Side-Channel Analysis of the Xilinx ZYNQ UltraScale+ Encryption Engine

B. Hettwer[*†], S. Leger[*], D. Fennes[†], S. Gehrer[‡], T. Güneysu[†]

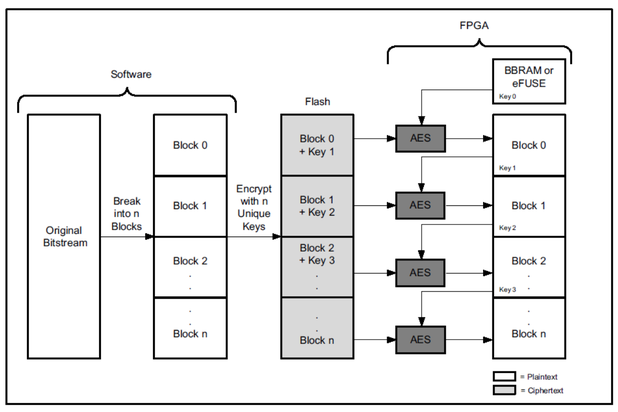
[*]*Robert Bosch GmbH, Corporate Research, Stuttgart, Germany*

[†]*Horst Görtz Institute for IT-Security, Ruhr University Bochum, Germany*

[‡] *Robert Bosch LLC, Pittsburgh, USA*

I. Motivation

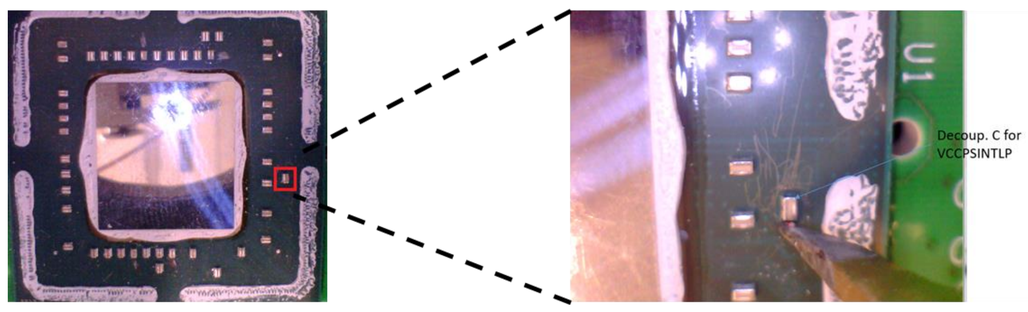
- ZYNQ UltraScale+ on-chip encryption engine
  - AES-256 in GCM mode
  - Used for bitstream encryption and authentication
- Protocol-based SCA countermeasure: **key rolling**[1]
  - Limits data collection for the adversary
  - No recommendation about a suitable block size



- **Goal:** Find appropriate value for key rolling parameter

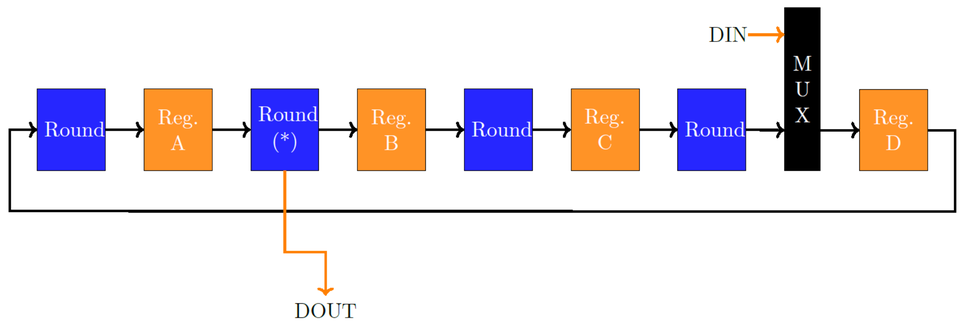
II. Setup

- **Target:** ZYNQ UltraScale+ evaluation board ZCU 102
  - Flip-chip packaging → Removed metal cap with a small driller
- Leakage vector: EM signal induced by on-chip decoupling capacitors
  - Placed EM probe directly to decoupling capacitor related to AES power rail (VCCPSINTLP)
- Worst case scenario: Profiling attack on a single device



III. Attack Procedure (I)

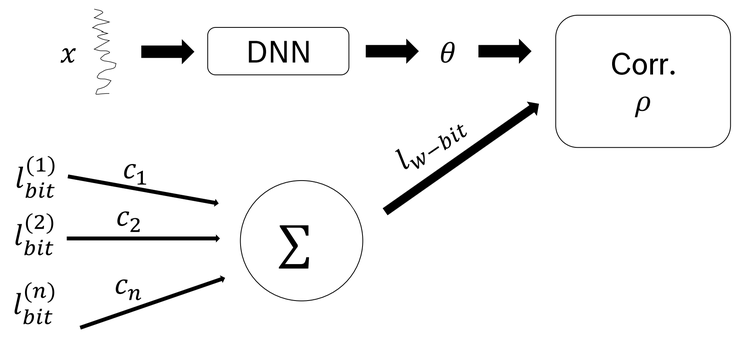
1. Reverse engineering of AES-256 architecture (correlation with known secret)



2. Development of attack procedure over first **five AES rounds**.
   - GCM mode → key has to be extracted with **at most 190 encryptions**!
3. Exploitation of attacker model using Correlation Power Analysis (CPA) with LDA preprocessing
   - Only first round attack successful (one subkey byte)

IV. Attack Procedure (II)

- Customized attacks using Deep Neural Networks (DNNs)
  - Extension of correlation optimization (CO) proposed by Robyns et al.[2]
  - **Idea**: Train a DNN to produce an encoding θ of the input data x that maximizes the Pearson correlation ρ with a hypothetical power leakage l. Approximate leakage coefficients c_i by second small DNN (similar to stochastic approach of Schindler et al.[3])



- Successfully extracted 2nd round AES key
  - Round 3 and later requires 32-bit hypothesis attacks → Complexity too high and Signal-to-noise-Ratio too low
  - > 1000 encryptions needed in our setup

V. Conclusion

- Complete extraction of the AES-256 key has not been successful within 190 encryptions …
  - … but part of the key could be recovered with less than 50 encryptions
  - "*Attacks always become better, never get worse*" – Old NSA saying
  - Lifetime of products can be 20 years or longer (e. g. in automotive industry)
- Recommendation for key rolling parameter: **20 – 30 enc.**
  - Security margin against future attacks
  - Reasonable boot time overhead (15–25%)

VI. References

1. Image Source: *Xilinx ZYNQ UltraScale+ Device, Technical Reference Manual*, v1.9
2. Robyns, P., Quax, P., Lamotte, W.: *Improving CEMA using Correlation Optimization*. IACR Transactions on Cryptographic Hardware and Embedded Systems 2019(1), 1–24 (Nov 2018)
3. Schindler, W., Lemke, K., Paar, C.*: A stochastic model for differential side channel cryptanalysis*. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 30–46. Springer, Heidelberg (2005)