Enhancing the Signal to Noise Ratio

in Differential Cryptanalysis, using Algebra

Martin Albrecht, Carlos Cid, Thomas Dullien, Jean-Charles Faugère and Ludovic Perret

ESC 2010, Remich, 10.01.2010

Outline

1. Introduction
2. The Main Idea
3. Decreasing the Noise
4. Increasing the Signal
5. Conclusion

Outline

1 Introduction

2 The Main Idea

3 Decreasing the Noise

4 Increasing the Signal

5 Conclusion

Differential Cryptanalysis I

- Formally introduced by Eli Biham and Adi Shamir [4].
- Can be used to distinguish an n-bit block cipher.
- Considers the distribution of output **differences** for the non-linear components of the cipher (e.g. the S-Box).
- Constructs **differential characteristics** for a number of rounds N

$$P^{'} \oplus P^{''} = \Delta P \rightarrow \Delta C = C^{'} \oplus C^{''}$$

  that are valid with probability p.
- If $p \gg 2^{-n}$ query the cipher with a large number of pairs with ΔP.
- Distinguish the cipher by counting the number of pairs with ΔC.
- A pair for which the characteristic holds is called a **right pair**.

Differential Cryptanalysis II

One can use it to recover key information.

- Instead of characteristics for the full N-round cipher, consider characteristics valid for r rounds only ($r = N - R$, with $R > 0$).
- Guess some key bits in last rounds, partially decrypt the known ciphertexts, and verify if the result matches the one predicted by the characteristic.
- Candidate (last round) keys are counted.
- Random noise is expected for wrong key guesses.
- Eventually a peak may be observed in the candidate key counters, pointing to the correct round key.

Signal/Noise Ratio I

- The number of right pairs that are needed to distinguish the right candidate key depends on
  1. the probability of the characteristic p,
  2. the number k of simultaneous subkey bits that are counted,
  3. the average count α how many keys are suggested per analysed pair,
  4. the fraction β of the analysed pairs among all the pairs.
- If we are looking for k subkey bits then we count the number of occurrences of 2^k possible key values in 2^k counters.
- The counters contain an average count of $\frac{m \cdot \alpha \cdot \beta}{2^k}$ counts were
  - m is the number of pairs,
  - $m \cdot \beta$ is the expected number of pairs to analyse and
  - α the number of suggested keys on average.
  - Since suggestions are spread across 2^k counters, we divide by 2^k.

Signal/Noise Ratio II

- The right subkey value is counted $m \cdot p$ times by the right pairs, plus the random counts for all the possible subkeys.
- The signal to noise ration is therefore:

$$S/N = \frac{m \cdot p}{m \cdot \alpha \cdot \beta / 2^k} = \frac{2^k \cdot p}{\alpha \cdot \beta}.$$

In this work we aim to improve this ratio for a given cipher.

Characteristics vs. Differentials

It would be sufficient to consider the probability p of the differential – i.e. the sum of all p_i for all characteristics with $\Delta P \longrightarrow \Delta C$ – instead of the probability of the characteristic.

However, in practice authors often work with the probabilities of characteristics because it is easier to estimate their probabilities.

Algebraic Techniques in Differential Cryptanalysis

- In [1] a combination of differential cryptanalysis with algebraic attacks against block ciphers was proposed.
- All three proposed techniques (**Attack-A**, **Attack-B** and **Attack-C**) require Gröbner basis computations during the online phase of the attack.
- This limitation prevented to apply the techniques to PRESENT-80 reduced to more than 16 rounds because then the computation time would exceed exhaustive key search.

In this work we only perform Gröbner basis computations in a pre-computation (or offline) phase.

Outline

1 Introduction

2 The Main Idea

3 Decreasing the Noise

4 Increasing the Signal

5 Conclusion

Ideal Membership as Implication I

- Consider an arbitrary function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ and its polynomial representation $f_0, \dots, f_{m-1}$
- Let $x_0, \dots x_{n-1}$ be the input variables and $y_0, \dots, y_{m-1}$ the output variables
- Consider the ideal $I = \langle f_0, \dots, f_{m-1} \rangle$:
  - Every member g of this ideal is a combination of $f_0, \dots, f_{m-1}$.
  - If $f_0, \dots, f_{m-1}$ vanish, so does g.
  - This can be read as: $f_0, \dots, f_{m-1}$ **implies** g.

"If $f_0, \dots, f_{m-1}$ hold, so does g".

Ideal Membership as Implication II

- Let c be a condition on the input variables (in polynomial form).
- Calculate a Gröbner basis for $\langle c, f_0, \ldots, f_{m-1} \rangle$ in an elimination ordering which eliminates input variables first
- The smallest elements of this Gröbner basis will be polynomials with a minimum number of input variables (if possible, none). Call them $g_0, \ldots, g_{r-1}$
- These polynomials are **implied** by the functions $f_0, \ldots, f_{m-1}$ and the condition c.

"If $f_0, \ldots, f_{m-1}$ and the condition c hold, so do $g_0, \ldots, g_{r-1}$"

Ideal Membership as Implication III

- The polynomials $g_0, \ldots, g_{r-1}$ generate the **elimination ideal** [3, p.256]

$$I \bigcap \mathbb{F}_2[y_0, \ldots, y_{m-1}]$$

- This means: **all** on the output bits that are implied by f under condition c are **combinations** of $g_0, \ldots, g_{r-1}$
- If we pick the term ordering right, $g_0, \ldots, g_{r-1}$ have minimal degree.

For a given function f under a precondition c you can calculate **all** conditions on the output bits that **must** hold.

Ideal Membership as Implication IV

Some example applications:

Differential: Given two parallel executions of a block cipher round and an input differential: What conditions on the output hold with probability 1?

Integral: Given many parallel executions of a block cipher round and a condition on the inputs: What conditions on the output hold with probability 1?

A Small Example I

- Consider the 4-bit S-Box of PRESENT [5]:

$$S = (12, 5, 6, 11, 9, 0, 10, 13, 3, 14, 15, 8, 4, 7, 1, 2).$$

- Two pairs of input bits $X'_{1,0}, \ldots, X'_{1,3}$ and $X''_{1,0}, \ldots, X''_{1,3}$,
- The respective output bits are $Y'_{1,0}, \ldots, Y'_{1,3}$ and $Y''_{1,0}, \ldots, Y''_{1,3}$.
- S can be described as boolean polynomials in $Y_{i,j}$'s and $X_{i,j}$'s.
- Assume that we have the input difference $(0, 0, 0, 1)$ for this S-Box; that is, we have that $X'_{1,3} + X''_{1,3} = 1$.
- We are interested in all linearly independent low degree equations in the $Y_{i,j}$'s that must hold if this input difference holds.

A Small Example II

- We define I to be the ideal spanned by
  1. the S-Box polynomials on $X'_{1,j}, Y'_{1,j}$,
  2. the S-Box polynomials on $X''_{1,j}, Y''_{1,j}$,
  3. the set $\{X'_{1,0} + X''_{1,0},\ X'_{1,1} + X''_{1,1},\ X'_{1,2} + X''_{1,2},\ X'_{1,3} + X''_{1,3} + 1\}$ and
  4. the field polynomials $\{X^2_{i,j} - X_{i,j}\}$ and $\{Y^2_{i,j} - Y_{i,j}\}$.
- We define a **block ordering** [3, p.168] where the variables $X_{i,j}$ are in the first block and the variables $Y_{i,j}$ are in the second, that is, we have that all $X_{i,j} > Y_{i,j}$.
- Inside the second block we choose the degree lexicographical ordering (**deglex**) on the $Y_{i,j}$.
- We compute the reduced Gröbner basis G of I.

A Small Example III

All polynomials of G only containing the variables $Y_{i,j}$ are listed below:

$$
\begin{aligned}
&Y'_{1,3} + Y'_{1,3} + 1,\\
&Y'_{1,0} + Y'_{1,2} + Y''_{1,0} + Y''_{1,2} + 1,\\
&Y''_{1,0}Y''_{1,2} + Y'_{1,2} + Y''_{1,0} + Y''_{1,1} + Y''_{1,3},\\
&Y''_{1,0}Y''_{1,1} + Y''_{1,0}Y''_{1,3} + Y''_{1,1}Y''_{1,2} + Y''_{1,2}Y''_{1,3} + Y'_{1,1} + Y''_{1,0} + Y''_{1,1},\\
&Y'_{1,2}Y''_{1,2} + Y''_{1,1}Y''_{1,2} + Y''_{1,2}Y''_{1,3},\\
&Y'_{1,2}Y''_{1,0} + Y''_{1,1}Y''_{1,2} + Y''_{1,2}Y''_{1,3} + Y'_{1,1} + Y'_{1,2} + Y''_{1,0} + Y''_{1,3},\\
&Y'_{1,1}Y''_{1,2} + Y'_{1,2}Y''_{1,1} + Y'_{1,2}Y''_{1,3} + Y''_{1,1}Y''_{1,2} + Y'_{1,1} + Y'_{1,2} + Y''_{1,1},\\
&Y'_{1,1}Y''_{1,1} + Y'_{1,1}Y''_{1,3} + Y''_{1,1}Y''_{1,2} + Y''_{1,1}Y''_{1,3} + Y''_{1,2}Y''_{1,3} + Y''_{1,1},\\
&Y'_{1,1}Y''_{1,0} + Y'_{1,2}Y''_{1,1} + Y'_{1,2}Y''_{1,3} + Y''_{1,0}Y''_{1,3} + Y''_{1,1}Y''_{1,2} + Y''_{1,2}Y''_{1,3} + Y'_{1,1} + Y''_{1,3},\\
&Y'_{1,1}Y'_{1,2} + Y'_{1,2}Y''_{1,3} + Y''_{1,1}Y''_{1,2} + Y''_{1,2}Y''_{1,3} + Y'_{1,2}
\end{aligned}
$$

A Small Example IV

This list is exactly the reduced **deglex** Gröbner basis G_Y for the **elimination ideal**

$$I_Y = I \bigcap \mathbb{F}_2[Y'_{1,0}, \dots, Y'_{1,3}, Y''_{1,0}, \dots, Y''_{1,3}].$$

One can show that there are no other linear or quadratic polynomial p which are not a simple algebraic combination of these polynomials.

In Other Words

This list describes the relations in the $Y_{i,j}$ completely.

Relaxations I

If we can compute the Gröbner basis $g_0, \ldots, g_{r-1}$, we are done.

For many functions f computing $g_0, \ldots, g_{r-1}$ is infeasible. However, to recover **some** equations we might not need to compute the full Gröbner basis.

As an example consider the same S-Box and the same input difference $(0, 0, 0, 1)$. If we only compute the Gröbner basis up to degree 2 we can still recover some properties of the $Y_{i,j}$'s.

Relaxations II

$$Y'_{1,3} + Y''_{1,3} + 1,$$
$$Y'_{1,0} + Y'_{1,2} + Y''_{1,0} + Y''_{1,2} + 1,$$
$$Y''_{1,0}Y''_{1,2} + Y'_{1,2} + Y''_{1,0} + Y''_{1,1} + Y''_{1,3},$$
$$Y''_{1,0}Y''_{1,1} + Y''_{1,0}Y''_{1,2} + Y''_{1,0}Y''_{1,3} + Y''_{1,1}Y''_{1,2} + Y''_{1,2}Y''_{1,3} + Y'_{1,1} + Y'_{1,2} + Y''_{1,3},$$
$$Y'_{1,2}Y''_{1,0} + Y'_{1,2}Y''_{1,2} + Y''_{1,0}Y''_{1,2} + Y'_{1,1} + Y''_{1,1},$$
$$Y'_{1,1}Y''_{1,0} + Y'_{1,1}Y''_{1,2} + Y''_{1,0}Y''_{1,3} + Y''_{1,2}Y''_{1,3} + Y'_{1,2} + Y''_{1,1} + Y''_{1,3},$$
$$Y'_{1,1}Y'_{1,2} + Y'_{1,2}Y'_{1,3} + Y''_{1,1}Y''_{1,2} + Y''_{1,2}Y''_{1,3},$$
$$\mathbf{Y}''_{1,0}\mathbf{Y}''_{1,1}\mathbf{Y}''_{1,3} + \mathbf{Y}''_{1,1}\mathbf{Y}''_{1,2}\mathbf{Y}''_{1,3} + \mathbf{Y}'_{1,1}\mathbf{Y}''_{1,3} + \mathbf{Y}''_{1,1}\mathbf{Y}''_{1,3} + \mathbf{Y}''_{1,2}\mathbf{Y}''_{1,3},$$
$$\mathbf{Y}'_{1,2}\mathbf{Y}''_{1,0}\mathbf{Y}''_{1,2} + \mathbf{Y}'_{1,2}\mathbf{Y}''_{1,1} + \mathbf{Y}'_{1,2}\mathbf{Y}''_{1,3} + \mathbf{Y}''_{1,0} + \dots,$$
$$\dots$$

Outline

1 Introduction

2 The Main Idea

3 Decreasing the Noise

4 Increasing the Signal

5 Conclusion

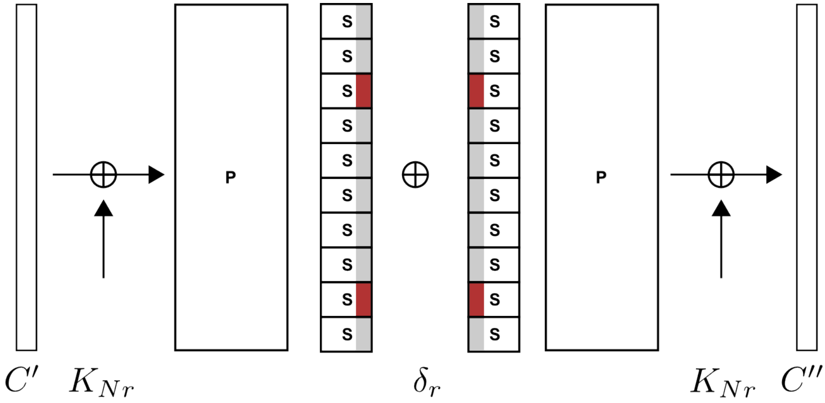
Discarding Wrong Pairs I

- In [1] **Attack-C** is proposed to discard wrong pairs.
- The attacker considers an equation system only for the rounds $> r$.
- Denote the equation system for the last R rounds of the encryption of P' to C' and P'' to C'' as F'_R and F''_R respectively.
- The algebraic part of **Attack-C** is a Gröbner basis computation on the polynomial system

$$F = F'_R \cup F''_R \cup \{X'_{r+1,i} + X''_{r+1,i} + \Delta X_{r+1,i} \mid 0 \leq i < B_s\}.$$

- Whenever the Gröbner basis is $\{1\}$ the pair can be discarded.
- No strong assurances are given about how many pairs are actually discarded by **Attack-C**.

Discarding Wrong Pairs II



Discarding Wrong Pairs III

Our approach:

- We consider the same system of equations as in **Attack-C**.
- But we replace the tuples of constants C' and C'' by symbols.
- We then compute a Gröbner basis for an elimination ordering with C' and C'' smallest.
- Thus, we recover equations in the variables C' and C''.
- These equations must must evaluate to zero on the actual ciphertext values if the input difference for round $r+1$ holds.
- To estimate the quality of the filter, we can calculate the probability that all these polynomials evaluate to zero for random values for C' and C''.
- The cost of the filter is only a few polynomial evaluations average.

Example: PRESENT I

We consider the characteristics from [9] also considered in [1] and construct filters for PRESENT reduced to $14 + R$ rounds.

We construct the polynomial ring $P =$

$$
\mathbb{F}_2[\quad \begin{array}{ll}
K_{0,0}, \dots, K_{0,79}, & K_{1,0}, \dots, K_{1,3}, \\
Y'_{1,0}, \dots, Y'_{1,63}, & Y''_{1,0}, \dots, Y''_{1,63}, \\
X'_{1,0}, \dots, X'_{1,63}, & X''_{1,0}, \dots, X''_{1,63}, \\
\dots, & K_{14+R,0}, \dots, K_{14+R,3}, \\
Y'_{14+R,0}, \dots, Y'_{14+R,63}, & Y''_{14+R,0}, \dots, Y''_{14+R,63}, \\
X'_{14+R,0}, \dots, X''_{14+R,63}, & X''_{14+R,0}, \dots, X''_{14+R,63}, \\
C'_0, \dots, C'_{63}, & C''_0, \dots, C''_{63}]
\end{array}
$$

and attach the following block ordering:

$$
\underbrace{K_{0,0}, \dots, X''_{14+R,63}}_{\text{degrevlex}}, \underbrace{C'_0, \dots, C''_{63}, C''_0, \dots, C''_{63}}_{\text{degrevlex}}.
$$

Example: PRESENT II

We setup an equation system as in **Attack-C** of [1] except that the ciphertext bits (C_i' and C_i''). are symbols and computed the Gröbner basis up to degree $D = 3$ using POLYBORI 0.6.3 [6] and filter out any polynomial that contains non-ciphertext variables.

For each R we list the number of linear, quadratic and cubic equations we found ($d = 1, 2, 3$) and the logarithm of the approximate quality of the filter.

R	$d = 1$	$d = 2$	$d = 3$	$\approx \log_2 p$	comment
1	58	2		-58.830	
2	46	14	6	-50.669	Wang: $2^{-50.07}$
3	16	1	11	-18.296	Attack-C: $< 2^{-22.00}$
4			16	-3.082	optimal: $2^{-3.35}$

Example: KTANTAN32

We used the best differential for 42 rounds of KTANTAN32 [7] by the designers and extended it to 71 rounds. The characteristic has a probability of 2^{-31}.

N	$d = 1$	$d = 2$	$d = 3$	$d = 4$	$d = 5$	$\approx \log_2 p$
78	31	3	0	0	0	-32.0
80	28	11	0	0	0	-31.4
82	25	23	0	0	0	-31.0
84	20	32	4	32	0	-29.0
86	16	46	23	75	106	< -24.0
90	8	42	133	612	1762	< -22.0
92	4	33	133	743	2646	-20.4
94	1	25	124	662	2345	-18.5
96	0	8	52	287	1264	-14.3
98	0	3	10	46	156	-9.1
100	0	1	3	18	47	-4.6
102	0	0	0	4	9	-0.9
103	0	0	0	2	4	-0.4

Outline

1 Introduction

2 The Main Idea

3 Decreasing the Noise

4 Increasing the Signal

5 Conclusion

Gathering More Information I

Now we consider increasing the amount of correct data that is always suggested by a right pair.

Increasing this value usually has considerable costs attached to it

1. more data needs to be managed and thus usually the counter tables get bigger,
2. in order to generate more date, more partial decryptions must be performed which increases the computation time.

Furthermore, the number of key bits which can used might be limited by the number of rounds R we can consider.

Gathering More Information II

Our approach is to use data available from the first few rounds.

Assume for example:

1. an SP-network,
2. a differential characteristic $\Delta = (\Delta P, \Delta Y_1, \ldots, \Delta Y_r)$ valid for r rounds with probability p,
3. a right pair (P', P'') for Δ,
4. only one S-Box is active in round 1, with input $X'_{1,j}$ and $X''_{1,j}$, and
5. there is a key addition immediately before the S-Box operation.

Gathering More Information III

We have

$$S(P'_j + K_{0,j}) = S(X'_{1,j}) = Y'_{1,j} \text{ and } S(P''_j + K_{0,j}) = S(X''_{1,j}) = Y''_{1,j}.$$

The polynomial equations arising from the relation

$$\Delta Y_{1,j} = Y'_{1,j} + Y''_{1,j} = S(P'_j + K_{0,j}) + S(P''_j + K_{0,j})$$

give us a very simple equation system to solve, with only the key variables $K_{0,j}$ as unknowns.

We can:

- recover b bits of information about the key, if ΔY_1 holds with probability 2^{-b}.
- replace P', P'' by symbols to get polynomials in K_0, P' and P''.
- compute similar polynomials for more than one round.

Gathering More Information IV

Assume that

1. we can indeed compute the Gröbner basis with P', P'' symbols for the first q rounds,
2. the probability of the characteristic restricted to q rounds is 2^{-b},
3. the Gröbner basis of $I \cap \mathbb{F}_2[K_0, P', P'']$ has m_q elements.

We have b bits of additional information and thus can write

$$S/N = \frac{2^{k+\mathbf{b}} \cdot p}{\alpha \cdot \beta}$$

without performing any additional partial decryptions.

However, we have to perform m_q polynomial evaluations (where we replace P', P'' by their actual values).

Also, this approach still has the memory overhead.

Buckets

We can spread all pairs into 2^b **buckets**, labelled by the 2^b possible conditions on the key variables.

For example, for PRESENT we have $K_{53} + K_{55} + P'_{53} + P'_{55}$ and $K_{54} + K_{55} + P'_{54} + P'_{55}$. Thus, we create 2^2 buckets for each set of equations suggest by the values of $P'_{53} + P'_{55}$ and $P'_{54} + P'_{55}$.

We maintain **smaller** counters for each bucket independently. All right pairs for the **characteristic** must suggest the same equations and thus the same bucket. Pairs which do not follow the characteristic will be assigned a random bucket out of 2^b choices. We have

$$S/N = \frac{2^k \cdot p}{\alpha \cdot \beta / 2^b} = \frac{2^{k+b} \cdot p}{\alpha \cdot \beta}.$$

If we are allowed to choose P' in addition to ΔP we can check the buckets sequentially by picking the right combination of bits in P'.

Example: PRESENT I

- Consider two rounds of PRESENT and the characteristic from [9].
- Setup a polynomial ring with two blocks such that the variables P_i and K_i are lexicographically smaller than any other variables.
- Within the blocks choose a degree lexicographical term ordering.
- Setup an equation system and add the linear equations suggested by the characteristic.
- Compute a Gröbner basis up to degree five.

Example: PRESENT II

This computation returned 22 polynomials. We give a selection below:

$$
\begin{aligned}
&(K_1 + P'_1 + 1)(K_0 + K_3 + K_{29} + P'_0 + P'_3),\\
&(K_2 + P'_2)(K_0 + K_3 + K_{29} + P'_0 + P'_3),\\
&K_1K_2 + K_1P'_2 + K_2P'_1 + P'_1P'_2 + K_0 + K_1 + K_3 + K_{29} + P'_0 + P'_1 + P'_3,\\
&\dots\\
&K_5 + K_7 + P'_5 + P'_7,\\
&K_6 + K_7 + P'_6 + P'_7,\\
&K_{53} + K_{55} + P'_{53} + P'_{55},\\
&K_{54} + K_{55} + P'_{54} + P'_{55}
\end{aligned}
$$

This system gives 8 bits of information about the key. The first two rounds of the characteristic pass with probability 2^{-8}.

Example: NOEKEON I

We consider one round of NOEKEON [2] with

$$\Delta X_1 = 00000000\ 00001020\ 00000080\ 00010181$$

and

$$\Delta Y_1 = 00000081\ 00010101\ 00001020\ 00000000$$

based on the best differential provided by the NOEKEON designers.

The first round differential holds with probability 2^{-14}. Consequently, we recover 14 linear polynomials.

Example: KTANTAN32

We consider the first 24 rounds of KTANTAN32 and the previously mentioned characteristic. We computed the full Gröbner basis. This computation recovers 39 polynomials of which we list the 8 smallest non-redundant below. Note that the characteristic also imposes restrictions on the plaintext.

$$
\begin{aligned}
&(P'_{19}+1)(P'_3P'_8+P'_{10}P'_{12}+K_3+K_{53}+P'_7+P'_{18}+P'_{23}),\\
&P'_8P'_{10}P'_{19}+K_8P'_{19}+P'_3P'_8+P'_6P'_{19}+P'_{10}P'_{12}+P'_{16}P'_{19}+K_3+K_{53}+\dots,\\
&P'_{19}P'_{22}+K_1+K_{11}+P'_6+P'_{11}+P'_{17}+P'_{21}+P'_{26},\\
&P'_{23}P'_{26}+K_{65}+P'_{21}+P'_{25}+P'_{30},\\
&P'_1+1, P'_2, P'_5+1, P'_9+1
\end{aligned}
$$

These eight equations give up to four bits (depending on the value of P'_{19}) of information about the key.

Outline

1 Introduction

2 The Main Idea

3 Decreasing the Noise

4 Increasing the Signal

5 Conclusion

Conclusion

- We demonstrated cryptographic applications of Gröbner basis algorithms beyond polynomial system solving[1].
- Using the rich algebraic structure of Gröbner bases we compute properties for various block ciphers which can be used to improve "classical" differential cryptanalysis attacks.
- The techniques proposed and used in this work are not limited to differential cryptanalysis.

[1] Of course, we are not the first to notice that, cf. [8]

Thank you!

Literature I

Martin Albrecht and Carlos Cid.
Algebraic Techniques in Differential Cryptanalysis.
In *Fast Software Encryption 2009*, Lecture Notes in Computer Science, Berlin, Heidelberg, New York, 2009. Springer Verlag.

J. Daemen an M. Peeters, G. Van Assche, and V. Rijmen.
Nessie Proposal: NOEKEON.
In *First Open NESSIE Workshop*, 2000.
http://gro.noekeon.org/.

Thomas Becker and Volker Weispfenning.
Gröbner Bases - A Computational Approach to Commutative Algebra.
Springer Verlag, Berlin, Heidelberg, New York, 1991.

Literature II

Eli Biham and Adi Shamir.
Differential Cryptanalysis of DES-like Cryptosystems.
In *Advances in Cryptology — CRYPTO 1990*, volume 537 of *Lecture Notes in Computer Science*, pages 3–72, Berlin, Heidelberg, New York, 1991. Springer Verlag.

A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, Matthew Robshaw, Y. Seurin, and C. Vikkelsoe.
PRESENT: An ultra-lightweight block cipher.
In *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 7427 of *Lecture Notes in Computer Science*, pages 450–466, Berlin, Heidelberg, New York, 2007. Springer Verlag.
Available at `http://www.crypto.rub.de/imperia/md/content/texte/publications/conferences/present_ches2007.pdf`.

Literature III

Michael Brickenstein and Alexander Dreyer.
PolyBoRi: A framework for Gröbner basis computations with Boolean polynomials.
In *Electronic Proceedings of MEGA 2007*, 2007.
Available at
http://www.ricam.oeaw.ac.at/mega2007/electronic/26.pdf.

Christophe De Cannière, Orr Dunkelman, and Miroslav Knežević.
KATAN and KTANTAN — a family of small and efficient hardware-oriented block ciphers.
In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009*, volume 5747 of *Lecture Notes in Computer Science*, pages 272–288. Springer Verlag, 2009.

Literature IV

Toshinobu Kaneko Takeshi Shimoyama.
Quadratic relation of s-box and its application to the linear attack of full round DES.
In *Advances in Cryptology — CRYPTO 1998*, volume 1462 of *Lecture Notes in Computer Science*, pages 200–211. Springer Verlag, 1998.

Meiqin Wang.
Differential Cryptanalysis of reduced-round PRESENT.
In Serge Vaudenay, editor, *Africacrypt 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 40–49, Berlin, Heidelberg, New York, 2008. Springer Verlag.