

# Algebraic-Differential Cryptanalysis of DES

Jean-Charles Faugère Ludovic Perret  
Pierre-Jean Spaenlehauer

LIP6  
CNRS  
INRIA Paris - Rocquencourt  
SALSA team

Weworc 2009



# Plan

- 1 Introduction
- 2 Algebraic cryptanalysis of DES using Minisat
  - Data Encryption Standard
  - Modeling
  - Experimental results
- 3 Algebraic-differential cryptanalysis of DES
  - Algebraic-differential cryptanalysis
  - Results on six, seven and eight rounds

# Plan

- 1 Introduction
- 2 Algebraic cryptanalysis of DES using Minisat
  - Data Encryption Standard
  - Modeling
  - Experimental results
- 3 Algebraic-differential cryptanalysis of DES
  - Algebraic-differential cryptanalysis
  - Results on six, seven and eight rounds

# Algebraic Cryptanalysis



***Claude Shannon :***

***" Breaking a good cipher  
should require as much  
work as solving a system  
of simultaneous equations  
in a large number of unknowns "***

# Algebraic Cryptanalysis

- Algebraic representation of a cryptographic primitive.
- Tools for efficient polynomial system solving.

## Remark

There is a very strong link between the modeling and the tools used for the resolution.

## Challenge

Can algebraic cryptanalysis be efficient against block ciphers ?

## Our work

- SAT Solvers attacks against DES using different modelings of the DES S-boxes.
- Incorporation of elements from differential cryptanalysis
  - new attacks against 6,7 and 8 rounds of DES using dedicated characteristics.
- **Tradeoff** between time and data complexity.

# Polynomial System Solving

- 1 Gröbner Bases algorithms (Buchberger, Faugère F4 and F5).
- 2 SAT Solvers.

# Polynomial System Solving

- 1 Gröbner Bases algorithms (Buchberger, Faugère F4 and F5).
- 2 SAT Solvers.

## SAT Solvers ?

- Very efficient and flexible dedicated softwares.
- SAT-competition. Active research field.
- **Easy to use. Low memory consumption.**





Courtois N.T. , Bard G.V. and Jefferson C.

*Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF (2) via SAT-Solvers.*

<http://eprint.iacr.org/2007/024.pdf>

- Replace each monomial by a new variable
- Cut linear equations into smaller equations (by adding new variables)
- + optimizations

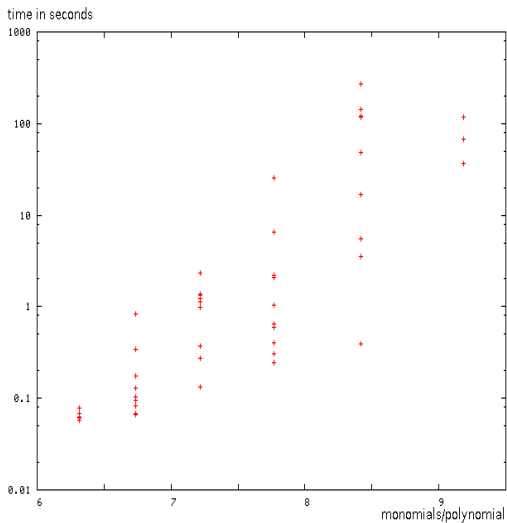
## MiniSat2



Een, N. and Sorensson, N.

*MiniSat: A SAT solver with conflict-clause minimization*

# Sparse quadratic systems



# Plan

- 1 Introduction
- 2 Algebraic cryptanalysis of DES using Minisat
  - Data Encryption Standard
  - Modeling
  - Experimental results
- 3 Algebraic-differential cryptanalysis of DES
  - Algebraic-differential cryptanalysis
  - Results on six, seven and eight rounds

# Data Encryption Standard

- Iterative Block Cipher
- Bloc size : 64 bits
- Effective size of the key : 56 bits
- Encryption standard between 1976 and 2002

Why did we choose to study the DES ?

## Main attacks against DES



Wiener, M.J.

*Efficient DES key search.* Technical Report



Biham, E. and Shamir, A.

*Differential cryptanalysis of the full 16-round DES.* Crypto'1992



Knudsen, L.R.

*Partial and higher order differentials and applications to the DES.* BRICS report

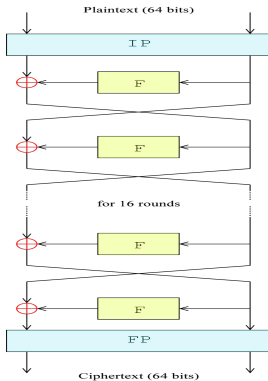


Matsui, M.

*Linear cryptanalysis method for DES cipher.* EUROCRYPT'1993

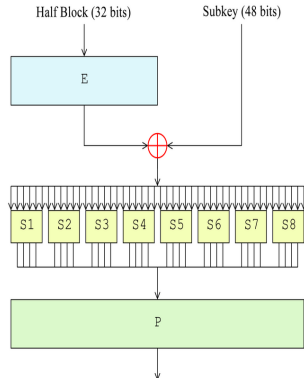
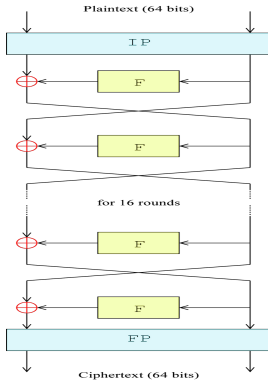
# DES Structure

## Feistel network



# DES Structure

## Feistel network



S-boxes : non-linear part of the system

# Algebraic cryptanalysis of DES using Minisat

## Starting point



N.T. Courtois, G.V. Bard

*Algebraic Cryptanalysis of the Data Encryption Standard*

IMA Int. Conf. 2007

## General principle

- 1 known plaintext.
- Modeling the cryptosystem by a set of clauses.
- Use Minisat to extract the key.

## Remark

We can combine this approach with an exhaustive search over some bits of the key.



## S-boxes modeling (I)

- We have considered many modelings of the DES S-boxes.
- The choice of the modeling is very important.

### Our modeling

We search (exhaustively) for the set of polynomials which verify :

$$P(x_1, \dots, x_6, y_1, \dots, y_4) = \prod(x_i + \alpha_i) \prod(y_i + \beta_i), \alpha_i, \beta_i \in \{0, 1\}$$

such that

$$S(x_1, \dots, x_6) = (y_1, \dots, y_4) \Rightarrow P(x_1, \dots, x_6, y_1, \dots, y_4) = 0$$

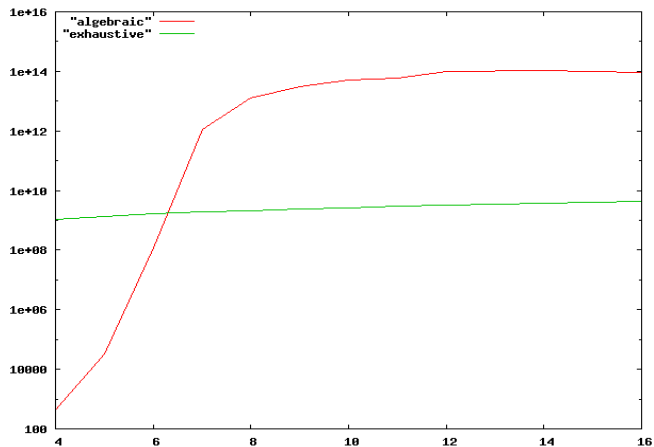
Complexity :  $3^{10}$

## S-box modeling (II)

S-box	Nb of clauses
S1	1624
S2	1844
S3	1767
S4	1881
S5	1812
S6	1705
S7	1673
S8	2047

For 6 rounds : 792 variables and 90086 clauses.  
+ partial exhaustive search on 28 bits of the key.

# Experimental results



# Plan

- 1 Introduction
- 2 Algebraic cryptanalysis of DES using Minisat
  - Data Encryption Standard
  - Modeling
  - Experimental results
- 3 Algebraic-differential cryptanalysis of DES
  - Algebraic-differential cryptanalysis
  - Results on six, seven and eight rounds

# Our approach

## Limit

Algebraic cryptanalysis usually consider only one known plaintext.

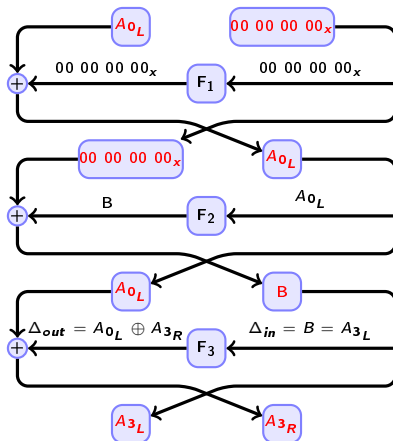
We will combine algebraic cryptanalysis and statistical techniques to exploit efficiently the knowledge of several plaintexts.

- Tradeoff time/plaintexts.
- In particular, we will consider differential cryptanalysis.

# Differential cryptanalysis (I)

- The principle was known by the DES designers.
- Based on a statistical bias of the S-boxes.
- Key recovery attack.
- We try to predict how the difference of 2 plaintexts will diffuse through the cipher.

# Differential cryptanalysis of the 3 rounds reduced DES



## Differential cryptanalysis (II)

### more than 3 rounds

- Statistical methods.
- *differential characteristics*.
- A lot of plaintexts needed.



# Motivations

Compromise between algebraic cryptanalysis and differential cryptanalysis.

- We can use the strong correlation between the subkeys.
- The notion of difference is easy to represent with clauses.
- We only need **one** pair following the characteristic to retrieve the key.

## General algorithm

Repeat until the key is found :

- Choose a differential characteristic.
- Choose two plaintexts with difference fixed by the characteristic.
- Construct the system of clauses for DES, and add the clauses corresponding to the characteristic.
- Solve with MiniSat. If the result is UNSATISFIABLE, restart (it means that the pair didn't follow the characteristic). If the result is SATISFIABLE, then MiniSat returns the key.

# Six rounds

## Approach

- Classical differential characteristics.
- Combination of different characteristics to reduce the data complexity.

## Six rounds

### Approach

- Classical differential characteristics.
- Combination of different characteristics to reduce the data complexity.

### How to combine

- We can run MiniSat 6 times with 7 plaintexts.
- Six 3-rounds characteristics  $\Delta_1, \dots, \Delta_6$ .
- 7 plaintexts  $m_0, \dots, m_6$  such that  $m_i = m_0 \oplus \delta_i$ .

# Experimental results

Cryptanalysis	Plaintexts	Time
Differential (Biham, Shamir)	240	0,3 seconds
Differential (Knudsen)	46	a few seconds
Algebraic with SAT Solver (Courtois, Bard)	1	$2^{25}$ seconds
Algebraic-differential	32	3000 seconds
Algebraic-differential (with combinaison of characteristics)	22	<10 hours

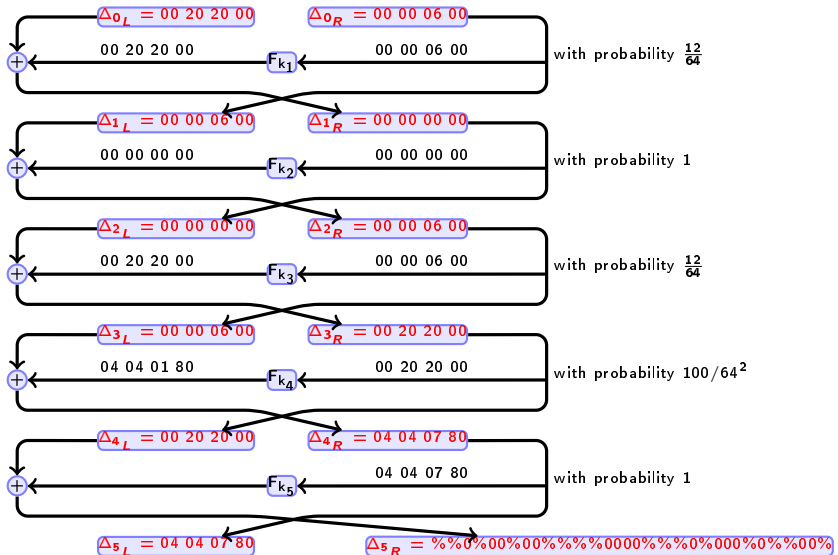
## Seven rounds

For seven rounds and more, the classical differential characteristics don't seem to be adapted.

We have used a dedicated differential characteristic.

- Truncated characteristic with probability  $1/1000$ .

S-Box	$\delta_{in}$	$\delta_{out}$	Proba
S1	$4_x$	$6_x$	10/64
	$8_x$	$3_x$	12/64
S2	$4_x$	$10_x$	10/64
	$4_x$	$12_x$	10/64
	$8_x$	$9_x$	10/64
	$8_x$	$10_x$	16/64
	$12_x$	$5_x$	14/64
S3	$4_x$	$9_x$	12/64
	$8_x$	$3_x$	10/64
	$12_x$	$5_x$	12/64
	$12_x$	$6_x$	12/64
S4	$4_x$	$6_x$	12/64
	$4_x$	$9_x$	12/64
Boîte-S	$\delta_{in}$	$\delta_{out}$	Proba
S5	$4_x$	$6_x$	10/64
	$8_x$	$6_x$	10/64
	$8_x$	$10_x$	10/64
	$12_x$	$3_x$	10/64
	$12_x$	$6_x$	10/64
	$12_x$	$10_x$	10/64
S6	$8_x$	$6_x$	16/64
	$12_x$	$3_x$	12/64
	$12_x$	$5_x$	10/64
S7	$8_x$	$10_x$	12/64
	$12_x$	$12_x$	14/64
S8	$4_x$	$12_x$	10/64
	$12_x$	$5_x$	10/64
	$12_x$	$6_x$	10/64





## Experimental results

### 7 rounds cryptanalysis

- 2000 chosen plaintexts
- 3 hours

Not so much results on 7 rounds in the literature.

## Eight rounds

We have found a 5-round truncated differential characteristic with probability  $1/5800$ .

+ partial exhaustive search over 8 bits of the key.

### 8 rounds cryptanalysis

- 11600 chosen plaintexts and  $2^{25}$  seconds.

# Summary

Rounds	Cryptanalysis	Nb of plaintexts	Time
6	diff (Biham,Shamir)	240 (chosen)	0,3 s
	diff (Knudsen)	46 (chosen)	<10 s
	alg (Courtois,Bard)	1 (known)	$2^{25}$ s
	<b>diff + alg</b>	<b>32 (chosen)</b>	<b>3000 s</b>
	<b>diff + alg</b>	<b>22 (chosen)</b>	<b>&lt;10 h</b>
7	<b>diff + alg</b>	<b>2000 (chosen)</b>	<b>10000 s</b>
8	diff (Biham,Shamir)	50000 (chosen)	100 s
	lin (Matsui)	$2^{20}$ (known)	40 s
	<b>diff + alg</b>	<b>11500 (chosen)</b>	<b><math>2^{25}</math> s</b>
	diff+lin (Hellman,Langford)	512 (chosen)	few seconds

# Conclusion

- Use of statistical methods in algebraic cryptanalysis.
  - New attacks on 6, 7 and 8 rounds of DES using dedicated characteristics.
- Tradeoff plaintexts/time.

# Conclusion

- Use of statistical methods in algebraic cryptanalysis.
  - New attacks on 6, 7 and 8 rounds of DES using dedicated characteristics.
- Tradeoff plaintexts/time.

## Related work



M. Albrecht and C. Cid

*Algebraic Techniques in Differential Cryptanalysis*

FSE2009

# Conclusion

- Use of statistical methods in algebraic cryptanalysis.  
→ New attacks on 6, 7 and 8 rounds of DES using dedicated characteristics.
- Tradeoff plaintexts/time.

## Related work



M. Albrecht and C. Cid

*Algebraic Techniques in Differential Cryptanalysis*

FSE2009

## Future work

- Extension of this attack for more rounds ?
- Algebraic-differential cryptanalysis of DES with Gröbner Bases ?
- Other cryptosystems ?
- Other statistical tools (differential-linear cryptanalysis, ...) ?