A direct proof of APN-ness of the Kasami functions

Claude Carlet[1], Kwang Ho Kim[2,3] and Sihem Mesnager[4]

[1] Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, Laboratoire de Géométrie, Analyse et Applications, LAGA, University Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France and Department of informatics, University of Bergen, Norway.
claude.carlet@gmail.com
[2] Institute of Mathematics, State Academy of Sciences, Pyongyang, Democratic People's Republic of Korea
khk.cryptech@gmail.com
[3] PGItech Corp., Pyongyang, Democratic People's Republic of Korea
[4] Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, Laboratoire de Géométrie, Analyse et Applications, LAGA, University Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France, and Telecom ParisTech, 91120 Palaiseau, France.
smesnager@univ-paris8.fr

Abstract. Using recent results on solving the equation $X^{2^k+1}+X+a=0$ over a finite field $\mathbb{F}_{2^n}$, we address an open question raised by the first author in WAIFI 2014 concerning the APN-ness of the Kasami functions $x \mapsto x^{2^{2k}-2^k+1}$ with $gcd(k,n)=1$, $x \in \mathbb{F}_{2^n}$
Keywords: APN function · Equation · Müller-Cohen-Matthews (MCM) polynomial · Dickson polynomial · Zeros of a polynomial · Irreducible polynomial.

Keywords: Mathematics Subject Classification. 06E30, 11D04, 12E05, 12E12, 12E20.

1 Introduction

Vectorial (multi-output) Boolean functions are functions from the finite field $\mathbb{F}_{2^n}$ (of order 2^n) to the finite field $\mathbb{F}_{2^m}$, for given positive integers n and m. These functions are called (n,m)-functions and include the (single-output) Boolean functions (which correspond to the case $m=1$). In symmetric cryptography, multi-output Boolean functions are called *S-boxes*. They are fundamental parts of block ciphers. Being the only source of nonlinearity in these ciphers, S-boxes play a central role in their robustness, by providing confusion (a requirement already mentioned by C. Shannon [17]), which is necessary to withstand known (and hopefully future) attacks. When they are used as S-boxes in block ciphers, the number m of their output bits equals or is less than the number n of input bits, most often. Such functions can also be used in stream ciphers, with m significantly smaller than n, in the place of Boolean functions to speed up the ciphers. A survey by the first author on vectorial Boolean functions for cryptography and coding theory can be found in [2]. An important class of vectorial functions is that of *almost perfect nonlinear* (APN) functions. An (n, n)-function F is called APN if, for every $a \in \mathbb{F}_{2^n}^*$ and every $b \in \mathbb{F}_{2^n}$, the equation $F(x) + F(x + a) = b$ has at most 2 solutions, that is, has 0 or 2 solutions. APN functions correspond to optimal objects within other areas of mathematics (e.g. coding theory, combinatorics, and projective geometry), which makes them also interesting objects from a theoretical point of view. The first known APN functions have been power functions $F : x \mapsto x^d$, $x \in \mathbb{F}_{2^n}$. One class of such functions is that of Kasami APN power functions $F : x \mapsto x^{2^{2k}-2^k+1}$ with $gcd(k, n) = 1$, $x \in \mathbb{F}_{2^n}$. The proof that Kasami functions are APN is difficult, see [10, 7]. The first author suggested in [3] to find a direct proof of the APN-ness of Kasami functions. This paper provides such a proof. It is structured as follows. In Section, 2 we introduce some preliminaries devoted to APN functions. Section 3 describes the fourth section of [3] and recalls the exact problem raised by the first author in [3]. Using the recent advances in solving the equation $X^{2^k+1} + X + a = 0$ over finite fields [12, 11], we present in Section 4 a direct proof of the APN-ness of Kasami functions.

2 Preliminaries and notation

Let n be a positive integer. The finite field of order 2^n will be denoted by $\mathbb{F}_{2^n}$. In addition, we shall denote by Tr the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ defined by $Tr(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$.

Differentially uniform functions are defined as follows.

Definition 1. *([13, 14]) Let n and m be any positive integers (that we shall take in practice such that $m \leq n$) and let δ be any positive integer. An (n, m)-function F is called* differentially δ-uniform *if, for every nonzero $a \in \mathbb{F}_{2^n}$ and every $b \in \mathbb{F}_{2^m}$, the equation $F(x) + F(x + a) = b$ has at most δ solutions. The minimum of such value δ for a given function F is denoted by δ_F and called the* differential uniformity *of F.*

The differential uniformity is necessarily even since the solutions of equation $F(x) + F(x + a) = b$ go by pairs (if x is a solution of $F(x) + F(x + a) = b$ then $x + a$ is also a solution).

When F is used as an S-box inside a cryptosystem, the differential uniformity measures its contribution to the resistance against the differential attack. The smaller is δ_F, the better is the resistance.

The differential uniformity δ_F of any (n, m)-function F is bounded below by 2^{n-m}. When the differential uniformity δ_F equals 2^{n-m}, then F is called *perfect nonlinear* (PN). Perfect nonlinear functions can also be called *bent functions*, since equivalently, they achieve the best possible nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1}$, see [13]. It is well-known that perfect nonlinear (n, n)-functions do not exist (precisely, they exist if and only if n is even and $m \leq \frac{n}{2}$); but they do exist in other characteristics than 2 (see *e.g.* [4]); they are then often called *planar* functions (instead of "perfect nonlinear").

Definition 2. *([1, 15, 16]) An (n,n)-function F is called* almost perfect nonlinear *(APN) if it is differentially 2-uniform, that is, if for every $a \in \mathbb{F}_2^{n*}$ and every $b \in \mathbb{F}_2^n$, the equation $F(x) + F(x+a) = b$ has 0 or 2 solutions.*

Since (n,m)-functions have differential uniformity at least 2^{n-m} when $m \leq n/2$ (n even) and strictly larger when n is odd or $m > n/2$, we shall use the term of APN function only when $m = n$. In this paper we are only dealing with APN functions. The first known APN functions have been power functions $F : x \mapsto x^d$, $x \in \mathbb{F}_{2^n}$. When F is APN, the exponent d is said to be an *APN exponent.* We present in Table 1, the known APN exponents up to equivalence (given any n, two exponents are said equivalent if they are in the same cyclotomic class of 2 modulo $2^n - 1$) and up to inversion (for n odd, since it is known, see e.g. [2], that APN exponents are invertible modulo $2^n - 1$ if and only if n is odd).

Table 1. Known APN exponents up to equivalence (any n) and up to inversion (n odd)

Functions	Exponents d	Conditions
Gold	$2^i + 1$	$gcd(i,n) = 1$
Kasami	$2^{2i} - 2^i + 1$	$gcd(i,n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{t/2} - 1$, t even	$n = 2t + 1$
	$2^t + 2^{(3t+1)/2} - 1$, t odd	
Inverse	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

In this paper we focus on Kasami APN functions (see [10] and also [7]). The proof that such function is APN is difficult. The first author suggested in [3] to find a a direct proof of APN-ness of the Kasami functions.

3 Description of the open question raised by C. Carlet in [3]

3.1 Recall of the content of Section 4.4 in [3]

Section 4.4 of [3] is entitled "Find a direct proof of APN-ness of the Kasami functions in even dimension which would use the relationship between these functions and the Gold functions". It recalls that the proof by Hans Dobbertin in [8] of the fact that Kasami functions $F(x) = x^{2^{2k}-2^k+1}$, where $\gcd(i,n) = 1$, are AB (and therefore APN) for n odd uses that these functions are the (commutative) composition of a Gold function and of the inverse of another

Gold function. This proof is particularly simple. The direct proofs in [10] and [7] that the Kasami functions above are APN for n even are harder, as well as the determination in [6] (Theorem 11) of their Walsh spectrum, which also allows to prove their APN-ness, and which uses a similar but slightly more complex relation to the Gold functions when n is not divisible by 6. It is then written in [3] that it would be interesting to see if, for n odd and for n even, these relations between the Kasami functions and the Gold functions can lead to alternative direct proofs, *hopefully simpler*, of the APN-ness of Kasami functions.

Since the Kasami function is a power function, it is APN if and only if, for every $b \in \mathbb{F}_{2^n}$ the system

$$\begin{cases} X + Y = 1 \\ F(X) + F(Y) = b \end{cases} \tag{1}$$

has at most one pair $\{X, Y\}$ of solutions in $\mathbb{F}_{2^n}$.

• For n odd, $2^k + 1$ is coprime with $2^n - 1$ and $F(x) = G_2 \circ G_1^{-1}(x)$, where $G_1(x)$ and $G_2(x)$ are respectively the Gold functions x^{2^k+1} and $x^{2^{3k}+1}$. Hence, F is APN if and only if the system

$$\begin{cases} x^{2^k+1} + y^{2^k+1} = 1 \\ x^{2^{3k}+1} + y^{2^{3k}+1} = b \end{cases} \tag{2}$$

has at most one pair $\{x, y\}$ of solutions. Let $y = x + z$. Then $z \neq 0$. The system (2) is equivalent to:

$$\begin{cases} \left(\frac{x}{z}\right)^{2^k} + \left(\frac{x}{z}\right) = \frac{1}{z^{2^k+1}} + 1 \\ \left(\frac{x}{z}\right)^{2^{3k}} + \left(\frac{x}{z}\right) = \frac{b}{z^{2^{3k}+1}} + 1 \end{cases} \tag{3}$$

or equivalently

$$\begin{cases} \left(\frac{x}{z}\right)^{2^k} + \left(\frac{x}{z}\right) = \frac{1}{z^{2^k+1}} + 1 \\ \frac{1}{z^{2^k+1}} + 1 + \left(\frac{1}{z^{2^k+1}} + 1\right)^{2^k} + \left(\frac{1}{z^{2^k+1}} + 1\right)^{2^{2k}} = \frac{b}{z^{2^{3k}+1}} + 1 \end{cases} \tag{4}$$

that is, by simplifying and multiplying the second equation by $z^{2^{3k}+2^{2k}}$:

$$\begin{cases} \left(\frac{x}{z}\right)^{2^k} + \left(\frac{x}{z}\right) = \frac{1}{z^{2^k+1}} + 1 \\ z^{2^{3k}+2^{2k}-2^k-1} + z^{2^{3k}-2^k} + 1 = bz^{2^{2k}-1} \end{cases} \tag{5}$$

that is, denoting $v = z^{2^{2k}-1}$ and $c = b + 1$:

$$\begin{cases} \left(\frac{x}{z}\right)^{2^k} + \left(\frac{x}{z}\right) = \frac{1}{v^{\frac{1}{2^k-1}}} + 1 \\ (v+1)^{2^k+1} + cv = 0 \end{cases} \tag{6}$$

Proving that F is APN is equivalent to proving that, for every $c \in \mathbb{F}_{2^n}$, the second equation can be satisfied by at most one value of v such that the first equation can admit solutions, i.e. such that $Tr\left(\frac{1}{z^{2^k+1}}+1\right)=0$. It is recalled in [3] that Reference [9] studies the equation $x^{2^k+1}+c(x+1)=0$, but observed that this does not seem to allow completing a proof. Then is stated the:

Open Question 1: For n odd, is it possible to complete this proof?

• For n even, note first that System (1) has a solution such that $X=0$ or $Y=0$ if and only if b $=1$. We restrict now ourselves to the case where n is not divisible by 6. Then $(\frac{2^n-1}{3},3)=1$ and every element X of $\mathbb{F}_{2^n}^*$ can be written (in 3 different ways) in the form $\omega x^{2^k+1}, \omega\in\mathbb{F}_4^*, x\in\mathbb{F}_{2^n}^*$. Indeed, the function $x\longmapsto x^{2^k+1}$ is 3-to-1 from $\mathbb{F}_{2^n}^*$ to the set of cubes of $\mathbb{F}_{2^n}^*$, and every integer i is, by the Bézout theorem, the linear combination over $\mathbb{Z}$ of $\frac{2^n-1}{3}$ and 3; the element α^i of $\mathbb{F}_{2^n}^*$ (where α is primitive) is then the product of a power of $\alpha^{\frac{2^n-1}{3}}$ and of a power of α^3. Note that $2^{2k}-2^k+1=(2^k+1)^2-3\cdot 2^k$ is divisible by 3. So, F is APN if and only if the system

$$\begin{cases}\omega x^{2^k+1}+\omega' y^{2^k+1}=1\\ x^{2^{3k}+1}+y^{2^{3k}+1}\quad=b\end{cases}, \tag{7}$$

where $\omega,\omega'\in\mathbb{F}_4^*$ and $x,y\in\mathbb{F}_{2^n}^*$, has no solution for $b=1$ and has at most one pair $\{\omega x^{2^k+1},\omega' y^{2^k+1}\}$ of solutions for every $b\neq 1$. We consider the case $x^{2^k+1}=y^{2^k+1}$ (and $\omega\neq\omega'$) apart. In this case, the first equation $(\omega+\omega')x^{2^k+1}=1$ is equivalent to $x\in\mathbb{F}_4^*$ and $\omega+\omega'=1$. Then because of the second equation, for $b=0$, we have two solutions such that $x^{2^k+1}=y^{2^k+1}$ (since ω and ω' are nonzero) and for $b\neq 0$ we have none. Hence, F is APN if and only if the system

$$\begin{cases}\omega x^{2^k+1}+\omega' y^{2^k+1}=1\\ x^{2^{3k}+1}+y^{2^{3k}+1}\quad=b\end{cases} \tag{8}$$

where $\omega,\omega'\in\mathbb{F}_4^*$ and $x,y\in\mathbb{F}_{2^n}^*$ are such that $x^{2^k+1}\neq y^{2^k+1}$, has no solution for $b\in\mathbb{F}_2$ and has at most one pair $\{\omega x^{2^k+1},\omega' y^{2^k+1}\}$ of solutions for every $b\notin\mathbb{F}_2$. Since $x^{2^k+1}\neq y^{2^k+1}$, we can as above denote $y=x+z$ where $z\neq 0$, $v=z^{2^{2k}-1}$ and $c=b+1$, and we obtain the system:

$$\begin{cases}(\omega+\omega')\left(\frac{x}{z}\right)^{2^k+1}+\omega'\left(\frac{x}{z}\right)^{2^k}+\omega'\left(\frac{x}{z}\right)=\frac{1}{z^{2^k+1}}+\omega'\\ \left(\frac{x}{z}\right)^{2^{3k}}+\left(\frac{x}{z}\right)\qquad\qquad\qquad\qquad=\frac{b}{z^{2^{3k}+1}}+1\end{cases} \tag{9}$$

where $z\neq 0, v\neq 0$.

Remark 3. System (9) is slightly different from the system obtained in [3]; it is better adapted to finding a direct proof of the APN-ness of Kasami functions.

As in the case of n odd, it is written in [3] that the results of [9] do not seem to allow completing a direct proof of APN-ness. Then is stated the:

Open Question 2: For n even not divisible by 6, is it possible to complete this proof?
Open Question 3: For n divisible by 6, is it possible to adapt the method?

4 Proofs of APN-ness of Kasami functions

In this section, we complete the direct proofs of the APN-ness of Kasami functions, for n odd and for n even.

Let $q = 2^k$. We will use the following result.

Lemma 4. *(Lemma 7 of [11]) Let $(n, k) = 1$. The equation $X^{q+1} + X + a = 0$ has only 0, 1 or 3 solutions in $\mathbb{F}_{2^n}$. If the equation $X^{q+1} + X + a = 0$ has three solutions in $\mathbb{F}_{2^n}$, then there exists an $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$ such that $a = \frac{(u+u^q)^{q^2+1}}{(u+u^{q^2})^{q+1}}$. Furthermore, in that case the three solutions are $x_1 = \frac{1}{1+(u+u^q)^{q-1}}$, $x_2 = \frac{u^{q^2-q}}{1+(u+u^q)^{q-1}}$ and $x_3 = \frac{(u+1)^{q^2-q}}{1+(u+u^q)^{q-1}}$.*

Proof. The fact the $X^{q+1} + X + a = 0$ has only 0, 1 or 3 solutions in $\mathbb{F}_{2^n}$ is well known (see e.g. [9, 12]). The fact that if $X^{q+1} + X + a = 0$ has three solutions in $\mathbb{F}_{2^n}$, then there exists an $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $a = \frac{(u+u^q)^{q^2+1}}{(u+u^{q^2})^{q+1}}$, is a direct consequence of Proposition 5 and Proposition 1 in [9].

For $a = \frac{(u+u^q)^{q^2+1}}{(u+u^{q^2})^{q+1}}$, $u \notin \mathbb{F}_2$, the fact that $x_1 = \frac{1}{1+(u+u^q)^{q-1}}$, $x_2 = \frac{u^{q^2-q}}{1+(u+u^q)^{q-1}}$ and $x_3 = \frac{(u+1)^{q^2-q}}{1+(u+u^q)^{q-1}}$ are different solutions to $X^{q+1}+X+a = 0$ can be checked by straightforward substitution. □

4.1 Case when n is odd

Since $(n, k) = 1$ and n is odd, it holds that $(q - 1, 2^n - 1) = (q + 1, 2^n - 1) = 1$. Carlet's question can be restated as: Prove that for every $c \in \mathbb{F}_{2^n}$ the following system of equations:

$$\begin{cases} Tr\left(\frac{1}{v^{\frac{1}{q-1}}}\right) = 1 \\ (v+1)^{q+1} + cv = 0 \end{cases} \tag{10}$$

has at most one $\mathbb{F}_{2^n}-$solution.

Proof. If $c = 0$, then the statement is right as evidently Equation (10) has the unique solution 1. Let us then assume $c \neq 0$. By the variable substitution $v = c^{1/q}V + 1$, the second equation becomes $V^{q+1} + V + c^{-1/q} = 0$. By Lemma 4, we know $V^{q+1} + V + c^{-1/q} = 0$ has 0, 1 or 3 $\mathbb{F}_{2^n}-$solutions for any $c \in \mathbb{F}_{2^n}$. If this equation has at most one solution, then Equation (10) also has at most one solution.

Let us assume that this equation has 3 solutions in $\mathbb{F}_{2^n}$. Then, by Lemma 4 there exists an $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $c^{-1/q} = \frac{(u+u^q)^{q^2+1}}{(u+u^{q^2})^{q+1}}$. Furthermore, these three solutions are: $V_1 = \frac{1}{1+(u+u^q)^{q-1}}$, $V_2 = \frac{u^{q^2-q}}{1+(u+u^q)^{q-1}}$ and $V_3 = \frac{(u+1)^{q^2-q}}{1+(u+u^q)^{q-1}}$.

Thus, the three solutions to $(v+1)^{q+1} + cv = 0$ are the following:

– $v_1 = c^{1/q}V_1 + 1 = \frac{(u+u^{q^2})^{q+1}}{(u+u^q)^{q^2+1}} \cdot \frac{1}{1+(u+u^q)^{q-1}} + 1 = \frac{(u+u^{q^2})^{q+1}}{(u+u^q)^{q^2+1}} \cdot \frac{u+u^q}{u+u^{q^2}} + 1 = \frac{(u+u^{q^2})^q}{(u+u^q)^{q^2}} + 1 = \frac{1}{(u+u^q)^{q^2-q}}$.

– $v_2 = \frac{u^{q^2}(u+u^{q^2})^q}{u^q(u+u^q)^{q^2}} + 1 = \frac{u^{q^2}(u+u^{q^2})^q + u^q(u+u^q)^{q^2}}{u^q(u+u^q)^{q^2}} = \frac{u^{q^3}(u+u^q)^q}{u^q(u+u^q)^{q^2}} = \frac{u^{q^3-q}}{(u+u^q)^{q^2-q}}$.

– $v_3 = \frac{(u+1)^{q^2}(u+u^{q^2})^q}{(u+1)^q(u+u^q)^{q^2}} + 1 = \frac{(u+1)^{q^2}(u+u^{q^2})^q + (u+1)^q(u+u^q)^{q^2}}{(u+1)^q(u+u^q)^{q^2}} = \frac{(u+1)^{q^3}(u+u^q)^q}{(u+1)^q(u+u^q)^{q^2}} = \frac{(u+1)^{q^3-q}}{(u+u^q)^{q^2-q}}$.

But, we have $Tr\left(\frac{1}{v_1^{\frac{1}{q-1}}}\right) = Tr\left(\frac{1}{v_2^{\frac{1}{q-1}}}\right) = Tr\left(\frac{1}{v_3^{\frac{1}{q-1}}}\right) = 0$ since

– $\frac{1}{v_1^{\frac{1}{q-1}}} = u^q + u^{q^2}$;

– $\frac{1}{v_2^{\frac{1}{q-1}}} = \frac{(u+u^q)^q}{u^{q(q+1)}} = \frac{1}{u^q} + \frac{1}{u^{q^2}}$;

– $\frac{1}{v_3^{\frac{1}{q-1}}} = \frac{(u+u^q)^q}{(u+1)^{q(q+1)}} = \frac{(u+1)^q + (u+1)^{q^2}}{(u+1)^{q(q+1)}} = \frac{1}{(u+1)^q} + \frac{1}{(u+1)^{q^2}}$.

Hence, Equation (10) has no $\mathbb{F}_{2^n}$−solution in this case. □

4.2 Case when n is even

A simplest direct proof : Müller-Cohen-Matthews polynomials are defined as follows:

$$f_{k,2^k+1}(X) := \frac{T_k(X)^{2^k+1}}{X^{2^k}}$$

where $T_k(X) := \sum_{i=0}^{k-1} X^{2^i}$. The following fact is well-known.

Lemma 5. *[5, 12] If $(n,k) = 1$ and k is odd, then $f_{k,2^k+1}$ is a permutation on $\mathbb{F}_{2^n}$.*

A very concise proof of this fact is also given by Section 6 in [6], by using a classical result (by Dickson in 1896) on Dickson polynomials.

Now, equality $F(X) + F(X+1) + 1 = f_{k,2^k+1}(X + X^2)$ can be checked by direct calculation. If n is even, then k is odd as $(n,k) = 1$. So $F(X) + F(X+1)$ is 2-to-1 by above Lemma, i.e., the Kasami functions are APN. □

Continuing the discussion: While a very simple direct proof for n even already exists as presented above, here we will try to continue the discussion from Section 1. One should keep in mind the following facts:

1. When n is divisible by 4, $Tr(\omega) = \omega + \omega^2 + \cdots + \omega^{2^{n-1}} = 0$ for each $\omega \in \mathbb{F}_4^*$.
2. When n is even not divisible by 4, $Tr(\omega) = 1$, for each $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$ and $Tr(1) = 0$.
3. Since k is odd, it holds that $\omega^{q-1} = \omega = \omega^{\frac{1}{q-1}}$, $\omega^q = \omega^2$, $\omega^{q+1} = 1$, $\omega^{q^2} = \omega$ for each $\omega \in \mathbb{F}_4^*$.

Now, let us assume $\omega = \omega'$ i.e. $\omega + \omega' = 0$. The system (9) is equivalent to:

$$\begin{cases} \left(\frac{x}{z}\right)^q + \left(\frac{x}{z}\right) &= \frac{1}{\omega' z^{q+1}} + 1 \\ \left(\frac{x}{z}\right)^{q^3} + \left(\frac{x}{z}\right) &= \frac{b}{z^{q^3+1}} + 1 \end{cases}$$

or equivalently with $\varpi = \frac{1}{\omega'}$

$$\begin{cases} \left(\frac{x}{z}\right)^q + \left(\frac{x}{z}\right) = \frac{\varpi}{z^{q+1}} + 1 \\ \frac{\varpi}{z^{q+1}} + 1 + \left(\frac{\varpi}{z^{q+1}} + 1\right)^q + \left(\frac{\varpi}{z^{q+1}} + 1\right)^{q^2} = \frac{b}{z^{q^3+1}} + 1. \end{cases}$$

By simplifying and multiplying the second equation by $z^{q^3+q^2}$,

$$\begin{cases} \left(\frac{x}{z}\right)^q + \left(\frac{x}{z}\right) = \frac{\varpi}{z^{q+1}} + 1 \\ z^{q^3+q^2-q-1} + \varpi z^{q^3-q} + 1 = b\varpi^2 z^{q^2-1} \end{cases}$$

that is, denoting $v = \varpi^2 z^{q^2-1}$ and $c = b + 1$:

$$\begin{cases} \left(\frac{x}{z}\right)^q + \left(\frac{x}{z}\right) &= \frac{1}{v^{\frac{1}{q-1}}} + 1 \\ (v+1)^{q+1} + cv = 0. \end{cases}$$

Let ε be such that $1 = \varepsilon + \varepsilon^2$ that is, $\varepsilon \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Then, one has $\varepsilon^q + \varepsilon = 1$ and $\varepsilon^q = \frac{1}{\varepsilon}$.

By the same arguments as in Section 2.1, when $(v+1)^{q+1} + cv = 0$ has three solutions, there exists an $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$ such that $\frac{1}{v^{\frac{1}{q-1}}} \in \{u + u^q, \frac{1}{u} + \frac{1}{u^q}, \frac{1}{u+1} + \frac{1}{(u+1)^q}\}$. Let us define $S := \{\frac{\varpi}{u+u^q}(u+\varepsilon)^{q+1}, \frac{\varpi}{u+u^q}(u+1+\varepsilon)^{q+1}\}$.

- If $\frac{1}{v^{\frac{1}{q-1}}} = u + u^q$, then $z^{q+1} = \varpi v^{\frac{1}{q-1}} = \frac{\varpi}{u+u^q}$ and $x^{q+1} \in \{z^{q+1}(u+\varepsilon)^{q+1}, z^{q+1}(u+1+\varepsilon)^{q+1}\} = S$.
- If $\frac{1}{v^{\frac{1}{q-1}}} = \frac{1}{u} + \frac{1}{u^q}$, then $z^{q+1} = \varpi v^{\frac{1}{q-1}} = \frac{\varpi u^{q+1}}{u+u^q}$ and $x^{q+1} \in \{z^{q+1}(\frac{1}{u}+\varepsilon)^{q+1}, z^{q+1}(\frac{1}{u}+1+\varepsilon)^{q+1}\} = \{\frac{\varpi u^{q+1}}{u+u^q}(\frac{1}{u}+\varepsilon)^{q+1}, \frac{\varpi u^{q+1}}{u+u^q}(\frac{1}{u}+1+\varepsilon)^{q+1}\} = S$.
- If $\frac{1}{v^{\frac{1}{q-1}}} = \frac{1}{u+1} + \frac{1}{(u+1)^q}$, then $z^{q+1} = \varpi v^{\frac{1}{q-1}} = \frac{\varpi(u+1)^{q+1}}{u+u^q}\}$ and $x^{q+1} \in \{z^{q+1}(\frac{1}{u+1}+\varepsilon)^{q+1}, z^{q+1}(\frac{1}{u+1}+1+\varepsilon)^{q+1}\} = \{\frac{\varpi(u+1)^{q+1}}{u+u^q}(\frac{1}{u+1}+\varepsilon)^{q+1}, \frac{\varpi(u+1)^{q+1}}{u+u^q}(\frac{1}{u+1}+1+\varepsilon)^{q+1}\} = S$.

That is, $x^{q+1} \in S$ for all cases. Thus, for $b = \frac{u+u^{q^3}}{(u+u^q)^{q^2-q+1}}$ with $u \in \mathbb{F}_4 \setminus \mathbb{F}_2$, there are two solutions $\{\frac{(u+\varepsilon)^{q+1}}{u+u^q}, \frac{(u+1+\varepsilon)^{q+1}}{u+u^q}\}$ with $\omega = \omega'$.

It remains to prove that for these values of b there are no solutions with $\omega \neq \omega'$. This will require more discussion left to the reader.

5 Conclusion

In this paper, we have provided a direct and simpler proof of the APN-ness of Kasami Functions. This solves an open question raised by the first author at the conference WAIFI 2014, which remained unanswered during six years.

References

1. Beth; T. and Ding, C. On almost perfect nonlinear permutations. Proceedings of Eurocrypt' 93, Lecture Notes in Computer Science 765, pp. 65-76, 1994.
2. Carlet, C. Vectorial Boolean Functions for Cryptography, Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Crama, Y., Hammer, P., (eds), pp. 398-469, Cambridge University Press, 2010.
3. Carlet, C. Open Questions on nonlinearity and on APN Functions. Koç, Ç, Mesnager, S., Savas, E. (Eds.): WAIFI 2014, LNCS 9061, 83–107, Springer, 2015.
4. Carlet, C. and Ding, C. Highly Nonlinear Mappings. Special Issue "Complexity Issues in Coding and Cryptography", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, Journal of Complexity 20, pp. 205-244, 2004.
5. Cohen, S.D. and Matthews, R.W.: A class of exceptional polynomials. *Transactions of the American Mathematical Society*, 345:897 – 909, 1994.
6. Dillon, J.F. and Dobbertin, H.: New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, 10(3):342 – 389, 2004.
7. Dobbertin, H. Kasami power functions, permutation polynomials and cyclic difference sets. In: Proceedings of the NATO-A.S.I.Workshop Difference sets, sequences and their correlation properties, Bad Windsheim, Kluwer Verlag, pp. 133–158, 1998.
8. Dobbertin, H. Another proof of Kasami's Theorem. Des. Codes Crypt. 17, 177–180, 1999.
9. Helleseth, T. and Kholosha, A. $x^{2^l+1} + x + a$ and related affine polynomials over $\mathbb{F}_{2^k}$. Crypt. Commun. 2(1), 85–109, 2010.
10. Janwa, H. and Wilson, R. Hyperplane sections of Fermat varieties in P3 in char. 2 and some applications to cyclic codes. Proceedings of AAECC-10 Conference, pp. 139–152, 1998.
11. Kim, K.H., Choe, J., Mesnager, S. Solving $X^{q+1} + X + a = 0$ over finite fields *Cryptology ePrint Archive 2019 and arXiv:1912.12648.*
12. Kim, K.H., Mesnager, S. Solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $\gcd(n,k) = 1$. *Cryptology ePrint Archive 2019/307* (To appear in journal Finite Field ans their Applications).
13. Nyberg, K. Perfect non-linear S-boxes. *Proceedings of EUROCRYPT' 91, Lecture Notes in Computer Science* 547, pp. 378-386, 1992.

14. Nyberg, K. On the construction of highly nonlinear permutations. Proceedings of EUROCRYPT' 92, Lecture Notes in Computer Science 658, pp. 92–98, 1993.
15. Nyberg, K. Differentially uniform mappings for cryptography. Proceedings of EUROCRYPT' 93, Lecture Notes in Computer Science 765, pp. 55–64, 1994.
16. Nyberg, K. and Knudsen, L. R. Provable security against differential cryptanalysis. Proceedings of CRYPT0' 92, Lecture Notes in Computer Science 740, pp. 566-574, 1993.
17. Shannon, C.E. Communication theory of secrecy systems. *Bell system technical journal*, 28, pp. 656-715, 1949.