An overview of Mutual Information Analysis

Nicolas Debande[1,2], Thanh-Ha Le[1], Shiqian Wang and Maël Berthier[1]
[1]: Morpho
[2]: TELECOM-Paristech

Comparison between CPA and MIA

Correlation Power Analysis (CPA): $\rho(W,\varphi(H_K)) = \frac{cov(W,\varphi(H_K))}{\sigma_W \sigma_{\varphi(H_K)}}$

Target: Linear dependency
-> Easy to compute

Side-Channel Analysis:

H_K: prediction corresponding to the key K of an intermediate value
$\phi(H_K)$: selection function of H_K (ex: Hamming weight, Hamming distance)
W: side-channel observation

Leakage Model:

The power consumption of an embedded device can be modeled as follows:

$$C(t) = \phi \circ f(S) + B$$

where ϕ depends on the hardware design and the device, f depends on the algorithm. We model the leakage of a register with the Hamming Distance between two consecutive intermediate values S_0 and S_1.

Mutual Information Analysis (MIA):

$$I(W,\varphi(H_K)) = \sum_{w\in W, h\in\varphi(H_K)} \mathrm{P}[W=w,\varphi(H_K)=h] \log \frac{\mathrm{P}[W=w,\varphi(H_K)=h]}{\mathrm{P}[W=w]P[\varphi(H_K)=h]}$$

Target: Linear dependency and non-linear dependency
-> Not evident to estimate

Information Theory:

The uncertainty of a random variable can be quantified. It's called the entropy of the variable and is defined as follows:

$$\mathrm{H}(X) = \sum_{x\in X} \mathrm{p}(x).\log\frac{1}{\mathrm{p}(x)}$$

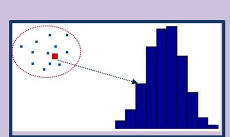
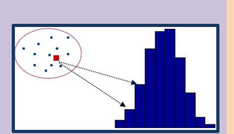
Side Channel Analysis aims to detect a dependency between a set of measurements and a set of computed predictions with the good part of the key. Mutual information is suitable for this detection. Indeed, this quantifies the amount of common information between W and H_K.

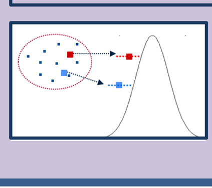
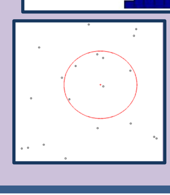
MIA Estimator Classification

PDF estimators

Non-parametric methods

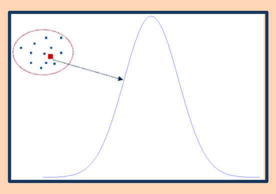
The probability density function is estimated.

Histogram  B-Splines 

Kernel  KNN 

Parametric methods

An hypothesis is made on the distribution of the power consumption.

Parametric Estimation 

Statistical methods

Statistical tests

Cramér-von-Mises Distance:

$$D_{CvM}(W\|H_K) = \int_{-\infty}^{+\infty} (F_W(x_t) - F_{H_K}(x_t))^2 \mathrm{d}x_t$$

Kolmogarov-Smirnov Distance:

$$D_{KS}(W\|H_K) = sup_{x_t}|F_W(x_t) - F_{H_K}(x_t)|$$

with F the empirical cumulative function

Statistical tools

Use tools as statistical moment to estimate dependencies.

Cumulant:

$$I(S(K)) \approx \frac{1}{4}\sum_{ij\neq ii}(R_{ij}^{S(K)})^2 + \frac{1}{12}\sum_{ijk\neq iii}(T_{ijk}^{S(K)})^2 + \frac{1}{48}\sum_{ijkl\neq iiii}(Q_{ijkl}^{S(K)})^2$$

with $S(K) = (W ; H_K)$ and R, T and Q are 2nd, 3rd and 4th-order cumulants respectively

Experimental Results

Method	DPA	CPA	Spearman	Kendall	Correlation Of Distance	MIA Equidistant Histogram	MIA Equipro-bable Histogram	MIA bins and Interpo-lation	MIA Adaptive Partitio-ning	MIA Kernel	MIA KNN	MIA Linear B-Splines	MIA Quadratic B-Splines	CvM Distance	KS Distance	MIA Cumulant
Average Success rate with 500 Msg	98%	100%	98%	100%	96%	76%	75%	70%	62%	80%	<20%	85%	94%	40%	<30%	97%
Nb of Msg for a 80% SR	300	350	350	300	500	F	F	F	F	F	F	F	500	F	F	400

Combined Attacks

Extended CPA: An Alternative to CPA

Extended CPA (ECPA): $\rho_{i,j}(W,\varphi(H_K)) = \frac{cov(P_i(W), P'_j(\varphi(H_K)))}{\sigma_{P_i(W)}\sigma_{P'_j(\varphi(H_K))}}$

where $(P_i)_{i=0,1,2...}$ and $(P'_j)_{j=0,1,2...}$ are two orthogonal polynomial families (Legendre, Hermite, etc).

Combining Techniques

Combined attacks aim to combine relevant information revealed by CPA, ECPA and MIA:

$$CA_{f,g}(W,\varphi(H_K)) = I(W,\varphi(H_K)) \times g(\rho(W,\varphi(H_K))) \times f(\rho_e(W,\varphi(H_K)))$$

where f and g must be increasing functions.

Group1: $f(x) = x, g(x) = 1$

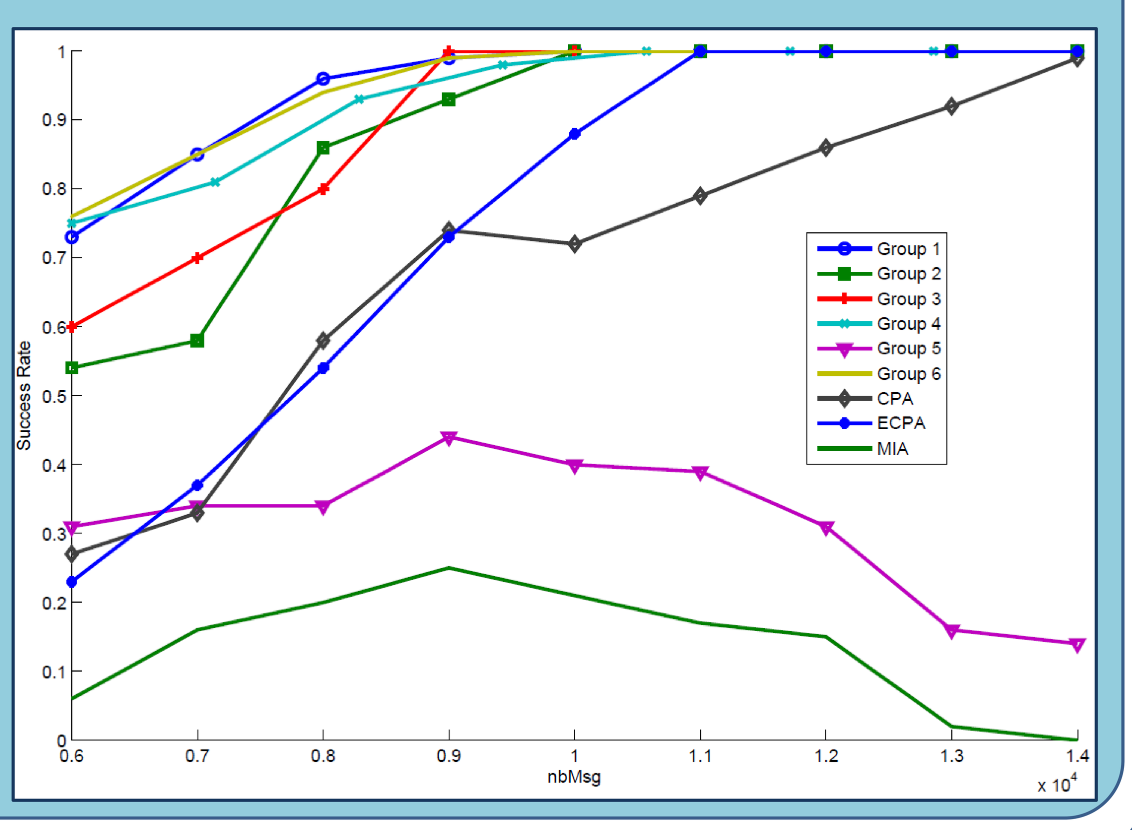
Group2: $f(x) = 1, g(x) = x$

Group3: $f(x) = x, g(x) = x$

Group4: $f(x) = \frac{1+x}{1-x}, g(x) = 1$

Group5: $f(x) = 1, g(x) = \frac{1+x}{1-x}$

Group6: $f(x) = \frac{1+x}{1-x}, g(x) = \frac{1+x}{1-x}$



Conclusions and Perspectives

- Efficiency of the different MIA estimators are strongly dependent of the probability density function of the observations
- Attacks which combine MIA and CPA are most of the time stronger than CPA only or MIA only
- For protected implementations, MIA could be better than CPA/DPA

This work is partially sponsored by the SPACES project

SPACES
Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems

CHES 2011 – Poster Session
September/October 2011