DE LA RECHERCHE À L'INDUSTRIE

cea

A DFA ON AES BASED ON THE ENTROPY OF ERROR DISTRIBUTIONS

FDTC2012 |

Ronan Lashermes, Guillaume Reymond, Jean-Max Dutertre, Jacques Fournier, Bruno Robisson and Assia Tria

9 SEPTEMBER 2012

www.cea.fr

leti

Ecole Nationale Supérieure des Mines
SAINT-ETIENNE
Site Georges Charpak

Introduction

- In order to design secure cryptosystems, one has to assess the risks of potential attacks.
- We want to discuss about the practical implementation of attacks, more precisely about the fault models.

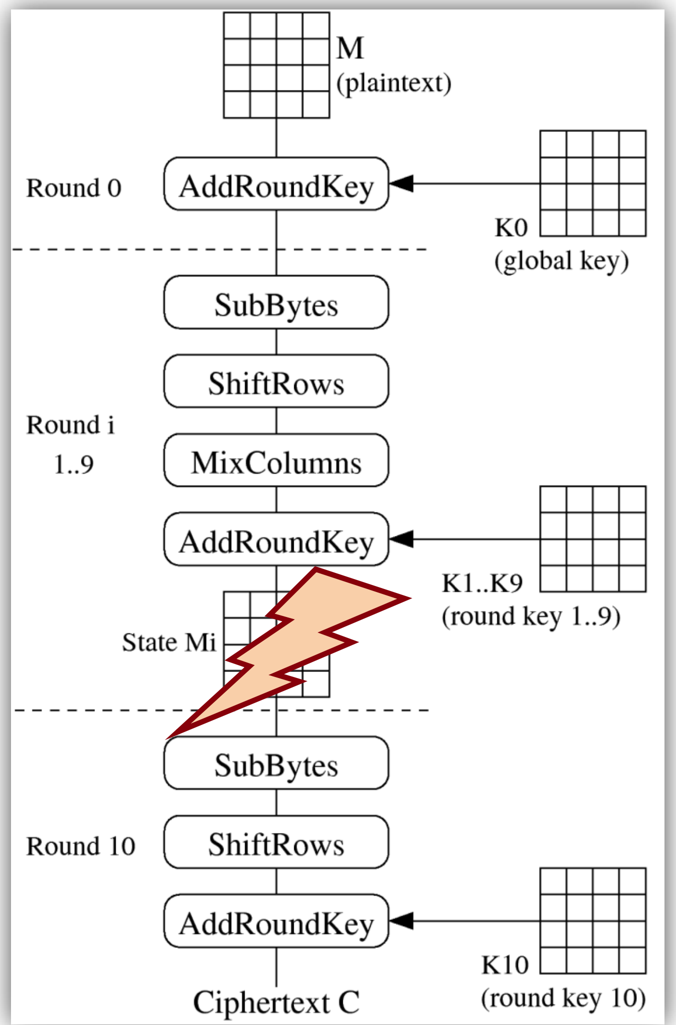
- We want a DFA:
  - General: can be used with all injection means.
  - Adaptive: the efficiency increases when the fault model is more restrictive.
  - Simple to implement.
  - Without prior knowledge of the fault model…
  - Or with prior knowledge and higher efficiency.
  - Helped by some countermeasures!

OUTLINE

SECTION 1
CONTEXT

CONTEXT: DFA ON AES

AES-128

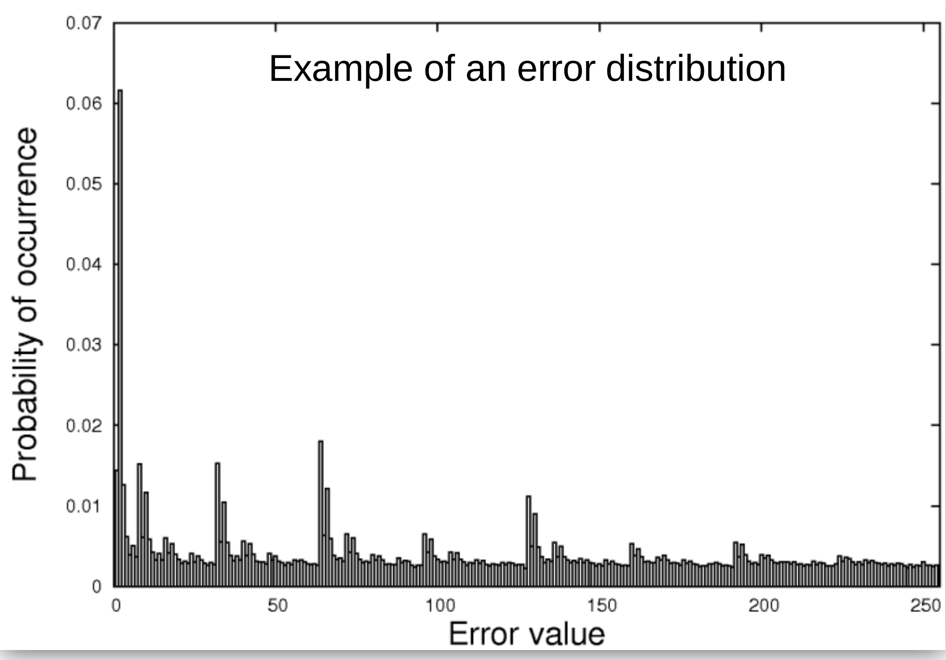


Differential Fault Analysis

- Attacker corrupts one of the intermediate states of the AES.
- Attacker performs a differential cryptanalysis between the correct cipher (C) and the erroneous one (D) to infer information about the secret key.

CONTEXT: FAULT MODELS

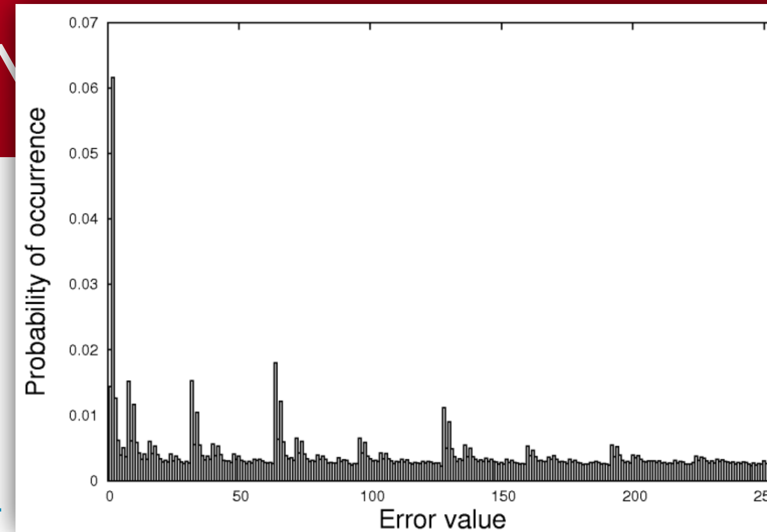
- The fault model is the set of restrictions put on the injected faults.
- Common examples are:
  - Single bit faults ($2^{3*16} = 2^{48}$ authorized faults on the State)
  - Single byte faults ($(4*2^8)^{4} = 2^{40}$ authorized faults on the State)
- Key extraction analyses are:
  - Either restrictive (*Giraud's: 2^{48}, Piret's: 2^{40} …*)
  - Either inefficient: a high number of fault injections is required (*Moradi's: $2^{127.9}$…*)
- We represent a fault model with an error distribution. (*2^{128}*)

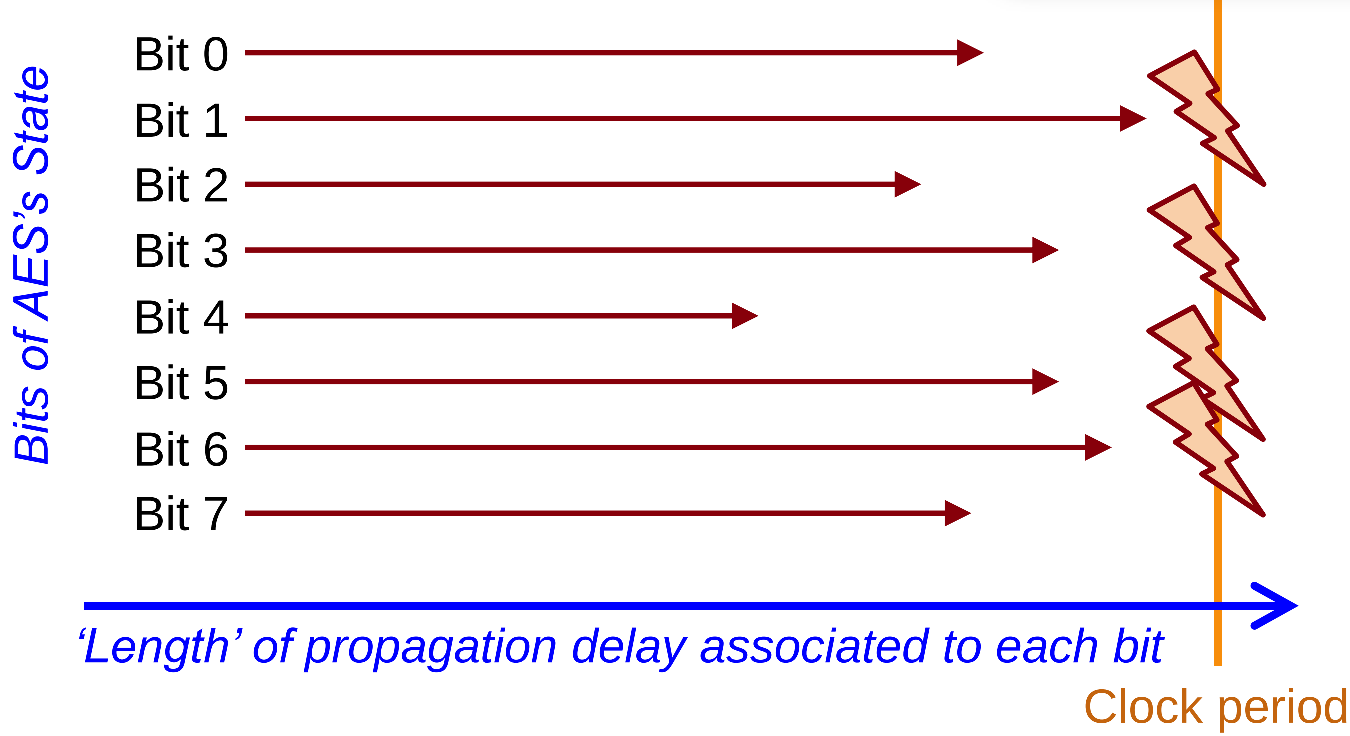


CONTEXT: FAULT INJECTION

CLOCK GLITCHES

- Clock glitches create memorization faults in registers through setup time violations.
- Faults are probabilistic.
- Distributions can be used for all injection means.



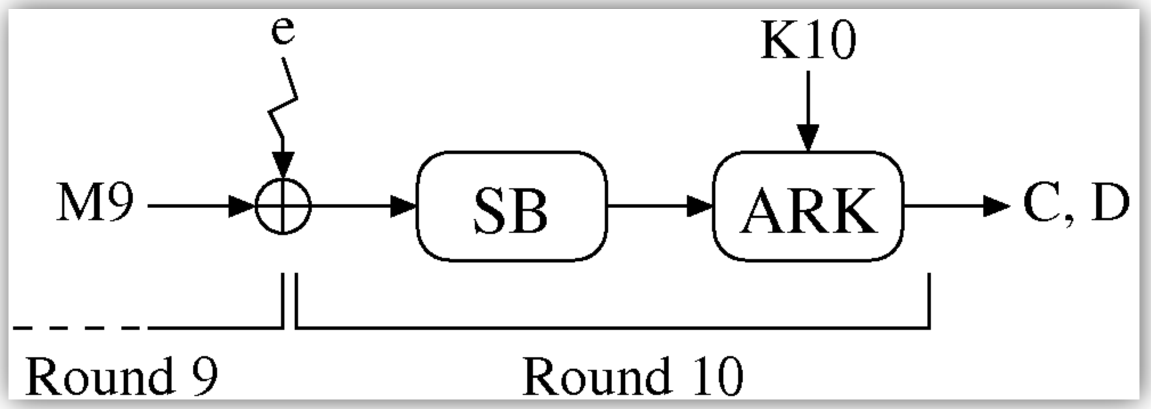


SECTION 2
ENTROPY-BASED METHODOLOGY

ENTROPY: OUR ANALYSIS

- In order to work, our analysis needs the following hypotheses:
  - The faults are bit-flip.
  - The faults are not uniformly distributed.*
  - The faults are injected on M9.
- *From now on we shall concentrate on individual bytes…*

- The correct key byte is noted $K10$.
- For each realization i:
  - First a valid encryption is executed (C_i).
  - Then a fault is injected on M9 and the faulty cipher value is memorized (D_i).



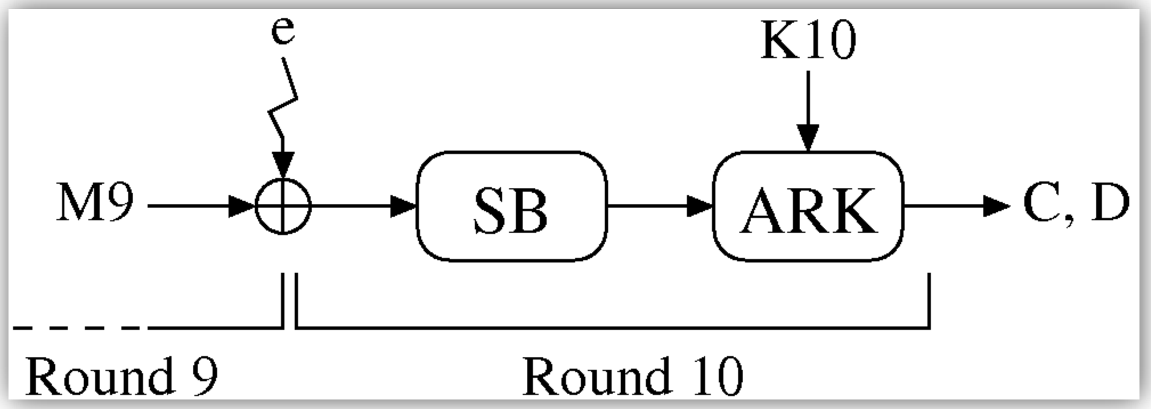
* A work based on a similar principle can be found in *DFA on DES middle rounds by M. Rivain (CHES 2009)*

ENTROPY: RECONSTRUCTING THE FAULT MODEL

- From C_i and D_i (correct and faulty ciphers)
- Given a key guess s,
- The fault guess $e_{i,s}$ is computed with:

$$M9_{i,s} = SB^{-1}(C_i \oplus s)$$

$$e_{i,s} = M9_{i,s} \oplus SB^{-1}(D_i \oplus s)$$



RK-table

- We can know construct the Realization/Key hypothesis (RK) table, filled with *($e_{i,s}$)*.

Realization \ Key	0	1	...	255
0	$e_{0,0}$	$e_{0,1}$	$\dots$	$e_{0,255}$
1	$e_{1,0}$	$e_{1,1}$	$\dots$	$e_{1,255}$
...	$\dots$	$\dots$	$\dots$	$\dots$
i_{max}	$e_{i_{max},0}$	$e_{i_{max},1}$	$\dots$	$e_{i_{max},255}$

- This table has two interesting properties:
  - Only one column (for $s = K10$) corresponds to faults actually injected.
  - For every wrong key guess, the corresponding column is quasi-random.

ENTROPY: DECISION CRITERION

Finding the correct column

- The uniformity of a distribution is simply determined with Shannon entropy:

$$H(p_s) = -\sum_{e=0}^{255} p_s(e) \log_2 p_s(e)$$

- Decision criterion:
  - $H(p_s) \xrightarrow[i_{max}\to\infty]{} 8$ if $s \neq K10$
  - $H(p_{K10}) \xrightarrow[i_{max}\to\infty]{} H_{inj} < 8$
- Valid only for sets of faults of infinite size

ENTROPY: DECISION CRITERION

Finding the correct column with a finite number of realizations

- Comparison with pseudo-random sets.
- i_{max}: number of realizations, $\mu_{i_{max}}^{rand}$: the mean, $\sigma_{i_{max}}^{rand}$: the standard deviation.
- $H(p_s)$ the measured entropy for the key guess *s*.
- We can express the confidence *cf* that an entropy of value *H* is not random by:

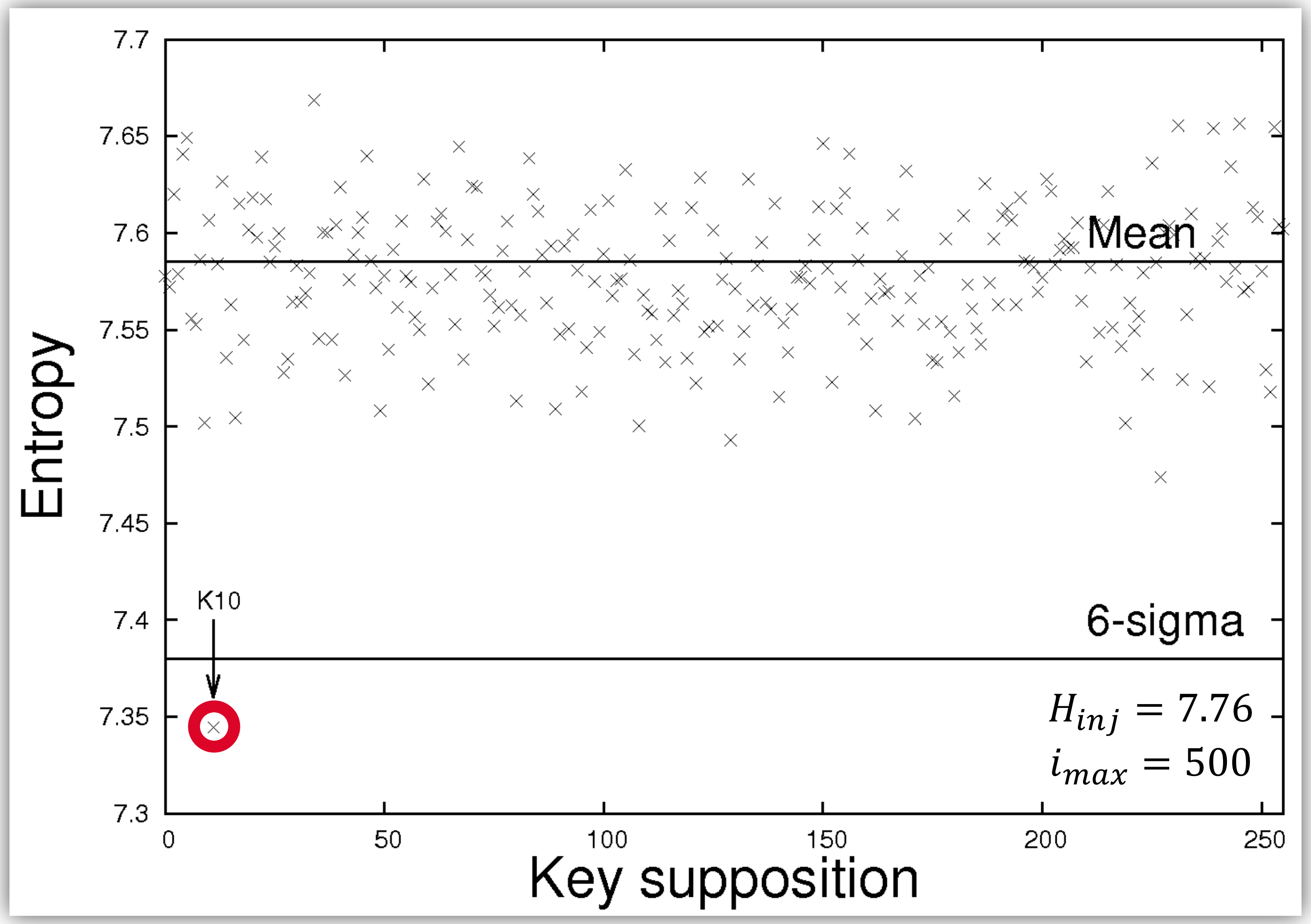
$$cf_{i_{max}}(H) = \frac{\mu_{i_{max}}^{rand} - H}{\sigma_{i_{max}}^{rand}}$$

- Decision criterion:

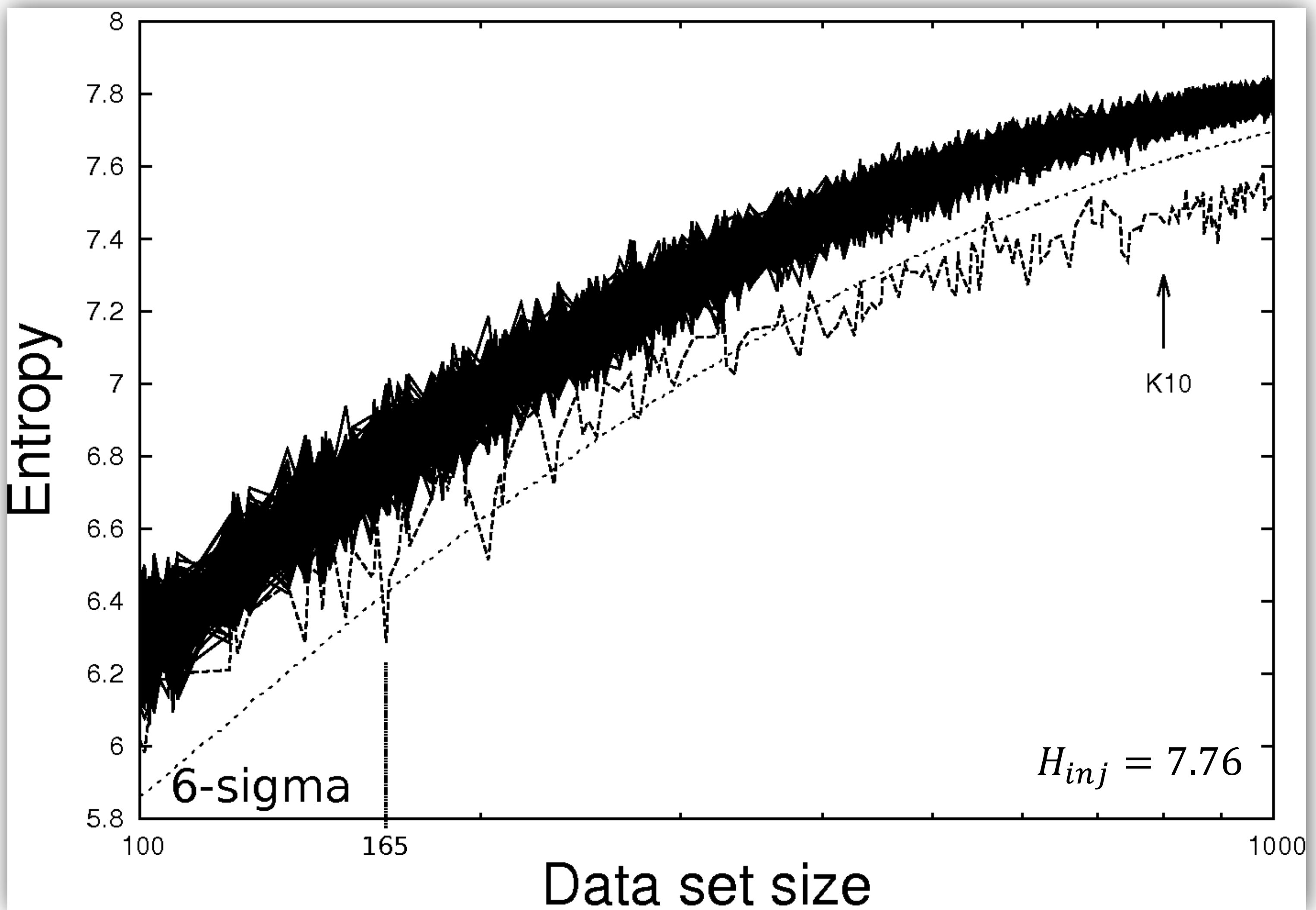
$$K10 = s \Leftrightarrow cf_{i_{max}}\big(H(p_s)\big) > X$$

- We chose with empirical calibration $X = 6$

ENTROPY: DECISION CRITERION EXAMPLE



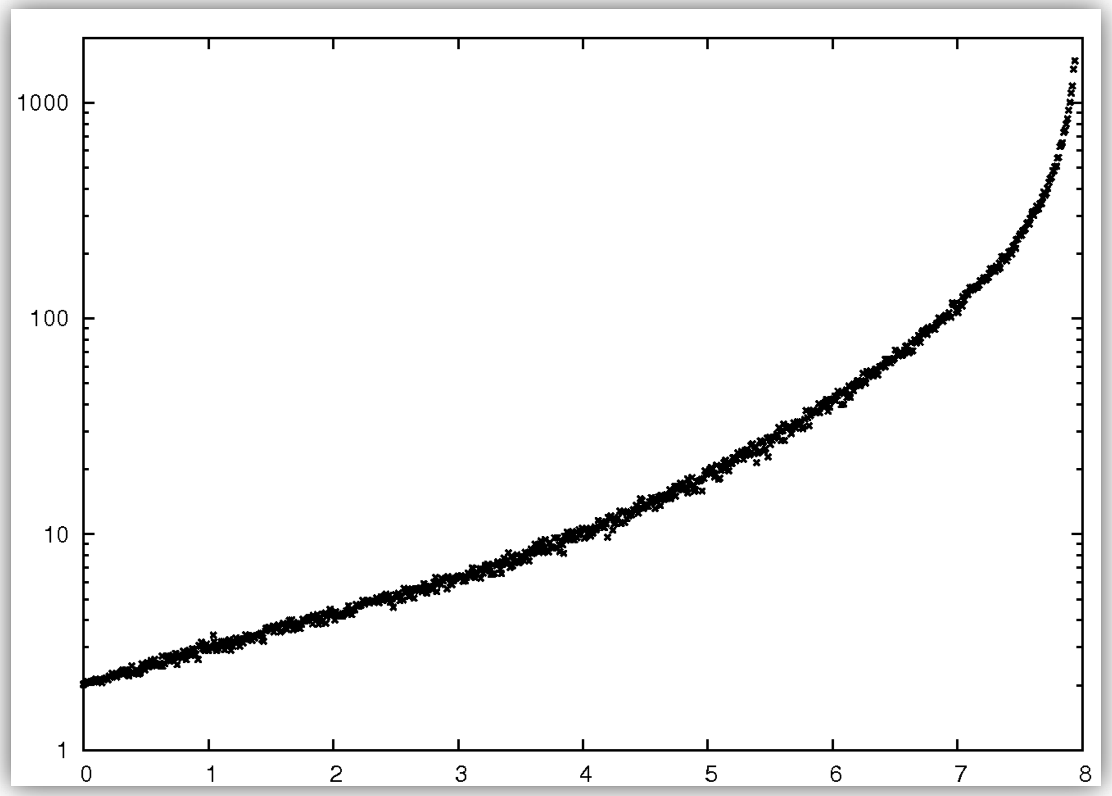
HOW ENTROPIES EVOLVE



ENTROPY: EFFICIENCY

- Using simulation, the entropy of the injection means may be linked with the attack efficiency.
- Attack efficiency is the average minimum number of faults needed to meet the decision criterion.

Average number of faults needed to find the key



Entropy of the injection means

ENTROPY: SUMMARY

- Our DFA is:
  - General: can be used with all injection means.
  - Adaptive: the efficiency increases when the fault model is tighter.
  - Simple to implement.
  - Without prior knowledge of the fault model…
  - ~~Or with prior knowledge and higher efficiency.~~
  - ~~Helped by some countermeasures!~~

- It is not particularly efficient: can we improve it?

	Average best attack
Shannon entropy	6.41
Giraud’s	2.24

Perfect single bit faults (simulation)

SECTION 3
IMPROVING ENTROPY-BASED TOOLS

Considering a known fault model

- We want to improve the efficiency of the attack by including information of a known model.
- Let *t(e)* be the expected distribution, we use the relative entropy:

$$RH(p_s, t) = \sum_{e=0}^{255} p_s(e) \log_2 \left(\frac{p_s(e)}{t(e)} \right)$$

	Average best attack
Shannon entropy	6.41
Relative entropy	2.24
Giraud's	2.24

Perfect single bit faults (simulation)

IMPROVING TOOLS

How to learn the fault model *t(e)*

- Use the Shannon entropy in a first attack.
- Inject faults on M10 and observe the resulting fault model.
- We have previous knowledge of the system, the injection means, the countermeasure…

- **Bertoni's countermeasure = 1 parity bit**
- Thus all odd bit faults are eliminated. This creates non uniformity!

Modeling basic countermeasures

- $d(e)$ is the detection rate for error e.
- $D = \sum_{e=0}^{255} p_{K10}(e)\, d(e)$ is the global detection rate.

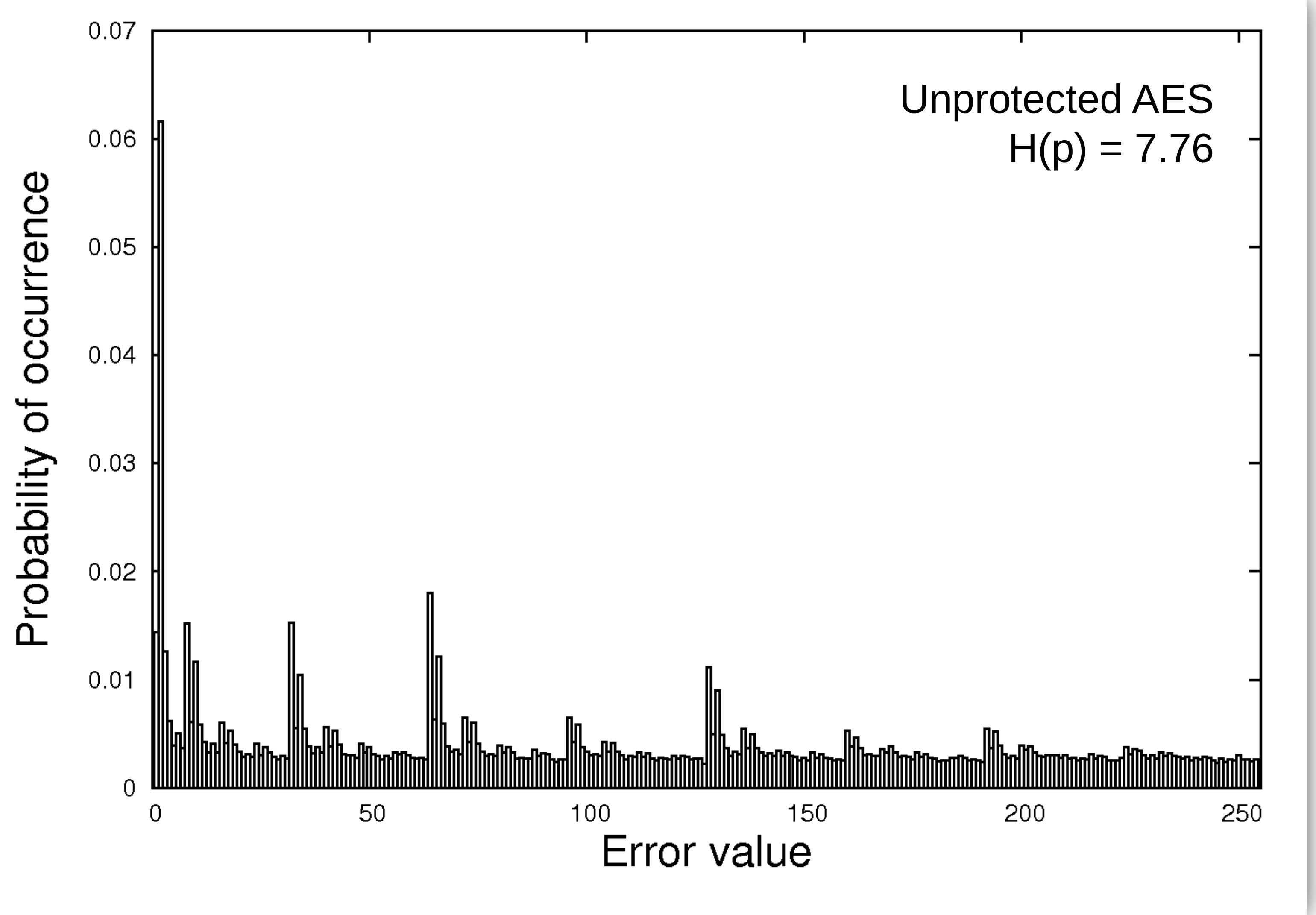
- Two cases:
  - Virtual model with result discrimination: the attacker knows for which realizations the countermeasure was activated. The new "virtual" distribution is:

$$v(e) = \frac{p_{K10}(e)\big(1 - d(e)\big)}{1 - D}$$

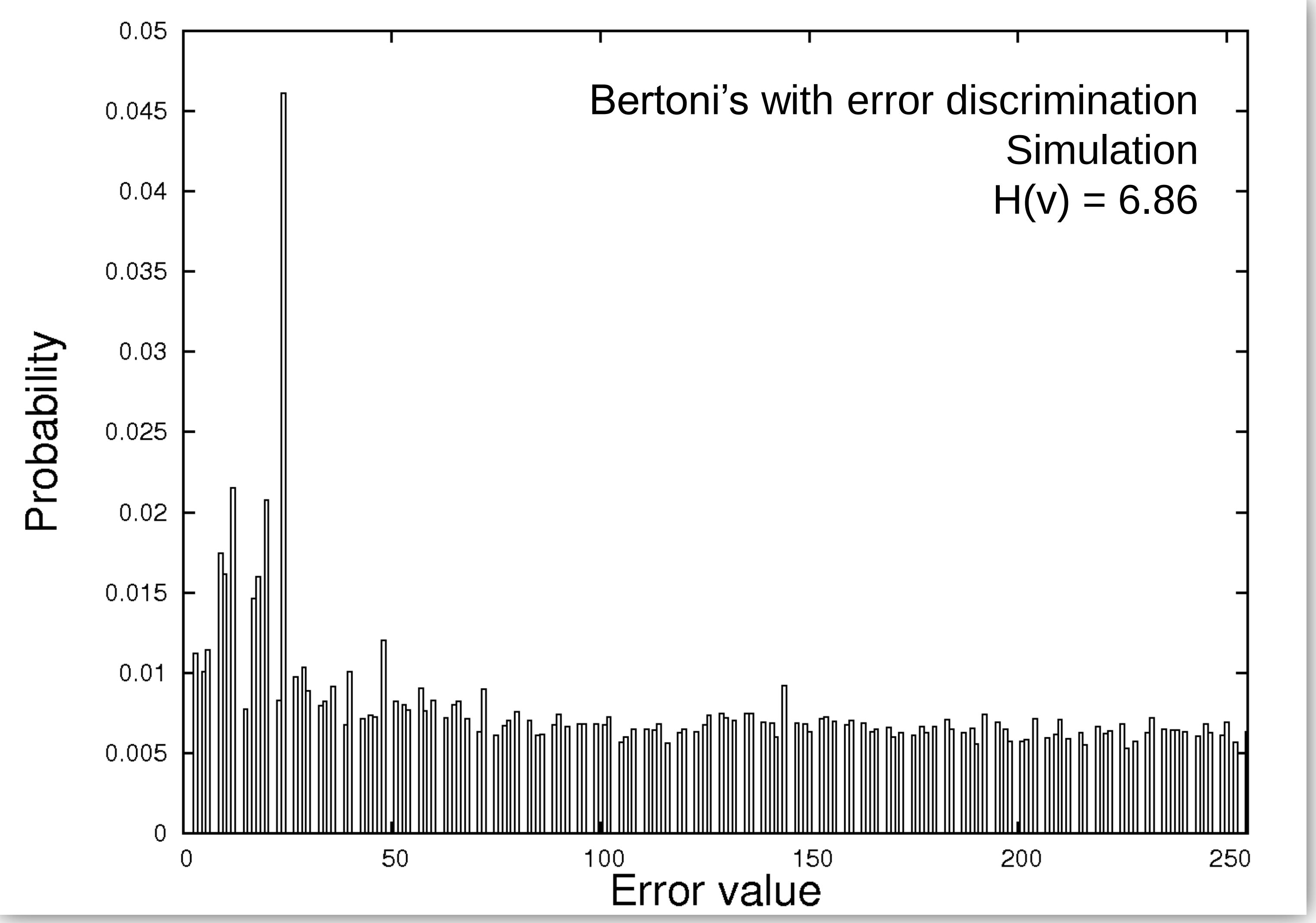
  - Virtual model without result discrimination: the attacker does not know for which realizations the countermeasure was activated. The new "virtual" distribution is:

$$w(e) = \frac{1}{256}D + p_{K10}(e)\big(1 - d(e)\big) = \frac{1}{256}D + (1 - D)v(e)$$

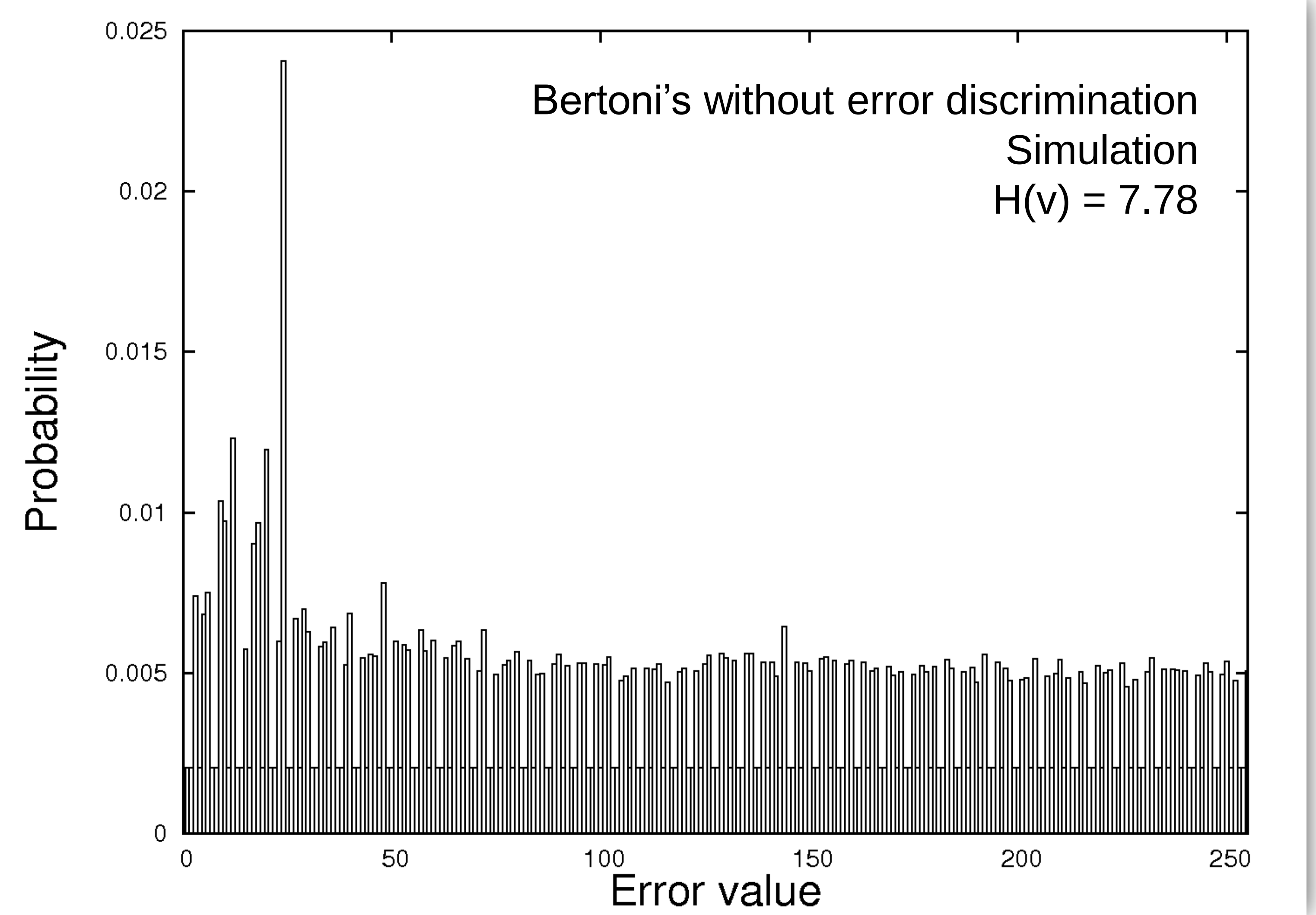
IMPROVING TOOLS: UNPROTECTED AES



IMPROVING TOOLS: BERTONI'S COUNTERMEASURE



IMPROVING TOOLS : BERTONI'S COUNTERMEASURE



Conclusion

- Our DFA is:
  - General: can be used with all injection means.
  - Adaptive: the efficiency increases when the fault model is tighter.
  - Simple to implement.
  - Without prior knowledge of the fault model…
  - Or with prior knowledge and higher efficiency.
  - Helped by some countermeasures!

- We loosened the constraints on the injection means.
- We can find the key and the fault model in parallel.
- All faults contribute to find the key. The analysis is done by taking into account all faults as a whole.

- Countermeasures must create non uniformity.

CONCLUSION

Perspectives

- Verify that all injection means have non uniform distribution for injected faults.
- Represent the fault model with something different than a distribution.
- Test this methodology on other algorithms. It should work if we can compute the injected faults with the secret as a parameter.
- Cartography for localized injection means should include a fault entropy evaluation.

Thank you for your attention.

Any questions?

Cézanne

Commissariat à l'énergie atomique et aux énergies alternatives
Centre Microélectronique de Provence | 13541 GARDANNE
T. +33 (0)4 42 61 66 00
Etablissement public à caractère industriel et commercial | RCS Paris B 775 685 019

Direction de la Recherche Technologique
Département Systèmes et Intégration Systèmes
Service Technologie des Communications et de la Sécurité