UMassAmherst
The Commonwealth's Flagship Campus

Combining Clock and Voltage Noise Countermeasures against Power Side-Channel Analysis

Jacqueline Lagasse, Christopher Bartoli,
and Wayne Burleson

July 16, 2019

Motivation

- Power side-channel attacks continue to be a major vulnerability for many critical systems, typically by exposing the key of an encryption module
- Many existing countermeasures are highly invasive, can potentially introduce other vulnerabilities, can not use standard IP blocks
- Small devices cannot tolerate large overheads for existing side-channel countermeasures

Objectives

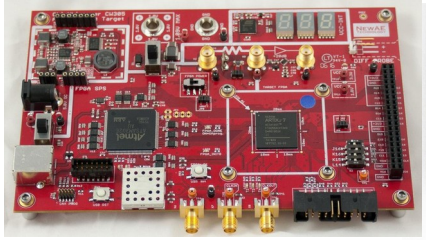

Fig. 1: CW305 Target Board

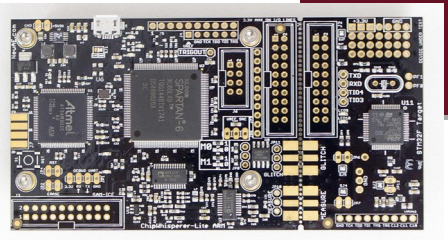

Fig. 2: CW1173 Capture Board

- Combine existing non-invasive countermeasures to produce a countermeasure that is more effective than the sum of its parts
  - Voltage Noise (VN)
    - Shift Register LUT (SRL)
    - Linear Feedback Shift Register (LFSR)
  - Clock Randomization (CR)
- Use AES-128 as encryption module on state-of-the-art ChipWhisperer® FPGA boards

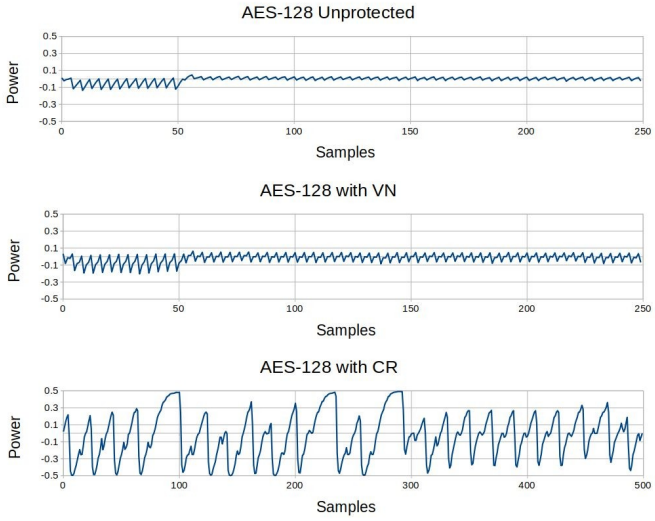

Fig. 3: Power traces of AES alone and with countermeasures

Design

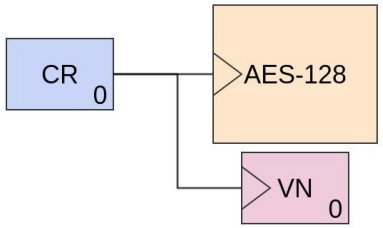

Fig. 4: Combining CR and VN

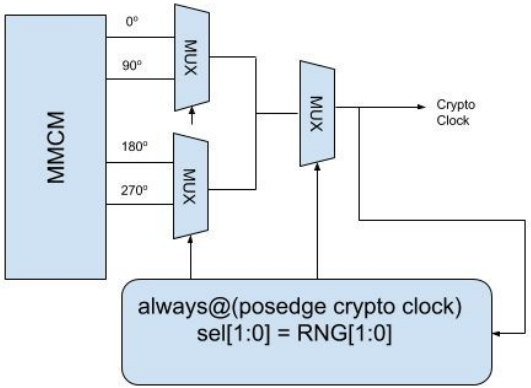

Fig. 5: Clock Randomization (CR)

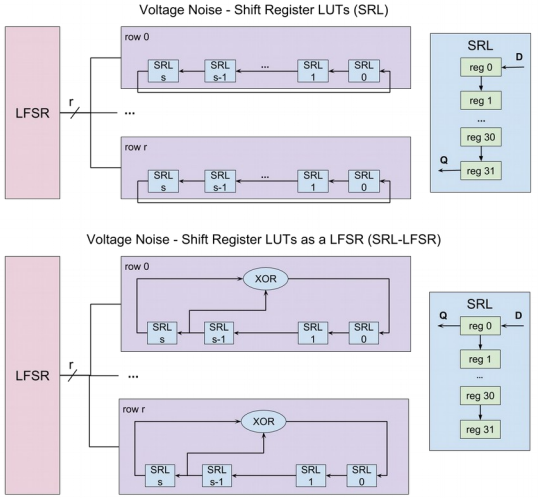

Fig. 6: Voltage Noise (VN)

- VN is a noisy circuit; SRL pushes seeded values through shift registers in rings, SRL-LFSR arranges rings of shift registers as LFSR; both use random number generator (RNG) to select which rings are currently enabled
- CR creates multiple phase shifted clocks, RNG used to select which phase is current output of clock; adds delay and trace misalignment
- Combine by feeding output of CR into VN, now AES and VN are misaligned

Experiment

- Correlation Power Analysis (CPA) computes correlation between each possible byte and captured power trace over many traces
- Measure Partial Guessing Entropy (PGE), ranking of key guesses by correlation
- Sliding Window (SW) preprocessing attack can be used before CPA to realign traces misaligned by CR countermeasure

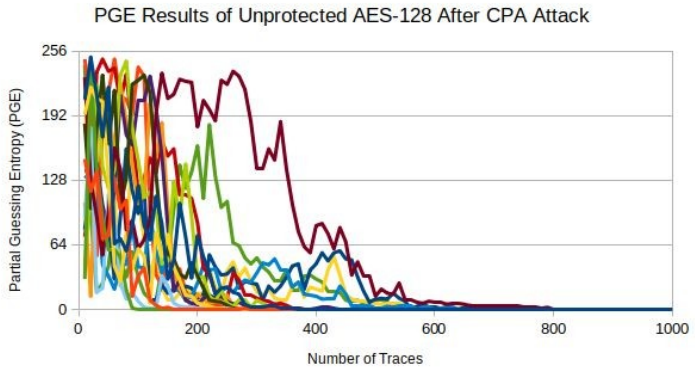

Fig. 7: Partial Guessing Entropy (PGE)

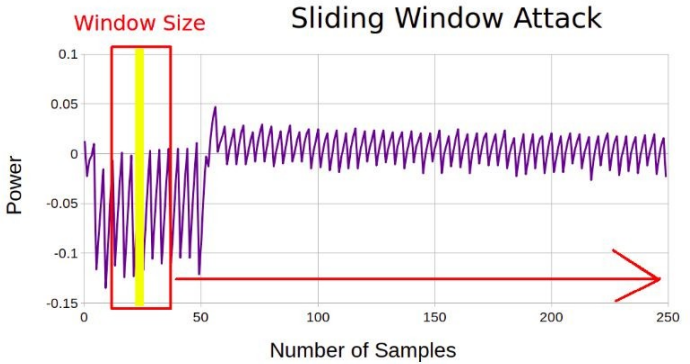

Fig. 8: Sliding Window (SW) Preprocessing

Results

- VN protects ~1k traces vs CPA solo
- CR protects ~300k traces vs CPA solo
- Compared to CR alone, combining increases protection against CPA by 71% and 48%, CPA-SW by 63% and 61% for SRL and SRL-LFSR respectively

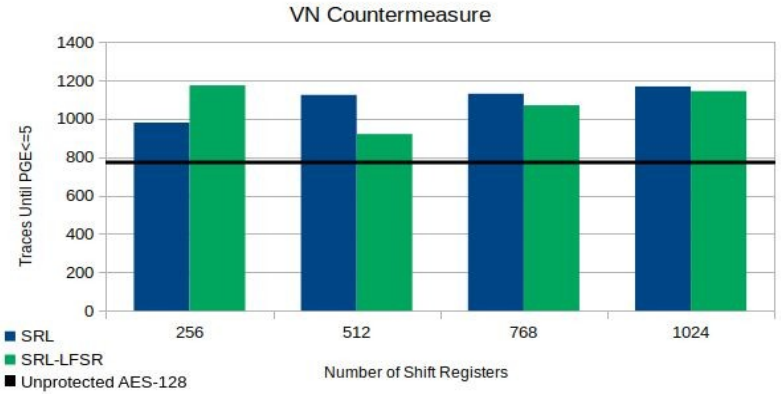

Fig. 10: VR Results

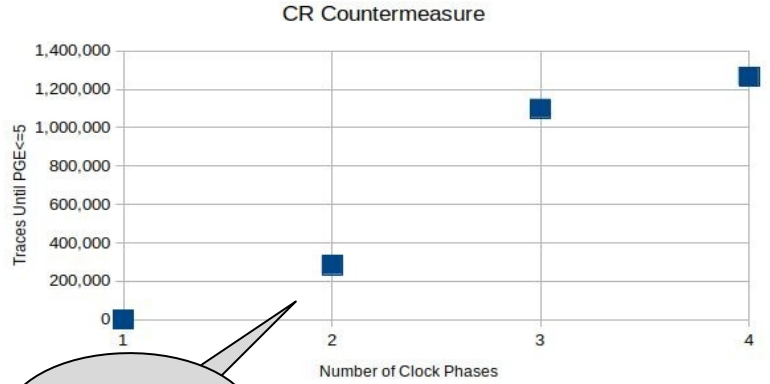

Fig. 9: CR Results

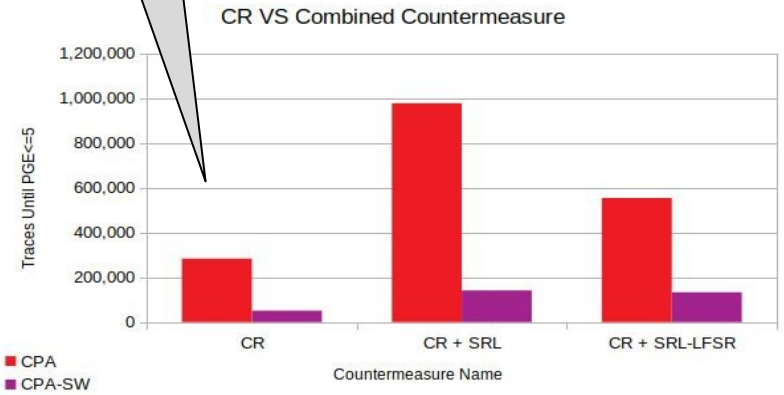

Fig. 11: Combined Results