Univariate Side Channel Attacks and Leakage Modeling

Julien Doget, Emmanuel Prouff, Matthieu Rivain and François-Xavier Standaert

Oberthur Technologies & CryptoExperts & UCL & LAGA-MTII Paris 8

Oberthur Technologies

Outline

Oberthur Technologies

Outline

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB, BSCPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB, BSCPA, FODPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB, BSCPA, FODPA, SODPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB, BSCPA, FODPA, SODPA, PODPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB, BSCPA, FODPA, SODPA, PODPA, Z02DPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB, BSCPA, FODPA, SODPA, PODPA, Z02DPA, FFT2DPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB, BSCPA, FODPA, SODPA, PODPA, Z02DPA, FFT2DPA, BSECPA

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB, BSCPA, FODPA, SODPA, PODPA, Z02DPA, FFT2DPA, BSECPA, CPACOP

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB, BSCPA, FODPA, SODPA, PODPA, Z02DPA, FFT2DPA, BSECPA, CPACOP, ...

Oberthur Technologies

Problematics

- Focus on Univariate First-Order SCA
  - SCA focusses on a single intermediate variable manipulation.
  - we don't deal with higher-order SCA!
- What do we want to do?
  - Exhibit a linear dependency
- Which tools do we have in the literature?
  - DPA, CPA, PPA, MIA, BPA, DBA, ICA, IPA, MCA, DiPA, MDCA, MLPA, DPAMB, BSCPA, FODPA, SODPA, PODPA, Z02DPA, FFT2DPA, BSECPA, CPACOP, ...
- What well-established theory says about dependency test?
  - Linear correlation: Pearson's coefficient
  - Quantity of shared Information: mutual information (or Kullback-Leibler Distance)

Oberthur Technologies

It's round, it rolls ... it's a wheel !

Linear correlation

- Measures linear dependencies between two sets
- Observations and estimations
- Estimations ?

Oberthur Technologies

It's round, it rolls ... it's a wheel !

Linear correlation

- Measures linear dependencies between two sets
- Observations and estimations
- Estimations ?

Linear estimation

- Exhibits a linear model from observations
- What to do with this model ?

Oberthur Technologies

Outline

Oberthur Technologies

Abstract

- Study the relationship between some well-used distinguishers: DPA and variants, PPA and CPA.
  - Do they differ one to each other?
  - Do they involve different statistical tools?
  - Is one of them always better than the other ones?
- Study some distinguishers that do not need an *a priori* modeling of the observations.

$\Rightarrow$ We rule on how to lead a linear univariate side-channel attack!

Oberthur Technologies

Preliminaries

- (Noisy) Observation of a processing:

$$L \longleftarrow V_k = S(k, P)$$

- $(p_i)_i$: known values taken by P.
- $(v_{k,i})_i$: unknown values taken by V_k.
- $(\ell_{k,i})_i$: known values taken by L.

Assumption on Leakages

- Composed of two parts:
  - A deterministic part $\delta(\cdot)$,
  - An independent noise B,
- such that $L = \delta(V_k) + B$.

Oberthur Technologies

SCA-attack Outlines

1. Measurement : get a sample $(\ell_{k,i})_i$ related to a sample $(p_i)_i$ of plaintexts.
2. Model Selection : Design/Select a function $\mathbf{m}(\cdot)$ to model $\delta(\cdot)$.
3. Prediction : For every $\hat{k}$, compute

$$m_{\hat{k},i} = \mathbf{m}(v_{\hat{k},i}) \quad = \mathbf{m}(S(\hat{k}, p_i)) \ .$$

   The r.v. corresponding to $m_{\hat{k},i}$ is denoted by $M_{\hat{k}}$.
4. Distinguisher Selection : Choose a statistical distinguisher Δ.
5. Key Discrimination : For every $\hat{k}$, compute the distinguishing value $\Delta_{\hat{k}}$:

$$\Delta_{\hat{k}} = \Delta\left((\ell_{k,i})_i, (m_{\hat{k},i})_i\right) \ .$$

6. Key Candidate Selection : Output the o key hypotheses that maximize $\Delta_{\hat{k}}$.

Oberthur Technologies

Differences

What differs from an attack to another

- The distinguisher Δ
- The model **m**

$\rightarrow$ How to choose the distinguisher?

$\rightarrow$ How to choose the model?

$\Longrightarrow$ Link between the two questions?

Oberthur Technologies

Differential Power Analysis

single-bit DPA

- Example: $\mathbf{m}(v_{\hat{k},i}) = S_0(p_i \oplus \hat{k})$, where S_0 is the 0th coordinate function of S.
- $\mathrm{Im}(\mathbf{m}) = \{w_0, w_1\}$
- (e.g. $w_0 = 0$ and $w_1 = 1$).
- $\Delta_{\hat{k}} = \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_0\right) - \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_1\right) = \textbf{SB-DPA}(\hat{k})$.

Oberthur Technologies

Differential Power Analysis

single-bit DPA

- Example: $\mathbf{m}(v_{\hat{k},i}) = S_0(p_i \oplus \hat{k})$, where S_0 is the 0th coordinate function of S.
- $\mathrm{Im}(\mathbf{m}) = \{w_0, w_1\}$
- (e.g. $w_0 = 0$ and $w_1 = 1$).
- $\Delta_{\hat{k}} = \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_0\right) - \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_1\right) = \textbf{SB-DPA}(\hat{k})$.

all-or-nothing DPA

- Example: $\mathbf{m}(v_{\hat{k},i}) = \mathrm{HW}(S(p_i \oplus \hat{k}))$.
- $\mathrm{Im}(\mathbf{m}) = \{\cdots, \omega_0, \cdots, \omega_1, \cdots\}$
- (e.g. $\mathrm{Im}(\mathbf{m}) = \{0, \cdots, 8\}$ and $w_0 = 0$ and $w_1 = 8$).
- $\Delta_{\hat{k}} = \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_0\right) - \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_1\right) = \textbf{AON-DPA}(\hat{k})$.

Oberthur Technologies

Generalized DPA

generalized DPA

- Example: $\mathbf{m}(v_{\hat{k},i}) = \mathrm{HW}(S(p_i \oplus \hat{k}))$.
- $\mathrm{Im}(m) = \cdots \cup \Omega_0 \cup \cdots \cup \Omega_1 \cup \cdots$
- (e.g. $\mathrm{Im}(\mathbf{m}) = \Omega_0 \cup \Omega_1$ and $\Omega_0 = \{0, ..., 4\}$ and $\Omega_1 = \{5, \cdots, 8\}$).
- $\Delta_{\hat{k}} = \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} \in \Omega_0\right) - \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} \in \Omega_1\right) = \textbf{G-DPA}(\hat{k})$.

Oberthur Technologies

Partition Power Analysis

PPA

- Example: $\mathbf{m}(v_{\hat{k},i}) = \mathrm{HW}(S(p_i \oplus \hat{k}))$.
- $\mathrm{Im}(\mathbf{m}) = \{\omega_i;\ i\}$ (e.g. $\mathrm{Im}(\mathbf{m}) = \{0, \cdots, 8\}$).
- $\Delta_{\hat{k}} = \sum_{\omega_i \in \mathrm{Im}(\mathbf{m})} \alpha_i \cdot \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_i\right) = \mathbf{PPA}_{(\alpha_i)_i}(\hat{k})$,
- $\alpha_i \in \mathbb{R}$

Correlation Power Analysis

CPA

- Example: $\mathbf{m}(v_{\hat{k},i}) = \mathrm{HW}(S(p_i \oplus \hat{k}))$.
- $\mathrm{Im}(\mathbf{m}) = \{\omega_i;\ i\}$
- (e.g. $\mathrm{Im}(\mathbf{m}) = \{0, \cdots, 8\}$.
- $\Delta_{\hat{k}} = \widehat{\rho}\left(L, M_{\hat{k}}\right) = \frac{\widehat{\mathrm{cov}}\left(L, M_{\hat{k}}\right)}{\widehat{\sigma}(L) \cdot \widehat{\sigma}\left(M_{\hat{k}}\right)} = \mathbf{CPA}(\hat{k})$,
- $\widehat{\sigma}(L)$ and $\widehat{\sigma}\left(M_{\hat{k}}\right)$: estimators of the standard dev. of L and $V_{\hat{k}}$.
- $\widehat{\mathrm{cov}}\left(L, M_{\hat{k}}\right)$: estimator of the covariance between L and $V_{\hat{k}}$
- Note: $\widehat{\mathrm{cov}}\left(L, M_{\hat{k}}\right) = \widehat{\mathbb{E}}\left(L M_{\hat{k}}\right) - \widehat{\mathbb{E}}(L)\widehat{\mathbb{E}}\left(M_{\hat{k}}\right)$.

Oberthur Technologies

Assumption and Definition

Target Uniformity

$(v_{\hat{k},i})_i$ is balanced for every key hypothesis $\hat{k}$.

$\Rightarrow \hat{\sigma}(V_{\hat{k}})$ and $\widehat{\mathbb{E}}(V_{\hat{k}})$ are constant w.r.t. $\hat{k}$ and are perfect!

Oberthur Technologies

Assumption and Definition

Target Uniformity

$(v_{\hat{k},i})_i$ is balanced for every key hypothesis $\hat{k}$.

$\Rightarrow \hat{\sigma}(V_{\hat{k}})$ and $\widehat{\mathbb{E}}(V_{\hat{k}})$ are constant w.r.t. $\hat{k}$ and are perfect!

SCA-reduction

A $(\mathbf{m}, \Delta)$-SCA is SCA-reducible to a $(\mathbf{m}', \Delta')$-SCA if there exists a function $\mathbf{f}$ s.t. $\mathbf{m} = \mathbf{f} \circ \mathbf{m}'$ and for every $(k, \hat{k})$ and every samples $(\ell_{k,i})_i$ and $(v_{\hat{k},i})_i$, there exists a strictly monotonous function $\mathbf{g}$ s.t.:

$$\Delta\left((\ell_{k,i})_i, (m_{\hat{k},i})_i\right) = \mathbf{g} \circ \Delta'\left((\ell_{k,i})_i, (m'_{\hat{k},i})_i\right) \quad ,$$

where $m_{\hat{k},i} = \mathbf{m}(v_{\hat{k},i})$ and $m'_{\hat{k},i} = \mathbf{m}'(v_{\hat{k},i})$.

Oberthur Technologies

Outline

Oberthur Technologies

single-bit DPA

single-bit DPA

- $\mathrm{Im}(\mathbf{m}) = \{w_0, w_1\}$
- $\textbf{SB-DPA}(\hat{k}) = \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_0\right) - \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_1\right)$.

Oberthur Technologies

single-bit DPA

single-bit DPA

- $\mathrm{Im}(\mathbf{m}) = \{w_0, w_1\}$
- $\textbf{SB-DPA}(\hat{k}) = \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_0\right) - \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_1\right)$.

Choose $\mathbf{f} = \mathrm{Id}$ and $\mathbf{g} = \mathrm{Id}$. In fact, just a rewriting!

PPA reduction

$$\textbf{SB-DPA}(\hat{k}) = \alpha_0 \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_0\right) + \alpha_1 \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_1\right) = \textbf{PPA}_{(\alpha_0,\alpha_1)}(\hat{k})$$

Oberthur Technologies

all-or-nothing DPA

all-or-nothing DPA

- $\mathrm{Im}(\mathbf{m}) = \{\cdots, \omega_0, \cdots, \omega_1, \cdots\}$
- $\textbf{AON-DPA}(\hat{k}) = \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_0\right) - \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_1\right)$.

Oberthur Technologies

all-or-nothing DPA

all-or-nothing DPA

- $\mathrm{Im}(\mathbf{m}) = \{\cdots, \omega_0, \cdots, \omega_1, \cdots\}$
- $\textbf{AON-DPA}(\hat{k}) = \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_0\right) - \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_1\right)$.

Choose $\mathbf{f} = \mathrm{Id}$ and $\mathbf{g} = \mathrm{Id}$. In fact, just a rewriting!

PPA reduction

- $\alpha_0 = 1$, $\alpha_1 = -1$ and $\alpha_i = 0$ for every $\omega_i \in \mathrm{Im}(\mathbf{m}) - \{\omega_0, \omega_1\}$
- $\textbf{AON-DPA}(\hat{k}) = \alpha_0 \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_0\right) + \alpha_1 \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_1\right) + \sum_{i \neq 0,1} 0 \cdot \alpha_1 \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = w_i\right) = \textbf{PPA}_{(\alpha_i)_i}(\hat{k})$

Oberthur Technologies

generalized DPA

generalized DPA

- $\mathrm{Im}(m) = \cdots \cup \Omega_0 \cup \cdots \cup \Omega_1 \cup \cdots$
- $\textbf{G-DPA}(\hat{k}) = \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} \in \Omega_0\right) - \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} \in \Omega_1\right)$.

Oberthur Technologies

generalized DPA

generalized DPA

- $\mathrm{Im}(m) = \cdots \cup \Omega_0 \cup \cdots \cup \Omega_1 \cup \cdots$
- $\textbf{G-DPA}(\hat{k}) = \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} \in \Omega_0\right) - \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} \in \Omega_1\right)$.

Choose $\mathbf{f} = \mathrm{Id}$ and $\mathbf{g} = \mathrm{Id}$. In fact, just a rewriting!

PPA reduction

$$\textbf{G-DPA}(\hat{k}) =$$
$$\sum_{\omega \in \Omega_0} \frac{\widehat{\Pr}\left(M_{\hat{k}} = \omega\right)}{\widehat{\Pr}\left(M_{\hat{k}} \in \Omega_0\right)} \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega\right) - \sum_{\omega \in \Omega_1} \frac{\widehat{\Pr}\left(M_{\hat{k}} = \omega\right)}{\widehat{\Pr}\left(M_{\hat{k}} \in \Omega_1\right)} \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega\right)$$
$$+ \sum_{\omega \in \mathrm{Im}(\mathbf{m}) \setminus \Omega_0 \cup \Omega_1} 0 \cdot \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega\right) = \textbf{PPA}_{(\alpha_i)_i}(\hat{k})$$

What about the PPA distinguisher?

PPA

- $\mathrm{Im}(\mathbf{m}) = \{\omega_i;\ i\}$.
- $\mathbf{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \mathrm{Im}(\mathbf{m})} \alpha_i \cdot \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_i\right)$.

What about the PPA distinguisher?

PPA

- $\mathrm{Im}(\mathbf{m}) = \{\omega_i;\ i\}$.
- $\mathbf{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \mathrm{Im}(\mathbf{m})} \alpha_i \cdot \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_i\right)$.

- After defining $\mathbf{f}(\omega_i) = \frac{\alpha_i}{\widehat{\mathrm{Pr}}\left(M_{\hat{k}} = \omega_i\right)}$ and $M'_{\hat{k}} = \mathbf{f}(M_{\hat{k}})$ we get:

$$\mathbf{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \mathrm{Im}(\mathbf{m})} \mathbf{f}(\omega_i) \cdot \widehat{\mathrm{Pr}}\left(M_{\hat{k}} = \omega_i\right) \cdot \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} = \omega_i\right)$$

$$= \sum_{\alpha \in \mathrm{Im}(\mathbf{f})} \alpha \cdot \widehat{\mathrm{Pr}}\left(M_{\hat{k}} \in \mathbf{f}^{-1}(\alpha)\right) \cdot \widehat{\mathbb{E}}\left(L \mid M_{\hat{k}} \in \mathbf{f}^{-1}(\alpha)\right)$$

$$= \sum_{\alpha \in \mathrm{Im}(\mathbf{f})} \widehat{\mathrm{Pr}}\left(M'_{\hat{k}} = \alpha\right) \cdot \widehat{\mathbb{E}}\left(\alpha \cdot L \mid M'_{\hat{k}} = \alpha\right) = \widehat{\mathbb{E}}\left(LM'_{\hat{k}}\right)$$

Oberthur Technologies

CPA

On the other side, the CPA distinguisher for the same model function $\mathbf{m}' = \mathbf{f} \circ \mathbf{m}$ gives:

$$\begin{aligned}
\mathbf{CPA}(\hat{k}) &= \frac{\widehat{\mathbb{E}}\left(LM'_{\hat{k}}\right) - \widehat{\mathbb{E}}(L)\widehat{\mathbb{E}}\left(M'_{\hat{k}}\right)}{\widehat{\sigma}(L)\,\widehat{\sigma}\left(M'_{\hat{k}}\right)} \\
&= \frac{1}{\widehat{\sigma}(L)\,\widehat{\sigma}\left(M'_{\hat{k}}\right)} \cdot \widehat{\mathbb{E}}\left(LM'_{\hat{k}}\right) - \frac{\widehat{\mathbb{E}}(L)\widehat{\mathbb{E}}\left(M'_{\hat{k}}\right)}{\widehat{\sigma}(L)\,\widehat{\sigma}\left(M'_{\hat{k}}\right)} \\
&= a \cdot \widehat{\mathbb{E}}\left(LM'_{\hat{k}}\right) + b
\end{aligned}$$

CPA and PPA are SCA-equivalent

From

$$\mathbf{PPA}_{(\alpha_i)_i}(\hat{k}) = \widehat{\mathbb{E}}\left(LM'_{\hat{k}}\right)$$

and

$$\mathbf{CPA}(\hat{k}) = a \cdot \widehat{\mathbb{E}}\left(LM'_{\hat{k}}\right) + b$$

we deduce that the two attacks are equivalent thanks to a change of model $\mathbf{m} \rightarrow \mathbf{m}' = \mathbf{f} \circ \mathbf{m}$.

Oberthur Technologies

Model-free Distinguishers

- MIA
  - Requires non-bijective function as sensitive variable
  - Very expensive computationnal cost (pdf estimation)
  - Less efficient than correlation-based attacks

Oberthur Technologies

Model-free Distinguishers

- MIA
  - Requires non-bijective function as sensitive variable
  - Very expensive computationnal cost (pdf estimation)
  - Less efficient than correlation-based attacks
- Linear regression

Oberthur Technologies

Linear Regression

Input

- A set of N input data $(x_i)_i$
  - for us $(p_i)_i$
- A set of N observations
  - in our case $(\ell_{k,i})_i$
- A set of $n < N$ basis functions $(g_j)_j$
  - For instance: $n = 9$, $g_0(x) = 1$ and $g_j(p_i) = v_{\hat{k},i}[j]$ the j^{th} bit of $v_{\hat{k},i}$

Oberthur Technologies

Linear Regression

Input

- A set of N input data $(x_i)_i$
  - for us $(p_i)_i$
- A set of N observations
  - in our case $(\ell_{k,i})_i$
- A set of $n < N$ basis functions $(g_j)_j$
  - For instance: $n = 9$, $g_0(x) = 1$ and $g_j(p_i) = v_{\hat{k},i}[j]$ the j^{th} bit of $v_{\hat{k},i}$

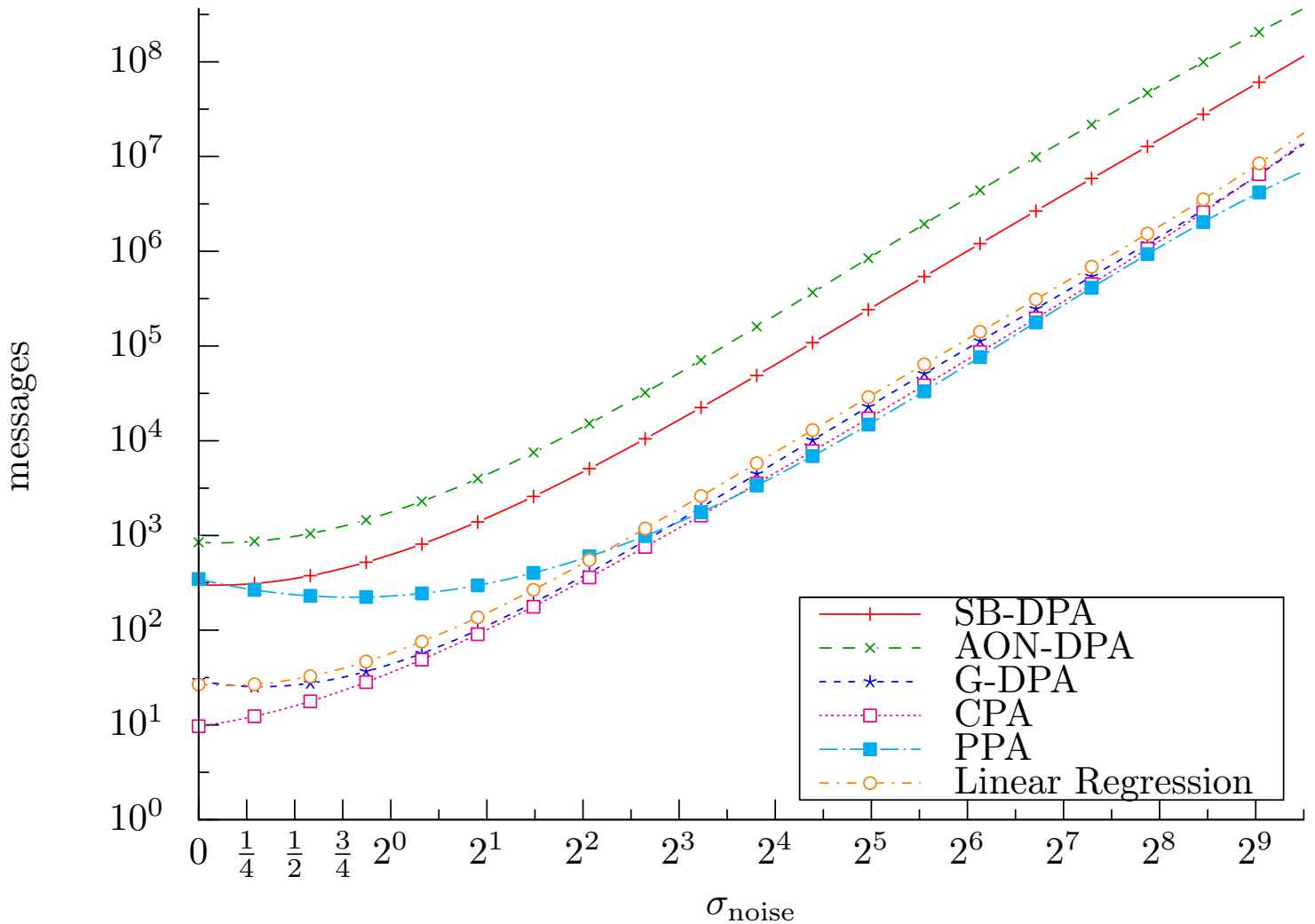
Output

- n values $(\hat{\beta}_i)_i \in \mathbb{R}$ that minimizes the Euclidean Distance between the vector $\left(\sum_j \hat{\beta}_j g_j(x_i)\right)_i$ and the vector $(\ell_{k,i})_i$ *i.e.*

$$(\hat{\beta}_i)_i = \min_{(\beta_i)_i} \sum_i \left(\ell_{k,i} - \sum_j \beta_j \cdot v_{\hat{k},i}\right)^2 .$$

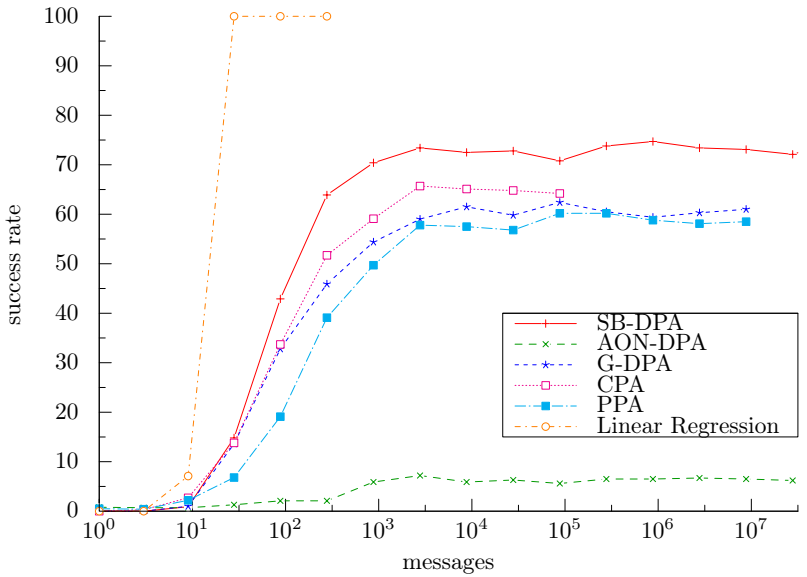
Oberthur Technologies

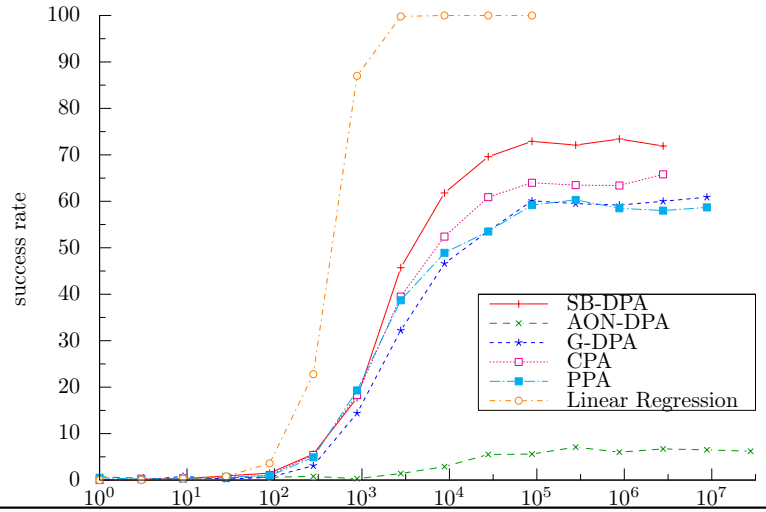
Perfect Model Scenario

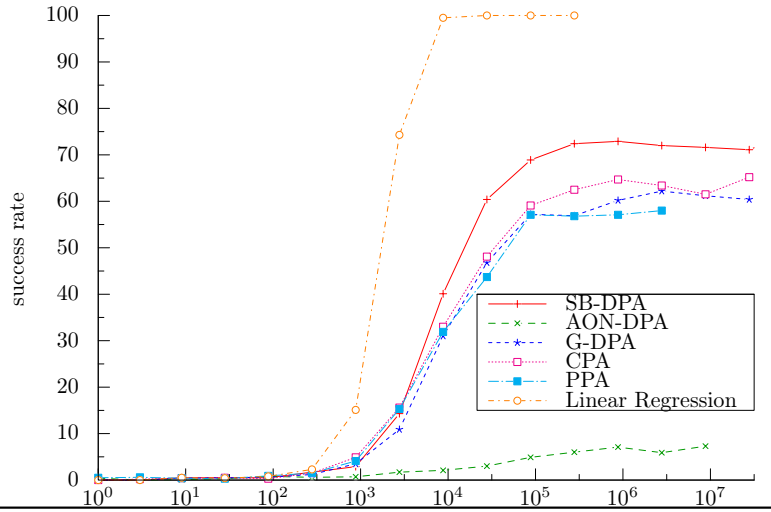


Random Linear Leakage Scenario

$$\delta(x) = \varepsilon_0 + \sum_i^n \varepsilon_i x_i$$







Oberthur Technologies

Outline

Oberthur Technologies

To conclude

- Linear Correlation
  - Only One distinguisher is statistically sound: CPA
  - "Enhance" CPA equals to refine the model
  - It's a matter of model

Oberthur Technologies

To conclude

- Linear Correlation
  - Only One distinguisher is statistically sound: CPA
  - "Enhance" CPA equals to refine the model
  - It's a matter of model
- Linear Estimation
  - Exhibit the model is the good way
  - MIA is the theoretically perfect distinguisher
  - Linear regression seems to be the pratically perfect distinguisher

Oberthur Technologies

Further works

- What about non linear leakages
  - Soundness in real life ?
  - Behavior of former distinguishers.
  - New statistical tools (*e.g.* non linear regression).
- Multivariate attacks
- A way to template attacks ?

Oberthur Technologies

Au revoir

That's all Folks!