On a method for constructing APN permutations

Petr Lisoněk
Simon Fraser University
Burnaby, BC, Canada

The Fourteenth International Workshop on Coding and Cryptography (WCC 2026)

Paris, France
11 June 2026

Background

Definition

We say that a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *almost perfect nonlinear (APN) if for all* $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, *the equation*

$$f(x + a) - f(x) = b$$

has at most two solutions $x \in \mathbb{F}_{2^n}$.

More generally such f is called a *differentially 2-uniform function.*

Background

Differentially uniform functions are important in symmetric cryptography (block ciphers, message authentication codes, hash functions) where they protect against the differential cryptanalysis attack.

In block ciphers, APN functions find applications in the construction of *S-boxes* (substitution boxes) which are the only non-linear components of the cipher.

In the design of block ciphers it is beneficial if the S-boxes are *invertible,* that is, if they are *permutations* of $\mathbb{F}_{2^n}$.

Background

$f(x) = x^3$ is APN for all n (but it is a permutation of $\mathbb{F}_{2^n}$ only when n is odd).

$f(x) = 1/x$ (with $f(0) = 0$) is APN iff n is odd (it is a permutation of $\mathbb{F}_{2^n}$ for all n). This function is used in the S-box of the *Advanced Encryption Standard (AES)* with $n = 8$; it is differentially 4-uniform when n is even.

The question about existence of APN permutations of $\mathbb{F}_{2^n}$ for even $n > 6$ is the Big APN Problem.

Talk outline

We investigate whether the method used by Browning et al. to obtain an APN permutation of $\mathbb{F}_{2^6}$ can be successful in other dimensions as well.

We recall our earlier formalization of this method and our previous relevant results (Chase and Lisoněk 2022).

We report on computational investigations that use these results in odd dimensions $n \leq 15$.

Walsh zero space

Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. For $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ we define the Walsh transform of f at (a, b) as

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

We say that (a, b) is a *Walsh zero* of f if $\mathcal{W}_f(a, b) = 0$.

Definition

Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Suppose that S is an $\mathbb{F}_2$-linear subspace of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $\dim_{\mathbb{F}_2} S = n$ and each element of S except $(0, 0)$ is a Walsh zero of f. We say that S is a *WZ space of f*.

Functions CCZ-equivalent to a permutation

Definition

We say that two WZ spaces S, T of the same function *intersect trivially if* $S \cap T = \{(0,0)\}$. *Then we say that* $\{S, T\}$ *is a* TI-pair (trivially intersecting pair).

Proposition

Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Then f is CCZ-equivalent to a permutation of $\mathbb{F}_{2^n}$ if and only if there exist two WZ spaces of f that intersect trivially.

This was used to construct an APN permutation of $\mathbb{F}_{2^6}$ by Browning et al. in 2009 (presented at Fq9 conference) using the *Kim function* for f. Recall that the CCZ equivalence preserves the APN property.

EA equivalence and EA invariants

Two functions f and g from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ are *extended affine equivalent (EA equivalent)* if there exist affine permutatations A_1 and A_2 of $\mathbb{F}_{2^n}$ and affine function $A_3 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that

$$g(x) = A_2(f(A_1(x))) + A_3(x) \quad \text{for all } x \in \mathbb{F}_{2^n}.$$

EA equivalence implies CCZ equivalence.

Properties of f and g preserved by EA equivalence are called *EA invariants.* They can be used to show that two functions are **not** EA equivalent.

WZ spaces of Gold functions

Gold functions $x \mapsto x^{2^i+1}$ where $\gcd(i, n) = 1$ are a well studied class of APN functions on $\mathbb{F}_{2^n}$. In this talk we deal with Gold functions exclusively in odd dimensions n.

Being permutations of $\mathbb{F}_{2^n}$, they possess the obvious WZ spaces $Z_{a0} = \{(a, 0) : a \in \mathbb{F}_{2^n}\}$ and $Z_{0b} = \{(0, b) : b \in \mathbb{F}_{2^n}\}$, which are here listed for the purpose of introducing notation, as they will occur in subsequent propositions.

Walsh zero criterion for Gold functions

Theorem (Gold 1968)

Suppose n is odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $f(x) = x^{2^i+1}$ such that $\gcd(i, n) = 1$. Then (a, b) is a Walsh zero of f if and only if $\mathrm{Tr}(ab^{-\frac{1}{2^i+1}}) = 0$ or $a \neq 0$, $b = 0$.

TI-pairs of WZ spaces of Gold functions

Recall from earlier that the Dillon-type construction of a permutation CCZ-equivalent to a function f requires two TI-pairs of WZ spaces of f. This motivates our earlier results which will be reviewed in the next few slides.

The reference [CL] denotes

B. Chase, P. Lisoněk, Construction of APN permutations via Walsh zero spaces. Cryptography and Communications 14 (2022), 1345–1357.

TI-pairs of WZ spaces of Gold functions

Proposition ([CL] Prop. 5.1)

Let $n = 3k$ where k is odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with $\gcd(i, n) = 1$. Let

$$Z = \{(x, \mu^{-(2^i+1)}(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i} \mu x))) : x \in \mathbb{F}_{2^n}\}$$

where ξ is a fixed element of $\mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$ and μ is a fixed element of $\mathbb{F}_{2^n}^*$. Then Z is a WZ space of f and the pair $\{Z_{0b}, Z\}$ intersects trivially.

TI-pairs of WZ spaces of Gold functions

Proposition ([CL] Prop. 5.2)

Let n be odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with $\gcd(i, n) = 1$. Let

$$Z = \{(\mu(b + b^{\frac{1}{2^i}}), \mu^{2^i+1} b) : b \in \mathbb{F}_{2^n}\}$$

with μ a fixed element of $\mathbb{F}_{2^n}^*$. Then Z is a WZ space of f and the pair $\{Z_{a0}, Z\}$ intersects trivially.

TI-pairs of WZ spaces of Gold functions

Proposition ([CL] Prop. 5.3)

Let $n = 3k$ where k is odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with $\gcd(i, n) = 1$. Let

$$Y = \{(x, \mu^{-(2^i+1)}(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i} \mu x))) : x \in \mathbb{F}_{2^n}\}$$

where ξ is a fixed element of $\mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$ and μ is a fixed element of $\mathbb{F}_{2^n}^*$. Let

$$Z = \{(\nu(b + b^{\frac{1}{2^i}}), \nu^{2^i+1} b) : b \in \mathbb{F}_{2^n}\}$$

with ν a fixed element of $\mathbb{F}_{2^n}^*$. Suppose also that $\mathrm{Tr}((\xi + \xi^{2^i})(\mu\nu)^{-2^i}) = 0$. Then Y and Z are WZ spaces of f and the pair $\{Y, Z\}$ intersects trivially.

This proposition will be used later to construct APN permutations that are provably not EA equivalent to Gold functions and their inverses.

TI-pairs of WZ spaces of Gold functions

Proposition ([CL] Prop. 5.4)

Let $n = 3k$ where k is odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with $\gcd(i, n) = 1$. Let

$$Y = \{(\nu(b + b^{\frac{1}{2^i}}), \nu^{2^i+1} b) : b \in \mathbb{F}_{2^n}\}$$

with ν a fixed element of $\mathbb{F}_{2^n}^*$. Suppose ξ is a fixed primitive element of $\mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$. Let

$$Z = X \times S$$

with $S = \mathrm{span}_{\mathbb{F}_2}\{\mu, \xi\mu\}$ for some fixed $\mu \in \mathbb{F}_{2^n}^*$ and Z is constructed by applying Proposition 4.1. Suppose also that $\mathrm{Tr}((\xi + \xi^{2^i})\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) = 1$. Then Y and Z are WZ spaces of f and the pair $\{Y, Z\}$ intersects trivially.

Computations

We applied Propositions [CL] 5.1 through 5.4 to construct many APN permutations of $\mathbb{F}_{2^n}$ for odd $n \leq 15$. As the parameter spaces are too large to traverse exhaustively, random sampling of parameters was used.

EA invariants algebraic degree and minimum algebraic degree were used to assert EA-**in**equivalence of some of the newly obtained APN permutations with Gold functions and their compositional inverses.

Some instances of our Proposition 5.3 produce APN permutations of algebraic degree 4, whereas the algebraic degree is 2 for Gold functions, and it is $(n+1)/2$ for their inverses. In this case it appears that these APN permutations are new. An example in dimension 9 is listed in the conference abstract.

Functions $f_{\xi,\mu,\nu}$

We denote by $f_{\xi,\mu,\nu}$ the APN permutation that is constructed by our method and Proposition 5.3 for $i = 1$ and for specific admissible choices of the parameters ξ, μ and ν.

Lemma

For each $\xi \in \mathbb{F}_{2^3}$ and each $\mu, \nu \in \mathbb{F}_{2^n}$ we have $f_{\xi,\mu,\nu} = f_{\xi+1,\mu,\nu}$.

To produce explicit examples, taking $\mu = 1$ and $\nu = 1$ leads to admissible parameter choices, since for any ξ we then have

$$\mathrm{Tr}((\xi + \xi^{2^i})(\mu\nu)^{-2^i}) = \mathrm{Tr}(\xi + \xi^{2^i}) = 0$$

and the condition of Proposition 5.3 is satisfied for each ξ.

Examples of new APN permutations

Proposition

For each $\xi \in \mathbb{F}_{2^3} \setminus \mathbb{F}_2$ the function $f_{\xi,1,1}$ defined on $\mathbb{F}_{2^9}$ is an APN permutation of algebraic degree 4.

Proposition

For each $\xi \in \mathbb{F}_{2^3} \setminus \mathbb{F}_2$ the function $f_{\xi,1,1}$ defined on $\mathbb{F}_{2^{15}}$ is an APN permutation of algebraic degree 4.

Work in progress

Find other EA invariants (other than the algebraic degree) that would allow to get more insight into (in-)equivalence of APN permutations that we produce. Most of the known EA invariants are either very hard to compute or they are not suitable for our situation. This may allow to find more new APN permutations.

It is possible that the other three Propositions in [CL] (Prop. 5.1, 5.2, 5.4) also produce APN permutations that are not EA equivalent to Gold functions, but more refined invariants are needed to prove this. In lower dimensions perform a full EA equivalence test if needed.

Work in progress (cont'd)

Verify computationally that the functions $f_{\xi,1,1}$ have algebraic degree 4 also in higher applicable dimensions, that is, $n = 6k + 3$ for $k > 2$, and thus they are not EA equivalent to Gold functions and their inverses in those dimensions either. Interpolate a *sparse* univariate polynomial.

Examine the influence of the choice of the dual bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ on the resulting polynomial form of $f_{\xi,\mu,\nu}$. (The role of these dual bases is explained in the proof of our main construction which is included in the conference abstract. A linear code over $\mathbb{F}_2$ is involved in the construction.) While all such resulting polynomial forms will be EA equivalent, they still may differ substantially in their complexity and shape. Aim for computer-free constructions.

References

K.A. Browning, J.F. Dillon, R.E. Kibler, M.T. McQuistan, APN polynomials and related codes. Journal of Combinatorics, Information and System Science 34 (2009), 135–159.

K.A. Browning, J.F. Dillon, M.T. McQuistan, A.J. Wolfe, An APN permutation in dimension six. Finite fields: theory and applications. Contemporary Mathematics 518 (2010), 33–42.

B. Chase, P. Lisoněk, Construction of APN permutations via Walsh zero spaces. Cryptography and Communications 14 (2022), 1345–1357.

B. Chase, P. Lisoněk, Kim-type APN functions are affine equivalent to Gold functions. Cryptography and Communications 13 (2021), 981–993.