Algebraic Precomputations in Differential Cryptanalysis

Martin Albrecht[1] Carlos Cid[1] Thomas Dullien[2]
Jean-Charles Faugère[3] Ludovic Perret[3]

1 Information Security Group, Royal Holloway, University of London
2 Lehrstuhl für Kryptologie und IT-Sicherheit, Ruhr-Universität Bochum
3 SALSA Project -INRIA, UPMC, Univ Paris 06

Tools for Cryptanalysis 2010, Egham, UK

Outline

Outline

Algebraic Techniques in Differential Cryptanalysis

- In [AC09] 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.

Here we only compute Gröbner bases in a pre-computation phase.

Outline

Ideal Membership as Implication I

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

"If $f_0, \ldots, f_{m-1}$ 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 polynomials $f_0, \ldots, f_{m-1}$ 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** [BW91, p.256]

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

- 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.

A Small Example I

- Consider the 4-bit S-Box of PRESENT [BKL+07]:

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

- 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** [BW91, 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:

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

A Small Example IV

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

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

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

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

Outline

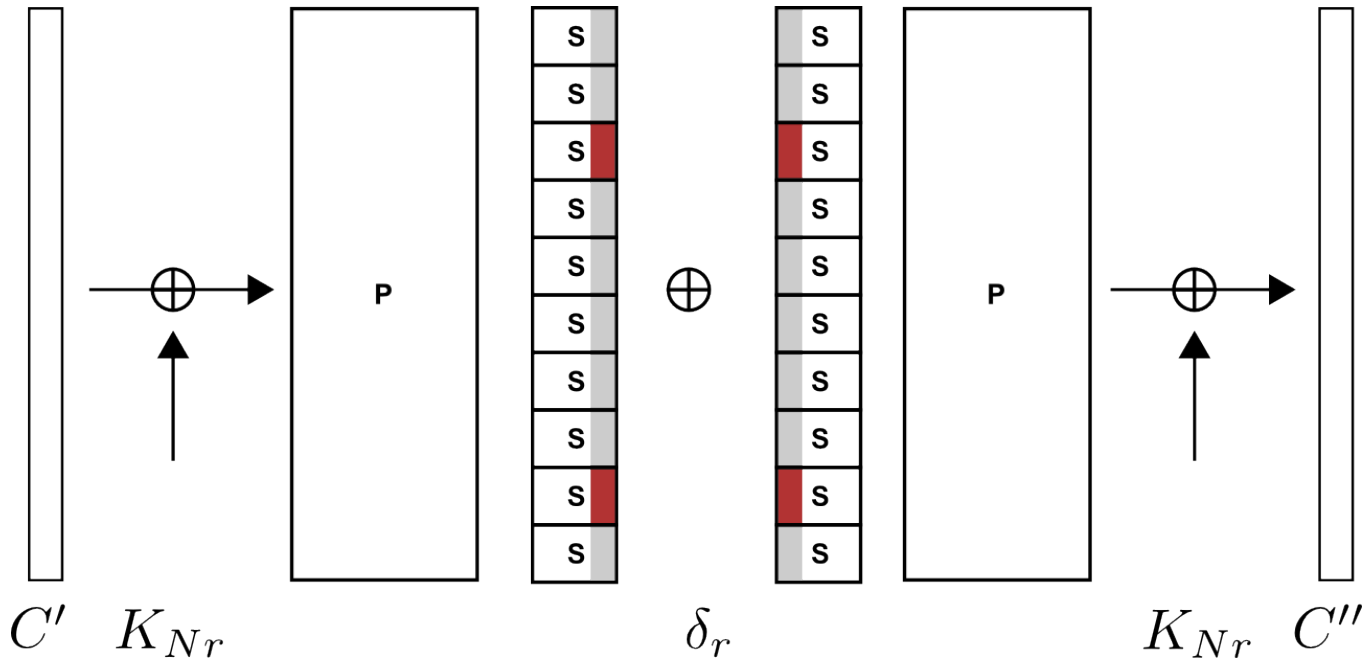
Discarding Wrong Pairs I

- In [AC09] **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:

- Consider the same system of equations as in **Attack-C**.
- Replace the tuples of constants C' and C'' by symbols.
- Compute a Gröbner basis for an elimination ordering where C' and C'' smallest.
- Recover equations in the variables C' and C''.
- These equations 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, 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 setup an equation system as in **Attack-C** of [AC09] 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 [BD07] 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	$d = 1$	$d = 2$	$d = 3$	$\approx \log_2 p$	$\approx \log_2$ opt.	$\approx \log_2$ [Wan08]
1	58	2		-58.830		
2	46	14	6	-50.669	-51.67	-50.07
3	16	1	11	-18.296	-25.13	
4			16	-3.082	-3.35	

Example: KTANTAN32

We used the best differential for 42 rounds of KTANTAN32 [CDK09] 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

Outline

Gathering More Information I

Assume:

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 II

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 III

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 $I \cap \mathbb{F}[K_0, P', P'']$ has m_q elements.

We have b bits of additional information. However, we have to perform m_q polynomial evaluations (where we replace P', P'' by their actual values).

Example: PRESENT I

- Consider two rounds of PRESENT and the characteristic from [Wan08].
- 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:

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

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

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.

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

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

Outline

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. [TS98]

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.

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`.

Literature II

Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick 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`.

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

Literature III

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.

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.

Literature IV


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.