Extra Vector Crypto (Zvbc32e, Zvkgs)
Ratification Plan

Presented by: Nicolas Brunie, unofficially from Vector Crypto TG
Agenda

- Presenting extra vector crypto extensions project and plan
- Seek feedback and approval of chairs for plan
Background

Proposal to complement the newly ratified vector crypto specification:

- A few instructions were left aside when crypto TG specified vector crypto
- Allow implementations with smaller ELEN (32) to support vector carryless multiply
- Allow more efficient implementations of Cyclic Redundancy Checks (CRCs)
- Allow more efficient implementations of parallel GHASH (e.g. AES-GCM)
Overview

Suggest two new vector crypto ISA extensions:

- Defining Zvbc32e: 32-bit vector carryless multiply
  - `vclmul.v[vx]` and `vclmulh.v[vx]` for SEW=32-bit only.

- Defining Zvkgs: vector-scalar variants of Zvkg
  - `vgmul.vs` and `vghsh.vs`

- Define timing mandate (including when Zvkt is supported)
Design Considerations

● Double use case for Zvbc32e
  ○ Enable ELEN=32 implementations
  ○ Improve efficiency of ELEN=64 implementations on some workload

● Need a new opcode scheme for Zvkgs
  ○ No 3-operand destructive .vs variant has never been defined before

● Limited extra hardware requirement
  ○ 32-bit vector carryless multiply can easily reuse Zvbc hardware
  ○ Zvkgs extend Zvkg to the .vs operand mode already supported in Zvkned and Zvksed

● We expect specification to be mostly straightforward / Non controversial
  ○ Already discussed in vector crypto TG
  ○ No real new operation
Key Milestones

Jira Spec: [https://jira.riscv.org/browse/RVS-1915](https://jira.riscv.org/browse/RVS-1915)

<table>
<thead>
<tr>
<th>Key Milestones</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan Approval</td>
<td>Dec 15th, 2023</td>
</tr>
<tr>
<td>Internal Review Start</td>
<td>Jan 31st, 2024</td>
</tr>
<tr>
<td>Architecture Review Request</td>
<td>Apr 1st, 2024</td>
</tr>
<tr>
<td>Freeze Milestone</td>
<td>May 31st, 2024</td>
</tr>
<tr>
<td>Public Review Start</td>
<td>July 1st, 2024</td>
</tr>
<tr>
<td>Ratification-Ready Milestone</td>
<td>Sep 15th, 2024</td>
</tr>
<tr>
<td>TSC Approval</td>
<td>Oct 15th 2024</td>
</tr>
<tr>
<td>Board Ratification</td>
<td>Q4 2024</td>
</tr>
</tbody>
</table>
Proof-of-concept and RISC-V Tests

Proof-of Concept
- 32-bit CRC routines
- Parallel GHASH implementation examples

Software Support (OS, RTOS, Hypervisor, etc.)
- OpenSSL for Zvkg (API compatibility to be confirmed)

Simulator Support
- QEMU: To be planned
- Spike: planned
- SAIL: planned

Tests (ACT for ISA or Software)
- To be defined
# ISA Freeze Checklist

<table>
<thead>
<tr>
<th>ISA Item</th>
<th>Task Description</th>
<th>Plan</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opcode Support</td>
<td>Enough opcode encoding to support GCC.</td>
<td>Planned (only needed for Zvkgs)</td>
<td>Nicolas Brunie</td>
</tr>
<tr>
<td>Simulator Support</td>
<td>Enough simulator support so that basic RISC-V tests can be run. See the policy for more details.</td>
<td>Planned</td>
<td>Nicolas Brunie</td>
</tr>
<tr>
<td>psABI</td>
<td>ABI extensions (if necessary)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>gcc</td>
<td>Support GCC (optimizations not required)</td>
<td>Planned</td>
<td>SiFive</td>
</tr>
<tr>
<td>RISC-V Test Input</td>
<td>Test configuration input (YAML schema &amp; values, Test Coverage YAML rules, see the policy)</td>
<td>Planned (to be built on top of vector crypto tests)</td>
<td>Nicolas Brunie</td>
</tr>
<tr>
<td>RISC-V Tests</td>
<td>Basic tests that do not cover corner cases. See the policy for more details.</td>
<td>Planned (vector crypto code sample extension)</td>
<td>Nicolas Brunie</td>
</tr>
<tr>
<td>RISC-V SAIL</td>
<td>Email <a href="mailto:tech-arch-review@lists.riscv.org">tech-arch-review@lists.riscv.org</a> for review. Policy in development.</td>
<td>Planned (dependent on vector crypto support in SAIL, PRs #236 and #241)</td>
<td>Nicolas Brunie</td>
</tr>
</tbody>
</table>
Summary

- TG Charter: N/A (fast track)
- Draft specification: https://github.com/riscv/riscv-crypto/pull/362
- Ratification Plan: 
- Status checklist: 

Current Status:
- Fast track project accepted by AR committee
- Plan being presented to Tech Chairs for review and approval

Assumption(s):
- Handled as fast track (no TG creation)
- Availability of vector crypto SAIL implementation
- Availability of vector and vector crypto ACT tests

Dependency:
- The work relevant to the new extensions should be handled by people from SiFive
- Some dependencies on others for remaining work for previous extensions (vector crypto in particular)

Goal is to freeze the extension by end of Q2’24 and ratify by end of Q4’24.
BACKUP