Boomerang uniformity of some classes of functions

Kirpa Garg*, Sartaj Ul Hasan*, and Pantelimon Stănică**

*Department of Mathematics, Indian Institute of Technology Jammu, Jammu 181221, India
**Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943, USA

Abstract

We give bounds for the boomerang uniformity of the perturbation of some special classes of permutation functions, namely, Gold, Kasami and inverse functions via trace maps. Consequently, we obtain some classes of functions with low boomerang uniformity as often required for practical purposes.

1 Introduction

Let n, m be positive integers. By $\mathbb{F}_{2^n}$ we denote the finite field with 2^n elements. The finite field $\mathbb{F}_{2^n}$ can also be identified with the vector space $\mathbb{F}_2^n$, and so the elements of $\mathbb{F}_{2^n}$ can be identified with binary vectors of n bits. A vectorial Boolean function or (n, m)-function is a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. Thus, (n, m)-functions can be understood as transformations that take an n-bit sequence as input, and produce an m-bit sequence as output. When $n = m$, then f can be uniquely represented by a univariate polynomial in $\mathbb{F}_{2^n}[X]$. Vectorial Boolean functions are very important objects due to their wide range of applications in coding theory and cryptography. In cryptography, these functions are often used as substitution boxes (S-boxes) in modern block ciphers.

Differential cryptanalysis, introduced by Biham and Shamir [1], is one of the most powerful attacks on block ciphers. The resistance of a vectorial Boolean function against the differential attack is measured by its differential uniformity. For any (n, n)-function f and $a \in \mathbb{F}_q$, where $q = 2^n$, the derivative of f in the direction a is defined as $D_f(X, a) := f(X + a) + f(X)$, for all $X \in \mathbb{F}_q$. The Difference Distribution Table (DDT) entry of f at a point $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$, denoted by $\Delta_f(a, b)$, is the number of solutions $X \in \mathbb{F}_q$ of the equation $D_f(X, a) = b$. The differential uniformity of f, denoted by δ_f, is given by $\delta_f := \max\{\Delta_f(a, b) : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$. We shall use Tr to denote the trace (either absolute, or relative, which will be obvious from the context) of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^m}$, $\mathrm{Tr}(x) = \mathrm{Tr}_{q^n/q^m}(x) = \sum_{i=0}^{n/m-1} x^{q^{mi}}$.

The boomerang attack on block ciphers was proposed by Wagner [13]. In EUROCRYPT-2018, Cid et al. [5] introduced a systematic approach known as the Boomerang Connectivity Table (BCT), to analyze the boomerang style attack. Boura and Canteaut [2] further studied BCT and coined the term boomerang uniformity, which is essentially the maximum value in the BCT, to quantify the resistance of a vectorial Boolean function against the boomerang attack. For any $a, b \in \mathbb{F}_q$, the Boomerang Connectivity Table (BCT) entry at $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, denoted as $\mathcal{B}_f(a, b)$, is the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following system

$$\begin{cases} f(X) + f(Y) = b \\ f(X + a) + f(Y + a) = b. \end{cases}$$

The boomerang uniformity of f is defined as $\beta_f := \max\{\mathcal{B}_f(a, b) \mid a, b \in \mathbb{F}_{2^n}^*\}$.

For any permutation f, Cid et al. [5, Lemma 1] showed that $\mathcal{B}_f(a, b) \geq \Delta_f(a, b)$ for all $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$. Moreover, the authors showed that APN permutations have boomerang uniformity 2. Motivated by the work of Cid et al. [5, Lemma 1], many functions with low boomerang uniformity

have been studied in the last couple of years (see, for example, [3], [7]-[11], [12], [14] and the references therein). Hence, construction of polynomials with low differential and boomerang uniformity is important for designing S-boxes of many block ciphers. For example, the inverse function over $\mathbb{F}_{2^8}$ is used to design the S-box of the Advanced Encryption Standard (AES), and it is a differentially 4-uniform and boomerang 6-uniform permutation over $\mathbb{F}_{2^8}$. In this paper, we deal with the boomerang uniformity of some classes of functions by calculating solutions of some linear equations over $\mathbb{F}_{2^n}$. We provide upper bounds for their boomerang uniformity. These bounds also hold when these functions are permutations.

We shall now give the structure of the paper. In Section 2, we give general bounds for the boomerang uniformity of the perturbed functions over $\mathbb{F}_{2^n}$, and further compute the bounds for boomerang uniformity of perturbed Gold function. Moreover, bounds for the boomerang uniformity of Kasami function under some special conditions are determined. In Section 3, bound for the boomerang uniformity of perturbed inverse function have been computed. We conclude the paper in Section 4.

2 Boomerang uniformity of the perturbed Gold and Kasami functions

We recall the following lemma about the differential uniformity of a class of perturbed functions.

Lemma 2.1 ([4, Proposition 3]) *Let $F(X) = G(X) + \gamma \mathrm{Tr}(H(X))$, where $G(X), H(X) \in \mathbb{F}_{2^n}[X]$ and $\gamma \in \mathbb{F}_{2^n}^*$. Then $\Delta_F \leq 2\Delta_G$.*

It is straightforward to prove the following lemma that gives a nice relationship between the BCT entries of the functions F and G.

Lemma 2.2 *Let $F(X) = G(X) + \gamma \mathrm{Tr}(H(X)) \in \mathbb{F}_{2^n}[X]$, where $\gamma \in \mathbb{F}_{2^n}^*$. Then for any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$*

$$\mathcal{B}_F(a, b) \leq \mathcal{B}_G(a, b) + \mathcal{B}_G(a, b + \gamma) + N_1 + N_2,$$

where

$$N_1 = \left| \left\{ (X, Y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mid \begin{cases} G(X + a) + G(Y + a) = b + \gamma \\ G(X) + G(Y) = b \end{cases} \right\} \right| \tag{1}$$

and

$$N_2 = \left| \left\{ (X, Y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mid \begin{cases} G(X + a) + G(Y + a) = b \\ G(X) + G(Y) = b + \gamma \end{cases} \right\} \right|. \tag{2}$$

We shall now use Lemma 2.2 to compute bounds for the boomerang uniformity of the function F for some particular type of functions G. The following theorem gives a bound for the boomerang uniformity of function F when the function G is a permutation Gold function.

Theorem 2.3 *Let $F(X) = X^{2^k+1} + \gamma \mathrm{Tr}(H(X)) \in \mathbb{F}_{2^n}[X]$, where $\gamma \in \mathbb{F}_{2^n}^*$ and $gcd(k, n) = 1$. Then $\beta_F \leq 12$.*

We now put a restriction on $H(X)$ and take $H(X) = X + X^{2^k+1}$. It is obvious from Lemma 2.1 that the differential uniformity of $F = X^{2^k+1} + \gamma \mathrm{Tr}(X + X^{2^k+1})$ over $\mathbb{F}_2^n$, where $\gamma \in \mathbb{F}_{2^n}^*$ and $\gcd(n, k) = 1$ is bounded above by 4. We shall compute the bounds for boomerang uniformity of the function $F = X^{2^k+1} + \gamma \mathrm{Tr}(X + X^{2^k+1})$ in the next theorem by first finding out DDT entries in the following lemma.

Lemma 2.4 *Let $F(X) = X^{2^k+1} + \gamma \mathrm{Tr}(X + X^{2^k+1}) \in \mathbb{F}_{2^n}[X]$, where $\gamma \in \mathbb{F}_{2^n}^*$ and $\gcd(n, k) = 1$. Then for any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, the DDT entries of the function F are given by*

$$\Delta_F(a, b) = \begin{cases} 0 & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right) \right) = (1, 0), \\ 2 & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right) \right) \in \{(1, 1), (0, 1)\}, \\ 4 & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right) \right) = (0, 0), \quad \text{where } b' := F(a) + b. \end{cases}$$

Theorem 2.5 *Let* $F(X) = X^{2^k+1}+\gamma\mathrm{Tr}(X+X^{2^k+1}) \in \mathbb{F}_{2^n}[X]$, *where* $\gamma \in \mathbb{F}_{2^n}^*$ *and* $\gcd(k,n) = 1$. *Then for any* $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, *the BCT entries of the function* F *are given by*

$$\mathcal{B}_F(a,b) = \begin{cases} 0 & \text{if } (T_\gamma, T_b, T_a, T_Z) = (0,1,0,0), \\ 2 & \text{if } T_\gamma = 1, \\ 4 & \text{if } (T_\gamma, T_b, T_a, T_Z) \in \{(0,0,1,0),(0,0,1,1),(0,0,0,1)\}, \\ 8 & \text{if } (T_\gamma, T_b, T_a, T_Z) \in \{(0,1,0,1),(0,1,1,0),(0,1,1,1)\}, \\ 12 & \text{if } (T_\gamma, T_b, T_a, T_Z) = (0,0,0,0), \end{cases}$$

where $(T_\gamma, T_b, T_a, T_Z) := \left(\mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{b}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{F(a)}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{F(Z)}{a^{2^k+1}}\right)\right)$ *and* Z *is a solution of the equation* $aZ^{2^k} + a^{2^k}Z + \gamma = 0$. *Moreover, when* n *is odd,* $\beta_F \leq 8$.

We know that the Kasami function $X^{2^{2i}-2^i+1}$ is a permutation with boomerang uniformity two over $\mathbb{F}_{2^n}$ for odd n, where $i < n$ and $\gcd(i,n) = 1$. In the following theorem, we shall take $G(X) = X^{2^{2(n-1)}-2^{n-1}+1}$ and give a bound for the boomerang uniformity of the function $F(X) = G(X) + \gamma\mathrm{Tr}(H(X))$ over the finite field $\mathbb{F}_{2^n}$.

Theorem 2.6 *Let* $F(X) = X^{2^{2(n-1)}-2^{n-1}+1} + \gamma\mathrm{Tr}(H(X)) \in \mathbb{F}_{2^n}[X]$, *where* $\gamma \in \mathbb{F}_{2^n}^*$. *Then* $\beta_F \leq 12$, *when* n *is odd.*

3 Boomerang uniformity of the perturbed inverse function

In this section, we shall give bounds for the boomerang uniformity for the general case of perturbed inverse functions. In fact, we prove in the following theorem that for even n, the bound is sixteen and twenty when $n \equiv 2 \pmod 4$ and $n \equiv 0 \pmod 4$, respectively, and twelve for odd n.

Theorem 3.1 *Let* $F(X) = X^{2^n-2}+\gamma\mathrm{Tr}(H(X)) \in \mathbb{F}_{2^n}[X]$, *where* $\gamma \in \mathbb{F}_{2^n}^*$. *Then the Boomerang uniformity* β_F *of* F *is given by*

$$\beta_F \leq \begin{cases} 12 \text{ if } n \text{ is odd}, \\ 16 \text{ if } n \equiv 2 \pmod 4, \\ 20 \text{ if } n \equiv 0 \pmod 4. \end{cases}$$

Hasan et al. [6] considered the function $F(X) = X^{2^n-2} + \gamma\mathrm{Tr}(H(X))$ where $\gamma = 1$ and $H(X) = \frac{X^2}{X+1}$ and they showed that this function has boomerang uniformity at most twelve over $\mathbb{F}_{2^n}$, where n is even. However, in the following theorem, we compute the bounds for the boomerang uniformity for the function $X^{2^n-2} + \gamma\mathrm{Tr}\left(H(x)\right)$ over $\mathbb{F}_{2^n}$, where $H(x) = \frac{X^2+1}{X}$. In fact, we find some conditions on γ so as to obtain slightly better bounds for its boomerang uniformity.

Theorem 3.2 *Let* $F(X) = X^{2^n-2} + \gamma\mathrm{Tr}\left(\frac{X^2+1}{X}\right) \in \mathbb{F}_{2^n}[X]$, *where* n *is even,* $\gamma \in \mathbb{F}_{2^n}^*$ *such that* $\mathrm{Tr}(\gamma) = 0$. *Then the Boomerang uniformity of* F

$$\beta_F \leq \begin{cases} 6 & \text{if } \mathrm{Tr}(\gamma^{-1}) = 0 \\ 12 & \text{if } \mathrm{Tr}(\gamma^{-1}) \neq 0. \end{cases}$$

Theorem 3.3 *Let* $F(X) = X^{2^n-2} + \gamma\mathrm{Tr}\left(\frac{X^2+1}{X}\right) \in \mathbb{F}_{2^n}[X]$, *where* $\gamma \in \mathbb{F}_{2^n}^*$ *satisfies* $\mathrm{Tr}(\gamma) = 0$. *Then the boomerang uniformity of* F, $\beta_F = 2$, *when* n *is odd.*

4 Further comments

We have computed the bounds for the boomerang uniformity of a general class of perturbed functions. Subsequently, we considered special cases of perturbed Gold, Kasami and inverse functions. We also considered some classes of functions for some specific functions $H(X)$. It would be interesting to investigate the boomerang uniformity of the function $F(X) = G(X) + \gamma \mathrm{Tr}(H(X)) \in \mathbb{F}_{2^n}[X]$ by taking different functions G, H and constants γ.

Acknowledgements

We would like to thank Mohit Pal for his careful reading of the initial draft and for several useful discussions.

References

[1] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems,* J. Cryptol. 4(1) (1991) 3–72.

[2] C. Boura, A. Canteaut, *On the boomerang uniformity of cryptographic S-boxes,* IACR Trans. Symmetric Cryptol. 3 (2018) 290–310.

[3] M. Calderini, I. Villa, *On the boomerang uniformity of some permutation polynomials,* Cryptogr. Commun. 12(6) (2020) 1161–1178.

[4] P. Charpin, G. Kyureghyan, *Monomial functions with linear structure and permutation polynomials,* Finite Fields: Theory and Applications, Contemp. Math. 518, Amer. Math. Soc. 3:16 (2010) 99–111.

[5] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, L. Song, *Boomerang connectivity table: a new cryptanalysis tool.* In: J. Nielsen, V. Rijmen (ed) Advances in Cryptology-EUROCRYPT'18, LNCS 10821 683-714, Springer, Cham (2018).

[6] S. U. Hasan, M. Pal, P. Stănică, *The c-diferential uniformity and boomerang uniformity of two classes of permutation polynomials,* IEEE Trans. Inf. Theory 68(1) (2022) 679–691.

[7] S. U. Hasan, M. Pal, P. Stănică, *Boomerang uniformity of a class of power maps,* Des. Codes Cryptogr. 89(11) (2021) 2627–2636.

[8] K. Li, C. Li, T. Helleseth, L. Qu, *Cryptographically strong permutations from the butterfly structure,* Des. Codes Cryptogr. 89(4) (2021) 737–761.

[9] K. Li, L. Qu, B. Sun, C. Li, *New results about the boomerang uniformity of permutation polynomials,* IEEE Trans. Inf. Theory 65(11) (2019) 7542–7553.

[10] N. Li, Z. Hu, M. Xiong, X. Zeng, 4*-uniform BCT permutations from generalized butterfly structure,* `https://arxiv.org/abs/2001.00464`.

[11] S. Mesnager, C. Tang, M. Xiong, *On the boomerang uniformity of quadratic permutations,* Des. Codes Cryptogr. 88(10) (2020) 2233–2246.

[12] Z. Tu, N. Li, X. Zeng, J. Zhou, *A class of quadrinomial permutations with boomerang uniformity four,* IEEE Trans. Inf. Theory 66(6) (2020) 3753–3765.

[13] D. Wagner, *The boomerang attack,* In: L. R. Knudsen (ed.) Fast Software Encryption-FSE 1999. LNCS 1636, Springer, Berlin, Heidelberg, pp. 156–170, (1999).

[14] Y. Wang, Q. Wang, W. Zhang, *Boomerang uniformity of normalized permutation polynomials of low degree,* Applicable Algebra Eng., Commun. Comput. 31(3-4) (2020) 307–322.