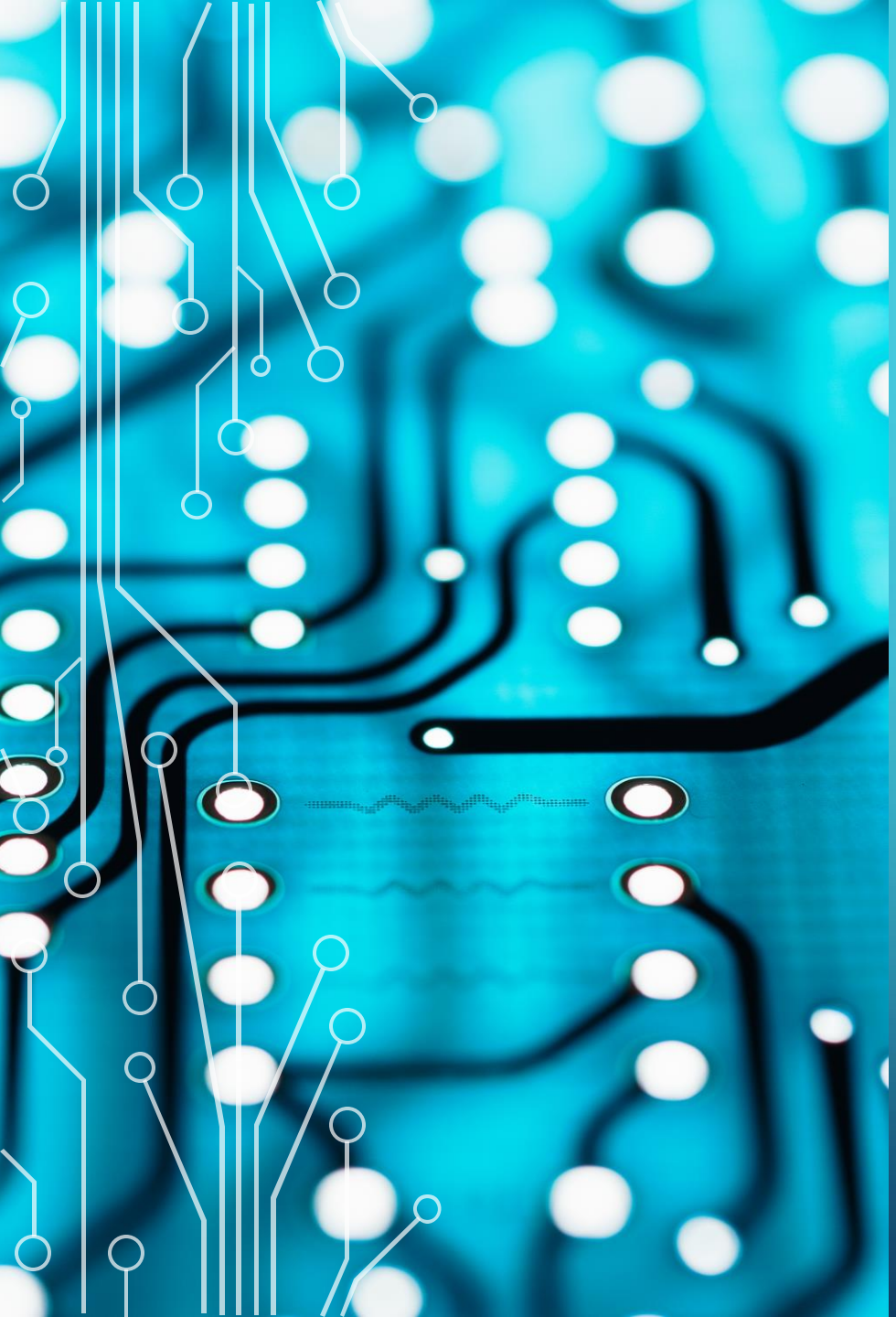
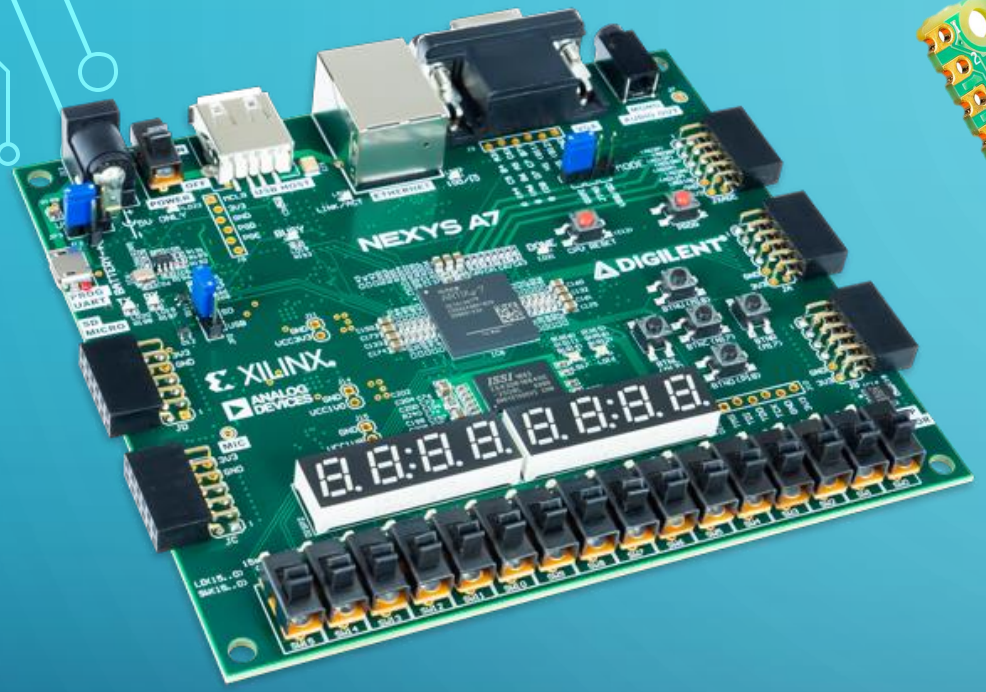
ECE 4300.01
COMPUTER ARCHITECTURE
GROUP A

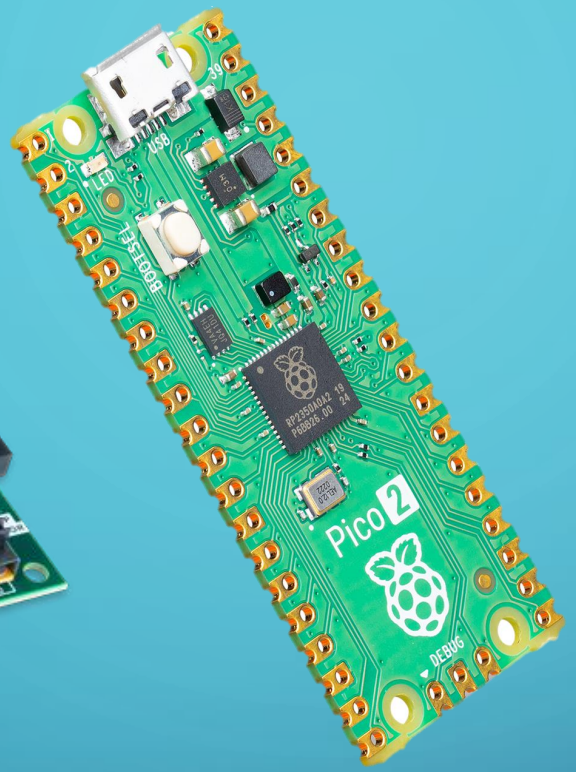
ELLA SHEPHERD, AARON TRAN, MAX GROSS, ANISH CHINNAKONDA

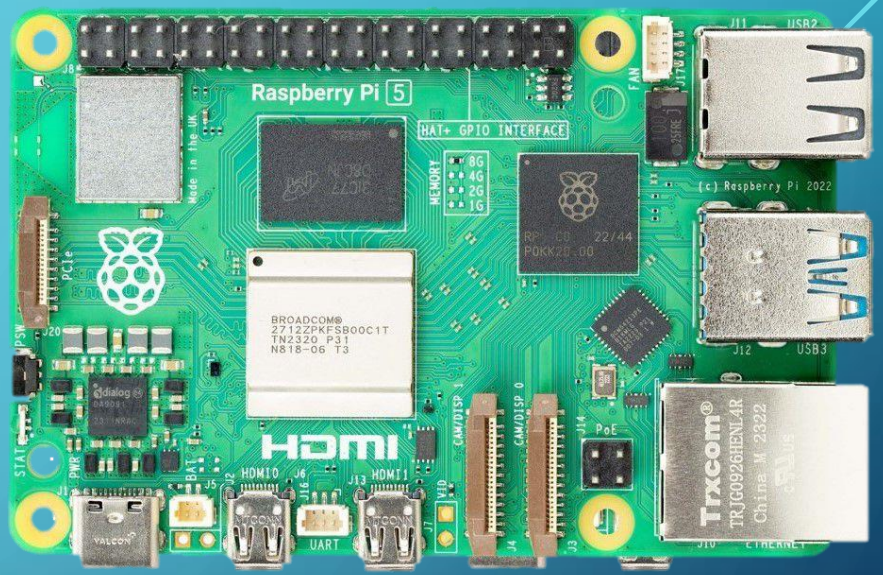


PROMPT 1

- “Studying the complete benchmarking of the SHA-2/SHA-3 hash functions on softcore processors (NIOS/Intel, MicroBlaze/AMD, or RISC-V architecture created by UC Berkeley)”







NEXYS A7

With

MICROBLAZE

RASPBERRY PI PICO 2

With

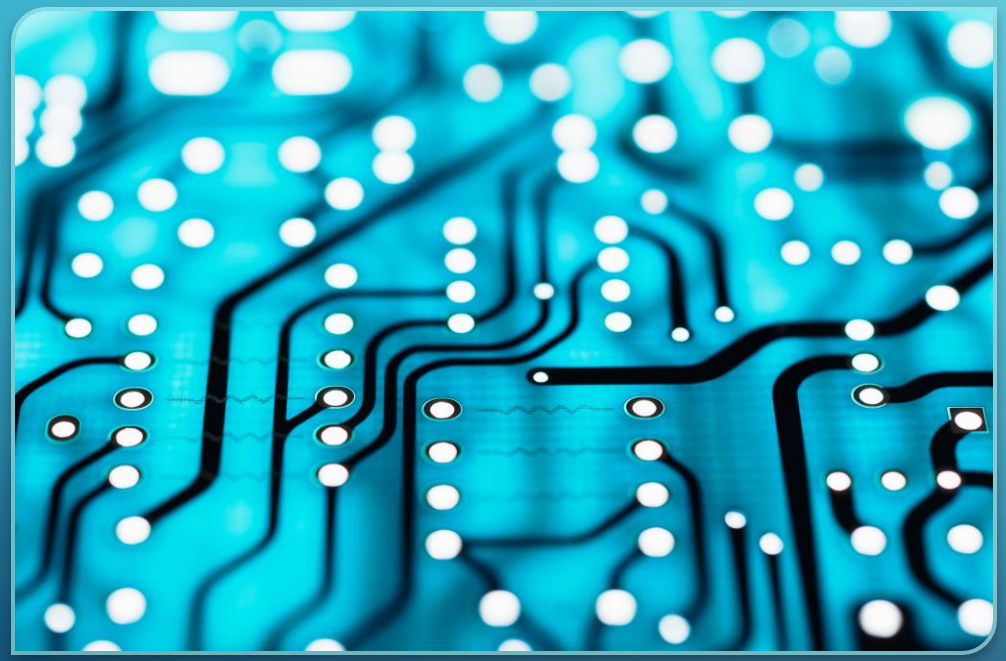
RISCV

RASPBERRY PI 5

With

ARM

TESTING CRITERIA

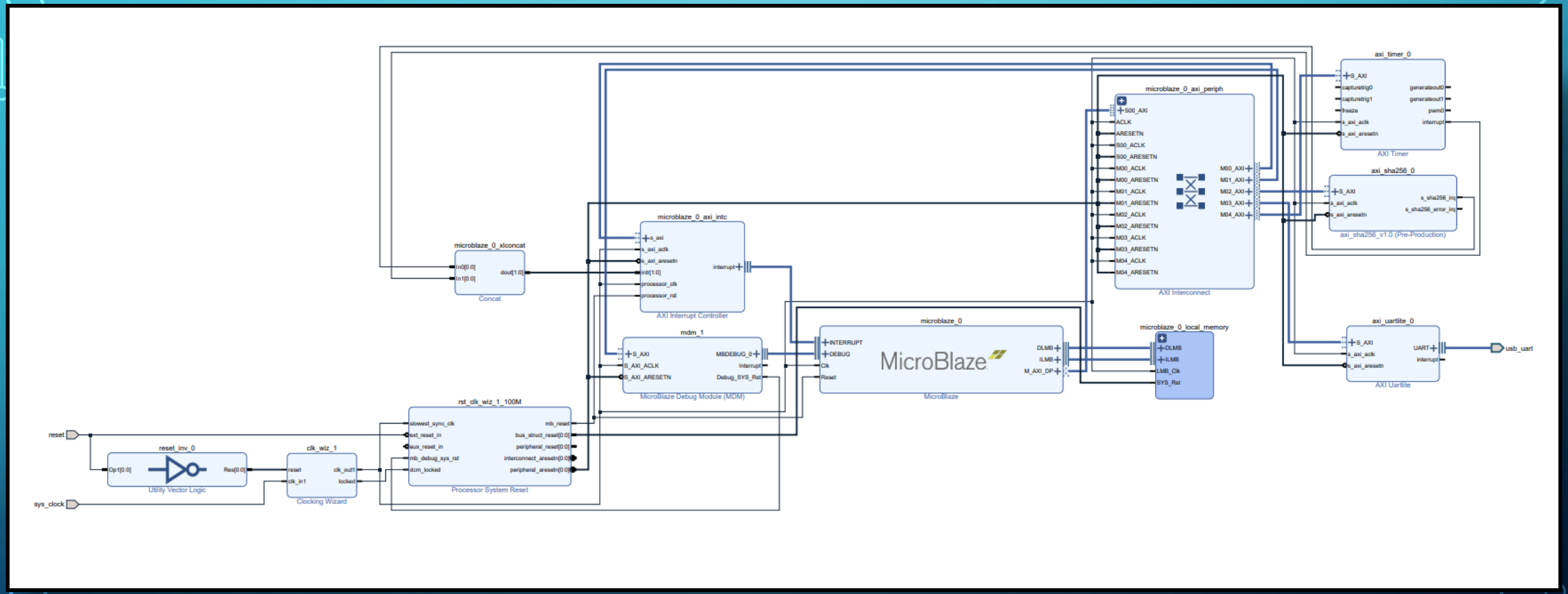


- Implementing to get a hash of 16 Kbytes repeatedly, then listening for power to log how much time it takes.
- Doing this by testing for…
  - 16 Kbytes for 3 seconds
  - USB C for power measurements

NEXYS A7 WITH MICROBLAZE

- 100 MHz FPGA Softcore Microcontroller
- Microblaze V – a Risk-V based architecture
- AXI bus
  - AXI UARTLite @9600 Baud
  - AXI Hardware Timer
  - AXI Interrupt Handler
  - AXI SHA256 Hardware Accelerator

MICROBLAZE BLOCK DIAGRAM



CURRENT PROGRESS - MICROBLAZE

- Source Code Provided Compiles
- AXI Registers are Read/Writable and pass SelfTest()
- Unable to create a hash

```
---- Opened the serial port COM6 ----
---Entering main---

 Running AXI_SHA256_Reg_SelfTest() for microblaze_0_axi_intc...
******************************
* User Peripheral Self Test
******************************

User logic slave module test...
   - slave register write/read passed

AXI_SHA256_Reg_SelfTest PASSED

Benchmarking sha256...

 Running sha256() for microblaze_0_axi_intc...
sha256 FAILED
---Exiting main---
```

RASPBERRY PI PICO 2 WITH RISCV

- **Raspberry Pi Pico 2** uses the RP2350 MCU with 520 KB SRAM, 4 MB flash, and 150 MHz dual-core performance.
- Supports both **Arm Cortex** and **RISC-V** cores. RISC-V selected for all benchmarking.
- Benchmarking **SHA-2 (SHA-256/512)** and **SHA-3 (Keccak)** hash functions entirely on RISC-V.
- Perform **power analysis** by monitoring current on VSYS during hash computations at set frequencies.
- Generate **performance vs energy** plots comparing software and hardware-accelerated SHA-256 runs.

EXAMPLE:
RASPBERRY PI 5 WITH ARM

•Physical Hardware block built into the System on Chip of the Raspberry PI 5 inside the ARM Cortex-A76 CPU on the PI's Broadcom BCM2712

•Utilizes ARMv8-A Cryptographic Extension on ARM Cortex-A76 CPU

•Processes cryptography in hardware crypto extension much faster than the CPU could do in software. The main OS is not involved beyond normal scheduling.

•OpenSSL libraries route the crypto instruction to the hardware engine so that the main OS doesn't have to perform the cryptography instruction.

•Capable of executing AES(Advanced Encryption Standard)/SHA(Secure Hash Algorithm) instructions on the ARM crypto extension

•Supports AES encryption/Decryption and SHA-2 and SHA-256

UPCOMING, DUE 11/26

Course Project	Deliverables
1) **Document subfolder:**	Final IEEE Formatted Report
2) **Code Subfolder:**	Any codes or profiling tools used during the project will be added under this subfolder
3) **Presentation subfolder:**	- Presentation Slides - Video Presentation Recording - Slider Presentation Poster (leverage the importance of the work that the project has done)
4) **Demo Folder:**	An interesting demo recorded as a video, which shows an exciting part of the project with running example on the code is developed or used by the team