Squeezing a vectorial nonlinear binary transformation between the generator and parity check matrices of a linear code

Claude Gravel* and Daniel Panario**

*claudegravel1980@gmail.com (*unaffiliated*)
**School of Mathematics and Statistics, Carleton University, Canada, daniel@math.carleton.ca

We propose a new primitive that could serve as a component in the design of block cipher algorithms over a vector space of characteristic two. The primitive consists of squeezing a vectorial non-linear boolean function between two linear transformations. It consists of a (linear compression) $\to$ (keyed nonlinear transformation) $\to$ (linear decompression) feed back with its input and then linearly transformed. We impose that the compression and decompression be orthogonal linear codes for the system to be invertible even if the nonlinear part is not invertible. Our scheme has the *practical* advantage that many interesting properties of an entire round reduce only to those of the nonlinear transformation. As a matter of fact, we prove a lower bound on the minimal number of iterations, assuming independent keys uniformly distributed among iterations, to avoid path both in the space of first order differences (differential cryptanalysis) and in the space of linear first order correlations (linear cryptanalysis) up to a desired threshold. We neither focus in this paper on the key scheduling algorithm nor on the nonlinear part and solely analyse how the linear components must be set up to be resilient against the aforementioned cryptanalytic attacks. We also show that round functions of well-known block ciphers such as DES or IDEA, family of block ciphers such as Feistel networks (and some generalized Feistel networks that are built over fields of characteristic two), or symmetric cryptographic scheme such as the Massey-Lai scheme for instance are all specific cases of our transformation.

More precisely, let $n > 0$, $N \geq N_i > 0$, and $N \geq N_o > 0$ be integers, $V = \mathbb{F}_2^n$, and consider the vectorial function $F : V^N \to V^N$, introduced for the first time in this paper, given by

$$F_k(x) = T\big(x + B\big(f_k\big(A(x)\big)\big)\big), \tag{1}$$

where $k \in K$ and K is a vector space over $\mathbb{F}_2$ (the keyspace with $\dim K \geq Nn$), $f_k : V^{N_i} \mapsto V^{N_o}$ is a vectorial nonlinear function, T is an invertible matrix of size $N \times N$ over V, A is a full rank matrix of size $N_i \times N$ over V, and B is a full random matrix of size $N_o \times N$ over V such that $AB^t = 0$. We refer to n as the word size, N as the number of words, N_i as the number of input words to f_k, N_o as the number of output words to f_k, $\frac{N}{N_i} \in \mathbb{Q}$ as the compression/contraction factor, and $\frac{N}{N_o} \in \mathbb{Q}$ as the decompression/expansion factor.

Theorem 1. For all $k \in K$, the function F_k is invertible even if f_k is not invertible and so is any composition of F_k's.

Theorem 2. Both the differential and linear cryptanalyses of F_k solely reduces to those of f_k for all k no matter the input $x \in V^N$.

Let $F = F_{k_\ell} \cdots F_{k_1}$ be a composition of ℓ functions F_{k_i} with independently identically distributed keys k_i over K, δ be the maximal differential uniformity over all f_k, λ be the maximal linear correlation (Walsh coefficient) over all f_k, and $\ell^\star = \max\{\frac{N}{N_i}, \frac{N}{N_o}\}$.

Theorem 3. Both the differential uniformity and maximal correlation (Walsh coefficient) of F is not larger $\delta^{\ell^\star}$ and $\lambda^{\ell^\star}$, respectively, whenever $\ell > \ell^\star$.

References

[1] Biham, Eli and Shamir, Adi. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[2] Carlet, Claude. Boolean functions for cryptography and error correcting codes. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 257–397. Cambridge University Press, 2010.

[3] Carlet, Claude. Vectorial boolean functions for cryptography. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 398–469. Cambridge University Press, 2010.

[4] Gravel, Claude, Panario, Daniel and Thomson, David. Unicyclic strong permutations, 2018. https://arxiv.org/abs/1809.03551.

[5] Heys, Howard M. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26(3):189–221, 2002.

[6] Lai, Xuejia and Massey, James L. A Proposal for a New Block Encryption Standard. In *Advances in Cryptology, EUROCRYPT '90*, pages 389–404. Springer-Verlag, 1991.

[7] Lidl, Rudolf and Niederreiter, Harold. *Finite Fields.* Cambridge University Press, 1997.

[8] Xiao, Guo-Zhen and Massey, James L.. A spectral characterization of correlation-immune combining functions. *IEEE Trans. Information Theory*, 34(3):569–571, 1988.

[9] Matsui, Mitsuru. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology — EUROCRYPT '93*, pages 386–397. Springer-Verlag, 1994.

[10] Mullen, Gary L. and Panario, Daniel. *Handbook of Finite Fields.* Chapman & Hall/CRC, 2013.

[11] Nyberg, Kaisa. Statistical and linear independence of binary random variables. Technical report, 2017. https://eprint.iacr.org/2017/432.

[12] Siegenthaler, T. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Info. Th.*, 30:776–780, 1984.

[13] Junod, Pascal and Vaudenay, Serge. FOX Specifications Version 1.2, 2005.