POLEN: Combining Polymorphism and Program Encryption to Guarantee Data and Code Confidentiality

Lionel Morel – joint work with Nicolas Belleville, Damien Couroussé, Irenée Groz.

Context - Motivations

Side-channel attacks

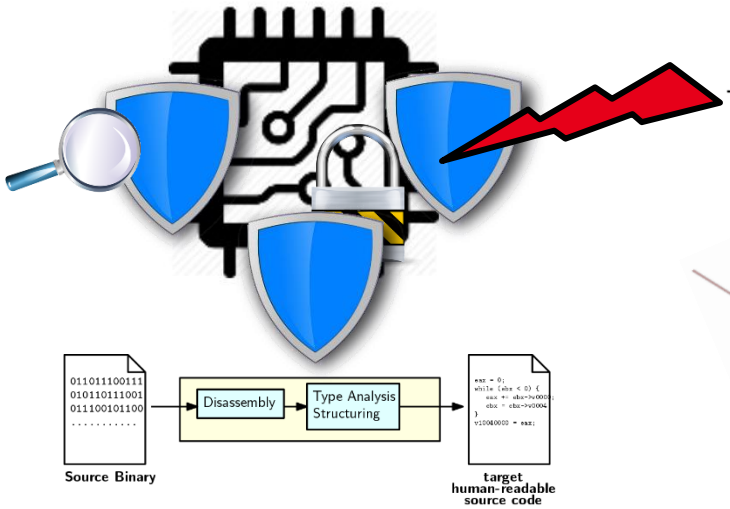
Hiding

Masking

Fault attacks

Fault Tolerance

Fault Detection



Reverse-engineering

Encryption

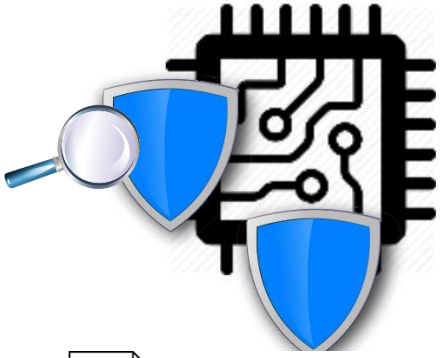
SW/HW co-design of Security Solutions:

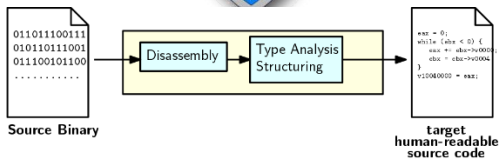
- Complementarity of HW ans SW solutions
- Systematic application of SW counter-measures

➔ Work within the compiler

Polen: HW and Compiler to address SCA + Reverse

Side-channel attacks





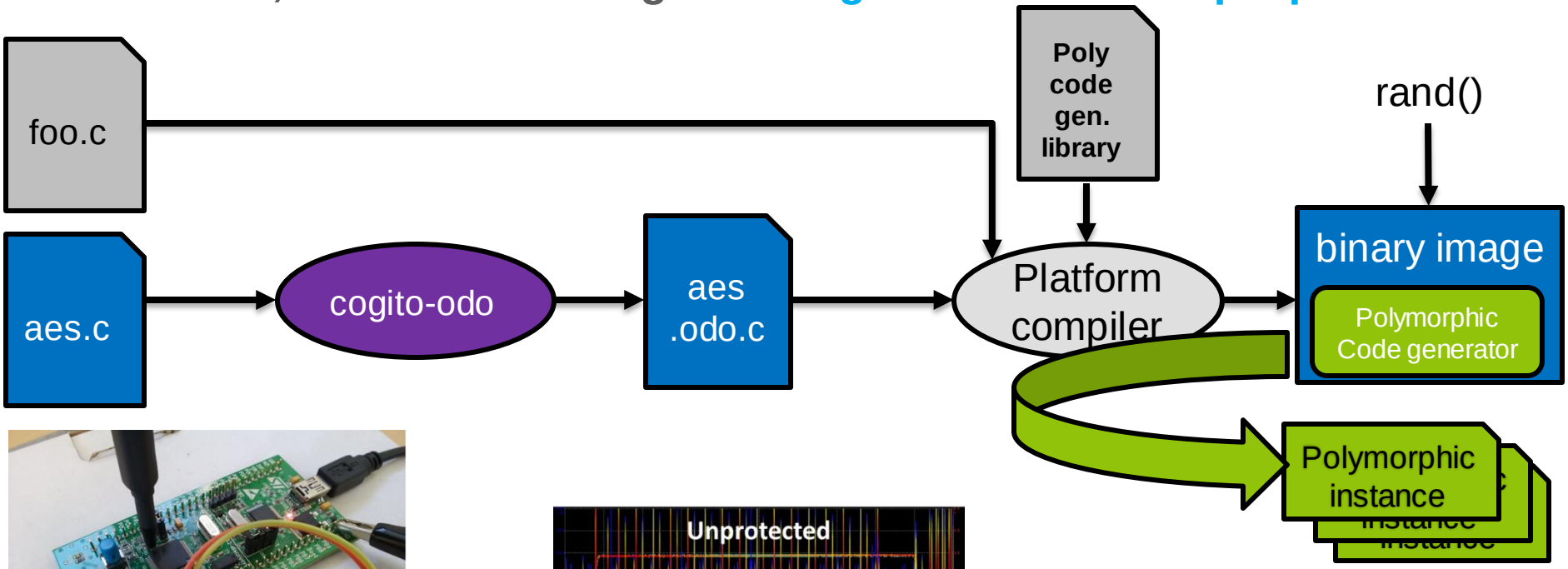
Reverse-engineering

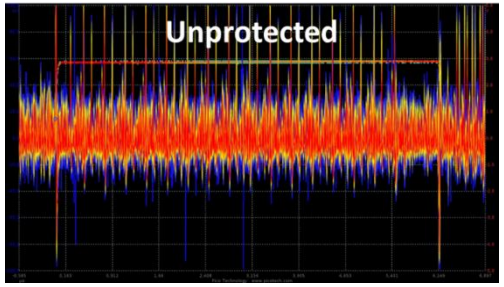
POLYMORPHISM: Automatic hiding based on dynamic code generation

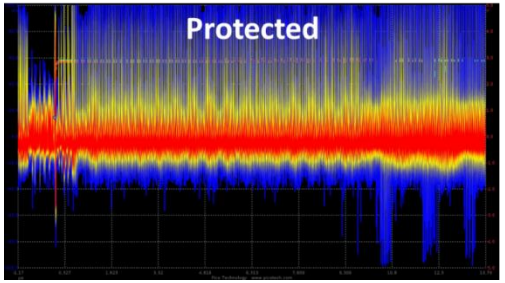
ENCRYPTION: Compile-time program encryption + HW support for decryption

Code Polymorphism

- **Principle: regularly change the behavior of a component, at runtime, while maintaining unchanged its functional properties.**



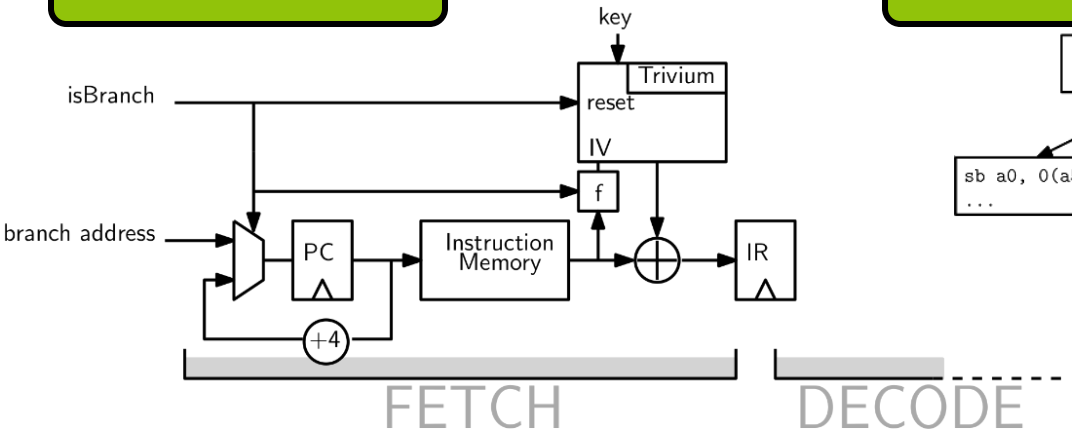




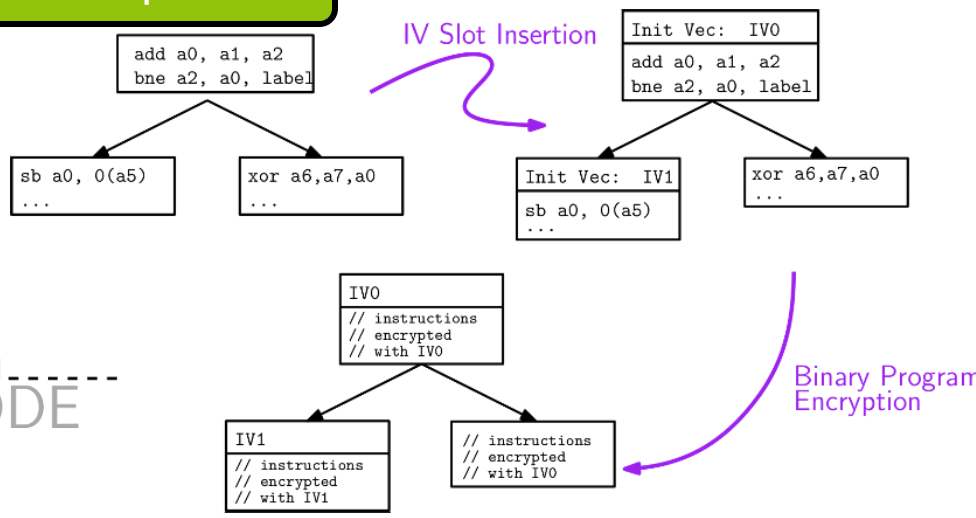
N. Belleville, D. Couroussé, K. Heydemann, and H.-P. Charles. 2018. Automated Software Protection for the Masses Against Side-Channel Attacks. ACM Trans. Archit. Code Optim. 15, 4, Article 47 (November 2018), 27 pages.

Code Encryption

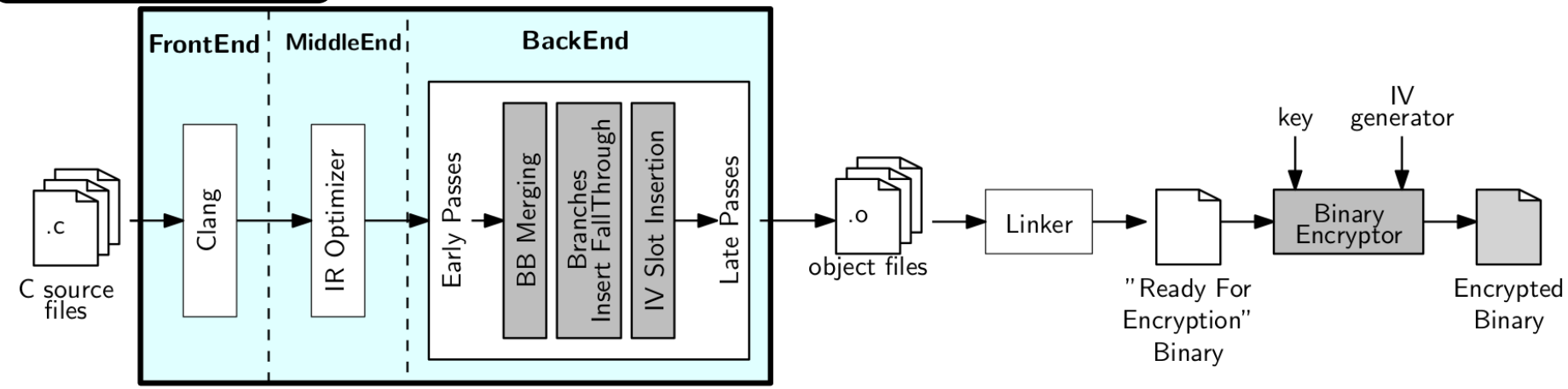
Hardware



Compiler

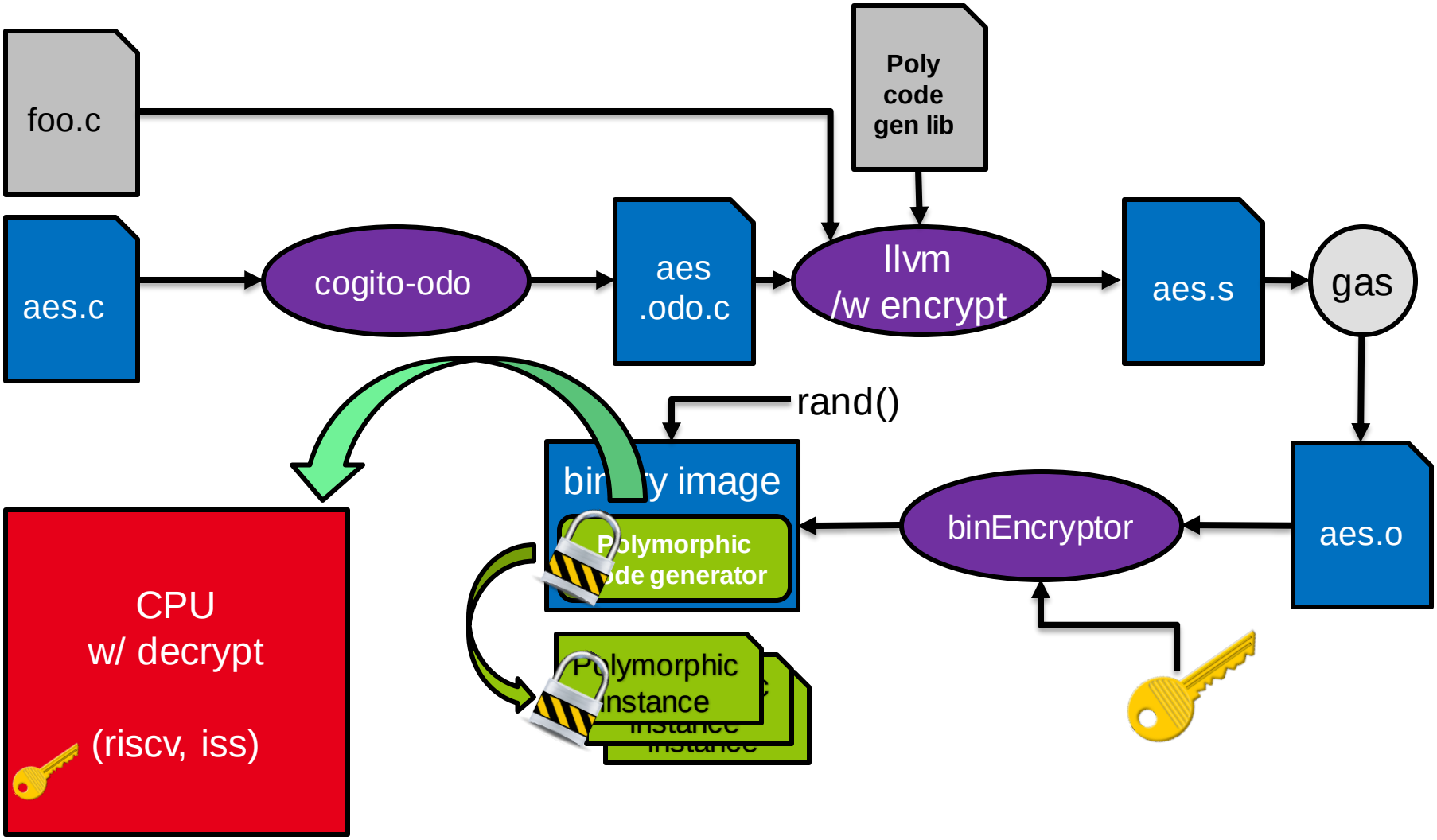


Toolchain



T. Hiscock, O. Savry and L. Goubin, "Lightweight Software Encryption for Embedded Processors," 2017 Euromicro Conference on Digital System Design (DSD), Vienna, 2017, pp. 213-220.

POLEN : Current Status



Polen: Current Status

- **Cogito-odo** now targets **RISCV ISA** (+ARMv7)
- **llvm-RISCV** back-end generating **encryption-ready** binaries
- Standalone **binary encryptor**
- **HW decryption** added to the **Spike** Instruction Set Simulator
- Currently working on the encryption of polymorphic instances

	SCA	Static Reverse	Dynamic Reverse
Encrypted Program	✗	✓	✗
Code Polymorphism	✓	✗	✓
Encrypted program + Polymorphism	✓	✓	✓

COGITO

RISC-V

leti
Centre de Grenoble
17 rue des Martyrs
38054 Grenoble Cedex

list
Centre de Saclay
Nano-Innov PC 172
91191 Gif sur Yvette Cedex