

# On the bijectivity of the map $\chi$

Anna-Maurin Graner      Björn Kriepke  
Lucas Krompholz      Gohar M. Kyureghyan

Institute of Mathematics

University of Rostock

Germany

`{anna-maurin.graner,bjoern.kriepke,lucas.krompholz,gohar.kyureghyan}@uni-rostock.de`

## Abstract

We prove that for  $n > 1$  the map  $\chi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ , defined by  $y = \chi(x)$  with  $y_i = x_i + x_{i+2} \cdot (1 + x_{i+1})$  for  $1 \leq i \leq n$ , is bijective if and only if  $q = 2$  and  $n$  is odd, as it was conjectured in [8].

## 1 Introduction

Let  $q$  be any prime power and  $n$  a positive integer. Several cryptographic primitives, including ASCON [4] and SHA-3 [6], use the map  $\chi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$  given by  $y = \chi(x)$  with

$$y_i = x_i + x_{i+2} \cdot (1 + x_{i+1})$$

for  $1 \leq i \leq n$ , where the indices are computed modulo  $n$ . Let the symbol  $\odot$  denote the element wise multiplication of two vectors (also known as the Hadamard product), i.e.,  $z = x \odot y$  with  $z_i = x_i \cdot y_i$  for all  $i = 1, \dots, n$ . Further, denote by  $S$  the cyclic left shift operator on  $\mathbb{F}_q^n$ , that is  $S(x_1, \dots, x_n) = (x_2, \dots, x_n, x_1)$ . Let  $S^j$  denote the  $j$ -th iterate of  $S$  for  $j \geq 0$ . Note that  $S^0$  is the identity map. Then  $\chi$  can also be written as

$$\chi(x) = x + S(x) \odot S^2(x) + S^2(x).$$

It is known that  $\chi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  is bijective if and only if  $n$  is odd [2]. Some partial results are proved about bijectivity of  $\chi$  for  $q \neq 2$ . In [8] it was shown that for  $k \geq 1$  the map  $\chi$  is not a permutation, when

- $q$  is odd,
- $q = 2^k$  and  $n$  is even,
- $q = 2^{2k}$  and  $n > 1$  is odd,
- $q = 2^{3k}$  and  $n > 1$  is odd.

In [7] the following additional parameters were ruled out using an approach based on Gröbner basis:

- $q = 2^{5k}$  or  $q = 2^{7k}$  and  $n$  is a multiple of 3 or 5.

It was conjectured in [8] that  $\chi$  is not a permutation in all other cases except when  $q = 2$  and  $n$  odd. We confirm this conjecture using linear algebra methods. More precisely, we prove in Lemmas 3 to 5 that the following result holds:

**Theorem 1.** *For  $q = 2$  the map  $\chi$  is a permutation if and only if  $n$  is odd. For any prime power  $q > 2$ , the map  $\chi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$  is a permutation if and only if  $q$  is even and  $n = 1$ .*

We conclude our note with a short proof for the rank of the linear part of  $\chi(x+a) + \chi(x)$ , which appears in the study of the differential properties of the map  $\chi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ .

## 2 Deriving the linear system

The map  $\chi$  is not a permutation if and only if there exist vectors  $a, x \in \mathbb{F}_q^n$  with  $a \neq 0$  such that

$$\chi(x+a) - \chi(x) = 0. \quad (1)$$

Note that for any  $j$  the map  $S^j$  is linear over  $\mathbb{F}_q$ . Furthermore, the Hadamard product is commutative and distributive with respect to addition, i.e.  $x \odot y = y \odot x$  and  $x \odot (y+z) = x \odot y + x \odot z$  for all  $x, y, z \in \mathbb{F}_q^n$ . Moreover, we have  $S^j(x \odot y) = S^j(x) \odot S^j(y)$ . Using these properties, we obtain

$$\begin{aligned} \chi(x+a) &= x+a + S(x+a) \odot S^2(x+a) + S^2(x+a) \\ &= x+a + [S(x) + S(a)] \odot [S^2(x) + S^2(a)] + S^2(x) + S^2(a) \\ &= x+a + S(x) \odot S^2(x) + S(x) \odot S^2(a) + S(a) \odot S^2(x) + S(a) \odot S^2(a) + S^2(x) + S^2(a) \\ &= \chi(x) + a + S(x) \odot S^2(a) + S(a) \odot S^2(x) + S(a) \odot S^2(a) + S^2(a) \end{aligned}$$

and therefore

$$\chi(x+a) - \chi(x) = a + S^2(a) + S(a \odot S(x) + x \odot S(a) + a \odot S(a)).$$

For a fixed  $a \in \mathbb{F}_q^n \setminus \{0\}$ , the equation  $\chi(x+a) - \chi(x) = 0$  has a solution  $x$  if and only if

$$-a - S^2(a) = S(a \odot S(x) + x \odot S(a) + a \odot S(a))$$

has a solution, which, by applying  $S^{-1}$  on both sides, is equivalent to

$$-S^{-1}(a) - S(a) - a \odot S(a) = a \odot S(x) + x \odot S(a). \quad (2)$$

The right-hand side of (2) is a linear map in  $x$  and hence it reduces to a system of linear equations over  $\mathbb{F}_q$ . We represent this system of equations using matrices:

$$\begin{pmatrix} a_2 & a_1 & & & & & \\ & a_3 & a_2 & & & & \\ & & a_4 & a_3 & & & \\ & & & \ddots & \ddots & & \\ & & & & a_{n-1} & a_{n-2} & \\ & & & & & a_n & a_{n-1} \\ a_n & & & & & & a_1 \end{pmatrix} \cdot x = - \begin{pmatrix} a_1 a_2 + a_2 + a_n \\ a_2 a_3 + a_3 + a_1 \\ a_3 a_4 + a_4 + a_2 \\ \vdots \\ a_{n-2} a_{n-1} + a_{n-1} + a_{n-3} \\ a_{n-1} a_n + a_n + a_{n-2} \\ a_n a_1 + a_1 + a_{n-1} \end{pmatrix}, \quad (3)$$

where  $a = (a_1, \dots, a_n)$ . We denote the coefficient matrix in (3) by  $A(a)$  and the vector in its right-hand side by  $b(a)$ . We abbreviate  $A(a) \cdot x = b(a)$  often by  $(A(a)|b(a))$ .

Observe that the map  $\chi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$  is bijective if and only if for any non-zero  $a \in \mathbb{F}_q^n$  equation (3) has no solution. Our goal is now to check whether (3) has a solution  $x$  for some fixed non-zero  $a$ .

### 3 The case $q > 2$

In this section we show that for  $q > 2$  the map  $\chi$  is a permutation on  $\mathbb{F}_q^n$  if and only if  $q$  is even and  $n = 1$ . We consider separately the cases  $n = 1, 2, 3$  and  $n > 3$ .

First let us assume that  $n = 1$ . In that case  $S(x) = x$  is the identity map and therefore  $\chi(x) = x + S(x) \odot S^2(x) + S^2(x) = x + x^2 + x = x^2 + 2x = x(x + 2)$ , which is a permutation if and only if  $q$  is even, as for  $q$  odd we have  $\chi(0) = \chi(-2)$  and  $\chi$  is not injective.

*Remark 2.* In general for any  $n$  it holds that  $\chi(0, \dots, 0) = \chi(-2, \dots, -2)$  and therefore  $\chi$  is never a permutation in odd characteristic, as noted in [8]. Therefore, from now on we could restrict ourselves to even characteristic. However, the rest of the proof presented here is valid independently of the characteristic of  $\mathbb{F}_q$ , with the minor exception in the case  $n = 3$ .

We continue with  $n = 2$ . In this case (3) has the form

$$\left( \begin{array}{cc|c} a_2 & a_1 & -a_1 a_2 - 2a_2 \\ a_2 & a_1 & -a_1 a_2 - 2a_1 \end{array} \right).$$

This has a solution for example in the case  $a = (1, 1)$  which shows that  $\chi$  is not a permutation.

Next, let  $n = 3$ . Now the system (3) looks like

$$\left( \begin{array}{ccc|c} a_2 & a_1 & & -a_1 a_2 - a_2 - a_3 \\ & a_3 & a_2 & -a_2 a_3 - a_3 - a_1 \\ a_3 & & a_1 & -a_3 a_1 - a_1 - a_2 \end{array} \right). \quad (4)$$

Note that the determinant of the coefficient matrix is  $2a_1 a_2 a_3$ . Therefore, if  $q$  is odd, we can choose  $a_1, a_2, a_3$  all nonzero and the corresponding system always has a solution. In

the case  $q$  even, assume that  $a_2 \neq 0$ . Let  $r_1, r_2, r_3$  be the rows of the system (4). By replacing  $r_3$  with  $a_3r_1 + a_1r_2 + a_2r_3$  we obtain

$$\left( \begin{array}{ccc|c} a_2 & a_1 & & a_1a_2 + a_2 + a_3 \\ & a_3 & a_2 & a_2a_3 + a_3 + a_1 \\ & & 0 & a_1^2 + a_2^2 + a_3^2 + a_1a_2 + a_1a_3 + a_2a_3 + a_1a_2a_3 \end{array} \right). \quad (5)$$

This system has a solution if there exist choices of  $a_1, a_2, a_3 \in \mathbb{F}_q$  such that  $a_2, a_3 \neq 0$  and

$$a_1^2 + (a_2 + a_3 + a_2a_3)a_1 + (a_2a_3 + a_2^2 + a_3^2) = 0, \quad (6)$$

which is a quadratic equation in  $a_1$ . Having in mind, that in binary fields a quadratic equation  $X^2 + uX + v = 0$  has always a solution if  $u = 0$ , we put  $a_2 + a_3 + a_2a_3 = 0$  in (6). Equivalently, by adding 1 on both sides,  $(a_2 + 1)(a_3 + 1) = 1$ . As  $q > 2$ , we can choose an element  $a_3 \in \mathbb{F}_q \setminus \{0, 1\}$  and then  $a_2 = \frac{1}{a_3+1} + 1 = \frac{a_3}{a_3+1} \neq 0$ . For these  $a_2, a_3 \neq 0$  the quadratic equation (6) has a solution  $a_1 \in \mathbb{F}_q$ , implying the existence of  $(a_1, a_2, a_3) \neq 0$  for which the linear system (5) has a solution  $x$ .

We have thus proved the following lemma.

**Lemma 3.** *Let  $q > 2$ . If  $n = 1$  then  $\chi$  is a permutation if and only if  $q$  is even. If  $n = 2, 3$  then  $\chi$  is not a permutation.*

Let now  $n > 3$ . Again, we show that for certain choices of the vector  $a \in \mathbb{F}_q^n \setminus \{0\}$  the equation (3) admits a solution  $x$ . Let  $a_n = 0$ . Then the linear system (3) reduces to

$$\left( \begin{array}{cccc|c} a_2 & a_1 & & & -a_1a_2 - a_2 \\ & a_3 & a_2 & & -a_2a_3 - a_3 - a_1 \\ & & a_4 & a_3 & -a_3a_4 - a_4 - a_2 \\ & & & \ddots & \vdots \\ & & & & a_{n-1} & a_{n-2} & 0 & -a_{n-2}a_{n-1} - a_{n-1} - a_{n-3} \\ & & & & 0 & 0 & a_{n-1} & -a_{n-2} \\ & & & & 0 & 0 & a_1 & -a_1 - a_{n-1} \end{array} \right).$$

Further, let all  $a_1, \dots, a_{n-1}$  be non-zero and assume

$$\det \begin{pmatrix} a_{n-1} & a_{n-2} \\ a_1 & a_1 + a_{n-1} \end{pmatrix} = 0,$$

or equivalently,  $a_{n-1}(a_1 + a_{n-1}) = a_1a_{n-2}$ . Under this assumption there is a solution  $x \in \mathbb{F}_q^n$ . Indeed we can choose  $x_{n-1}$  arbitrarily, for example  $x_{n-1} = 1$ , and then  $x_n = -\frac{a_{n-2}}{a_{n-1}}$ . The remaining components are obtained by simple back substitution, as the other diagonal entries are all nonzero.

Now it remains to see that there are non-zero  $a_1, a_{n-1}, a_{n-2} \in \mathbb{F}_q$  such that the assumption  $a_{n-1}(a_1 + a_{n-1}) = a_1a_{n-2}$  is satisfied. Note that because  $n > 3$  the components  $a_1, a_{n-1}, a_{n-2}$  do not coincide. Let  $a_{n-1} = 1$  and choose  $a_1 \in \mathbb{F}_q \setminus \{0, -1\}$  arbitrarily. Then  $a_1 + 1 \neq 0$  and  $a_{n-2} = \frac{a_1+1}{a_1} \neq 0$ , fulfilling the requirements.

We have thus proved the following result.

**Lemma 4.** *Let  $q > 2$  and  $n > 3$ . Then  $\chi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$  is not a permutation.*

## 4 The special case $q = 2$

It is known that for  $q = 2$  the map  $\chi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  is bijective if and only if  $n$  is odd. If  $n$  is even it is easy to see that  $\chi$  is not a permutation. Indeed,

$$\chi(1, 0, 1, 0, \dots, 1, 0) = (0, \dots, 0) = \chi(0, \dots, 0),$$

as it has been noted in [2]. The fact that  $\chi$  is a permutation for  $n$  odd was proved in [2] by using a seed-and-leap method to compute the preimage of a given element  $y \in \mathbb{F}_2^n$ . A more detailed proof of this approach can be found in [3]. Another method to compute the inverse of  $\chi$  for  $n$  odd is given in Appendix D of [1], however without a proof. In [5] an explicit inverse formula of  $\chi$  is given and proved.

To have a unified proof for Theorem 1, we present here a short proof for the statement that  $\chi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  is bijective if  $n$  is odd, applying the method developed in the previous sections.

Let now  $n$  be odd. If  $n = 1$  then  $\chi(x) = x^2 = x$  which is a permutation. So now assume  $n \geq 3$ . Let  $a \in \mathbb{F}_2^n \setminus \{0\}$  be arbitrary. We aim to show that there is no solution  $x$  to  $\chi(x) + \chi(x + a) = 0$ . It can be easily seen that  $\chi$  is shift-invariant, i.e.  $S(\chi(x)) = \chi(S(x))$  for all  $x \in \mathbb{F}_2^n$ . Therefore, if  $\chi(x) + \chi(x + a) = 0$  has a solution, then it follows that also

$$0 = S(0) = S(\chi(x) + \chi(x + a)) = \chi(S(x)) + \chi(S(x) + S(a))$$

and there also exists a solution  $S(x)$  for  $S(a)$ .

In the following we show that (3) has no solution by considering three cases. First we assume that  $a$  has two consecutive entries which are zero. Next we will assume that  $a$  has a zero entry such that the entries before and after are both nonzero. And finally we will assume that  $a$  only has nonzero entries.

Suppose now (3) has a solution  $x$  for a non-zero  $a$  with  $a_i = a_{i+1} = 0$  for some  $1 \leq i \leq n$ . Since  $\chi$  is shift-invariant, by considering an appropriate shift of  $a$ , we may assume without loss of generality that  $a_n = a_1 = 0$ . The last row of (3) then looks as follows:

$$\left( \begin{array}{cc|c} 0 & & 0 \mid a_{n-1} \end{array} \right).$$

As the system has a solution  $x$ , it then follows that  $a_{n-1} = 0$ . However, then by considering the  $(n-1)$ -th row, it follows that also  $a_{n-2} = 0$ . By repeating this argument we obtain  $a = 0$ , a contradiction.

Next we assume that there exists an index  $i \in \{1, \dots, n\}$  such that  $a_i = 0$  and  $a_{i-1} = a_{i+1} = 1$ . Again, by considering shifts of  $a$ , we may assume that  $i = n$ . From the last two rows of (3) it then immediately follows that  $a_{n-2} = x_n = 0$ . If  $a_{n-3} = 0$ , then we are in the previous case. Otherwise, we can repeat this argument and obtain that  $a_{n-2k} = 0$  for all integers  $k$ . However, using that  $n = 2m + 1$  is odd, we then also obtain  $a_{n-2m} = a_1 = 0$ , a contradiction to the assumption that  $a_1 \neq 0$ .

Finally, we need to consider  $a = (1, \dots, 1)$ . In this case (3) reduces to

$$\left( \begin{array}{cccccc|c} 1 & 1 & & & & & 1 \\ & 1 & 1 & & & & 1 \\ & & 1 & 1 & & & 1 \\ & & & \ddots & \ddots & & \vdots \\ & & & & 1 & 1 & 1 \\ & & & & & 1 & 1 \\ 1 & & & & & & 1 \end{array} \right)$$

By adding every of the first  $n - 1$  rows to the last one, we obtain (using that  $n - 1$  is even) the row

$$\left( 0 \quad \quad \quad 0 \mid 1 \right)$$

which means that the equation has no solution.

The above considerations imply the following result:

**Lemma 5.** *The map  $\chi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  is a permutation if and only if  $n$  is odd.*

**Open Problem 6.** Can our approach be used to find more information on the image set of  $\chi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ , like its size or the preimage distribution?

## 5 Rank of the coefficient matrix $A(a)$ over $\mathbb{F}_2$

The equation (3) appears in the study of differential and linear properties of  $\chi$ . In particular, the ranks of matrices  $A(a)$  allow to determine the Walsh spectrum of  $\chi$ . In [8] the following proposition is proved:

**Proposition 7.** *For any  $a \in \mathbb{F}_2^n$  the rank of the matrix  $A(a)$  over  $\mathbb{F}_2$  is given by*

$$\text{rank } A(a) = \omega(a) := \begin{cases} n - 1, & a = (1, \dots, 1) \\ \text{wt}(a) + \text{r}(a), & \text{otherwise} \end{cases}$$

where  $\text{wt}(a)$  is the Hamming weight and  $\text{r}(a)$  is the number of 001-patterns in  $a$ . More precisely,  $\text{r}(a)$  is the number of indices  $i = 1, \dots, n$  such that  $(a_i, a_{i+1}, a_{i+2}) = (0, 0, 1)$  where the indices are computed modulo  $n$ .

We present a shorter proof of this fact using induction on  $n$ .

**Claim 8.** *Proposition 7 is true for  $n = 1, 2, 3$ .*

*Proof.* For  $n = 1$ , observe that  $A(a_1) = (2a_1) = (0)$ , and  $\text{rank } A(0) = \text{rank } A(1) = 0 = \omega(1) = \omega(0)$ . For  $n = 2$  we have

$$A(a_1, a_2) = \begin{pmatrix} a_2 & a_1 \\ a_2 & a_1 \end{pmatrix}.$$

It is easily seen that,  $\text{rank } A(0,0) = 0 = \omega(0,0)$  and  $\text{rank } A(1,1) = \text{rank } A(1,0) = \text{rank } A(0,1) = 1 = \omega(1,1) = \omega(1,0) = \omega(0,1)$ . Let  $n = 3$ , in which case

$$A(a_1, a_2, a_3) = \begin{pmatrix} a_2 & a_1 & \\ & a_3 & a_2 \\ a_3 & & a_1 \end{pmatrix}. \quad (7)$$

Using the shift-invariance of the rank of  $A(a)$ , we only need to consider the cases when  $a$  equals  $(0,0,0)$ ,  $(1,0,0)$ ,  $(1,1,0)$ , or  $(1,1,1)$ . It is easily seen that  $\text{rank } A(0,0,0) = 0 = \omega(0,0,0)$  and  $\omega(1,0,0) = 2 = \text{rank } A(1,0,0)$  and  $\omega(1,1,0) = 2 = \text{rank } A(1,1,0)$  and  $\omega(1,1,1) = 2 = \text{rank } A(1,1,1)$ .  $\square$

**Claim 9.** *Proposition 7 is true for  $a = (0, \dots, 0)$  and  $a = (1, \dots, 1)$  with  $n \geq 3$ .*

*Proof.* If  $a = (0, \dots, 0)$  then  $A(a)$  is the zero matrix and  $\text{rank } A(a) = 0 = \omega(a)$  is clear.

If  $a = (1, \dots, 1)$ , then the first  $n - 1$  rows of  $A(a)$  are linearly independent, so  $\text{rank } A(a) \geq n - 1$ . On the other hand,  $(1, \dots, 1)$  is in the kernel of  $A(a)$ , so  $\text{rank } A(a) \leq n - 1$  and therefore  $\text{rank } A(a) = n - 1 = \omega(a)$ .  $\square$

We now proceed by induction on  $n$ . Let  $n > 3$  be fixed and assume that the claim is true for all vectors  $u \in \mathbb{F}_2^k$  with  $k < n$ . Let  $a \in \mathbb{F}_2^n$ . If  $a = (0, \dots, 0)$  or  $a = (1, \dots, 1)$  then the claim is true by Claim 9. Therefore, we may assume that  $a \neq (0, \dots, 0), (1, \dots, 1)$ . Note that from the shift-invariance of  $\chi$  it follows that the rank of  $A(a)$  is invariant under shifts of  $a$ . Equivalently, this can also be seen by switching rows and columns. Therefore, we can assume that  $a_1 = 1, a_n = 0$ . We write the vector  $a$  in the following form:

$$a = (\underbrace{1, *, \dots, *, 0}_{=u}, \underbrace{1, \dots, 1}_{=v}, \underbrace{0, \dots, 0}_{=w})$$

More precisely, let  $k$  be the last index such that  $a_k = 1$  and  $a_j$  be the first index such that  $a_i = 1$  for all  $i = j, \dots, k$ . Then  $u = (a_1, \dots, a_{j-1}) = (1, *, \dots, *, 0)$ ,  $v = (a_j, \dots, a_k) = (1, \dots, 1)$  and  $w = (a_{k+1}, \dots, a_n) = (0, \dots, 0)$ . Note that we allow the vector  $u$  to be empty. This happens if and only if  $a = (1, \dots, 1, 0, \dots, 0)$ , equivalently,  $j = 1$ . If  $a$  contains at least one occurrence of a 001-pattern, then by shift-invariance we can assume that  $w$  contains at least two zeros. Otherwise,  $w = (0)$ .

Note that  $\text{wt}(a) = \text{wt}(u) + \text{wt}(v) = \text{wt}(u) + (k - j + 1)$ . Now consider the 001-patterns. Any 001-pattern in  $a$  either is completely contained inside  $u$ , ends exactly at  $a_j$  or ends at  $a_1$ . In the first case the 001-pattern is also contained in  $u$ . In the second case we know that  $u = (1, *, \dots, *, 0, 0)$  ends in at least two zeros, and it also has a 001-pattern which ends at  $a_1$ . The last case occurs if and only if  $w$  has at least two zeros. It follows that

$$r(a) = \begin{cases} r(u) + 1 & w \text{ contains at least two zeros} \\ r(u) & \text{otherwise.} \end{cases}$$

Then the matrix  $A(a)$  has the following form:

$$= \begin{pmatrix} \begin{array}{ccc|ccc} a_2 & a_1 & & & & \\ & \ddots & \ddots & & & \\ & & a_{j-1} & a_{j-2} & & \\ 0 & & a_j & a_{j-1} & & \\ \hline & & a_{j+1} & a_j & & \\ & & & \ddots & \ddots & \\ & & & & a_{k-1} & a_{k-2} \\ & & & & a_k & a_{k-1} \\ \hline & & & & a_{k+1} & a_k \\ & & & & a_{k+2} & a_{k+1} \\ & & & & & \ddots \\ & & & & & \ddots \\ & & & & & a_n & a_{n-1} \\ & & & & & & a_1 \end{array} \\ \begin{array}{ccc|ccc} a_2 & a_1 & & & & \\ & \ddots & \ddots & & & \\ & & 0 & a_{j-2} & & \\ 0 & & 1 & & & \\ \hline & & & & & \\ & & & 1 & 1 & \\ & & & & \ddots & \ddots \\ & & & & & 1 & 1 \\ & & & & & 1 & 1 \\ \hline & & & & & 0 & 1 \\ & & & & & 0 & 0 \\ & & & & & & \ddots \\ & & & & & & \ddots \\ & & & & & & 0 & 0 \\ & & & & & & & 1 \end{array} \end{pmatrix} \quad (8)$$

Note that  $A(a)$  is a block diagonal matrix. The first block is the matrix  $A(u)$  with  $\text{rank } A(u) = \omega(u)$  by the induction hypothesis. This also holds in the degenerate case that  $u$  is empty if we then define  $\omega(u) = 0$ . The second block has rank  $k - j$ . Note that if  $k = j$  then the second block is empty. The third block has rank 2 if  $w$  includes at least two zeros, otherwise it has the form  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  and has rank 1. Remember that the rank of a block diagonal matrix is the sum of the ranks of the blocks on the diagonal. It follows



that

$$\begin{aligned}
 \text{rank } A(a) &= \omega(u) + (k - j) + \begin{cases} 2 & w \text{ contains at least two zeros} \\ 1 & \text{otherwise} \end{cases} \\
 &= \text{wt}(u) + (k - j + 1) + \text{r}(u) + \begin{cases} 1 & w \text{ contains at least two zeros} \\ 0 & \text{otherwise} \end{cases} \\
 &= \text{wt}(a) + \text{r}(a) = \omega(a).
 \end{aligned}$$

For clarity, we also write down how (8) looks in the degenerate cases, namely that  $u$  empty,  $j = k$  or both. We keep the horizontal and vertical lines to show which blocks vanish. If  $u$  is empty and  $j < k$ , then  $a = (1, \dots, 1, 0, \dots, 0)$  and

$$A(a) = \left( \begin{array}{ccc|ccc} 1 & 1 & & & & \\ & \ddots & \ddots & & & \\ & & 1 & 1 & & \\ & & & 1 & 1 & \\ \hline & & & & 0 & 1 \\ 0 & & & & & 0 & 0 & \ddots & \ddots & & \\ & & & & & & \ddots & \ddots & & 0 & 0 \\ & & & & & & & & & 1 & 1 \end{array} \right).$$

If  $u$  is not empty and  $j = k$ , then  $a = (1, *, \dots, *, 0, 1, 0, \dots, 0)$  and

$$A(a) = \left( \begin{array}{ccc|ccc} a_2 & a_1 & & & & \\ & \ddots & \ddots & & & \\ & & 0 & a_{j-2} & & \\ \hline 0 & & & 1 & 0 & 0 \\ \hline & & & & 0 & 1 \\ & & & & 0 & 0 & \ddots & \ddots & & 0 & 0 \\ & & & & & & \ddots & \ddots & & 1 & 1 \end{array} \right).$$

If  $u$  is empty and  $j = k$ , then  $a = (1, 0, \dots, 0)$  and

$$A(a) = \left( \begin{array}{ccc|ccc} 0 & 1 & & & & \\ & 0 & 0 & & & \\ & & \ddots & \ddots & & \\ & & & 0 & 0 & \\ \hline 0 & & & & 1 & \end{array} \right).$$

## References

- [1] Alex Biryukov, Charles Bouillaguet, and Dmitry Khovratovich. *Cryptographic Schemes Based on the ASASA Structure: Black-box, White-box, and Public-key*. Cryptology ePrint Archive, Paper 2014/474. 2014. URL: <https://eprint.iacr.org/2014/474> (visited on 01/18/2024).
- [2] Joan Daemen. “Cipher and hash function design strategies based on linear and differential cryptanalysis”. PhD thesis. KU Leuven, 1995.
- [3] Joan Daemen, René Govaerts, and Joos Vandewalle. “An efficient nonlinear shift-invariant transformation”. In: *Proceedings of the 15th Symposium on Information Theory in the Benelux*. Werkgemeenschap voor Informatie- en Communicatietheorie, 1994.
- [4] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schl  ffer. “Ascon v1.2: Lightweight Authenticated Encryption and Hashing”. In: *Journal of Cryptology* 34.3 (June 2021), p. 33. ISSN: 1432-1378. DOI: [10/gtfgst](https://doi.org/10.1007/s10623-024-01395-w).
- [5] Fukang Liu, Santanu Sarkar, Willi Meier, and Takanori Isobe. “The Inverse of  $\chi$  and Its Applications to Rasta-Like Ciphers”. In: *Journal of Cryptology* 35.4 (Oct. 2022), p. 28. ISSN: 1432-1378. DOI: [10/gtfgn7](https://doi.org/10.1007/s10623-024-01395-w).
- [6] NIST. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. Tech. rep. Federal Information Processing Standard (FIPS) 202. U.S. Department of Commerce, Aug. 2015. DOI: [10.6028/NIST.FIPS.202](https://doi.org/10.6028/NIST.FIPS.202).
- [7] Kamil Ota  . *A Solution to a Conjecture on the Maps  $\chi_n^{(k)}$* . Cryptology ePrint Archive, Paper 2023/1782. 2023. URL: <https://eprint.iacr.org/2023/1782> (visited on 01/18/2024).
- [8] Jan Schoone and Joan Daemen. “Algebraic properties of the maps  $\chi_n$ ”. In: *Designs, Codes and Cryptography* (2024). DOI: [10.1007/s10623-024-01395-w](https://doi.org/10.1007/s10623-024-01395-w).