Decomposition of Permutations in a Finite Field

SVETLA NIKOVA[1], VENTZISLAV NIKOV[2], AND VINCENT RIJMEN[1]

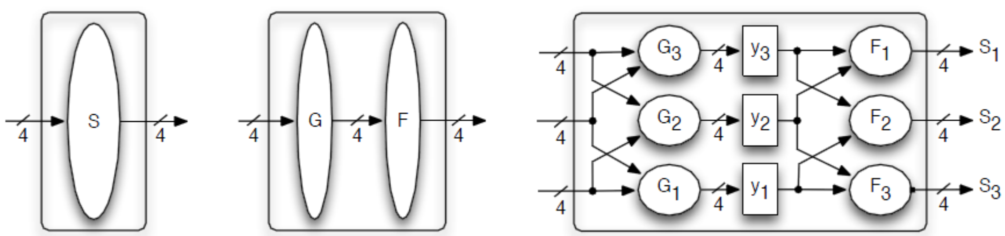
[1] IMEC-COSIC, KU LEUVEN, BELGIUM

[2] NXP SEMICONDUCTORS, BELGIUM

Decomposition of Permutations in relation to Side-Channel Countermeasures (1/3)

2010 Present 4x4 S-box decomposition on 2 quadratic S-boxes
"Side-Channel Resistant Crypto for less than 2300 GE" A. Poschmann et al.

2012 All 4x4 and 3x3 S-boxes decompositions on quadratic S-boxes
"Threshold Implementations of all 3x3 and 4x4 S-boxes" B. Bilgin et al.

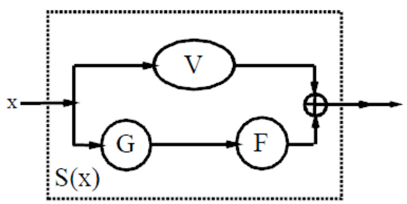


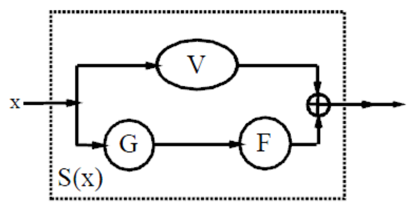
Here the cubic S(.) can be decomposed on 2 quadratic F(.) and G(.) S-boxes.

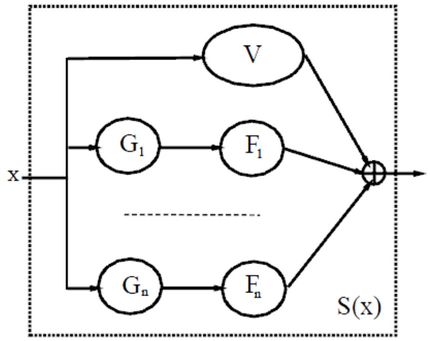
Decomposition goal – reduce the degree

Decomposition of Permutations in relation to Side-Channel Countermeasures (2/3)

2012 Factorization of S-boxes
“Enabling 3-share Threshold Implementations for any 4-bit S-box” T. Kutzner et al.







Again the cubic S(.) can be decomposed on 3 quadratic S-boxes.

Factorization goal – again reduce the degree

Decomposition of Permutations in relation to Side-Channel Countermeasures (3/3)

2012 Polynomial evaluation of S-boxes, cyclotomic class and parity split addition chains
"Higher-order masking schemes for S-boxes" C. Carlet et al.

2013 Divide-and-Conquer Strategy for Polynomial evaluation
"Analysis and improvement of the generic higher-order masking scheme of FSE 2012" A. Roy, S. Vivek

2014 Generalized Divide-and-Conquer Strategy for Polynomial evaluation
"Fast Evaluation of Polynomials over Finite Fields and Application to Side-channel Countermeasures" C. Carlet et al.

2015 Generalized Factorization for Polynomial evaluation
"Algebraic Decomposition for Probing Security" C. Carlet et al.

The role of decomposition in Side-Channel countermeasures

TI (masking) of nonlinear permutations

No efficient, general algorithm known

Lower algebraic degree more easy to secure

Affine-equivalent S-boxes have affine-equivalent secure implementations (masking)

Database of permutations with their TI implementations

Decomposition of Permutations

Theorem (Carlitz, 1953)

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. $a, b \epsilon GF(q)$ and $a \neq 0$).

Such a decomposition is called the **Carlitz rank**

Carlitz length: the number of inversions in this decomposition

Our goals

We target a decomposition on quadratic (or cubic) permutations.

When $n = 4$ no quadratic decompositions of the **inversion** exist.

We extend these results for any permutation in GF(2^n) with $n = 3 \ \dots \ 16$.

We are looking for decompositions on quadratic permutations of important cryptographic S-boxes for $n = 3 \ \dots \ 16$ - **AB** and **APN** functions.

Method for finding the decomposition

Our method finds decomposition of the inversion on quadratic (or cubic) power permutations.

Algorithm (high level):

Create a "basis" of quadratic (or cubic) power permutations (monomials x^k)

Optimized search for

- Decomposition using only the degree of the monomials k
- At the same time keeping track of the length of the decomposition
- Optimization to look for decompositions with smaller length only

The result is a list of decompositions with the smallest length

Method for finding the decomposition

Recall $x^{2^n-2} = x^{-1}$ and x^k is a permutation of GF(2^n) if and only if $\gcd(k, 2^n - 1) = 1$

Hence for $n = 2^m$ no quadratic power permutations exist.

The (algebraic) degree of a permutation x^k is equal to $wt(k)$.

Permutations x^k and $x^{2^i} \circ x^k$ are affine equivalent since x^{2^i} are linear permutations.

When $n = 12$ the only quadratic monomial 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 when $n = 12$.

Method for finding the decomposition

Our **Algorithm** finds decomposition of the inversion on quadratic (or cubic) power permutations.

- Build a set *CP* of power permutations not belonging to the same cyclotomic class.
  Take the subset of quadratic CP_Q (or cubic CP_C) power functions
- For each x^k from CP_Q compute the order of k as the smallest power m_k s. t. $wt(k^{m_k} \; mod \; 2^n - 1) = 1$
- Denote the power set of k by $P(k) = \{k^i \; mod \; 2^n - 1 \mid i = 1, \ldots, m_k\}$, add $P(k)$ to a set *P*
- Enumerate the representatives k in P e.g. k_i for $i = 1, \ldots, l = |P|$
- Compute $z(j, j_1, \ldots, j_l) = 2^j \prod_{i=1}^{l} {k_i}^{j_i} \; mod \; 2^n - 1$, for $j_i = 0, \ldots, m_{k_i} - 1$, $j = 0, \ldots, n-1$ and check whether it is equal to $2^n - 2$
- If found, then the smallest $\sum_{i=1}^{l} (j_i \; mod \; m_{k_i})$ gives the shortest decomposition.
  The complexity of this exhaustive search is $n \prod_{i=1}^{l} m_{k_i}$
- If exhaustive search is not feasible $(n = 13, 15$ and $16)$ search can be optimized by restricting the decomposition length i.e. restricting m_{k_i}

An example

Let $n = 9$, then there are $l = 4$ quadratic monomials with powers $k = 3, 5, 9$ and 17, where only x^3 has odd parity.

The order m_k /i.e. $wt(k^{m_k}\ mod\ 2^n - 1) = 1$/ is $12, 72, 6$ and 24, respectively.

Compute $z(j, j_1, \ldots, j_l) = 2^j \prod_{i=1}^{l} k_i{}^{j_i}\ mod\ 2^n - 1$, for $j_i = 0,\ldots,m_{k_i} - 1$, $j = 0, \ldots, n - 1$ and check whether it is equal to $2^n - 2$.

When found, then the smallest $\sum_{i=1}^{l}(j_i\ mod\ m_{k_i})$ gives the shortest decomposition. The complexity of this exhaustive search is $n \prod_{i=1}^{l} m_{k_i}$.

For $n = 9$ we have: $x^{-1} = x^2 \circ x^{17} \circ x^5 \circ x^3$, the smallest decomposition length is 3 and the worst complexity is $9 * 12 * 72 * 6 * 24 = 2^{20}$

Decomposition of inversion

All decompositions we found for the inversion are with **minimal length**.

For n **not divisible by 4** we found decompositions on **quadratic** permutations
for **n divisible by 4** we found decompositions on **cubic** permutations.

We acknowledge that Amir Moradi has found the particular set of cubic decompositions for AES, i.e. the x^{254} case (personal communication).

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

Generic decomposition of all permutations

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.*

The Theorem of Carlitz uses a subset of affine transforms of the type $ax + b$, where a, b are field elements.

Recall an affine permutation can also be presented as $\sum_{i=0}^{n-1} \ (a_i \ x^{2^i})$.

Since Carlitz considers only $ax + b$, by using affine permutations instead we can achieve shorter Carlitz length.

The classes with even/odd Carlitz length have even/odd parity.

Decomposition of particular permutations

For **5 bit S-boxes**: $AB_1 = x^3$, $AB_2 = x^5$, $AB_3 = x^7$, $AB_4 = x^{11}$, $AB_5 = x^{15}$

$AB_3 = x^4 \circ x^5 \circ x^5$, $AB_4 = x^8 \circ x^3 \circ x^5 \circ x^5$, $AB_5 = x^5 \circ x^3$, i.e. decompositions of length 2, 3 and 2 and those are the shortest decompositions.

We also applied the Carlitz decomposition for all **3 and 4 bit S-boxes**

For $\boldsymbol{n = 3}$: 1 class with length 0, 1 class with length 1, 1 class with length 2 and 1 class with length 3

For $\boldsymbol{n = 4}$: 1 class with length 0, 1 class with length 1, 59 $(+5)$ with length 2, 150 classes with length 3 and 91 (-5) with length 4 (among them all 6 quadratic classes)

Conclusions and open questions

We have shown that any permutation (for $3 \leq \mathrm{n} \leq 16$) can be decomposed in **quadratic** permutations, when **n is not divisible by $\mathbf{4}$** and in **cubic** permutations, when **n is divisible by $\mathbf{4}$**.

Open questions:

- Can the inversion be decomposed on quadratic permutations for **$\mathbf{n}$ divisible by $\mathbf{4}$** (and $n > 4$)?
- Can we find shorter decomposition length?