On-Device Power Analysis Across Hardware Security Domains

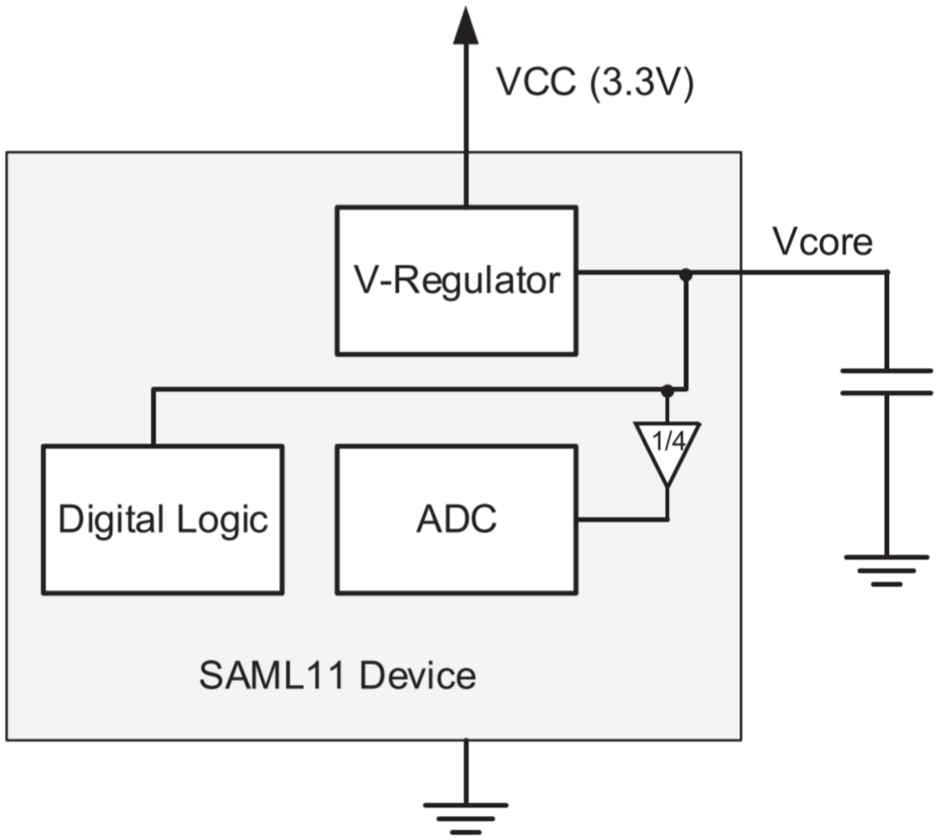
Colin O'Flynn, Alex Dewar

Dalhousie University

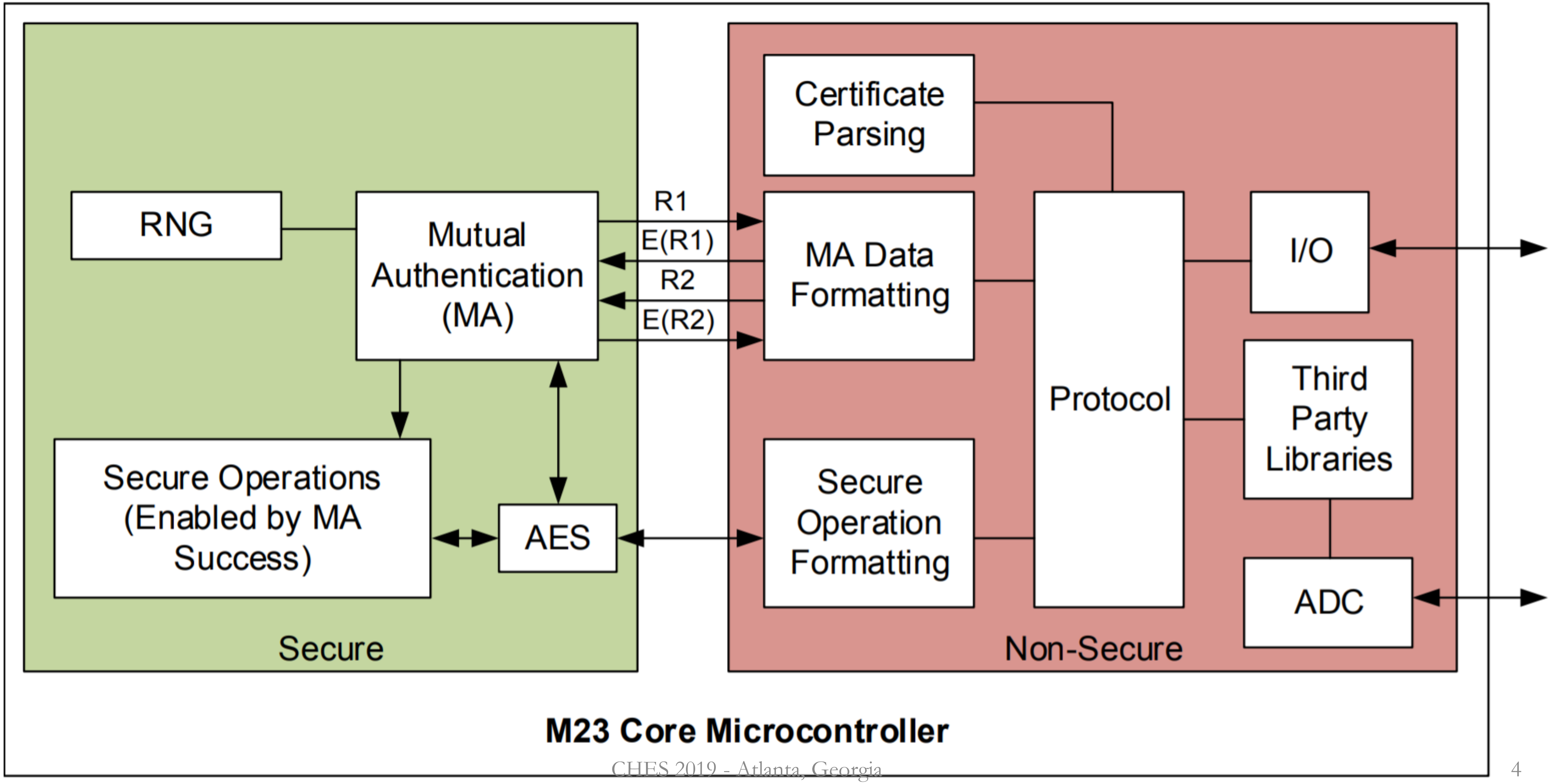
What am I doing for next 17 mins (in 42 slides)?

- Introduction Remote & Cross-Domain Attacks
- Attacker Model, TrustZone-M, and SAML11
- Basic CPA Attack on SAML11, bit depth / sample rate effect
- Internal regulator attack experiments
- Attacking a standard SAML11 development kit
- Countermeasures

On-Device Power Analysis



Introducing… TrustZone-M



On-Device Power Analysis across Hardware Security Boundaries

```c
uint8_t get_pt(uint8_t *pt)
{
        while (!adc_done);
        adc_done = 0;
        ADC->CTRLC.bit.FREERUN = 1;
        ADC->SWTRIG.bit.FLUSH = 1; //flush adc conversions
        nsc_func_enc(key, 4, pt, pt);
        simpleserial_put('r', 16, pt);
        return 0x00;
}
```

```c
/*
 * \brief Non-secure callable function 1
 */
void __attribute__((cmse_nonsecure_entry)) nsc_func_enc(const uint8_t *keys, uint32_t key_len, const uint8_t *src, uint8_t *dst)
{
        return idau_aes_enc(keys, key_len, src, dst);
}
```

```c
void DMAC_0_Handler(void)
{
        PORT_SEC->Group->OUTSET.reg = 1 << 7;
        ADC->CTRLC.bit.FREERUN = 0;//disable freerun
        DMAC->CHINTFLAG.bit.TCMPL = 1; //clear transfer complete flag
        adc_done = 1;
}
```

Specific Implementation Example

- SAML11 → One of first M23 cores available on market (June 2018)
- Original datasheet (since changed) made an interesting claim…

- Built-in cryptographic accelerator accessible through cryptographic libraries stored in ROM
  - Supporting AES-128 encryption/decryption, SHA-256 authentication, GCM encryption and authentication
  - Cryptographic libraries are especially designed for side channel and fault injection attacks prevention

Product Usage of TrustZone-M / SAML11

- When starting work no products on market used the SAML11
- Made some assumptions about design of products, backed up by datasheet examples:

13.2.5.1 SAM L11 Peripherals Configuration Example

Below is a typical configuration examples where all peripherals except the ADC, TC0, and Event System (EVSYS) are reserved to the Secure application:

- Secure/Non-Secure Peripherals PAC configuration:
  - PAC.NONSECA=PAC.NONSECB=0x0000_0000
  - PAC.NONSECC=0x0000_00091 (ADC, TC0 and EVSYS available for the Non-Secure application)

Assumptions / Attacker Powers

- Attacker must have previously performed an attack to gain code execution on the non-secure space (or otherwise has such access).

- Attacker can run considerable amount of tests / data recovery.
  - We can consider a remote attacker as in-scope… realistically we will look at "quasi-remote".

  - Quasi-remote means not full system access (cannot do DPA at board-level), but perhaps has debugger/communication access.

Example of "Quasi-Remote" Attacker Threat

- Unlocking ECUs is big business.
- Requiring tuners to solder to PCB & capture power traces is a large hurdle.
- But requiring them to plug in a debug connector is very much "in-scope" for these attacks.
  - If DPA attack runs in reasonable time, allows tuners to perform such attacks even with unique keys.

TrustZone-A Attacks

1. General remote attacks presented by Bernstein [Ber05].
2. Arm Cache-timing attacks used to break TrustZone-A [LGS+16], [ZSS+16], [ZSS+18], [LW19], [NCC18].
3. Remote fault attacks also demonstrated on TrustZone-A, such as RowHammer shown on TrustZone-A by [Car17] and CLKscrew [TSS17].

"Remote" Side-Channel Attacks

- Cortex-M frequently lack a true cache, making cache-timing attacks difficult.

- Previous work on side-channel *power* analysis done with a 'remote' threat model includes:

1. Building voltage-monitoring circuitry on a shared FPGA fabric ([SGMT18b] initially, [RPD+18] and [ZS18] show follow-on).

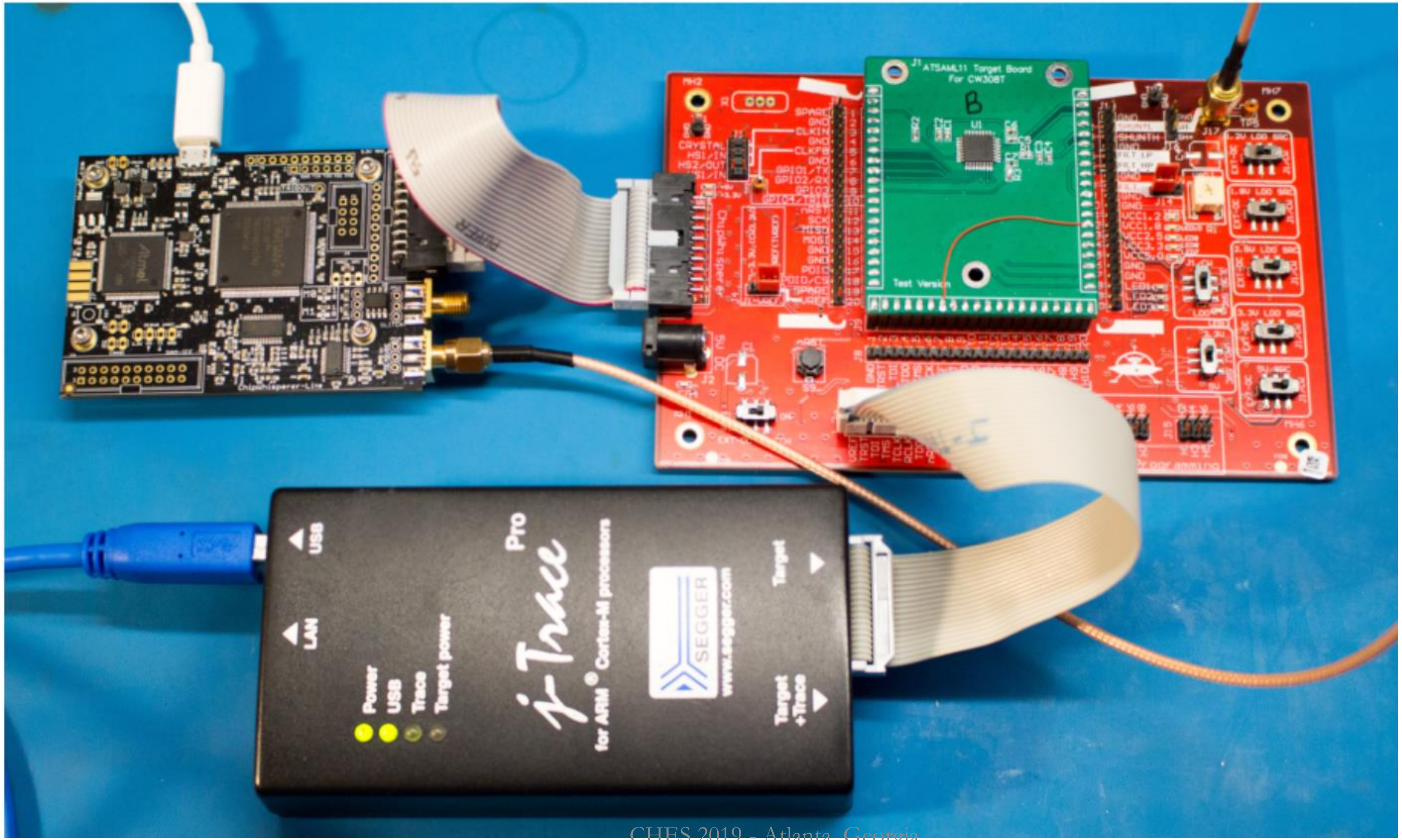
2. Using on-board ADC of a microcontroller [GKT19].

May require very large set of data transferred out!

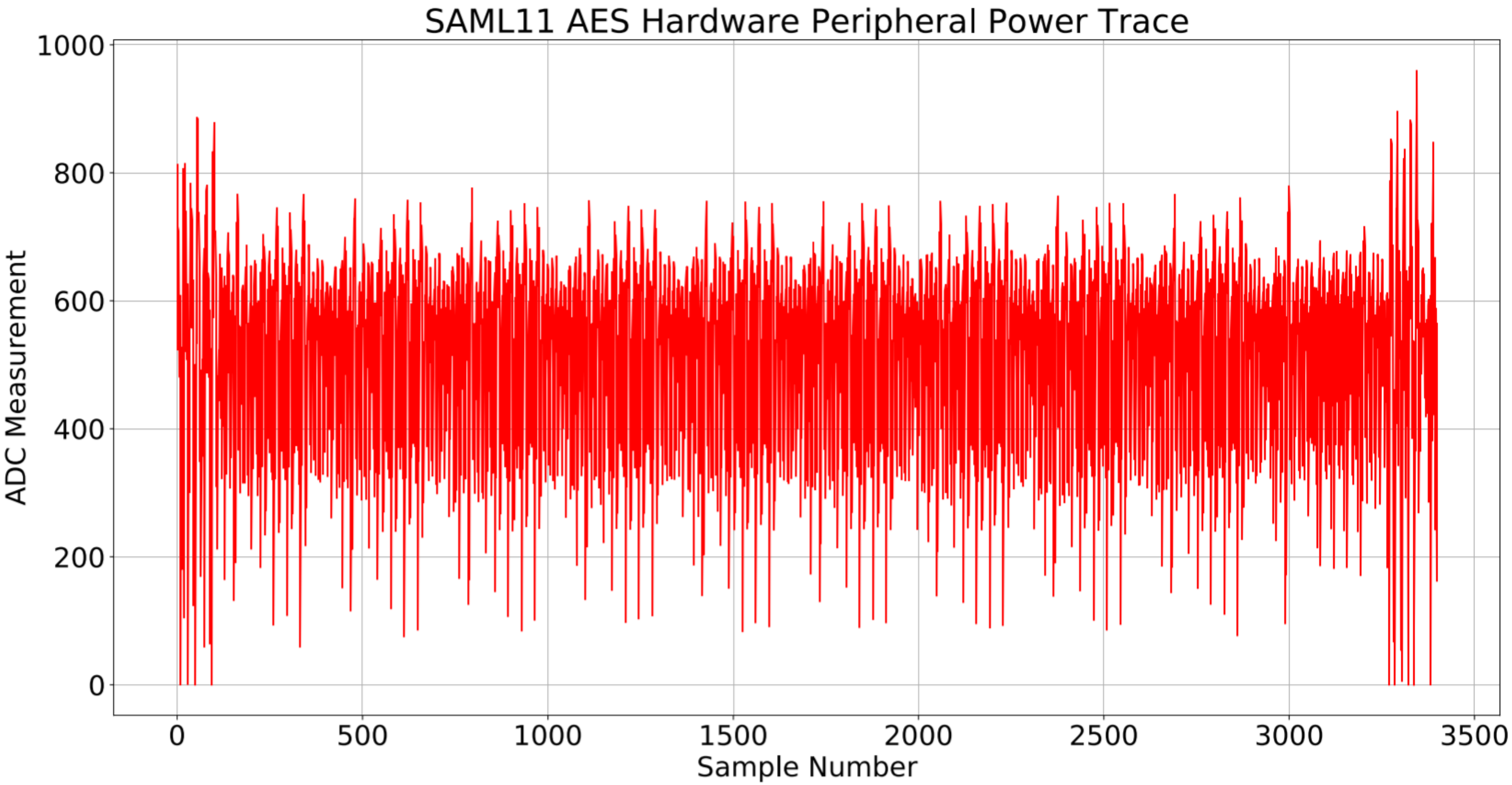
“Nearby” Side-Channel Attacks

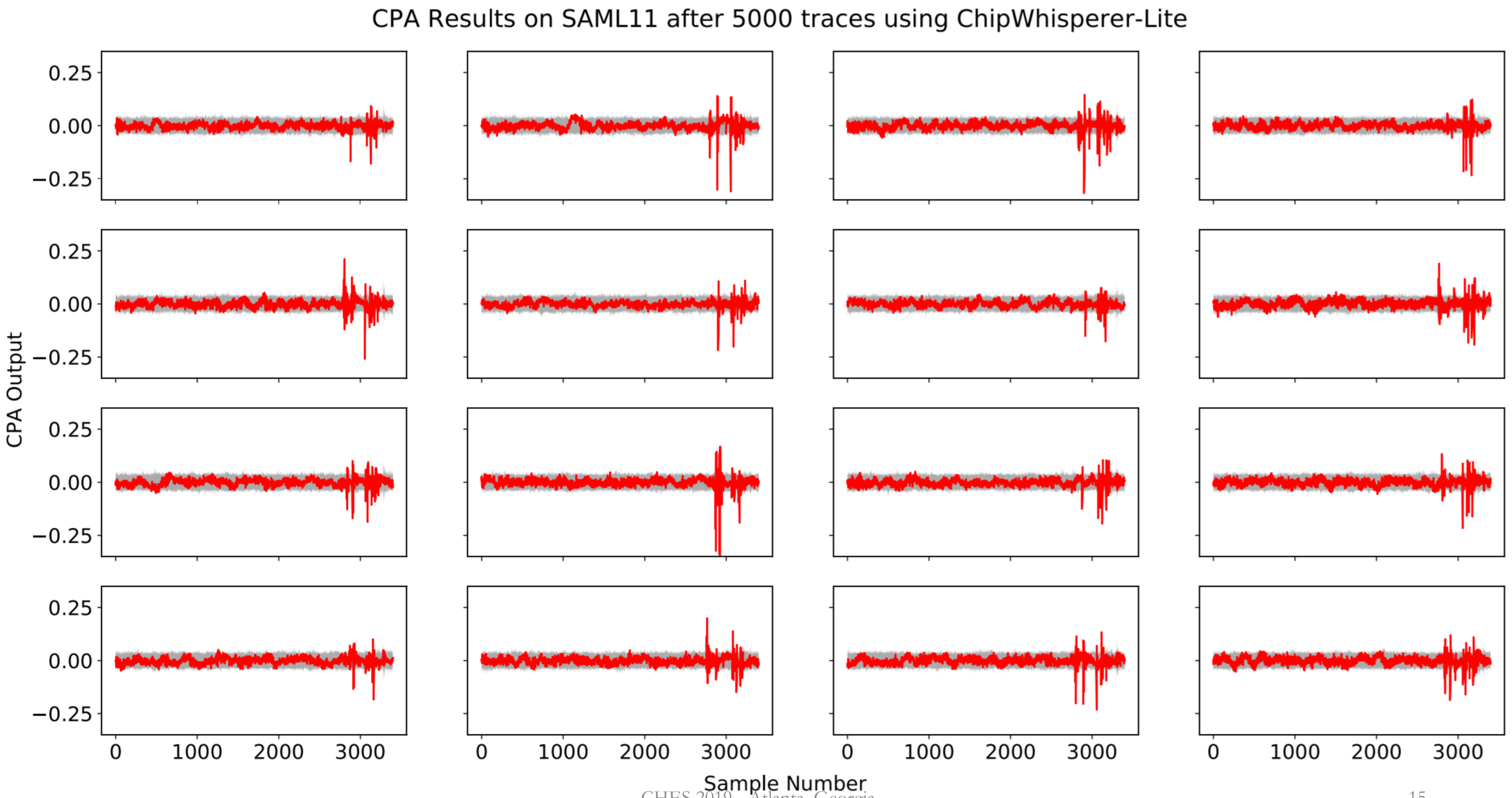
- Measuring voltage on I/O pin leaks information [SPK+10].
- Band-limited signal measured on switch-mode “line” side can be used for AES attack [SLT16].
- Band-limited radio signals have been previously used in attacking RSA/asymmetric [GST14], [GPPT15].
- Recently AES attacked with radio signal leakage [CPM+18].

Part 1 – External CPA Attack

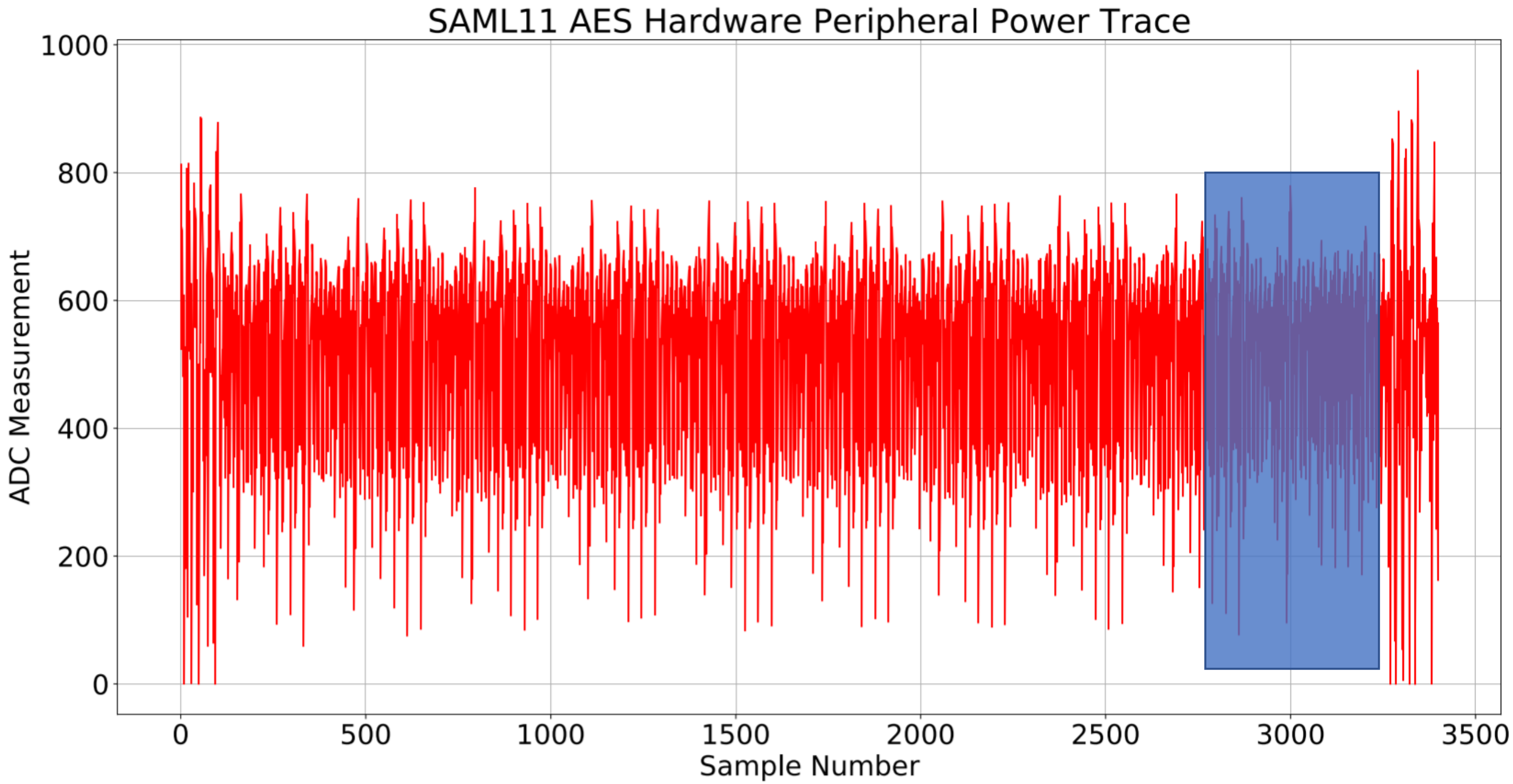


AES Accelerator Attack




CPA Results on SAML11 after 5000 traces using ChipWhisperer-Lite
CPA Output
0.25
0.00
−0.25
0
1000
2000
3000
Sample Number

AES Accelerator Attack

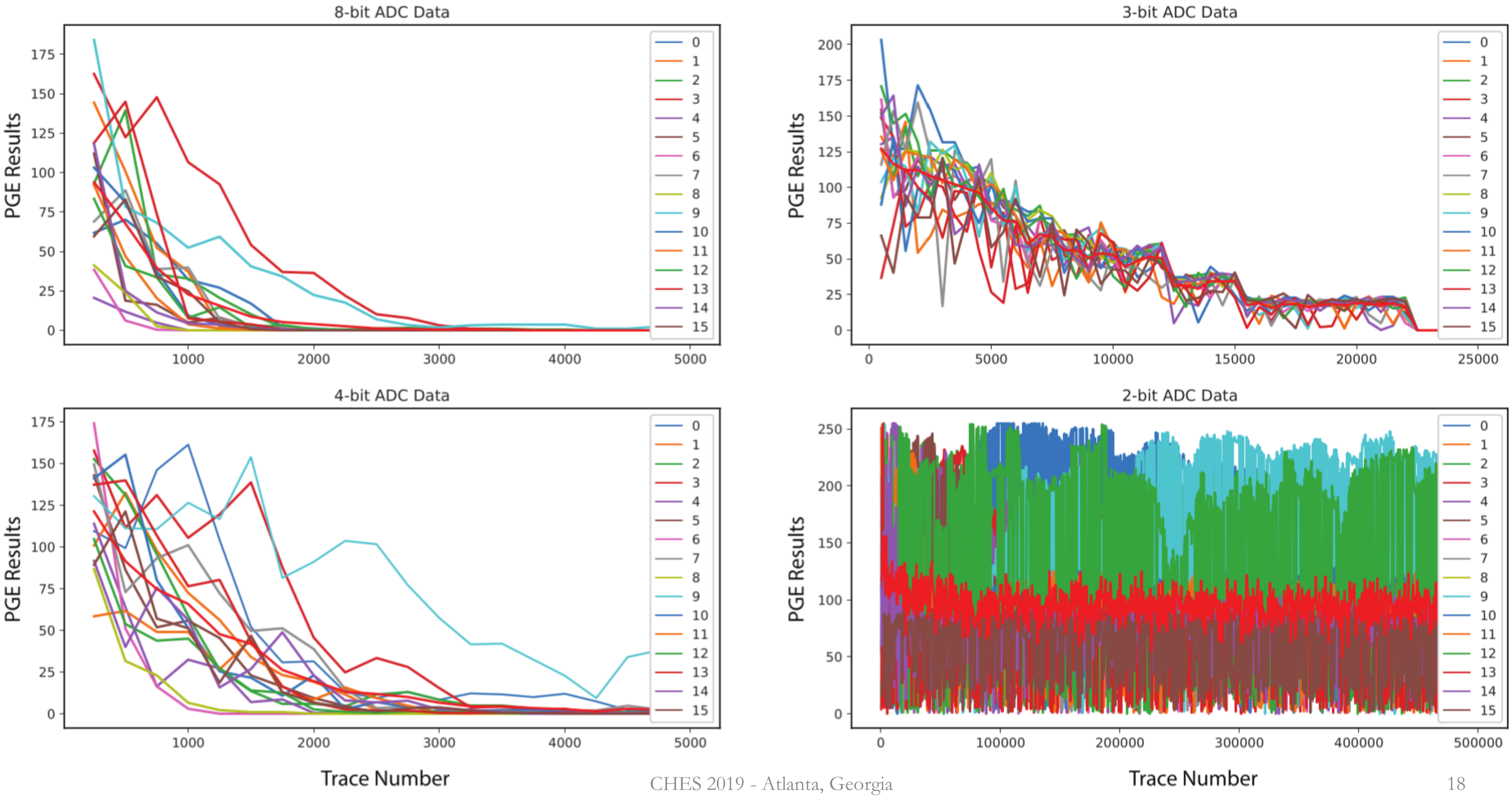


Effective Bit Depth of Samples?

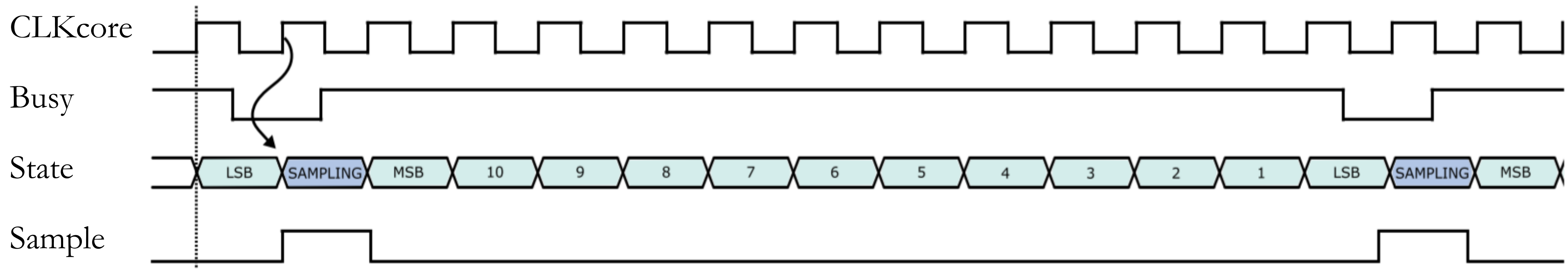
$$SNR_{dB} = 6.02N + 1.78dB$$

ADC Bits	Max Value	Min Value	Effective Bits
10	929	429	8.97
8	232	107	6.98
4	14	6	3.17
3	7	3	2.32
2	3	1	1.58

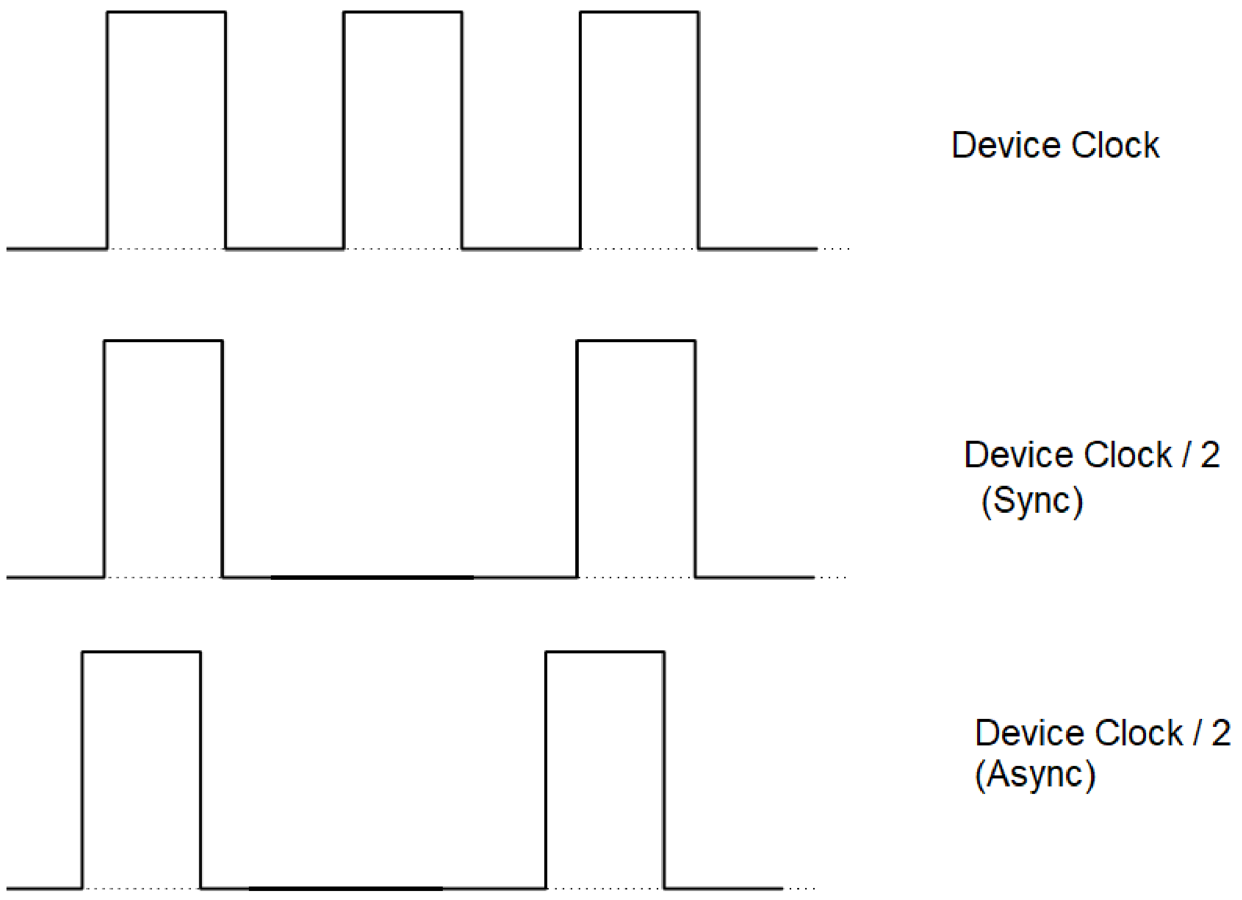
PGE Comparison for Reduced Bit Depth



Sample Rate Reduction due to Internal ADC



Synchronous Sampling Mode

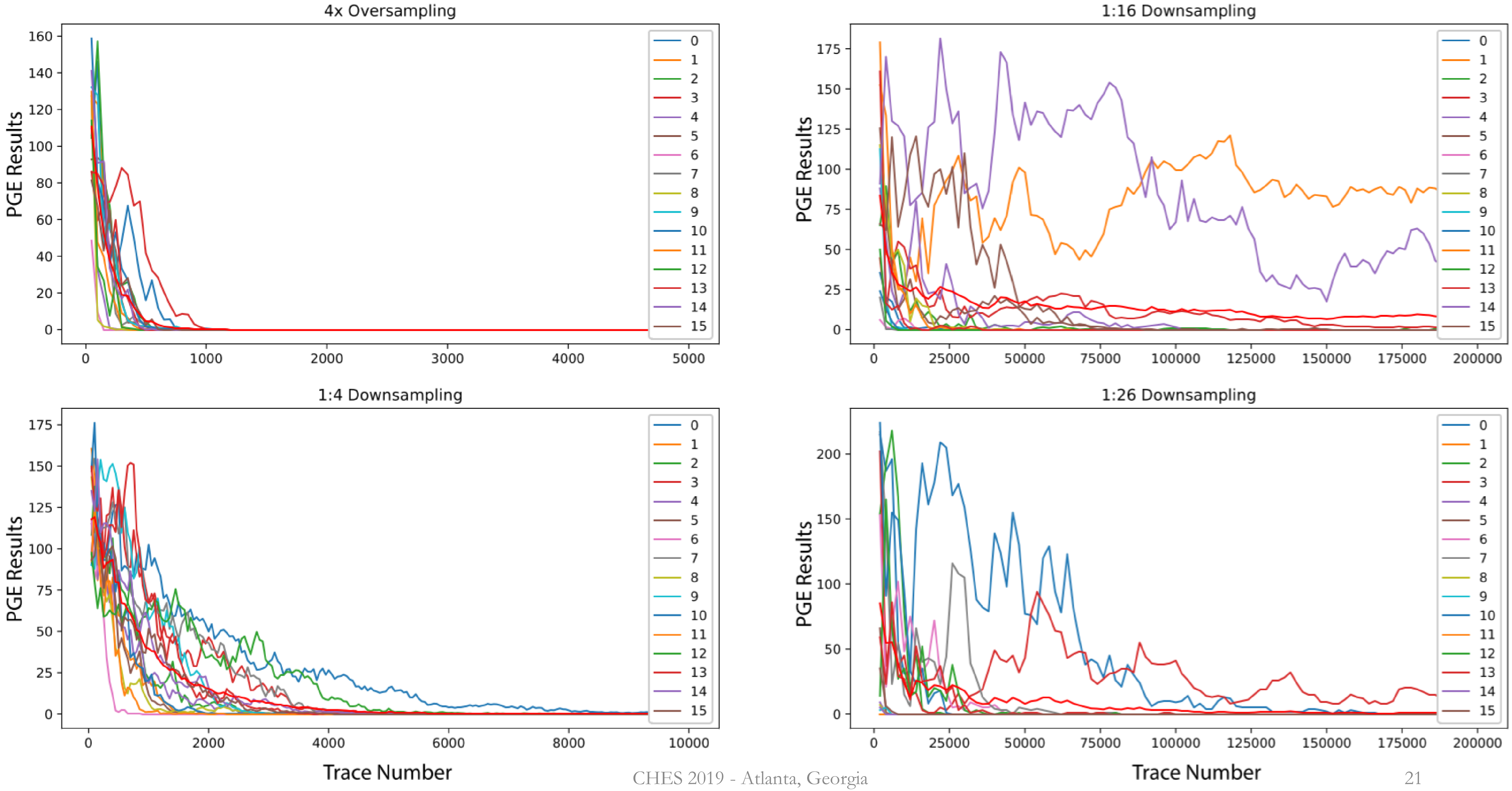


ADC clock (even when under sampling) is *still fully synchronous.*

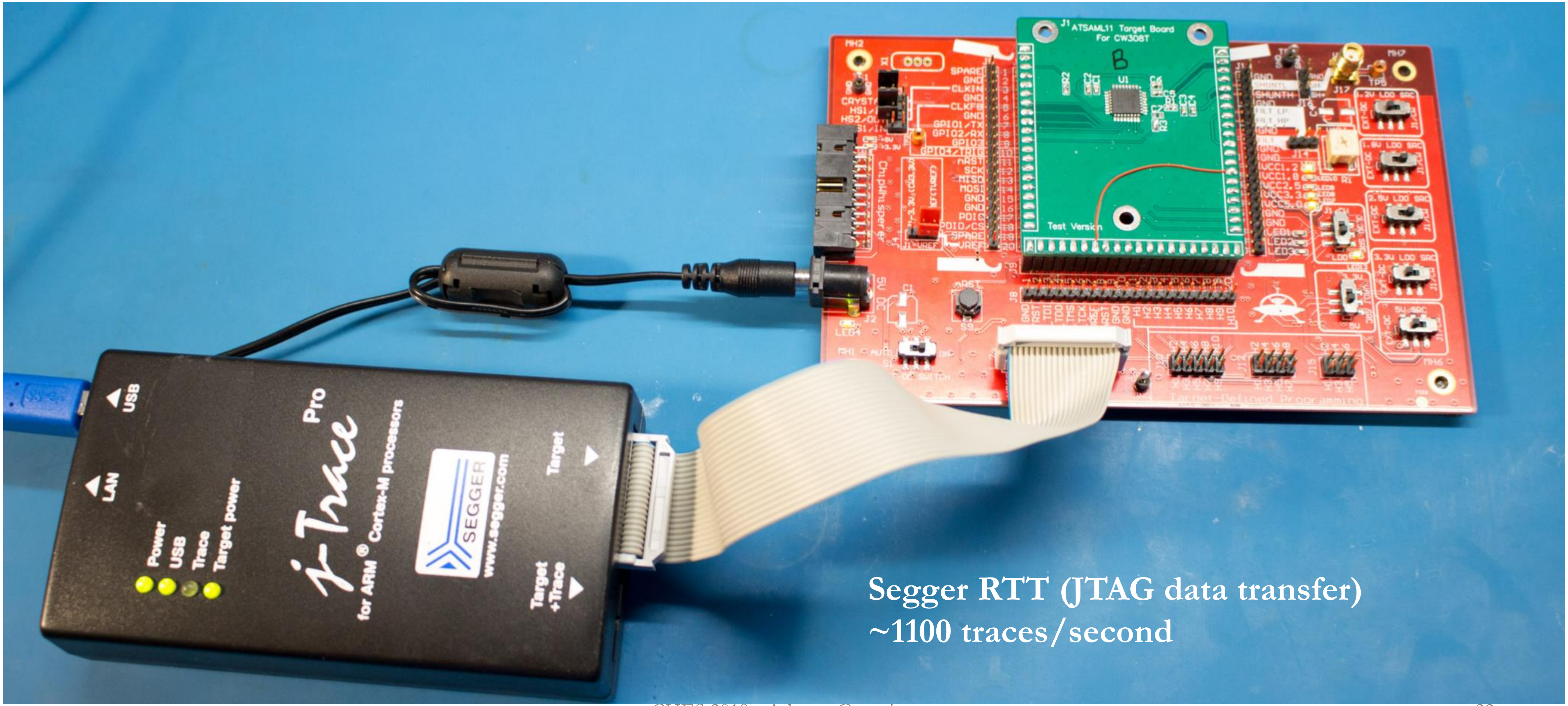
Sample point does not have time jitter relative to clock edge.

Similar sample rate measured without clock synchronization will have very substantial jitter due to minor frequency mismatches.

PGE Comparison for Reduced Sample Rate

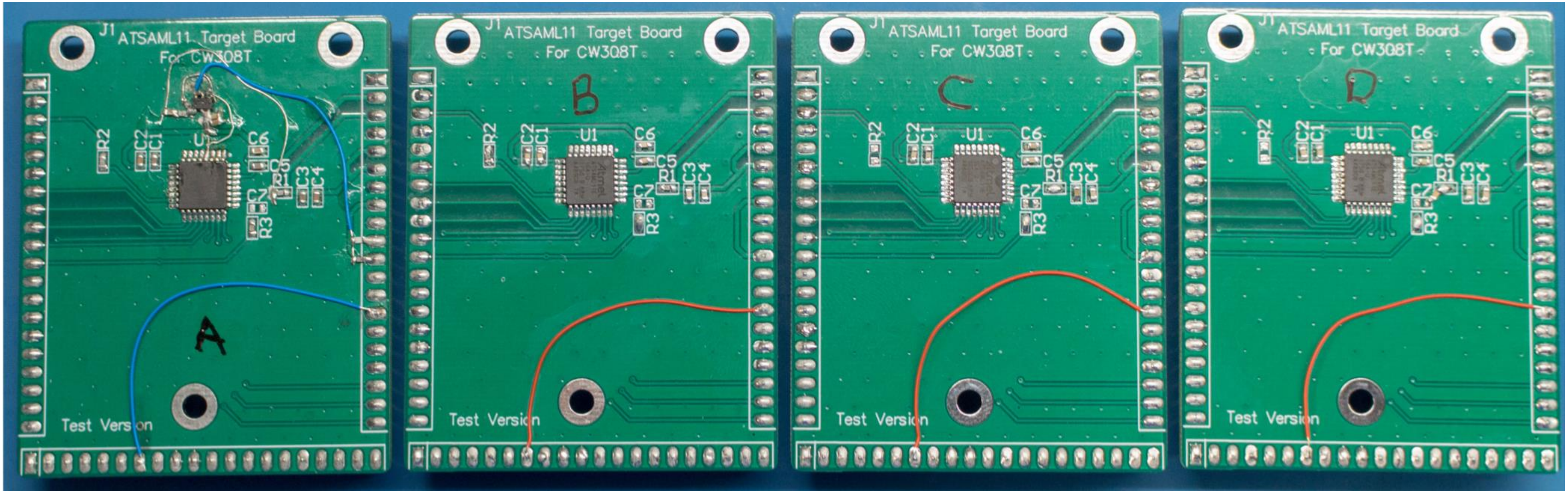


Part 2 – On-Board Attack



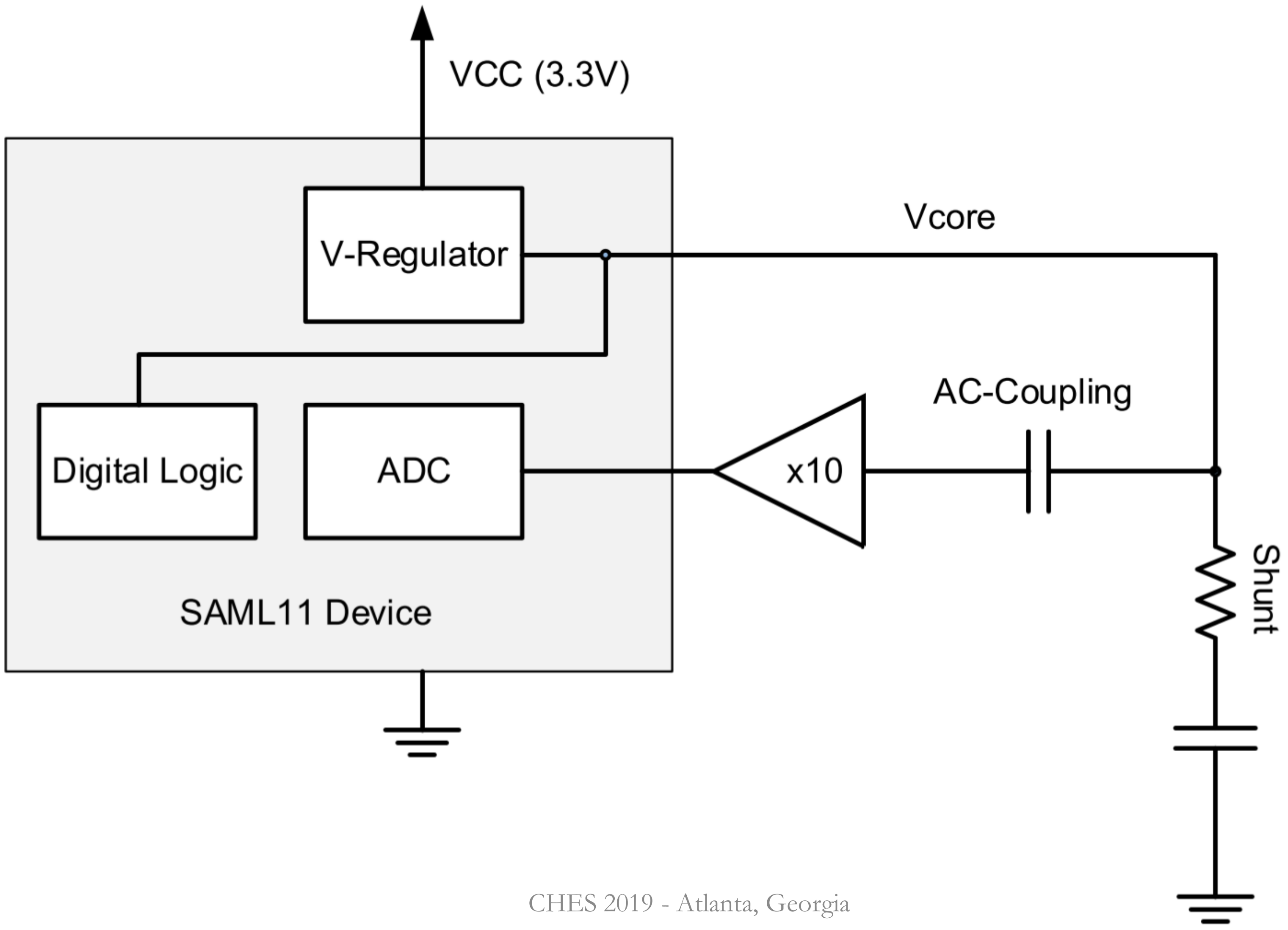
Segger RTT (JTAG data transfer)
~1100 traces/second

Test Boards

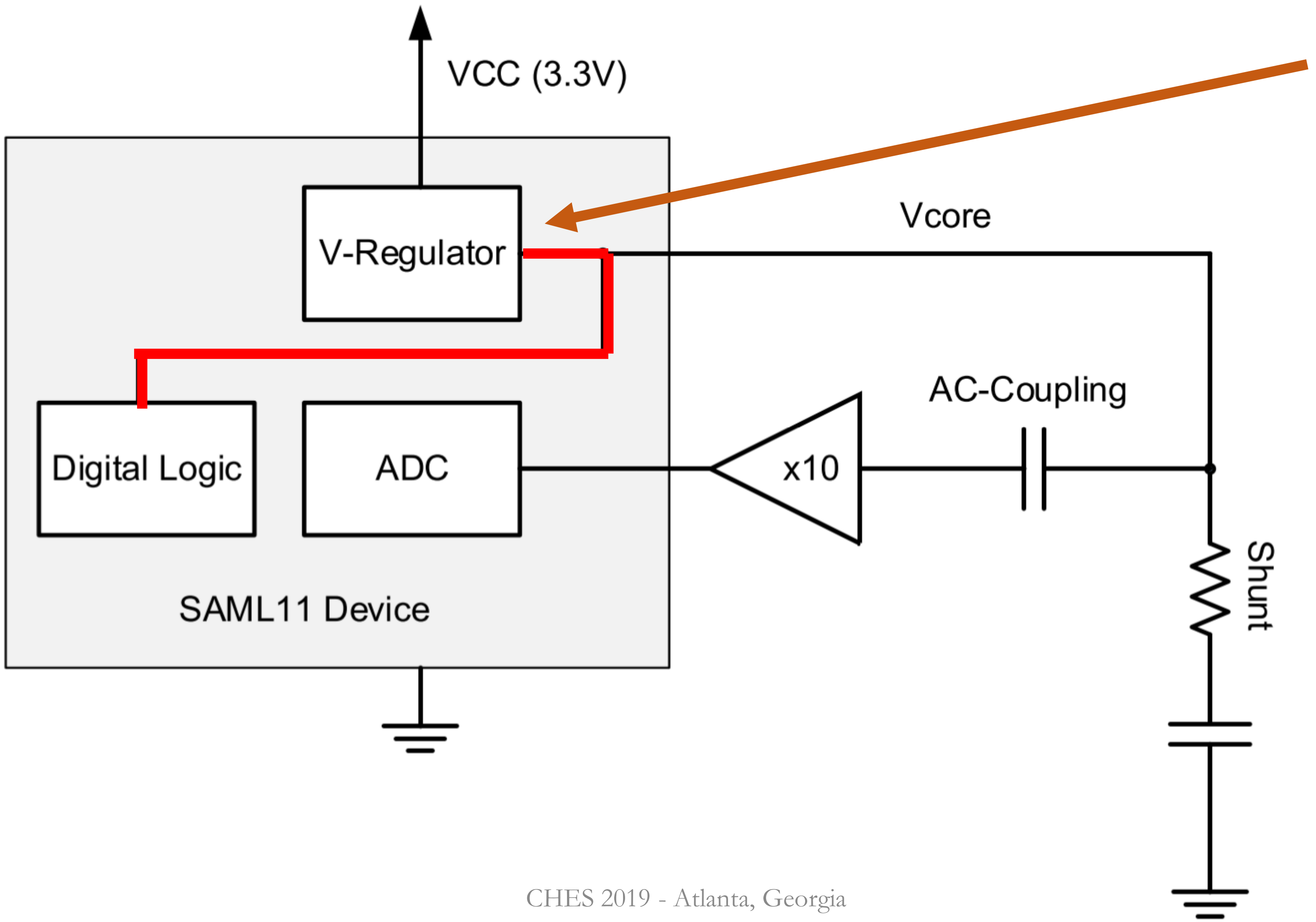


Expected reduction of SNR from A→D

Test A – Highest SNR

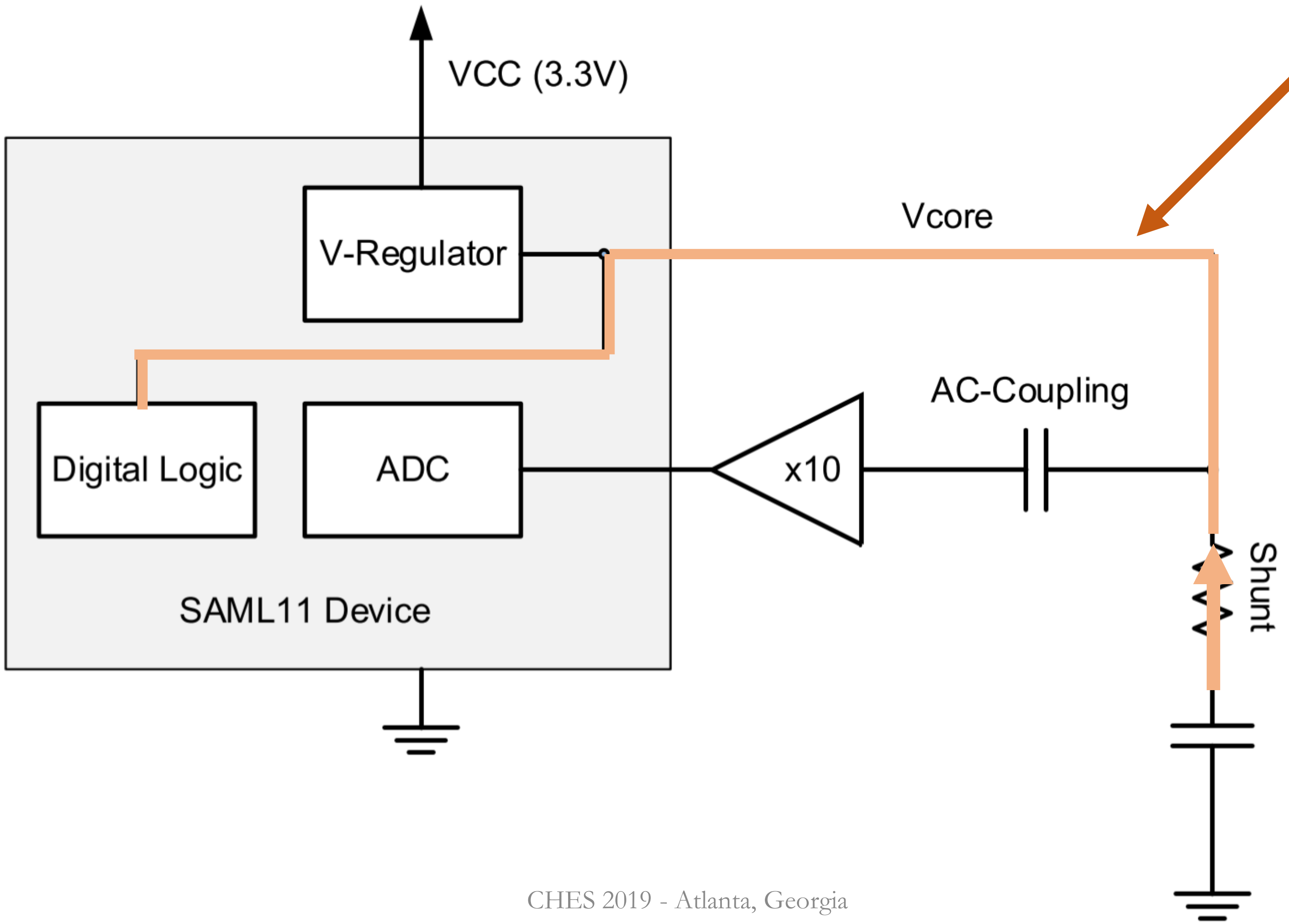


Sidenote about Internal Regulators



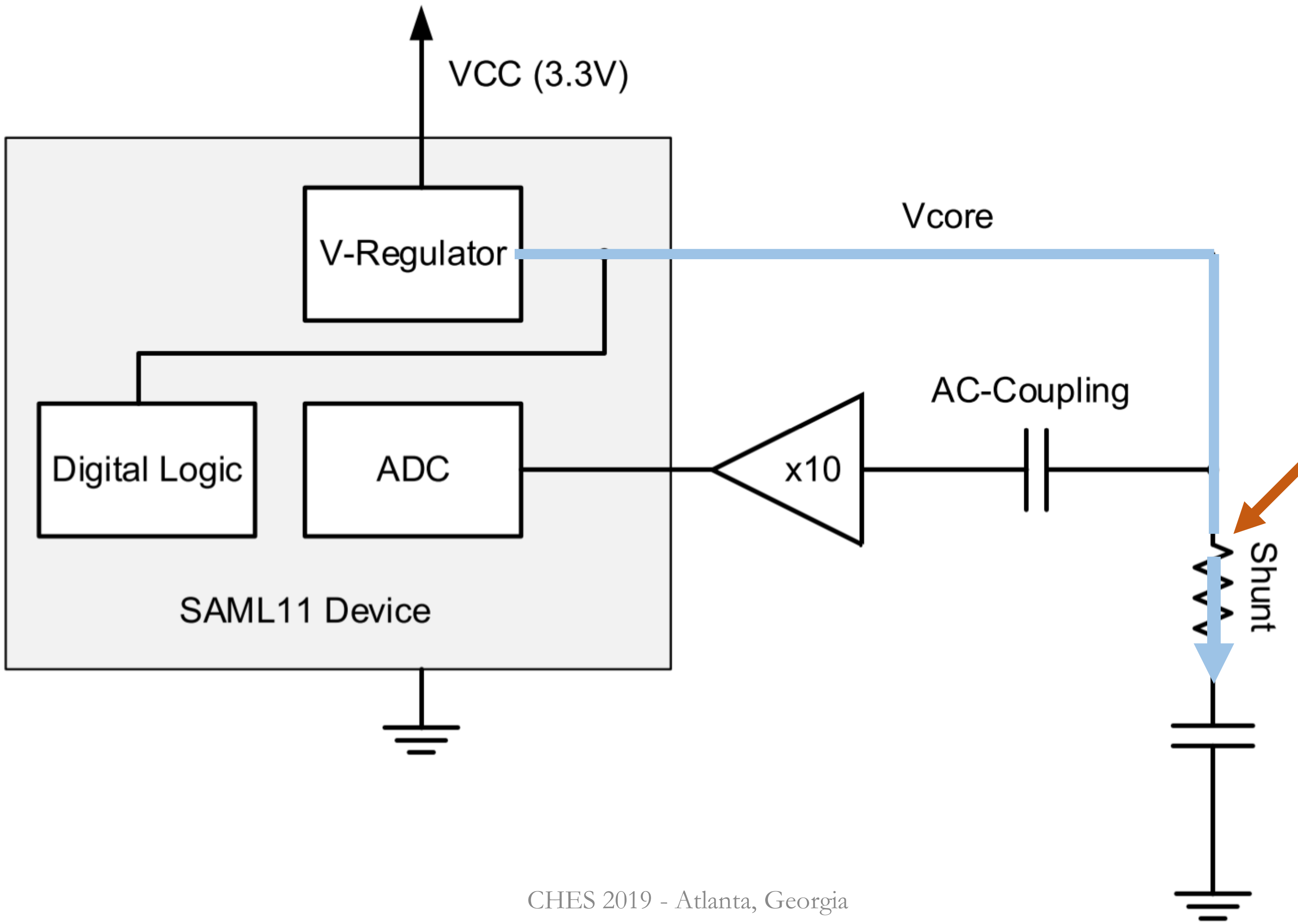
Does not react to fast transients, external decoupling capacitor required in most devices.

Sidenote about Internal Regulators

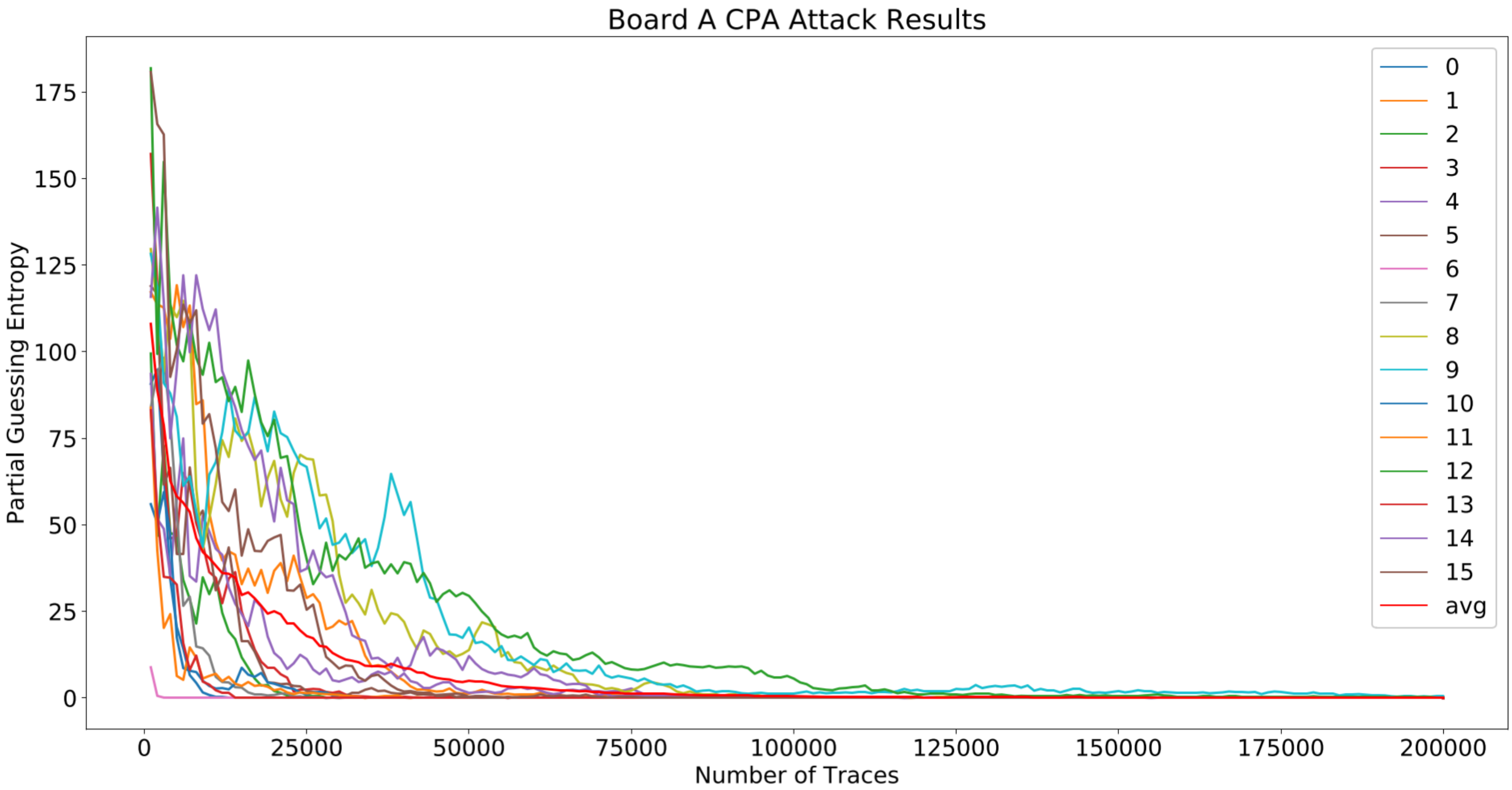


Majority of high-freq currents flowing from capacitor.

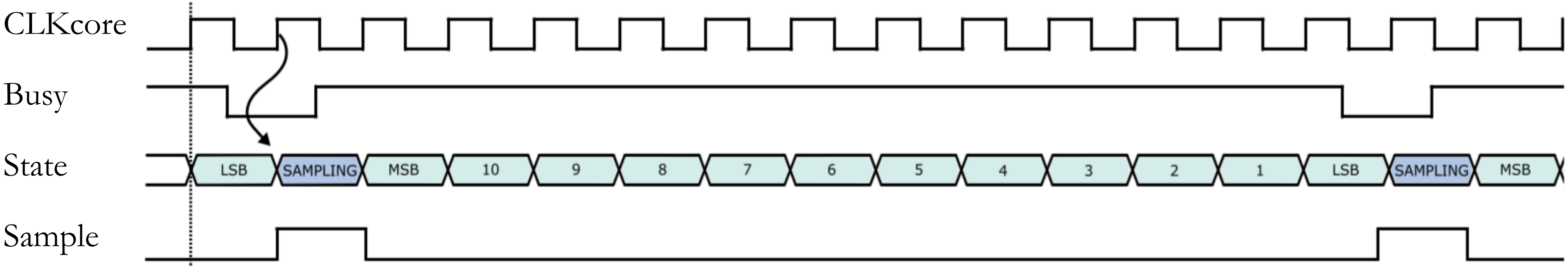
Sidenote about Internal Regulators



Regulator recharges capacitor (shows up as noise).


Board A CPA Attack Results
Partial Guessing Entropy
0
25
50
75
100
125
150
175
Number of Traces
0
25000
50000
75000
100000
125000
150000
175000
200000
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
avg

Clock Cycle Offset for AES to Measurement



Guessing Entropy & Cycle Offset

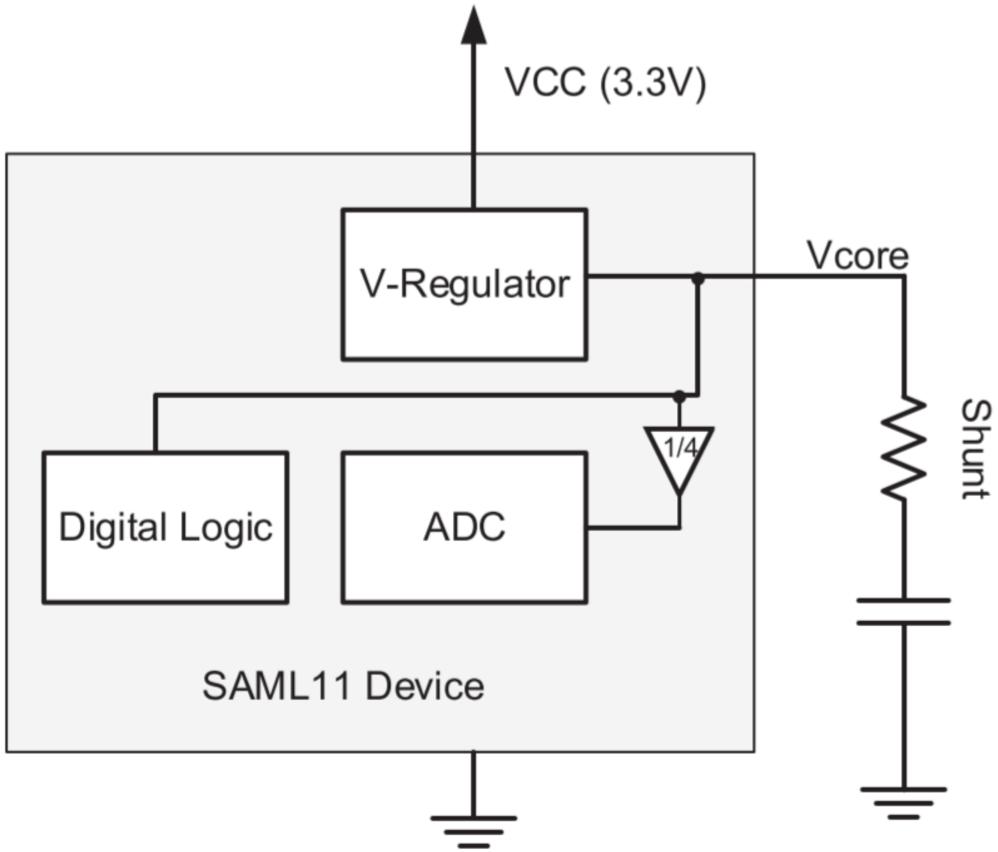
Cycle offset from AES call to start of sampling.

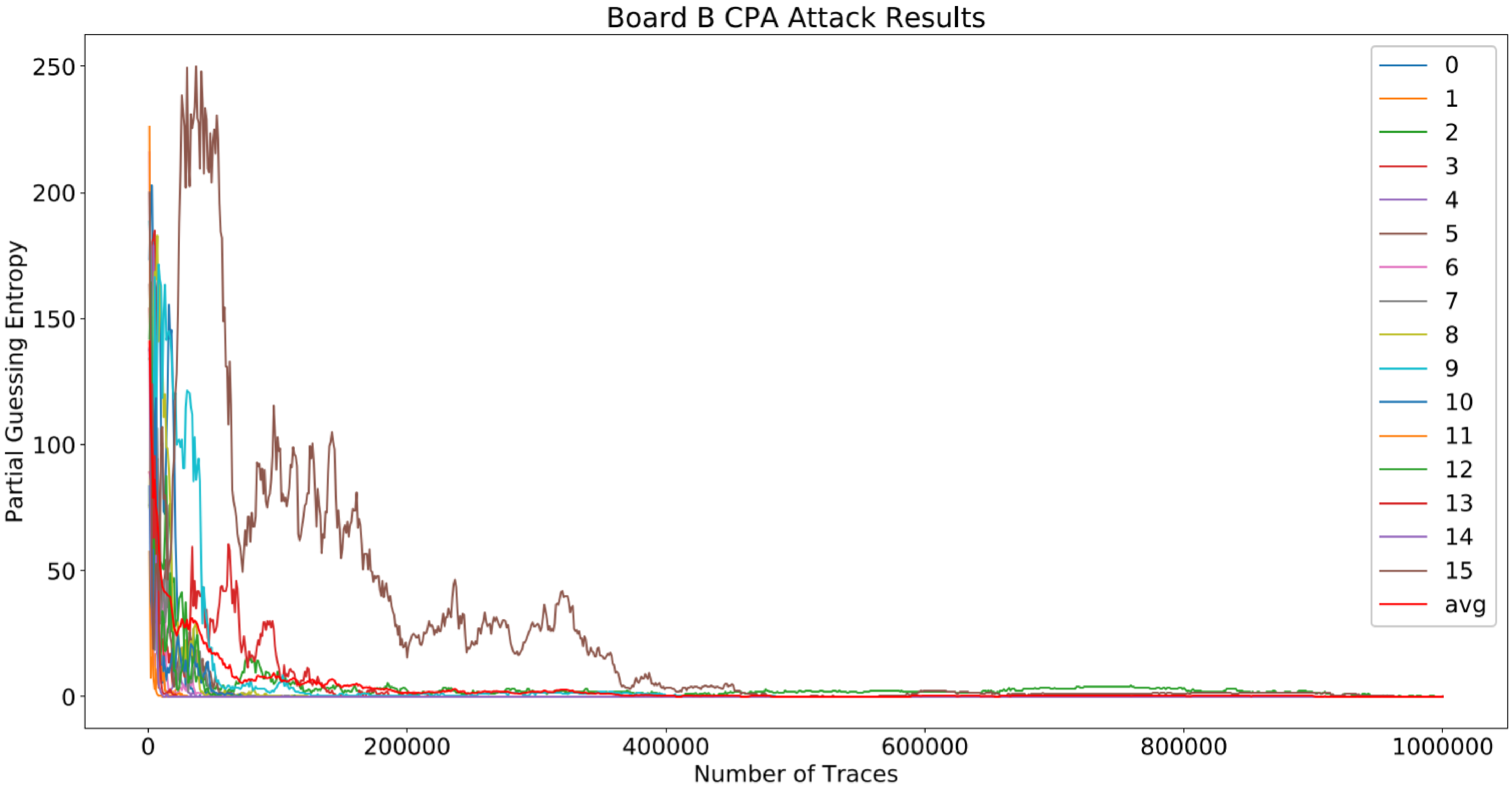
PGE of byte after 200K samples *(considering all output samples, not selecting best leakage points).*

Key Byte Targeted

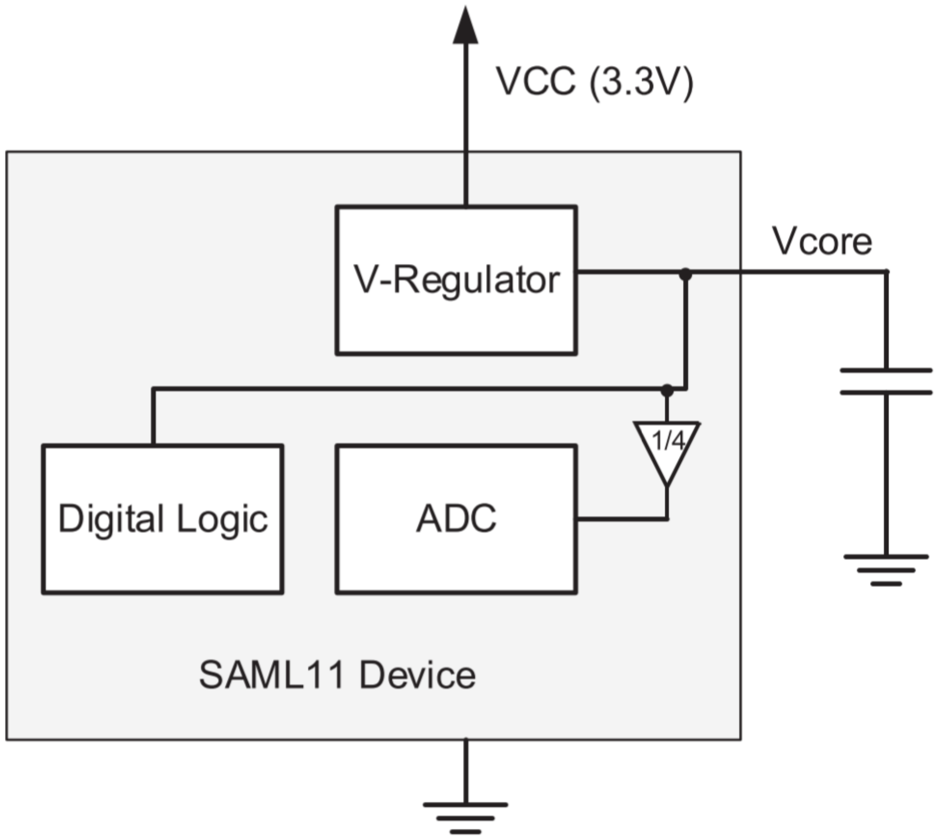
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
5	0.1	116.2	0.1	20.0	109.8	0.0	0.0	0.0	0.0	27.5	0.0	26.0	0.1	0.0	0.1	0.0
6	0.0	0.4	0.0	29.9	0.0	0.2	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
7	0.0	0.2	0.0	12.8	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
8	0.0	0.2	0.0	17.1	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
9	9.9	0.0	0.0	0.0	0.0	53.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1
10	61.5	0.0	10.4	30.5	0.0	40.1	0.0	0.0	0.0	32.6	0.0	0.0	0.0	0.0	0.0	0.0
11	3.4	0.0	0.0	82.1	0.0	0.0	0.0	31.1	0.0	61.5	2.1	0.0	0.0	3.6	0.0	0.0
12	1.1	2.1	0.8	0.0	7.8	83.0	0.0	5.6	0.0	0.0	0.1	3.6	0.0	10.9	6.6	0.0
13	0.8	3.5	0.0	0.0	0.0	174.9	0.0	47.8	0.0	0.0	3.5	0.0	0.0	5.2	0.6	0.0
14	0.1	0.4	0.0	0.0	0.0	179.2	0.0	33.2	0.0	0.0	1.2	0.5	0.0	20.4	0.2	0.0
15	0.0	0.0	0.0	0.0	38.9	20.8	0.0	0.1	0.0	0.0	0.9	7.6	115.1	10.9	49.9	0.0
16	102.1	0.0	0.0	0.0	0.0	0.0	0.0	99.2	0.0	8.2	152.6	0.0	0.0	45.2	0.0	0.9
17	0.0	0.0	0.2	33.4	0.0	124.4	0.0	0.0	0.0	68.9	0.0	0.0	77.4	0.2	0.0	0.0
18	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	3.5	0.2	0.0	0.0	10.9	0.0	0.4	0.0
19	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.2	2.5	2.2	7.2	0.0	37.0	0.2	0.0	0.2

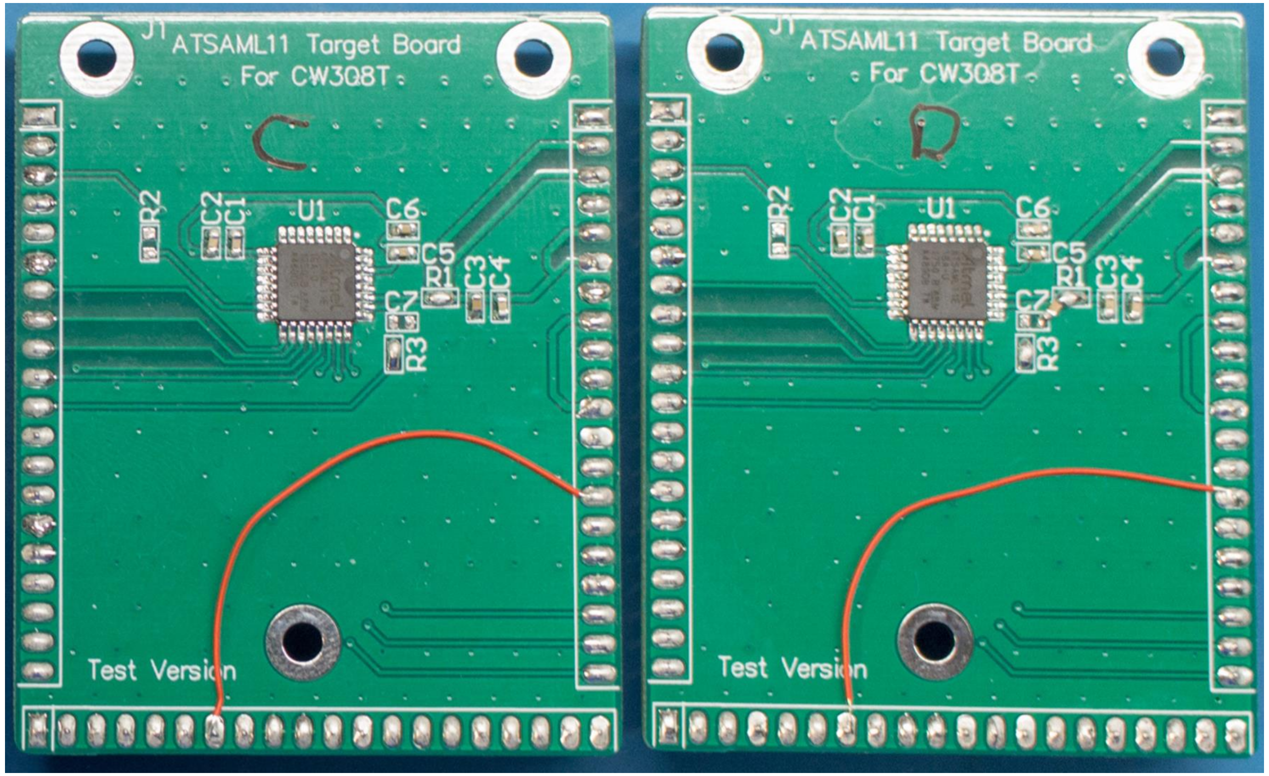
Board 'B'


VCC (3.3V)
V-Regulator
Vcore
1/4
Shunt
Digital Logic
ADC
SAML11 Device

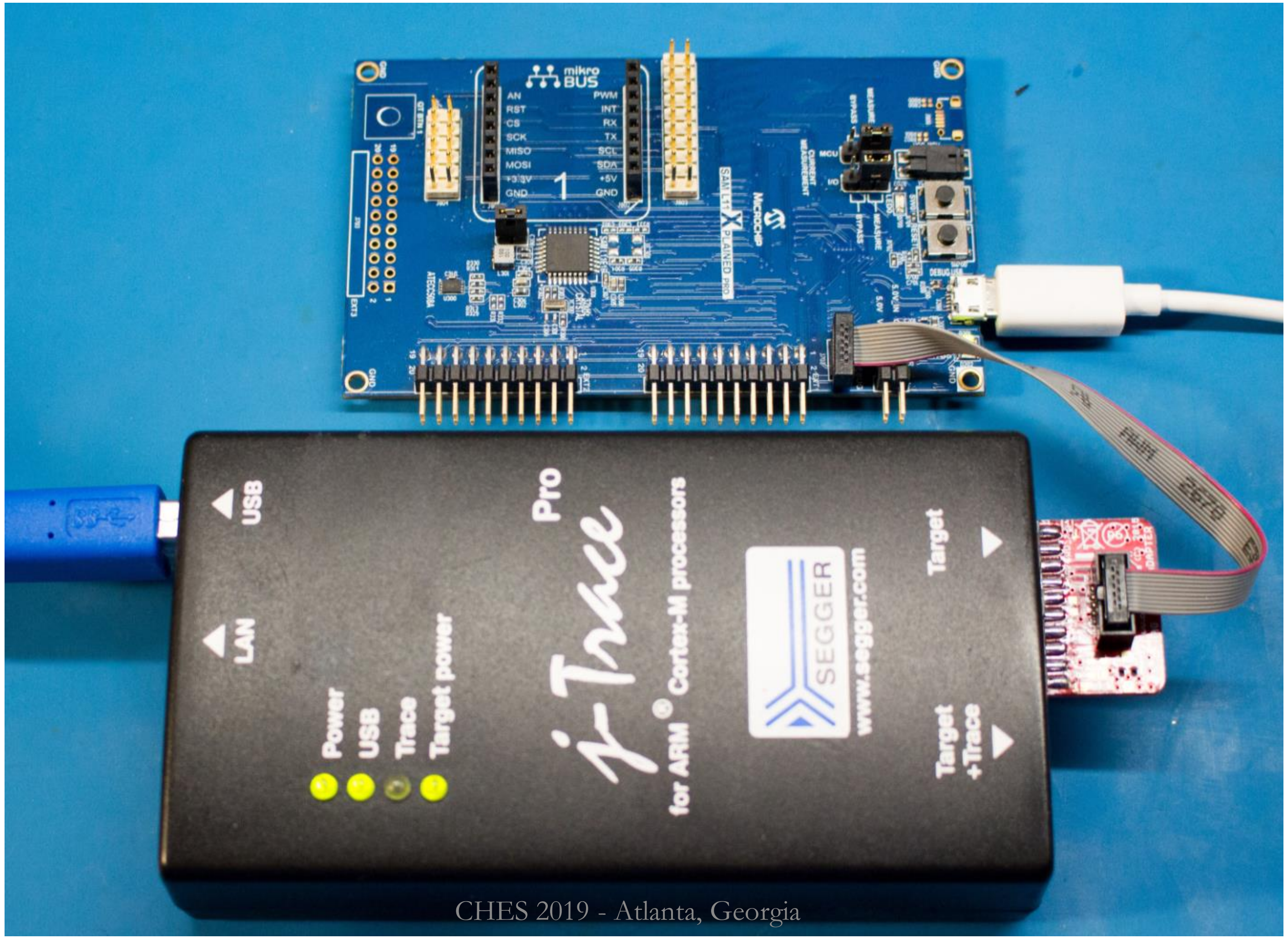

Board B CPA Attack Results
Partial Guessing Entropy
250
200
150
100
50
0
0
200000
400000
600000
800000
1000000
Number of Traces
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
avg

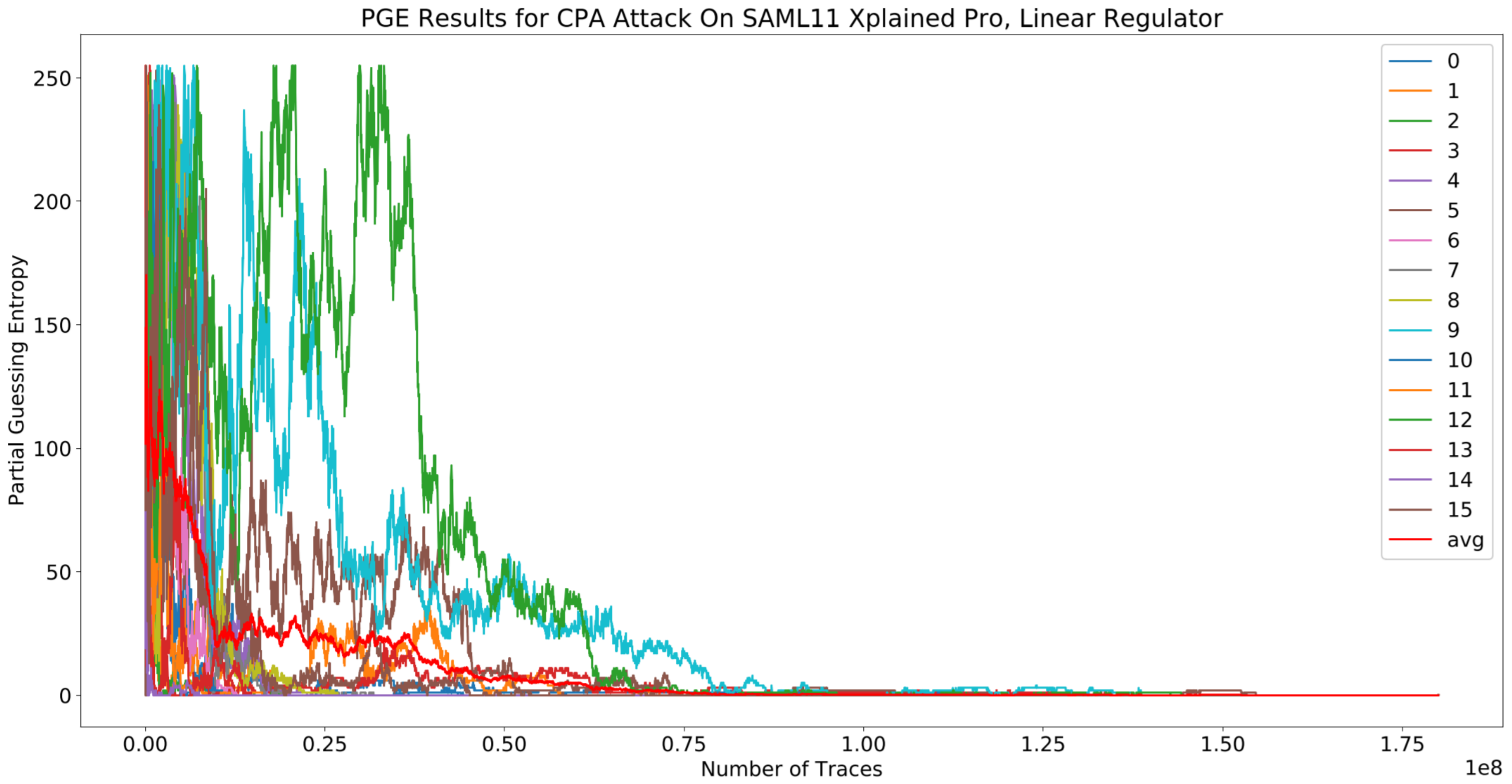
Board C/D → Dev Kit



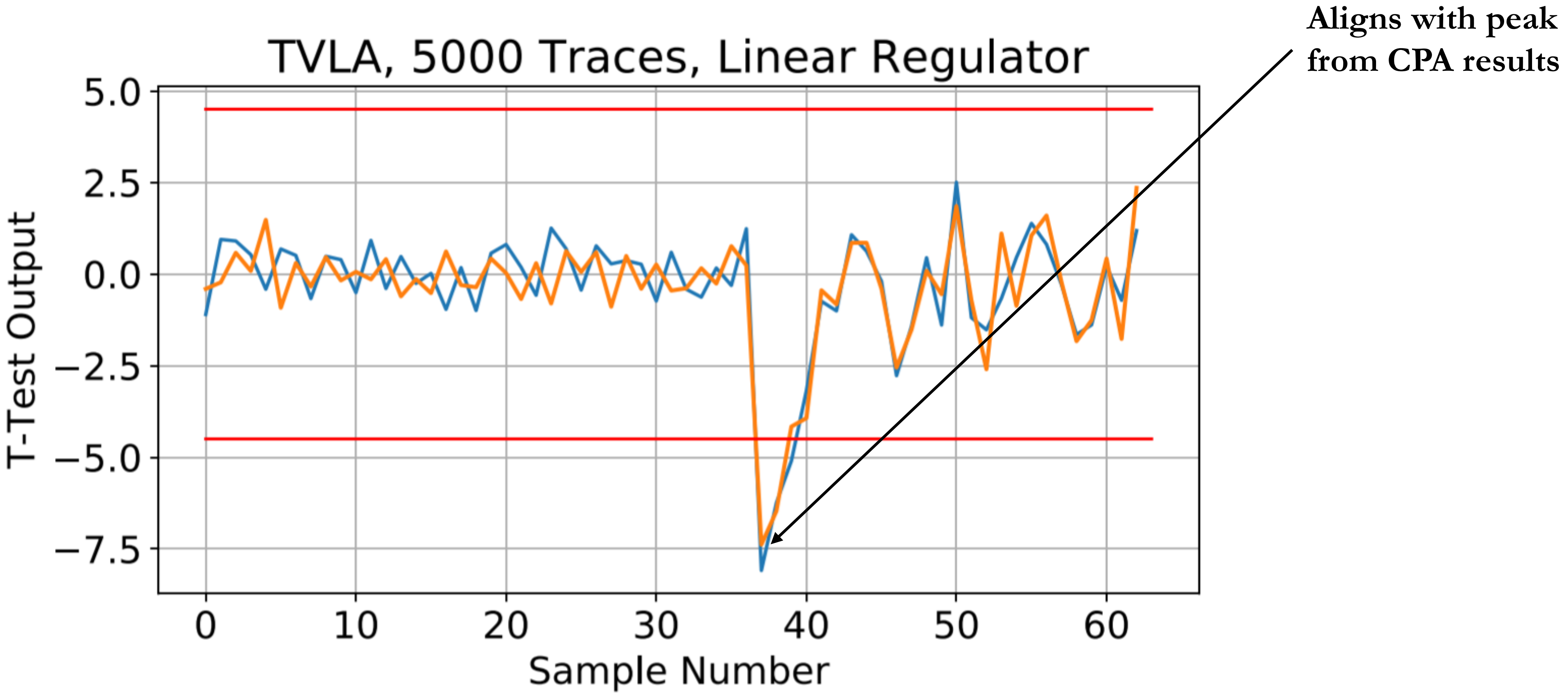


Part 3 - Development Kit Attack



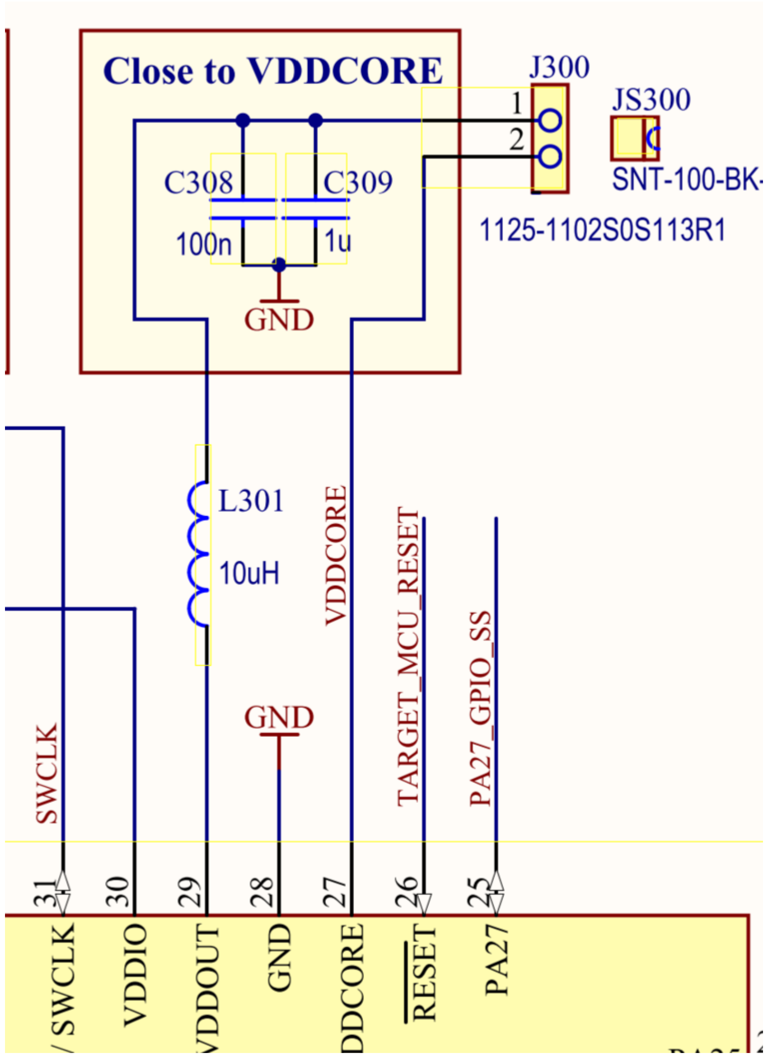

PGE Results for CPA Attack On SAML11 Xplained Pro, Linear Regulator
Partial Guessing Entropy
Number of Traces
1e8
0
50
100
150
200
250
0.00
0.25
0.50
0.75
1.00
1.25
1.50
1.75
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
avg

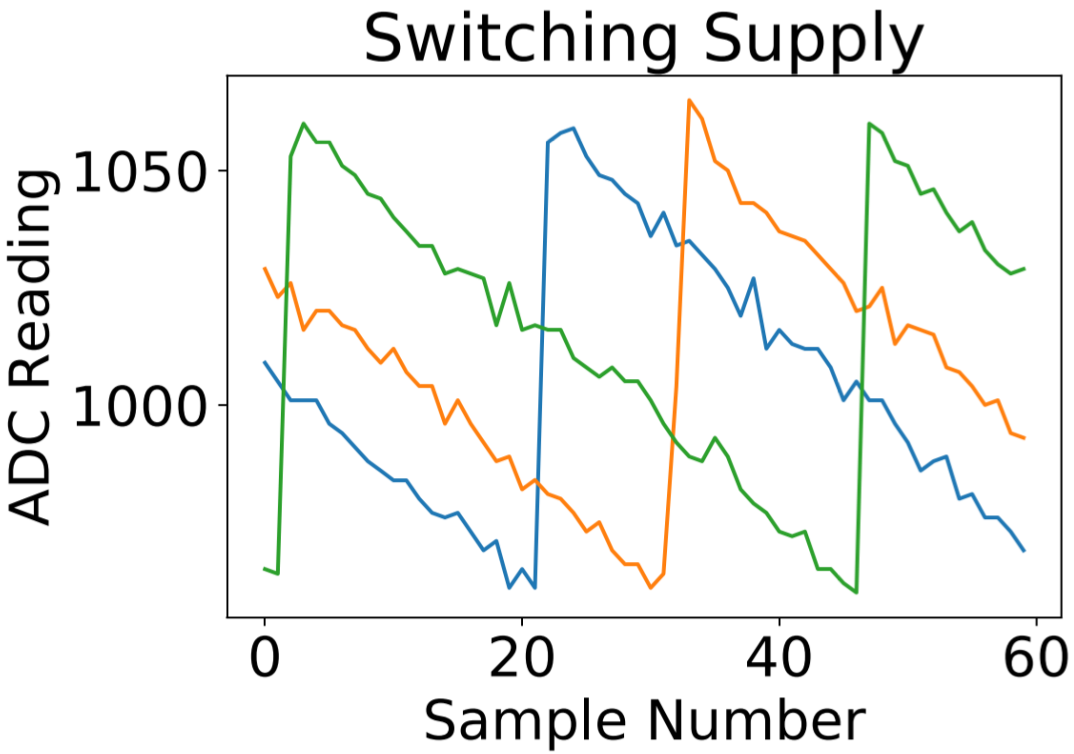
Finding Leakage – TVLA Testing



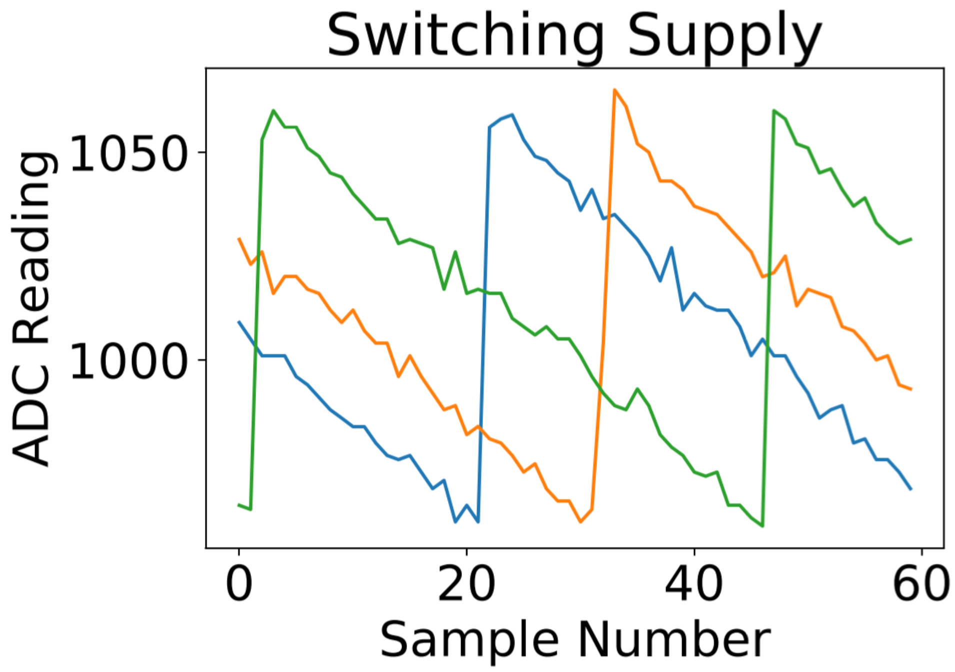
Caveat: Due to strong down-sampling, hard to focus T-Test on middle 1/3 of AES only

Switching Power Supply Mode

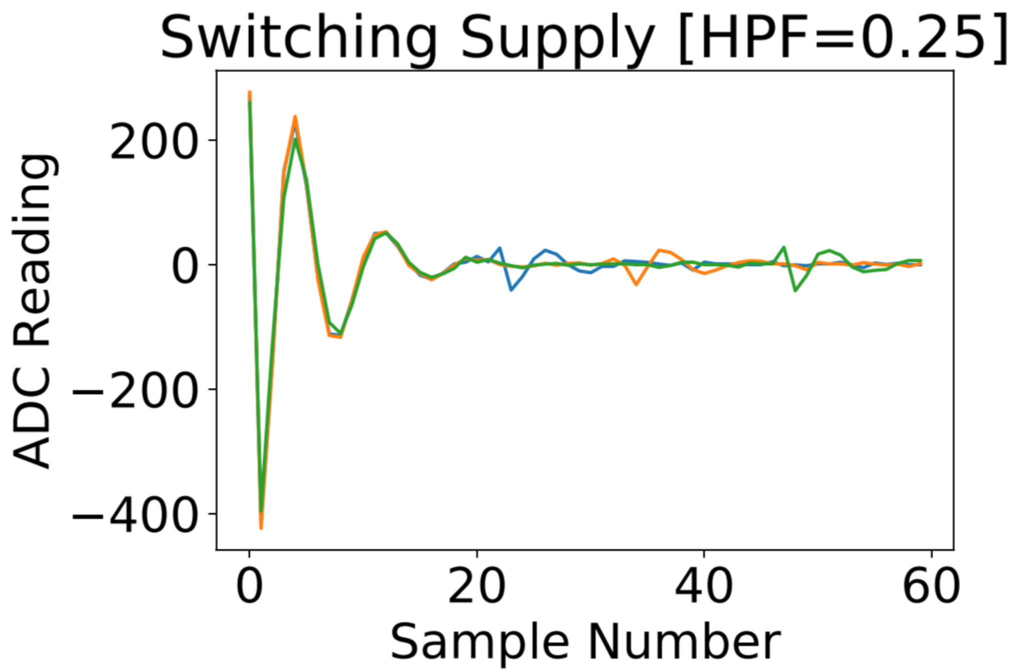




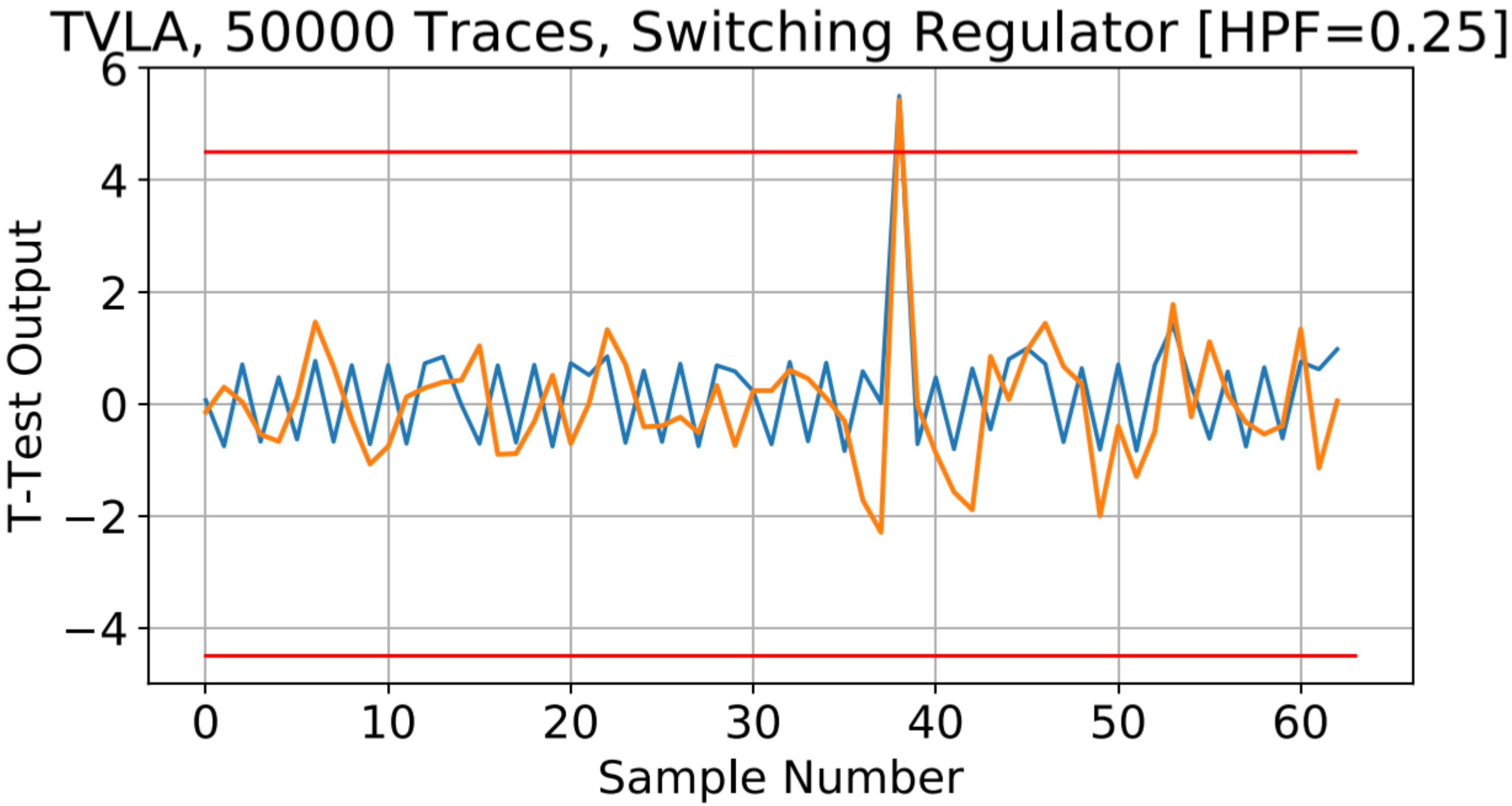
Switching Power Supply Mode

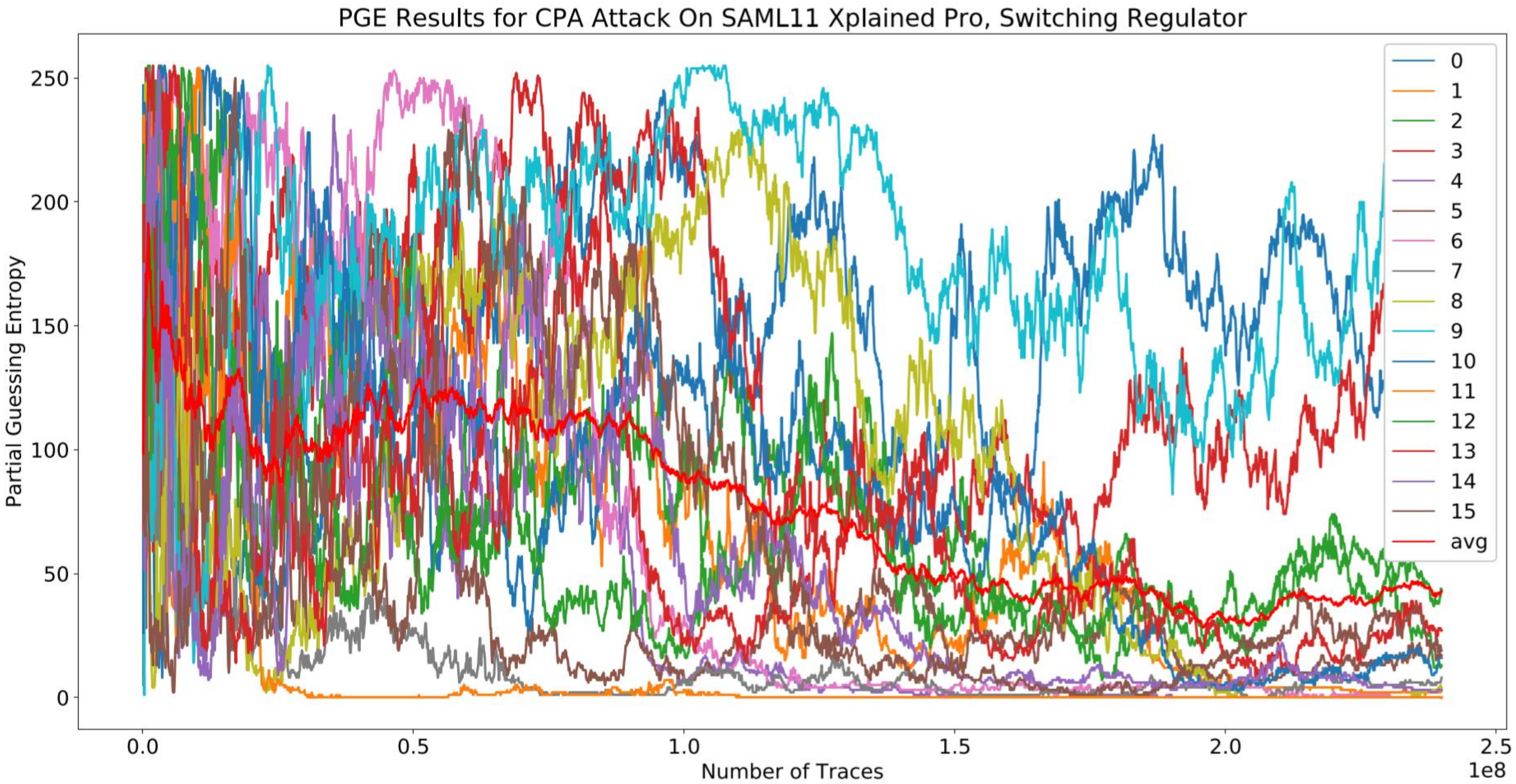


High Pass Filter



TVLA of Switching Regulator




PGE Results for CPA Attack On SAML11 Xplained Pro, Switching Regulator
Partial Guessing Entropy
Number of Traces
1e8
0
50
100
150
200
250
0.0
0.5
1.0
1.5
2.0
2.5
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
avg

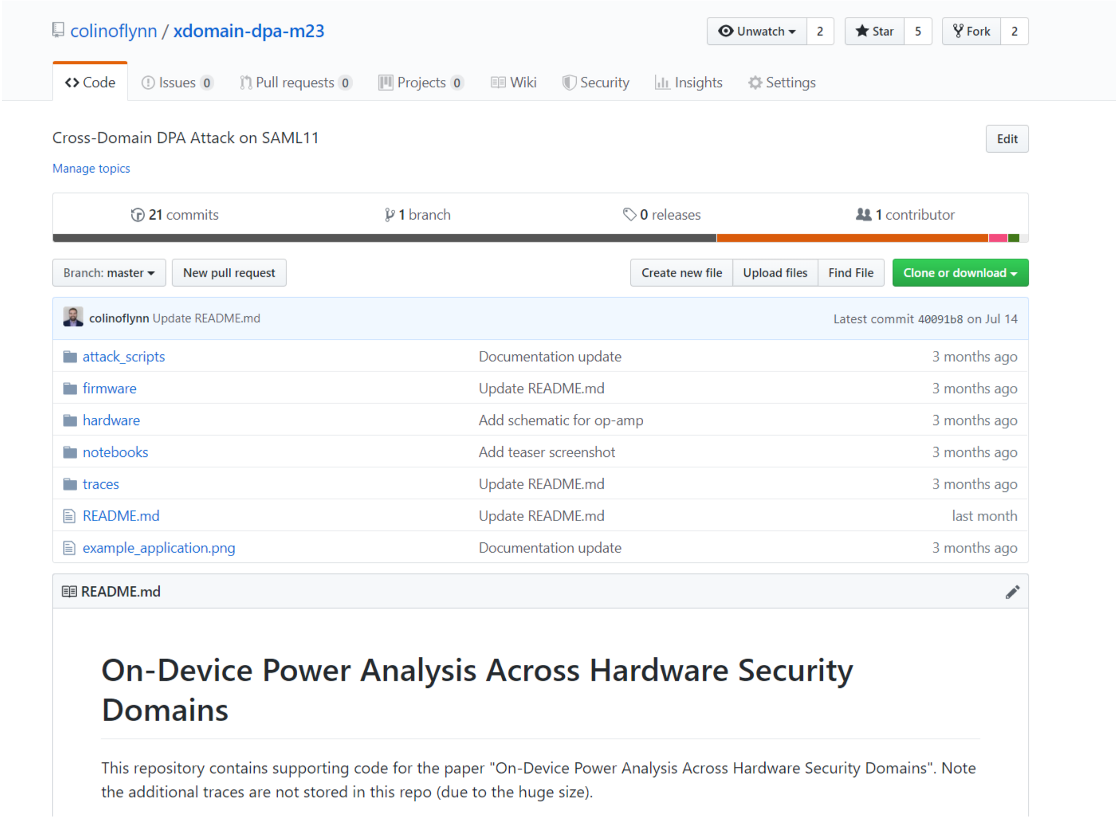
Cross-Domain Attacks

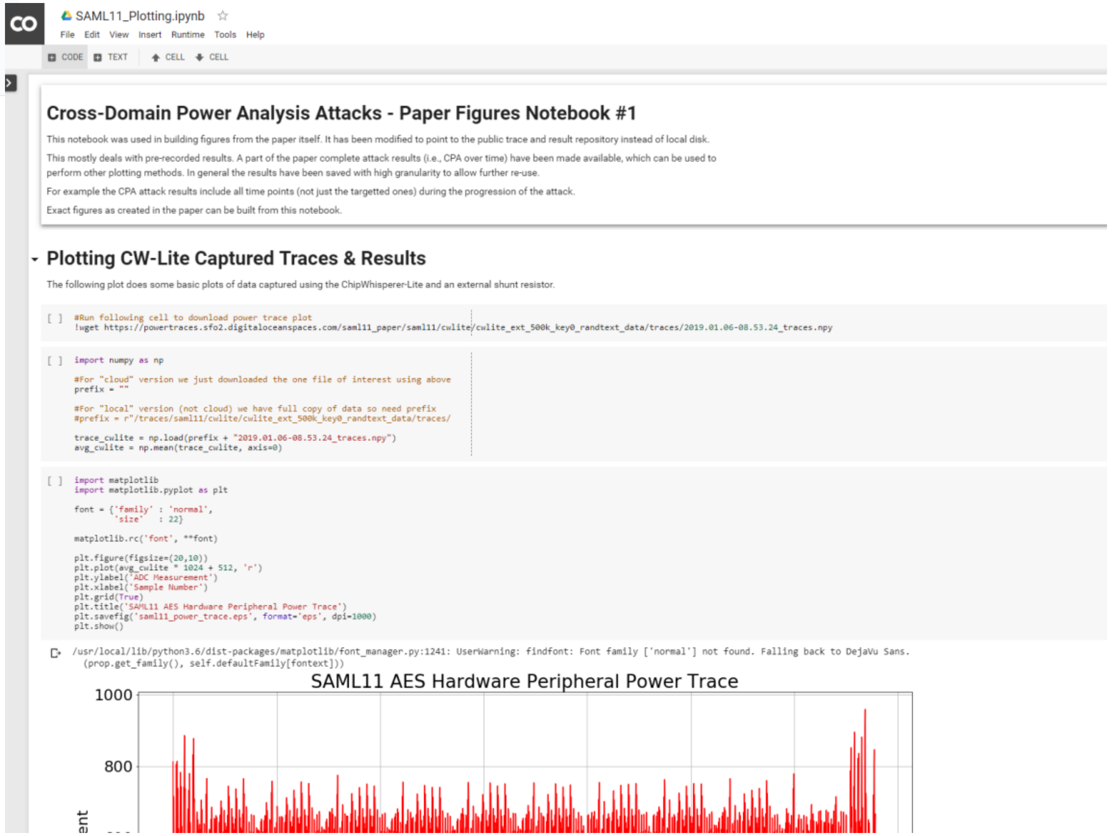
- Cross-domain attack uses availability of peripherals in non-secure world to attack secure world.
- A remote exploit in non-secure world could be used to recover data from secure world.
- Requires lots of data (~160 000 000 traces, 5GB).
  - Is ‘remote’ plausible → Not convinced.
  - Is ‘nearby’ plausible → Yes.

- Countermeasures include:
  - Moving peripherals to secure world (caveat – we don’t want some libs in non-secure).
  - Validating environment (caveat – secure code cannot touch non-secure).

Availability of Datasets, Code, Etc

https://github.com/colinoflynn/xdomain-dpa-m23





- **520M+** trace sets
- **285GB** of data files…

Thank-You and Questions

https://github.com/colinoflynn/xdomain-dpa-m23

Email: colin@oflynn.com (Colin) adewar@dal.ca (Alex)
Twitter: @colinoflynn

Thank you to many reviews & notes from those that wished to remain anonymous.