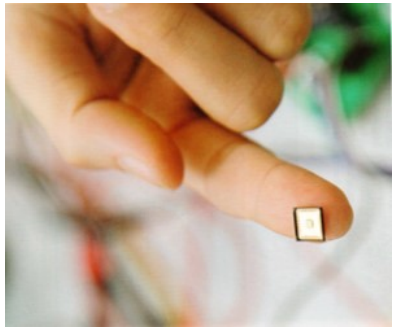
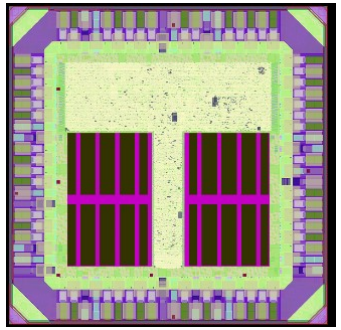
VIETNAM NATIONAL UNIVERSITY HANOI
INFORMATION TECHNOLOGY INSTITUTE

ADEN4IOT: A RISC-V based System-on-Chip platform for Internet-of-Things Applications





Xuan-Tu Tran & Duy-Hieu Bui
Laboratory for Smart Integrated Systems (SISLAB)
VNU Information Technology Institute

Contents

- Introduction to VNU Information Technology Institute
- Internet of Things & security challenges
- RISC-V & Opensource Ecosystem
- ADEN4IoT: an ULP sensor node for IoT
- Conclusions

Contents

- Introduction to VNU Information Technology Institute
- Internet of Things & security challenges
- RISC-V & Opensource Ecosystem
- ADEN4IoT: an ULP sensor node for IoT
- Conclusions

Hardware Design working group

- 10 members: 06 staffs; 04 students
- Research interests
  - Hardware security & security hardware
  - Domain specific accelerator: AI, Image & Video processing
  - RISC-V & Opensource ecosystems
  - Analog & mixed signal
  - HW/SW co-design

Xuan-Tu Tran
Prof.

Bui Duy Hieu
PhD

Manh-Hiep Dao, PhD student
Lightweight ECC for RFID

Hai-Ninh Dang
PCB & Embedded system

Ngo-Doanh Nguyen
System design & IP integration

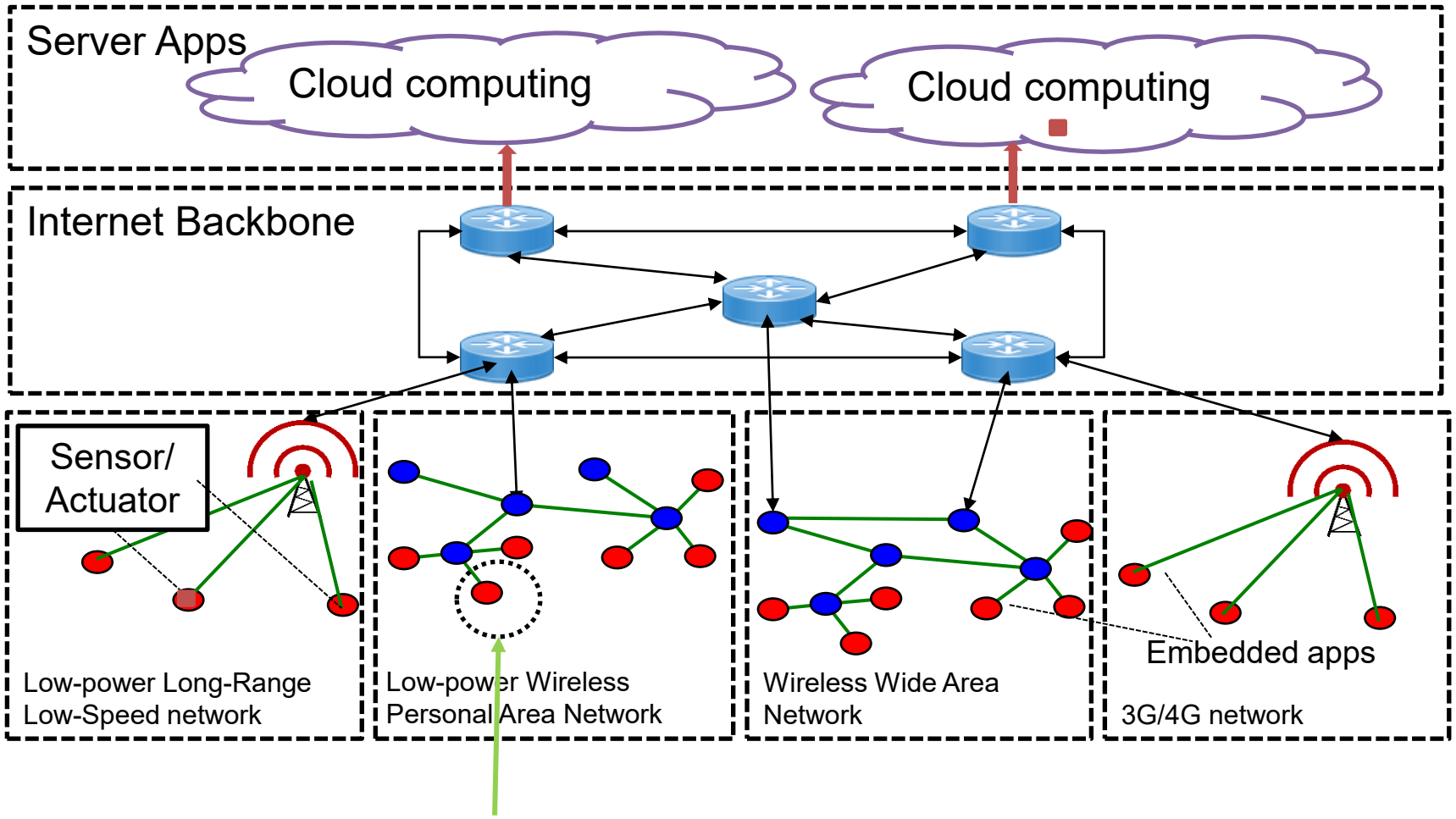
Duc-Manh Tran
Analog-mixed signal

The-Anh Nguyen
Undergraduate
Analog-mixed signal

Contents

- Introduction to VNU Information Technology Institute
- Internet of Things & security challenges
- RISC-V & Opensource Ecosystem
- ADEN4IoT: an ULP sensor node for IoT
- Conclusions

IoT organization



Ultra-low-power, ultra-low-cost constrained devices or edge devices

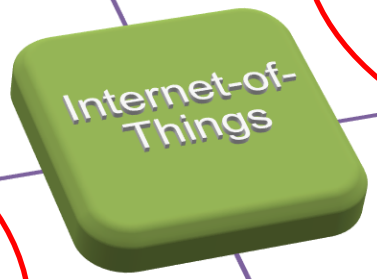
Key research issues related to IoT

Open-source ecosystem

Different IoT workloads

- **Sensor nodes**
- **Edge/gateway devices**
- **On-demand/configurability**

- Saving battery !
- Always a big challenge in LSI design

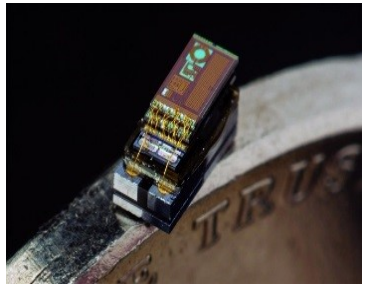


Sensitive data in storage/transmission

Application separations

More intelligent & smarter edge devices

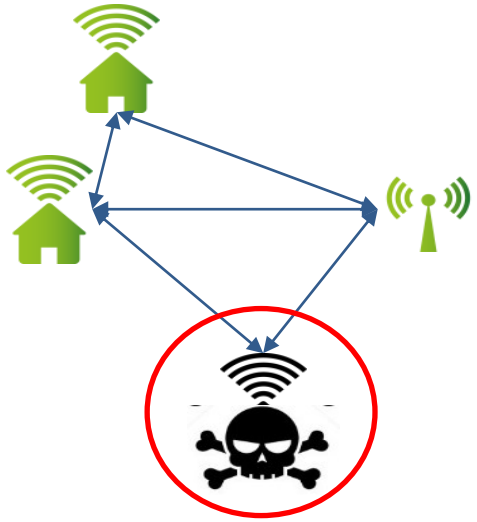
IoT raises security & privacy problems



M³ - Michigan Micro-Mote: 1 mm³

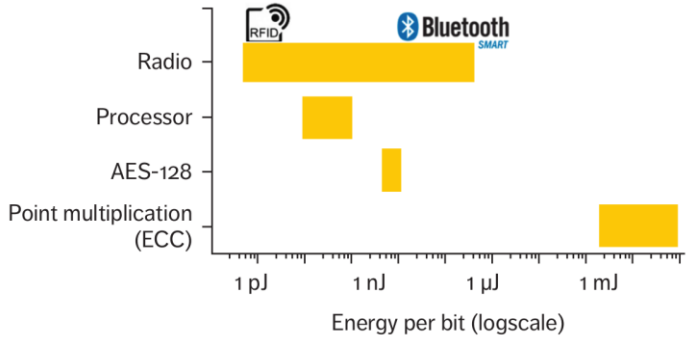
Constrained devices

- Small memory
- Limited processing
- Ultra low power
- Long-lifetime new *attacks & standards*



Information security & privacy issues

- Personal data exposed through IoT devices & networks
- New attack surfaces created



Strong cryptography algorithms required

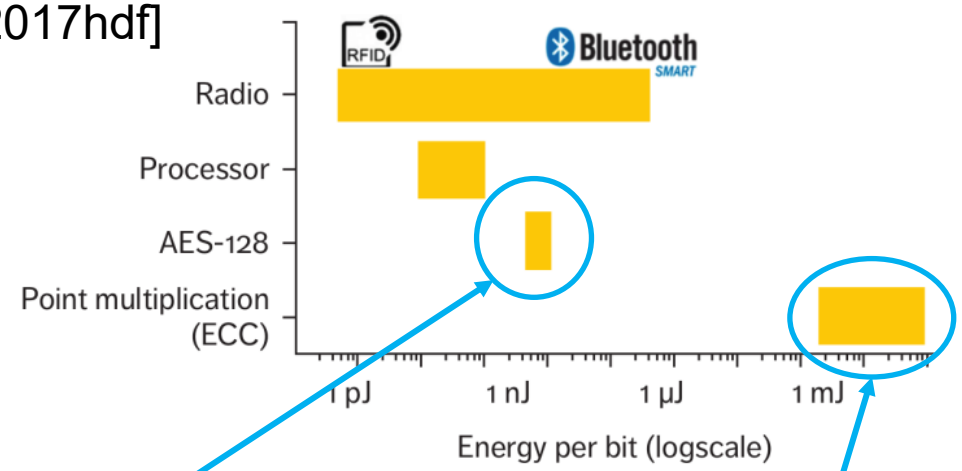
- Complicated computation
- High power
- System throughput

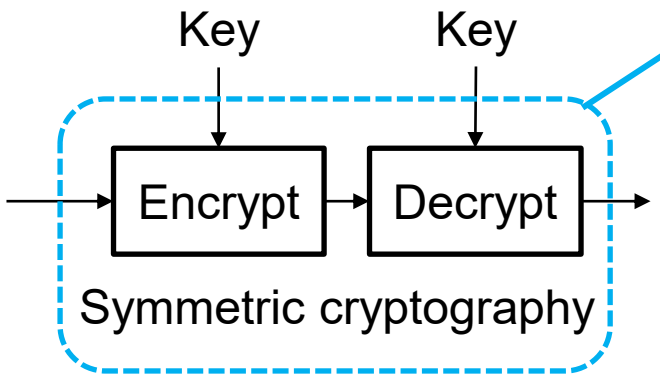
⇨ Designing an ultra-low-power IC with security features for IoT

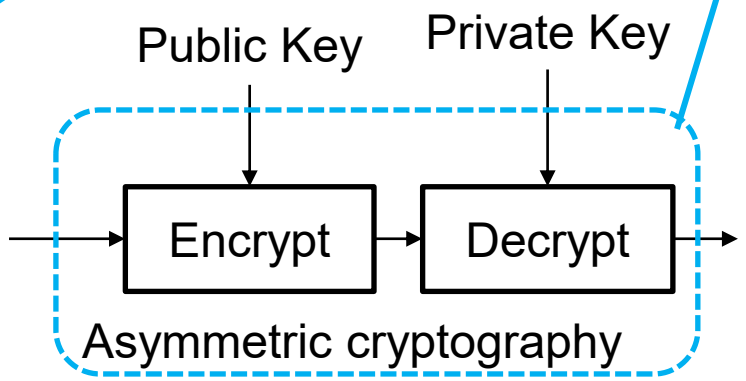
Security Requirements

- Data protection
- Data integrity
- Authentication/Identification
- Communication protection
- Firmware/Software protection
- Availability

[Yang2017hdf]







⇒ Symmetric cryptography provides low-cost and low-power primitives to support these requirements

Contents

- Introduction to VNU Information Technology Institute
- Internet of Things & security challenges
- RISC-V & Opensource Ecosystem
- ADEN4IoT: an ULP sensor node for IoT
- Conclusions

RISC-V Ecosystem

A booming community!

- Many RISC-V cores/SoCs available
  - 111 RISC-V cores (>40% open-source license)
  - 31 SoC Platforms (>80% open-source license)
  - 12 SoCs
- RISC-V Ecosystem: active development
  - Compiler: GCC, LLVM
  - Simulator: Validator, Firesim (FPGA)
  - Configurable IPs: SHA-3, testchip IPs
  - Interconnect: AXI4, Tilelink
  - Google Open MPW and Open-source Skywater 130nm PDK pushes the HW development (with RISC-V) further

⇒ New opportunities for Vietnamese researchers to contribute to these projects

Opensource HW: a new opportunities

- Open source hardware is maturing

CHIPYARD

SiFive

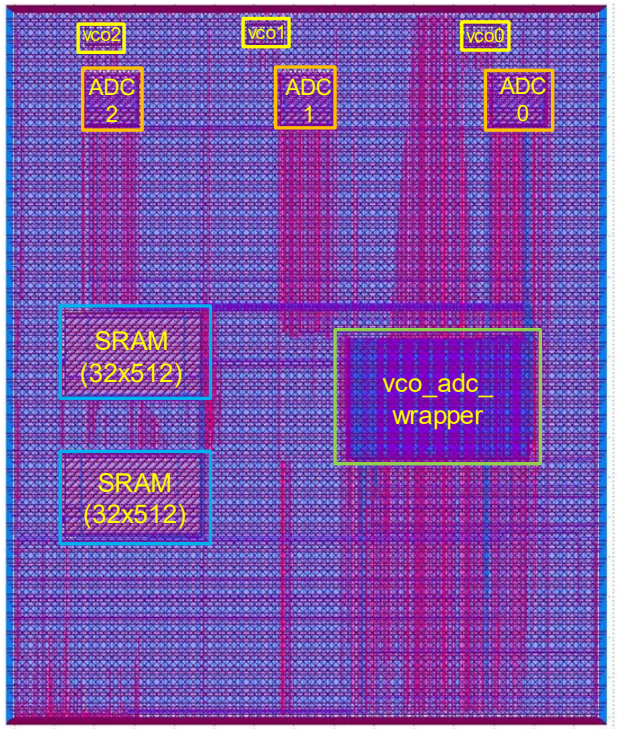
Pulp-platform

HEX-Five Security

Keystone

Google + skywater TECHNOLOGY

FOSS 130nm Production PDK
github.com/google/skywater-pdk



- New opportunities

Low power

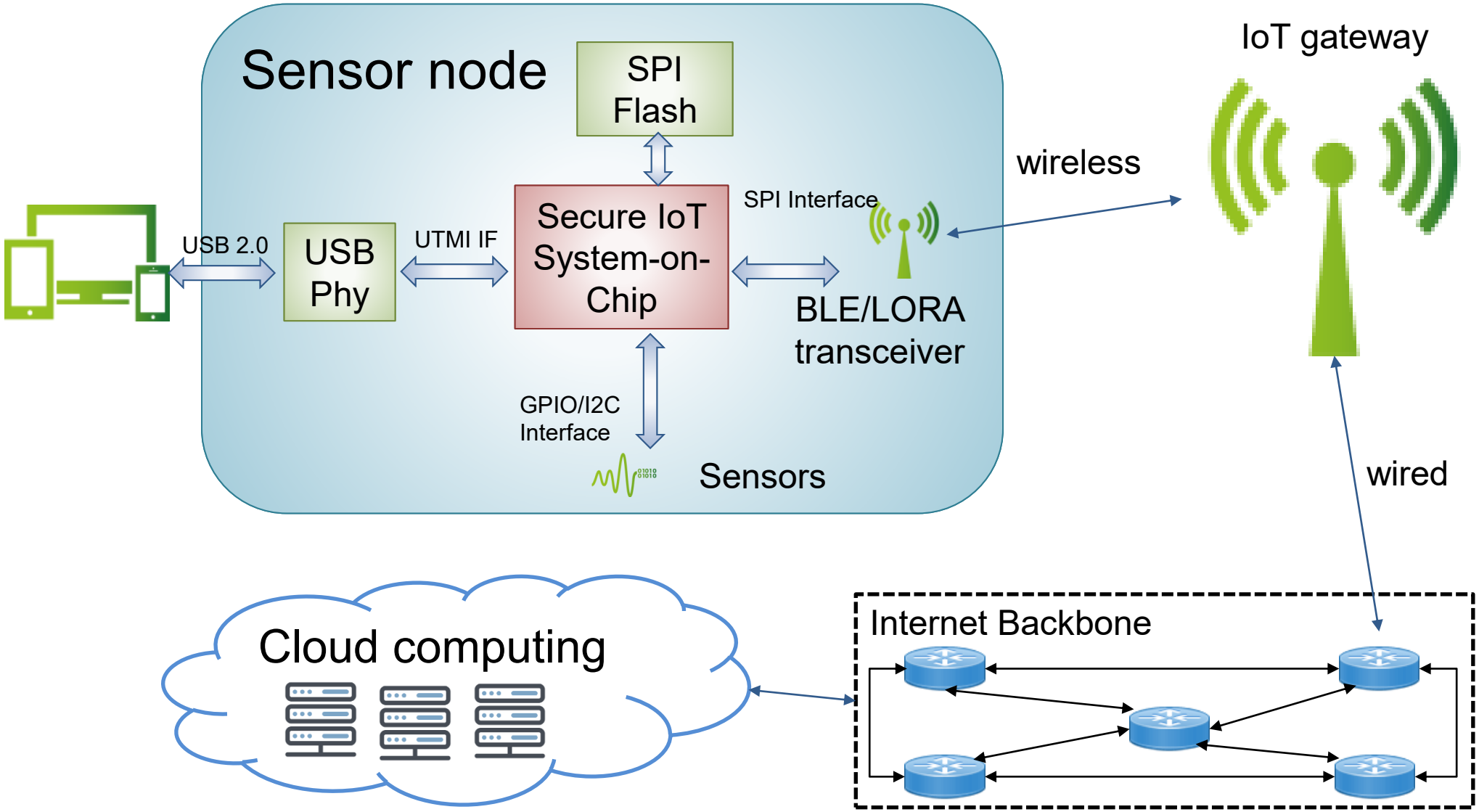
Security

High performance (5G, AI)

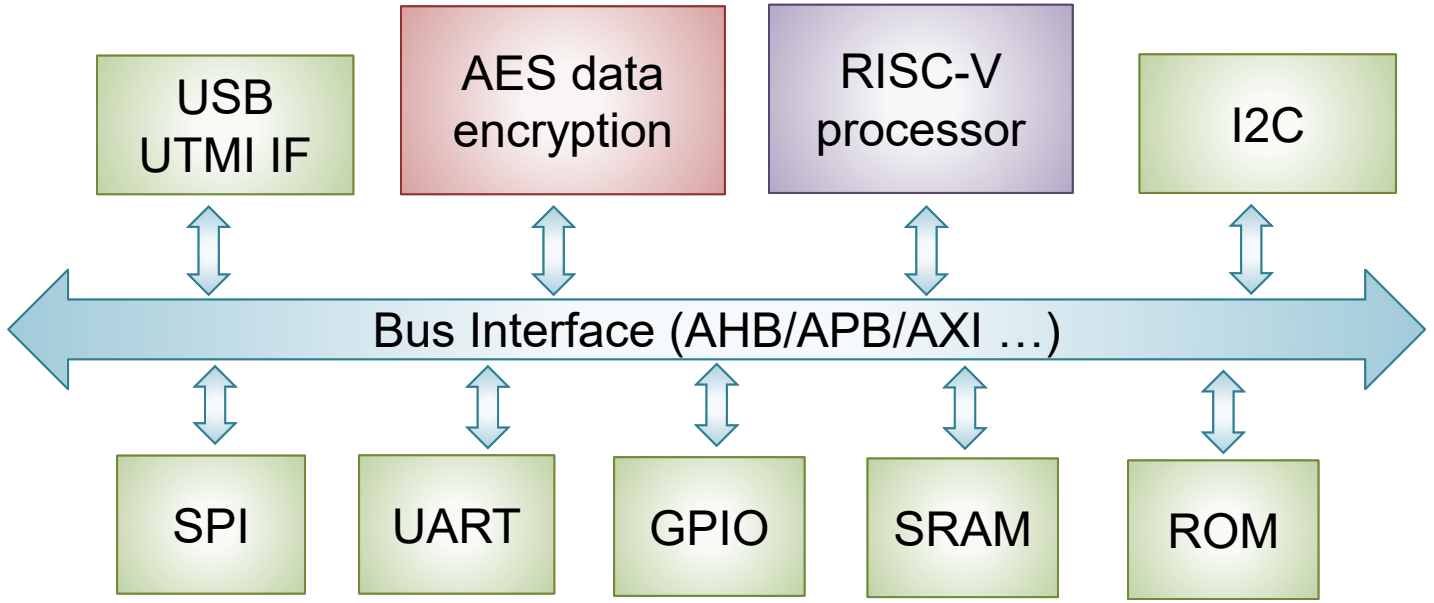
Contents

- Introduction to VNU Information Technology Institute
- Internet of Things & security challenges
- RISC-V & Opensource Ecosystem
- ADEN4IoT: an ULP sensor node for IoT
- Conclusions

ADEN4IOT: Low power sensor nodes



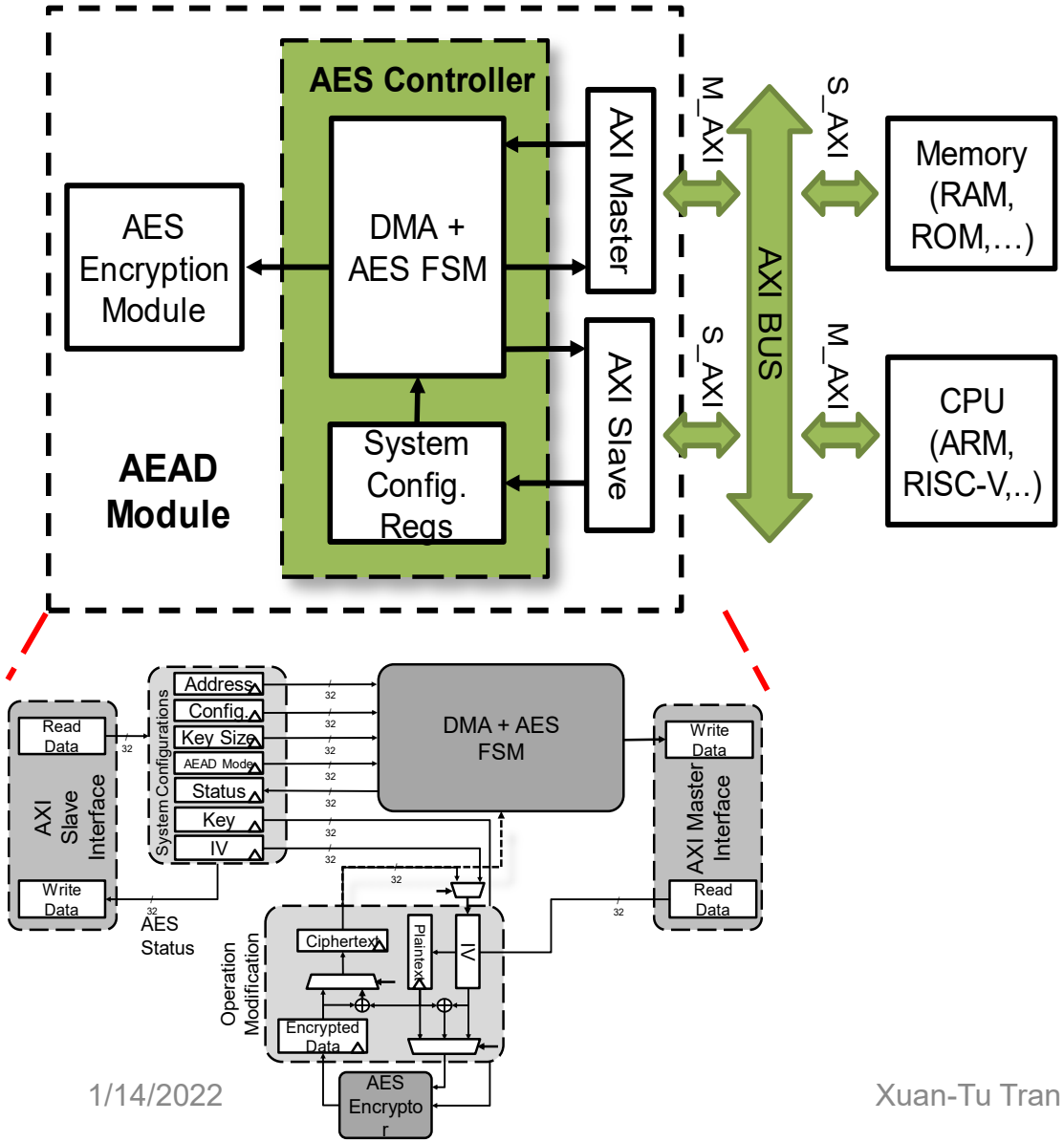
Integrated IoT systems with security features



- Authenticated Encryption with Associated Data (AEAD) using AES
- Low power RISC-V core for configuration, control and data aquasition
- Communication interface: SPI, UART, I2C, GPIO

⇒ System-on-chip based on RISC-V for Ultra-Low-Power consumption

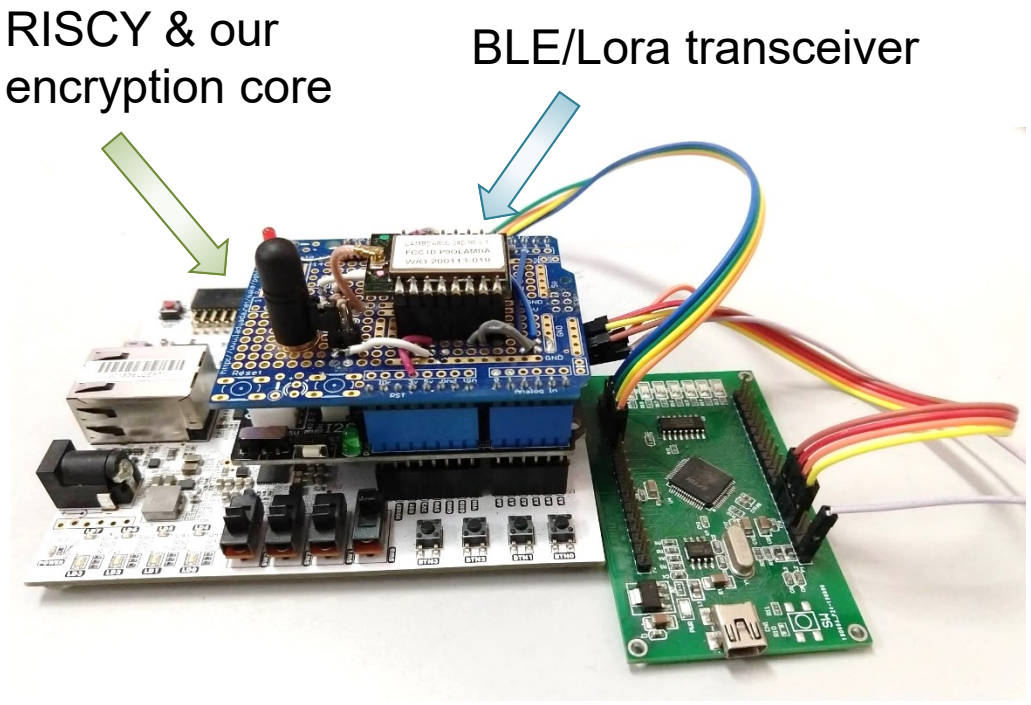
Our proposed Lightweight AEAD Encryption Module



- AXI4 interface
  - Slave: configurations
  - Master: Ligthtweight Direct Memory Access
- Low-power AES architecture
  - 32-bit datapath
  - Power Optimization in S-box, datapath, controls
  - Key size: 128-bit, 192-bit, 256-bit
- AEAD modes
  - HW/SW co-design to reduce HW area

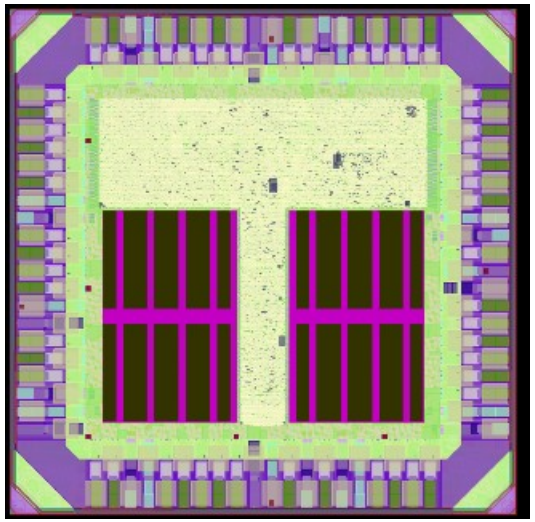
ADEN4IOT prototype

- Processor: RISCY (Pulp-platform)
- Default clock: 25MHz
- SISLAB IPs through AXI4 bus



FPGA Prototype for early software development

- AES core + Interface: ~23kGEs
- Enc. Throughput: 123Mbps@60MHz
- Enc. Power: 0.7mW@60MHz
- Full chip: 17mW @60MHz
  - 10mW without IO cells

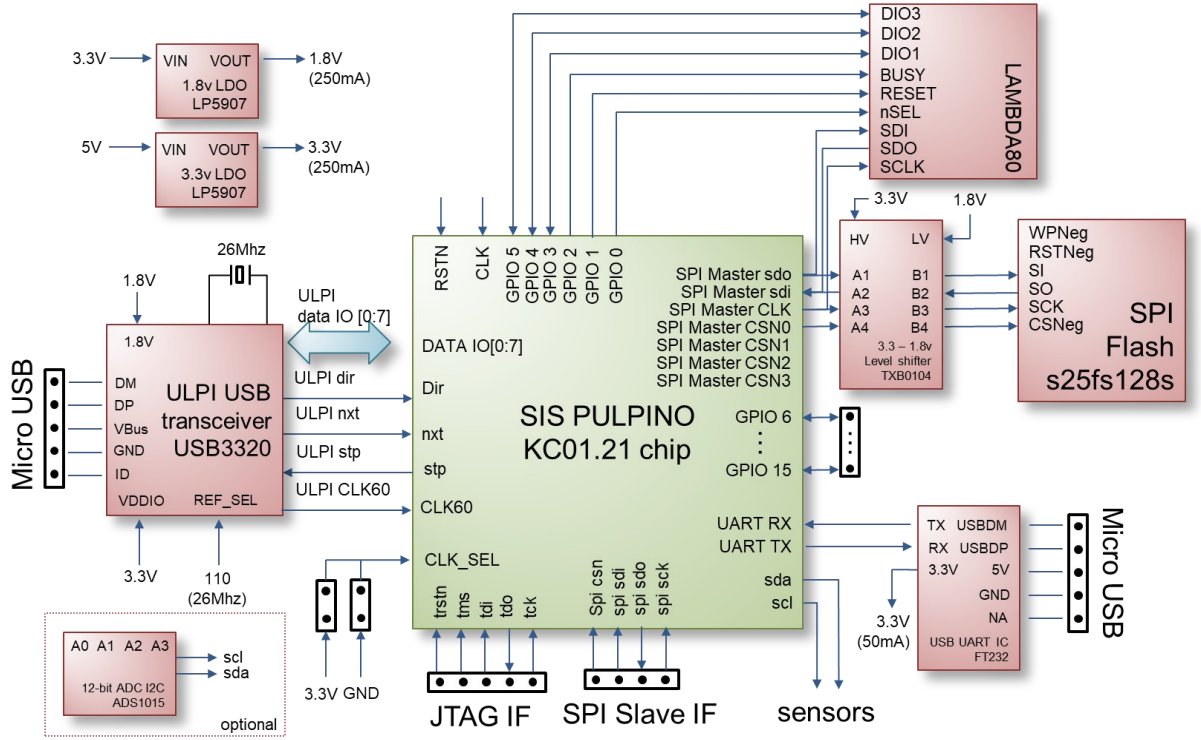


ASIC prototype on TSMC 65nm

Nguyen *et al.*, "A Lightweight AEAD Encryption core to secure IoT applications, APCCAS'20.

Sensor nodes

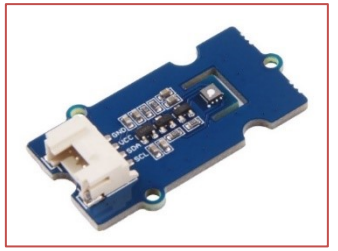
- Power-supply: 3.3V-5.0V
- Operating Frequency: 10-60MHz
- SPI Flash to store SW programs
- BLE/Lora transceiver
- Sensors:
  - Air Quality (PM2.5)
  - CO, H_2, NH_3, CH_4
  - pH,
  - Temperature



PM2.5 Air Quality Sensor

CO, H2, NH3, CH4 sensor

PH Sensor



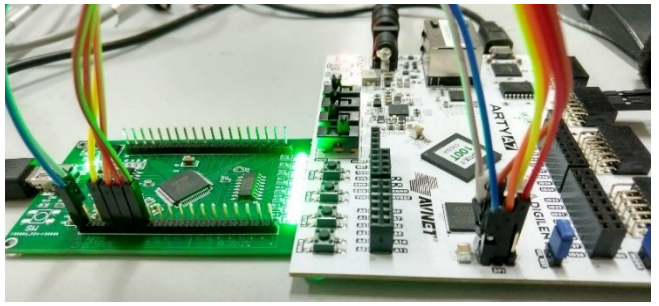
Temperature & Humidity Sensor

SW Programming environment

- Embedded SW programming
  - Compiler: GCC
  - Arduino compatible
  - SPI Interface for Debugging
- Libraries
  - AES & AEAD encryption
  - BLE/Lora for SX1280 transceiver
  - Sensors
- Software Development Kit
  - Arduino
  - Platform IO
- Cloud platform
  - Node-RED

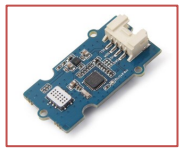
GCC

GDB
The GNU Project Debugger



FTDI 2232 Mini

SX1280 (Lambda80)



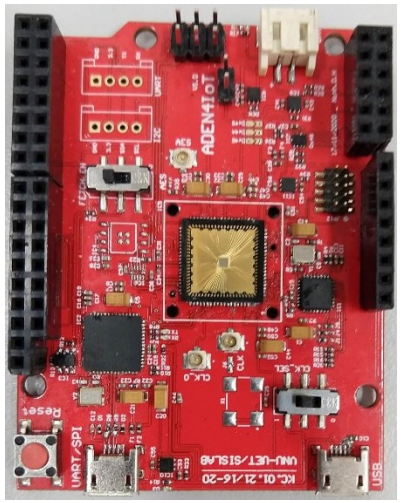
PlatformIO

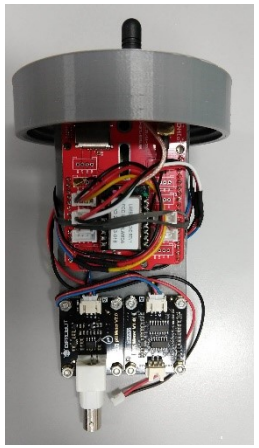
ARDUINO

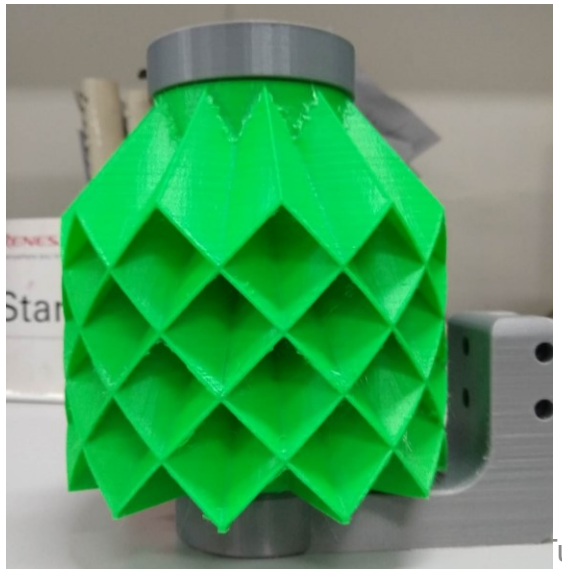
Node-RED

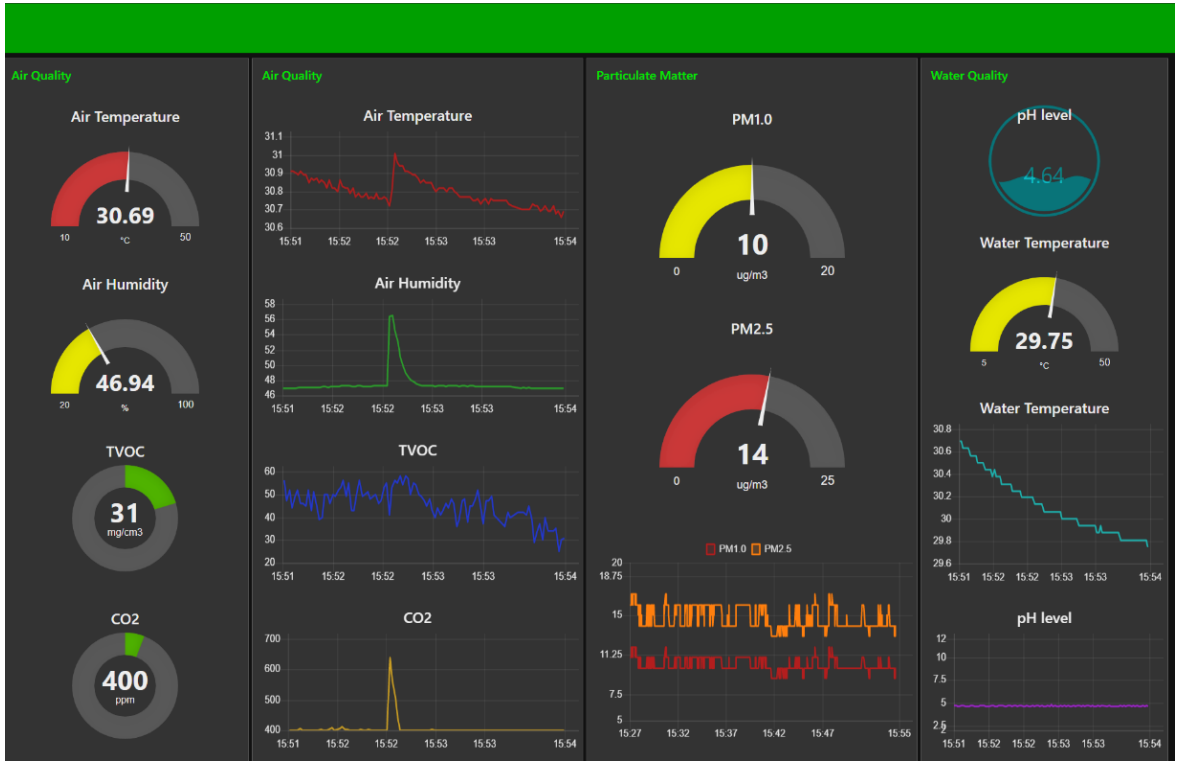
Demo apps: environment monitoring

Devices with sensors (version 1.0)









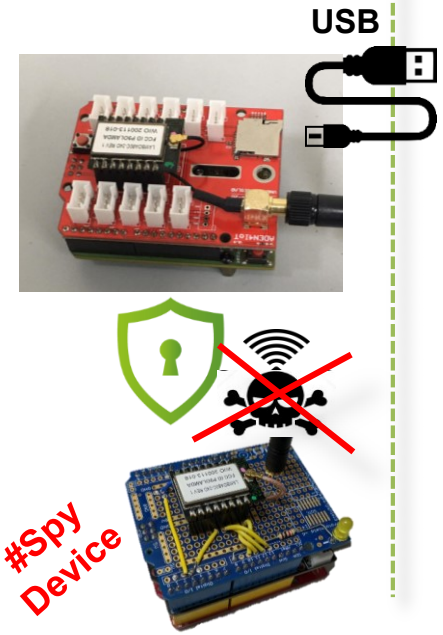
- Chip's Active power: 17mW
- Full system power consumption: 40mA@3.7V

=> Further optimization (on-going)

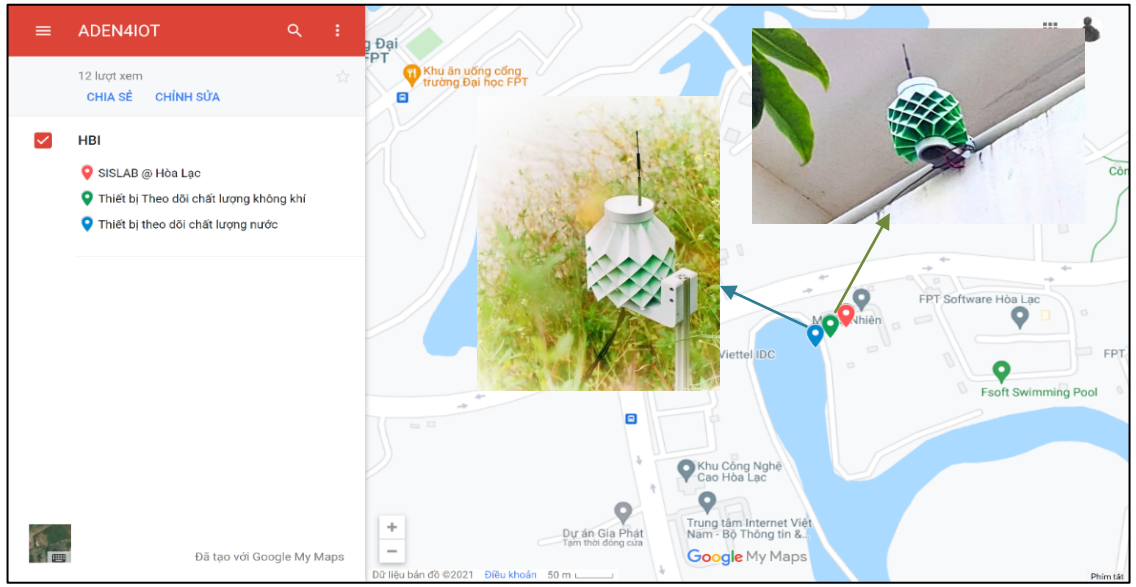
Real Demonstration in Hoa Lac Hi-tech Park

Slave sensor-node

Master sensor-node



Application gateway



Contents

- Introduction to VNU Information Technology Institute
- Internet of Things & security challenges
- RISC-V & Opensource Ecosystem
- ADEN4IoT: an ULP sensor node for IoT
- Conclusions

Conclusions

- New challenges and opportunities for developing processors, HW for security & low-power solutions for Internet of Things
- ADEN4IoT – a platform for securing IoT applications built from Open-Source HW/SW ecosystem
  - Our proposed low-power AES cores
  - A lightweight DMA interface to accelerate AES encryption
  - HW/SW co-design for AEAD modes
  - A single RISC-V CV32E40P processor
  - SW development environments & libraries for data encryption, communication & sensors

Thank you for your attention!

Xuan-Tu Tran & Duy-Hieu Bui

Laboratory for Smart Integrated Systems (SISLAB)

VNU Information Technology Institute (VNU-ITI)

Website: http://iti.vnu.edu.vn