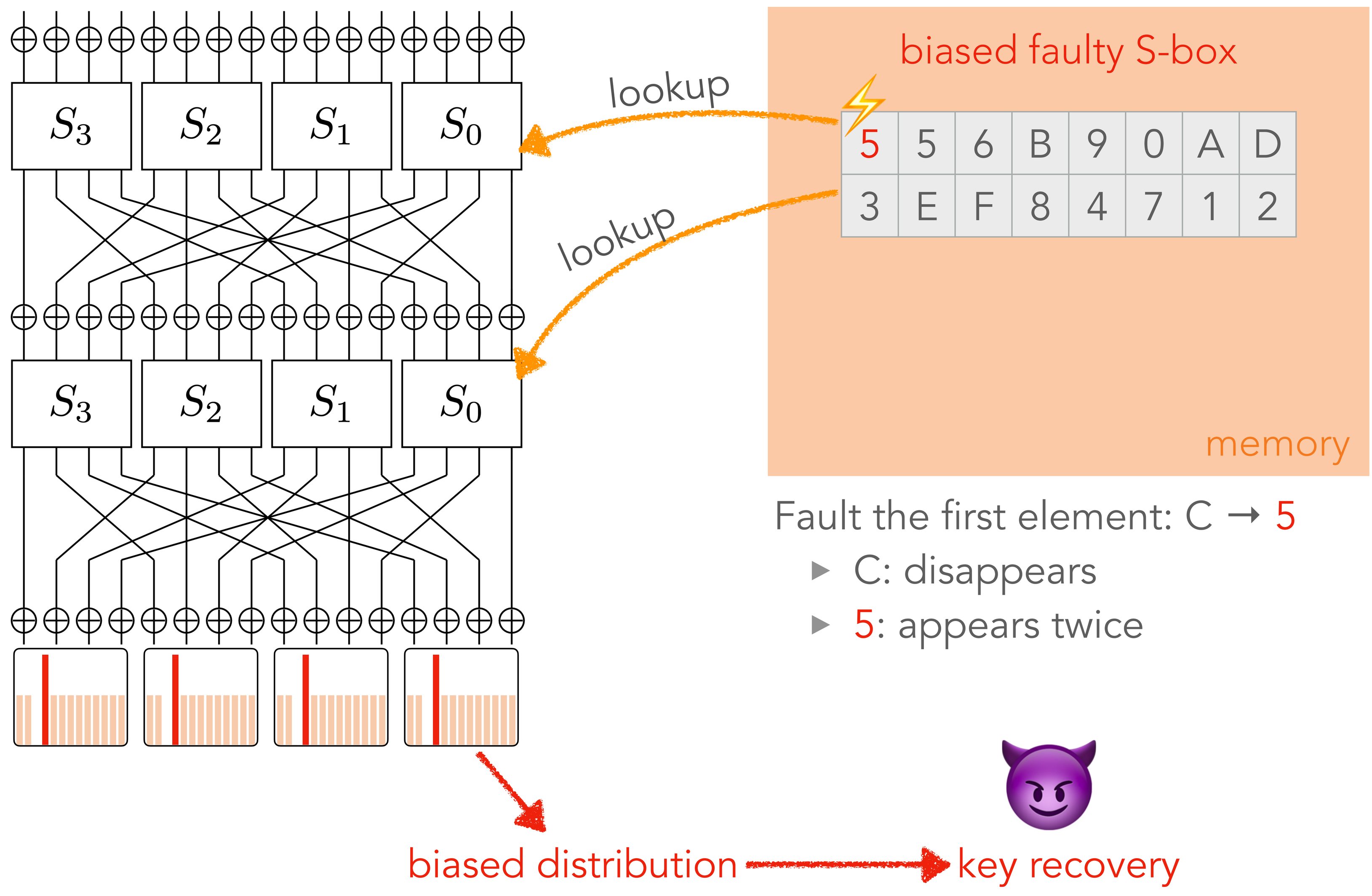
Attacks and Countermeasures in Persistent Fault Model

Viet Sang Nguyen, Vincent Grosso, Pierre-Louis Cayrel

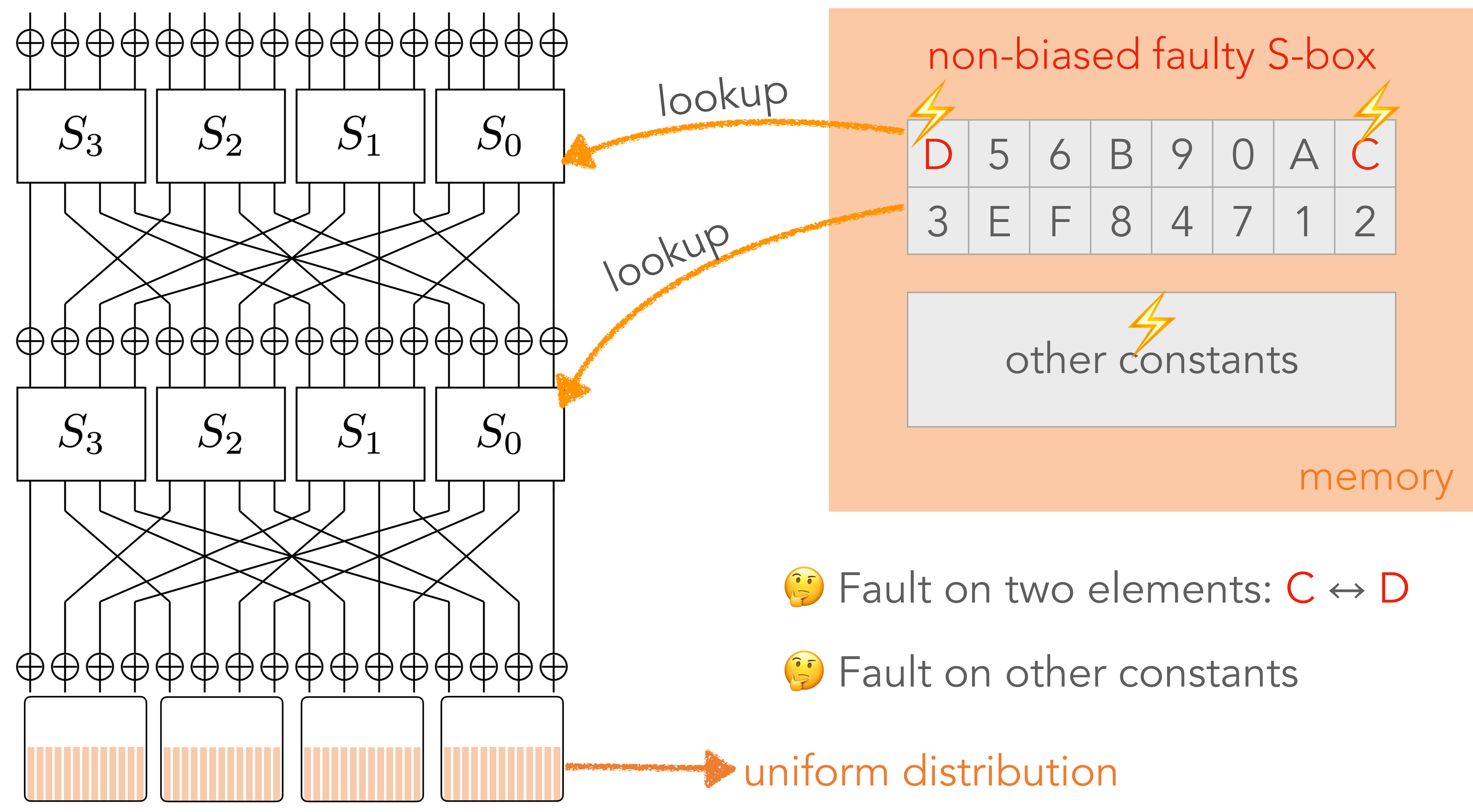
Université Jean Monnet, Laboratoire Hubert Curien, CNRS UMR 5516
42000 Saint-Étienne, France
viet.sang.nguyen@univ-st-etienne.fr

1 Introduction: Persistent Fault Attacks



- Many attacks exploit biased faulty S-boxes, for example, [1,2,3]
- SOTA countermeasures use the same idea: detecting biases [4,5]

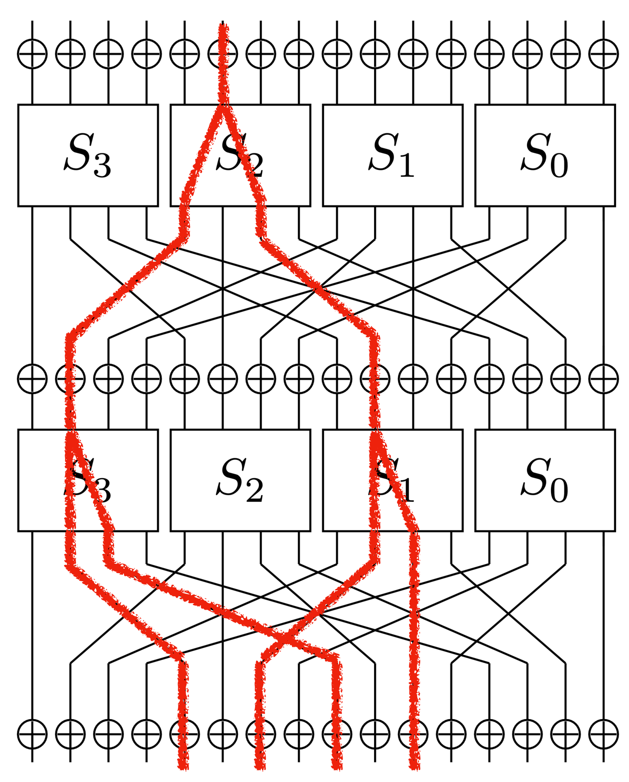
2 Research Questions



- Bypass SOTA countermeasures of detecting biases [4,5]
- Cannot use analyses of previous attacks [1,2,3] for key recovery
- Do we have another method to recover the key?
- Do we have a stronger countermeasure?

3 Results: Linear Attack

	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



- We use multiple linear attack [6] to exploit the weakness of the non-biased faulty S-box
- Linear attack aims at gaining *advantage* over the exhaustive search
- If the correct key guess of n bits is ranked as the i-th candidate among 2^n possibilities by a key-ranking statistic, the advantage over the exhaustive search is:

$$a = n - \log_2(i)$$

- We are interested in the attack complexity:
  - advantage a
  - number of plaintext-ciphertext pairs N
  - probability of success P_S

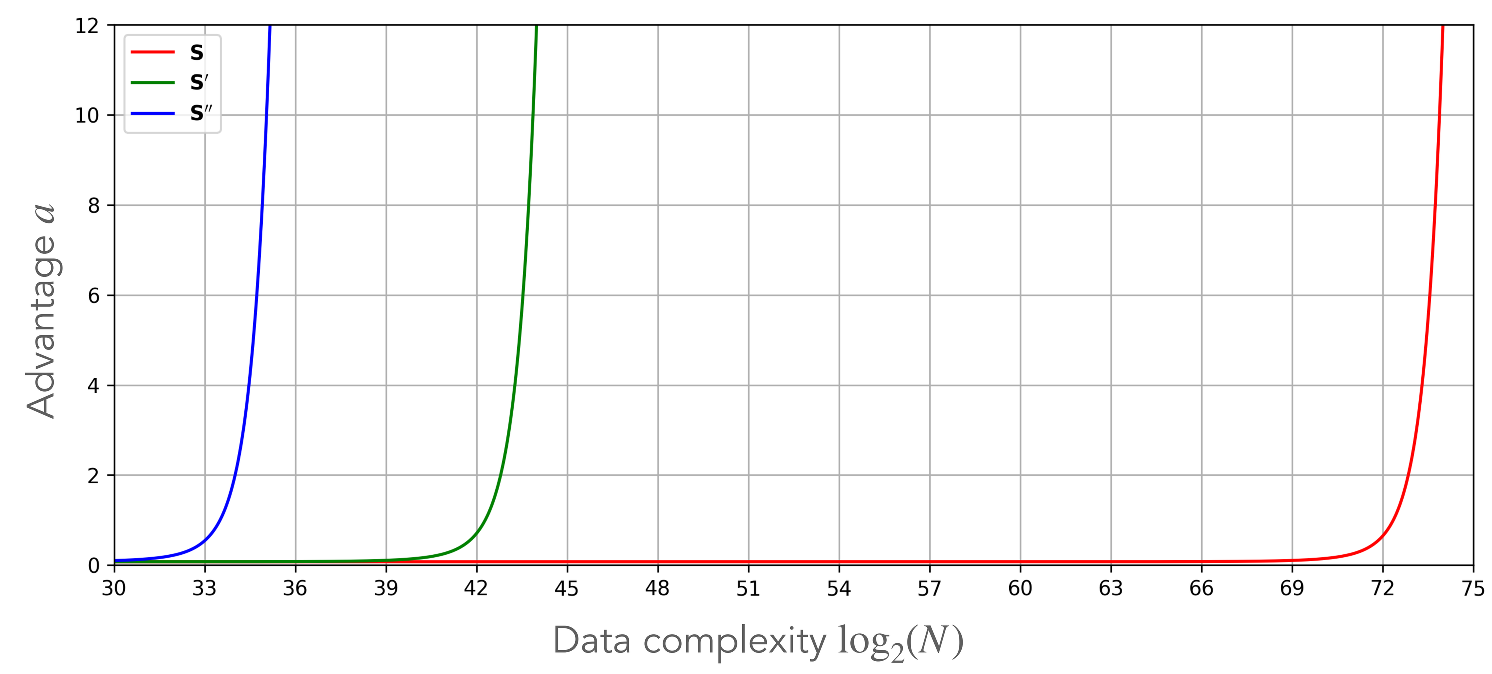


Figure of advantage and data complexity for attack on full-round PRESENT corresponding to a fixed success probability $P_S = 0.95$

Source	S-box	P_S	#Rounds	Time	Memory	Capacity	Data	Collect. Time
[6]	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

Table of attack complexity comparison. The attack of [6] is on a reduced-round cipher, while our attack is on a full-round cipher.
The data collection time is estimated on a 100MHz device with the assumption that an S-box lookup operation takes 1 cycle, thus 31x16=496 cycles per encryption.

4 Discussion

- [FAQ] The attack complexity might still be too high for a fault attack. However, it is important to emphasize that this attack works even when the SOTA countermeasures [4,5] are in place. This finding underscores that these countermeasures are not entirely sufficient to prevent persistent fault attacks.
- [FAQ] Fault injection might be a challenge. This attack requires multiple precise faults to swap elements. Multiple precise bit flips were shown to be feasible in practice [7]. Experiments are left as future work for now :)

5 More Information

- How to bypass the countermeasures?
- How to exploit a fault induced in another constant rather than S-box?
- What is the idea of a stronger countermeasure?

Full paper

About author

[1] Zhang el al.: Persistent Fault Analysis on Block Ciphers, CHES 2018
[2] Zhang el al.: Persistent Fault Attack in Practice, CHES 2020
[3] Someimany el al.: Practical Multiple Persistent Fault Analysis, CHES 2021
[4] Caforio and Banik: A Study of Persistent Fault Analysis, SPACE 2019
[5] Tissot et al.: BALoo, First and Efficient Countermeasure Dedicated to Persistent Fault Attacks, IOLTS 2023
[6] Flórez-Gutiérrez and Naya-Plasencia: Improving Key-Recovery in Linear Attacks, Application to 28-round PRESENT, EUROCRYPT 2020
[7] Selmke et al.: Precise Laser Fault Injections into 90 nm and 45 nm SRAM-cells, CARDIS 2016

PROPHY ANR-22-CE39-0008-01