Counting and recovering the quadratic relations of a vectorial function

Irene Villa

University of Trento, Italy*

Abstract

A recent paper by Calderini et al. investigates the use of a CCZ transformation to mask the quadratic central map in a multivariate scheme, providing an instance leading to a system of degree four. A following paper by Caminata et al. presents two methods to reduce the masked system back to a quadratic system. In this work we further study the method based on the quadratic relations between input and output of the masked function, generalizing it and applying to any CCZ transformation (of any quadratic map). Moreover, we study how the existence of these quadratic relations can be used to study whether a function can be CCZ equivalent to a quadratic map and, more generally, to study whether two functions can be CCZ equivalent. In fact, this analysis gives us necessary conditions that can be checked also in relatively large dimensions. Particularly, we completely analyse the cases of vectorial Boolean functions with 1 and 2 output bits.

Key Words : Vectorial Functions, CCZ Equivalence, Quadratic Relations, Multivariate Cryptography.

1 Introduction

The idea behind multivariate cryptography is to construct a system of equations, over a finite field, possessing some hidden structure such that only the legitimate user is able to invert the system, that is to find a preimage (or all the preimages) of a given output. A classical technique used is to start from a quadratic system feasible to invert, and then apply two random affine invertible transformations to the input and to the output of the system, leading to a random-looking quadratic system that is difficult to invert. A recent work [4] studies the use of a more general transformation in order to hide the structure of the system: the so-called *CCZ transformation*. In [4], the authors propose to start from a quadratic system with a specific structure, using the so-called Oil-and-Vinegar polynomials, and apply a random transformation (belonging to a subclass of the CCZ transformations), leading to a system of degree (at most) four. The authors of a following work [5] show that for the specific instance proposed, the CCZ

*irene.villa[at]unitn[dot]it

transformation does not offer additional security since an attacker can easily recover a system of quadratic equations describing the scheme. Another work [1] attacks the proposal in [4] with a specific choice of parameters, recovering an equivalent key and so breaking the system.

In this work, we generalize the technique used in [5] based on the so-called *quadratic relations*, and prove its effectiveness on a generic instance of CCZ transformation from a generic quadratic system. Interestingly, the study of quadratic relations offers insight into another problem investigated in the context of vectorial functions: given a function between two finite fields, determine whether it is CCZ equivalent to a quadratic function. This problem has been already studied, see for example the work of Edel and Pott [8] restricted to the class of APN functions. In this work, we derive some necessary conditions for a function to be CCZ equivalent to a quadratic map, and, more generally, some necessary conditions for two functions to be CCZ equivalent. Moreover, we completely study the case of vectorial Boolean functions, so defined over fields of even characteristic, with 1 or 2 bits in output.

1.1 Preliminaries

Fixed a finite field $\mathbb{F}_q$, namely the finite field with $q = p^\kappa$ elements for p a prime number, and given two positive integers n and m, we refer to a map $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ as an (n, m)-vectorial function, or simply as an (n, m)-function. Notice that the function F can be described in terms of m $(n, 1)$-functions $f_1, \ldots, f_m$, which are called the *coordinate functions* of F, where $F(z) = [f_1(z), \ldots, f_m(z)]$ for $z \in \mathbb{F}_q^n$. The *component functions* of F are the $(n, 1)$-functions obtained as (nonzero) linear combinations of its coordinate functions. With $\mathbf{0}_m$ we denote the constant zero (n, m)-function.

An $(n, 1)$-function f can be uniquely represented as a multivariate polynomial in n variables over $\mathbb{F}_q$ of the form

$$f(z) = \sum_{\substack{v=(v_1,\ldots,v_n) \\ 0 \le v_i < q}} a_v z_1^{v_1} \cdots z_n^{v_n}, \quad a_v \in \mathbb{F}_q,$$

where with abuse of notation we identify with z the n variables $z_1, \ldots, z_n$. In the following, we will do similar identifications with the variables $w = (w_1, \ldots, w_m)$, $x = (x_1, \ldots, x_t)$, and $y = (y_1, \ldots, y_{n-t})$. The *algebraic degree* of f is then defined as $\deg(f) = \max\{\sum_{i=1}^n v_i \mid a_v \neq 0\}$. Thus, an (n, m)-vectorial function F can be uniquely represented as a collection of m multivariate polynomials in n variables, where the variables appear in degree at most $q - 1$, and its algebraic degree is defined as $\deg(F) = \max\{\deg(f_1), \ldots, \deg(f_n)\}$. In the subsequent sections, we often identify vectorial functions with system of such multivariate polynomials. When $m = n$, the function admits an equivalent representation as a univariate polynomial over $\mathbb{F}_{q^n}$ of degree at most $q^n - 1$.

Given two (n, m)-functions F and G, we say that they are *affine equivalent* if there exist an affine invertible map A_1 of $\mathbb{F}_q^m$ and an affine invertible map A_2 of $\mathbb{F}_q^n$ such that $G = A_1 \circ F \circ A_2$. They are *extended affine equivalent* (shortly EA equivalent) if there exists an (n, m)-affine map A such that $F + A$ is affine equivalent to G. They are called *CCZ equivalent* if there exists an affine invertible map $\mathcal{A}$ of $\mathbb{F}_q^n \times \mathbb{F}_q^m$ such that $\mathcal{A}(\Gamma_F) = \Gamma_G$, where $\Gamma_F = \{(z, F(z)) : z \in \mathbb{F}_q^n\}$ and $\Gamma_G = \{(z, G(z)) : z \in \mathbb{F}_q^n\}$ are the graphs of F and

G respectively. We call affine, EA, and CCZ transformations the operations performed in order to obtain respectively an affine, EA, and CCZ equivalent function. The affine equivalence is a particular case of the EA equivalence, which is itself a particular case of the CCZ equivalence. Affine and EA transformations preserve the algebraic degree of the function, except when the starting function is affine in the case of EA equivalence, whereas the CCZ transformation might lead to a function of different degree. A function is called *CCZ quadratic* if it is CCZ equivalent to a quadratic function, where a quadratic function is of algebraic degree 2.

A particular case of CCZ transformation is the *twisting*, introduced in [6]. Given an integer t with $0 \leq t \leq \min(n, m)$, two (n, m)-functions F and G are equivalent via a t-twist if $\Gamma_G = M_t(\Gamma_F)$, where M_t is the linear invertible map operating as follows: $(x, y, u, v) \mapsto (u, y, x, v)$, with $x \in \mathbb{F}_q^t, y \in \mathbb{F}_q^{n-t}, u \in \mathbb{F}_q^t, v \in \mathbb{F}_q^{m-t}$. This transformation is *admissibile*, i.e. $M_t(\Gamma_F)$ is the graph of a function, if there exist two functions $T : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t$ and $U : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^{m-t}$ such that for every fixed $y \in \mathbb{F}_q^{n-t}$ the function $T(x, y)$ is invertible with respect to $x \in \mathbb{F}_q^t$, and denoting $T_y^{-1}(x)$ the inverse function, we have

$$F(x, y) = \begin{bmatrix} T(x, y) \\ U(x, y) \end{bmatrix}, \text{ and } G(x, y) = \begin{bmatrix} T_y^{-1}(x) \\ U(T_y^{-1}(x), y) \end{bmatrix}. \tag{1}$$

Canteaut and Perrin in [6] showed that, over $\mathbb{F}_q = \mathbb{F}_2$, any CCZ transformation can be described in terms of a twist and two EA transformations, result that can be generalized to functions over any finite field, see Theorem 1 in the following section.

To conclude, we define a quadratic relation for a vectorial function.

Definition 1. *Given an (n, m)-function F, a* quadratic relation *for F is a quadratic $(n + m, 1)$-function $\mathcal{R} : \mathbb{F}_q^n \times \mathbb{F}_q^m \to \mathbb{F}_q$, thus $\mathcal{R}(z, w)$ is of the form*

$$\sum_{1 \leq i \leq j \leq n} \alpha_{ij} z_i z_j + \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \beta_{ij} z_i w_j + \sum_{1 \leq i \leq j \leq m} \gamma_{ij} w_i w_j + \sum_{1 \leq i \leq n} \delta_i z_i + \sum_{1 \leq i \leq m} \zeta_i w_i + \varepsilon,$$

such that for any $\bar{z} \in \mathbb{F}_q^n$ it holds that $\mathcal{R}(\bar{z}, F(\bar{z})) = 0$. We equivalently say that F satisfies *$\mathcal{R}$, and we denote with θ_F the number of linearly independent quadratic relations that F satisfies.*

Remark 1. *If the polynomials are defined over $\mathbb{F}_2$, then we can assume $\alpha_{ii} = \gamma_{jj} = 0$, for $i = 1, \ldots, n$ and $j = 1, \ldots, m$.*

2 The characterization of CCZ-equivalence by the twistings for generic finite fields

What follows in this section is entirely based on the work of Canteaut and Perrin in [6], in which the authors consider the finite field $\mathbb{F}_2$. Precisely, it shows how their work can be extended to functions on generic finite fields, leading to the following theorem.

Theorem 1. *For a finite field $\mathbb{F}$, let $F : \mathbb{F}^n \to \mathbb{F}^m$ and $G : \mathbb{F}^n \to \mathbb{F}^m$ be two CCZ equivalent functions. Then we can obtain G from F (and vice-versa) by*

composing an EA transformation, a t-twist and an EA transformation, for some integer t with $0 \leq t \leq \min(n, m)$.

The proof presented in [6] almost directly adapt to the generic case of a finite field $\mathbb{F} = \mathbb{F}_q$, with q power of some prime number p. There are some details that one has to take care of to adjust the proof. For completeness we report them here.

First, let us recall some definitions. With $\cdot$ we denote some non-degenerate symmetric bilinear form for a vector space over $\mathbb{F}_q$ (often called "inner product"). With abuse of notation, we use the same symbol for the inner product over $\mathbb{F}_q^n$, over $\mathbb{F}_q^m$ and over $\mathbb{F}_q^n \times \mathbb{F}_q^m$. Thus, the Walsh transform of F, for $(a, b) \in \mathbb{F}_q^n \times \mathbb{F}_q^m$, has the following form

$$\mathcal{W}_F(a, b) = \sum_{z \in \mathbb{F}_q^n} \zeta^{tr(b \cdot F(z) + a \cdot z)} = \sum_{z \in \mathbb{F}_q^n} \zeta^{tr((a,b) \cdot (z, F(z)))},$$

where ζ is a primitive complex p-root of unity and tr denotes the trace map $tr : \mathbb{F}_q \to \mathbb{F}_p$. Set $\mathcal{V} = \mathbb{F}_q^n \times \{0\} \subset \mathbb{F}_q^n \times \mathbb{F}_q^m$.

Lemma 1. *Given $\mathcal{A}$ an affine bijection of $\mathbb{F}_q^n \times \mathbb{F}_q^m$ and F an (n, m)-function, set $\mathcal{L}$ the linear part of $\mathcal{A}$, that is $\mathcal{A}(z, w) = \mathcal{L}(z, w) + c$, $c \in \mathbb{F}_q^{n+m}$, and $\mathcal{Z}_F$ the Walsh zeroes of F, that is $\mathcal{Z}_F = \{(a, b) \in \mathbb{F}_q^n \times \mathbb{F}_q^m \mid \mathcal{W}_F(a, b) = 0\} \cup \{(0, 0)\} \subseteq \mathbb{F}_q^n \times \mathbb{F}_q^m$. Then $\mathcal{A}$ is admissible for F if and only if $\mathcal{L}^T(\mathcal{V}) \subseteq \mathcal{Z}_F$, where $\mathcal{L}^T$ is the linear adjoint operator of $\mathcal{L}$.*

Proof. Set $\mathcal{A}(z, w) = (\mathcal{A}_1(z, w), \mathcal{A}_2(z, w)) = \mathcal{L}(z, w) + c = (\mathcal{L}_1(z, w), \mathcal{L}_2(z, w)) + c$. $\mathcal{A}$ is admissible for F if and only if $F_1(z) = \mathcal{A}_1(z, F(z))$ is a bijection of $\mathbb{F}_q^n$, in which case we have $\mathcal{A}(\Gamma_F) = \Gamma_G$ with $G(z) = F_2 \circ F_1^{-1}(z)$ and $F_2(z) = \mathcal{A}_2(z, F(z))$. This is equivalent to $\mathcal{L}_1(z, F(z))$ being a permutation, that is having all its (nonzero) components balanced.

Recall that an $(n, 1)$-function f is balanced if and only if $\mathcal{W}_f(0, \alpha) = 0$ for every $\alpha \in \mathbb{F}_q^*$, see for example [9, Corollary 1]. Therefore, $\mathcal{L}_1(z, F(z))$ is balanced if and only if for every nonzero $a \in \mathbb{F}_q^n$ we have $\sum_{z \in \mathbb{F}_q^n} \zeta^{tr(a \cdot \mathcal{L}_1(z, F(z)))} = 0$. Since we have the following equivalences

$$\sum_{z \in \mathbb{F}_q^n} \zeta^{tr(a \cdot \mathcal{L}_1(z, F(z)))} = \sum_{z \in \mathbb{F}_q^n} \zeta^{tr((a,0) \cdot \mathcal{L}(z, F(z)))} = \sum_{z \in \mathbb{F}_q^n} \zeta^{tr(\mathcal{L}^T(a,0) \cdot (z, F(z)))}$$

it holds that $\mathcal{A}$ is admissible if and only if $\mathcal{L}^T(a, 0) \in \mathcal{Z}_F$ for every nonzero $a \in \mathbb{F}_q^n$, that is if and only if $\mathcal{L}^T(\mathcal{V}) \subseteq \mathcal{Z}_F$. □

The remaining part of the proof is a direct adaptation of the analysis presented in [6]. To ease the reading, we report the main steps of the proof, together with some needed definitions, and we refer the reader to [6] for the missing proofs.

Given V a vector subspace of $\mathbb{F}_q^n \times \mathbb{F}_q^m$, the *thickness* of V is defined as the dimension of the projection of V on $\mathcal{V}^\perp$, denoted as $t(V)$. An EL-mapping (*extended linear mapping*) of $\mathbb{F}_q^n \times \mathbb{F}_q^m$ is a linear permutation whose matrix representation has the form $\begin{bmatrix} \phi & 0 \\ \psi & \varphi \end{bmatrix}$, where ϕ is a linear permutation of $\mathbb{F}_q^n$, φ is a linear permutation of $\mathbb{F}_q^m$, and ψ is an (n, m)-linear function.

Lemma 2. *Given $\mathcal{L}$ a linear permutation of $\mathbb{F}_q^n \times \mathbb{F}_q^m$, $V = \mathcal{L}(\mathcal{V})$, then $V = (\Lambda^T M_t)(\mathcal{V})$, for $t = t(V) \leq \min(n, m)$ and Λ some EL-mapping of $\mathbb{F}_q^n \times \mathbb{F}_q^m$.*

Lemma 3. *Consider F, G, G' (n, m)-functions CCZ equivalent, so $\Gamma_G = \mathcal{A}(\Gamma_F)$ and $\Gamma_{G'} = \mathcal{A}'(\Gamma_F)$. Consider the linear parts of the affine permutations $\mathcal{L}, \mathcal{L}'$, and assume that $\mathcal{L}^T(\mathcal{V}) = \mathcal{L}'^T(\mathcal{V})$. Then G and G' are EA-equivalent.*

Consider now $F, G : \mathbb{F}_q^n \to \mathbb{F}_q^m$ CCZ equivalent maps, with $\Gamma_G = \mathcal{A}(\Gamma_F)$. This implies $\mathcal{L}^T(\mathcal{V}) \subseteq \mathcal{Z}_F$, where $\mathcal{L}$ is the linear part of $\mathcal{A}$. From the previous results, we know that there exist an integer $t \leq \min(n, m)$ and an EL-mapping Λ such that $\mathcal{L}^T(\mathcal{V}) = (\Lambda^T M_t)(\mathcal{V})$. Therefore $\mathcal{L}' = (\Lambda^T M_t)^T = M_t \Lambda$ is an admissible mapping for F, thus there exists a function G' such that $\Gamma_{G'} = (M_t \Lambda)(\Gamma_F)$. Hence, we have that G and G' are EA equivalent, so there exists an EA transformation A such that $\Gamma_G = A(\Gamma_{G'})$, implying that $\Gamma_G = (A \circ M_t \circ \Lambda)(\Gamma_F)$. Finally, we obtained the desired result: two CCZ-equivalent functions can be obtained by composing an EA transformation, a t-twist and an EA transformation.

3 The invariance of the existence of quadratic relations

Assume to have a vectorial function possessing some quadratic relations. We want to study how these relations are modified when we apply a CCZ transformation to the function.

We start by first considering an affine transformation. Assume that $F, F' : \mathbb{F}_q^n \to \mathbb{F}_q^m$ are two affine equivalent functions. So $F' = A_1 \circ F \circ A_2$ for A_1, A_2 affine bijections of $\mathbb{F}_q^m$, $\mathbb{F}_q^n$ respectively. Moreover, assume that F possesses N quadratic relations $\mathcal{R}_\ell$, for $1 \leq \ell \leq N$, over $\mathbb{F}_q$ of the form

$$\sum_{1 \leq i \leq j \leq n} \alpha_{ij}^{(\ell)} z_i z_j + \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \beta_{ij}^{(\ell)} z_i w_j + \sum_{1 \leq i \leq j \leq m} \gamma_{ij}^{(\ell)} w_i w_j + \sum_{1 \leq i \leq n} \delta_i^{(\ell)} z_i + \sum_{1 \leq i \leq m} \zeta_i^{(\ell)} w_i + \varepsilon^{(\ell)}.$$

By replacing $z \mapsto A_2(z)$ and $w \mapsto A_1^{-1}(w)$, we obtain N quadratic relations for F'. Moreover, since A_1 and A_2 are affine invertible maps, if the relations for F are linearly independent, the same holds for F'. Indeed, since we can divide the action of an affine invertible transformation into steps which modify one variable at the time, we can directly consider, without loss of generality, the single transformation $z_1 \mapsto u z_1 + u_2 z_2 + \cdots + u_n z_n + c = u z_1 + \phi(\bar{z}) + c$, with $u \neq 0$. The above relation transforms into the following

$$\begin{aligned}
\mathcal{R}'_\ell =& \alpha_{11}^{(\ell)} (u z_1 + \phi(\bar{z}) + c)^2 + \sum_{2 \leq j \leq n} \alpha_{1j}^{(\ell)} (u z_1 + \phi(\bar{z}) + c) z_j + \sum_{2 \leq i \leq j \leq n} \alpha_{ij}^{(\ell)} z_i z_j \\
&+ \sum_{1 \leq j \leq m} \beta_{1j}^{(\ell)} (u z_1 + \phi(\bar{z}) + c) w_j + \sum_{\substack{2 \leq i \leq n \\ 1 \leq j \leq m}} \beta_{ij}^{(\ell)} z_i w_j + \sum_{1 \leq i \leq j \leq m} \gamma_{ij}^{(\ell)} w_i w_j \\
&+ \delta_1^{(\ell)} (u z_1 + \phi(\bar{z}) + c) + \sum_{2 \leq i \leq n} \delta_i^{(\ell)} z_i + \sum_{1 \leq i \leq m} \zeta_i^{(\ell)} w_i + \varepsilon^{(\ell)}.
\end{aligned}$$

Suppose they are not linearly independent, so there exists $\lambda \in \mathbb{F}_q^N$ such that $\lambda \cdot [\mathcal{R}'_\ell]_{\ell=1}^N$ is constantly zero. To ease the notation, let us denote the corresponding coefficients as $\alpha_{ij} = \lambda \cdot [\alpha_{ij}^{(\ell)}]_{\ell=1}^N$, $\beta_{ij} = \lambda \cdot [\beta_{ij}^{(\ell)}]_{\ell=1}^N$, and so on. Then the coefficient of z_1^2 must to be zero, that is $u^2\alpha_{11} = 0$, and so $\alpha_{11} = 0$. This implies that the coefficient for $z_1 z_j$, for $j = 2, \ldots, n$, is $u\alpha_{1j}$, which must then be zero. By continuing with this reasoning, we obtain that all the coefficients in the linear combinations are zero, and so also the quadratic relations for F are linearly dependent.

To study the extended affine transformation, we are left with considering the simple addition of an affine map, so we consider two functions F, F' such that $F' = F + A$. Following the previous analysis, in the quadratic relations of F we need to replace $w \mapsto w - A(z)$. Therefore, we still have N quadratic relations for F'. Denoting $A_i(z)$ the i-th coordinate function of $A(z)$, the relations for F' have the following form

$$\begin{aligned}\mathcal{R}'_\ell = &\sum_{1\le i\le j\le m} \gamma_{ij}^{(\ell)}(w_i - A_i(z))(w_j - A_j(z)) + \sum_{\substack{1\le i\le n\\ 1\le j\le m}} \beta_{ij}^{(\ell)} z_i (w_j - A_j(z)) \\ &+ \sum_{1\le i\le j\le n} \alpha_{ij}^{(\ell)} z_i z_j + \sum_{1\le i\le n} \delta_i^{(\ell)} z_i + \sum_{1\le i\le m} \zeta_i^{(\ell)}(w_i - A_i(z)) + \varepsilon^{(\ell)},\end{aligned}$$

for $1 \le \ell \le N$. Suppose that they are linearly dependent, thus there exists a nonzero $\lambda \in \mathbb{F}_q^N$ such that $\lambda \cdot [\mathcal{R}'_\ell]_{\ell=1}^N$ is constantly zero. As before, we simplify the notation of the coefficients by denoting them as α_{ij}, β_{ij} and so on.

Hence we have that the coefficients γ_{ij} are all zero, because of the presence of the terms $w_i w_j$, implying that also the coefficients β_{ij} and δ_i are zero, because of the presence of the terms $z_i w_j$ and w_i respectively. Similarly, it follows that also the remaining coefficients are zero. This implies that also the quadratic relations for F are linearly dependent.

To conclude this analysis, given the characterisation of the CCZ transformation by means of EA transformations and twist, we are left with the case of two functions equivalent via a twist. Set therefore $F, G : \mathbb{F}_q^n \to \mathbb{F}_q^m$ and t, with $0 < t \le \min(n, m)$, such that F and G are of the form as specified in (1). Without loss of generality, we have that F possesses some quadratic relation $\mathcal{R}_F(z, w) = \mathcal{R}_F(x, y, u, v)$, where $z = (x, y)$ and $w = (u, v)$. Since in the t-twist we are swapping the role of x and u, it means that G possesses the quadratic relation $\mathcal{R}_G(z, w) = \mathcal{R}_F(u, y, x, v)$. Therefore, we have that the action of a twist send a set of linearly independent quadratic relations to a set of linearly independent quadratic relations. Therefore, we can state the following theorem.

Theorem 2. *The number of linearly independent quadratic relations for a vectorial function is invariant under the action of a CCZ transformation.*

4 Application to multivariate cryptography

As already mentioned, in this work we extend the result showed in [5] by applying it to a more generic situation.

We assume to have a multivariate cryptosystem in which the secret central quadratic map $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is masked via the action of a (random) CCZ

transformation into the public map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$. No further assumptions are made on the form of F or on the form of the CCZ transformation used. Assumed that we intercept a value $c \in \mathbb{F}_q^m$, we will refer to it as the *target output*, and we want to recover its preimage(s) with respect to $\mathcal{P}$ (namely the *target input(s)*).

Set $f_1, \ldots, f_m$ to be the coordinate functions of F, then F possesses (at least) m linearly independent quadratic relations of the form

$$\{f_i(z_1, \ldots, z_n) - w_i\}_{i=1}^m.$$

From the result of Theorem 2, we have that also $\mathcal{P}$ possesses (at least) m linearly independent quadratic relations.

Proposition 1. *Consider n, m positive integers, $\mathbb{F}_q$ a finite field, $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ a quadratic map and $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ CCZ equivalent to F. Then $\mathcal{P}$ possesses (at least) m linearly independent quadratic relations.*

Following the idea of the linearization attack (used by Patarin in [11] to break the Matsumoto-Imai cryptosystem [10]), and following its adaptation proposed in [5], an attacker can perform the following steps. First, recover the quadratic relations of $\mathcal{P}$ by solving the linear system obtained by considering enough input-output pairs of $\mathcal{P}$. Since a quadratic relation $\mathcal{R}(z, w)$ has the form

$$\sum_{1 \le i,j \le n} \alpha_{ij} z_i z_j + \sum_{\substack{1 \le i \le n \\ 1 \le j \le m}} \beta_{ij} z_i w_j + \sum_{1 \le i,j \le m} \gamma_{ij} z_i z_j + \sum_{1 \le i \le n} \delta_i z_i + \sum_{1 \le i \le m} \zeta_i w_i + \varepsilon,$$

in order to recover its coefficients we need to compute about $\binom{n+m+2}{2}$ input/output pairs and then perform Gaussian elimination on a matrix of approximately the same size. Once (at least) m linearly independent quadratic relations are recovered, since we did not assume any particular structure on the central quadratic system, we simply take the target output, evaluate it in the quadratic relations and obtain a system of quadratic polynomials in n variables. Thus, for each target output, we can reconstruct a quadratic system containing the target input as a solution.

Remark 2. *This applies also to the case in which the central map F is not quadratic but it is CCZ quadratic. Indeed, the public system $\mathcal{P}$ is still CCZ equivalent to some quadratic map, and thus all previous analysis applies.*

To conclude, we report the analysis regarding the computational cost for recovering the quadratic relations and then the quadratic system for the target output. The proof is an adaptation of the proof of Theorem 2 in [5].

Theorem 3. *For a finite field $\mathbb{F}_q$ and two positive integers n, m, consider a vectorial function $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ of degree $d < n$, such that $\mathcal{P}$ is CCZ quadratic. From the equations of $\mathcal{P}$ and from a fixed $c \in \mathbb{F}_q^m$, we can produce:*

1. *a system of quadratic relations for $\mathcal{P}$ with complexity $\mathcal{O}(\max\{mn^{d+2}, m^3 n^d, m^6, n^6\})$;*
2. *a quadratic system with the same solution as $\mathcal{P}(z) = c$ with additional negligible complexity.*

Proof. Notice that we can assume the public system $\mathcal{P}$ of degree $d \geq 3$.
1. In order to produce the quadratic relations, we need to perform these steps:
a) computing around $\binom{n+m+2}{2}$ random evaluation of the public system and
b) performing Gaussian elimination on the corresponding matrix to recover the coefficients of the quadratic relations.
The complexity of evaluating the public system at a single chosen input is $\mathcal{O}(m\binom{n+d}{d})$, since we have m equations of degree d in n variables. This has to be done about $\binom{n+m+2}{2}$ times, in order to produce the system to be solved. The complexity of solving the linear system of approximate size $\binom{n+m+2}{2}$ is $\mathcal{O}(\binom{n+m+2}{2}^3)$. Therefore, the complexity of this method is $\mathcal{O}(m\binom{n+d}{d}\binom{n+m+2}{2} + \binom{n+m+2}{2}^3) = \mathcal{O}(mn^{d+2} + m^3n^d + m^6 + n^6)$.
2. To produce the desired quadratic system, we evaluate the output variables at c. Hence, we evaluate $\binom{m+2}{2} + mn$ terms. The complexity of this final operation is $\mathcal{O}(m\binom{m+2}{2} + m^2n) = \mathcal{O}(m^3 + m^2n)$. □

To have a manageable public key in the multivariate scheme, the degree d of the public system should not be too large. Thus, if we assume to have $n \geq m$, for small degrees d we have the complexities given in Table 1.

d	$\mathcal{O}(\max\{mn^{d+2}, m^3n^d, m^6, n^6\})$
3	$\mathcal{O}(n^6)$
4	$\mathcal{O}(mn^6)$
5	$\mathcal{O}(mn^7)$

Table 1: Complexity in Theorem 3 for $n \geq m$ and $3 \leq d \leq 5$

5 Application to a problem in vectorial functions

Among the possible interesting analysis that can be performed on vectorial functions, their classification up to some equivalence notion is a well-studied problem that it is still far from being solved. For example, in the case of vectorial Boolean functions ($q = 2$, $m = n$) the classification up to CCZ equivalence is complete only for $n \leq 4$, see [2]. Determining whether a given function is CCZ equivalent to some other function, is in general not an easy task. Computationally, this is solved in the general case by considering the linear codes generated by the functions and then checking via code equivalence, see [3]. This results in a heavy computational work, which might be already challenging in dimension $n = 12$. Therefore, especially in large dimensions, researchers make use of CCZ invariants, properties that are preserved by a CCZ transformation, to check if two functions are potentially CCZ equivalent. Thus, Theorem 2 provides us a further CCZ invariant that can be used, namely the number of linearly independent quadratic relations satisfied.

Sometimes it is interesting to study whether a function is CCZ equivalent to a quadratic map, that is if it is CCZ quadratic. This question is particularly relevant in the area of cryptographic Boolean functions, where many interesting

properties are invariant under the CCZ transformation and quadratic functions are relatively easy to study, but they might suffer from some weaknesses. This question has been already addressed in [8], where some necessary conditions have been determined for the restricted class of APN functions. In the mentioned work, the authors show that if an APN function is CCZ equivalent to a quadratic map, then the group of authomorphisms of a particular design over $\mathbb{F}_2^n \times \mathbb{F}_2^n$ associated to the function must contain an elementary abelian group of order 2^{3n}.

In this section, we use the technique of quadratic relations to determine whether a function is potentially equivalent to a quadratic map. Indeed, Proposition 1 implies the following result.

Corollary 1. *If a vectorial function $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ does not possess at least m linearly independent quadratic relations, then F is not CCZ quadratic.*

Remark 3. *As reported in Theorem 3, the complexity of computing the number of linearly independent quadratic relations is $\mathcal{O}(\max\{mn^{d+2}, m^3n^d, m^6, n^6\})$, where d is the algebraic degree of the function.*

Before presenting computational results that illustrate the potential of this approach, we first carry out further analyses, which in certain cases leads to improved outcomes. First we will consider the quadratic relations obtained from the affine components of a vectorial function. Then we will restrict to the Boolean case and study the quadratic relations of quadratic vectorial Boolean functions with small output space.

5.1 The quadratic relations of the affine components

Assume that a function $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ has some components of degree at most 1, which we simply referred to as affine components. Possessing affine components is CCZ invariant, thus EA invariant and so, up to adding an affine vectorial function, we can directly consider constant zero components, and these components form a vector subspace of some dimension $k \leq m$. Without loss of generality, assume that the first k coordinates of F are zero, that is $F = \begin{bmatrix} \mathbf{0}_k \\ G \end{bmatrix}$, with G an $(n, m-k)$-function. Hence F satisfies the following relations, which are linearly independent quadratic relations:

$$\{w_j = 0\}_{j=1,\dots,k}, \quad \{w_j \cdot w_i = 0\}_{j=1,\dots,k}^{i=j,\dots,m}, \quad \{w_j \cdot z_i = 0\}_{j=1,\dots,k}^{i=1,\dots,n}.$$

Thus it holds

$$\theta_F \geq k + km + k - \frac{k(k+1)}{2} + kn = k(n+m+2) - \frac{k(k+1)}{2}.$$

Notice that if we are over $\mathbb{F}_q = \mathbb{F}_2$, we exclude the relations w_j^2, for $j = 1, \dots, k$, obtaining $\theta_F \geq k + km - \frac{k(k+1)}{2} + kn = k(n+m+1) - \frac{k(k+1)}{2}$.

Proposition 2. *Given $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ a vectorial function with $q^k - 1$ affine components, up to EA transformation, let us write F as $F = \begin{bmatrix} \mathbf{0}_k \\ G \end{bmatrix}$, with $G : \mathbb{F}_q^n \to \mathbb{F}_q^{m-k}$. Then $\theta_F = \theta_G + \lambda$, with*

$$\lambda = \begin{cases} k(n+m+1) - \frac{k(k+1)}{2}, & \text{if } q = 2, \\ k(n+m+2) - \frac{k(k+1)}{2}, & \text{otherwise.} \end{cases}$$

Proof. To prove this, notice that the quadratic relations related to the constant zero components cover all terms involving w_j, for $j \leq k$. Therefore, up to this set of relations, any quadratic relations for F can be seen as a relation not involving w_j, for $j \leq k$, thus a relation for G. Therefore $\theta_F = \theta_G + \lambda$. □

Corollary 2. *A CCZ quadratic vectorial function $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ with $q^k - 1$ affine components possesses at least*

$$\begin{cases} k(n+m) - \frac{k(k+1)}{2} + m, & \text{if } q = 2 \\ k(n+m+1) - \frac{k(k+1)}{2} + m, & \text{otherwise} \end{cases}$$

linearly independent quadratic relations.

Proof. Up to CCZ transformation, we can assume G quadratic. Therefore, $\theta_G \geq m - k$ and so we obtain the final formula. □

5.2 The quadratic relations of a quadratic vectorial Boolean function

To further study the case in which a vectorial function can be CCZ quadratic, it can help to study the number of quadratic relations that a quadratic function satisfies. Indeed, if for fixed n, m, we are able to identify the set $\Delta = \{\theta_F : F \text{ quadratic } (n,m)\text{-function}\}$, then we know that, given $G : \mathbb{F}_q^n \to \mathbb{F}_q^m$, whenever $\theta_G \notin \Delta$, then G is not CCZ quadratic.

In this section, we restrict ourselves to the binary case and we start with small values of m. Moreover, given the analysis in the previous section, we restrict to consider a quadratic vectorial Boolean function without affine components.

If $m = 1$, then we know that a quadratic Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is EA equivalent to

$$z_1 z_2 + \cdots + z_{2d-1} z_{2d}$$

for some $1 \leq d \leq n/2$. If $d = 1$, then $\theta_f = 3$, where the 3 independent relations satisfied are

$$\{w_1 + z_1 z_2, \quad z_1 w_1 + w_1, \quad z_2 w_1 + w_1\}.$$

If $d > 1$, then $\theta_f = 1$ and the only relation satisfied is the trivial one, namely

$$\{w_1 + z_1 z_2 + \cdots + z_{2d-1} z_{2d}\}.$$

With pen and paper, it is possible to verify that in both cases no other relation $\mathcal{R}(z, f(z)) = 0$ is satisfied. Thus we obtained the first result.

Proposition 3. *Assume that $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is CCZ quadratic with $2^{m-1} - 1$ affine components, and set $\lambda = (m-1)(n+m+1) - \frac{(m-1)m}{2}$. Thus F is CCZ equivalent to $\begin{bmatrix} f_1 \\ \boldsymbol{0}_{m-1} \end{bmatrix}$, with $f_1 = z_1 z_2 + \cdots + z_{2d-1} z_{2d}$ for some $1 \leq d \leq n/2$, and*

- *if $d = 1$ then $\theta_F = \lambda + 3$;*
- *if $d \geq 1$ then $\theta_F = \lambda + 1$.*

We move now to the case $m = 2$, thus $F = \begin{bmatrix} f_1 \\ f_2 \end{bmatrix}$; without loss of generality we assume $F(0) = 0$, so a possible quadratic relation $\mathcal{R}(z, w) =$ has the form

$$\sum_{1 \le i < j \le n} \alpha_{ij} z_i z_j + \sum_{i=1}^{n} \sum_{j=1}^{2} \beta_{ij} z_i w_j + \gamma_{12} w_1 w_2 + \sum_{i=1}^{n} \delta_i z_i + \sum_{j=1}^{2} \zeta_j w_j. \quad (2)$$

Remark 4. *Notice that, given a quadratic $F : \mathbb{F}_2^n \to \mathbb{F}_2^2$, if $\mathcal{R}(z, F(z)) = 0$ necessarily implies $\gamma_{12} = 0$ and $\beta_{i2} = 0$, for all $1 \le i \le n$, then $\theta_F = \theta_{f_1} + 1$. Equivalently, if $\gamma_{12} = 0$ and $\beta_{i1} = 0$, for all $1 \le i \le n$, then $\theta_F = \theta_{f_2} + 1$.*

Up to EA equivalence, we assume $f_1 = z_1 z_2 + \cdots + z_{2d-1} z_{2d}$. To classify these functions, we assume $\theta_{f_1} \ge \theta_{f_2} \ge \theta_{f_1+f_2}$. Moreover, when easy to compute, we assume that if f_2 is EA equivalent to some $z_1 z_2 + \cdots + z_{2d'-1} x_{2d'}$, then we impose $d' \ge d$. The same must hold for $f_1 + f_2$. Thus we have four cases:

1. $\theta_{f_1} = \theta_{f_2} = \theta_{f_1+f_2} = 3$, that implies $f_1 = z_1 z_2$;
2. $\theta_{f_1} = \theta_{f_2} = 3$, $\theta_{f_1+f_2} = 1$, that implies $f_1 = z_1 z_2$;
3. $\theta_{f_1} = 3$, $\theta_{f_2} = \theta_{f_1+f_2} = 1$, that implies $f_1 = z_1 z_2$;
4. $\theta_{f_1} = \theta_{f_2} = \theta_{f_1+f_2} = 1$, that implies $f_1 = z_1 z_2 + \cdots + z_{2d-1} z_{2d}$ $(d > 1)$.

To check the details of the following classification, the interest reader is referred to the appendix. Here, we report directly the results and for each representative we compute the number of linearly independent quadratic relations.

5.2.1 Case $\theta_{f_1} = \theta_{f_2} = \theta_{f_1+f_2} = 3$

In this case, up to EA transformation we have only one function, namely

$$F = \begin{bmatrix} z_1 z_2 \\ z_1 z_3 \end{bmatrix}.$$

Since only 3 variables are involved, we can directly consider a quadratic relation only involving the variables z_1, z_2, z_3, leading to

$$\begin{aligned} \mathcal{R}(z, F(z)) =& (\alpha_{12} + \beta_{11} + \beta_{21} + \zeta_1) z_1 z_2 + (\alpha_{13} + \beta_{12} + \beta_{32} + \zeta_2) z_1 z_3 \\ &+ \alpha_{23} z_2 z_3 + (\beta_{31} + \beta_{22} + \gamma_{12}) z_1 z_2 z_3 + \sum \delta_i z_i. \end{aligned}$$

Thus, we have $\theta_F = 8$, with the following independent relations:

$$\begin{array}{llll} w_1 + z_1 z_2, & z_1 w_1 + w_1, & z_2 w_1 + w_1, & w_1 w_2 + z_3 w_1, \\ w_2 + z_1 z_3, & z_1 w_2 + w_2, & z_3 w_2 + w_2, & w_1 w_2 + z_2 w_2. \end{array}$$

Notice that we can group the relations as 3 relations derived from f_1, 3 relations derived from f_2, 2 relations involving $w_1 w_2$.

5.2.2 Case $\theta_{f_1} = \theta_{f_2} = 3$ and $\theta_{f_1+f_2} = 1$

In this case, up to EA transformation we have only one function, namely

$$F = \begin{bmatrix} z_1 z_2 \\ z_3 z_4 \end{bmatrix}.$$

Notice that only 4 variables are involved, leading to the following:

$$\begin{aligned}\mathcal{R}(z, F(z)) =&(\alpha_{12} + \beta_{11} + \beta_{21} + \zeta_1) z_1 z_2 + \alpha_{13} z_1 z_3 + \alpha_{14} z_1 z_4 + \alpha_{23} z_2 z_3 + \alpha_{24} z_2 z_4 \\ &+ (\alpha_{34} + \beta_{32} + \beta_{42} + \zeta_2) z_3 z_4 + \beta_{31} z_1 z_2 z_3 + \beta_{41} z_1 z_2 z_4 + \beta_{12} z_1 z_3 z_4 \\ &+ \beta_{22} z_2 z_3 z_4 + \gamma_{12} z_1 z_2 z_3 z_4 + \sum \delta_i z_i.\end{aligned}$$

Thus we have $\theta_F = 6$, having 3 relations derived from f_1 and 3 relations derived from f_2:

$$\begin{array}{lll} w_1 + z_1 z_2, & z_1 w_1 + w_1, & z_2 w_1 + w_1, \\ w_2 + z_3 z_4, & z_3 w_2 + w_2, & z_4 w_2 + w_2. \end{array}$$

5.2.3 Case $\theta_{f_1} = 3$ and $\theta_{f_2} = \theta_{f_1+f_2} = 1$

Assuming $f_1 = z_1 z_2$ and, up to swapping f_2 with $f_1 + f_2$, setting $f_2 = z_1 \ell_1(z_3, \ldots, z_n) + z_2 \ell_2(z_3, \ldots, z_n) + q(z_3, \ldots, z_n)$, where ℓ_1, ℓ_2 are linear maps and q is a quadratic map, we have the following cases.

Subcase $q = 0$

If $q = 0$, then up to EA transformation, since $\theta_{f_2} = \theta_{f_1+f_2} = 1$, we can assume

$$F = \begin{bmatrix} z_1 z_2 \\ z_1 z_3 + z_2 z_4 \end{bmatrix}.$$

Notice that only 4 variables are involved, leading to the following:

$$\begin{aligned}\mathcal{R}(z, F(z)) =&(\alpha_{12} + \beta_{11} + \beta_{21} + \zeta_1) z_1 z_2 + (\alpha_{13} + \beta_{12} + \beta_{32} + \zeta_2) z_1 z_3 \\ &+ \alpha_{14} z_1 z_4 + \alpha_{23} z_2 z_3 + (\alpha_{24} + \beta_{22} + \beta_{42} + \zeta_2) z_2 z_4 + \alpha_{34} z_3 z_4 \\ &+ (\beta_{31} + \beta_{22} + \gamma_{12}) z_1 z_2 z_3 + (\beta_{41} + \beta_{12} + \gamma_{12}) z_1 z_2 z_4 + \beta_{32} z_2 z_3 z_4 \\ &+ \beta_{42} z_1 z_3 z_4 + \sum \delta_i z_i.\end{aligned}$$

Thus, we have $\theta_F = 7$, with relations

$$\begin{array}{l} w_1 + z_1 z_2, \quad z_1 w_1 + w_1, \quad z_2 w_1 + w_1, \quad w_2 + z_1 z_3 + z_2 z_4, \\ w_1 w_2 + z_4 w_1 + z_3 w_1, \quad w_1 w_2 + z_4 w_1 + z_2 w_2 + z_2 z_4, \quad w_1 w_2 + z_1 w_2 + z_2 w_2 + w_2. \end{array}$$

The relations can be grouped into 3 relations derived from f_1, 1 derived from f_2 and 3 involving $w_1 w_2$.

Subcase $q \neq 0$

If $q \neq 0$, then it is possible to verify that $\mathcal{R}(z, F(z)) = 0$ implies $\gamma_{12} = \beta_{j2} = 0$, for any j. So, from Remark 4, it follows that $\theta_F = \theta_{f_1} + 1 = 4$, having 3 relations for f_1 and 1 relation for f_2.

To show the above, we further divide this subcase.

- Assume $\ell_1 = \ell_2 = 0$. Up to EA equivalence, we assume

$$F = \begin{bmatrix} z_1 z_2 \\ z_3 z_4 + z_5 z_6 + \cdots + z_{2r-1} z_{2r} \end{bmatrix}$$

with $3 \leq r \leq n/2$.

Referring to the quadratic relation denoted in (2), we notice that in order to satisfy $\mathcal{R}(z, F(z)) = 0$ it must be $\gamma_{12} = 0$, by considering the presence of terms like $z_1 z_2 z_3 z_4$. Moreover, we have $\beta_{j2} = 0$, because of terms like $z_3 z_4 z_j$ (if $j \neq 3, 4$) and $z_5 z_6 z_j$ (if $j \neq 5, 6$).

- Assume If $\ell_1 \neq 0$ and $\ell_2 = 0$. Up to EA equivalence

$$F = \begin{bmatrix} z_1 z_2 \\ z_1 z_3 + z_4 z_5 + \cdots + z_{2r} z_{2r+1} \end{bmatrix}$$

with $2 \leq r < n/2$.

Similarly as before, we can notice that $\gamma_{12} = 0$ because of the presence of terms like $z_1 z_2 z_4 z_5$, and also $\beta_{j2} = 0$ because of terms $z_4 z_5 z_j$ (if $j \neq 4, 5$) and $z_1 z_3 z_j$ (if $j = 4, 5$).

- Assume If $\ell_1, \ell_2 \neq 0$. Up to EA equivalence,

$$F = \begin{bmatrix} z_1 z_2 \\ z_1 z_3 + z_2 z_4 + z_5 z_6 + \cdots + z_{2r-1} z_{2r} \end{bmatrix}$$

with $3 \leq r \leq n/2$.

Following the same steps done as in the previous cases, we have $\gamma_{12} = 0$ because of $z_1 z_2 z_5 z_6$ and $\beta_{j2} = 0$ because of $z_5 z_6 z_j$ (if $j \neq 5, 6$) and $z_1 z_3 z_j$ (if $j = 5, 6$).

5.2.4 Case $\theta_{f_1} = \theta_{f_2} = \theta_{f_1+f_2} = 1$

In this last case, we set $f_1 = z_1 z_2 + z_3 z_4 + \cdots + z_{2d-1} z_{2d}$, for some $d \geq 2$. We write f_2 as

$$f_2 = q(z_{2d+1}, \ldots, z_n) + g(z_1, \ldots, z_n),$$

where in g we isolate the terms of f_2 involving the first $2d$ variables and q is the remaining quadratic map in the variables $z_{2d+1}, \ldots, z_n$, that is $g = \sum_{i=1}^{2d} \sum_{j=i+1}^{n} c_{ij} z_i z_j$. We consider 3 different subcases.

Subcase $g = 0$ and $q \neq 0$

If $g = 0$, then, up to EA equivalence,

$$F = \begin{bmatrix} z_1 z_2 + z_3 z_4 + \cdots + z_{2d-1} z_{2d} \\ z_{2d+1} z_{2d+2} + z_{2d+3} z_{2d+4} + \cdots + z_{2r-1} z_{2r} \end{bmatrix}$$

for some $d + 1 < r \leq n/2$.

For this case we have $\gamma_{12} = 0$ because of terms like $z_1 z_2 z_{2d-1} z_{2d}$, and $\beta_{j1} = 0$ because of terms like $z_1 z_2 z_j$ (if $j \neq 1, 2$) and $z_3 z_4 z_j$ (if $j \neq 3, 4$). Thus, by considering Remark 4, we have $\theta_F = 2$.

Subcase $g \neq 0$ and $q \neq 0$

If $g, q \neq 0$ then, up to EA equivalence,

$$F = \begin{bmatrix} z_1z_2 + z_3z_4 + \cdots + z_{2d-1}z_{2d} \\ z_{2d+1}z_{2d+2} + \cdots + z_{2r-1}z_{2r} + g(z_1, \ldots, z_n) \end{bmatrix}$$

for some $d+1 \leq r \leq n/2$. In a quadratic relation $\mathcal{R}$ for F we have $\gamma_{12} = 0$ for terms like $z_1z_2z_{2d+1}z_{2d+2}$. Recall that $g(z_1, \ldots, z_n) = \sum_{i=1}^{2d}\sum_{j=i+1}^{n} c_{ij}z_iz_j$. We have also that $\beta_{i2} = 0$ for $2d+2 < i \leq n$ because of terms like $z_{2d+1}z_{2d+2}z_i$.

If $r > d+1$, then we also have $\beta_{i2} = 0$ for $i = 2d+1, 2d+2$ because of terms $z_iz_{2d+3}z_{2d+4}$. From this, we can also see that for $i \leq 2d$, in $\mathcal{R}(z, F(z))$ the term $z_iz_{2d+1}z_{2d+2}$ is multiplied by $\beta_{i2} + \beta_{(2d+1)}c_{i,2d+2} + \beta_{(2d+2)}c_{i,2d+1} = \beta_{i2}$ and so also for $i \leq 2d$ we have $\beta_{i2} = 0$. So, Remark 4 tells us that $\theta_F = 2$.

Assume then $r = d+1$, that is $f_2 = z_{2d+1}z_{2d+2} + g(z_1, \ldots, z_n)$. We consider different cases of g. Notice that for every i s.t. $c_{i(2d+1)} = c_{i(2d+2)} = 0$, then $\beta_{i2} = 0$ because of the term $z_iz_{2d+1}z_{2d+2}$.

- If $c_{i(2d+1)} = c_{i(2d+2)} = 0$ for every $1 \leq i \leq 2d$, then also $\beta_{i2} = 0$ for $i \leq 2d$. If there is some $c_{ij} \neq 0$ with $(i,j) \neq (2k-1, 2k)$, therefore $\beta_{2d+1} = \beta_{2d+2} = 0$ because of the terms $z_iz_jz_{2d+1}$ and $z_iz_jz_{2d+2}$. Otherwise, up to reordering the variables, we have $g = z_1z_2 + \cdots + z_{2k-1}z_{2k}$, for some $1 \leq k < d$, indeed $g \neq f_1$ since $\theta_{f_1+f_2} = 1$. So, for a quadratic relation $\mathcal{R}(z, F(z))$, we have that $\beta_{2d+1,1} = \beta_{2d+1,1} = 0$ because of terms $z_{2d-1}z_{2d}z_{2d+1}$ and $z_{2d-1}z_{2d}z_{2d+2}$, and so $\beta_{2d+1,2} = \beta_{2d+1,2} = 0$ because of terms $x1z_2z_{2d+1}$ and $z_1z_2z_{2d+2}$. Therefore, by Remark 4 we have $\theta_F = 2$.
- Otherwise, there is some index $1 \leq i \leq 2d$ such that $(c_{i(2d+1)}, c_{i(2d+2)}) \neq (0,0)$. Recall that we already have $\beta_{i2} = 0$ for $2d+2 < i \leq n$.
  - If there exist $j \geq 2d+3$ and $1 \leq k \leq 2d$ such that $c_{kj} = 1$, then without loss of generality we can assume $c_{1(2d+3)} = 1$, and up to affine transformation $z_{2d+3} \mapsto \sum_{j=2}^{n} c_{1j}z_j$ we can assume $c_{1j} = 0$ for every $j \neq 2d+3$. If there exists $i \neq 2$ such that $(c_{i(2d+1)}, c_{i(2d+2)}) \neq (0,0)$, then $\beta_{12} = 0$ because of term $z_1z_iz_{2d+1}$ or $z_1z_iz_{2d+2}$. Thus also $\beta_{j2} = 0$, for $j \neq 1, 2, 2d+3$ because of term $z_1z_jz_{2d+3}$. Since also $\beta_{22} = 0$ for $z_2z_{2d+1}z_{2d+2}$, it follows that $\theta_F = 2$, from Remark 4.
    Otherwise, we are in the case $(c_{i(2d+1)}, c_{i(2d+2)}) = (0,0)$ for $i \geq 3$ and $(c_{2(2d+1)}, c_{2(2d+2)}) \neq (0,0)$, so $\beta_{i2} = 0$ for all $i \neq 2, 2d+1, 2d+2$. Wlog we can assume $(c_{2(2d+1)}, c_{2(2d+2)}) = (1,0)$. Also, $\beta_{i1} = 0$ for $i \neq 1, 2, 2d+3$ because of term $z_1z_2z_i$, and so also $\beta_{(2d+1)2} = \beta_{(2d+2)2} = 0$ for terms $z_1z_{2d+1}z_{2d+3}$ and $z_1z_{2d+2}z_{2d+3}$, and so $\beta_{22} = 0$ for term $z_2z_{2d+1}z_{2d+2}$. From Remark 4, it follows that $\theta_F = 2$.
  - So, we assume $g = g(z_1, \ldots, z_{2d+2})$, and wlog $(c_{1(2d+1)}, c_{1(2d+2)}) \neq (0,0)$, so $(c_{1(2d+1)}, c_{1(2d+2)}) = (1,0)$.
    In the relation $\mathcal{R}(z, F(z))$, we have the following pairs of term and

coefficient, for $3 \leq i \leq 2d$,

$$\begin{aligned}
z_1 z_{2d+1} z_{2d+2} &\to \beta_{12} + \beta_{(2d+2)2}, \\
z_i z_{2d+1} z_{2d+2} &\to \beta_{i2} + \beta_{(2d+1)2} c_{i(2d+2)} + \beta_{(2d+2)2} c_{i(2d+1)}, \\
z_1 z_i z_{2d+1} &\to \beta_{12} c_{i(2d+1)} + \beta_{i2} + \beta_{(2d+1)2} c_{1i}, \\
z_1 z_i z_{2d+2} &\to \beta_{12} c_{i(2d+2)} + \beta_{(2d+2)2} c_{1i}, \\
z_2 z_{2d+1} z_{2d+1} &\to \beta_{22} + \beta_{(2d+1)2} c_{2(2d+2)} + \beta_{(2d+2)2} c_{2(2d+1)}.
\end{aligned}$$

Thus $\beta_{12} = \beta_{(2d+2)2}$ and $\beta_{12}(c_{i(2d+2)} + c_{1i}) = 0$. If there exists $j \neq 1, 2$ such that $c_{j(2d+2)} + c_{1j} = 1$, then $\beta_{12} = \beta_{(2d+2)2} = 0$. So, $\beta_{i2} = \beta_{(2d+1)2} c_{1i} = \beta_{2d+1} c_{i(2d+2)}$ implying $\beta_{(2d+1)2}(c_{1i} + c_{i(2d+2)}) = 0$. Since $c_{j(2d+2)} + c_{1j} = 1$, then $\beta_{(2d+1)2} = \beta_{i2} = 0$, for every $3 \leq i \leq 2d$, and also $\beta_{22} = 0$. It follows that also in this case $\theta_F = 2$. We are left with $c_{i(2d+2)} = c_{1i}$ for every $3 \leq i \leq 2d$. Now, by applying the transformation $z_{2d+2} \mapsto z_{2d+2} + z_1$, we obtain a map f_2 of the form $f_2 = z_{2d+1} z_{2d+2} + g(z_2, \ldots, z_{2d+2}) + a_{12} z_1 z_2$. Thus, by iterating this process for all indexes i such that $(c_{i(2d+1)}, c_{i(2d+2)}) \neq (0, 0)$, we get that also in this case the only quadratic relations are either derived from f_1 or from f_2, thus $\theta_F = 2$.

Subcase $g \neq 0$ and $q = 0$

If $g \neq 0$ and $q = 0$, thus $f_2 = z_1 \ell_1(z_2, \ldots, z_n) + z_2 \ell_2(z_3, \ldots, z_n) + \cdots + z_{2d} \ell_{2d}(z_{2d+1}, \ldots, z_n)$, with $\ell_i(z_{i+1}, \ldots, z_n) = \sum_{j=i+1}^{n} c_{ij} z_j$ Notice that, up to affine transformation, the function $F = \begin{bmatrix} f_1 & f_2 \end{bmatrix}^\top$ involves only (up to) $4d$ variables.

For this case, we consider two distinct situations: $d = 2$ and $d > 2$.

- If $d = 2$, then $f_1 = z_1 z_2 + z_3 z_4$ and $f_2 = z_1 \ell_1(z_2, \ldots, z_8) + \cdots + z_4 \ell_4(z_5, \ldots, z_8)$. Via computer search and some preliminary restrictions, we recover the following list of CCZ inequivalent quadratic functions (we directly list f_2).

$$\begin{aligned}
f_2 &= z_1 z_5 + z_2 z_6, & f_2 &= z_1 z_3 + z_2 z_5, \\
f_2 &= z_1 z_2 + z_1 z_3 + z_2 z_4, & f_2 &= z_1 z_7 + z_2 z_6 + z_3 z_5, \\
f_2 &= z_2 z_6 + z_3 z_5, & f_2 &= z_1 z_4 + z_2 z_6 + z_3 z_5, \\
f_2 &= z_1 z_8 + z_2 z_7 + z_3 z_6 + z_4 z_5.
\end{aligned}$$

All the above functions are such that $\theta_F = 2$ with the following exceptions:

1. $f_2 = z_1 z_3 + z_2 z_5$ with $\theta_F = 3$, with relations

$$w_1 + z_1 z_2 + z_3 z_4, \quad w_2 + z_1 z_3 + z_2 z_5, \quad w_1 z_3 + w_2 z_2 + z_2 z_5 + z_3 z_4.$$

2. $f_2 = z_1 z_2 + z_1 z_3 + z_2 z_4$ with $\theta_F = 6$ and relations

$$\begin{aligned}
&w_1 + z_1 z_2 + z_3 z_4, && w_1 z_3 + w_2 z_2 + w_1 + z_2 z_4, \\
&w_2 + z_1 z_2 + z_1 z_3 + z_2 z_4, && w_1 z_4 + w_2 z_1 + w_1 + z_1 z_3, \\
&w_1 z_2 + w_1 z_3 + w_2 z_3 + w_1 + z_1 z_3, && w_1 z_1 + w_1 z_4 + w_2 z_4 + w_1 + z_2 z_4.
\end{aligned}$$

- If $d \geq 3$ then

$$f_1 = z_1z_2 + z_3z_4 + z_5z_6 + \cdots + z_{2d-1}z_{2d},$$
$$f_2 = z_1\ell_1 + z_2\ell_2 + z_3\ell_2 + \cdots + z_{2d}\ell_{2d}.$$

Moreover, we assume that f_2 is affine equivalent to $z_1z_2 + \cdots + z_{2d'-1}z_{2d'}$ with $d' \geq d$ (the same for $f_1 + f_2$).

If there is an index i, $1 \leq i \leq 2d$, such that ℓ_i contains a variable z_r with $r > 2d$, then $\gamma_{12} = 0$ because of the term $z_1z_2z_iz_r$ or $z_3z_4z_iz_r$. Otherwise, if for all index $1 \leq i \leq 2d$, ℓ_i contains only the variables up to z_{2d}, then it must exist an index $j \leq 2d-3$ such that $\ell_j \neq c_{j(2d-1)}z_{2d-1} + c_{j(2d)}z_{2d}$, otherwise $f_2 = z_{2d-1}\phi_1 + z_{2d}\phi_2$ for some linear maps ϕ_1, ϕ_2 and so $d' = 2 < d$, a contradiction. So consider such $j \leq 2d-3$ with $c_{jr} = 1$ for some $j+1 \leq r \leq 2d-2$. If $(j,r) \neq (2k-1, 2k)$ then $\gamma_{12} = 0$ because of the term $z_jz_rz_{2d-1}z_{2d}$. If such pair (j,r) does not exist, then $f_2 = z_{2d-1}\phi_1 + z_{2d}\phi_2 + \sum_{j\in J} z_{2j-1}z_{2j}$, for some $J \subseteq \{1, \ldots, d-1\}$. Since $d' \geq d$, then $|J| \geq d-2$, Thus, wlog we can assume $J = \{2, \ldots, d-1\}$ and so also in this case $\gamma_{12} = 0$ because of the term $z_1z_2z_3z_4$.

Hence $\gamma_{12} = 0$. Since $\theta_{f_1} = \theta_{f_2} = 1$, to have $\theta_F > 2$ there must exist a quadratic relation $\mathcal{R}$ admitting two indices i and j such that

$$\beta_{i1} = 1, \qquad \beta_{j2} = 1$$

Moreover, since also $\theta_{f_1+f_2} = 1$, then up to swapping the role of f_1 and f_2, we can assume $\beta_{i2} = 0$.

  - If $i \leq 2d$, then up to change the label on the variables, we can assume $i = 1$. Now, for any $2 \leq r \leq d$, up to swapping $z_{2r} \leftrightarrow z_{2r-1}$ and up to transforming $z_{2r} \mapsto z_{2r} + z_{2r-1}$, we can assume wlog that $c_{1(2r-1)} = 0$. Notice that these transformations do not change f_1 (up to adding some linear terms). The term $z_1z_{2r-1}z_{2r}$ in $\mathcal{R}(z, F(z))$ is multiplied by $\beta_{11} + \beta_{12}c_{(2r-1)(2r)} + \beta_{(2r)2}c_{1(2r-1)} + \beta_{(2r-1)2}c_{1(2r)} = 1 + \beta_{(2r-1)2}c_{1(2r)}$ implying that $\beta_{(2r-1)2} = c_{1(2r)} = 1$ for any $2 \leq r \leq d$. Instead, in $\mathcal{R}$ the term $z_1z_3z_6$ is multiplied by $\beta_{12}c_{36} + \beta_{32}c_{16} + \beta_{62}c_{13} = 1$ so $\mathcal{R}$ is not a quadratic relation for F.
  - Assume therefore that $i > 2d$, and wlog set $i = 2d+1$.
    Similarly as before, for $1 \leq r \leq d$, up to swapping $z_{2r} \leftrightarrow z_{2r-1}$ and up to transforming $z_{2r-1} \mapsto z_{2r} + z_{2r-1}$, we can assume wlog that $c_{(2r)(2d+1)} = 0$. As before, these transformations potentially only add to f_1 linear terms. For $1 \leq r \leq d$, consider the term $z_{2r}z_{2r-1}z_{2d+1}$ in $\mathcal{R}(z, F(z))$, which is multiplied by $\beta_{(2d+1)1} + \beta_{(2d+1)2}c_{(2r-1)(2r)} + \beta_{(2r)2}c_{(2r-1)(2d+1)} + \beta_{(2r-1)2}c_{(2r)(2d+1)} = 1 + \beta_{(2r)2}c_{(2r-1)(2d+1)}$, implying that $\beta_{(2r)2} = c_{(2r-1)(2d+1)} = 1$. Instead, in $\mathcal{R}$ the term $z_1z_4z_{2d+1}$ is multiplied by $\beta_{12}c_{4(2d+1)} + \beta_{42}c_{1(2d+1)} + \beta_{(2d+1)2}c_{14} = 1$ so $\mathcal{R}$ is not a quadratic relation for F.

Therefore if $d \geq 3$ we have only 2 linearly independent quadratic relations, 1 derived from f_1 and 1 from f_2, do $\theta_F = 2$.

We summarise what obtained in the following proposition.

Proposition 4. *Assume that* $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *is CCZ quadratic with* $2^{m-2} - 1$ *affine components. Thus* F *is CCZ equivalent to* $\begin{bmatrix} f_1 \\ f_2 \\ \mathbf{0}_{m-2} \end{bmatrix}$*, for some* f_1, f_2 *quadratic Boolean functions. Let* $\lambda = (m-2)(n+m+1) - \frac{(m-1)(m-2)}{2}$*. Then, one of the following condition is satisfied.*

- *If* $\theta_F = \lambda + 8$*, then* $f_1 = z_1 z_2$ *and* $f_2 = z_1 z_3$*.*
- *If* $\theta_F = \lambda + 7$*, then* $f_1 = z_1 z_2$ *and* $f_2 = z_1 z_3 + z_2 z_4$*.*
- *If* $\theta_F = \lambda + 6$*, then*
  - $f_1 = z_1 z_2$ *and* $f_2 = z_3 z_4$*; or*
  - $f_1 = z_1 z_2 + z_3 z_4$ *and* $f_2 = z_1 z_2 + z_1 z_3 + z_2 z_4$*.*
- *If* $\theta_F = \lambda + 4$*, then* $f_1 = z_1 z_2$ *and*
  - $f_2 = z_3 z_4 + z_5 z_6 + \cdots + z_{2r-1} z_{2r}$*, for some* $3 \leq r \leq n/2$*; or*
  - $f_2 = z_1 z_3 + z_4 z_5 + \cdots + z_{2r} z_{2r+1}$*, for some* $2 \leq r < n/2$*; or*
  - $f_2 = z_1 z_3 + z_2 z_4 + z_5 z_6 + \cdots + z_{2r-1} z_{2r}$*, for some* $3 \leq r \leq n/2$*.*
- *If* $\theta_F = \lambda + 3$*, then* $f_1 = z_1 z_2 + z_3 z_4$ *and* $f_2 = z_1 z_3 + z_2 z_5$*.*
- *If* $\theta_F = \lambda + 2$*, then*
  - $f_1 = z_1 z_2 + z_3 z_4 + \ldots + z_{2d-1} z_{2d}$ *and* $f_2 = z_{2d+1} z_{2d+2} + z_{2d+3} z_{2d+4} + \cdots + z_{2r-1} z_{2r}$*, for some* $2 \leq d \leq n/2$ *and* $d+2 \leq r \leq n/2$*; or*
  - $f_1 = z_1 z_2 + z_3 z_4 + \ldots + z_{2d-1} z_{2d}$ *and* $f_2 = z_{2d+1} z_{2d+2} + \cdots + z_{2r-1} z_{2r} + \sum_{i=1}^{2d} \sum_{j=i+1}^{n} c_{ij} z_i z_j$*, for some* $2 \leq d \leq n/2$ *and* $d+1 \leq r \leq n/2$*; or*
  - $f_1 = z_1 z_2 + z_3 z_4$ *and* $f_2 \in \{z_1 z_5 + z_2 z_6, z_1 z_7 + z_2 z_6 + z_3 z_5, z_2 z_6 + z_3 z_5, z_1 z_4 + z_2 z_6 + z_3 z_5, z_1 z_8 + z_2 z_7 + z_3 z_6 + z_4 z_5\}$*; or*
  - $f_1 = z_1 z_2 + z_3 z_4 + \ldots + z_{2d-1} z_{2d}$ *and* $f_2 = \sum_{i=1}^{2d} \sum_{j=i+1}^{n} c_{ij} z_i z_j$*.*

6 Computational analysis

We restrict the computational analysis to functions defined over $\mathbb{F}_q = \mathbb{F}_2$ and with $m = n$, for relatively small values of n. We also make use of the representation as univariate polynomials over $\mathbb{F}_{2^n}$. For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, we denote by θ_F the number of linearly independent quadratic relations satisfied by F, and by k_F the dimension of the affine component space.

Computationally, we observe that the statement of Corollary 1 does not represent a necessary and sufficient condition. Indeed, there are functions not CCZ quadratic, but still possessing (more than) m linearly independent quadratic relations. This can be verified using, for example, the complete classification, up to CCZ equivalence, of the functions $F : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$, computed by Brinkmann in [2] (4151 functions). To be sure to compute the exact set of quadratic relations, we construct the linear system by considering all pairs of input-output, and not just around $\binom{n+m+2}{2}$ pairs. In Table 2 we report the outcome of the

$[\theta_F,k_F]$	$\sharp\{F\}$	$[\theta_F,k_F]$	$\sharp\{F\}$	$[\theta_F,k_F]$	$\sharp\{F\}$	$[\theta_F,k_F]$	$\sharp\{F\}$
[21, 0]	3576	[21,1]	425	[21,2]	29	[21,3]	1
[22,0]	45	[22,1]	43	[22,2]	12	[22,3]	2
[23,0]	1	[23,1]	5	[23,2]	6	[23,3]	1
[24,2]	1	[24,3]	2	[25,3]	1	[26,4]	1

Table 2: The number of representative function $F : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ ($\sharp\{F\}$) having θ_F linearly independent quadratic relations and $2^{k_F} - 1$ affine components

analysis, showing that all (4,4)-functions possess at least 21 linearly independent quadratic relations but clearly they are not all CCZ quadratic.

However, using the result of Corollary 2, we can deduce that the function $F(x) = x^{15} + a^4x^{12} + a^8x^9 + a^3x^8 + a^2x^6 + a^9x^4 + ax^3 + a^{12}x^2 + a^6x$, with $a \in \mathbb{F}_{2^4}$ primitive element, is not CCZ quadratic. Indeed, F is such that $k_F = 3$ and $\theta_F = 21$, satisfying $\theta_F < k_F(n+n) - k_F(k_F+1)/2 + n = 22$. This is the only function that leads to such a contradiction in this dimension.

We can also apply Proposition 3 and Proposition 4, from which we obtain the following.

- If $k_F = 3$, then F is CCZ quadratic if $\theta_F \in \{k_F(2n+1) - k_F(k_F+1)/2 + r : r \in [1,3]\} = \{22, 24\}$, therefore
  - $F(x) = x^{15} + a^{12}x^{14} + a^9x^{13} + a^6x^{12} + a^3x^{11} + x^{10} + a^{12}x^9 + a^9x^8 + a^6x^7 + a^3x^6 + x^5 + a^{12}x^4 + a^9x^3 + a^6x^2 + a^3x$ is not CCZ quadratic since $k_F = 3$ and $\theta_F = 25$,
  - $F(x) = x^{15} + a^6x^{14} + a^{12}x^{13} + a^{11}x^{12} + a^9x^{11} + a^7x^9 + a^6x^8 + a^3x^7 + a^{13}x^6 + a^3x^4 + a^{14}x^3 + a^9x^2 + a^12x$ is not CCZ quadratic since $k_F = 3$ and $\theta_F = 23$.
- If $k_F = 2$, then F is CCZ quadratic if $\theta_F \in \{k_F(2n+1) - k_F(k_F+1)/2 + r : r \in [2,3,4,6,7,8]\} = \{17, 18, 19, 21, 22, 23\}$, therefore
  - $F(x) = a^4x^{15} + a^4x^{14} + a^6x^{13} + a^4x^{12} + a^9x^{11} + a^8x^{10} + x^9 + a^4x^8 + a^5x^7 + a^{14}x^6 + a^2x^5 + a^{12}x^4 + a^3x^3 + a^{11}x^2$ is not CCZ quadratic since $k_F = 2$ and $\theta_F = 24$.

Remark 5. *From Table 2 we can notice that the pair of values $[\theta_F, k_F]$ can be used as a first discriminating factor to divide functions into CCZ classes.*

We verify that in larger dimensions more functions are not CCZ quadratic thanks to Corollary 1 and Corollary 2. Specifically, to continue the analysis, we restrict it to power functions $F(x) = x^d$ with $\deg(F) > 2$ up to CCZ equivalence (using the cyclotomic equivalence, see [7]). To the best of our knowledge, a characterization of when a power function is CCZ quadratic is only known for APN functions. Indeed, for APN power maps being CCZ quadratic implies being quadratic, see [12]. Thus, for a generic power function (not APN) there are no results about the CCZ equivalence to a quadratic function.

For each power function F, we compute the values θ_F and k_F, and we set $c_F = \theta_F - k_F(n+n) + k_F(k_F+1)/2 - n$. Thus if $\theta_F < n$, then F is not CCZ quadratic thanks to Corollary 1, whereas if $c_F < 0$, then F is not CCZ quadratic thanks to Corollary 2. In Table 3 we report the analysis performed

on dimensions $n = 4, \ldots, 12$, where for dimensions $n \geq 10$ we consider CCZ inequivalent power maps x^d with $d \leq 200$.

n	$\sharp\{F(x) = x^d\}$	$\sharp\{F \mid \theta_F < n\}$	$\sharp\{F \mid c_F < 0\}$	$\sharp\{\ [\theta_F, k_F]\ \}$
4	2	0	0	2
5	2	0	0	2
6	7	0	1	6
7	7	0	0	3
8	24	2	4	17
9	32	3	5	9
10	55* $(d \leq 200)$	16	18	13
11	62* $(d \leq 200)$	27	27	5
12	85* $(d \leq 200)$	40	41	20

Table 3: Total number of representative power functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $\deg(F) > 2$, amounts of those satisfying $\theta_F < n$ and of those satisfying $c_F < 0$, and amount of distinct pairs $[\theta_F, k_F]$

Moreover, in each dimension $n = 4, \ldots, 9$ we found a case of power function with $k_F = n-1$ but such that $\theta_F = k_F(2n+1) - k_F(k_F+1)/2 + n$, thus thanks to Proposition 3 F is not CCZ quadratic. The cases identified by Proposition 4 were already identified by having $c_F < 0$.

Remark 6. *Notice that, in general, a vectorial function does not always satisfy some quadratic relation. For example, in our computational experiments, we verify that in dimension $n = 8$ the power function $F(x) = x^{27}$ is such that $\theta_F = 0$, and in dimension $n = 9$, the function $F(x) = x^{83}$ is such that $\theta_F = 0$. Both functions have algebraic degree 4. In dimension $n = 10$ we have found power functions with $\theta_F = 0$ of algebraic degrees $4, 5, 6$, and in dimensions $n = 11, 12$ of algebraic degrees $3, 4, 5, 6$.*

Conclusions

In this work we study the notion of quadratic relations possessed by a vectorial function and prove that the number of linearly independent quadratic relations is invariant under the CCZ transformation. We show that these relations can be used to reduce any function CCZ equivalent to a quadratic function to a system of quadratic polynomials. Thus, a generalization of the scheme proposed in [4] with a generic CCZ transformation does not offer additional security compared to the case of a quadratic system with an affine transformation. We further show that the number of linearly independent quadratic relations can be used to determine if a function cannot be CCZ equivalent to a quadratic function, and in general it can be used to show that two functions are not CCZ equivalent. We verified computationally that, for large enough dimensions, many functions (not CCZ equivalent to quadratic functions) can be identified with this technique. We conclude by stressing that this method consists of solving a linear system of size $\binom{n+m+2}{2}$, which might be possible to compute for larger dimensions than other methods.

References

[1] Beierle, C., and Felke, P. Not Easy to Prepare a Pesto: Cryptanalysis of a Multivariate Public-Key Scheme from CCZ Equivalence. Cryptology ePrint Archive, Paper 2025/1452, 2025.

[2] Brinkmann, M. Extended affine and CCZ equivalence up to dimension 4. Cryptology ePrint Archive, Paper 2019/316, 2019.

[3] Browning, K., Dillon, J., Kibler, R., and McQuistan, M. APN polynomials and related codes. *Journal of Combinatorics, Information and System Sciences 34* (01 2009).

[4] Calderini, M., Caminata, A., and Villa, I. A new multivariate primitive from CCZ equivalence. *Journal of Cryptology 38*, 3 (Jun 2025), 25.

[5] Caminata, A., Gorla, E., Mabe, M., Vigorito, M., and Villa, I. Cryptanalysis of a multivariate CCZ scheme. *Designs, Codes and Cryptography 94*, 4 (Mar 2026), 75.

[6] Canteaut, A., and Perrin, L. On CCZ-equivalence, extended-affine equivalence, and function twisting. *Finite Fields and Their Applications 56* (2019), 209–246.

[7] Dempwolff, U. CCZ equivalence of power functions. *Designs, Codes and Cryptography 86*, 3 (2018), 665–692.

[8] Edel, Y., and Pott, A. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications 3*, 1 (2009), 59–81.

[9] Kamlovskii, O. V., and Pankov, K. N. Some classes of balanced functions over finite fields with a small value of the linear characteristic. *Problems of Information Transmission 58*, 4 (2022), 389–402.

[10] Matsumoto, T., and Imai, H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques* (1988), Springer, pp. 419–453.

[11] Patarin, J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In *Annual International Cryptology Conference* (1995), Springer, pp. 248–261.

[12] Yoshiara, S. Equivalences of power APN functions with power or quadratic APN functions. *Journal of Algebraic Combinatorics 44*, 3 (2016), 561–585.

A Equivalence classes for quadratic $F : \mathbb{F}_2^n \to \mathbb{F}_2^2$

We give the details missed in the analysis presented in Section 5.2, for the classification, up to EA transformation, of two output Boolean functions.

Set $F = \begin{bmatrix} f_1 \\ f_2 \end{bmatrix}$. In this analysis, we fix the ANF of f_1, we perform some affine transformation to remove some terms in f_2 but such that the ANF of f_1 does not change, up to summing some linear terms.

Remark 7. *When we say* an affine transformation not involving $x_1, \ldots, x_t$ *it means that the mentioned affine (invertible) transformation* $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *can be split in consecutive affine transformations of a single variable, thus of the form* $x_j \mapsto \phi_j(x) = a_{j1}x_1 + \cdots + a_{jn}x_n$*, for* $j = i_1, \ldots, i_r$ *but such that* $\{1, \ldots, t\} \cap \{i_1, \ldots, i_r\} = \emptyset$*. This implies that for* $f(x) = \sum_{i,j=1}^{t} a_{ij}x_ix_j$ *we have* $f \circ A = f$*.*

Case $\theta_{f_1} = 3$ and $\theta_{f_2} = 3$. We assume $f_1 = x_1x_2$ and, up to replacing f_2 with $f_1 + f_2$, we consider $f_2 = \sum_{i,j} a_{ij}x_ix_j$, with $a_{12} = 0$. Rewrite f_2 as

$$f_2(x) = x_1\ell_1(x_3, \ldots, x_n) + x_2\ell_2(x_3, \ldots, x_n) + \sum_{3 \le i < j \le n} a_{ij}x_ix_j.$$

- If $\ell_1 = \ell_2 = 0$, then up to affine transformation not involving x_1, x_2, we can assume $f_2(x) = x_3x_4$.
- If $\ell_1 \neq 0$, then up to affine transformation (not involving x_1, x_2) we can assume $f_2(x) = x_1x_3 + a_{23}x_2x_3 + x_2\ell_2(x_4, \ldots, x_n) + x_3\ell_3(x_4, \ldots, x_n) + q(x_4, \ldots, x_n)$. Now, if we perform the affine transformation $x_1 \mapsto x_1 + a_{23}x_2 + \ell_3(x_4, \ldots, x_n)$, then we get to $\bar{f}_2 = x_1x_3 + x_2\ell_2(x_4, \ldots, x_n) + q(x_4, \ldots, x_n)$. Thus, in order to have $\theta_{\bar{f}_2} = 3$, it must be $\ell_2 = q = 0$, so $f_2 = x_1x_3 + a_{23}x_2x_3 + x_3\ell_3(x_4, \ldots, x_n)$. Up to the affine transformation $x_1 \mapsto x_1 + a_{23}x_2$, we can assume wlog $a_{23} = 0$ (f_1 is modified into $x_1x_2 + a_{23}x_2$). If $\ell_3 \neq 0$ then we can assume wlog $\ell_3 = x_4$ and with $x_4 \mapsto x_4 + x_1$ we get $f_2 = x_3x_4$, otherwise if it is zero, then $f_2 = x_1x_3$.

Thus, up to EA equivalence, the case $\theta_{f_1} = \theta_{f_2} = 3$ can only be either with $f_2 = x_1x_3$, for which $\theta_{f_1+f_2} = 3$, or with $f_2 = x_3x_4$, for which $\theta_{f_1+f_2} = 1$.

Case $\theta_{f_1} = 3$ and $\theta_{f_2} = \theta_{f_1+f_2} = 1$. We assume $f_1 = x_1x_2$ and, up to replacing f_2 with $f_1 + f_2$, we assume $f_2 = x_1\ell_1(x_3, \ldots, x_n) + x_2\ell_2(x_3, \ldots, x_n) + q(x_2, \ldots, x_n)$ Up to affine transformation that does not involve x_1, x_2, we can assume $q = 0$ or $q = x_3x_4 + \cdots + x_{2d-1}x_{2d}$, for some $2 \le d \le n/2$

If $q = 0$, then ℓ_1, ℓ_2 must be nonzero and distinct (since $\theta_{f_2} = \theta_{f_1+f_2} = 1$). Up to affine transformation not involving x_1, x_2, we can assume $\ell_1 = x_3$ and $\ell_2 = x_4$, so $f_2 = x_1x_3 + x_2x_4$.

Assume $q = x_3x_4 + \cdots + x_{2d-1}x_{2d}$. Now, for every term x_i in ℓ_1 (resp. ℓ_2) if $i = 2j$ with $j \le d$ we perform the affine transformation $x_{2j-1} \mapsto x_{2j-1} + x_1$ (resp. $x_{2j-1} \mapsto x_{2j-1} + x_2$); if $i = 2j - 1$ with $j \le d$ we perform the affine transformation $x_{2j} \mapsto x_{2j} + x_1$ (resp. $x_{2j} \mapsto x_{2j} + x_2$). Notice that if an extra x_1x_2 term is generated, this is removed by summing $f_1 = x_1x_2$.

Thus, we have removed all variables $x_3, \ldots, x_{2d}$ from ℓ_1, ℓ_2 and we are left with the following cases:

- if $\ell_1 = \ell_2 = 0$, then clearly $d > 2$ and $f_2 = x_3x_4 + \cdots + x_{2d-1}x_{2d}$.
- if $\ell_1 \neq 0$ and $\ell_2 = 0$ then up to affine transformation wlog we can assume $\ell_1 = x_{2d+1}$ and $f_2 = x_1x_{2d+1} + x_3x_4 + \cdots + x_{2d-1}x_{2d}$. Notice that in this case $d \ge 2$.
- the case $\ell_1 = 0$ and $\ell_2 \neq 0$ is equivalent to the previous one.
- if $\ell_1, \ell_2 \neq 0$, then up to affine transformation either $\ell_1 = \ell_2 = x_{2d+1}$ and by applying $x_1 \mapsto x_1 + x_2$ we are back to the previous case, otherwise we can assume $\ell_1 = x_{2d+1}$ and $\ell_2 = x_{2d+2}$ so $f_2 = x_1x_{2d+1} + x_2x_{2d+2} + x_3x_4 + \cdots + x_{2d-1}x_{2d}$.

Case $\theta_{f_1} = \theta_{f_2} = \theta_{f_1+f_2} = 1$. Assume $f_1 = x_1x_2 + x_3x_4 + \cdots + x_{2d-1}x_{2d}$, for some $2 \leq d \leq n/2$, and denote f_2 as $f_2 = q(x_{2d+1}, \ldots, x_n) + g(x_1, \ldots, x_n)$, with $g(x) = \sum_{i=1}^{2d} \sum_{j=i+1}^{n} c_{ij}x_ix_j$. Then, if $q \neq 0$, up to affine transformation not involving the first $2d$ variables, we can assume $f_2 = x_{2d+1}x_{2d+2} + \cdots + x_{2t-1}x_{2t} + g(x_1, \ldots, x_n)$.

The case $f_1 = x_1x_2 + x_3x_4$ and $f_2 = x_1\ell_1(x_2, \ldots, x_8) + \cdots + x_4\ell_4(x_5, \ldots, x_8)$. As written in Subsection 5.2.4, for this case, which involves only 8 variables, we first perform some theoretical restrictions on the choice of the possible coefficients involved, and then we conclude with a computer search, using MAGMA, to check the CCZ equivalence between the quadratic functions obtained, with the restriction that $\theta_{f_1} = \theta_{f_2} = \theta_{f_1+f_2} = 1$. We report here the preliminary theoretical analysis.

All the following restrictions are up to EA transformation not involving $x_1, \ldots, x_4$, thus not modifying f_1. Moreover, up to summing f_1 to f_2, we also assume that x_3x_4 does not appear in f_2, that is $\ell_3 = \ell_3(x_5, \ldots, x_8)$.

- We have that $\ell_4 = 0$ or $\ell_4 = x_5$.
- If $\ell_4 = 0$, then $\ell_3 = 0$ or $\ell_3 = x_5$;
  if $\ell_4 \neq 0$, then $\ell_3 = 0$ or $\ell_3 = x_5$ or $\ell_3 = x_6$.
- If $\ell_3 = \ell_4 = 0$, then $\ell_2 = x_5$ (ℓ_2 cannot be zero otherwise $\theta_{f_2} = 3$);
  otherwise otherwise if $\ell_3 = \ell_3(x_5)$ then $\ell_2 = \ell_2(x_3, x_4, x_5)$ or $\ell_2 = x_6$;
  otherwise if $\ell_3 = x_6$ and $\ell_4 = x_5$ then $\ell_2 = \ell_2(x_3, x_4, x_5, x_6)$ or $\ell_2 = x_7$.
- If $\ell_2 = \ell_2(x_3, x_4, x_5)$ and $\ell_3 = \ell_3(x_5)$ then $\ell_1 = \ell_1(x_2, \ldots, x_5)$ or $\ell_1 = x_6$;
  otherwise if $\ell_2 = \ell_2(x_3, \ldots, x_6)$ then $\ell_1 = \ell_1(x_2, \ldots, x_6)$ or $\ell_1 = x_7$;
  otherwise if $\ell_2 = x_7$, $\ell_3 = x_6$ and $\ell_4 = x_5$ then $\ell_1 = \ell_1(x_2, \ldots, x_7)$ or $\ell_1 = x_8$.

Using the above restrictions, we perform a computational analysis, and obtain the following list of CCZ inequivalent quadratic functions, with $\theta_{f_2} = \theta_{f_1+f_2} = 1$,

$$
\begin{aligned}
f_1 &= x_1x_2 + x_3x_4, & f_2 &= x_1x_5 + x_2x_6;\\
f_1 &= x_1x_2 + x_3x_4, & f_2 &= x_1x_3 + x_2x_5;\\
f_1 &= x_1x_2 + x_3x_4, & f_2 &= x_1x_2 + x_1x_3 + x_2x_4;\\
f_1 &= x_1x_2 + x_3x_4, & f_2 &= x_1x_7 + x_2x_6 + x_3x_5;\\
f_1 &= x_1x_2 + x_3x_4, & f_2 &= x_2x_6 + x_3x_5;\\
f_1 &= x_1x_2 + x_3x_4, & f_2 &= x_1x_4 + x_2x_6 + x_3x_5;\\
f_1 &= x_1x_2 + x_3x_4, & f_2 &= x_1x_8 + x_2x_7 + x_3x_6 + x_4x_5.
\end{aligned}
$$