

# 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



## 1 Introduction

- Definition
- From beginning...
- ...to nowadays
- Problematics
- Motivations

## 2 Description

- Preliminaries
- Description

## 3 Our Work - Analyses

- All DPAs reduce to PPA
- From PPA to CPA
- Model-Free
- Experiments

## 4 Conclusion



## 1 Introduction

- Definition
- From beginning...
- ...to nowadays
- Problematics
- Motivations

## 2 Description

- Preliminaries
- Description

## 3 Our Work - Analyses

- All DPAs reduce to PPA
- From PPA to CPA
- Model-Free
- Experiments

## 4 Conclusion



# Side Channel Analyses / Attacks

## Attacker knowledge

Kerckhoff' principle

Black Box model Only inputs and outputs

White Box model All is known



# Side Channel Analyses / Attacks

## Attacker knowledge

Kerckhoff's principle

**Black Box model** Only inputs and outputs

**White Box model** All is known

**Grey Box model** Some intermediate values are known



# Side Channel Analyses / Attacks

## Attacker knowledge

Kerckhoff' principle

**Black Box model** Only inputs and outputs

**White Box model** All is known

**Grey Box model** Some intermediate values are known

## SCA principle

- Observe environment degradation
  - Obtain intermediate values
- ⇒ SCA is in Grey Box model

## Government

- 1943 US: Oscilloscope used to decypher teletype-encryption machine
- 1956 UK: Acoustic attack against Egyptian Hagelin cipher machines
- 1973 TEMPEST: A signal problem
- 1985 DE: Van Eck phreaking: eletromagnetic emissions of CRT and LCD



## Initial Works

1996 Timming Attack by Kocher *et al.*

1998 Single-bit DPA by Kocher *et al.*





## Initial Works

1996 Timming Attack by Kocher *et al.*

1998 Single-bit DPA by Kocher *et al.*

## Improvements

1999 Multi-bit DPA by Messerges *et al.*

2000 High-Order DPA by Messerges *et al.*

2002 Template Attacks by Chari *et al.*

2003 CPA by Brier *et al.*



- 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



- 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



- 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



- 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



- 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



- 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



- 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





- 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



- 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



- 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



- 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



- 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



- 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



- 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



- 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



- 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



- 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



- 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



- 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



- 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

- 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



- 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, ...

- 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)





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

## Linear correlation

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



# 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?



## 1 Introduction

- Definition
- From beginning...
- ...to nowadays
- Problematics
- Motivations

## 2 Description

- Preliminaries
- Description

## 3 Our Work - Analyses

- All DPAs reduce to PPA
- From PPA to CPA
- Model-Free
- Experiments

## 4 Conclusion



- 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.

⇒ We rule on how to lead a linear univariate side-channel attack!

- (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  $L = \delta(V_k) + B$ .



# 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

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

The r.v. corresponding to  $m_{\hat{k},i}$  is denoted by  $M_{\hat{k}}$ .

4. **Distinguisher Selection** : Choose a statistical distinguisher  $\Delta$ .
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  $\Delta_{\hat{k}}$ .



## What differs from an attack to another

- The distinguisher  $\Delta$
- The model  $m$

→ How to choose the distinguisher?

→ How to choose the model?

⇒ Link between the two questions?



# 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  $S$ .
- $\text{Im}(\mathbf{m}) = \{w_0, w_1\}$
- (e.g.  $w_0 = 0$  and  $w_1 = 1$ ).
- $\Delta_{\hat{k}} = \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_0) - \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_1) = \text{SB-DPA}(\hat{k})$ .



# 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  $S$ .
- $\text{Im}(\mathbf{m}) = \{w_0, w_1\}$
- (e.g.  $w_0 = 0$  and  $w_1 = 1$ ).
- $\Delta_{\hat{k}} = \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_0) - \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_1) = \text{SB-DPA}(\hat{k})$ .

## all-or-nothing DPA

- Example:  $\mathbf{m}(v_{\hat{k},i}) = \text{HW}(S(p_i \oplus \hat{k}))$ .
- $\text{Im}(\mathbf{m}) = \{\dots, w_0, \dots, w_1, \dots\}$
- (e.g.  $\text{Im}(\mathbf{m}) = \{0, \dots, 8\}$  and  $w_0 = 0$  and  $w_1 = 8$ ).
- $\Delta_{\hat{k}} = \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_0) - \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_1) = \text{AON-DPA}(\hat{k})$ .



## generalized DPA

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

# Partition Power Analysis

## PPA

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

# Correlation Power Analysis

## CPA

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

## Target Uniformity

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

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



# 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  $\hat{\mathbb{E}}(V_{\hat{k}})$  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.:

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

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

## 1 Introduction

- Definition
- From beginning...
- ...to nowadays
- Problematics
- Motivations

## 2 Description

- Preliminaries
- Description

## 3 Our Work - Analyses

- All DPAs reduce to PPA
- From PPA to CPA
- Model-Free
- Experiments

## 4 Conclusion



$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## single-bit DPA

- $\text{Im}(\mathbf{m}) = \{w_0, w_1\}$
- $\text{SB-DPA}(\hat{k}) = \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_0) - \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_1)$



# single-bit DPA

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## single-bit DPA

- $\text{Im}(\mathbf{m}) = \{w_0, w_1\}$
- $\text{SB-DPA}(\hat{k}) = 1 \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_0) + -1 \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_1)$

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## single-bit DPA

- $\text{Im}(\mathbf{m}) = \{w_0, w_1\}$
- $\text{SB-DPA}(\hat{k}) = \underbrace{1}_{\alpha_0} \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_0) + \underbrace{-1}_{\alpha_1} \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = w_1)$

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

# all-or-nothing DPA

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## all-or-nothing DPA

- $\text{Im}(\mathbf{m}) = \{\dots, \omega_0, \dots, \omega_1, \dots\}$
- $\text{AON-DPA}(\hat{k}) =$   

$$\hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_0) - \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_1)$$

# all-or-nothing DPA

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## all-or-nothing DPA

- $\text{Im}(\mathbf{m}) = \{\dots, \omega_0, \dots, \omega_1, \dots\}$

- $\text{AON-DPA}(\hat{k}) =$

$$1 \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_0) + -1 \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_1)$$

# all-or-nothing DPA

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## all-or-nothing DPA

- $\text{Im}(\mathbf{m}) = \{\dots, \omega_0, \dots, \omega_1, \dots\}$

- $\text{AON-DPA}(\hat{k}) =$

$$1 \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_0) + -1 \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_1) + \sum_{i \neq 0,1} 0 \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## all-or-nothing DPA

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## all-or-nothing DPA

$$\blacksquare \text{Im}(\mathbf{m}) = \{\cdots, \omega_0, \cdots, \omega_1, \cdots\}$$

$$\blacksquare \text{AON-DPA}(\hat{k}) =$$

$$\underbrace{1}_{\alpha_0} \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_0) + \underbrace{-1}_{\alpha_1} \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_1) + \sum_{i \neq 0,1} \underbrace{0}_{\alpha_i} \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

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

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## generalized DPA

- $\text{Im}(\mathbf{m}) = \dots \cup \Omega_0 \cup \dots \cup \Omega_1 \cup \dots$

- $\text{G-DPA}(\hat{k}) =$

$$\hat{\mathbb{E}}(L \mid M_{\hat{k}} \in \Omega_0) - \hat{\mathbb{E}}(L \mid M_{\hat{k}} \in \Omega_1)$$

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## generalized DPA

- $\text{Im}(\mathbf{m}) = \dots \cup \Omega_0 \cup \dots \cup \Omega_1 \cup \dots$

- $\text{G-DPA}(\hat{k}) =$

$$\sum_{\omega \in \Omega_0} \frac{\widehat{P}_r(M_{\hat{k}} = \omega)}{\widehat{P}_r(M_{\hat{k}} \in \Omega_0)} \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega) - \sum_{\omega \in \Omega_1} \frac{\widehat{P}_r(M_{\hat{k}} = \omega)}{\widehat{P}_r(M_{\hat{k}} \in \Omega_1)} \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega)$$



$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## generalized DPA

- $\text{Im}(\mathbf{m}) = \dots \cup \Omega_0 \cup \dots \cup \Omega_1 \cup \dots$

- $\text{G-DPA}(\hat{k}) =$

$$\sum_{\omega \in \Omega_0} \frac{\widehat{P}_r(M_{\hat{k}} = \omega)}{\widehat{P}_r(M_{\hat{k}} \in \Omega_0)} \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega) - \sum_{\omega \in \Omega_1} \frac{\widehat{P}_r(M_{\hat{k}} = \omega)}{\widehat{P}_r(M_{\hat{k}} \in \Omega_1)} \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega)$$

$$+ \sum_{\omega \in \text{Im}(\mathbf{m}) \setminus \Omega_0 \cup \Omega_1} 0 \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega)$$

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

## generalized DPA

- $\text{Im}(\mathbf{m}) = \dots \cup \Omega_0 \cup \dots \cup \Omega_1 \cup \dots$

- $\text{G-DPA}(\hat{k}) =$

$$\begin{aligned} & \sum_{\omega \in \Omega_0} \underbrace{\frac{\widehat{P}_r(M_{\hat{k}}=\omega)}{\widehat{P}_r(M_{\hat{k}} \in \Omega_0)}}_{\alpha_i, \omega_i \in \Omega_0} \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega) - \sum_{\omega \in \Omega_1} \underbrace{\frac{\widehat{P}_r(M_{\hat{k}}=\omega)}{\widehat{P}_r(M_{\hat{k}} \in \Omega_1)}}_{\alpha_i, \omega_i \in \Omega_1} \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega) \\ & + \sum_{\omega \in \text{Im}(\mathbf{m}) \setminus \Omega_0 \cup \Omega_1} \underbrace{0}_{\alpha_i, \omega_i \notin \Omega_0 \cup \Omega_1} \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega) \end{aligned}$$

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



# What about the PPA distinguisher?

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$



# What about the PPA distinguisher?

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

$$\begin{aligned} & \text{PPA}_{(\alpha_i)_i}(\hat{k}) \\ &= \sum_{\omega_i \in \text{Im}(\mathbf{m})} \frac{\alpha_i}{\widehat{\mathbb{P}}_r(M_{\hat{k}} = \omega_i)} \cdot \widehat{\mathbb{P}}_r(M_{\hat{k}} = \omega_i) \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i) \end{aligned}$$

# What about the PPA distinguisher?

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

$$\begin{aligned} & \text{PPA}_{(\alpha_i)_i}(\hat{k}) \\ &= \sum_{\omega_i \in \text{Im}(\mathbf{m})} \underbrace{\frac{\alpha_i}{\widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} = \omega_i)}}_{\mathbf{f}(\omega_i)} \cdot \widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} = \omega_i) \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i) \end{aligned}$$

# What about the PPA distinguisher?

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

$$\begin{aligned}
 & \text{PPA}_{(\alpha_i)_i}(\hat{k}) \\
 &= \sum_{\omega_i \in \text{Im}(\mathbf{m})} \underbrace{\frac{\alpha_i}{\widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} = \omega_i)}}_{\mathbf{f}(\omega_i)} \cdot \widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} = \omega_i) \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i) \\
 &= \sum_{\alpha \in \text{Im}(\mathbf{f})} \alpha \cdot \widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} \in \mathbf{f}^{-1}(\alpha)) \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} \in \mathbf{f}^{-1}(\alpha))
 \end{aligned}$$

# What about the PPA distinguisher?

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

$$\begin{aligned}
 & \text{PPA}_{(\alpha_i)_i}(\hat{k}) \\
 &= \sum_{\omega_i \in \text{Im}(\mathbf{m})} \underbrace{\frac{\alpha_i}{\widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} = \omega_i)}}_{\mathbf{f}(\omega_i)} \cdot \widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} = \omega_i) \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i) \\
 &= \sum_{\alpha \in \text{Im}(\mathbf{f})} \alpha \cdot \widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} \in \mathbf{f}^{-1}(\alpha)) \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} \in \mathbf{f}^{-1}(\alpha)) \\
 &= \sum_{\alpha \in \text{Im}(\mathbf{f})} \widehat{\mathbb{P}}_{\mathbf{r}}(\mathbf{f}(M_{\hat{k}}) = \alpha) \cdot \hat{\mathbb{E}}(\alpha \cdot L \mid \mathbf{f}(M_{\hat{k}}) = \alpha)
 \end{aligned}$$



# What about the PPA distinguisher?

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

$$\begin{aligned}
 & \text{PPA}_{(\alpha_i)_i}(\hat{k}) \\
 &= \sum_{\omega_i \in \text{Im}(\mathbf{m})} \underbrace{\frac{\alpha_i}{\widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} = \omega_i)}}_{\mathbf{f}(\omega_i)} \cdot \widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} = \omega_i) \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i) \\
 &= \sum_{\alpha \in \text{Im}(\mathbf{f})} \alpha \cdot \widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} \in \mathbf{f}^{-1}(\alpha)) \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} \in \mathbf{f}^{-1}(\alpha)) \\
 &= \sum_{\alpha \in \text{Im}(\mathbf{f})} \widehat{\mathbb{P}}_{\mathbf{r}}(\underbrace{\mathbf{f}(M_{\hat{k}})}_{M'_{\hat{k}}} = \alpha) \cdot \hat{\mathbb{E}}(\alpha \cdot L \mid \underbrace{\mathbf{f}(M_{\hat{k}})}_{M'_{\hat{k}}} = \alpha)
 \end{aligned}$$



# What about the PPA distinguisher?

$$\text{PPA}_{(\alpha_i)_i}(\hat{k}) = \sum_{\omega_i \in \text{Im}(\mathbf{m})} \alpha_i \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i)$$

$$\begin{aligned}
 & \text{PPA}_{(\alpha_i)_i}(\hat{k}) \\
 &= \sum_{\omega_i \in \text{Im}(\mathbf{m})} \underbrace{\frac{\alpha_i}{\widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} = \omega_i)}}_{\mathbf{f}(\omega_i)} \cdot \widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} = \omega_i) \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} = \omega_i) \\
 &= \sum_{\alpha \in \text{Im}(\mathbf{f})} \alpha \cdot \widehat{\mathbb{P}}_{\mathbf{r}}(M_{\hat{k}} \in \mathbf{f}^{-1}(\alpha)) \cdot \hat{\mathbb{E}}(L \mid M_{\hat{k}} \in \mathbf{f}^{-1}(\alpha)) \\
 &= \sum_{\alpha \in \text{Im}(\mathbf{f})} \widehat{\mathbb{P}}_{\mathbf{r}}(\underbrace{\mathbf{f}(M_{\hat{k}})}_{M'_{\hat{k}}} = \alpha) \cdot \hat{\mathbb{E}}(\alpha \cdot L \mid \underbrace{\mathbf{f}(M_{\hat{k}})}_{M'_{\hat{k}}} = \alpha) \\
 &= \hat{\mathbb{E}}(LM'_{\hat{k}})
 \end{aligned}$$

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

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

# CPA and PPA are SCA-equivalent

---

From

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

and

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

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

# Model-free Distinguishers

---

## ■ MIA

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

# Model-free Distinguishers

---

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



# 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  $g_j(p_i) = v_{k,i}[j]$  the  $j^{\text{th}}$  bit of  $v_{k,i}$

# 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  $j^{\text{th}}$  bit of  $v_{\hat{k},i}$

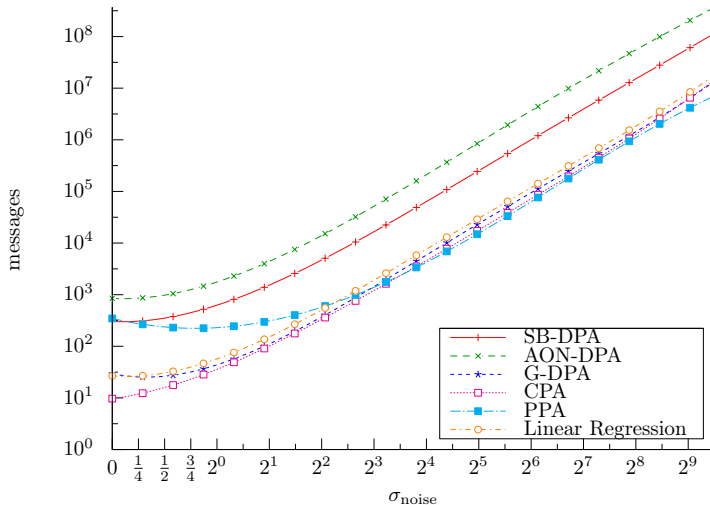
## Output

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

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



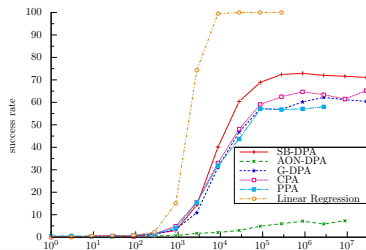
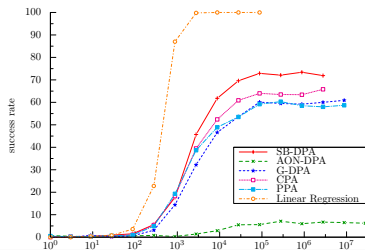
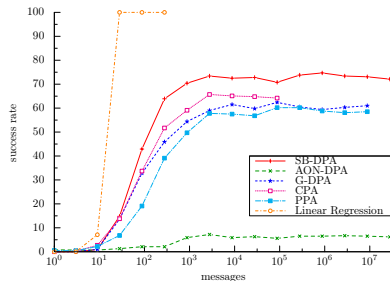
# Perfect Model Scenario





# Random Linear Leakage Scenario

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



## 1 Introduction

- Definition
- From beginning...
- ...to nowadays
- Problematics
- Motivations

## 2 Description

- Preliminaries
- Description

## 3 Our Work - Analyses

- All DPAs reduce to PPA
- From PPA to CPA
- Model-Free
- Experiments

## 4 Conclusion



## ■ Linear Correlation

- ▶ Only One distinguisher is statistically sound: CPA
- ▶ “Enhance” CPA equals to refine the model
- ▶ It's a matter of model



## ■ 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



- 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?



That's all Folks!

