The new RISC-V Entropy Source Instruction Set Architecture (ISA) Standard

Richard Newell
FPGA Business Unit, Microchip Technology

Abstract

After a brief summary of the RISC-V International on-going activities for securing RISC-V processors and their applications, the focus of this talk will be on the recently ratified Entropy Source control-status registers (CSRs). Unlike the ISAs offered by Intel, AMD, and ARM. the usual cryptographic conditioner is intentionally not included. Therefore, these CSRs provide a standardized way to gather entropy without limiting the security strength of the overall implementation. They are meant to be compatible with all modern random bit generation standards, particularly SP800-90B and AIS-31.