UDC 004.912

Ocheretnyi V.O.
(Ternopil Ivan Puluj National Technical University)

RESULTS OF THE STATISTICAL TEST SECURITY HASH ALGORITHMS CANDIDATES COMPETITION FOR SELECTING STANDARD HASH ALGORITHM SHA-3

УДК 004.912

Очеретний В.О.

РЕЗУЛЬТАТИ СТАТИСТИЧНОГО ТЕСТУ БЕЗПЕЧНОСТІ ГЕШ-АЛГОРИТМІВ КОНКУРСУ КАНДИДАТІВ ЗА ВИБІР СТАНДАРТНОГО ГЕШ-АЛГОРИТМУ SHA-3

One of the prospective directions of development of the theory and methods providing the integrity and authenticity of information are the cryptographic checksums. Methods of forming the cryptographic checksums can be divided into two classes: those based on symmetric cryptographic transformation (message authentication code (MAC code)) and hash functions using single-ended transformations (digital signatures) with the use the secret keys. Such functions can be applied immediately as a cryptographic checksum, and in other transformations. For example, for generating a digital signature requires an effective function of displaying messages of a small fixed length (hash value, hash code, or simply hash). Those functions are called hash functions [1–3].

Proceeding from the general theoretical assumptions of the theory of secret systems, potentially persistent are systems in which the characters cryptograms were not statistically dependent on the character of the plaintext. For the estimate these relationships using statistical tests. Several years ago, the hash algorithm SHA-1 has been compromised, and a prospect for the SHA-2 is also very vague because of its close resemblance with the SHA-1. Therefore, the Institute of NIST in November 2007 announced the contest among cryptographers to design a new hash algorithm [2]. The main demands made by the National Institute of Standards and Technology (NIST) to the algorithms candidates provide for the establishment class of hash functions potentially persistent to attacks aimed at SHA-2 and also maintaining or increasing the efficiency of hashing in comparison with the SHA-2 [1]. Algorithm winner of the SHA-3 must support the output block size 224, 256, 384 and 512 bits. Using digest hash codes of length 160-bit is not allowed because of the possibility of finding collisions brute-force attack (exhaustive search of all variants). During the competition remain the same requirements as for the previous hash functions: the maximum size of the input value, the amount of output value, collisional resistance, resistance to finding the preimage and second preimage stream mode calculations, "one pass" [1]. Algorithms for computing functions for different sizes of blocks should be identical and have a minimum of differences in implementation. Use completely different sets of algorithms for four fixed values of the length of the output is not allowed [1]. The studies confirmed resistance hashing algorithms Blake and Grostl to known attacks cryptanalyst, and algorithms finalists JH, Keccak, Skein may be exposed to threats, which reduces their cryptographic strength. Promising avenue for further research is to evaluate the properties of algorithms for collision finalists for the selection of a standard hash algorithm SHA-3.

Literarure sources.

1. Status Report on the First Round of the SHA-3 Cryptographic Hash Algorithm Competition Andrew Regenscheid, Ray Perlner, Shu-jen Chang, John Kelsey, Mridul Nandi, Souradyuti Paul. URL: www.nist.gov/index.html.
2. 2. Finalists hash algorithms, SHA-3. URL: http://habrahabr.ru/blogs/crypto/109946. 3. Hash function. Requirements to the hash function. URL: http://www.scriru.com/14/27/24244176976.php.