Efficient Entropy Estimation for Mutual Information Analysis using B-splines

Alexandre VENELLI

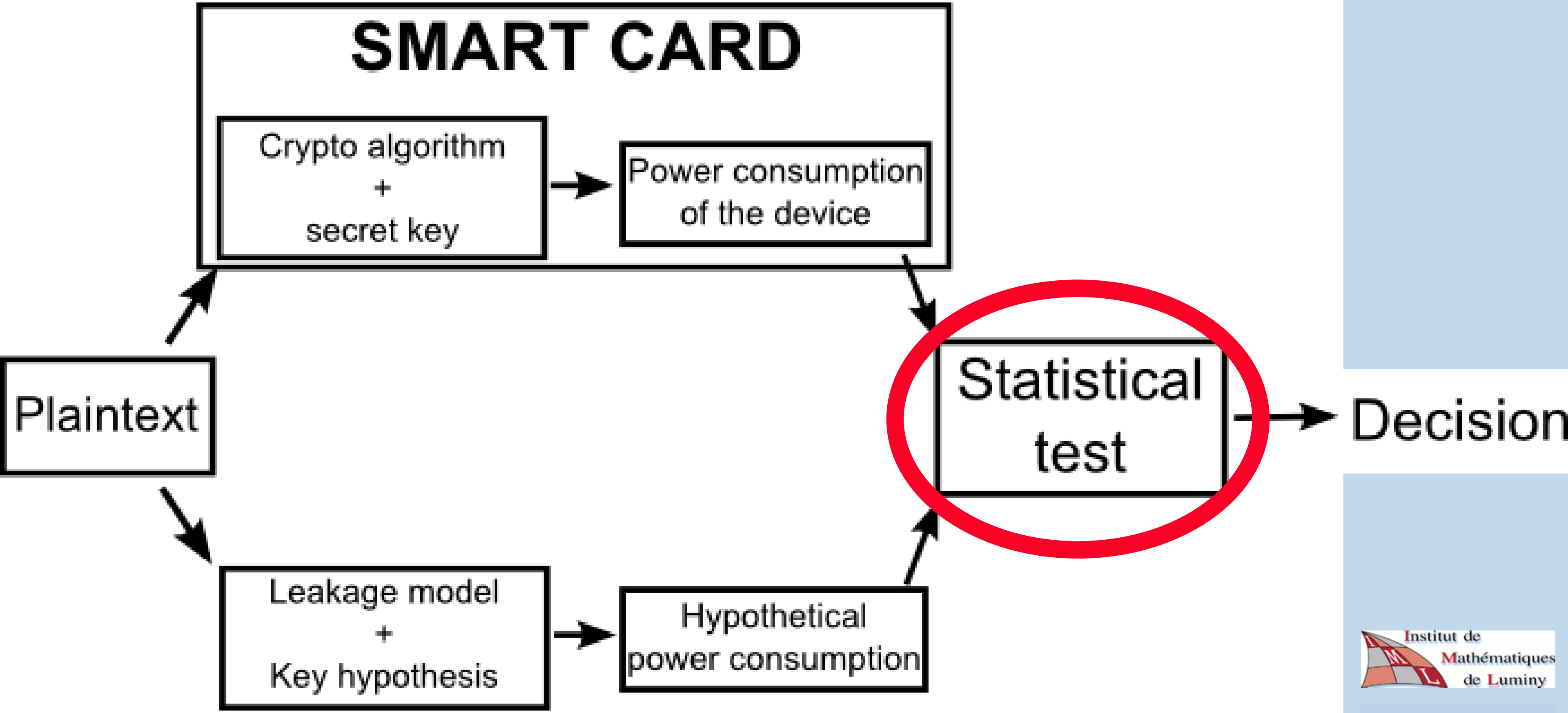
ATMEL
Secure Microcontroller Solutions
Rousset, FRANCE

IML – ERISCS
Université de la Méditerranée
Marseille, FRANCE

Outline

- Differential side-channel attacks – Power analysis
- Mutual Information Analysis
- Proposed B-splines estimation technique
- Experimental results
- Conclusion

Differential side-channel attack workflow



SMART CARD

Crypto algorithm + secret key

Power consumption of the device

Plaintext

Statistical test

Decision

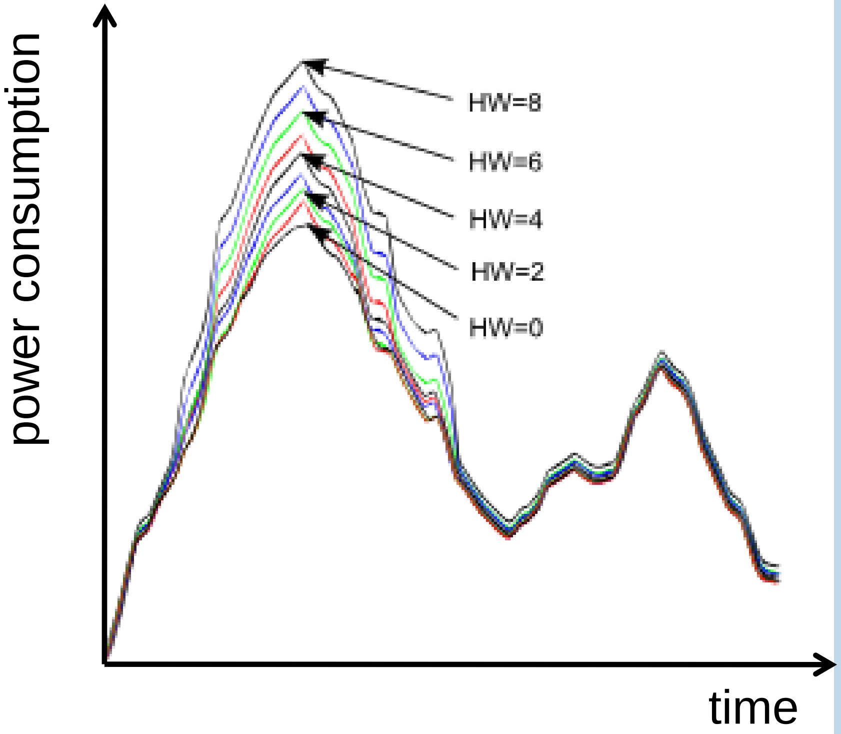
Leakage model + Key hypothesis

Hypothetical power consumption

Power analysis and leakage model

- Messerges et al. 1999
  - Linear relation between power consumption and Hamming Weight of a processed data.

$$\boxed{P(t) = a.H(M) + b}$$



Some statistical tests used in practice (1)

- Kocher et al. 1999
  - Simplified T-Test (distance of means)
- Brier et al. 2004
  - Pearson correlation factor,
  - Correlation Power Analysis (CPA)

Some statistical tests used in practice (2)

- Gierlichs et al. 2008
  - Mutual Information Analysis (MIA) + histograms
- Veyrat-Charvillon et al. 2009
  - Cramér-von Mises test (nonparametric)
- This presentation
  - MIA + B-splines estimation (nonparametric)

Remainder on information theory

- Let X be a random variable with M_X possible states X_i with $i = \{1 \ldots M_X\}$.
- Entropy of X:

$$\boxed{H(X) = \sum_{i=1}^{M_X} p(X_i) \log(p(X_i))}$$

- Mutual information:
  - $$\boxed{I(X;Y) = H(X) - H(X|Y)}$$
  - $$\boxed{I(X;Y) = H(X) + H(Y) - H(X,Y)}$$

Problem : estimating mutual information

- Mutual Information:
  - very powerful,
  - yet difficult to estimate.

- Using the definition of entropy, the density has to be estimated.

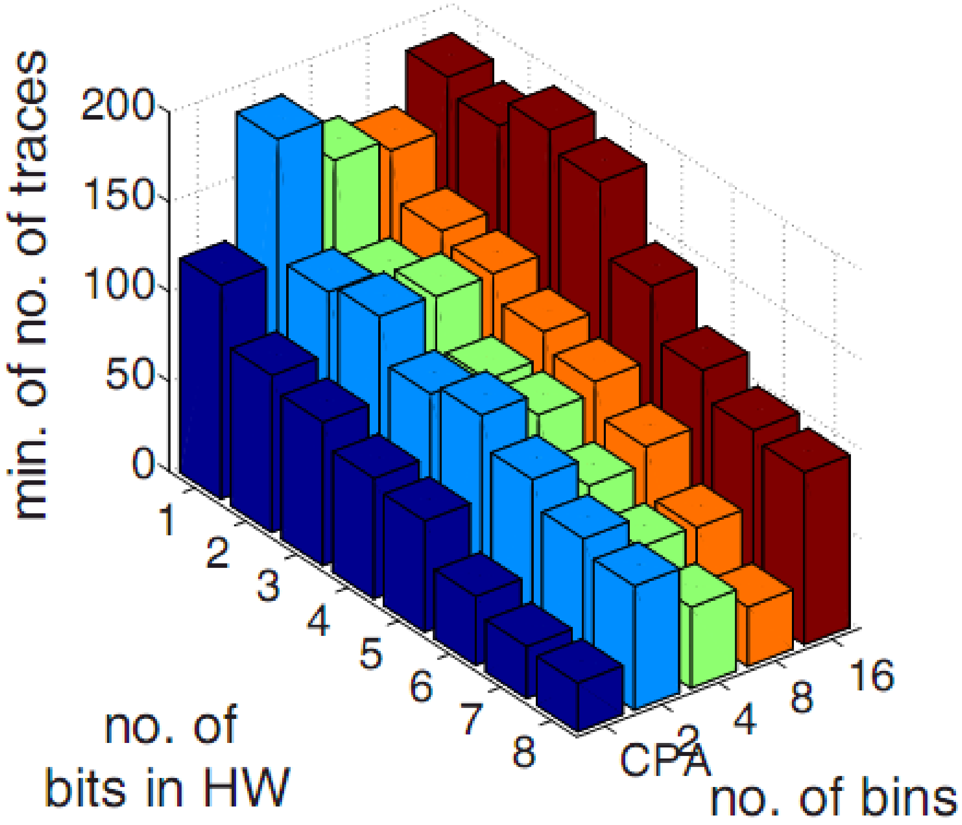
- Goal: estimate a density given a finite number of data points drawn from that density function.

- Different approaches:
  - histograms, kernel density estimation, …

Histogram based estimation

⊕	⊖
- Easy to calculate and understand.	- Systematic errors due to the finite size of the dataset.

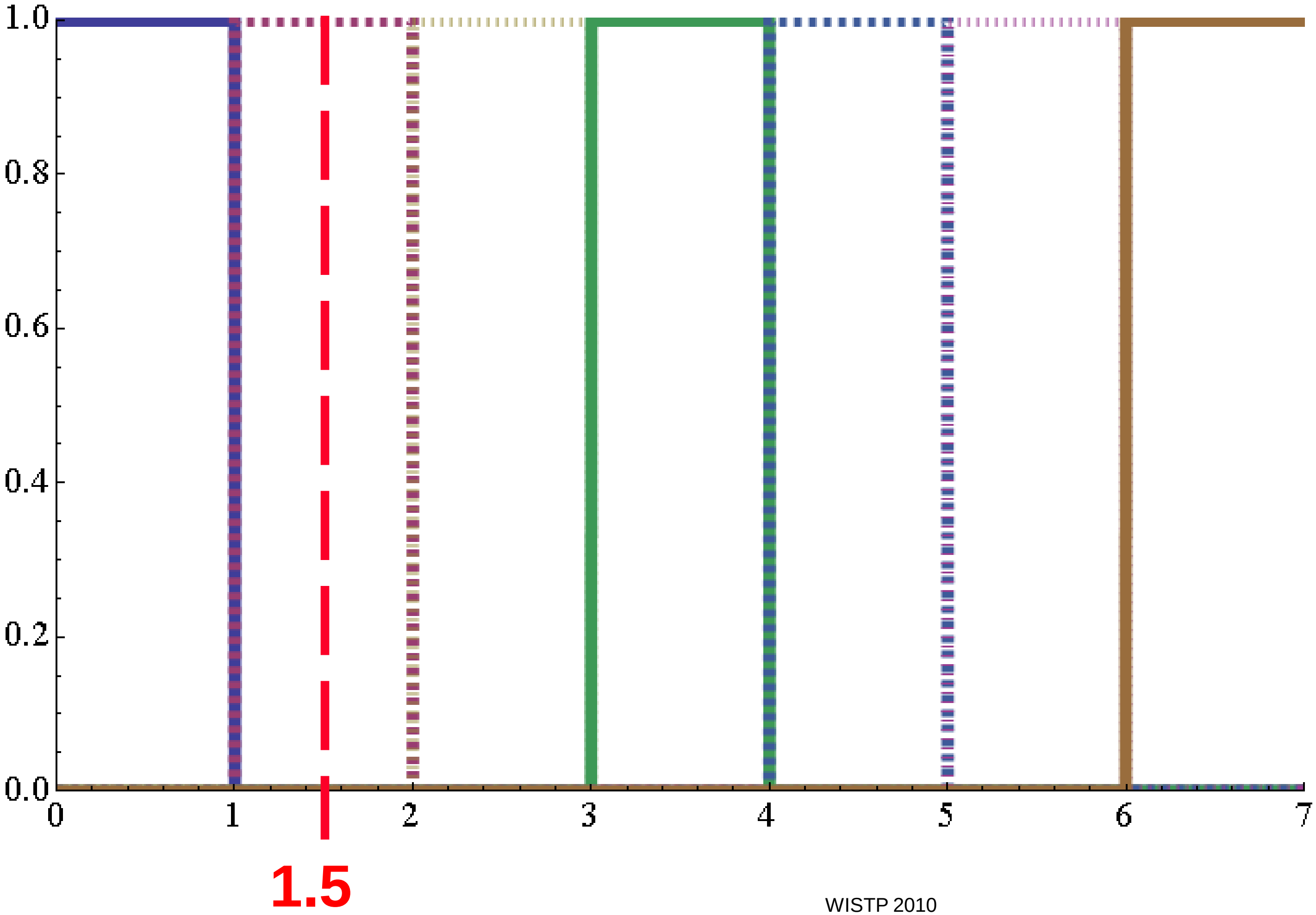
MIA vs CPA



- **<u>Figure taken from :</u>**
  Moradi A, Mousavi N, Paar C, Salmasizadeh M.
  A Comparative Study of Mutual Information Analysis under a Gaussian Assumption. **Information Security Applications. 2009:193–205.**

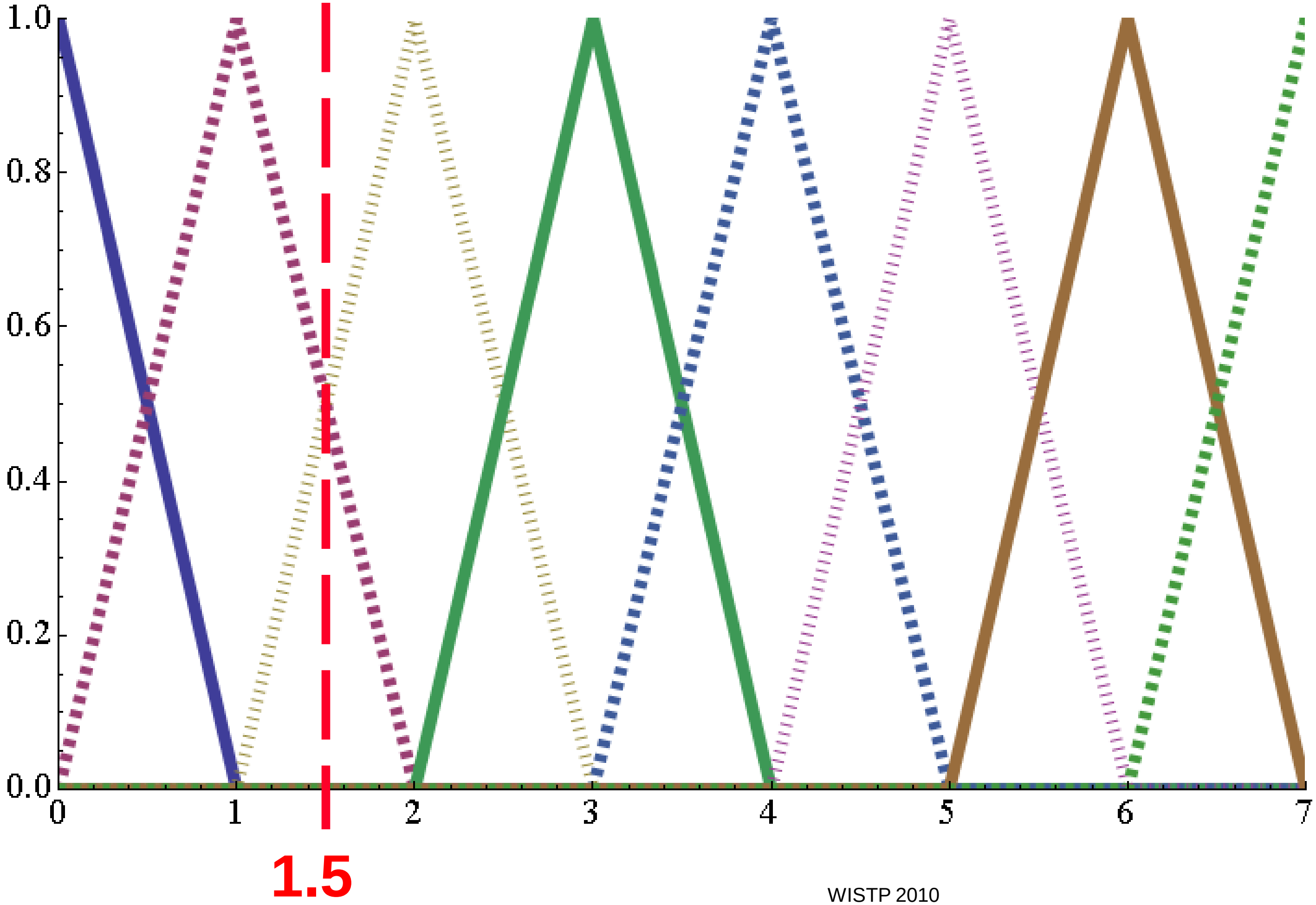
What are B-spline functions ? (1)

Degree-0 basis functions



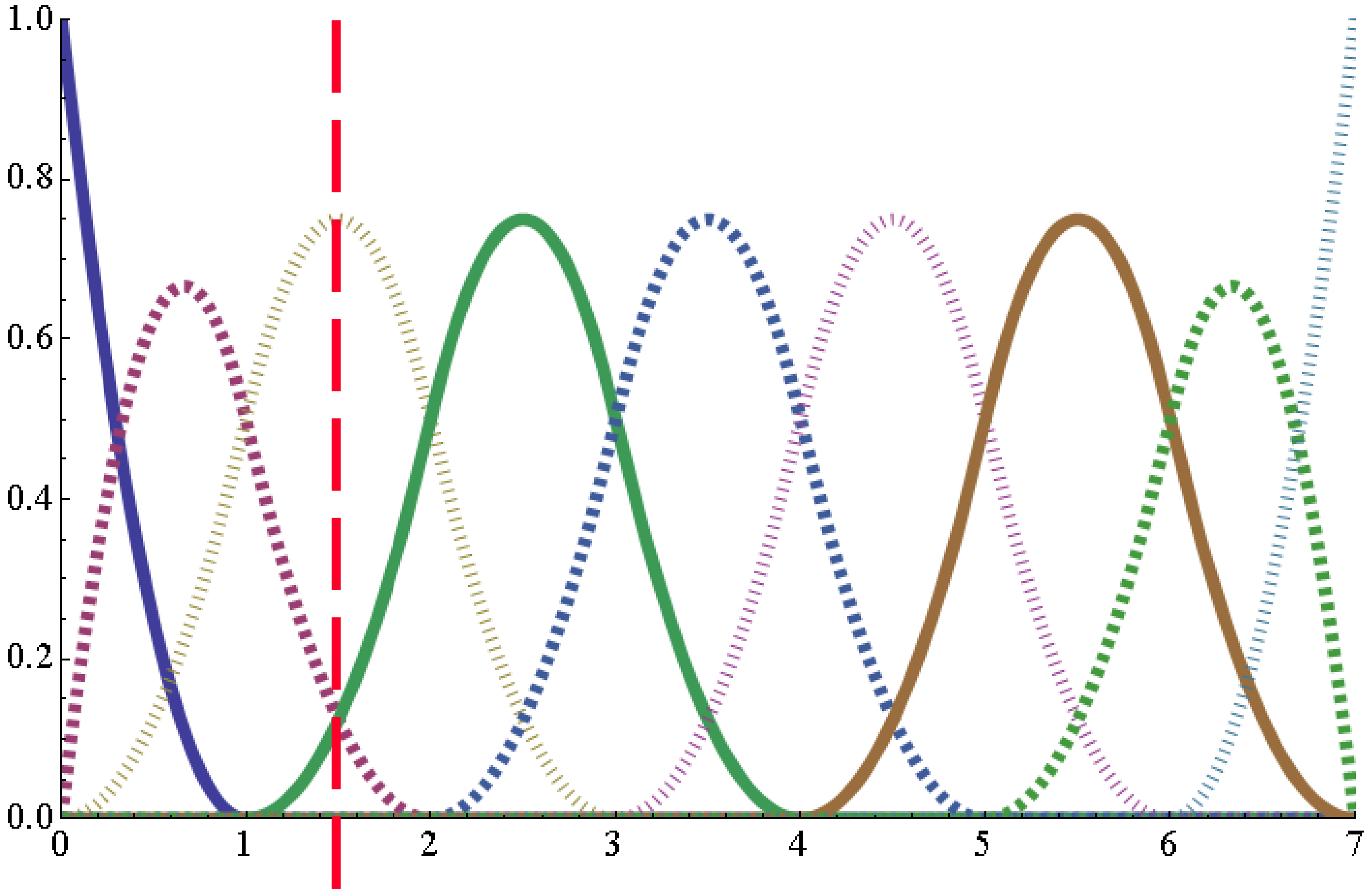
What are B-spline functions ? (2)

Degree-1 basis functions



What are B-spline functions ? (3)

Degree-2 basis functions



1.5

B-splines for MI estimation

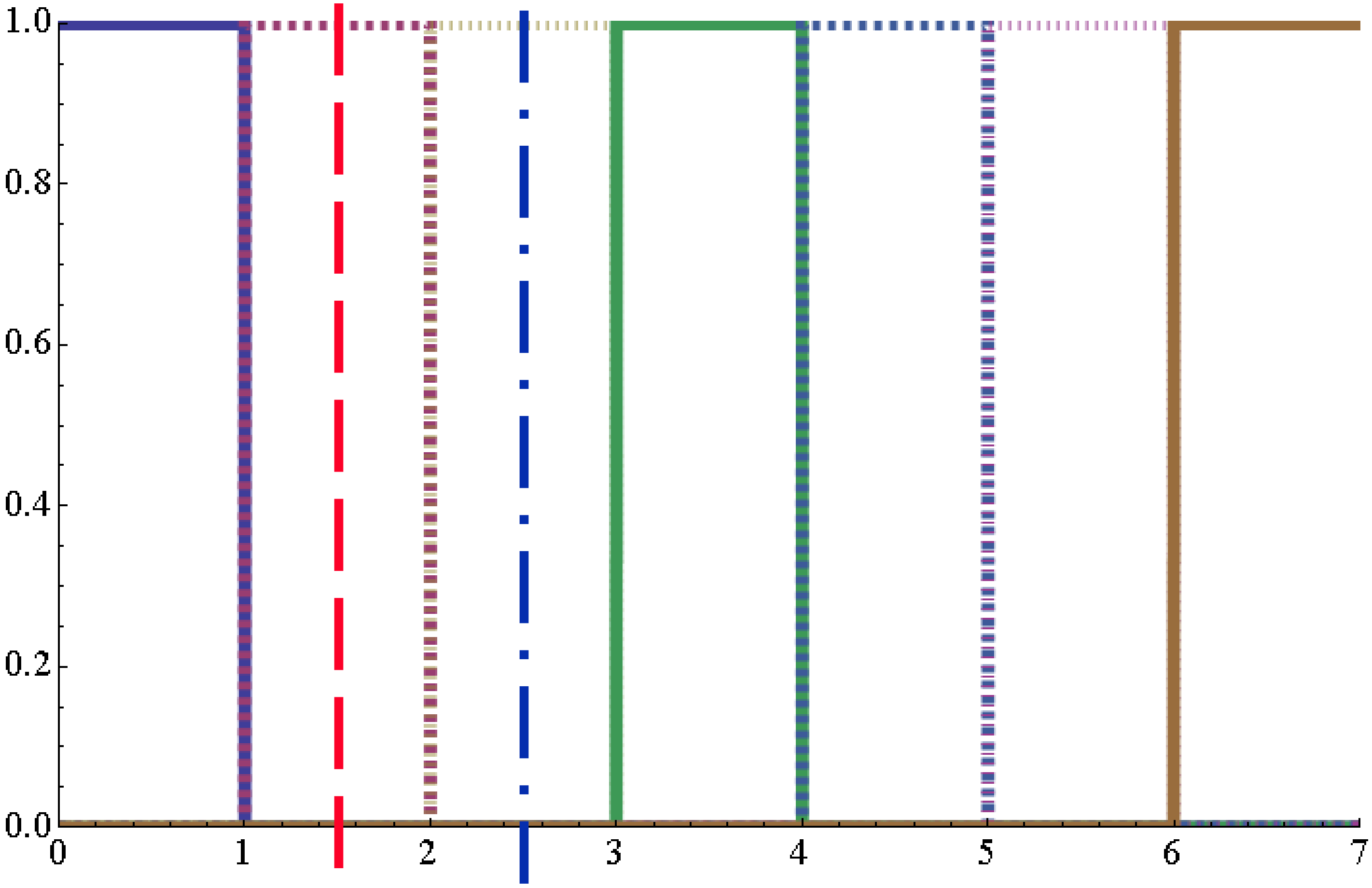
- Idea proposed by Daub et al. 2004 in the context of medical studies.

- Instead of using a step function with histograms, a polynomial B-spline function is used to weight a data point.

- Hence, data points can be in one or several intervals.

MI estimation in the presence of noise

Histograms

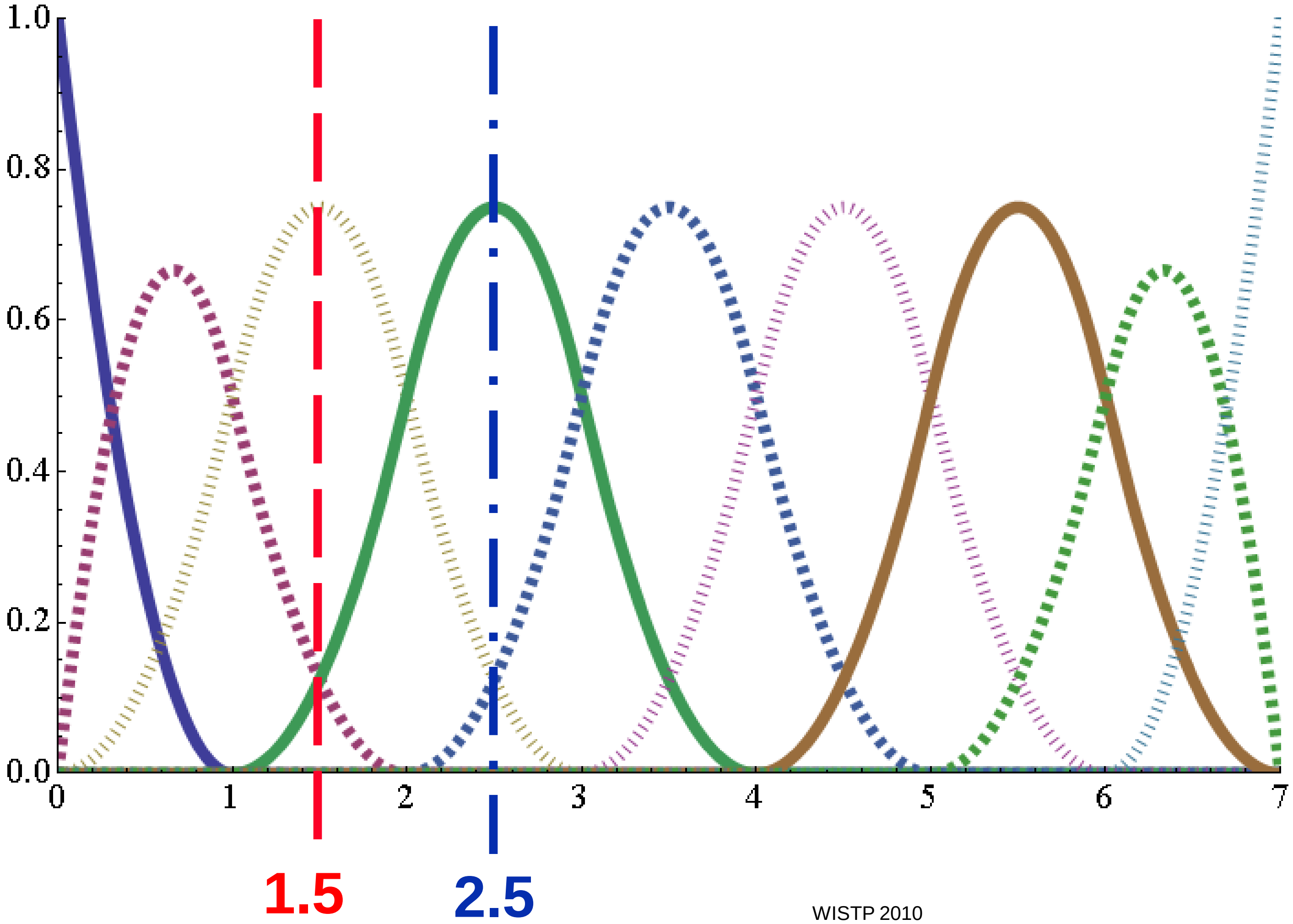


1.5

2.5

MI estimation in the presence of noise

Degree-2 B-spline functions



B-splines for MI estimation

⊕	⊖
- Better efficiency than histograms - Interesting propriety for side-channel	- Slower to compute than histograms

Cramér-von Mises with B-splines

- Cramér-von Mises test in Veyrat-Charvillon et al. 2009.
- Its needs cumulative density functions.
- B-splines can be used to estimate these density functions.

Experimental results

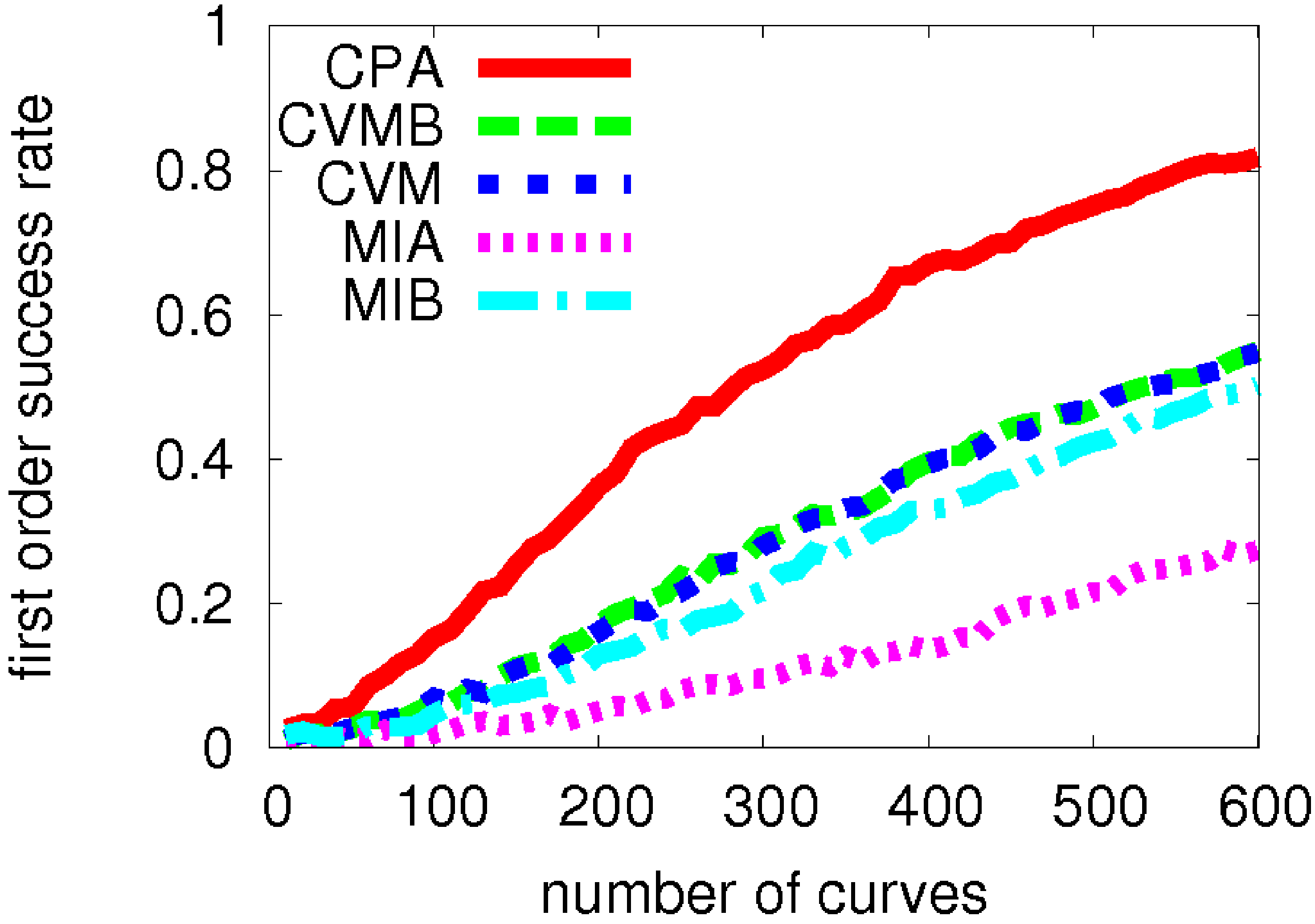
- Metrics to measure the efficiency of side-channel attacks by Standaert et al. 2008:
  - *first order success rate*: given a number of traces, the probability that the correct hypothesis is the first best hypothesis of an attack.
  - *guessed entropy*: average position of the correct hypothesis in the sorted hypothesis vector of an attack

- Attacks efficiency tested with 2 different setups:
  - on « DPA Contest 2008/2009[a] » power curves of a DES,
  - on power curves acquired on a Atmel STK600 board with a ATmega2560 chip of a multiprecision multiplication.

a: HTTP://WWW.DPACONTEST.ORG

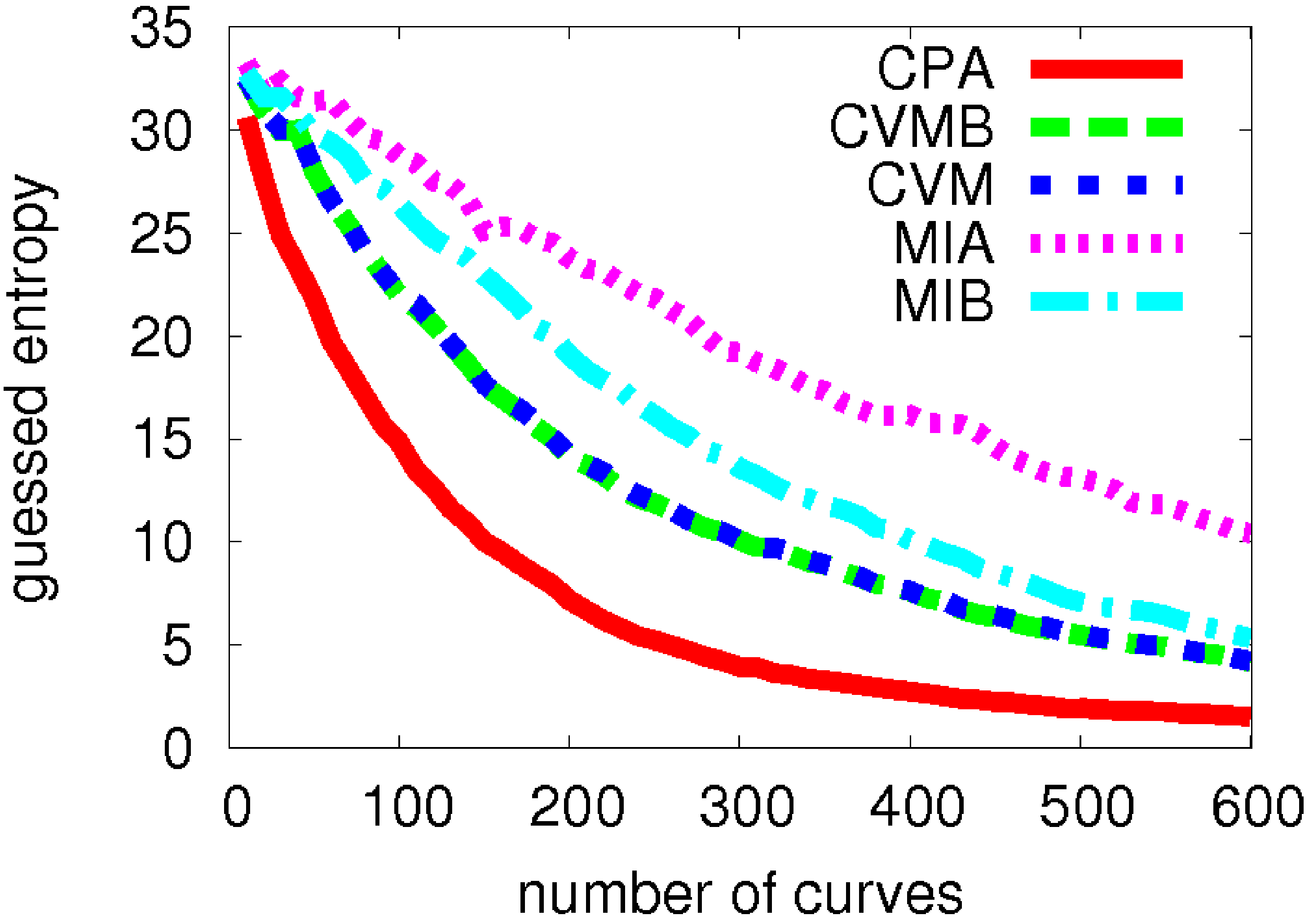
DES – DPA Contest 2008/2009

First order success rate



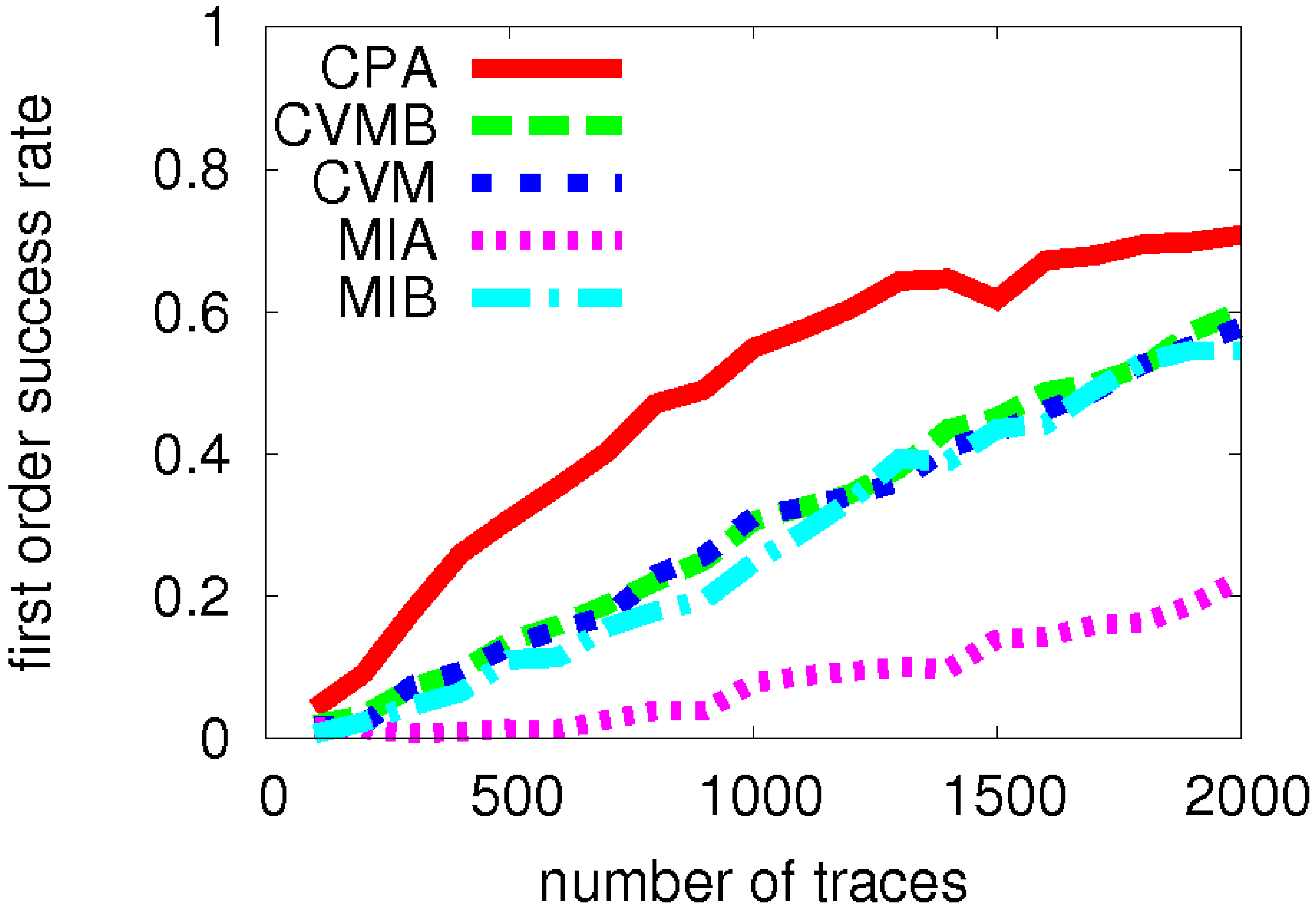
DES – DPA Contest 2008/2009

Guessed Entropy



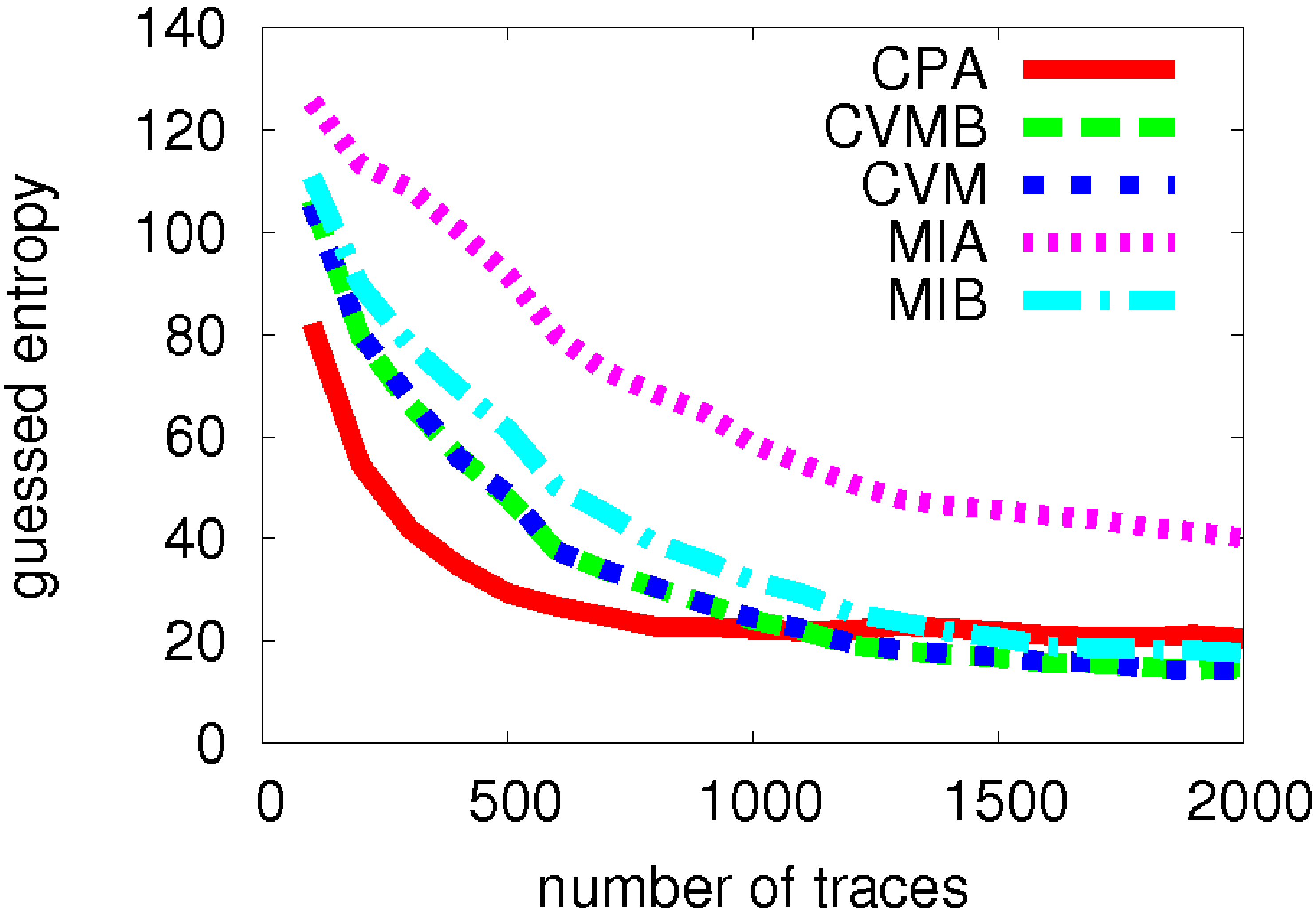
Multiplication – STK600 / Atmega 2560

First order success rate



Multiplication – STK600 / Atmega 2560

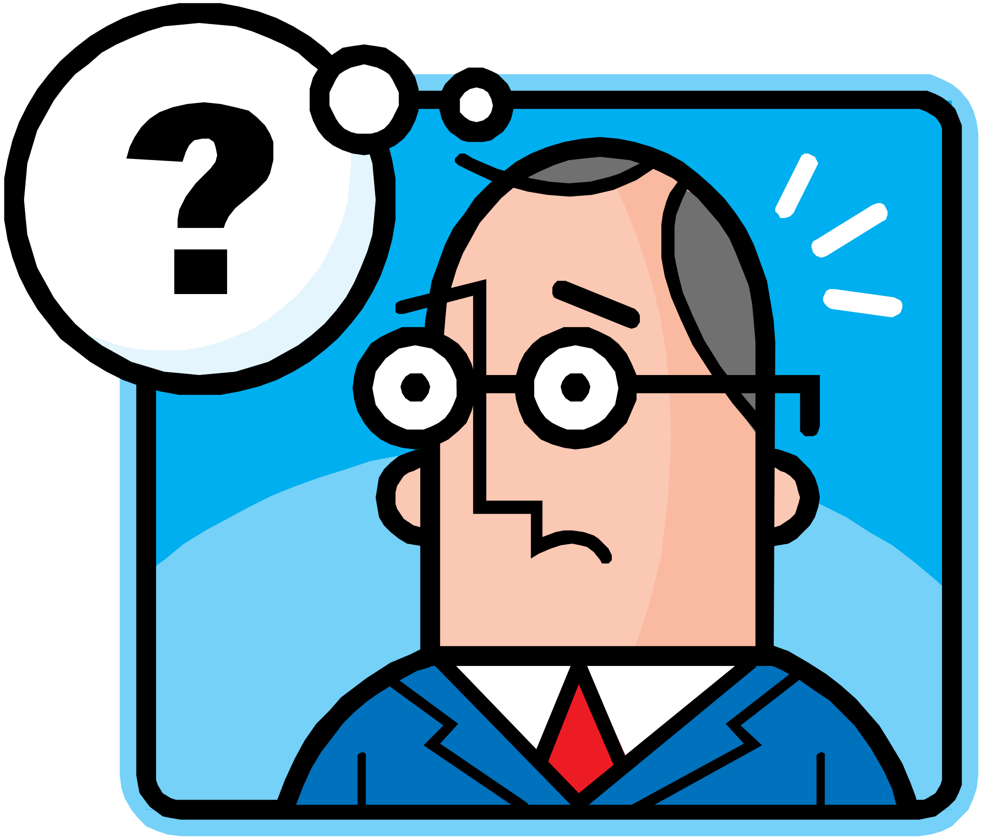
Guessed entropy



Conclusion

- B-splines offer a lot more efficiency than classical histograms for an acceptable computational overhead.
- However MIA still is not as performant as CPA on most platforms.
- A New Hope:
  - Other efficient entropy estimators,
  - Higher order side-channel analysis.

Questions ?



Institut de Mathématiques de Luminy

eRISCS

ATMEL®