Higher order differential attacks on iterated block ciphers using almost bent round functions

Anne Canteaut, Marion Videau

Higher order differential attacks on iterated block ciphers using almost bent round functions

Anne Canteaut and Marion Videau
INRIA projet CODES,
BP 105, 78153 Le Chesnay Cedex, FRANCE
e-mail: {Anne.Canteaut, Marion.Videau}@inria.fr

Abstract — **We show that the use of a round function whose Walsh coefficients are divisible by a high power of 2 may lead to a higher order differential attack.**

I. Higher order differential attacks

We consider an r-round iterated block cipher with block size n: $F_{k_r} \circ F_{k_{r-1}} \circ \ldots \circ F_{k_1}$ where the round function F_k is a permutation of $\mathbf{F}_2^n$ for any k. Such a cipher is vulnerable to linear cryptanalysis if there exists (α, β), $\alpha \neq 0$ such that $\alpha \cdot F_k(x) + \beta \cdot x$ takes the same value for most values of $x \in \mathbf{F}_2^n$. This property is related to the Walsh spectrum of F_k.

For any $\alpha \in \mathbf{F}_2^n$, φ_α denotes the linear function $x \mapsto \alpha \cdot x$ where "$\cdot$" is the usual dot product. The *Walsh spectrum* of a function F from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$ is the multiset

$$\{\mathcal{F}(\varphi_\alpha \circ F + \varphi_\beta) = \sum_{x \in \mathbf{F}_2^n} (-1)^{\alpha \cdot F(x) + \beta \cdot x},\ \alpha \in \mathbf{F}_2^n \backslash \{0\}, \beta \in \mathbf{F}_2^n\} .$$

The *nonlinearity* of F is the Hamming distance between all $\varphi_\alpha \circ F$ and the set of affine functions. It is equal to

$$2^{n-1} - \frac{1}{2}\mathcal{L}(F) \quad \text{where} \quad \mathcal{L}(F) = \max_{\alpha \in \mathbf{F}_2^n} \max_{\beta \in \mathbf{F}_2^n} |\mathcal{F}(\varphi_\alpha \circ F + \varphi_\beta)| .$$

The minimum value for $\mathcal{L}(F)$ is $2^{\frac{n+1}{2}}$ and the functions achieving this value are called *almost bent functions*. They provide a high resistance to both linear and differential attacks [2].

The derivative of a function F over $\mathbf{F}_2^n$ with respect to a linear subspace V is defined by $D_V F(x) = \sum_{v \in V} F(x+v)$ where the sum is an addition modulo 2. Suppose that for any round keys, the reduced cipher, i.e., the function $G = F_{k_{r-1}} \circ \ldots \circ F_{k_1}$, has degree d (the degree of G is the maximum degree of its Boolean components). Then, for any $(d+1)$-dimensional subspace V, we have $\sum_{v \in V} G(x+v) = 0$ for all $x \in \mathbf{F}_2^n$. It leads to a differential attack of order $(d+1)$ [4]:

1. Select a random plaintext $x_0 \in \mathbf{F}_2^n$ and get the ciphertexts c_v corresponding to all plaintexts $x_0 + v$, $v \in V$.
2. For each candidate for k_r, compute $\sum_{x \in V} F_{k_r}^{-1}(c_v)$.

The key k_r for which this sum vanishes is the correct last-round key with a high probability. But, the bound $deg(G) \leq (deg(F))^{r-1}$ only enables to apply the attack to the ciphers with low degree round functions.

II. Divisibility of the Walsh spectrum and degree of a composed function

The trivial bound $deg(F \circ F) \leq deg(F)^2$ can be improved when the values occurring in the Walsh spectrum of F are divisible by a high power of 2. By using a relation between the Walsh coefficients of the sum of some Boolean functions and the Walsh coefficients of their product, we can prove

Theorem 1 *Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$ such that all values occurring in its Walsh spectrum are divisible by 2^ℓ. Then, for any function F' from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$, we have*

$$deg(F' \circ F) \leq n - \ell + deg(F') .$$

This result is of great interest when F is almost bent since the Walsh coefficients of any almost bent function over $\mathbf{F}_2^n$ are divisible by $2^{\frac{n+1}{2}}$ [2]. It leads to a new attack on any 5-round Feistel cipher using a highly nonlinear substitution function. In a Feistel cipher with block size $2n$, the round function is defined by $(L, R) \mapsto (R, L + S_k(R))$ where L and R are the left and right halves of the input and S_k is a function over $\mathbf{F}_2^n$ called the substitution function. The right part of the output of the third round, R_3, can be derived from the ciphertext (L_5, R_5) and from k_5: $R_3 = R_5 + S_{k_5}(L_5)$. Moreover, when we consider any plaintext (x, c_0) whose right part is a constant, we have $R_3(x) = x + c_1 + S_{K_3}(c_0 + S_{K_2}(x + c_1))$. When the confusion function S is almost bent, Theorem 1 implies that $deg(R_3) \leq \frac{n-1}{2} + deg(S)$. Thus, we have exhibited a new differential attack of order $\delta = \min((deg(S)^2 + 1, \frac{n+1}{2} + deg(S))$. Since the degree of an almost bent function cannot exceed $(n+1)/2$, this attack is feasible except for almost bent functions of maximal degree. But, it can be improved and performed for any almost bent functions when the round key is inserted by addition. It also applies when S_k is a permutation of an even number of variables which has the highest known nonlinearity. Except the inverse function, all known permutations S achieving $\mathcal{L}(S) = 2^{n/2+1}$ are such that all their Walsh coefficients are divisible by either $2^{n/2}$ or $2^{n/2+1}$ [3].

Theorem 1 also provides an explanation and a generalization of a 7-order differential attack on a reduced version of MISTY1 [6, 1]. This weakness originates from the use of almost bent substitution boxes in the cipher.

References

[1] S. Babbage and L. Frisch. On MISTY1 higher order differential cryptanalysis. In *ICISC 2000*, LNCS 2015, pp. 22–36. Springer-Verlag, 2000.

[2] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In *EUROCRYPT'94*, LNCS 950, pp. 356–365. Springer-Verlag, 1995.

[3] H. Dobbertin. One-to-one highly nonlinear power functions on $GF(2^n)$. *Appl. Algebra Engrg. Comm. Comput.*, 9(2):139–152, 1998.

[4] L. R. Knudsen. Truncated and higher order differentials. In *FSE'94*, LNCS 1008, pp. 196–211. Springer-Verlag, 1995.

[5] X. Lai. Higher order derivatives and differential cryptanalysis. In *Symposium on Communication, Coding and Cryptography in honor of J. Massey on the occasion of his 60'th birthday*, 1994.

[6] H. Tanaka, K. Hisamatsu, and T. Kaneko. Strength of MISTY1 without FL function for higher order differential attack. In *AAECC-13*, LNCS 1719, pp. 221–230. Springer-Verlag, 1999.