How to design BCDL Logic with the best Trade-off between Complexity and Robustness

Shivam Bhasin, Jean-Luc Danger, Tarik Graba, Sylvain Guilley
Telecom Paristech, Paris, France

Abstract

Dual Rail Logic is a countermeasure against Side-Channel Attacks (SCA) which can be costly or less robust if no effort is given during the design stage. We show that it is possible to reduce the implementation complexity by taking advantage of a bottom-up approach when designing with BCDL logic. Moreover the constraints of using global signals and balancing the True and False networks can be greatly simplify at the Place/Route stage. The proposed methods take advantage of swapping mechanisms and could provide higher levels of robustness against SCA. Examples are given in FPGAs an ASICs.