Simona Samardjiska, Danilo Gligoroski

Left MQQs whose left parastrophe is also quadratic

Comment.Math.Univ.Carolin. 53,3 (2012) 397 –421.

Abstract: A left quasigroup (Q, q) of order 2^w that can be represented as a vector of Boolean functions of degree 2 is called a left multivariate quadratic quasigroup (LMQQ). For a given LMQQ there exists a left parastrophe operation $q_\backslash$ defined by: $q_\backslash(u, v) = w \Leftrightarrow q(u, w) = v$ that also defines a left multivariate quasigroup. However, in general, $(Q, q_\backslash)$ is not quadratic. Even more, representing it in a symbolic form may require exponential time and space. In this work we investigate the problem of finding a subclass of LMQQs whose left parastrophe is also quadratic (i.e. is also an LMQQ), and in the same time can be easily constructed. These LMQQs are affine in the second argument, and their left parastrophe can be easily expressed from the quasigroup operation. We give necessary and sufficient conditions for an LMQQ of this type to have a left parastrophe that is also an LMQQ. Based on this, we distinguish a special class that satisfies our requirements and whose construction is deterministic and straightforward.

Keywords: left multivariate quadratic quasigroup, left parastrophe, algebraic degree, matrix of Boolean polynomials

AMS Subject Classification: 20N05, 11T55, 11T71

References

[1] Albert A.A., *Quasigroups. I*, Trans. Amer. Math. Soc. **54** (1943), 507–519.

[2] Ahlawat R., Gupta K., Pal S.K., *Fast generation of multivariate quadratic quasigroups for cryptographic applications*, Proceeding of Mathematics in Defence, 2009.

[3] Belousov V.D., *Osnovi teorii kvazigrup i lup* (in Russian), Nauka, Moscow, 1967.

[4] Carter G., Dawson E., Nielsen L., *A latin square version of DES*, in Proc. Workshop of Selected Areas in Cryptography, Ottawa, Canada, 1995.

[5] Chen Y., Knapskog S.J., Gligoroski D., *Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity*, INSCRYPT, Proceedings of the 6th International Conference on Information Security and Cryptology, 2010.

[6] Christov A., *Kryptografie založená na teorii kvazigrup*, Diploma Thesis, Charles University, Prague, 2009, available at: `http://artax.karlin.mff.cuni.cz/ chria3am/thesis/`.

[7] Cooper J., Donovan D., Seberry J., *Secret sharing schemes arising from Latin Squares*, Bull. Inst. Combin. Appl. **4** (1994), 33–43.

[8] Gligoroski D., Markovski S., Kocarev L., Gusev M., *Edon80 Hardware Synchronous stream cipher*, SKEW 2005 - Symmetric Key Encryption Workshop, Aarhus Denmark, 2005.

[9] Gligoroski D., Markovski S., Knapskog S.J., *Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups*, MATH'08: Proceedings of the American Conference on Applied Mathematics, pp. 44–49, 2008. Extended version of the paper: *Public key block cipher based on multivariate quadratic quasigroups*, in Cryptology ePrint Archive, Report 2008/320, `http://eprint.iacr.org`.

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

[11] Gligoroski D., Ødegård R.S., Mihova M., Knapskog S.J., Drápal A., Klima V., *Cryptographic Hash Function* EDON-$\mathcal{R}$, SHA-3 Algorithm Submission, 2008.

[12] Gligoroski D., Klima V., Knapskog S.J., El-Hadedy M., Amundsen J., Mjølsnes S.F., *Cryptographic Hash Function* BLUE MIDNIGHT WISH , SHA-3 Algorithm Submission, 2008.

[13] Klimov A., Shamir A., *A new class of invertible mappings*, 4th Workshop on Cryptographic Hardware and Embedded Systems CHES 2002, pp. 471-484, Springer, 2002.

[14] Markovski S., Mileva A., *Cryptographic Hash Function NaSHA*, SHA-3 Algorithm Submission, 2008.

[15] Matsumoto M., Saito M., Nishimura T., Hagita M., *CryptMT Stream Cipher Version 3*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/028, 2007, available at: `http://www.ecrypt.eu.org/stream/papers.html`.

[16] Nguyen D.V., Chilappagari S.K., Marcellin M.W., Vasić B., *LDPC codes from latin squares free of small trapping sets*, arXiv:1008.4177, 2010, available at: `http://arxiv.org/abs/1008.4177`.

[17] Rivest R.L., *Permutation polynomials modulo* 2^w, Finite Fields Appl. **7** (2001), 287–292.

[18] Samardjiska S., Chen Y., Gligoroski D., *Algorithms for construction of multivariate quadratic quasigroups (MQQs) and their parastrophe operations in arbitrary Galois fields*, Journal of Information Assurance and Security **7** (2012), 164–172.

[19] Samardjiska S., Markovski S., Gligoroski D., *Multivariate quasigroups defined by T-functions*, Proceedings of the 2nd International Conference on Symbolic Computation and Cryptography, 2010, pp. 117–127.

[20] Schnorr C.P., Vaudenay S., *Black Box Cryptanalysis of hash networks based on multipermutations*, in Advances of Cryptology - EUROCRYPT'94, Springer, Berlin, 1995.

[21] Shannon C.E., *Communication theory of secrecy systems*, Bell Sys. Tech. J. **28** (1949), 657–715.

[22] Smith J.D.H., *An Introduction to Quasigroups and Their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.

[23] Zhang L., Huang Q., Lin S., Abdel-Ghaffar K., Blake I.F., *Quasicyclic LDPC codes on Latin squares and the ranks of their parity-check matrices*, in Inf. Theory and Appl. Workshop, 2010.