On Adaptive Bandwidth Selection for Efficient MIA

M. Carbone, S. Tiran, S. Ordas, M. Agoyan, Y. Teglia, G.R. Ducharme and P. Maurine.

COSADE
14th April, 2014

life.augmented

Institut de Mathématiques et de Modélisation de Montpellier

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier

Outline

- Context
- Kernel Density Estimation (KDE)
- How to set the tuning parameters of Kernel-MIA?
- Experimental results
- Conclusion

Context

Context

- Distinguishers

- Leakage models

Context

- Distinguishers
  - Difference-of-Means (Kocher'99)⇨ DPA
  - Pearson's Correlation (Brier'04) ⇨ CPA
  - Mutual Information (Gierlichs'08 /Aumonier '08) ⇨ MIA
- Leakage models

Context

- Distinguishers
  - Difference-of-Means (Kocher'99)⇰ DPA
  - Pearson's Correlation (Brier'04) ⇰ CPA
  - Mutual Information (Gierlichs'08 /Aumonier '08) ⇰ MIA
- Leakage models
  - Word (Messerges'99)
  - Multi-bit (Bevan'04)
  - Identity (Gierlichs'08)

Context

- Distinguishers
  - Difference-of-Means (Kocher'99)⇨ DPA
  - Pearson's Correlation (Brier'04) ⇨ CPA
  - Mutual Information (Gierlichs'08 /Aumonier '08) ⇨ MIA

- Leakage models
  - Word (Messerges'99)
  - Multi-bit (Bevan'04)
  - Identity (Gierlichs'08)

- Mutual Information Analysis (MIA)

Context

- Distinguishers
  - Difference-of-Means (Kocher'99)⇨ DPA
  - Pearson's Correlation (Brier'04) ⇨ CPA
  - Mutual Information (Gierlichs'08 /Aumonier '08) ⇨ MIA
- Leakage models
  - Word (Messerges'99)
  - Multi-bit (Bevan'04)
  - Identity (Gierlichs'08)

- Mutual Information Analysis (MIA)
  - o_t : side-channel observation.
  - $L(.,k)$: selection function of a sensitive intermediate variable according to each key hypothesis.
  - $MI_k(t) = H(o_t(.)) - H(o_t(.)|L(.,k))$.

Context

- Distinguishers
  - Difference-of-Means (Kocher’99)⇨ DPA
  - Pearson’s Correlation (Brier‘04) ⇨ CPA
  - Mutual Information (Gierlichs’08 /Aumonier ‘08) ⇨ MIA

- Leakage models
  - Word (Messerges’99)
  - Multi-bit (Bevan’04)
  - Identity (Gierlichs’08)

- Mutual Information Analysis (MIA)
  - o_t : side-channel observation.
  - $L(.,k)$: selection function of a sensitive intermediate variable according to each key hypothesis.
  - $MI_k(t) = H(o_t(.)) - H(o_t(.)|L(.,k))$.

- PDF-based approaches
  - Parametric
    - Cumulant (Le’10)
    - Copula (Veyrat-Charvillon’11)

Context

- Distinguishers
  - Difference-of-Means (Kocher'99) ⇨ DPA
  - Pearson's Correlation (Brier'04) ⇨ CPA
  - Mutual Information (Gierlichs'08 /Aumonier '08) ⇨ MIA
- Leakage models
  - Word (Messerges'99)
  - Multi-bit (Bevan'04)
  - Identity (Gierlichs'08)

- Mutual Information Analysis (MIA)
  - o_t : side-channel observation.
  - $L(.,k)$: selection function of a sensitive intermediate variable according to each key hypothesis.
  - $MI_k(t) = H(o_t(.)) - H(o_t(.)|L(.,k))$.

- PDF-based approaches
  - Parametric
    - Cumulant (Le'10)
    - Copula (Veyrat-Charvillon'11)
  - NonParametric
    - Histogram (Gierlichs'08)
    - Bspline (Venelli'10)
    - Kernel (Prouff'10 / Standaert'10).
    - Maximal Information Coefficient (Linge'13)

Context

- Distinguishers
  - Difference-of-Means (Kocher'99) ⇨ DPA
  - Pearson's Correlation (Brier'04) ⇨ CPA
  - Mutual Information (Gierlichs'08 /Aumonier '08) ⇨ MIA
- Leakage models
  - Word (Messerges'99)
  - Multi-bit (Bevan'04)
  - Identity (Gierlichs'08)

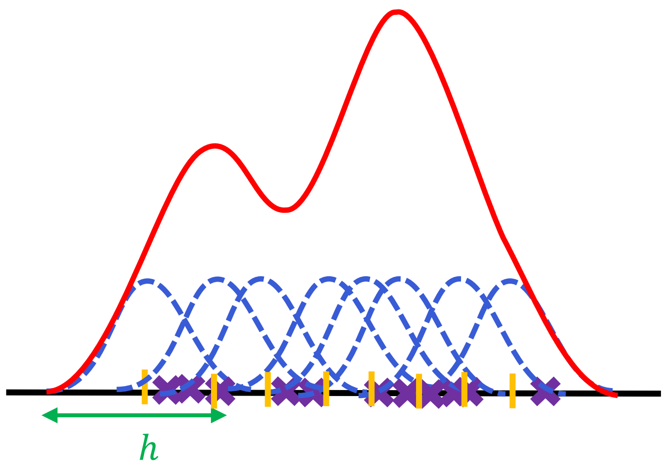
- Mutual Information Analysis (MIA)
  - o_t : side-channel observation.
  - $L(.,k)$: selection function of a sensitive intermediate variable according to each key hypothesis.
  - $MI_k(t) = H(o_t(.)) - H(o_t(.)|L(.,k))$.

- PDF-based approaches
  - Parametric
    - Cumulant (Le'10)
    - Copula (Veyrat-Charvillon'11)
  - NonParametric
    - Histogram (Gierlichs'08)
    - Bspline (Venelli'10)
    - Kernel (Prouff'10 / Standaert'10).
    - Maximal Information Coefficient (Linge'13)

Kernel density estimation (KDE) overview

- Classical form of KDE

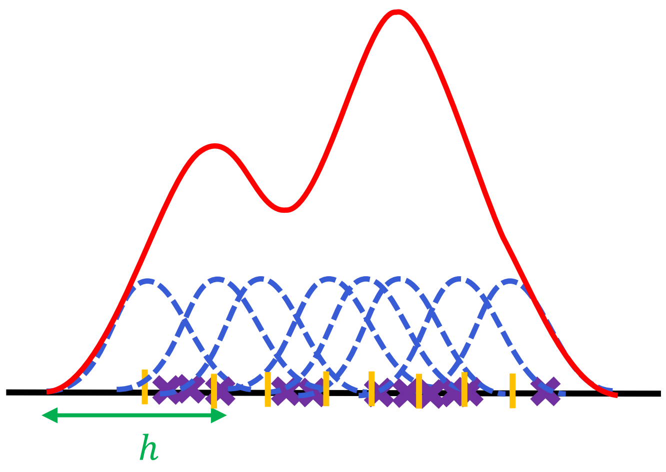
$$\hat{f}(q_b) = \frac{1}{Nh}\sum_{n=1}^{N} K\left(\frac{q_b - Y_n}{h}\right), \; 1 \leq b \leq B$$



Kernel density estimation (KDE) overview

- Classical form of KDE

$$\hat{f}(q_b) = \frac{1}{Nh}\sum_{n=1}^{N} K\left(\frac{q_b - Y_n}{h}\right),\ 1 \le b \le B$$

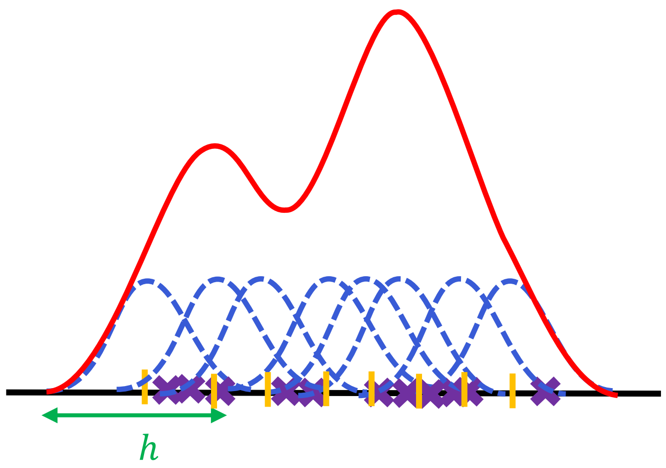


- Tuning parameters
  - Kernel functions (K)
    - Non-negative real-valued integrable functions.
    - Sophisticated weighting functions.

Kernel density estimation (KDE) overview

- Classical form of KDE

$$\hat{f}(q_b) = \frac{1}{Nh}\sum_{n=1}^{N} K\left(\frac{q_b - Y_n}{h}\right), \quad 1 \le b \le B$$

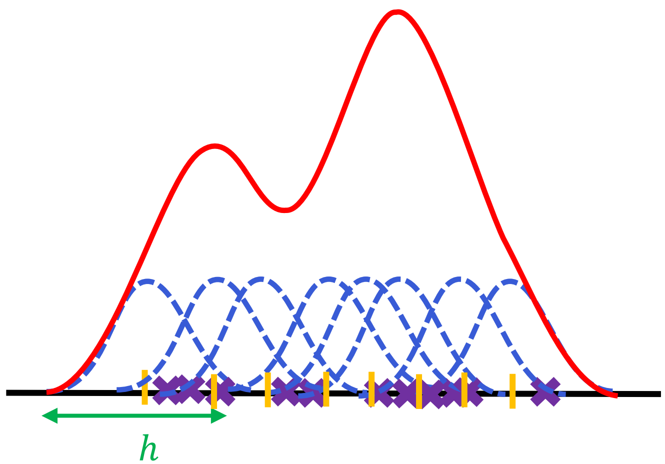


- Tuning parameters
  - Kernel functions (K)
    - Non-negative real-valued integrable functions.
    - Sophisticated weighting functions.
  - Query points (q_b)
    - Mesh grid covering all the observations.
    - Binning approach (iterative version of KDE).
    - Accuracy of PDF estimates/approximation of integrals for entropies (rectangular method).

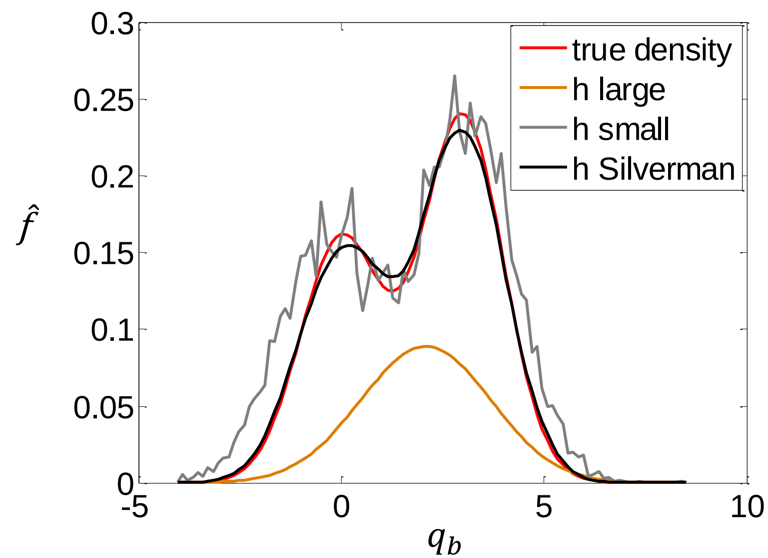
Kernel density estimation (KDE) overview

- Classical form of KDE

$$\hat{f}(q_b) = \frac{1}{Nh}\sum_{n=1}^{N} K\left(\frac{q_b - Y_n}{h}\right),\ 1 \le b \le B$$

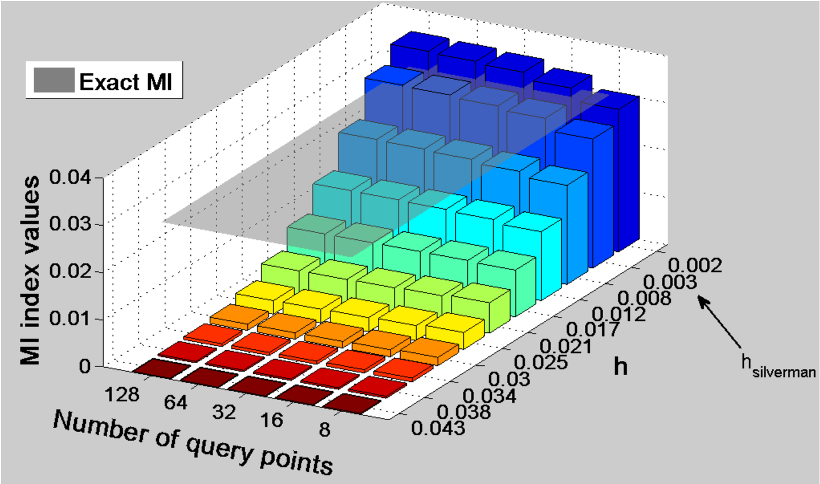


- Tuning parameters
  - Kernel functions (K)
    - Non-negative real-valued integrable functions.
    - Sophisticated weighting functions.
  - Query points (q_b)
    - Mesh grid covering all the observations.
    - Binning approach (iterative version of KDE).
    - Accuracy of PDF estimates/approximation of integrals for entropies (rectangular method).
  - Bandwidth (h)
    - Trade-off bias /variance ⇨ big impact in KDE.
    - Silverman's rule commonly used

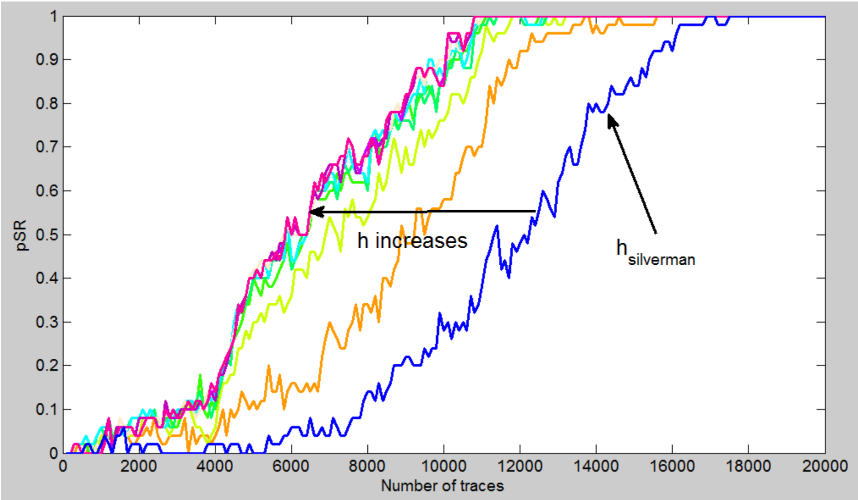


Tuning parameters of Kernel-MIA

- Simulation of 10000 pairs (HW,L) drawn under non-linear leakage

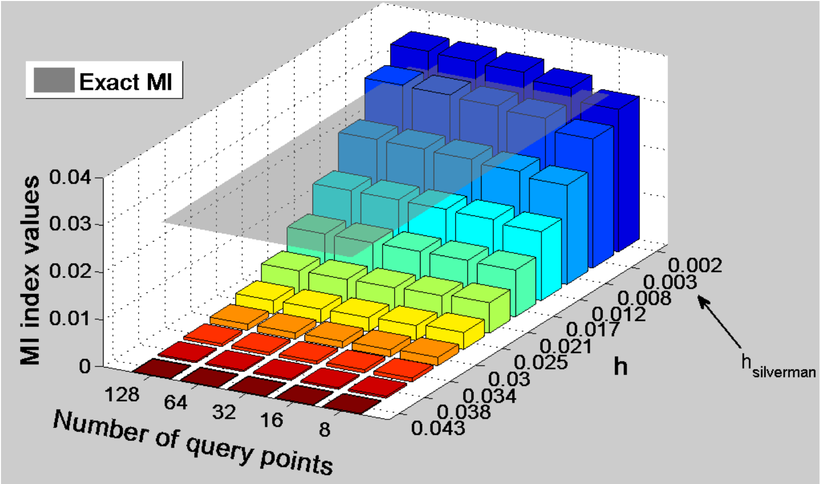


- Partial Success Rate on 1^{st} Sbox at the last round using HD function at the word level (DPA Contest v2).

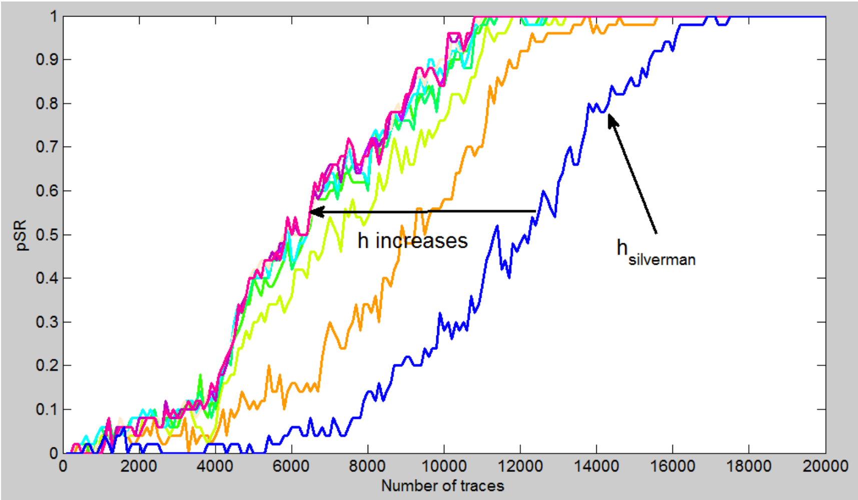


Tuning parameters of Kernel-MIA

- Simulation of 10000 pairs (HW,L) drawn under non-linear leakage



- Partial Success Rate on 1^{st} Sbox at the last round using HD function at the word level (DPA Contest v2).



Accurate PDF estimation $\neq$ Efficient MIA !

- ABS criterion : $\frac{\widehat{MI_k(h)} - \overline{\widehat{MI_{-k}(h)}}}{\overline{\widehat{MI_{-k}(h)}}}$

where $\overline{\widehat{MI_{-k}(h)}}$ the mean of all estimators except $\widehat{MI_k(h)}$.

- ABS criterion : $\frac{\widehat{MI_k}(h) - \overline{\widehat{MI_{-k}}(h)}}{\overline{\widehat{MI_{-k}}(h)}}$
  where $\overline{\widehat{MI_{-k}}(h)}$ the mean of all estimators except $\widehat{MI_k}(h)$.

- $h_S = 2{,}34\ \hat{\sigma} N^{-\frac{1}{5}}$
  where $\hat{\sigma}$ the standard deviation.

- $h_{ABS} = max_{h \in \mathcal{J}} \left[\frac{\widehat{MI_k}(h) - \overline{\widehat{MI_{-k}}(h)}}{\overline{\widehat{MI_{-k}}(h)}} \right]$
  where $\mathcal{J} = \{h_i\}_{1 \leq i \leq H}$

ABS criterion

- ABS criterion : $\frac{\widehat{MI_k(h)} - \overline{\widehat{MI_{-k}(h)}}}{\overline{\widehat{MI_{-k}(h)}}}$

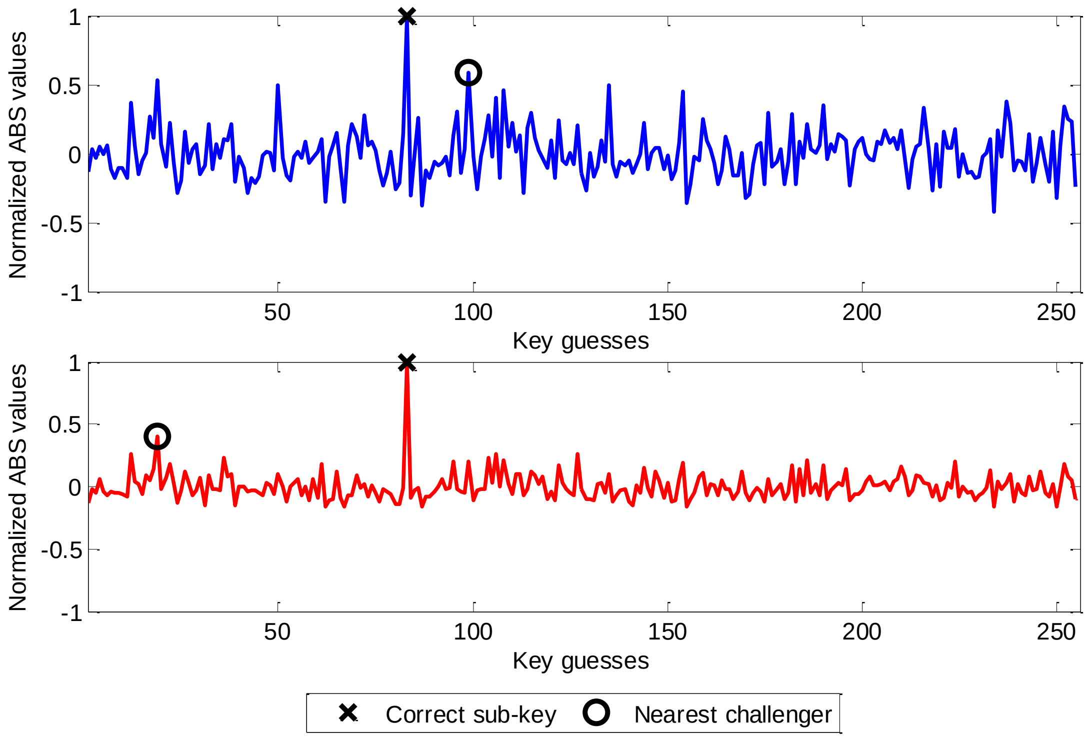
  where $\overline{\widehat{MI_{-k}(h)}}$ the mean of all estimators except $\widehat{MI_k(h)}$.

- $h_S = 2{,}34\ \hat{\sigma} N^{-\frac{1}{5}}$

  where $\hat{\sigma}$ the standard deviation.

- $h_{ABS} = max_{h \in \mathcal{J}} \left[\frac{\widehat{MI_k(h)} - \overline{\widehat{MI_{-k}(h)}}}{\overline{\widehat{MI_{-k}(h)}}} \right]$

  where $\mathcal{J} = \{h_i\}_{1 \le i \le H}$



1^{st} Sbox at the last round using HD function at the word level (DPA Contest v2) after the processing of all the traces

ABS criterion

- ABS criterion : $\frac{\widehat{MI_k(h)} - \overline{\widehat{MI_{-k}(h)}}}{\overline{\widehat{MI_{-k}(h)}}}$

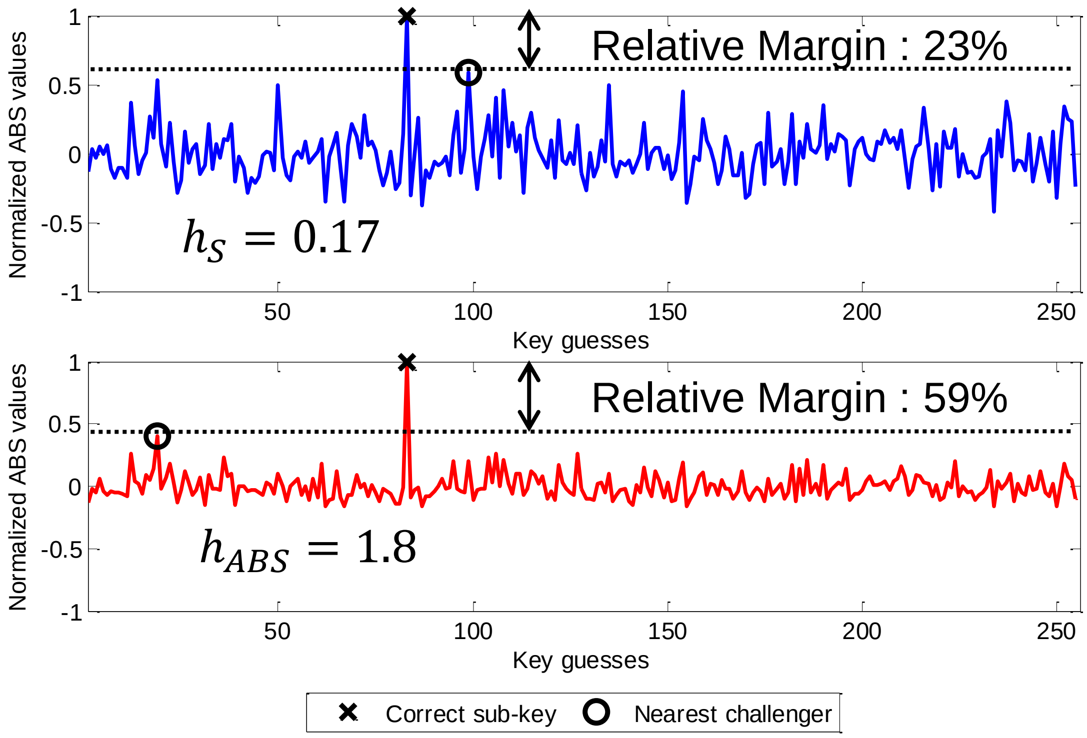
  where $\overline{\widehat{MI_{-k}(h)}}$ the mean of all estimators except $\widehat{MI_k(h)}$.

- $h_S = 2{,}34\ \hat{\sigma} N^{-\frac{1}{5}}$

  where $\hat{\sigma}$ the standard deviation.

- $h_{ABS} = max_{h \in \mathcal{J}} \left[\frac{\widehat{MI_k(h)} - \overline{\widehat{MI_{-k}(h)}}}{\overline{\widehat{MI_{-k}(h)}}} \right]$

  where $\mathcal{J} = \{h_i\}_{1 \leq i \leq H}$



1^{st} Sbox at the last round using HD function at the word level (DPA Contest v2) after the processing of all the traces

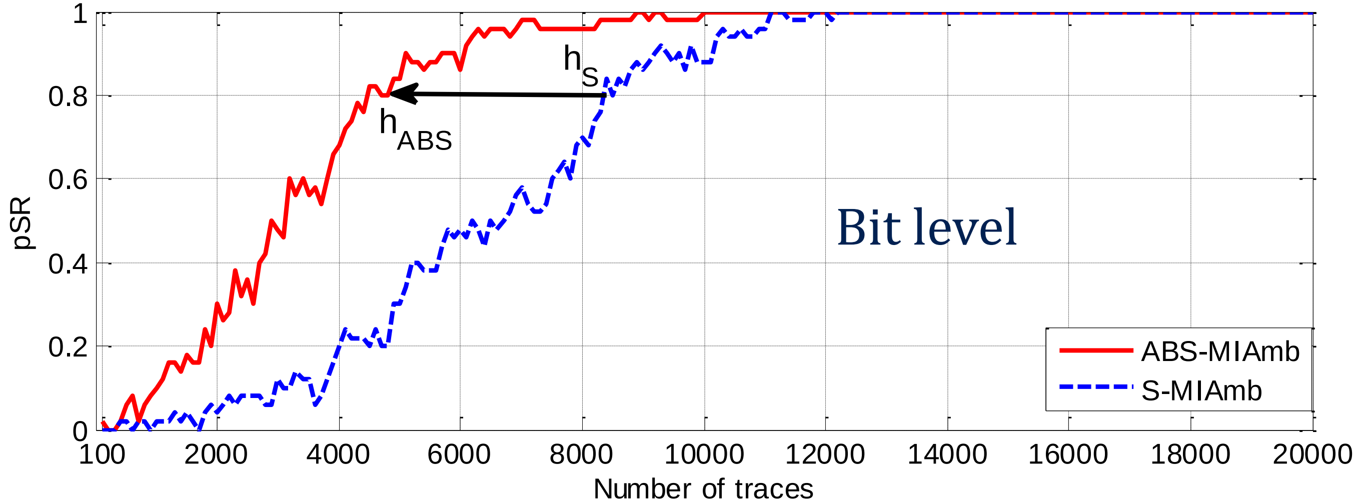
Experimental Results

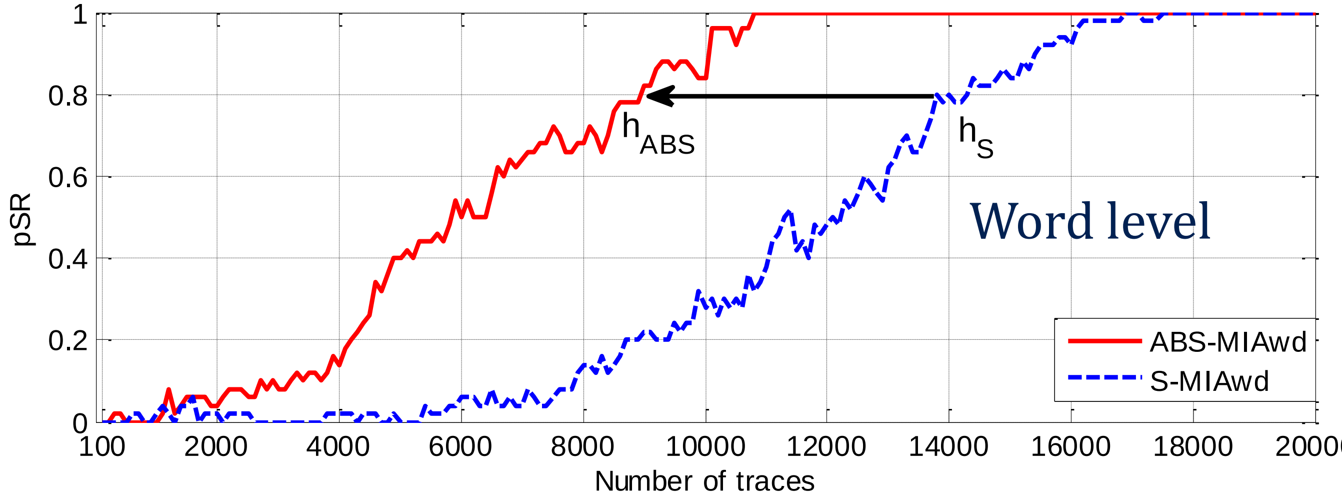
- 3 attacks were considered: ABS-MIA, S-MIA and CPA (as a benchmark)
- Success Rate metric (Standaert '08) used to measure the attack efficiency.
- Comparisons were conducted according to 2 scenarii at the
  - Bit level (Multi-bit, 'mb').
  - Word level ('wd').
- Evaluations were performed across 2 different data sets
  - DpaContestV2.
  - EM traces provided from an hardware FPGA implementing AES.

Experimental Results : Efficiency

Experimental Results : Efficiency

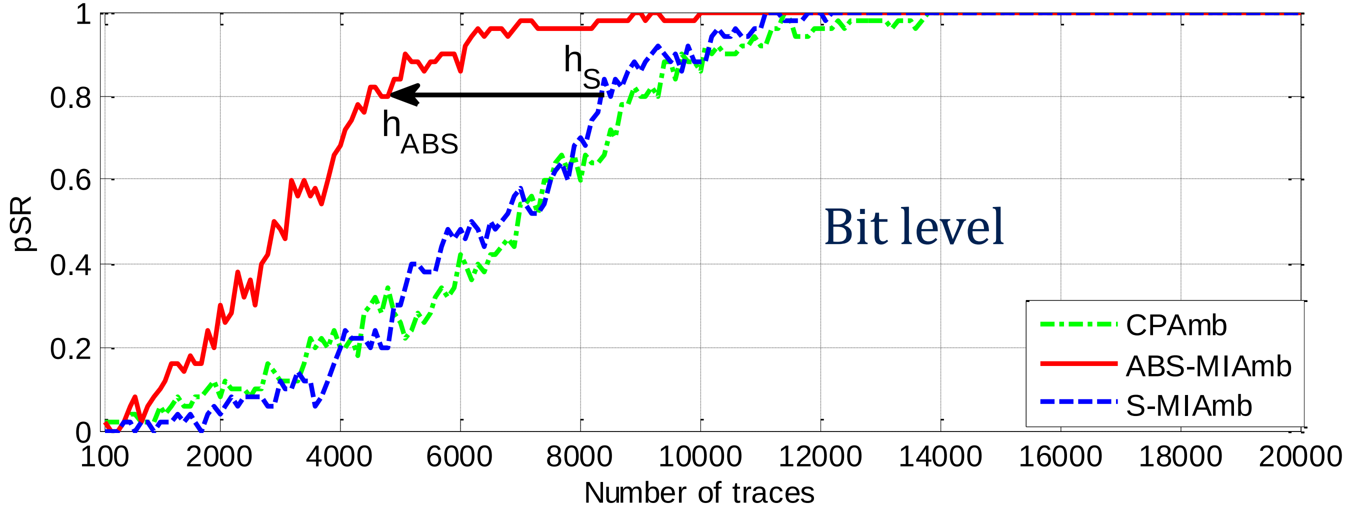
DPAcontestV2 (AES, 10^{th} round , Sbox1, HD).

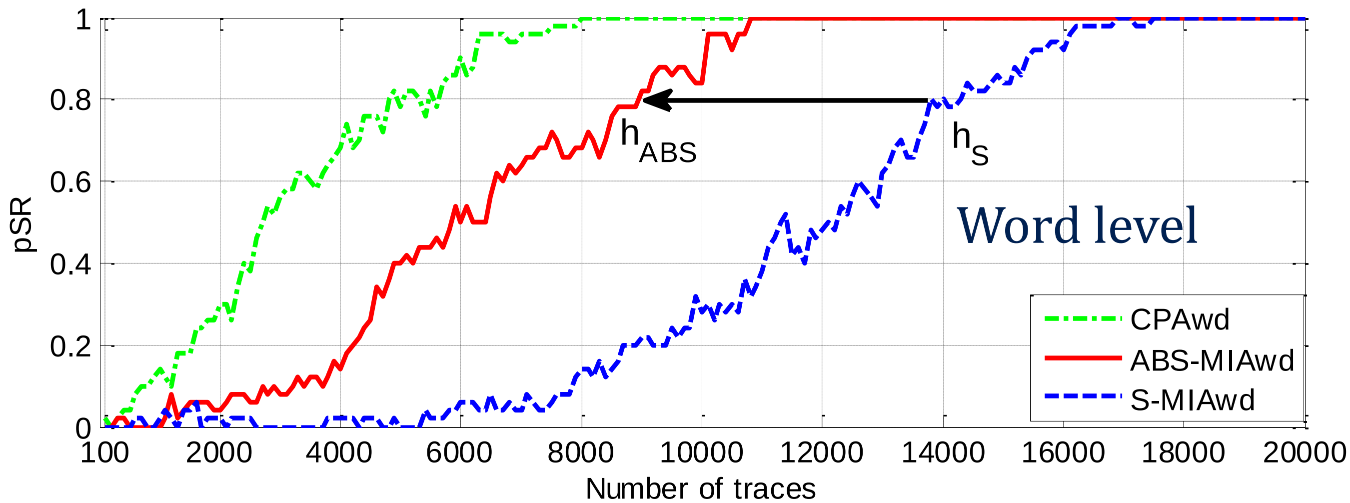




Experimental Results : Efficiency

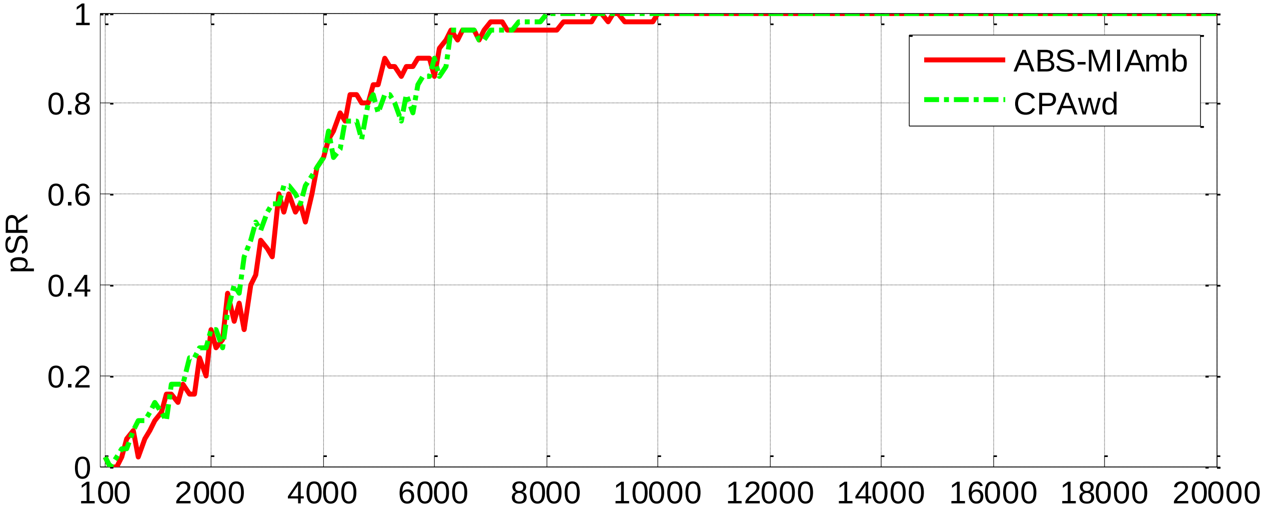
DPAcontestV2 (AES, 10^{th} round , Sbox1, HD).





Experimental Results : Efficiency

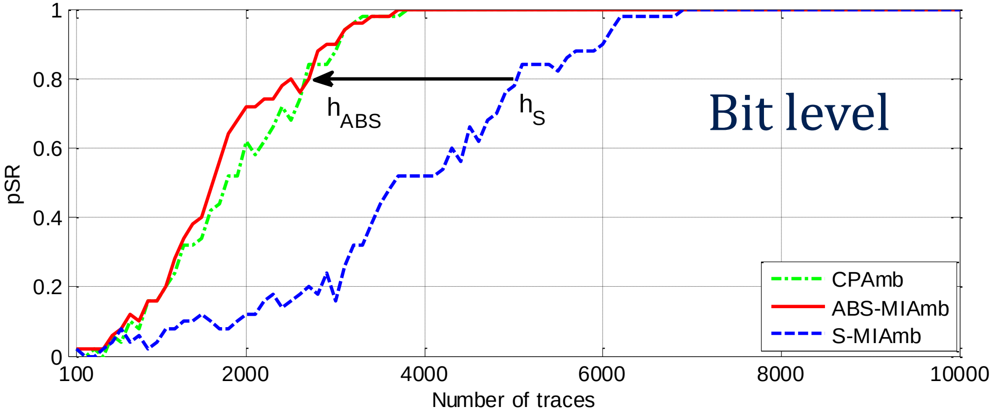
DPAcontestV2 (AES, 10^{th}round, Sbox1, HD).

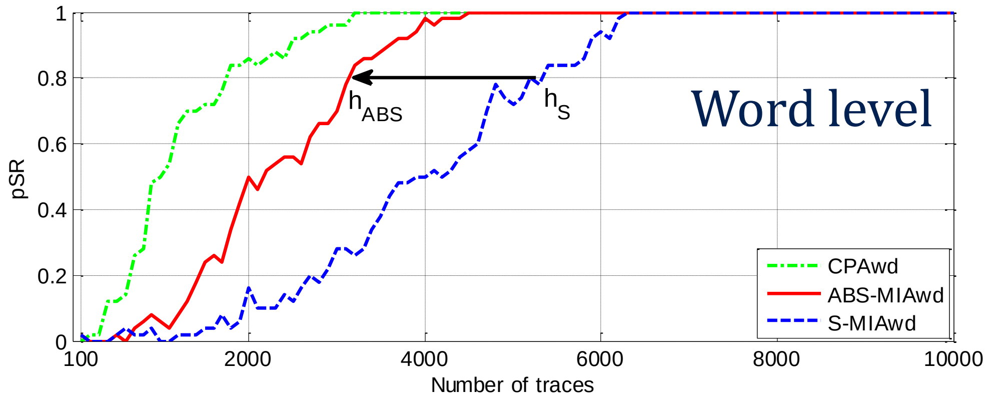


Experimental Results : Genericity

Experimental Results : Genericity

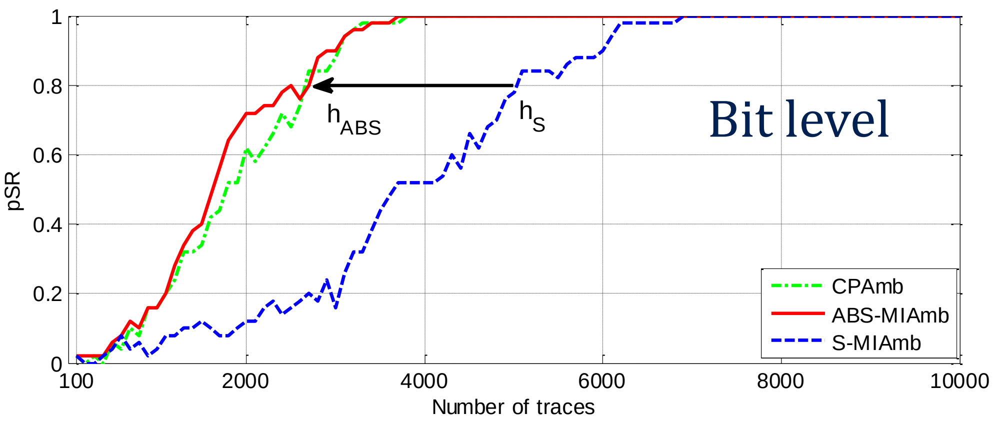
EM traces (AES, 10^{th}round, Sbox4, HD)

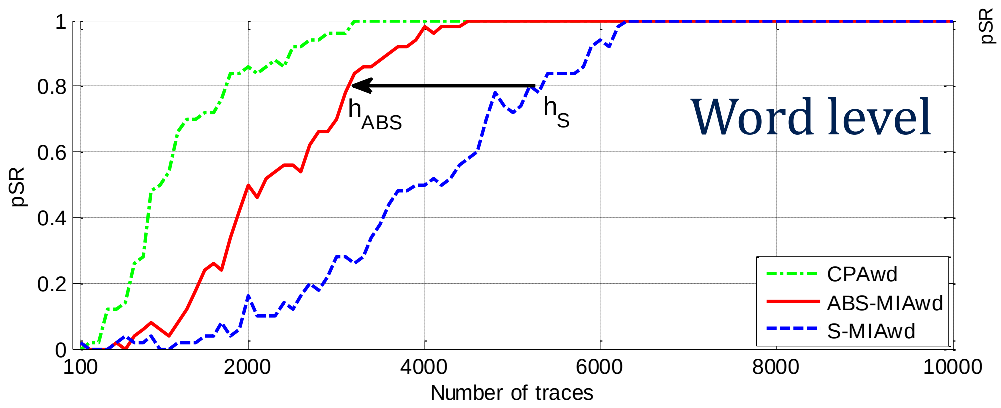




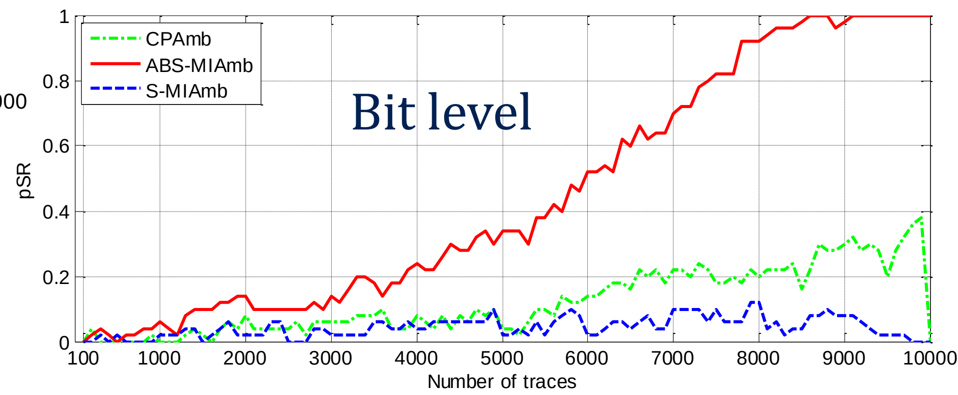
Experimental Results : Genericity

EM traces (AES, 10^{th}round, Sbox4, HD)





EM traces (AES, 10^{th}round, Sbox4, HW)



Conclusion

- Accurately estimating PDF $\neq$ Efficiently performing MIA.
- Our proposal increases efficiency and genericity.
- Other tuning parameters could be evaluated by our approach.

Thank you for your attention !

mathieu.carbone@st.com
mathieu.carbone@lirmm.fr