XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP2113B: CHACHA20-POLY1305

Balanced IP Core for ChaCha20-Poly1305 Authenticated Encryption

Product Brief
ver. 1.0
September 20, 2023

sales@xiphera.com

Introduction

XIP2113B from Xiphera is a balanced[1] Intellectual Property (IP) core designed for ChaCha20-Poly1305 Authenticated Encryption with Associated Data (AEAD) scheme protecting both confidentiality and authenticity at the same time. The current definitive standard for ChaCha20-Poly1305 is RFC 8439, "ChaCha20 and Poly1305 for IETF Protocols" [3].

ChaCha20-Poly1305 is a combination of the ChaCha20 stream cipher [2] and Poly1305 message authentication code [1], both algorithms designed by Daniel J. Bernstein, and it is used an AEAD scheme in multiple protocols, including TLS 1.3 [4].

XIP2113B has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP2113B does not rely on any FPGA manufacturer-specific features.

Key Features

- **Moderate** resource requirements: The entire XIP2113B requires 7346 Lookup Tables (LUTs) (AMD® Zynq® MPSoC).
- **Performance:** XIP2113B achieves a throughput in the tens of Gbps range[2], for example 6.96+ Gbps in Xilinx® Zynq® MPSoC. Even higher throughputs can be achieved with parallel instantiations of XIP2113B.
- **High Throughput with Short Latency:** XIP2113B offers very high throughput for a single stream of data as it is capable to process one 16-byte block per clock cycle after certain

[1] Xiphera's balanced (denoted by 'B' at the end of the ordering code) IP cores strike a balanced compromise between performance and FPGA resource usage.

[2] The highest throughput is achieved for long messages.

initial latency. The length of the initial latency depends on the length of the message and XIP2113B has been carefully optimized to minimize this initial latency.

- **Constant Latency:** The execution time of XIP2113B is independent of the key values and message contents (apart from the message length), and consequently provides full protection against timing-based side-channel attacks.
- **Standard Compliance:** XIP2113B is fully compliant with RFC 8439 "ChaCha20 and Poly1305 for IETF Protocols" [3].

Functionality

The input message into XIP2113B is split into two parts: the first part is only authenticated and the second part is both authenticated and encrypted (or decrypted)[3]. For example, the first part can be the header of a packet and the second part can be the payload. This way the header remains in cleartext and can be used, for instance, for routing the message to the correct recipient. However, the header is still authenticated and the recipient can verify that it has not been tampered with. The first part is called associated data and the second part is message payload (either plaintext or ciphertext).

The output of ChaCha20-Poly1305 is the associated data (AD, without padding, just as it was inputted), the encrypted payload (without padding), and the 16-byte authentication tag. In the decryption direction, the computation is similar, but Poly1305 takes the ciphertext before it is XORred with the keystream. In the end, the authentication tag that is computed during decryption is compared with the received tag. If they match, the received message is authentic; if not, it should be rejected.

XIP2113B uses a 256-bit key and a 96-bit nonce. They are used directly as the key and nonce for the ChaCha20 stream cipher. The key for Poly1305 is computed with ChaCha20 by setting the counter value to zero and by using 256 bits of the 512-bit keystream word k_0 as the Poly1305 key; the other half is discarded. As the computation of this authentication key depends on both the key and the nonce, the authentication key needs to be recomputed for every message even if they are encrypted with the same key.

Block Diagram

The internal high-level block diagram of XIP2113B is depicted in Figure 1.

Interfaces

The external interfaces of XIP2113B are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP2113B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

[3]Both the first path (authentication only) and the second part (authentication and encryption/decryption) can also be zero bytes long.

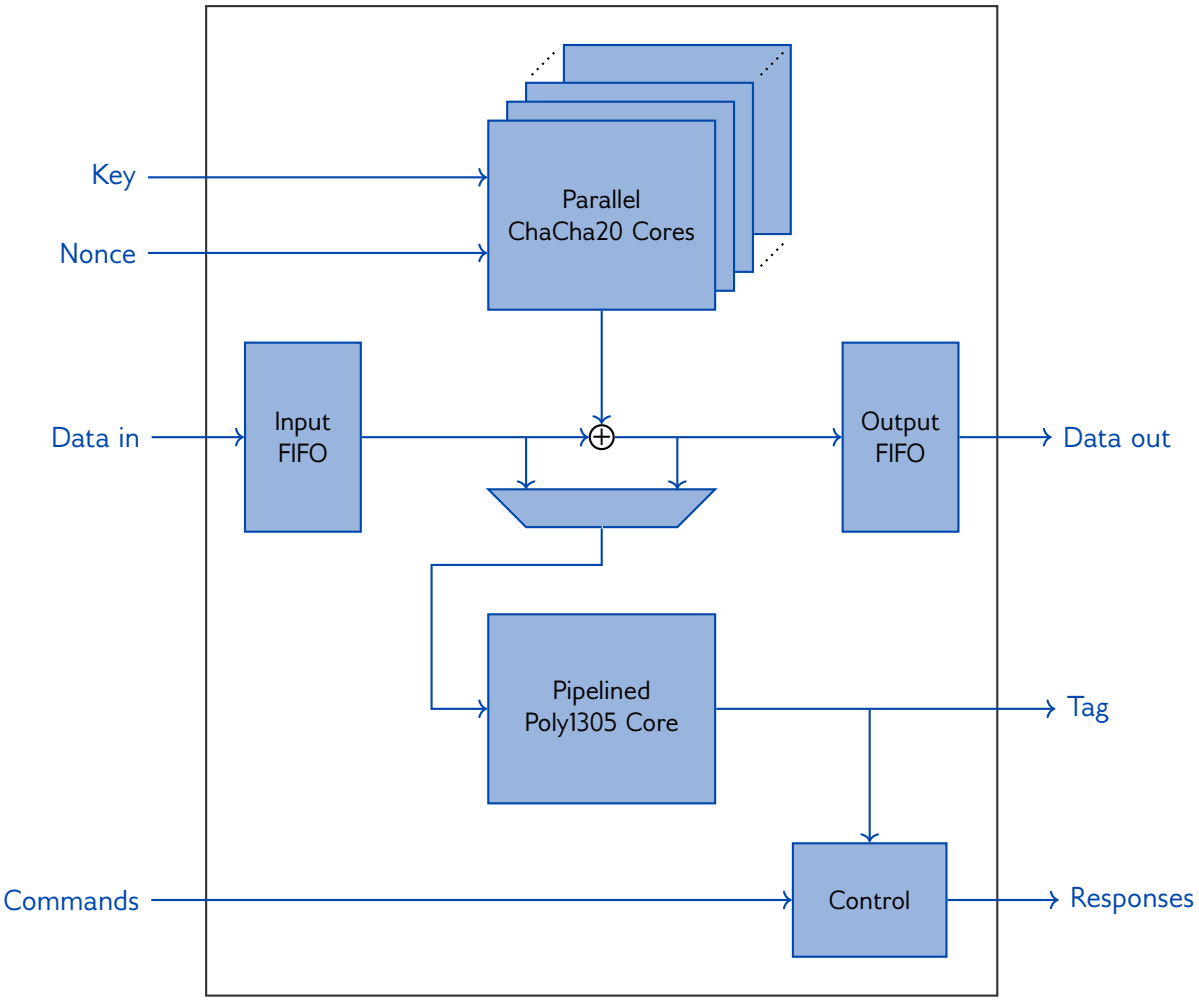

Figure 1: Internal high-level block diagram of XIP2113B

FPGA Resources and Performance

Table 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}	Max. throughput*
Xilinx® Zynq® MPSoC†	7346 LUT , 40 DSP	299.13 MHz	6.96 Gbps
Xilinx® Kintex® UltraScale+†	7291 LUT , 40 DSP	401.12 MHz	9.34 Gbps

Table 1: Resource usage and performance of XIP2113B on representative AMD® FPGA families.

Example Use Cases

Figure 3 describes how ChaCha20-Poly1305 is used in TLS 1.3 for protecting confidentiality and authenticity of communication.

*$Throughput = \frac{f_{MAX} * 128\ bits * 4}{22\ clock\ cycles}$

†Vivado 2021.1, default compilation settings, industrial speedgrade.

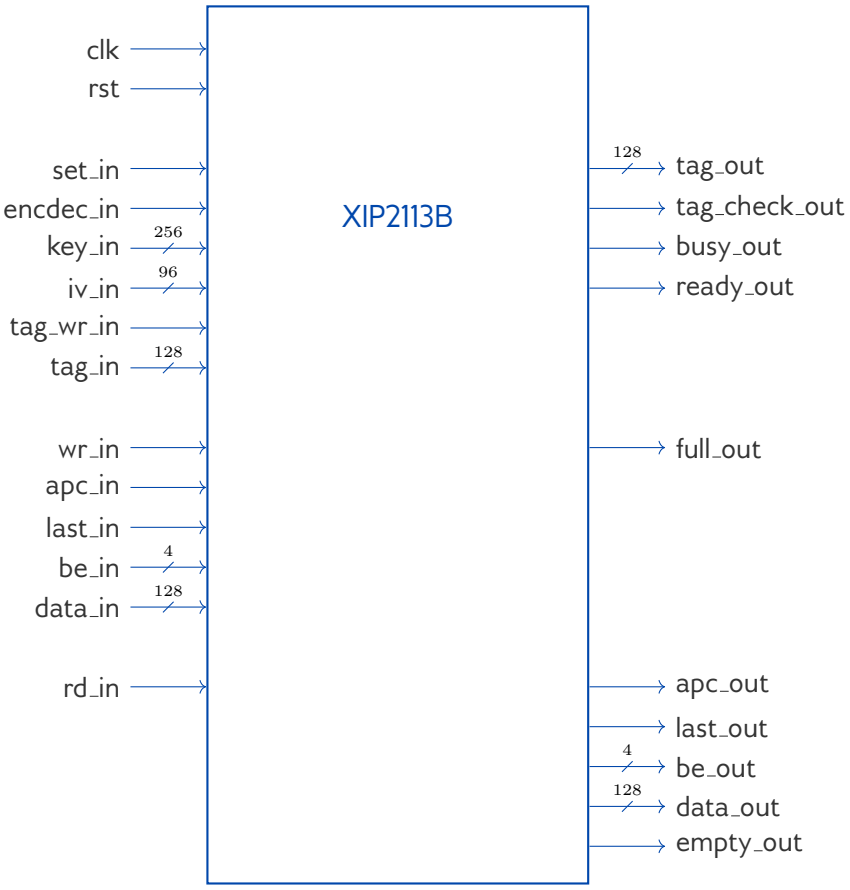

Figure 2: External interfaces of XIP2113B

A TLS Record starts with a five-byte TLS header. The headers of TLS 1.3 records that are encrypted with ChaCha20-Poly1305 always begin with a fixed three-byte pattern 170303 because TLS 1.3 records are disguised as TLS 1.2 records (17 stands for application data that is encrypted). The last two bytes (L1—L0) of a header encode the length of the record including the payload, the message type, optional padding, and the authentication tag. This five-byte TLS Header is the associated data for ChaCha20-Poly1305 encryption and it is taken into account in the computation of the authentication tag, but is not encrypted.

The payload of the TLS 1.3 Record follows the header and contains the actual message appended with the real type (T) of the TLS 1.3 Record (for example, 17 for application data) and optional padding. This payload is the plaintext for ChaCha20-Poly1305 encryption. The record sent over the network consists of the TLS Header followed by the TLS payload. The TLS Payload contains the encrypted payload and the 16-byte authentication tag computed from the header and the encrypted payload during ChaCha20-Poly1305 encryption.

Upon receiving the TLS 1.3 Record, the receiver decrypts the record by using the header as the associated data and the encrypted payload as the ciphertext. If an authentication tag computed during the decryption matches with the authentication tag received in the TLS Record, then the Poly1305 authentication of ChaCha20-Poly1305 is successful and the receiver can trust that the decrypted message was, indeed, sent by the legitimate sender.

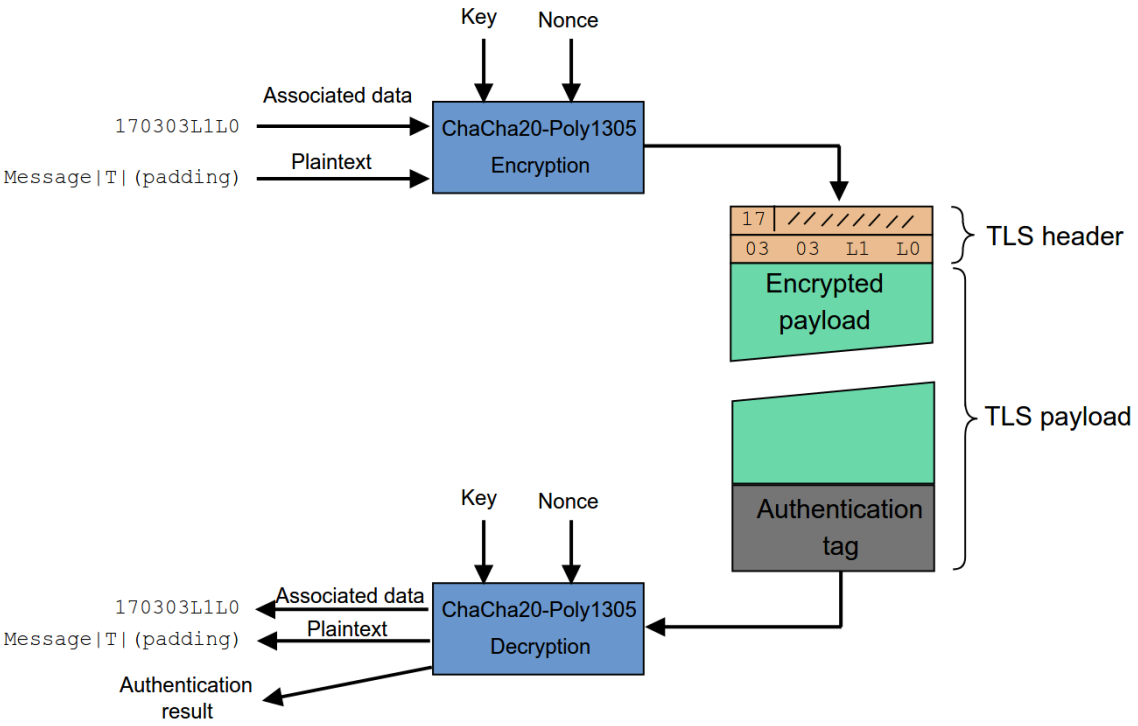

Figure 3: Example use case for XIP2113B in TLS 1.3.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP2113B 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.

Export Control

XIP2113B protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP2113B is controlled by Council Regulation (EC) No 428/2009 of 5 May 2009 and its subsequent changes.

XIP2113B 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) 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] Daniel J. Bernstein. The Poly1305-AES Message-Authentication Code. In *Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers*, pages 32–49, 2005.

[2] Daniel J. Bernstein. New stream cipher designs. chapter The Salsa20 Family of Stream Ciphers, pages 84–97. Springer-Verlag, Berlin, Heidelberg, 2008.

[3] Y. Nir and A. Langley. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439, RFC Editor, June 2018.

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