A Lower Bound for the Nonlinearity of Exponential Welch Costas Functions

Risto Hakala

A Lower Bound for the Nonlinearity of Exponential Welch Costas Functions

Risto M. Hakala

Department of Information and Computer Science,
Aalto University,
P.O. Box 15400, FI-00076 Aalto, Finland
risto.m.hakala@aalto.fi

Abstract. We study the nonlinearity of Exponential Welch Costas functions using the Fourier transform on $\mathbb{Z}_n$. Exponential Welch Costas functions are bijections from $\mathbb{Z}_{p-1}$ to $\mathbb{Z}_{p-1}$ defined using the exponential function of $\mathbb{Z}_p$, where p is an odd prime. Their linearity properties were recently studied by Drakakis, Requena, and McGuire, who conjectured that the absolute values of the Fourier coefficients of an Exponential Welch Costas function are bounded from above by $O(p^{0.5+\epsilon})$, where ϵ is a small constant. In this paper, we establish an upper bound of order $O(\sqrt{p}\log p)$, which is asymptotically strictly less than the bound conjectured by Drakakis et al.

Keywords: Nonlinearity, Welch Costas functions, exponential function, Fourier transform.

1 Introduction

Linear cryptanalysis [9, 8] is a prominent cryptanalytic method that exploits linearity properties of S-boxes in the cipher. Traditional linear cryptanalysis is intended for ciphers containing S-boxes that can be viewed as vector-valued Boolean functions. It relies on biased linear combinations between the input and output bits of these functions. Fourier analysis is commonly used in studying the resistance of a function to linear cryptanalysis. It allows us to determine the most biased linear combination for a function by finding the largest absolute value of the Fourier coefficients of the function. This quantity is called the linearity of the function and it indicates the maximum correlation between the function and affine functions. The nonlinearity of the function is defined as the minimum distance of a function to the set of affine functions: higher distance means higher nonlinearity and better resistance to linear cryptanalysis. Optimal resistance against linear cryptanalysis is achieved by bent functions [11], which have a flat Fourier spectrum.

A Fourier transform on binary vector spaces is utilized when linearity properties of Boolean functions are studied using Fourier analysis. Since non-Boolean functions are also used in symmetric ciphers, e.g., in SAFER [6, 7], linear cryptanalysis and the notion of nonlinearity have been extended to include these types

of functions as well. For example, Carlet and Ding [2] studied non-Boolean functions that have optimal nonlinearity; Baignères, Stern, and Vaudenay [1] studied how linear cryptanalysis can be used to analyze ciphers containing non-Boolean functions. The generalized notion of nonlinearity is defined using a Fourier transform on arbitrary finite groups, where the chosen groups depend on the definition of the studied function.

In this paper, we study the nonlinearity of Exponential Welch Costas (EWC) functions and their inverses, Logarithmic Welch Costas (LWC) functions. EWC and LWC functions are bijections from $\mathbb{Z}_{p-1}$ to $\mathbb{Z}_{p-1}$, where p is an odd prime, and they are used as S-boxes, e.g., in SAFER with $p = 257$. The nonlinearity of EWC and LWC functions has been previously studied by Drakakis, Requena, and McGuire [4] using the Fourier transform on $\mathbb{Z}_{p-1}$. Using a heuristic argument, they estimated that the absolute values of the Fourier coefficients of an EWC function are upper bounded by $O(p^{0.5+\epsilon})$, where ϵ is a small constant. We continue the research initiated by Drakakis et al. and derive an upper bound for the Fourier coefficients of an EWC function. The bound is of order $O(\sqrt{p}\log p)$, which improves the estimate given before.

Studying nonlinearities using Fourier analysis reduces into determining the maximum absolute value of the exponential sum defined by the Fourier transform. The exponential sum studied in this paper is closely related to the exponential sum introduced and studied by Mordell [10]. The main difference between these sums is that Mordell's sum is incomplete and taken over pth roots of unity, while the sum in this paper is complete and taken over $(p-1)$th roots of unity. Our analysis is also different, but contains analogical elements since the results depend on similar trigonometric sums.

The paper is organized as follows. In Sect. 2, we introduce the definitions needed in the paper and set up our notation. In Sect. 3, we derive an upper bound for the linearity of an Exponential Welch Costas function. We conclude the paper in Sect. 4.

2 Preliminaries

In this section, we introduce some necessary definitions and set up the notation. Let n and m be positive integers. We use $\mathbb{Z}_n$ to denote the ring of integers modulo n, p to denote an odd prime, and g to denote a generator of the multiplicative group $\mathbb{Z}_p^*$. We also denote $e(z) = \exp(2\pi i z)$ and $e_n(z) = e(z/n)$ for a real number z.

2.1 Welch Costas Permutations

We recall the definition of an Exponential Welch Costas function from [3]. We consider $\mathbb{Z}_{p-1}$ to be the set $\{0, 1, \ldots, p-2\}$ and $\mathbb{Z}_p^*$ to be the set $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$. Using this convention, we define $f\colon \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$ as

$$f(x) = (g^x \bmod p) - 1.$$

This function is called the Exponential Welch Costas function, and it defines a Costas permutation. Its inverse function $f^{-1}(x) = \log_g(x+1)$ is called the Logarithmic Welch Costas function.

2.2 Linearity and Nonlinearity

Nonlinearity is defined the same way as Drakakis et al. [4]. The Fourier transform of $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$ is defined by

$$\hat{f}(\alpha,\beta) = \sum_{x\in\mathbb{Z}_n} e_m(\beta f(x)) e_n(\alpha x) \quad \text{for } \alpha \in \mathbb{Z}_n \text{ and } \beta \in \mathbb{Z}_m.$$

Definition 1. *The linearity of $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$ is defined by*

$$\mathcal{L}(f) = \max_{\alpha\in\mathbb{Z}_n} \max_{\substack{\beta\in\mathbb{Z}_m \\ \beta\neq 0}} |\hat{f}(\alpha,\beta)|.$$

Definition 2. *The nonlinearity of $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$ is defined by*

$$\mathcal{NL}(f) = \frac{n - \mathcal{L}(f)}{m}.$$

It is not hard to show that a bijection and its inverse have the same nonlinearity [4, Theorem 2]. Also, the nonlinearity of an EWC function depends only on the prime p, not on the generator g of $\mathbb{Z}_p^*$ [4, Theorem 3]. It follows that all EWC and LWC functions over $\mathbb{Z}_{p-1}$ have the same nonlinearity.

3 Nonlinearity of Exponential Welch Costas Functions

In this section, we derive an upper bound for the linearity of an EWC function. The bound can be used to obtain a lower bound for the nonlinearity. Let p be an odd prime and $f\colon \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$ be an EWC function defined by

$$f(x) = (g^x \bmod p) - 1.$$

We obtain an upper bound for

$$|\hat{f}(\alpha,\beta)| = \left| \sum_{x=0}^{p-2} e_{p-1}(\beta f(x) + \alpha x) \right| \quad \text{for } \alpha,\beta \in \mathbb{Z}_{p-1} \text{ with } \beta \neq 0.$$

We split the sum into separate parts and obtain estimates for each individual part. These estimates are given in Lemmas 1 and 2 and then used in the proof of Theorem 1 to obtain a bound for the linearity of f. Lemma 1 was shown by Drakakis et al. [4] and used to approximate the average linearity of f, but we also present the proof here for completeness.

Lemma 1. *For any integers $\alpha \in \mathbb{Z}_{p-1}$ and $r \in \mathbb{Z}_p$ with $r \neq 0$, we have*

$$\left| \sum_{x=0}^{p-2} e_p(rf(x)) e_{p-1}(\alpha x) \right| \leq \sqrt{p}.$$

Proof. Denote

$$W = \sum_{x=0}^{p-2} e_p(rf(x)) e_{p-1}(\alpha x).$$

We get

$$\begin{aligned} |W|^2 &= \sum_{x,y=0}^{p-2} e_p(r(g^x - g^y)) e_{p-1}(\alpha(x-y)) \\ &= \sum_{z=0}^{p-2} e_{p-1}(\alpha z) \sum_{y=0}^{p-2} e_p(rg^y(g^z - 1)). \end{aligned}$$

Since

$$\sum_{y=0}^{p-2} e_p(rg^y(g^z - 1)) = \begin{cases} p-1 & \text{if } z = 0 \text{ or } r = 0, \\ -1 & \text{otherwise,} \end{cases}$$

we obtain

$$|W|^2 = \begin{cases} (p-1)^2 & \text{if } \alpha = r = 0, \\ 0 & \text{if } \alpha \neq 0,\ r = 0, \\ 1 & \text{if } \alpha = 0,\ r \neq 0, \\ p & \text{if } \alpha, r \neq 0, \end{cases}$$

and the result follows. □

We use the ideas presented in the proof of Lemma 8.80 in [5] to prove the following result.

Lemma 2. *For any integers $p \geq 3$ and $\beta \in \mathbb{Z}_{p-1}$ with $\beta \neq 0$, we have*

$$\sum_{r=0}^{p-1} \left| \sum_{y=0}^{p-2} e_{p-1}(\beta y) e_p(-ry) \right| < \frac{2}{\pi} p \ln p + 4p.$$

Proof. Denote

$$S(r) = \sum_{y=0}^{p-2} e_{p-1}(\beta y) e_p(-ry).$$

For an integer $r \in \mathbb{Z}_p$, we have

$$\begin{aligned} S(r) &= \sum_{y=0}^{p-2} e_{p-1}(\beta y) e_p(-ry) = \sum_{y=0}^{p-2} e\left(\frac{\beta y}{p-1} - \frac{ry}{p} \right) \\ &= \sum_{y=0}^{p-2} e\left(\left(\frac{\beta}{p-1} - \frac{r}{p} \right) y \right) = \frac{e(\varphi(r)(p-1)) - 1}{e(\varphi(r)) - 1}, \end{aligned}$$

where we denote

$$\varphi(r) = \frac{\beta}{p-1} - \frac{r}{p}.$$

Thus,

$$|S(r)| = \frac{|\sin \pi\varphi(r)(p-1)|}{|\sin \pi\varphi(r)|}.$$

Let R' denote the set $\{\beta-1, \beta, \beta+1, \beta+2\} \subseteq \mathbb{Z}_p$. We will find an upper bound for $\sum_{r=0}^{p-1}|S(r)|$ by comparing sums with integrals. For this purpose, we first find individual upper bounds for $|S(r)|$, $r \in R'$, since the divisor $|\sin \pi\varphi(r)|$ in $|S(r)|$ is close to zero when $r \in R'$. For $s \geq 6$, we have

$$\Big(\frac{\pi}{s}\Big)^{-1} \sin\Big(\frac{\pi}{s}\Big) \geq \Big(\frac{\pi}{6}\Big)^{-1} \sin\Big(\frac{\pi}{6}\Big), \quad \text{so} \quad \sin\Big(\frac{\pi}{s}\Big) \geq \frac{3}{s}.$$

It follows that

$$\frac{1}{|\sin \pi\varphi(r)|} = \frac{1}{\sin \pi|\varphi(r)|} \leq \frac{1}{3|\varphi(r)|} \tag{1}$$

holds if $|\varphi(r)| \leq 1/6$. Since $1 \leq \beta \leq p-2$, we have $|\varphi(r)| < 2/p$ for all $r \in R'$. Therefore, (1) holds for $p \geq 12$ and $r \in R'$. Since also $|\sin\theta| \leq |\theta|$ for all θ, we get

$$\begin{aligned} |S(r)| &= \frac{|\sin \pi\varphi(r)(p-1)|}{|\sin \pi\varphi(r)|} \leq \frac{|\pi\varphi(r)(p-1)|}{3|\varphi(r)|} \\ &= \frac{\pi}{3}(p-1) \quad \text{for } p \geq 12 \text{ and } r \in R'. \end{aligned} \tag{2}$$

We then estimate the remaining part of the sum. Suppose that $p \geq 5$ and let R denote the set $\mathbb{Z}_p \setminus R'$. Since $|\sin\theta| = |\sin(-\theta)| = |\sin(\pi-\theta)|$ for all θ, we obtain

$$\begin{aligned} \sum_{r\in R}|S(r)| &= \sum_{r=0}^{\beta-2}|S(r)| + \sum_{r=\beta+3}^{p-1}|S(r)| = \sum_{r=p}^{\beta+p-2}|S(r)| + \sum_{r=\beta+3}^{p-1}|S(r)| \\ &= \sum_{r=\beta+3}^{\beta+p-2}|S(r)| \leq \sum_{r=\beta+3}^{\beta+p-2}\frac{1}{|\sin \pi\varphi(r)|} = \sum_{r=\beta+3}^{\beta+p-2}|\csc \pi\varphi(r)| \\ &= \sum_{r=\beta+3}^{\beta+p-2}\csc\Big(\pi\Big(\frac{r}{p} - \frac{\beta}{p-1}\Big)\Big) \\ &\leq \int_{\beta+2}^{\beta+p-1}\csc\Big(\pi\Big(\frac{t}{p} - \frac{\beta}{p-1}\Big)\Big)\,dt. \end{aligned}$$

We denote $u = \pi(t/p - \beta/(p-1))$, so $t = pu/\pi + \beta p/(p-1)$ and $dt = (p/\pi)\,du$. Let

$$\begin{aligned} \theta_1 &= \pi\Big(\frac{\beta+2}{p} - \frac{\beta}{p-1}\Big) = \pi\Big(\frac{2p-2-\beta}{p(p-1)}\Big) \quad \text{and} \\ \theta_2 &= \pi\Big(\frac{\beta+p-1}{p} - \frac{\beta}{p-1}\Big) = \pi\Big(1 - \frac{p-1+\beta}{p(p-1)}\Big). \end{aligned}$$

Since $1 \le \beta \le p-2$, we have $\theta_1 \ge \pi/(p-1)$ and $\pi - \theta_2 \ge \pi/(p-1)$. Therefore,

$$\begin{aligned}\sum_{r\in R}|S(r)| &\le \frac{p}{\pi}\int_{\theta_1}^{\theta_2}\csc u\,du \le \frac{2p}{\pi}\int_{\pi/(p-1)}^{\pi/2}\csc u\,du\\ &= -\frac{2p}{\pi}\ln\tan\frac{\pi}{2(p-1)} = \frac{2p}{\pi}\ln\cot\frac{\pi}{2(p-1)}\\ &\le \frac{2p}{\pi}\ln\frac{2(p-1)}{\pi} = \frac{2p}{\pi}\ln\frac{2}{\pi} + \frac{2p}{\pi}\ln(p-1) \quad \text{for } p \ge 5. \end{aligned} \tag{3}$$

From (2) and (3), we get

$$\begin{aligned}\sum_{r=0}^{p-1}|S(r)| &\le \frac{4\pi}{3}(p-1) + \frac{2p}{\pi}\ln\frac{2}{\pi} + \frac{2p}{\pi}\ln(p-1)\\ &= \left(\frac{4\pi}{3} + \frac{2}{\pi}\ln\frac{2}{\pi}\right)p + \frac{2p}{\pi}\ln(p-1) - \frac{4\pi}{3}\\ &< \frac{2}{\pi}p\ln p + 4p \quad \text{for } p \ge 12.\end{aligned}$$

This inequality can be quickly checked for $3 \le p \le 11$, so the result follows. □

Theorem 1. *Let f be an EWC function and p be an odd prime. Then*

$$\mathcal{L}(f) < \frac{2}{\pi}\sqrt{p}\ln p + 4\sqrt{p}.$$

Proof. Let $\alpha, \beta \in \mathbb{Z}_{p-1}$ be integers with $\beta \ne 0$. We have

$$\hat{f}(\alpha,\beta) = \sum_{x=0}^{p-2} e_{p-1}(\beta f(x) + \alpha x) = \sum_{x=0}^{p-2} e_{p-1}(\beta f(x))e_{p-1}(\alpha x).$$

For integers z, y, and n with $n \ge 2$, we have

$$\sum_{r=0}^{n-1} e_n(r(z-y)) = \begin{cases} n & \text{if } y \equiv z \bmod n,\\ 0 & \text{if } y \not\equiv z \bmod n,\end{cases}$$

so

$$\begin{aligned}e_{p-1}(\beta f(x)) &= \frac{1}{p}\sum_{y=0}^{p-2} e_{p-1}(\beta y)\sum_{r=0}^{p-1} e_p(r(f(x)-y))\\ &= \frac{1}{p}\sum_{r=0}^{p-1}\sum_{y=0}^{p-2} e_{p-1}(\beta y)e_p(rf(x))e_p(-ry).\end{aligned}$$

The value $r = 0$ can be omitted from the sum above since $\sum_{y=0}^{p-2} e_{p-1}(\beta y) = 0$. By Lemmas 1 and 2, we obtain

$$\begin{aligned}
|\hat{f}(\alpha,\beta)| &= \left| \sum_{x=0}^{p-2} \frac{1}{p} \sum_{r=1}^{p-1} \sum_{y=0}^{p-2} e_{p-1}(\beta y) e_p(rf(x)) e_p(-ry) e_{p-1}(\alpha x) \right| \\
&\leq \frac{1}{p} \sum_{r=1}^{p-1} \left| \sum_{y=0}^{p-2} e_{p-1}(\beta y) e_p(-ry) \right| \left| \sum_{x=0}^{p-2} e_p(rf(x)) e_{p-1}(\alpha x) \right| \\
&< \frac{2}{\pi} \sqrt{p} \ln p + 4\sqrt{p}.
\end{aligned}$$

□

4 Conclusion

We derived an upper bound of order $O(\sqrt{p} \log p)$ for the linearity of an Exponential Welch Costas function. For reasonable values of p, the bound is not very tight as is easily shown by experiments. However, the bound shows that the nonlinearity of an Exponential Welch Costas function is asymptotically better than conjectured by Drakakis et al. [4]. These results apply for Logarithmic Welch Costas functions as well.

Acknowledgements. The author would like to thank Gary McGuire for bringing [4] to his attention and Kaisa Nyberg for helpful suggestions. The research work has been supported by Helsinki Graduate School in Computer Science and Engineering, Academy of Finland (project #122736), Nokia Foundation, and KAUTE Foundation.

References

1. Baignères, T., Stern, J., Vaudenay, S.: Linear cryptanalysis of non binary ciphers. In: SAC 2007. LNCS, vol. 4876, pp. 184–211. Springer (2007)
2. Carlet, C., Ding, C.: Highly nonlinear mappings. Journal of Complexity 20(2–3), 205–244 (2004)
3. Drakakis, K., Gow, R., McGuire, G.: APN permutations on $\mathbb{Z}_n$ and Costas arrays. Discrete Applied Mathematics 157(15), 3320–3326 (2009)
4. Drakakis, K., Requena, V., McGuire, G.: On the nonlinearity of Exponential Welch Costas functions. IEEE Transactions on Information Theory 56(3), 1230–1238 (2010)
5. Lidl, R., Niederreiter, H.: Finite fields, Cambridge University Press, vol. 20. Encyclopedia of mathematics and its applications, 2nd edn. (1997)
6. Massey, J.L.: SAFER K-64: A byte-oriented block-ciphering algorithm. In: FSE 1993. LNCS, vol. 809, pp. 1–17. Springer (1994)
7. Massey, J.L.: SAFER K-64: One year later. In: FSE 1994. LNCS, vol. 1008, pp. 212–241. Springer (1995)

8. Matsui, M.: Linear cryptanalysis method for DES cipher. In: EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer (1994)
9. Matsui, M., Yamagishi, A.: A new method for known plaintext attack of FEAL cipher. In: EUROCRYPT 1992. LNCS, vol. 658, pp. 81–91. Springer (1993)
10. Mordell, L.J.: On the exponential sum $\sum_{x=1}^{X} \exp(2\pi i(ax + bg^x)/p)$. Mathematika 19(1), 84–87 (1972)
11. Rothaus, O.S.: On "bent" functions. Journal of Combinatorial Theory, Series A 20(3), 300–305 (1976)