Dynamic Reconfiguration as Countermeasure against DPA

Stanislav Jeřábek

Czech Technical University in Prague
Faculty of Information Technology, Department of Digital Design

Contents

Reliability vs. Security

Reliability

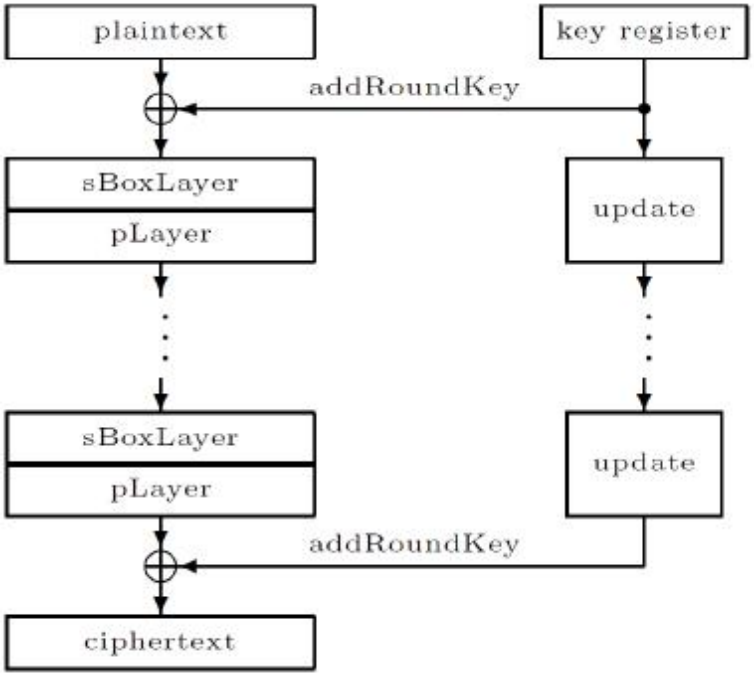
- Area or Time redundancy
- Generally worse security

Security

- Masking or another computation
- More faults possible

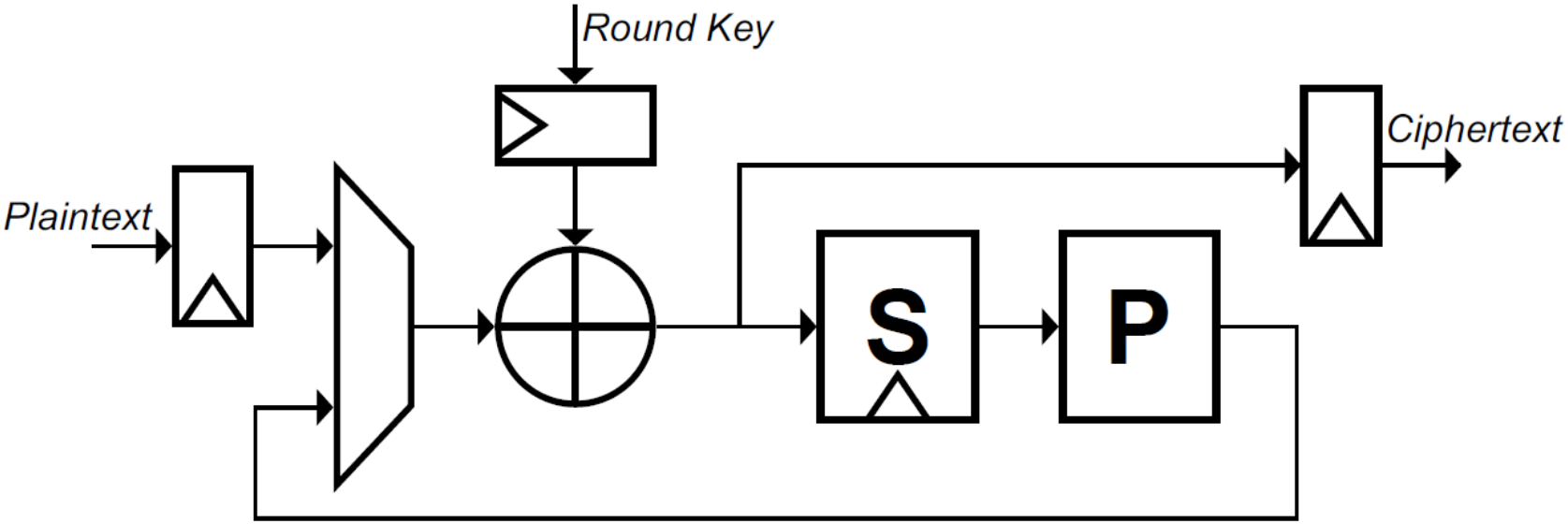
Present cypher

- Ultra–Lightweight cipher
- Block–cipher (64 bits)
- 80/128 bit key
- 32 rounds



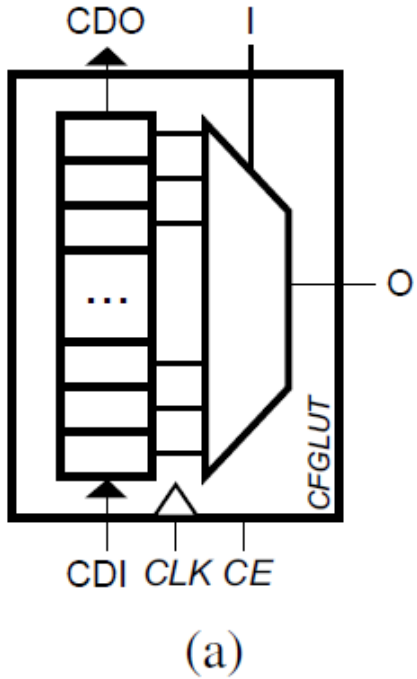
Countermeasure possibilities

- Masking
- Threshold implementation



S–box splitting

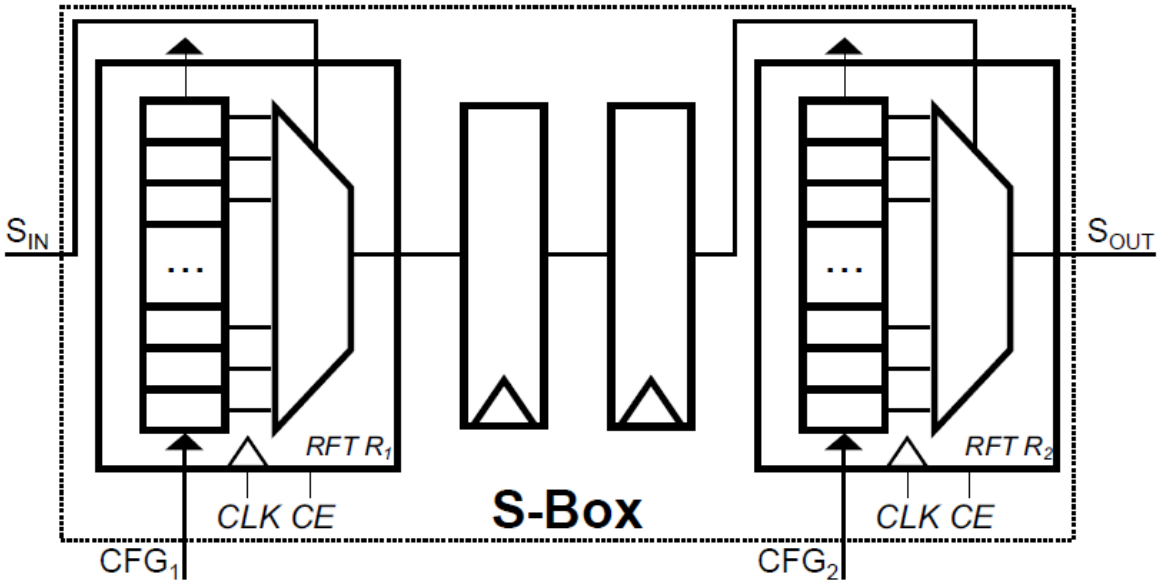
- Built–in CFGLUT
- Random reconfiguration
- Two entities
- Same function



(a)

DPA development board

- Artix–7 FPGA
- Threshold implementation



Other techniques

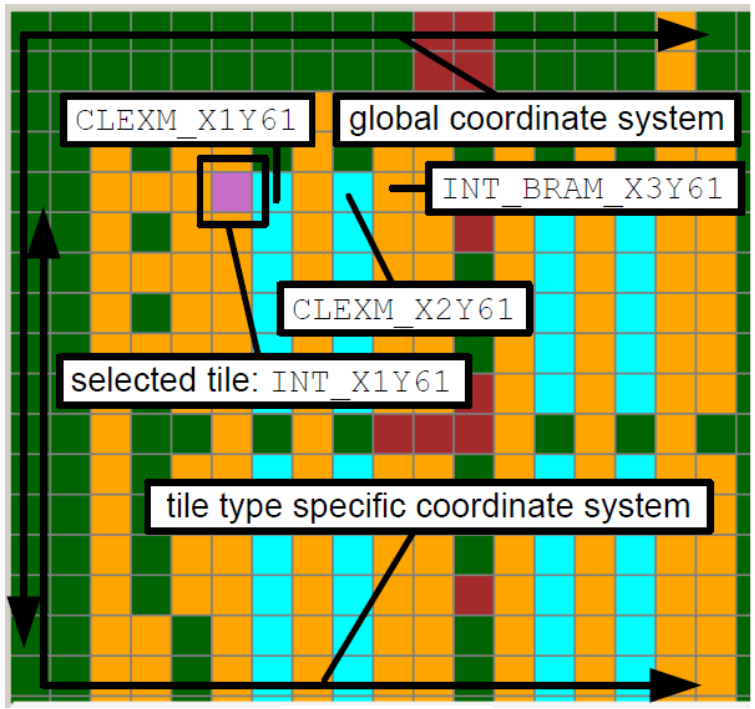
- 0/1 computations in parallel
- Another masking or threshold implementations

Preserving reliability

- Place & route knowledge

FPGA structure

- Pretty unknown
- Existing toolchains
- XDL format
- TORC



TORC

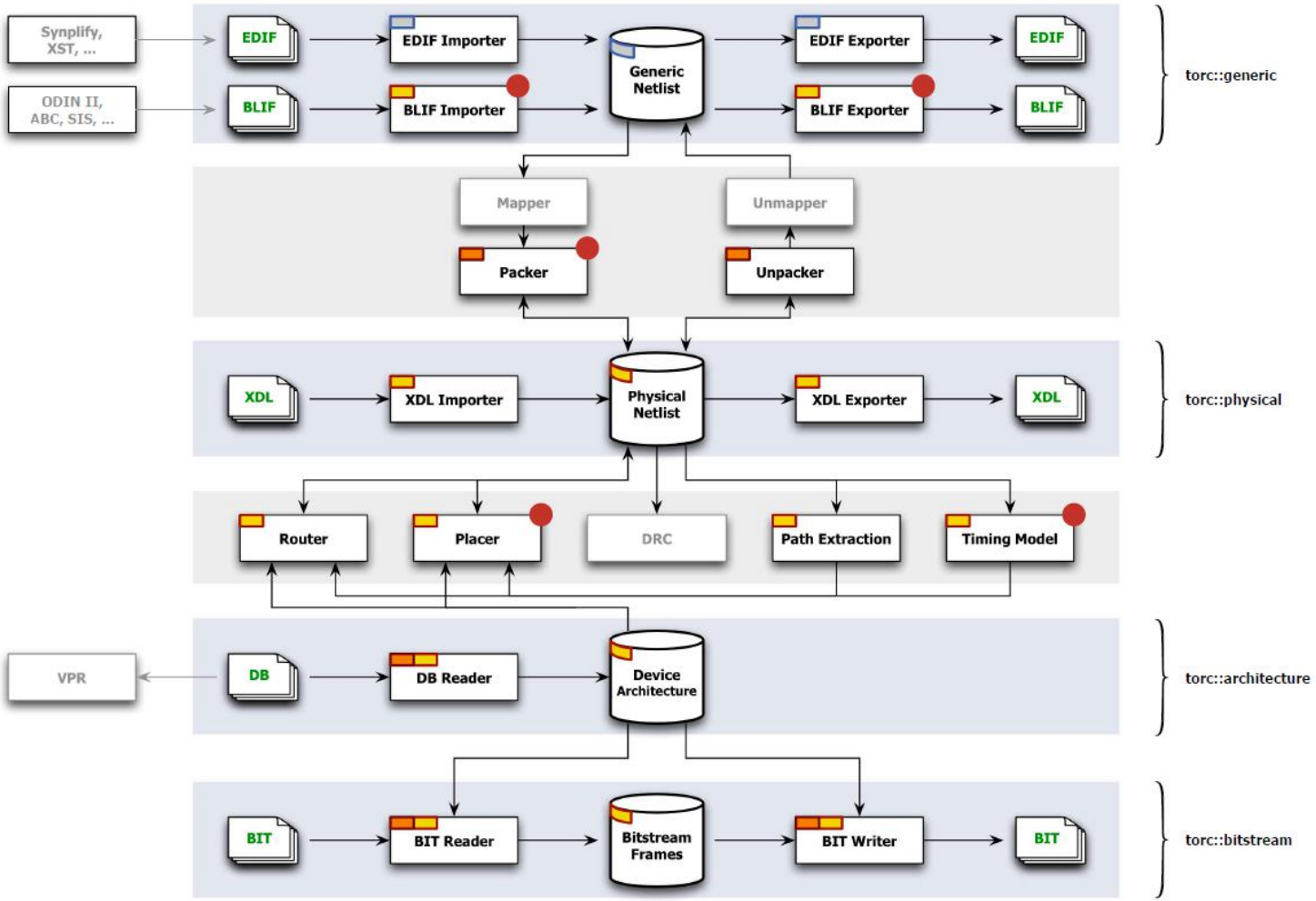


Figure 1: Torc block diagram. *Red dots indicate components still under development.*

Thank you for your attention!