Towards a characterization of left quasigroup polynomials of small degree over fields of characteristic 2

*Danilo Gligoroski and Simona Samardjiska**
Norwegian University of Science and Technology, Norway

Permutation polynomials (PPs) defined over fields of characteristic 2 are particularly important because of their broad application in cryptography and coding theory. However, their characterization even for small degrees is still a challenging open problem. After the work of Dickson [1] who characterized completely PPs over any finite field up to degree 5, and PPs of degree 6 for odd characteristic, it was only recently that Li et al. [2] extended the characterization of PP for degree 6 and 7 for fields of characteristic 2.

A natural generalization of the notion of permutation polynomials is that of left quasigroup polynomials (LQPs). A particularly interesting class is that of LQPs that are of algebraic degree 2. Their multivariate representation is known under the name of Multivariate Quadratic Quasigroups (MQQs), and these are the basis of the MQQ public key cryptosystems [3,4].

Following the work of Dickson and Li et al., we take a step towards characterization of LQPs of degree up to 6 defined over $\mathbb{F}_{2^k}$ that are of algebraic degree 2. We investigate different types of bivariate polynomials of degree at most 6, and give some necessary and sufficient conditions for these polynomials to define LQPs.

[1] Dickson, L.E.: The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. In: *Ann. of Math.* (1) 11 (1896/97), 65–120.

[2] Li, J., Chandler, D. B., Xiang, Q.: Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2. In: *Finite Fields Appl.*, Vol. 16 (6), (2010), 406–419.

[3] Gligoroski, D., Ødegård, R. S., Jensen, R. E., Perret, L., Faugère, J.-C., Knapskog, S. J., and Markovski, S.: MQQ-SIG, an ultra-fast and provably CMA resistant digital signature scheme, In Proc. of INTRUST 2011, LNCS vol. 7222, pp. 184–203, 2012.

[4] Samardjiska, S., Chen, Y., Gligoroski, D.: Algorithms for Construction of MQQs and Their Parastrophe Operations in Arbitrary Galois Fields. In: *JIAS*, Vol. 7 (3), (2012), 164–172.