NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

EFFLUX: High-Performance Hardware Security Evaluation Boards

Introduction to EFFLUX –F2, Measurement setup and Interfaces

Arpan Jati
Naina Gupta
Anupam Chattopadhyay
Somitra Sanadhya

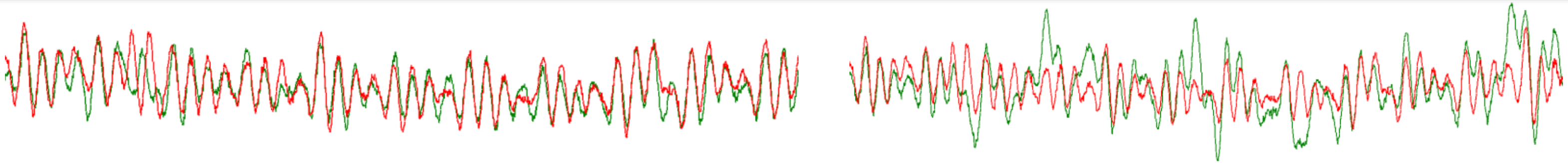
PACE, NTU, SINGAPORE

23rd January 2025

Introduction

- Side channel power analysis:
  - Capturing power or EM traces during the execution of a cryptographic circuit and analyzing them.
  - Many ways to capture traces from a variety of circuits.
  - But using a board designed for trace capture like SASEBO-GII, SAKURA-X, CW305 etc. helps obtain reliable and repeatable results.
- While working with lightweight ciphers and analysis of small logic circuits, it is easily realized that:
  - The leakage is very close or below the **noise floor** and the signal is not easily discernable on the oscilloscope.
  - The analysis takes many **large sets of traces,**
  - The result are often **inconclusive**, especially for small circuits.
  - Trace **averaging** required to improve quality.

EFFLUX F2: Motivation...



Better Example | Bad Example

Example of two subsequent GIFT-128 traces (8-bit, 30dB amplifier), SAKURA-X

- As can be seen from the figure above, the noise from the board affects the captured traces.
- **This means:** A large number of traces are required to instill confidence that a protected design is secure, in some cases, 10's of millions of traces are used.
- We faced these problems while working on such lightweight ciphers and started on designing and improving trace capture boards.

FPGA Board: Design Goals

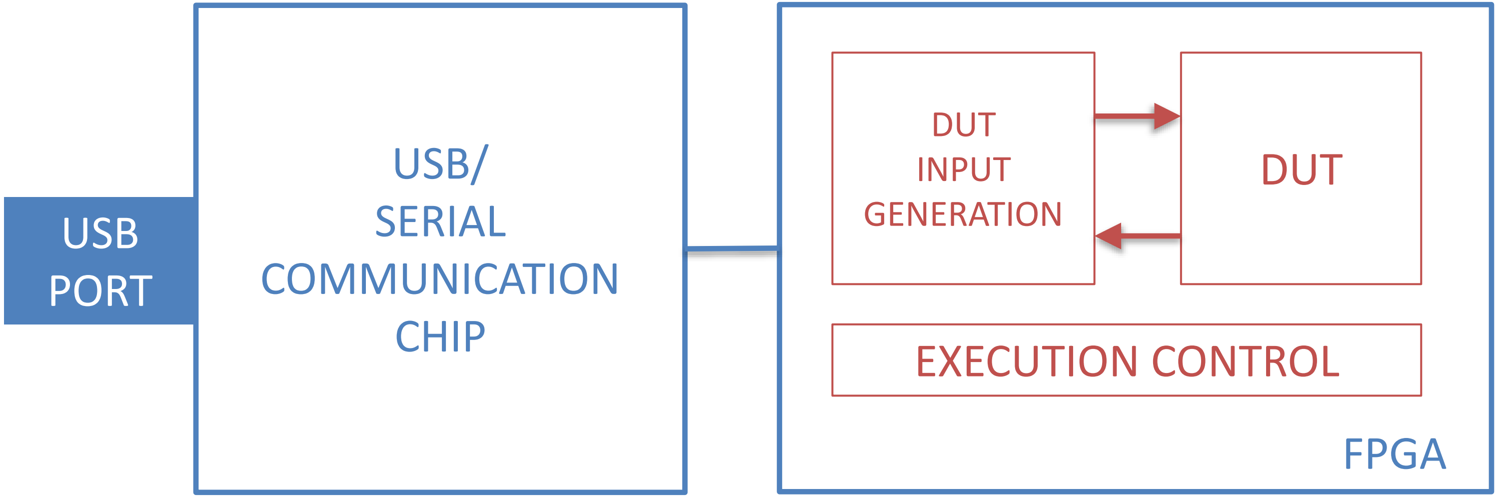
1) Low EMI and Very Low Noise

- To improve measurement quality (both power and EM).
- We aim to improve the SNR significantly to make the experiments faster and more reliable.

2) Single FPGA design

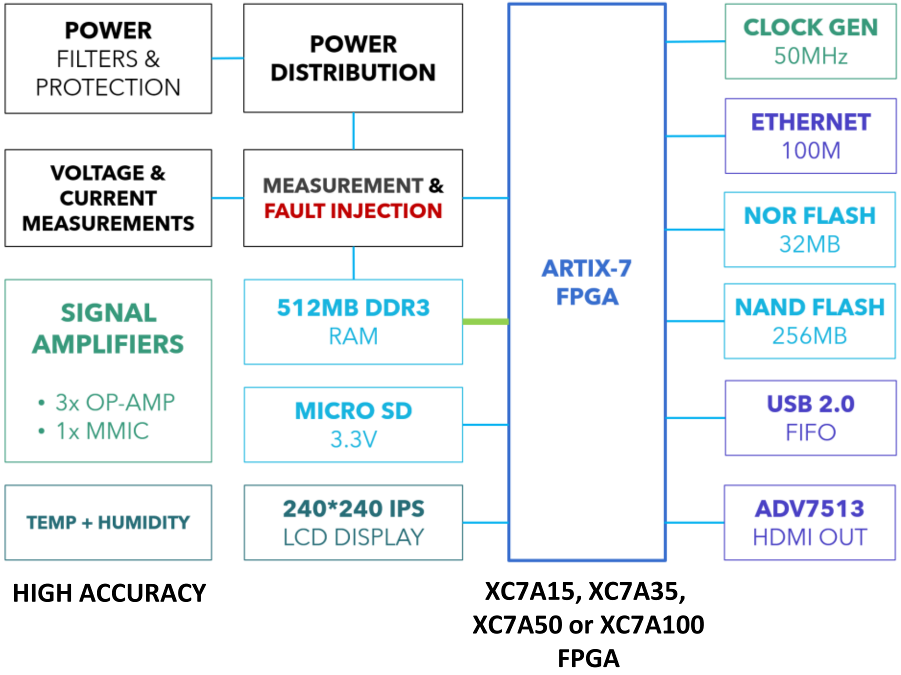
- To simplify the design and reduce system noise and cost.
- Two FPGAs are better for many applications, but with careful hardware and software design, we can use a single FPGA in most applications, without much side-effects.

Block Diagram for Single FPGA Interface

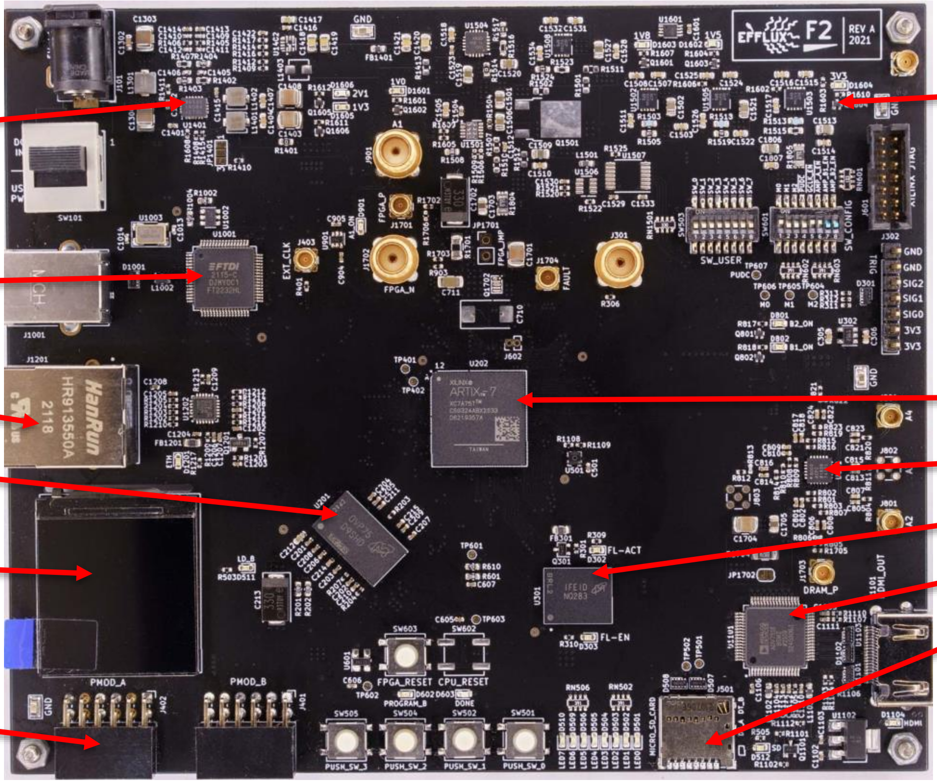


EFFLUX-F2 Block Diagram

- All the devices like RAM, Flash, USB IF, Display interfaces and Ethernet PHY etc., are connected to the FPGA.
- A **specifically designed power supply targeting low noise and EMI emissions** is powering all the devices on the board.
- To keep **noise at a minimum**, there are **no additional microcontroller** or CPLD for housekeeping purposes.
- Further, **all the devices** other than the FPGA do **not contain any additional processing units** to **avoid noise generation**.
- All **noisy peripherals can be power-gated** to **reduce noise in the captured power traces**, this includes high frequency clock generators.

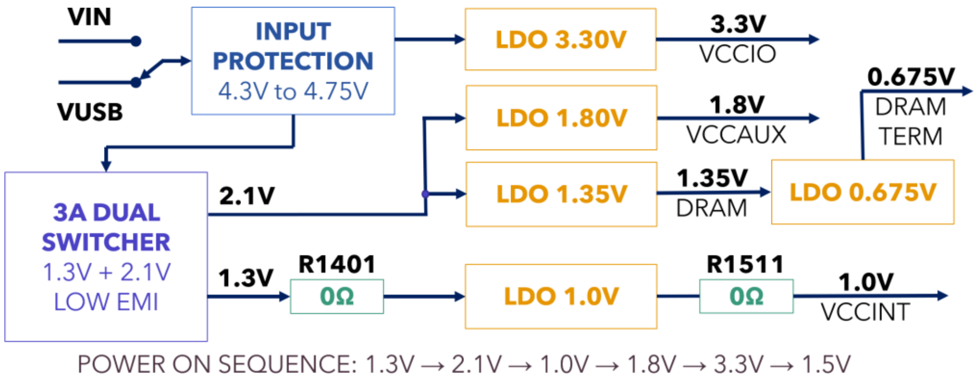


EFFLUX F2 - PCB



EFFLUX F2: FPGA BOARD

Power Delivery



First stage: Uses a dual switching regulator.

Second Stage: Linear low dropout regulators.

- **Power filter:** Wide-band high order filter with an *insertion loss* of more than **60dB** for frequencies between 100 KHz and 100 MHz.
- **LC EMI filter:** 3rd order π type built using discrete components, before reaching a low EMI switching regulator.
- **Low Noise Regulators**
- **Multiple stages if required.**

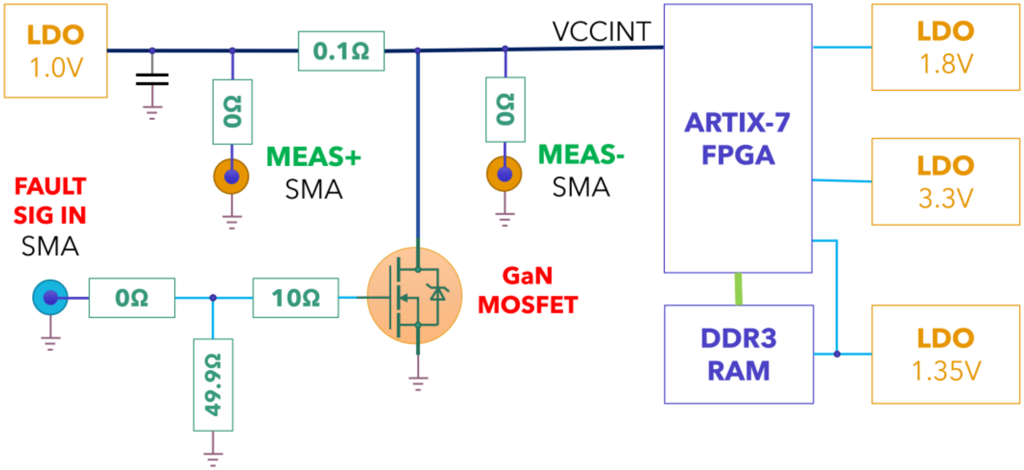
FPGA VCORE Measurement and Fault Injection

Power Measurement

- The voltage drop through the 0.1Ω resistor is amplified by the selected amplifier and can be used as the leakage signal.

Fault Injection

- The power supply is designed to handle shorts to the ground for small duration.
- The MOSFET has a current rating of more than 20A and resistance close to 3mΩ.



High Side Power Measurement: Voltage drop across a resistor.

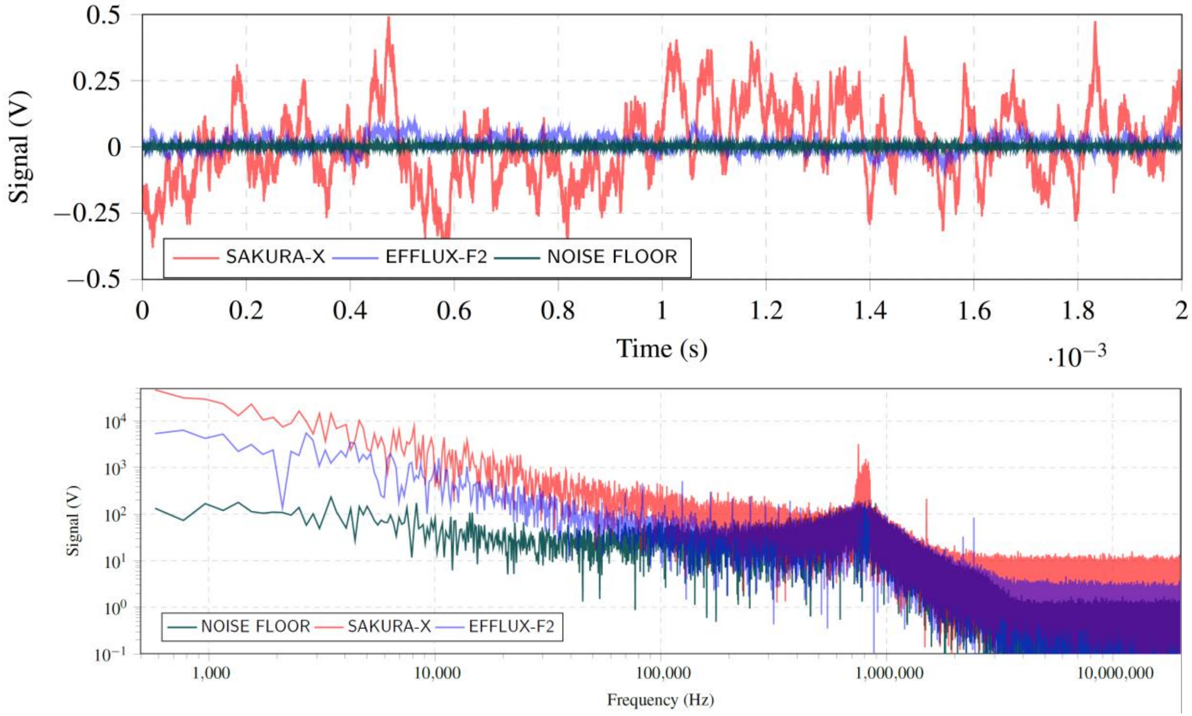
Fault Injection / Power Glitching: Short to ground using a fast MOSFET.

Low Noise Design

- In this work, we follow many design techniques targeted for low noise:
  - reducing **high current loop** areas
  - appropriately sized and placed capacitors
  - proper **ground planes**
  - protecting sensitive signals from noisy traces
- LDO (Low dropout) linear regulators
  - are known for their low noise, **high PSRR** (Power Supply Rejection Ratio) and good transient response.
  - We use these devices as **post regulators** (described above) after the initial switching mode power supplies.
- The switching regulators are also running with **spread-spectrum** enabled
  - this distributes the conducted and radiated EM over a wider frequency band.
- These steps allow us to significantly reduce ripple on the power rails.
- We also use resistors and components (references, OPAMPs and regulators) with **low TCR** (Temperature Coefficient of Resistance) of 10ppm/°C or better and high accuracy 0.1%
  - better signal drift characteristics.
- This helps in experiments that run over a long time and face changing DC levels caused by temperature effects.

Battery Powered System (board generated noise)

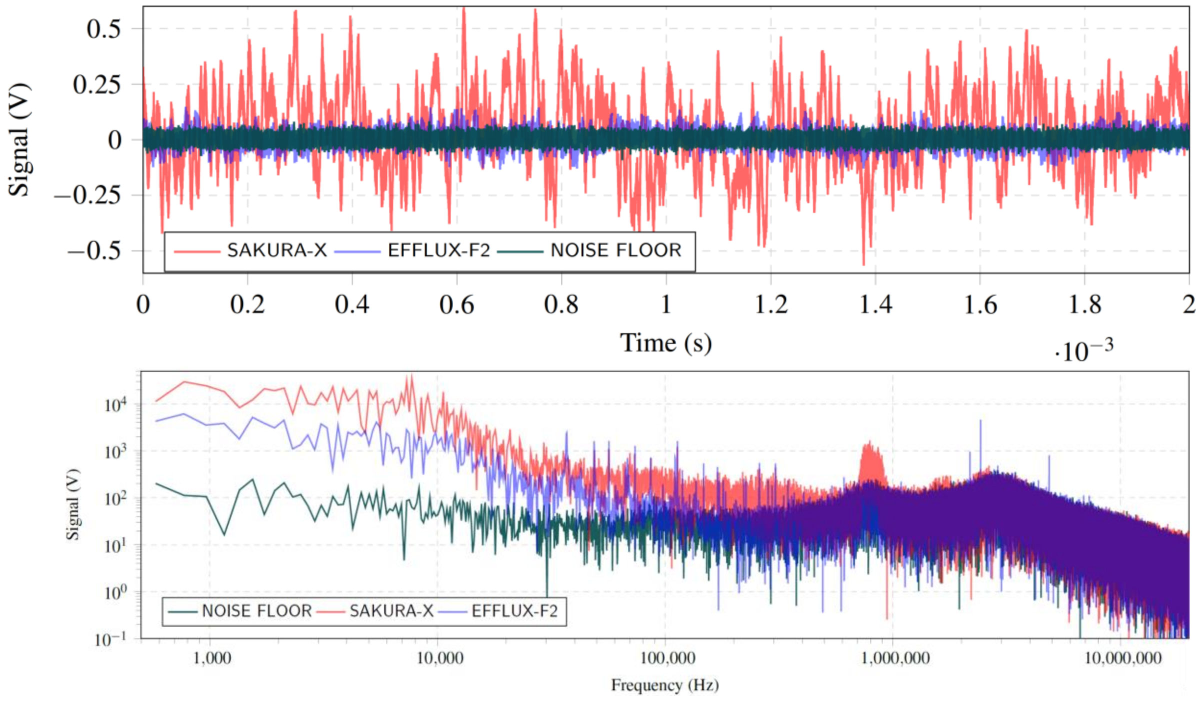
- Powered using two Li-Ion cells in series at a voltage of 8.2V.
- The setup is designed to show the inherent noise of the power supplies.
  - No noise introduced from external power sources.
- Band-limiting the signals to 1 MHz
- EFFLUX-F2 (shown in blue) has a much lower noise amplitude when compared to the SAKURA-X board.
- For SAKURA-X regulator switching at 800 kHz, is visible. EFFLUX-F2 has much reduced emissions.



EFFLUX-F2 vs. SAKURA-X. Battery Powered devices, 1 MHz bandwidth. The graph on top shows amplified voltage signal from the VCCINT rail while the bottom one shows the corresponding FFT (log-log scale).

USB Powered System (typical use case)

- Powered from USB (connected to PC) at a voltage of 5.1V.
- To show the input power noise filtering, no filter was used, and the signal was band limited by the amplifier's bandwidth which is around 10 MHz (Wideband setup).
- EFFLUX-F2 (shown in blue) has much lower noise when compared to the SAKURA-X.



EFFLUX-F2 vs. SAKURA-X. USB Powered devices, 10 MHz bandwidth. The graph on top shows amplified voltage signal from the VCCINT rail while the bottom one shows the corresponding FFT (log-log scale).

Statistical analysis of the measured noise

To obtain the board noise levels, we divide the measured voltages by the amplifier gain 76dB (6300X).

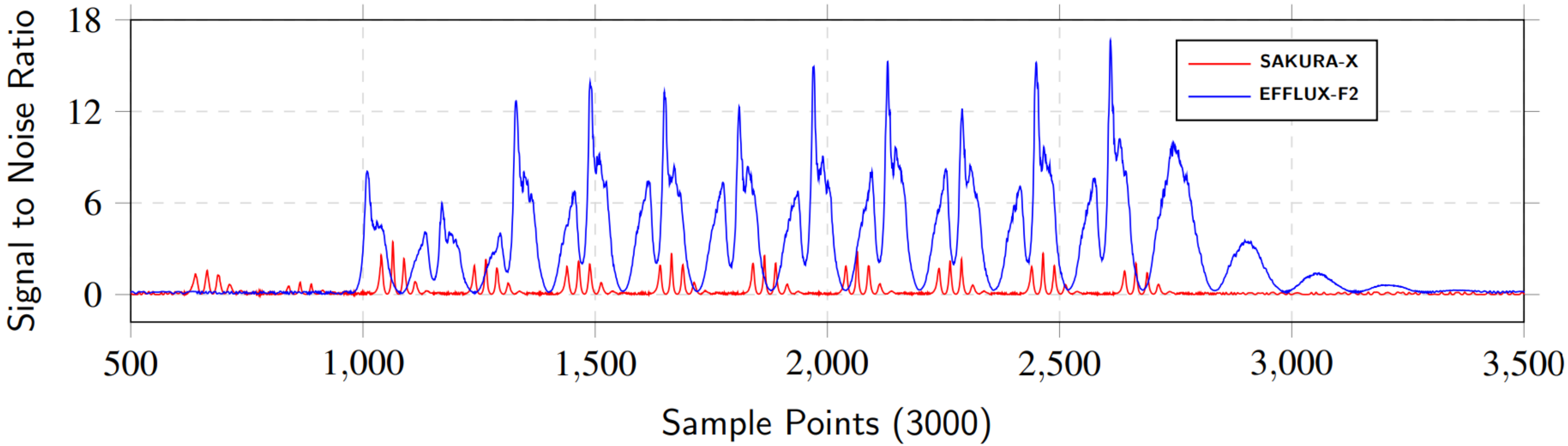
When directly comparing the two boards:

- USB powered, EFFLUX-F2 has 4.62X **lower RMS noise** than SAKURA-X.
- Battery powered, EFFLUX-F2 has 5.14X **lower RMS noise** than SAKURA-X.
- low noise floor of our measurement setup allows us to demonstrate the accuracy of the results with **high confidence**.

	Parameter	Measured at amplifier output			Calculated at amplifier input		
		NOISE FLOOR	SAKURA-X	EFFLUX-F2	NOISE FLOOR	SAKURA-X	EFFLUX-F2
Battery-powered	MEAN	2.504 mV	10.907 mV	12.437 mV	396.838 nV	1.729 μV	1.971 μV
	RMS	5.626 mV	149.032 mV	28.977 mV	891.819 nV	23.622 μV	4.593 μV
	Vpp 6σ	33.759 mV	894.193 mV	173.862 mV	5.351 μV	141.733 μV	27.558 μV
	STDEV	5.039 mV	148.633 mV	26.172 mV	798.662 nV	23.559 μV	4.148 μV
	VARIANCE	25.389 μV	22.092 mV	684.992 μV	0.638 pV	555.018 pV	17.209 pV
	Parameter	Measured at amplifier output			Calculated at amplifier input		
		NOISE FLOOR	SAKURA-X	EFFLUX-F2	NOISE FLOOR	SAKURA-X	EFFLUX-F2
USB-powered	MEAN	3.419 mV	32.492 mV	4.387 mV	541.936 nV	5.150 μV	695.386 nV
	RMS	20.584 mV	176.850 mV	38.207 mV	3.263 μV	28.031 μV	6.056 μV
	Vpp 6σ	123.502 mV	1.061 V	229.241 mV	19.576 μV	168.188 μV	36.335 μV
	STDEV	20.298 mV	173.839 mV	37.954 mV	3.217 μV	27.554 μV	6.016 μV
	VARIANCE	411.998 μV	30.220 mV	1.441 mV	10.351 pV	759.234 pV	36.191 pV

Noise measurement statistics: battery-powered @ 1 MHz B/W, USB-powered @ 10 MHz B/W. The amplifier input is connected to the boards.

Signal-to-Noise Ratio (SNR): Comparison

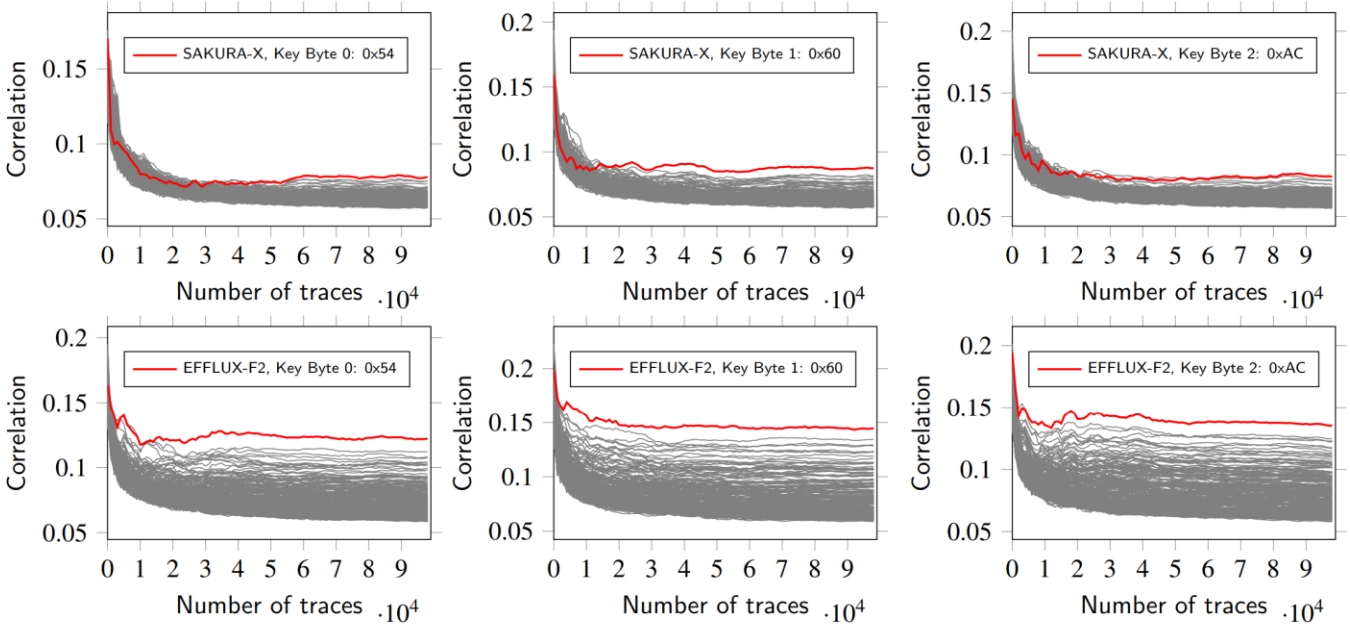


Signal-to-Noise Ratio Comparison: The maximum SNR in the points of interest (last round of AES) for SAKURA-X is measured at sample point 2664 and is 2.020. Whereas, for EFFLUX-F2, the maximum SNR is measured at sample point 2609 and is 16.562.

The SNR of EFFLUX-F2 is **8.2X higher** than SAKURA-X

Correlation Power Analysis (CPA)

Unprotected GIFT



SAKURA-X

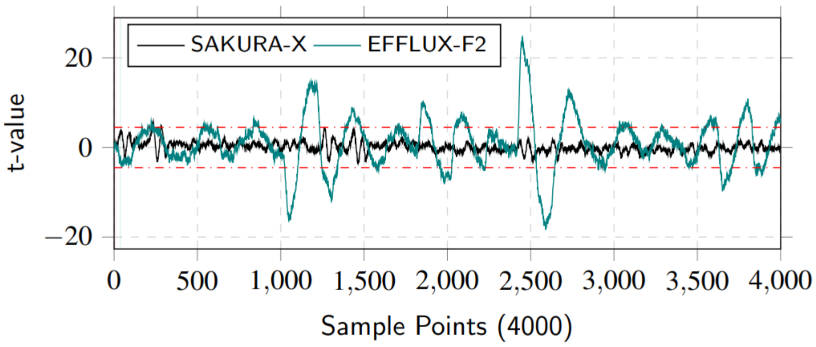
EFFLUX-F2

For key byte 0, almost 60K traces are required using SAKURA-X to distinguish it from other possible key values. Whereas, for EFFLUX-F2, 12K traces are enough, thereby achieving a reduction of almost 5X.

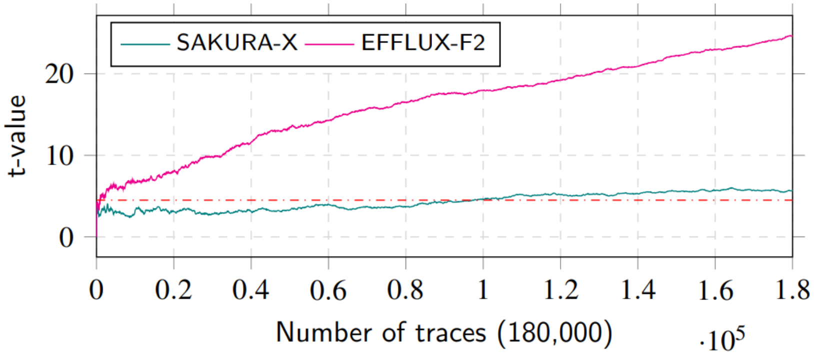
Similarly, for key bytes 1 and 2, 5X and 17X more traces are required respectively.

Test Vector Leakage Assessment (TVLA)

Partially Protected GIFT-128 (Threshold Implementation)



Pointwise t-values



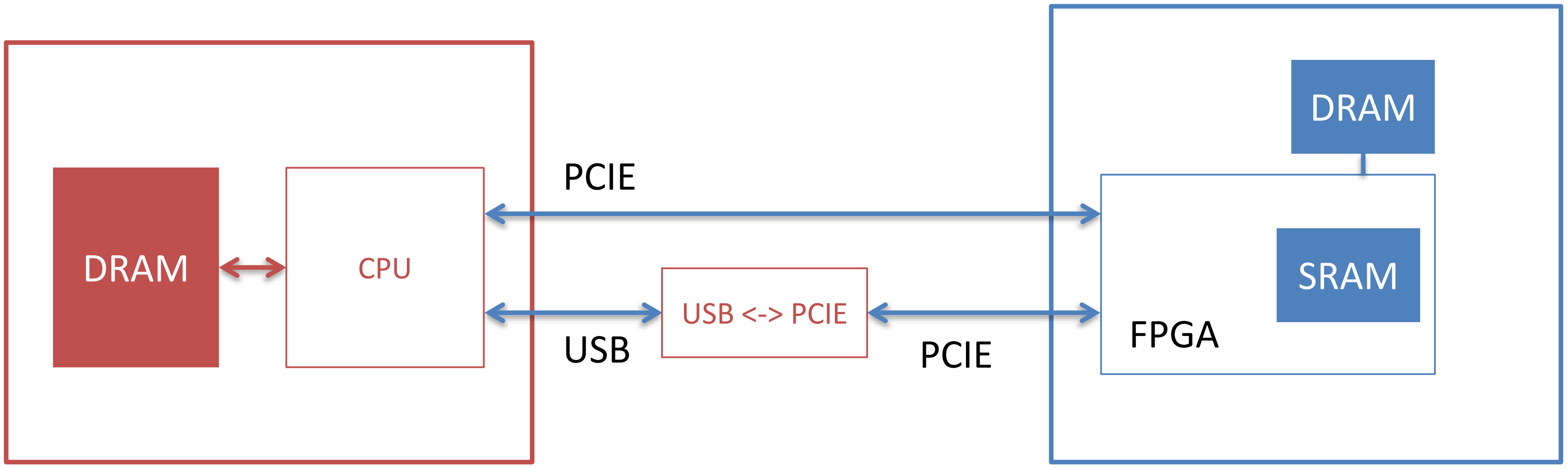
Incremental TVLA

- **Partially-protected** implementation -> **removed the register layer between the decomposed S-boxes**.
- For SAKURA-X the ±4.5 threshold crossed only at a few sample points (around sample point 250).
- Whereas, using EFFLUX-F2, it is **quite prominent** from multiple sample points that the design leaks.
- From the incremental TVLA values. For SAKURA-X, the threshold is crossed **only after 100,000 traces**.
- Whereas EFFLUX-F2 shows leakage even before 5000 traces have been analyzed, and the t-value is increasing steadily.
- Thus, significantly reducing the leakage analysis time for a partially protected design.

Trace Capture: Need for higher performance

- Many experiments require several million traces.
- The data transfer speed quickly becomes the bottleneck, requiring:
    - Local generation using seeds and PRNGs
    - Synchronization issues
- USB 2.0 speeds are not enough once the plaintext/input becomes large 10-100's of KB or more.
- An interface is simply designed to transfer some data from the memory space of one device to the other.
- DMA over PCIe is the fastest way to achieve that.
    - GPUs
    - Accelerators

PCIe Interface

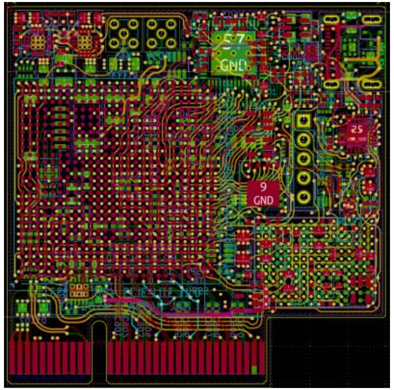


PCIe can be used to bridges two memories.
Fast DMA operations mean significantly high performance

EFFLUX US+ PCIE LITE

Board:

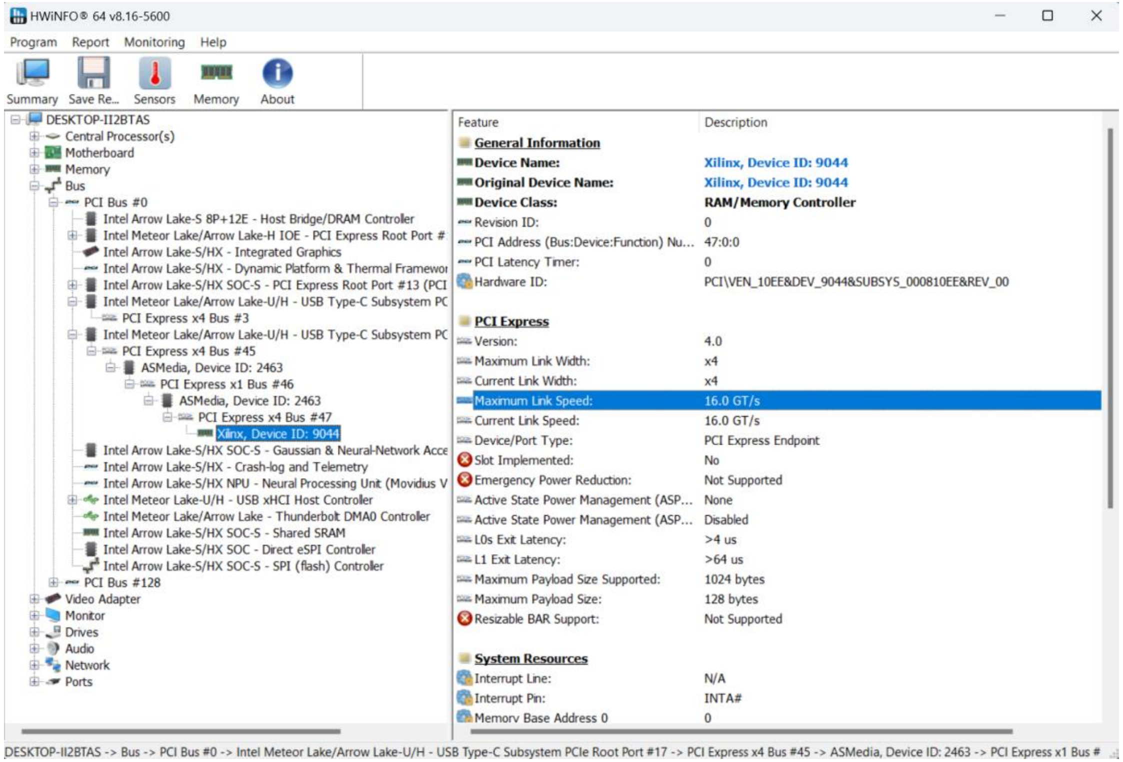
- Xilinx Artix/Kintex UltraScale+ XCAU10P/ XCAU15P/XCAU20P/XCKU3P/XCKU5P as targets.
- Powered from PCIE port or external USB.
- USB PD supported. Requests from controller 12V.



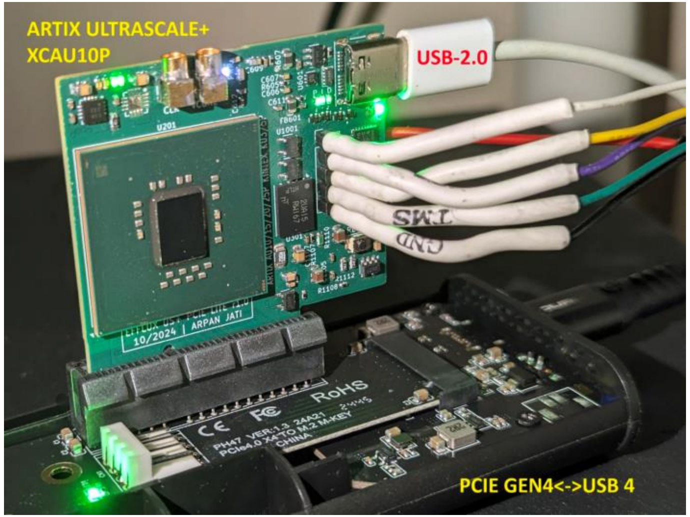
Control/Data Interface:

- USB FT2232 10-30MB/s
- PCIE GEN4 7.9 GB/s

EFFLUX US+ PCIE LITE: PCIE over USB 4



HWiNFO tool showing connected speeds and properties.



EFFLUX US+ PCIE LITE connected to a Intel Core Ultra 7 265K processor via USB4 using a ASM2464PD based I/F board at full PCIE GEN4 (16GT/s). The Xilinx FPGA shows up as a **memory controller.**

…