Attacks and Countermeasures in Persistent Fault Model

Viet-Sang Nguyen

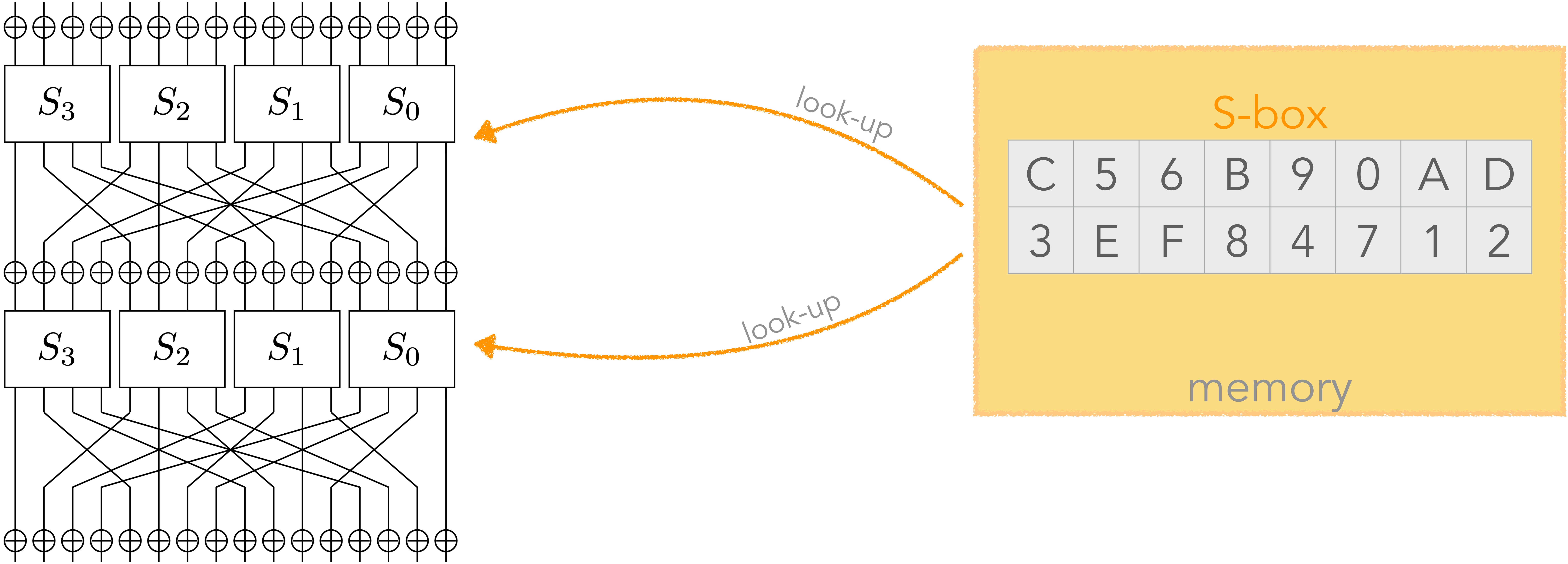
JAIF
Rennes, France
1 October, 2024

joint work with Vincent Grosso and Pierre-Louis Cayrel

UNIVERSITÉ DE LYON
UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE
Laboratoire Hubert Curien
UMR • CNRS • 5516 • Saint-Étienne
anr
PROPHY ANR-22-CE39-0008-01

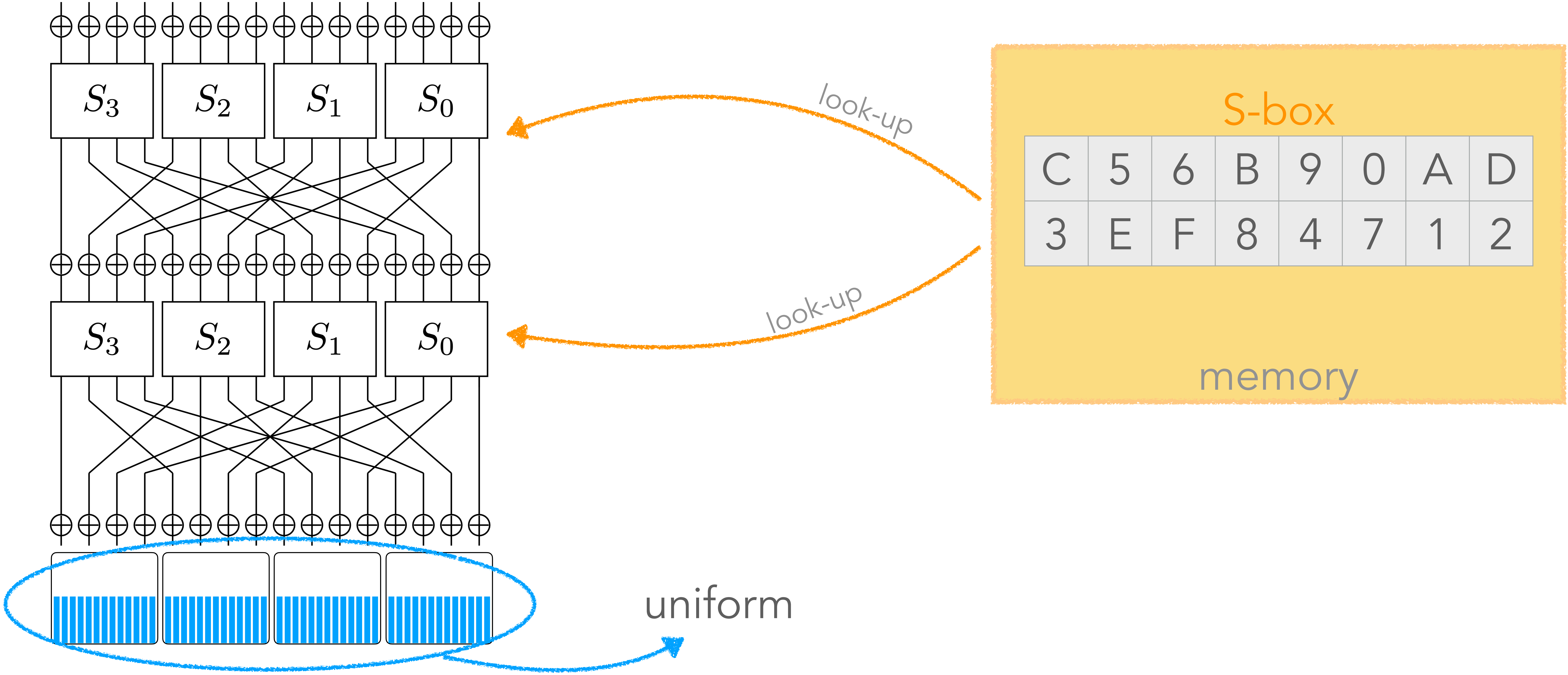
Persistent fault attacks (PFA)

S-box in cipher



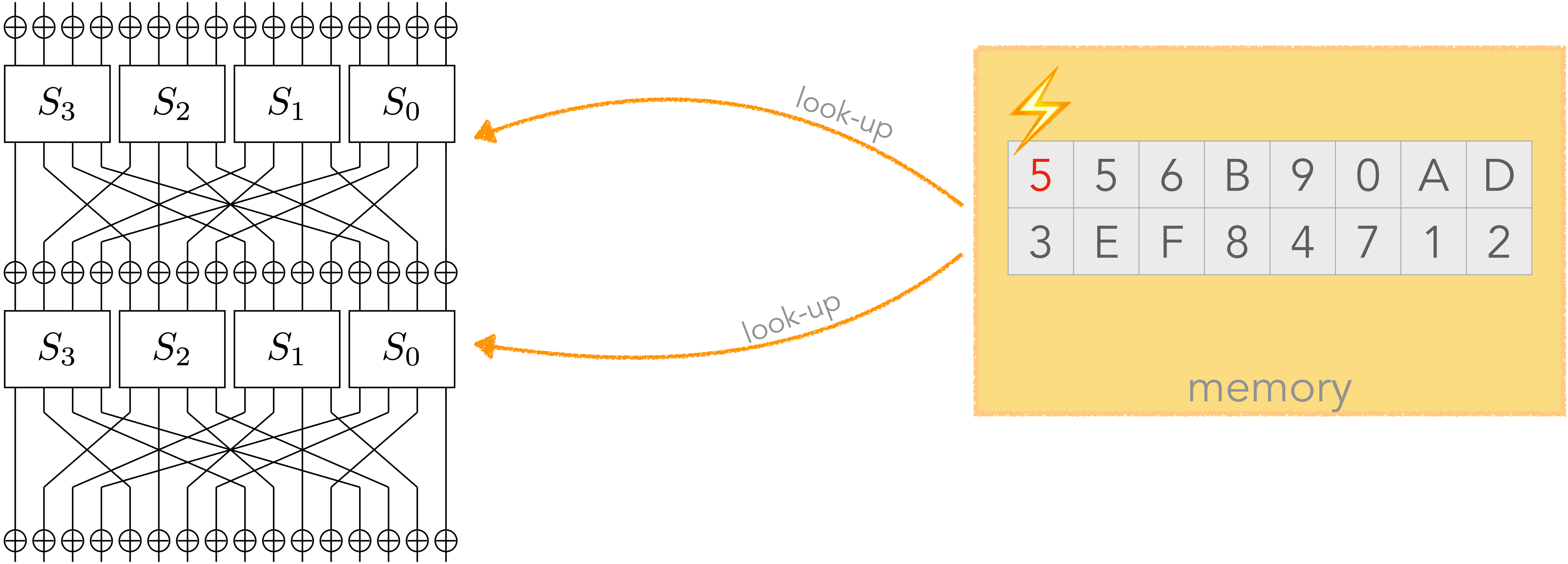
C	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

S-box in cipher



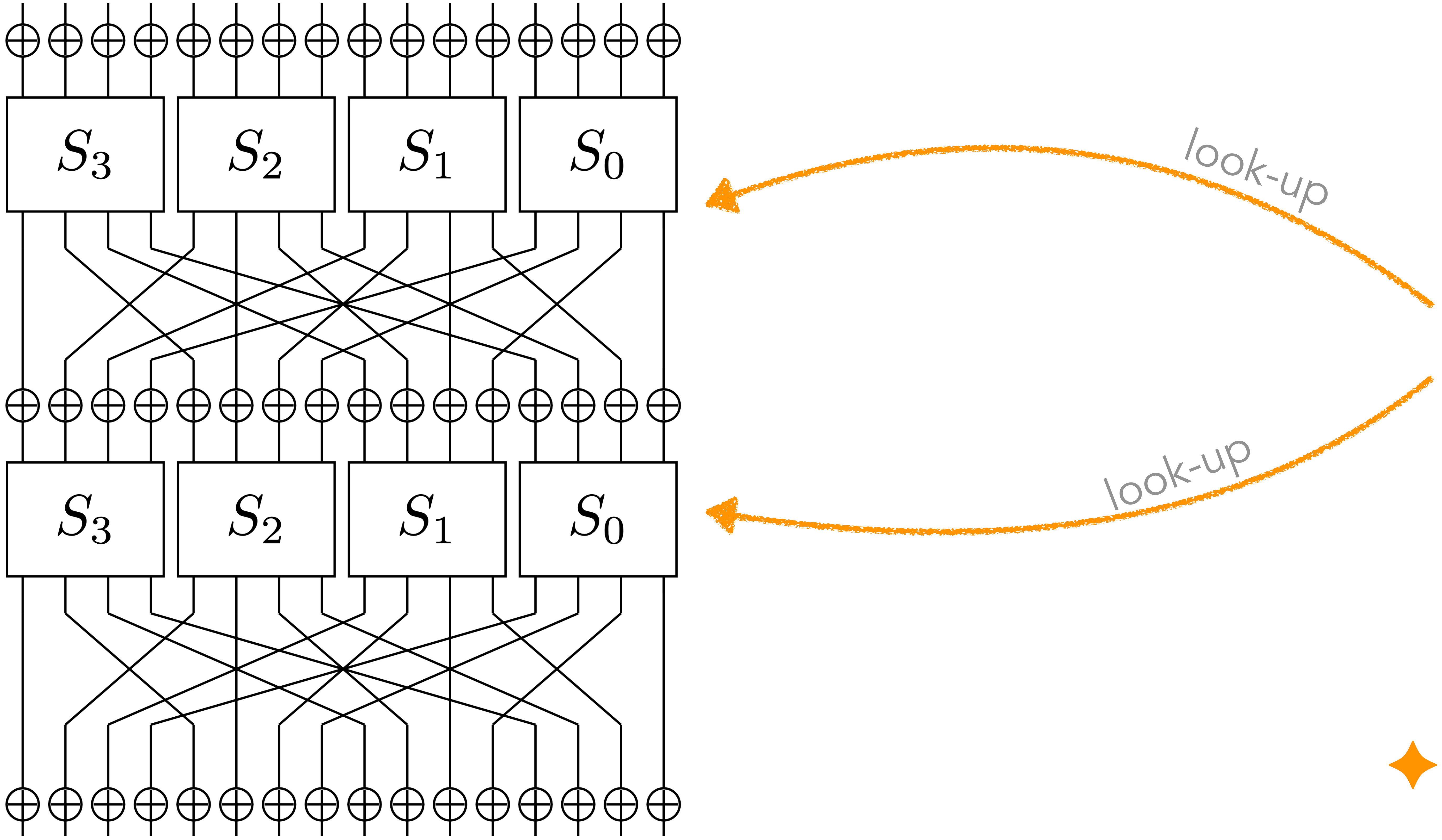
C	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

Faulting S-box



5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

Faulting S-box

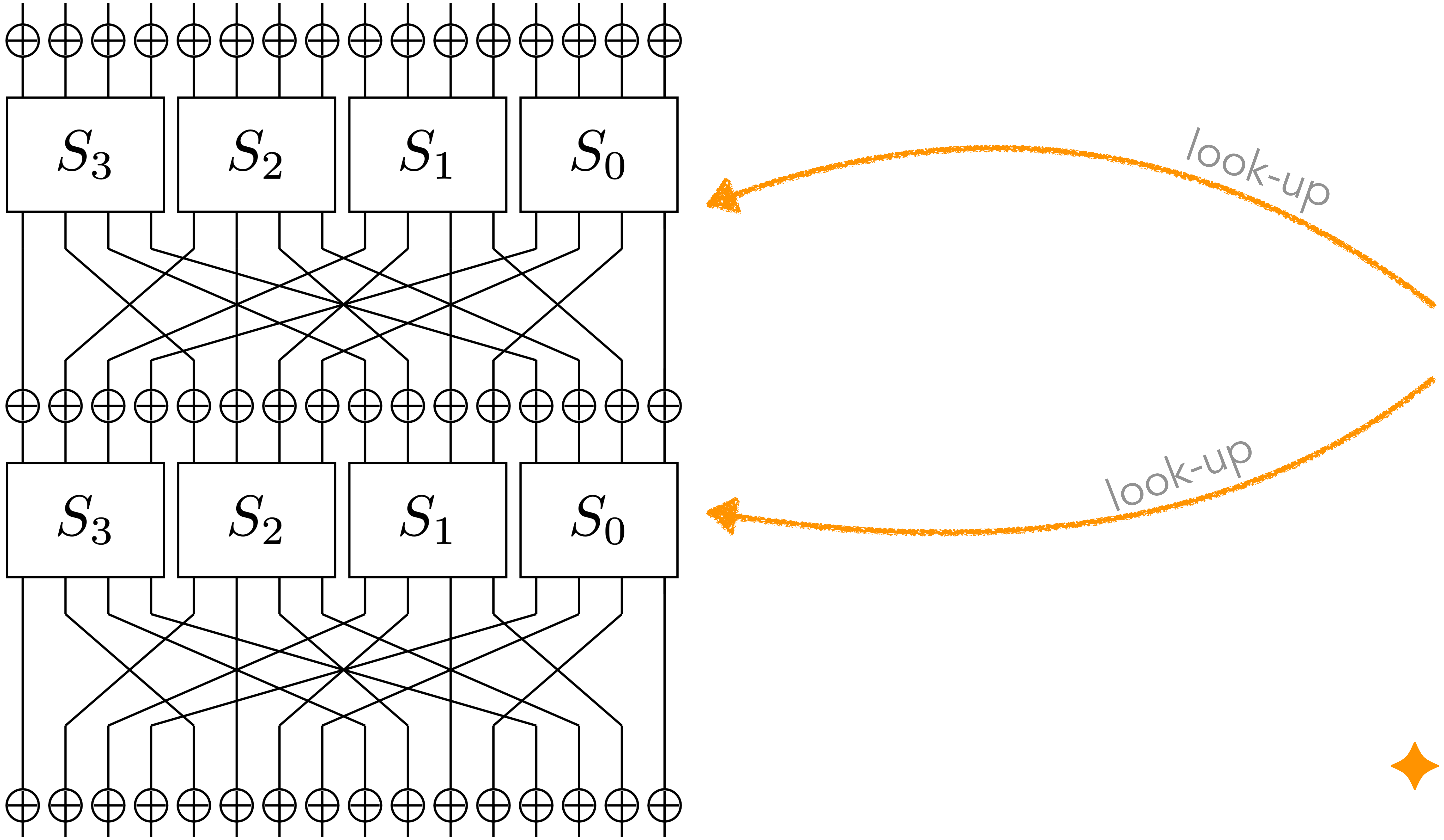


5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

memory

- Fault on first element: C → 5
  - C: disappears
  - 5: appears twice

Faulting S-box



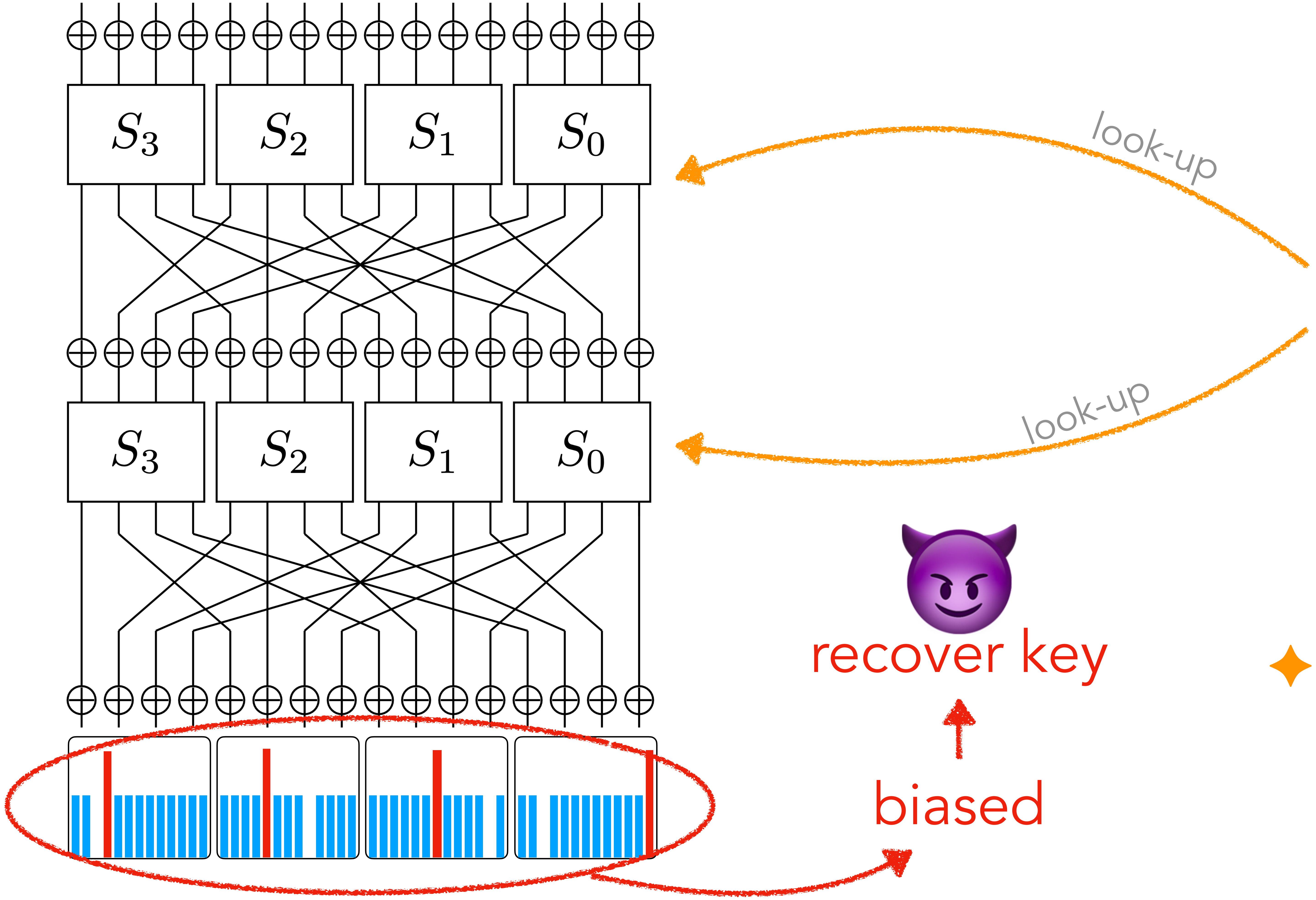
⚡biased faulty S-box

5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

memory

- Fault on first element: C → 5
  - C: disappears
  - 5: appears twice

Faulting S-box



⚡biased faulty S-box

5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

memory

- Fault on first element: C → 5
  - C: disappears
  - 5: appears twice

Many existing PFAs

- [ZLZBHDQR18], [GPT19], [PZRB19], [CGR20], [ESP20], [ZZJZBZLGR20], [XZYZHR21], [SBHRBM22], [TL22], [ZHFGTRZG23],…
  - Different analysis techniques
  - Aim to reduce number of data

Many existing PFAs

- [ZLZBHDQR18], [GPT19], [PZRB19], [CGR20], [ESP20], [ZZJZBZLGR20], [XZYZHR21], [SBHRBM22], [TL22], [ZHFGTRZG23],…
  - Different analysis techniques
  - Aim to reduce number of data

They all rely on a biased faulty S-box !!!

Countermeasures

- Detect the "bias"

⚡biased faulty S-box

5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

Countermeasures

- Detect the "bias"
  - #appearance (6): 1 ✅
  - #appearance (3): 1 ✅
  - #appearance (5): 2 ❌

⚡biased faulty S-box

5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

Countermeasures

- Detect the “bias”
  - #appearance (6): 1 ✅
  - #appearance (3): 1 ✅
  - #appearance (5): 2 ❌

⚡biased faulty S-box

5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

- Caforio and Banik [CB19] and Tissot et al. [TGB23] use this principle

Previous works

⚡ biased faulty S-box

5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

- Analyses based on biased faulty S-box

- Countermeasures detect bias

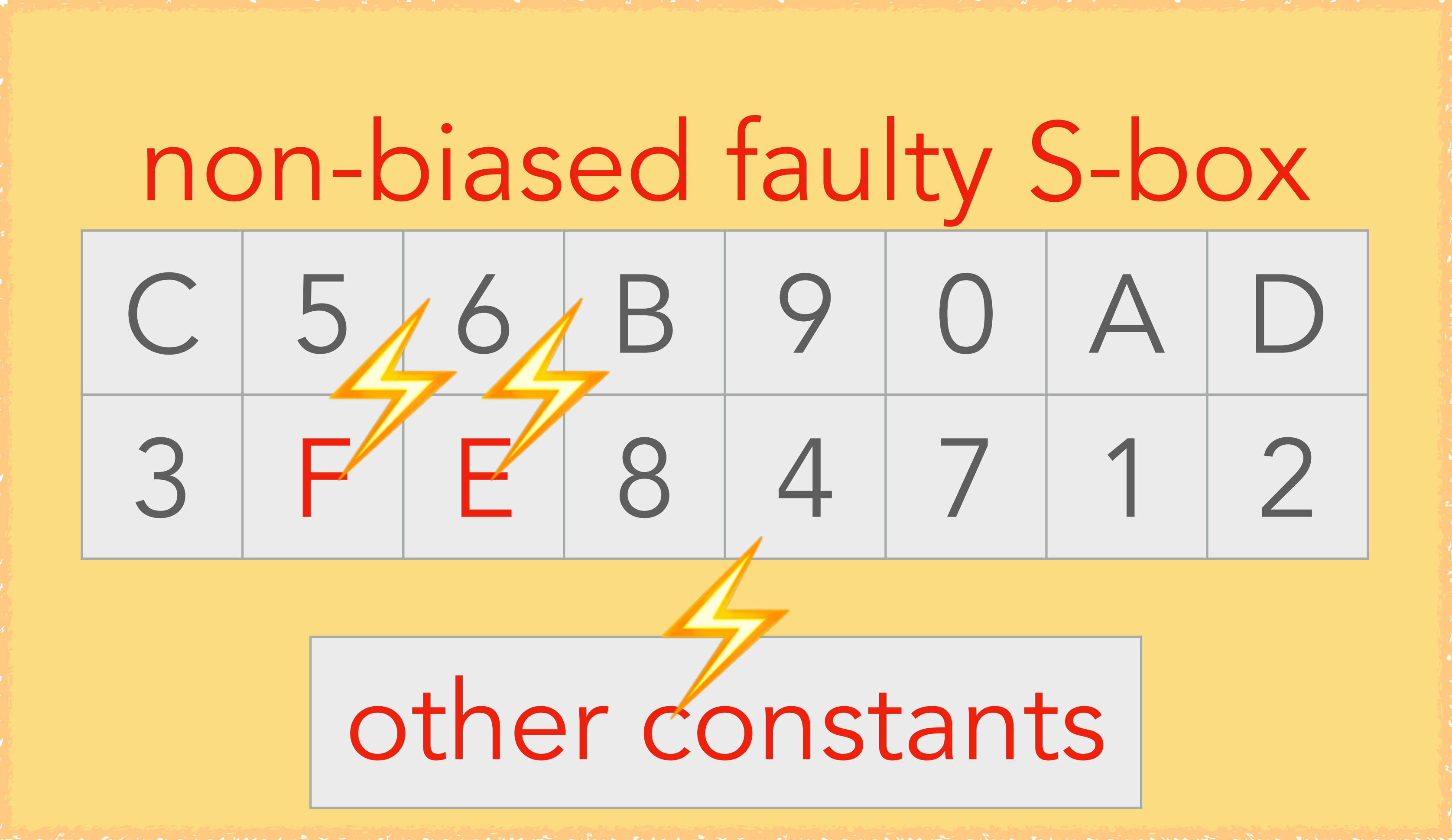
🤔

What if we have a non-biased faulty S-box ?
(eg., swap 2 elements)

🤔🤔

What if we fault another constant (not S-box) ?

Research question



non-biased faulty S-box

C	5	6	B	9	0	A	D
3	F	E	8	4	7	1	2

other constants

Previous works

biased faulty S-box

5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

Research question

non-biased faulty S-box

C	5	6	B	9	0	A	D
3	F	E	8	4	7	1	2

other constants

- ✦ Analyses based on biased faulty S-box

- ✦ Countermeasures detect bias

Previous works

⚡ biased faulty S-box

5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

Research question

non-biased faulty S-box

C	5	6	B	9	0	A	D
3	⚡ F	⚡ E	8	4	7	1	2

⚡ other constants

- ✦ Analyses based on biased faulty S-box
- ✦ Countermeasures detect bias → Bypassed ✅

Previous works

Research question

⚡ biased faulty S-box

5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

non-biased faulty S-box

C	5	6	B	9	0	A	D
3	⚡F	⚡E	8	4	7	1	2

⚡ other constants

- Analyses based on biased faulty S-box → Not applicable 😕

- Countermeasures detect bias → Bypassed ✅

Previous works

⚡ biased faulty S-box

5	5	6	B	9	0	A	D
3	E	F	8	4	7	1	2

Research question

non-biased faulty S-box

C	5	6	B	9	0	A	D
3	F ⚡	E ⚡	8	4	7	1	2

⚡ other constants

- ✦ Analyses based on biased faulty S-box → Not applicable 😕

Do we have other analysis for key recovery?

- ✦ Countermeasures detect bias → Bypassed ✅

1

Non-biased faulty S-box

non-biased faulty S-box

C	5	6	B	9	0	A	D
3	F	E	8	4	7	1	2

1

Non-biased faulty S-box

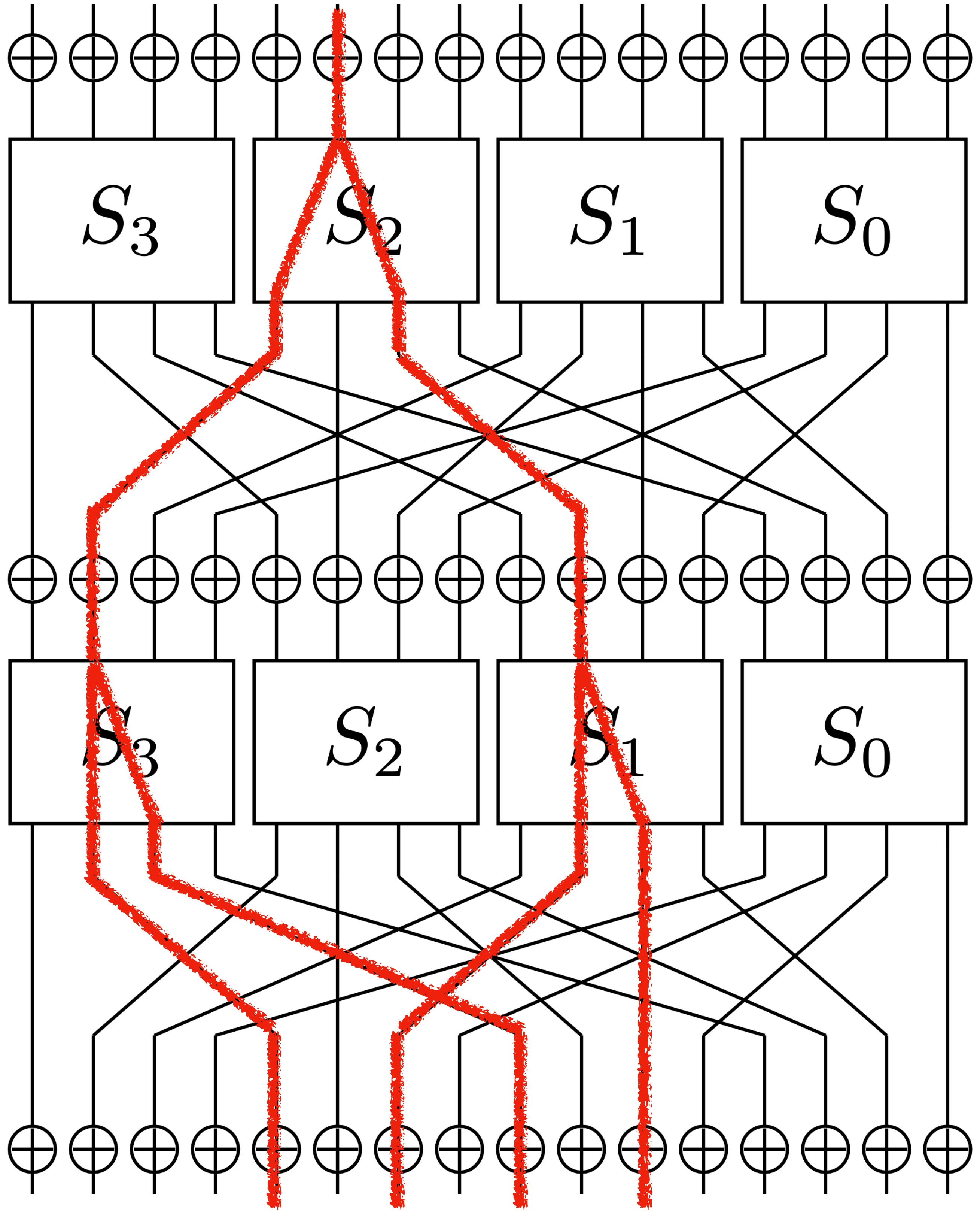
👉 Use linear attack

non-biased faulty S-box

C	5	6	B	9	0	A	D
3	F	E	8	4	7	1	2

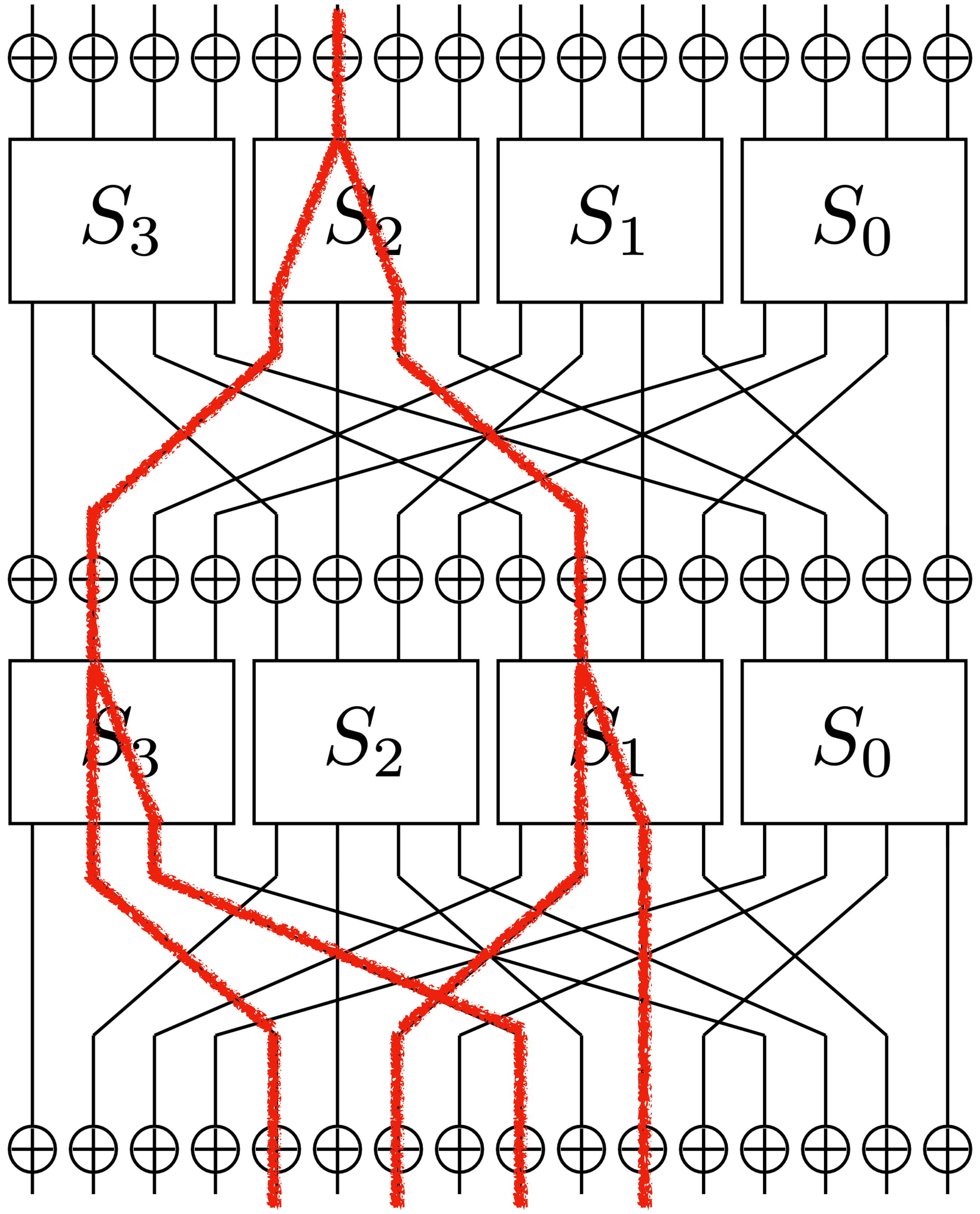
Linear attack

- ✦ Exploit the weakness of an S-box
- ✦ Target PRESENT cipher
- ✦ Use *multiple linear attack* [FN20] (Flórez-Gutiérrez and Naya-Plasencia)



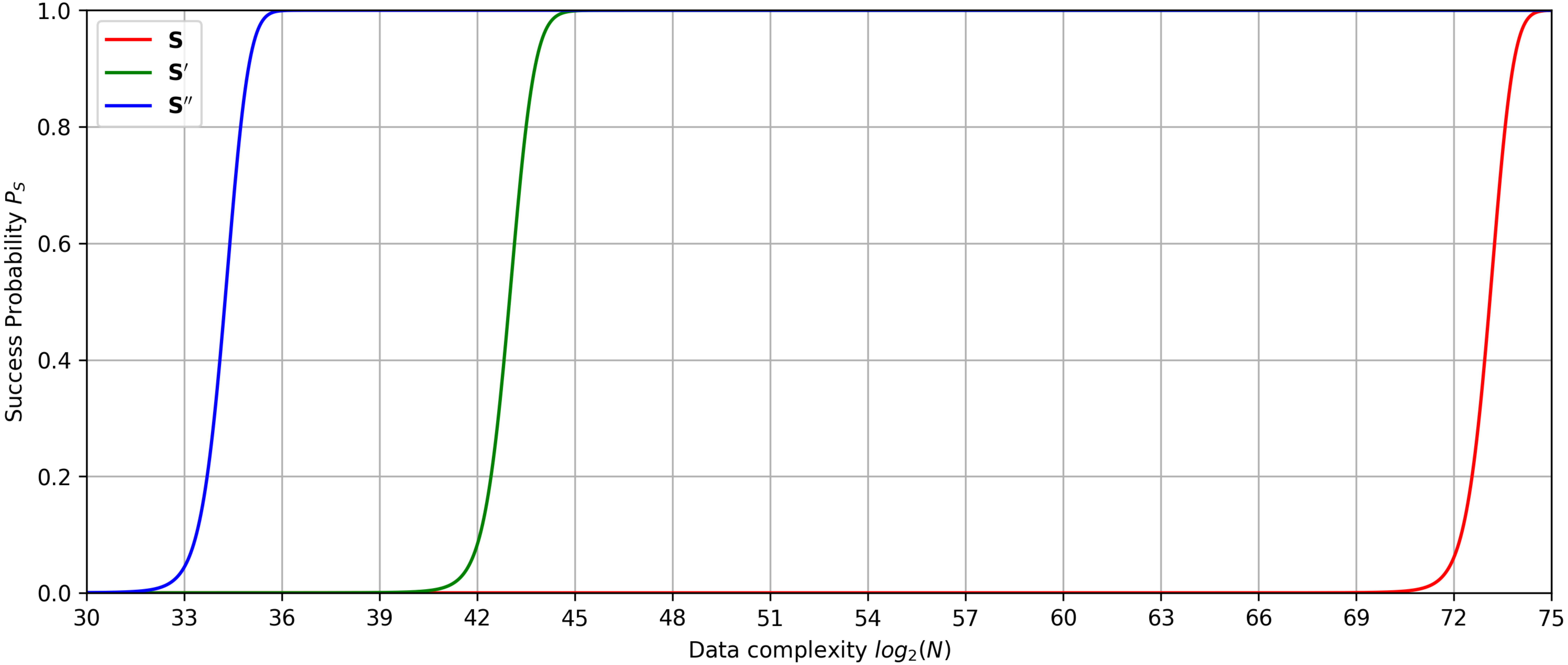
Linear attack

- Exploit the weakness of an S-box
- Target PRESENT cipher
- Use *multiple linear attack* [FN20] (Flórez-Gutiérrez and Naya-Plasencia)
- We care about
  - Data complexity
  - Success probability



	x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Orig.	**S**(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
2 faults	**S’**(x)	C	5	6	B	9	0	A	3	D	E	F	8	4	7	1	2
3 faults	**S”**(x)	C	5	8	B	9	0	A	D	3	6	F	E	4	7	1	2

	x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Orig.	**S**(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
2 faults	**S'**(x)	C	5	6	B	9	0	A	3	D	E	F	8	4	7	1	2
3 faults	**S''**(x)	C	5	8	B	9	0	A	D	3	6	F	E	4	7	1	2



	x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Orig.	**S**(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
2 faults	**S′**(x)	C	5	6	B	9	0	A	3	D	E	F	8	4	7	1	2
3 faults	**S″**(x)	C	5	8	B	9	0	A	D	3	6	F	E	4	7	1	2

Source	S-box	P_S	#Rounds	Time	Memory	Capacity	Data	Collect. Time
[FN20]	**S**	0.95	27	2^{72}	2^{44}	$2^{-54.8}$	$2^{63.4}$	$2^{20.8}$ years
This work	**S′**	0.95	31	2^{70}	2^{44}	$2^{-37.2}$	$2^{44.0}$	2.8 years
This work	**S″**	0.95	31	2^{70}	2^{44}	$2^{-28.4}$	$2^{35.1}$	2.1 days

	x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Orig.	**S**(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
2 faults	**S′**(x)	C	5	6	B	9	0	A	3	D	E	F	8	4	7	1	2
3 faults	**S″**(x)	C	5	8	B	9	0	A	D	3	6	F	E	4	7	1	2

Source	S-box	P_S	#Rounds	Time	Memory	Capacity	Data	Collect. Time
[FN20]	**S**	0.95	27	2^{72}	2^{44}	$2^{-54.8}$	$2^{63.4}$	$2^{20.8}$ years
This work	**S′**	0.95	31	2^{70}	2^{44}	$2^{-37.2}$	$2^{44.0}$	2.8 years
This work	**S″**	0.95	31	2^{70}	2^{44}	$2^{-28.4}$	$2^{35.1}$	2.1 days

	x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Orig.	**S**(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
2 faults	**S′**(x)	C	5	6	B	9	0	A	3	D	E	F	8	4	7	1	2
3 faults	**S″**(x)	C	5	8	B	9	0	A	D	3	6	F	E	4	7	1	2

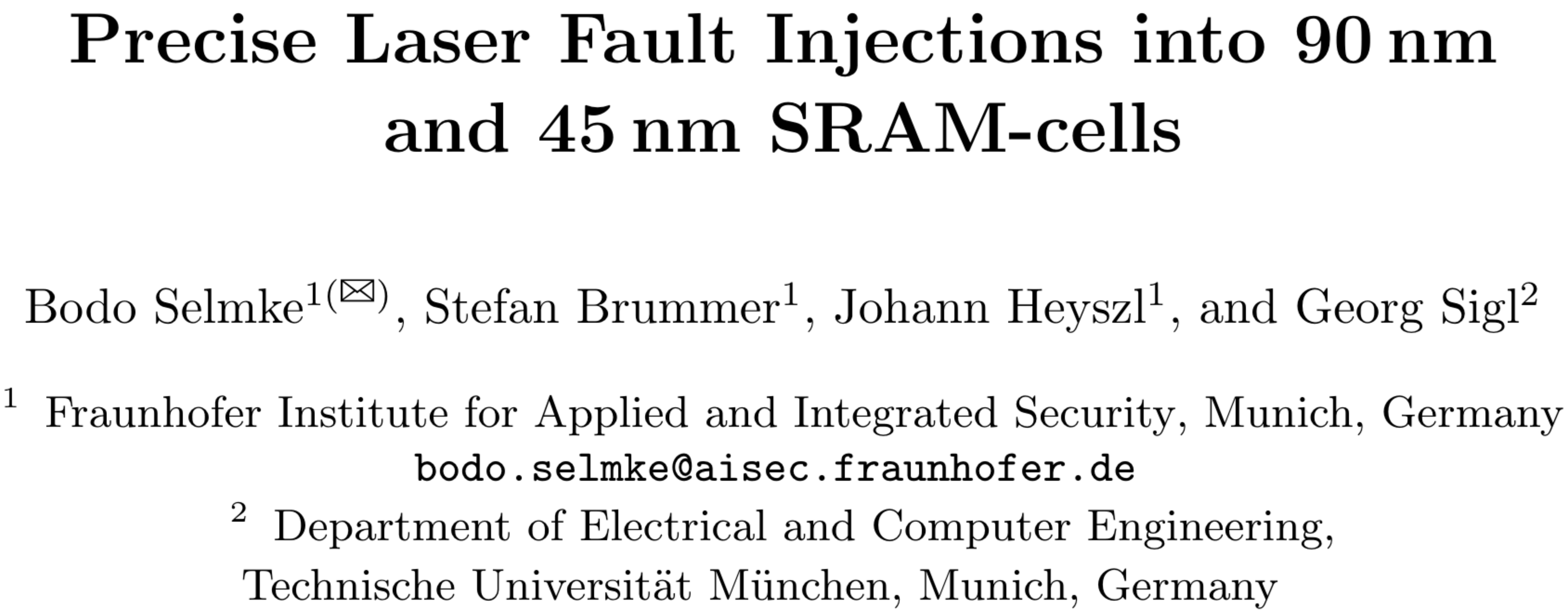
Source	S-box	P_S	#Rounds	Time	Memory	Capacity	Data	Collect. Time
[FN20]	**S**	0.95	27	2^{72}	2^{44}	$2^{-54.8}$	$2^{63.4}$	$2^{20.8}$ years
This work	**S′**	0.95	31	2^{70}	2^{44}	$2^{-37.2}$	$2^{44.0}$	2.8 years
This work	**S″**	0.95	31	2^{70}	2^{44}	$2^{-28.4}$	$2^{35.1}$	2.1 days

🧑‍⚖️

Reviewer:

The fault injection seems not realistic !?

But there exists evidence…



Precise Laser Fault Injections into 90 nm and 45 nm SRAM-cells

Bodo Selmke[1](✉), Stefan Brummer[1], Johann Heyszl[1], and Georg Sigl[2]

[1] Fraunhofer Institute for Applied and Integrated Security, Munich, Germany
bodo.selmke@aisec.fraunhofer.de
[2] Department of Electrical and Computer Engineering,
Technische Universität München, Munich, Germany

[SBHS16] at CARDIS 2016

Not enough motivation to do fault injection !?

Not enough motivation to do fault injection !?

- Multiple precise faults are difficult to achieve !?

Not enough motivation to do fault injection !?

- Multiple precise faults are difficult to achieve !?

💡 Let me ask the experts at JAIF

Not enough motivation to do fault injection !?

- Multiple precise faults are difficult to achieve !?

💡Let me ask the experts at JAIF

- Attack complexity is too high !?

Not enough motivation to do fault injection !?

- Multiple precise faults are difficult to achieve !?

  💡Let me ask the experts at JAIF

- Attack complexity is too high !?

  💡I have another idea

Not enough motivation to do fault injection !?

- Multiple precise faults are difficult to achieve !?

  💡Let me ask the experts at JAIF

- Attack complexity is too high !?

  💡I have another idea

- But we want to emphasize the risks of the current countermeasures [CB19], [TGB23]

Not enough motivation to do fault injection !?

- ✦ Multiple precise faults are difficult to achieve !?

💡Let me ask the experts at JAIF

- ✦ Attack complexity is too high !?

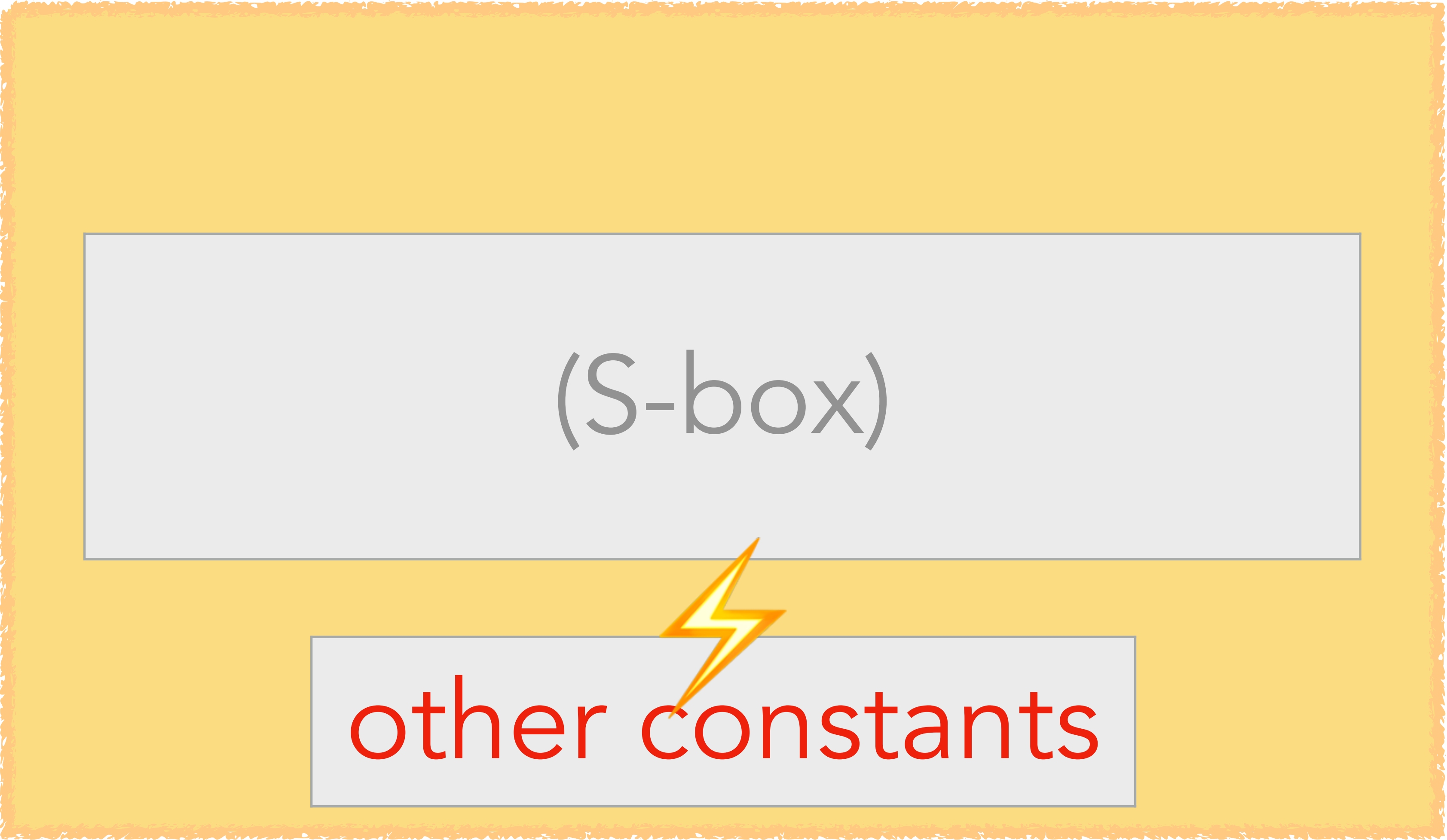
💡I have another idea

- ✦ But we want to emphasize the risks of the current countermeasures [CB19], [TGB23]

Detecting biases in the S-box is not sufficient

2

Faulting another constant

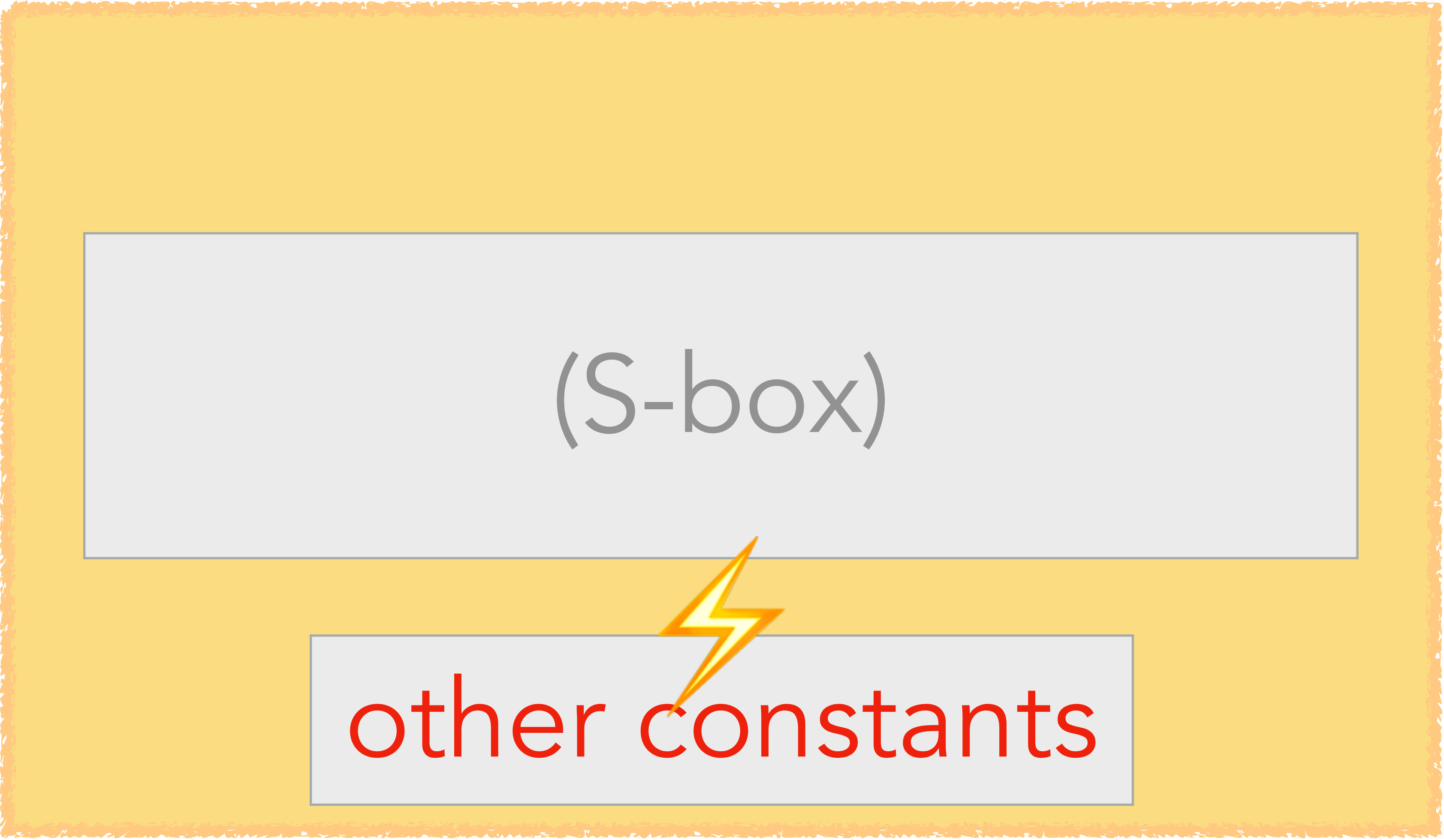


(S-box)

other constants

2

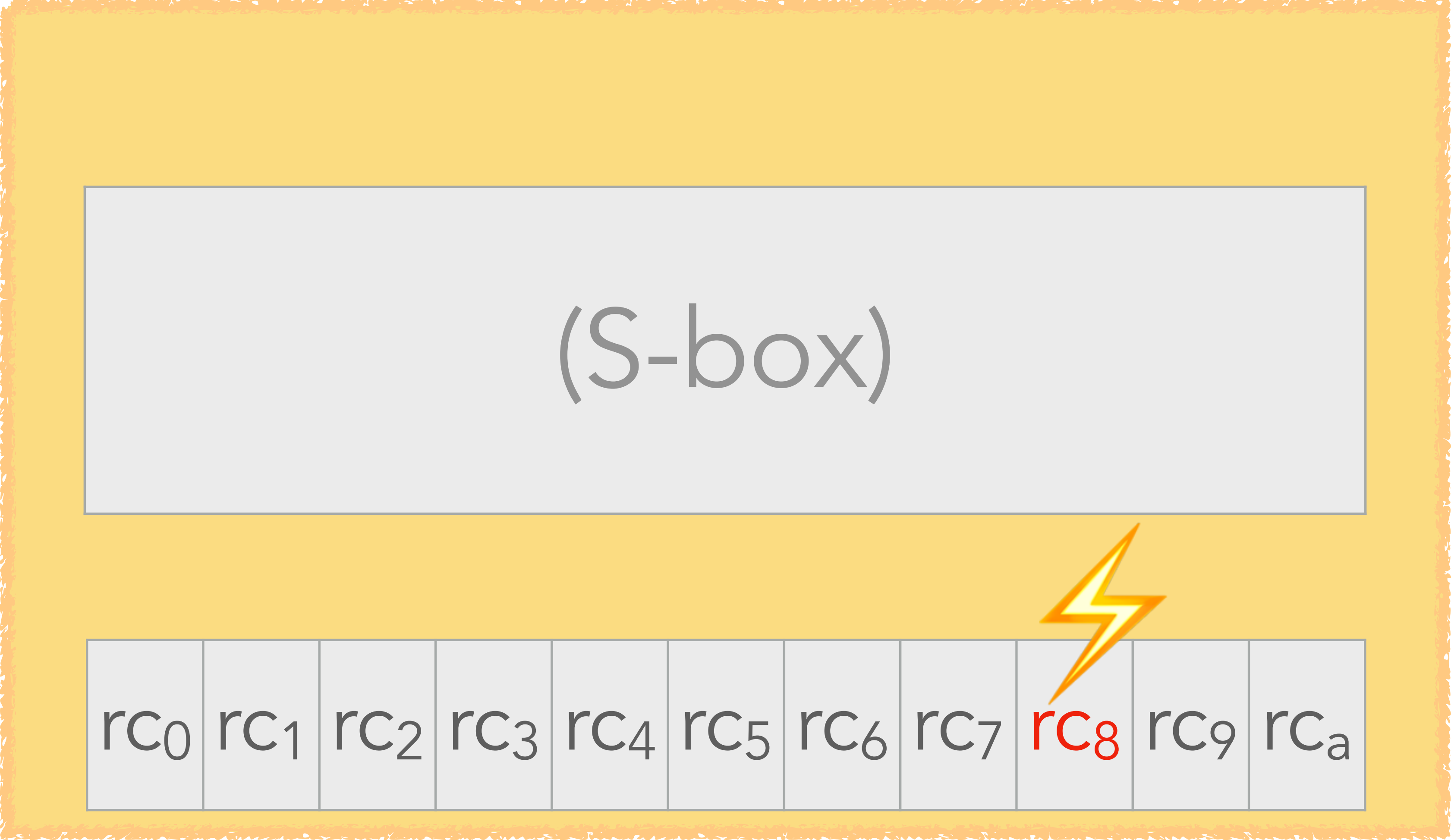
Faulting another constant



👉 Round constant of AES

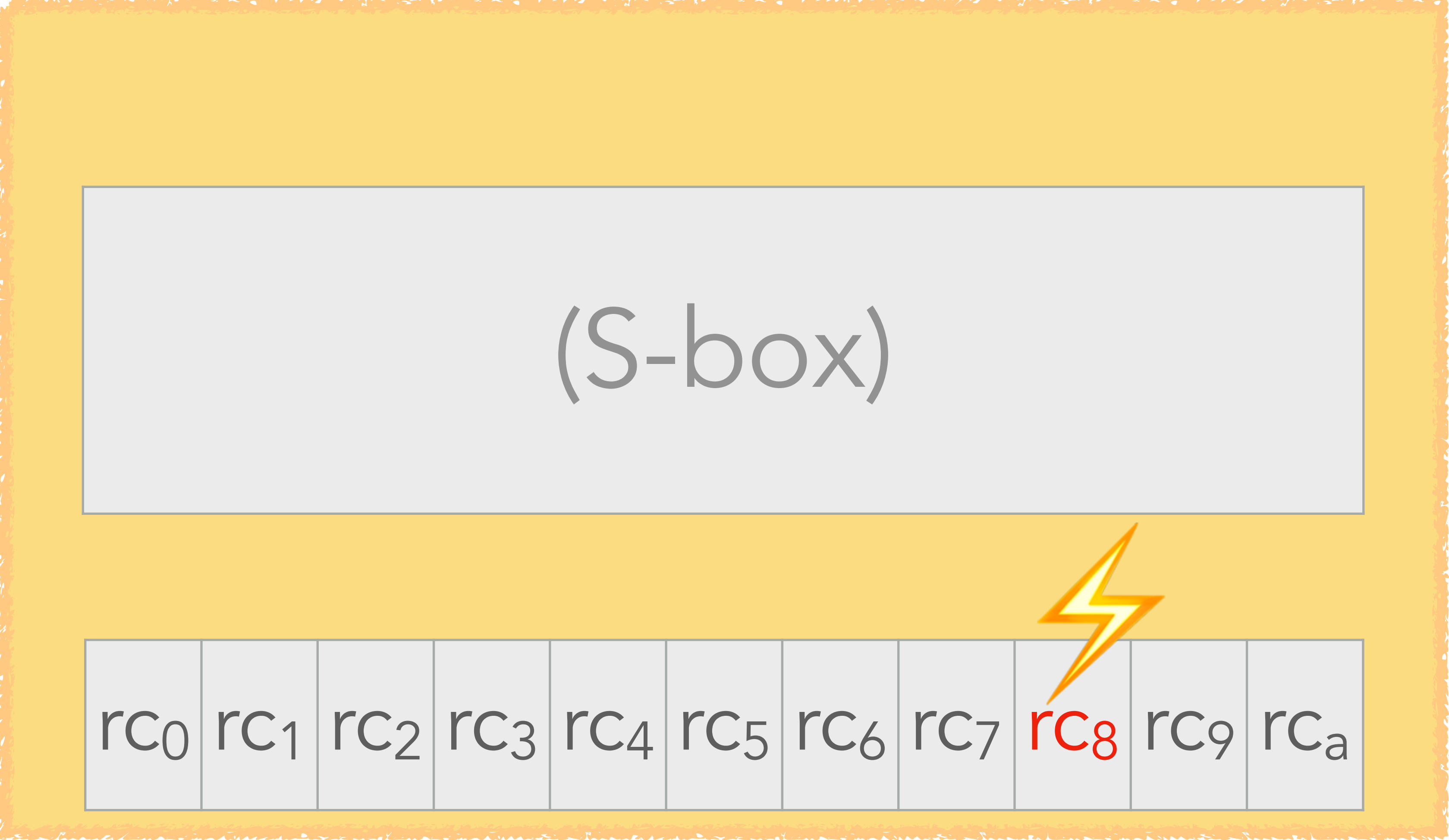
Faulting 8th round constant

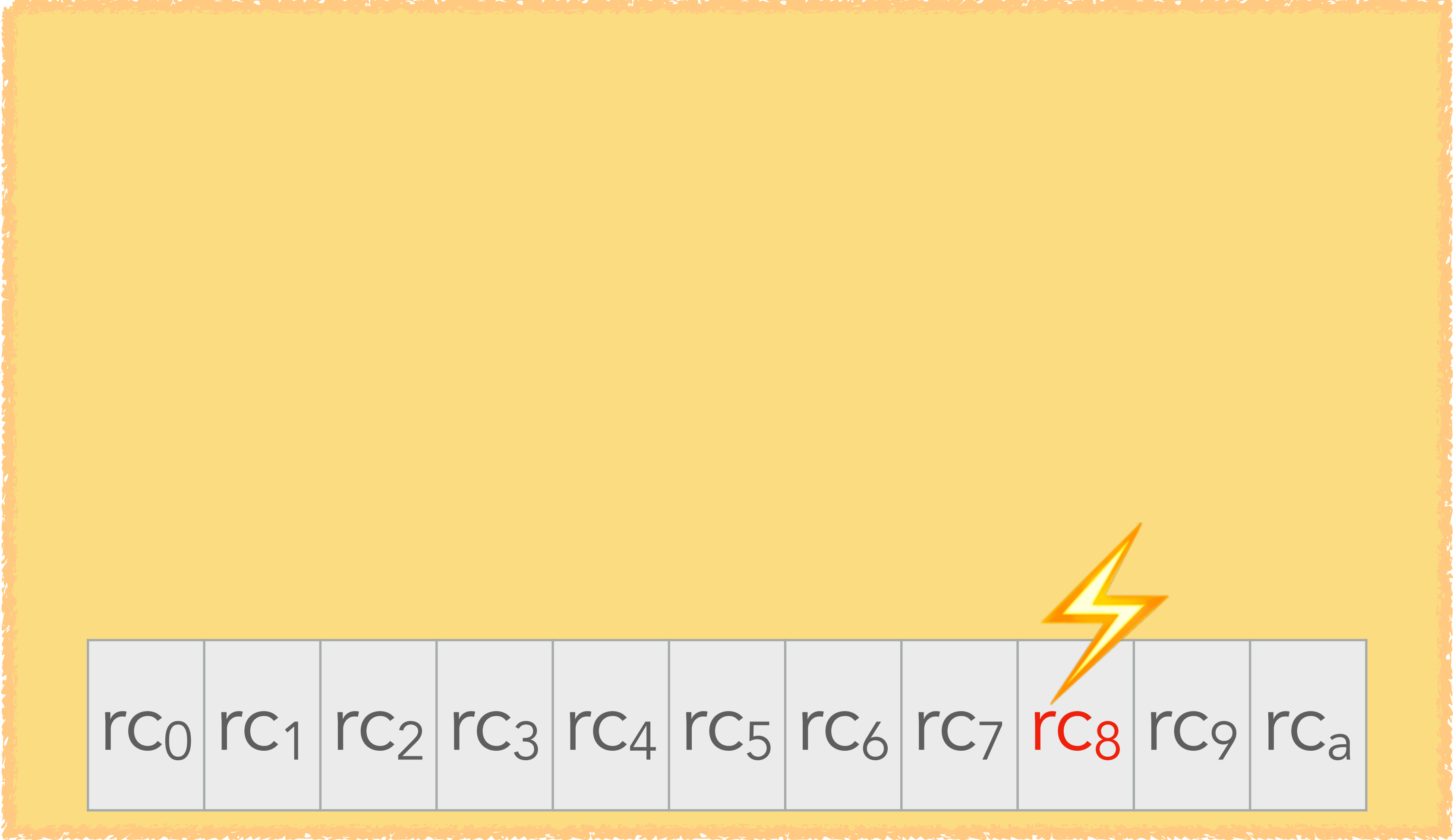
(Implementation with an S-box table may be vulnerable to cache timing attack)



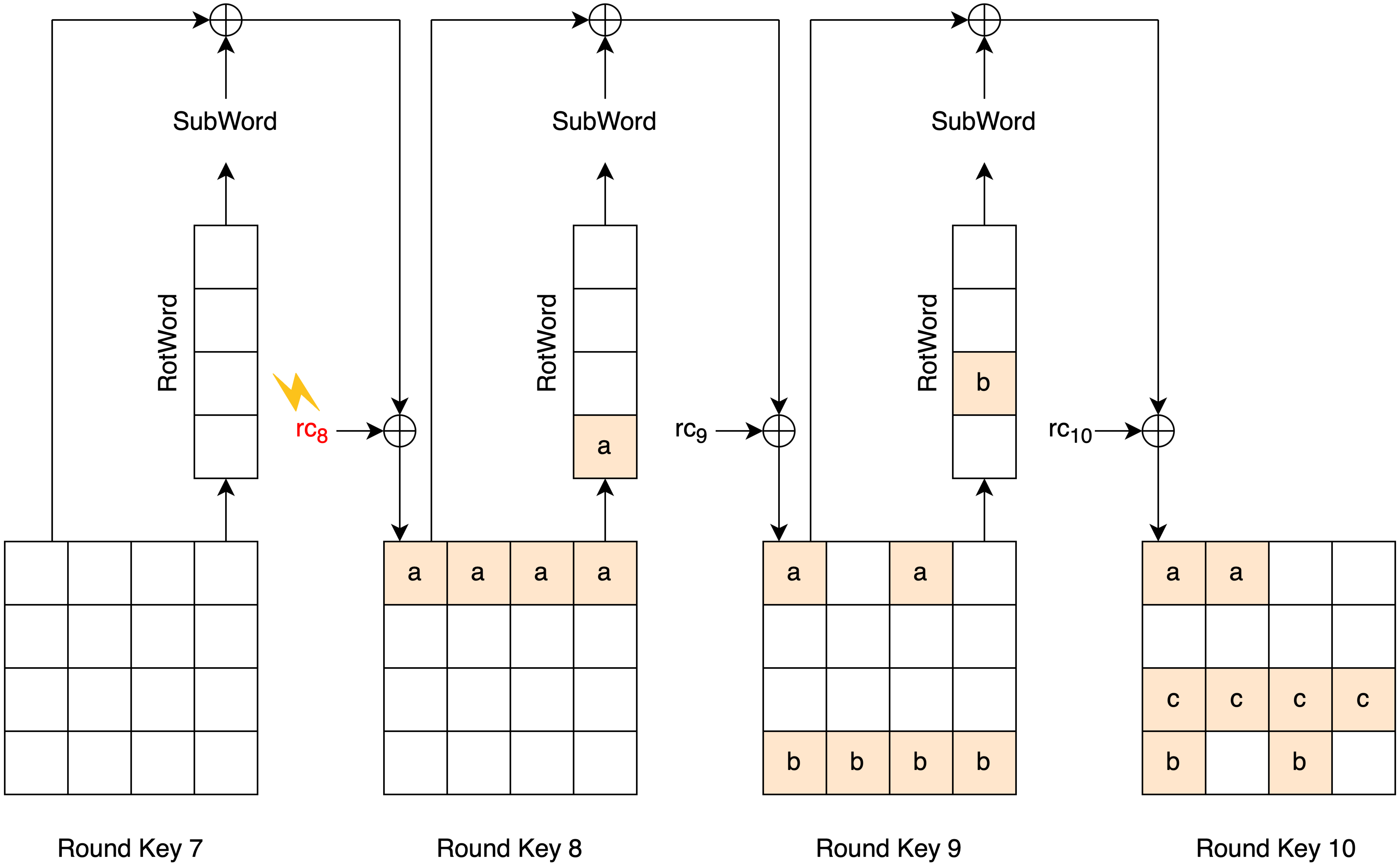
Faulting 8th round constant

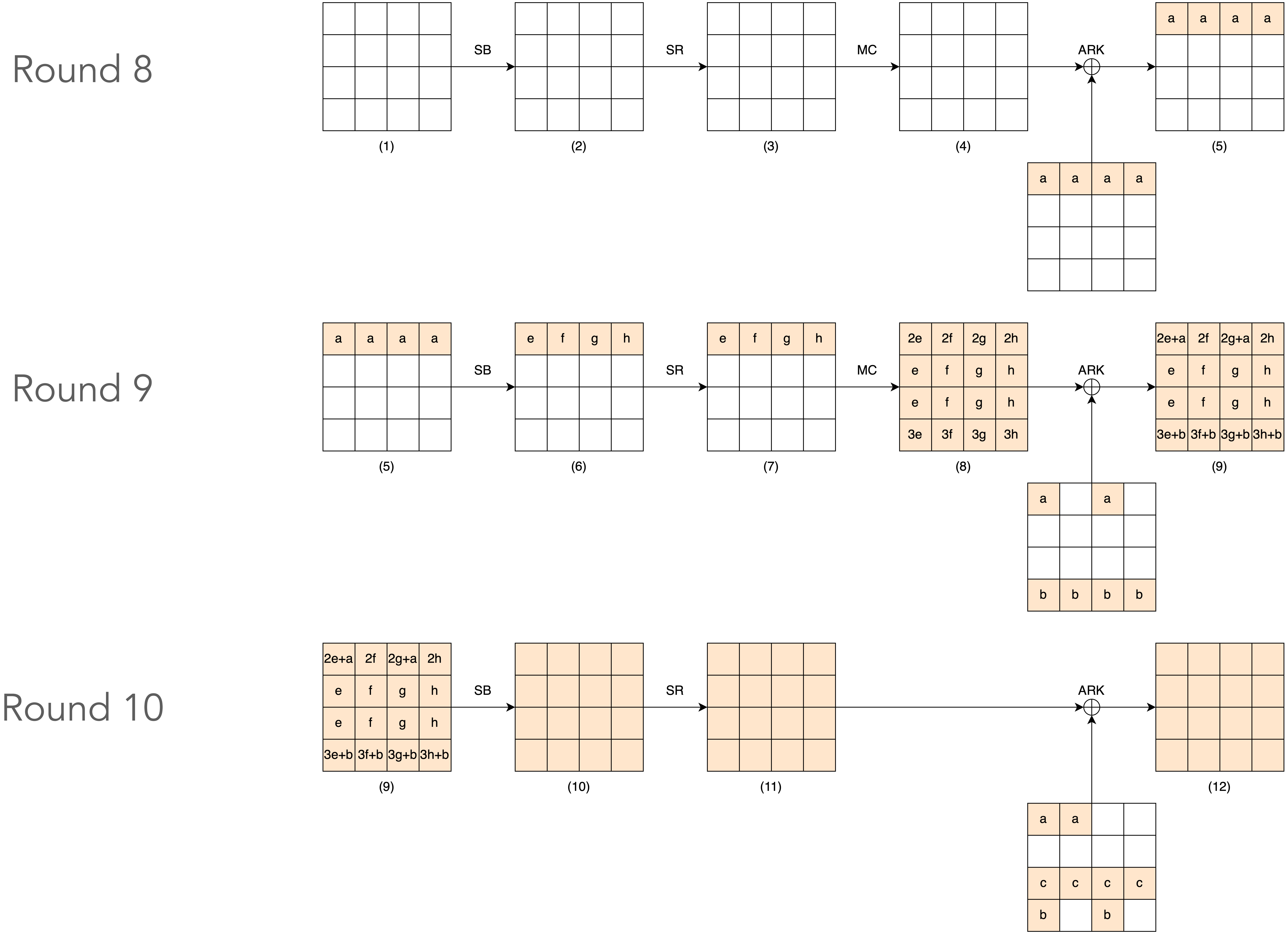
(Implementation with an S-box table may be vulnerable to cache timing attack)


(S-box)
rc_0 rc_1 rc_2 rc_3 rc_4 rc_5 rc_6 rc_7 rc_8 rc_9 rc_a


rc_0 rc_1 rc_2 rc_3 rc_4 rc_5 rc_6 rc_7 rc_8 rc_9 rc_a

Implementation *with* or *without* S-box table: doesn't matter !


SubWord
SubWord
SubWord
RotWord
RotWord
RotWord
a
b
rc_8
rc_9
rc_{10}
a a a a
a a
b b b b
a a
c c c c
b b
Round Key 7
Round Key 8
Round Key 9
Round Key 10

Round 8
SB
SR
MC
ARK
a a a a
(1)
(2)
(3)
(4)
(5)
a a a a
Round 9
a a a a
SB
e f g h
SR
e f g h
MC
2e 2f 2g 2h
e f g h
e f g h
3e 3f 3g 3h
ARK
2e+a 2f 2g+a 2h
e f g h
e f g h
3e+b 3f+b 3g+b 3h+b
(5)
(6)
(7)
(8)
(9)
a a
b b b b
Round 10
2e+a 2f 2g+a 2h
e f g h
e f g h
3e+b 3f+b 3g+b 3h+b
SB
SR
ARK
(9)
(10)
(11)
(12)
a a
c c c c
b b

Data complexity

- Number of correct-faulty ciphertext pairs
  - 2 pairs → 20 candidates
  - 3 pairs → 1 candidate (correct key)

💡

Non-biased faulty S-box with linear attack

💡

Fault beyond S-box elements
(round constant)

🤔🤔🤔

How to bypass the current countermeasures?

🤔🤔🤔

How to bypass the current countermeasures?

What is the idea of a stronger countermeasure?

🤔🤔🤔

How to bypass the current countermeasures?

What is the idea of a stronger countermeasure?

Reach out to me ! 🙋🏻

Attacks and Countermeasures in Persistent Fault Model

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

joint work with Vincent Grosso and Pierre-Louis Cayrel

UNIVERSITÉ DE LYON

UNIVERSITÉ JEAN MONNET
SAINT-ÉTIENNE

Laboratoire Hubert Curien
UMR ▪ CNRS ▪ 5516 ▪ Saint-Étienne

anr
PROPHY ANR-22-CE39-0008-01

References

- [CGR20] Carré, Guilley, Rioul: “Persistent fault analysis with few encryptions”, COSADE 2020
- [ESP20] Engels, Schellenberg, Paar: “SPFA: SFA on multiple persistent faults”, FDTC 2020
- [GPT19] Gruber, Probst, Tempelmeier: “Persistent fault analysis of OCB, DEOXYS and COLM”, FDTC 2019
- [PZRB19] Pan, Zhang, Ren, Bhasin: “One fault is all it needs: Breaking higher-order masking with persistent fault analysis”, DATE 2019
- [SBHRBM22] Soleimany, Bagheri, Hadipour, Ravi, Bhasin, Mansouri: “Practical multiple persistent faults analysis”, CHES 2022
- [TL22] Tang, Liu: “MPFA: An efficient multiple faults-based persistent fault anal- ysis method for low-cost FIA”, TCAD 2022
- [XZYZHR21] Xu, Zhang, Yang, Zhao, He, Ren: “Pushing the limit of PFA: Enhanced persistent fault analysis on block ciphers”, TCAD 2021
- [ZHFGTRZG23] Zhang, Huang, Feng, Gong, Tao, Ren, Zhao, Gou: “Efficient persistent fault analysis with small number of chosen plaintexts”, CHES 2023
- [ZLZBHDQR18] Zhang, Lou, Zhao, Bhasin, He, Ding, Qureshi, Ren: “Persistent Fault Analysis on Block Ciphers”, CHES 2018
- [ZZJZBZLGR20] Zhang, Zhang, Jiang, Zhu, Bhasin, Zhao, Liu, Gu, Ren: “Persistent fault attack in practice”, CHES 2020
- [TGB23] Tissot, Grosso, Bossuet: “BALoo: First and efficient countermeasure dedicated to persistent fault attacks”, IOLTS 2023
- [CB19] Caforio, Banik: “A study of persistent fault analysis”, SPACE 2019
- [FN20] Flórez-Gutiérrez, Naya-Plasencia: “Improving key-recovery in linear attacks: Application to 28-round PRESENT”, EUROCRYPT 2020