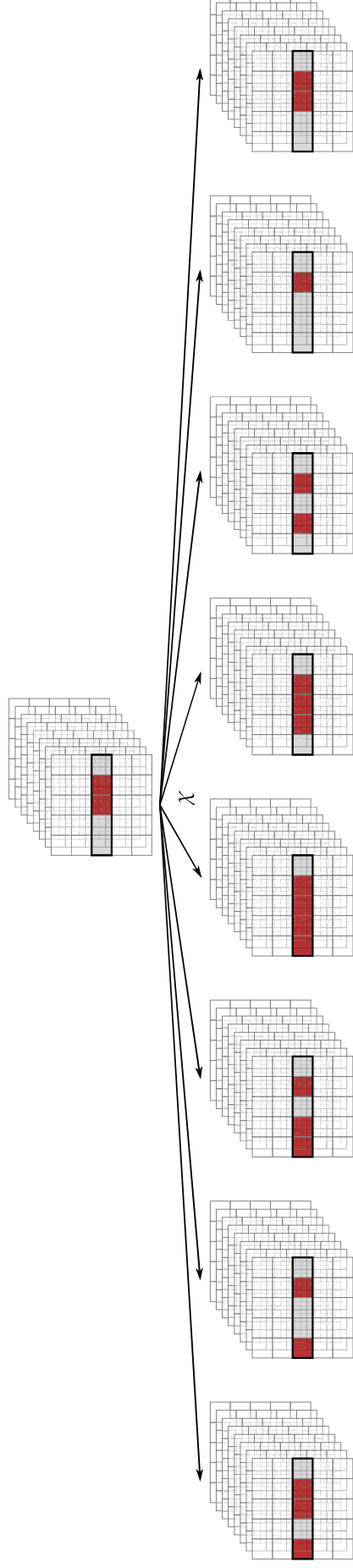
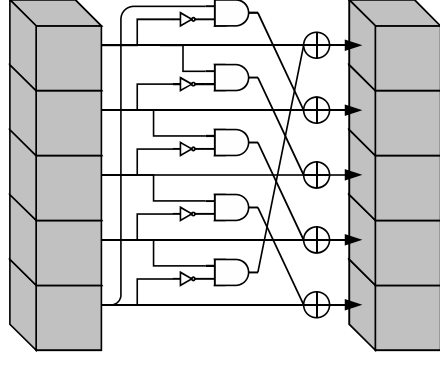


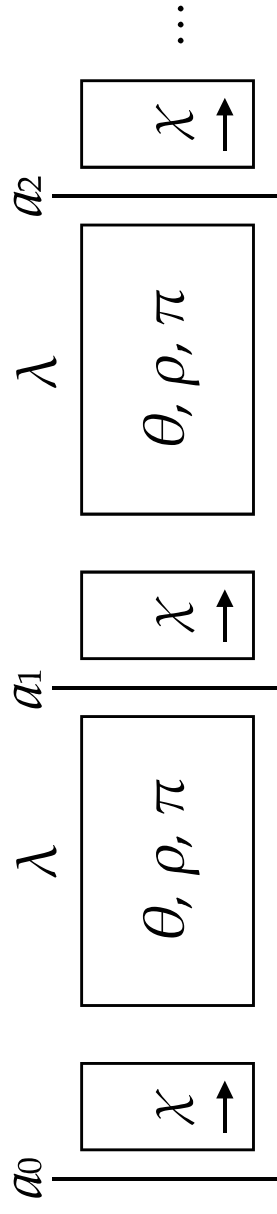
Non-linear mapping χ

- Transforms each **row** independently
- E.g., a difference going through χ
 - Output: affine space

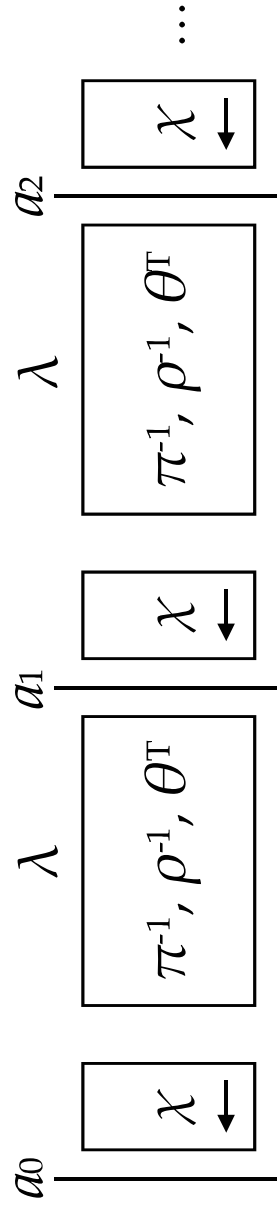


Differential and linear trails in KECCAKTools

- KECCAKTools
 - A set of documented C++ classes to help analyze KECCAK
Freely available on <http://keccak.noekeon.org>
 - Implements differential and linear trail propagation
- KeccakFPropagation works in “affine” direction:
 - Differential trails



- Linear trails: forward propagation means backwards in time



Bounds for differential trails in KECCAK- f [1600]

Rounds	Lower bound	Best known
1	2	2
2	8	8
3	32 [KECCAK team]	32 [Duc et al.]
4		134 [KECCAK team]
5		510 [Naya-Plasencia et al.]
6	74 [KECCAK team]	1360 [KECCAK team]
24	296	???

■ Pessimistic view

- Wide gap between bounds and known trails
- **Open problem:** narrow this gap (and also for linear trails)
- Bound too loose to prove ideal behavior

■ Optimistic view

- Proven absence of exploitable differential trail
- Trail weight apparently growing quickly with number of rounds

The best 3-round differential trail in KECCAK-f[1600]

