Vector Crypto Standardization Status Summary

Overall Approved Definition-of-Done Status: Kick-Off

Next Major Definition-of-Done Milestone: Stable

Specification

- Almost Stable
  - Update Round-based AES-decrypt to use the NIST standard (vs. alternative) definition
  - Needs translation into ASCIIDOC

OpCode Encoding/OpCode consistency review

- Opcodes and encodings proposed
- Formal review not started

Architecture Tests

ABI Extensions

GCC and Assembler

- (Intrinsics)

(links to GitHub, etc., as relevant to each of the topics here)

(links to PLTC and IIT Madras status pages, TBD)

LLVM

SAIL

Spike

QMU

Proof-of-Concept