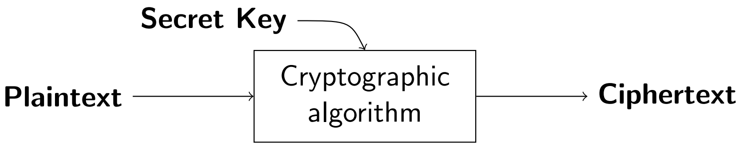
Algebraic Side-Channel Analysis

Jean-Charles Faugère Christopher Goyet Guénaël Renault
équipe SALSA, CNRS/INRIA/LIP6/UPMC, THALES

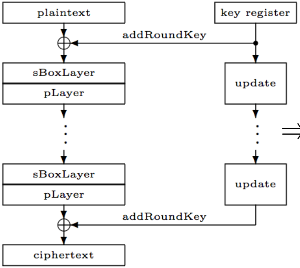
Classical cryptanalysis - symmetric block cipher



Security of the algorithm : cryptosystem seen as ideal mathematical object

- Differential cryptanalysis
- Linear cryptanalysis
- Algebraic cryptanalysis
- ...

Algebraic cryptanalysis



$$\Rightarrow \left\{ \begin{array}{l} x_1x_2 + x_1k_2 + x_1 + x_2k_1 + x_3 + x_4s_4 + \\ \quad s_1s_4 + s_3s_4 + s_3 + s_4k_4 + s_4 + k_1k_2 + k_1 + k_3, \\ x_4 + s_1s_3 + s_2 + s_4 + k_4 + 1, \\ \vdots \\ s_{21} + s_{52}y_{124} + s_3y_{124} + y_{121}y_{124} + y_{121} + \\ \quad y_{123}y_{124} + y_{124}k_{122} + y_{124}k_{123} + y_{124} + k_{121} \end{array} \right.$$

$$\Downarrow$$

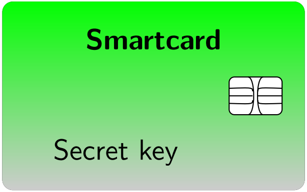
Solving

$$\Downarrow$$

find the secret key

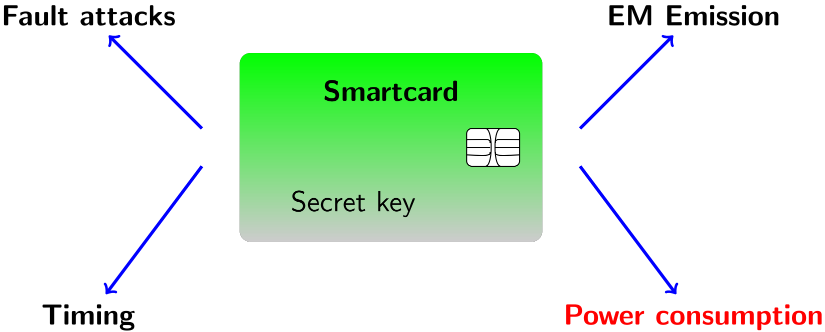
Physical attacks

Cryptographic algorithm is implemented in a device (smartcards, FPGA, ...) $\rightsquigarrow$ physical vulnerabilities



Physical attacks

Cryptographic algorithm is implemented in a device (smartcards, FPGA, ...) $\rightsquigarrow$ physical vulnerabilities



"A correct implementation of a strong protocol is not necessarily secure" (Kocher, 1999)

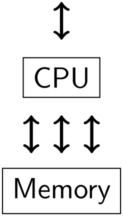
Physical attacks

Importance of the Security of the implementation :

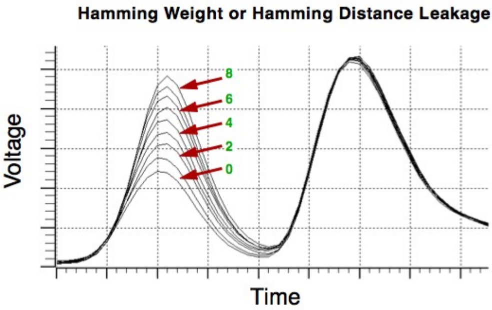
- **side-channel analysis** (SCA) targeting physical implementation
- physical leakage during the execution of an algorithm depends on **intermediate variables**
- classical SCA exploits leakage of variables that depend on the **secret key** (statistical methods: SPA, DPA, CPA, maximum likelihood, ...)
- Invasive and semi-invasive attacks: depackaging, memory extraction, fault attacks (UV attacks, laser, focused ion beams, clock glitches, power glitches, temperature, ...)

Example: Simple Power Analysis

- against smartcard with a 8-bits microcontroller
- voltage consumed can reveal Hamming weights of intermediate operations
- averages of hundreds of traces :

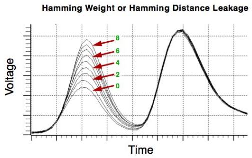


$\Rightarrow$



Algebraic Side-Channel Attacks (ASCA)

New kind of attacks recently by Renauld and Standaert (CHES2009) mixing **SPA** and **algebraic cryptanalysis**



$$\begin{cases} x_4 + s_1 s_3 + s_2 + s_4 + k_4 + 1, \\ \vdots \\ s_3 y_{124} + y_{121} y_{124} + y_{121} + \dots \\ y_{124} k_{122} + y_{124} k_{123} + y_{124} + k_{121} + \dots \end{cases}$$

$$\begin{cases} x_4 + s_1 s_3 + s_2 + s_4 + k_4 + 1, \\ s_1 s_2 + s_1 s_3 + s_1 s_4 + \dots \\ \vdots \\ s_{121} s_{122} + s_{121} s_{123} + s_{121} s_{124} + \dots \\ s_3 y_{124} + y_{121} y_{124} + y_{121} + \dots \\ y_{124} k_{122} + y_{124} k_{123} + y_{124} + k_{121} + \dots \end{cases}$$

main idea of ASCA

1. Online Phase: physical leakages measures
2. Offline Phase: algebraic attack
   - modeling cipher and additionnal information by a system of equations
   - solving this system

- Algebraic Side-Channel Attacks
  Renauld, Standaert, Inscrypt 2009
- Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA
  Renauld, Standaert, Veyrat-Charvillon, CHES 2009
- Algebraic Methods in Side-Channel Collision Attacks and Practical Collision Detection
  Bogdanov, Kizhvatov, Pyshkin, Indocrypt 2008
- Blind Differential Cryptanalysis for Enhanced Power Attacks
  Handschuh, Preneel, Selected Areas in Cryptography 2006
- Multi-Linear cryptanalysis in Power Analysis Attacks
  Roche, Tavernier, 2009
- ...

Algebraic Side-Channel Attacks

Interesting aspects

- require much less observations than a DPA
- solving step seems very **fast** (with a SAT-solver)
- can deal with masking countermeasure

Algebraic Side-Channel Attacks

Interesting aspects

- require much less observations than a DPA
- solving step seems very **fast** (with a SAT-solver)
- can deal with masking countermeasure

However, the effectiveness depends on

- the shape of the system of equations (cipher modeling)
- the leakage model
- the amount of available information
- the heuristics used in the SAT-solver
- ...

$\rightsquigarrow$ very difficult to explain and predict results of experiments

Algebraic Side-Channel Attacks

Main goal: analysis of algebraic phase

- explain the effectiveness of the solving step
- how many measures are needed?
- some leakages more valuables than others?
- which cipher intermediate operations to target?
- impact of the leakage model?

So, we need a more stable and understandable solving method (without heuristics) $\Longrightarrow$ Gröbner basis

Algebraic Side-Channel Attacks

A first experiment with assumptions:

- a very simple SPN block cipher : PRESENT
- every layers send their results throught a 8-bits bus
- leakages measured on the bus
- assumed error-free
- Hamming weight model

$\Rightarrow$ very good situation for attacker

Algebraic Side-Channel Attacks

A first experiment with assumptions:

- a very simple SPN block cipher : PRESENT
- every layers send their results throught a 8-bits bus
- leakages measured on the bus
- assumed error-free
- Hamming weight model

⇒ very good situation for attacker

SAT-solver

system solved in less than 3s

Algebraic Side-Channel Attacks

A first experiment with assumptions:

- a very simple SPN block cipher : PRESENT
- every layers send their results throught a 8-bits bus
- leakages measured on the bus
- assumed error-free
- Hamming weight model

$\Rightarrow$ very good situation for attacker

SAT-solver

system solved in less than 3s

direct Gröbner basis attacks (F4)

after 2 hours of computation $\rightarrow$ out of memory (20GB)
$\Rightarrow$ needs a little study of the system structure

Global to local study

- S-boxes are the only nonlinear part of many block ciphers
- They give the resistance against algebraic attacks

Main criterion to evaluate the algebraic resistance of a block cipher is the **Algebraic Immunity** of the S-boxes

$\Rightarrow$ We start to study the S-boxes

Algebraic Immunity (Carlet, Courtois, ...)

Main criterion for algebraic attack = **Algebraic Immunity**

Notations

- Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a n-bits S-box.
- $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ respectively its input and output bits.
- polynomials $F_i(X_1, \ldots, X_n) = Y_i$, $i \leq i \leq n$ are the coordinate functions (i.e. outputs of S as a function of its inputs)

Definition of Algebraic Immunity (Ars2005)

Let $I_S = \langle \{Y_i - F_i(X_1, \ldots, X_n), X_i^2 - X_i, Y_i^2 - Y_i, i \in \{1 \ldots n\}\} \rangle$.
Then the **Algebraic Immunity** of S is defined by

$$AI(S) = \min\{deg(P), P \in I_S \backslash \{0\}\}$$

The number of such lowest degree relations is also an important invariant

Algebraic Immunity (Carlet, Courtois, ...)

How to compute the **Algebraic Immunity** for a given S-box S?
It is enough to compute a Grobner basis with the DRL order of

$$I_S = \langle \{Y_i - F_i(X_1, \ldots, X_n), X_i^2 - X_i, Y_i^2 - Y_i, i \in \{1 \ldots n\}\} \rangle$$

Indeed, we have

Prop

The reduced Grobner basis G_S of I_S with respect to a graded order contains a linear basis of the lowest relations of S (i.e. the polynomials $P \in I_S$ such that $deg(P) = AI(S)$).

Example with the AES S-box

The Algebraic Immunity of the inverse function over $\mathbb{F}_{2^8}$ (e.g. AES S-box) equals **2**. Indeed, the inverse function is represented by a set of 39 quadratics equations over $\mathbb{F}_2$ (Courtois 2002)

A new notion of Algebraic Immunity

ASCA context ⇒ consider **leakage information**

Notations

For every value ℓ of the leakage model, we denote

- $E_\ell(X_1, \ldots, X_n, Y_1, \ldots, Y_n)$ the equations representing the leakage information ℓ
- $I_\ell = \langle E_\ell(X_1, \ldots, X_n, Y_1, \ldots, Y_n) \cup \{Y_i - F_i(X_1, \ldots, X_n), X_i^2 - X_i, Y_i^2 - Y_i, i \in \{1 \ldots n\}\}\rangle$

Definition of Algebraic Immunity with Leakage

The lowest degree relations in I_ℓ are called **Algebraic Immunity With Leakage** ℓ of the S-box S. It is denoted by $AI_L(S, \ell)$ and the number of such relations is denoted by $\#AI_L(S, \ell)$.

Algebraic Immunity with Leakage: HW example

Assumption : leakage L of S gives

- HW of input value
- HW of output value
- $\ell = (w_{in}, w_{out})$

$\Rightarrow$ the ideal I_ℓ contains at least 2 independent linear polynomials:

$$X_1 + \cdots + X_n + (w_{in} \text{ mod } 2) \in I_\ell$$
$$Y_1 + \cdots + Y_n + (w_{out} \text{ mod } 2) \in I_\ell$$

Results

$\forall$ S-box S, and $\forall \ell \in \{0, ..., n\}^2$

$$AI_L(S, \ell) = 1$$
$$\#AI_L(S, \ell) \geq 2$$

Is It enough to solve our system ?

HW example ($\ell = (w_{in}, w_{out})$)

$\Rightarrow$ the ideal I_ℓ contains at least these 2 independent linear polynomials:

$$X_1 + \cdots + X_n + (w_{in} \text{ mod } 2) \in I_\ell$$
$$Y_1 + \cdots + Y_n + (w_{out} \text{ mod } 2) \in I_\ell$$

Does not help enough for solving our system:

- no linear relation between input and output
- substitution layer is always **nonlinear**

But now, we know that leakages may gives rise to linear equations!!
Is there any other more interesting?

HW example ($\ell = (w_{in}, w_{out})$)

Trivial example: $w_{in} = 0$

$\forall$ S-box S, if $w_{in} = 0$ then $X_1 = X_2 = \cdots = X_n = 0$
and the Y_i are given by

$$Y_1, \ldots, Y_n = S(0, \ldots, 0) = y_1, \ldots, y_n$$

$\#AI_L(S, \ell) = 2n$ is maximal with this case and
the corresponding S-box is completely described by linear relations

HW example ($\ell = (w_{in}, w_{out})$)

Trivial example: $w_{in} = 0$

$\forall$ S-box S, if $w_{in} = 0$ then $X_1 = X_2 = \cdots = X_n = 0$
and the Y_i are given by

$$Y_1, \ldots, Y_n = S(0, \ldots, 0) = y_1, \ldots, y_n$$

$\#AI_L(S, \ell) = 2n$ is maximal with this case and
the corresponding S-box is completely described by linear relations

PRESENT S-box example: $\#AI_L(S, (w_{in}, w_{out}))$

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0					16				
1					9				
2			15	15	8	13	15		
3			9	5	9	5	9		
4	16	15	14	2	11	3	12	13	16
5		13	13	2	7	10	11	13	
6		15	12	15	7	15	14		
7			13		13				
8			16						

A lot of interesting linear equations can appear, depending on the leakage value

Another invariant

Definition

$\forall$ S-box $S, \forall$ leakage value ℓ
we define

$$\begin{aligned} N_S(\ell) &= \#V(I_\ell) \\ &= \#\{x \in \mathbb{F}_2^n \text{ s.t. leakage of } S = \ell\} \end{aligned}$$

Another invariant

Definition

$\forall$ S-box $S, \forall$ leakage value ℓ
we define

$$\begin{aligned} N_S(\ell) &= \#V(I_\ell) \\ &= \#\{x \in \mathbb{F}_2^n \text{ s.t. leakage of } S = \ell\} \end{aligned}$$

Prop

Let n the bus size of S. If $AI_L(S, \ell) = 1$ and $N_S(\ell)$ is non-zero then

$$\#AI_L(S, \ell) \geq 2n + 1 - N_S(\ell)$$

$N_S(\ell)$ small $\rightsquigarrow$ a lot of linear relations between input and output

Take a look at PRESENT S-box

Assumptions : 8-bits bus and Hamming weight leakage model

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0					16				
1					9				
2			15	15	8	13	15		
3			9	5	9	5	9		
4	16	15	14	**2**	**11**	3	12	13	16
5		13	13	2	7	10	11	13	
6		15	12	15	7	15	14		
7			13		13				
8			16						

Figure: $\#AI_L(S, w_{in}, w_{out})$

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0					1				
1					8				
2			2	2	18	4	2		
3			8	12	8	20	8		
4	1	2	3	**24**	**7**	22	6	4	1
5		4	4	16	12	8	8	4	
6		2	6	2	12	2	4		
7			4		4				
8			1						

Figure: $N_S(w_{in}, w_{out})$

Observations

- confirm that small $N_S \Rightarrow$ large $\#AI_S$
- Most of leakages give a lot of linear relations: $\mathbb{E}(\#AI_L) = 7,9$
- We are now able to sort leakages by relevance

Take a look at PRESENT S-box

Assumptions : 8-bits bus and Hamming weight leakage model

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0					16				
1					9				
2			15	15	8	13	15		
3			9	5	9	5	9		
4	16	15	14	2	11	3	12	13	16
5		13	13	2	7	10	11	13	
6		15	12	15	7	15	14		
7			13		13				
8			16						

Figure: $\#AI_L(S, w_{in}, w_{out})$

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0					1				
1					8				
2			2	2	18	4	2		
3			8	12	8	20	8		
4	1	2	3	24	7	22	6	4	1
5		4	4	16	12	8	8	4	
6		2	6	2	12	2	4		
7			4		4				
8			1						

Figure: $N_S(w_{in}, w_{out})$

Observations

- confirm that small $N_S \Rightarrow$ large $\#AI_S$
- Most of leakages give a lot of linear relations: $\mathbb{E}(\#AI_L) = 7,9$
- We are now able to sort leakages by relevance

Take a look at PRESENT S-box

Assumptions : 8-bits bus and Hamming DISTANCE leakage model

Definition:

$d = HD(x, S(x)) = HW(x \oplus S(x))$

HD model :

- $AI_L(d) = 1$
- $\#AI_L(d) \geq 1$
- $\mathbb{E}(\#AI_L) = 2,3$

d	0	1	2	3	4	5	6	7	8
$N_S(d)$	0	0	16	56	81	64	30	8	1
$\#AI_L(S,d)$	0	0	10	3	1	1	1	9	16

Figure: HD model and PRESENT S-Box

Solving strategy

Return to our experiment :

- choose an order on variables
- triangular structure $\rightarrow$ blocks of equations (Layers, SBoxes, ...)
- blocks corresponding to Sboxes $\rightarrow$ Grobner basis of I_ℓ
- polynomial system modeling PRESENT partly linearized

Results:

Successive Gröbner basis computation (F4)
$\rightarrow$ better control on the degree
$\rightarrow$ better solving strategy

Criterion of success

Results on PRESENT (31 rounds):

With our solving strategy $\Rightarrow$ about 5min, 1GB, degree limited to 2

- $\mathbb{E}(\#AI_L) = 7,9$
- $\mathbb{P}(\#AI_L \geq 8) \approx \frac{1}{2}$

$\Rightarrow$ Expected linear relations for one substitution layer ≈ 64

Criterion of success

Results on PRESENT (31 rounds):

With our solving strategy ⇒ about 5min, 1GB, degree limited to 2

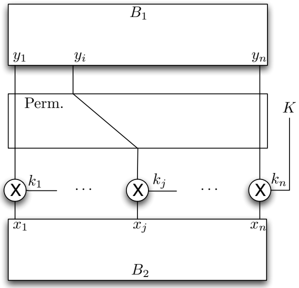
- $\mathbb{E}(\#AI_L) = 7,9$
- $\mathbb{P}(\#AI_L \geq 8) \approx \frac{1}{2}$

⇒ Expected linear relations for one substitution layer ≈ 64

Why this attack can work

- with leakages in only 3 or 4 rounds?
- in unknown plaintext/ciphertext scenario?

Consecutive leakages



$N_S(\ell) \leq 6 \Rightarrow$ fixed input/output bits

$\rightsquigarrow$ subkey bits easily deduced

$\rightsquigarrow$ really happens with Gröbner basis computation

Characterization of resistant S-Boxes

Requirements:

- No fixed bits
- few linear relations

$\rightsquigarrow$ maximizing N_S for all leakages

HW model :

$$N_S(w_{in}, w_{out}) = \#(HW^{-1}(w_{in}) \bigcap S^{-1}(HW^{-1}(w_{out})))$$

Then, S must satisfy

$$HW^{-1}(w_{in}) = S^{-1}(HW^{-1}(w_{out}))$$

and

$$w_{in} = w_{out} \text{ or } w_{in} = n - w_{out}$$

Characterization of resistant S-Boxes

Example of such 4-bits S-box:

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	0	B	5	C	E	6	9	8	7	5	3	1	A	2	4	F

$HW(x)$	$HW(S(x))$
0	0
1	3
2	2
3	1
4	4

Characterization:

$$S(x) = \pi(x) + f(HW(x))(1, ..., 1)$$

- $\pi(x) =$ stable permutation on constant HW
- $f =$ boolean function s.t. $\forall x \in \{0, \ldots, n\}, f(x) = f(n - x)$

However, nonlinearity(S) $\simeq$0 $\Rightarrow$ very weak against linear cryptanalysis

Experiments

Experiments performed against PRESENT and AES

Analysis supported by experiments:

	GB	SAT-solver
• checking resistant S-boxes	✓	✓
• reject of leakages with large N_S	✓	✓
• reject of leakages with small N_S	✗	✗
• no consecutive leaked rounds	✗	✗
• importance of the model: HD example	✗	✗

Analysis remains valid with both Gröbner basis and SAT-solver

Conclusion

- New notion of Algebraic Immunity
- Good understanding of influence of leakage information
  - Results of experiments are explained
  - Leakages informations can be sorted by importance
  - A first criterion for resistant devices against ASCA

Perspectives

- Finding resistant S-boxes against ASCA and linear cryptanalysis (current work with Claude Carlet)
- Study more realistic leakage models
- Dealing with errors