RISC-V Vector Cryptography and Post-Quantum Cryptography Plans

Markku-Juhani O. Saarinen

PQShield Ltd, Oxford, UK

Abstract

I'll cover aspects of RISC-V Vector processor ISA (Instruction Set Architecture) and its support for cryptography from both computer architecture and (Linux/Android) software stack viewpoint. I'll also offer an update on the official Cryptography ISA development and currently considered options for ISA-level hardware support for NIST Standard PQC (Post-Quantum Cryptography).

The speaker is the Acting Chair of the RISC-V Post-Quantum Task Group and has previously contributed to the design of official RISC-V Entropy Source, Scalar Cryptography, and Vector cryptography extensions.