XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP5012C: RSA SIGNATURE VERIFICATION

RSA Signature Verification IP Core

Product Brief
ver. 1.0
August 1, 2023

sales@xiphera.com

Introduction

XIP5012C from Xiphera is a very compact Intellectual Property (IP) core designed for RSA (Rivest-Shamir-Adleman) signature verification. XIP5012C supports all modulus lengths up to 4096 bits, and it can also be used for RSA public key exponentiation. RSA signature verification is used in numerous contemporary security protocols and applications, including TLS 1.3.

XIP5012C has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP5012C does not rely on any FPGA manufacturer-specific features.

Key Features

- **Minimal Resource Requirements:** The entire XIP5012C requires 470 LUTs (lookup tables) and 1-2 memory blocks (Xilinx® Artix-7®)[1] FPGA.
- **Performance:** Despite its small size, XIP5012C can support more than 10 digital signature verification operations per second.
- **Standard Compliance:** XIP5012C is compliant with FIPS 186-4 [1].

Functionality

XIP5012C computes exponentiations with a public exponent, and it supports all modulus sizes up to 4096 bits[2]. The modulus size can also be set to a lower value to speed up the computations. The public exponent must an odd number and fit into one 32-bit word. Both the modulus size

[1] The exact number depends on the targeted FPGA architecture

[2] Upon request, the current upper limit of 4096 bits can be increased. This will have an impact on the FPGA resource utlization.

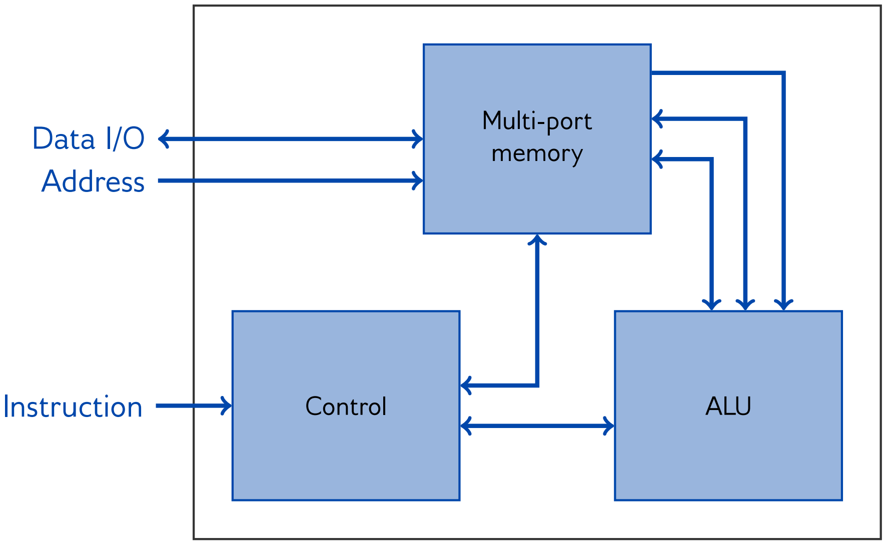

Figure 1: Internal high-level block diagram of XIP5012C

and the exponent can be changed during the operation of XIP5012C by writing new values into registers in XIP5012C.

Block Diagram

The internal high-level block diagram of XIP5012C is depicted in Figure 1.

Interfaces

The external interfaces of XIP5012C are depicted in Figure 2.

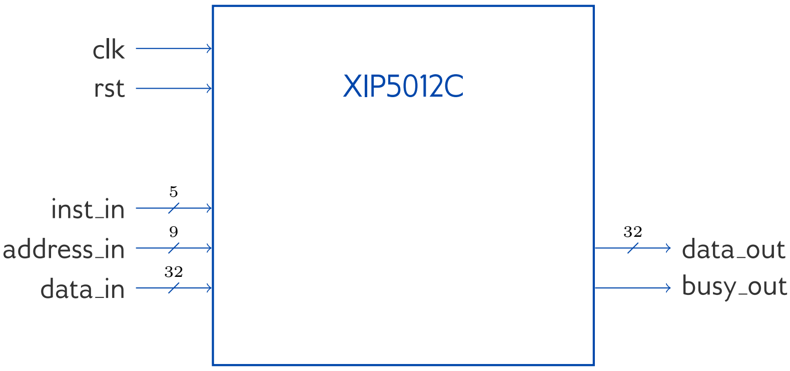

Figure 2: External interfaces of XIP5012C

This Product Brief describes a high-level overview of the functionality and capabilities of XIP5012C. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP5012C, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

FPGA Resources and Performance

Table 1 presents the FPGA resource requirements for representative low-cost FPGA families. On request, the resource estimates can also be supplied for other FPGA families.

Device	Resources	f_{MAX}
Intel® Cyclone® V SX SoC[*]	265 ALM, 4 M10K	131.61 MHz
Intel® Cyclone® 10 LP[*]	482 LE, 4 M9K	99.82 MHz
Intel® MAX® 10[*]	483 LE, 4 M9K	135.81 MHz
Xilinx® Artix-7® [†]	470 LUT, 1 RAMB36	175.96 MHz
Xilinx® Spartan-7® [†]	471 LUT, 1 RAMB36	176.80 MHz
Xilinx® Zynq-7000® [†]	471 LUT, 1 RAMB36	141.14 MHz
Lattice® ECP5® [‡]	419 LUT4, 4 EBR	105.55 MHz
Microchip® PolarFire® [§]	643 4LUT, 4 LSRAM	128.67 MHz

Table 1: Resource usage and performance of XIP5012C on representative FPGA families.

Example Use Cases

Example use cases of XIP5012C include hardware-isolated verification of digital certificates: XIP5012C verifies the signature of an incoming certificate using a trusted RSA public key (modulus and exponent) from a secure key memory. If and only if XIP5012C successfully verifies the signature, the incoming certificate (and its public key) can be stored in the secure key memory and can be used for verifying other certificates in the future.

In addition to XIP5012C, this use case requires a SHA-256 IP Core (for example XIP3022B or XIP3027C from Xiphera) and a secure key memory; please contact Xiphera for further details.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP5012C 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

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.

[*] Quartus® Prime Lite 20.1.1, default compilation settings, industrial speedgrade.

[†] Vivado 2020.2, default compilation settings, industrial speedgrade.

[‡] Diamond 3.12.0, default compilation settings, synthesised with Synplify.

[§] Libero 2022.1.0.10, default compilation settings, industrial speedgrade.

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 186-4 Digital Signature Standard (DSS). Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2013.