From Cryptography to Hardware: Analyzing and Protecting Embedded Xilinx BRAM for Cryptographic Applications

Shivam Bhasin

Joint Work With:
Sylvain Guilley, Annelie Heuser, Wei He, Jean-Luc Danger

Abstract. Design of cryptographic applications need special care. For instance, physical attacks like Side-Channel Analysis (SCA) are able to recover the secret key, just by observing the activity of the computation, even for mathematically robust algorithms like AES. SCA considers the "leakage" of a well chosen intermediate variable correlated with the secret. Field programmable gate-arrays (FPGA) are also prone to SCA. Modern FPGA are power packed with features to facilitate designers like look-up tables (LUT), embedded block memories (BRAM), DSP cores etc. Certain countermeasures can be deployed, like dual-rail logic or masking, to resist SCA on FPGA. However to design an effective countermeasure, it is of prime importance for a designer to know the main leakage sources of the device.

In this presentation, we analyze the leakage source of a Xilinx Virtex-V FPGA by studying 3 different AES architectures. The analysis is based on real measurements by using specific leakage models of the sensitive variable, adapted to each architecture. Our results demonstrate that, BRAM which were considered to leak less traditionally, are found to be equally vulnerable if we change the attack target from address register to output latch. We also show that if the leakage model is known, simple countermeasures with only 16% overhead can be deployed to overcome the leakage. Next we propose methods to exploit BRAM for designing countermeasures. BRAM can be used to optimize intrinsic countermeasures like masking and dual-rail logic, which otherwise have significant overhead (at least 2X). The optimization are applied on a AES co-processor and tested for area overhead and resistance on Xilinx Virtex-V chips.