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

14/11/18
What we *said* we’d do:

WP-A
≡
a side-channel resistant RISC-V implementation

- side-channel hardened implementation techniques (e.g., vs. DPA),
- side-channel aware ISA design (cf. [5, 3]),
- design transparency ⇒ more accurate leakage modelling.
What we said we’d do:

WP-B
≡
RISC-V support for next-generation cryptography

- domain-specific (micro-)architectural design,
- support for implementation of light-weight and post-quantum cryptography,
- (secure) design and use of embedded FPGA fabric (e.g., EFLX, per [1], cf. [2, 4]).
What we *said* we’d do:

WP-C
≡
a democratised side-channel evaluation lab.

- cloud-based leakage assessment (simulated and real platform),
What we did do (in 2018/Q1 to 2018/Q3):

1. started some new work, e.g.,
   WP-A: cryptographic ISE design and reference implementations
   https://github.com/scarv/xcrypto
   WP-A: BSP-like experimental infrastructure
   • cores: PicoRV32, Rocket Core, ...
   • boards: Arty, iCEstick, SAKURA-X, Zebo, ZedBoard, ...
   WP-A: support for hiding-based countermeasures against DPA-like attack,
   WP-C: prototype AWS-based acquisition infrastructure.
What we did do (in 2018/Q1 to 2018/Q3):

1. started some new work, e.g.,
   - WP-A: cryptographic ISE design and reference implementations
   - WP-A: BSP-like experimental infrastructure
     - cores: PicoRV32, Rocket Core, . . .
   - WP-A: support for hiding-based countermeasures against DPA-like attack,
   - WP-C: prototype AWS-based acquisition infrastructure.

2. continued some previous work, e.g.,
   - https://github.com/danpage/mascab
   - https://github.com/danpage/scale
Questions?
References


