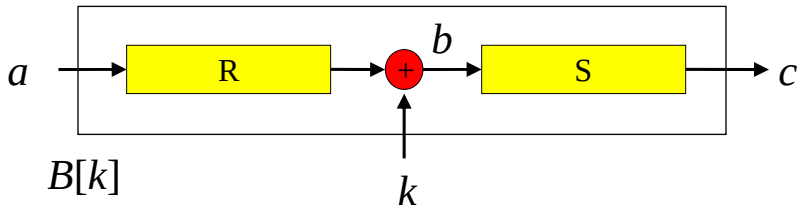
Plateau Trails

Joan Daemen* and Vincent Rijmen**

*STMicroelectronics **IAIK

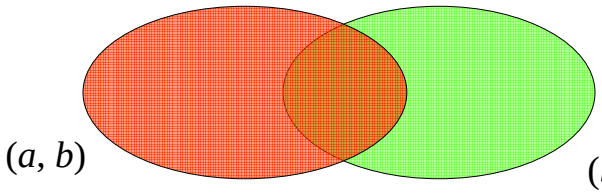
Consider a 2-round mapping



- $B[k](x) = S(k \oplus R(x))$
- Trails over $B[k]$: $Q = (a, b, c)$
  - Differential (a, b) over R
  - Differential (b, c) over S

Probability of trails over $B[k]$

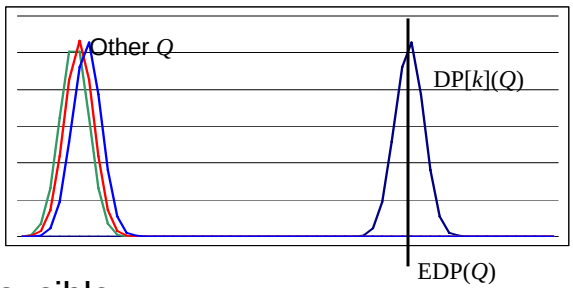
- Set of pairs following Q is intersection of
  - set of pairs following (a,b)
  - set of pairs following (b,c)
- If conditions are independent: $DP(a,b,c) = DP(a,b) \times DP(b,c)$
- $EDP(a,b,c) = EDP(a, b) \times EDP(b,c)$
  - Valid because addition with k makes conditions independent



3

Assumed distribution of $DP[k](Q)$

- In general $DP[k](Q) = EDP(Q)$ is not true, however…
- $\Pr(DP[k](Q) = i) \approx \delta(i - EDP(Q))$



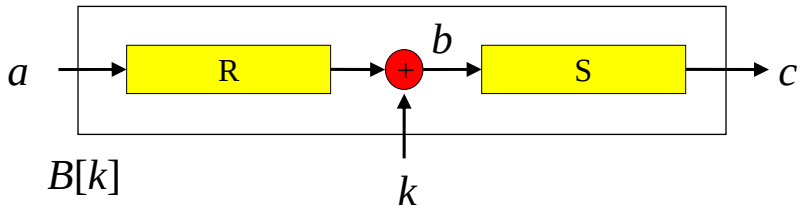
- Looks plausible …
- But actually, it's wishful thinking

4

Planar differentials and maps

- Planar differential (a, b):
  - Set of input pairs that follow the differential form an *affine space*
  - Set of output pairs that follow the differential form an affine space
- *Planar map:*
  - All differentials over the map are planar
  - Example: differentially 4-uniform S-boxes

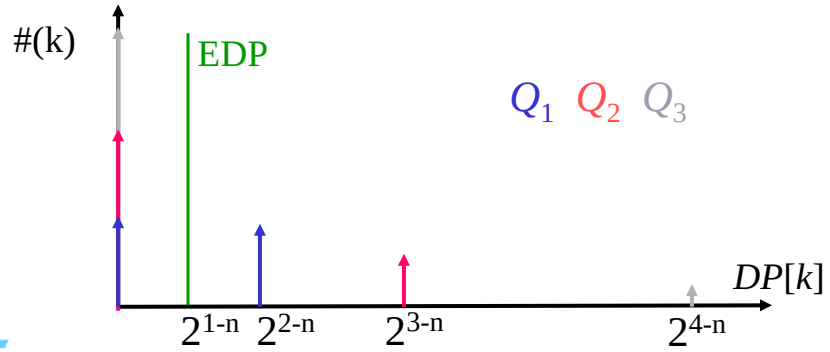
Plateau trail theorem



- If (a, b), (b, c) are planar differentials
- Then $DP[k](a, b, c) = 0$, or
  $= 2^{h(Q)} \pounds 2^{-n}$

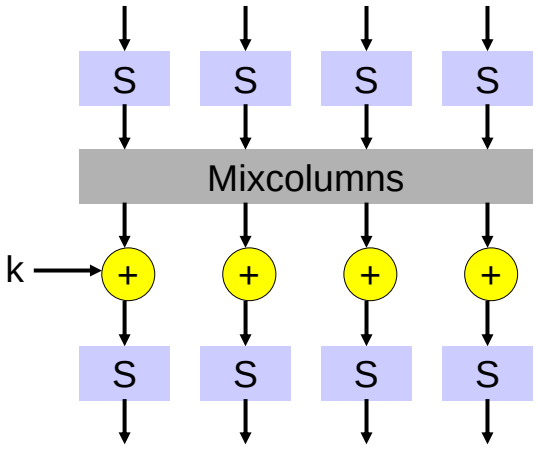
Distribution of $DP[k](Q)$

- $DP[k](Q) = 2^{h(Q)-n}$ for $2^{n-h(Q)}$ $EDP(Q)$ keys
- $DP[k](Q) = 0$ for the other keys



7

AES super box



8

AES super box trails: 5 active S-boxes

$h(Q)$

$-\log(EDP(Q))$	1	2	3	4	5
30		12.6	12.6	10.6	6.2
31	20.9	22.1	21.2	18.1	11.0
32	29.8	30.0	28.2	23.4	
33	37.1	36.9	33.7	26.4	
34	43.2	42.9	36.2		
35	48.0	47.5			

More rounds

- Four-round trails
  - Overwhelming majority are plateau trails
  - Probably vast majority are planar
- Then also most eight-round trails, ten-round trails, ... would be plateau trails