Implementation Challenges for Ideal Lattice-Based Cryptography on Reconfigurable Hardware

Jean-Luc Danger
Telecom ParisTech

Abstract

Most commercial FPGAs are scantily protected against attacks, either physical attacks, or attack on the configuration port. Moreover there are many unknown variables when using them: the interconnection details are proprietary and some validation blocks are unspecified. This talk presents a custom FPGA architecture and design methods which aim at enhancing the robustness against physical attacks. The FPGA has 2048 cells and has been designed in ST 65 nm technology. Its topology is tree-based, hence providing a good level of timing determinsism, and offering a base to use differential logic as WDDL or BCDL. Design methods to balance efficiently the differential logic are presented. The analysis performed on PRESENT WDDL implementation show a significant robustness gain.