On Cryptographic Properties of a Class of Power Permutations in Odd Characteristic

Mohit Pal

University of Bergen

mohit.pal@uib.no

April 15, 2024

Table of contents

Notations and definitions

- We denote, by $\mathbb{F}_q$, the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer.

Notations and definitions

- We denote, by $\mathbb{F}_q$, the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer.
- By $\mathbb{F}_q^* = \langle g \rangle$, we denote the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$, where g is a primitive element of $\mathbb{F}_q$.

Notations and definitions

- We denote, by $\mathbb{F}_q$, the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer.
- By $\mathbb{F}_q^* = \langle g \rangle$, we denote the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$, where g is a primitive element of $\mathbb{F}_q$.
- Let f be a function form the finite field $\mathbb{F}_q$ to itself then f can be uniquely represented as a univariate polynomial over $\mathbb{F}_q$ of the form $f(X) = \sum_{i=0}^{q-1} a_i X^i$, $a_i \in \mathbb{F}_q$.

Notations and definitions

- We denote, by $\mathbb{F}_q$, the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer.
- By $\mathbb{F}_q^* = \langle g \rangle$, we denote the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$, where g is a primitive element of $\mathbb{F}_q$.
- Let f be a function form the finite field $\mathbb{F}_q$ to itself then f can be uniquely represented as a univariate polynomial over $\mathbb{F}_q$ of the form
$$f(X) = \sum_{i=0}^{q-1} a_i X^i,\ a_i \in \mathbb{F}_q.$$
- We call a polynomial $f \in \mathbb{F}_q[X]$, a permutation polynomial (PP) over $\mathbb{F}_q$ if the associated mapping $x \mapsto f(x)$ is a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$.

Differential uniformity

- One of the most important developments in block cipher cryptanalysis was the invention of differential cryptanalysis by Biham and Shamir.

Differential uniformity

- One of the most important developments in block cipher cryptanalysis was the invention of differential cryptanalysis by Biham and Shamir.
- A function f is called differentially δ-uniform if for every $a \in \mathbb{F}_q^*$ and every $b \in \mathbb{F}_q$, the equation $f(X + a) - f(X) = b$ admits at most δ solutions.

Differential uniformity

- One of the most important developments in block cipher cryptanalysis was the invention of differential cryptanalysis by Biham and Shamir.
- A function f is called differentially δ-uniform if for every $a \in \mathbb{F}_q^*$ and every $b \in \mathbb{F}_q$, the equation $f(X+a) - f(X) = b$ admits at most δ solutions.
- When $\delta = 1$, we say that the function f is perfect nonlinear (PN) function.

Differential uniformity

- One of the most important developments in block cipher cryptanalysis was the invention of differential cryptanalysis by Biham and Shamir.
- A function f is called differentially δ-uniform if for every $a \in \mathbb{F}_q^*$ and every $b \in \mathbb{F}_q$, the equation $f(X + a) - f(X) = b$ admits at most δ solutions.
- When $\delta = 1$, we say that the function f is perfect nonlinear (PN) function.
- When $\delta = 2$, we say that the function f is almost perfect nonlinear (APN) function.

Boomerang Attacks

- The boomerang attacks were introduced by David Wagner in 1999.

Boomerang Attacks

- The boomerang attacks were introduced by David Wagner in 1999.
- We assume that the cipher E can be decomposed into two parts E_0 and E_1 such that $E = E_1 \circ E_0$ as shown in the figure below

Boomerang Attacks

- The boomerang attacks were introduced by David Wagner in 1999.
- We assume that the cipher E can be decomposed into two parts E_0 and E_1 such that $E = E_1 \circ E_0$ as shown in the figure below

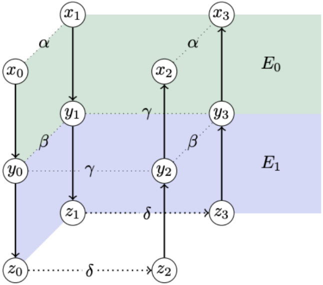


Figure: Basic Boomerang Attack

Boomerang Attacks

- A good differential $\alpha \xrightarrow{E_0} \beta$ over E_0 that holds with probability p.

Boomerang Attacks

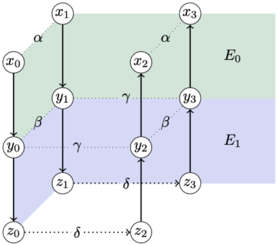
- A good differential $\alpha \xrightarrow{E_0} \beta$ over E_0 that holds with probability p.
- A good differential $\gamma \xrightarrow{E_1} \beta$ over E_1 that holds with probability q.

Boomerang Attacks

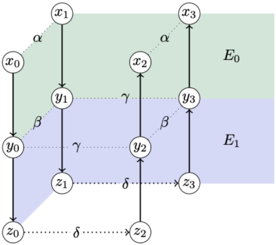
- A good differential $\alpha \xrightarrow{E_0} \beta$ over E_0 that holds with probability p.
- A good differential $\gamma \xrightarrow{E_1} \beta$ over E_1 that holds with probability q.
- These two differentials can now be used to construct a distinguisher over the whole cipher.

Boomerang Attacks

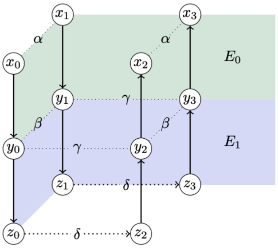
- A good differential $\alpha \xrightarrow{E_0} \beta$ over E_0 that holds with probability p.
- A good differential $\gamma \xrightarrow{E_1} \beta$ over E_1 that holds with probability q.
- These two differentials can now be used to construct a distinguisher over the whole cipher.
- We start with a pair of plaintexts x_0 and x_1 with a difference α.
- When encrypting these two plaintexts, we expect the corresponding intermediate texts $y_0 := E_0(x_0)$ and $y_1 := E_0(x_1)$ to have a difference β with probability p.



- With $z_0 := E_1(y_0)$ and $z_1 := E_1(y_1)$ being the respective ciphertexts, we now construct two more ciphertexts $z_2 := z_0 + \delta$ and $z_3 := z_1 + \delta$ by adding the difference δ to each of z_0 and z_1.
- Then the pairs (z_0, z_2) and (z_1, z_3) both have a difference of δ, the ciphertext difference in the second differential.
- Decrypting these two ciphertexts, provides us with two more intermediate texts, $y_2 := E_1^{-1}(z_2)$ and $y_3 := E_1^{-1}(z_3)$ and two more plaintexts, $x_2 := E_0^{-1}(y_2)$ and $x_3 := E_0^{-1}(y_3)$.
- Assuming independence of the two ciphertext pairs (z_0, z_2) and (z_1, z_3), both of their respective intermediate pairs (y_0, y_2) and (y_1, y_3) will have a differences of γ with probability q^2.



- Combining this with the probability that (x_0, x_1) follows the first differential, we have with probability pq^2 that $y_0 + y_1 = \beta$, $y_0 + y_2 = \gamma$ and $y_1 + y_3 = \gamma$.
- This forces the difference between y_2 and y_3 to be β.
- Again assuming independence from the other pairs, the pair (y_2, y_3) will follow the first differential with probability p, resulting in a plaintext difference of α between x_2 and x_3.
- Taking all of these steps together, we estimate that the probability to see a difference α between x_2 and x_3 is equal to p^2q^2.



Boomerang Uniformity

- To simplify this analysis, in 2018, Cid et al. introduced the notion of boomerang connectivity table (BCT)

Boomerang Uniformity

- To simplify this analysis, in 2018, Cid et al. introduced the notion of boomerang connectivity table (BCT)
- In this paper the BCT entries were defined for permutation functions in even characteristic and the knowledge of the inverse of the permutation was required to compute the BCT entries

Boomerang Uniformity

- To simplify this analysis, in 2018, Cid et al. introduced the notion of boomerang connectivity table (BCT)
- In this paper the BCT entries were defined for permutation functions in even characteristic and the knowledge of the inverse of the permutation was required to compute the BCT entries
- In 2019, Li et al. gave an equivalent technique to compute BCT, which does not require the compositional inverse of the permutation polynomial $f(X)$ at all

Boomerang Uniformity

- For any $a, b \in \mathbb{F}_q$, the BCT entry of the function f at point (a, b), denoted by $\mathcal{B}_f(a, b)$, is the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of the following system of equations

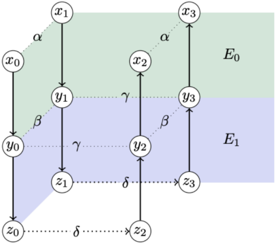
$$\begin{cases} f(X) - f(Y) = b, \\ f(X + a) - f(Y + a) = b. \end{cases}$$

Boomerang Uniformity

- For any $a, b \in \mathbb{F}_q$, the BCT entry of the function f at point (a, b), denoted by $\mathcal{B}_f(a, b)$, is the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of the following system of equations

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

- The boomerang uniformity of the function f, denoted by $\mathcal{B}_f$, is then defined as the maximum of $\mathcal{B}_f(a, b)$, where $a, b \in \mathbb{F}_q^*$.



- Cid et al. showed that for permutation functions f, the boomerang uniformity is greater than or equal to the differential uniformity

- Cid et al. showed that for permutation functions f, the boomerang uniformity is greater than or equal to the differential uniformity
- However, perhaps, due to lack of any explicit example in the case of non-permutations, in several follow up papers the term “permutation” was not emphasized and it has been stated that for any function f, the differential uniformity is less than the boomerang uniformity

- Cid et al. showed that for permutation functions f, the boomerang uniformity is greater than or equal to the differential uniformity
- However, perhaps, due to lack of any explicit example in the case of non-permutations, in several follow up papers the term “permutation” was not emphasized and it has been stated that for any function f, the differential uniformity is less than the boomerang uniformity
- In 2021, Hasan et al. showed that for non-permutations, the differential uniformity is not necessarily smaller than the boomerang uniformity

Monomials with known boomerang uniformity in odd characteristic

	p	d	Condition	$\mathcal{B}_f$	Is PP?
C_1	3	$\frac{p^n+3}{2}$	n odd	3	Yes
C_2	$p > 2$	$p^m - 1$	$n = 2m, p \not\equiv 2 \pmod 3$	2	No
C_3	$p > 2$	$\frac{(p^m+3)(p^m-1)}{2}$	$n = 2m$	2	No
C_4	$p > 2$	$\frac{p^n-3}{2}$	$p^n \equiv 3 \pmod 4$	≤ 6	No
C_5	$p > 2$	$p^n - 2$	any n	≤ 5	Yes
C_6	$p > 2$	$k(p^m - 1)$	$n = 2m, \ \gcd(k, p^m + 1) = 1$	2	No

Table: Monomials X^d over $\mathbb{F}_{p^n}$ with known boomerang uniformity.

Our Contribution

- We consider the class of power maps $f(X) = X^{\frac{p^n+3}{2}} \in \mathbb{F}_{p^n}[X]$

Our Contribution

- We consider the class of power maps $f(X) = X^{\frac{p^n+3}{2}} \in \mathbb{F}_{p^n}[X]$
- Helleseth and Sandberg considered the differential uniformity of this class of power maps and showed that its differential uniformity Δ_f is given by

$$\Delta_f \leq \begin{cases} 1 & \text{if } p = 3 \text{ and } n \text{ is even}, \\ 3 & \text{if } p \neq 3 \text{ and } p^n \equiv 1 \pmod 4, \\ 4 & \text{otherwise.} \end{cases}$$

Our Contribution

- We consider the class of power maps $f(X) = X^{\frac{p^n+3}{2}} \in \mathbb{F}_{p^n}[X]$
- Helleseth and Sandberg considered the differential uniformity of this class of power maps and showed that its differential uniformity Δ_f is given by

$$\Delta_f \leq \begin{cases} 1 & \text{if } p = 3 \text{ and } n \text{ is even}, \\ 3 & \text{if } p \neq 3 \text{ and } p^n \equiv 1 \pmod 4, \\ 4 & \text{otherwise.} \end{cases}$$

- It is easy to see that when $p^n \equiv 3 \pmod 4$ then f is a permutation.

Our Contribution

- We consider the class of power maps $f(X) = X^{\frac{p^n+3}{2}} \in \mathbb{F}_{p^n}[X]$
- Helleseth and Sandberg considered the differential uniformity of this class of power maps and showed that its differential uniformity Δ_f is given by

$$\Delta_f \leq \begin{cases} 1 & \text{if } p = 3 \text{ and } n \text{ is even,} \\ 3 & \text{if } p \neq 3 \text{ and } p^n \equiv 1 \pmod{4}, \\ 4 & \text{otherwise.} \end{cases}$$

- It is easy to see that when $p^n \equiv 3 \pmod{4}$ then f is a permutation.
- We considered the boomerang uniformity of the power permutation $X^{\frac{p^n+3}{2}}$, where $p^n \equiv 3 \pmod{4}$ for all $p > 3$ and showed that the boomerang uniformity is ≤ 23

Our Contribution

- Moreover, we also obtained the compositional inverse of this power permutation

Theorem

Let $q \equiv 3 \pmod 4$ then the compositional inverse of the power permutation $f(X) = X^{\frac{q+3}{2}}$ is given by

$$f^{-1}(X) = \begin{cases} X^{\frac{q+1}{4}} & \text{if } p \equiv 3 \pmod 8, \\ X^{\frac{3q-1}{4}} & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Our Contribution

- We also determined the algebraic degree of the compositional inverse

Theorem

Let $p \equiv 3 \pmod 4$ *and* $n = 2m+1$ *for some non-negative integer* m *then the algebraic degree of the inverse of the power permutation* $f(X) = X^{\frac{p^n+3}{2}}$ *is*

$$\begin{cases} \frac{(4m+1)p-4m+1}{4} & \text{if } p \equiv 3 \pmod 8, \\ \frac{(4m+3)p-4m-1}{4} & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Future Directions

References

- Boura, C., Canteaut, A.: On the boomerang uniformity of cryptographic S-boxes. IACR Trans. Symmetric Cryptol. 3, 290–310 (2018).
- Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: a new cryptanalysis tool. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, LNCS, vol. 10821, pp. 683–714. Springer, Cham (2018).
- Hasan, S.U., Pal, M., Stănică, P.: Boomerang uniformity of a class of power maps. Des. Codes Cryptogr. 89, 2627–2636 (2021).
- Li, K., Qu, L., Sun, B., Li, C.: New results about the boomerang uniformity of permutation polynomials. IEEE Trans. Inform. Theory **65**(11), 7542–7553 (2019).
- Wagner, D.: The boomerang attack. In: Knudsen, L.R. (ed.) FSE 1999, LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999).

Thank you for your attention!