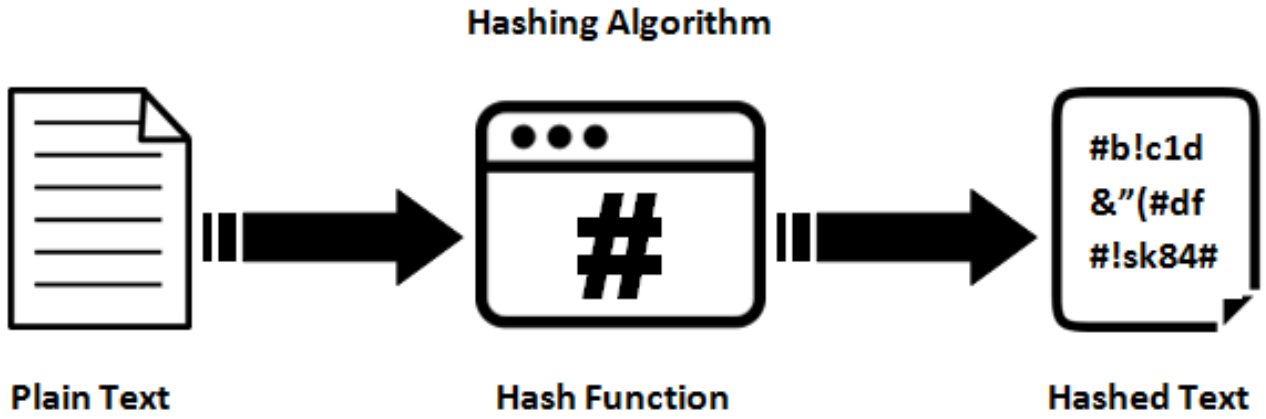
Benchmarking SHA-2/ SHA-3 on MicroBlaze

By: Michael Rosales, Michael Yen, Nathaniel Case, and Noah Mendoza

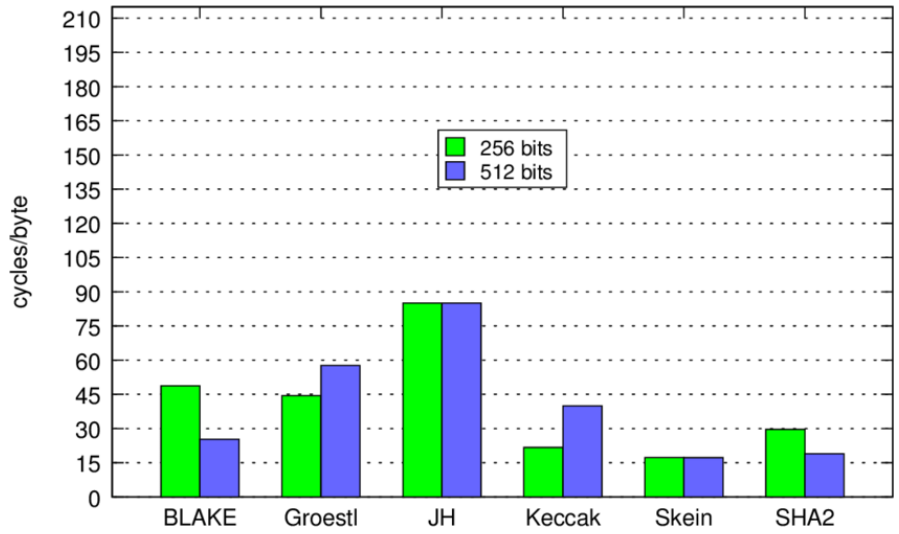
What This Presentation Discusses

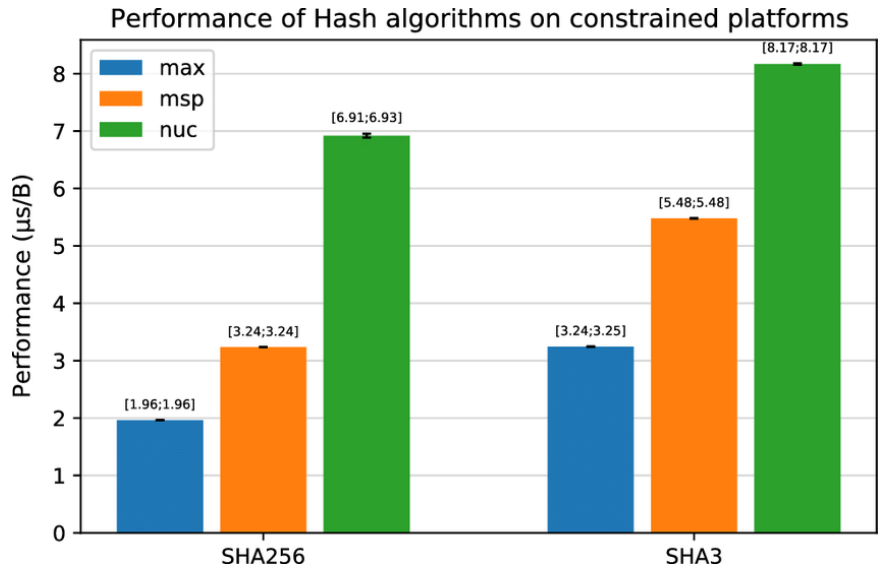
- **Purpose**: Benchmark SHA-2 and SHA-3 on MicroBlaze in constrained environments.
- **Why MicroBlaze?** Customizable, ideal for embedded systems.
- **Metrics**: Execution time, throughput, energy.
- **Insights**: Efficiency vs. security trade-offs.
- **Impact**: Informs secure algorithm selection.



Motivations

- **Relevance**: SHA-2/SHA-3 ensure secure communication and data integrity.
- **Need**: Comparison driven by new cryptographic threats.
- **Focus**: Constrained systems like IoT and CubeSats.
- **MicroBlaze**: Customizable and ideal for benchmarking.
- **Impact**: Balances efficiency and security insights.





State of the Art Technology Relating to This

SHA-2: Efficient and widely used for secure communication, including digital signatures.

SHA-3: Enhanced security with sponge construction, resistant to physical attacks.

Bitcoin: SHA-256 is the primary hashing algorithm for mining and transactions.

IoT and Cloud Systems: SHA-3 is used in IoT devices, while SHA-2 and SHA-3 are integrated into cloud providers (AWS, Google Cloud, Azure).

MicroBlaze: Benchmarks provide insights into performance in constrained environments.

System and Setup

01

Hardware: Nexys A7-100T FPGA with MicroBlaze processor.

02

Processor Configuration:

- 32-bit architecture, clocked at 100 MHz.
- Instruction and data caches enabled.
- DDR2 SDRAM added for larger datasets.

03

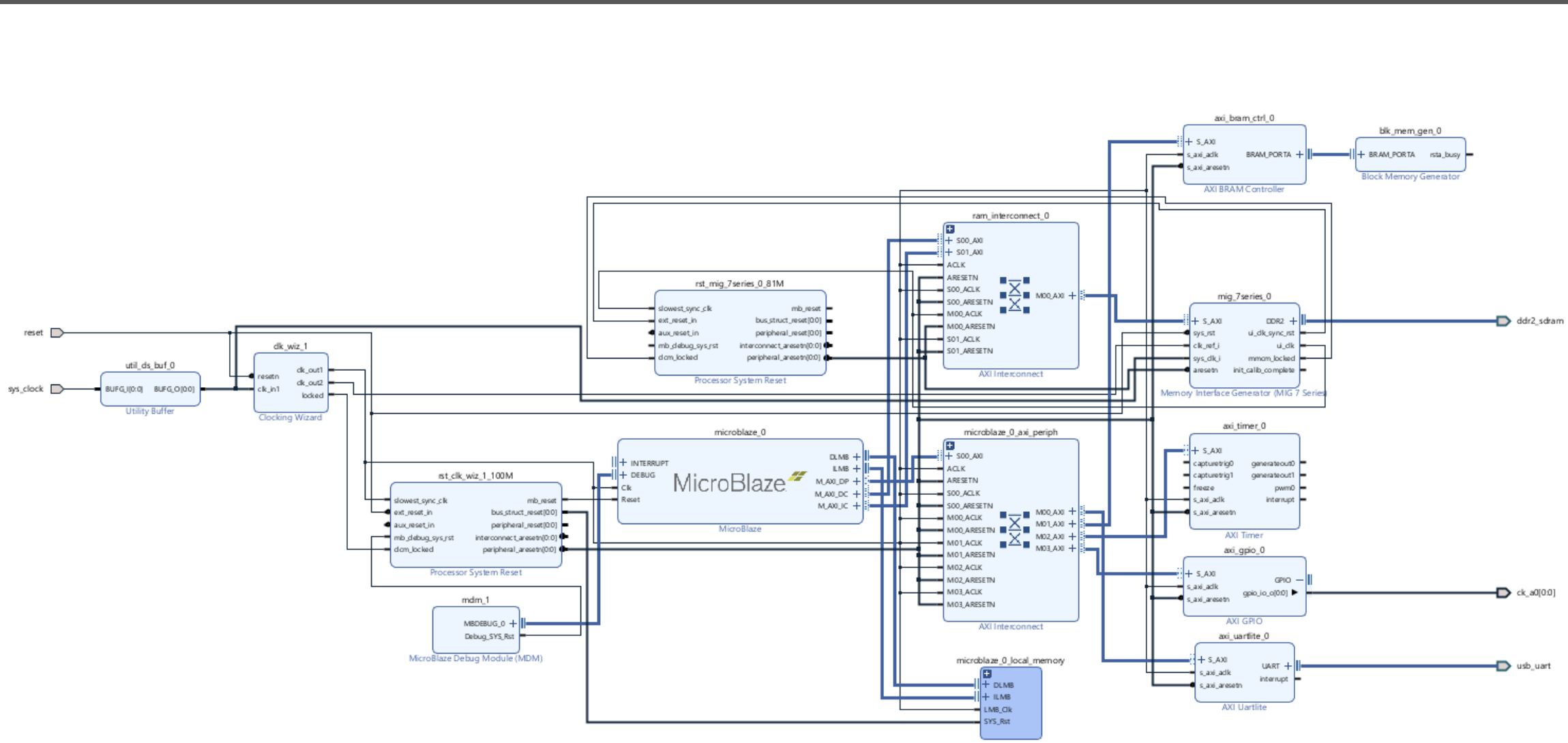
Peripherals:

- AXI UARTLite for input/output.
- AXI Timer for measuring cycles.
- GPIO for debugging.

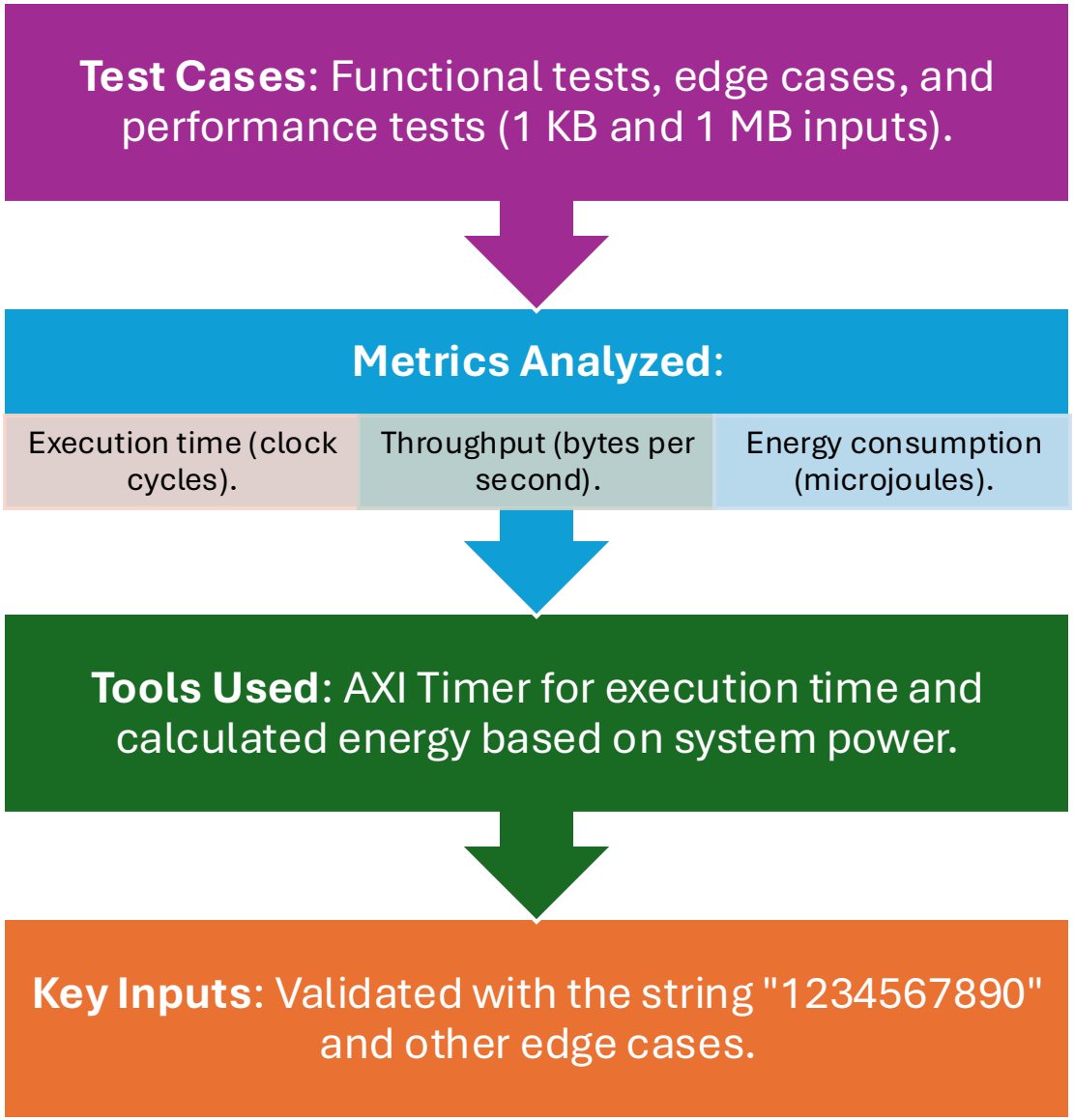
04

Software:

- Open-source SHA-2 and SHA-3 implementations.
- Xilinx Vitis for development and benchmarking.


reset
sys_clock
util_ds_buf_0
BUFG_I[0:0]
BUFG_O[0:0]
Utility Buffer
clk_wiz_1
resetn
clk_in1
clk_out1
clk_out2
locked
Clocking Wizard
rst_mig_7series_0_81M
slowest_sync_clk
ext_reset_in
aux_reset_in
mb_debug_sys_rst
dcm_locked
mb_reset
bus_struct_reset[0:0]
peripheral_reset[0:0]
interconnect_aresetn[0:0]
peripheral_aresetn[0:0]
Processor System Reset
ram_interconnect_0
S00_AXI
S01_AXI
ACLK
ARESETN
S00_ACLK
S00_ARESETN
M00_ACLK
M00_ARESETN
S01_ACLK
S01_ARESETN
M00_AXI
AXI Interconnect
axi_bram_ctrl_0
S_AXI
s_axi_aclk
s_axi_aresetn
BRAM_PORTA
AXI BRAM Controller
blk_mem_gen_0
BRAM_PORTA
rsta_busy
Block Memory Generator
mig_7series_0
S_AXI
sys_rst
clk_ref_i
sys_clk_i
aresetn
DDR2
ui_clk_sync_rst
ui_clk
mmcm_locked
init_calib_complete
Memory Interface Generator (MIG 7 Series)
ddr2_sdram
microblaze_0
INTERRUPT
DEBUG
Clk
Reset
DLMB
ILMB
M_AXI_DP
M_AXI_DC
M_AXI_IC
MicroBlaze
MicroBlaze
rst_clk_wiz_1_100M
Processor System Reset
mdm_1
MBDEBUG_0
Debug_SYS_Rst
MicroBlaze Debug Module (MDM)
microblaze_0_axi_periph
S00_AXI
M00_AXI
M01_AXI
M02_AXI
M03_AXI
AXI Interconnect
microblaze_0_local_memory
DLMB
ILMB
LMB_Clk
SYS_Rst
axi_timer_0
S_AXI
capturetrig0
capturetrig1
freeze
generateout0
generateout1
pwm0
interrupt
AXI Timer
axi_gpio_0
S_AXI
GPIO
gpio_io_o[0:0]
AXI GPIO
ck_a0[0:0]
axi_uartlite_0
S_AXI
UART
interrupt
AXI Uartlite
usb_uart

Performance Analytics



SHA 2-256 Vs. SHA 3-256

- **Execution Time**: SHA 2-256 is faster; SHA 3-256 is slower due to sponge construction.
- **Throughput**: SHA 2-256 achieves 12,288 bytes/s (1 KB), SHA 3-256 only 8,677 bytes/s.
- **Energy**: SHA 2-256 is more efficient; SHA 3-256 uses more energy for larger inputs.
- **Conclusion**: SHA 2-256 is better for efficiency, SHA 3-256 for stronger security.

	SHA 2-256			
Test Type	**Elapsed Cycles**	**Execution Time (µs)**	**Throughput (bytes/s)**	**Energy Consumed (µJ)**
Edge Test (Empty Input)	8332655	83326	0	92575
Performance Test (1KB)	8332791	83327	12288	92576
Performance Test (1MB)	550589815	5505898	109	6117052
Functional Test (1234567890)	8332615	83326	120	92575

	SHA 3-256			
Test Type	**Elapsed Cycles**	**Execution Time (µs)**	**Throughput (bytes/s)**	**Energy Consumed (µJ)**
Edge Test (Empty Input)	8436960	84369	0	16536
Performance Test (1KB)	11801316	118013	8677	23130
Performance Test (1MB)	509016809	5090168	118	997672
Functional Test (1234567890)	8436959	84369	118	16536

SHA 2-384 Vs. SHA 3-384

- **Execution Time**: SHA 2-384 is faster; SHA 3-384 slower for larger inputs.
- **Throughput**: SHA 2-384: 8,777 bytes/s (1 KB), SHA 3-384: 6,245 bytes/s.
- **Energy**: SHA 2-384 is more efficient; SHA 3-384 uses more energy.
- **Conclusion**: SHA 2-384 excels in efficiency, SHA 3-384 in security.

	SHA 2-384			
Test Type	**Elapsed Cycles**	**Execution Time (µs)**	**Throughput (bytes/s)**	**Energy Consumed (µJ)**
Edge Test (Empty Input)	11665804	116658	0	116658
Performance Test (1KB)	11665920	116659	8777	129608
Performance Test (1MB)	686904071	6869040	87	7631503
Functional Test (1234567890)	11665743	116657	85	129605

	SHA 3-384			
Test Type	**Elapsed Cycles**	**Execution Time (µs)**	**Throughput (bytes/s)**	**Energy Consumed (µJ)**
Edge Test (Empty Input)	11770011	117700	0	23069
Performance Test (1KB)	16394718	163947	6245	32133
Performance Test (1MB)	1966725523	19667255	30	3854781
Functional Test (1234567890)	11770032	117700	84	23069

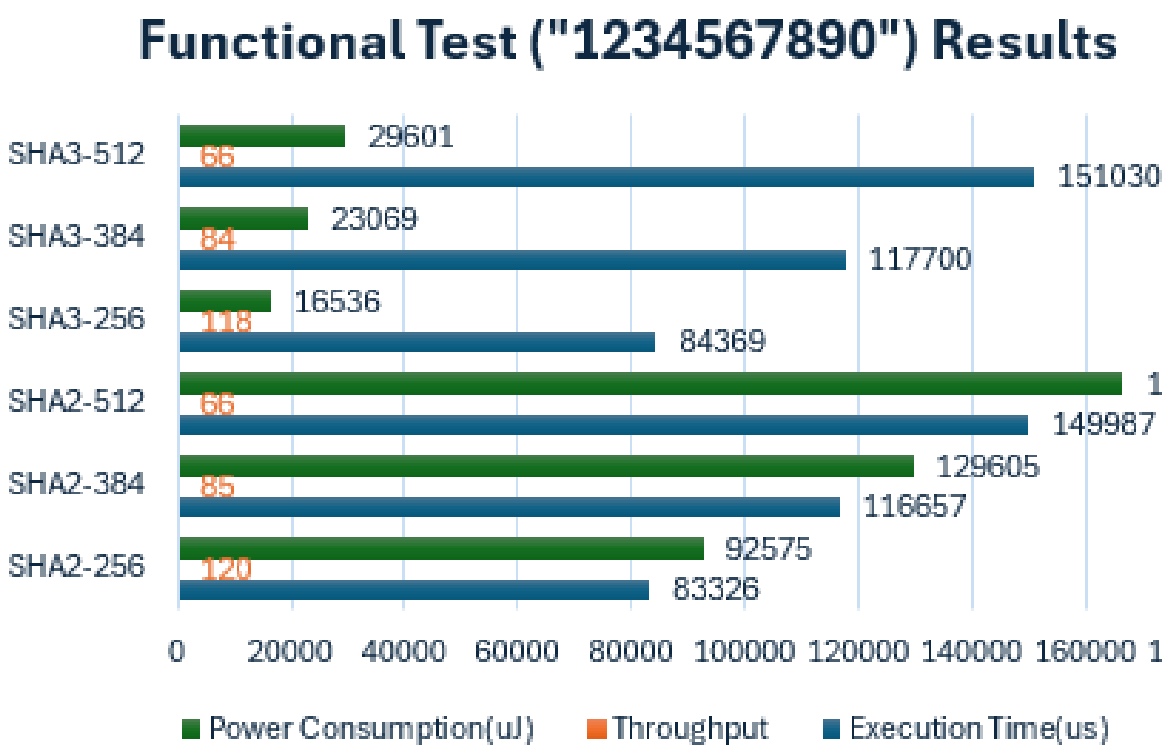
SHA 2-512 Vs. SHA 3-512

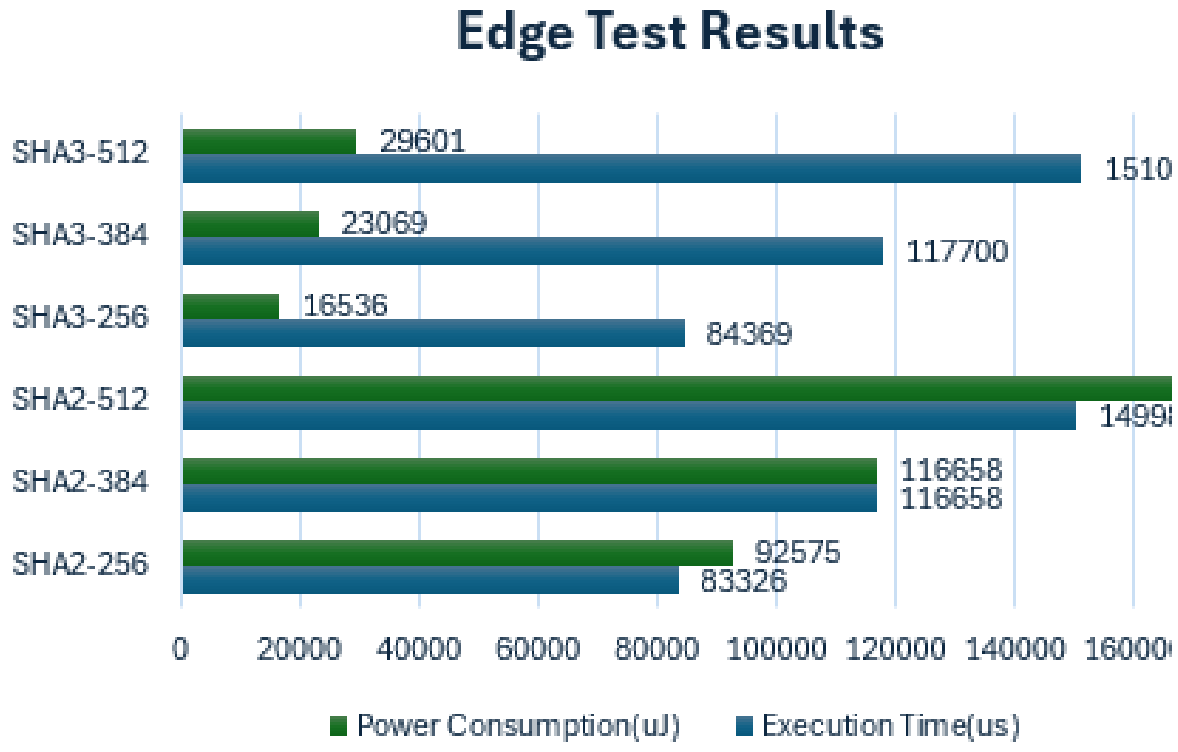
- **Execution Time**: SHA 2-512 is faster; SHA 3-512 is slower.
- **Throughput**: SHA 2-512: 6,827 bytes/s; SHA 3-512: 4,489 bytes/s.
- **Energy**: SHA 2-512 uses less energy; SHA 3-512 uses more for large inputs.
- **Conclusion**: SHA 2-512 excels in efficiency; SHA 3-512 offers stronger security.

	SHA 2-512			
Test Type	**Elapsed Cycles**	**Execution Time (µs)**	**Throughput (bytes/s)**	**Energy Consumed (µJ)**
Edge Test (Empty Input)	14998762	149987	0	166635
Performance Test (1KB)	14998927	149989	6827	166637
Performance Test (1MB)	690268252	6902682	87	7668879
Functional Test (1234567890)	14998773	149987	66	166635

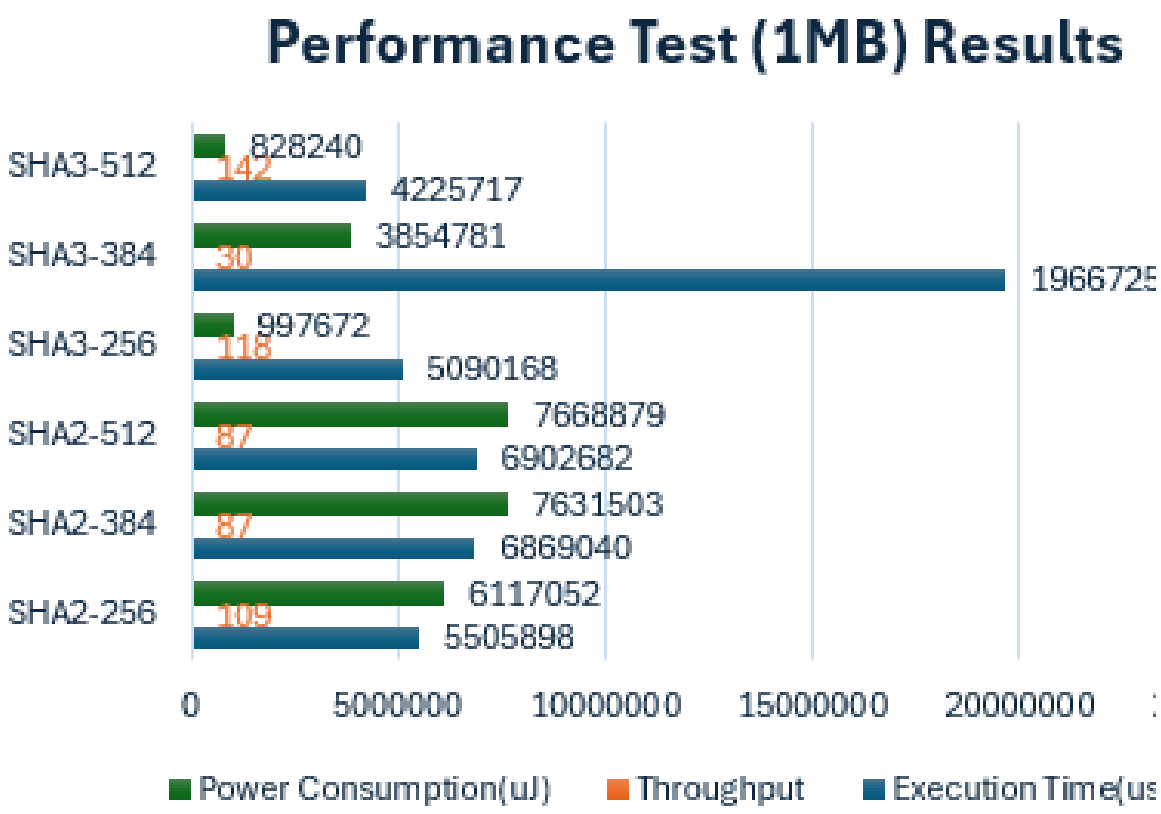
	SHA 3-512			
Test Type	**Elapsed Cycles**	**Execution Time (µs)**	**Throughput (bytes/s)**	**Energy Consumed (µJ)**
Edge Test (Empty Input)	15103082	151030	0	29601
Performance Test (1KB)	22810932	228109	4489	44709
Performance Test (1MB)	422571709	4225717	142	828240
Functional Test (1234567890)	15103077	151030	66	29601

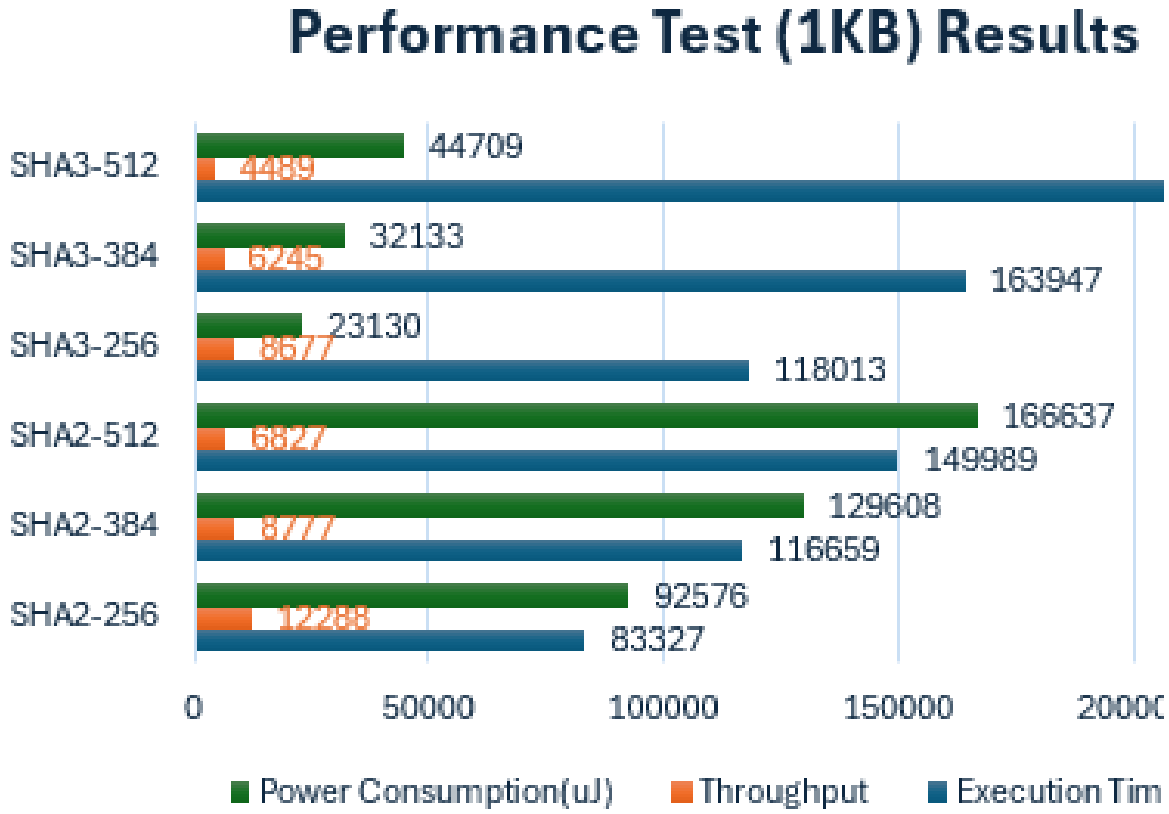
Edge Test and Functional Test





Performance Tests (1MB/1KB)





Conclusion

Hash Length: SHA-2 and SHA-3 outputs:

256-bit: 64 chars,
384-bit: 96 chars,
512-bit: 128 chars.

Performance: SHA-2 is faster; SHA-3 offers stronger security.

Energy: SHA-2 is efficient for small inputs; SHA-3 for larger ones.

Trade-offs: SHA-2 suits constrained systems; SHA-3 fits high-security needs.

Future Works

- **Processor Comparison**: Test algorithms on other processors, such as Intel Nios II or RISC-V.
- **Input Variability**: Use larger, randomized, or real-world datasets (e.g., logs, sensor data).
- **Compiler Optimizations**: Analyze performance using optimization flags like -O3.
- **Hardware Acceleration**: Implement and compare hardware-accelerated versions on FPGA logic.
- **Power Profiling**: Use precise tools to refine energy consumption analysis.