ON DECORRELATED FAST CIPHER

Wu Wenling  Li Bao  Feng Denguuo  Qing Sihan
(Engineering Research Center for Information Security Technology,
Chinese Academy of Sciences, Beijing 100080)

Abstract  Decorrelated Fast Cipher (DFC) is a candidate for the Advanced Encryption Standard (AES). It is shown that the cryptographic properties of the confusion permutation of DFC are weak in this paper. With the same F-function of DFC, a Feistel cipher VDFC which has no resistance against differential cryptanalysis is constructed. This demonstrates the importance of the key addition into DFC sufficiently. As a result, DFC may not be qualified candidate for the AES.

Key words  Round function; Permutation; Differential cryptanalysis; Nonlinearity

I. Introduction

For many applications, the data encryption standard algorithm is nearing the end of its lifetime. Its 56-bit key is too small, as shown by a recent distributed key search process. Although triple-DES can solve the key length problem, the DES algorithm was primarily designed for hardware encryption, yet the great majority of its applications today implement it in software, where it is relatively inefficient.

For these reasons, the US National Institute of Standards and Technology (NIST) has issued a call for a successor algorithm, to be called the Advanced Encryption Standard (AES). Decorrelated Fast Cipher (DFC) is a candidate for AES which have been issued by NIST. They have a 128-bit block length and a 256-bit key length (though keys of 128 and 192 bits must also be supported).

1. The structure of DFC

DFC encrypts a 128-bit plaintext block, which is split into two 64-bit halves. In each round the right half and a 128-bit subkey are fed into the function F. The output of F is XORed with the left half, then the halves are swapped. This process is repeated for all but the final round, where the final swap is left out. At the end of the rounds, the halves are concatenated to form the ciphertext block. Decryption follows the same procedure, except that the subkeys are used in reverse order.

2. The F-function

The F-function (as for “Round Function”) is fed with one 128-bit parameter (subkey), or equivalently two 64-bit parameters: an “a-parameter” and a “b-parameter”. It processes a 64-bit input and outputs a 64-bit string.

\[ F_{a/b}(x) = CP((((a + b) \mod 2^{64} + 13)) \mod 2^{64})_{64} \]

where CP is a permutation over the set of all 64-bit strings.

3. The Confusion Permutation (CP)

The CP uses a look-up table RT (as for “Round Table”) which takes a 6-bit integer as input and provides a 32-bit string output.
Let $X = X_l | X_r$ be the input of CP where $X_l$ and $X_r$ are two 32-bit strings. We define

$$CP(X) = |(X_r \oplus RT (\text{trunc}_6(X_l)))|(X_l \oplus \text{KC}) + \text{KD}) \mod 2^{64}$$

where $\text{KC} = \text{eb64749a}$ and $\text{KD} = 86dlbf275b9b241d$.

II. Cryptographic Properties of CP

Let $CP = (f_0, f_1, \cdots, f_{63}) : GF(2)^{64} \to GF(2)^{64}$

$$X \to Z$$

Then

$$z_0 = f_0(x_0, \cdots, x_{63})$$
$$z_1 = f_1(x_0, \cdots, x_{31}, x_{33}, \cdots, x_{63})$$
$$z_2 = f_2(x_0, \cdots, x_{31}, x_{34}, \cdots, x_{63})$$
$$\vdots$$
$$z_i = f_i(x_0, \cdots, x_{31}, x_{31+i+1}, \cdots, x_{63})$$
$$\vdots$$
$$z_{31} = f_{31}(x_0, \cdots, x_{31}, x_{63})$$
$$z_{32} = f_{32}(x_0, \cdots, x_{31})$$
$$z_{33} = f_{33}(x_1, \cdots, x_{31})$$
$$\vdots$$
$$z_j = f_j(x_{j-32}, \cdots, x_{31})$$
$$\vdots$$
$$z_{62} = f_{62}(x_{30}, x_{31}) = x_{31} \oplus x_{30} \oplus 1$$
$$z_{63} = f_{63}(x_{31}) = x_{31} \oplus 1$$

We have the following result:

**Theorem 1**

1. CP is not complete,
2. The nonlinearity of CP is 0,
3. The differential uniform of CP is 1.

**Proof**

1. and 2. are from $z_{63} = x_{31} + 1$.
3. Let $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$, $CP(X) \oplus CP(X \oplus e_{32}) = e_1$, hence, the differential uniform of CP is 1.

Q.E.D.

III. Variant of DFC(VDFC)

The structure of VDFC is the same as DFC, its round function is $CP(X, K_i) = CP(X \oplus K_i)$, $K_i$ is the subkey of the $i$-th round. The difference between DFC and VDFC is only subkey addition.

**Lemma 1**

Let $G(X) = X + KD : GF(2)^{64} \to GF(2)^{64}$, then

1. $|\{X \in GF(2)^{64} : G(X) \oplus G(X \oplus e_{24}) = e_{24}\}| \geq 5 \times 2^{61}$,