

Motivation & state-of-the art

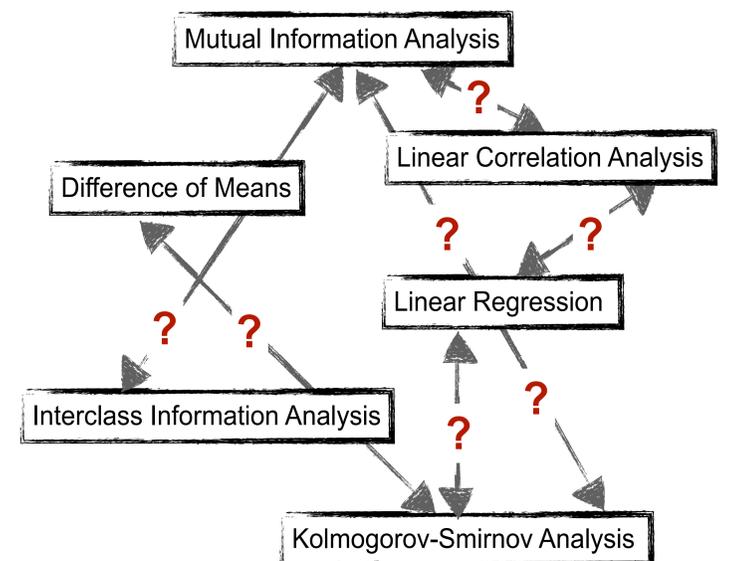
- Different side-channel distinguishers may have different efficiencies
- But their fair comparison is still a difficult task, since many factors come into play

Empirical Criteria

- Success rate (SR)
- Guessing entropy
- Displays the practical outcome
- Ad-hoc computation

Theoretical Criteria

- Relative distinguishing margin
- Displays the theoretical distinguishability
- Equivalent to practical outcome?



Success Metric

Notations

k Key guess, k^* Correct key

$\mathcal{D}(k)$ Distinguisher

Difference

$$\Delta(k^*, k) = \mathcal{D}(k^*) - \mathcal{D}(k)$$

Estimated difference

$$\hat{\Delta}_m(k^*, k) = \hat{\mathcal{D}}_m(k^*) - \hat{\mathcal{D}}_m(k)$$

Estimation bias

$$EB(k^*, k) = \mathbb{E}\{\hat{\Delta}_m(k^*, k)\} - \Delta(k^*, k)$$

Estimation variance

$$EV(k^*, k) = Var\{\hat{\Delta}_m(k^*, k)\}$$

- ✓ Coincides with the empirical success rate
- ✓ Gives more insights on the parameters
- ✓ Depends on the number of measurements
- ✓ “Simple” closed form expression for any additive distinguisher
- Derived from the theoretical success rate through approximations

$$SM(\mathcal{D}, \hat{\mathcal{D}}_m) = \min_{k \neq k^*} \frac{E\{\hat{\Delta}_m(k^*, k)\}}{\sqrt{Var(\hat{\Delta}_m(k^*, k))}}$$

Practical Evaluation

Correlation Power Analysis (CPA)

Mutual Information Analysis (MIA) histograms

Mutual Information Analysis (MIA) kernels

Kolmogorov-Smirnov Analysis (KSA)

Theoretical Criteria

- Does **not** depend on
- the number of traces
 - estimation method

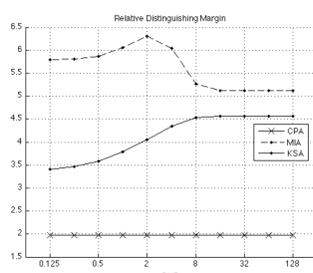


Figure 1

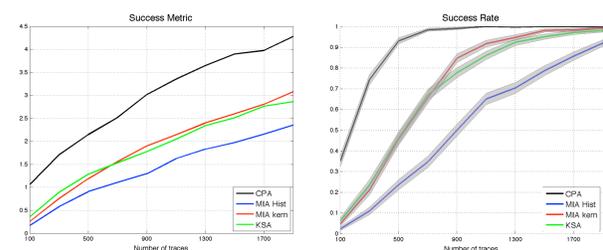
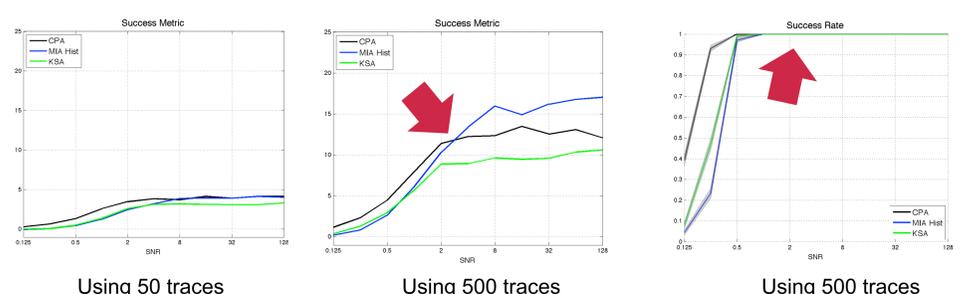


Figure 2



Success Metric

- Depends on the estimation method (Fig. 1)
- Coincides with the success rate (Fig. 1)
- Depends on the number of measurements (Fig. 2)
- More insights (Fig. 2)