Abstract

Modern embedded systems should not only be optimized in terms of classical parameters like power, performance, and area (PPA) but also needs to be secured by design. Accordingly, the Electronic Design Automation (EDA) tools to manufacture Integrated Circuits (ICs) of these embedded systems must also be tuned to handle both the PPA optimization and security realms in the design process. The classical EDA flows cannot detect side-channel leakages at early design stages or provide countermeasures against fault attacks (FAs) and side-channel attacks (SCAs), let alone optimized countermeasures which have low foot-prints on power, performance, and area. Moreover, the existing EDA flow optimization techniques could be conflicting with the security requirements of IC design and provide adversaries with leakage surfaces. Hence, the primary goal of this thesis is to propose a modified EDA flow that aims to reduce overall design cycle time in the tight time-to-market scenario by detecting early security flaws in the designs and adopting techniques to generate SCA and FA-resistant lightweight designs.

In this thesis, first, we propose a machine learning-based synthesis approach that could quickly explore from a huge design search space to identify power-efficient and cryptographically robust S-Box constructions, which are important primitives for block ciphers. Secondly, we address the problem of verification of side-channel leakages in crypto circuits at the early design stages to avoid significant loss incurred if the design is found to be vulnerable at the post-silicon stage. Nevertheless, our proposed solution can also detect leakage vulnerability of the design due to the optimizations introduced by state-of-art EDA tools performing High-level Synthesis. Thirdly, we propose frameworks that can tune classical EDA tools to perform secure-aware optimizations while generating SCA and FA-resistant designs. Our proposed security-aware synthesis technique generates side-channel countermeasures along with ensuring a low hardware footprint as compared to traditional SCA countermeasure generation schemes that may incur significant hardware. The security-aware floorplan technique

can perform tentative placement of registers/modules based on the understanding of its sensitivity towards fault attacks thereby increasing the robustness of the design against state-of-art fault injection attacks. Finally, we demonstrate the scalability of our proposed methods on a complete block cipher design as a final contribution to this thesis. We present hardware modifications that a designer can use to create a side channel-resistant lightweight block cipher with strong resistance to classical crypt-analysis while maintaining a modest area footprint.