Diffusion in Cryptography
One-page Summary

Laurent Poinsot and Sami Harari

laurent.poinsot@univ-tln.fr

The diffusion of information into functions involved in secret-key cryptography is a crucial criterion for robustness of algorithms against some statistical attacks such as differential and linear cryptanalysis. Many authors have used their own definition for diffusion in order to formalize the properties of solidity of their cryptosystems. These notions, although more or less distinct, share the same objective : the quantitative study of the correlation between the amount of information in input and in output of a function. This paper is a summary of several of these notions and an attempt to explicit the underlying concepts of the general term diffusion.

We present four notions of diffusion during this paper. The first one, the *method of diffusion* introduced by Shannon, can be used to delimit in an abstract way the area of the problems of diffusion. Shannon described in a probabilistic way, the diffusion of information as the mean to dissipate the statistical structure of the set of plaintexts into long range statistics in the set of ciphertexts. Hence, the goal is to break the most frequent patterns of plaintexts into long parts of enciphered messages.

Then we introduce some quantitative characterizations of diffusion at the bit and symbol levels which seem to be relevant measures of diffusion. They are defined as the number of output bits or output bundles of bits of a boolean function which change when only one input bit or one bit of an input bundle is complemented. So these notions are very primitive and computational.

In the third part of our paper, we approach the *complete diffusion* which is a notion introduced by Lai and Massey for the diffusion part of the design of their cryptosystem IDEA. It means that all the output symbols of boolean functions which satisfy complete diffusion are dependant of every input symbols. Moreover we present a necessary condition of Massey on complete diffusion based on computational graphs.

Finally, we describe the approach given by Daemen and Rijmen to design Rijndael. This approach is explicitly based on resistance against the differential and linear cryptanalysis of block ciphers and generalizes in some kind the diffusion at the symbol level introduced in the second part.