XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

# XIP7131C: TLS 1.3 CLIENT

## TLS 1.3 Client IP Core

Product Brief
ver. 1.0
October 23, 2021

sales@xiphera.com

## Introduction

XIP7131C is a compact[1] Intellectual Property (IP) core for TLS 1.3 client-side functionality. Transport Layer Security (TLS) is a cryptographic protocol, which provides communication security in computer networks and is used for securing a multitude of different applications ranging from casual Internet browsing to critical infrastructure communications. TLS 1.3 was published as RFC 8446 [9] in August 2018, and it is the most recent version of the TLS standard and includes major modifications and security improvements compared to the earlier TLS versions.

XIP7131C provides a hardware-based security solution level required for mission-critical applications. XIP7131C is optimized for low-area footprint, and it is ideally suited for high-volume FPGA applications, for example industrial automation, energy distribution, and secure edge computing. While the IP core itself has been optimized for low FPGA resource usage, it is capable of encrypting and decrypting bulk transmission speeds in excess of 1 Gbps after the secure connection has been established.

XIP7131C supports the TLS 1.3 handshakes for session establishment and the TLS 1.3 record protocol for bulk communication. The IP core implements all cryptographic computations and key management activities required for secure TLS connections with a server. Critical cryptographical computations and key management are both isolated inside the FPGA from the rest of the system, offering a very high level of protection from different types of attacks. All computations are performed in constant time, thus nullifying timing-based side-channel attacks and protecting also against various other types of side-channel attacks.

Due to the need to optimize the resource requirements, the supported cryptographic algorithms were carefully selected. XIP7131C supports X25519 [8], Ed25519 [5], SHA-2 [3], HMAC [6], HKDF [7], and AES-GCM [2] [4] with 128-bit keys. Internally, XIP7131C includes a True Random Number Generator (TRNG) for generating truly random numbers needed in the TLS protocol, for example, ephemeral[2] keys.

[1] Xiphera's "C" (compact) IP cores have been optimised to minimize the digital logic resource utilization.
[2] An *ephemeral* cryptographic key is generated and used only for a single session.

The TLS 1.3 IP Core is available for all Intel® FPGAs.

## Key Features

- **Optimized Resource Requirements:** The entire XIP7131C requires less than 8500 ALMs (Adaptive Logic Modules) in Intel® Cyclone® V implementation.
- **Short Session Establishment Time:** The FPGA-dependant execution time of the TLS 1.3 handshake calculations is less than 100 ms at 100MHz clock, and the FPGA execution time is constant and does not depend on the key values, thus providing protection against timing-based side-channel attacks.
- **Performance:** Despite its small size, XIP7131C can support bulk traffic encryption and decryption speeds in excess of 1 Gbps.
- **Follows RFC 8446:** XIP7131C follows the latest TLS 1.3 standard defined in RFC 8446 [9] with specifically selected ciphers to miminize area requirements.
- **Hardware-based Security** The primary design goal of XIP7131C is to avoid the potential weaknesses in software-based security, including but not limited to dependence on operating system security, vulnerabilities in third party cryptographic software libraries, and bugs in underlying processor architectures.
- **Hardware-based Cryptographic Operations** All the cryptographic mathematical operations are performed entirely in the FPGA, providing a substantial security and performance advantages compared to software-based TLS implementations.
- **Hardware-based Key Management** All the cryptographic keys are stored in dedicated internal FPGA memory, which provides a substantial security advantage over software-based key management, and amongst other benefits is a requirement for IEC 62443 Security Level 3 designs.

## Functionality

The functionality of XIP7131C complies with the TLS 1.3 protocol definition in RFC 8446 [9], and it implements at hardware level the required functionality for TLS 1.3 client side operation. The TLS 1.3 client (the FPGA-based XIP7131C IP core) opens a TLS connection with a server by running the client side of the TLS 1.3 handshake protocol. First XIP7131C generates a ClientHello message including the client's ephemeral X25519 public share and sends it to the server. The server responds with a ServerHello message which includes the server's ephemeral X25519 public share, the server's certificate, a signature over the exchanged messages. After XIP7131C has received the ServerHello message it computes the shared session secret from the received public share and its own private share, verifies the certificate and the digital signature, and derives the required keys from the shared session secret for securing the bulk communications.

After a secure connection has been established, the bulk communication is protected with the Authentication Encryption with Associated Data (AEAD) scheme AES-GCM with 128-bit key length. This AEAD scheme protects both confidentiality and integrity, the former meaning that no malicious party in the middle of the communication can see the contents of

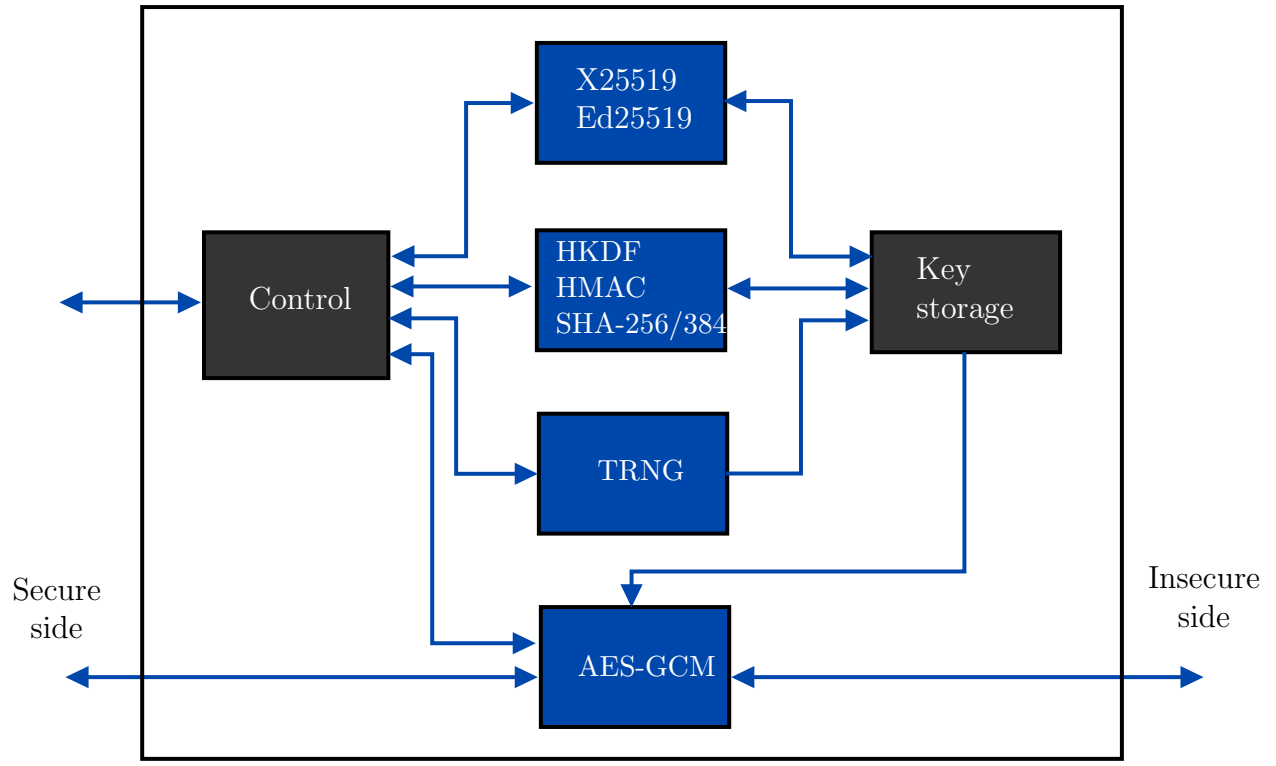


Figure 1: Internal high-level block diagram of XIP7131C

the communication, and the latter that the communicated messages cannot be manipulated without being noticed. XIP7131C adds the required TLS 1.3 fields to each outgoing frame for a given IP address and destination port and encrypts the data payload. For the incoming messages XIP7131C removes the TLS 1.3 fields from the message frames, and decrypts the encrypted data payload.

## Block Diagram

The internal high-level block diagram of XIP7131C is depicted in Figure 1.

## Interfaces

The external interfaces of XIP7131C are depicted in Figure 2.

The integration of XIP7131C with the rest of the FPGA design is straightforward, and its symbol with the I/O signals in logically grouped Avalon [1] buses is depicted in Figure 3 and Table 1. XIP7131C can be integrated with the rest of the FPGA design with Intel Platfrom designer by using the delivered _hw.tcl file, and XIP7131C is typically connected between modular scatter DMA controller (mSGDMA) and Ethernet MAC (EMAC).

This Product Brief describes a high-level overview of the functionality and capabilities of XIP7131C. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP7131C, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

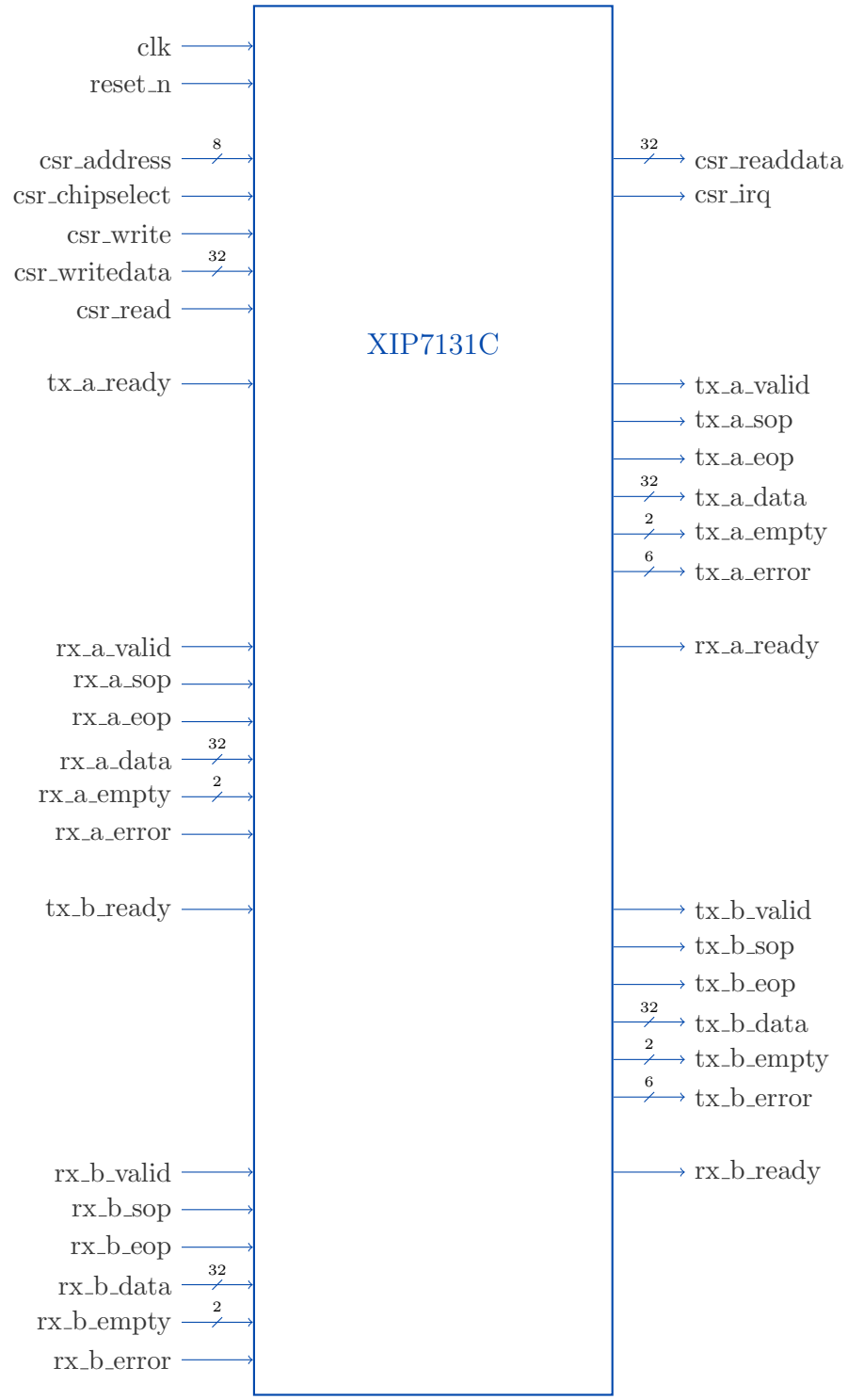


Figure 2: External interfaces of XIP7131C

## FPGA Resources and Performance

Table 2 presents the FPGA resource requirements for representative implementations on Intel® families. On request, the resource estimates can also be supplied for other Intel® FPGA families.

The latency for opening a secure connection depends on multiple things including the com-

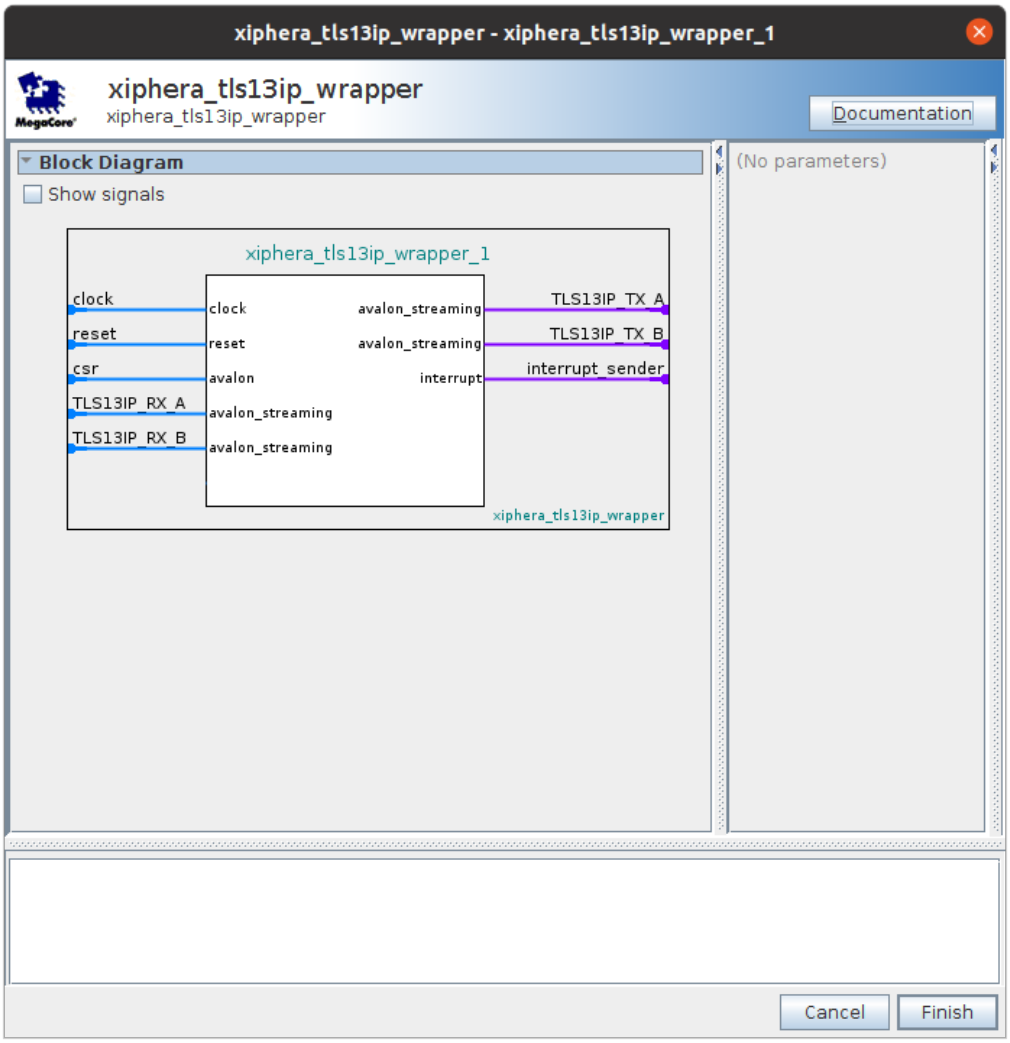


Figure 3: Avalon bus interfaces of XIP7131C

| Name | Functionality |
|---|---|
| `clock` | Clock[1] |
| `reset` | Active high reset |
| `csr` | Avalon memory mapped control bus [2] |
| `TLSIP13_TX_A` | Avalon streaming slave for mSGDMA [3] [4] |
| `TLSIP13_RX_A` | Avalon streaming source for mSGDMA [4] |
| `TLSIP13_TX_B` | Avalon streaming source for EMAC [4] [5] |
| `TLSIP13_RX_B` | Avalon streaming slave for EMAC [4] |

[1] $f_clk \geq \frac{Ethernet\ linerate}{32}$
[2] 8-bit wide address bus
[3] modular Scatter-Gather Direct Memory Access
[4] 32-bit wide address bus
[5] Ethernet Media Access Controller

Table 1: The I/O buses of XIP7131C grouped into Avalon buses

| Device | Resources |
|---|---|
| Intel® MAX® 10 * | 20532 LE, 32 M9K, 2 multipliers |
| Intel® Cyclone® V * | 8407 ALM, 32 RAM blocks, 1 DSP block |
| Intel® Cyclone® 10 GX * | 10275 84, 32 RAM blocks, 1 DSP block |

* Quartus II Prime 20.2., default compilation settings, industrial speedgrade

Table 2: Resource usage and performance of XIP7131C on representative Intel® FPGA families.

munication delay between the FPGA and the server as well as the delay of the server. However, the cryptographic computations related to the handshake —generating the ClientHello message, processing the ServerHello message, verifying the certificate, deriving the keys, etc.—require less than 100 ms in total with $f_{CLK}$ at 100MHz. As examples on the latency of individual cryptographic operations XIP7131C computes one X25519-related elliptic curve operation in slightly over 10 ms and verifies a single Ed25519 digital signature is less than 20 ms.

The bulk communication using AES-GCM with 128-bit keys achieves maximum throughput in excess of 1 Gbps, especially with long packet sizes.

## Example Use Cases

XIP7131C can be used in a variety of ways to provide hardware-based security for TLS 1.3 connections. Figures 4, 5, 6, and 7 present example use cases where XIP7131C is instantiated on an FPGA to protect the TLS 1.3 -based traffic between the client and a remote server. The term *protected zone* in Figures 4, 5, and 6 means that sensitive plaintext information can be sent inside the protected zone, whereas the term *unprotected zone* refers to the fact XIP7131C is required to provide the required security for otherwise unprotected communications in the unprotected zone.

The example depicted in Figure 4 describes a use case where XIP7131C is used with other FPGA IP and an external processor, and the secure TLS 1.3 connection to a cloud-based server is set up and managed exclusively by XIP7131C.

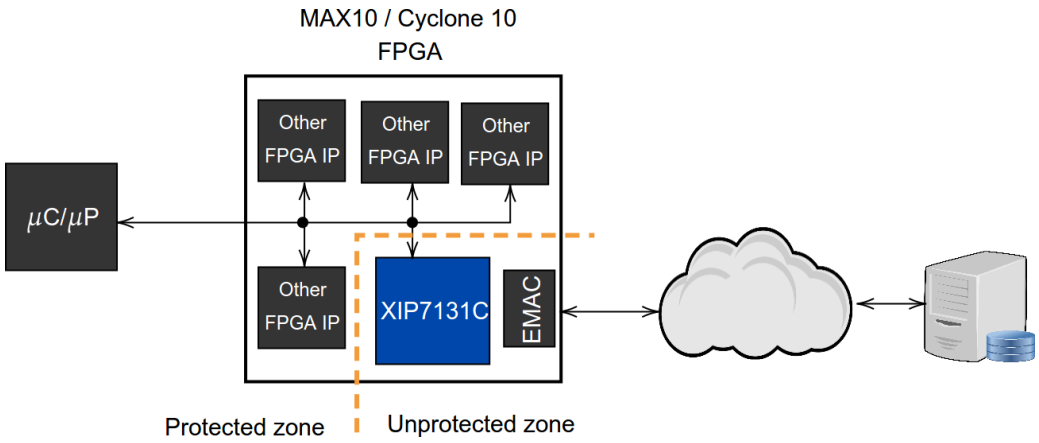


Figure 4: XIP7131C used in combination with other FPGA IP and an external processor.

The second example depicted in Figure 5 describes a use case where only XIP7131C and EMAC are instantiated in an FPGA (for example, Intel® MAX® 10 or Intel® Cyclone® 10)

and thus provides a hardware-based single-chip "firewall" completely isolating the external processor from all security-critical functionality.

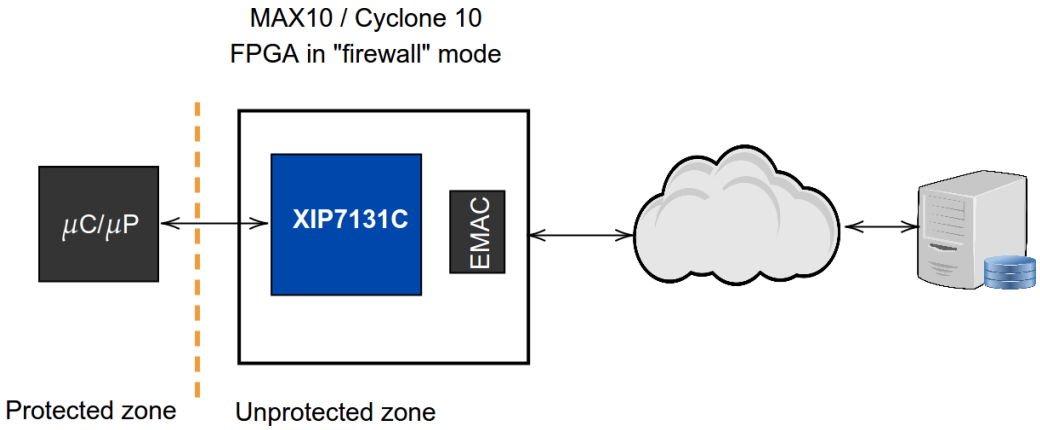


Figure 5: XIP7131C used in standalone mode providing a single-chip "firewall" solution.

XIP7131C can also be used to provide mission-critical TLS 1.3 connectivity in designs based on an FPGA with a hard processor, for example Intel® Cyclone® V SOC. The two primary use cases are depicted in Figures 6 and 7, with Figure 6 focusing on Secure Gateway mode and Figure 7 on the cryptographic co-processor mode.

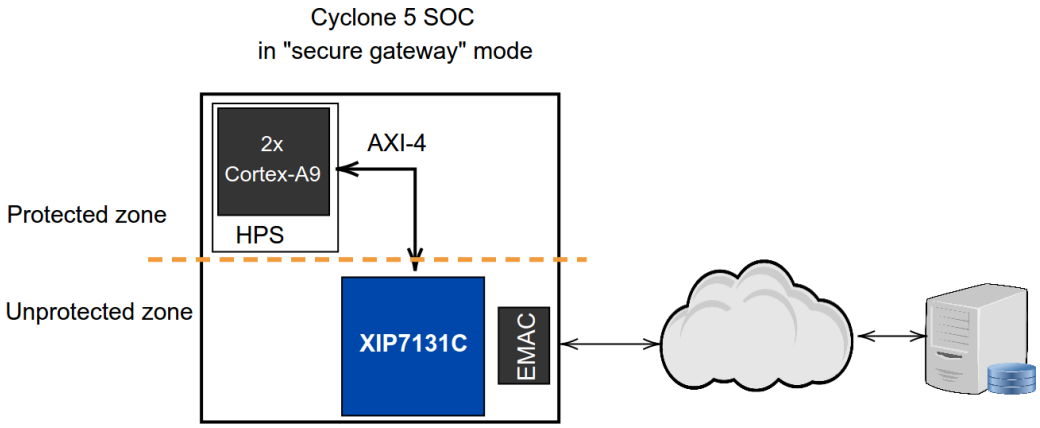


Figure 6: XIP7131C used in secure gateway mode with Intel® Cyclone® V SOC.

There are also other use cases for XIP7131C in addition to the ones depicted in this Product Brief, and XIP7131C can be used also with other Intel® FPGA families.

## Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP7131C can be shipped in a number of formats, including netlist, source code, or encrypted source code. Additionally, a detailed datasheet is included.

Xiphera will also deliver an example C software program to facilitate the integration of XIP7131C with a host processor.

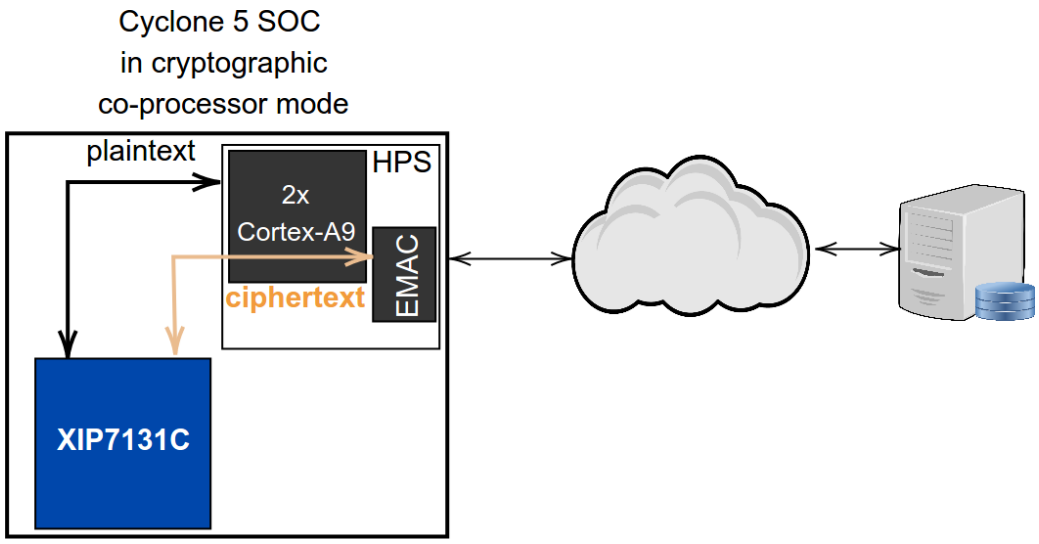


Figure 7: XIP7131C used in cryptographic co-processor mode with Intel® Cyclone® V SOC.

## Export Control

XIP7131C protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP7131C is controlled by Council Regulation (EC) No 428/2009 of 5 May 2009 and its subsequent changes.

XIP7131C can be immediately shipped to all European Union member states, Australia, Canada, Japan, New Zealand, Norway, Switzerland, United Kingdom, and the United States.

Export to other countries requires authorization from The Ministry for Foreign Affairs of Finland, and a typical processing time for an export authorization is a few weeks.

## About Xiphera

Xiphera specializes in secure and efficient implementations of standardized cryptographic algorithms on Field Programmable Gate Arrays (FPGAs). Our 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.

## Contact

Xiphera Oy
Otakaari 5
FIN-02150 Espoo
Finland
sales@xiphera.com
+358 20 730 5252

# References

[1] Avalon® interface specifications. https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/manual/mnl_avalon_spec.pdf.

[2] Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001.

[3] FIPS PUB 180-4 Secure Hash Standard (SHS). Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2015.

[4] Morris J. Dworkin. SP 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. Technical report, Gaithersburg, MD, United States, 2007.

[5] Simon Josefsson and Ilari Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032, January 2017.

[6] Dr. Hugo Krawczyk, Mihir Bellare, and Ran Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, February 1997.

[7] Dr. Hugo Krawczyk and Pasi Eronen. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869, May 2010.

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

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