Proteus

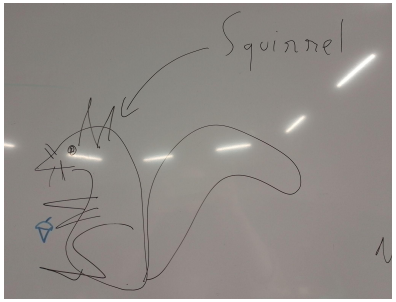
Extensible RISC-V processor
& Security Applications

KU LEUVEN

DistriNet

BINSEC

frama C



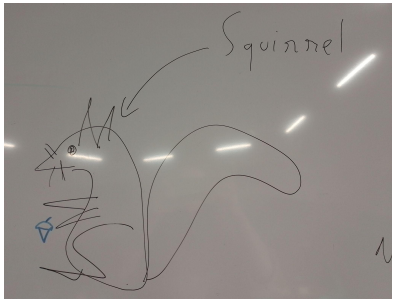
PhD student doing program/protocol verification

** List probably non-exhaustive*

** Special congrats if you recognize all tools!*

BINSEC

frama C

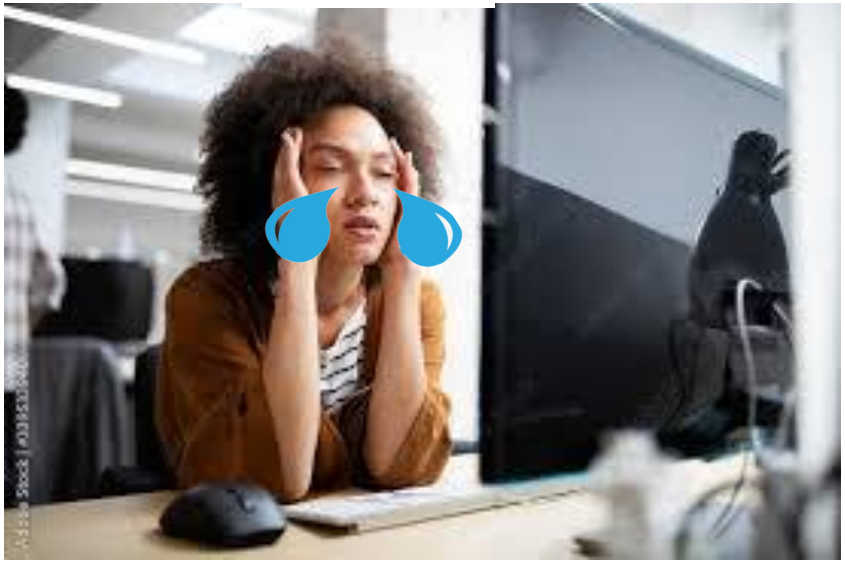
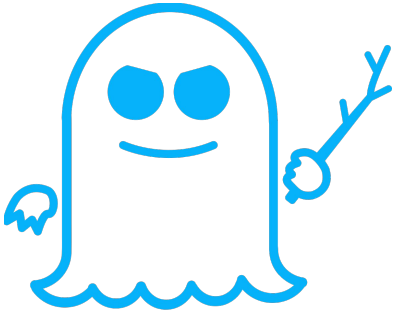


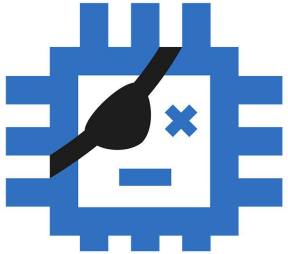
PhD student
getting paper accepted

** List probably non-exhaustive* ** Special congrats if you recognize all tools!*








PhD student in despair discovering mu-arch atks

** List probably non-exhaustive*

** Special congrats if you recognize all attacks!*


DON'T WORRY. WE GOT YOUR BACK.
makeameme.org

Proteus: An Extensible RISC-V Core for Hardware Extensions

Marton Bognar[1]*, Job Noorman[1], Frank Piessens[1]

- **Static** / **Dynamic** pipeline (textbook implem)
- **Optimizations**: OoO Speculative Execution, Cache, ~Prefetchers, more to come!
- **Configurable**: #Exec units, ROB size
- **Extensible**: plugin system
- **SpinalHDL** > Verilog > FPGA / Simulator
- **Validate:** HW fuzzing / verif. setup (in progress)

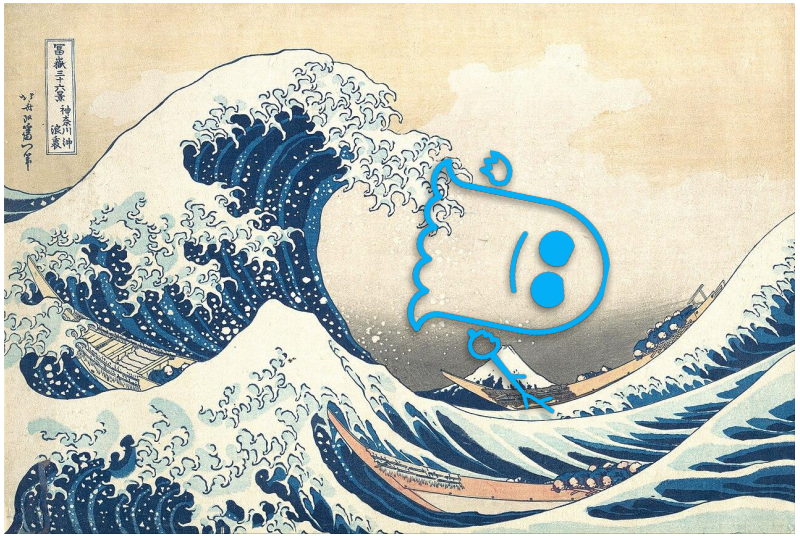
PROSPECT: Provably Secure Speculation for the Constant-Time Policy

Lesly-Ann Daniel[1], Marton Bognar[1], Job Noorman[1], Sébastien Bardin[2], Tamara Rezk[3] and Frank Piessens[1]

[1]imec-DistriNet, KU Leuven, 3001 Leuven, Belgium
[2]CEA, List, Université Paris Saclay, France
[3]INRIA, Université Côte d'Azur, Sophia Antipolis, France

- HW-SW co-design (SW marks secrets)
- **CT code secure against Spectre**
- Without sacrificing speculation
- Holds for many variants of Spectre

Wave your troubles awaaaaay!



Spectre waved away

Architectural Mimicry: Innovative Instructions to Efficiently Address Control-Flow Leakage in Data-Oblivious Programs

Hans Winderix
imec-DistriNet
KU Leuven

Marton Bognar
imec-DistriNet
KU Leuven

Job Noorman
imec-DistriNet
KU Leuven

Lesly-Ann Daniel
imec-DistriNet
KU Leuven

Frank Piessens
imec-DistriNet
KU Leuven

- HW-SW co-design (new ISA)
- Secure secret-dependent control-flow
- Support for linearization/balancing
- **Accelerate CT code**

Surf on the wave for extra speeeeed!

High-speed surfing on the Proteus wave

What comes next?

Better support

- **Compiler** support for HW defenses
- Hardware **validation**

More features

- **Wave away** more troubles! (DDP)
- **Surf** faster! (Accelerate CT code)
- Deliver **coffee**? (But hard problem)

https://github.com/proteus-core

Surf / wave your troubles away with Proteus too!