Revealing the secrets of success

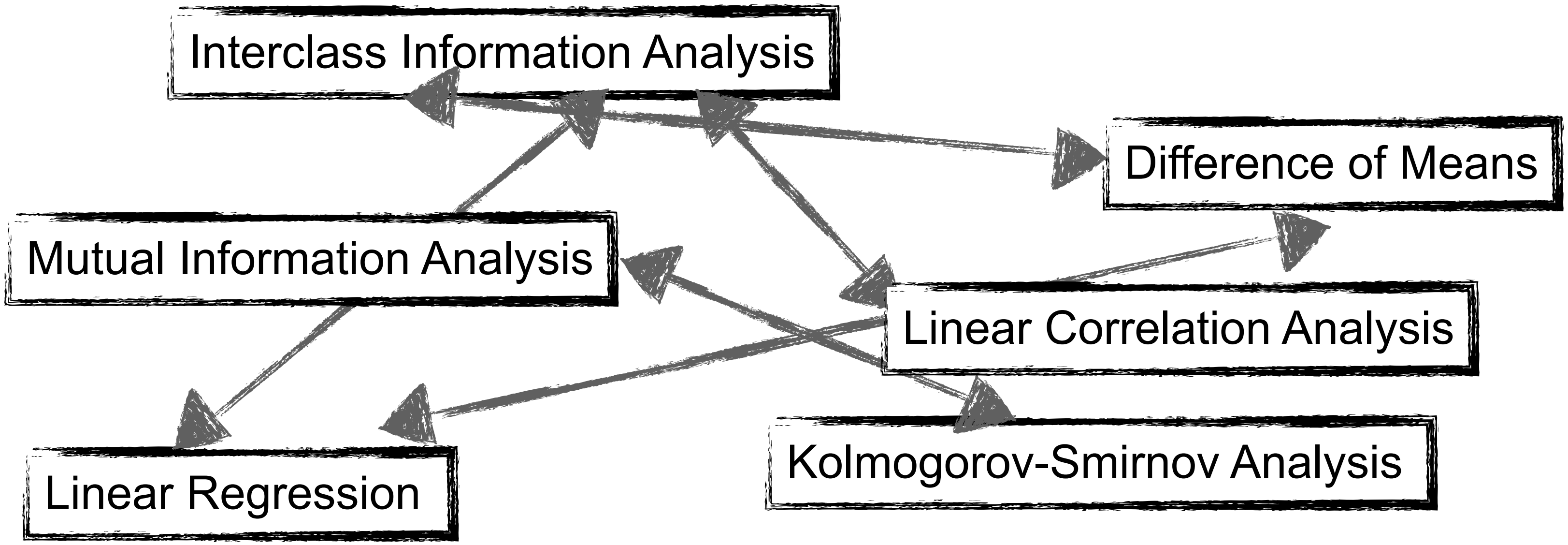
Theoretical efficiency of side-channel distinguishers

Annelie Heuser, Sylvain Guilley, Olivier Rioul

Outline

- Motivation
- State of the art
- New metric: *success metric* (SM)
- Empirical evaluation
- Closed-form expression of SM
- Outlook

Problem Statement



How to compare side-channel distinguishers?

Empirically

- Real measurements (portable?)
- Simulations (model suitable?)

Theoretically

- Is this realistic?

State of the Art

Empirical Criteria

[Standaert+09] Unified framework for the analysis of side-channel key recovery attacks

- Estimated success rate (*o*-th order)
- Estimated guessing entropy

State of the Art

Theoretical Criteria

[WhitnallOswald11] A fair evaluation framework for comparing side-channel distinguisher

- Theoretical evaluation criteria
  (e.g., nearest distinguishing margin)
- Distinguisher is provided with full information about the leakage
- New insights in the theoretical behavior

State of the Art

[Fei+12] Algorithmic confusion analysis for DPA

- Closed-form expression of one-bit DPA for the success rate using a multivariate normal CDF

Algorithmic confusion coefficient

Signal-to-noise ratio

Number of traces

State of the Art

Empirical Criteria	Theoretical Criteria	Closed-form expression
displays the practical outcome	displays the theoretical distinguishability	reflects relevant parameters
ad-hoc computation	equivalent to the practical outcome?	only DPA; multivariate CDF estimation

New metric

- coincides with the empirical success rate
- more insights on parameters
- “simple“ closed-form expression for any additive distinguisher

Notation

Side-channel Model

K RV modeling the key

k^* secret key on the device

$$Y = Y(k) = g(z,k)$$ sensitive variable depending on the key

$$Y^* = Y(k^*) = g(z,k^*)$$ sensitive variable - correct key guess

measured leakage $X = \alpha Y^* + N$ with $N \sim \mathcal{N}(0,\sigma^2)$

Notation

Distinguisher

distinguisher	$\mathcal{D}(X, Y)$ (short $\mathcal{D}(k)$)
difference	$\Delta(k^*, k) = \mathcal{D}(k^*) - \mathcal{D}(k)$
estimated difference	$\widehat{\Delta}_m(k^*, k) = \widehat{\mathcal{D}}_m(k^*) - \widehat{\mathcal{D}}_m(k)$

Notation

Statistical parameter from Estimation Theory

Estimation **B**ias $$\mathrm{EB}(k^*,k) = \mathbb{E}\{\widehat{\Delta}_m(k^*,k)\} - \Delta(k^*,k)$$

Estimation **V**ariance $$\mathrm{EV}(k^*,k) = Var\{\widehat{\Delta}_m(k^*,k)\}$$

such that the mean-squared error of the estimation is given by

$$\mathbb{E}\{(\widehat{\Delta}_m(k^*,k) - \Delta(k^*,k))^2\} = \mathrm{EB}(k^*,k)^2 + \mathrm{EV}(k^*,k)$$

Success Metric

To derive our new metric we start with the **theoretical success rate**:

$$\begin{aligned} SR &= \mathbb{P}\Big(\widehat{\mathcal{D}}_m(X;Y(k^*)) > \widehat{\mathcal{D}}_m(X;Y(k)) \quad (\forall k \neq k^*)\Big) \\ &= \mathbb{P}\Big(\widehat{\Delta}_m(k^*,k) > 0 \quad (\forall k \neq k^*)\Big) \end{aligned}$$

Failure rate

$$FR = 1 - SR = \mathbb{P}\big(\exists k \neq k^* \; / \; \widehat{\Delta}_m(k^*,k) \leq 0\big)$$

Success Metric

Approximate the failure rate:

1. Union bound

$$\mathbb{P}(\exists k \neq k^* \;/\; \widehat{\Delta}_m(k^*, k) \leq 0) \leq \sum_{k \neq k^*} \mathbb{P}(\widehat{\Delta}_m(k^*, k) \leq 0)$$

Failure rate

Normal approximation

Chebyshev/
Chernov bound

Success Metric

2. Normal Approximation

Assumption $\widehat{\Delta}_m(k^*, k) \sim \mathcal{N}(\Delta(k^*, k), \mathrm{EV}(k^*, k))$

$$\mathbb{P}(\widehat{\Delta}_m(k^*, k) \leq 0)$$

$$= \mathbb{P}\left(\frac{\widehat{\Delta}_m(k^*, k) - \mathbb{E}(\widehat{\Delta}_m(k^*, k))}{\sqrt{\mathrm{EV}(k^*, k)}} \leq -\frac{(\Delta(k^*, k) + \mathrm{EB}(k^*, k))}{\sqrt{\mathrm{EV}(k^*, k)}}\right)$$

$$\approx Q\left(\frac{\Delta(k^*, k) + \mathrm{EB}(k^*, k)}{\sqrt{\mathrm{EV}(k^*, k)}}\right) \longrightarrow \infty$$

$$Q(x) = \frac{1}{2\pi} \int_x^{\infty} e^{-t^2/2}\, \mathrm{d}t = \mathbb{P}(X > x)$$

$$\mathbb{P}(\widehat{\Delta}_m(k^*, k) \leq 0) \longrightarrow 0$$ **exponentially** for large *m*

3. First order approximation

Since we achieved exponentially convergence

$$\sum_{k^* \neq k} \mathbb{P}(\widehat{\Delta}_m(k^*, k) \leq 0) \approx \max_{k \neq k^*} \mathbb{P}(\widehat{\Delta}_m(k^*, k) \leq 0).$$

Relation to failure rate

FR = 1 - SR

Normal approximation

$$Q\left(\frac{\Delta(k^*, k) + \mathrm{EB}(k^*, k)}{\sqrt{\mathrm{EV}(k^*, k)}}\right)$$

$$\min_{k \neq k^*} \frac{\Delta(k^*, k) + \mathrm{EB}(k^*, k)}{\sqrt{\mathrm{EV}(k^*, k)}}$$

Success Metric

Derived from the **theoretical success** rate through **approximations**, we define the ***success metric*** as

$$\mathrm{SM}(\mathcal{D}, \widehat{\mathcal{D}}_m) = \min_{k \neq k^*} \frac{\Delta(k^*, k) + \mathrm{EB}(k^*, k)}{\sqrt{\mathrm{EV}(k^*, k)}}$$

$$= \min_{k \neq k^*} \frac{\mathbb{E}\{\widehat{\Delta}_m(k^*, k)\}}{\sqrt{Var(\widehat{\Delta}_m(k^*, k))}}$$

Roughly speaking $$1 - SR \approx e^{-\frac{SM^2}{2}}$$

Empirical Evaluation

Setup

$$Y = HW(\mathtt{Sbox}^{-1}[M \oplus k])$$

$\mathtt{Sbox} : \mathbb{F}_2^6 \to \mathbb{F}_2^4$ is the first DES Sbox

$$X = \alpha Y(k^*) + N \qquad \alpha = 1 \quad N \sim \mathcal{N}(0, \sigma^2)$$

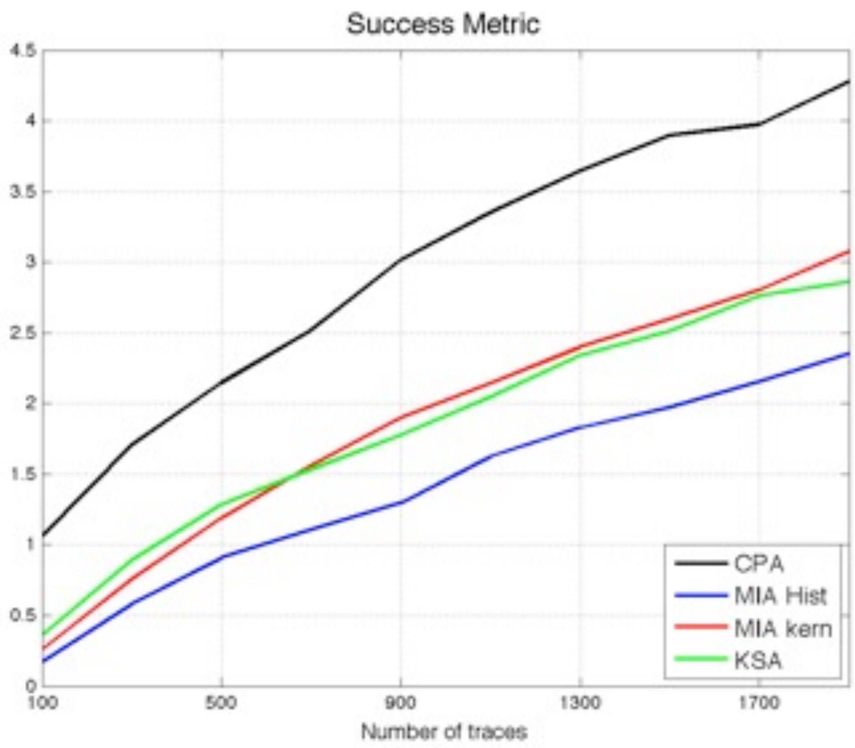
in each setting we conducted 300 experiments

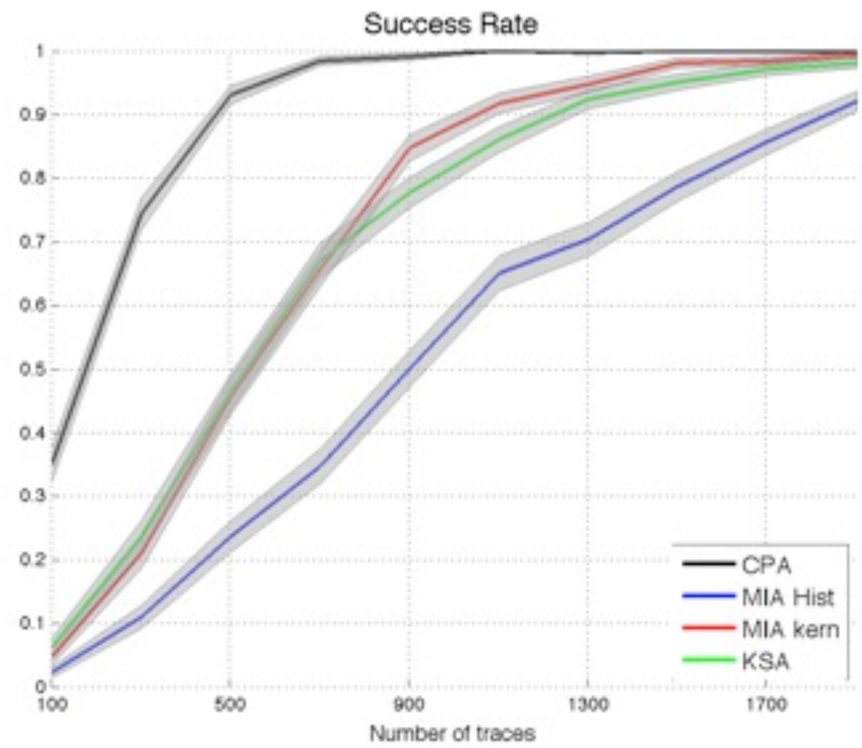
Distinguisher

- Correlation Power Analysis (CPA)
- Mutual Information Analysis (MIA)
  - Histograms
  - Parzen window
- Kolmogorov-Smirnov Analysis (KSA)

Empirical Evaluation

Noise level = 4





SR and SM coincide

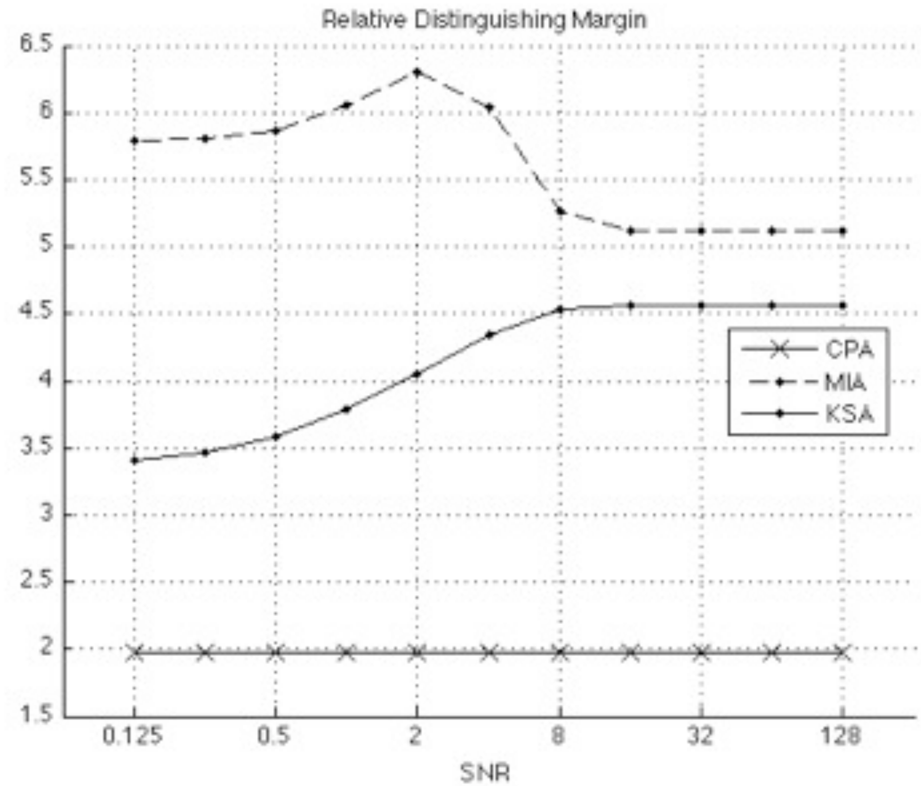
Empirical Evaluation

Relative Distinguishing Margin
[WhitnallOswald11]

$$\mathrm{RDM}(\mathcal{D}) = \frac{\mathcal{D}(k^*) - \max_{k \neq k^*} \mathcal{D}(k)}{\sqrt{Var(\mathcal{D}(K))}}$$

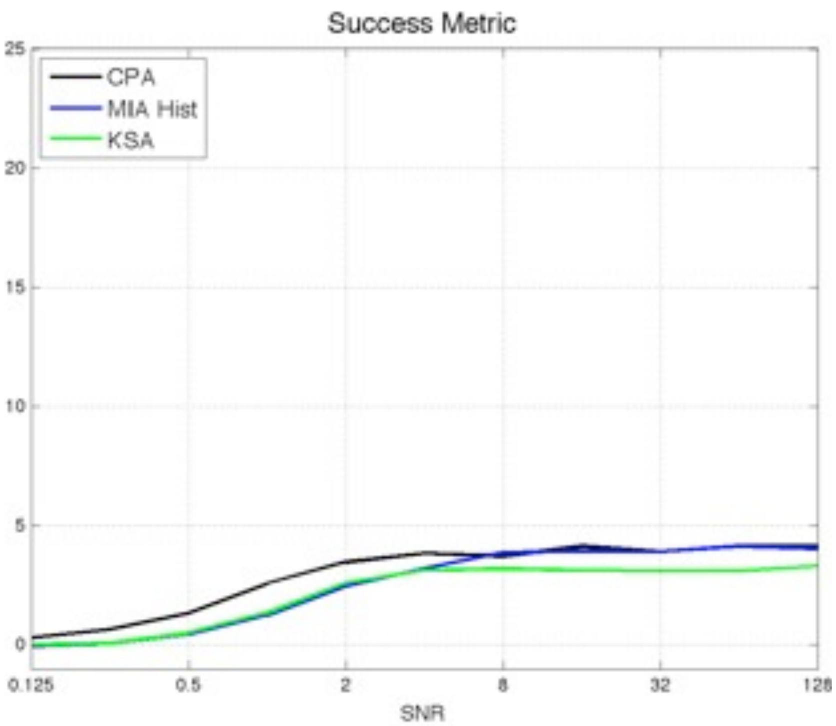
Theoretical Criteria

does **not** depends on
- number of traces
- estimation method

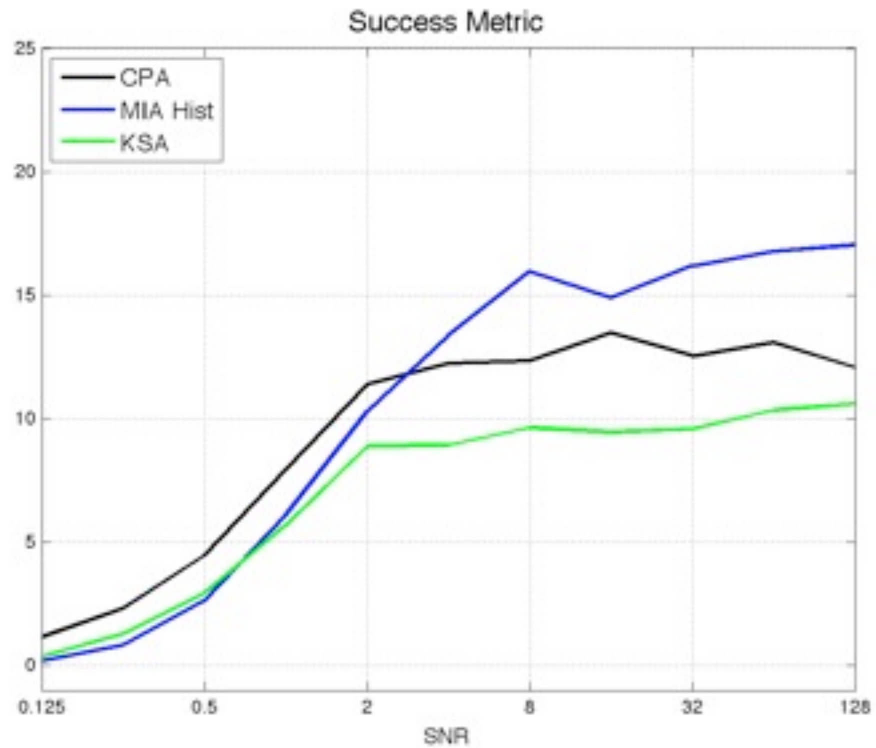


Empirical Evaluation

Using 50 traces



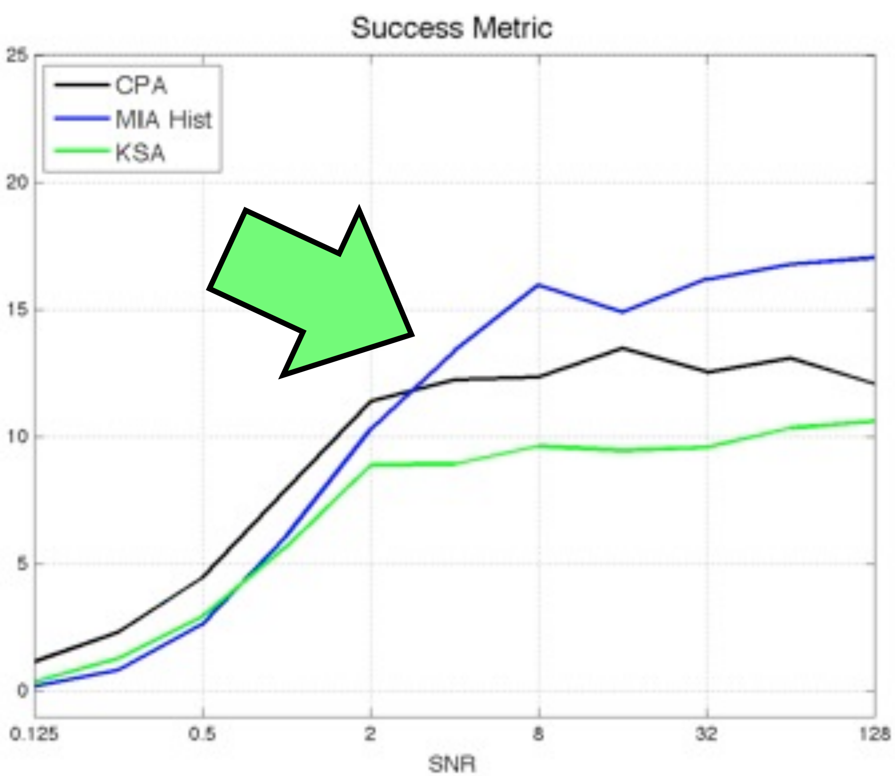
Using 500 traces

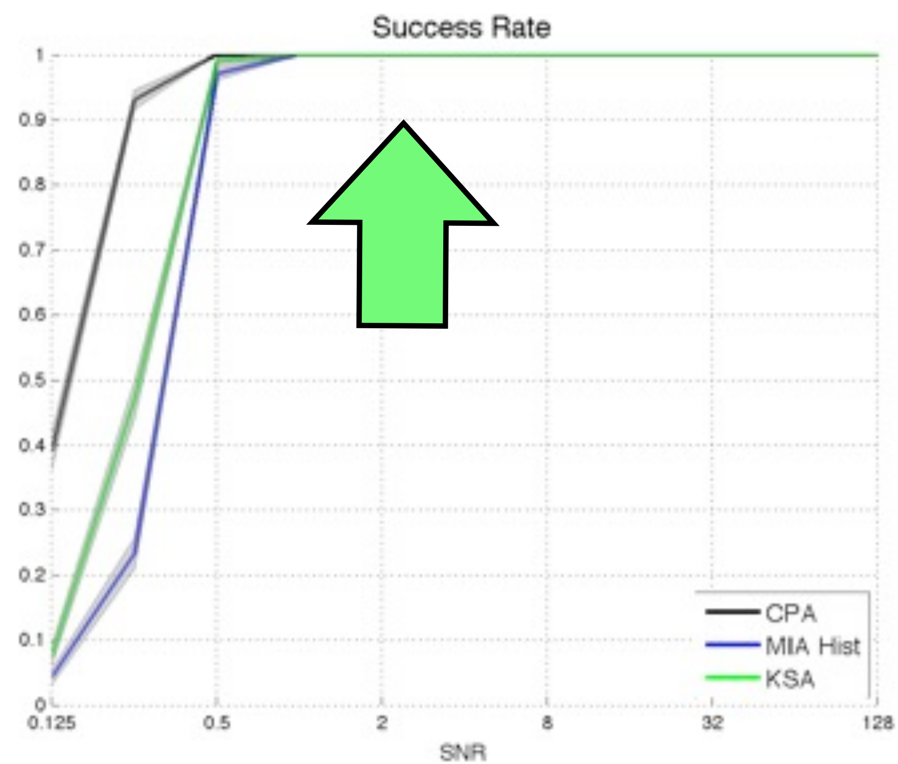


SM depends on the number of traces

Empirical Evaluation

Using 500 traces





Success Metric

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

Closed-form expressions for additive distinguisher

Generalized Confusion Coefficient

[Fei+12]

$$\kappa(k^*, k) = \mathbb{P}(Y(k^*) \neq Y(k))$$

only valid for one-bit models

=

One-bit models

$$\kappa(k^*, k) = \mathbb{E}\{(\frac{Y(k^*) - Y(k)}{2})^2\}, \quad =$$

$$\kappa'(k^*, k) = \mathbb{E}\{Y(k^*)^2(\frac{Y(k^*) - Y(k)}{2})^2\}$$

We assume that that the sensitive variable is normalized

Closed-form Expression

CPA

$$\min_{k \neq k^*} \frac{\epsilon \kappa(k^*, k)}{\sqrt{\epsilon^2(\kappa'(k^*, k) - \kappa^2(k^*, k)) + \sigma^2 \kappa(k^*, k)}} \sqrt{m}$$

$$\epsilon = 2\alpha$$

one-bit DPA

$$\frac{\sqrt{m}}{\sqrt{\max_{k \neq k^*} \frac{1-\kappa(k^*,k)}{\kappa(k^*,k)} + \frac{1}{\kappa(k^*,k)\,\mathrm{SNR}}}}$$

$$\mathrm{SNR} = \frac{\epsilon^2}{\sigma^2}$$

Conclusion & Future Work

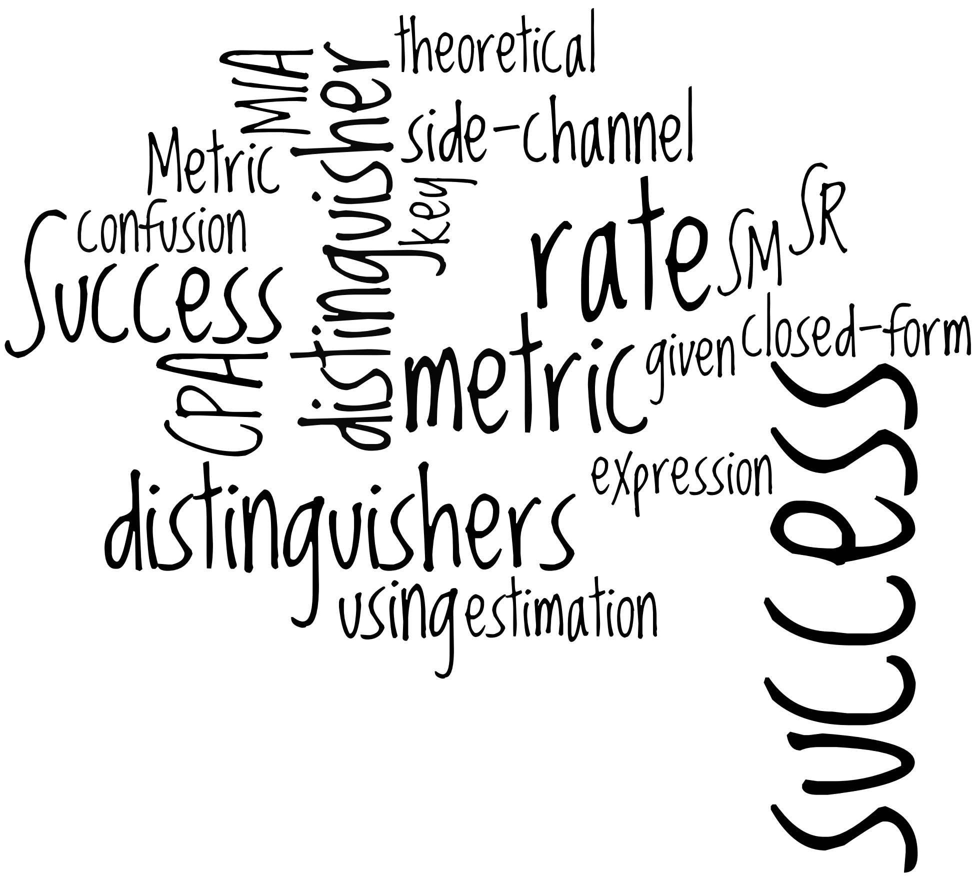
Conclusion

- Introduced the success metric that is derived from the theoretical success rate
- Success metric coincide with the empirical success rate
- We are able to make predictions about crossings that are not visible in the SR
- Extended the idea of confusion
- Derived a closed-form expression for the success metric that is easier to compute

Future Work

- Explain the ranking of various distinguishers
- Determine the influence of the leakage model
  - Sbox
  - Mask
  - nonlinear relationship between X and Y*
- Determine the influence of the estimation

Questions?


theoretical
MIA
distinguisher
Metric
side-channel
confusion
Jkey
rate
SM
SR
Success
CPA
metric
given
closed-form
success
expression
distinguishers
using
estimation