KU LEUVEN

COSIC

Beyond the limits: SHA-3 in just 49 slices

Victor Arribas

10/09/2019

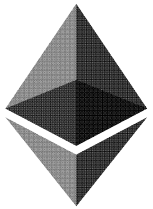
FPL 2019

Hash functions

Authentication

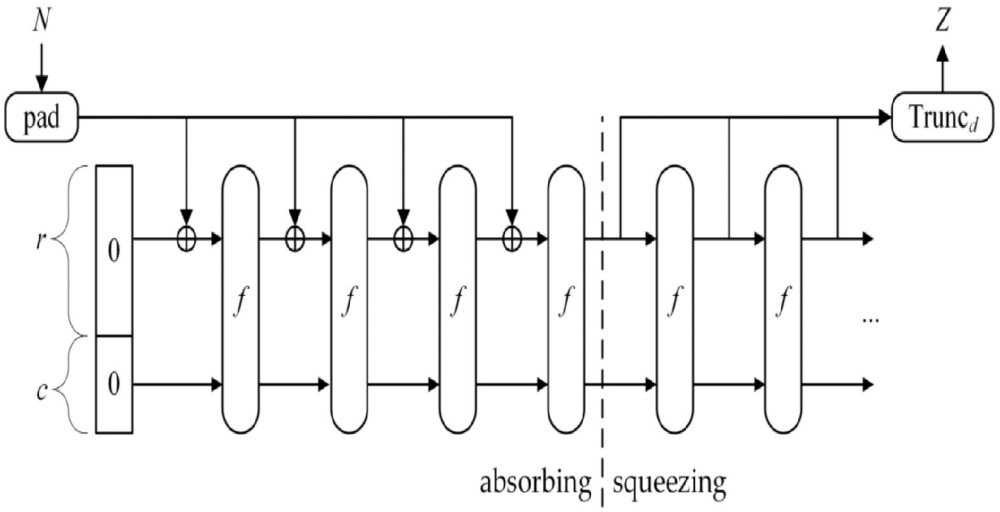
Key derivation

Digital signature

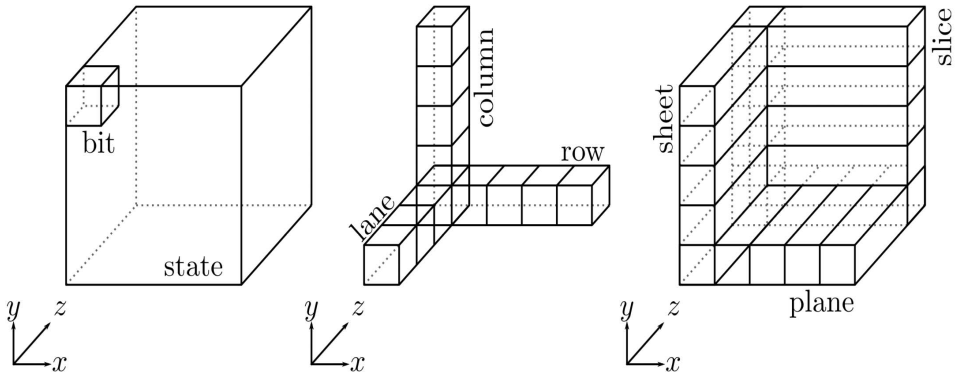


Cryptocurrencies

SHA-3

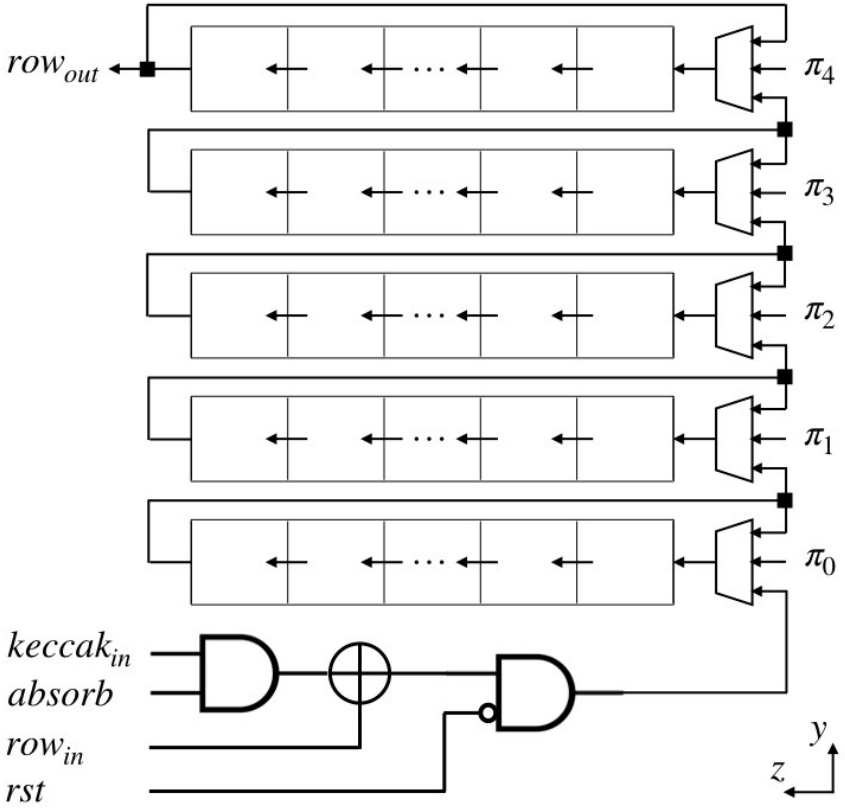


Sponge construction

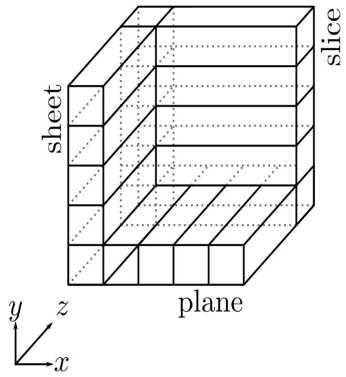


Keccak

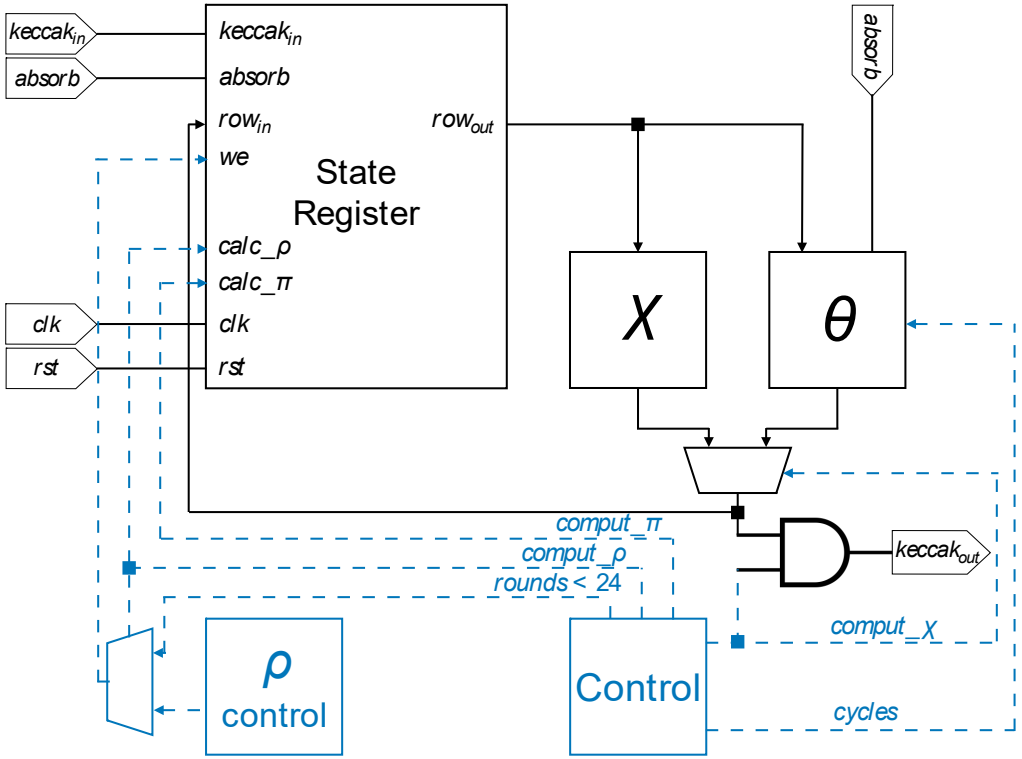
Row-based processing



- SRLs to compute 5 permutations $(\theta, \rho, \pi, \chi, \iota)$
- Compute θ, χ and ι perms. in row fashion



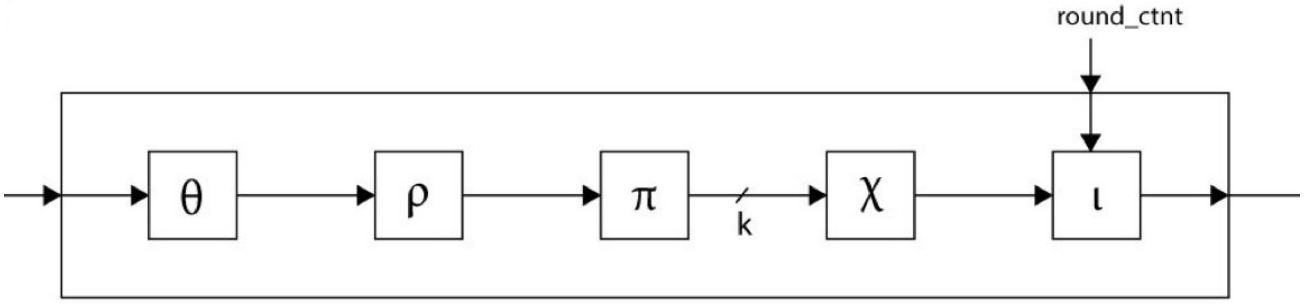
Row-based processing



- SHA3-AF: use of special gates AND2L & OR2L
- SHA3-A: limit to LUT6_2
- Up to 46% area reduction
- Latency heavily affected

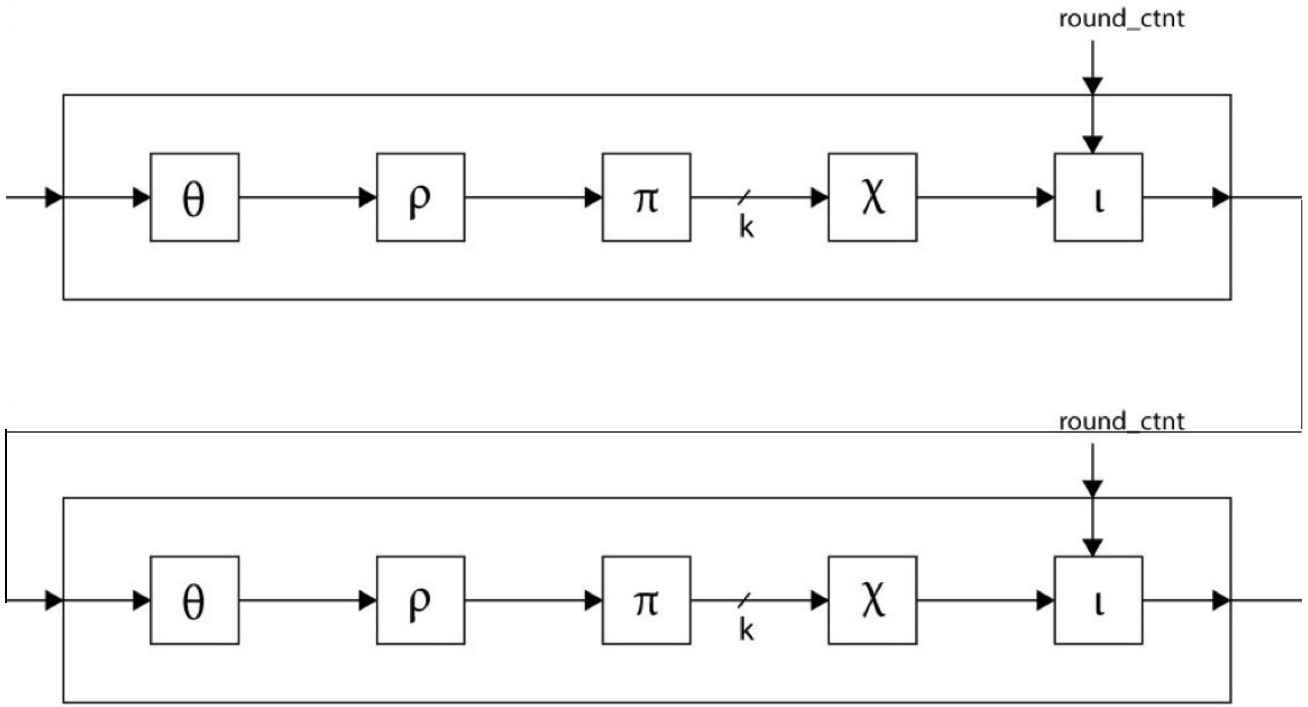
Area-Throughput efficiency

$$E = \frac{T}{A}$$



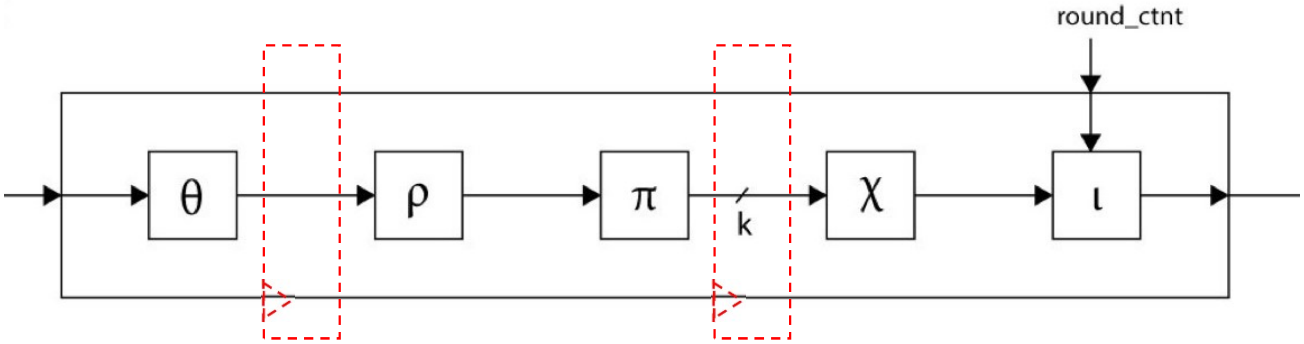
Area-Throughput efficiency

$$E = \frac{T}{A}$$

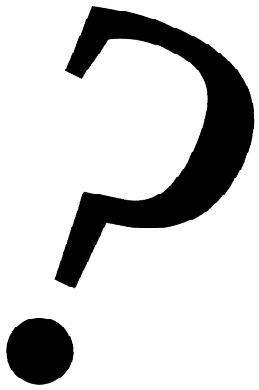


Area-Throughput efficiency

$$E = \frac{T}{A}$$

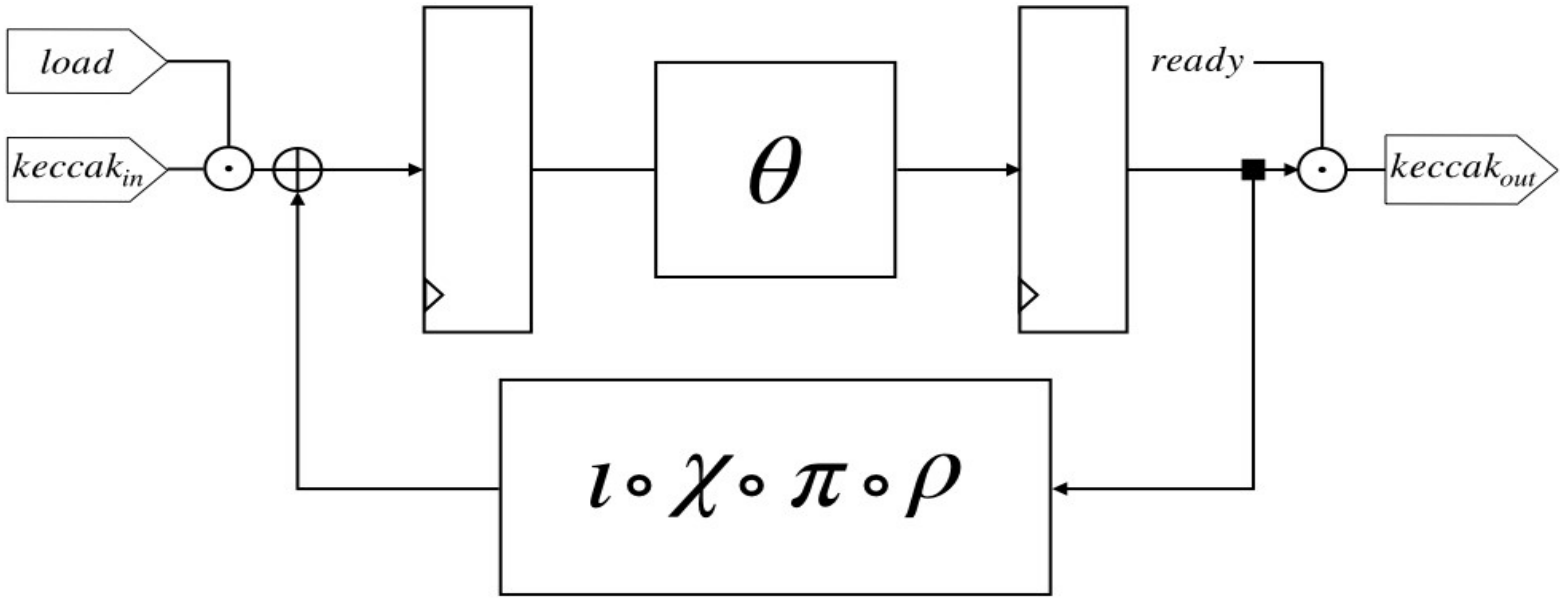


- Where?
- How many?



Area-Throughput efficiency

$$E = \frac{T}{A}$$



- Up to 70% area-throughput efficiency improvement

Physical attacks

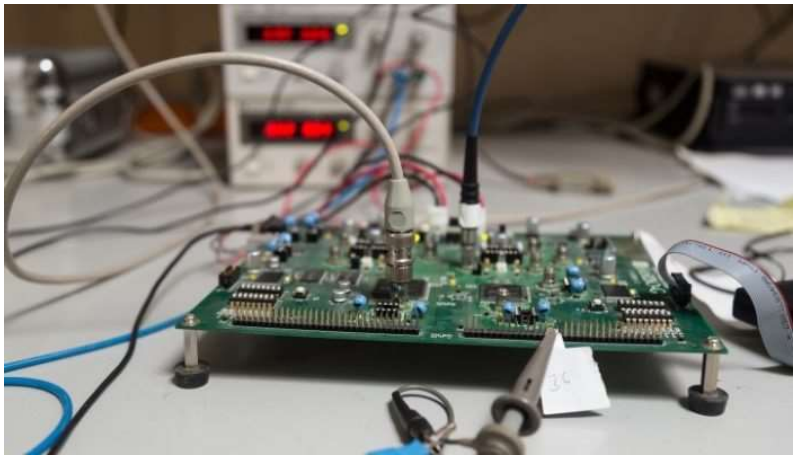
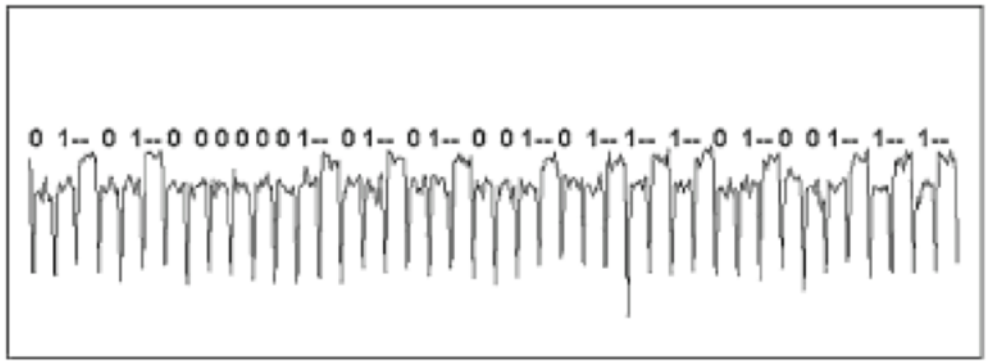


Photo by Peter Maene



Source: https://anysilicon.com/side-channel-attacks-differential-power-analysis-dpa-simple-power-analysis-spa-works/

- SCA Protected implementations needed
- Row-based proc. Implementations promise to have the lowest overhead

Thank you!