XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP7500: CRYPTO MODULE IP CORE

Multipurpose Cryptographic Suite

Product Brief
ver. 1.0.2
May 13, 2024

info@xiphera.com

Introduction

Xiphera's Crypto Module IP core offers an integrated security platform enabling customer-tailored set of highly-optimized cryptographic services for microcontrollers or SoC implementations. Customers can select their desired solution from a wide range of cryptographic functionalities which can be used to ensure data confidentiality, integrity, and authenticity in the customer solution.

Crypto Module IP Core offers the following cryptographic feature set for implementation:

- AES in different modes of operation (for example, GCM, CBC, CTR, XTS)
- Symmetric ciphers: ChaCha20-Poly1305, Ascon
- Hash algorithms: SHA-2, SHA-3, SHAKE, HMAC
- Key derivation with HKDF
- True and pseudo random number generators
- Public key cryptography: ECDH(E), ECDSA, Curve25519 (X25519/Ed25519), RSA
- Post-quantum cryptography: ML-KEM (CRYSTALS-Kyber), ML-DSA (CRYSTALS-Dilithium)

XIP7500 has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP7500 does not rely on any FPGA manufacturer-specific features.

Key Features

- **Standard Compliance:** Fully compatible with applicable NIST, IETF, and IEEE standards, RFCs, and test vectors for compliance and certification programs.

- **Fully Hardware-Based Implementation:** XIP7500 comes without hidden software components for performance and ease of validation.
- **Highly Optimised Implementation:** Options for both resource conservation and footprint optimisation, or high performance and throughput.
- **Versatile Configurations:** XIP7500 enables composing the most optimal set of features to fit customer functionality, performance, and resource requirements.
- **Secure Architecture:** XIP7500 protects against timing-based attacks with constant latency independent of input values.
- **Easy Integration:** The AXI-4 and APB interfaces of XIP7500 support easy integration to various systems.
- **Unified Implementation:** All major FPGA architectures supported.

Functionality

Table 1 shows the IP cores that can be selected as a part of the Crypto Module and their different variants available.

IP Core Offering	Compact	Balanced	High-speed
AES-128/256 (ECB, CBC, OFB, CFB, and CTR modes)		✓	
AES-128/256-GCM		✓	
AES-256-XTS		✓	
ChaCha20-Poly1305		✓	
Ascon		✓	
SHA-2-224/256/384/512, HMAC, HKDF	✓	✓	
SHA-3-224/256/384/512, (c)SHAKE128/256	✓		✓
True Random Number Generation		✓	
Pseudorandom Number Generation		✓	
ECDH(E)/ECDSA on NIST P curves	✓		✓
X25519/Ed25519	✓		
RSA Signature Verification	✓		
ML-KEM-512/768/1024 (CRYSTALS-Kyber)		✓	
ML-DSA-44/65/87 (CRYSTALS-Dilithium)		✓	

Table 1: IP cores that can be selected in Crypto module and the available variants

Block Diagram

The internal high-level block diagram of XIP7500 is depicted in Figure 1.

Interfaces

The Crypto Module is easily integrated into custom solutions via the AXI-4 and APB interfaces.

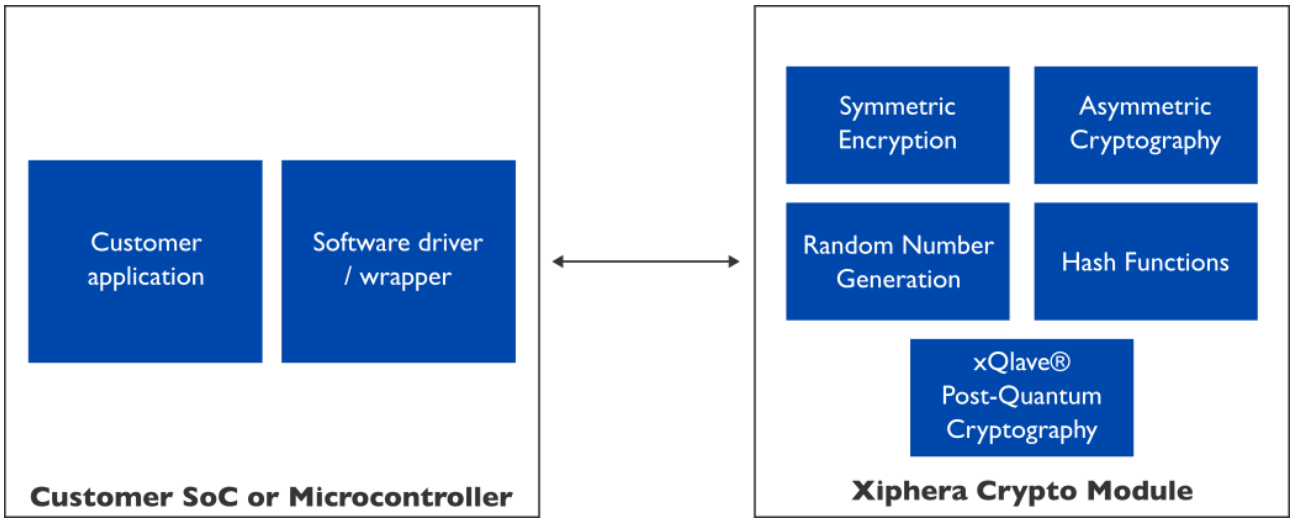

Figure 1: Internal high-level block diagram of XIP7500

Example Use Cases

Following is the list of use cases in which Xiphera's Crypto Module can be used to ensure security:

- Secure communications
- Data integrity and authenticity
- Data at rest encryption
- HSM (Hardware Security Module)
- Key generation
- Secure boot
- Root of Trust

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP7500 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