SCARV: a side-channel hardened RISC-V platform

https://github.com/scarv

Daniel Page
Department of Computer Science, University of Bristol,
Merchant Venturers Building, Woodland Road,
Bristol BS8 1UB, United Kingdom.
csdsp@bristol.ac.uk

21/11/19
Recap:

$$\text{SCARV} \approx \text{RISC-V} + \text{cryptography}$$
$$\approx \text{RISC-V} + \text{cryptographic engineering}$$
$$\approx \text{RISC-V} + \text{implementation} + \text{implementation attacks}$$

where

- WP-A \(\approx\) a side-channel resistant RISC-V implementation
- WP-B \(\approx\) RISC-V support for next-generation cryptography
- WP-C \(\approx\) a democratised side-channel evaluation lab.
Summary:

1. **XCrypto**: a cryptographic ISE for RISC-V.

   [https://github.com/scarv/xcrypto](https://github.com/scarv/xcrypto)

   - accelerate software-based cryptographic workloads vs. base ISA,
   - allow flexibility wrt. parameterisation, countermeasures, etc.
   - example: multi-precision integer arithmetic

   \[
   \text{xc.mmul.3 (rd2, rd1), rs1, rs2, rs3 } \Rightarrow \left\{ 
   \begin{align*}
   t &\leftarrow (\text{GPR}[rs1] \times_{u} \text{GPR}[rs2]) +_{u} \text{GPR}[rs3] \\
   \text{GPR}[rd1] &\leftarrow t_{\text{XLEN}-1...0} \\
   \text{GPR}[rd2] &\leftarrow t_{2\cdot\text{XLEN}...\text{XLEN}}
   \end{align*}
   \right.
   \]

   - involved with RISC-V Cryptographic Extensions Task Group wrt. a standard scalar (vs. vector) ISE.
Summary:

2. Micro-architectural design $\leftrightarrow$ (analogue) information leakage.
   - micro-architectural impact on share slicing in masked implementations,
   - FENL: a fence for micro-architectural leakage.
Summary:

3. SCARV: a side-channel hardened RISC-V micro-controller.

https://github.com/scarv/scarv

- RISC-V compatible, RV32IMC-based processor core plus SoC,
- test-bed for XCrypto, FENL, etc.
- in-progress Zephyr port → demonstrator(s).

https://www.zephyrproject.org
Summary:

4. **SCA3S:** Side-Channel Analysis as a Service.

- Continuous Integration (CI) mode \(\approx\) "LGTM for side-channels",
- build-it, break-it, fix-it [1] contests (e.g., CHES challenge),
- ...

https://semmle.com/lgtm
Questions?