Provably Secure S-Box Implementation Based on Fourier Transform

Emmanuel Prouff, Christophe Giraud & Sébastien Aumônier

Oberthur Card Systems

Overview

- Differential Power Analysis on block ciphers
- Notion of DPA-resistance
- A new method to protect S-Box
- Application to AES
- Conclusion

DPA on block ciphers

- Correlate the intermediate values and the power consumption.

DPA on block ciphers

- Correlate the intermediate values and the power consumption.
- Countermeasures:

DPA on block ciphers

- Correlate the intermediate values and the power consumption.
- Countermeasures:
  - Linear operations: simple

DPA on block ciphers

- Correlate the intermediate values and the power consumption.
- Countermeasures:
  - Linear operations: simple
  - Non-linear parts (*i.e.* S-Box): tricky

DPA on block ciphers

- Correlate the intermediate values and the power consumption.
- Countermeasures:
  - Linear operations: simple
  - Non-linear parts (*i.e.* S-Box): tricky
    - Re-computation method

Oberthur Card Systems

DPA on block ciphers

- Correlate the intermediate values and the power consumption.
- Countermeasures:
  - Linear operations: simple
  - Non-linear parts (*i.e.* S-Box): tricky
    - Re-computation method
    - Duplication method

DPA on block ciphers

- Correlate the intermediate values and the power consumption.
- Countermeasures:
  - Linear operations: simple
  - Non-linear parts (*i.e.* S-Box): tricky
    - Re-computation method
    - Duplication method
    - S-Box secure calculation

Oberthur Card Systems

Notion of DPA-resistance

- Let $\mathcal{M}$ denote a method to implement the S-Box access using a value depending of a round-key as input.

Oberthur Card Systems

Notion of DPA-resistance

- Let $\mathcal{M}$ denote a method to implement the S-Box access using a value depending of a round-key as input.
- The *Advantage of an adversary* over $\mathcal{M}$ is the number of round-keys eliminated by DPA.

Oberthur Card Systems

Notion of DPA-resistance

- Let $\mathcal{M}$ denote a method to implement the S-Box access using a value depending of a round-key as input.
- The *Advantage of an adversary* over $\mathcal{M}$ is the number of round-keys eliminated by DPA.
- $\mathcal{M}$ is DPA-resistant $\Longleftrightarrow Adv(\mathcal{M}) = 0$.

Oberthur Card Systems

Notion of DPA-resistance

- Let $\mathcal{M}$ denote a method to implement the S-Box access using a value depending of a round-key as input.
- The *Advantage of an adversary* over $\mathcal{M}$ is the number of round-keys eliminated by DPA.
- $\mathcal{M}$ is DPA-resistant $\Longleftrightarrow Adv(\mathcal{M}) = 0$.
- $Adv(\mathcal{M}) = 0 \Longleftrightarrow$ all the variables at the unit level of $\mathcal{M}$ are independent from the sensitive input.

Oberthur Card Systems

Generalities about the Fourier Transform

Generalities about the Fourier Transform

- The Fourier Transform $\widehat{F}$ of a function F defined over $\mathbb{F}_2^n$ is defined by:

$$\forall X \in \mathbb{F}_2^n,\ \widehat{F}(X) = \sum_{A \in \mathbb{F}_2^n} F(A)(-1)^{A \cdot X}$$

where $A \cdot X = \sum_{i \in \{0,\dots,n-1\}} A_i \cdot X_i \mod 2$.

Oberthur Card Systems

Generalities about the Fourier Transform

- The Fourier Transform $\widehat{F}$ of a function F defined over $\mathbb{F}_2^n$ is defined by:

$$\forall X \in \mathbb{F}_2^n,\ \widehat{F}(X) = \sum_{A \in \mathbb{F}_2^n} F(A)(-1)^{A \cdot X}$$

where $A \cdot X = \sum_{i \in \{0,\ldots,n-1\}} A_i \cdot X_i \mod 2$.

- As $\widehat{\widehat{F}} = 2^n F$, we have:

$$\forall X \in \mathbb{F}_2^n,\ F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A \cdot X}$$

DPA-resistant S-Box Implementation

$$\forall X \in \mathbb{F}_2^n,\ F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A \cdot X}$$

Oberthur Card Systems

DPA-resistant S-Box Implementation

$$\forall X \in \mathbb{F}_2^n,\ F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A \cdot X}$$

- Securely compute $F(X)$ from $\widetilde{X} = X \oplus R_1$ and R_1?

Oberthur Card Systems

DPA-resistant S-Box Implementation

$$\forall X \in \mathbb{F}_2^n,\ F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A \cdot X}$$

- Securely compute $F(X)$ from $\widetilde{X} = X \oplus R_1$ and R_1?
- Noticing that $A \cdot X = A \cdot \widetilde{X} \oplus R_1 \cdot (\widetilde{X} \oplus A) \oplus \widetilde{X} \cdot R_1$

Oberthur Card Systems

DPA-resistant S-Box Implementation

$$\forall X \in \mathbb{F}_2^n,\ F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A \cdot X}$$

- Securely compute $F(X)$ from $\widetilde{X} = X \oplus R_1$ and R_1?
- Noticing that $A \cdot X = A \cdot \widetilde{X} \oplus R_1 \cdot (\widetilde{X} \oplus A) \oplus \widetilde{X} \cdot R_1$
- We obtain:

$$(-1)^{\widetilde{X} \cdot R_1} F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A \cdot \widetilde{X} \oplus R_1 \cdot (\widetilde{X} \oplus A)}$$

Oberthur Card Systems

DPA-resistant S-Box Implementation

$$\forall X \in \mathbb{F}_2^n,\ F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A \cdot X}$$

- Securely compute $F(X)$ from $\widetilde{X} = X \oplus R_1$ and R_1?
- Noticing that $A \cdot X = A \cdot \widetilde{X} \oplus R_1 \cdot (\widetilde{X} \oplus A) \oplus \widetilde{X} \cdot R_1$
- We obtain:

$$(-1)^{\widetilde{X} \cdot R_1} F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A \cdot \widetilde{X} \oplus R_1 \cdot (\widetilde{X} \oplus A)}$$

- Mask correction performed *on-the-fly*.

DPA-resistant S-Box Implementation

$$(-1)^{\widetilde{X}\cdot R_1} F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X} \oplus \; R_1\cdot(\widetilde{X} \; \oplus A)}$$

DPA-resistant S-Box Implementation

$$(-1)^{\widetilde{X}\cdot R_1} F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot \widetilde{X} \oplus \ R_1 \cdot (\widetilde{X} \ \oplus A)}$$

- Weaknesses:

DPA-resistant S-Box Implementation

$$(-1)^{\widetilde{X}\cdot R_1} F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X} \oplus \ R_1\cdot(\widetilde{X} \ \oplus A)}$$

- Weaknesses:
  - $R_1 \cdot \widetilde{X} = 0$ when $X = 11 \cdots 11$

DPA-resistant S-Box Implementation

$$(-1)^{\widetilde{X}\cdot R_1} F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X}\oplus \boxed{R_1\cdot(\widetilde{X}} \oplus A)}$$

- Weaknesses:
  - $R_1 \cdot \widetilde{X} = 0$ when $X = 11 \cdots 11$

DPA-resistant S-Box Implementation

$$(-1)^{\widetilde{X}\cdot R_1} F(X) = \frac{1}{2^n} \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X}\oplus \boxed{R_1\cdot(\widetilde{X}} \oplus A)}$$

- Weaknesses:
  - $R_1 \cdot \widetilde{X} = 0$ when $X = 11\cdots 11$
  - $(-1)^{\widetilde{X}\cdot R_1} F(X) = \pm F(X)$

DPA-resistant S-Box Implementation

$$(-1)^{\widetilde{X}\cdot R_1} F(X) = \frac{1}{2^n} \boxed{\sum_{A\in\mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X}\oplus \boxed{R_1\cdot(\widetilde{X}} \oplus A)}}$$

- Weaknesses:
  - $R_1 \cdot \widetilde{X} = 0$ when $X = 11\cdots 11$
  - $(-1)^{\widetilde{X}\cdot R_1} F(X) = \pm F(X)$

DPA-resistant S-Box Implementation

$$(-1)^{\widetilde{X}\cdot R_1} F(X) = \frac{1}{2^n} \boxed{\sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X} \oplus \boxed{R_1\cdot(\widetilde{X}} \oplus A)}}$$

- Weaknesses:
  - $R_1 \cdot \widetilde{X} = 0$ when $X = 11 \cdots 11$
  - $(-1)^{\widetilde{X}\cdot R_1} F(X) = \pm F(X)$
- New formula:

$$\boxed{(-1)^{(\widetilde{X}\oplus R_2)\cdot R_1} F(X) + R_3 = \left\lfloor \frac{1}{2^n} \left(R' + \sum_{A \in \mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X} \oplus R_1\cdot(\widetilde{X}\oplus A \oplus R_2)} \right) \right\rfloor}$$

where $R_2, R_3, R_4 \in \mathbb{F}_2^n$ and $R' = 2^n R_3 + R_4$.

DPA-resistant S-Box Implementation

$$(-1)^{(\widetilde{X}\oplus R_2)\cdot R_1} F(X) + R_3 = \left\lfloor \frac{1}{2^n}\left(R' + \sum_{A\in\mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X}\oplus R_1\cdot(\widetilde{X}\oplus A\oplus R_2)} \right) \right\rfloor$$

Oberthur Card Systems

DPA-resistant S-Box Implementation

$$(-1)^{(\widetilde{X}\oplus R_2)\cdot R_1} F(X) + R_3 = \left\lfloor \frac{1}{2^n}\left(R' + \sum_{A\in\mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X}\oplus R_1\cdot(\widetilde{X}\oplus A\oplus R_2)}\right)\right\rfloor$$

- We obtain $\pm F(X) + R_3$ and we want $F(X) \oplus R_3$

DPA-resistant S-Box Implementation

$$(-1)^{(\widetilde{X}\oplus R_2)\cdot R_1} F(X) + R_3 = \left\lfloor \frac{1}{2^n} \left(R' + \sum_{A\in\mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X}\oplus R_1\cdot(\widetilde{X}\oplus A\oplus R_2)} \right) \right\rfloor$$

- We obtain $\pm F(X) + R_3$ and we want $F(X) \oplus R_3$
- Procedure based on Goubin's method:

$$\pm F(X) + R_3 \mapsto F(X) \oplus R_3$$

Oberthur Card Systems

DPA-resistant S-Box Implementation

$$(-1)^{(\widetilde{X}\oplus R_2)\cdot R_1} F(X) + R_3 = \left\lfloor \frac{1}{2^n} \left(R' + \sum_{A\in\mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X}\oplus R_1\cdot(\widetilde{X}\oplus A\oplus R_2)} \right) \right\rfloor$$

- We obtain $\pm F(X) + R_3$ and we want $F(X) \oplus R_3$
- Procedure based on Goubin's method:

$$\pm F(X) + R_3 \mapsto F(X) \oplus R_3$$

- Our new method:

$$(X \oplus R_1, R_1, \widehat{F}) \mapsto (F(X) \oplus R_3, R_3)$$

Oberthur Card Systems

DPA-resistant S-Box Implementation

$$(-1)^{(\widetilde{X}\oplus R_2)\cdot R_1} F(X) + R_3 = \left\lfloor \frac{1}{2^n}\left(R' + \sum_{A\in\mathbb{F}_2^n} \widehat{F}(A)(-1)^{A\cdot\widetilde{X}\oplus R_1\cdot(\widetilde{X}\oplus A\oplus R_2)} \right) \right\rfloor$$

- We obtain $\pm F(X) + R_3$ and we want $F(X) \oplus R_3$
- Procedure based on Goubin's method:

$$\pm F(X) + R_3 \mapsto F(X) \oplus R_3$$

- Our new method:

$$(X \oplus R_1, R_1, \widehat{F}) \mapsto (F(X) \oplus R_3, R_3)$$

- Efficiency: exponential in the dimension of the S-Box

Oberthur Card Systems

Application to AES

Application to AES

- Every operations are linear except the S-Box (inversion in $\mathbb{F}_{2^8}$)

Oberthur Card Systems

Application to AES

- Every operations are linear except the S-Box (inversion in $\mathbb{F}_{2^8}$)
- Transform Masking Method : flaw when accessing the S-Box

Oberthur Card Systems

Application to AES

- Every operations are linear except the S-Box (inversion in $\mathbb{F}_{2^8}$)
- Transform Masking Method : flaw when accessing the S-Box
- Remark: each element of $\mathbb{F}_{2^8}$ can be represented as a linear polynomial over $\mathbb{F}_{2^4}$.

Application to AES

- Every operations are linear except the S-Box (inversion in $\mathbb{F}_{2^8}$)
- Transform Masking Method : flaw when accessing the S-Box
- Remark: each element of $\mathbb{F}_{2^8}$ can be represented as a linear polynomial over $\mathbb{F}_{2^4}$.

$\Rightarrow$ Tower Field Methods

Application to AES

- Every operations are linear except the S-Box (inversion in $\mathbb{F}_{2^8}$)
- Transform Masking Method : flaw when accessing the S-Box
- Remark: each element of $\mathbb{F}_{2^8}$ can be represented as a linear polynomial over $\mathbb{F}_{2^4}$.

$\Rightarrow$ Tower Field Methods

- Down to $\mathbb{F}_{2^4}$ and apply our method to protect inversion

AES: implementation results

Comparison of several methods to protect AES against DPA:

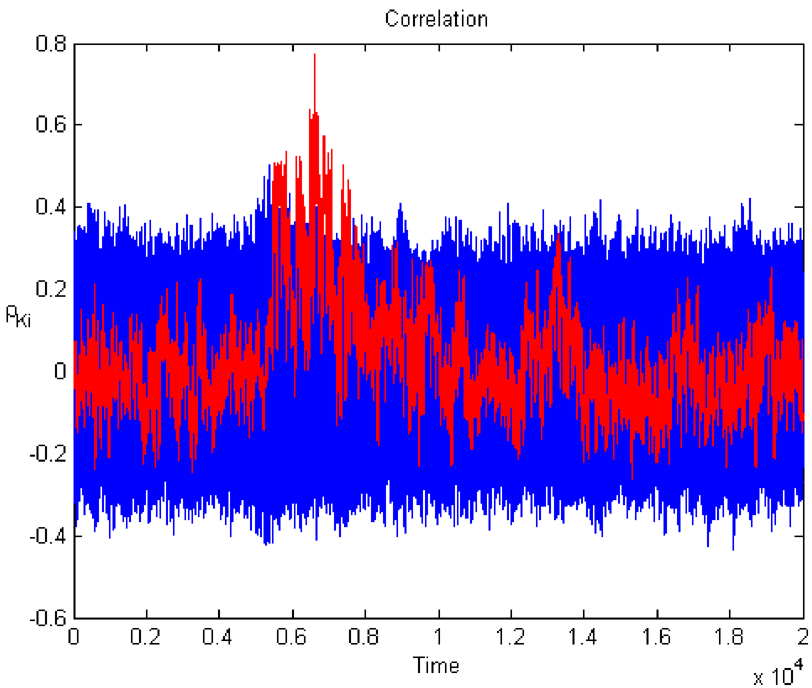
Method	Timings (ms)	RAM (bytes)	ROM (bytes)
Straightforward implementation	5	32	1150
This paper	32	39	3100
Oswald *et al.* (FSE'05)	26	42	3400
Trichina *et al.* (WISA'04)	21	291	3050

AES: practical study

AES: practical study

CPA on straightforward method

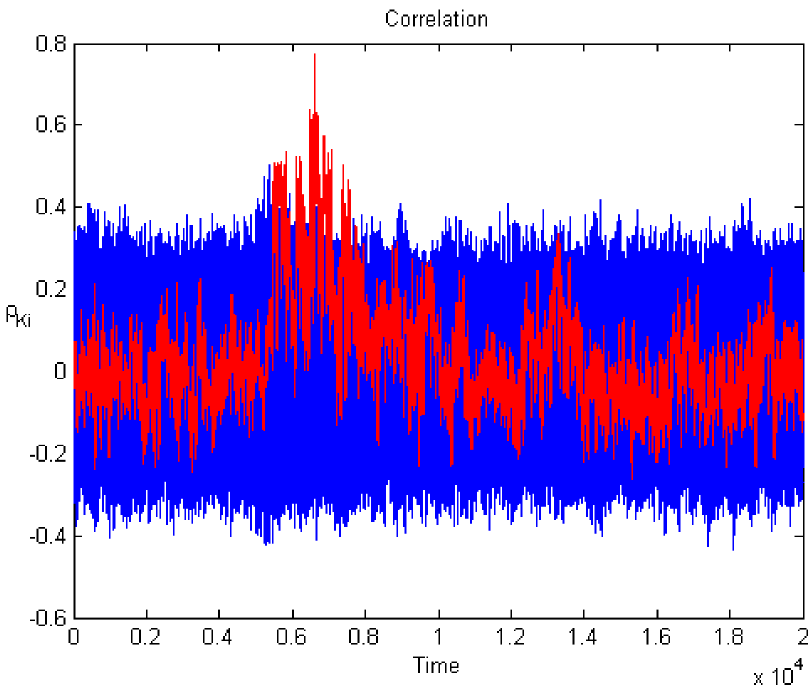
using 100 random plaintexts



AES: practical study

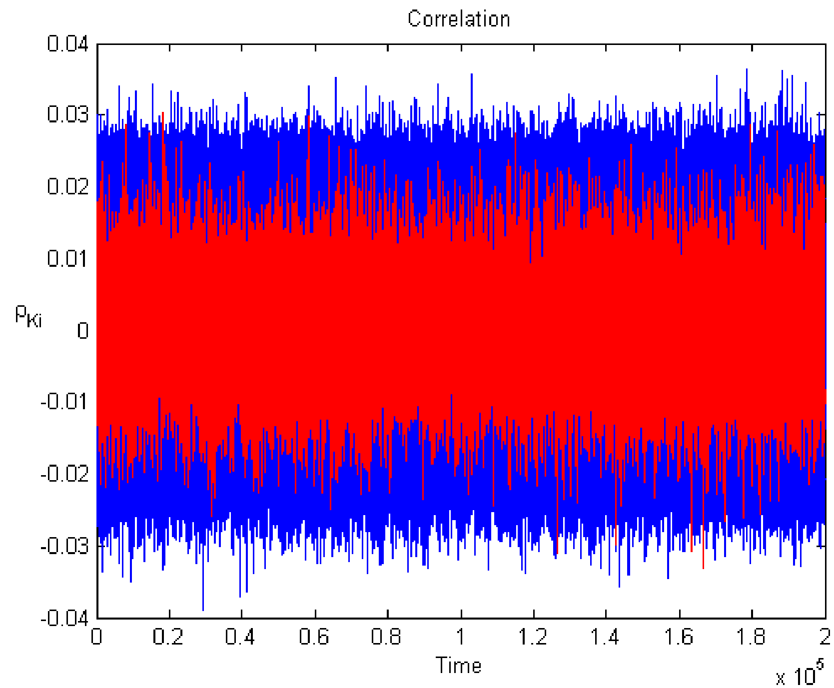
CPA on straightforward method

using 100 random plaintexts



CPA on our method

using $20\,000$ random plaintexts



Oberthur Card Systems

Conclusion

Conclusion

- Alternative method to obtain DPA-resistant S-Box implementations

Conclusion

- Alternative method to obtain DPA-resistant S-Box implementations
- The DPA-resistance is proved

Oberthur Card Systems

Conclusion

- Alternative method to obtain DPA-resistant S-Box implementations
- The DPA-resistance is proved
- Very efficient when working on small fields

Conclusion

- Alternative method to obtain DPA-resistant S-Box implementations
- The DPA-resistance is proved
- Very efficient when working on small fields
- Perspectives:

Conclusion

- Alternative method to obtain DPA-resistant S-Box implementations
- The DPA-resistance is proved
- Very efficient when working on small fields
- Perspectives:
  - Upgrade our security model to take into account High Order DPA

Oberthur Card Systems

Conclusion

- Alternative method to obtain DPA-resistant S-Box implementations
- The DPA-resistance is proved
- Very efficient when working on small fields
- Perspectives:
  - Upgrade our security model to take into account High Order DPA
  - Find other transformations than the Fourier Transform

Oberthur Card Systems