Deutsches Zentrum für Luft- und Raumfahrt

Scale4Edge

Prototyping custom RISC-V instructions with Seal5 and CoreDSL

Jan Schlamelcher, Thomas Goodfellow, Bewoayia Kebianyor, Gregor Nitsche, Philipp van Kempen and Kim Grüttner

Goal

Evaluating a prototyping flow using Seal5 for RISC-V custom instructions

Test case: ChaCha20 Cipher

- Generates blocks of pseudo-random bytes by repeated use of cheap ALU operations
- Central "Quarter Round"transformation performed 80 times for each block, each with 4 sets of ADD+XOR+ROL operations
- No ROL instruction in the base RV32I ISA means each set uses 5 instructions
- Scope for 4 customized XOR+ROL instructions

ChaCha20 Quarter Round

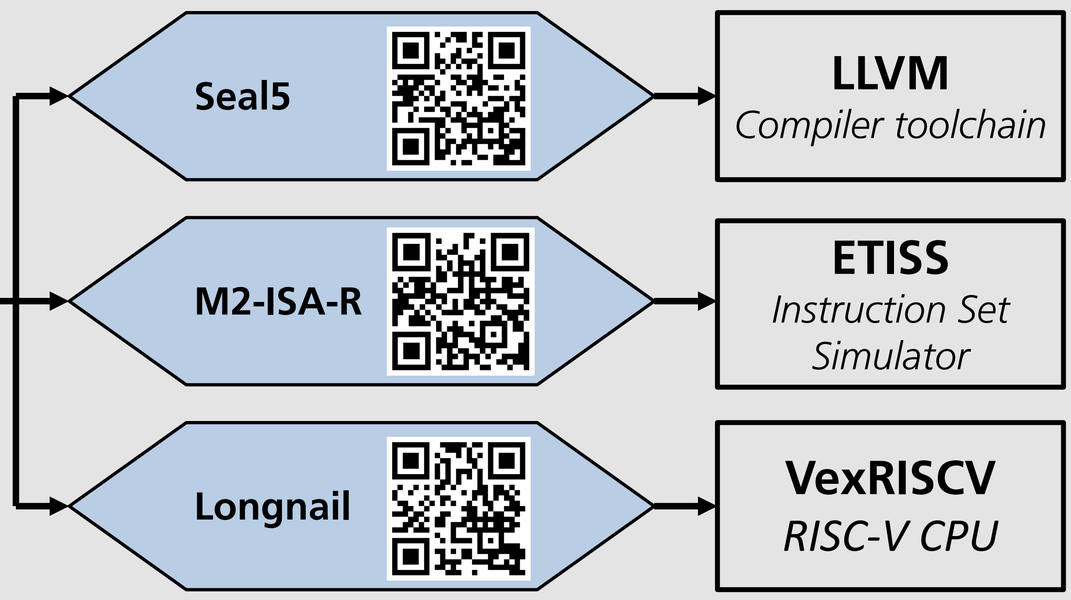
```
a += b; d ^= a; d <<<= 16;
c += d; b ^= c; b <<<= 12;
a += b; d ^= a; d <<<= 8;
c += d; b ^= c; b <<<= 7;
```

Method

Describe the custom XOR+ROL instructions in CoreDSL and from that generate a compiler toolchain, instruction simulator, and CPU that all support the new instructions

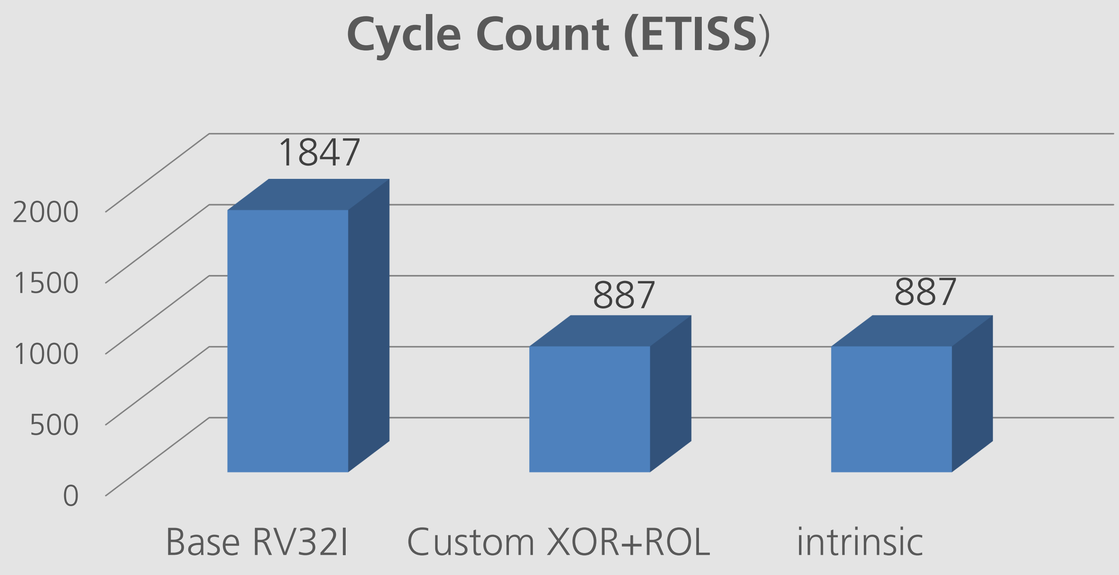
CoreDSL for a combined XOR+ROL

```
if (rd != 0) {
  unsigned<32> xor = X[rs1] ^ X[rs2];
  X[rd] = (xor << 16) | (xor >> 16);
}
```



… then build & execute the ChaCha20 test case with these generated products

Results



Simulator Evaluation

- Seal5-generated compiler automatically exploits new XOR+ROL, eliminating three instructions from each operation set
- This optimization provides a **52% speed-up** to the entire cipher block generation
- Attempting manual optimization through instrinsic functions gave no further speedup – **instruction selection works well!**

- Generating an extended compiler takes only **~10 minutes** (on a 32 core server)
- Adding the XOR+ROL instructions to the VexRISCV core **increases its size by only ~1%**
- Hardware synthesis takes ~**5 minutes**

Federal Ministry of Education and Research

This work has been developed in the ZuSE project Scale4Edge. Scale4Edge is funded by the German ministry of education and research (BMBF) (reference number 16ME0465).

MSc. Jan Schlamelcher | System Evolution and Operation (SE-EVO)
Telefon +49 441 770507 357 | Jan.Schlamelcher@dlr.de
DLR.de | Institut Systems Engineering für zukünftige Mobilität