On Inverses of APN Exponents

Gohar Kyureghyan* and Valentin Suder†

We present results on the inverses modulo $2^n - 1$ of the known APN exponents. The classical modular inversion is the problem to invert numbers modulo a *fixed* number. We consider a dual problem, inverting a fixed number d modulo $2^n - 1$ for *all* suitable n.

Let d be a fixed positive integer and $n \geq 2$ such that $\gcd(2^n - 1, d) = 1$. Then d is invertible modulo $2^n - 1$ for all such n. We denote by d^{-1} the least positive residue of d modulo $2^n - 1$. Are there any properties shared by the inverses d^{-1} modulo any $2^n - 1$? Is it possible to find an explicit formula for d^{-1} modulo $2^n - 1$ for all n?

We study these questions for several families of integers, mainly for the exponents of the known APN power functions on $\mathbb{F}_{2^n}$. We called them APN exponents. The inverses of APN exponents are APN as well. It is usually said that the known APN and AB power permutations are known (with their shifts and inverses modulo $2^n - 1$), cf. [1]. However, for a better understanding of APN and AB exponents, it could be helpful to have explicit representations of these inverses. An important parameter for an APN exponent is its binary weight, which defines the algebraic degree of the corresponding function and thus resistance of it to some cryptological attacks. The study of inverses of APN exponents was originated in [2] and [3], where the inverses and their binary weights for the so-called Gold and Niho exponents were found respectively. Here we give the inverses and their binary weights for the so-called Welch and Dobbertin exponents. Further, we observe that the inverse of the Dobbertin exponent defines an APN function on $\mathbb{F}_{2^n}$ of algebraic degree $\frac{n+3}{2}$, which is the first example of such a function. We generalize also the work of Nyberg [2], and give results for exponents of the shape $2^k - 1$.

References

[1] C. Carlet, Vectorial Boolean Functions for Cryptography, http://www.math.univ-paris13.fr/ carlet/chap-vectorial-fcts-corr.pdf.

[2] K. Nyberg, Differentially uniform mappings for cryptography. *Advances in cryptology – EUROCRYPT'93*, LNCS 765, 55–64, 1993.

[3] M. Portmann and M. Rennhard, Almost Perfect Nonlinear Permutations. *Semester Project – Swiss Federal Institute of Technology Zurich*, 1997.

*Otto-von-Guericke University, Department of Mathematics: gohar.kyureghyan@ovgu.de
†INRIA Paris-Rocquencourt, Project-Team SECRET: valentin.suder@inria.fr