X-Authentication-Warning: morille.ens.fr: vaudenay owned process doing -bs
Date: Thu, 15 Apr 1999 10:26:50 +0200 (MET DST)
From: Serge Vaudenay <Serge.Vaudenay@ens.fr>
X-Sender: vaudenay@morille.ens.fr
To: AESFirstRound@nist.gov
cc: Shiho MORIAI <shiho@sucaba.isl.ntt.co.jp>
Subject: randomness

Dear Jim,

here is a formal report on the randomness which is related to Shiho's presentation during the rump session. Please let me know if you have any problem to read it.

Best regards

Serge

Comparison of the Randomness Provided by Some AES Candidates

Serge Vaudenay[1]*and Shiho Moriai[2]

[1] Ecole Normale Supérieure – CNRS
[2] NTT Laboratories

April 15, 1999

Abstract. Using the decorrelation techniques we compare the randomness of three schemes used in the AES candidates. The target schemes are the original Feistel scheme and two modified Feistel schemes: the MARS-like structure and the CAST256-like structure. As a result, the required numbers of rounds for Luby-Rackoff's randomness (which is related to resistance against chosen plaintext attacks) are 3, 5, and 7, respectively. Moreover, the required numbers of rounds for achieving the decorrelation bias of order two of 2^{-128} are 9, 25, and 35, respectively. This holds for truly random round functions. Imperfect random round functions can achieve similar decorrelation by using decorrelation modules like in DFC, but need a number of rounds of at least 9, 30 and 42 respectively.

1 Introduction

So far, none of the comments on the AES candidates address the problem of randomness provided by the design proposals. Randomness means that no oracle circuit with polynomially many oracle gates can distinguish between the encryption function and a truly random permutation. Originally, Luby and Rackoff proved that a random 3-round Feistel scheme on m-bit blocks was indistinguishable from a truly random permutation by an attack limited to $2^{\frac{m}{4}}$. Our motivation is to see how Luby-Rackoff Theorem extends to the Feistel scheme variants which are used in MARS and CAST-256. We compare the randomness of three schemes used in the AES candidates using the decorrelation techniques which were introduced by Vaudenay [5].

The target schemes in this paper are the Feistel scheme (Figure 1), which is used in DEAL, DFC, E2, LOKI97, MAGENTA, RC6 and Twofish, and two

*This work was done during the stay at NTT Laboratories

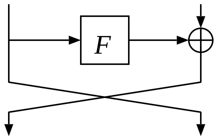

Figure 1: The Feistel Scheme

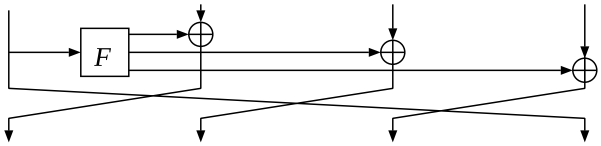

Figure 2: The MARS-like Scheme

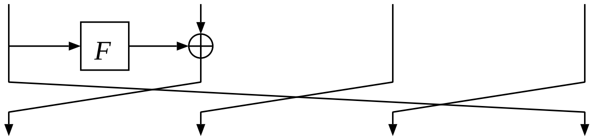

Figure 3: The CAST256-like Scheme

modified Feistel schemes: the MARS-like scheme (Figure 2) which is used in MARS, and the CAST256-like scheme (Figure 3) which is used in CAST-256.[1]

2 Comparison in Luby-Rackoff's randomness

This section studies how many rounds are required for Luby-Rackoff's randomness when considering round functions as random ones. This is related to the "lack of randomness" provided by the upper level design. The required numbers of rounds for the Feistel scheme and the CAST256-like scheme are shown in [8, Section 3.2]. In their paper both of the Feistel scheme and the CAST256-like scheme are generalized as the Type-1 Transformation, and the required number of rounds is proven to be $2k-1$, where k is the number of branches. That is, the required numbers of rounds for the Feistel scheme and CAST256-like scheme are 3 and 7, respectively.

The required number of rounds for the MARS-like scheme can easily be proven to be $k+1$, which is 5 here. (This will be detailed in the full paper.)

[1] The $\oplus$ on figures can be replaced by any other group operation without affecting the present results.

3 Comparison of Decorrelation Bias

We use the decorrelation bias of order d of a permutation in the sense of a given norm $||.||_a$ defined by

$$\mathrm{DecP}^d_{||.||_a}(C) = ||[C]^d - [C^*]^d]||_a$$

where C^* is a random permutation uniformly distributed. (For details, see [5, 7].) Intuitively, $\mathrm{DecP}^d_{||.||}(C)$ is a measure of efficiency of attacks limited to d chosen plaintexts.

Luby-Rackoff Theorem states that

$$\mathrm{DecP}^d_{||.||_a}(C) \leq 2d^2.2^{-\frac{m}{2}}$$

for a random 3-round regular Feistel cipher with $m = 128$ (the block length). Similarly we obtain that

$$\mathrm{DecP}^d_{||.||_a}(C) \leq kd^2.2^{-\frac{m}{k}}$$

for a random 7-round CAST256-like cipher with $k = 4$ (the number of branches) and

$$\mathrm{DecP}^d_{||.||_a}(C) \leq 2d^2.2^{-\frac{m}{k}}$$

for a random 5-round MARS-like cipher with $k = 4$. In particular, this means we cannot guaranty security (in this way) when the number of plaintext d is larger than 2^{16} for both CAST-256 and MARS although regular Feistel schemes reach the $d = 2^{32}$ bound.

Decorrelation of order $d = 2$ plays a crucial role for the resistance against differential and linear cryptanalysis. Namely, we need a pairwise decorrelation bias smaller than 2^{-128} in order to ensure that both attacks are inefficient. The multiplicativity of decorrelation biases enables to get the smallest number of rounds in order to achieve it. We obtain that we need at least 9, 35 and 25 rounds for regular Feistel, CAST256-like and MARS-like schemes respectively.

4 Imperfect Decorrelation

The previous results are meaningful when the round function is perfectly random. We can still obtain provable decorrelation bias upper bound with real functions, as in the Peanut construction (on which DFC is based). For this we apply a theorem which is stated in [6]. This construction basically says that we use

$$\sigma(ax + b \bmod p \bmod 2^m)$$

for a permutation σ, keyed numbers a and b, where p is the smallest prime number greater than 2^m. With $m = 128$, regular Feistel schemes can use $p = 2^{64} + 13$, but CAST-256 and MARS need $p = 2^{32} + 15$. By applying the same construction we obtain that the number of rounds for regular Feistel, CAST256-like and MARS-like schemes are 9, 42 and 30 respectively.

5 Conclusion

CAST-256 has 48 rounds, which is fairly enough. MARS has 32 rounds, which is right on the edge of our randomness bounds. DEAL and MAGENTA are 6-round Feistel scheme, which is not enough at all. DFC purposely stands on the edge with 8 rounds. E2 (12 rounds), LOKI97 (16 rounds), RC6 (20 rounds) and Twofish (16 rounds) have far beyond the smallest number of safe rounds.

Other designs like CRYPTON, Rijndael, SAFER+ and Serpent can be investigated as well. A preliminary study suggested that these designs required too many rounds for randomness, because the size of the elementary round functions is too small. No clue is suggested for investigating FROG or HPC.

We believe that the ability to prove almost randomness is an important feature for the next encryption standard. For this we would recommend to select the finalists from

CAST-256, DFC, E2, MARS, RC6, and Twofish.

(We removed LOKI97 from this list because of the attacks which were announced against it.)

References

[1] E. Biham, A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.

[2] H. Feistel. Cryptography and Computer Privacy. *Scientific American*, vol. 228, pp. 15–23, 1973.

[3] M. Luby, C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing*, vol. 17, pp. 373–386, 1988.

[4] M. Matsui. The First Experimental Cryptanalysis of the Data Encryption Standard. In *Advances in Cryptology CRYPTO'94*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 839, pp. 1–11, Springer-Verlag, 1994.

[5] S. Vaudenay. Provable Security for Block Ciphers by Decorrelation. In *STACS 98*, Paris, France, Lectures Notes in Computer Science 1373, pp. 249–275, Springer-Verlag, 1998.

[6] S. Vaudenay. On the Lai-Massey Scheme. Technical report LIENS-99-3, Ecole Normale Supérieure, 1999.
URL:`ftp://ftp.ens.fr/pub/reports/liens/liens-99-3.A4.ps.Z`

[7] S. Vaudenay. Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness. Technical report LIENS-99-2, Ecole Normale Supérieure, 1999.
URL:`ftp://ftp.ens.fr/pub/reports/liens/liens-99-2.A4.ps.Z`

[8] Y.Zheng, T.Matsumoto, and H.Imai. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. In *Advances in Cryptology CRYPTO'89*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 435, pp. 461–480, Springer-Verlag, 1990. 1990