Abstract

Network-on-Chip (NoC) has emerged as a promising communication backbone for the emerging, as well as future multi-core Systems-on-Chip (MCSoCs) that integrate many intellectual property (IP) cores. NoC based MCSoCs have several advantages over conventional bus-based ones, such as improved energy efficiency. These advantages allow the NoC based communication infrastructure to be considered for many applications, including digital signal processing (DSP), in realizing efficient and high-performance architectures. Further, the life cycle of an integrated circuit (IC) product nowadays revolves around several third-party organizations, such as IP vendors and IC fabrication houses. With the involvement of so many entities, it has become essential to incorporate security features at every stage of system integration. In this direction, the security-aware design of the NoC based architectures for several application areas, including DSP, is also being considered. This dissertation concentrates on implementing energy-efficient and secure NoC architectures for DSP applications. A NoC based energy-efficient and reconfigurable fast Fourier transform architecture, which utilizes the constant-geometry (CG) property, has been proposed. Further, a variant of the CG signal flow graph (CGSFG), namely butterfly-separated CGSFG, has been introduced. Next, an energy-efficient NoC topology with diagonal links, namely ZMesh, has been proposed. Next, a ZMesh NoC based reconfigurable Viterbi decoder architecture has been presented, which leverages the properties of ZMesh to realize several configurations of its algorithm efficiently. Next, two runtime mechanisms to thwart hardware Trojan-based attacks in NoCs have been proposed. The attacks considered are illegal packet request and packet drop attacks. Analysis of the proposed attacks has been carried out even on the DSP algorithms to establish their significance. The proposed security mechanisms are realized at the hardware level and are shown to account for low overheads in terms of both energy efficiency and application execution time. Further, a technique to embed delay-based physical unclonable functions (PUFs) has been presented. The crossbars present in the NoC routers are modified such that they can function both as a standard crossbar and as a PUF. The proposed embedded PUFs can be applied to chip authentication, as well as secret key generation.

Keywords: Network-on-Chip; energy-efficiency; security; digital signal processing; fast Fourier transform; Viterbi decoding; hardware Trojan; physical unclonable function.