

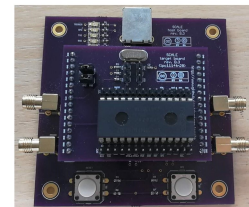
Crypto
engineer



Masking
Code



Realistic Device



Reverse-engineering
u-Arch

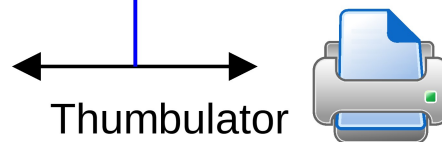
Leakage
detection
e.g.
TVLA/Chi2



uELMO

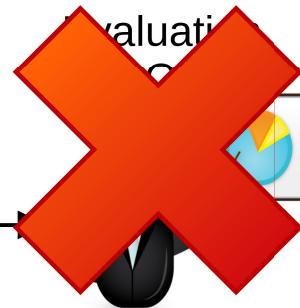


Leaking states



Thumbulator

Attack
evaluation



Quality guarantee with
F-test