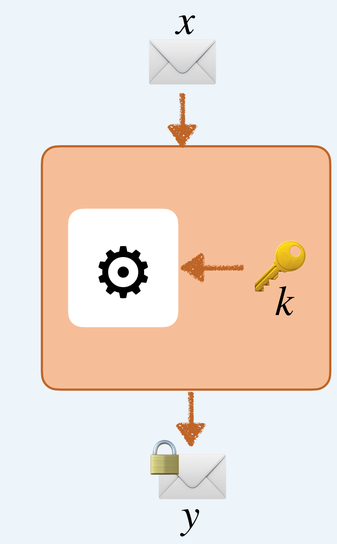
# Resistance of Threshold Implementations against Statistical Ineffective Fault Attacks

**Viet Sang Nguyen, Vincent Grosso, Pierre-Louis Cayrel**

Université Jean Monnet, CNRS, Laboratoire Hubert Curien URM5516, F-42023, Saint-Étienne, France

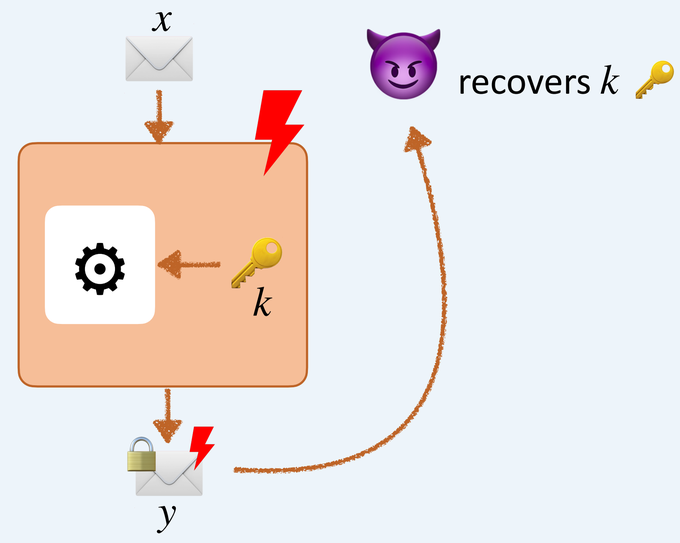
## Background

### Cryptography



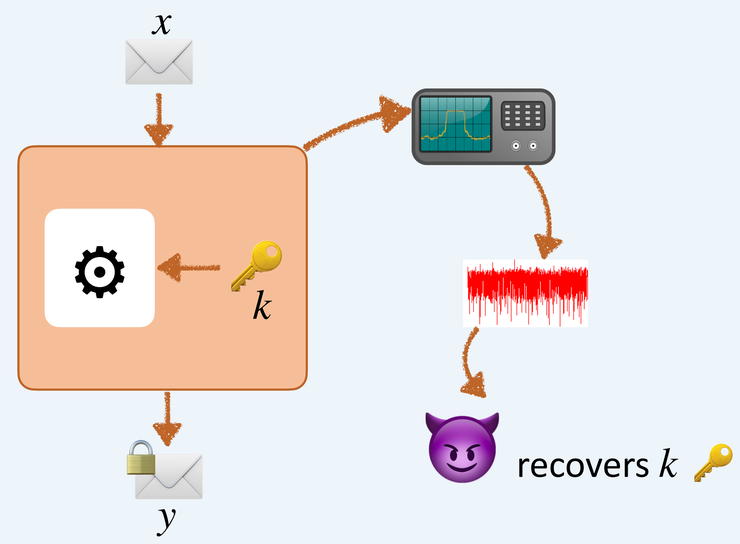

Key $k$ 🔑 must be protected

### Fault Attacks




Countermeasure: duplicate the computation, then compare the two outputs to detect faults

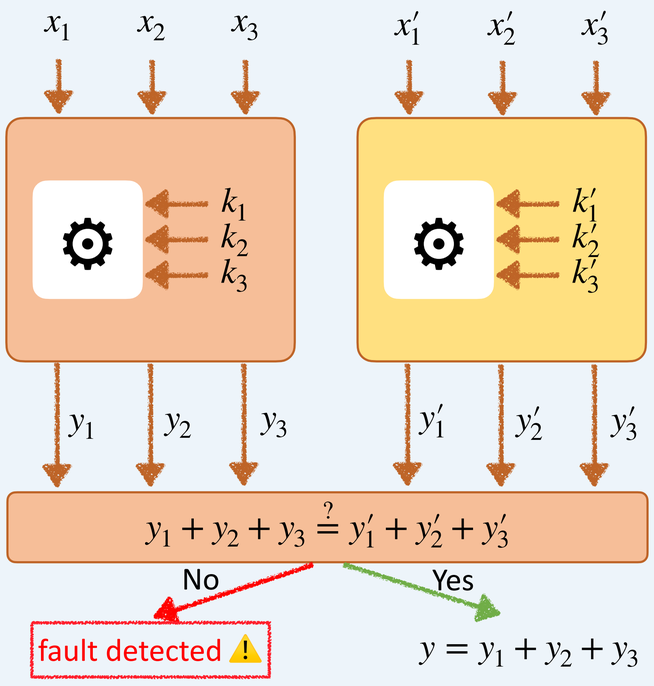
### Side-Channel Attacks




Countermeasure: avoid leakages by computation on shares $(x_1, x_2, x_3)$ and $(k_1, k_2, k_3)$
where $x_1 + x_2 + x_3 = x$ and $k_1 + k_2 + k_3 = k$

## State Of The Art

### Combined Countermeasure



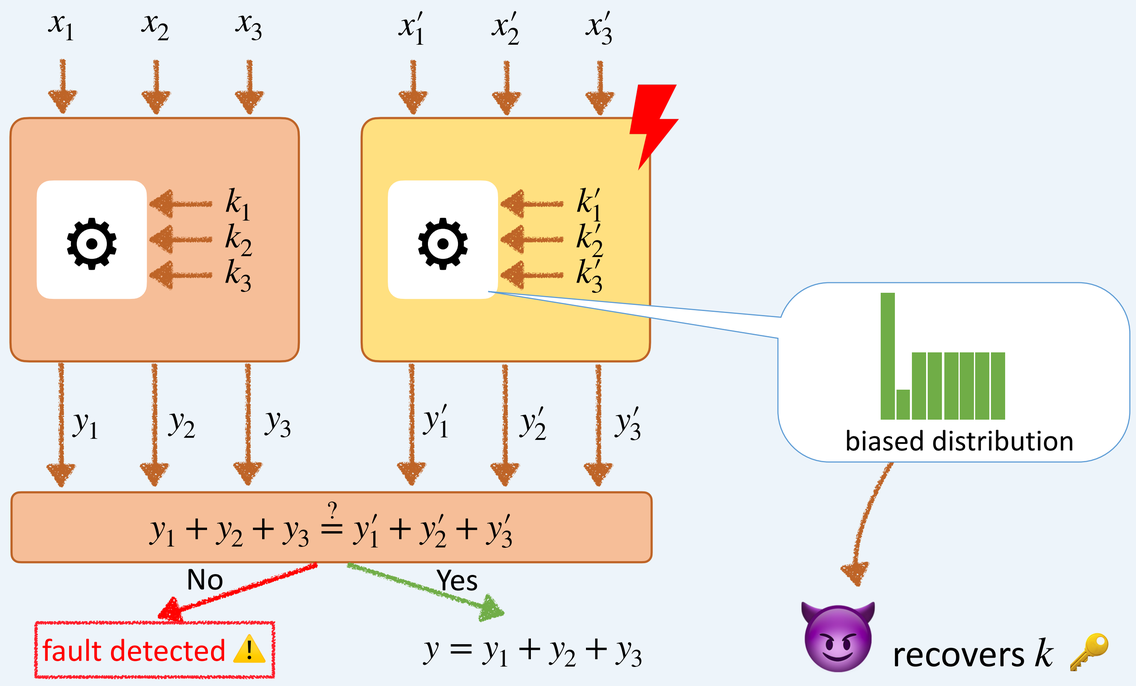

👉 Duplicate the computation

👉 Compute on shares

$x_1 + x_2 + x_3 = x'_1 + x'_2 + x'_3 = x$

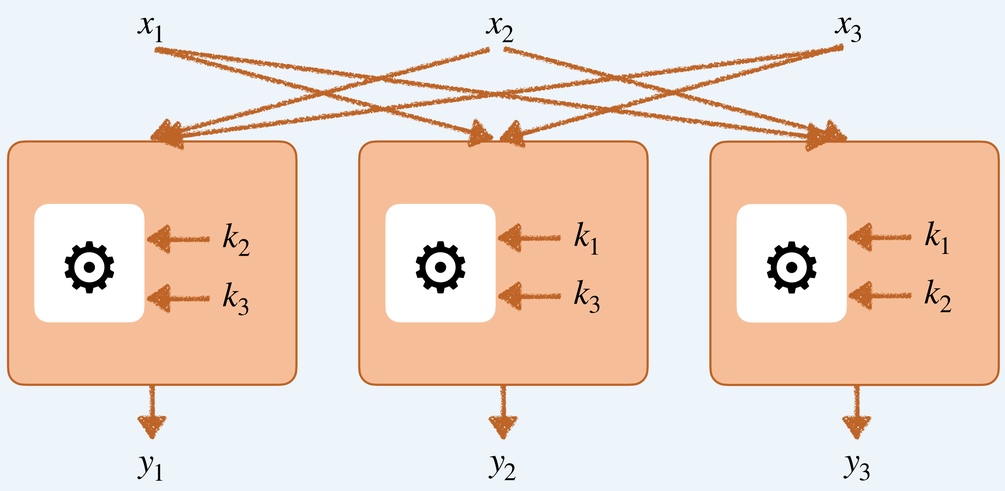
$k_1 + k_2 + k_3 = k'_1 + k'_2 + k'_3 = k$

### Statistical Ineffective Fault Attack




## Our Proposal

### Countermeasure

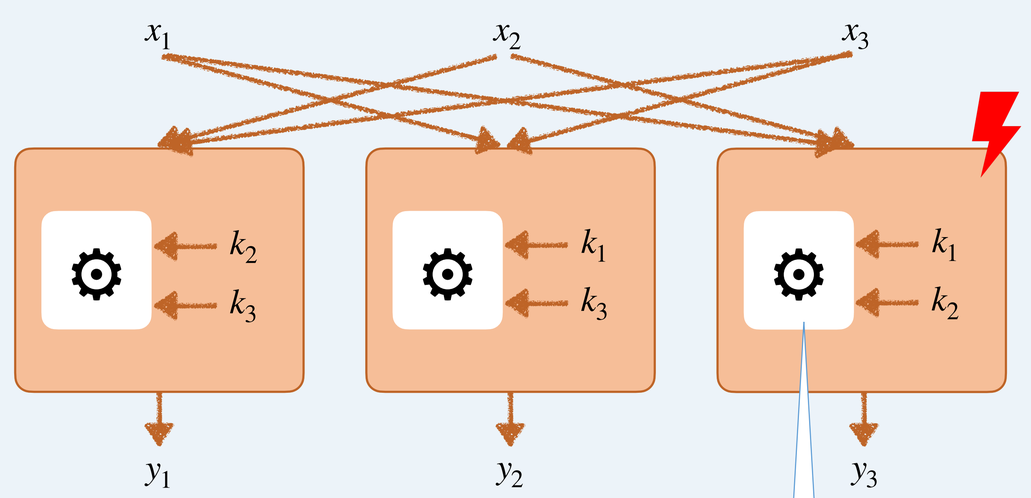



👉 Compute on non-complete set of shares

👉 Parallelize computations to harden precise fault injection

👉 No need duplication

### Result




PROPHY ANR-22-CE39-0008-01