# Differentially low uniform permutations from the Gold and the Bracken-Leander functions


Marco Calderini

Department of Informatics, University of Bergen, Norway



**Abstract**

Functions with low differential uniformity can be used in block ciphers as S-boxes since they have good resistance to differential attacks. In this extended abstract, we give two constructions of differentially 6-uniform permutations over $\mathbb{F}_{2^{2m}}$ by modifying the Gold function and the Bracken-Leander function on a subfield.


## 1 Introduction

Let $n$ be a positive integer, we will denote by $\mathbb{F}_{2^n}$ the finite field with $2^n$ elements and its multiplicative group by $\mathbb{F}_{2^n}^\star$. Permutation maps defined over $\mathbb{F}_{2^n}$ are used as S-boxes of some symmetric cryptosystems. So, it is important to construct permutations with good cryptographic properties in order to design a cipher that can resist to the known attacks. In particular, among these properties we have a low differential uniformity for preventing differential attacks [1], high nonlinearity for avoiding linear cryptanalysis [6] and also high algebraic degree to resist to higher order differential attacks [5].

The best differential uniformity of a function $F$ defined over $\mathbb{F}_{2^n}$ is 2. Functions achieving this value are called almost perfect nonlinear (APN). For odd values of $n$ there are known families of APN permutations; while for $n$ even there exists only one example of APN permutation over $\mathbb{F}_{2^6}$ [2] and the existence of more ones remains an open problem. For ease of implementation, usually, the integer $n$ is required to be even in a cryptosystem. Therefore, finding permutations with good cryptographic properties over $\mathbb{F}_{2^n}$ with $n$ even is an interesting research topic for providing more choices for the S-boxes.

The construction of low differentially uniform permutations with the highest nonlinearity over $\mathbb{F}_{2^n}$ (with $n$ even) is a difficult task. In Table 1 we give 5 families of primarily constructed differentially 4-uniform permutations with the best known nonlinearity.

In the last years, many constructions of differentially 4-uniform permutations have been found by modifying the inverse function on some subsets of $\mathbb{F}_{2^n}$ (see for instance [7, 8, 9, 10, 11]). In particular, in [7, 10, 11] the authors change the inverse function on some subfields of $\mathbb{F}_{2^n}$.

Table 1: Primarily-constructed differentially 4-uniform over $\mathbb{F}_{2^n}$

| **Name** | **F(x)** | **deg** | **Conditions** |
|---|---|---|---|
| Gold | $x^{2^i+1}$ | 2 | $n=2k$, $k$ odd $\gcd(i,n)=2$ |
| Kasami | $x^{2^{2i}-2^i+1}$ | i+1 | $n=2k$, $k$ odd $\gcd(i,n)=2$ |
| Inverse | $x^{2^n-2}$ | $n-1$ | $n=2k$, $k\geq 1$ |
| Bracken-Leander | $x^{2^{2k}+2^k+1}$ | 3 | $n=4k$, $k$ odd |
| Bracken-Tan-Tan | $\zeta x^{2^i+1}+\zeta^{2^m}x^{2^{-m}+2^{m+i}}$ | 2 | $n=3m$, $m$ even, $m/2$ odd, $\gcd(n,i)=2$, $3\|m+i$ and $\zeta$ is a primitive element of $\mathbb{F}_{2^n}$ |

In this abstract, we investigate the piecewise construction as in [7, 10, 11] by modifying the image of the Gold and Bracken-Leander function on some subfields of $\mathbb{F}_{2^n}$. We show that in these cases it is possible to obtain permutations with differential uniformity at most 6. Moreover, if we modify these functions using the inverse function (or a function equivalent to it), then we can obtain permutations with algebraic degree $n-1$ (which is the highest possible) and high nonlinearity. These results extend those given in [12], where the authors modified the 4-uniform Gold function for constructing differentially 6-uniform permutations.

## 2 Preliminaries

Any function $F$ from $\mathbb{F}_{2^n}$ to itself can be represented as a univariate polynomial of degree at most $2^n-1$, that is

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i.$$

The *2-weight* of an integer $0 \le i \le 2^n-1$, denoted by $w_2(i)$, is the (Hamming) weight of its binary representation. The algebraic degree of a function $F$ is given by $\deg(F) = \max\{w_2(i) \mid a_i \neq 0\}$. Functions of algebraic degree 1 are called *affine*. Linear functions are affine functions with constant term equal to zero and they can be represented as $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$. For any permutation $F$ it is well known that $\deg(F) \le n-1$.

For any $m \ge 1$ such that $m|n$ we can define the (linear) *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ by $\mathrm{Tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}$. When $m=1$ we will denote $\mathrm{Tr}_1^n(x)$ by Tr.

For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we denote the *Walsh transform* in $a, b \in \mathbb{F}_{2^n}$ by

$$\mathcal{W}_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax+bF(x))}.$$

The *nonlinearity* of a vectorial Boolean function $F$ is given by

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^\star} |\mathcal{W}_F(a,b)|.$$

When $n$ is odd, it has been proved that $\mathcal{NL}(F) \le 2^{n-1} - 2^{\frac{n-1}{2}}$; for $n$ even, the best known nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$, and it is conjectured that $\mathcal{NL}(F) \le 2^{n-1} - 2^{\frac{n}{2}}$.

**Definition 2.1** *For a function $F$ from $\mathbb{F}_{2^n}$ to itself, and any $a \in \mathbb{F}_{2^n}^\star$ and $b \in \mathbb{F}_{2^n}$, we denote by $\delta_F(a,b)$ the number of solutions of the equation $F(x+a)+F(x) = b$. The maximum value $\delta$ among the $\delta_F(a,b)$'s is called the differential uniformity of $F$, and $F$ is said to be differentially $\delta$-uniform.*

There are several equivalence relations of functions for which the differential uniformity and the nonlinearity are preserved. Two functions F and $F'$ from $\mathbb{F}_{2^n}$ to itself are called:

- *affine equivalent* if $F' = A_1 \circ F \circ A_2$ where the mappings $A_1, A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine permutations;
- *extended affine equivalent* (EA-equivalent) if $F' = F'' + A$, where the mappings $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is affine and $F''$ is affine equivalent to $F$;
- *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ the image of the graph of $F$ is the graph of $F'$, that is, $\mathcal{L}(G_F) = G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$.

Obviously, affine equivalence is included in the EA-equivalence, and it is also well known that EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse [4]. The algebraic degree is invariant for the affine equivalence and also for the EA-equivalence for nonlinear functions, but not for the CCZ-equivalence (and inverse transformation).

## 3 Constructing differentially 6-uniform permutations

In this section we will study the piecewise construction for the case of Gold and the Bracken-Leander function. We refer to the full version of the paper [3] for more details on the proofs of the results given in this section.

The following lemma give a characterisation for the solutions of $(x+1)^{2^k+1} + x^{2^k+1} = b$, when $b$ belongs to some specific subfield $\mathbb{F}_{2^s}$ of $\mathbb{F}_{2^n}$.

**Lemma 3.1** *Let $n = sm$ with $s$ even and $m$ odd. Let $k$ be such that $\gcd(k,n) = 2$. For any $b \in \mathbb{F}_{2^s}$ the equation*

$$x^{2^k} + x = b$$

*does not admit any solution $x$ in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$.*

**Proof:** See [3]. □

**Theorem 3.2** *Let $n = sm$ with $s$ even such that $s/2$ is odd and $m$ odd. Let $k$ be such that $\gcd(k,n) = 2$ and $f$ be at most differentially 6-uniform permutation over $\mathbb{F}_{2^s}$. Then*

$$F(x) = f(x) + (f(x) + x^{2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

*is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$.*

**Proof:** Using the Lemma 3.1 it is possible to analyse the solutions of the equation

$$F(x) + F(x+a) = b,$$

distinguishing the cases where: both $x$ and $x+a$ are in $\mathbb{F}_{2^s}$; one is in $\mathbb{F}_{2^s}$ and the other not; none is contained in $\mathbb{F}_{2^s}$. See [3] for a detailed proof. □

Also for the Bracken-Leander function we can characterize the solutions of the equation $(x+1)^{2^{2k}+2^k+1} + x^{2^{2k}+2^k+1} = b$, when $b$ is in some specific subfield.

**Lemma 3.3** *Let $n = 4k = sm$ with $k$ and $m$ odd. For any $b \in \mathbb{F}_{2^s}$ the equation*

$$x^{2^{2k}+2^k} + x^{2^{2k}+1} + x^{2^k+1} + x^{2^{2k}} + x^{2^k} + x = b \tag{1}$$

*does not admit any solution $x$ in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$.*

**Proof:** See [3]. □

Similarly to Theorem 3.2 we obtain:

**Theorem 3.4** *Let $n = 4k = sm$, with $k$, $m$ odd and $s$ even. Let $f$ be at most differentially 6-uniform permutation over $\mathbb{F}_{2^s}$. Then*

$$F(x) = f(x) + (f(x) + x^{2^{2k}+2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^{2k}+2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

*is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$.*

From Theorem 3.2 and Theorem 3.2 we obtain a general construction for functions with differential uniformity at most 6. In the following, we will show that using a function $f$ equivalent to the inverse function we can obtain a permutation of degree $n-1$ with high nonlinearity.

We, first, give the following result, which is a necessary and sufficient condition for a permutation to have maximal degree.

**Lemma 3.5** *Let $F$ be a function defined over $\mathbb{F}_{2^n}$. Then, $F$ in its polynomial representation has a term of algebraic degree $n-1$ if and only if there exists a linear monomial $x^{2^j}$ such that $\sum_{x \in \mathbb{F}_{2^n}} F(x)x^{2^j} \neq 0$. In particular, if $F$ is a permutation then $\deg(F) = n-1$.*

**Proof:** See [3]. $\square$

**Corollary 3.6** *Let $n = sm$ with $s$ even such that $s/2$ is odd and $m$. Let $k$ be such that* $\gcd(k, n) = 2$ *and $f(x) = A_1 \circ Inv \circ A_2(x)$, where $Inv(x) = x^{-1}$ and $A_1, A_2$ are affine permutations over $\mathbb{F}_{2^s}$. Then*

$$F(x) = f(x) + (f(x) + x^{2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

*is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$. Moreover, if $s > 2$ then the algebraic degree of $F$ is $n-1$.*

**Proof:** We need to prove only that the degree of $F$ is $n-1$. From Lemma 3.5, since $\deg(f(x)) = s-1$ there exists $h(x) = x^{2^j}$ in $\mathbb{F}_{2^s}[x]$ (with $j \leq s-1$) such that $\sum_{x \in \mathbb{F}_{2^s}} f(x)h(x) \neq 0$.

Thus, since $\deg(x^{2^k+1}) = 2 < s-1$ we obtain

$$\sum_{x \in \mathbb{F}_{2^n}} F(x)h(x) = \sum_{x \in \mathbb{F}_{2^s}} f(x)h(x) + \sum_{x \in \mathbb{F}_{2^n}} x^{2^k+1}h(x) + \sum_{x \in \mathbb{F}_{2^s}} x^{2^k+1}h(x) = \sum_{x \in \mathbb{F}_{2^s}} f(x)h(x) \neq 0.$$

Then, $\deg(F) = n-1$ since $F$ is a permutation. $\square$

Similarly we have the following construction using the Bracken-Leander function.

**Corollary 3.7** *Let $n = 4k = sm$ with $k$, $m$ odd and $s$ even. Let $f(x) = A_1 \circ Inv \circ A_2(x)$, where $Inv(x) = x^{-1}$ and $A_1, A_2$ are affine permutations over $\mathbb{F}_{2^s}$. Then*

$$F(x) = f(x) + (f(x) + x^{2^{2k}+2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^{2k}+2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

*is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$. Moreover, if $s > 4$ then* $\deg(F) = n-1$.

**Remark 3.8** *When $s = 2$ and $G(x) = x^{2^k+1}$ or $s = 4$ and $G(x) = x^{2^{2k}+2^k+1}$ we have* $\deg(G) = s-1$. *Thus, we could obtain a permutation of degree less than $n-1$ in Corollary 3.6 and Corollary 3.7.*

For the nonlinearity of the constructed functions we have the following.

**Proposition 3.9** *The nonlinearity of the functions in Corollary 3.6 and Corollary 3.7 is at least $2^{n-1} - 2^{\frac{n}{2}} - 2^{\frac{s}{2}+1}$.*

**Proof:** See [3]. $\square$

It is well known that the algebraic degree is not preserved by the CCZ-equivalence and in particular by the inverse transformation. However, for any permutation of maximal algebraic degree we have the following easy observation.

**Proposition 3.10** *Let $F$ be a permutation defined over $\mathbb{F}_{2^n}$. Then,* $\deg(F) = n-1$ *if and only if* $\deg(F^{-1}) = n-1$.

**Proof:** Suppose $\deg(F) = n-1$ and let $h(x)$ a linear monomial for which we have $\sum_{x \in \mathbb{F}_{2^n}} F(x)h(x) \neq 0$. Since $F$ is a permutation we obtain $\sum_{x \in \mathbb{F}_{2^n}} F(x)h(x) = \sum_{x \in \mathbb{F}_{2^n}} xh(F^{-1}(x))$, which implies $\deg(h \circ F^{-1}) = n-1$. Since $h$ is linear we have that $\deg(F^{-1}) = n-1$. $\square$

From this result we have that also the compositional inverses of the functions given in Corollary 3.6 and Corollary 3.7 are differentially 6-uniform functions with high nonlinearity and algebraic degree $n-1$.

Denoting by $\omega = \zeta^{\frac{2^n-1}{3}}$ the primitive element of $\mathbb{F}_4$, in Table 2 and Table 3 we give the CCZ-inequivalent functions that can be obtained by Corollary 3.6 for $n = 6, 10$ considering $f(x) = A \circ Inv$.

Table 2: CCZ-inequivalent permutations from Corollary 3.6 over $\mathbb{F}_{2^6}$

| $A(x)$ | deg | $\mathcal{N}\ell(G)$ | Bound on $\mathcal{N}\ell$ | $\delta$ |
|---|---|---|---|---|
| $x$ | 2 | 24 | 20 | 4 |
| $x+\omega$ | 4 | 20 | 20 | 6 |
| $\omega x^2+\omega$ | 5 | 20 | 20 | 6 |
| $\omega x$ | 5 | 22 | 20 | 6 |
| $\omega^2 x^2+\omega$ | 5 | 22 | 20 | 6 |

Table 3: CCZ-inequivalent permutations from Corollary 3.6 over $\mathbb{F}_{2^{10}}$

| $A(x)$ | deg | $\mathcal{N}\ell(G)$ | Bound on $\mathcal{N}\ell$ | $\delta$ |
|---|---|---|---|---|
| $x$ | 2 | 480 | 476 | 4 |
| $x+\omega$ | 8 | 476 | 476 | 6 |
| $\omega x^2+\omega$ | 9 | 476 | 476 | 6 |
| $\omega x$ | 9 | 478 | 476 | 6 |
| $\omega^2 x^2+\omega$ | 9 | 478 | 476 | 6 |

In Table 4 we report some permutations constructed from Corollary 3.7 for $n = 12$ (in this case $s = 4$ and $m = 3$). As before, we consider $f(x) = A \circ Inv$ with $A$ affine permutations defined over $\mathbb{F}_4[x]$ (for $A(x) = x^2$ we obtain the Bracken-Leander function).

Table 4: CCZ-inequivalent permutations from Corollary 3.7 over $\mathbb{F}_{2^{12}}$

| $A(x)$ | deg | $\mathcal{N}\ell(G)$ | Bound on $\mathcal{N}\ell$ | $\delta$ |
|---|---|---|---|---|
| $x^2$ | 3 | 1984 | 1976 | 4 |
| $x^2+1$ | 8 | 1976 | 1976 | 6 |
| $\omega^2 x^2+\omega$ | 11 | 1976 | 1976 | 6 |
| $x+\omega$ | 11 | 1978 | 1976 | 6 |
| $\omega x^2$ | 11 | 1980 | 1976 | 6 |

# References


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

[2] K. A. Browning, J. F. Dillon, M. T. McQuistan, A. J. Wolfe, *An APN permutation in dimension six.* In: Contemporary Mathematics, Vol. 518, Am. Math Soc., pp. 33–42 (2010).

[3] M. Calderini, *Differentially low uniform permutations from known 4-uniform functions.* arXiv preprint arXiv:1910.14337 (2019).

[4] C. Carlet, P. Charpin, V. Zinoviev, *Bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. **15**, 125–156 (1998).

[5] L. Knudsen, *Truncated and higher order differentials.* FSE 1994, Lecture Notes in Computer Sciences, vol. 1008, 196–211 (1995).

[6] L. Matsui, *Linear cryptanalysis method for DES cipher.* Advances in Cryptology EUROCRYPT93, Lecture Notes in Computer Science, vol. 765, Springer, Berlin Heidelberg, 386–397 (1994).

[7] J. Peng, C. H. Tan, *New differentially 4-uniform permutations by modifying the inverse function on subfields.* Cryptogr. Commun. 9, 363–378 (2017) .

[8] L. J. Qu, Y. Tan, C. H. Tan, C. Li, *Constructing differentially 4-uniform permutations over $F_{2^{2k}}$ via the switching method.* IEEE Trans. Inf. Theory 59(7), 4675–4686 (2013).

[9] D. Tang, C. Carlet, X. Tang, *Differentially 4-uniform bijections by permuting the inverse function.* Des. Codes. Cryptogr. 77, 117–141 (2015).

[10] G. Xu, L. Qu, *Two classes of differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ with $n$ even.* Adv. Math. Comm., 14(1), 97–110 (2019).

[11] Z. Zha, L. Hu, S. Sun, *Constructing new differentially 4-uniform permutations from the inverse function*. Finite Fields Appl. 25, 64–78 (2014) .

[12] Z. Zha, L. Hu, J. Shan, *Differentially 6-uniform permutations by modifying the Gold function.* In: IEEE Int. Conf. on Information and Automation (ICIA), 961–965 (2014).