Decomposition of Permutations in a Finite Field

Svetla Nikova[1], Ventzislav Nikov[2], and Vincent Rijmen[1]

[1] KU Leuven, imec-COSIC, Belgium, {name.surname}@esat.kuleuven.be
[2] NXP Semiconductors, Belgium, venci.nikov@gmail.com

We describe a method to decompose any power function, as a sequence of permutations of lower algebraic degree. As a result we obtain decompositions of the inversion in $GF(2^n)$ for small n from 3 up to 16, as well as for the AB functions when $n = 5$. We find with this method 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 and prove that for $3 \leq n \leq 16$ any permutation can be decomposed in quadratic (or cubic) permutations.

In several previous works [6–9] the authors have also presented decompositions of permutations into simpler operations in order to apply side-channel countermeasures efficiently, i.e. with less field multiplications. However, our goal is different - we target a composition of quadratic (or cubic) permutations. So far it has been proven that when $n = 4$ no quadratic decompositions of the inversion exist [4, 5] in the context of Threshold Implementation. Here we extend these results for any permutation in $GF(2^n)$ with $3 \leq n \leq 16$.

In 1953 *Carlitz* [1] proved the following **Theorem: Given a finite field $GF(q)$ 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. $a, b \in GF(q)$ and $a \neq 0$).** In other words any permutation can be presented as a decomposition of affine and inverse permutations [2, 3]. Such a decomposition is called the *Carlitz rank*. The length i.e. the number of inversions in this decomposition is referred as the *Carlitz length.*

Our goal is to find a decomposition on quadratic permutations of some important cryptographic S-boxes for $n = 3, \ldots, 16$ - namely AB and APN functions and especially the inversion. Since we are looking only for decompositions relevant for the S-boxes used in symmetric cryptographic primitives the choice of n between 3 and 16 is entirely justified.

All decompositions we found for the inversion are with minimal length. We applied our algorithm also for $AB_3 = x^7$, $AB_4 = x^{11}$ and $AB_5 = x^{15}$ and found that for $AB_3 = x^4 \circ x^5 \circ x^5$ i.e. decomposition of length 2; for $AB_4 = x^8 \circ x^3 \circ x^5 \circ x^5$ i.e. decomposition of length 3; for $AB_5 = x^5 \circ x^3$ i.e. decomposition of length 2; and those are the shortest decompositions.

n	Decomposition x^{-1}	Length	n	Decomposition 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	$x^{17} \circ \ldots \circ x^{17}$	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	$x^5 \circ \ldots \circ x^5$	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

We prove the following **Theorem: For $3 \leq n \leq 16$ any permutation can be decomposed in quadratic permutations, when n is not divisible by 4 and in cubic permutations, when n is divisible by 4.** Note that the Carlitz Theorem uses a subset of affine transforms of the type $ax + b$, where a, b are field elements. We use instead all affine transformations and apply the theorem over the affine equivalent classes (not only over S-boxes), the length of the decomposition can also be shorter. Note that the classes with even/odd Carlitz length have even/odd parity.

An application of our main result relates to the decompositions of S-boxes for $n = 3$ and $n = 4$. All single permutation transpositions $(0, j)$ belong always to the first class since the classes are enumerated lexicographically starting from the affine class. Moreover, all 4 classes for $n = 3$ can be obtained with Carlitz length up to 3. The class with affine permutations has length 0. There is 1 class with length 1 (it contains the inversion), one class with length 2 and the remaining one class is with length 3.

All 302 classes for $n = 4$ can be obtained with Carlitz length up to 4. The class with affine permutations has length 0, and the class which contains the inversion is the only class with length 1. Then there are 59 Classes with length 2. If all affine transforms are used, five more classes with length 2 can be found. The remaining 91 classes are with length 4 and among them are all the 6 quadratic classes.

References

1. L. Carlitz. "Permutations in a finite field", Proc. Amer. Math. Soc. 4 (1953), 538.
2. L. Carlitz. "A note on permutation functions over a finite field", Proc. Amer. Math. Soc. 14 (1963), 101.
3. M. Zieve. "On a thorem of Carlitz", J. Group Theory 17 (2014), 667669.
4. B. Bilgin, S. Nikova, V. Rijmen, V. Nikov, G. Stutz. "Threshold Implementations of all 3×3 and 4×4 S-boxes", CHES 2012, LNCS 7428, 76-91.
5. B. Bilgin, S. Nikova, V. Nikov, V. Rijmen, N. Tokareva, V. Vitkup. "Threshold implementations of small S-boxes", Cryptography and Communications 7(1), 2015, 30 pages.
6. C. Carlet, L. Goubin, E. Prouff, M. Quisquater, M. Rivain. "Higher-order masking schemes for S-boxes", FSE 2012, LNCS 7549, 366-384.
7. A. Roy, S. Vivek. "Analysis and improvement of the generic higher-order masking scheme of FSE 2012", CHES 2013, LNCS 8086, 417-434.
8. J.-S. Coron, A. Roy, S. Vivek. "Fast Evaluation of Polynomials over Finite Fields and Application to Side-channel Countermeasures", CHES 2014, LNCS 8731, 170-187.
9. C. Carlet, E. Prouff, M. Rivain, T. Roche. "Algebraic Decomposition for Probing Security", CRYPTO 2015, LNCS 9215, 742-763.