Algebraic-Differential Cryptanalysis of DES

Jean-Charles FAUGÈRE, Ludovic PERRET, Pierre-Jean SPAENLEHAUER

UPMC, Univ Paris 06, LIP6
INRIA, Centre Paris-Rocquencourt, SALSA Project
CNRS, UMR 7606, LIP6
104, avenue du Président Kennedy
75016 Paris, France

Abstract. Algebraic cryptanalysis is as a general framework that permits to assess the security of a wide range of cryptographic schemes. However, the feasibility of algebraic cryptanalysis against block ciphers remains the source of speculation and especially in targeting modern block ciphers. The main problem is that the size of the corresponding algebraic system is so huge (thousand of variables and equations) that nobody is able to predict correctly the complexity of solving such polynomial systems. To make algebraic attacks efficient it seems clear that new ideas are required. One possible room for improvement is related to the modeling. A new trend in this area is to combine statistical and algebraic attacks. In this paper, we will present an attack against round-reduced version on DES mixing algebraic and differential techniques. The use of differential permits to ease the solving step; whilst algebraic techniques allows to decrease the numbers of pairs required for a classical differential cryptanalysis. In particular, we have reduced the minimum numbers of pairs required for 6, 7 and 8 rounds of DES. On the other hand, the cost of the attack is higher than a standard usual differential cryptanalysis (but remaining at a reasonable level). For instance, for 6 rounds of DES we have reduced the number of pairs to 32 and the cost is 3000 seconds (to be compared with 240 pairs for the original attack of Biham and Shamir).

1 Introduction

Algebraic cryptanalysis is as a general method to evaluate the security of a cryptographic scheme. It is a general technique that applies potentially to a wide range of cryptosystems, [3, 13–15, 22–25] and in particular to block ciphers. The basic principle of such cryptanalysis is to model a cryptographic primitive by a set of algebraic equations. The system of equations is constructed in such a way as to have a correspondence between the solutions of this system, and a secret information of the cryptographic primitive (for instance, the secret key of a block cipher).

On the one hand algebraic techniques have been successfully applied against a number of multivariate schemes and in stream cipher cryptanalysis. On the other hand, the feasibility of algebraic cryptanalysis against block ciphers still remains the source of speculation. The main problem is that the size of the corresponding algebraic system is so huge (thousand of variables and equations) that nobody is able to predict correctly the complexity of solving such polynomial systems. Consequently, although it has received much attention since its proposal in [13, 12] against the US NIST Advanced Encryption Standard (AES) and Serpent block ciphers, this method has so far had limited success in targeting modern block ciphers. But, It is worth to remark that there is not a unique algebraic description of a cryptographic primitive. Although it is an open issue how to optimally model a cryptosystem, it is crucial to use this degree of freedom to derive the best system with respect to equations solving. For instance, so far algebraic cryptanalysis against block ciphers only required *one* message/ciphertext pair. But recent developments [26, 1, 2] involving the combination of algebraic and statistical techniques have shown the potential benefit of using several message/ciphertext pairs. In this paper, we will consider an attack mixing algebraic and differential techniques against DES. We shall call this attack *algebraic-differential* attack. In practice to evaluate the complexity of this attack we have to evaluate the complexity of solving a system of polynomial equations. To solve this system of equations we can use different techniques:

Gröbner bases [8],Triangular set methods [17] or SAT solvers. In this short paper and for practical reasons, we restrict ourselves to SAT solvers. Precisely, we have used MiniSat[1].

After this short introduction, the paper is organized as follows. In section 2, we will describe more precisely our algebraic-differential attack. In the last section, we present experimental results against round reduced versions of DES. Precisely, we have considered DES reduced to 6, 7 and 8 rounds. For theses reduced versions, our attack permits to decrease the number of pairs usually required to mount a differential attack. On the other hand, the complexity of our approach is higher (but remaining at a reasonable level). This is due to the fact that we have to solve an non-linear system of equations (rather than a key guessing technique for a differential attack). However, the number of messages is a critical quantity for mounting a statistical attack in practice. So, we believe that it is worth to decrease the amount of data required.

2 Algebraic-Differential Attack

In its usual form, algebraic cryptanalysis only requires one plaintext/ciphertext pair to be mounted. In this paper, we will consider the use of several such pairs. More precisely, let $(M_i, C_i)_{1 \leq i \leq N}$ be a set of N message/ciphertext pairs encrypted with the same secret key. For each $i, 1 \leq i \leq N$, we can construct an algebraic system of equation $F_i(M_i, C_i)$ whose variables correspond to the bits of the secret key, but also to the intermediate states[2] of the cipher (we refer to [16, 31] for details regarding the algebraic modeling of DES). Instead of trying to solve each system F_i individually, the idea is to solve their union :

$$\bigcup_i F_i(M_i, C_i).$$

Obviously, the secret key will also be a solution of this larger system.

Unfortunately, if the messages are chosen randomly, it is very unlikely that this approach leads to any practical improvement. Although the key variables remains the same for all the systems, new variables corresponding to the intermediate states of each message/ciphertext pair must be introduced. This way, the number of variables is significantly increased making the new system usually harder to solve in practice (see [26]).

The key idea is to choose a suitable set of correlated messages. To do so, we have considered differential cryptanalysis [4–6]; which is a rather standard attack for DES. The basic idea of this classical technique is to predict how the difference of two well chosen messages M and M' will evolve throughout the rounds of DES. A probabilistic relationship between the differences of consecutive rounds of a block cipher is called a *differential characteristic* in literature. If an attacker is able to find such a differential characteristic with a good probability, the attacker can eventually recover the secret key.

From an algebraic system–solving perspective, differential cryptanalysis permits to predict linear equations between the intermediate variables of two systems $F(M, C)$ and $F'(M', C')$ generated from two distinct message/ciphertext pairs (M, C) and (M', C'). Thus, we can explicitly add linear equations as predicted by the differential characteristic to the system $F \cup F'$, and try to solve this new system. A related idea has been used by Albrecht and Cid [1, 2] to attack PRESENT [7]. Interestingly enough, we will see that the best characteristics known in the literature are not necessarily the best for our algebraic-differential attack.

3 Experimental Results

In this section, we will present the practical results obtained with our algebraic-differential attack. As already explained, we have used MiniSAT for solving the algebraic systems.

[1] http://minisat.se/

[2] such variables must be introduced in order to keep the degree of the system sufficiently low.

3.1 6 rounds

To mount the attack, we have considered the two 3-rounds characteristics proposed by Biham and Shamir in [4]. In this case, the probability that a pair of plaintexts follows the characteristic is 1/16. For a random key and random pairs of plaintexts, the average time needed by MiniSAT to find a contradiction – when the pair doesn't follow the characteristic – is 161 seconds. On the other hand, when a pair follows the characteristic, the average time needed by MiniSAT to recover the key is 244 seconds. The probability of following the characteristic is 1/16, thus the expected time to recover the key is $161 \cdot 15 + 244 = 2659$ seconds. The required number of chosen plaintext-ciphertext is 32. We can now compare this attack with a direct SAT-solver attack [13] and with differential cryptanalysis :

- This attack. Expected time : 2659 seconds, 32 chosen ciphertexts.
- Differential cryptanalysis [4]. Expected time : less than 1 second, 240 chosen ciphertexts.
- Direct attack [13] (Bard, Courtois). Expected time : 2^{25} seconds, 1 known ciphertext.

We see here that this attack needs less ciphertexts than differential cryptanalysis, and can also be mounted in reasonable time.

Reducing the number of ciphertexts. A fundamental difference between this attack and classical differential cryptanalysis is that we need only one "good" pair (i.e. a pair following a given characteristic) to recover the key. Thus, we can use many characteristics simultaneously to increase the probability of success of our approach, and then reducing the required ciphertexts. First of all, we need to find several 3-rounds characteristics. It is proven that the 3-rounds characteristics given in [4] are the only 3-rounds characteristics with probability 1/16. So, we have to find characteristics occurring with smaller probabilities. We have found four characteristics with probability $(14/64)^2$. By combining those characteristics, we were able to reduce the expected number of required ciphertexts to 22 (with an average running time of less than ten hours).

3.2 7 rounds

For seven rounds, things are a bit more complicated. The 3-rounds characteristics we used for the 6-rounds are not good enough. An attack with those characteristics would be less efficient than exhaustive search. Thus, we need a 4-rounds characteristic at least. By examining the different S-boxes and the propagation of their outputs, we came up with a full 4-round characteristic – and some additional constraints on the fifth round – with probability around 1/998. Then an algebraic-differential attack mounted with this characteristic needs about 2000 chosen ciphertexts and will cost 10000 seconds.

3.3 8 rounds

An extension of the characteristic used previously gives a 5-round characteristic which can be used for eight rounds. However, the probability of this characteristic is about 1/31500. Unfortunately, the number of ciphertexts required would be greater than the number of ciphertexts in the classical differential attack. To reduce the number of ciphertexts, we have to relax some constraints to increase the probability of the characteristic. This also increases the expected time of the attack. However, we can combine this differential-algebraic attack with an exhaustive search over eight bits of the key to be more efficient. Finally, the attack on eight rounds needs 11500 chosen ciphertexts and the expected time is about 2^{25} seconds.

The following table shows comparisons between the attacks presented in this paper, classical statistical attacks [4, 27, 29] and the direct SAT-solver attacks [16].

♯ rounds	Cryptanalysis	♯ ciphertexts	Time (in seconds)
6	diff. (Biham,Shamir)[4]	240(chosen)	< 1
	diff. (Knudsen)[27]	46(chosen)	< 10
	alg. (Courtois,Bard)[16]	1 (known)	2^{25}
	diff. + alg.	32 **(chosen)**	3000
	diff. + alg.	22 **(chosen)**	< 36000
7	**diff. + alg.**	2000 **(chosen)**	10000
8	diff(Biham,Shamir)[4]	50000 (chosen)	100
	lin(Matsui)[29]	2^{20} (known)	40
	diff. + alg.	11500 **(chosen)**	2^{25}

4 Conclusion

In this note, we have described an algebraic-differential attack against round-reduced versions of DES. It turns out that our approach permits to decrease the number of pairs required in a pure statistical attack. This is a work in progress. In particular, we are planning to use more advanced tools to solve the algebraic systems: for instance, the F_5 [21] algorithm. In particular, we expect to decrease the complexity of the solving step for 8 rounds attacks.

References

1. M. Albrecht, C. Cid. *Algebraic Techniques in Differential Cryptanalysis.* Fast Software Encryption (FSE 2008), Lecture Notes in Computer Science, to appear.
2. M. Albrecht, and C. Cid. *Algebraic Techniques in Differential Cryptanalysis.* Proceedings of the First International Conference on Symbolic Computation and Cryptography, SCC 2008, Beijing, China, April 2008.
3. G. Ars. *Applications des bases de Gröbner à la cryptographie.* Thèse de doctorat, Université de Rennes I, 2004.
4. E. Biham, and A. Shamir. *Differential Cryptanalysis of DES-like Cryptosystems.* Advances in Cryptology – CRYPTO 1990, Lecture Notes in Computer Science, vol. 537, Springer–Verlag, pp. 2-21, 1991.
5. E. Biham, and A. Shamir. *Differential Cryptanalysis of DES-like Cryptosystems.* Journal of Cryptology, 4(1):3–72, 1991.
6. E. Biham, and A. Shamir. *Differential Cryptanalysis of of the Full 16-round DES.* Advances in Cryptology – CRYPTO 1992, Lecture Notes in Computer Science, vol. 740, Springer–Verlag, pp. 487–496, 1992.
7. A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT*: An ultra-lightweight block cipher.* Cryptographic Hardware and Embedded Systems – CHES 2007, Lecture Notes in Computer Science, vol. 7427, pp. 450–466, Springer–Verlag, 2007.
8. B. Buchberger. *Ein algorithmisches Kriterium fur die Lösbarkeit eines algebraischen Gleichungssystems (An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations).* Aequationes mathematicae 4/3, 1970, pp. 374-383. (English translation in: B. Buchberger, F. Winkler (eds.), Grobner Bases and Applications, Proceedings of the International Conference "33 Years of Gröbner Bases", 1998, RISC, Austria, London Mathematical Society Lecture Note Series, Vol. 251, Cambridge University Press, 1998, pp. 535 -545.)
9. J. Buchmann, A. Pyshkin, and R-P Weinmann. *Block Ciphers Sensitive to Gröbner Basis Attacks.* Topics in Cryptology – CT RSA'06, Lecture Notes in Computer Science, vol. 3860, Springer–Verlag, pp. 313–331, 2006.
10. J. Buchmann, A. Pyshkin, and R-P Weinmann. *A Zero-Dimensional Gröbner Basis for AES-*128. Topics in Cryptology - CT RSA'06, Lecture Notes in Computer Science, vol. 4047, Springer–Verlag, pp. 78–88, 2006.
11. C. Cid, S. Murphy, and M.J. B. Robshaw. *Small Scale Variants of the AES.* Fast Software Encryption (FSE 2005), Lecture Notes in Computer Science, vol. 3557, Springer–Verlag, pp. 267–287, 2005.

12. C. Cid, S. Murphy, and M.J. B. Robshaw. *Algebraic Aspects of the Advanced Encryption Standard.* Springer Verlag, 2006.
13. N. Courtois, and J. Pieprzyk. *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations.* Advances in Cryptology – ASICAC 2002, Lecture Notes in Computer Science, vol. 2501, pp. 267–287, 2002.
14. N. Courtois, and W. Meier. *Algebraic Attacks on Stream Ciphers with Linear Feedback.* Advances in Cryptology – EUROCRYPT 2003, Lecture Notes in Computer Science, vol. 2656, pp. 345–359, 2003.
15. N. Courtois. *Fast Algebraic Attacks on Stream Ciphers with Linear Feedback.* Advances in Cryptology – CRYPTO 2003, Lecture Notes in Computer Science, vol. 2729, pp. 176–194, 2003.
16. N. Courtois. G.V. Bard *Algebraic Cryptanalysis of the Data Encryption Standard.* Lecture Notes in Computer Science, vol. 4887, pp. 152–169, 2007.
17. D. A. Cox, J.B. Little and D. O'Shea. *Ideals, Varieties, and algorithms: an Introduction to Computational Algebraic Geometry and Commutative algebra.* Undergraduate Texts in Mathematics. Springer-Verlag. New York, 1992.
18. J. Daemen, V. Rijmen. *The Design of Rijndael: The Wide Trail Strategy.* Springer-Verlag (2001).
19. B. Debraize. *Méthodes de cryptanalyse pour les schémas de chiffrement symétrique.* Thèse de doctorat, Université de Versailles, 2008.
20. FIPS. Specification for the Advanced Encryption Standard (aes)). Federal Information Processing Standards Publication 197, 2001. Available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
21. J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Basis without Reduction to Zero:* F_5. Proceedings of ISSAC, pp. 75–83. ACM press, July 2002.
22. J.-C. Faugère, and A. Joux. *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner bases.* Advances in Cryptology – CRYPTO 2003, Lecture Notes in Computer Science, vol. 2729, Springer-Verlag, pp. 44–60, 2003.
23. J.-C. Faugère, and L. Perret. *Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects.* Advances in Cryptology – EUROCRYPT 2006, Lecture Notes in Computer Science, vol. 4004, pp. 30–47, 2006.
24. J.-C. Faugère, and L. Perret. *Cryptanalysis of* $2R^-$ *Schemes.* Advances in Cryptology – CRYPTO 2006, Lecture Notes in Computer Science, vol. 4117, pp. 357–372, 2006.
25. J.-C. Faugère, F. Levy-dit-Vehel, and L. Perret. *Cryptanalysis of MinRank.* Advances in Cryptology -CRYPTO 2008, Lecture Notes in Computer Science, vol. 5157, pp. 280–296, 2008.
26. J.-C. Faugère, and L. Perret. *Algebraic Cryptanalysis of Curry and Flurry using Correlated Messages.* Available at `http://eprint.iacr.org/2008/402`.
27. L.R. Knudsen *Truncated and Higher Order Differentials.* Fast Software Encryption (FSE 1995), Lecture Notes in Computer Science, vol. 1008, Springer–Verlag, pp. 196–211, 1995.
28. X. Lai. *Higher Order Derivatives and Differential Cryptanalysis.* Communications and Cryptography, Kluwer Academic Publishers, pp. 227–233, 1994.
29. M. Matsui. *Linear Cryptanalysis Method for DES Cipher.* Advances in Cryptology - Eurocrypt 1993, Lecture Notes in Computer Science, vol. 765, Springer–Verlag, pp. 386–397, 1993.
30. S. Murphy and M. Robshaw. Essential Algebraic Structure Within the AES. In M. Yung, editor, *Advances in Cryptology — CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 1–16. Springer Verlag, 2002. Available at http://www.isg.rhul.ac.uk/ mrobshaw/rijndael/aes-crypto.pdf.
31. H. Raddum and I. Semaev. *New Technique for Solving Sparse Equation Systems.* Cryptology ePrint Archive: Report 2006/475. Available at `http://eprint.iacr.org/2006/475`.