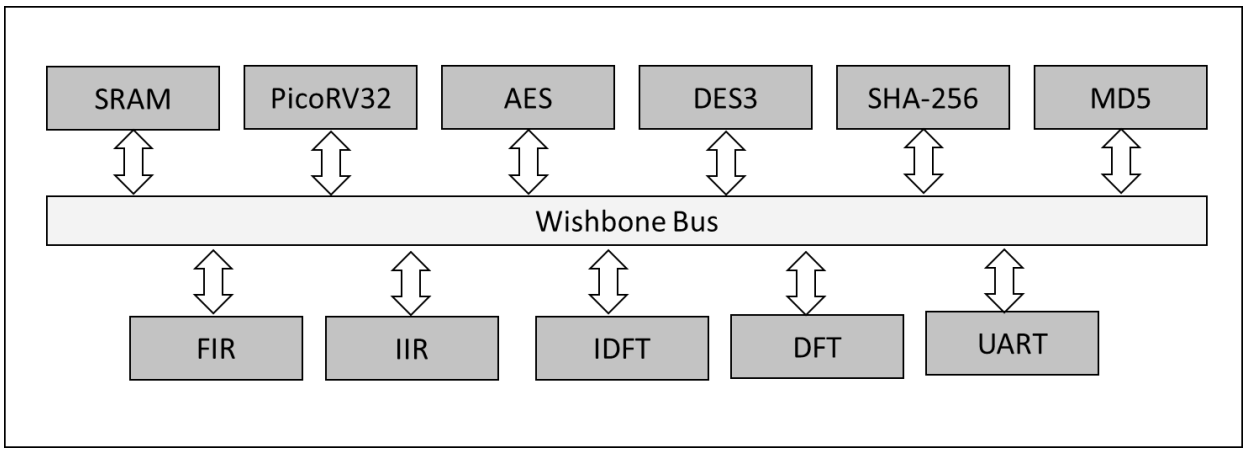
SoC Model with Wishbone Bus



System Overview:

This is a shared bus based SoC with Wishbone interconnect. It has a RISC-V CPU, namely PicoRV32, and a dual port SRAM as the on-chip memory. Four crypto modules i.e., AES, DES3, SHA-256, and MD5 are included for generic cryptographic operations. It features four DSP blocks, including FFT, IDFT, IIR, and FIR as hardware accelerators. A UART module is incorporated in the SoC for off-chip communication. All the IP cores are obtained from open-source repositories.

SoC Components:

PicoRV32:

PicoRV32 is a CPU core that implements 32-bit RISC-V ISA. It can be configured as RV32E, RV32I, RV32IC, RV32IM, or RV32IMC core, and it optionally contains a built-in interrupt controller. Toolchain (gcc, binutils, etc..) for the core can be obtained from RISC-V Website. Detailed description of the core can be found in [1].

Wishbone Shared Bus:

This is a generic wishbone bus (B3). The number of masters and slaves are configurable. Ten slaves can be connected with a configurable memory map. Data and address width are defined in bits. Data width must be full bytes (i.e., multiple of 8). The ports are flattened i.e., all masters share the bus signal ports. For instance, with four masters and a data width of 32 bit the master cycle input port is 4-bit wide and the master data input port is 128-bit wide. The signals are arranged from right to left, meaning the master data input is defined as [data width x (number of masters – 1)] and each master port is assigned to [(master+1)*data width-1:master*data width]. The memory map is defined with the slave *range width* and slave *range match* parameters. The *range width* sets the number of most significant bits that are relevant to define the memory range. The *range match* accordingly sets the value of those bits of the address that define the memory range. Detailed description of the core can be found in [2].

AES:

The AES core implements a symmetric-key algorithm, in which the same key is used for both encrypting and decrypting the data. The block size is restricted to 128 bits. The key size can be 128, 192, or 256 bits. It operates on a 4×4 matrix of bytes, called the state. Some rounds of transformation convert the plaintext into the final cipher-text. The number of rounds is six plus the key size divided by 32. One round reads the state into four 4-byte variables y_0, y_1, y_2, y_3; transforms the variables; xor's them by a 16-byte round key; and puts the result into z_0, z_1, z_2, z_3.

When targeting a variable-length plaintext, the plaintext must first be partitioned into separate cipher blocks, and then be encrypted under some mode of operation, generally using randomization based on an additional initialization vector. The cipher feedback (CFB) mode, output feedback (OFB) mode are specified in FIPS 81. The counter (CTR) mode is specified by NIST in SP800-38A. The advantage of these modes is only using encryption algorithm for both encryption and decryption. So the AES hardware price may be reduced by 50% (does not need decryption hardware).

DES3:

DES3 is an implementation of Triple DES algorithm in verilog. It takes 56-bit keys and 64 bits of data as input and generates a 64-bit encrypted/decrypted result. The following variants of the DES3 crypto block can be implemented:

1) Area Optimized (CBC Mode) This is a sequential implementation and needs 48 cycles to complete a full encryption/decryption cycle.

2) Performance Optimized (EBC Mode) This is a pipelined implementation that has a 48 cycle pipeline (plus 1 input and 1 output register). It can perform a complete encryption/decryption every cycle.

SHA-256:

This IP core is a hardware implementation of SHA-256 cryptographic hash function with support for both SHA-256 and SHA-224. The implementation is written in Verilog 2001 compliant code. The implementation includes the main core as well as wrappers that provides interfaces for simple integration. This is a low area implementation that iterates over the rounds but there is no sharing of operations such as adders.

MD5:

This IP core that implements the MD5 message digest algorithm. Some of the features of the core are as following:

- Up to 128-bit input message
- Parameterized 'salts' that default to the MD5-prescribed values
- MD5 compliant 128-bit output
- Verilog entry
- Very minimal amount of control signals (3)
- Synchronous logic

IIR:

This core is a Transposed Direct Form implementation of an Infinite Impulse Response (IIR) filter, from a standard difference equation. The multiplier blocks within the design are generated from the Spiral

Multiplier Block Generator. An FIR can be generated by simply setting a_0 to one and all other a_k constants

$$a_0 y[n] = \sum_{k=0}^{N-1} b_k x[n-k] - \sum_{k=1}^{N-1} a_k y[n-k]$$

Standard Difference Equation

to zero. The values of the b_k constants form the notches of the FIR. In the Transposed Direct Form I implementation, the IIR is generated from two separate FIR filters, connected by an adder. In the Transposed Direct Form II implementation, the FIR filter tool is not used at all, and the two multiplier block outputs are taken directly through adders and input into the flip flop array.

FIR:

This core is a Transposed Direct Form implementation of a Finite Impulse Response (FIR) filter, from a standard difference equation. The multiplier blocks within the design are generated from the Spiral Multiplier Block Generator. An FIR can be generated by simply setting a_0 to one and all other a_k constants

$$a_0 y[n] = \sum_{k=0}^{N-1} b_k x[n-k] - \sum_{k=1}^{N-1} a_k y[n-k]$$

Standard Difference Equation

to zero. The values of the b_k constants form the notches of the FIR. In the Transposed Direct Form I implementation, the IIR is generated from two separate FIR filters, connected by an adder. In the Transposed Direct Form II implementation, the FIR filter tool is not used at all, and the two multiplier block outputs are taken directly through adders and input into the flip flop array.

DFT:

This is a customized Discrete Fourier Transform (DFT) soft IP core in synthesizable RTL Verilog. It uses fast Fourier transform algorithms (FFTs). The user has control over a variety of parameters that control the functionality and cost/performance tradeoffs such as area and throughput. The salient features of the design are as following:

- DFT Size = 64
- ***direction = forward***
- data type = 16-bit fixed point, unscaled
- architecture = fully streaming
- radix = 2
- streaming width = 2
- data ordering = natural input / natural output
- BRAM budget = 1000
- Input/output stream: 2 complex words per cycle
- Throughput: one transform every 32 cycles

- Latency: 145 cycles

IDFT:

This is a customized Discrete Fourier Transform (DFT) soft IP core in synthesizable RTL Verilog. It uses fast Fourier transform algorithms (FFTs). The user has control over a variety of parameters that control the functionality and cost/performance tradeoffs such as area and throughput. The salient features of the design are as following:

- DFT Size = 64
- ***direction = inverse***
- data type = 16-bit fixed point, unscaled
- architecture = fully streaming
- radix = 2
- streaming width = 2
- data ordering = natural input / natural output
- BRAM budget = 1000
- Input/output stream: 2 complex words per cycle
- Throughput: one transform every 32 cycles
- Latency: 145 cycles

UART:

The UART (Universal Asynchronous Receiver/Transmitter) core provides serial communication capabilities, which allow communication with modem or other external devices, like another computer using a serial cable and RS232 protocol. This core is designed to be maximally compatible with the industry standard National Semiconductors' 16550A device.

Features:

- WISHBONE interface in 32-bit or 8-bit data bus modes (selectable)
- FIFO only operation
- Register level and functionality compatibility with NS16550A (but not 16450).
- Debug Interface in 32-bit data bus mode.

SoC Simulation & Emulation:

This SoC can be simulated with directed and random testbenches written in HDL. IP level, bus-level, and system level testbenches for the hardware accelerators are provided. IP level and bus-level simulation can be performed via Verilator and/or ModelSim. FPGA mapping is required for system level emulation. RISC-V tool chain can be used to compile programs (c code compiled to binaries using RISC-V tool chain) for the RV32 processor core and the generated firmware HEX / MEM file can be stored in the RAM block of the SoC. Generated SoC can be synthesize the design to get area, power, and timing results.

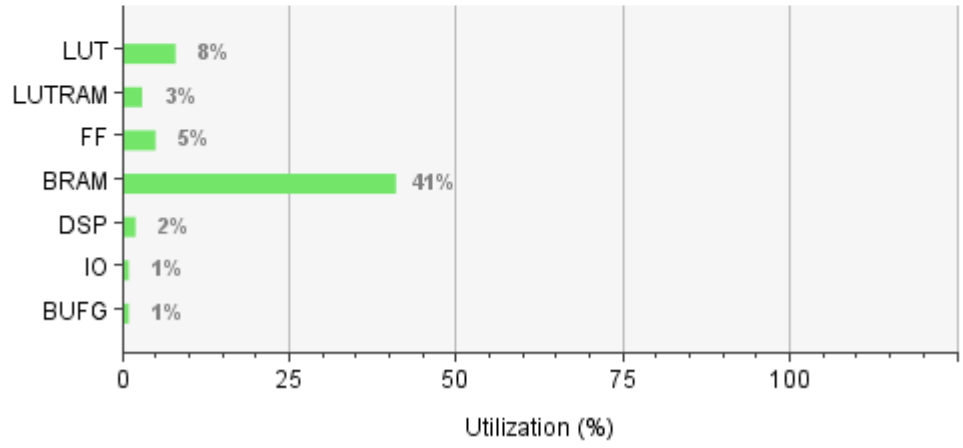
Implementation Results:

The SoC model is synthesized on a Xilinx FPGA using Vivado Design Suite. The implementation results are shown below:

Product Family: Zynq UltraScale+
Part: xczu7ev-ffvf1517-1LV-i

Area Overhead / Resource Utilization Report:

Resource	Utilization	Available	Utilization %
LUT	19172	230400	8.32
LUTRAM	2618	101760	2.57
FF	23334	460800	5.06
BRAM	126.50	312	40.54
DSP	40	1728	2.31
IO	6	464	1.29
BUFG	1	544	0.18



Power Overhead / On-chip Power Report:

Power estimation from Synthesized netlist. Activity derived from constraints files, simulation files or vectorless analysis. Note: these early estimates can change after implementation.

Total On-Chip Power:	**1.746 W**
Design Power Budget:	**Not Specified**
Power Budget Margin:	**N/A**
Junction Temperature:	**26.5°C**
Thermal Margin:	73.5°C (85.5 W)
Effective ϑJA:	0.8°C/W
Power supplied to off-chip devices:	0 W
Confidence level:	Medium

Launch Power Constraint Advisor to find and fix invalid switching activity