ÉQUIPE PROJET
PACAP

Tel : 02 99 84 25 01
Mail : nicolas.kiss@inria.fr

Inria Rennes Bretagne-Atlantique
Campus de Beaulieu, 263 Avenue
Général Leclerc, 35042 Rennes

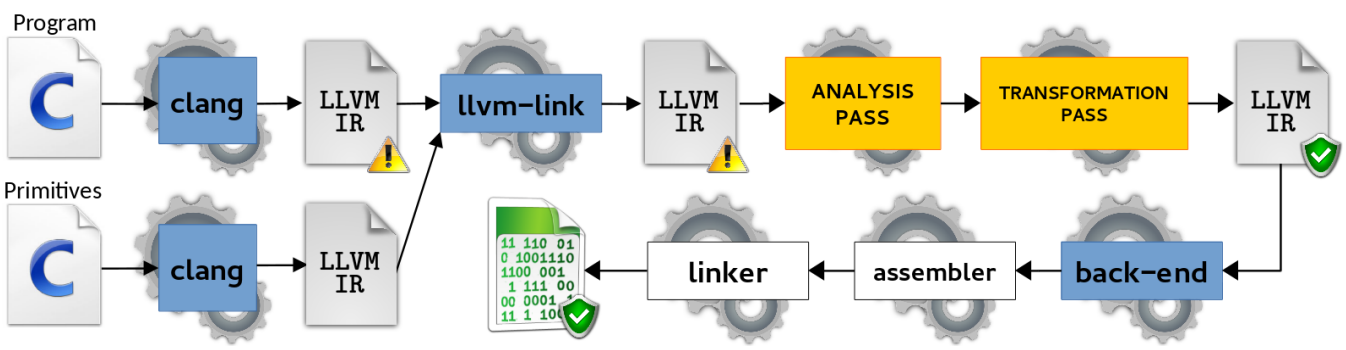
SECODE

Compiler-based automation of side-channel countermeasures

Nicolas KISS Erven ROHOU Damien HARDY

Compiler-automated transformation

The idea is to insert software protections against physical threats (e.g. masking, error correcting codes) automatically during compilation.



Advantages of compile-time transformation :

- Automation of the whole process (no source or assembly editing)
- Invisible for the software programmer (like compiler optimizations)
- Low-level control over the target program (e.g. memory allocation)
- Coverage of most Instruction Set Architectures (ARM, AVR, x86, ...)

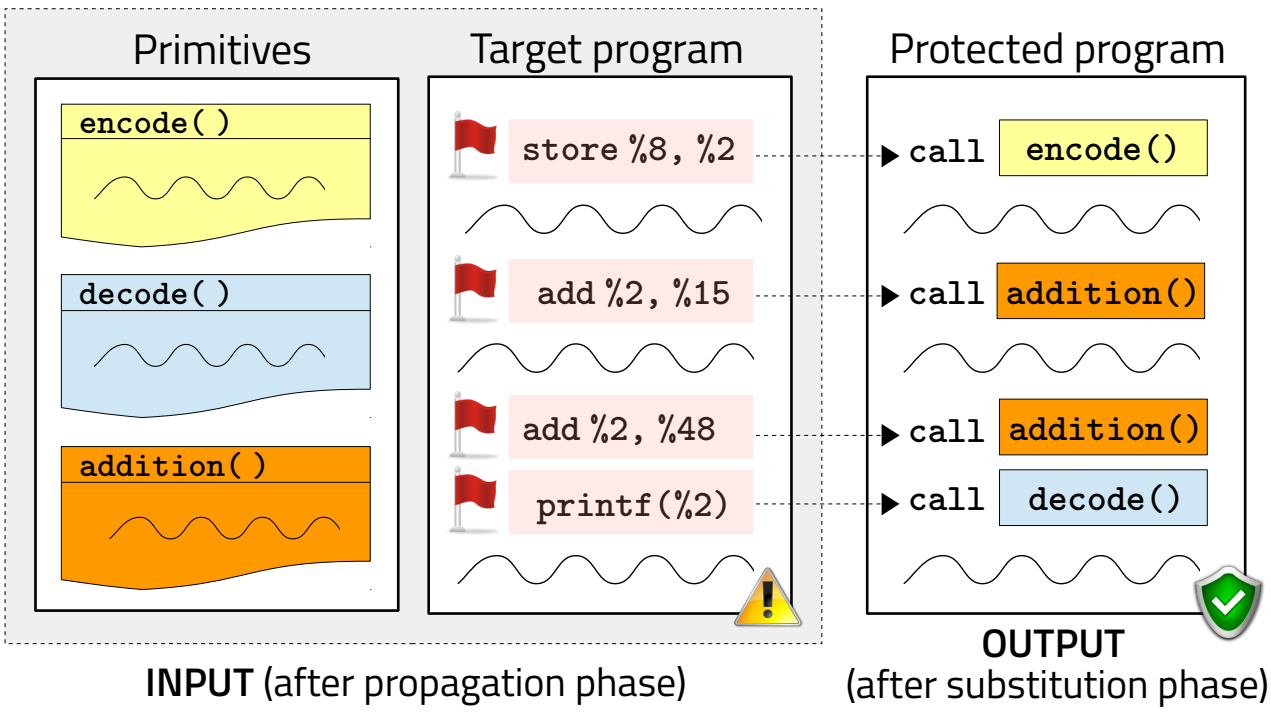
Reconfigurable countermeasures

USER

- Annotate the sensitive variables in the source program ( ) with a specific keyword.
- Define the transformation primitives (data type, operators) as functions in a separate C/C++ file. They can be written without having any knowledge about LLVM.

COMPILER

- **Propagation phase** :
  A data-flow analysis is performed to locate each sensitive instruction in the target program ( ).
- **Substitution phase** :
  Each sensitive variable is type-transformed to have a new data type. Each sensitive instruction is removed and replaced by a call to a primitive.

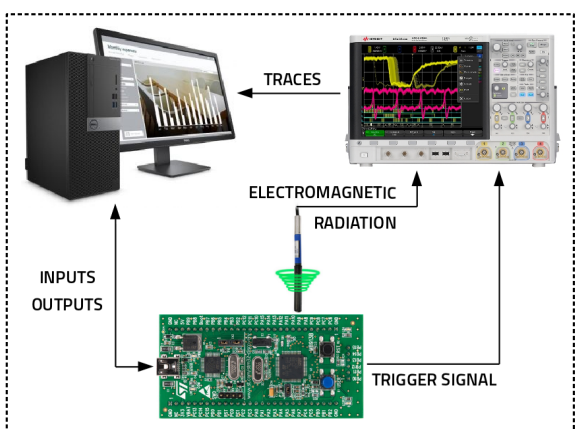


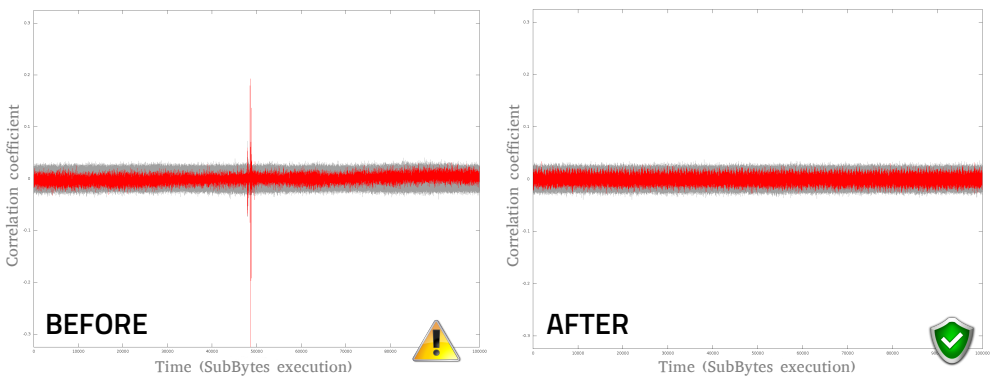
Experimental results

Application of **Boolean Masking** on an AES-128 implementation

Setup :

STM32F100RBT6B microcontroller (ARM Cortex-M3, 24MHz, 8KB RAM)





Side-channel analysis :

- Correlation Power Analysis (1st order) on AES 1st round
- 20,000 executions (traces)

Result : No correlation

Future work

Study the implementability of other transformations with primitives, such as :

- Orthogonal Direct Sum Masking (ODSM), Rotating Sboxes Masking (RSM)
- Hamming codes, Reed–Solomon codes, Linear Complementary Dual codes

This work was partially funded by the French National Research Agency (ANR) as part of the project SECODE (ANR-15-CHR2-0007).

Other SECODE partners are listed on the right.