Pre-Silicon Modeling of a Secure ADC for Treaty Verification

CVT – Consortium for Verification Technology

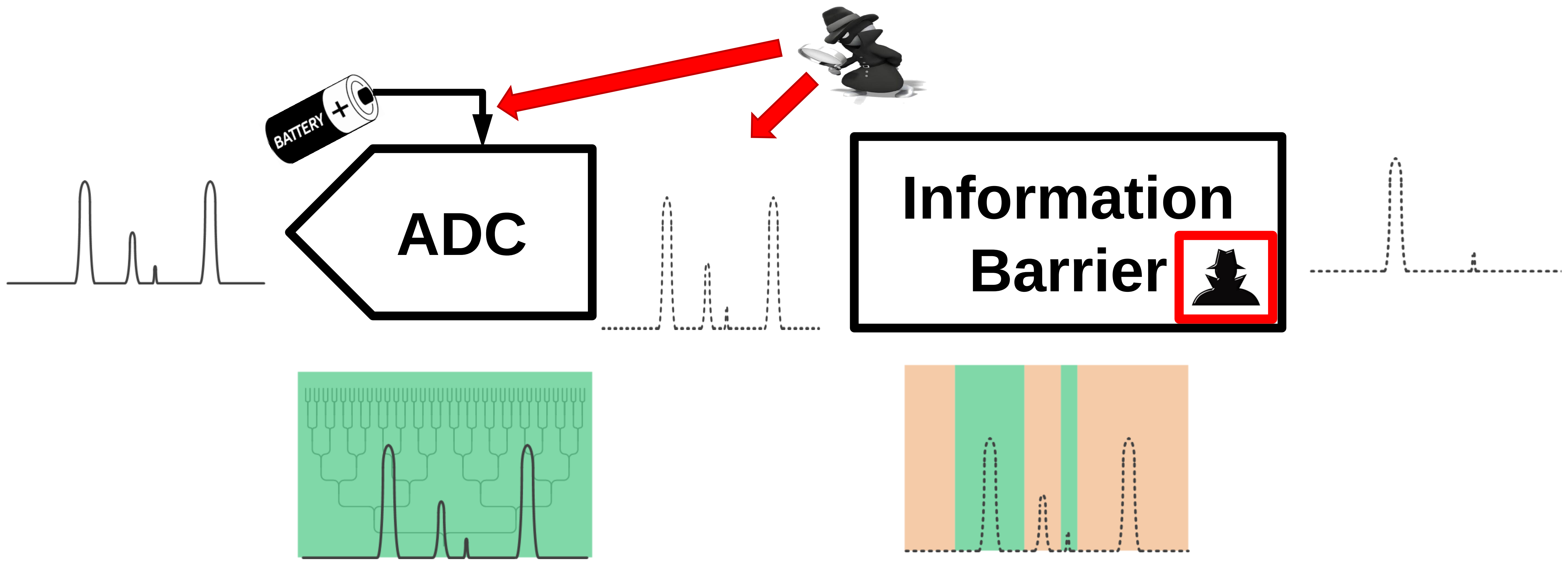
Fred Buhler, Prof. M. Flynn, Prof. D. Wehe

Background: Treaty Verification

For treaty verification, both parties must agree on a measurement protocol that provides adequate assurance that treaty obligations are met, but without yielding sensitive information.

- Past approaches include digitizing entire spectrums, including (including the sensitive information) followed by data-barriers and post-processing to remove the sensitive information.
- This work investigates electronic measurement techniques that only digitize the agreed upon spectrum, removing the possibility of sensitive information leakage.

Current Systems: Untrusted Observers & Side-Attacks



- Software and FPGA information barriers are hackable
- ADC interface can be monitored
- Power changes are proportional to ADC conversion

Two stage SAR ADC archetecture

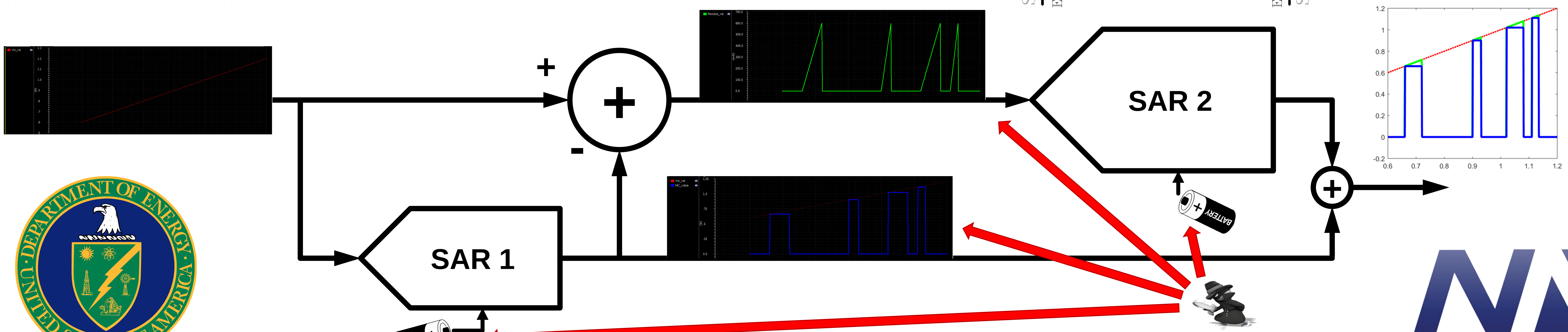
- First stage only detects if input is within an agreeed upon spectrum
- Error amplifier limited to desired window
- Second stage digitizes the error

Untrusted Observers & Side-Attacks

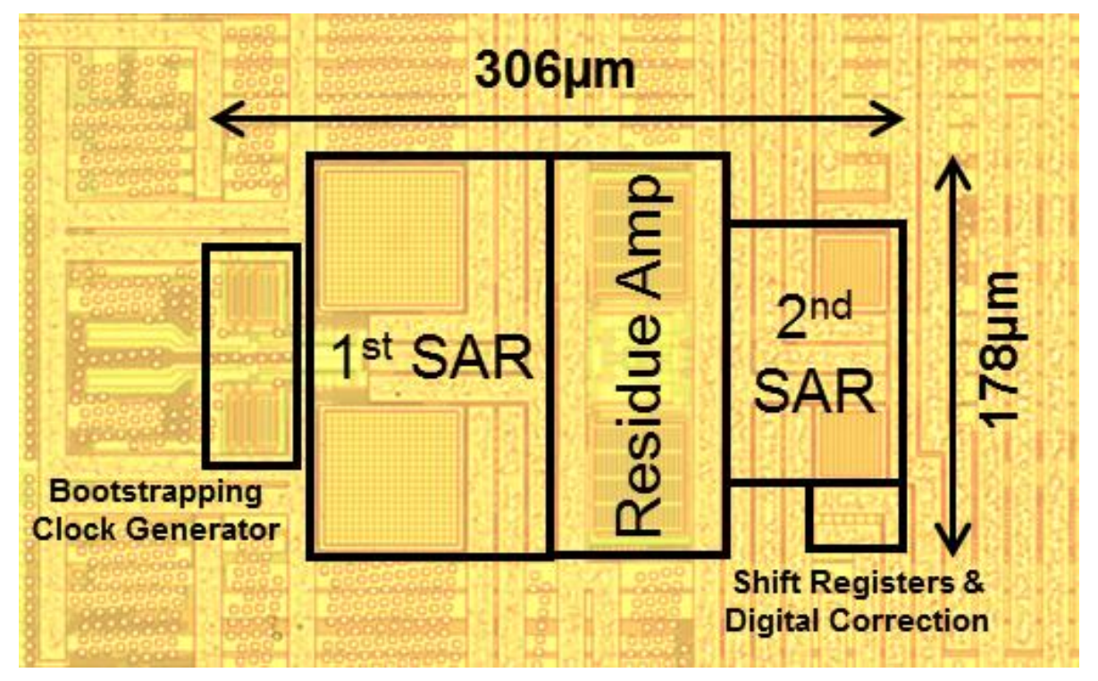
- Untrusted Observer Immunity: Each stage is physically (capacitor size) and electrically (saturation) limited to the agreed upon spectrum
- Side Attack Immunity: SAR decision tree removes power supply correlation with ADC code

Proposed System

LOGIC
DAC_TEST_LOGIC
stupid_SRAM
MC CDAC
MC_ADC
ideal_MC_DAC
Comparator
comparator_ideal
Stage 1
Error Amp
Residue Amp
residueAmp_ideal
Error Amp
Stage 2
CDAC 2
Comparator



Untrusted Observer Learns Nothing


306µm
1st SAR
Residue Amp
2nd SAR
178µm
Bootstrapping Clock Generator
Shift Registers & Digital Correction

National Nuclear Security Administration