A Solution to a Conjecture on the Maps $\chi_n^{(k)}$

Kamil Otal

TÜBİTAK BİLGEM National Institute of Electronics and Cryptology, Kocaeli, Türkiye
kamil.otal@gmail.com

Abstract

The Boolean map $\chi_n^{(k)} : \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^n$, $x \mapsto u$ given by $u_i = x_i + (x_{(i+1) \bmod n} + 1)x_{(i+2) \bmod n}$ appears in various permutations as a part of cryptographic schemes such as KECCAK-f, ASCON, Xoodoo, Rasta, and Subterranean (2.0). Schoone and Daemen investigated some important algebraic properties of $\chi_n^{(k)}$ in [IACR Cryptology ePrint Archive 2023/1708]. In particular, they showed that $\chi_n^{(k)}$ is not bijective when

- n is even,
- n is odd and k is even,
- n is odd and k is a multiple of 3.

They left the remaining cases as a conjecture. In this paper, we examine this conjecture by taking some smaller sub-cases into account by reinterpreting the problem via the Gröbner basis approach. As a result, we prove that $\chi_n^{(k)}$ is not bijective when

- n is a multiple of 3 or 5, and k is a multiple of 5 or 7.

We then present an algorithmic method that solves the problem for any given arbitrary n and k by generalizing our approach. We also discuss the systematization of our proof and computational boundaries.

1 Introduction

Let $\mathbb{F}_p$ be the finite field of size prime p, $\mathbb{F}_{p^k}$ denote the k.th degree field extension of $\mathbb{F}_p$, and $\mathbb{F}_{p^k}^n$ represent the standard n-dimensional vector space of n-tuples over $\mathbb{F}_{p^k}$. Fix p and define the Boolean map $\chi_n^{(k)} : \mathbb{F}_{p^k}^n \to \mathbb{F}_{p^k}^n$, $x \mapsto u$ given by $u_i = x_i + (x_{(i+1) \bmod n} + 1)x_{(i+2) \bmod n}$. There are various cryptographic uses of such functions in the literature, we list some known examples as follows.

- For $p = 2$, $\chi_5^{(1)}$ is used in KECCAK-f [3] (which is a part of the NIST's standard cryptographic hash algorithm SHA-3 [1]) and ASCON [12] (the winner of the NIST lightweight cryptography competition [18]).
- For $p = 2$, $\chi_3^{(1)}$ is used in another cryptographic algorithm Xoodoo [8].

- ◇ For $p = 2$, $\chi_n^{(1)}$ is used in Rasta [11] where n represents the block-length and always odd.
- ◇ For $p = 2$, Subterranean (2.0) [6, 9] uses $\chi_{257}^{(1)}$.

It is important to understand the algebraic properties of the maps $\chi_n^{(k)}$ since they are used in many cryptographic applications. Each of the properties of $\chi_n^{(k)}$ could be exploited in an attack, or conversely be used to argue for security properties. For instance, in [7] and [10], the differential and correlation properties (related to differential [4] and linear [15] cryptanalysis) have been studied. We can list some of the results about the cryptographically important algebraic properties of $\chi_n^{(k)}$ as follows.

- ◇ For $p = 2$ and $k = 1$, it is known from [7] that $\chi_n^{(k)}$ is invertible if and only if n is odd.
- ◇ For $p = 2$ and $k = 1$, the order of $\chi_n^{(k)}$ and its cycle structure are also known from [17].
- ◇ For $p = 2$, $k = 1$, and n is odd; we know a direct formula for the inverse function of $\chi_n^{(k)}$ from [14].
- ◇ Recently, Schoone and Daemen investigated various algebraic properties of such functions thoroughly in [16]. We can summarize their results as follows.
  - For $p = 2$ and $k = 1$, the map can be represented as a univariate polynomial through an isomorphism between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$. We remark that this representation can be used to attack ciphers, see [5] and [13] for example. The authors study these univariate representations for $\chi_n^{(k)}$ to give an insight in these representations.
  - They investigated how many monomials of a certain degree occur in the formula of the inverse of the map $\chi_n^{(k)}$.
  - They examined the bijectivity of $\chi_n^{(k)}$ (note that the bijectivity is an important property since it is a must feature for the confusion layer of SPN ciphers and some sponge constructions). Their results can be listed as follows.
    - When p is odd, $\chi_n^{(k)}$ is not invertible.
    - When $p = 2$ and n is even, $\chi_n^{(k)}$ is not invertible.
    - When $p = 2$, n is odd, and k is even; $\chi_n^{(k)}$ is not invertible.
    - When $p = 2$, n is odd, and k is a multiple of 3; $\chi_n^{(k)}$ is not invertible.
    - For the remaining cases, they conjectured that $\chi_n^{(k)}$ is not invertible.

In this paper, we focus on this conjecture and start from the simplest cases. We reinterpret the problem by utilizing the Gröbner basis approach. We also apply some algebraic manipulations carefully by the help of the computer algebra program Magma [2]. As a result, we provide concrete solutions for n is a multiple of 3 or 5, and k is

a multiple of 5 or 7. We then present an algorithmic method that solves the problem for any given arbitrary n and k by generalizing our approach. We also discuss the systematization of our proof and computational boundaries.

2 When n is a Multiple of 3

The conjecture in [16] comprises only fields of even characteristics, therefore we fix $p = 2$ for the rest of the paper.

One of the simplest cases within the conjecture is the $n = 3$ and $k = 5$ case. A brute force algorithm examining whether there exist distinct $x = (x_0, x_1, x_2), y = (y_0, y_1, y_2) \in \mathbb{F}_{2^5}^3$ satisfying $\chi_3^{(5)}(x) = \chi_3^{(5)}(y)$, i.e.

$$\begin{aligned} x_0 + x_1x_2 + x_2 &= y_0 + y_1y_2 + y_2 \\ x_1 + x_2x_0 + x_0 &= y_1 + y_2y_0 + y_0 \\ x_2 + x_0x_1 + x_1 &= y_2 + y_0y_1 + y_1 \end{aligned}$$

easily gives $x = (1, 1, w)$ and $y = (w^{13}, w^{12}, w^{22})$ as a solution, where $w \in \mathbb{F}_{2^5}$ is a root of the 5th degree irreducible polynomial $X^5 + X^2 + 1$ over $\mathbb{F}_2$.

Another simple case is for $n = 3$ and $k = 7$. A brute force algorithm examining whether there exist distinct $x = (x_0, x_1, x_2), y = (y_0, y_1, y_2) \in \mathbb{F}_{2^7}^3$ satisfying $\chi_3^{(7)}(x) = \chi_3^{(7)}(y)$ easily gives $x = (1, 1, w)$ and $y = (w^{86}, w^{81}, w^{43})$ as a solution, where $w \in \mathbb{F}_{2^7}$ is a root of the 7th degree irreducible polynomial $X^7 + X + 1$ over $\mathbb{F}_2$.

In general, a brute force searches for $2n$ unknowns $x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}$ among 2^k elements, i.e. 2^{2kn+1} computations of $\chi_n^{(k)}(x)$ are expected. However, the number of expected solutions is 2^{kn} since we have $2n$ unknowns and n equations. Therefore, a solution appears by approximately 2^{kn+1} computations. On the other hand, the following theorem lets us generalize our results for larger k and n values without any additional computational cost.

Theorem 1. *Let $n = ms$ and $k = lr$ for some integers $l, m, r, s > 1$. Suppose that x and y are two distinct elements from $\mathbb{F}_{2^r}^s$ satisfying $\chi_s^{(r)}(x) = \chi_s^{(r)}(y)$. Then any m times repetitions of x and y (i.e. $x^m = x||x||\cdots||x$ and $y^m = y||y||\cdots||y$) are distinct and satisfy $\chi_n^{(k)}(x^m) = \chi_n^{(k)}(y^m)$.*

Proof. It is clear that $\mathbb{F}_{2^r}$ is a subset of $\mathbb{F}_{2^k} (= \mathbb{F}_{2^{rl}})$. Also note that we concatenate the images $u = \chi_s^{(k)}(x)$ and $v = \chi_s^{(k)}(y)$ m times when we concatenate x and y m times since $\mathbb{Z}_s$ is embedded in $\mathbb{Z}_n (= \mathbb{Z}_{ms})$ periodically. □

As a result, our computation cost for the brute force is 2^{rs+1} (rather than 2^{kn+1}), where r and s are some prime numbers dividing k and n, respectively.

Corollary 1. *The conjecture in [16] is true when $n = 3m$ and $k = 5l$ or $7l$ for some positive integers m and l.*

3 When n is a Multiple of 5

The complexity of the brute force is smaller than we expected at the beginning thank to Theorem 1 (i.e. 2^{rs+1} rather than 2^{kn+1}, where r and s are some prime numbers dividing k and n, respectively). Therefore, we need to figure out the case in which n has only large prime divisors. Note that the brute force approach can be exhaustive while r and s get bigger. In this section, we solve this problem by utilizing the Gröbner basis approach together with some additional algebraic manipulations.

We start with the case $n = 5$ and $k = 5$. Note that the equation system

$$\begin{aligned} x_0 + x_1x_2 + x_2 &= y_0 + y_1y_2 + y_2 \\ x_1 + x_2x_3 + x_3 &= y_1 + y_2y_3 + y_3 \\ x_2 + x_3x_4 + x_4 &= y_2 + y_3y_4 + y_4 \\ x_3 + x_4x_0 + x_0 &= y_3 + y_4y_0 + y_0 \\ x_4 + x_0x_1 + x_1 &= y_4 + y_0y_1 + y_1 \end{aligned}$$

is required for our purpose. We can extend this system by adding

$$\begin{aligned} x_0 &= 0 \\ y_0 &= 1 \end{aligned}$$

to satisfy $x \neq y$. We need only one solution, hence we can add two more restrictions as follows.

$$\begin{aligned} x_1 &= 0 \\ x_2 &= 0 \end{aligned}$$

and fix y_4 as the primitive element of $\mathbb{F}_{2^5}$ by adding

$$y_4^5 + y_4^2 + 1 = 0.$$

Remark that we selected y_4 as the primitive element since y_4 is the last element in the lexicographic order, hence all the other $x_0, \ldots, x_4, y_0, \ldots, y_3$ values can be represented as a function of y_4 when we apply the Gröbner basis computations. The ideal I generated by the polynomials

$$\begin{aligned} &x_0, \\ &x_1, \\ &x_2, \\ &y_0 + 1, \\ &y_4^5 + y_4^2 + 1, \\ &x_0 + x_1x_2 + x_2 + y_0 + y_1y_2 + y_2, \\ &x_1 + x_2x_3 + x_3 + y_1 + y_2y_3 + y_3, \\ &x_2 + x_3x_4 + x_4 + y_2 + y_3y_4 + y_4, \\ &x_3 + x_4x_0 + x_0 + y_3 + y_4y_0 + y_0, \\ &x_4 + x_0x_1 + x_1 + y_4 + y_0y_1 + y_1 \end{aligned}$$

over $\mathbb{F}_2$ is reduced to

$$\begin{aligned}
&x_0,\\
&x_1,\\
&x_2,\\
&x_3+1,\\
&x_4+y_4,\\
&y_0+1,\\
&y_1+y_4^3+y_4^2+y_4+1,\\
&y_2+y_4^2+y_4,\\
&y_3+y_4,\\
&y_4^5+y_4^2+1,
\end{aligned}$$

by using the Gröbner basis approach via Magma [2], which corresponds to the solution $x = (0, 0, 0, 1, w)$ and $y = (1, w^3 + w^2 + w + 1, w^2 + w, w, w)$, where w is a root of $X^5 + X^2 + 1$ over $\mathbb{F}_2$.

A similar procedure can be applied for the $n = 5$ and $k = 7$ case, by considering $X^7 + X + 1$ instead of $X^5 + X^2 + 1$, and the following result is obtained:

$$\begin{aligned}
&x = (0, 0, 0, w^5 + w^4 + w^2 + w, w) \text{ and}\\
&y = (1, w^5 + w^4 + w^3 + w^2 + w, w^2 + w, w^5 + w^4 + w^2 + 1, w),
\end{aligned}$$

where w is a root of $X^7 + X + 1$ over $\mathbb{F}_2$. As a result, we can obtain the following corollary by the help of Theorem 1.

Corollary 2. *The conjecture in [16] is true when $n = 5m$ and $k = 5l$ or $7l$ for some positive integers m and l.*

4 A Generalization of Our Method

We can generalize the method in Section 3 for more general n values. We can apply the following procedure for this purpose.

1. Let s be the smallest prime divisor of n and r be the smallest prime divisor of k. If $s \in \{2, 3, 5\}$ and $r \in \{2, 3, 5, 7\}$ then the conjecture in [16] is true by the results up to now. Otherwise, we apply the next step.

2. Construct the ideal I generated by $2s$ polynomials

$$\begin{aligned}
&x_0,\\
&x_1,\\
&\vdots\\
&x_{s-3},\\
&y_0+1,\\
&f(y_{s-1}),\\
&x_0+x_1x_2+x_2+y_0+y_1y_2+y_2,\\
&x_1+x_2x_3+x_3+y_1+y_2y_3+y_3,\\
&\vdots\\
&x_{s-1}+x_0x_1+x_1+y_{s-1}+y_0y_1+y_1
\end{aligned}$$

   generated by $2s$ variables $x_0, x_1, \ldots, x_{s-1}, y_0, y_1, \ldots, y_{s-1}$, where $f(X)$ is a primitive polynomial of degree r over $\mathbb{F}_2$.

3. Apply the Gröbner basis reduction procedure by considering the lexicographic order $x_0 < x_1 < \cdots < x_{s-1} < y_0 < y_1 < \cdots < y_{s-1}$.

4. If the resulting ideal has a common zero (x, y), then take x^m and y^m as the solution for the main problem. Otherwise, repeat Step 2 by changing one of the first $s-2$ polynomials in the ideal I linearly (i.e. taking x_1+1 instead of x_1 for example) or removing one of the first $s-2$ polynomials (i.e. x_1 can be removed for example).

5 Conclusion and Future Work

We remark that the 4-step procedure in Section 4 yields one solution with high probability since the expected number of solutions is 2^{nk}. We also emphasize that the procedure in Section 4 can be manipulated for any other Boolean functions in case of necessity.

Another advantage of our method is that the problem is reduced to prime n and prime k from odd n and odd k. Therefore, we can reduce the conjecture in [16] as follows: $\chi_n^{(k)}$ is not invertible for any prime n and prime k.

On the other hand, our method is an algorithmic solution and gives no result when n and k are sufficiently large prime numbers because of the computational cost. Therefore, it seems interesting as a future work to look for another mathematical solution that contains all possible n and k values even if they are large prime numbers.

References

[1] FIPS 202 SHA-3 Standard: Permutation-based hash and extendable-output functions.

[2] Magma computational algebra system. http://magma.maths.usyd.edu.au/magma/. Accessed: 2023-11-08.

[3] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. KECCAK Specifications. *Submission to NIST (round 2)*, 3(30):320–337, 2009.

[4] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4:3–72, 1991.

[5] Carlos Cid, Lorenzo Grassi, Aldo Gunsing, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. Influence of the linear layer on the algebraic degree in SP-Networks. *IACR Transactions on Symmetric Cryptology*, 2022(1):110–137, Mar. 2022.

[6] L. Claesen, J. Daemen, M. Genoe, and G. Peeters. Subterranean: A 600 mbit/sec cryptographic vlsi chip. In *Proceedings of 1993 IEEE International Conference on Computer Design ICCD'93*, pages 610–613, 1993.

[7] Joan Daemen. *Cipher and hash function design strategies based on linear and differential cryptanalysis.* PhD thesis, Doctoral Dissertation, March 1995, KU Leuven, 1995.

[8] Joan Daemen, Seth Hoffert, Gilles Van Assche, and Ronny Van Keer. The design of Xoodoo and Xoofff. *IACR Transactions on Symmetric Cryptology*, pages 1–38, 2018.

[9] Joan Daemen, Pedro Maat Costa Massolino, Alireza Mehrdad, and Yann Rotella. The Subterranean 2.0 cipher suite. *IACR Transactions on Symmetric Cryptology*, pages 262–294, 2020.

[10] Joan Daemen, Alireza Mehrdad, and Silvia Mella. Computing the distribution of differentials over the non-linear mapping χ. In *International Conference on Security, Privacy, and Applied Cryptography Engineering*, pages 3–21. Springer, 2021.

[11] Christoph Dobraunig, Maria Eichlseder, Lorenzo Grassi, Virginie Lallemand, Gregor Leander, Eik List, Florian Mendel, and Christian Rechberger. Rasta: a cipher with low anddepth and few ands per bit. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I 38*, pages 662–692. Springer, 2018.

[12] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2: Lightweight authenticated encryption and hashing. *Journal of Cryptology*, 34:1–42, 2021.

[13] Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, Markus Schofnegger, and Qingju Wang. An algebraic attack on

ciphers with low-degree round functions: Application to full MiMC. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 477–506. Springer, 2020.

[14] Fukang Liu, Santanu Sarkar, Willi Meier, and Takanori Isobe. The inverse of χ and its applications to Rasta-like ciphers. *Journal of Cryptology*, 35(4):28, 2022.

[15] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 386–397. Springer, 1993.

[16] Jan Schoone and Joan Daemen. Algebraic properties of the maps χ_n. *IACR Cryptology ePrint Archive, 2023/1708*, 2023.

[17] Jan Schoone and Joan Daemen. The state diagram of χ_n. *IACR Cryptology ePrint Archive, 2023/328*, 2023.

[18] Meltem Sönmez Turan, Kerry McKay, Donghoon Chang, Lawrence E Bassham, Jinkeon Kang, Noah D Waller, John M Kelsey, and Deukjo Hong. Status report on the final round of the NIST Lightweight Cryptography Standardization Process. 2023.