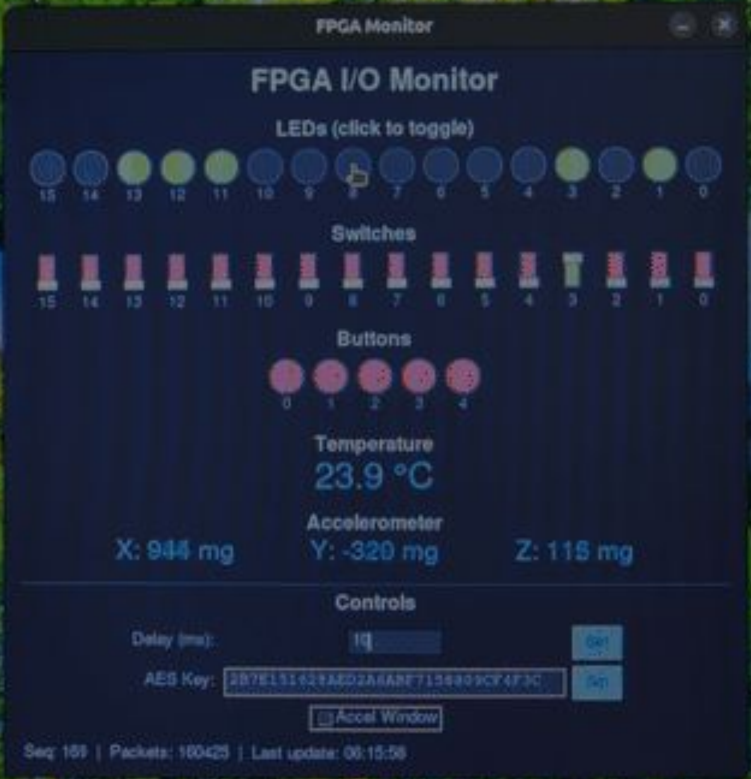
IoT Gateway

WITH AES-128 CRYPTOGRAPHY

Miguel Vila (107276)
Sistemas Integrados para Aplicações Embutidas



Temperature
23.9 °C

Accelerometer
X: 944 mg Y: -320 mg Z: 118 mg

Controls

Delay (ms): 10

AES Key: 2B7E151628AED2A6ABF7158809CF4F3C

□ Accel Window

Seq: 169 | Packets: 160425 | Last update: 06:15:58

universidade de aveiro
deti departamento de eletrónica, telecomunicações e informática

Context ?

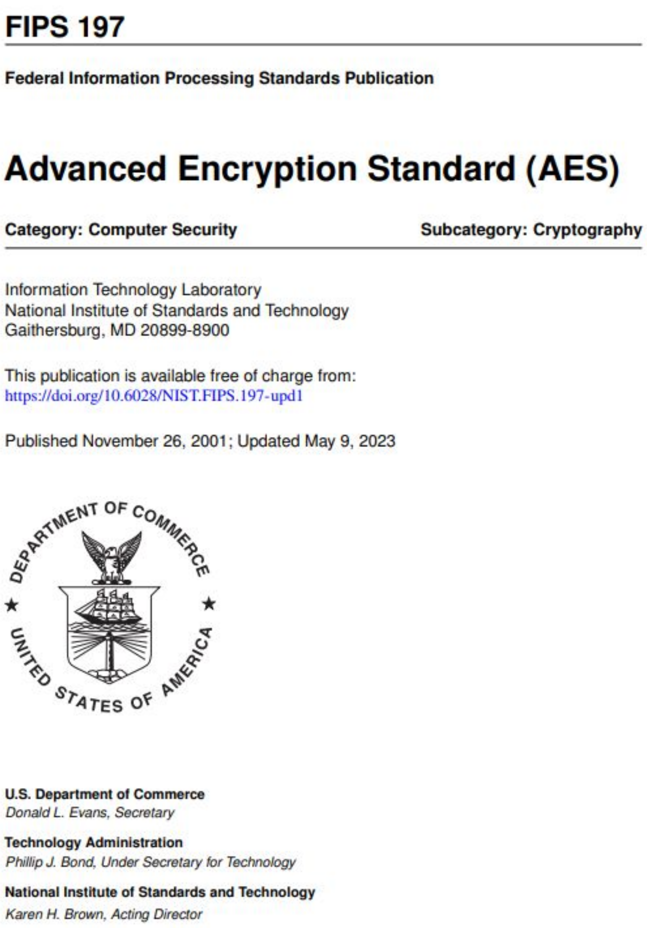
- IoT devices transmit sensitive sensor data over networks
- Lightweight, low-latency encryption is essential for constrained devices
- Software-only encryption is slow and exposes timing side-channels

Problem ?

How to provide real-time, secure sensor telemetry on resource-constrained embedded hardware?

Approach?

- Implement AES-128 encryption as a custom hardware accelerator on FPGA
- Integrate with sensors, networking, and a monitoring application
- Build a complete end-to-end encrypted IoT gateway



FIPS 197

Federal Information Processing Standards Publication

Advanced Encryption Standard (AES)

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

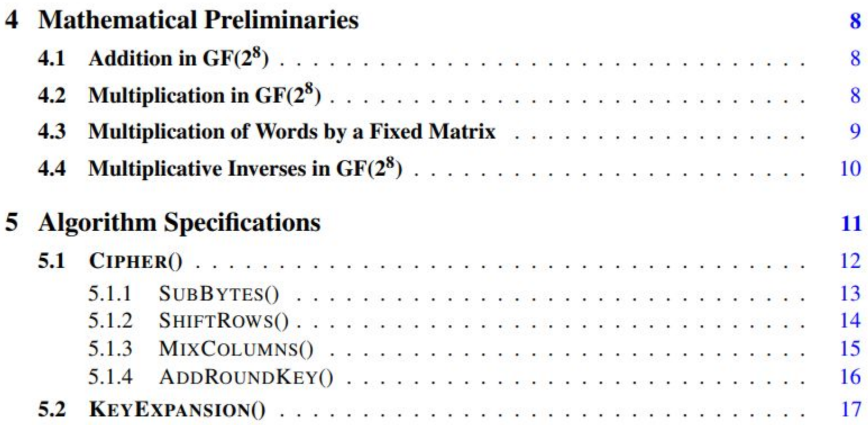
This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.197-upd1

Published November 26, 2001; Updated May 9, 2023

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Karen H. Brown, Acting Director



4 Mathematical Preliminaries 8

4.1 Addition in GF(2^8) 8

4.2 Multiplication in GF(2^8) 8

4.3 Multiplication of Words by a Fixed Matrix 9

4.4 Multiplicative Inverses in GF(2^8) 10

5 Algorithm Specifications 11

5.1 CIPHER() 12

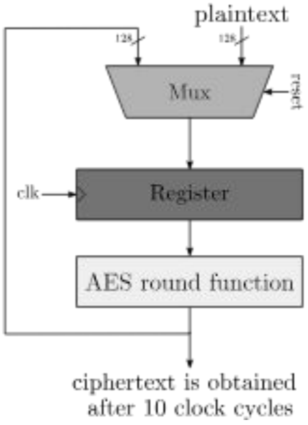
5.1.1 SUBBYTES() 13

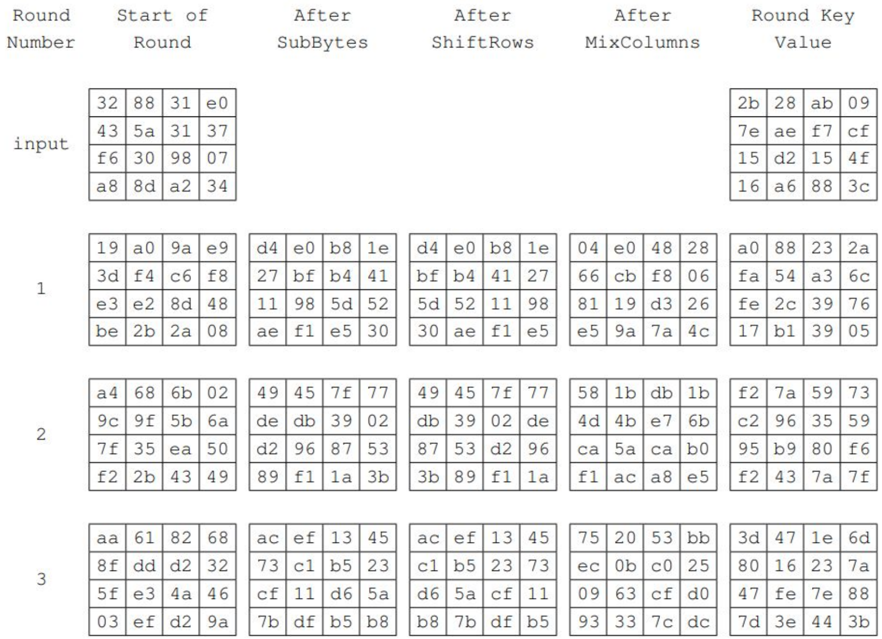
5.1.2 SHIFTROWS() 14

5.1.3 MIXCOLUMNS() 15

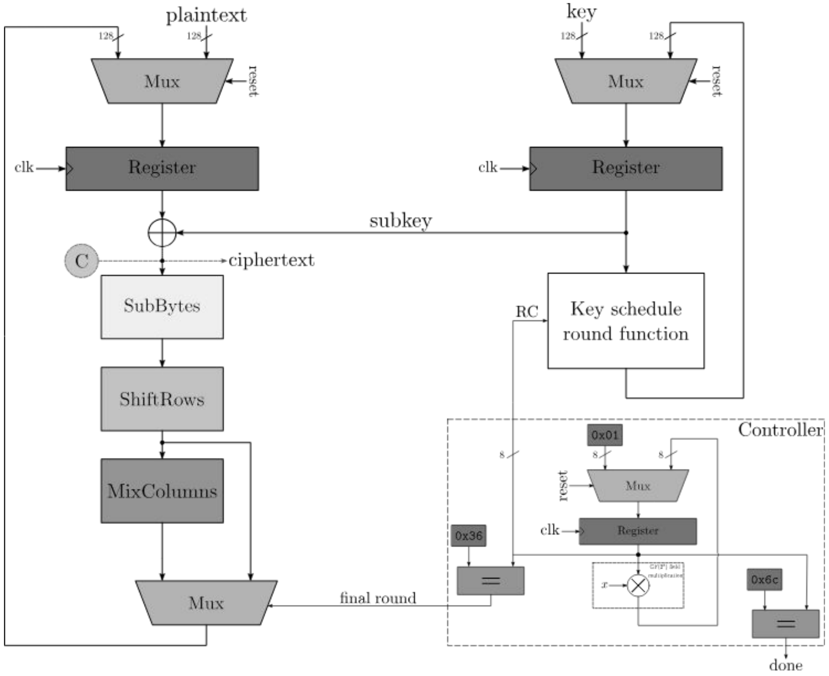
5.1.4 ADDROUNDKEY() 16

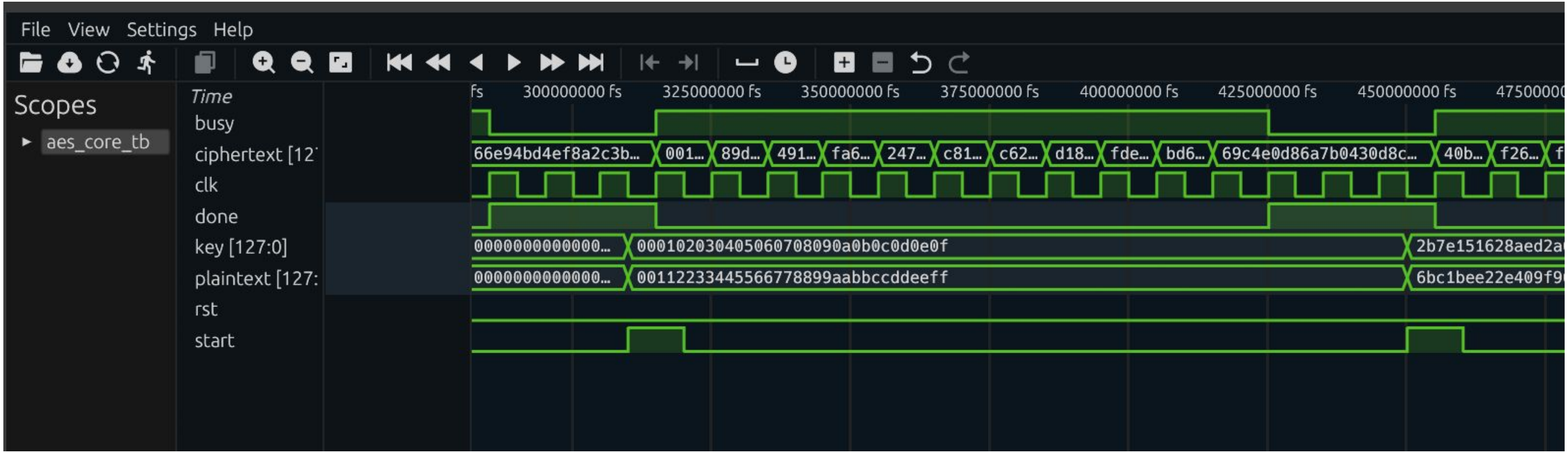
5.2 KEYEXPANSION() 17



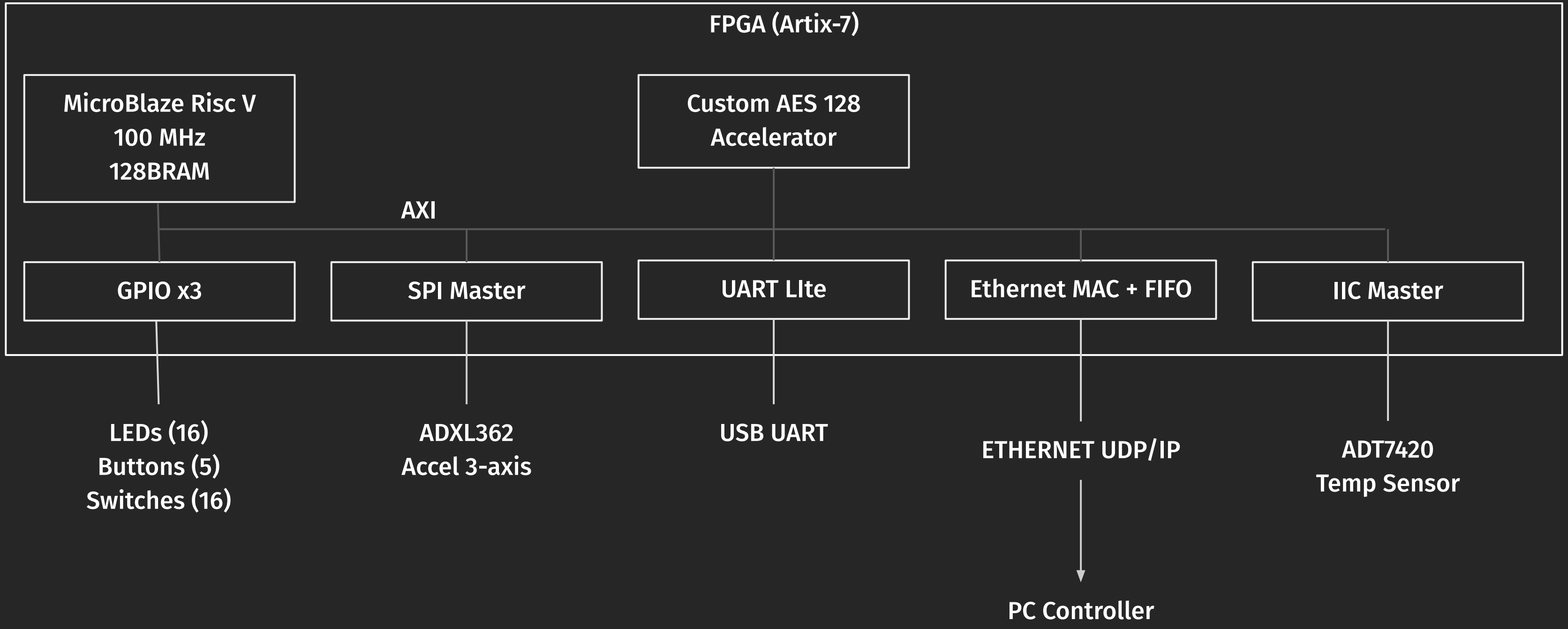


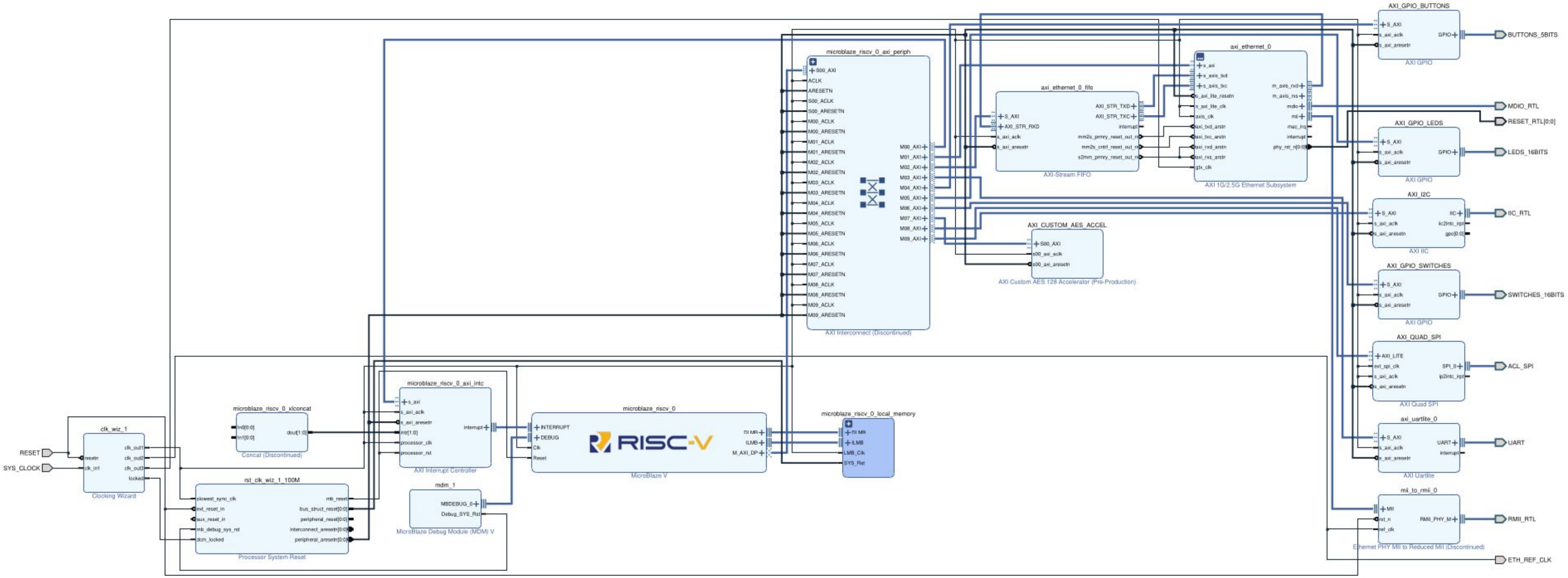
Round Number	Start of Round	After SubBytes	After ShiftRows	After MixColumns	Round Key Value
input	32 88 31 e0 43 5a 31 37 f6 30 98 07 a8 8d a2 34				2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c
1	19 a0 9a e9 3d f4 c6 f8 e3 e2 8d 48 be 2b 2a 08	d4 e0 b8 1e 27 bf b4 41 11 98 5d 52 ae f1 e5 30	d4 e0 b8 1e bf b4 41 27 5d 52 11 98 30 ae f1 e5	04 e0 48 28 66 cb f8 06 81 19 d3 26 e5 9a 7a 4c	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05
2	a4 68 6b 02 9c 9f 5b 6a 7f 35 ea 50 f2 2b 43 49	49 45 7f 77 de db 39 02 d2 96 87 53 89 f1 1a 3b	49 45 7f 77 db 39 02 de 87 53 d2 96 3b 89 f1 1a	58 1b db 1b 4d 4b e7 6b ca 5a ca b0 f1 ac a8 e5	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f
3	aa 61 82 68 8f dd d2 32 5f e3 4a 46 03 ef d2 9a	ac ef 13 45 73 c1 b5 23 cf 11 d6 5a 7b df b5 b8	ac ef 13 45 c1 b5 23 73 d6 5a cf 11 b8 7b df b5	75 20 53 bb ec 0b c0 25 09 63 cf d0 93 33 7c dc	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b



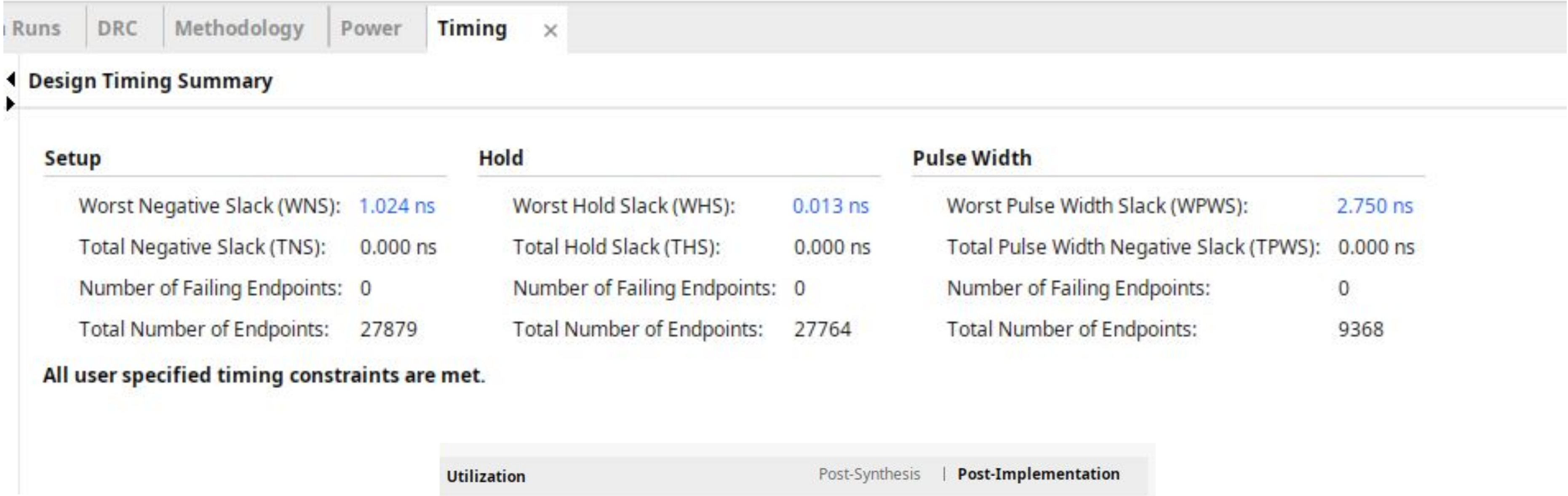

File View Settings Help
Scopes
aes_core_tb
Time
busy
ciphertext [12
clk
done
key [127:0]
plaintext [127:
rst
start
fs
300000000 fs
325000000 fs
350000000 fs
375000000 fs
400000000 fs
425000000 fs
450000000 fs
47500000
66e94bd4ef8a2c3b…
001…
89d…
491…
fa6…
247…
c81…
c62…
d18…
fde…
bd6…
69c4e0d86a7b0430d8c…
40b…
f26…
f
0000000000000…
000102030405060708090a0b0c0d0e0f
2b7e151628aed2a
0000000000000…
00112233445566778899aabbccddeeff
6bc1bee22e409f9

System Architecture





RESET
SYS_CLOCK
clk_wiz_1
resetn
clk_in1
clk_out1
clk_out2
clk_out3
locked
Clocking Wizard
microblaze_riscv_0_xlconcat
In0[0:0]
In1[0:0]
dout[1:0]
Concat (Discontinued)
rst_clk_wiz_1_100M
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
microblaze_riscv_0_axi_intc
s_axi
s_axi_aclk
s_axi_aresetn
intr[1:0]
processor_clk
processor_rst
interrupt
AXI Interrupt Controller
mdm_1
MBDEBUG_0
Debug_SYS_Rst
MicroBlaze Debug Module (MDM) V
microblaze_riscv_0
INTERRUPT
DEBUG
Clk
Reset
RISC-V
DLMB
ILMB
M_AXI_DP
MicroBlaze V
microblaze_riscv_0_local_memory
DLMB
ILMB
LMB_Clk
SYS_Rst
microblaze_riscv_0_axi_periph
S00_AXI
ACLK
ARESETN
S00_ACLK
S00_ARESETN
M00_ACLK
M00_ARESETN
M01_ACLK
M01_ARESETN
M02_ACLK
M02_ARESETN
M03_ACLK
M03_ARESETN
M04_ACLK
M04_ARESETN
M05_ACLK
M05_ARESETN
M06_ACLK
M06_ARESETN
M07_ACLK
M07_ARESETN
M08_ACLK
M08_ARESETN
M09_ACLK
M09_ARESETN
M00_AXI
M01_AXI
M02_AXI
M03_AXI
M04_AXI
M05_AXI
M06_AXI
M07_AXI
M08_AXI
M09_AXI
AXI Interconnect (Discontinued)
axi_ethernet_0_fifo
S_AXI
AXI_STR_RXD
s_axi_aclk
s_axi_aresetn
AXI_STR_TXD
AXI_STR_TXC
interrupt
mm2s_prmry_reset_out_n
mm2s_cntrl_reset_out_n
s2mm_prmry_reset_out_n
AXI-Stream FIFO
axi_ethernet_0
s_axi
s_axis_txd
s_axis_txc
s_axi_lite_resetn
s_axi_lite_clk
axis_clk
axi_txd_arstn
axi_txc_arstn
axi_rxd_arstn
axi_rxs_arstn
gtx_clk
m_axis_rxd
m_axis_rxs
mdio
mii
mac_irq
interrupt
phy_rst_n[0:0]
AXI 1G/2.5G Ethernet Subsystem
AXI_CUSTOM_AES_ACCEL
S00_AXI
s00_axi_aclk
s00_axi_aresetn
AXI Custom AES 128 Accelerator (Pre-Production)
AXI_GPIO_BUTTONS
S_AXI
s_axi_aclk
s_axi_aresetn
GPIO
AXI GPIO
BUTTONS_5BITS
MDIO_RTL
RESET_RTL[0:0]
AXI_GPIO_LEDS
S_AXI
s_axi_aclk
s_axi_aresetn
GPIO
AXI GPIO
LEDS_16BITS
AXI_I2C
S_AXI
s_axi_aclk
s_axi_aresetn
IIC
iic2intc_irpt
gpo[0:0]
AXI IIC
IIC_RTL
AXI_GPIO_SWITCHES
S_AXI
s_axi_aclk
s_axi_aresetn
GPIO
AXI GPIO
SWITCHES_16BITS
AXI_QUAD_SPI
AXI_LITE
ext_spi_clk
s_axi_aclk
s_axi_aresetn
SPI_0
ip2intc_irpt
AXI Quad SPI
ACL_SPI
axi_uartlite_0
S_AXI
s_axi_aclk
s_axi_aresetn
UART
interrupt
AXI Uartlite
UART
mii_to_rmii_0
MII
rst_n
ref_clk
RMII_PHY_M
Ethernet PHY MII to Reduced MII (Discontinued)
RMII_RTL
ETH_REF_CLK



Design Timing Summary

Setup

Worst Negative Slack (WNS): 1.024 ns

Total Negative Slack (TNS): 0.000 ns

Number of Failing Endpoints: 0

Total Number of Endpoints: 27879

Hold

Worst Hold Slack (WHS): 0.013 ns

Total Hold Slack (THS): 0.000 ns

Number of Failing Endpoints: 0

Total Number of Endpoints: 27764

Pulse Width

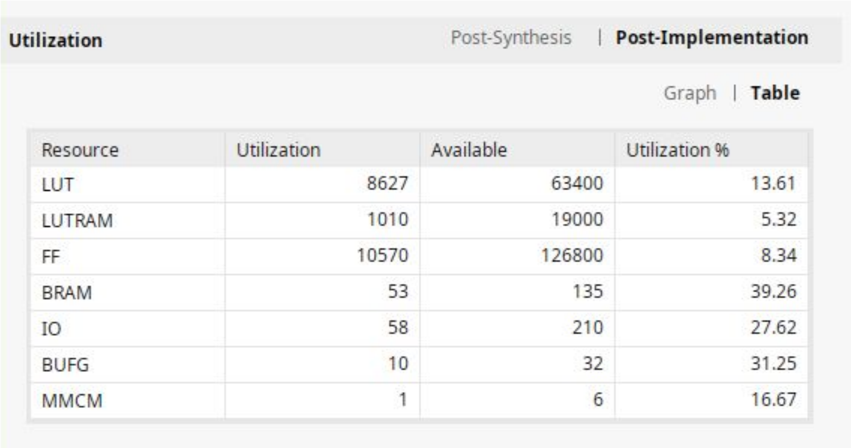
Worst Pulse Width Slack (WPWS): 2.750 ns

Total Pulse Width Negative Slack (TPWS): 0.000 ns

Number of Failing Endpoints: 0

Total Number of Endpoints: 9368

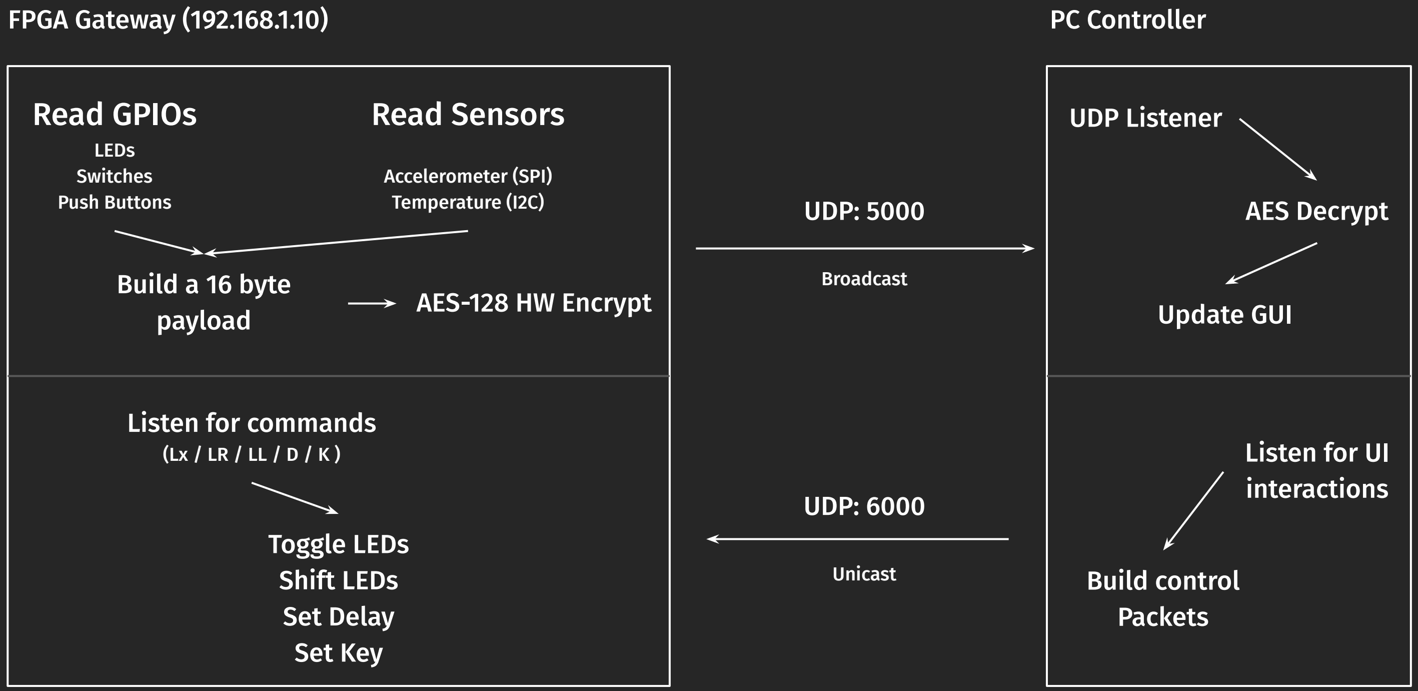
All user specified timing constraints are met.



Utilization

Resource	Utilization	Available	Utilization %
LUT	8627	63400	13.61
LUTRAM	1010	19000	5.32
FF	10570	126800	8.34
BRAM	53	135	39.26
IO	58	210	27.62
BUFG	10	32	31.25
MMCM	1	6	16.67

Data Flow



FPGA Gateway (192.168.1.10)

Read GPIOs

LEDs
Switches
Push Buttons

Read Sensors

Accelerometer (SPI)
Temperature (I2C)

Build a 16 byte payload

AES-128 HW Encrypt

Listen for commands
(Lx / LR / LL / D / K)

Toggle LEDs
Shift LEDs
Set Delay
Set Key

UDP: 5000

Broadcast

UDP: 6000

Unicast

PC Controller

UDP Listener

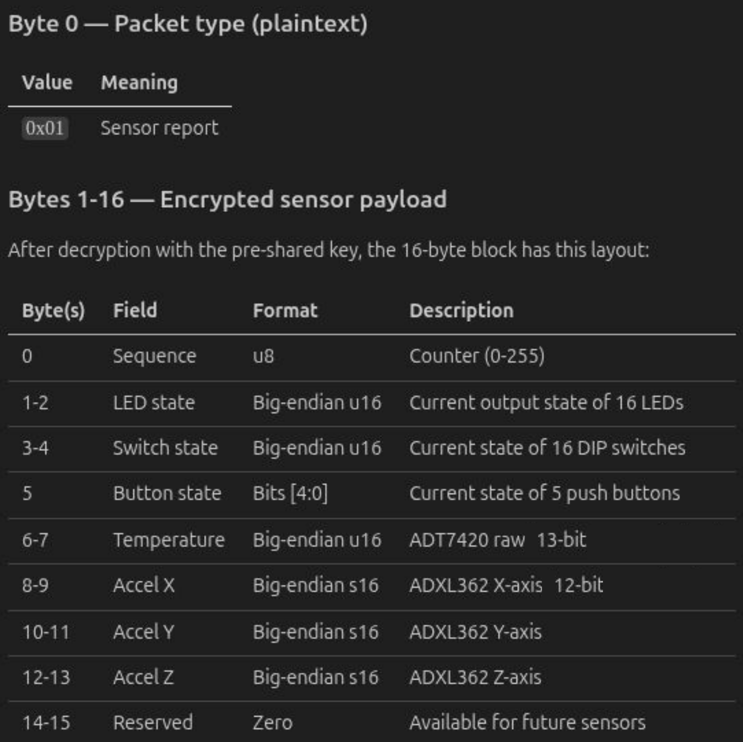
AES Decrypt

Update GUI

Listen for UI interactions

Build control Packets

Packet Format



Byte 0 — Packet type (plaintext)

Value	Meaning
0x01	Sensor report

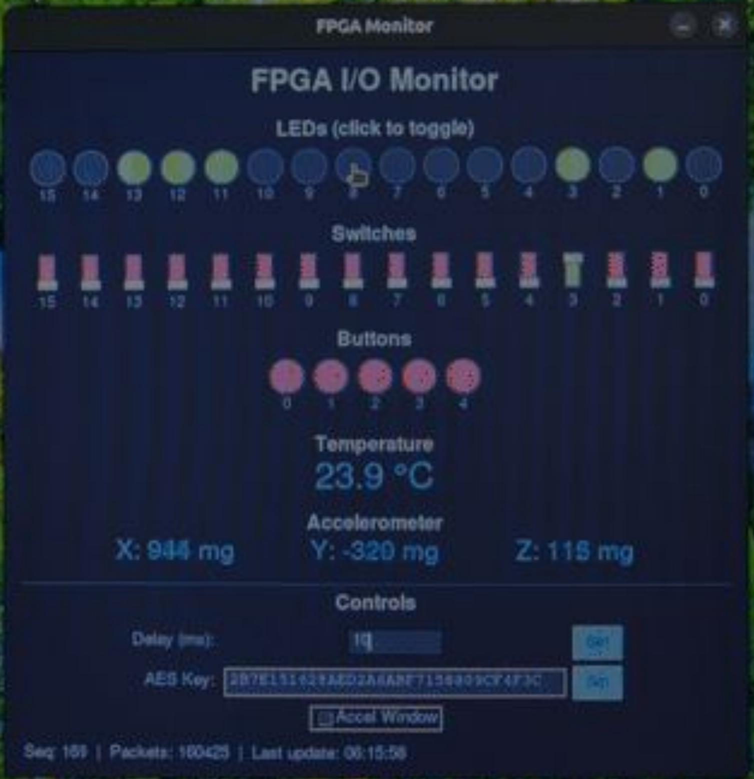
Bytes 1-16 — Encrypted sensor payload

After decryption with the pre-shared key, the 16-byte block has this layout:

Byte(s)	Field	Format	Description
0	Sequence	u8	Counter (0-255)
1-2	LED state	Big-endian u16	Current output state of 16 LEDs
3-4	Switch state	Big-endian u16	Current state of 16 DIP switches
5	Button state	Bits [4:0]	Current state of 5 push buttons
6-7	Temperature	Big-endian u16	ADT7420 raw 13-bit
8-9	Accel X	Big-endian s16	ADXL362 X-axis 12-bit
10-11	Accel Y	Big-endian s16	ADXL362 Y-axis
12-13	Accel Z	Big-endian s16	ADXL362 Z-axis
14-15	Reserved	Zero	Available for future sensors

DEMO

Lets see it in action!



FPGA I/O Monitor

LEDs (click to toggle)

Switches

Buttons

Temperature

23.9 °C

Accelerometer

X: 944 mg Y: -320 mg Z: 115 mg

Controls

Delay (ms): 10 Set

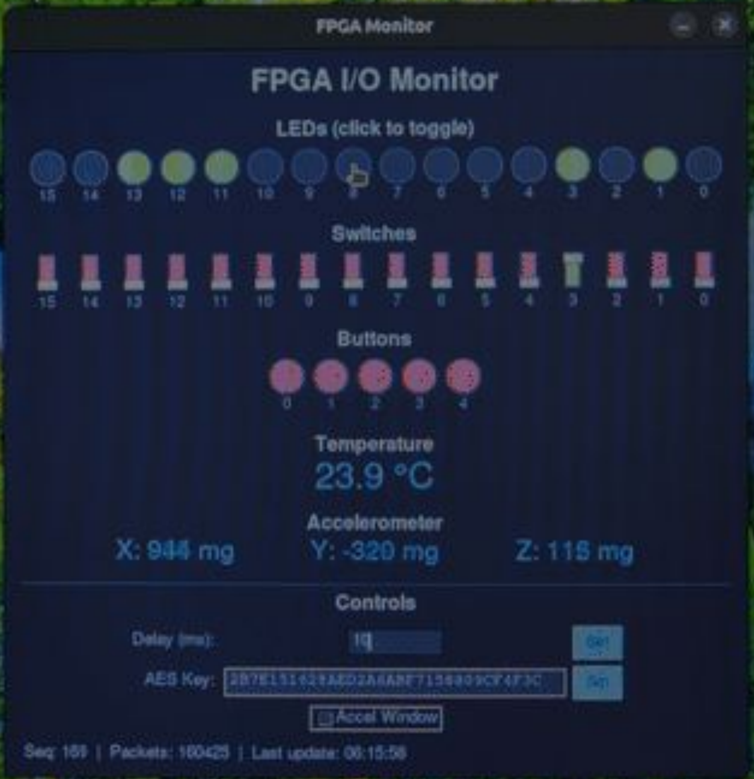
AES Key: 2B7E151628AED2A6ABF7158809CF4F3C Set

□ Accel Window

Seq: 169 | Packets: 160425 | Last update: 06:15:58

universidade de aveiro
deti departamento de eletrónica, telecomunicações e informática

Final Remarks



23.9 °C

X: 944 mg Y: -320 mg Z: 115 mg

Delay (ms): 10

AES Key: 2B7E151628AED2A6ABF7158809CF4F3C

□ Accel Window

Seq: 169 | Packets: 160425 | Last update: 06:15:58

universidade de aveiro
deti departamento de eletrónica, telecomunicações e informática