Security Solutions in the First-Generation Zynq All-Programmable SoC
Invited Abstract

Steve Trimberger
Xilinx

Abstract
FPGAs have grown from a simple logic replacement to fully-programmable SoC, with multi-core CPU subsystems, a broad spectrum of peripherals, hundreds of thousands of gates of programmable logic and high-speed multi-gigabit transceivers. As the complexity of the underlying hardware has grown, so has the value of the applications built in them and the data handled by them. Traditional FPGA bitstream security has been enhanced to address these greater security requirements. This paper presents an overview of the security features of the Zynq All-Programmable SoC. The secure boot process includes asymmetric and symmetric authentication as well as symmetric encryption to protect software and programmable hardware during programming. During operation the hardware can disable test ports, monitor on-chip power and temperature and detect tampering with configuration data. ARM Trust Zone is integrated through the AXI busses into both the processor and the programmable logic subsystems.