The Schedulability of AES As a Countermeasure Against Side Channel Attacks

Stephane Fernandes Medeiros
Université libre de Bruxelles

ULB

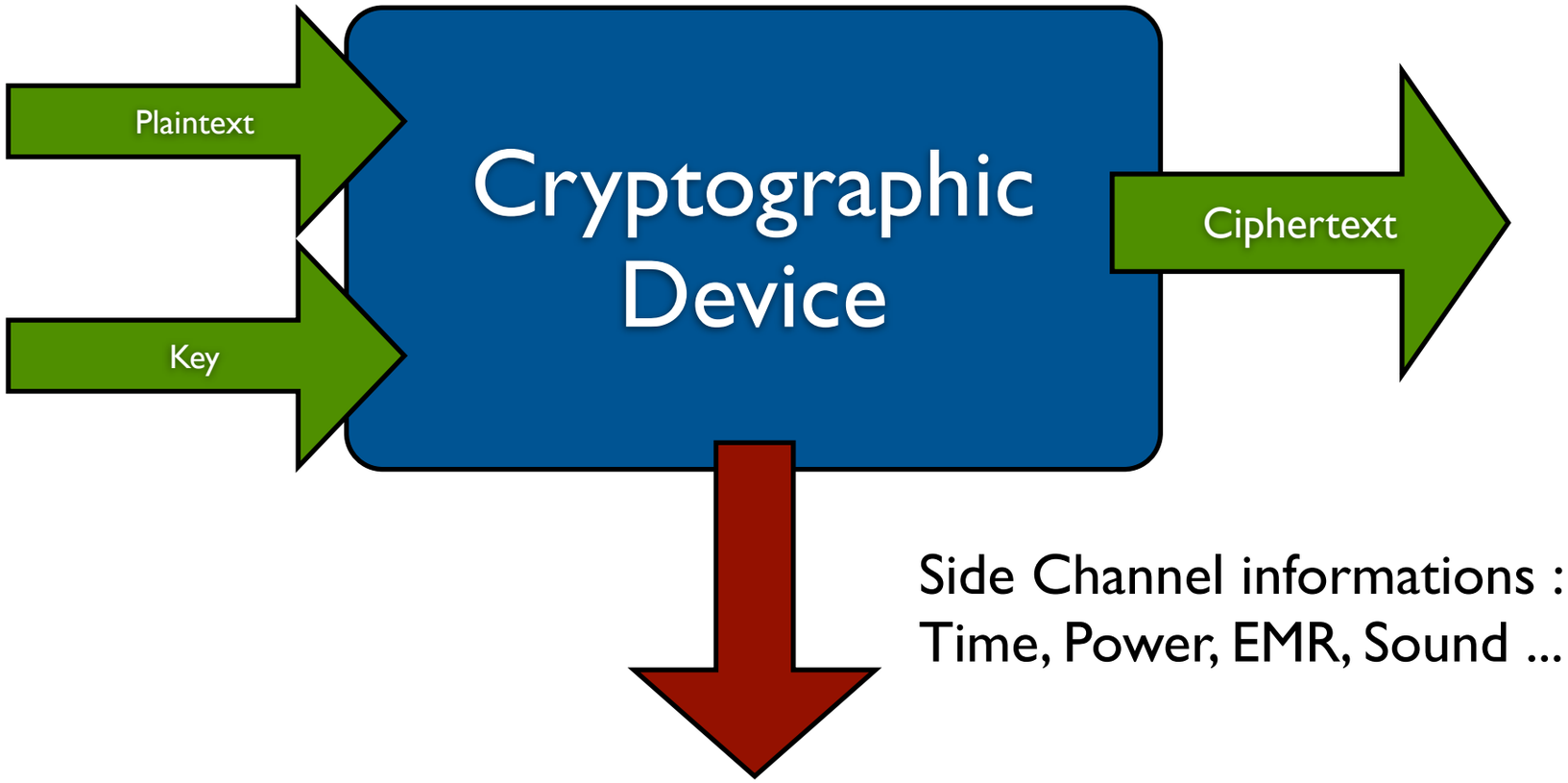
QualSEC

I

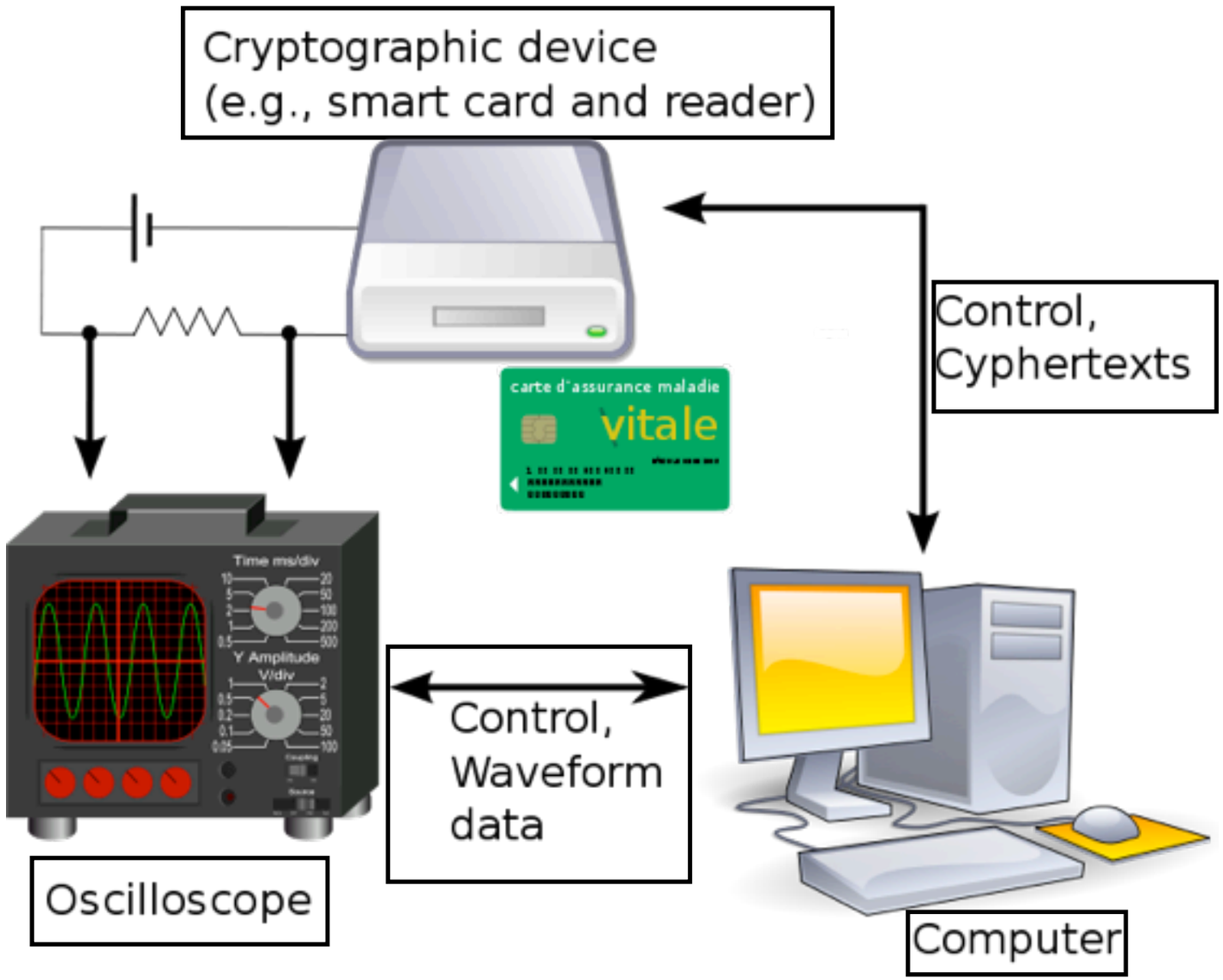
The Schedulability of AES As a Countermeasure Against

Side Channel Attacks

Side Channel Attacks

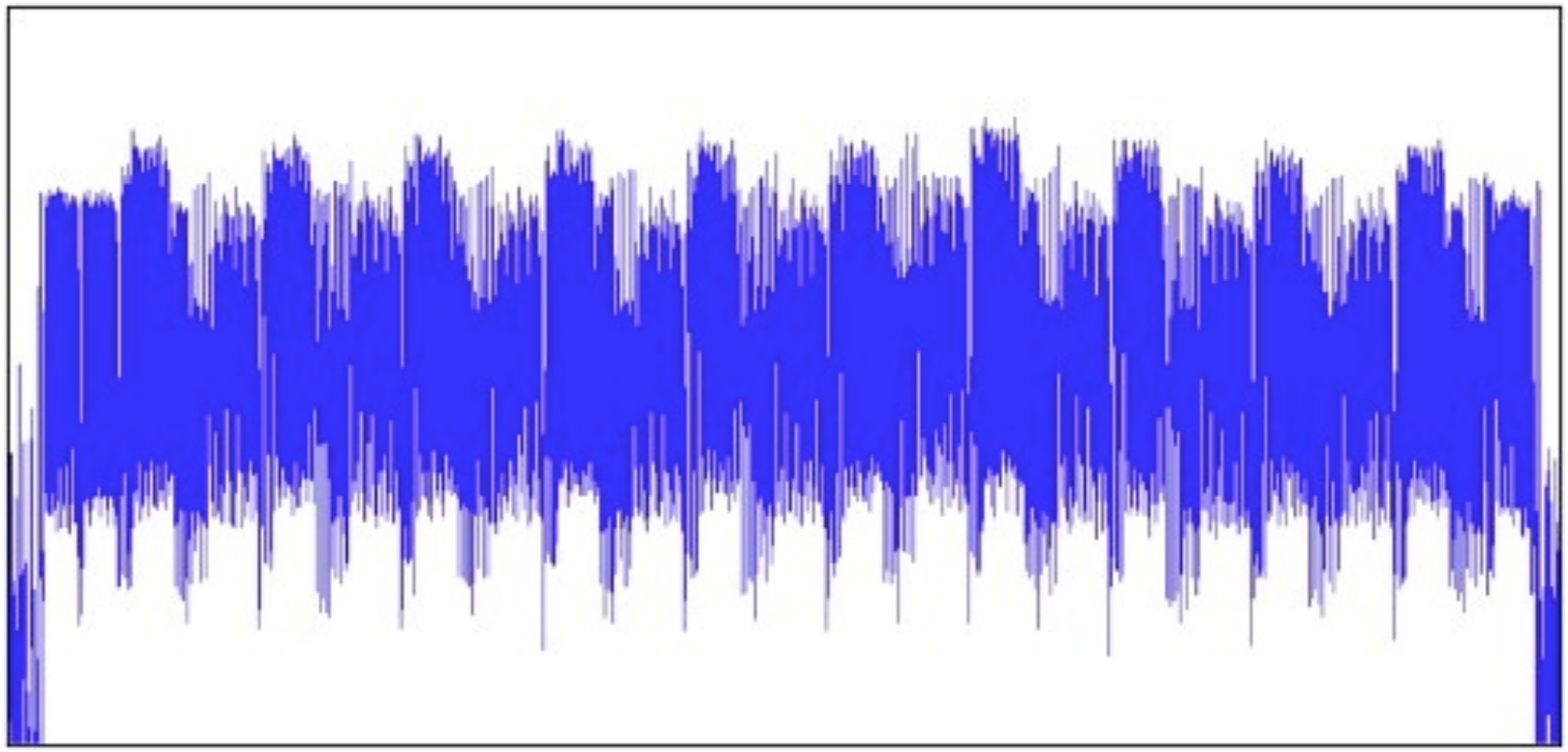


Power Analysis

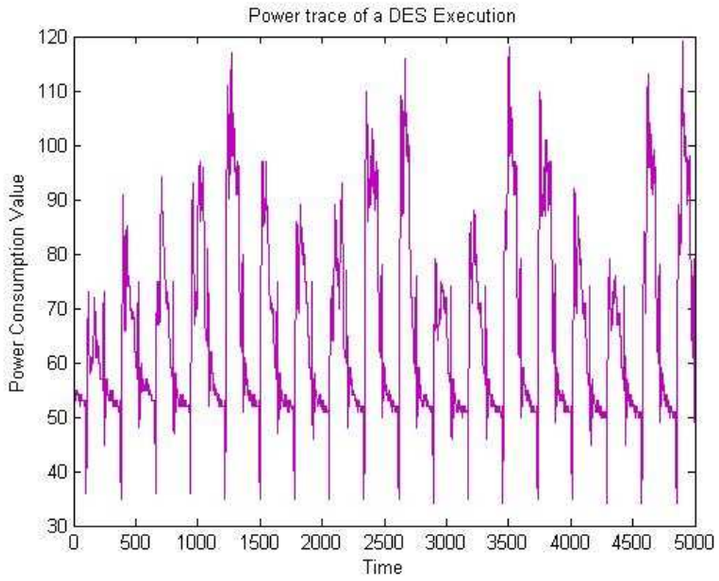


wikipedia

Power Analysis

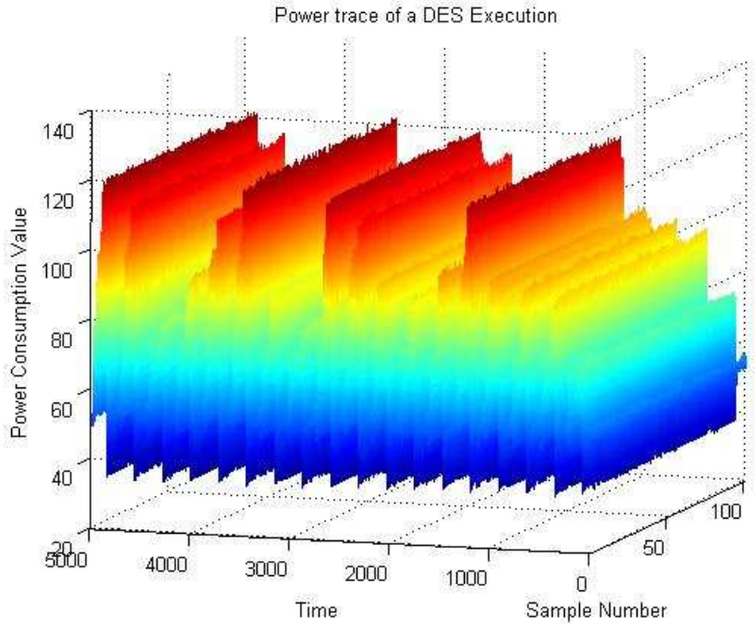


Power Analysis



<=>

1.0	1.2	0.8	0.2	1.4	2.0	…	…	…	0.1



<=>

1.0	1.2	0.8	0.2	1.4	2.0	…	…	…	0.1
…	…	…	…	…	…	…	…	..	..
1.1	1.0	0.8	0.2	1.5	2.0	…	…	…	0.2

II

The

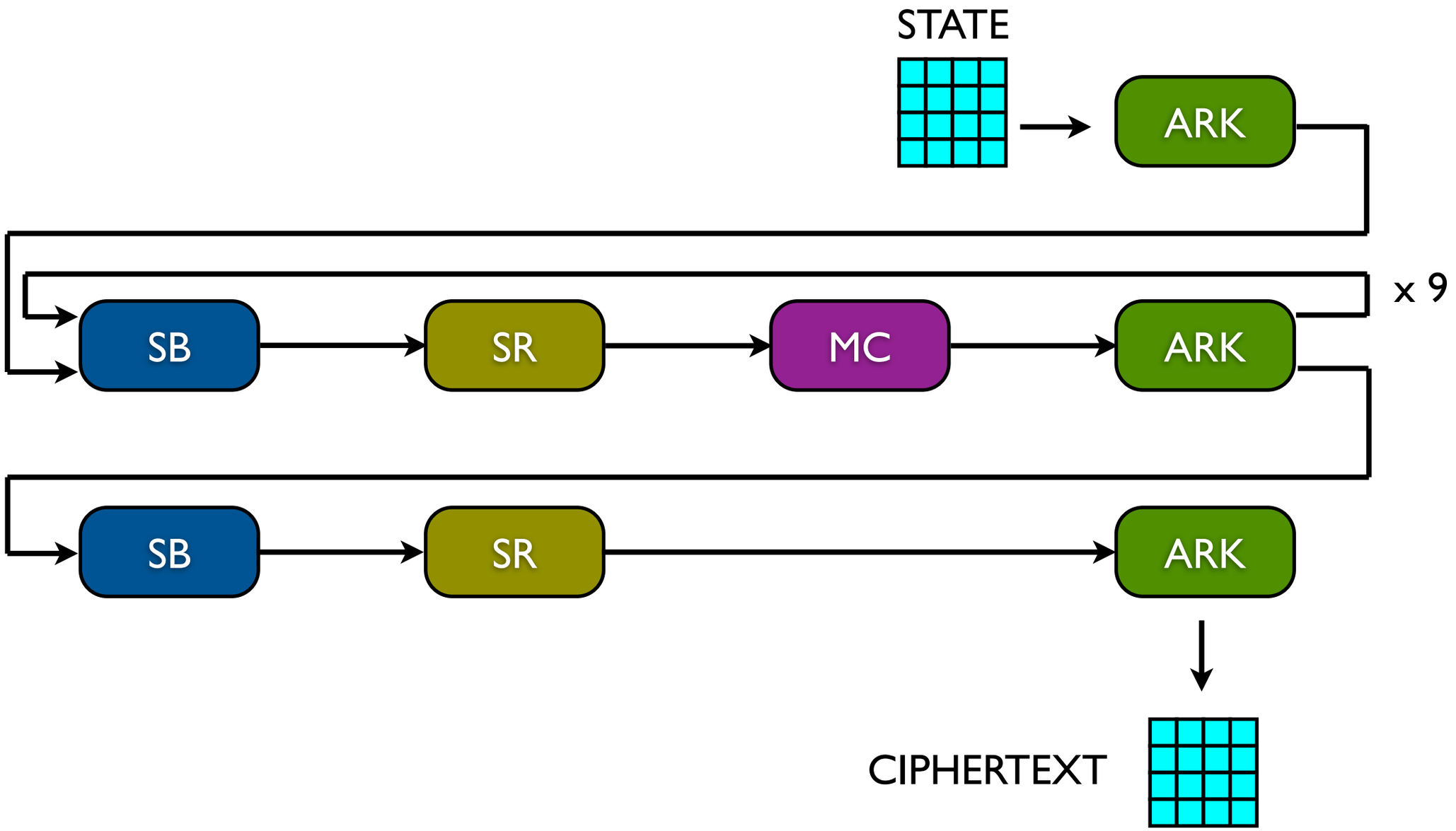
Schedulability

of AES As a Countermeasure Against Side Channel Attacks

AES

- Symmetric block cypher
- 128 bits Plaintext & Key
- Operations applied to 4x4 STATE matrix
- 4 operations: AddRoundKey, SubBytes, ShiftRows and MixColumns

AES



SchedAES Notations

- OP-k-i-j or OP-k-i or OP-k-j
  - OP : ARK (AddRoundKey), SB (SubByte), SR (ShiftRow) or MC (MixColumn)
  - k : round index
  - i : STATE line index
  - j : STATE column index

Observations

- Operations on single byte (ARK and SB)
- Operations on 4 bytes (SR and MC)
- No need to perform 16 ARK-k-i-j to execute one SB-(k+1)-i-j
- No need to perform 16 SB-k-i-j to execute one MC-k-j
- ...

Scheduler Algorithm

Algorithm 1 AES Scheduler: pseudo-code

1: {Initialization}
2: $\Theta = \{ ARK_{0,0,0}, ARK_{0,0,1}, ARK_{0,0,2}, ARK_{0,0,3}, ARK_{0,1,0}, ARK_{0,1,1}, ARK_{0,1,2}, ARK_{0,1,3}, ARK_{0,2,0}, ARK_{0,2,1}, ARK_{0,2,2}, ARK_{0,2,3}, ARK_{0,3,0}, ARK_{0,3,1}, ARK_{0,3,2}, ARK_{0,3,3} \}$
3: {Execution loop}
4: **while** not finished **do**
5: α = randomly pick operation in Θ
6: perform α
7: Θ = updateTheta(α)
8: **end while**

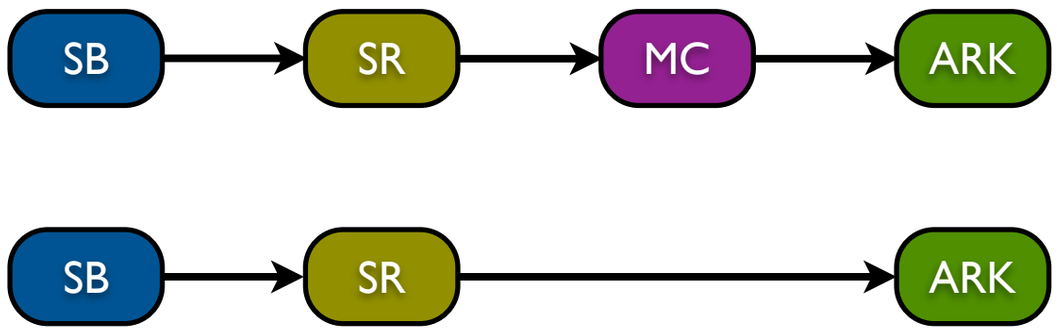
Algorithm 2 updateTheta: pseudo-code

Require: operation α , set of possible operations Θ
Ensure: set of possible operations Θ updated

1: remove α from Θ
2: *operation_name* = operation part of α
3: k = round index of α
4: i = line index of α
5: j = column index of α
6: **if** *operation_name* is ARK **then**
7: arkUpdate(k,i,j)
8: **else if** *operation_name* is SB **then**
9: sbUpdate(k,i,j)
10: **else if** *operation_name* is SR **then**
11: srUpdate(k,i)
12: **else if** *operation_name* is MC **then**
13: mcUpdate(k,j)
14: **end if**

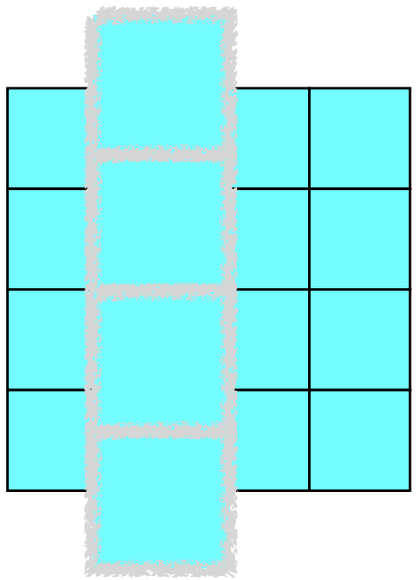
SchedAES

AddRoundKey

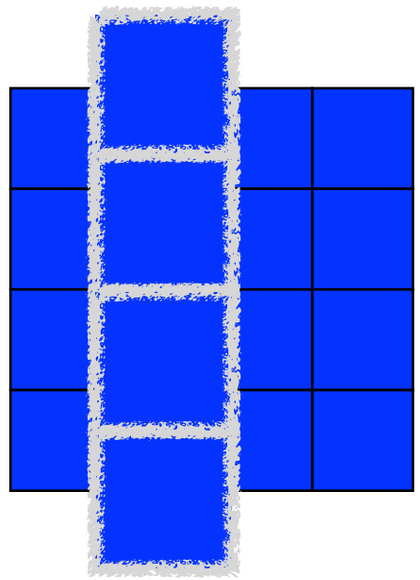


SchedAES

AddRoundKey



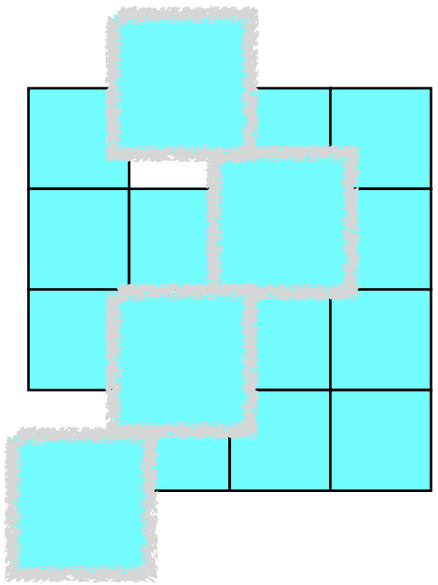
$MC_{k,1}$!



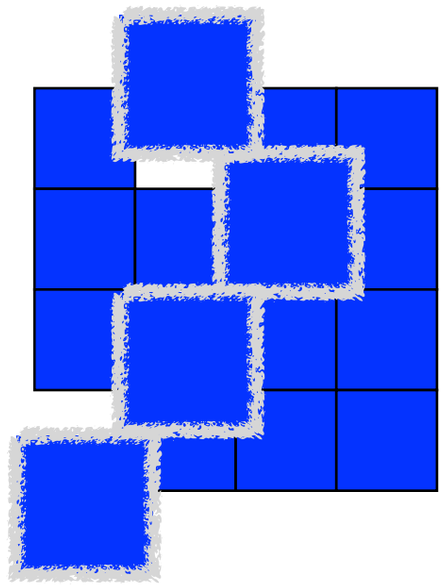
$ARK_{k,0,1}$ & $ARK_{k,1,1}$ &
$ARK_{k,2,1}$ & $ARK_{k,3,1}$?

SchedAES

AddRoundKey



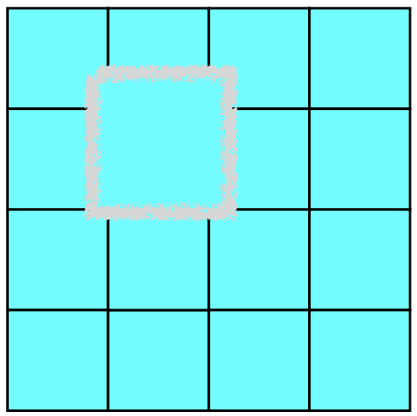
$MC_{k,1}$!

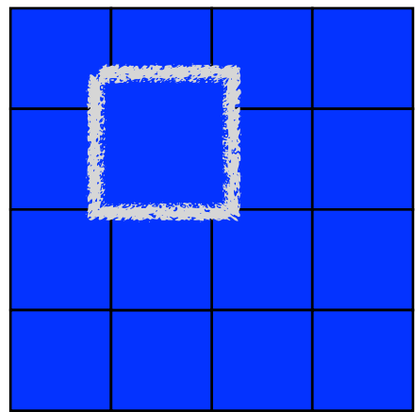


$ARK_{k,0,1}$ & $ARK_{k,1,2}$ &
$ARK_{k,2,1}$ & $ARK_{k,3,0}$?

SchedAES

AddRoundKey 10



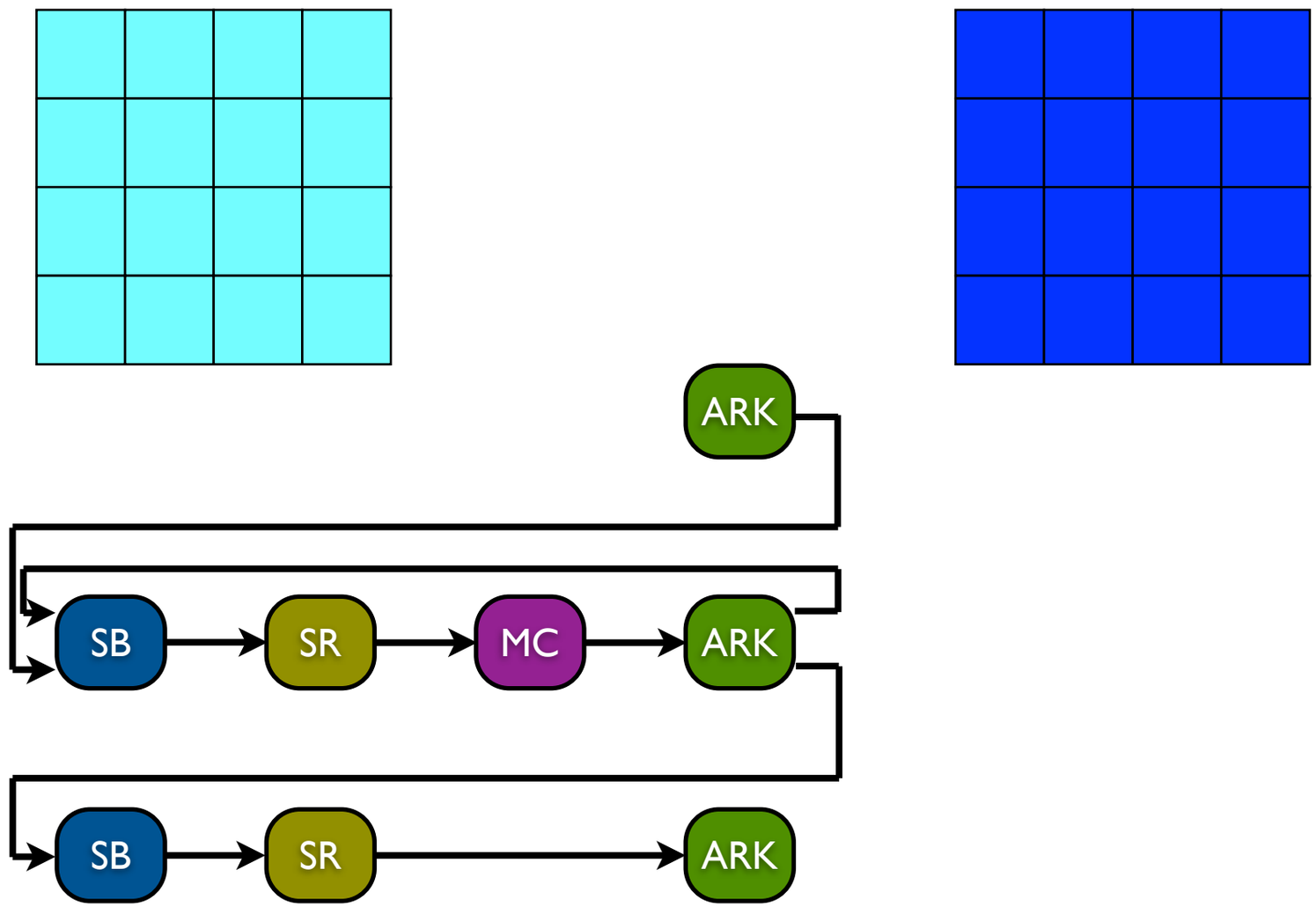


$SB_{10,1,1}$!

$ARK_{10,1,1}$?

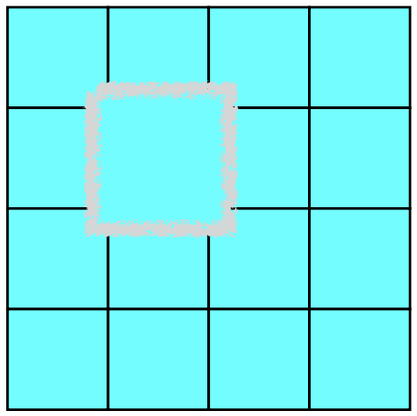
SchedAES

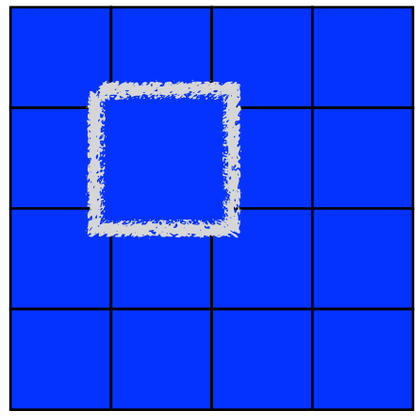
SubByte



SchedAES

SubByte



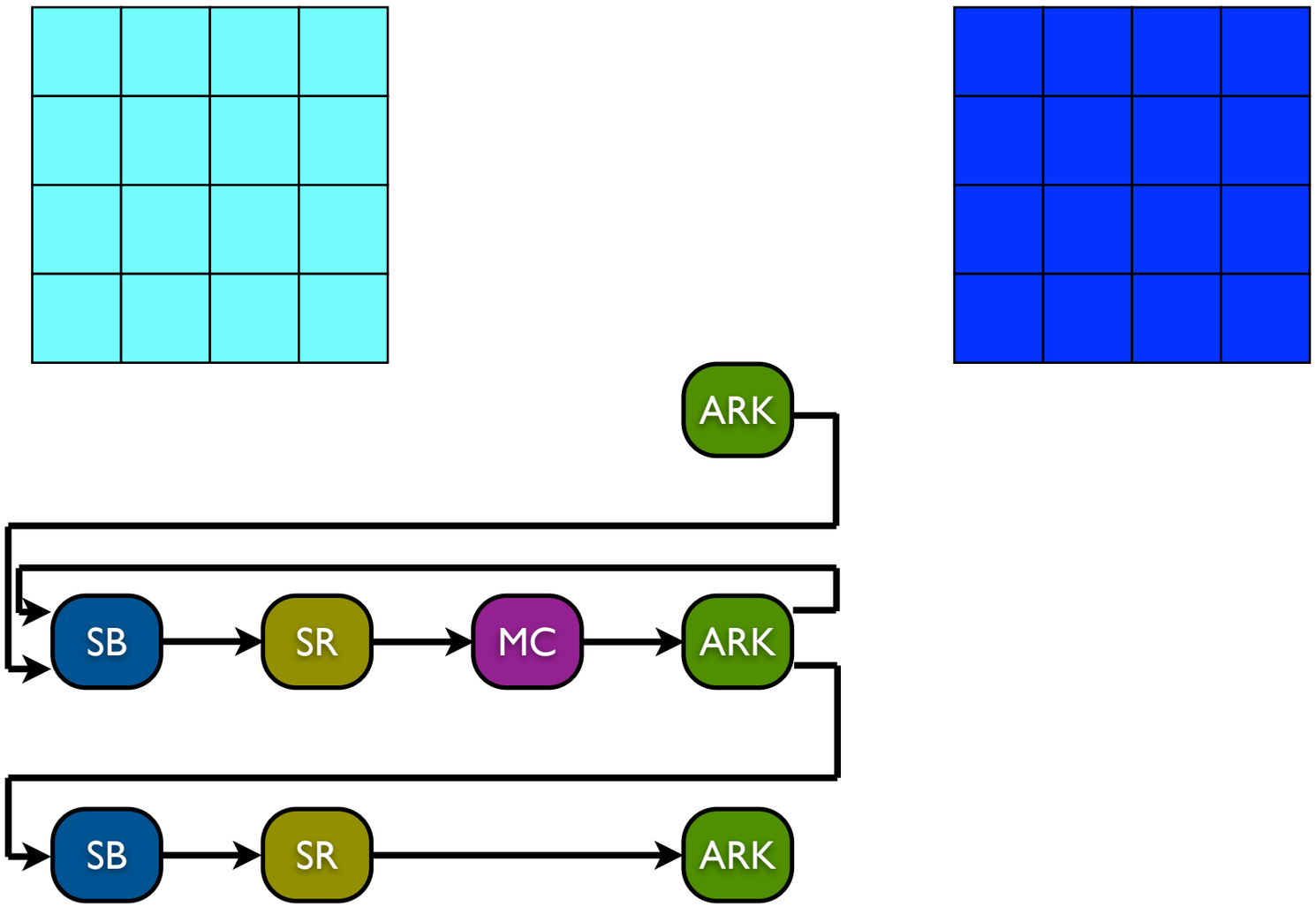


$ARK_{(k-1),1,1}$!

$SB_{k,1,1}$?

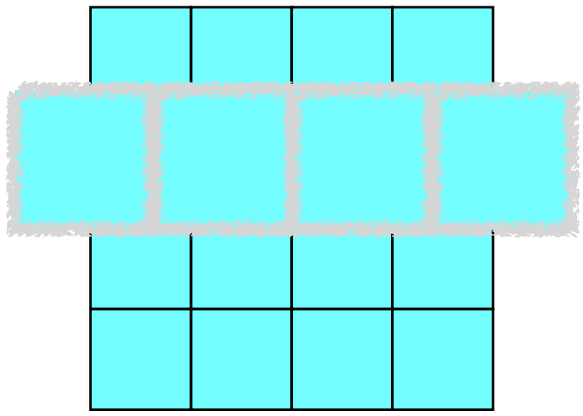
SchedAES

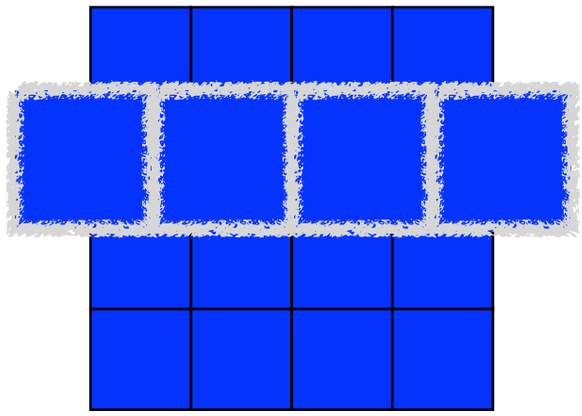
ShiftRow



SchedAES

ShiftRow



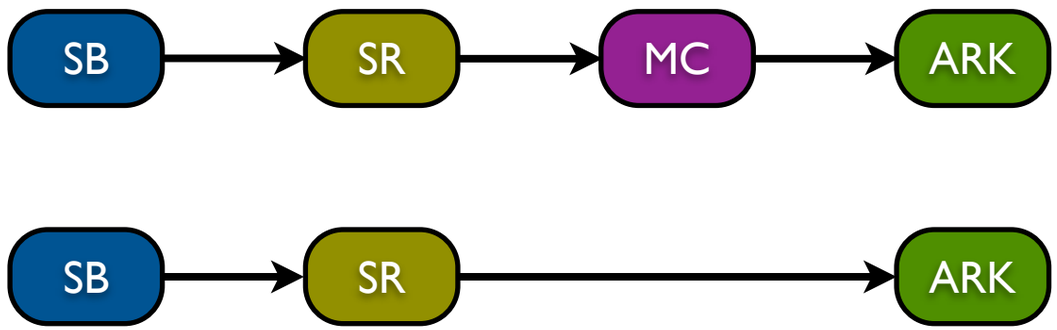


$ARK_{(k-1),1,0}$ & $ARK_{(k-1),1,0}$
& $ARK_{(k-1),1,0}$ & $ARK_{(k-1),1,0}$
& $SR_{(k-1),1}$!

$SR_{k,1}$?

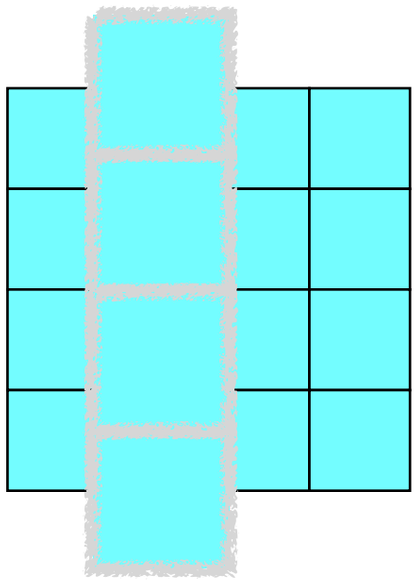
SchedAES

MixColumn

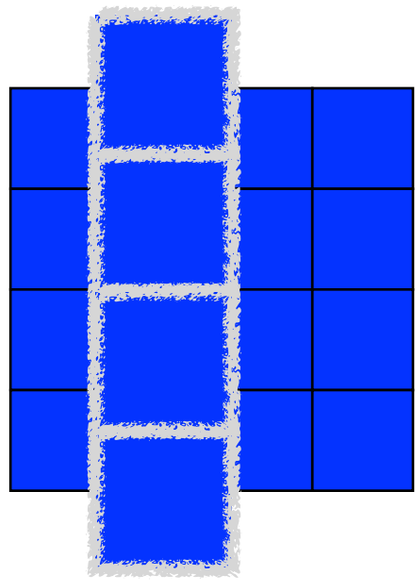


SchedAES

MixColumn



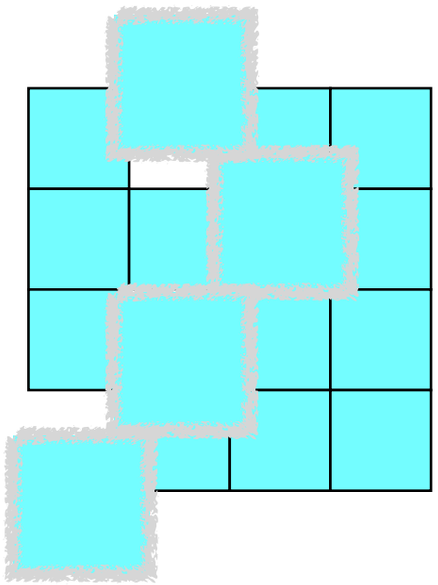
$SB_{k,0,1}$ & $SB_{k,0,1}$ &
$SB_{k,0,1}$ & $SB_{k,0,1}$!



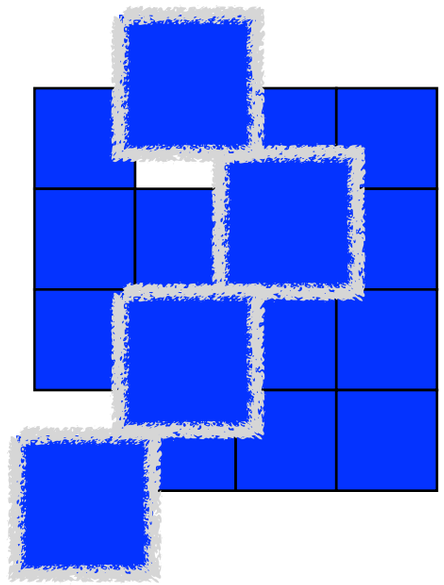
$MC_{k,1}$?

SchedAES

MixColumn



$SB_{k,0,1}$ & $SB_{k,1,2}$ &
$SB_{k,2,1}$ & $SB_{k,3,0}$!



$MC_{k,1}$?

III

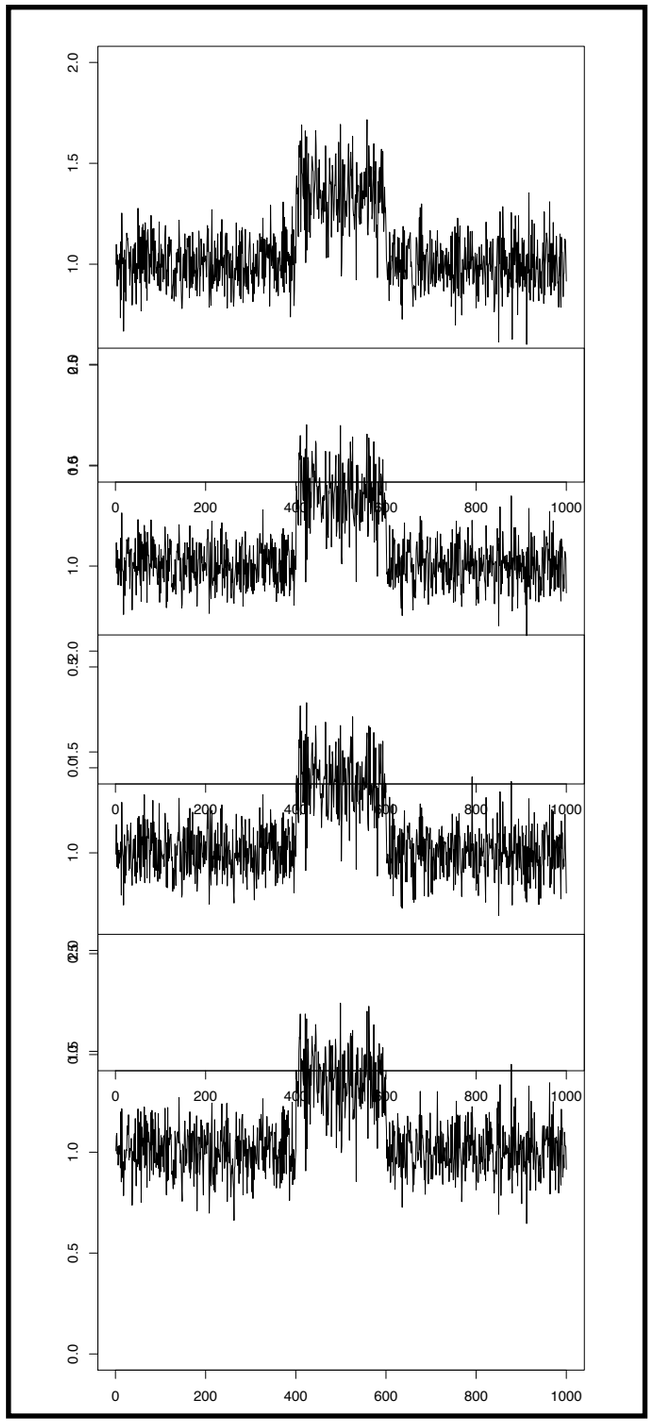
The Schedulability of AES As a Countermeasure

Against Side Channel Attacks

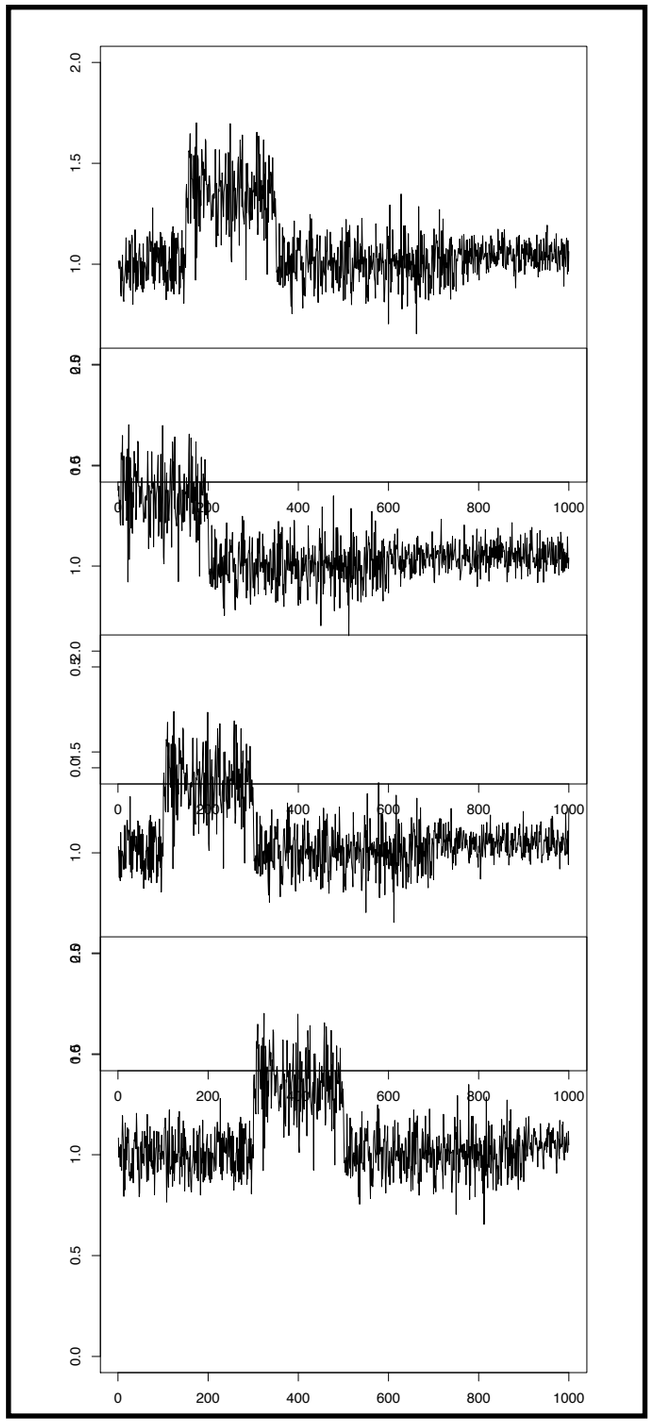
Hiding - Shuffling

- Induce power traces misalignment
- Dummy operations
- Instructions swapping

Hiding - Shuffling



Hiding - Shuffling



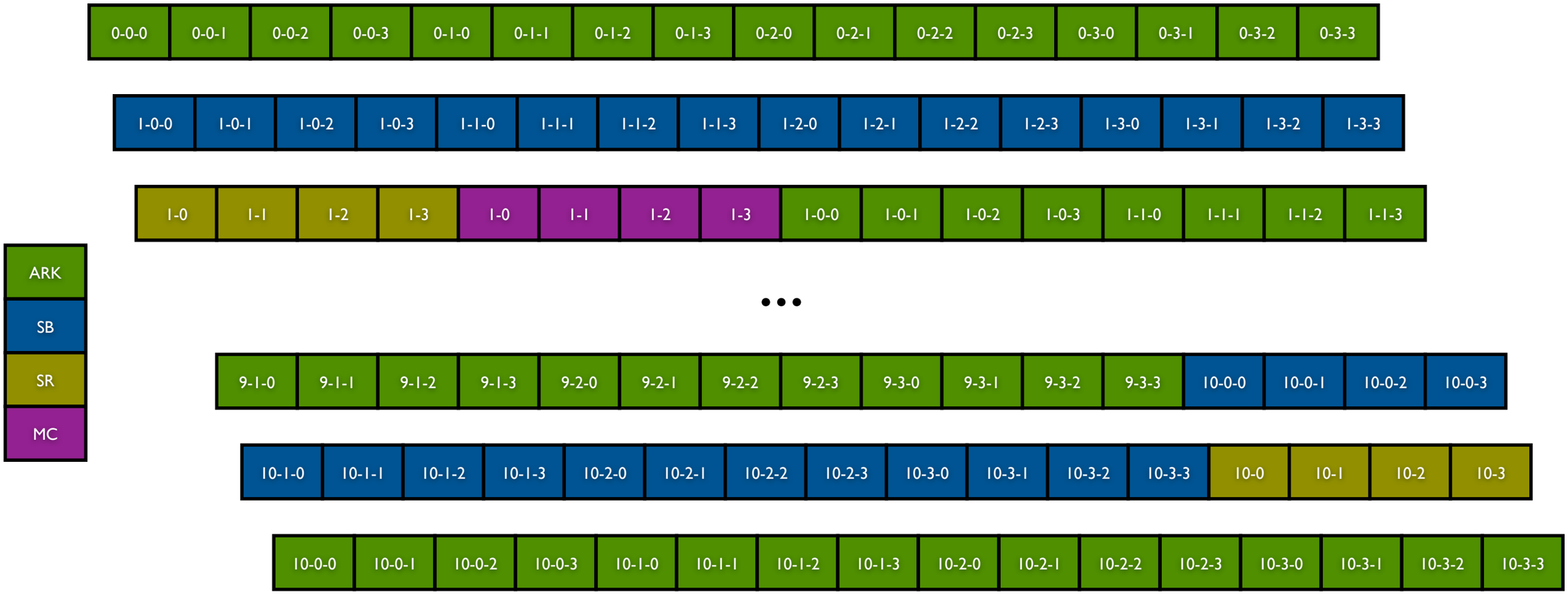
Execution Traces

- Sequence of operations : Op_1 - Op_2 - ... - Op_n
- One or multiple points (values) per Op
- Op_1 - Op_2 - Op_3 - Op_4 and Op_1 - Op_2 - Op_3 - Op_4 are aligned
- Op_1 - Op_2 - Op_3 - Op_4 and Op_1 - Op_4

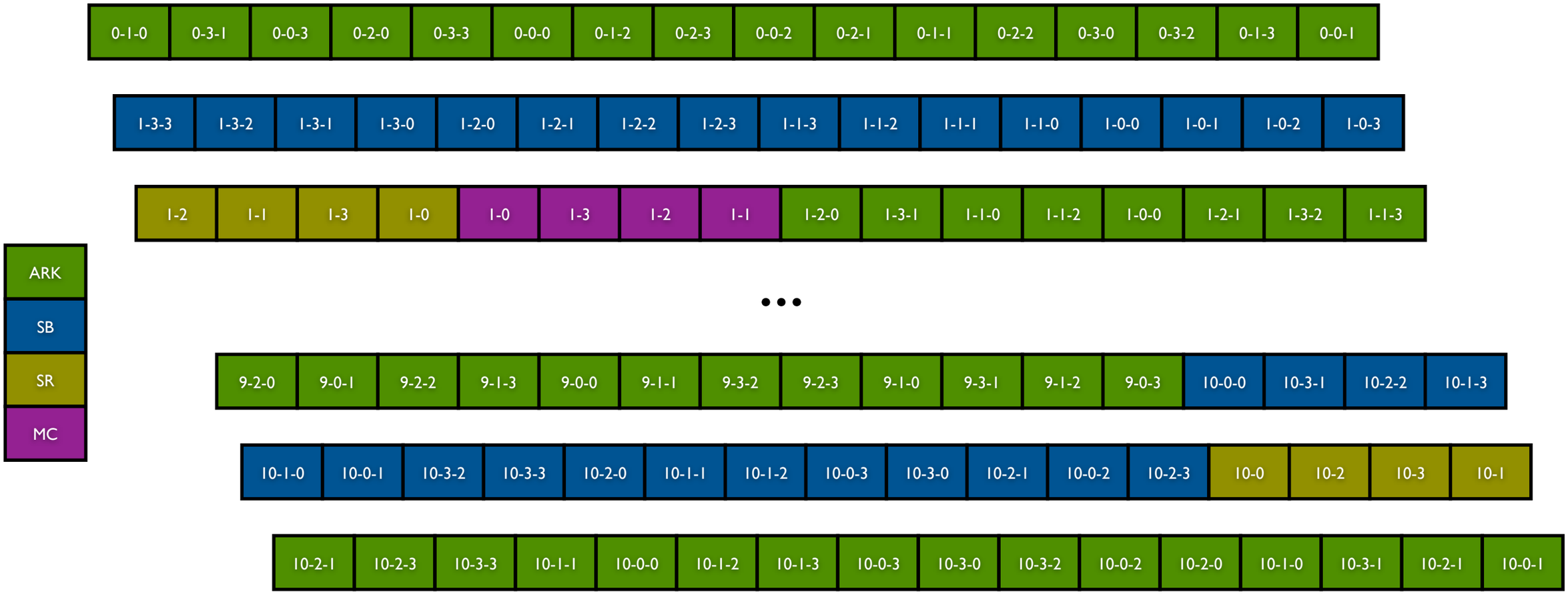
Tillich [ACNS 2007]

- Random permutation inside AES operations
- Use a masking Scheme
- Randomize 1,5 firsts rounds and 2 lasts rounds

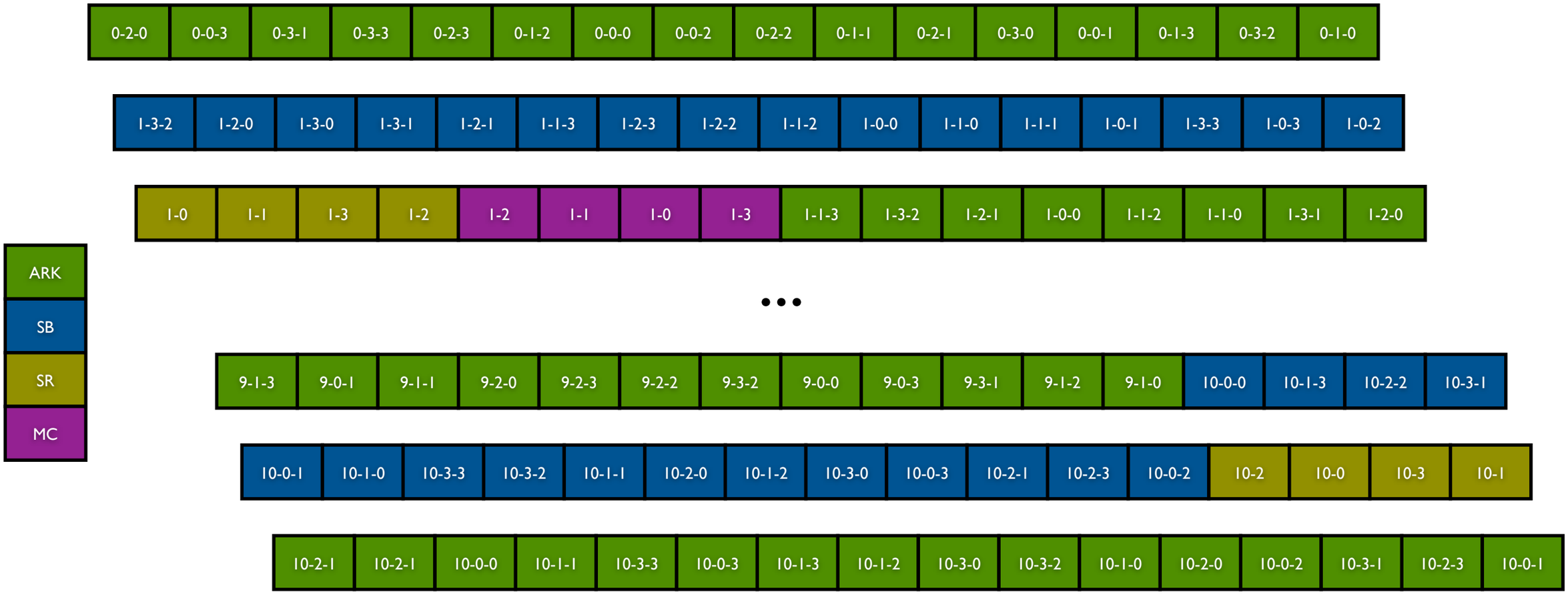
AES


0-0-0 0-0-1 0-0-2 0-0-3 0-1-0 0-1-1 0-1-2 0-1-3 0-2-0 0-2-1 0-2-2 0-2-3 0-3-0 0-3-1 0-3-2 0-3-3
1-0-0 1-0-1 1-0-2 1-0-3 1-1-0 1-1-1 1-1-2 1-1-3 1-2-0 1-2-1 1-2-2 1-2-3 1-3-0 1-3-1 1-3-2 1-3-3
1-0 1-1 1-2 1-3 1-0 1-1 1-2 1-3 1-0-0 1-0-1 1-0-2 1-0-3 1-1-0 1-1-1 1-1-2 1-1-3
ARK
SB
SR
MC
• • •
9-1-0 9-1-1 9-1-2 9-1-3 9-2-0 9-2-1 9-2-2 9-2-3 9-3-0 9-3-1 9-3-2 9-3-3 10-0-0 10-0-1 10-0-2 10-0-3
10-1-0 10-1-1 10-1-2 10-1-3 10-2-0 10-2-1 10-2-2 10-2-3 10-3-0 10-3-1 10-3-2 10-3-3 10-0 10-1 10-2 10-3
10-0-0 10-0-1 10-0-2 10-0-3 10-1-0 10-1-1 10-1-2 10-1-3 10-2-0 10-2-1 10-2-2 10-2-3 10-3-0 10-3-1 10-3-2 10-3-3

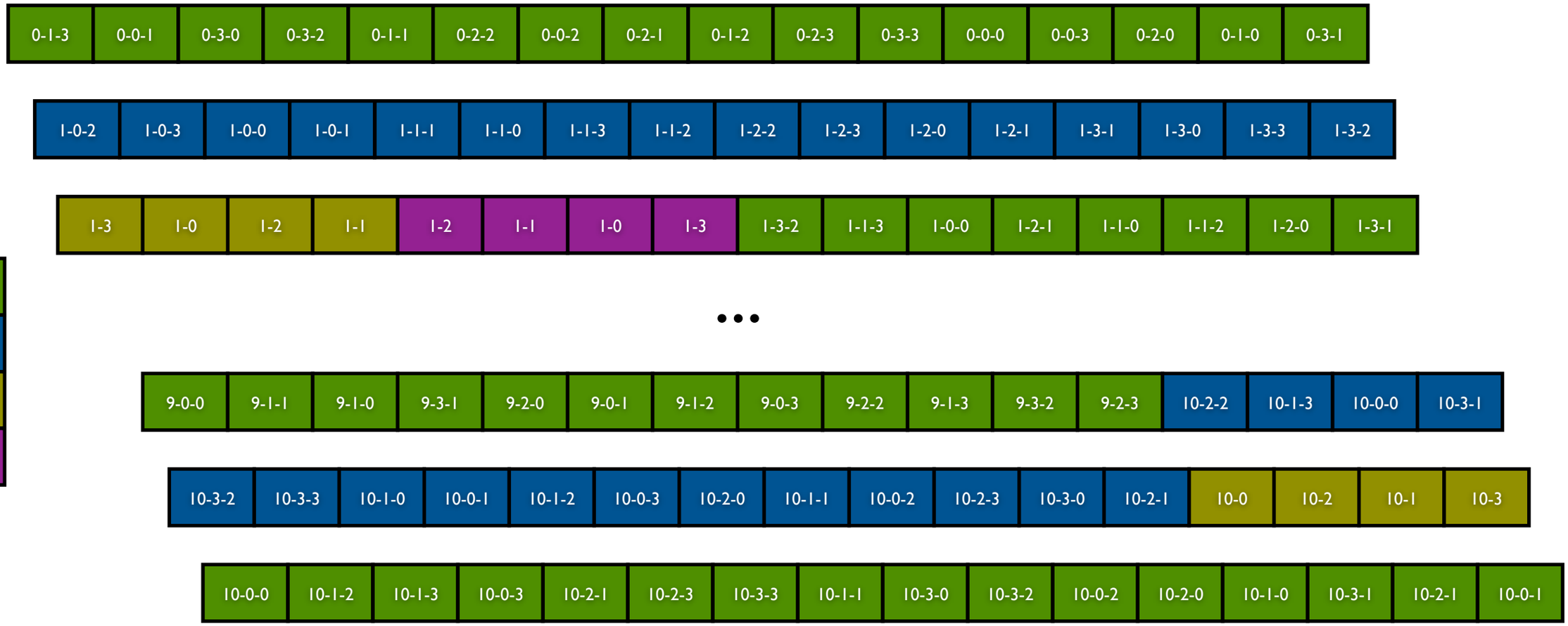
Tillich (1)


0-1-0 0-3-1 0-0-3 0-2-0 0-3-3 0-0-0 0-1-2 0-2-3 0-0-2 0-2-1 0-1-1 0-2-2 0-3-0 0-3-2 0-1-3 0-0-1
1-3-3 1-3-2 1-3-1 1-3-0 1-2-0 1-2-1 1-2-2 1-2-3 1-1-3 1-1-2 1-1-1 1-1-0 1-0-0 1-0-1 1-0-2 1-0-3
1-2 1-1 1-3 1-0 1-0 1-3 1-2 1-1 1-2-0 1-3-1 1-1-0 1-1-2 1-0-0 1-2-1 1-3-2 1-1-3
ARK
SB
SR
MC
• • •
9-2-0 9-0-1 9-2-2 9-1-3 9-0-0 9-1-1 9-3-2 9-2-3 9-1-0 9-3-1 9-1-2 9-0-3 10-0-0 10-3-1 10-2-2 10-1-3
10-1-0 10-0-1 10-3-2 10-3-3 10-2-0 10-1-1 10-1-2 10-0-3 10-3-0 10-2-1 10-0-2 10-2-3 10-0 10-2 10-3 10-1
10-2-1 10-2-3 10-3-3 10-1-1 10-0-0 10-1-2 10-1-3 10-0-3 10-3-0 10-3-2 10-0-2 10-2-0 10-1-0 10-3-1 10-2-1 10-0-1

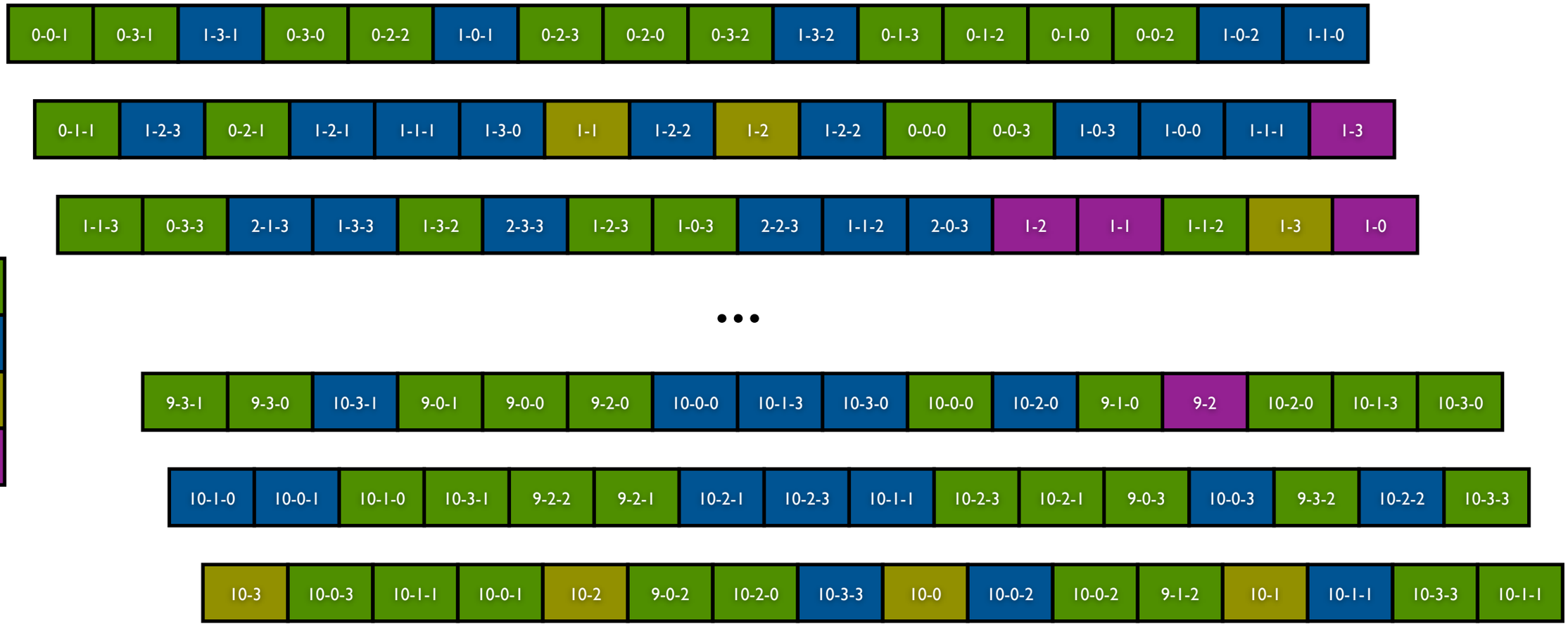
Tillich (2)


0-2-0 0-0-3 0-3-1 0-3-3 0-2-3 0-1-2 0-0-0 0-0-2 0-2-2 0-1-1 0-2-1 0-3-0 0-0-1 0-1-3 0-3-2 0-1-0
1-3-2 1-2-0 1-3-0 1-3-1 1-2-1 1-1-3 1-2-3 1-2-2 1-1-2 1-0-0 1-1-0 1-1-1 1-0-1 1-3-3 1-0-3 1-0-2
1-0 1-1 1-3 1-2 1-2 1-1 1-0 1-3 1-1-3 1-3-2 1-2-1 1-0-0 1-1-2 1-1-0 1-3-1 1-2-0
ARK
SB
SR
MC
• • •
9-1-3 9-0-1 9-1-1 9-2-0 9-2-3 9-2-2 9-3-2 9-0-0 9-0-3 9-3-1 9-1-2 9-1-0 10-0-0 10-1-3 10-2-2 10-3-1
10-0-1 10-1-0 10-3-3 10-3-2 10-1-1 10-2-0 10-1-2 10-3-0 10-0-3 10-2-1 10-2-3 10-0-2 10-2 10-0 10-3 10-1
10-2-1 10-2-1 10-0-0 10-1-1 10-3-3 10-0-3 10-1-3 10-1-2 10-3-0 10-3-2 10-1-0 10-2-0 10-0-2 10-3-1 10-2-3 10-0-1

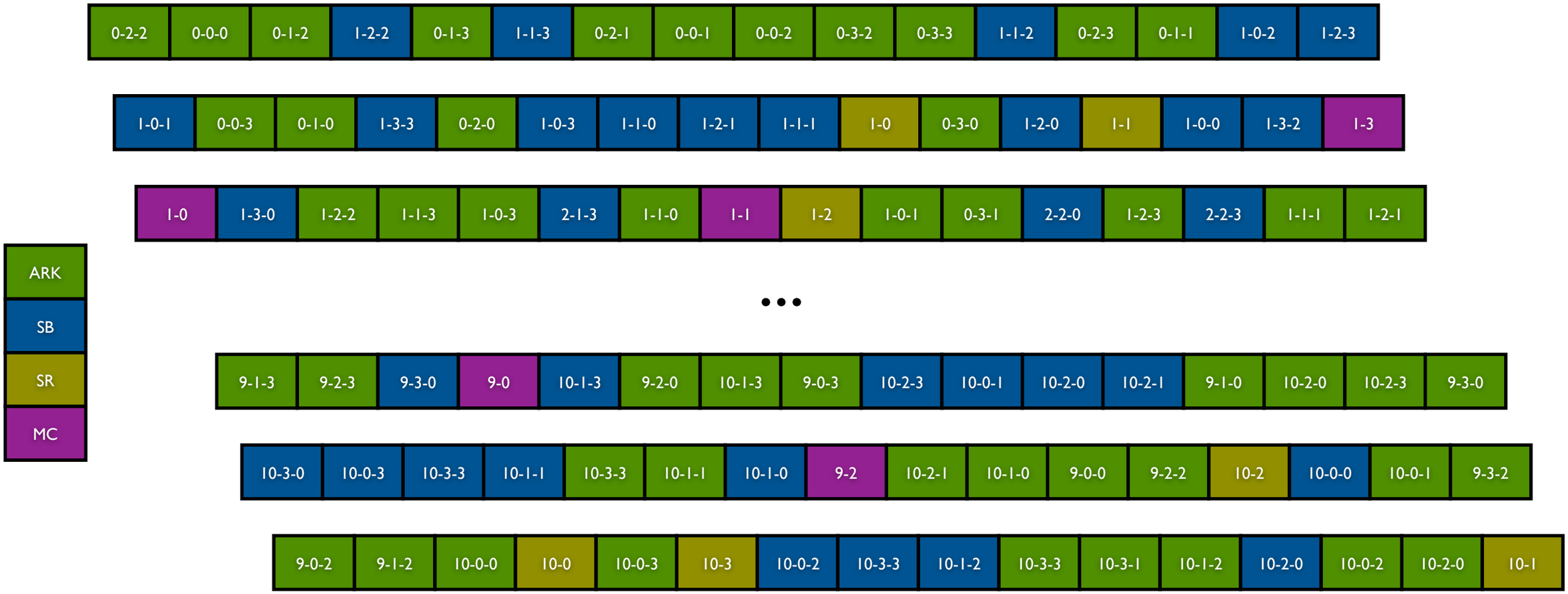
Tillich (3)


0-1-3 0-0-1 0-3-0 0-3-2 0-1-1 0-2-2 0-0-2 0-2-1 0-1-2 0-2-3 0-3-3 0-0-0 0-0-3 0-2-0 0-1-0 0-3-1
1-0-2 1-0-3 1-0-0 1-0-1 1-1-1 1-1-0 1-1-3 1-1-2 1-2-2 1-2-3 1-2-0 1-2-1 1-3-1 1-3-0 1-3-3 1-3-2
1-3 1-0 1-2 1-1 1-2 1-1 1-0 1-3 1-3-2 1-1-3 1-0-0 1-2-1 1-1-0 1-1-2 1-2-0 1-3-1
ARK
SB
SR
MC
• • •
9-0-0 9-1-1 9-1-0 9-3-1 9-2-0 9-0-1 9-1-2 9-0-3 9-2-2 9-1-3 9-3-2 9-2-3 10-2-2 10-1-3 10-0-0 10-3-1
10-3-2 10-3-3 10-1-0 10-0-1 10-1-2 10-0-3 10-2-0 10-1-1 10-0-2 10-2-3 10-3-0 10-2-1 10-0 10-2 10-1 10-3
10-0-0 10-1-2 10-1-3 10-0-3 10-2-1 10-2-3 10-3-3 10-1-1 10-3-0 10-3-2 10-0-2 10-2-0 10-1-0 10-3-1 10-2-1 10-0-1

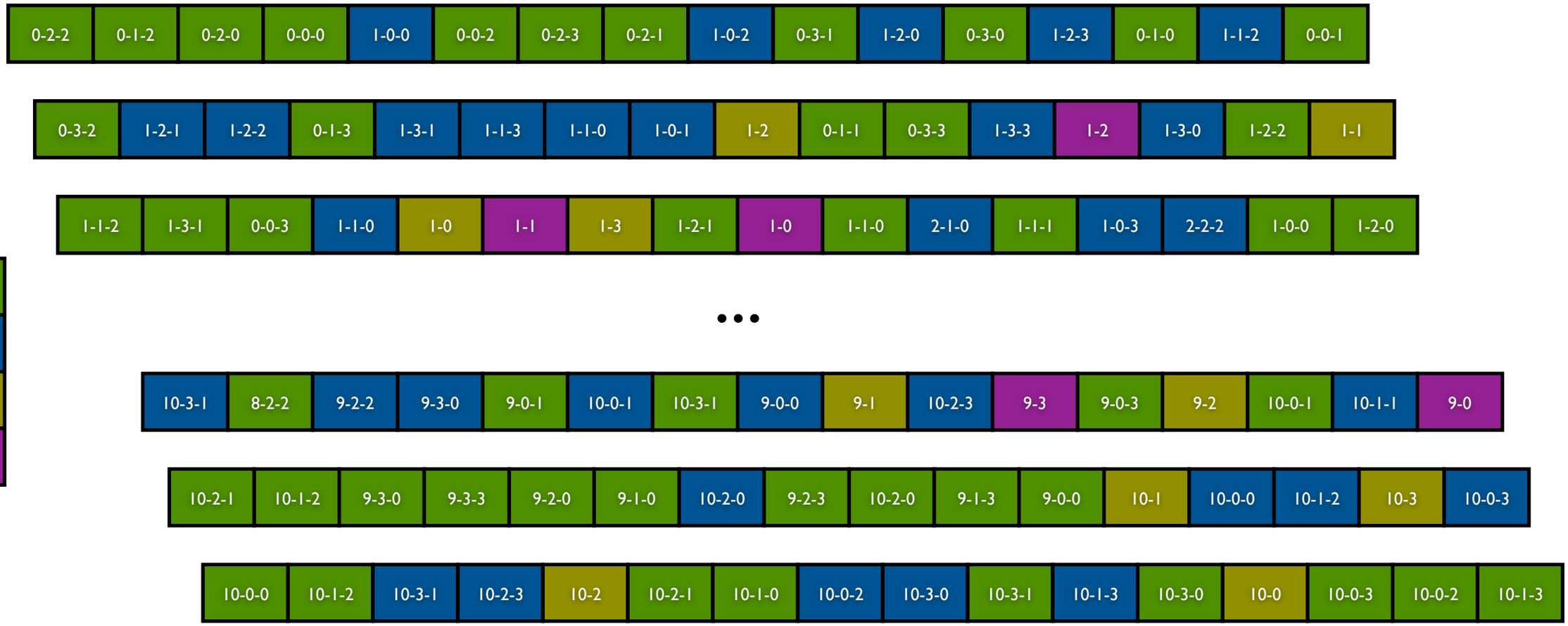
SchedAES (1)


0-0-1 0-3-1 1-3-1 0-3-0 0-2-2 1-0-1 0-2-3 0-2-0 0-3-2 1-3-2 0-1-3 0-1-2 0-1-0 0-0-2 1-0-2 1-1-0
0-1-1 1-2-3 0-2-1 1-2-1 1-1-1 1-3-0 1-1 1-2-2 1-2 1-2-2 0-0-0 0-0-3 1-0-3 1-0-0 1-1-1 1-3
1-1-3 0-3-3 2-1-3 1-3-3 1-3-2 2-3-3 1-2-3 1-0-3 2-2-3 1-1-2 2-0-3 1-2 1-1 1-1-2 1-3 1-0
ARK
SB
SR
MC
...
9-3-1 9-3-0 10-3-1 9-0-1 9-0-0 9-2-0 10-0-0 10-1-3 10-3-0 10-0-0 10-2-0 9-1-0 9-2 10-2-0 10-1-3 10-3-0
10-1-0 10-0-1 10-1-0 10-3-1 9-2-2 9-2-1 10-2-1 10-2-3 10-1-1 10-2-3 10-2-1 9-0-3 10-0-3 9-3-2 10-2-2 10-3-3
10-3 10-0-3 10-1-1 10-0-1 10-2 9-0-2 10-2-0 10-3-3 10-0 10-0-2 10-0-2 9-1-2 10-1 10-1-1 10-3-3 10-1-1

SchedAES (2)

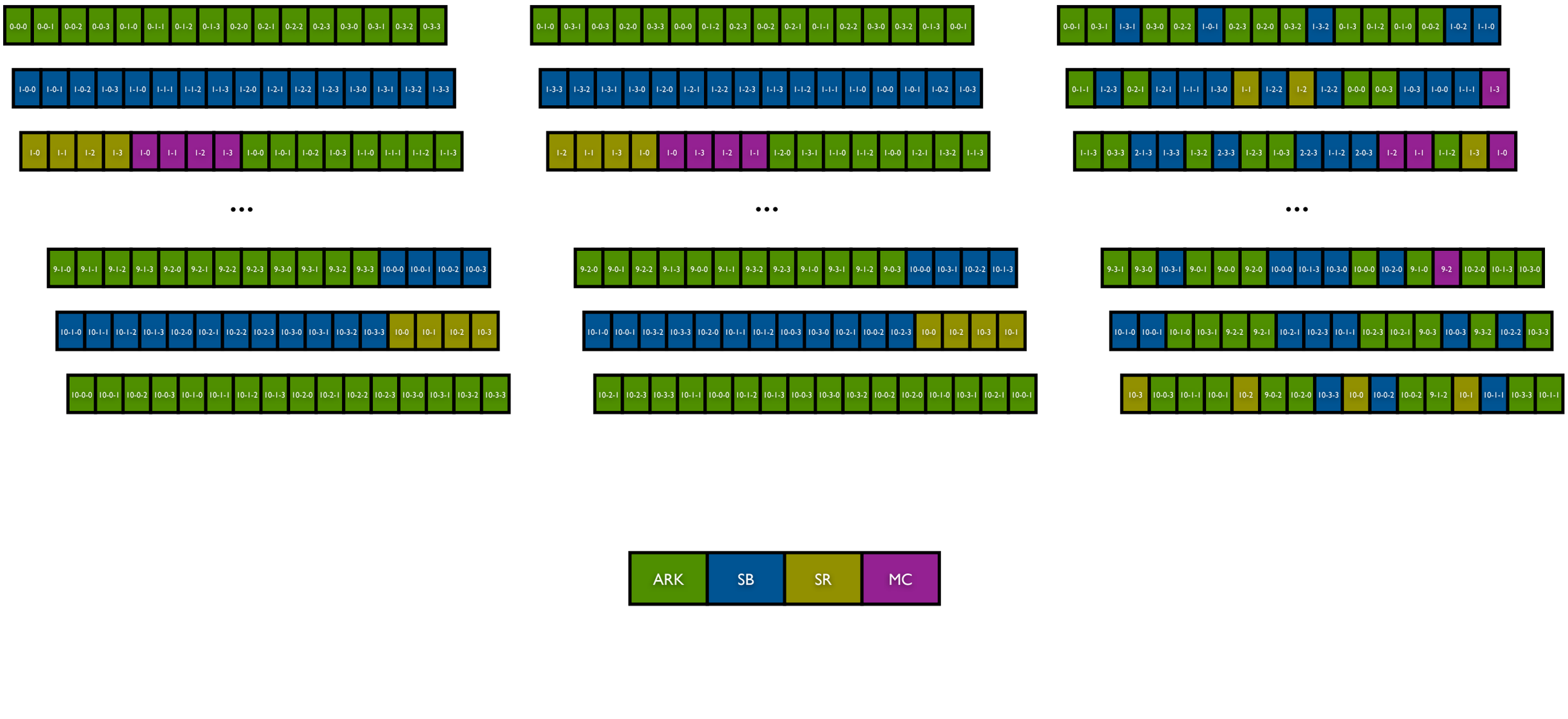

0-2-2 0-0-0 0-1-2 1-2-2 0-1-3 1-1-3 0-2-1 0-0-1 0-0-2 0-3-2 0-3-3 1-1-2 0-2-3 0-1-1 1-0-2 1-2-3
1-0-1 0-0-3 0-1-0 1-3-3 0-2-0 1-0-3 1-1-0 1-2-1 1-1-1 1-0 0-3-0 1-2-0 1-1 1-0-0 1-3-2 1-3
1-0 1-3-0 1-2-2 1-1-3 1-0-3 2-1-3 1-1-0 1-1 1-2 1-0-1 0-3-1 2-2-0 1-2-3 2-2-3 1-1-1 1-2-1
ARK
SB
SR
MC
• • •
9-1-3 9-2-3 9-3-0 9-0 10-1-3 9-2-0 10-1-3 9-0-3 10-2-3 10-0-1 10-2-0 10-2-1 9-1-0 10-2-0 10-2-3 9-3-0
10-3-0 10-0-3 10-3-3 10-1-1 10-3-3 10-1-1 10-1-0 9-2 10-2-1 10-1-0 9-0-0 9-2-2 10-2 10-0-0 10-0-1 9-3-2
9-0-2 9-1-2 10-0-0 10-0 10-0-3 10-3 10-0-2 10-3-3 10-1-2 10-3-3 10-3-1 10-1-2 10-2-0 10-0-2 10-2-0 10-1

SchedAES (3)


0-2-2 0-1-2 0-2-0 0-0-0 1-0-0 0-0-2 0-2-3 0-2-1 1-0-2 0-3-1 1-2-0 0-3-0 1-2-3 0-1-0 1-1-2 0-0-1
0-3-2 1-2-1 1-2-2 0-1-3 1-3-1 1-1-3 1-1-0 1-0-1 1-2 0-1-1 0-3-3 1-3-3 1-2 1-3-0 1-2-2 1-1
1-1-2 1-3-1 0-0-3 1-1-0 1-0 1-1 1-3 1-2-1 1-0 1-1-0 2-1-0 1-1-1 1-0-3 2-2-2 1-0-0 1-2-0
ARK
SB
SR
MC
• • •
10-3-1 8-2-2 9-2-2 9-3-0 9-0-1 10-0-1 10-3-1 9-0-0 9-1 10-2-3 9-3 9-0-3 9-2 10-0-1 10-1-1 9-0
10-2-1 10-1-2 9-3-0 9-3-3 9-2-0 9-1-0 10-2-0 9-2-3 10-2-0 9-1-3 9-0-0 10-1 10-0-0 10-1-2 10-3 10-0-3
10-0-0 10-1-2 10-3-1 10-2-3 10-2 10-2-1 10-1-0 10-0-2 10-3-0 10-3-1 10-1-3 10-3-0 10-0 10-0-3 10-0-2 10-1-3

AES - Tillich -SchedAES

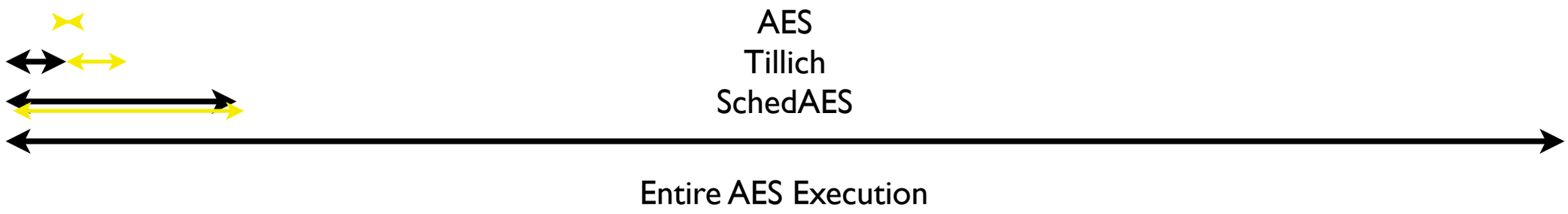
execution traces comparison



Results

Schedulability

	ARK0-x-y	SB1-x-y
AES	(4*x) + y	(4*x) + y + 16
Tillich	[0,15]	[16,31]
SchedAES	[0,60]	[1,62]



Comparison

	Size	Time	Security SB
AES	1,0	1,0	1,0
Tillich*	1,05	1,21	5,0
SchedAES	2,0	7,02	>50,0

security: number of traces needed for full key recovery

Future Works

- KeyScheduling
- More permissive with SR
- Software Attack (& Hardware)
- Apply power traces alignement techniques
- Other selection policies for the scheduler

Conclusion

Conclusion

- Slower but stronger scheme
- Not a stand alone countermeasure
- Can be applied to other algorithms

Thank You /

Questions ?

ULB

QualSEC