Cryptographic Extensions TG

Chair: G. Richard Newell, Associate Technical Fellow, Microchip Technology

Vice-Chair: Derek Atkins, Chief Technology Officer, Veridify Security

Charter

The Cryptographic Extensions Task Group will propose ISA extensions to the vector extensions for the standardized and secure execution of popular cryptography algorithms. To ensure that processor implementers are able to support a wide range of performance and security levels the committee will create a base and an extended specification. The base will be comprised of low-cost instructions that are useful for the acceleration of common algorithms. The extended specification will include greater functionality, reserve encodings for more algorithms, and will facilitate improved security of execution and higher performance. The scope will include symmetric and asymmetric cryptographic algorithms and related primitives such as message digests. The committee will also make ISA extension proposals for lightweight scalar instructions for 32 and 64 bit machines that improve the performance and reduce the code size required for software execution of common algorithms like AES and SHA and lightweight algorithms like PRESENT and GOST, as well as ISA proposals regarding the use of random bits and secure key management.

Useful Links

Cryptographic Extensions task group GitHub Site

- Latest releases of the draft cryptographic extensions specification: https://github.com/riscv/riscv-crypto/releases
    - Draft Scalar Crypto SpecificaDraft Scalar Crypto Specification (v0.9.1)
    - Draft Vector Crypto Specification (v0.7.0)
- Issues (internal task group issues tracked on GitHub)

Scalar Crypto Standardization Status Summary

Vector Crypto Standardization Status Summary

Meeting notes archive on Google Drive (since Oct. 2020)

(Older meeting notes may be found posted on the CETG mailing list)

Instruction list (worksheet) with branding/naming proposals (Work in Progress)

JIRA (Cross-task-group issue tracking system) – Cryptographic Extensions task group open issues

Slack (messaging system):

- RISC-V International workspace on Slack
- Link to join the RISC-V workspace
    - Cryptographic Extensions public channel on Slack: #tech-crypto

Tech groups calendar

Old RISC-V groups site: https://lists.riscv.org/g/tech-crypto-ext