

# Design criteria for symmetric primitives

Anne Canteaut<sup>1</sup>

INRIA - Projet CODES  
BP 105 - 78153 Le Chesnay Cedex - France

Despite the many recent advances in public-key cryptography, secret-key algorithms will continue to be important since they are generally much faster than public-key cryptosystems. Therefore, they are widely used in all applications with high throughput requirements. Even if both AES and NESSIE projects have led to several new symmetric primitives, some important problems remain open. For instance, it has been recently shown that the security level offered by all available stream ciphers was lower than expected. *More generally, finding some new criteria for evaluating the security of symmetric primitives (block ciphers, stream ciphers, hash functions) is a constant challenging problem for the cryptographic research community.*

The development of cryptanalysis in the last fifteen years has led to the definitions of some well-defined design criteria. For example, it has been proved that the use of highly nonlinear substitution functions in a block cipher guarantees a high resistance to linear cryptanalysis. The resistance to differential attacks can also be quantified by some properties of the substitution function. For stream ciphers, it is well-known that the use of a correlation-immune Boolean function in combining generators avoids correlation attacks. The designers of symmetric ciphers now provide evidence that their ciphers cannot be broken by these classical attacks. However, these well-known requirements are obviously necessary but not sufficient security conditions. It is then essential to go further in the analysis of symmetric primitives.

**Determination of the design criteria corresponding to all known attacks** The gap is usually very large between the conception of an attack on a particular system and the definition of a general property which quantifies its efficiency. Obviously, all proposed attacks are not so well-understood and it is not always easy to determine their fields of application.

For instance, higher-order differential cryptanalysis has been introduced in 1994 [9]. It allows to distinguish a block cipher from a random permutation by exhibiting a small subspace of plaintexts whose images sum to a certain value predicted in advance. This attack has been applied to several block ciphers. But, the involved weakness seems to be due to very different properties: the use of a substitution function having either a low degree [9] or a particular Walsh spectrum [4], or the use of a diffusion function with a particular structure when the S-box is composed of several bijective mappings (e.g. this last situation occurs for byte-oriented ciphers) [6]. The *a priori* very different natures of these properties make think that they can all be included in a more general criterion, which may be used as a measure of the resistance to this type of attacks.

Other cryptanalytic methods have been recently proposed for breaking some particular symmetric primitives. An example is the recent attack on AES proposed by Courtois and Pieprzyk [5] which relies on the existence of many multivariate quadratic relations between the plaintext bits, the ciphertext bits and the key bits. *Such specific attacks should be formalized and generalized. This work is essential in order to precisely determine their application fields.*

**Relevance of some “intuitive” design criteria** Optimizing the resistance to some classical attacks usually leads to the choice of functions which possess very particular structures. For instance, all known substitution functions which oppose a maximal resistance to both differential and linear attacks are linearly equivalent to some power functions over a finite field (e.g. see [2]). The intuition is that such a strong algebraic property may introduce a weakness which could be exploited by another attack. Therefore, the distance of the substitution functions to the set of all power functions may be used as a design criterion (it is known that the S-boxes of DES are optimal regarding this criterion [8]). However, it is not clear that this property is really relevant

---

<sup>1</sup>Joint work with Claude Carlet (Univ. Paris 8 and INRIA - projet CODES), Pascale Charpin (INRIA - projet CODES), Eric Filiol (INRIA - projet CODES and ESAT, Rennes) and Marion Videau (INRIA - projet CODES)

since no associated attack has been found so far. Many other specific structural properties appear in the study of optimal objects. For example, almost all known bent functions (i.e., the Boolean functions which lie as far as possible to all affine functions) are constant on a large subspace of their inputs [7]. This property may have some important consequences because bent functions appear in the constructions of highly nonlinear balanced functions (used in stream ciphers) and of optimal substitution functions. *It is then essential to try to mount an attack based on these structural properties in order to determine whether they induce a weakness or not.*

*Determining the relevance of all these “intuitive” criteria is very important because of the existence of some tradeoffs between all of them.* This situation occurs in the design of stream ciphers based on linear feedback shift registers. Many different criteria have been defined concerning the Boolean functions used in combination and filtering generators: algebraic degree, correlation-immunity, nonlinearity, several propagation criteria, lack of linear structures... Some of them are essential for a given class of generators (e.g. the correlation-immunity order and the nonlinearity are very important parameters for combination generators [3]). However, it is still an open problem to determine which of them are really relevant in a particular context. We do not know if the use of a combination function having linear structures or the use of a filtering function with bad propagation characteristics has an impact on the security of the corresponding stream cipher. Determining the relevance of all these criteria for the different types of generators is important to design secure stream ciphers.

Some advances in these areas seem to be essential in order to be able to better evaluate the security of symmetric primitives. *It clearly requires to intensify and to combine the search for new cryptanalytic methods and the study of the involved mathematical objects and properties.*

## References

- [1] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions. In *EUROCRYPT'2000*, LNCS 1807, pp. 507–522. Springer-Verlag, 2000.
- [2] A. Canteaut, P. Charpin, and H. Dobbertin. A new characterization of almost bent functions. In *Fast Software Encryption 99*, LNCS 1636, pp. 186–200. Springer-Verlag, 1999.
- [3] A. Canteaut and M. Trabbia. Improved fast correlation attacks using parity-check equations of weight 4 and 5. In *EUROCRYPT'2000*, LNCS 1807, pp. 573–588. Springer-Verlag, 2000.
- [4] A. Canteaut and M. Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. In *EUROCRYPT 2002*, LNCS 2332, pp. 518–533. Springer-Verlag, 2002.
- [5] N.T. Courtois and J. Pierpizick. Cryptanalysis of block ciphers with overdefined systems of equations. In *ASIACRYPT 2002*. Springer-Verlag, 2002. To appear.
- [6] J. Daemen, L.R. Knudsen, and V. Rijmen. The block cipher Square. In *Fast Software Encryption 97*, LNCS 1267, pp. 149–165. Springer-Verlag, 1997.
- [7] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption 94*, LNCS 1008, pp. 61–74. Springer-Verlag, 1995.
- [8] G. Gong and S.W. Golomb. Transform domain analysis of DES. *IEEE Trans. Inform. Theory*, 45(6):2065–2073, 1999.
- [9] L. R. Knudsen. Truncated and higher order differentials. In *Fast Software Encryption 94*, LNCS 1008, pp. 196–211. Springer-Verlag, 1995.
- [10] L.R. Knudsen and D. Wagner. Integral cryptanalysis. In *Fast Software Encryption 2002*, LNCS 2365, pp. 112–127. Springer-Verlag, 2002.