

On a conjecture on APN permutations

Daniele Bartoli* and Marco Timpanella†

Abstract

The single trivariate representation proposed in [C. Beierle, C. Carlet, G. Leander, L. Perrin, A Further Study of Quadratic APN Permutations in Dimension Nine, arXiv:2104.08008] of the two sporadic quadratic APN permutations in dimension 9 found by Beierle and Leander [4] is further investigated. In particular, using tools from algebraic geometry over finite fields, we prove that such a family does not contain any other APN permutation for larger dimensions.

Keywords: APN permutations, algebraic varieties, Lang-Weil bound.

1 Introduction

Vectorial Boolean functions play an important role in cryptography, as they are one of the key ingredients in the design of secure cryptographic primitives. In order for these primitives to resist to differential attacks [5], vectorial Boolean functions with strong properties must be employed. One of these properties has been captured in the definition of APN functions.

Definition 1.1. *A function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, n, m positive integers, is APN if for every $\alpha \in \mathbb{F}_2^n$, $\alpha \neq 0$, and $\beta \in \mathbb{F}_2^m$, the equation $F(x + \alpha) + F(x) = \beta$ has at most two solutions for $x \in \mathbb{F}_2^n$.*

Because of their applications, APN functions have been widely investigated; see for instance [1, 6, 8, 9, 11] and the survey [12]. In the design of symmetric primitives, APN functions are often required to be permutations. However, it seems that APN permutations are as rare as they are interesting, and very little is known about them. Up to CCZ-equivalence, all of the APN permutations known so far belong to a few families, namely:

1. APN monomial functions in odd dimension;
2. one infinite family of quadratic polynomials in odd dimension [7];

*Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Perugia, Italy. daniele.bartoli@unipg.it

†Dipartimento di Matematica e Fisica, Università degli Studi della Campania “Luigi Vanvitelli”, Caserta, Italy. marco.timpanella@unicampania.it

3. Dillon's permutation in dimension 6 [13];
4. two sporadic quadratic APN permutations in dimension 9 [4].

Note that only the first two items above are actually infinite families.

The example in [13] was found to be a particular case of a specific structure called "butterfly"; see [17]. Such a structure was later generalized, but unfortunately it was proved in [9] that it is impossible for a generalized butterfly to be APN unless it operates on 6 bits.

Very recently, the two sporadic quadratic permutations in dimension 9 obtained in [4] have been investigated in [3]. A single trivariate representation (up to EA-equivalence) of those two permutations as

$$C_u : \mathbb{F}_{2^m}^3 \rightarrow \mathbb{F}_{2^m}^3 \\ (x, y, z) \mapsto (x^3 + uy^2z, y^3 + uxz^2, z^3 + ux^2y)$$

was proposed.

In particular, for $m \geq 3$ being a multiple of 3 and $u \in \mathbb{F}_{2^m}$ not being a 7-th power, the authors of [3] found that the differential uniformity of C_u is bounded above by 8. Also, based on numerical experiments, they conjecture that C_u is not APN if m is greater than 3; see [3, Conjecture 1].

In this note, using a connection with algebraic surfaces over finite fields and an estimate on the number of \mathbb{F}_{2^m} -rational points related to the Lang-Weil bound, we prove that, when $m \geq 20$ is a multiple of 3 and $u \in \mathbb{F}_{2^m} \setminus \{0\}$ is not a 7-th power, the trivariate function C_u is not APN. As by [3, Remark 4] it was already observed that C_u is not APN for $m \in \{6, 9, 12, 15, 18\}$, our result proves the first statement in [3, Conjecture 1].

2 Connection with algebraic surfaces

In the following we let $q = 2^m$, where $m \geq 3$ is a multiple of 3. Proving that C_u is not APN is equivalent to showing that the homogeneous system

$$\begin{cases} \alpha x^2 + \alpha^2 x + u\gamma y^2 + u\beta^2 z = 0 \\ \beta y^2 + \beta^2 y + u\alpha z^2 + u\gamma^2 x = 0 \\ \gamma z^2 + \gamma^2 z + u\beta x^2 + u\alpha^2 y = 0 \end{cases} \quad (1)$$

has at least 4 solutions for a certain choice of $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$, $(\alpha, \beta, \gamma) \neq (0, 0, 0)$; see [3, Theorem 2]. As the authors point out in the proof of [3, Theorem 2], System (1) has at most 2 solutions if $\alpha\beta\gamma = 0$, and hence in the following we will assume $\alpha\beta\gamma \neq 0$. Also, we will consider $\alpha \neq u^2\beta^3/\gamma^2$.

Note that $(0, 0, 0)$ and (α, β, γ) are always solutions of System (1).

From the first equation of System (1),

$$z = \frac{\alpha x^2 + \alpha^2 x + u\gamma y^2}{u\beta^2},$$

and thus we obtain

$$\begin{cases} r_1(x, y) := \alpha^3 x^4 + \alpha^5 x^2 + u^2 \beta^4 \gamma^2 x + u^2 \alpha \gamma^2 y^4 + u \beta^5 y^2 + u \beta^6 y = 0 \\ r_2(x, y) := \alpha^2 \gamma x^4 + (\alpha^4 \gamma + u \alpha \beta^2 \gamma^2 + u^3 \beta^5) x^2 + u \alpha^2 \beta^2 \gamma^2 x \\ \quad + u^2 \gamma^3 y^4 + u^2 \beta^2 \gamma^3 y^2 + u^3 \alpha^2 \beta^4 y = 0. \end{cases} \quad (2)$$

Taking the linear combination $\gamma r_1(x, y) + \alpha r_2(x, y) = 0$, System (2) is equivalent to

$$\begin{cases} \alpha^3 x^4 + \alpha^5 x^2 + u^2 \beta^4 \gamma^2 x + u^2 \alpha \gamma^2 y^4 + u \beta^5 y^2 + u \beta^6 y = 0 \\ (\alpha^2 \gamma^2 + u^2 \alpha \beta^3) x^2 + (\alpha^3 \gamma^2 + u \beta^2 \gamma^3) x + (u \alpha \gamma^3 + \beta^3 \gamma) y^2 + (u^2 \alpha^3 \beta^2 + \beta^4 \gamma) y = 0. \end{cases} \quad (3)$$

Since $(\alpha^2 \gamma^2 + u^2 \alpha \beta^3) \neq 0$,

$$x^2 = \frac{(\alpha^3 \gamma^2 + u \beta^2 \gamma^3) x + (u \alpha \gamma^3 + \beta^3 \gamma) y^2 + (u^2 \alpha^3 \beta^2 + \beta^4 \gamma) y}{\alpha^2 \gamma^2 + u^2 \alpha \beta^3}, \quad (4)$$

and

$$\begin{aligned} x^4 &= \frac{(\alpha^3 \gamma^2 + u \beta^2 \gamma^3)^2 x^2 + (u \alpha \gamma^3 + \beta^3 \gamma)^2 y^4 + (u^2 \alpha^3 \beta^2 + \beta^4 \gamma)^2 y^2}{(\alpha^2 \gamma^2 + u^2 \alpha \beta^3)^2} \\ &= \frac{Ax + By^4 + Cy^2 + Dy}{(\alpha^2 \gamma^2 + u^2 \alpha \beta^3)^3}, \end{aligned} \quad (5)$$

where

$$\begin{aligned} A &= \gamma^6 (\alpha^3 + u \beta^2 \gamma)^3, \\ B &= \alpha \gamma^2 (\alpha \gamma^2 + u^2 \beta^3) (u \alpha \gamma^2 + \beta^3)^2, \\ C &= (\alpha^4 \gamma^2 + u^2 \alpha^3 \beta^3 + u \alpha \beta^2 \gamma^3 + \beta^5 \gamma) \cdot \\ &\quad \cdot (u^4 \alpha^4 \beta^4 + u \alpha^3 \gamma^5 + u^3 \alpha^2 \beta^3 \gamma^3 + \alpha^2 \beta^3 \gamma^3 + u^2 \alpha \beta^6 \gamma + u^2 \beta^2 \gamma^6), \\ D &= \gamma^4 \beta^2 (\alpha^3 + u \beta^2 \gamma)^2 (u^2 \alpha^3 + \beta^2 \gamma). \end{aligned}$$

Using (4) and (5) in System (3) reads

$$\begin{cases} u^3 \beta^6 \gamma^2 (u \alpha^7 + u^2 \alpha^4 \beta^2 \gamma + u \alpha^2 \beta \gamma^4 + u^3 \alpha \beta^4 \gamma^2 + u^5 \beta^7 + \gamma^7) x = Q(y) \\ (\alpha^2 \gamma^2 + u^2 \alpha \beta^3) x^2 + (\alpha^3 \gamma^2 + u \beta^2 \gamma^3) x + (u \alpha \gamma^3 + \beta^3 \gamma) y^2 + (u^2 \alpha^3 \beta^2 + \beta^4 \gamma) y = 0, \end{cases} \quad (6)$$

with

$$\begin{aligned} Q(y) &= (u+1)^2 (u^2 + u + 1)^2 \alpha \beta^6 \gamma^2 (\alpha \gamma^2 + u^2 \beta^3) y^4 + \beta^4 (u^4 \alpha^8 \gamma^2 + u^6 \alpha^7 \beta^3 + u^5 \alpha^5 \beta^2 \gamma^3 \\ &\quad + u^4 \alpha^4 \beta^5 \gamma + u \alpha^3 \beta \gamma^6 + u^3 \alpha^2 \beta^4 \gamma^4 + \alpha^2 \beta^4 \gamma^4 + u^5 \alpha \beta^7 \gamma^2 + u^2 \alpha \beta^7 \gamma^2 + u^3 \alpha \gamma^9 \\ &\quad + u^7 \beta^{10} + u^2 \beta^3 \gamma^7) y^2 + u \beta^6 (u^5 \alpha^7 \beta^2 + u^3 \alpha^4 \beta^4 \gamma + u^3 \alpha^3 \gamma^6 + \alpha^3 \gamma^6 + u^2 \alpha^2 \beta^3 \gamma^4 \\ &\quad + u^4 \alpha \beta^6 \gamma^2 + u^6 \beta^9 + u \beta^2 \gamma^7) y. \end{aligned}$$

Note that $H(\alpha, \beta, \gamma) := u\alpha^7 + u^2\alpha^4\beta^2\gamma + u\alpha^2\beta\gamma^4 + u^3\alpha\beta^4\gamma^2 + u^5\beta^7 + \gamma^7$ factorizes as

$$(\xi^5\beta + \xi\alpha + \gamma) \cdot (\xi^5\beta + \eta\xi\alpha + \eta^3\gamma) \cdot (\xi^5\beta + \eta^2\xi\alpha + \eta^6\gamma) \cdot (\xi^5\beta + \eta^2\xi\alpha + \eta^2\gamma) \cdot \\ (\xi^5\beta + \eta^4\xi\alpha + \eta^5\gamma) \cdot (\xi^5\beta + \eta^5\xi\alpha + \eta\gamma) \cdot (\xi^5\beta + \eta^6\xi\alpha + \eta^4\gamma),$$

where $\mathbb{F}_8^* = \langle \eta \rangle$ and $\xi = \sqrt[7]{u} \notin \mathbb{F}_q$, since u is not a 7-th power by assumption. Thus, there are no $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$, $(\alpha, \beta, \gamma) \neq (0, 0, 0)$ such that $H(\alpha, \beta, \gamma) = 0$.

Now, after taking the resultant of the two equations of System (6) and eliminating x , we are left with a polynomial in y of degree 8, namely

$$\bar{P}_{\alpha, \beta, \gamma}(y) = u\alpha\beta^{10}(\alpha\gamma^2 + u^2\beta^3)^3y(y + \beta)P_{\alpha, \beta, \gamma}(y),$$

where

$$P_{\alpha, \beta, \gamma}(y) = A_6y^6 + A_5y^5 + A_4y^4 + A_3y^3 + A_2y^2 + A_1y + A_0, \quad (7)$$

and

$$\begin{aligned} A_6 &= (u+1)^4(u^2+u+1)^4\alpha^2\beta^4\gamma^4, \\ A_5 &= (u+1)^4(u^2+u+1)^4\alpha^2\beta^5\gamma^4, \\ A_4 &= (u+1)^4(u^2+u+1)^4\alpha^2\beta^6\gamma^4, \\ A_3 &= (u+1)^4(u^2+u+1)^4\alpha^2\beta^7\gamma^4, \\ A_2 &= u^2(u^6\alpha^{14} + u^2\alpha^8\beta^4\gamma^2 + \alpha^4\beta^2\gamma^8 + u^8\alpha^3\beta^5\gamma^6 + u^2\alpha^3\beta^5\gamma^6 + u^{10}\alpha^2\beta^8\gamma^4 \\ &\quad + u^7\alpha\beta^4\gamma^9 + u\alpha\beta^4\gamma^9 + u^8\beta^{14}u^8 + u^9\beta^7\gamma^7 + u^3\beta^7\gamma^7 + u^4\gamma^{14}), \\ A_1 &= \beta A_2, \\ A_0 &= u^4(u+1)(u^2+u+1)\alpha^2\beta^3\gamma^4(u\alpha^7 + u^2\alpha^4\beta^2\gamma + u\alpha^2\beta\gamma^4 + u^3\alpha\beta^4\gamma^2 + u^5\beta^7 + \gamma^7). \end{aligned}$$

Note that $u^2+u+1 \neq 0$. Indeed, if m is odd and $u^2+u+1 = 0$ then $u \in \mathbb{F}_4$, a contradiction. On the other hand if m is even then $u^3 = 1$ and, by $3 \mid (2^m - 1)/7$, $u^{(2^m-1)/7} = 1$, a contradiction to our assumptions on u .

Remark 2.1. Observe that this approach also shows that C_u is a differentially d -uniform function with $d \leq 8$, as stated in [3, Theorem 2]. Indeed, the above computations prove that this is true if $\alpha \neq u^2\beta^3/\gamma^2$. On the other hand, assume that $\alpha = u^2\beta^3/\gamma^2$. Then the second equation of System (3) reads

$$u\gamma^2(u^5\beta^7 + \gamma^7)x + \beta(u^3\gamma^7y^2 + \gamma^7y^2 + u^8\beta^8y + \beta\gamma^7y) = 0,$$

where $u^5\beta^7 + \gamma^7 \neq 0$ as u is not a 7-th power. Thus, after eliminating x , System (3) is equivalent to

$$\begin{cases} x = \frac{\beta(u^3\gamma^7y^2 + \gamma^7y^2 + u^8\beta^8y + \beta\gamma^7y)}{u\gamma^2(u^5\beta^7 + \gamma^7)} \\ Q_1(y) = 0, \end{cases}$$

where

$$Q_1(y) = u^{10}\gamma^4\beta^{19}y \cdot (y + \beta) \cdot ((u + 1)^4(u^2 + u + 1)^4\beta^{10}\gamma^{28}(y^6 + \beta y^5 + \beta^2 y^4 + \beta^3 y^3) + u^2(u^5\beta^7 + \gamma^7)^2(u^{10}\beta^{14} + u^5\beta^7\gamma^7 + u^2\beta^7\gamma^7 + \gamma^{14})^2(y^2 + \beta y) + u^4(u + 1)(u^2 + u + 1)(u^5\beta^7 + \gamma^7)^3\beta^9\gamma^{14}).$$

As the degree of $Q_1(y)$ is 8, System (3) has at most 8 solutions if $\alpha = u^2\beta^3/\gamma^2$. Finally, if $\alpha\beta\gamma = 0$ System (3) has at most 2 solutions (see the first part of the proof of [3, Theorem 2]), and hence C_u is differentially d -uniform with $d \leq 8$.

As a polynomial in the variables α, β, γ, y , $P_{\alpha, \beta, \gamma}(y)$ defines a surface V of degree 16 embedded in the three-dimensional projective space $\text{PG}(3, \overline{\mathbb{F}}_2)$. Good references for a more comprehensive introduction to algebraic varieties and curves are [14, 15]. For a survey on the use of algebraic varieties over finite fields in polynomial problems, we refer to [2].

Recall that System (1) always possesses the solutions $(0, 0, 0)$ and (α, β, γ) . Therefore, in order to prove that C_u is not APN, it is enough to exhibit at least a choice of (α, β, γ) for which V has an \mathbb{F}_q -rational point not lying on $y = 0$ and $y = \beta$; see Theorem 2.5. To prove the existence of such a point, we use the following results.

The following is a particular case of [1, Lemma 2.1].

Proposition 2.2. *Let H be a plane of $\text{PG}(3, \overline{\mathbb{F}}_2)$ such that $V \cap H$ contains a non-repeated absolutely irreducible component defined over \mathbb{F}_q . Then V possesses a non-repeated absolutely irreducible component defined over \mathbb{F}_q .*

Proposition 2.3. *There exists an \mathbb{F}_q -rational component of V distinct from $y = 0$ and $y = \beta$.*

Proof. First note that $y = 0$ and $y = \beta$ are not components of V : it is enough to observe that $P_{\alpha, \beta, \gamma}(0)$ and $P_{\alpha, \beta, \gamma}(\beta)$ (seen as polynomials in α, β, γ, y) are not the zero polynomial (this is readily seen by a direct computation).

Consider now the curve \mathcal{C} defined as the intersection of V with the plane of equation $\gamma = 0$. By direct computation, this curve has homogeneous equation

$$u^8(\alpha^7 + u\beta^7)^2 y(y + \beta) = 0.$$

The component $y = 0$ is \mathbb{F}_q -rational, absolutely irreducible, and non-repeated. Then Proposition 2.2 yields the existence of an \mathbb{F}_q -rational component of V through the line $y = 0 = \gamma$, which is therefore distinct from both $y = 0$ and $y = \beta$. \square

To ensure the existence of a suitable \mathbb{F}_q -rational point of V , we report the following result.

Theorem 2.4. [10, Theorem 7.1] *Let $\mathcal{V} \subset \text{AG}(n, \mathbb{F}_q)$ be an absolutely irreducible variety defined over \mathbb{F}_q of dimension $r > 0$ and degree δ . If $q > 2(r + 1)\delta^2$, then the following estimate holds:*

$$|\#(\mathcal{V} \cap \text{AG}(n, \mathbb{F}_q)) - q^r| \leq (\delta - 1)(\delta - 2)q^{r-1/2} + 5\delta^{13/3}q^{r-1}.$$

Theorem 2.5. *If $m \geq 20$, C_u is not APN.*

Proof. By Proposition 2.3, the surface V contains an absolutely irreducible component W defined over \mathbb{F}_q of degree at most 16.

Since $m \geq 20$ the surface W contains at least $48q$ \mathbb{F}_q -rational points with $\gamma = 1$ (it is enough to apply Theorem 2.4 to the dehomogenization W_* of W with respect to γ).

Affine \mathbb{F}_q -rational points of V_* lying on $\alpha\beta y(y + \beta) = 0$ are contained in the three lines

$$\alpha = 0 = y, \quad \alpha = 0 = y + \beta, \quad \beta = 0 = y.$$

The intersection between V and $\alpha + u^2\beta^3 = 0$ is a degree-44 curve which has at most $44q + 1$ \mathbb{F}_q -rational points; see [16]. Therefore there exists at least an \mathbb{F}_q -rational point $(\bar{\alpha}, \bar{\beta}, 1, \bar{y})$ of V_* with $\bar{\alpha}\bar{\beta}\bar{y}(\bar{y} + \bar{\beta})(\bar{\alpha} + u^2\bar{\beta}^3) \neq 0$. This provides a root $\bar{y} \notin \{0, \bar{\beta}\}$ of $P_{\bar{\alpha}, \bar{\beta}, 1}(y)$ (see (7)), and so C_u is not APN. \square

Acknowledgements

The research of D. Bartoli and M. Timpanella was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The authors are grateful to C. Beierle, C. Carlet, G. Leander, and L. Perrin for a number of valuable comments on an earlier draft.

References

- [1] Y. Aubry, G. McGuire, F. Rodier, A few more functions that are not APN infinitely often, *Finite fields: theory and applications* **518**, 23–31 (2010).
- [2] D. Bartoli, Hasse-Weil type theorems and relevant classes of polynomial functions. In: *London Mathematical Society Lecture Note Series, Proceedings of 28th British Combinatorial Conference*, Cambridge University Press, to appear.
- [3] C. Beierle, C. Carlet, G. Leander, L. Perrin, A Further Study of Quadratic APN Permutations in Dimension Nine, arXiv:2104.08008, (2021).
- [4] C. Beierle, G. Leander, New instances of quadratic APN functions, arXiv:2009.07204, (2020).
- [5] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptol.* **4**(1), 3–72 (1991).
- [6] L. Budaghyan, M. Calderini, I. Villa, On equivalence between known families of quadratic APN functions, *Finite Fields Appl.* **66**, 101704 (2020).
- [7] L. Budaghyan, C. Carlet, G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, *IEEE Trans. Inf. Theory* **54**(9), 4218–4229 (2008).

- [8] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter, I. Villa, Constructing APN Functions Through Isotopic Shifts, *IEEE Trans. Inf. Theory* **66**, 5299–5309 (2020).
- [9] A. Canteaut, L. Perrin, and S. Tian, If a generalised butterfly is APN then it operates on 6 bits, *Cryptogr. Commun.* **11**, 1147–1164 (2019).
- [10] A. Cafure, G. Matera, Improved explicit estimates on the number of solutions of equations over a finite field, *Finite Fields Appl.* **12**, 155–185 (2006).
- [11] C. Carlet, K. H. Kim, S. Mesnager, A direct proof of APN-ness of the Kasami function, *Des. Codes Cryptogr.* **89**, 441–446 (2021).
- [12] M. Delgado, The state of the art on the conjecture of exceptional APN functions, *Note Mat.* **37**, 41–51 (2017).
- [13] K. Browning, J. F. Dillon, M. McQuistan, and A. J. Wolfe, An APN permutation in dimension six. In: *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications* **518**, American Mathematical Society, 33–42 (2010).
- [14] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, Springer-Verlag, New York (1977).
- [15] J. W. P. Hirschfeld, G. Korchmáros, F. Torres, *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton (2008).
- [16] M. Homma, S.J. Kim, Sziklai’s conjecture on the number of points of a plane curve over a finite field III, *Finite Fields Appl.* **16**, 315–319 (2010).
- [17] L. Perrin, A. Udovenko, A. Biryukov, Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. In M. Robshaw and J. Katz, editors, *Advances in Cryptology - CRYPTO 2016, Proceedings, Part II*, volume 9815 of LNCS, pages 93–122. Springer, 2016.