Analysis of the algebraic side channel attack

Claude Carlet, Jean-Charles Faugère, Christopher Goyet, Guénaël Renault

Noname manuscript No.
(will be inserted by the editor)

Analysis of the Algebraic Side Channel Attack

Claude Carlet · Jean-Charles Faugère · Christopher Goyet · Guénaël Renault

the date of receipt and acceptance should be inserted later

Abstract At CHES 2009, Renauld, Standaert and Veyrat-Charvillon introduced a new kind of attack called Algebraic Side-Channel Attacks (ASCA). They showed that side-channel information leads to effective algebraic attacks. These results are mostly experiments since strongly based on the use of a SAT solver. This article presents a theoretical study in order to explain and to characterize the algebraic phase of these attacks. We study more general algebraic attacks based on Gröbner methods. We show that the complexity of the Gröbner basis computations in these attacks depends on a new notion of algebraic immunity defined in this paper, and on the distribution of the leakage information of the cryptosystem. We also study two examples of common leakage models: the Hamming weight and the Hamming distance models. For instance the study in the case of the Hamming weight model gives that the probability of obtaining at least 64 (resp. 130) linear relations is about 50% for the substitution layer of PRESENT (resp. AES). Moreover if the S-boxes are replaced by functions maximizing the new algebraic immunity criterion then the algebraic attacks (Gröbner and SAT) are intractable. From this theoretical study, we also deduce an invariant which can be easily computed from a given S-Box and provides a sufficient condition of weakness under an ASCA. This new invariant does not require any sophisticated algebraic techniques to be defined and computed. Thus, for cryptographic engineers without an advanced knowledge in algebra (e.g. Gröbner basis techniques), this invariant may represent an interesting tool for rejecting weak S-boxes.

Claude Carlet
Université Paris 8, UMR LAGA, MTII team
2, rue de la liberté
93526 Saint-Denis, Cedex 02, France
E-mail: claude.carlet@univ-paris8.fr

Jean-Charles Faugère · Christopher Goyet · Guénaël Renault
UPMC, Université Paris 6, LIP6
INRIA, Centre Paris-Rocquencourt, PolSys Project-team
CNRS, UMR 7606, LIP6
4, place Jussieu
75252 Paris, Cedex 5, France
E-mail: jean-charles.faugere@inria.fr
E-mail: christopher.goyet@lip6.fr
E-mail: guenael.renault@lip6.fr

Christopher Goyet
Thales Communications & Security
160 Boulevard de Valmy
92700 Colombes, France
E-mail: christopher.goyet@fr.thalesgroup.com

1 Introduction

Algebraic Side Channel Attacks (ASCA) are a new kind of attack recently introduced in [RSVC09] by Renauld, Standaert and Veyrat-Charvillon. It is a natural combination of classical algebraic cryptanalysis and side channel attacks which take full advantage of both classical attacks. It should be mentioned that several methods combining side channel and algebraic attacks (see [Bog07, BKP08] for the first algebraic collision attacks) or differential attacks (see [SWP03, HP06, Bog08]) have already been suggested. As for these methods, the main idea of ASCA is to begin with an on-line phase where leakage information is recorded by a side channel, and to end with a powerful off-line phase where this data is used by algebraic cryptanalysis to recover the key. In contrary to standard Differential Power Analysis, the goal of the on-line phase is not to recover directly a bit of the key but it is only to catch a lot of partial information on the intermediate data manipulated during the encryption. Thus, all the leakages of all the cipher rounds are potentially useful. Contrary to the

articles [SWP03,SLFP04,HP06,Bog07,BKP08,Bog08, MME10], ASCA could succeed with the observation of a single encrypted plaintext and would work with completely masked implementations. During this on-line phase, a leakage model is selected, for example a common leakage model is the Hamming weight of data transiting on a bus (see for instance [CJRR99, ABDM00] for a discussion of this model). Next, the off-line phase makes use of the collected leakage information in an algebraic attack. In the present study, the side channel information is assumed to be reliable for use in the algebraic attack phase, which is not the case with real measures because of the presence of noise. Even though recent works have shown how algebraic approaches may deal with errors ([OKPW10, AC10]), our goal is to start to explain and to understand the efficiency of ASCA, and more precisely the algebraic phase of ASCA with reliable leakage information. This algebraic attack phase consists of modeling the cryptosystem and the leakage model by a system of polynomial equations. Solving this system is equivalent to recovering the bits of the key. In classical algebraic cryptanalysis, solving the system of equations representing a modern block cipher remains a source of speculation because of the complexity of solving such polynomial systems. On the contrary, the system of equations obtained with the algebraic collision attacks ([Bog07,BKP08]) has been well detailed so that the complexity of resolution of such systems is well understood. On the other hand, in the ASCA context, the leakage model seems to provide enough information to efficiently solve in practice the system of equations, but the apparent simplicity of this solving step remained unexplained and its computational complexity was not enough analyzed.

In [RS09] and [RSVC09], algebraic side-channel attacks are evaluated against 8-bit implementations of PRESENT and AES. The main leakage model studied is the Hamming weight model. Thus, the authors of [RS09,RSVC09] (as in [HP06]) assume the knowledge of the Hamming weights of some intermediate computations. The system of equations representing the block cipher and the leakage model is translated into a satisfiability problem and solved by a SAT solver. Under these assumptions, this attack seems very powerful. Indeed, the key is always recovered in less than one minute if all the 8-bit Hamming weights after the XORs (in AddRoundKey and MixColumns functions) and after the substitution layers are known for a 31-round PRESENT and for a 10-round AES. When fewer Hamming weights are known, the number of consecutive rounds with Hamming weights is an important criterion for a successful attack. There are also some effective attacks in unknown plaintext/ciphertext situations or against masked implementations. It is clear that the known Hamming weights allow to exclude most of the possible values of the key, however, the success rate of these attacks depends on several parameters: the amount of available information, the leakage function or the shape of the system of equations. All these results are also very dependent on the heuristics used in the SAT solver, and so the experiments are very difficult to explain when SAT solver techniques are used.

The main goal of this article is to explain the effectiveness of this attack, to describe the criterion of success and therefore to find the theoretical conditions to prevent algebraic side channel attacks. To achieve this goal, Gröbner techniques are used instead of a SAT solver because of their computation without heuristics and so, more stable and more understandable. We also assume the same hypothesis as in [RS09,RSVC09], particularly that an initial on-line phase provides a sequence of leakage information, and we only focus on the algebraic cryptanalysis phase. Furthermore, we do not discuss about side channel countermeasures, and we refer to [RS09,RSVC09] for detailed discussions. We show in section 2 that the complexity of the Gröbner basis computation in these attacks depends on a new notion of algebraic immunity and on the distribution of leakage information. This Algebraic Immunity with Leakage is defined by the degree and also the number of lowest degree relations which are given by a black box (S-Boxes, Key derivation, etc) and its leakage information. This new algebraic immunity is completely related to the complexity of the Gröbner basis computation and thus, represents a good criterion for effective Gröbner attacks. From this theoretical study and this new criterion, we deduce a new invariant, which could also be connected to SAT solvers efficiency. For a given block cipher, this invariant, denoted by N_B, is easily computed by a local study of the black boxes B defining the cryptosystem. In contrary to the Algebraic Immunity with Leakage, this computation does not require any knowledge of advanced algebra which may be more useful for cryptographic engineers who are not fluent with Gröbner basis techniques. More precisely, if we denote by B the black box, L the leakage model, l a value of the function L, and n the bus size, then the invariant is the function $N_B(l)$ giving the cardinality of the corresponding set $\{x \in \mathbb{F}_2^n \text{ s.t. } \mathrm{L}(x, B(x)) = l\}$. We prove that the number of linear relations given by the leakage l is greater or equal than $2n+1-N_B(l)$ (in practice, this bound is often achieved). Thus, from this new invariant, we deduce a sufficient condition for the weakness of a black box under a Gröbner attack with leakage. This condition corresponds to the case where the black box is such that $N_B(l)$ is small for a lot of values of l. We

verify this condition in practice by using Gröbner basis techniques and some of the best SAT solvers. Thus, this invariant may be seen as a general algebraic sufficient condition (independent of the solving strategy) for an effective algebraic side channel attack. Even if this invariant does not provide a theoretical necessary condition of weakness, we successfully describe several scenarios of unsuccessful Gröbner and SAT solver attacks when $N_B(l)$ is large. For example, if the S-boxes are replaced by functions maximizing the function N_B then both algebraic attacks become impractical. The same holds when all leakage data maximizes N_B.

From this new theoretical point of view, we analyze the precedent results on ASCA which were heuristic. To simplify and to keep the point of view of [RS09, RSVC09], we mostly study the 8-bit Hamming weight leakage, but we also consider the Hamming distance which is a more general model. The results presented in Section 3.2 and in Annex A show that, with the Hamming weight model, the AES, PRESENT, CAMELLIA and SMS4 S-boxes are very weak with respect to this invariant: N_B is often small and the number of linear equations is on average 8 per S-box. With the Hamming distance model, ASCA is much more difficult and we show that, in this case, N_B is often large and the number of linear equations is on average between 1 and 2 per S-box. The local study of these S-boxes shows that these two models of leakage information can be used to partly linearize the polynomial system of equations. Moreover, if N_B is very small then few input or output bits of the S-box can be recovered. In section 4, these local results are used to explain the recovery of the key bits. Especially in the case of consecutive leakage in the Hamming weight model, the subkey bits can be easily deduced from previously recovered bits. Or else, we show that the system of equations representing the block cipher and the Hamming weight information contains enough linear equations to be efficiently solved: the probability of obtaining at least 64 (resp. 130) linear relations is about 50% for PRESENT (resp. AES) for example. Moreover, we show that if the number of rounds increases, the number of linear relations which provide subkey bit increase (see Section 4.3). Consequently, this work fully explains the efficiency of the attack. Thanks to this understanding, an efficient solving strategy is developed for Gröbner attacks (Section 4). In the case of the Hamming distance model, the attacks are much less efficient because N_B is larger in average, and the expected number of linear equations is very low (see Section 3.3). In section 5, the conditions for preventing algebraic side channel attacks are also discussed, and it seems that one of the safest way to design a block cipher resistant against all kinds of attacks is to increase the bus size.

2 Algebraic Cryptanalysis and side channel information

The basic principle of Algebraic Cryptanalysis is to model a cryptographic primitive by a set of algebraic equations over a finite field. The system of equations is constructed in such a way as to have a correspondence between the solutions of this system, and the secret information of the cryptographic primitive (for instance, the secret key of a block cipher). There are different ways to solve such a polynomial system : SAT solver, Gröbner basis, XSL([CP02]) etc. In this article, we particularly use the Gröbner basis method, a powerful tool for solving a polynomial system. We refer to [BFS04, Bar04, BFSY05] for a discussion on the complexity of Gröbner basis computation of overdetermined algebraic equations over finited fields. The Faugère's F4 and F5 [Fau99, Fau02] algorithms are the most efficient algorithms to compute Gröbner basis, so in our experiments we used the efficient implementation of F4 by Magma software [BCP97]. These algorithms have been successfully applied against a number of multivariate schemes [FJ03, FP06a, FP06b, FdVP08] and in stream cipher cryptanalysis [CM03, Ars05], but they stay unpractical against bloc ciphers [CP02, CL05]. Indeed, the size of the corresponding algebraic system is so huge (thousand of variables and/or equations with high degree) that nobody is able to predict correctly the complexity of solving such polynomial systems. The degree of these equations stay high because of non-linear substitution-box layers (S-Boxes) and the multitude of rounds. One of the main goals of algebraic attacks is to describe these S-Boxes by low degree equations. The number of such equations gives a criterion to evaluate the block cipher resistance against algebraic attacks and it is called Algebraic Immunity ([AA05, AF05, Ars05, AK06, FM07, Car09, Car10]).

In algebraic side channel attack, we also assume the knowledge of additional information obtained by side channel, for instance Hamming weights of intermediate values. In the polynomial system modeling of our problem we take into account this assumption. In particular, we see each round of the block cipher as successive black boxes operating on n-bit data (*i.e.* n is the size of the bus). From the knowledge of the polynomial systems representing such a black box and the corresponding Hamming weight leakages, one can model the complete block cipher with leakages as a block diagonal system of equations (each block corresponding to a round). This definition of the model by splitting the different steps of

size of n bits is used in our strategy for solving the entire system and it turns out that this algebraic system updated with equations corresponding to the leakage is easier to solve in practice. We will show in this section that the presence of this additional information may give rise to a number of independent linear relations. These relations enable us to mount an effective algebraic attack and that leads us to define a new notion of Algebraic Immunity with Leakage.

From now on, to make this study more general, the S-boxes, or any vectorial boolean function is seen as a *black box*, denoted by B in the following. Let n be the bus size of B, $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ be respectively its input and output bits. To restrict the study to solutions with coefficients in the field $\mathbb{F}_2$ (and not in its algebraic closure $\overline{\mathbb{F}_2}$), we always add the set of polynomials $S_{\text{Field Eq.}} = \{X_i^2 - X_i, Y_i^2 - Y_i, 1 \leq i \leq n\}$ (corresponding to the classical field equations) into the polynomial systems. We will denote by $I_{\text{Field Eq.}}$ the ideal of $\mathbb{F}_2[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ generated by the set $S_{\text{Field Eq.}}$. Finally, the subset $S_B = \{F_1, \ldots, F_{k_B}\} \subset \mathbb{F}_2[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ is the finite set of Boolean functions defining the outputs of B as a (explicit or implicit) function of its inputs.

2.1 Algebraic Immunity for Block ciphers

The notion of Algebraic Immunity often refers to stream ciphers and boolean functions, but in this article, we make reference to the Algebraic Immunity extended to boolean vectorial functions (sometimes called "graph algebraic immunity"). This definition slightly varies from one article to the next. Thus, we first remind the definition of the Algebraic Immunity which we are going to use and we give an algorithm to compute it (see [AA05, AF05, Ars05, AK06, FM07, Car09, Car10]).

The Algebraic Immunity is defined as the lowest degree of algebraic relations of a Boolean vectorial function. More formally, let $B : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a black box and $I_B \subset \mathbb{F}_2[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ the ideal generated by the equations representing B and the field equations:

$$I_B = \langle S_B \cup S_{\text{Field Eq.}} \rangle$$

Definition 1 The Algebraic Immunity of B is defined by $AI(B) = min\{deg(P), P \in I_B \setminus I_{\text{Field Eq.}}\}$

Remark 1 The number of such lowest degree relations is also an important invariant related to I_B, and it is always computed at the same time as the Algebraic Immunity.

To obtain the Algebraic Immunity of a black box B, we could compute a Gröbner basis of I_B with respect to a graded order([AF05]):

Theorem 1 *The reduced Gröbner basis G_B of I_B with respect to a graded order contains a linear basis of the lowest relations of B (i.e. the polynomials $P \in I_B$ such that $deg(P) = AI(B)$).*

Proof Every $f \in I_B$ is reduced to zero by a Gröbner basis of I_B. Thus, there is a polynomial $g \in G_B$ such that the leading monomial $LM(g)$ of g divides $LM(f)$. As we have a graded monomial order, $deg(g) = deg(LM(g))$ and $deg(f) = deg(LM(f))$. Thus, $deg(g) \leq deg(f)$ and we prove that G_B contains a linear generated family of the lowest relations of B. Then the definition of a reduced Gröbner basis implies that the linear generated family is a linearly independent family. □

Example 1 The Algebraic Immunity of the function calculating the inverse over $\mathbb{F}_{2^8}$ (e.g. AES S-box) equals 2. Indeed, the inverse function is represented by a set of 39 quadratic equations over $\mathbb{F}_2$ ([CP02]) as well as over $\mathbb{F}_{2^8}$ ([Ars05]).

2.2 Algebraic Immunity of S-boxes with Leakage

In the previous section, the concept of *Algebraic Immunity* is defined as the lowest degree of algebraic relations of a Boolean vectorial function. In the ASCA context, we are looking for the lowest degree relations of B with leakage information (e.g. Hamming weights, Hamming distances). Therefore, we need to introduce a slightly different notion of Algebraic Immunity to take the leakage into account. To do so, for every value l of the leakage model, we consider the ideal I_l of $\mathbb{F}_2[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ generated by the equations representing B, the field equations $S_{\text{Field Eq.}}$ and by L_l the set of equations representing the leakage information l, namely:

$$I_l = \langle S_B \cup L_l \cup S_{\text{Field Eq.}} \rangle .$$

From this ideal we can define this new notion of algebraic immunity.

Definition 2 Let B be a black box and l the value of the leakage model L. The *Algebraic Immunity With Leakage*, denoted by $AI_L(B, l)$, is defined by

$$AI_L(B, l) = min\{deg(P), P \in I_l \setminus I_{\text{Field Eq.}}\}$$

The number of linearly independent relations in I_l with degree $AI_L(B, l)$ will be denoted by $\#AI_L(B, l)$.

Similarly to the general notion of Algebraic Immunity, the relations of lowest degree can be explicitly obtained by the computation of a Gröbner basis of I_l with respect to a graded order (see [Ars05]).

An other important invariant related to I_l is the number of points in the associated variety $V(I_l)$, i.e.

the set of common roots of the polynomials in I_l. This number which depends on the black box B and on the value l of the leakage function L, is also linked to our Algebraic Immunity With Leakage and it will be denoted by $N_B(l)$:

Definition 3 $N_B(l)$ is defined as the number of points of the variety $V(I_l)$. In other words, $N_B(l)$ is equal to the cardinality of the set $\{x \in \mathbb{F}_2^n \text{ s.t. } \mathrm{L}(x, B(x)) = l\}$

We will show in Section 3 below that $AI_L(B,l)$ is equal to 1 in the cases of Hamming weight and Hamming distance model. In this particular situation where $AI_L(B,l)$ is equal to one (ie. there is at least one linear equation in the Ideal I_l), we prove the following relation between $\#AI_L(B,l)$ and $N_B(l)$:

Proposition 1 *Let n be the bus size of B. If $AI_L(B,l)$ is equal to 1 and $N_B(l)$ is non-zero then*

$$N_B(l) \geq 2n + 1 - \#AI_L(B,l) \ .$$

Proof As observed in Definition 3, we have $N_B(l) = \#V(I_l)$. Since I_l contains the field polynomials, it is radical. Its variety $V(I_l)$ is a subset of $\mathbb{F}_2^n$ and, from the Nullstellensatz, we have

$$\begin{aligned} \#V(I_l) &= \dim(\tfrac{\mathbb{F}_2[X_1,\ldots,X_n,Y_1,\ldots,Y_n]}{I_l}) \\ &= \dim(\mathrm{Span}(m^\alpha : \alpha \in \mathbb{N}^{2n},\ m^\alpha \notin \mathrm{LT}(I_l))) \end{aligned}$$

From this set of generating monomials, we only keep the set F of monomials which have a degree less than or equal than one:

$$F = \{m : \deg(m) \leq 1 \text{ and } m \notin \mathrm{LT}(I_l)\}$$

We have $\#V(I_l) \geq \dim(\mathrm{Span}(F))$. Now, let $E = \{m : \deg(m) \leq 1\}$ and $G = \{m : \deg(m) \leq 1 \text{ and } m \in \mathrm{LT}(I_l)\}$. It is clear that F is the set of monomials in E which are in $\mathrm{LT}(I_l)$ and G is the set of the monomials in E which are not in $\mathrm{LT}(I_l)$, thus the set E is equal to the following disjoint union $E = F \bigsqcup G$. Finally,

$$\begin{aligned} \#V(I_l) &\geq \dim(\mathrm{Span}(F)) \\ &= \dim(\mathrm{Span}(E)) - \dim(\mathrm{Span}(G)) \\ &= 2n + 1 - \#AI_L(B,l) \end{aligned}$$

□

We have defined the Algebraic Immunity with Leakage and showed its relation with $N_B(l)$. In the next section, these results will be useful to study two examples of leakage models: the Hamming weight and the Hamming distance leakage models.

3 Two common leakage models: the Hamming weight model and the Hamming distance model

In [RS09] and [RSVC09], algebraic side-channel attacks are evaluated against implementations of the block ciphers PRESENT and AES in 8-bit PIC microcontrolers. The main leakage model studied is the Hamming weight model, that is the number of bits set to 1 being processed at a given time (see for instance [CJRR99, ABDM00] for a discussion of this model). Thus the authors of [RS09, RSVC09] assume the knowledge of the Hamming weights of some intermediate computations. In this section, we also assume that a first on-line phase already provided leakages as the Hamming weights or the Hamming distances of the input and output of a black box B. The Algebraic Immunity with Leakage is of great help to study the influence of this additional information on the system of equations generated by B. Actually, we prove that the Algebraic Immunity with Leakage of B with Hamming weight model or with Hamming distance model is equal to 1 for every possible black box B which is exceptionally small. Moreover, we show that there are at least two independent linear equations in the case of Hamming weight model.

3.1 The system of equations corresponding to the Hamming weight

First of all, we need to describe the system of equations representing the Hamming weight of the data $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$. Note that if the Hamming weight of x is equal to w then any product of $w+1$ bits is always null, which corresponds to the following system:

$$R_w : \left\{ \prod_{i \in I} X_i = 0 \ : \ I \subset \{1 \ldots n\} \text{ s.t. } |I| = w + 1 \right\}$$

and there is only one product of w bits which is 1, which corresponds to the following system:

$$T_w : \left\{ \sum_{J \subset \{1 \ldots n\} \text{ s.t. } |J| = w} \left(\prod_{j \in J} X_j \right) = 1 \right\}$$

These two facts are sufficient to represent the Hamming weight model by the system of equations

$$L_w = R_w \cup T_w \tag{1}$$

Example 2 For instance, the system of equations $L_1 = \{x_1x_2 = x_1x_3 = x_1x_4 = x_2x_3 = x_2x_4 = x_3x_4 = 0, x_1 + x_2 + x_3 + x_4 = 1\}$ is satisfied only by $x = (x_1 \ldots x_4) \in \mathbb{F}_2^4$ such that $HW(x) = 1$:

The only sets L_w which contain a linear equation are the sets L_w with $w = 0$ or $w = 1$. When $w > 1$, these sets L_w do not contain linear equations.

Now that we have formulated the system of equations representing the Hamming weights, we are able to study the Hamming weight leakage model. We will show that the addition of these systems of equations representing the Hamming weight to the system modeling a black box B could give a lot of linear equations.

3.2 Hamming weight model leakage

We study the Algebraic Immunity With Leakage in the case of the Hamming weight model (see Section 2.2). So, we consider the ideal $I_{w_{in},w_{out}}$ of $\mathbb{F}_2[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ generated by the equations representing B, the field polynomials $S_{\text{Field Eq.}}$ and by $L_{w_{in}}, L_{w_{out}}$ the equations representing the Hamming weights w_{in}, w_{out} respectively (see the definition of L_w (1)), namely:

$$I_{w_{in},w_{out}} = \langle L_{w_{in}} \cup L_{w_{out}} \cup S_B \cup S_{\text{Field Eq.}} \rangle$$

In this case, the Algebraic Immunity With Leakage of the black box B with Hamming weight leakage is denoted by $AI_L(B, w_{in}, w_{out})$ and the number of linearly independent relations in $I_{w_{in},w_{out}}$ with degree $AI_L(B, w_{in}, w_{out})$ is denoted by $\#AI_L(B, w_{in}, w_{out})$.

We now prove that $AI_L(B, w_{in}, w_{out}) = 1$, and $\#AI_L(B, w_{in}, w_{out}) \geq 2$, i.e. that $I_{w_{in},w_{out}}$ contains at least two independent linear polynomials. This result is a consequence of the fact that there is always a linear relation in the ideal generated by the equations describing the Hamming weight. Although these two linear relations are not really useful in an algebraic attack, this result shows that the situation is completely different with the classical algebraic immunity.

Lemma 1 *Let $w \in \{0, \ldots, n\}$. The ideal $I_{hw}(w) \subset \mathbb{F}_2[X_1, \ldots, X_n]$, generated by L_w (1) and by $S_{\text{Field Eq.}}$, always contains the linear polynomial*

$$X_0 + \cdots + X_n + (w \bmod 2) \tag{2}$$

Proof The system of equations $L_w(1)$ defines the set $V(w) = \{x \in \mathbb{F}_2^n \text{ s.t. } HW(x) = w\} = HW^{-1}(w)$. Then, the radical ([CLO07]) ideal $I_{hw}(w)$ contains all polynomials vanishing on $V(w)$ (which is the variety of $I_{hw}(w)$ over $\mathbb{F}_2$). Clearly, the linear polynomial (2) vanishes on $V(w)$, hence it must be in $I_{hw}(w)$. □

We can now prove the following result :

Proposition 2 *Let G be the Gröbner basis of the ideal $I_{w_{in},w_{out}}$ for a graded monomial order. Then G contains at least 2 independent linear polynomials.*

Proof With the same notation as in lemma 1, we could note that there exist $(w_{in}, w_{out}) \in \mathbb{N}^2$ such that $I_{w_{in},w_{out}} = I_B + I_{hw}(w_{in}) + I_{hw}(w_{out})$. According to Lemma 1,

$$f = X_1 + \cdots + X_n + (w_{in} \bmod 2) \in I_{w_{in},w_{out}}$$
$$f' = Y_1 + \cdots + Y_n + (w_{out} \bmod 2) \in I_{w_{in},w_{out}}$$

then there is $g \in G$ such that the leading monomial $LM(g)$ of g divides $LM(f)$, the leading monomial of f. As $I_{w_{in},w_{out}}$ is a proper ideal, $LM(g) = LM(f) = X_i$, i depending on order, and as the monomial order is a graded order, g is a linear polynomial. The same holds for f'. □

Thus, the Algebraic Immunity with Leakage is always 1 and there are at least 2 independent linear polynomials when Hamming weight equations are added to the system of equations corresponding to B. It is quite natural that these two linear relations are in the ideal I_l since they correspond to information added by the leakage. But, it is important to see that these results are general. They do not depend on the bus size n and on the black box B. What is more interesting is the fact that, when the black box is fixed as a S-box, the number of linear independent relations is (in general) larger than 2 (see Section 6 and Appendix A). The aim of the analysis done in this paper is to study the impact of these linear relations on an algebraic attack. For instance, when the Hamming weight of the inputs is equal to 0, we have $X_1 = X_2 = \cdots = X_n = 0$, and the Y_i are given by $(y_1, \ldots, y_n) = B(x_1, \ldots, x_n) = B(0, \ldots, 0)$. In this case, the Gröbner basis computation gives:

$$\begin{aligned} I_{0,w_{out}} &= I_B + I_{hw}(0) + I_{hw}(w_{out}) = I_B + I_{hw}(0) \\ &= \langle X_1, \ldots, X_n, Y_1 + y_1, \ldots, Y_n + y_n \rangle \end{aligned}$$

which means that all the X_i and Y_i are fixed by the resolution. In this case, the number of independent linear equations is maximal. This (trivial) example corresponds to the case where the input (or output) is fixed by the leakage. These are the only cases where one can show that there are more than two linear relations in I_l without fixing the black box B.

When the black box B is fixed, the number of independent linear equations depends on the Hamming weight ordered pair of the input and output, and we already show with Proposition 1 that it is linked to the number of points which satisfy this couple. Thus, N_B (Definition 3) in the case of the Hamming weight model is denoted by $N_B(w_{in}, w_{out})$ and it is explicitly given by

$$\begin{aligned} &N_B(w_{in}, w_{out}) = \#(HW^{-1}(w_{in}) \cap B^{-1}(HW^{-1}(w_{out}))) \\ &= \#\{x \in \mathbb{F}_2^n \text{ s.t. } HW(x) = w_{in} \text{ and } HW(B(x)) = w_{out}\} \end{aligned}$$

Remark 2 $N_B(w_{in}, w_{out})$ is related to the likelihood $\mathbb{P}(HW(x) = w_{in}$ and $HW(B(x)) = w_{out})$ of the pair (w_{in}, w_{out}). Indeed, if we assume an equiprobability distribution of input bytes, this likelihood equals $2^{-n} N_B(w_{in}, w_{out})$.

In the particular case of an 8-bit bus size, Proposition 1 gives that $\#AI_L(B, w_{in}, w_{out})$ is always greater than or equal to $17 - N_B(w_{in}, w_{out})$ when $N_B(w_{in}, w_{out})$ is non-zero. Section 6 and Appendix A show that, for a lot of usual S-Boxes, $N_B(w_{in}, w_{out})$ is often small in the Hamming weight leakage model, and the interesting Hamming weight pairs are the ones such that $N_B(w_{in}, w_{out})$ is small. Indeed, in this case, the constraints on the X_i and Y_i variables are strong, and we obtain several linear equations (see Proposition 1). Moreover, if the integer $N_B(w_{in}, w_{out})$ is very small (typically ≤ 6 for an 8-bit bus) then some bits can even be fixed, this will be discussed in Section 4.3.

Remark 3 Note that there are a lot of linear relations because there are two Hamming weight leakages around B. If only one Hamming weight leakage (input or output) is added to the equations of B then the number of solutions satisfying this condition is equal to the binomial $\binom{n}{w}$ and is generally (if $w \neq 0, n$) too big to fix some bits and to obtain interesting linear equations. This situation is very similar to the Hamming distance model (see Section 3.3).

The next section studies the Hamming distance leakage which is a more general model than the Hamming weight model. Its main purpose is to study the relevance of the Algebraic Immunity with Leakage and the proposed invariant N_B with a different leakage model.

3.3 Hamming distance leakage model

The Hamming distance model is often more suited than the Hamming weight model to describe the power consumption of a device (see [BCO04] or [MOP07] for instance). Indeed, the power consumption of a microcontroller, for instance with CMOS technology, is typically described by the number of modified bits in registers or buses (due to the presence of many connected components: capacitors, logic/sequential cells etc...). The consumption of a transition from a value x to a value y is then modeled by $HD(x, y) = HW(x \oplus y)$.

The measured leakages in real devices strongly depend on the implementation. Thus, many different scenarios could be considered with the Hamming distance leakage model (for instance, the distance could be measured between different points). The aim of this analysis being to study the influence of additional information on the algebraic solving step, we do not necessarily seek the most realistic scenarios. Instead, we especially want to check the relevancy of the proposed analysis. In the ASCA context, similar to the Hamming weight model (Section 3.2), we will first assume that an initial on-line phase provides the Hamming distances between input and output of a black box B. We refer to Section 6 for a discussion about this assumption and consideration of other models.

As before, the Algebraic Immunity with Leakage is equal to 1 for every black box B. This is a consequence of Lemma 1 since the system of equations representing an Hamming distance is the system (1) where we substitute $X_i \oplus Y_i$ for X_i. Indeed, if we consider the ideal $I_d \subset \mathbb{F}_2[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ generated by the equations representing B, the field equations and by L_d (1) the equations representing the Hamming weight d of the XOR between the input and the output, namely:

$$I_d = \langle L_d(X_1 + Y_1, \ldots, X_n + Y_n) \cup S_B \cup S_{\text{Field Eq.}} \rangle$$

then we have the following proposition

Proposition 3 *Let G be the Gröbner basis of the ideal I_d for a graded monomial order. G contains at least one linear polynomial.*

Proof According to Lemma 1, we know that the ideal I_d always contains the polynomial

$$f = (X_0 + Y_0) + \cdots + (X_n + Y_n) + (d \bmod 2) \in I_d$$

The rest of the proof is similar to the proof of Proposition 2. □

Then there is always at least one linear equation when the Hamming distance equations are added to the system of equations corresponding to B. In the same way as previously, there could be many more in function of the Hamming distance. Once again, by Proposition 1, the number of independent linear equations is linked to the number of points which satisfy this Hamming distance. Thus, we define N_B in the case of the Hamming distance by

$$N_B(d) = \#\{x \in \mathbb{F}_2^n \text{ s.t. } HD(x, B(x)) = d\}$$

Unfortunately, in contrary to the Hamming weight model, there is rarely more than one linear polynomial in the Gröbner basis, what is due to $N_B(d)$ which is larger than previously (see Section 6 for the experiments done for PRESENT and AES).

In the next section we will study more precisely the influence of the number of independent linear relations on the complete solving.

4 Solving the complete system modeling the block cipher

As explained in Section 2, the problem is modeled by a system of equations which has a particular block diagonal structure. More precisely, it is composed of blocks of equations which correspond to the cipher rounds with the leakage information. Each block is composed of systems of equations corresponding to the black boxes (S-boxes, MixColumns) and leakages of corresponding input and output data. We can split the complete system into small systems and locally study each of them. This local study is described in Section 3. We showed that the equations of the leakage model with the equations modeling one black box could yield a lot of low degree equations, such as linear equations, or could even give values of intermediate variables. Thanks to this particular structure, we have developed an efficient solving strategy.

4.1 Solving Strategy

The inputs of our off-line problem can be seen as a finite sequence $\mathcal{L}$ of values corresponding to the leakages of the successive 8-bit black boxes of the block cipher. In order to efficiently solve the complete polynomial system, we first seek the elements in $\mathcal{L}$ that provide the greatest possible number of linear relations. To do so, according to Section 3, we sort the sequence $\mathcal{L}$ by increasing N_B. Following this order, the polynomial systems corresponding to the first elements are those that provide the most linear equations. Thus, rather than computing directly a Gröbner basis of the complete system, we first compute Gröbner bases of some of these smaller systems. In a second step, we solve the complete system with the additional linear relations computed during the first step. This strategy based on splitting allows us to have better control on the maximal degree reached during the second step.

Remark 4 This strategy allows us to select some of the leakage ordered pairs in $\mathcal{L}$, in particular one could reject the leakages with large N_B and small confidence in their measurements during the on-line phase.

4.2 A Sufficient Condition of Success

In the last step of the solving strategy, a polynomial system with several independent linear equations has to be solved. The efficiency of this step is strongly correlated with the number of these linear relations. More precisely, the efficiency heavily depends on the number of independent linear relations between the inputs and the outputs of the black boxes B.

n	35	47	56	64	69	78	90
$\mathbb{P}(R_{PRESENT} \geq n)$	99%	90%	70%	50%	30 %	10%	1%

Fig. 1 Probability to obtain more than n linear equations with one PRESENT's round

For computational feasibility, it is assumed that the dispersion through a round of a block cipher is so important that the rounds are supposed to be independent. The black boxes of the same round are also supposedly independent. Thus, under this assumption, for a given block cipher based on a black box B, the total number of linear relations only depends on the local study around B done in Section 2. From this local study, one can compute the distribution of the number of linear equations coming from the study of the polynomial system of one round.

Example with the block cipher PRESENT and Hamming weight leakage model.
In this example, the black box B is the 8-bit S-box built from two PRESENT S-boxes. From the study of the probability distribution of the random variable $L_{PRESENT}$ (see Section 6) measuring the number of linear relations obtained from the local study of B, one can see that half of the possible leakage values provide at least 8 linear independent relations. Thus, the expected number of linear equations obtained from the substitution layer of one round is equal to $8 \times E(L_{PRESENT}) \simeq 64$ for PRESENT and represents a practical behavior. Hence, the expected number of linear equations is about the same size as the block length for one round and $n \times k$ for the complete system with n rounds with leakages.

From the probability distribution of $L_{PRESENT}$, we computed the distribution of the random variable $R_{PRESENT}$ measuring the number of linear relations obtained with all S-boxes and all Hamming weight leakages of one round of PRESENT. Figure 1 shows some of these results. According to them, the probability of obtaining at least 64 linear relations is about 50% with PRESENT. Thus, the expected number of linear equations has a high probability of being reached even with a small number of rounds with leakage information.

Considering these results, we propose a sufficient condition for an effective Algebraic Side Channel Attack. This condition is defined in a very simple way. Indeed, the local study of the non-linear part of a block cipher seen as a black box done in Section 3 gives an easy way to estimate the total number of low degree equations. This local study relies on the new notion of Algebraic Immunity with Leakage, which is itself linked

to the function N_B as proved in Section 2. This function is very easy to compute from the definition of the black box and provides the following general condition.

Sufficient condition of success Let B be an n-bit black box. If $N_B(l)$ (see Definition 3) is small enough (say less than n) for half of the possible leakages l then a block cipher based on B is vulnerable to an Algebraic Side Channel Attack with Gröbner Basis method.

In a Gröbner basis point of view, this condition implies (from Proposition 1) that at least half of the leakages provide more than n independent linear relations. Thus, the final polynomial system will be at least "half" linearized and (generally) easy to solve. In practice, this condition of success has been successfully applied for different black boxes constructed from S-boxes of well-known block ciphers. For instance, we showed that N_B is often small for PRESENT S-box with the Hamming weight leakage model, which explained the linearization of the full system of equation.

This sufficient condition of success can be expressed more precisely in practice by mean of a complexity bound. Indeed, the proposed invariant N_B can be used to compute the complexity of the exhaustive search on inputs (and outputs) of the corresponding layer. Recall that $N_B(l)$ is equal to the number of possible input (or output) values for a black box B giving the leakage l. Thus, for a given n-bit black box B, the number of possible values decreases from 2^n to $N_B(l)$ thanks to the leakage l. For a fixed encryption and for a given layer with black boxes B_1 to B_m with the corresponding known leakage l_1 to l_m, the cost of exhaustive search on this layer is precisely equal to $\prod_{i=1}^{m} N_{B_i}(l_i)$. When the possible values of N_B are (almost) evenly distributed, the expected value of N_B is also a very good indicator and could be used to compute the average complexity of the exhaustive search of an input and an output of a round. Once more, we could assume that the rounds, as well as the boxes of a given round, are independent. Thus, the expected number of possible input values of the layer is $E(N_B)^m$ with m the number of boxes per rounds. In this case, the sufficient condition of success could be restated by saying that the block cipher is vulnerable to ASCA if this expected value implies that the complexity to recover the secret key is less than the assumed computing power of an attacker. This is usually the case in practice for PRESENT with the Hamming weight leakage model, where we have $E(N_B) \simeq 12.29$ and the average complexity of the exhaustive search of the layer input is $E(N_B)^8 \simeq 2^{29}$ (by comparison with a complexity of 2^{64} without leakage information). This condition is only sufficient because it does not consider implications from one leakage to the entire system and the ability of tools such that SAT solvers to exploit them.

Such a condition of success explains why it is possible to attack a block cipher when all the leakages of all the rounds are known and gives a first complexity bound for this attack. On the other hand, the authors of [RS09] showed that three or four consecutive leakages rounds are sufficient to quickly solve the complete polynomial system (see annex B where we reproduce the experimental results presented in [RS09, RSVC09]). Counting the number of linear equations given by these rounds is not sufficient to explain the efficiency of the method, in particular for the unknown Plaintext and Ciphertext scenario and the similarity between these results and those obtained in the known PC scenario. Moreover, the sufficient condition expressed in terms of exhaustive search can be improved by taking into account the implications between different rounds. Thus, in the next section, we study the particular situation where the leakages correspond to a few consecutive rounds.

4.3 Consecutive leakages

First we consider the basic case of two face to face black boxes B_1 and B_2 of consecutive rounds (Figure 2). The best case is when N_{B_i} ($i = 1$ and 2) is small enough ($<< n$ the bus size), such that the linear relations coming from the local study at B_1 and B_2 successfully fixed intermediate bits. For example, assume that two face to face bits y_i and x_j in the output of B_1 and the input of B_2 (see Figure 2) are known by the local study of B_1 and B_2 with Hamming weight leakages. The complete system of equations contains the equations modeling the permutation layer and the bitwise XOR (see Section 2), hence, during the second step of the strategy, the subkey bit k_j is easily deduced from the knowledge of the value of y_i and x_j. Once a subkey bit is fixed, other subkey bits in other rounds can be found with the key schedule equations.

Remark 5 This point of view explains why it is harder to successfully attack the problem with unknown plaintext and ciphertext when we do not know such consecutive leakages (see Appendix B when the number of rounds of Hamming weight information is less than 15 for PRESENT, and less than 5 for AES).

Following our sufficient condition and the study done in this section, the solving efficiency is due to a small N_B in average for the black box B. In the following, we exhibit a family of black boxes which are as far removed as possible from the condition of success and we

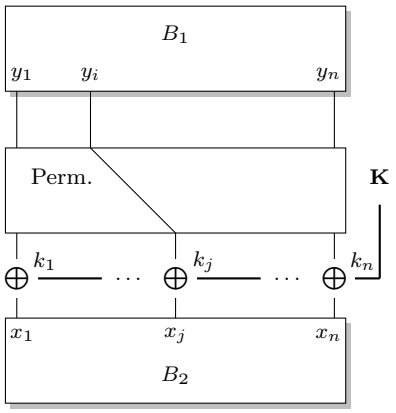

Fig. 2 Example of two consecutive rounds

verify experimentally that they are more resistant to algebraic side channel attacks. The condition of success exhibited in this section is not a necessary condition but the results of the next section tend to show that it is very close to be criterion of success.

5 Characterization of a family of resistant S-Boxes

Generally in the design of block ciphers using a substitution-permutation networks, S-boxes are the non-linear part. Thus, the S-boxes must be carefully chosen to make the cipher resistant against cryptanalysis. In our attacks, the S-boxes (seen as black boxes) leak information from the manipulated data. In this section, we only consider the situation covered by the Hamming weight model (i.e. a leakage l will be a couple of values corresponding to the Hamming weight of the input and output of the black box B). For the distance model a study is done, for example, in [Pro05]. The knowledge of this additional information enables us to model this cipher component by a system of equations containing $\#AI_L$ linear relations. As seen in Section 3.2, $\#AI_L$ clearly depends on the Hamming weight pairs but also on the black box. The expected value of the number of such linear relations is very large (greater than 7). These S-boxes are weak for our attacks and we are looking for a criterion for more resisting S-boxes. We study the influence of the black box on our criterion $N_B(w_{in}, w_{out})$, which is linked to $\#AI_L(B, w_{in}, w_{out})$. For that, we study the extreme case represented by the family of S-Boxes in complete contradiction with the sufficient condition of success exhibited in Section 4.2.

Since $N_B(w_{in}, w_{out})$ is explicitly given as the cardinality of the sets $\{x \in \mathbb{F}_2^n \text{ s.t. } HW(x) = w_{in} \text{ and } HW(B(x)) = w_{out}\}$, it is clear that a bijective black box B maximizing $N_B(w_{in}, w_{out})$ for every possible pair (w_{in}, w_{out}), must be such that the sets $HW^{-1}(w_{in})$ and $B^{-1}(HW^{-1}(w_{out}))$ have precisely the same elements. Moreover, in this case, we have

$$N_B(w_{in}, w_{out}) = \binom{n}{w_{in}} = \binom{n}{w_{out}}$$

Indeed for all $w \in \mathbb{N}$ and for all bijective black box B, we have

$$\#HW^{-1}(w) = \binom{n}{w} \text{ and } \#B^{-1}(HW^{-1}(w)) = \binom{n}{w}$$

Actually, a bijective black box B maximizing $N_B(w_{in}, w_{out})$ for every possible pair (w_{in}, w_{out}), must satisfy

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

Then such black box factors into

$$B(x) = \pi(x) \oplus f(HW(x))(1, \ldots, 1)$$

where π is a permutation stable under the Hamming weigth and f is a boolean function such that $f(HW(x)) = f(n - HW(x))$.

Example 3 The following table describes such an optimal 4-bit S-Box:

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

Therefore, there are optimal black boxes in the sense of maximizing N_B for every possible leakage, and experiments confirm that some of them are more resistant to our attacks. However, it seems that such black boxes are not resistant to differential and linear cryptanalysis. In the particular case of an even bus size, we are able to prove the following proposition:

Proposition 4 *Let n be an even number and let assume that the leakage model is the Hamming weight one. The n-bit black boxes in a complete contradiction with the sufficient condition of success (see Section 4.2) for an ASCA, i.e. satisfying $HW^{-1}(w_{in}) = B^{-1}(HW^{-1}(w_{out}))$, are not resistant to linear cryptanalysis. Actually, affine components exist for these S-boxes.*

Proof Let B be an n-bit black box verifying the assumptions of the proposition. In this case, we already saw that

$$N_B(w_{in}, w_{out}) = \binom{n}{w_{in}} = \binom{n}{w_{out}}$$

Thus, $w_{in} = w_{out}$ or $w_{in} = n - w_{out}$ which implies that $w_{out} \equiv w_{in} \mod 2$ in the case where n is an even integer. Hence we have $(1, \ldots, 1) \cdot B(x) = (1, \ldots, 1) \cdot x$ and the nonlinearity of B is equal to 0. □

In the case where n is an odd number, we could find some ASCA-resistant black boxes with a linearity slightly less than 2^n. However, all these found black boxes stay weak against linear cryptanalysis. Hence, the question arises of determining whether ASCA optimally resistant S-boxes can reach a good nonlinearity. But we were not able either to prove the inexistence of ASCA optimally resistant black boxes with a strong resistance against linear cryptanalysis, in spite of the following rewriting using the Krawtchouk polynomials $K_{n,w}$, which establishes a relation between the function N_B and the Walsh coefficient (essential for computing the linearity of a box). Krawtchouk polynomials are classical orthogonal univariate polynomials over the rationals associated with the binomial distribution. They are defined by

$$K_{n,w}(X) = \sum_{j=0}^{n} (-1)^j \binom{X}{j} \binom{n-X}{w-j}$$

We have $K_{n,w}(0) = \binom{n}{w}$ and for all $a \in \mathbb{F}_2^n$, we have

$$\sum_{x \in \mathbb{F}_2^n | HW(x)=w} (-1)^{a \cdot x} = K_{n,w}(HW(a)) \tag{3}$$

By the inverse Fourier transform, we deduce from (3) that for all $w = 0, \ldots, n$,

$$\sum_{a \in \mathbb{F}_2^n} K_{n,w}(HW(a))(-1)^{a \cdot x} = \begin{cases} 2^n \text{ if } HW(x) = w \\ 0 \qquad \text{otherwise} \end{cases}$$

Finally, for all $w, w' = 0, \ldots, n$, we have

$$\begin{aligned} &N_B(w, w') \\ &= \#\{x \in \mathbb{F}_2^n | HW(x) = w,\ HW(B(x)) = w'\} \\ &= 2^{-2n} \sum_{a,b,x \in \mathbb{F}_2^n} K_{n,w}(HW(a)) K_{n,w'}(HW(b))(-1)^{a \cdot x + b \cdot B(x)} \\ &= 2^{-2n} \sum_{a,b \in \mathbb{F}_2^n} K_{n,w}(HW(a)) K_{n,w'}(HW(b)) B_b^{\mathcal{W}}(a) \end{aligned}$$

where $B_b^{\mathcal{W}}(a) := \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot B(x)}$ be the Walsh transform of B.

Actually, as already proposed in [RS09], it seems that one of the safest way to design a substitution box resistant to all kinds of attacks is to increase the bus size. Indeed, $N_B(w_{in}, w_{out})$ also depends on the bus size n, and for all bijective black boxes, since $N_B(w_{in}, w_{out})$ defines a partition of $\mathbb{F}_2^n$ we have

$$\sum_{(w_{in}, w_{out}) \in \mathbb{N}^2} N_B(w_{in}, w_{out}) = 2^n$$

This shows that, in general, $N_B(w_{in}, w_{out})$ grows exponentially as n increases.

6 Experiments

In this part we show that the condition of success from Section 4.2 is supported by the experiments (positive and negative) we performed for PRESENT, AES and for the resistant S-box given in Section 5. Following our model described in Section 2, we build a complete system of polynomial equations as a function of the target cipher (PRESENT or AES) and as a function on the sequence $\mathcal{L}$ of leakage information which are taken into account. Since Magma [BCP97] provides an efficient implementation of the Faugère F4 algorithm, we use this computer algebra system for our experiments. For the SAT attacks, we use CryptoMiniSat [SNC09], glucose2, glueminisat, and plingeling which are the winners of the SAT Race 2010 and SAT Race 2011.

6.1 Experiments against PRESENT using the Hamming weight model

Here, the leakage comes from the inputs and outputs of S-boxes (we see two consecutive 4-bit PRESENT S-boxes as an 8-bit one).

PRESENT is a very simple Substitution-Permutation Network designed by Bogdanov *et al.* [BKL+07] for hardware efficiency and for extremely constrained environments. The non-linear layer uses a single 4-bits S-box S which is applied 16 times in parallel in each round. The action of this box is given by the following table.

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

Following the situation of [RS09], we assume that the device leaks the Hamming weights of the values commuting on its 8-bit bus. In this case, two S-boxes are processed at the same time, which is represented by a 8-bit black box B. From the definition of B one can easily deduce the table 3 giving $N_B(w_{in}, w_{out})$ in function of the input/output couples. We compare this table with the one (see Table 4) given $\#AI_L(B, w_{in}, w_{out})$ in function of the same couples. One can see that $N_B(w_{in}, w_{out})$ can give a good indicator when we are interested in maximizing the number of independent linear polynomials $\#AI_L(B, w_{in}, w_{out})$ during an algebraic attack. Even if $\#AI_L(B, w_{in}, w_{out})$ is not rigorously inversely proportional to $N_B(w_{in}, w_{out})$ it is close to be the case. A counterexample for this reciprocity is given by $N_B(3,3) = 12$ which is less than $N_B(2,4) = 18$ but $\#AI_L(B,3,3) = 5 < \#AI_L(B,2,4) = 8$.

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

Fig. 3 $N_B(w_{in}, w_{out})$ where B is two PRESENT S-Boxes

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						

Fig. 4 $\#AI_L(B, w_{in}, w_{out})$ where B is two PRESENT S-Boxes

Assume that the probability of appearing of an input byte of the 8-bit black box B is $1/256$. With Figures 3 and 4, we can easily compute the probability distribution of the random variable L_B measuring the number of linear relations that we obtain by adding the leakage information to our system. The Figure 5 presents a chart providing the probabilities $\mathbb{P}(L_B = k)$ inside the sectors labeled by k. The integers k that give null probability are not shown. We could note that the probability that at least 8 independent linear relations are produced is about 50%. Moreover, the expected value of L_B is $\simeq 7.9$.

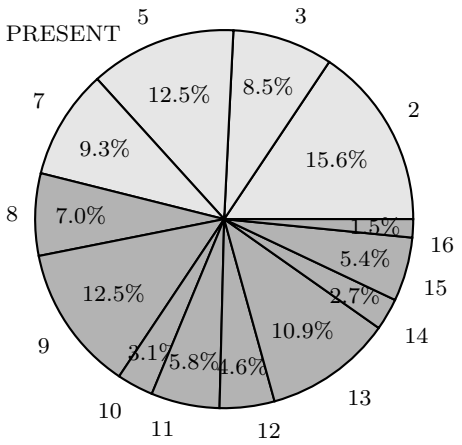

Fig. 5 $\mathbb{P}(L_B = k)$ for k with non zero probability and for HW leakages

We also compare Table 3 with the one given the number of fixed bits (see Table 6) in function of the input/output couples. One can see that when N_B is small the number of fixed bits can be large.

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0	0	0	0	0	16	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	0	8	10	0	4	8	0	0
3	0	0	0	0	0	0	0	0	0
4	16	10	4	0	0	0	4	6	16
5	0	4	4	0	0	0	2	4	0
6	0	10	2	10	0	6	8	0	0
7	0	0	6	0	4	0	0	0	0
8	0	0	16	0	0	0	0	0	0

Fig. 6 Number of fixed bits with two PRESENT S-Boxes

We will now use all this knowledge to explain the experiments behaviors observed during an algebraic attack of PRESENT under different scenarios.

As in [RS09], the knowledge of all Hamming weight pairs from the 31 rounds of PRESENT always leads to successful SAT solver and Gröbner attacks, in both cases known and unknown plaintext and ciphertext. Note that in this experiment, we already must apply our solving strategy (4.1). More precisely, we first have to successively compute the Gröbner basis of each round before computing the last Gröbner basis of the whole system. Indeed, if we try to directly compute the Gröbner basis of the system of equations modeling the initial problem, then the maximum degree reached during the computation is too big, and the computation is very slow.

Similar experiments allow us to check Remark 3: we explained that an important condition is the knowledge of the couple of Hamming weights around the S-box. So, we performed attacks on PRESENT with only the Hamming weights of input (or output) data of all S-Boxes. Our Gröbner basis solving strategy and SAT solvers are much less efficient, rather than failed, in this situation (which is very similar to the HD scenario). Indeed, without the knowledge of the plaintext and ciphertext, SAT solvers and Gröbner attacks always failed. It confirms that a large N_B, which could not fix enough intermediate bits (see Section 4.3), is not able to find subkey bits. Otherwise, if the plaintext and ciphertext were known, the low number of linear equations often allow some SAT solvers to recover the key. However, the solving step is very long with all used

SAT solvers (once again comparable to the HD model) and the Gröbner attack fails with an out of memory if we take much than 2 or 3 rounds. These experiments confirmed the necessity of always using weight couples.

Other experimental results confirmed that the number $N_B(w_{in}, w_{out})$ is a very good indicator to sort interesting Hamming weight couples for an ASCA. These experiments have checked Remark 4 for PRESENT. More precisely, one can reject the leakages (w_{in}, w_{out}) with large $N_B(w_{in}, w_{out})$ without consequences on the success rate. Conversely, if we reject the leakages (w_{in}, w_{out}) with small $N_B(w_{in}, w_{out})$ then all Gröbner basis attacks and all SAT attacks failed.

Following the condition of success, we also designed theoretically more resistant S-boxes in Section 5. Experiments with PRESENT, where we use such S-boxes as a substitute for original S-boxes, are also intractable (with both SAT and Gröbner) which confirm that these S-boxes are much more resistant to this kind of attack.

Thus, we are able to explain the experiments against PRESENT in [RS09]. In particular, the study in Section 4.3 explained the successful attacks when we know consecutive leakages. Note that the success rates given in [RS09, RSVC09] in the case of unknown plaintext and ciphertext attacks with randomly distributed leakage information (Appendix B) can be explained by the pigeonhole principle. For the example involving 31 rounds of PRESENT, the success rate is greater than zero when the number of rounds with leakages reaches approximately 15. By the pigeonhole principle, this corresponds to the case where there are at least two consecutive rounds with leakage and thus Section 4.3 explained these experimental results.

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0	0	0	0	0	1	0	0	0	0
1	0	0	2	0	1	3	2	0	0
2	0	2	3	8	5	4	4	2	0
3	1	1	4	17	16	10	5	2	0
4	0	3	9	11	21	16	9	1	0
5	0	1	7	10	19	14	3	2	0
6	0	0	3	7	5	8	4	0	1
7	0	1	0	2	2	1	1	1	0
8	0	0	0	1	0	0	0	0	0

Fig. 7 $N_B(w_{in}, w_{out})$ where B is the AES S-Box

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

Fig. 8 $\#AI_L(B, w_{in}, w_{out})$ where B is the AES S-Box

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0	0	0	0	0	16	0	0	0	0
1	0	0	10	0	16	6	12	0	0
2	0	10	7	2	3	2	6	10	0
3	16	16	2	0	0	0	2	10	0
4	0	10	0	0	0	0	2	16	0
5	0	16	1	0	0	0	5	8	0
6	0	0	6	1	3	1	6	0	16
7	0	16	0	10	8	16	16	16	0
8	0	0	0	16	0	0	0	0	0

Fig. 9 Number of fixed bits with the AES S-Box

6.2 Experiments against AES using the Hamming weight model

Here, the 8-bit leakage comes from the inputs and outputs of S-boxes and Mixcolumns.

The same study of the AES S-box B also shows (see Table 7 and Table 8) that $N_B(w_{in}, w_{out})$ is a very good indicator when we are interested in maximizing $\#AI_L(B, w_{in}, w_{out})$.

As before, we compute the probability distribution of the random variable L_B measuring the number of linear relations that we obtain by adding the leakage information to our system. The chart of the Figure 10 provides the probabilities $\mathbb{P}(L_B = k)$ inside the sectors labeled by k. The integers k that give null probability are not shown.

Surprisingly, the probability that at least 8 independent linear relations are produced is also about 50%, and the expected value of L_B is $\simeq 7.3$ which is almost equal as for PRESENT.

In the same way as PRESENT, we will now use all this knowledge to explain the experiments behaviors observed during an algebraic attack of AES under different scenarios.

As in [RSVC09] and [RS09], the knowledge of all Hamming weight pairs (i.e. around the S-boxes and around the Mixcolumns) from the 10 rounds of AES always leads to successful SAT and Gröbner attacks, in the case of known plaintext and ciphertext. The ASCA in unknown plaintext and ciphertext scenario is effective only with SAT solvers, the Gröbner computation requiring too much memory space.

Note that we only took the Hamming weights of the input and the output of the Mixcolumns step. Thus,

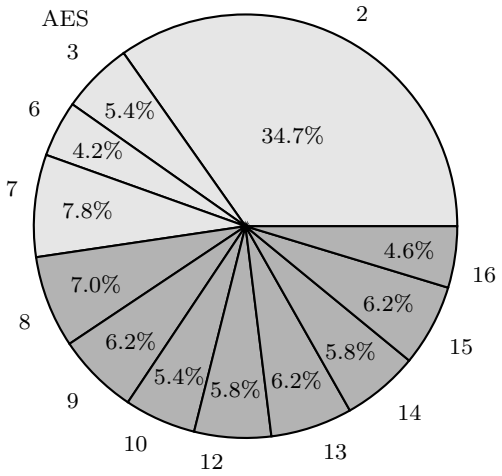

Fig. 10 $\mathbb{P}(L_B = k)$ for k with non zero probability and for HW leakages

the MixColumns transformation is seen as a black box and then, contrary to the experiments described in the article [RSVC09], previous ASCA are effective against AES even if the MixColumns operation is implemented as a table look-up. This difference of experimental results may be explained by the advances in SAT solvers heuristics.

The Mixcolumns transformation being a linear step, we also wonder whether its leakage was required. The experiments with only the Hamming weights leakage of the S-boxes (i.e. without leakage from MixColumns) are effective with SAT solvers, even if the solving step is much longer (in average a couple of hours against several dozen seconds).

We also make experiments with the theoretically resistant S-boxes designed in Section 6, which confirm that AES with these S-boxes are more resistant to both SAT and Gröbner attacks.

6.3 Experiments against PRESENT and AES using the Hamming distance between input and output of S-Boxes

In this model, similar to the Hamming weight model, we assume that an initial on-line phase only provides the 8-bit Hamming distances between input and output of the S-boxes. It should be noted that using only the Hamming distance between input and output of the S-Boxes seems too restrictive, as well as being not very realistic. Indeed, we should also assume that other distances are known, which of course would increase the efficiency and success rate of the attack. However, this model stays interesting because the purpose of these experiments is above all to confirm the relevance of the proposed criteria.

d	0	1	2	3	4	5	6	7	8
$N_B(d)$	0	0	16	56	81	64	30	8	1
$\#AI_L(B,d)$	0	0	10	3	1	1	1	9	16
Nb fixed bits	0	0	0	0	0	0	0	0	16

Fig. 11 HD model and 2 PRESENT's S-Boxes

d	0	1	2	3	4	5	6	7	8
$N_B(d)$	0	12	31	48	67	59	32	7	0
$\#AI_L(B,d)$	0	5	1	1	1	1	1	10	0
Nb fixed bits	0	0	0	0	0	0	0	1	0

Fig. 12 HD model and AES S-Box

We already foretold (see Section 3.3) that an ASCA will be much more difficult in this case. Actually, there is always at least one linear equation (see Proposition 3) when the Hamming distance equations are added to the system of equations corresponding to PRESENT or AES S-boxes but, unfortunately, in contrary to the Hamming weight model, there is rarely more than one. This fact can be explained for PRESENT and AES by studying the functions N_{PRESENT} and N_{AES} respectively. The Tables 11 and 12 detail the distribution of these functions and the corresponding $\#AI_L$ for AES and PRESENT S-boxes.

As one can see, the functions N_{PRESENT} and N_{AES} often take very large values. Thus, the number of expected linear relations will be very small. Moreover, one can guess that the number of linear relations for AES will be less than for PRESENT (since there are more large values for N_{AES} than for N_{PRESENT}). Actually, the expected number of linear relations is about 2.3 for PRESENT and 1.4 for AES S-Boxes (with an assumption on equiprobability distribution of input bytes), which is much less than in the case of the Hamming weight model (between 7 and 8, as seen above). It becomes manifest that a Gröbner attack will be much more difficult in this case. Actually, Gröbner attack in this situation needs too much memory to be practical.

In practice, we were not able to mount a complete Gröbner attack with 31 rounds of PRESENT (an attack on 3 rounds of PRESENT has been successful, but an out of memory error occurs with more rounds). Nonetheless, in known plaintext and ciphertext scenario, the constraints on the intermediate variables given by the Hamming distance equations seem sometimes sufficient for SAT solvers that we used. The solving time seems strongly dependent on the heuristics of the SAT solver and so it is difficult to correlate them to the number of linear equations or their distribution.

On the other hand, as we suspected by studying the function N_{AES}, every ASCA experiments on AES

with the Hamming distance leakage model have failed. This fact can be explained by the more complex algebraic structure of AES (including its keyschedule) which seems to avoid ASCA with only the Hamming distances between the inputs and outputs of S-Boxes.

Moreover, the chance to find the value of an intermediate bit is very low, which explains the negative experiments in unknown plaintext and ciphertext scenario in this case.

6.4 Experiments against PRESENT using the Hamming distance between consecutive encryptions

An interesting extension would be also to consider the leakages between consecutive encryptions of different plaintexts. This model provides, for a given spot, the Hamming distances between successive encryptions. As usual, we consider the 8-bit Hamming distances between inputs of all S-boxes from two consecutive encryptions with PRESENT, with a fixed secret key. The same goes with the outputs of all S-boxes.

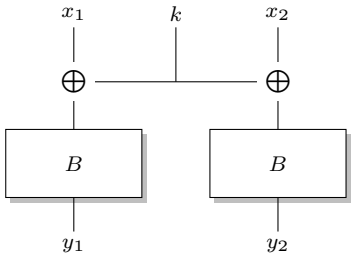

Fig. 13 Two encryptions with the same key

As presented in Figure 13, this model provides the Hamming distances $HD(x_1 \oplus k, x_2 \oplus k) = HD(x_1, x_2)$ and $HD(y_1, y_2) = HD(B(x_1 \oplus k), B(x_2 \oplus k))$. Thus, at the first round for instance, x_1 and x_2 are bytes of the plaintexts, then we assume that they are known and only the Hamming distance of the outputs are interesting (the same goes with the Hamming distances of inputs at the last round). In this particular case, for given x_1 and x_2, our invariant $N_B(d_{out})$ is defined by $\{k \in \mathbb{F}_2^8 \text{ s.t. } HD(B(x_1 \oplus k), B(x_2 \oplus k)) = d_{out}\}$, which is very similar to the previous Hamming distance between input and output of S-Boxes (Section 6.3). For instance, Figure 15 shows the values of $N_B(d_{out})$ and $\#AI_L(B, d_{out})$ when x_1=0xD8 and x_2=0xB1. Notice that the number of linear equations is often large despite the fact that N_B is also large. But, many of these equations are just equalities between the $3n$ unknown bits, hence are useless for fixing bits of the key.

nb of rounds	8	10	12	15	16
$\prod N_B$ last round	2^{47}	2^{48}	2^{50}	$2^{47.7}$	$2^{47.7}$
cryptominisat-2.9	2012	9984	2728	4581	19336
glucose2	1600	2794	12919	2716	17756
nb of rounds	19	20	21	30	50
$\prod N_B$ last round	$2^{43.5}$	2^{49}	2^{41}	$2^{47.4}$	$2^{47.2}$
cryptominisat-2.9	929	4080	2266	5973	11085
glucose2	4999	11144	2648	5050	2240

Fig. 14 Solving times in second of experiments against PRESENT using the Hamming distance between consecutive encryptions

d_{out}	0	1	2	3	4	5	6	7	8
$N_B(d_{out})$	0	0	32	48	64	64	32	16	0
$\#AI_L(B, d_{out})$	0	0	15	12	9	9	14	20	0
Nb fixed bits	0	0	2	0	0	0	0	0	0

Fig. 15 HD between 2 consecutive encryptions with PRESENT when x_1=0xD8 and x_2=0xB1

In practice, we have only done experiments on the very simple block cipher PRESENT with the fixed plaintexts and the fixed key shown in annexe C. The results are reported in figure 6.4. In the experiments we have done, the SAT solver attacks worked when there are leakages in all PRESENT's rounds, although the computation time can be very different between two instances. Following the condition of success, the exhaustive search on the 64 used bits of the last subkey is reduced to a complexity between 2^{41} and 2^{50}. The SAT solvers are much faster since they do not only use information of the last round, but also from previous rounds (and especially from the first round) thanks to the simplicity of the PRESENT key schedule.

As in Section 6.3, the Gröbner attack needed too much memory to solve the system with this model. Moreover, leakages on the round, on the last round, plaintext and ciphertext are all mandatory; all attacks without one of these have failed.

7 Conclusion

In this article we introduced a new criterion for the effectiveness of ASCA. This criterion rely on a new notion of algebraic immunity. In order to simplify the analysis of a given block cipher we introduce an invariant related to this block cipher. This invariant is a function which can be easily defined and computed from the definition of the given block cipher (no need of advanced algebra). From this new invariant we exhibit a sufficient condition of success of an ASCA and we were able to theoretically explain the experiments done by Renauld, Standaert and Veyrat-Charvillon in [RS09, RSVC09] by studying the distribution of the values taken by this

function. Experimental results confirmed our sufficient condition success and showed that it is a good condition for both effective Gröbner and SAT solver attacks. This understanding allowed us to design S-boxes optimally resistant to ASCA following this condition. However, we observe that these S-boxes are weak for linear and differential cryptanalysis, which confirms, as observed in [RS09], that a large bus size can be prescribed to design a resistant block ciphers. Following our new invariant for a block cipher, and with our experiments, we also show the influence of the leakage model over ASCA. In this paper, we studied the Hamming weight and Hamming distance leakage models, but other good leakage models can be selected. Some results on the influence of the leakage model over ASCA have already been presented (see [RS10]). They are all rely on experimental studies using SAT solvers, we will address the comparison of our approach with them in a future research paper. More generally, extending the attack to deal with erroneous equations is one of our long-range research aims. The well understanding of the algebraic phase of this attack done in this article is already a first step in this direction.

8 Acknowledgments

This work has greatly benefited from highly relevant comments of anonymous reviewers. The authors would like to thank them sincerely for their suggestions that improved this paper. They also thank O. Orcière for his rereadings and for his constructive comments.

References

[AA05] Frederik Armknecht and Gwénolé Ars. Introducing a new variant of fast algebraic attacks and minimizing their successive data complexity. In *Mycrypt*, pages 16–32, 2005.

[ABDM00] Mehdi-Laurent Akkar, Régis Bevan, Paul Dischamp, and Didier Moyart. Power Analysis, What Is Now Possible... In *ASIACRYPT*, pages 489–502, 2000.

[AC10] Martin Albrecht and Carlos Cid. Cold Boot Key Recovery using Polynomial System Solving with Noise. In *2nd International Conference on Symbolic Computation and Cryptography*, 2010.

[AF05] Gwénolé Ars and Jean-Charles Faugère. Algebraic Immunities of functions over finite fields. Research Report RR-5532, INRIA, 2005.

[AIK+00] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms, 2000.

[AK06] F. Armknecht and M. Krause. Constructing Single- and Multi-Output Boolean Functions with Maximal Immunity. In *Proceedings of ICALP 2006*, pages 180–191. Lecture Notes of Computer Science 4052, 2006.

[Ars05] Gwénolé Ars. *Applications des bases de Gröbner en cryptographie.* PhD thesis, University of Rennes, 2005.

[Bar04] Magali Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.* PhD thesis, Université de Paris VI, 2004.

[BCO04] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In *CHES'04*, pages 16–29, 2004.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The MAGMA algebra system: the user language. *J. Symb. Comput.*, 24:235–265, October 1997.

[BFS04] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the Complexity of Gröbner Basis Computation of Semi-Regular Overdetermined Algebraic Equations. In *Proc. of International Conference on Polynomial System Solving (ICPSS)*, pages 71–75, 2004.

[BFSY05] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Bo-Yin Yang. Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems. In *Proc. of MEGA 2005, Eighth Inter. Symposium on Effective Methods in Algebraic Geometry*, 2005.

[BKL+07] A. Bogdanov, L. R. Knudsen, G. Le, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In *CHES'07*. Springer, 2007.

[BKP08] Andrey Bogdanov, Ilya Kizhvatov, and Andrei Pyshkin. Algebraic Methods in Side-Channel Collision Attacks and Practical Collision Detection. In *INDOCRYPT*, pages 251–265, 2008.

[Bog07] Andrey Bogdanov. Improved Side-Channel Collision Attacks on AES. In Carlisle Adams, Ali Miri, and Michael Wiener, editors, *Selected Areas in Cryptography*, volume 4876 of *Lecture Notes in Computer Science*, pages 84–95. Springer Berlin / Heidelberg, 2007.

[Bog08] Andrey Bogdanov. Multiple-Differential Side-Channel Collision Attacks on AES. In E. Oswald and P. Rohatgi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2008 Proceedings*, volume 5154 of *Lecture Notes in Computer Science*, pages 30–44. Springer-Verlag, 2008.

[Car09] Claude Carlet. *On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions*, volume 13 of *NATO Science for Peace and Security Series, D: Information and Communication Security*, pages 104–116. IOS Press, 2009.

[Car10] Claude Carlet. *Vectorial Boolean Functions for Cryptography*, pages 398–469. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, 2010.

[CJRR99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards Sound Approaches to Counteract Power-Analysis Attacks. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, pages 398–412. Springer-Verlag, 1999.

[CL05] Carlos Cid and Gaëtan Leurent. An Analysis of the XSL Algorithm. In *ASIACRYPT*, pages 333–352, 2005.

[CLO07] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction*

to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics). Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[CM03] Nicolas Courtois and Willi Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback. In *EUROCRYPT*, pages 345–359, 2003.

[CP02] Nicolas Courtois and Josef Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In *ASIACRYPT*, pages 267–287, 2002.

[Fau99] Jean-Charles Faugère. A New Efficient Algorithm for Computing Gröbner bases (F4). In *Journal of Pure and Applied Algebra*, pages 75–83. ACM Press, 1999.

[Fau02] Jean-Charles Faugère. A New Efficient Algorithm for Computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

[FdVP08] Jean-Charles Faugère, Françoise Levy dit Vehel, and Ludovic Perret. Cryptanalysis of MinRank. In *CRYPTO*, pages 280–296, 2008.

[FJ03] Jean-Charles Faugère and Antoine Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In *CRYPTO*, pages 44–60, 2003.

[FM07] Simon Fischer and Willi Meier. Algebraic Immunity of S-Boxes and Augmented Functions. In *FSE*, pages 366–381, 2007.

[FP06a] Jean-Charles Faugère and Ludovic Perret. Cryptanalysis of $2R^-$ Schemes. In *CRYPTO*, pages 357–372, 2006.

[FP06b] Jean-Charles Faugère and Ludovic Perret. Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects. In *EUROCRYPT*, pages 30–47, 2006.

[HP06] Helena Handschuh and Bart Preneel. Blind Differential Cryptanalysis for Enhanced Power Attacks. In *Selected Areas in Cryptography*, pages 163–173, 2006.

[MME10] Amir Moradi, Oliver Mischke, and Thomas Eisenbarth. Correlation-Enhanced Power Analysis Collision Attack. In *CHES'10*, 2010.

[MOP07] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks : Revealing the Secrets of Smart Cards*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[Off06] Office of State Commercial Cryptography Administration. The SMS4 block cipher (in chinese), 2006. `http://www.oscca.gov.cn/UpFile/20062101642319799O.pdf`.

[OKPW10] Yossef Oren, Mario Kirschbaum, Thomas Popp, and Avishai Wool. Algebraic Side-Channel Analysis in the Presence of Errors. In *CHES'10*, 2010.

[Pro05] Emmanuel Prouff. DPA Attacks and S-Boxes. In *FSE*, pages 424–441, 2005.

[RS09] Mathieu Renauld and Francois-Xavier Standaert. Algebraic Side-Channel Attacks. In *Inscrypt 2009*. LNCS, Springer-Verlag, 2009.

[RS10] Mathieu Renauld and Francois-Xavier Standaert. Representation-, leakage- and cipher- dependencies in algebraic side-channel attacks. In *ACNS 2010 Industrial Track*, pages 1–18, 2010.

[RSVC09] Mathieu Renauld, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA. In *CHES'09*, pages 97–111, Berlin, Heidelberg, 2009. Springer-Verlag.

[SLFP04] Kai Schramm, Gregor Leander, Patrick Felke, and Christof Paar. A Collision-Attack on AES Combining Side Channel and Differential Attack. In *CHES'04*, pages 163–175, 2004.

[SNC09] Mate Soos, Karsten Nohl, and Claude Castelluccia. Extending SAT Solvers to Cryptographic Problems. In *SAT*, pages 244–257, 2009.

[SWP03] Kai Schramm, Thomas Wollinger, and Christof Paar. A new class of collision attacks and its application to DES. In *Fast Software Encryption FSE 03, volume LNCS 2887 of LNCS*, pages 206–222. Springer-Verlag, 2003.

A Annex : A study of several S-Boxes and 8-bit Hamming weight leakage model

In this part, we provide tables showing the distribution of N_B for different S-Boxes with the Hamming weight leakage model. All the results show that these S-boxes are weak against an ASCA.

A.1 CAMELLIA S-Boxes

CAMELLIA [AIK+00] is a block cipher developed by NTT and Mitsubishi in 2000. It is a Feistel cipher and uses four 8-bit S-Boxes. S-Box1 is given by a table and S-Box2, S-Box3 and S-Box4 are defined using S-Box1 as follows:

$$\text{S-Box2}[X] = \text{S-Box1}[X] \lll 1$$
$$\text{S-Box3}[X] = \text{S-Box1}[X] \lll 7$$
$$\text{S-Box4}[X] = \text{S-Box1}[X \lll 1]$$

where the symbol $\lll$ correspond to left rotation operation. Because of these definitions, it is easy to see that the four S-boxes have the same Hamming weights distribution. Thus, the Figures 16, 17 and 18 equally correspond to the four S-boxes.

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0	0	0	0	1	0	0	0	0	0
1	0	0	1	3	3	1	0	0	0
2	0	1	3	6	6	7	2	3	0
3	1	0	3	15	16	16	4	1	0
4	0	4	12	11	19	14	8	1	1
5	0	2	5	11	17	10	8	3	0
6	0	0	3	7	8	5	5	0	0
7	0	1	1	2	1	2	1	0	0
8	0	0	0	0	0	1	0	0	0

Fig. 16 $N_B(w_{in}, w_{out})$ where B is one of the CAMELLIA S-Boxes

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

Fig. 17 $\#AI_L(B, w_{in}, w_{out})$ where B is one of the CAMELLIA S-Boxes

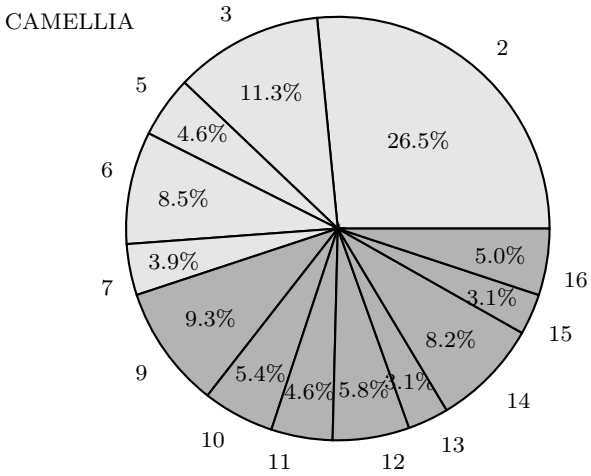

Fig. 18 $\mathbb{P}(L_B = k)$ for k with non zero probability and for HW leakages

A.2 SMS4 S-Box

SMS4 [Off06] is a block cipher used in the Chinese WLAN National Standard. It uses an 8-bit S-Box given by a table. The following Figures show its Algebraic Immunity with Hamming weights Leakage.

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	1	0	0	0
1	0	0	1	1	4	2	0	0	0
2	0	1	4	7	9	4	1	2	0
3	0	2	7	12	10	14	8	3	0
4	1	2	6	23	16	14	7	1	0
5	0	2	6	8	21	11	5	2	1
6	0	0	2	3	9	7	7	0	0
7	0	1	1	2	1	3	0	0	0
8	0	0	1	0	0	0	0	0	0

Fig. 19 $N_B(w_{in}, w_{out})$ where B is the SMS4 S-box

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

Fig. 20 $\#AI_L(B, w_{in}, w_{out})$ where B is the SMS4 S-box

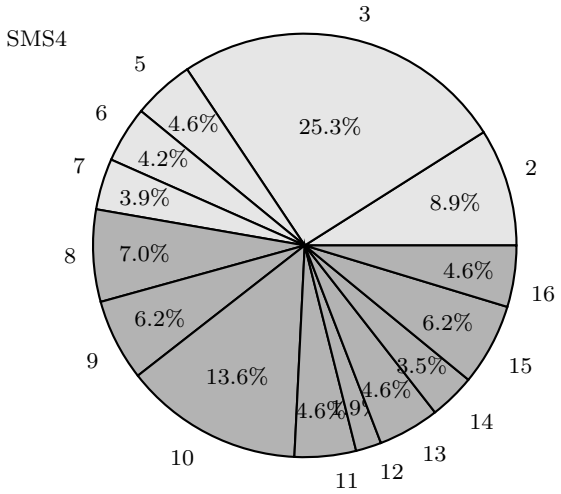

Fig. 21 $\mathbb{P}(L_B = k)$ for k with non zero probability and for HW leakages. The expected value of L_B is $\simeq 7.7$.

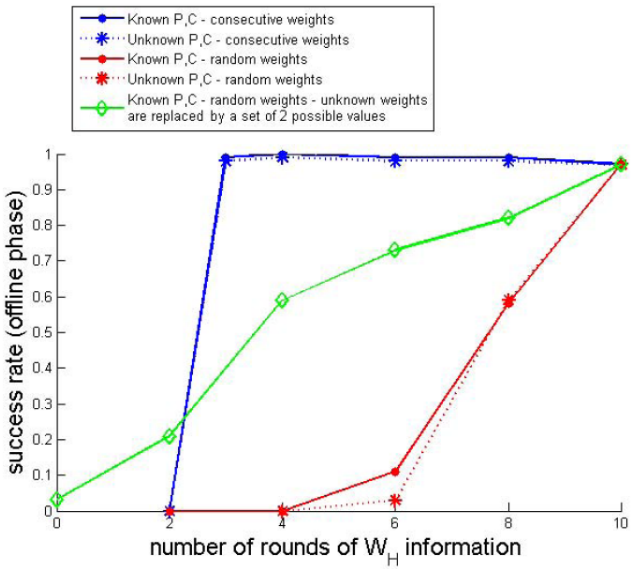

Fig. 23 Success rate of the attacks against an unprotected implementation of the AES in function of the amount of exploited leakages. One round of side-channel information is equivalent to 84 known Hamming weights

B Success rate of ASCA taken from [RSVC09, RS09]

We reproduce the following figures 22 and 23 corresponding to the results of ASCA with the SAT solver zChaff against PRESENT and AES presented in [RS09, RSVC09].

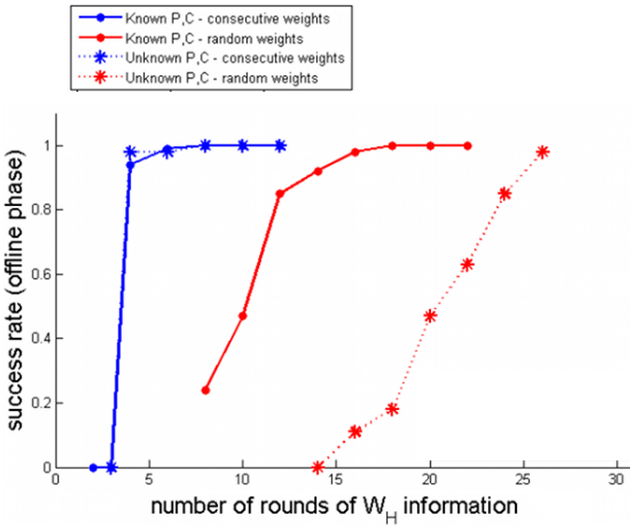

Fig. 22 31-round PRESENT, partial WH leakages

C Plaintexts and key used in experiments of section 6.4

Plaintexts and key used in section 6.4 for PRESENT are shown in hexadecimal notation.

key	`CF708A5E 7AC7F066 3FBA`
first plaintext	`1A3759CA 97F9A3A9`
second plaintext	`64CB8CB9 DBC97346`