TELECOM ParisTech

Institut Mines-Télécom

A Theoretical Study of Kolmogorov-Smirnov Distinguishers
Side-Channel Analysis vs Differential Cryptanalysis

Annelie Heuser, Olivier Rioul, Sylvain Guilley

COSADE 2014

Problem statement

- The distinguishing behavior of DPA, CPA has been intensively investigated
- „Generic“ distinguisher such as Kolmorov-Smirnov distinguisher still remain „unknown“
- We investigate!

- Side-channel resistant of an Sbox has been bounded to cryptanalytical metrics
- We show an exact link!

State-of-the art

Notations

- $k^\star$ secret key, $k \in \mathcal{K}$ key hypothesis
- $g(\mathcal{T}, \mathcal{K}) \to \mathcal{I}$, e.g., $g(T, k) = \texttt{Sbox}[T \oplus k]$
- measured leakage $X = \psi(g(T, k^*)) + N$, e.g., $\sum_{i=1}^{n} \omega_i [\texttt{Sbox}[T \oplus k^\star]]_i + N$
- sensitive variable $Y(k) = \psi'(g(T, k))$, e.g., $Y(k) = [\texttt{Sbox}[T \oplus k]]_b$ with $b \in \{1, \ldots, n\}$

Theoretical closed-form expression of DPA [Mangard+2006]

$$\rho(X, Y(k)) = \frac{\rho(Y(k^\star), Y(k))}{\sqrt{1 + \frac{1}{SNR}}} \quad ,$$

where ρ is the *absolute value* of the Pearson correlation coefficient.

TELECOM ParisTech

State-of-the art

Confusion coefficient [Fei+2012]

Definition (Confusion coefficient) *Let $k^\star$ denote the correct key and k any key hypothesis in $\mathcal{K}$, then the* confusion coefficient *is defined as*

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

Proposition *For binary and normalized equiprobable Y's*

$$\rho(X, Y) = \boxed{\frac{2}{\sqrt{1 + 1/SNR}}}\boxed{\left|\kappa(k^\star, k) - \frac{1}{2}\right|}$$

confusion coefficient

noise

Proof given in the paper!

TELECOM ParisTech

Contributions

- Derive closed-form expression for Kolmogorov-Smirnov distinguishers
- Show similarity to the closed-form expression of DPA
- Investigate the relationship between the confusion coefficient and side-channel metrics
- Relate the factor depending on the confusion coefficient to differential cryptanalysis

Kolmogorov Smirnov distinguisher

Definition (Standard KS distinguisher) [Veyrat-Charvillon+2009] *The (standard)* Kolmogorov-Smirnov distinguisher *is defined by*

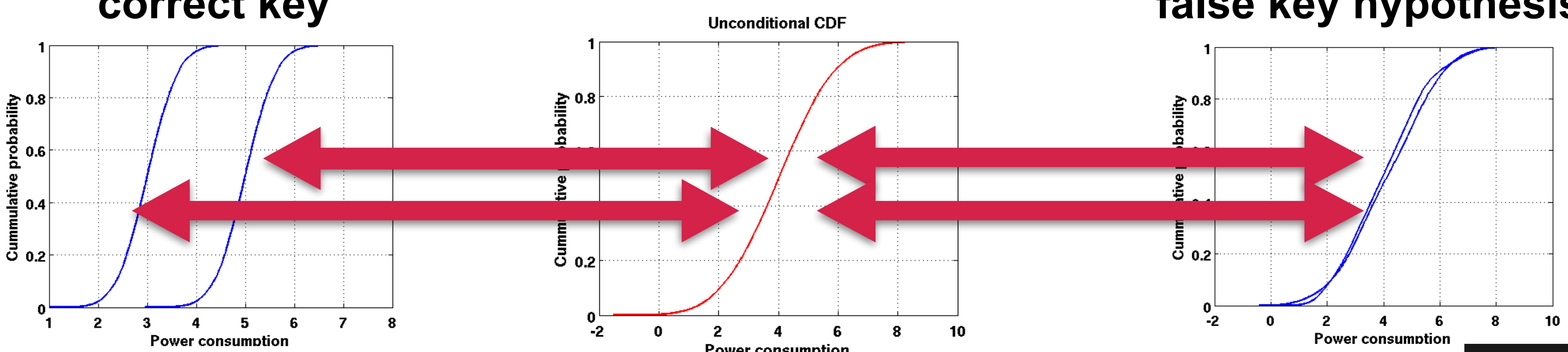
$$\boxed{\mathsf{KSA}(k) = \mathbb{E}_Y\{\|F(x|Y) - F(x)\|_\infty\},}$$

where the expectation is taken over Y*'s distribution,* $\|\cdot\|_\infty$ *is the* L^∞ *norm:* $\|\Psi(x)\|_\infty = \sup_{x\in\mathbb{R}}|\Psi(x)|$*, and* $F(x) = F_X(x)$*,* $F(x|y) = F_{X|Y=y}(x)$ *denote the cumulative distribution functions of* X *and* X *given* $Y(k) = y$*, respectively.*

Conditional CDFs correct key

Unconditional CDFs

Conditional CDFs false key hypothesis



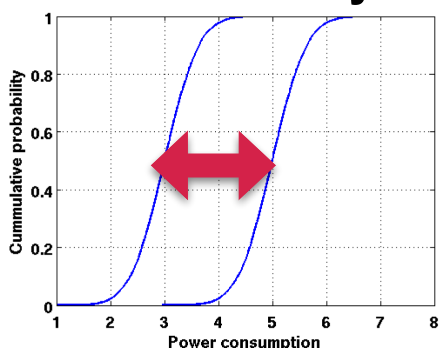
Kolmogorov Smirnov distinguisher

Definition (Inter-class KS distinguisher) [Maghrebi+2012] *The* inter-class Kolmogorov-Smirnov distinguisher *is defined by*

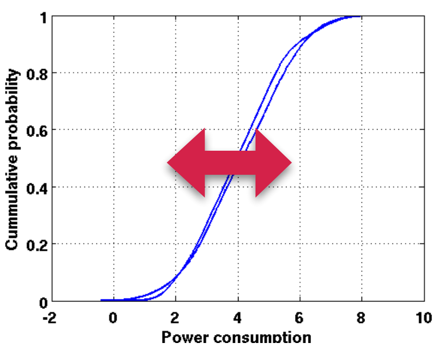
$$\boxed{\mathsf{iKSA}(k) = \frac{1}{2}\mathbb{E}_{Y,Y'}\{\|F(x|Y) - F(x|Y')\|_\infty\}},$$

where Y' is an independent copy of Y, and the expectation is taken over the joint distribution of Y and Y'. The $1/2$ factor makes up for double counts ($(Y, Y') \leftrightarrow (Y', Y)$).

Conditional CDFs correct key



Conditional CDFs false key hypothesis



Confusion condition

Condition (Confusion condition) *For any $k \neq k^\star$, the correspondence from $Y(k)$ to $Y(k^\star)$ is non-injective, i.e., there does* not *exist an injective (that is one-to-one) function $\xi : \mathcal{Y} \to \mathcal{Y}$ such that $Y(k^\star) = \xi\big(Y(k)\big)$ with probability one.*

Lemma *The confusion condition is equivalent to the condition that for all $k \neq k^\star$ there exist $y, y^\star \in \mathcal{Y}$ such that*

$$p(y^\star|y) \text{ is neither } 0 \text{ nor } 1.$$

Proof given in the paper!

First: noise factorization

Proposition (Noise factorization) *One has*

$$\mathsf{KSA}(k) = \boxed{c} \boxed{\sum_{y \in \mathcal{Y}} p(y) \big| p(y^\star | y) - p(y^\star) \big|}$$

$$\mathsf{iKSA}(k) = \boxed{\frac{c}{2}} \boxed{\sum_{\substack{y, y' \in \mathcal{Y} \\ y \neq y'}} p(y) p(y') \big| p(y^\star | y) - p(y^\star | y') \big|} \; ,$$

where $y^\star$ denotes any of the two possible values in $\mathcal{Y}$ and where

$$\boxed{c = 2\,\Phi\left(\frac{\Delta y}{2\sigma}\right) - 1} > 0 \; .$$

leakage model

noise

Proof given in the paper!

KSA and iKSA are *not* equivalent

TELECOM ParisTech

Second: Simple closed-form expression

Equiprobable bits [Fei+2012]

Assumption *For a* perfectly secret encryption algorithm, *each sensitive variable is equiprobable, i.e.,* $p(y) = p(y^\star) = 1/2$.

Proposition *For binary and equiprobable* Y*'s, the confusion condition in reduces to*

$$\kappa(k^\star, k) \quad \text{is neither } 0 \text{ nor } 1 \qquad (\forall k \neq k^\star).$$

Proposition KSA *and* iKSA *are completely equivalent in this case, with the following closed-form expression*

$$\mathsf{KSA}(k) = 2\,\mathsf{iKSA}(k) = c\,\boxed{\left|\kappa(k^\star, k) - \tfrac{1}{2}\right|}.$$

Proofs given in the paper!

KSA and iKSA *are* equivalent

confusion factor equivalent to DPA

Closed-forms DPA / (i)KSA

$$\text{DPA}(k) = \frac{2}{\sqrt{1 + 1/SNR}} \cdot \left|\kappa(k^\star, k) - \tfrac{1}{2}\right|$$

$$\text{KSA}(k) = 2\,\text{iKSA}(k) = \left(2\Phi\left(\sqrt{SNR}\right) - 1\right) \cdot \left|\kappa(k^\star, k) - \tfrac{1}{2}\right|$$

Even if DPA distinguishes on a *proportional* scale and (i)KSA on a *nominal* scale they exploit equivalently the differences between correct and incorrect key guesses

What does $\left|\kappa(k^\star, k) - \frac{1}{2}\right|$ mean?

Leakage model consists of an Sbox operation

$Y(k) = S(T \oplus k)$, where S is a $\mathbb{F}_2^n \to \mathbb{F}_2$ Boolean function

TELECOM ParisTech

Metrics in side-channel analysis

Definition (Relative distinguishing margin) [Whitnall+2011] *The* relative distinguishing margin $\mathrm{RDM}(\mathcal{D})$ *is defined as*

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

where K is the uniformly distributed random variable modeling the choice of the key k.

As the noise appears as a multiplicative factor
it is eliminated in the RDM.

TELECOM ParisTech

Metrics in side-channel analysis

Definition (Distinguishing margin) *The* distinguishing margin $\mathrm{DM}(\mathcal{D})$ *is the minimal distance between the distinguisher for the correct key and all incorrect keys. Formally,*

$$\mathrm{DM}(\mathcal{D}) = \mathcal{D}(k^\star) - \max_{k \neq k^\star} \mathcal{D}(k).$$

Proposition (Distinguishing margin of (i)KSA and DPA) *The distance to the nearest rival can be computed exactly as*

$$\mathrm{DM}(\mathcal{D}) = \lambda \cdot \left(\frac{1}{2} - \max_{k \neq k^\star} \left| \kappa(k^\star, k) - \frac{1}{2} \right| \right).$$

Proof given in the paper!

The smaller the maximal distance between the confusion coefficient and 0.5 the easier to attack!

TELECOM ParisTech

Metrics in cryptanalysis

Definition (Linear and differential uniformity) *Let* $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *be an Sbox. The linear* (Λ_S) *and differential* (Δ_S) *uniformities of* S *are defined as:*

$$\Lambda_S = \max_{a \in \mathbb{F}_2^n,\ k \in \mathbb{F}_2^{m\,*}} \left| \#\{x \in \mathbb{F}_2^n / (a \cdot x) \oplus (k \cdot S(x)) = 0\} - 2^{n-1} \right| \ ,$$

$$\Delta_S = \max_{a \in \mathbb{F}_2^m,\ k \in \mathbb{F}_2^{n\,*}} \#\{x \in \mathbb{F}_2^n / S(x) \oplus S(x \oplus k) = a\} \ .$$

- The *smaller* the linear/ differential uniformity, the *better* the Sbox from an cryptanalytical point of view
- *Linear* uniformity is related to *nonlinearity*: the smaller the linear uniformity the greater the nonlinearity

Confusion coefficient vs diff uniformity

Proposition (Differential uniformity vs the confusion coefficient) *When considering a Boolean function $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ with $m = 1$, then*

$$2^{-n}\Delta_S - \frac{1}{2} = \max_{k \neq k^\star} \left| \kappa(k^\star, k) - \frac{1}{2} \right| .$$

Proof given in the paper!

Proposition (Relationship between DM and Δ_S) *The distinguishing margin can be expressed with differential uniformity as*

$$\mathrm{DM}(\mathcal{D}) = \lambda \cdot \left(\tfrac{1}{2} - \max_{k \neq k^\star} \left| \kappa(k^\star, k) - \tfrac{1}{2} \right| \right) = \lambda \cdot (1 - 2^{-n}\Delta_S).$$

Proof given in the paper!

To harden the resistance the distance to 0.5

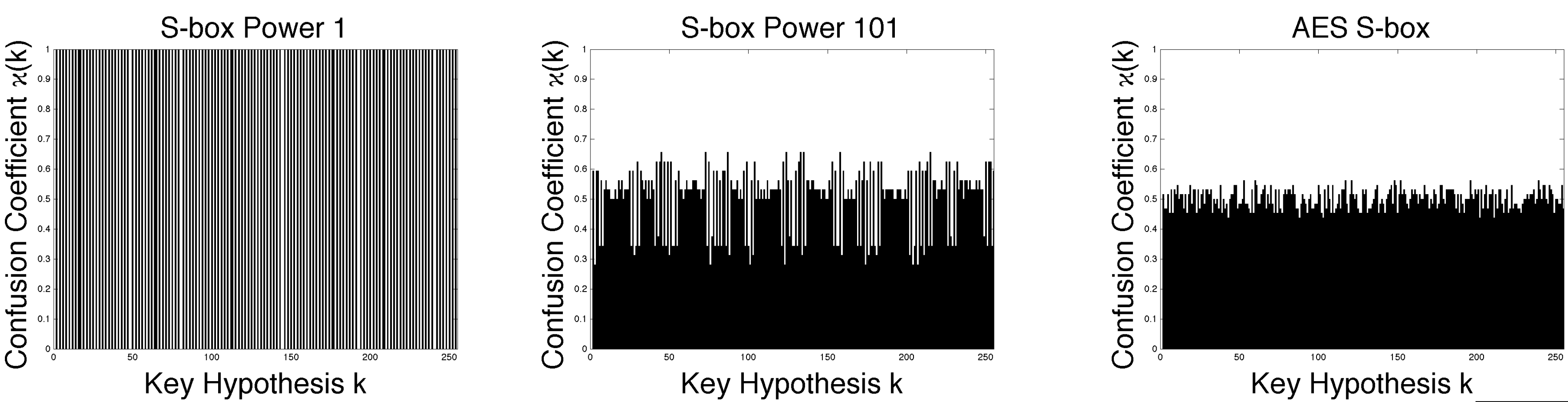
- Cryptanalysis: minimized
- Side-channel: maximized

Remark *There is no direct link between the* linear uniformity *and the confusion coefficient* $\kappa(k^\star, k)$.

Practical evaluation

- **3 different bijective S-boxes:**

  1. A "bad" $\texttt{Sbox}[\cdot]$, termed S_1, of equation $y \mapsto a \odot y \oplus b$,
  2. An "average" $\texttt{Sbox}[\cdot]$, termed S_{101}, of equation $y \mapsto a \odot y^{101} \oplus b$,
  3. A "good" $\texttt{Sbox}[\cdot]$, termed S_{254}, of equation $y \mapsto a \odot y^{254} \oplus b$.



TELECOM ParisTech

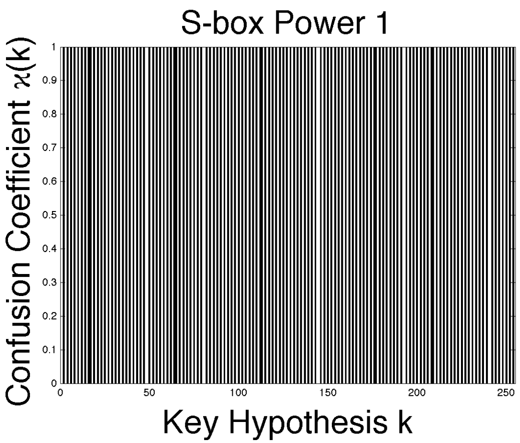
Practical evaluation

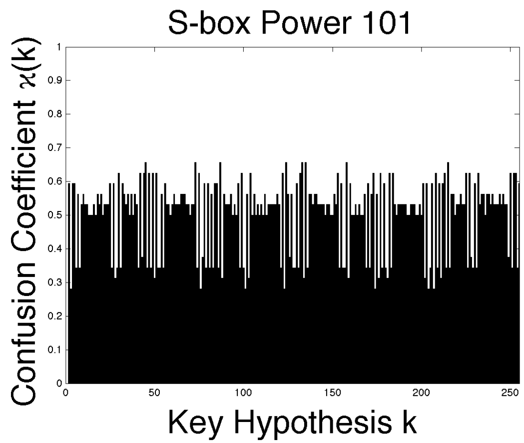
Table 1: Properties of the studied S-boxes (where $\sigma^2 = 0$ for DM).

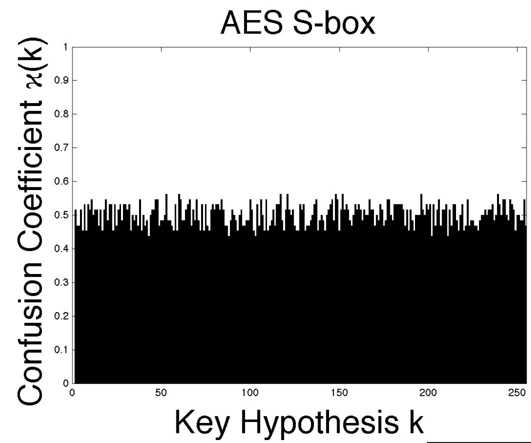
harder SCA

S-box	Δ_S	DM (i)KSA/DPA	RDM
S_1	256	0/0	0
S_{101}	184	0.28/0.56	2.58
S_{254}	144	0.44/0.88	9.82

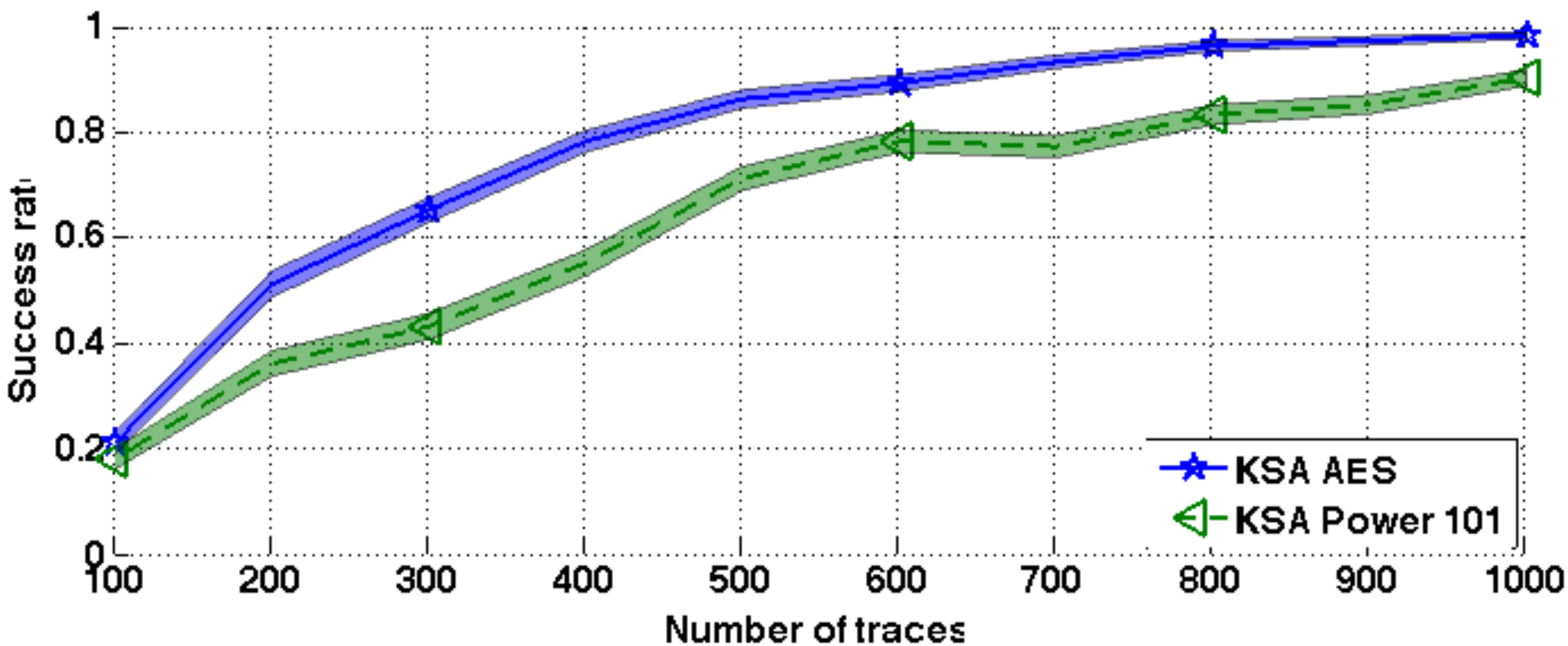
harder cryptanalysis







Practical evaluation



- Leakage arising from the Hamming Weight model
- Leakage model: 4th bit
- SNR = 1

TELECOM ParisTech

Thank you!!

conclusion

Step further to study information theoretic distinguishers

- Noise factorization
- Closed-form expression for (i)KSA in terms of the confusion coefficient
- (Proof of soundness - see paper)

Exact link between cryptanalysis and side-channel analysis

- Related the confusion coefficient to differential uniformity (not non-linearity)
- Case-study with 3 S-boxes

future work

- Extension to multi-bit scenario
- Apply the framework to other distinguisher (e.g., MIA)
- Extend the study between cryptanalysis and SCA

Thank you!!

Questions?