Plaintext-dependant Repetition Codes Cryptanalysis of Block Ciphers

Eric Filiol
INRIA Projet CODES, Domaine de Voluceau B.P. 105
78153 Le Chesnay Cédex, FRANCE
Eric.Filiol@inria.fr

January 22, 2003

This paper presents a new theoretical model of block cipher cryptanalysis. It is based on the use of a well-known error-correcting code: the repetition codes [1]. We demonstrate how to describe a block cipher with such a code before explaining how to design a new ciphertext only cryptanalysis of these cryptosystems on the assumption that plaintext belongs to a particular class. As the secret key remains the same for all ciphertext blocks of a given message, encryption process may be compared to noisy transmission of the key where noise is modeled by particular class of plaintext. We presents two cryptanalysis algorithms. The first one uses a single repetition code while the second one uses concatenated codes whose outer and inner codes are repetition codes. We compare the two algorithms and prove that the first one is more efficient than the second one. Open problems and technical parameters are finally given. Up to now first results on known block ciphers seem to confirm the possibility of practical cryptanalysis using this new approach but they still need to be independantly verified. The main point is to find equations of the form

$$< C, w > \overset{q}{=} < K, v >$$

when considering a particular plaintext subset such that $q \neq \frac{1}{2}$ and where $v, w \in {\mathbb{F}_2}^n \times {\mathbb{F}_2}^m$. These equations then form the repetion code itself.
Keywords: block cipher, cryptanalysis, coding theory, repetition codes.

References

[1] P. Camion, Majority Decoding of Large Repetition Codes for the R-ary Symmetric Channel. In: *Proceedings of the AAECC'88 Conference*, Lecture Notes in Computer Science 357, pp 458–466, Springer Verlag, 1989.