About Filiol's Observations on DES, AES and Hash Functions (draft)

Nicolas T. Courtois

CP8 Crypto Lab, SchlumbergerSema, 36-38 rue de la Princesse
BP 45, 78430 Louveciennes Cedex, France
http://www.nicolascourtois.net
courtois@minrank.org

Abstract. Recently Filiol proposed to test cryptographic algorithms by making statistics on the number of low degree terms in the boolean functions. The paper has been published on eprint on 23th of July 2002. In this paper we reproduce some of Filiol's simulations. We did not confirm his results: our results suggest that DES, AES, and major hash functions have no significative bias and their output bits behave just like random boolean functions.

Remark: Few hours after the publication of this paper on eprint, Filiol updated his paper. His new updated results show that there is indeed no bias in the terms of degree ≤ 2 in DES or AES. Thus Filiol confirmed our results. However he still does claim some other biases in DES and AES for different, more complex tests. Who knows...

Key Words: block ciphers, DES, AES, hash functions, SHA-1, Haval, RIPEMD, MD4, MD5, boolean functions.

1 Introduction

In a recent paper [2], Filiol proposes to test cryptographic algorithms by making statistics on the number of low degree terms in boolean functions. Finding any bias in real-life block ciphers or hash functions is very worrisome.

Filiol considers each of the outputs of an encryption scheme, or a hash function, as a boolean function in the key variables and plaintext variables.

$$f_i\left(p_1, \ldots, p_n, k_1, \ldots, k_{n'}\right).$$

Then he looks at the low degree terms in these boolean functions f_i, that can be computed using the Möbius Transform, see [2]. For example he counts the monomials of type $p_i k_j$. Then he tries to see if in the given boolean functions f_i, the number of such monomials, does or does not look like the f_i are random boolean functions. In order to see this he transforms this number to a variable that has standard normal distribution and computes D^2 being the sum of squares of all these variables, see [2]. We note that, following [2], in order to have a statistical bias susceptible to occur with probability $\alpha = 0.05$ we need to have one of the values $D^2 > 159.59$.

2 The Observations on DES made by Filiol

We consider each of the 64 outputs of DES as a boolean function of 64+56 variables:

$$f_i\left(p_1, \ldots, p_{64}, k_1, \ldots, k_{56}\right).$$

We are interested in the low degree terms in these 64 boolean functions f_i, and we are going to look at, for example terms of degree 1 and try to see if given the 64 samples, if their number does look like the f_i are random boolean functions. For example T_1^1 mesures the square of the standard deviation of the 64 normalised variables reflecting the number of linear terms in each of the the f_i.

In [2], it is shown that (apparently) some strong biases would exist in the boolean functions that constitute DES. We reproduced the computation made in [2], and did not find any such result. Here are our results, using the same notations than in [2]:

Algorithm	Rounds	T_1^1	T_1^2	$T_1^1\|p$	$T_1^1\|k$	$T_1^1\|pp$	$T_1^1\|kk$	$T_1^1\|pk$
DES Encr.	16	35.07	26.66	34.75	35.57	34.10	26.84	33.26
DES Decr.	16	33.68	38.14	34.75	39.75	34.10	21.79	29.95

Assuming that we followed exactly the paper by Filiol, that is not always perfectly clear, our results are different from the results of [2]. We did not confirm the biases found by Filiol. All the results are much smaller than 159.59 and look very normal.

Remark: We note that due to the reversible construction of DES, as long as the key variables are not concerned, the results should be the same for $T_1^1|p$ or $T_1^1|pp$ for both Encryption and Decryption. This is indeed what we observed, and it is also true for the figures given in the paper [2]. However the exact results are very different.

3 Results on AES

We also reproduced the simulations on AES.

Algorithm	Rounds	T_1^1	T_1^2	$T_1^1\|p$	$T_1^1\|k$	$T_1^1\|pp$	$T_1^1\|kk$	$T_1^1\|pk$
AES Encr.	10	59.62	58.11	57.84	61.52	63.57	71.14	62.39
AES Decr.	10	67.38	56.28	67.22	70.70	62.62	70.94	47.24

Again we did not observe any bias or irregularity. In some cases we obtained the same figures than Filiol. But not in any interesting case.

4 Hash Functions

In the paper [2] one reads the following statements:

$$\text{SHA-1} \succeq \text{RIPEMD160} \succeq \text{SHA-0}$$

However if we look at the results (assuming that they are correct) we do not see any bias, the test just gives some results for D^2. If we change a small detail in a hash function, for example XOR a constant to the key or change the test, all the results will change, and for example SHA-0 will become better than SHA-1. It seems that these results are always just noise, generated by the behaviour of the hash function in the close neighbourhood (in the sense of Hamming distance) of the key being zero and the plaintext being zero. If we choose a different neighbourhood the results will be just different. We get no information whatsoever. We conclude that these results probably does not give **any useful information** on the strength of the hash functions.

5 Conclusion

It is hard to believe that such biases, as suggested by Filiol, would exist for a cipher or hash functions that have several rounds, see [4].

Our results show that DES, AES, and major hash functions have probably no significative bias. In all our simulations they behaved just like random boolean functions. It seems that there was a mistake in the simulation results initially published by Filiol. However other, more complex irregularities may exist on DES or AES, who knows...

Acknowledgments: Nicolas Deig helped to program the simulations of this paper.

References

1. Joan Daemen, Vincent Rijmen: *AES proposal: Rijndael;* The latest revised version of the proposal is available on the internet, `http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf`
2. Eric Filiol: *A New Statistical Testing for Symmetric Ciphers and Hash Functions,* The preliminary version published on eprint on 23th of july 2002, `http://eprint.iacr.org/2002/099/`.
3. *Data Encryption Standard (DES),* Federal Information Processing Standards Publication (FIPS PUB) 46-3, National Bureau of Standards, Gaithersburg, MD (1999). Available from `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`
4. Serge Vaudenay: *Provable Security for Block Ciphers by Decorrelation;* Technical Report LIENS-98-8 of the Laboratoire d'Informatique de l'Ecole Normale Supérieure, 1998. Available at `http://lasecwww.epfl.ch/query.msql?ref=Vau98b`.