Cryptogr. Commun. (2019) 11:379–384
https://doi.org/10.1007/s12095-018-0317-2

Decomposition of permutations in a finite field

Svetla Nikova[1] · **Ventzislav Nikov**[2] · **Vincent Rijmen**[1]

Received: 29 November 2017 / Accepted: 14 June 2018 / Published online: 23 June 2018

Abstract We describe a method to decompose any power permutation, as a sequence of power permutations of lower algebraic degree. As a result we obtain decompositions of the inversion in $\mathrm{GF}(2^n)$ for small n from 3 up to 16, as well as for the APN functions, when $n = 5$. More precisely, we find decompositions into *quadratic* power permutations for any n not multiple of 4 and decompositions into *cubic* power permutations for n multiple of 4. Finally, we use the Theorem of Carlitz to prove that for $3 \leq n \leq 16$ any n-bit permutation can be decomposed in quadratic and cubic permutations.

Keywords Boolean functions · S-Box · Power permutations · Threshold implementation

Mathematics Subject Classification (2010) 94A60 · 94C10

1 Introduction

In order to efficiently implement complex S-boxes or permutations in hardware we need first to decompose them into simpler maps.

This article is part of the Special Issue on Mathematical Methods for Cryptography

✉ Svetla Nikova
svetla.nikova@esat.kuleuven.be

Ventzislav Nikov
venci.nikov@gmail.com

Vincent Rijmen
vincent.rijmen@esat.kuleuven.be

[1] KU Leuven, imec-COSIC, Leuven, Belgium

[2] NXP Semiconductors, Leuven, Belgium

Definition 1 (Decomposition) A decomposition of a function $f : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ is a finite sequence of functions $g_1, g_2, \dots g_t$ such that

$$f(x) = g_t \circ g_{t-1} \circ \cdots \circ g_2 \circ g_1(x).$$

This question has been investigated in the context of Threshold Implementation in [12, 16], where the decomposition and factorization of the Present S-box on quadratic S-boxes has been proposed. This research has been extended to all 3×3 and 4×4 S-boxes in [3, 4]. In the same context it was proven that when $n = 4$ all S-boxes belonging to the Alternative group have decomposition into quadratic permutations and all S-boxes not belonging to the Alternative group have no such decomposition, the inversion is among the latter [3, 4]. Decompositions of permutations into simpler operations, i.e. with less field multiplications, to enable more efficient side-channel countermeasures have been presented in [7, 8, 11, 17]. The goal of this paper is different - we target a decomposition of permutations into quadratic or cubic permutations.

Let us recall some well known results, which are used in the paper. There is no n-bit permutation with degree n [2], i.e. the maximal algebraic degree of a balanced n-variable Boolean function is $n - 1$. The inverse of an affine permutation is affine, the (algebraic) degree of a permutation x^d is equal to $wt(d)$ (Hamming weight), hence the permutations x^d and $x^d \circ x^{2^i}$ are affine equivalent since x^{2^i} are linear permutations. It has also been shown that x^d is a permutation of $\mathrm{GF}(2^n)$ if and only if $\gcd(d, 2^n - 1) = 1$ [2]. Note that for $n = 2^m$ there is no quadratic power function which is a permutation. It can easily be seen that the quadratic function x^3 is a permutation whenever n is odd. Indeed, since $2 = -1 \mod 3$ it follows that $2^n - 1 = 1 \mod 3$ or in other words $\gcd(3, 2^n - 1) = 1$. It can also been seen that x^3 is not a permutation when n is even. All involution permutations [15] are a product of disjoint cycles with 1 or 2 elements only.

Recall that a mapping f from $\mathrm{GF}(2^n)$ into $\mathrm{GF}(2^m)$ is called differentially δ-uniform (or simply δ-uniform) if for all $a \in \mathrm{GF}(2^n), a \neq 0$, and $b \in \mathrm{GF}(2^m)$ we have $|\{z \in \mathrm{GF}(2^n) | f(z + a) - f(z) = b\}| \leq \delta$. It is proven in [14] that the inversion mapping f i.e. $x^{-1} = x^{2^n - 2}$ in $\mathrm{GF}(2^n)$ has $\deg(f) = n - 1$, since $wt(2^n - 2) = n - 1$; it has odd parity; f is differentially 2-uniform if n is odd and it is differentially 4-uniform if n is even. The functions which are 2-uniform are also known as Almost Perfect Nonlinear (APN) functions.

Theorem 1 ([5]) *There are 5 APN permutations in* $\mathrm{GF}(2^5)$ *up to affine equivalence, all of those are affine equivalent to power functions* $APN_1^5 = x^3$, $APN_2^5 = x^5$, $APN_3^5 = x^7$, $APN_4^5 = x^{11}$, $APN_5^5 = x^{15}$. *Where* APN_5^5 *is equivalent to its inverse, and* APN_1^5 *(respectively* APN_2^5*) is equivalent to the inverse of* APN_4^5 *(respectively* APN_3^5*). Note that* APN_1^5 *and* APN_2^5 *are quadratic,* APN_3^5 *and* APN_4^5 *are cubic, and* APN_4^5 *has degree 4.*

There is only one known affine equivalence class of 6-bit APN permutations and it has degree 4. It is known that this permutation can be decomposed into two permutations of degree three and two, namely $APN^6 = g \circ f$, where f is cubic and g is quadratic.

Carlitz proved the following important theorem [9].

Theorem 2 *Given a finite field* $\mathrm{GF}(q)$ *with* $q > 2$ *then all permutation polynomials over it are generated by the special permutation polynomials* x^{q-2} *(the inversion) and* $ax + b$ *(affine i.e.* $a, b \in \mathrm{GF}(q)$ *and* $a \neq 0$*).*

In other words any permutation [10, 18] can be presented as decomposition of affine and inverse permutations. The number of inversions in this decomposition is referred as the *Carlitz rank* [1].

Our contribution in this paper is twofold - first, we describe a method to decompose any power function as a sequence of power permutations of lower algebraic degree. Using this method we provide decompositions of the inversion in GF(2^n) for small n from 3 up to 16, as well as for the APN functions when $n = 5$. Namely, there exist decompositions into *quadratic* power permutations for any n not multiple of 4 and decompositions into *cubic* power permutations for n multiple of 4. The second contribution of this paper is to extend the known, for $n = 4$, decomposition results to any permutation in GF(2^n) with $3 \leq n \leq 16$. In other words, we show that any permutation can be decomposed in cubic (or quadratic) permutations when n is (or not) multiple of 4. This general result is obtained thanks to the Theorem of Carlitz.

2 Decompositions

We will start with an algorithm which finds decompositions for the inversion into quadratic or cubic power permutations. Note that it is straightforward to apply the same method to other well known power functions as we demonstrate later for the APN functions when $n = 5$.

Let us recall that for $n = 2^m$ there is no quadratic power function which is a permutation, hence there will be no decomposition of the inversion on quadratic power permutations for such n. When $n = 12$ the only quadratic power permutation is x^{17}, but it has even parity while the inversion has an odd parity, hence no decomposition of the inversion on quadratic power permutations exists when $n = 12$. Since we consider $3 \leq n \leq 16$ then when n is multiple of 4 (i.e. $n = 4, 8, 12, 16$) we will look for decompositions on cubic power permutations, in all the other cases we will search for decompositions on quadratic power permutations. Let us denote by $\mathcal{A}(k)$ the *cyclotomic class* of a power permutation x^k, namely $\mathcal{A}(k) = \{k2^i \mod (2^n - 1),\ \text{such that}\ \gcd(k2^i, 2^n - 1) = 1\ \text{for}\ i = 0, \ldots, n-1\}$. Next, we consider the following algorithm (see Fig. 1) in which the first two steps are pre-computations followed by two alternatives for the search loop.

Since we are looking only for decompositions relevant to the S-boxes used in symmetric cryptographic primitives the choice of n between 3 and 16 is entirely justified. We would like to point out as well that the use of *cyclotomic classes* in the first step of the algorithm is similar to the algorithms in [7, 8, 11, 17], however our goal and the algorithm steps afterwards are different. Thus, the algorithm described above is adapted to serve well our purposes to find all desirable decompositions. Note that the exhaustive search worked out for all n except $n = 13, 15$ and 16.

All decompositions we found for the inversion given in Table 1 are with a minimal length. We applied our algorithm also for $APN_3^5 = x^7$, $APN_4^5 = x^{11}$ and $APN_5^5 = x^{15}$ and found that for $APN_3^5 = x^4 \circ x^5 \circ x^5$ i.e. decomposition of length 2; for $APN_4^5 = x^8 \circ x^3 \circ x^5 \circ x^5$ i.e. decomposition of length 3; for $APN_5^5 = x^5 \circ x^3$ i.e. decomposition of length 2; and those are the shortest decompositions.

A confirmation of the above results is given by the decompositions of the inversion in GF(2^8) i.e. the AES S-box which is of algebraic degree 7, presented in [13]: $x^{-1} = x^{32} \circ$

1. First we build the set of all cyclotomic classes $\mathcal{A}(k)$, which are permutations and denote this set by $\mathcal{CP}$. Note that for any permutation x^d, the degree d will belong to only one cyclotomic class $\mathcal{A}(k) \in \mathcal{CP}$. Further, we consider the subset of $\mathcal{CP}$ consisting of either quadratic or when there are no quadratic then cubic permutations denoted by $\mathcal{CP}_{\mathcal{Q}}$ (or $\mathcal{CP}_{\mathcal{C}}$).
2. For each k from $\mathcal{CP}_{\mathcal{Q}}$ (or $\mathcal{CP}_{\mathcal{C}}$) compute the order of k as the smallest power m_k such that $wt(k^{m_k} \bmod (2^n-1)) = 1$. In other words, $x^{k^{m_k}}$ has algebraic degree 1, i.e. is a linear function. Hence, for each set $\mathcal{A}(k)$ we construct a corresponding set $\mathcal{P}(k)$ which we call the *power set* of k, namely $\mathcal{P}(k) = \{k^i \bmod (2^n-1) \mid i = 1, \dots, m_k\}$. The collection of all power sets $\mathcal{P}(k)$ we denote by $\mathcal{P}$. Last define $\ell = |\mathcal{P}|$ and enumerate the representatives k of $\mathcal{P}(k) \in \mathcal{P}$ for example, k_i for $i = 1, \dots, \ell$. Note 2 is not among them since it generates linear permutation.
3. **Exhaustive search**
   For each $j_i = 0, \dots, m_{k_i} - 1$ and $j = 0, \dots, n-1$ compute the number $z(j, j_1, \dots, j_\ell) = 2^j \prod_{i=1}^{\ell} k_i^{j_i} \bmod (2^n-1)$. Then check the condition $(*)$, i.e. whether $z(j, j_1, \dots, j_\ell) = 2^n - 2$. Note that the number $\sum_{i=1}^{\ell} j_i$ corresponds to the length of the decomposition. If the check $(*)$ is satisfied then we remember the tuple $(j', j'_1, \dots, j'_\ell)$ which results in the shorter decomposition length. Naturally at the end we have the decomposition with the shortest length. The complexity of this exhaustive search is $n \prod_{i=1}^{\ell} m_{k_i}$.
4. **Adaptive search**
   We start in the same way as in the exhaustive search i.e. for each $j_i = 0, \dots, m_{k_i} - 1$ and $j = 0, \dots, n-1$, but with the additional constrain on the length of the decomposition, i.e. $\sum_{i=1}^{\ell} j_i \le t$ for a chosen t. However, when a tuple $(j', j'_1, \dots, j'_\ell)$ is found which satisfies the check $(*)$ and achieves a shorter decomposition length than the already known, then the search space is reduced to only those tuples which have even shorter decomposition length.

Fig. 1 Algorithm for decompositions of power permutations

$x^{19} \circ x^{13}$ i.e., a composition of 2 permutations of degree 3; $x^{-1} = x^{16} \circ x^{43} \circ x^{53}$ i.e., a composition of 2 permutations of degree 4; $x^{-1} = x^{128} \circ x^{23} \circ x^{11}$ i.e., a composition of a permutations of degree 3 with a permutation of degree 4.

Table 1 Decompositions of the inversion

n	Decomposition		n	Decomposition	
	x^{-1}	Length		x^{-1}	Length
3	$x^2 \circ x^3$	1	4	$x^2 \circ x^7$	1
5	$x^2 \circ x^3 \circ x^5$	2	6	$x^5 \circ x^5 \circ x^5$	3
7	$x^{2^6} \circ x^5 \circ x^5 \circ x^5$	3	8	$x^{2^5} \circ x^{13} \circ x^{19}$	2
9	$x^2 \circ x^{17} \circ x^5 \circ x^3$	3	10	$x^{17} \circ \dots \circ x^{17}$	15
11	$x^2 \circ x^5 \circ x^9 \circ x^9 \circ x^9 \circ x^9 \circ x^9 \circ x^9 \circ x^9$	8	12	$x^{2^3} \circ x^{97} \circ x^{97} \circ x^{97}$	3
13	$x^{2^{10}} \circ x^5 \circ x^{17} \circ x^{17} \circ x^{17}$	4	14	$x^5 \circ \dots \circ x^5$	21
15	$x^{2^2} \circ x^3 \circ x^9 \circ x^{33} \circ x^{129} \circ x^{129} \circ x^{129}$	6	16	$x^{2^{13}} \circ x^{11} \circ x^{37} \circ x^{161}$	3

To complete our result we use Theorem 2 (Carlitz) and below we state our main Theorem.

Theorem 3 *For $n \leq 16$ any permutation can be decomposed in quadratic permutations, when n is not multiple of 4 and in cubic permutations, when n is multiple of 4.*

Note that Theorem 2 uses a subset of affine transformations of the type $ax + b$ where a, b are field elements. Recall that any affine permutation can be written as $b + \sum_{i=0}^{n-1} a_i x^{2^i}$ called also linearized polynomials (plus a constant b) [6], where the coefficients a_i are field elements. Since Carlitz considers only a subset of them by using all affine permutations instead we can achieve shorter Carlitz rank. Note that the classes with even/odd Carlitz rank have even/odd parity. We should point out that although the decompositions we have found for the inversion are with minimal length, the decompositions found in Theorem 3 for any S-box might not have minimal length.

Another application of our main Theorem relates to the decompositions of the S-boxes when $n = 3$ and $n = 4$. We will use the notations introduced in [3] $\mathcal{A}_i^n$, $\mathcal{Q}_j^n$ and $\mathcal{C}_k^n$ where the upper index n indicates that we consider a permutation with 2^n elements, the lower index i, j, k is the number of the considered class among all affine equivalent classes when they are alphabetically ordered and the letter $\mathcal{A}, \mathcal{Q}, \mathcal{C}$ shows whether this is an Affine, Quadratic or Cubic class. All single permutation transpositions $(0, j)$ belong to the class Q_1^3 for 3×3 permutations. Moreover, all 4 classes for $n = 3$ can be obtained via $Inv \circ A \circ Inv \circ B \circ Inv$, where A, B and C are affine permutations i.e. with Carlitz rank at most 3. Class A_0^3 is the affine class, i.e., has rank 0 and the class Q_3^3 is the only class with rank 1, since it contains the inversion. Then the class Q_2^3 is with rank 2 and the remaining quadratic class Q_1^3 is with rank 3. Note that, from the construction used in the proof of the Carlitz Theorem, the single transpositions (i.e. class Q_1^3) are with Carlitz rank 3.

All 302 classes for $n = 4$ can be obtained as follows: $Inv \circ A \circ Inv \circ B \circ Inv \circ C \circ Inv$ i.e. with Carlitz rank at most 4. Class A_0^4 is the affine class and hence with rank 0, the cubic class C_{282}^4 is the only class with rank 1 since it contains the inversion. Then there are 59 classes with rank 2: {010, 016, 024, 041, 049, 050, 052, 053, 060, 061, 063, 064, 066, 067, 070, 071, 073, 074, 076, 081, 083, 089, 092, 095, 096, 099, 107, 118, 126, 127, 130, 131, 138, 140, 142, 150, 151, 164, 165, 168, 171, 172, 174, 180, 192, 201, 202, 211, 212, 217, 236, 249, 254, 262, 268, 270, 273, 281, 287}. Next there are 150 classes with rank 3 - namely all the classes not belonging to the Alternative group except C_{282}^4: {001, 003, 005, 007, 009, 011, 013, 015, 017, 019, 021, 023, 025, 027, 029, 030, 032, 035, 037, 039, 040, 042, 045, 047, 048, 051, 054, 056, 058, 059, 062, 065, 068, 069, 072, 075, 077, 079, 080, 082, 084, 087, 088, 090, 091, 093, 094, 097, 098, 100, 102, 105, 106, 108, 109, 112, 113, 116, 117, 119, 122, 125, 128, 129, 132, 133, 135, 137, 139, 141, 143, 144, 146, 149, 152, 153, 156, 157, 160, 163, 166, 167, 169, 170, 173, 175, 177, 179, 181, 182, 185, 186, 188, 190, 191, 193, 195, 197, 199, 200, 203, 204, 206, 207, 209, 210, 213, 216, 218, 220, 222, 224, 226, 227, 229, 230, 232, 235, 237, 239, 241, 242, 245, 246, 248, 250, 251, 253, 255, 256, 257, 261, 263, 265, 267, 269, 271, 272, 274, 276, 279, 283, 284, 285, 289, 290, 291, 295, 298, 301}. From the construction used in the proof of the Carlitz Theorem, the single transpositions $(0, j)$ (i.e. class C_1^4) are with Carlitz rank 3. The remaining 91 classes are with rank 4 and among them are all the 6 quadratic classes: {002, 004, 006, 008, 012, 014, 018, 020, 022, 026, 028, 031, 033, 034, 036, 038, 043, 044, 046, 055, 057, 078, 085, 086, 101, 103, 104, 110, 111, 114, 115, 120, 121, 123, 124, 134, 136, 145, 147, 148, 154, 155, 158, 159, 161, 162, 176, 178, 183, 184, 187, 189, 194, 196, 198, 205, 208, 214, 215, 219, 221, 223, 225, 228, 231, 233, 234, 238, 240, 243, 244, 247, 252, 258, 259, 260, 264, 266, 275, 277, 278, 280, 286, 288, 292, 293, 294, 296, 297, 299, 300}.

Five classes {006, 136, 161, 162, 278} will have rank 2 instead of rank 4 if all affine transformations are used instead of only the ones of the type $ax + b$.

3 Conclusions

We have shown that any permutation (for $3 \leq n \leq 16$) can be decomposed in quadratic permutations, when n is not multiple of 4 and in cubic permutations, when n is multiple of 4. There are still two open problems to be solved: Can the inversion be decomposed in quadratic permutations when n is multiple of 4 and $n > 4$? Can we find decompositions with shorter length?

Acknowledgements This work was supported in part by the Research Council KU Leuven: C16/15/058 and OT/13/071, and by the NIST Research Grant 60NANB15D346.

References

1. Aksoy, E., Cesmelioglu, A., Meidl, W., Topuzoglu, A.: On the Carlitz rank of a permutation polynomial. Finite Fields Appl. **15**, 428–440 (2009)
2. Beth, T., Ding, C.: On almost perfect nonlinear permutations, EUROCRYPT LNCS 765, pp. 65–76. Springer, Berlin (1993)
3. Bilgin, B., Nikova, S., Rijmen, V., Nikov, V., Stutz, G.: Threshold implementations of all 33 and 44 S-boxes, CHES LNCS 7428, pp. 76–91. Springer, Berlin (2012)
4. Bilgin, B., Nikova, S., Nikov, V., Rijmen, V., Tokareva, N., Vitkup, V.: Threshold implementations of small S-boxes. Cryptogr. Commun. **7**(1), 3–33 (2015)
5. Brinkmann, M., Leander, G.: On the classification of APN functions up to dimension five. DCC **49**(1-3), 273–288 (2008)
6. Carlet, C.: Vectorial Boolean functions for cryptography, chapter of the volume Boolean Methods and Models. Cambridge University Press, Cambridge (2016)
7. Carlet, C., Goubin, L., Prouff, E., Quisquater, M., Rivain, M.: Higher-order masking schemes for S-boxes, FSE LNCS 7549, pp. 366–384. Springer, Berlin (2012)
8. Carlet, C., Prouff, E., Rivain, M., Roche, T.: Algebraic decomposition for probing security, CRYPTO LNCS 9215, pp. 742–763. Springer, Berlin (2015)
9. Carlitz, L.: Permutations in a finite field. Proc. Amer. Math. Soc. **4**, 538 (1953)
10. Carlitz, L.: A note on permutation functions over a finite field. Proc. Amer. Math. Soc. **14**, 101 (1963)
11. Coron, J.-S., Roy, A., Vivek, S.: Fast evaluation of polynomials over finite fields and application to side-channel Countermeasures, CHES LNCS 8731, pp. 170–187. Springer, Berlin (2014)
12. Kutzner, S., Ha Nguyen, P., Poschmann, A.: Enabling 3-share threshold implementations for any 4-bit S-box, IACR Cryptology ePrint Archive, 510 (2012)
13. Moradi, A.: Advances in side-channel security. Habilitation Thesis, Ruhr-Universität Bochum (2016)
14. Nyberg, K.: Differentially uniform mappings for cryptography, EUROCRYPT LNCS 765, pp. 55–64. Springer, Berlin (1993)
15. Patarin, J.: Generic attacks on Feistel schemes, ASIACRYPT LNCS 2248, pp. 222–238. Springer, Berlin (2001)
16. Poschmann, A., Moradi, A., Khoo, K., Lim, C.-W., Wang, H., Ling, S.: Side-channel resistant crypto for less than 2,300 GE. J. Cryptol. **24**(2), 322–345 (2011)
17. Roy, A., Vivek, S.: Analysis and improvement of the generic higher-order masking scheme of FSE 2012, CHES LNCS 8086, pp. 417–434. Springer, Berlin (2013)
18. Zieve, M.: On a thorem of Carlitz. J. Group Theory **17**, 667–669 (2014)