Testing properties of Boolean mappings

Andrew Zubkov and Alexander Serov

Steklov Mathematical Institute, Russian Academy of Sciences,
Gubkina str. 8, 119991, Moscow, Russia
{zubkov,serov}@mi.ras.ru
http://www.mi.ras.ru

According to the principles of contemporary cryptography to ensure the security of information transmission the transform of messages should look as the random uniform transform. In particular, the structure of information transforms should not have simply describable features. Examples of such features are: the existence of low-degree approximations, dependencies between input and output bits, structural properties of analytic representations etc.

We review several methods of testing the existence of such non-desirable properties of Boolean multidimensional mappings spaces.

1. Well-known Discrete Fourier transform permits to find linear approximations for Boolean functions or linear statistical dependencies between the input and output bits of "black-box" transforms of Boolean vectors.

2. Nonlinear statistical dependence between some input and some output bits of "black-box" transform results in (and is equivalent to) the non-uniformity of their multidimensional distribution. Such non-uniformity may be detected by means of statistical test based on Pearson statistics, total variance distance between empirical and uniform distributions etc.

3. Testing analytical structure of Boolean function may be conducted by analyzing the set of low-degree coefficients in its representation as Zegalkin polynomial.

We apply these methods to hash functions MD4 and MD5. We have not succeed to find deviations from uniformity for whole transforms MD4 and MD5, but for some rounds of these functions there exist small deviations from uniformity assumptions.

References

1. Schneier, B.: Applied Cryptography. Protocols, Algorthms and Source Code in C. J. Wiley, 1996.
2. Stankovski, P.: Greedy distinguishers and nonrandomness detectors. INDOCRYPT'2010, Lect. Notes Comput. Sci. Vol. **6498** (2010) 210–226.