جامعة نيويورك ابوظبي
NYU | ABU DHABI

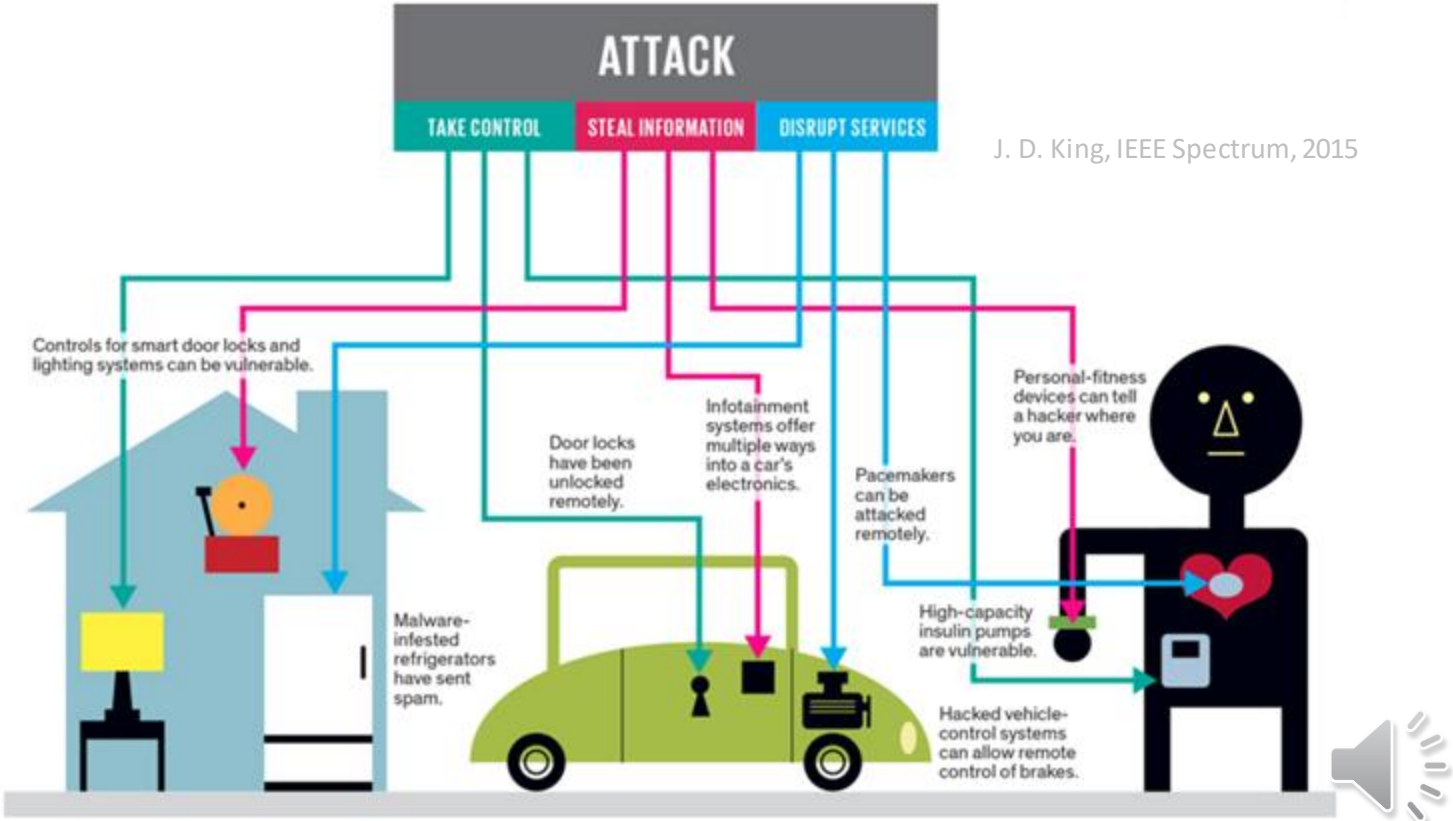
CENTER FOR CYBER SECURITY

DFX LAB
DESIGN FOR EXCELLENCE

X-Volt: Joint Tuning of Driver Strengths and Supply Voltages Against Power Side-Channel Attacks

Saideep Sreekumar, Mohammed Ashraf, Mohammed Nabeel, Ozgur Sinanoglu, Johann Knechtel

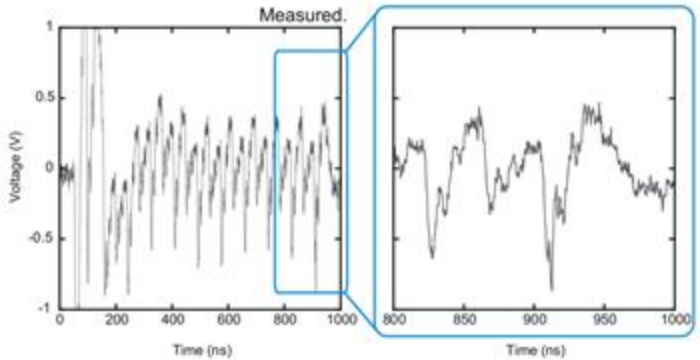
International Symposium on Physical Design – Online, March 29, 2023



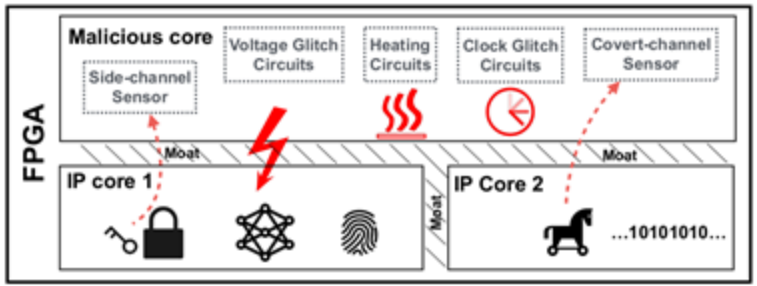
J. D. King, IEEE Spectrum, 2015

Sreekumar, et al., "X-Volt: Joint Tuning of Driver Strengths and Supply Voltages Against Power Side-Channel Attacks," ISPD'23, March 29

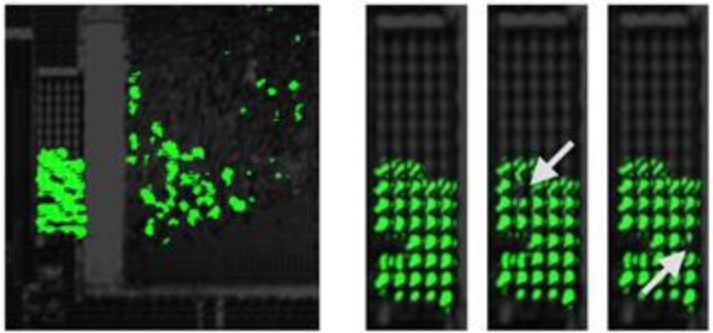
Data and Computation at Risk – Right at the Hardware



Fujimoto et al., EMC 2014

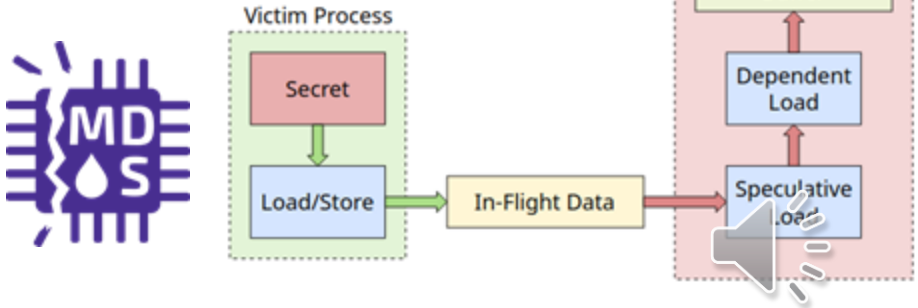


Alam et al., FDTC 2019



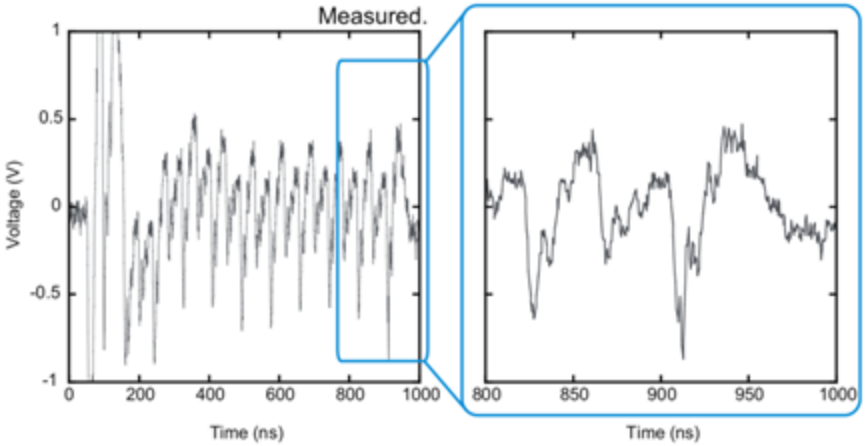
Tajik et al., CCS, 2017

https://www.bleepingcomputer.com, 2019

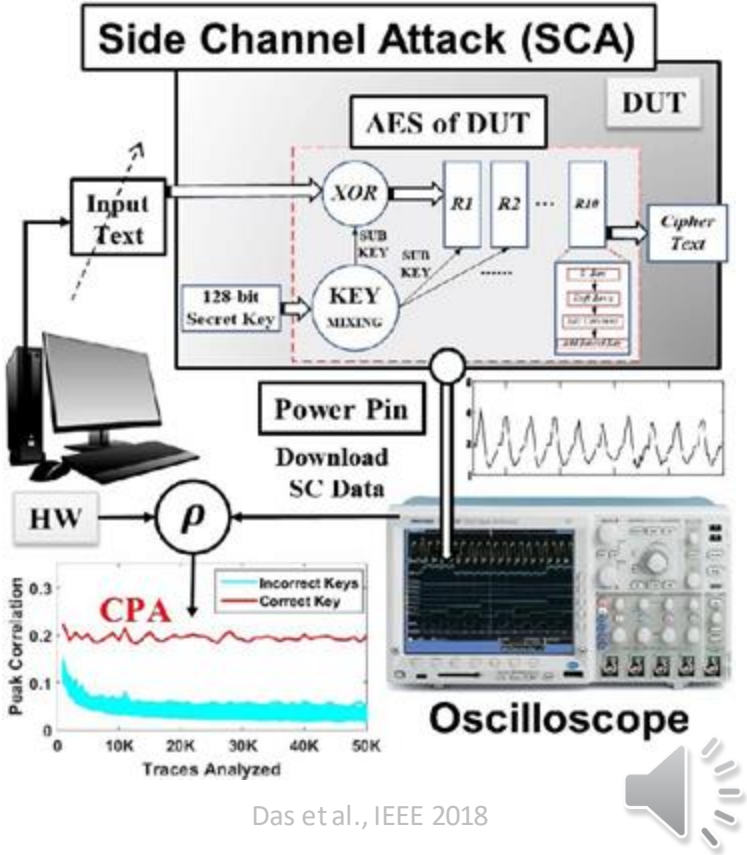


Sreekumar, et al., "X-Volt: Joint Tuning of Driver Strengths and Supply Voltages Against Power Side-Channel Attacks," ISPD'23, March 29

Side-Channel Attacks (SCA)



Fujimoto et al., EMC 2014

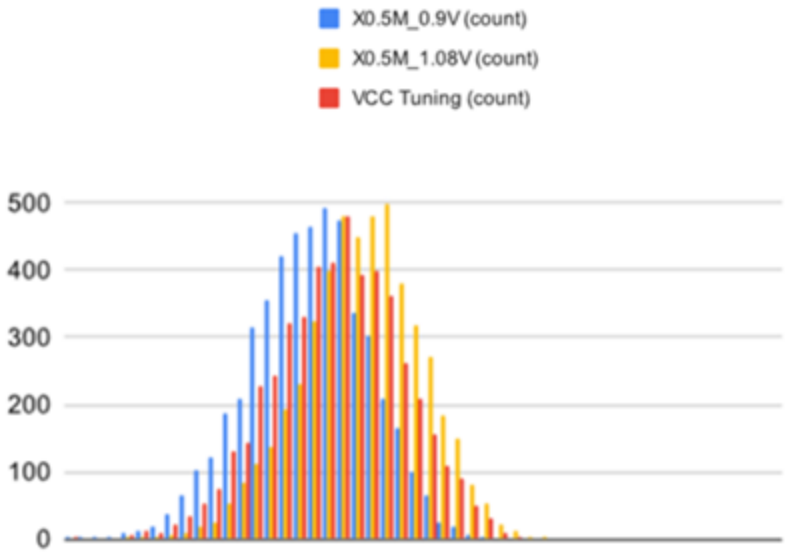


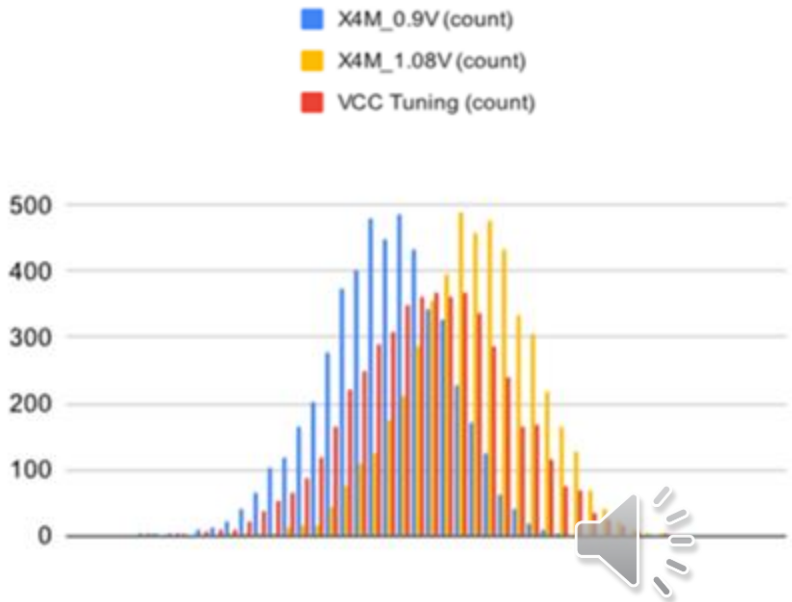
Das et al., IEEE 2018

Sreekumar, et al., "X-Volt: Joint Tuning of Driver Strengths and Supply Voltages Against Power Side-Channel Attacks," ISPD'23, March 29

Motivation

- VCC Tuning Countermeasure
- Improved impact when driver strength tuning is added.

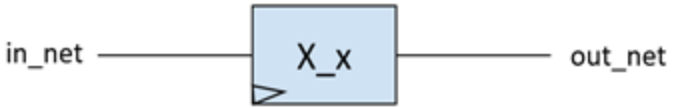


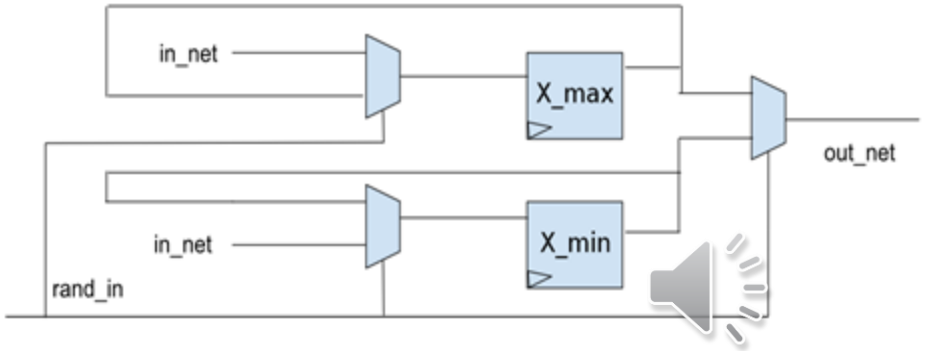


Sreekumar, et al., "X-Volt: Joint Tuning of Driver Strengths and Supply Voltages Against Power Side-Channel Attacks," ISPD'23, March 29

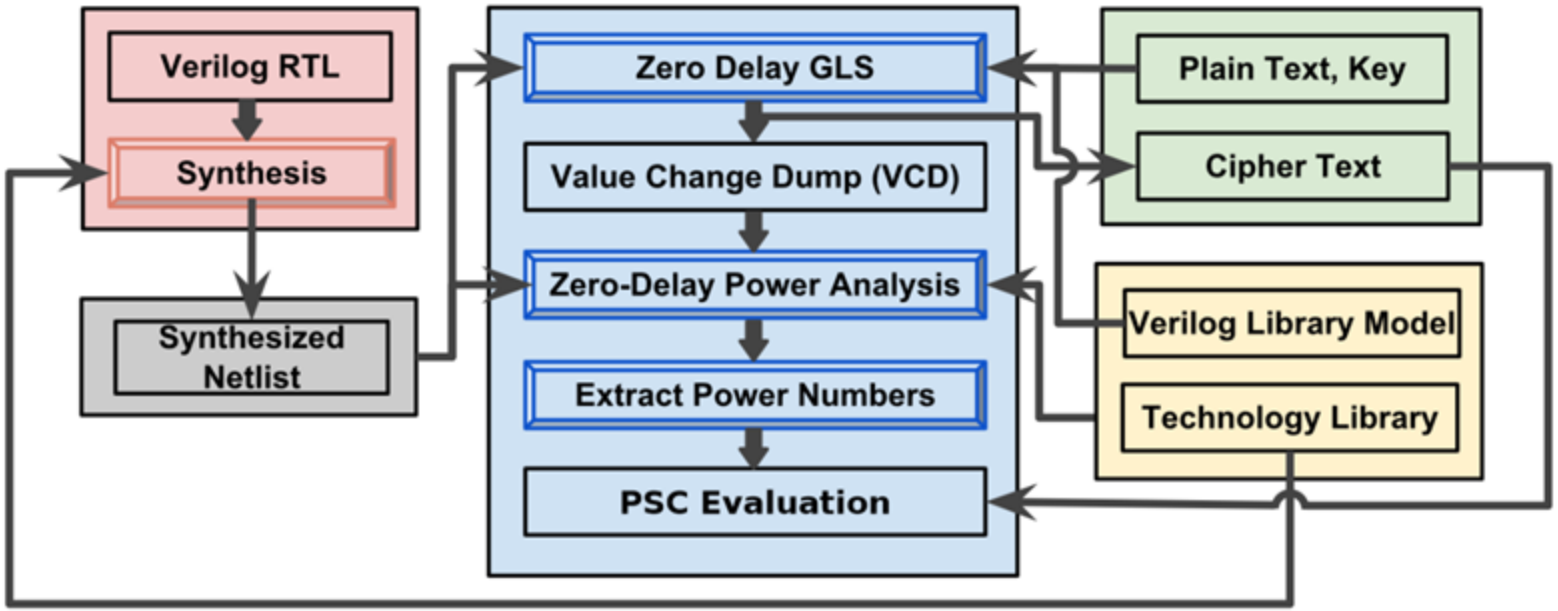
Runtime Tuning Implementation

- ASIC
  - Static tuning: Reconfigure driver strength in chosen registers
  - Dynamic tuning: Chosen registers replaced by register pair and MUX pair
  - VCC tuning: Assume IVR
- FPGA
  - Driver strength tuning: Connected via IO pins rather than additional registers
  - VCC tuning: Use onboard IVR

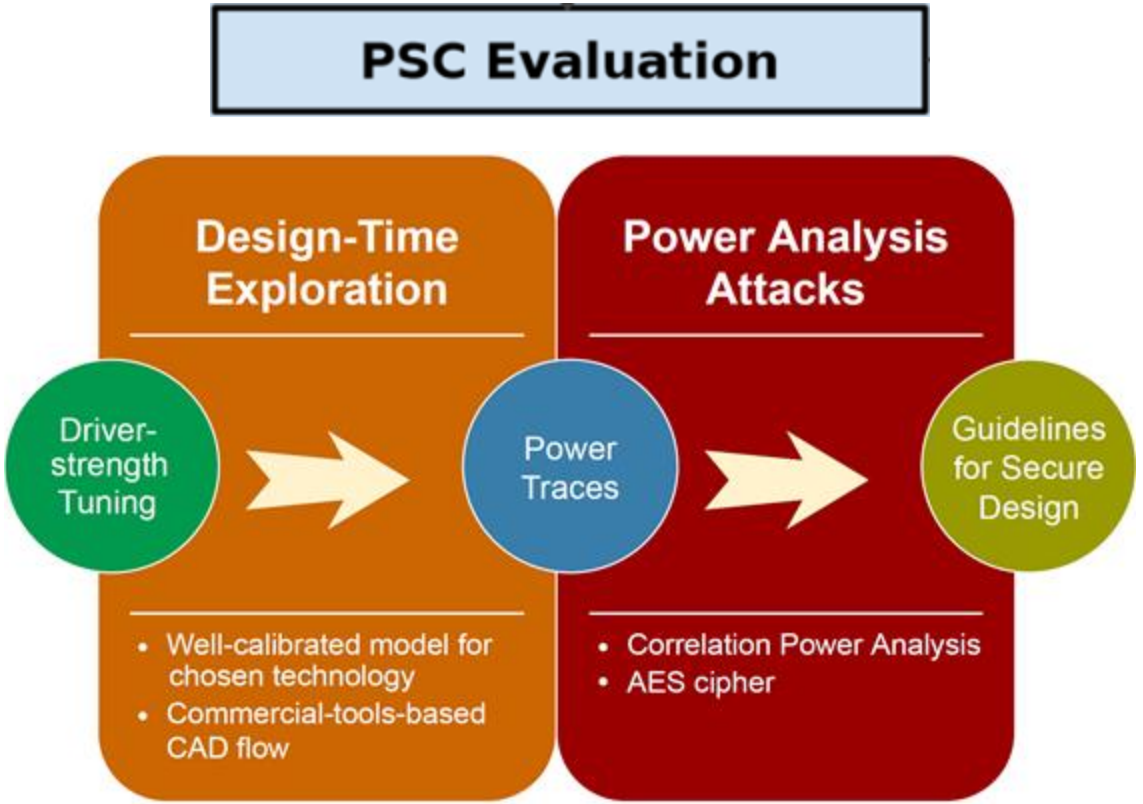




CAD Flow

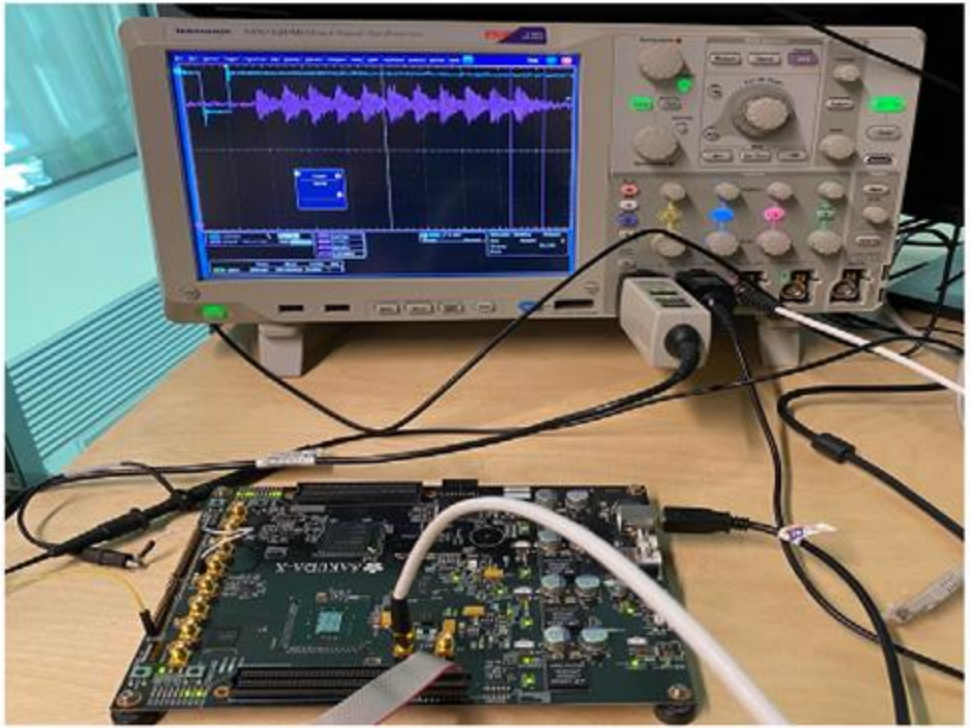

Verilog RTL
Synthesis
Synthesized Netlist
Zero Delay GLS
Value Change Dump (VCD)
Zero-Delay Power Analysis
Extract Power Numbers
PSC Evaluation
Plain Text, Key
Cipher Text
Verilog Library Model
Technology Library

CPA Setup

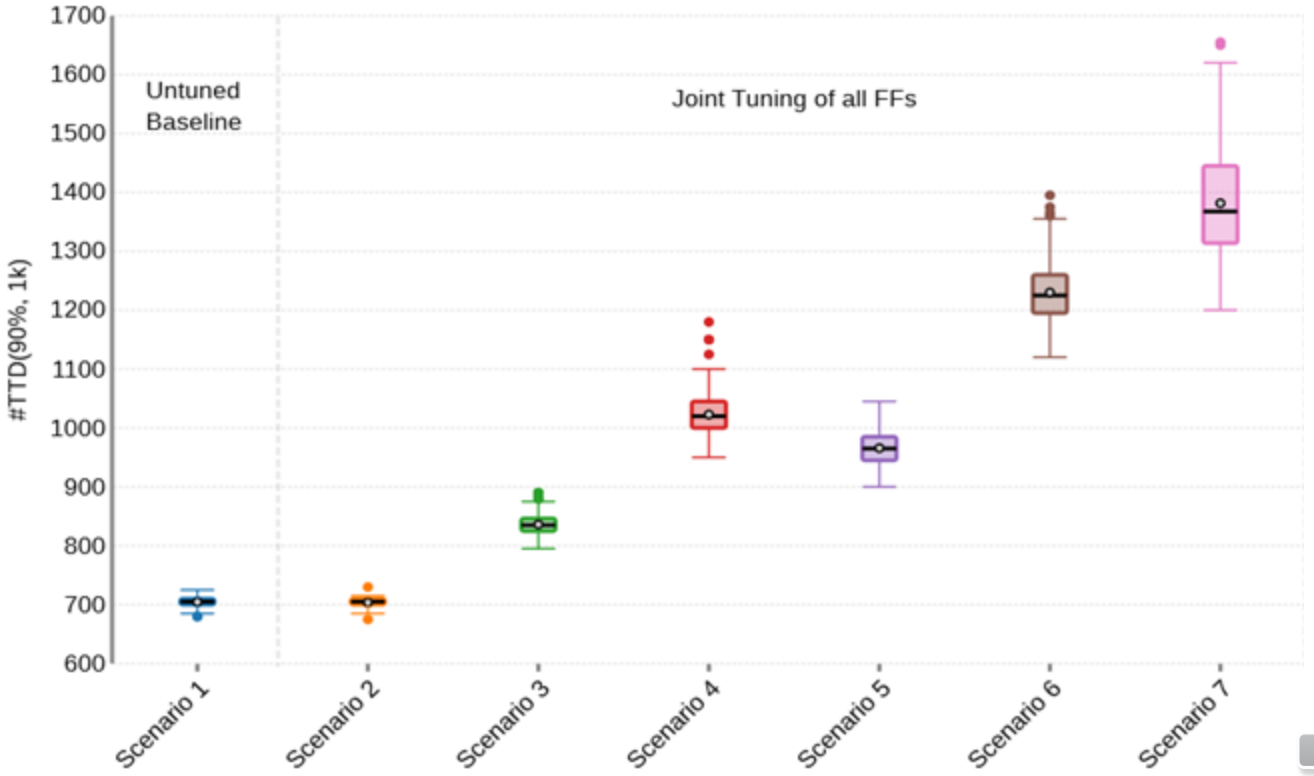


Sreekumar, et al., "X-Volt: Joint Tuning of Driver Strengths and Supply Voltages Against Power Side-Channel Attacks," ISPD'23, March 29

FPGA Setup

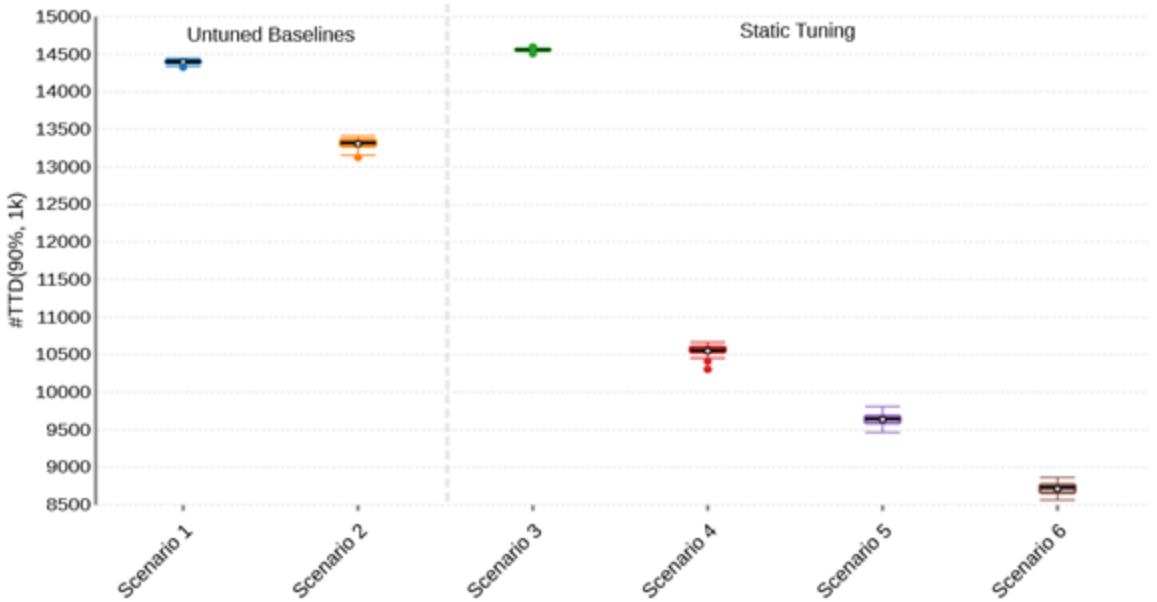


ASIC CPA Results

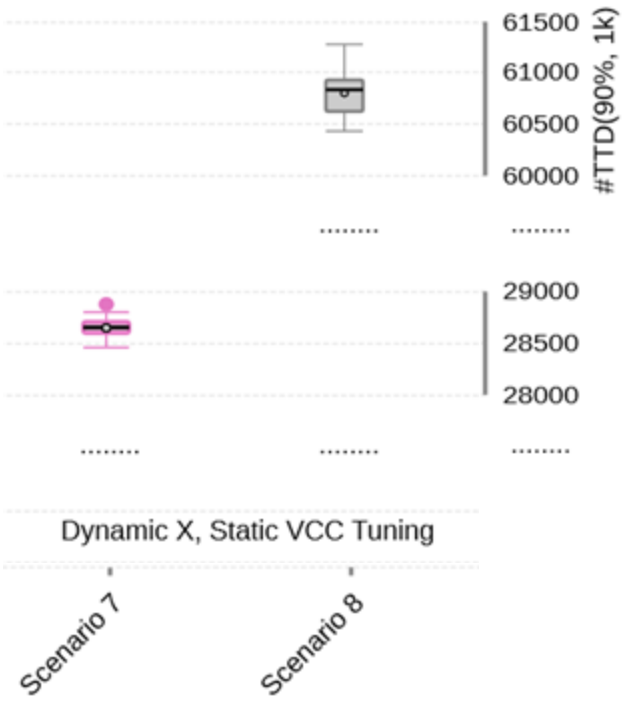


Sreekumar, et al., "X-Volt: Joint Tuning of Driver Strengths and Supply Voltages Against Power Side-Channel Attacks," ISPD'23, March 29

FPGA CPA Results



FPGA CPA Results



Sreekumar, et al., "X-Volt: Joint Tuning of Driver Strengths and Supply Voltages Against Power Side-Channel Attacks," ISPD'23, March 29

ASIC Layout Analysis Results

Design	Avg. Peak Power [mW] 0.9V / 1.08V	Critical-Path Delay [ns] 0.9V / 1.08V	Std.-Cell Area [μm^2] 0.9V / 1.08V
Baseline	2.709 / 3.100	9.64 / 9.79	54,928 / 43,639
All FFs Tunable	3.134 / 3.764 (+15.69% / +21.42%)	14.13 / 11.86 (+46.68% / +21.14%)	67,873 / 57,300 (+23.57% / +31.30%)
AES-Text FFs Tunable	2.779 / 3.237 (+02.58% / +04.42%)	14.13 / 11.68 (+46.68% / +19.31%)	57,272 / 46,324 (+04.27% / +06.15%)

ASIC Layout Analysis

FPGA Layout Analysis Results

Design	Avg. Peak Power [mW] 0.9V / 1.08V	Critical-Path Delay [ns]	FFs / LUTs Util. [# / #]
Baseline	0.969357 / 1.07049	9.052	952 / 3,137
Static X4	0.972771 / 1.07352 (+00.35% / +00.28%)	10.352 (+14.36%)	965 / 3,118 (+01.37% / -00.61%)
Static X16	0.971117 / 1.07347 (+00.18% / +00.27%)	10.352 (+14.36%)	965 / 3,118 (+01.37% / -00.61%)
Dynamic	0.973676 / 1.07214 (+00.45% / +00.15%)	9.994 (+10.41%)	1,028 / 3,183 (+07.98% / +01.47%)

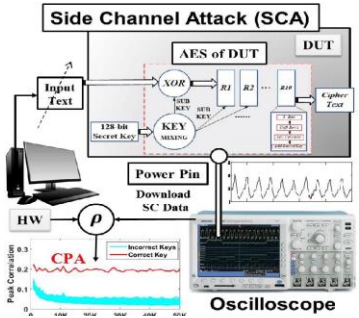
FPGA Layout Analysis

Design Guidelines

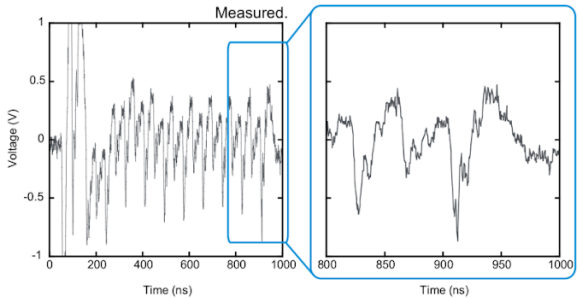
- Static tuning should be avoided.
- Dynamic tuning of both driver strength and VCC should be used when possible as it is most resilient.
- Dynamic driver-strength tuning is a preferred alternative compared to dynamic VCC tuning.
- Tuning all flip-flops is not always practical.

Conclusion & Future Work

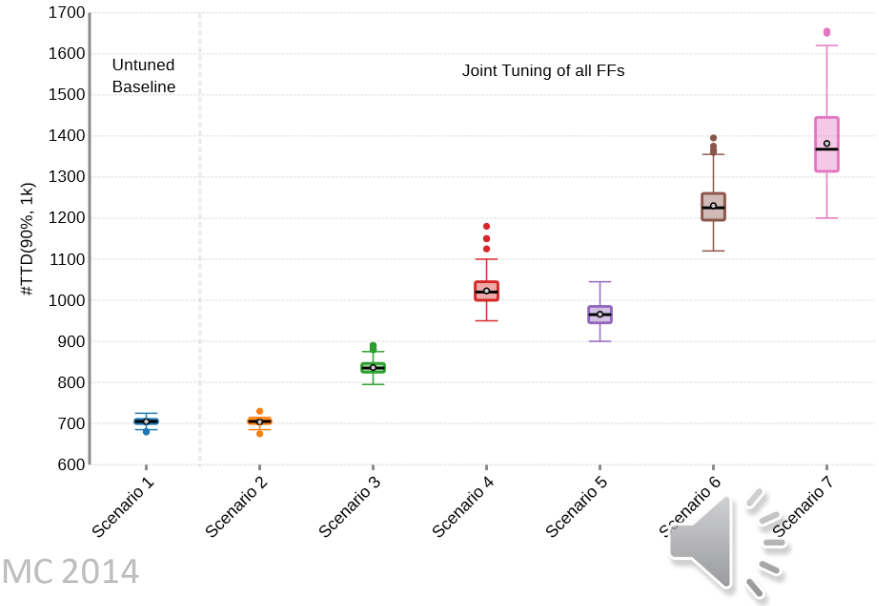
- More efficient tuning implementation for ASIC and FPGA.
- Study tuning in the context of leakage power attacks.
- Further study using other approaches for security assessment.



Das et al., IEEE 2018



Fujimoto et al., EMC 2014



Sreekumar, et al., "X-Volt: Joint Tuning of Driver Strengths and Supply Voltages Against Power Side-Channel Attacks," ISPD'23, March 29