An Excellent Permutation Operator for Cryptographic Applications

Josef Scharinger

Johannes Kepler University, Institute of Computational Perception,
4040 Linz, Austria
Josef.Scharinger@jku.at

1 Introduction

Permutations are a core component of almost every cipher. No matter if we consider the DES [5], AES [2] or most of the other encryption algorithms [6] relevant nowadays, we always find permutation operators as essential building blocks inside. In this contribution we will introduce key-dependent permutation operators of provably excellent quality inspired by chaotic Kolmogorov flows [1, 4]. From chaotic systems theory it is known [3] that the class of Kolmogorov flows exhibits the highest degree of instability among all dynamical systems. As will be demonstrated in the sequel, these outstanding properties make them a perfect inspiration for developing a novel class of strong cryptographic permutation operators.

2 Chaotic Kolmogorov Flows

Continuous Kolmogorov flows (see e.g. Figure 1) perform iterated stretching, squeezing and folding upon the unit square $\mathbb{E}$. It is guaranteed [1, 3] that their application leads to perfect mixing of the elements within the state space.

Formally this process of stretching, squeezing and folding is specified as follows. Given a partition $\pi = (p_1, p_2, \ldots, p_k)$ $(0 < p_i < 1, \sum_{i=1}^{k} p_i = 1)$ of the unit interval $\mathbb{U}$ and stretching and squeezing factors defined by $q_i = \frac{1}{p_i}$. Furthermore, let F_i defined by $F_1 = 0$ and $F_i = F_{i-1} + p_{i-1}$ denote the left border of the vertical strip containing the point $(x, y) \in \mathbb{E}$ to transform. Then the continuous Kolmogorov flow T_π will move $(x, y) \in [F_i, F_i + p_i) \times [0, 1)$ to the position

$$T_\pi(x, y) = (q_i(x - F_i), \frac{y}{q_i} + F_i). \tag{1}$$

3 Discrete Kolmogorov Systems

Chaotic Kolmogorov flows perform perfect mixing of the continuous unit square but how can we utilize them to mix a discrete data block of dimensions $n \times n$? We have developed the following formula. Given a list $\delta = (n_1, n_2, \ldots, n_k)$ $(0 < n_i < n, \sum_{i=1}^{k} n_i = n)$ of positive integers that adhere to the restriction that all $n_i \in \delta$

Fig. 1. Illustrating the chaotic and mixing dynamics associated when iterating a Kolmogorov system.

must partition the side length n. Furthermore let the quantities q_i be defined by $q_i = \frac{n}{n_i}$ and let N_i specified by $N_1 = 0$ and $N_i = N_{i-1} + n_{i-1}$ denote the left border of the vertical strip that contains the point (x, y) to transform. Then the discrete Kolmogorov system $T_{n,\delta}$ will move the point $(x, y) \in [N_i, N_i + n_i) \times [0, n)$ to the position

$$T_{n,\delta}(x, y) = (q_i(x - N_i) + (y \bmod q_i), (y \operatorname{div} q_i) + N_i). \tag{2}$$

In the final paper we will prove the following theorem:

Theorem 1. *Let the side-length $n = p^m$ be given as integral power of a prime p. Then the discrete Kolmogorov system T_{n,δ_r} as defined in equation 2 fulfills the properties of ergodicity, exponential divergence and mixing provided that at least $4m$ iterations are performed and lists δ_r used in every step r are chosen independently and at random.*

Based on this theorem it is well justified to claim that the permutation operator developed in this contribution is indeed an excellent key-dependent permutation operator for cryptographic applications.

References

1. V.I. Arnold and A. Avez. *Ergodic Problems of Classical Mechanics*. W.A. Benjamin, New York, 1968.
2. J. Daemen and V. Rijmen. AES proposal: Rijndael. In *First Advanced Encryption Standard (AES) Conference*, Ventura, CA, 1998.
3. S. Goldstein, B. Misra, and M. Courbage. On intrinsic randomness of dynamical systems. *Journal of Statistical Physics*, 25(1):111–126, 1981.
4. Jürgen Moser. *Stable and Random Motions in Dynamical Systems*. Princeton University Press, Princeton, 1973.
5. US Department of Commerce National Bureau of Standards. Data encryption standard. NBS FIPS PUB 46-1, 1977.
6. Bruce Schneier. *Applied Cryptography*. Addison-Wesley, 1996.