Simulation-based Pre-Silicon Side-Channel Analysis of AES-GCM

Emrah Karagoz*, Karthik Gedela,
Ferhat Yaman, Amitabh Das*,
Sourabh Goyal
AMD

AMD

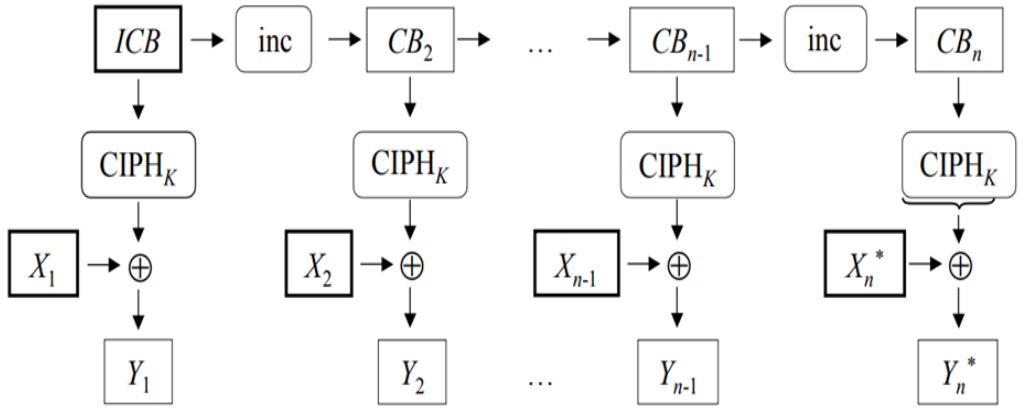
SPONSORED BY CEDA IEEE Council on Electronic Design Automation sigda acm

Motivation

SPONSORED BY CEDA® IEEE Council on Electronic Design Automation sigda acm

Motivation

- Implementations of cryptographic IPs need to be tested for side-channel attack robustness
- Shift-left of security verification for cryptographic IPs through Simulation-based Side Channel Analysis
- Target Crypto IP: AES-GCM
  - open-source, unprotected, hardware design, serial (sequential)/parallel cores
  - recommended memory encryption mode by NIST



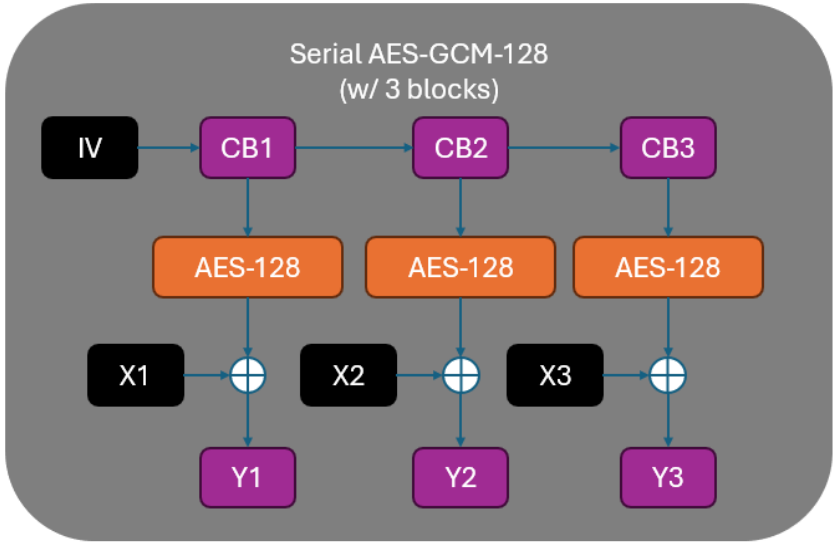
Source: NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

Main Idea

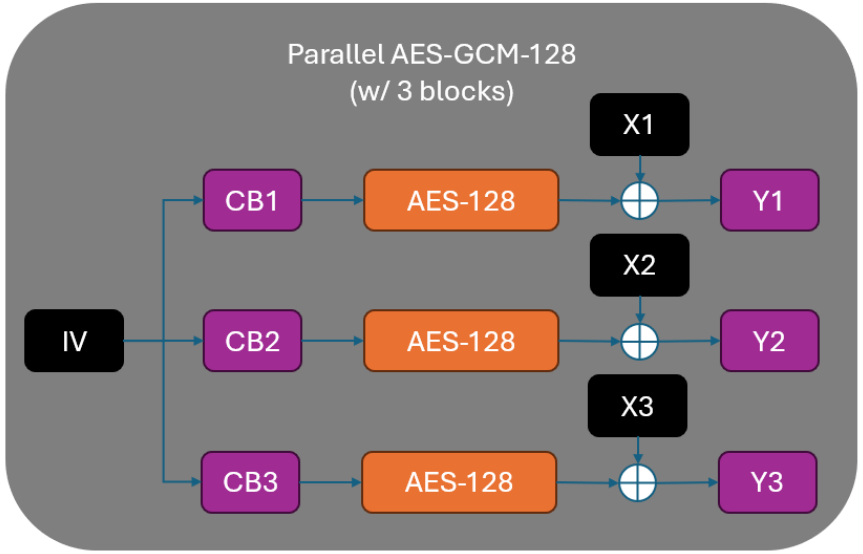
SPONSORED BY CEDA® IEEE Council on Electronic Design Automation SIGDA acm

Two cases: Serial and Parallel AES-GCM

- Demonstrated AES-GCM-128 on the RTL power side-channel analysis
  - Case 1: Serial AES-GCM-128
  - Case 2: Parallel AES-GCM-128 (with parallel AES cores)



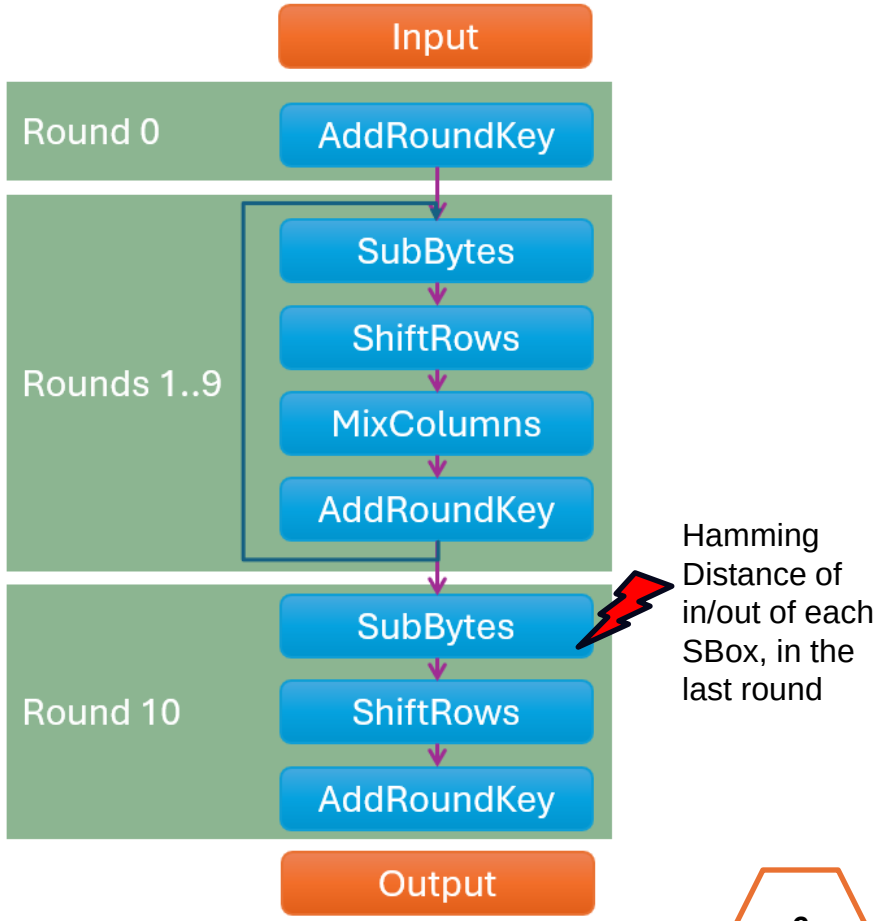
Plaintext = X1 X2 X3 … Xn
Ciphertext = Y1 Y2 Y3 … Yn



IV = Initial Vector
CB = Counter Blocks

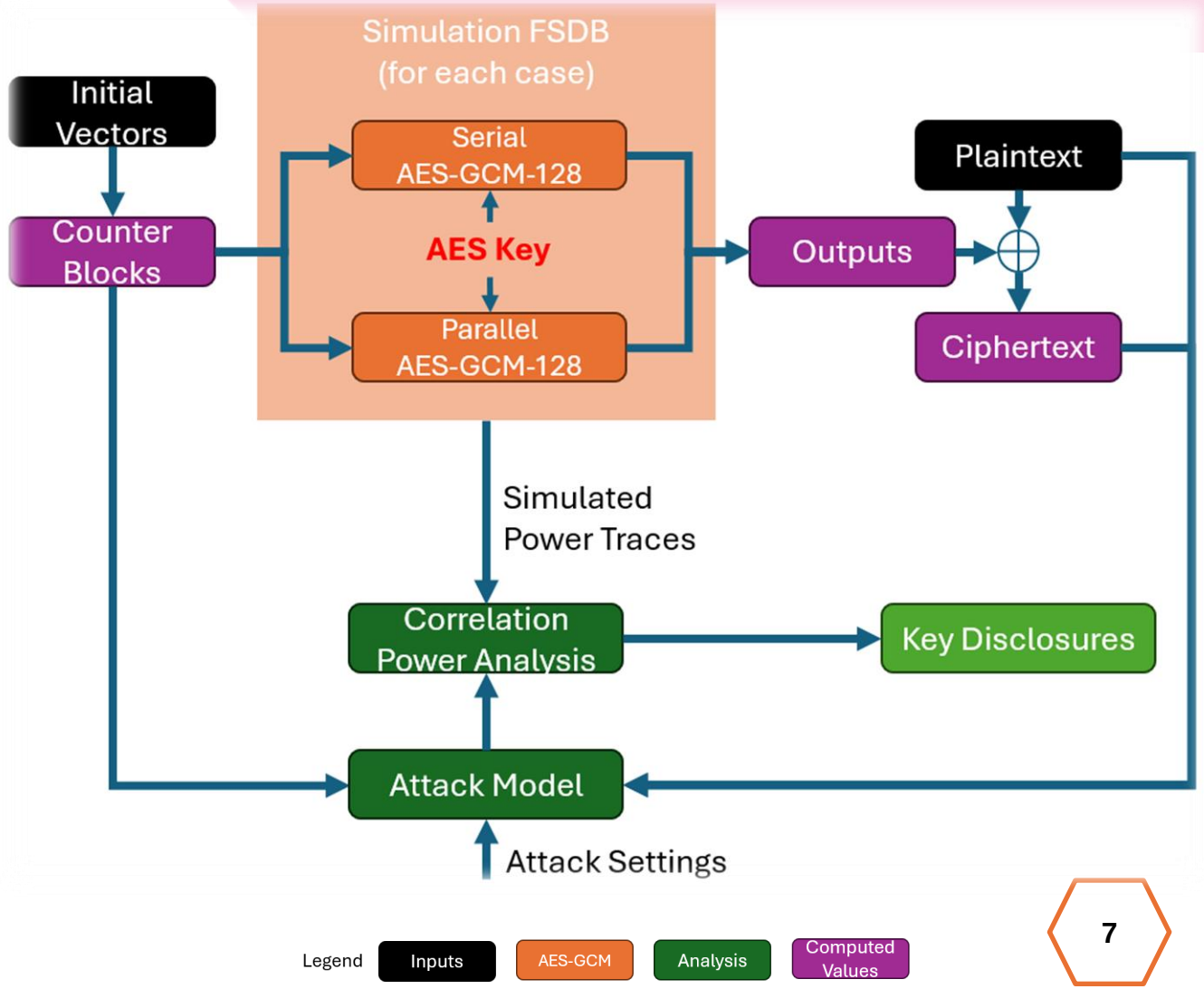
Determine the attack models/points

- Tried different models
  - w/ Hamming Weight/Distance and at AddRoundKey/SBox
- Successful attack w/ Hamming Distance model on the last round SBox
  - Used sum of Hamming Distance values in Parallel AES-GCM



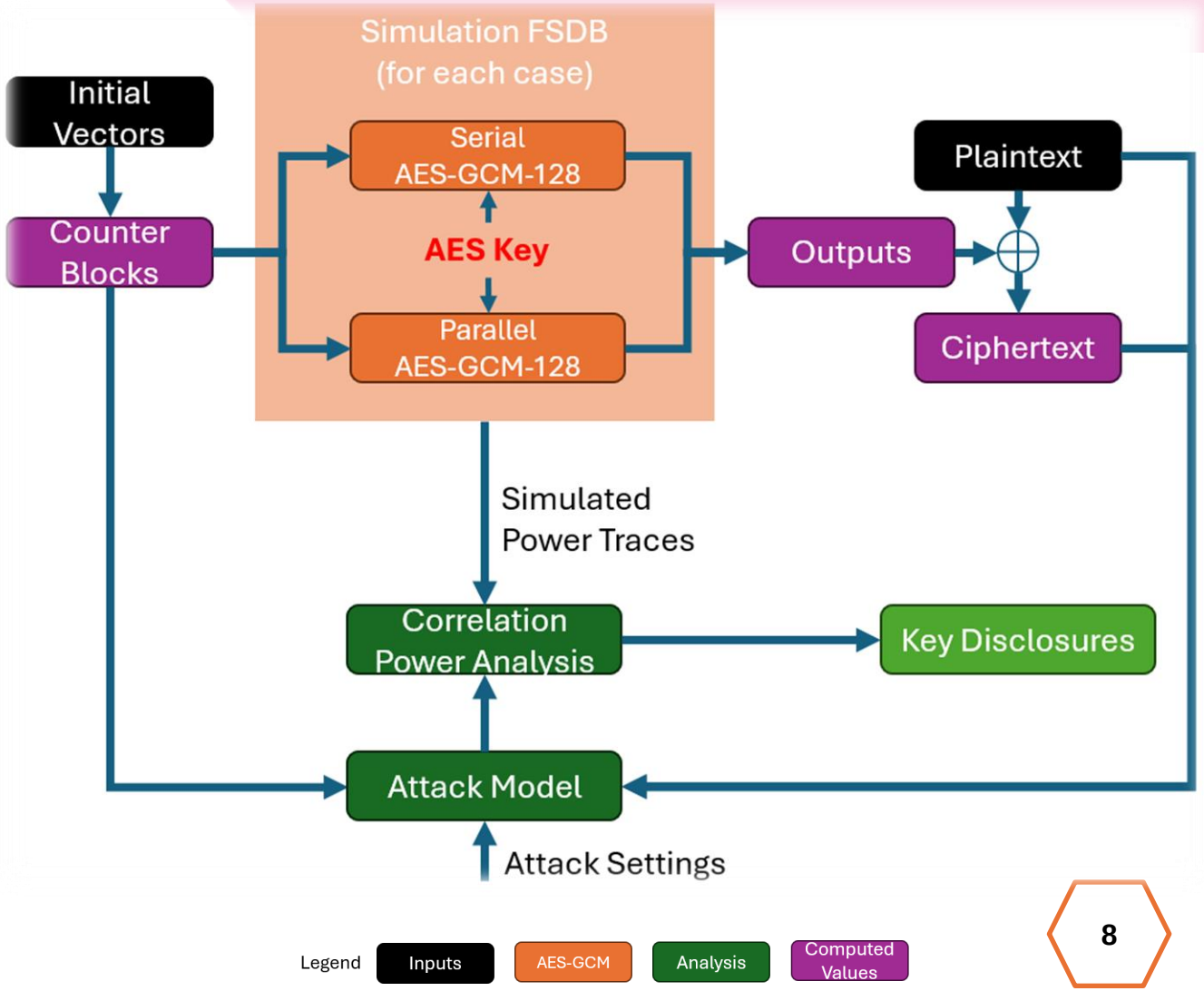
Attack Flow

- **Inputs**
  - Initial Vectors (Counter Blocks can be computed from initial vectors)
  - Plaintext/Ciphertext
- **Simulation**
  - RTL simulation on both cases (Serial & Parallel AES-GCM-128)
  - Obtain power traces based on the simulation
- **Attack model**
  - Develop attack model using Hamming Distance on last round SBox



Attack Flow (cont.)

- **Correlation Power Analysis**
  - Used Pearson's Correlation to correlate power traces and attack model for each guessed key byte
- **Key Disclosures**
  - Successful attack if the correlation coefficient of correct key byte is higher than the other candidate key bytes
  - Metrics: Simulated Minimum number of Traces to Disclose (SMTD)

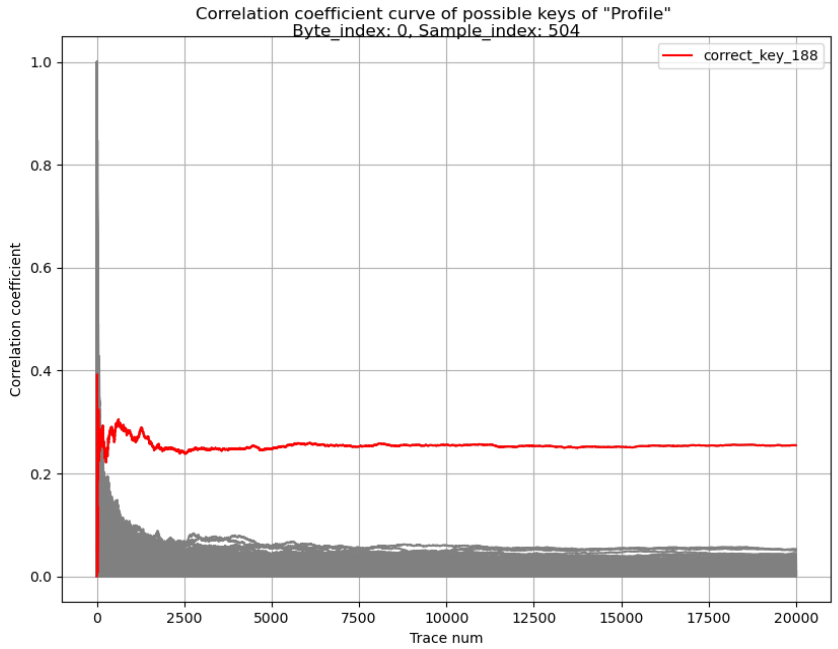


Results & Summary

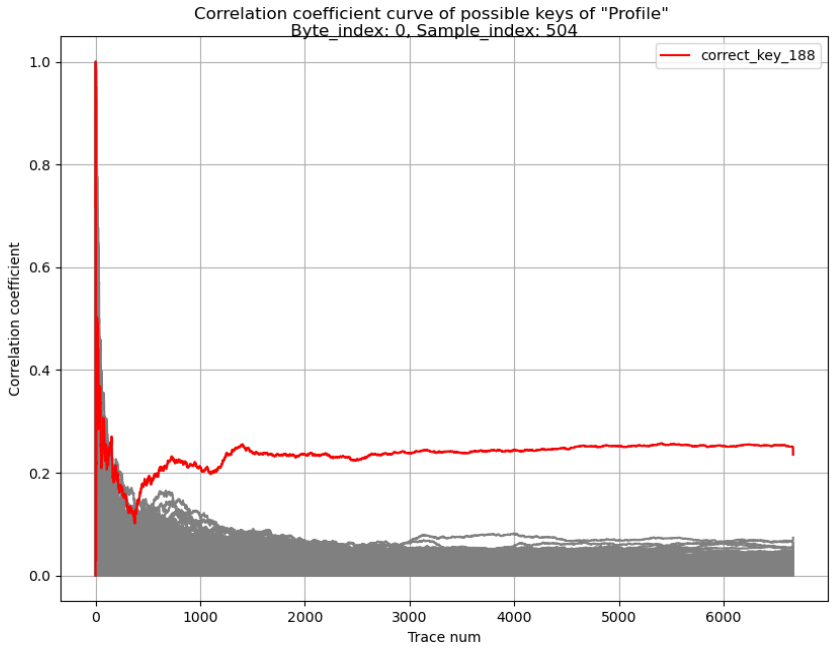
SPONSORED BY CEDA® IEEE Council on Electronic Design Automation sigda acm

Evidence/Results

- Full key disclosure
  - At 455 traces (w/ 455 input blocks) in Serial AES-GCM (w/ 20k input blocks)
  - At 398 traces (w/ 1194 input blocks) in Parallel AES-GCM (w/ 20k input blocks)



Case 1: Serial AES-GCM



Case 2:Paralel AES-GCM

Power traces generated using Ansys PowerArtist TM, security disclosure results generated using Ansys Redhawk SC Security TM

Summary

- Shift-left of security verification of AES-GCM performed through simulated power traces
- An open-source, unprotected hardware implementation of AES-GCM in serial (sequential) and parallel modes is used as the target for the analysis
- Developed attack models through Hamming Weight/Distance (HW/HD) at last round of AES
- Evaluation in SCA metrics of Simulated Minimum number of Traces to Disclose (SMTD) the key and TVLA t-score as the metrics for our SCA
- Obtained full key disclosure at last AES round

Emrah Karagoz

AMD, Sr. Software Development Engineer

Karthik Gedela

AMD, Silicon Design Engineer 2

Amitabh Das

AMD, PMTS Software Development Engineer

Ferhat Yaman

AMD, Software Development Engineer 2

Sourabh Goyal

AMD, Director Silicon Design Engineering

AI

Security

Systems

EDA

Design

62 THE CHIPS TO SYSTEMS CONFERENCE

SPONSORED BY CEDA® IEEE Council on Electronic Design Automation

sigda acm