Progress of K-ext Support on QEMU

Lucas Zewen Ye
Lucas.zw.ye@outlook.com
Wednesday, March 10, 2021

Scalar Crypto Instructions

- Instructions: Fully defined in Scalar Crypto & Shared from Bit-Manipulation.
- All extensions on Scalar Crypto Specification:
    - Scalar AES Acceleration
    - Scalar SHA-256 / SHA-512 Acceleration
    - Scalar SM3, SM4 Acceleration

Scalar AES Acceleration

31 30	29 28 27 26 25	24 23 22 21 20	19 18 17 16 15	14 13 12	11 10 9 8 7	6 5 4 3 2 1 0	
bs	11011	rs2	rt	000	00000	0110011	aes32esmi
bs	11001	rs2	rt	000	00000	0110011	aes32esi
bs	11111	rs2	rt	000	00000	0110011	aes32dsmi
bs	11101	rs2	rt	000	00000	0110011	aes32dsi

31 30	29 28 27 26 25	24 23 22 21 20	19 18 17 16 15	14 13 12	11 10 9 8 7	6 5 4 3 2 1 0	
00	11000	1 rcon<=10	rs1	001	rd	0010011	aes64ks1i
01	11111	rs2	rs1	000	rd	0110011	aes64ks2
00	11000	00000	rs1	001	rd	0010011	aes64im
00	11011	rs2	rs1	000	rd	0110011	aes64esm
00	11001	rs2	rs1	000	rd	0110011	aes64es
00	11111	rs2	rs1	000	rd	0110011	aes64dsm
00	11101	rs2	rs1	000	rd	0110011	aes64ds

Scalar SHA-256 / SHA-512 Acceleration

31 30 29 28 27 26 25	24 23 22 21 20	19 18 17 16 15	14 13 12	11 10 9 8 7	6 5 4 3 2 1 0	
00	01000	00010	rs1	001	rd	0010011	sha256sig0
00	01000	00011	rs1	001	rd	0010011	sha256sig1
00	01000	00000	rs1	001	rd	0010011	sha256sum0
00	01000	00001	rs1	001	rd	0010011	sha256sum1

Scalar SHA-256 / SHA-512 Acceleration

31 30 29 28 27 26 25	24 23 22 21 20	19 18 17 16 15	14 13 12	11 10 9 8 7	6 5 4 3 2 1 0	
00	01000	00110	rs1	001	rd	0010011	sha512sig0
00	01000	00111	rs1	001	rd	0010011	sha512sig1
00	01000	00100	rs1	001	rd	0010011	sha512sum0
00	01000	00101	rs1	001	rd	0010011	sha512sum1

31 30 29 28 27 26 25	24 23 22 21 20	19 18 17 16 15	14 13 12	11 10 9 8 7	6 5 4 3 2 1 0	
01	01000	rs2	rs1	000	rd	0110011	sha512sum0r
01	01001	rs2	rs1	000	rd	0110011	sha512sum1r
01	01010	rs2	rs1	000	rd	0110011	sha512sig0l
01	01110	rs2	rs1	000	rd	0110011	sha512sig0h
01	01011	rs2	rs1	000	rd	0110011	sha512sig1l
01	01111	rs2	rs1	000	rd	0110011	sha512sig1h

Scalar SM3, SM4 Acceleration

31 30	29 28 27 26 25	24 23 22 21 20	19 18 17 16 15	14 13 12	11 10 9 8 7	6 5 4 3 2 1 0	
00	01000	01000	rs1	001	rd	0010011	sm3p0
00	01000	01001	rs1	001	rd	0010011	sm3p1

31 30	29 28 27 26 25	24 23 22 21 20	19 18 17 16 15	14 13 12	11 10 9 8 7	6 5 4 3 2 1 0	
bs	11000	rs2	rt	000	00000	0110011	sm4ed
bs	11010	rs2	rt	000	00000	0110011	sm4ks

Implementation and Test of Scalar Instrs

- Based on the implementation of K-ext on `Spike`:
  - First PR
  - Patch
- Test
  - (1)Test from `riscv-crypto`
  - (2)Test from `rvkrypto-fips`

Our Work and Future Work

- What we have done
  - Scalar AES Acceleration (**Implementation** and **Test(1)**)
  - Scalar SHA-256 / SHA-512 Acceleration (**Implementation** and **Test(1)**)
  - Scalar SM3, SM4 Acceleration (**Implementation**)
- Relative Issues
  - [Overlap Patterns](https://github.com/riscv/riscv-crypto/issues/74)
  - [Compile Error](https://github.com/riscv/riscv-crypto/issues/80)
- Future Work
  - Test(1) and Test(2) on the SM3 and SM4, Test(2) on the Scalar Crypto AES, SHA Instructions (**1 week**)

Entropy Source Extension

- Future Work
  - Implement and Test(**1~2 weeks**)

RISC-V Crypto ISA

```
RV32, RV64
    pollentropy    rd   // Poll randomness. Encoding: csrrs rd, mentropy, x0
```

RISC-V Crypto ISA

```
RV32, RV64
    getnoise    rd   // Noise source test. Encoding: csrrs rd, mnoise, x0
```

In Total

Instructions	Implementation	Test(1)	Test(2)
Scalar AES Acceleration	DONE	DONE	NO
Scalar SHA-256 / SHA-512 Acceleration	DONE	DONE	NO
Scalar SM3, SM4 Acceleration	DONE	NO	NO
Entropy Source Extension	NO	NO	NO

Thanks for Listening

- [Scalar Crypto Specification](https://github.com/riscv/riscv-crypto/releases)
- [Our Github Repositories of QEMU](https://github.com/plctlab/plct-qemu/tree/plct-k-dev)
- [Implementation of Spike](https://github.com/riscv/riscv-isa-sim/pull/649)
- [Patch of the Implementation of Spike](https://github.com/riscv/riscv-isa-sim/pull/635)
- [Test(1)](https://github.com/riscv/riscv-crypto/tree/master/benchmarks)
- [Test(2)](https://github.com/rvkrypto/rvkrypto-fips)