Hardware for Secure Autonomy

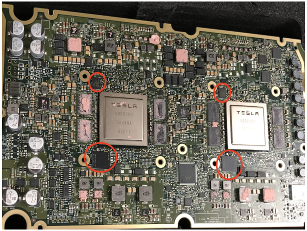
Md Tanvir Arafin

May 31, 2023

The C4I and Cyber Center
George Mason University
Fairfax, VA

Hardware Security & Autonomous Systems

Smart Yet Vulnerable Hardware



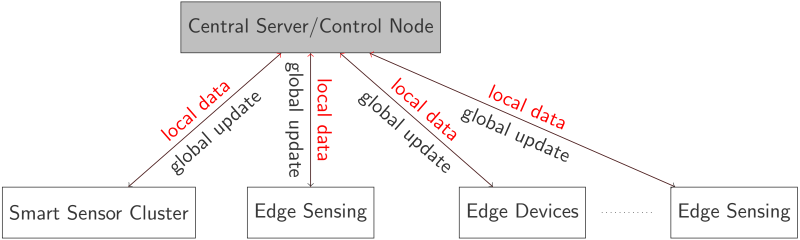
Subaru Cockpit [Image https://www.subaru.com/vehicles/outback/gallery.html]

Tesla Cockpit [Image https://www.tesla.com/tesla-gallery, Courtesy of Tesla, Inc.]

Autonomous Systems

Key Idea

Intelligent machines sense, plan, and act in a changing environment



Questions

How to verify data or processes at the edge?

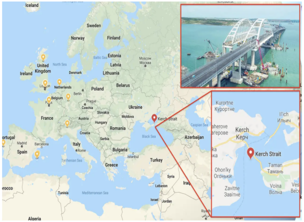
How to accelerate cryptography computation?

How to enable secure data aggregation and distributed learning?

Secure Sensing and Fusion at the Physical Layer

Global Positioning System (GPS) Spoofing: Evidence

Crimea, 2021



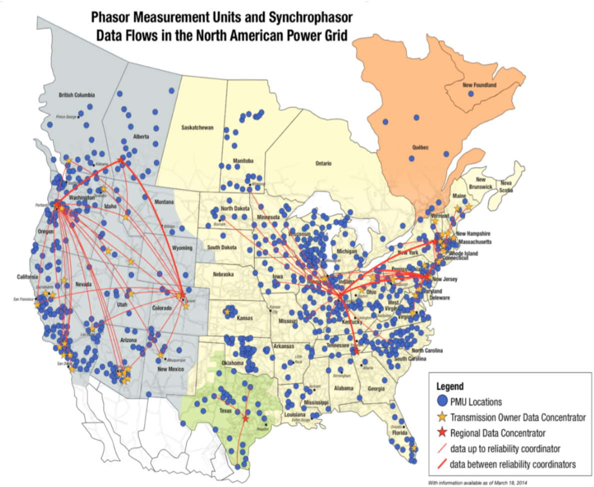
Pokemon GO, 2016

White Rose, 2013

Lockheed RQ-170, 2013

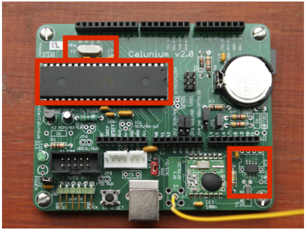
Russia spoofed AIS data. Source://www.theregister.com/2021/06/24/russia_ais_spoofing/

Synchronization in Smart Grid



Source: North American SynchroPhasor Initiative

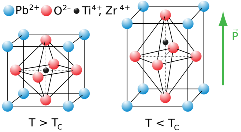
Crystal Oscillators



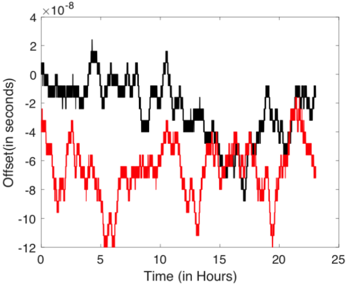
- Ubiquitous

  Piezo-electric quartz crystal

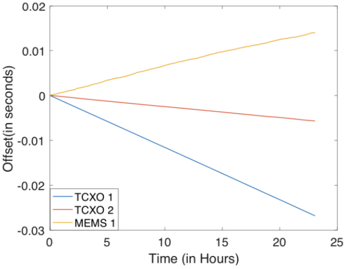
- Intrinsically Unclonable
  - Imperfect cutting
  - Cutting variations
  - Physically unclonable time offset
- Reliable Correct timing with temperature variation



Fault in Our Clocks



Clock offset between two GPS clocks

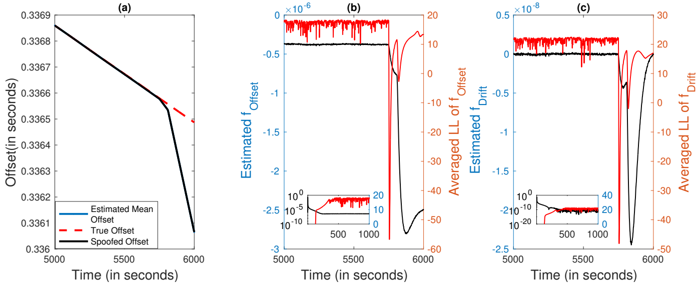


Clock offset for TCXO and MEMS clocks

Key Idea

Measure drift (unclonable) against the received GPS signal (untrusted) to detect spoofing

Results: Meaconing and Replay Attack



(a) Spoofing attack at 5130 seconds (b) Estimation of the frequency offset (black curve) and the LL of the frequency offset(red curve) and (c) Estimation of the frequency drift and the LL of the frequency drift.

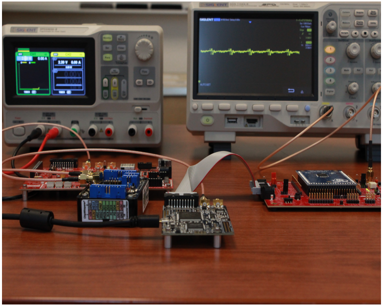
Arafin, Anand, & Qu, GLSVLSI 2017. A low-cost GPS spoofing detector designed for Internet of Things (IoT) applications. p 161. [Best Paper Nomination]

[Joint work with NIST]

Current Works & Capabilities

Physical Layer Security of Sensor Hardware

- Security of intelligent sensor processing units (ISPUs) from side-channel (SC) and fault injection attacks.
- Novel SC attacks and countermeasures using probabilistic modelling of logic computation.



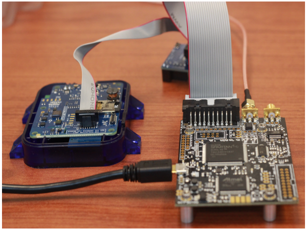
SC and FI set-up in our lab with Chip-Whisperer (CWLITE) boards.

Current Works & Capabilities

Physical Layer Security of Sensor Hardware

Sensor security for Wireless Industrial Node

- 3D accelerometer + gyro-based inertial measurement units
- Ultra-low-power 3-axis accelerometer
- 3-axis magnetometer, and barometer etc.



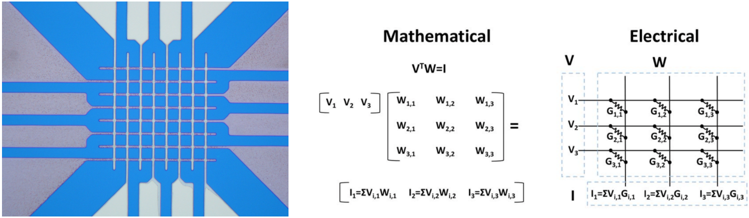
Sensor evaluation platform in our lab using CWLITE and STEVAL-STWINBX1 Development Kit

Secure Hardware Architecture for Intelligent Systems

Post Quantum Cryptography (PQC) Accelerators

Key Idea

Simple error correction techniques (i.e., parity) can lead to lightweight yet quantum-resistant cryptography.

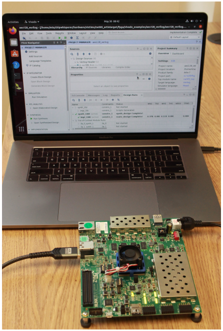

Mathematical
$V^TW=I$
$[V_1\ V_2\ V_3]$
$W_{1,1}$ $W_{1,2}$ $W_{1,3}$
$W_{2,1}$ $W_{2,2}$ $W_{2,3}$
$W_{3,1}$ $W_{3,2}$ $W_{3,3}$
=
$[I_1=\Sigma V_{i,1}W_{i,1}\ \ I_2=\Sigma V_{i,2}W_{i,2}\ \ I_3=\Sigma V_{i,3}W_{i,3}]$
Electrical
V
W
V_1
V_2
V_3
$G_{1,1}$ $G_{1,2}$ $G_{1,3}$
$G_{2,1}$ $G_{2,2}$ $G_{2,3}$
$G_{3,1}$ $G_{3,2}$ $G_{3,3}$
I
$I_1=\Sigma V_{i,1}G_{i,1}$ $I_2=\Sigma V_{i,2}G_{i,2}$ $I_3=\Sigma V_{i,3}G_{i,3}$

Fabricated device and basic matrix-vector computation

Arafin, Shen, Tehranipoor & Qu, GLSVLSI 2019. LPN-based Device Authentication Using Resistive Memory. p 9.

Current Works & Capabilities

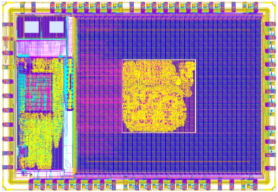
- Hardware accelerator prototyping for post-quantum cryptography (PQC) and fully-homomorphic encryption (FHE).
- Applied cybersecurity issues in domain-specific computation.
- FPGA prototyping in Xilinx Ultrascale+ and Versal devices.



Xilinx Ultrascale+ platform in our lab for acceleration prototyping.

Current Works & Capabilities

- Hardware accelerator tape-out capability for PQC and FHE.
- Semiconductor manufacturing and security research.
- Secure system-on-chip design for medical applications.
- Experience in open-source Skywater 130nm technology.

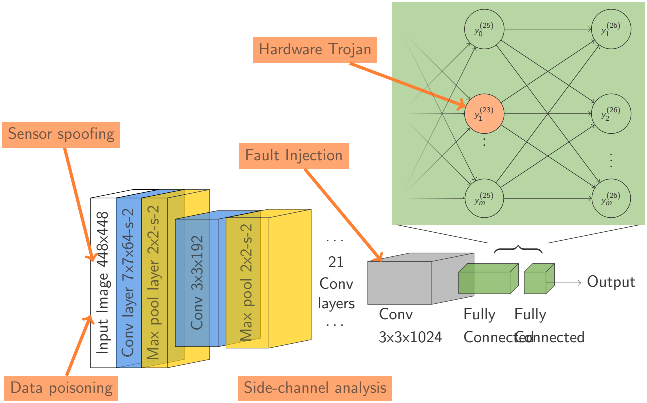


Low power RISC-V taped out by our lab on Skywater 130nm technology.*

*Fabrication support by Apple

Hardware Security in the System Level Information Fusion

Hardware Security of AI/ML Tools



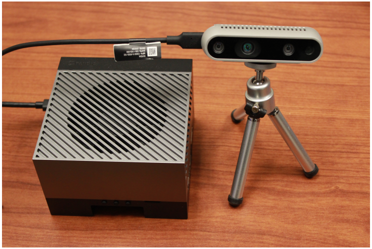
Xu, **Arafin**, Qu, ASP-DAC 2021, *Hardware Security of neural networks from a hardware perspective: A survey and beyond*

YOLO v1 [**CVPR16.Redmon.YOLO**].

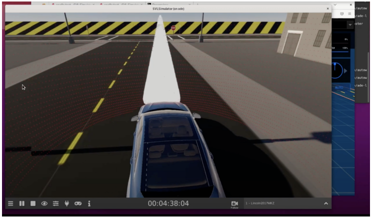
Funded by ARLIS

Current Works & Capabilities

- Driving and sensor fusion using Robot Operating System (ROS) and Autoware.
- Experimentation capabilities for secure vision pipeline.



Jetson Orin with 3D-vision capability.



Attack simulation on Autoware using ROS2 and Applo (CYSE 465 project).

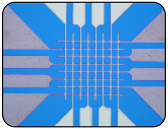
Conclusions

Conclusions

We bring both *experimental and theoretical* hardware and system security research capabilities in

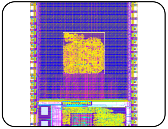
- Side-channel, fault injection attacks on real targets;
- FPGA prototyping and remote SCA analysis;
- ASIC design;
- Secure sensor fusion;
- Semiconductor supply chain issues.

Contributions and Accomplishments



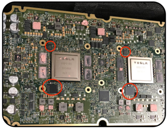
Device and Circuits

- PUFs [TC 2021 🏆, ASP-DAC 2017, ICCAD 2015]
- Approximate Computing [Computer 2017, GLSVLSI 2017 🥈]
- Supply Chain Integrity [ISCAS 2017]



Architecture

- Accelerators [ASPDAC 2021, SOCC 2020, GLSVLSI 2019]
- In-memory Computation [ASPDAC 2022, TVLSI 2018]
- Vulnerability [GLSVLSI 2020]



Systems

- ROT [CISS 2021, IOTSMS 2020, ASIAN-HOST 2018 🏆]
- ML Security [ASPDAC 2021, ASIAN-HOST 2020]
- Hardware Reverse Engineering

THANK
YOU

Additional Slides

Modeling a Clock

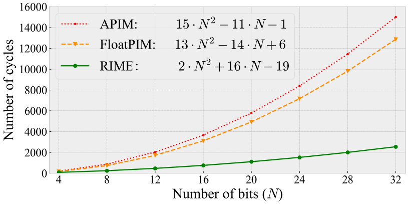
State Space Model

$$\mathbf{X_n} = \mathbf{F_n X_{n-1}} + \mathbf{W_n} \tag{4}$$

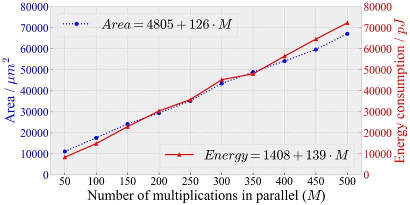
$$\xi_{\mathbf{n}} = \mathbf{H_n X_n} + \mathbf{V_n} \tag{5}$$

Clock state	$X = [x, y, D]$
Time offset	x
Frequency offset	y
Frequency drift	D
State transition matrix	F
Process noise	W

Energy-Efficient In-Memory Architecture for Cryptography



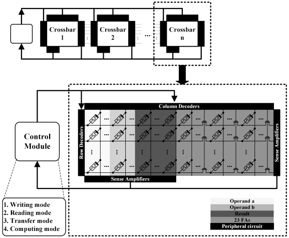
Latency of N-bit fixed-point multiplier.



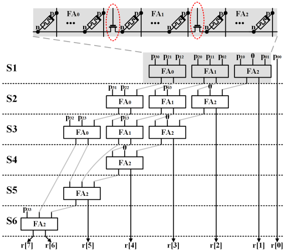
Area / μm^2 & energy consumption / pJ for a single 32-bit floating-point multiplier

Lu, **Arafin**, & Qu, ASP-DAC 2021. RIME: A scalable and energy-efficient processing-in-memory architecture for floating-point operations. p. 120.

Energy-Efficient In-Memory Architecture for Cryptography



Implementation of a RIME computation unit



FA₀
FA₁
FA₂
p
n
S1
S2
S3
S4
S5
S6
p₃₀ p₂₁ p₁₂ p₂₀ p₁₁ p₀₂ p₁₀ 0 p₀₁ p₀₀
p₃₁ p₂₂ p₀₃
p₃₂ p₂₃ p₁₃
p₃₃
0
r[7] r[6] r[5] r[4] r[3] r[2] r[1] r[0]

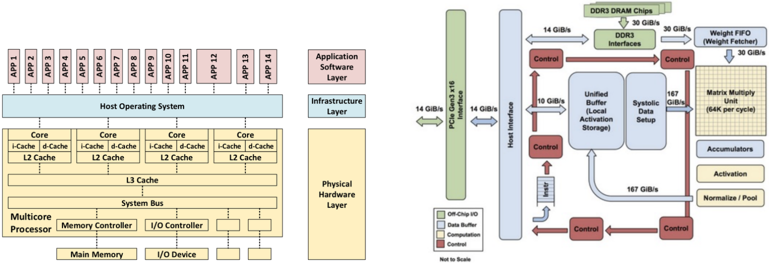
Implementation of a 4-bit Wallace-tree multiplier in RIME.

Lu, **Arafin**, & Qu, ASP-DAC 2021. RIME: A scalable and energy-efficient processing-in-memory architecture for floating-point operations. p. 120.

Hardware Lottery

Axiom

We are moving away from processor-centric to data-centric architecture



Multicore Architecture vs. TPU

Patterson, ISCA 2018 A New Golden Age for Computer Architecture: Domain-Specific Hardware/Software Co-Design. p. 1.

What We Do

Hardware Security

- Security is a *full-stack*, *cross-layered* problem
- Hardware: the weakest link

What We Do

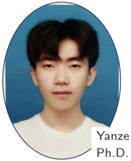
Hardware Security

- Security is a *full-stack, cross-layered* problem
- Hardware: the weakest link
- **Hardware: the strongest link**

Lab Members

Tanvir Arafin
PI
marafin@gmu.edu

Fahim Ahmed
Ph.D student*
fahmed32@gmu.edu



Yanze Wu
Ph.D. Student*
ywu42@gmu.edu

Huizhen Zhao
MS student
hzou9@gmu.edu

Adnan Alam
Undergraduate student
aalam24@gmu.edu