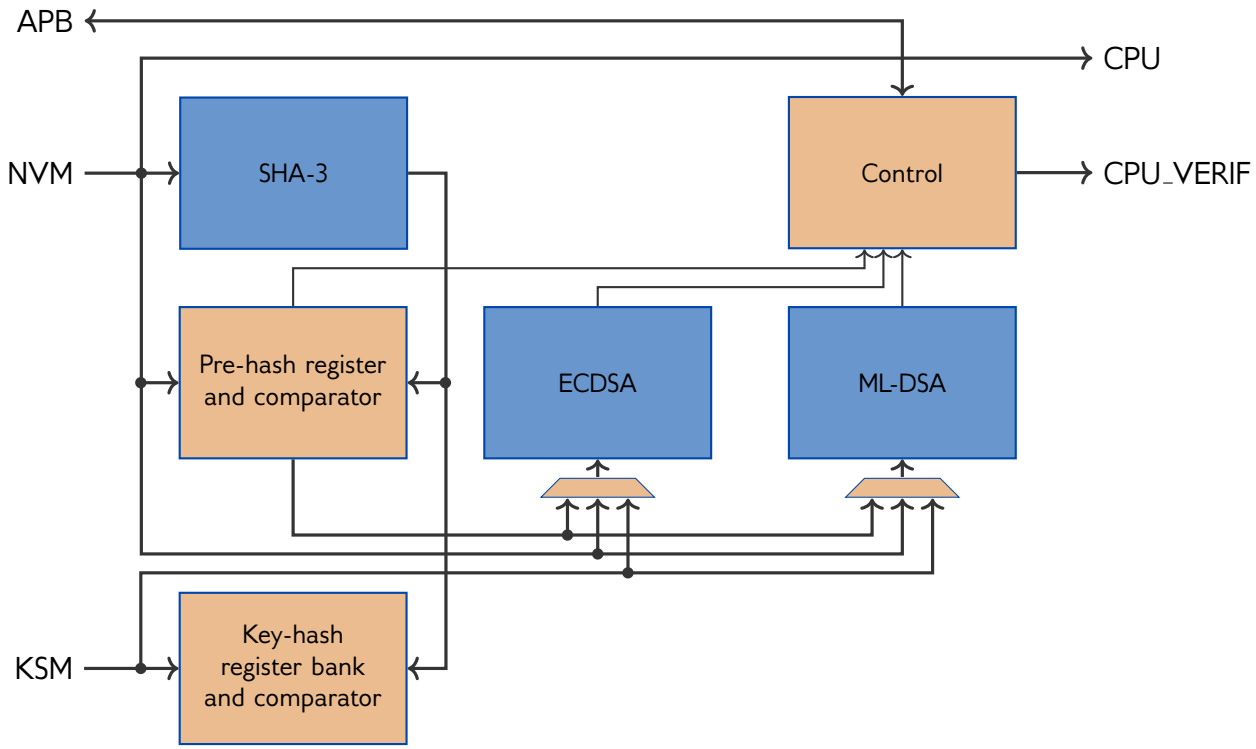

Figure 1: Internal high-level block diagram of XIP7410B

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP7410B 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.

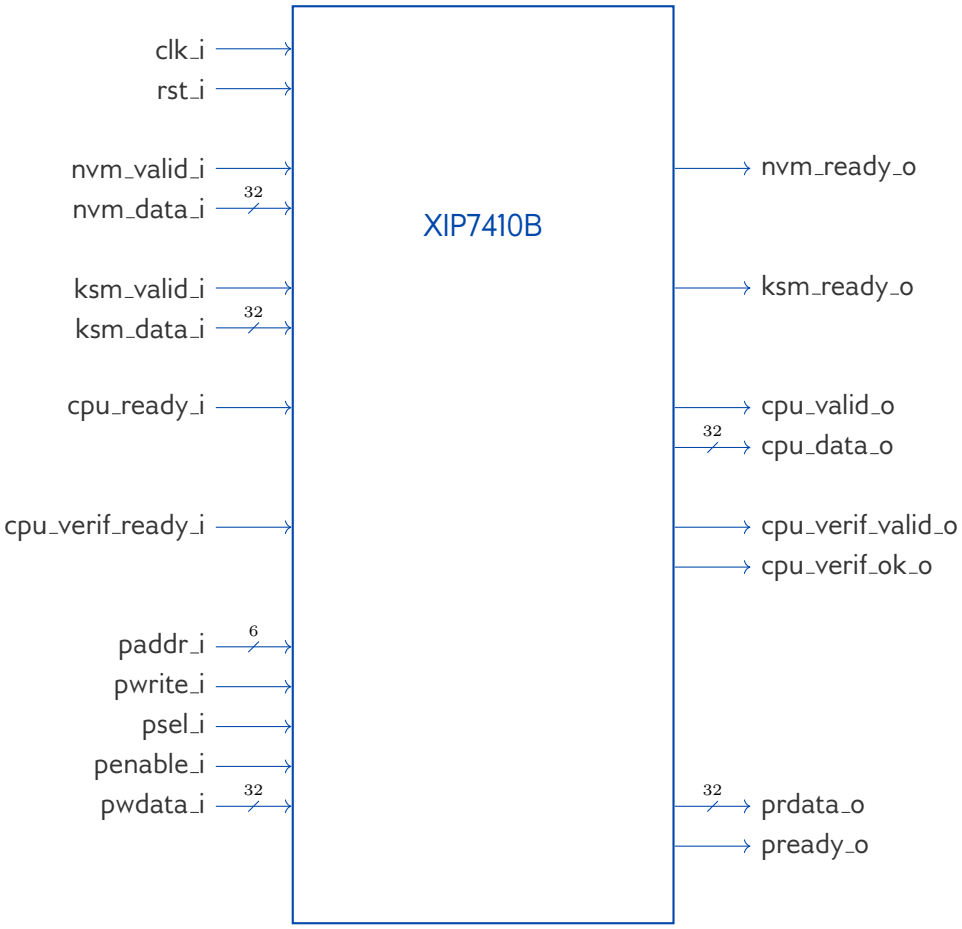

Figure 2: External interfaces of XIP7410B

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] 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.

[2] NIST Computer Security Division. Module-Lattice-Based Digital Signature Standard. FIPS Publication 203, National Institute of Standards and Technology, U.S. Department of Commerce, August 2024.