UDC 681.3.06 (0.43)

Korol O. G.

Lecturer of Department of Information Systems, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

ENHANCED MAC ALGORITHM BASED ON THE USE OF MODULAR TRANSFORMATIONS

The article considers the choice of cycle functions in the provable persistent key universal hashing scheme, proposed model and method of forming codes of integrity and authenticity of data on the basis of modular transformations, computational complexity reduce algorithm of the hashing schemes implementation using cyclic functions. The object of the research is the process of improving the integrity and authenticity of data packets in security protocols of telecommunication networks. The subject of the study are models, methods and algorithms for monitoring the integrity and authenticity of data packets in security protocols of telecommunication networks. The purpose of the study is to increase the integrity and authenticity of data packets in security protocols of telecommunication networks. The developed enhanced method of forming a cascade MAC differs from the known (algorithm UMAC) using modular hashing on the last stage of the MAC forming that provides high collision properties of strictly universal hashing and safety performance at the level of modern means of demonstrable strength protection. Were obtained estimates of the computational complexity of the formation of the MAC using modular hashing, found, that with comparable rates of resistance the complexity of modular hashing exceeds by 1–2 orders of known schemes based on block symmetric ciphers. However, the use of modular transformations provides provable security and high collision properties of strictly universal hashing.

Keywords: codes of integrity and authenticity of data, a modular transformation, universal classes of hash functions.

NOMENCLATURE

gcd(x, y) is a greatest common divisor of x and y;
D is a dispersion;
f is a composition of f_1 and f_2;
f_1 is a set of functions performing the mapping $X \to U$;
f_2 is a set of functions performing the mapping $U \to Y$;
m is a mathematical expectation;
H is a set of functions f;
H_0 is an initialization vector;
H_1 is a set of functions f_1;
H_2 is a set of functions f_2;
k is a number of elements in binary representation of n;
Key is a key rule;
L is a bit processor;
m_i is a i-bit in binary representation of n;
n is an exponent ;
$O(n)$ is a computational complexity;
p is a large prime integer;
q is a large prime integer;
U is a set of u numbers;
u is a count of numbers in set U;
X is a set of n numbers;
x is a number to be raised;
Y is a set of m numbers;
α is a generator of the ring of integers Z_p;
ε is a fixed accuracy;
$\vee$ is a bitwise logical OR operation;
$\perp n$ is a save lesser n-bits of m-bit result operation;
$\oplus$ is a modulo 2 (XOR).

INTRODUCTION

Studies have shown that the use of modular transformations allows realizing of provably resistant information hashing that satisfies the collisional properties of universal hash functions. Demonstrably safe level of strength is justified by reducing the problem of finding the source and / or the problem of recovering the secret key data to the solution of one of the well-known complexity-theoretic problems [1–3, 6].

At the same time, as shown by studies [1–3, 6], the universal hashing using modular transformations has a significant drawback – high computational complexity of the formation of the hash codes. In fact, for each information unit must perform a modular exponentiation that under transformation module appropriate orders significantly increases the time hashing information sequence. A promising direction in this regard is the development of multilayer universal hashing circuits using modular transformations on the last, the final stage of the hash code formation. This is as shown below, on the one hand provides a high collision properties of the resulting codes of integrity and authenticity of data generation circuit, on the other hand – provides high performance and provable strength level used transformations.

1 PROBLEM STATEMENT

The use of multilayer hash key circuits allows building of effective mechanisms for monitoring the integrity and authenticity of information in telecommunication systems and networks. However, the known multilayer structure (for example, the algorithm UMAC) together with the high speed and the cryptographic strength when applying a cryptographic transformation layer (using symmetric block cipher) lose universal hash properties, which leads to deterioration of the properties of the collision properties of generated message authentication codes. The purpose of the study is to develop a method of forming codes of integrity and authenticity of data based on provably resistant hash key that allows providing high levels of security and with applying certain restrictions on the modular transformations provide high collisional properties.

2 REVIEW OF THE LITERATURE

The analysis of [6–9] shows that the modular transformations are used today in the construction of keyless hash functions. Thus, in the fourth part of the international standard ISO/IEC 10118-4 defined two keyless hash function MASH-1 and MASH-2, which use modular arithmetic, namely the modular exponentiation to construct hash [9]. The very name of functions MASH-1 and MASH-2 occurs

DOI 10.15588/1607-3274-2015-1-8

from abbreviated Modular Arithmetic Secure Hash (secure hashing based on modular arithmetic), emphasizing the use of modular transformations in the formation of the hash image.

Table 1 shows the results of a comparative analysis of performance of some keyless hash functions, including the hash function on the modular arithmetic MASH-1 and MASH-2 [7].

The analysis showed that the major drawback of hash functions MASH-1 and MASH-2 is the low hash code formation rate. In fact, it is determined by the speed of RSA-like encryption, which is 2–3 orders of magnitude slower than modern block symmetric ciphers. However, due to the presence of the possibility of using the existing modular arithmetic hardware and software used in asymmetrical RSA-like cryptosystems, as well as because of the possibility of providing a provable strength level (on the classification of security models NESSIE) considered keyless hash MASH-1 and MASH-2 were standardized [7, 9, 16].

3 MATERIALS AND METHODS

Development of a universal key hashing method with demonstrable strength based on modular transformations.

In the basis of the proposed universal key hashing method with provable strength is the use of modular transformations, providing reduction of the problem of finding the inverse image or a secret key in hashing scheme to one of the well-known complexity-theoretic problems. Such a justification of strength by security models classification NESSIE is considered to be provable security, thus emphasizing the reducibility cryptanalysis to one of the well-known computationally intractable in a given time complexity-theoretic problems [6]. Table 2 shows the results of studies of cyclic functions: the first column contains the complexity-theoretical problem of the function, the second column shows the cyclic function analytical record, in the third column – estimate of the calculating complexity of the cyclic function values, the fourth – estimate of computational complexity of the function inverting (strength estimation).

Studies have shown that the most appropriate solution should obviously consider the use of the cyclic function, the problem of inverting which is associated with the solution of the complexity-theoretic problem of the extraction of square roots modulo *n*.

Under certain restrictions on the values of the composite module *n* this computational complexity inverting problem comparable to the problems of factorization and discrete logarithms. At the same time, the direct calculation of the

Table 1 – A comparative analysis of some keyless hash functions

The hash function	The length of hash	Applied conversion	Processing speed	Security model (by NESSIE)
SHA-2	256, 384, 512	logical and arithmetic	108..109 bit/sec	Practical Security
Whirlpool	512	In finite Galois fields	107..108 bit/sec	Practical Security
GOST 34311-95	256	Block symmetric encryption	107..108 bit/sec	Practical Security
RIPEMD-160	160	logical and arithmetic	108..109 bit/sec	Practical Security
MASH-1	*	Modular squaring	105..106 bit/sec	** «Provable» Security
MASH-2	*	Modular exponentiation 28+1 = 257	104..105 bit/sec	** «Provable» Security

* Determined by the dimension of the conversion module.

** If the parameters of the modular exponentiation comply with the limits for RSA-like systems.

Table 2 – Estimate of the complexity of some complexity-theoretic problems

Complexity-theoretic problem	Candidates for the construction of the cyclic function	Estimate of the computing complexity	Estimate of the inverting complexity
Integer factorization problem	$f(x_i, H_{i-1}) = x_i H_{i-1}$, Function is defined over large prime numbers $x_i = p$ and $H_{i-1} = q$	$O(n^2)$, where $n = \lceil \log_2 p \rceil +$ $+ \lceil \log_2 q \rceil$	$L_N(\alpha, \beta) = \exp\left((\beta + o(1))(\log N)^{\alpha} (\log\log N)^{1-\alpha}\right)$ For the field number of the general form of the inverting complexity $L_N\left(\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right)$, For a field number of a special type $N = a^b + c$ the complexity of the inversion is $L_N\left(\frac{1}{3}, \sqrt[3]{\frac{32}{9}}\right)$
RSA problem	$f(x_i, H_{i-1}) = (x_i \oplus H_{i-1})^e \bmod (N)$, $\gcd(e, \varphi(p, q)) = 1$, $N = pq$	$O(\log_2 e)$ multiplications, the fast exponentiation algorithm	
The discrete logarithm problem	$f(x_i, H_{i-1}) = \left(\alpha^{x_i \oplus H_{i-1}}\right) \bmod (p)$, α – generator Z_p	$O(\log_2 n)$ multiplications, the fast exponentiation algorithm, $O(n^3)$ for $\alpha = 2$, where $n = \lceil \log_2 p \rceil$	$\min\{\sqrt{p}, L_N(\alpha, \beta)\}$, where $L_N(\alpha, \beta) = \exp\left((\beta + o(1))(\log N)^{\alpha} (\log\log N)^{1-\alpha}\right)$ For a primitive field $GF(p)$ the complexity of the inversion is $\min\left\{\sqrt{p}, L_N\left(\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right)\right\}$, For a primitive field $GF(2^m)$ the inversion complexity is $L_N\left(\frac{1}{3}, 1.4\right)$
Diffie-Hellman problem	$f(x_i, H_{i-1}) = \left(\alpha^{x_i \oplus H_{i-1}}\right) \bmod (p)$, α – generator Z_p	$O(n^3)$ for $\alpha = 2$, where $n = \lceil \log_2 p \rceil$	

values of $a \equiv \left(x^2\right)\mathrm{mod}(n)$ requires significantly fewer operations.

It should be noted, however, that the use of a quadratic cycle function does not lead to construction of a universal hashing. Next to the computational complexity is a cyclic function

$$f\left(x_i, H_{i-1}\right) = \left(x_i \oplus H_{i-1}\right)^e \mathrm{mod}(N), \qquad (1)$$

inversion problem which is associated with the solution of the complexity-theoretic problem in RSA, where

$$\gcd(e, \varphi(p,q)) = 1,\ N = pq\,.$$

Thus, the use of cyclic function (1) based on modular exponentiation allows to construct a provably resistant universal hash function only under the constraints on the value of the modular exponent and absolute value of the change.

Another candidate for the cyclic function in the iterative hashing scheme is a function of the form:

$$f\left(x_i, H_{i-1}\right) = \left(\alpha^{x_i \oplus H_{i-1}}\right)\mathrm{mod}(p), \qquad (2)$$

inversion problem which is associated with the solution of the complexity-theoretic problem of the discrete logarithm.

Use of a cyclic function ensures the construction of provably resistant hash, collision properties which satisfy the conditions of universality.

Thus, studies have shown that for the construction of universal hash information with provable security level should be used the cyclic function of the form (1) or of the form (2).

Development of algorithms for iterative key hashing with demonstrable strength based on modular transformations.

Iterative key hash algorithms with demonstrable strength based on the use of modular transformations is based algorithm MASH-1, subject to change initialization vectors and use of the above cyclic functions satisfying certain restrictions on used modular transformations.

Iterative key hashing scheme using cyclic function (1) developed by analogy with the scheme in Section 2NHhashing is shown in Fig. 1. An algorithm for calculating the hash value based on the cyclic function (1) differs from the algorithm MASH-2, basically, by system settings and the determination of constants.

Using the cyclic function (2), the inversion problem of which is based on the solution of the complexity-theoretic problem of the discrete logarithm, construct the following hashing scheme (see Fig. 2).

Designed algorithms differ from the keyless hash algorithms MASH-1 and MASH-2 basically, by system settings and the determination of constants. In addition, the proposed schemes are key hashing, as the secret key data used interchangeable initialization vector H_0 = Key. For applied modular transformations in key hashing cyclic function imposed limitations discussed above.

Thus, the proposed universal hashing method using modular transformations allows formation of authenticators (hashes) to provide the required performance security. Designed algorithms allow practically implement the proposed hashing schemes in software and in hardware form.

4 EXPERIMENTS

Development of proposals for the implementation of the iterative hash key with demonstrable strength using modular transformations.

The proposed universal hashing method is an iterative scheme of formation of the hash code with the cyclic function, built using modular transformations. To ensure high collision properties of universal hashing proposed cyclic function must be implemented with the use of the expressions (1) or (2) with the corresponding constraints on the modular transformations.

The analysis shows that the most expensive from a computational point of view the operation in the implementation of cycle functions (1) and (2) is the operation of modular exponentiation. With the direct exponentiation operations through the chain of multiplications, computational complexity of the implementation of such cyclic functions increases in proportion to the exponent, i.e. for the construction of x the power n generally needs $n-1$ multiplications:

$$x^n = \underbrace{x \cdot x \cdot x \cdot \ldots \cdot x}_{n-1 \text{ multyplications}}\ .$$

An asymptotic estimate of the computational complexity of this exponentiation operation implementation is $O(n)$ multiplications.

To reduce the computational complexity of the implementation of the hashing scheme using cyclic functions (1) and (2) algorithm applied for fast

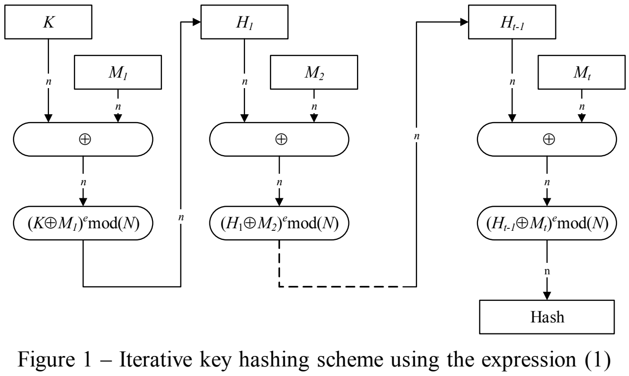

Figure 1 – Iterative key hashing scheme using the expression (1)

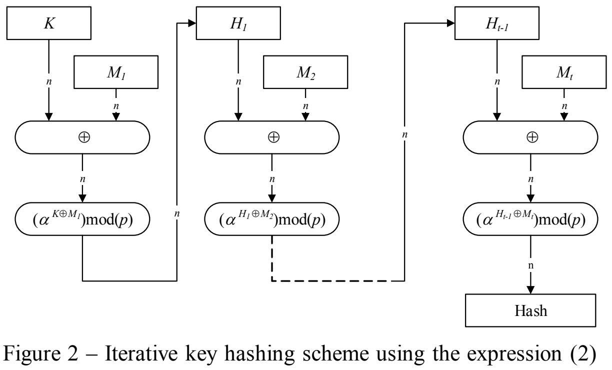

Figure 2 – Iterative key hashing scheme using the expression (2)

exponentiation, which is based on the representation of x^n in the following form:

$$x^n = x^{((\ldots((m_k \cdot 2 + m_{k-1}) \cdot 2 + m_{k-2}) \cdot 2 + \ldots) \cdot 2 + m_1) \cdot 2 + m_0} =$$

$$= ((\ldots(((x^{m_k})^2 \cdot x^{m_{k-1}})^2 \ldots)^2 \cdot x^{m_1})^2 \cdot x^{m_0}, \qquad (3)$$

where $(m_k, m_{k-1}, \ldots, m_0)$ – binary representation of n, i.e. $m_i \in \{0,1\}$ and

$$n = m_k \cdot 2^k + m_{k-1} \cdot 2^{k-1} + \ldots + m_1 \cdot 2 + m_0 \cdot \qquad (4)$$

Rearranging the factors in the representation of x^n we obtain the following expression:

$$x^n = x^{m_0} \cdot (x^2)^{m_1} \cdot (x^{2^2})^{m_2} \cdot (x^{2^3})^{m_3} \cdot \ldots \cdot (x^{2^k})^{m_k},$$

which implies that for the construction of a number x to the power of n required to implement at most k operations of squaring and at most k operations of multiplication, where $k+1$ – number of elements in the binary number n, i.e. $k = (\log_2 n) - 1$. Thus, the computational complexity of calculating the asymptotic x^n can be estimated as $O(\log_2 n)$.

The above algorithm can significantly speed up the computation of cyclic functions (1) and (2) underlying the proposed method of universal hashing. Table 3 shows the dependence of the implementation complexity of the operation of exponentiation through a chain of multiplications and through the representation (3), (4), indicating the minimum necessary order of the conversion module to achieve the required level of security.

The data in the second row of table 3 shown using the equivalence conditions (on computational complexity) of the squaring and multiplication operations.

Analysis of the data in table 4 shows that the implementation of the proposed universal hashing method through a traditional exponentiation algorithm computationally unattainable. The number of multiplications to be executed to compute a value of the cyclic function, even at the lowest level of security (cardinality of the set of key data block symmetric cipher is equal to 2^{80}) exceeds the capabilities of most modern computer systems.

The last row of table 3 is, in fact, is the computational complexity estimate of the proposed hashing scheme. Thus, at the lowest level of strength (cardinality of the set of key data block symmetric cipher is equal to 2^{80}) to calculate one value of cyclic function takes no more than 2046 operations multiplications. For a sufficient level of strength (cardinality of the set of key data BSC equal to 2128) relevant to the national standard encryption USA FIPS-197 (AES), to calculate the cyclic function need to do no more than 6142 multiplications. For high-level strength (cardinality of the set of key data BSC equal to 2256), corresponding to the current domestic standard symmetric cryptoconversion GOST 28147-89, to calculate the cyclic function does not need to perform more than 30718 multiplications.

Developing a model of MAC cascade formation using modular transformations and justification of practical recommendations on its use.

The article proposes a cascade formation model of codes of integrity and authenticity of data (MAC) using the modular transformations. The proposed model is based on a multi-layer universal hashing circuit using the last, the final stage of modular transformations.

Properties of multilayer (composite) design is best explained with the help of mappings language [4, 5]. Let X, Y, U are sets of n, m, u elements, $n < m < u$. H_1 is a set of functions f_1 performing the mapping $X \rightarrow U$ and H_2 is a set of functions f_2 performing the mapping $U \rightarrow Y$. Then $H = H_2 \circ H_1$ is a set of functions f, which is the composition $f = f_1 \circ f_2$.

Characteristics of a multilayered structure presented by the results of the following theorem [1–3].

Theorem 1. The composition of the universal hash functions class $\varepsilon_1 - U(N_1, n, u)$ and strictly universal hash functions class $\varepsilon_2 - SU(N_2, u, m)$ is strictly a universal class with parameters $\varepsilon - SU(N_1 N_2, n, m)$, where $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_1 \varepsilon_2$.

Thus, using the composition of authentication codes algorithms that are equivalent to an algorithm for computing the universal and strictly universal hash functions classes we obtain a multi-layer scheme for generating MAC [11–15]. Properties thus generated codes of integrity and authenticity of data will satisfy the properties of strictly universal class of hash functions.

In the method of forming codes of integrity and authenticity of data, the first layers are proposed to be realized with traditional UMAC high-speed but cryptographically weak universal hashing schemes algorithm, the last layer is proposed to implement using the developed safe (cryptographically strong) strictly universal hashing scheme based on the modular transformations.

Formally, the proposed cascade formation scheme of codes of integrity and authenticity of data shown in Fig. 3.

The main part of the information data is processed first layers of universal hashing. Formed as a result of such conversion hash code on the last processed final stage cryptographically strong universal hash function based on the modular transformation.

Thus, based on the proposed scheme, MAC formation using modular transformations is used:

– on the first layers high-speed universal hashing methods (NH-hashing, polynomial hashing, Carter-Wegman hashing) are used;

– on the last layer secure strictly universal hashing based on modular transformations (using cyclic functions (1) and / or (2)) is used.

Table 3 – Dependence of the implementation complexity regarding the exponentiation method

Exponentiation method	Procedure for conversion module / equivalent length of symmetric cryptographic algorithm key		
	1024 / 80	3072 / 128	15360 / 256
Through a series of multiplications	10308	10924	104623
Fast exponentiation algorithm	2046	6142	30718

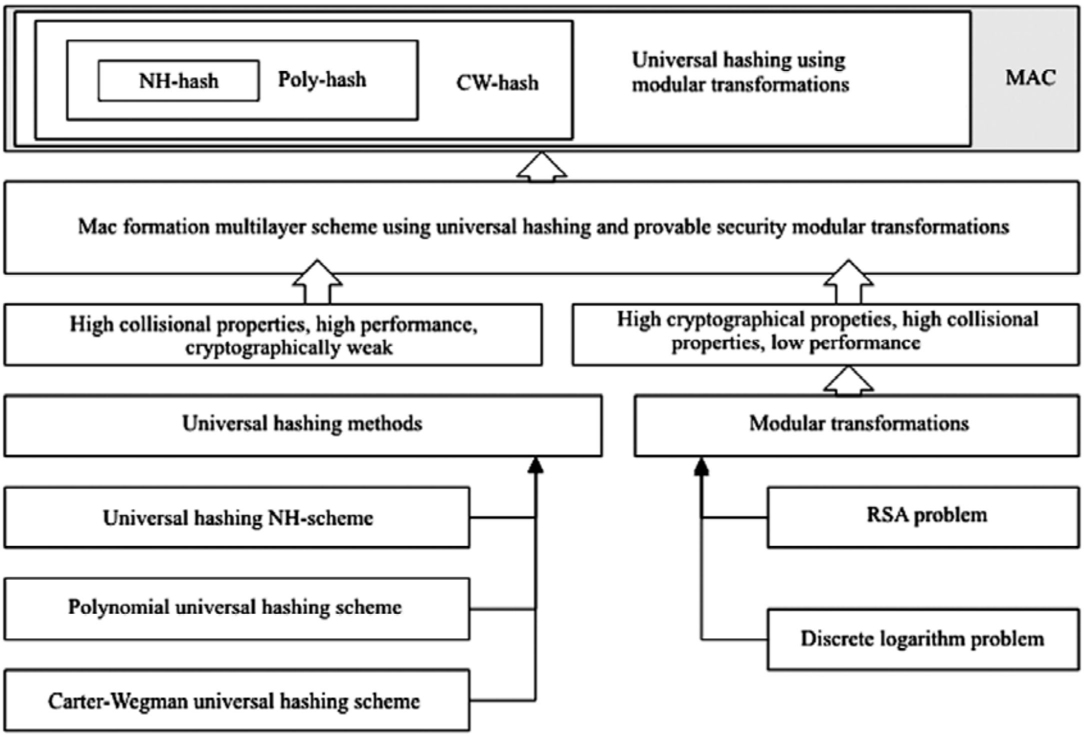
NH-hash
Poly-hash
CW-hash
Universal hashing using modular transformations
MAC
Mac formation multilayer scheme using universal hashing and provable security modular transformations
High collisional properties, high performance, cryptographically weak
High cryptographical propeties, high collisional properties, low performance
Universal hashing methods
Modular transformations
Universal hashing NH-scheme
Polynomial universal hashing scheme
Carter-Wegman universal hashing scheme
RSA problem
Discrete logarithm problem

Figure 3 – Proposed cascade formation scheme control codes of integrity and authenticity of data using the modular transformations

The work [3] proposes technique of statistical studies of collisional properties of MAC, in particular, introduces statistical indicators characterizing the collision properties of forming circuit of control codes integrity and authenticity of data, allowing using methods of probability theory and mathematical statistics to obtain estimates with prescribed confidence interval and the required accuracy.

Experimental studies of collisional properties of message authentication codes UMAC for the relevant sections of the conversion:

– in the first stage investigate collision properties of a mini-version of the universal hashing. To do this, the theoretical estimates of the number of generated hash codes collisions occurring in the course of the experiment must be confirmed;

– in the second stage conduct an experimental study of the properties of pseudo-conflict substrates based on analysis of the properties of the reduced Baby-Rijndael cipher model. Similar studies in the available literature aren't described, appear to be carried out by us for the first time;

– in the third stage conduct an experimental study of the properties of collision properties generated by using mini-UMAC integrity and authenticity of data control. This is the most important part of the research, as it would answer the question of maintaining the properties of universal hashing after application of the cryptographic transformation of the information layer.

Estimates of the number of collisions generated elements will be carried out focusing on the universal hashing collision properties. In fact, we need to confirm or refute the hypothesis of the saving of universal hashing collision properties at all stages of generating of the mini-UMAC control codes of integrity and authenticity of data.

5 RESULTS

Consider a cyclic functions MASH-1 and MASH-2 for the construction of the key universal hash functions and hash option when the initial state (initialization vector) is given by some key rule, i.e. choose H_0 = Key. In this case, we have a certain class of hash functions, depending on the parameter Key. For experimental studies selected the following parameters: $p = 17$, $q = 19$, $N = 323$. Study were to verify the conditions of universal hashing with exhaustive search of all the values of initialization vectors $(\text{Key} = 0, ..., 2^m - 1, m = 8)$ for a sample of the population values of information blocks. The results obtained are summarized in table 3.

Thus, studies have shown that the application of transformations using modular arithmetic allows to build universal and strictly universal hash functions classes,

Table 3 – The results of studies of collisional properties of a key hashing algorithms built on the basis of MASH-1 and MASH-2 by changing the values of the initialization vector secret key

	Based algorithm MASH-1	Based algorithm MASH-2
$\widetilde{m}(n_1)$	41.42	0
$\widetilde{D}(n_1)$	42.74	0
$P_\partial = P(\lvert\widetilde{m}(n_1) - m(n_1)\rvert < 5)$	0.98	≈ 1
$\widetilde{m}(n_2)$	3.99	1
$\widetilde{D}(n_2)$	0.01	0
$P_\partial = P(\lvert\widetilde{m}(n_2) - m(n_2)\rvert < 0.025)$	0.99	≈ 1
$\widetilde{m}(n_3)$	0.26	0.31
$\widetilde{D}(n_3)$	0.21	0.22
$P_\partial = P(\lvert\widetilde{m}(n_3) - m(n_3)\rvert < 0.1)$	0.97	0.97

which on one hand allow high collision properties, on the other hand, under certain restrictions on the value of the modular exponential ensure high security and the applicability of the model demonstrable strength.

For comparison with other key hashing schemes in terms of the resistance and performance will take the following assumptions. Let one multiplication operation on numbers with the order of 2^m requires $\left\lceil \frac{m}{L} \right\rceil$ operations of bitwise modulo two addition (XOR). This assumption is most often used when evaluating the complexity of the cryptographic algorithms implementation. In this case, the estimate of $\left\lceil \frac{m}{L} \right\rceil$ gives the approximate number of L-bit processor cycles necessary for the implementation of the one multiplication operation of numbers the bit length of which does not exceed m. At the same time, hashing using modular transformations process immediately $m/8$ information data bytes.

Table 4 shows the results of comparative studies of the performance of key hashing schemes for fixed security performance. Speed is expressed in an S amount of the 32-bit processor cycles necessary for generating one byte of the output data. Security indicator was fixed over the length of the secret key the attacker needed to hack. For schemes on modular arithmetic the equivalent length of the key block symmetric cryptographic algorithm is shown (see. Table 2).

The data presented in Table 4 show that the use of modular transformations for solving the key hashing problems significantly increases the computational complexity and reduces algorithms speed by 1–2 orders of magnitude. At the same time, the proposed key hashing schemes have provably resistant safety level (problem of finding the hashing key or the inverse image is reduced to solving a certain complexity-theoretic problem). In addition, it was shown above that such authentication schemes satisfy the properties of universal hashing to ensure the high collision characteristics of the generated MAC.

Table 5 shows a comparison of the computational complexity of some hash functions. Data on performance for the proposed MAC scheme with modular transformations are given for the minimum level of persistence (cardinality of the set of key data block symmetric cipher is equal to 2^{80}) and a sufficient level of strength (for modular transformations equivalent length block symmetric cipher key is 128 bits). Length of the MAC generated is 80, and 128 bits, respectively.

For all the functions listed in Table 5 (except the proposed using modular transformations) specific complexity of the codes of integrity and authenticity of data is not dependent on the amount of data processed. For the proposed model using a modular transformations specific complexity with increase of length of data to be processed is reduced. So for a high level of strength (equivalent length block symmetric cipher key is 128 bits) already for data blocks of 32768 bytes is comparable to well-known and used in network security protocols, algorithms form the MAC. For the lowest level of strength (cardinality of the set of key data block symmetric cipher is equal to 2^{80}) the proposed scheme of codes of integrity and authenticity of data cascade formation using modular transformations already for data packets of 2048 bytes is not inferior in performance used to date the formation of the MAC algorithm in network security protocols, including protocols IPsec.

6 DISCUSSION

Analysis of the data presented in Table 3 allows claiming the adequacy of the experimental results. For fixed accuracy ε were obtained high values of confidence probability that indicates the validity and reliability of the results according to their statistical properties of the entire population of data.

Analyze the results of statistical studies and compare them with the theoretical estimates: with $P_{amount} \cdot |H| = 1$ (the first criterion), with $|H|/|B| = 1$ (the second criterion) and with $P_{amount} \cdot |H| = 1$ (the third criterion).

As seen from the data in Table 3 realization of a key hashing scheme based on MASH-1 algorithm when replacing the values of the initialization vector with the secret key does not enable high collision properties. The number of collisions occurring substantially above the upper theoretical limit on both the first and the second criterion, consequently, this structure is not a universal hashing

Table 4 – Estimation of the complexity of hashing algorithms in the S number of the 32-bit processor cycles per byte of data processed

Hash function	Resilience (key length)	Number pf cycles S
SHA-2 (512)	512	80
SHA-2 (256)	256	64
SHA-1	160	80
RIPEMD-160	160	160
MD5	128	64
Modular arithmetic hashing	80	512
	128	1536
	256	7680

Table 5 – Estimate of the complexity of different MAC forming schemes

Algorithm	The length of the input data, bytes					
	2048	4096	8192	16384	32768	65536
HMAC-MD5 (128 bits)	9	9	9	9	9	9
HMAC-RIPE-MD (160 bits)	27	27	27	27	27	27
HMAC-SHA-1 (160 bits)	25	25	25	25	25	25
HMAC-SHA-2 (512 bits)	84	84	84	84	84	84
CBC MAC-Rijndael (128 bits)	26	26	26	26	26	26
CBC MAC-DES (64 bits)	62	62	62	62	62	62
Proposed MAC scheme using modular transformations (80 bits)	38	22	14	10	8	7
Proposed MAC scheme using modular transformations (128 bits)	294	150	78	42	24	15

scheme and so, is not a strictly universal hashing scheme. This result was obtained with a high confidence level $P_{\partial} = P(|\widetilde{m}(n_i) - m(n_i)| < \varepsilon) > 0.9$ for high precision. So for the first criterion the confidence interval was 41.42 ± 5 (confidence level 0.98), for the second criterion the confidence interval was 3.99 ± 0.025 (confidence level 0.99), and for the third criterion the confidence interval was 0.26 ± 0.1 (confidence level 0.97). The key hashing scheme based on MASH-1 algorithm by changing the values of the initialization vector with the secret key satisfies only the third criterion ($\widetilde{m}(n_3) = 0.26$).

The use of key hashing based on MASH-2 algorithm when replacing the values of the initialization vector with the secret key by contrast provides high collision characteristics of universal hashing. For all three criteria resulting estimates are below the upper theoretical limit $\widetilde{m}(n_i) < 1,\ i = 1, 2, 3$. This statement is confirmed with almost 100% probability. So for the first and the second dispersion criterion value $D(n_1)$ and $D(n_2)$ that characterize the dispersion of the hash rules values (MAC formation rules), with the equalities (3.1) and (3.2) with respect to their mathematical expectations $m(n_1)$ and $m(n_2)$ respectively, equals to zero which means the identity of the results obtained in all tests and practically certain that $m(n_1) = 0$, $m(n_2) = 0$. The resulting estimate for the third criterion also lies below the upper theoretical estimation ($\widetilde{m}(n_3) = 0.31$) and this value is confirmed with high confidence level of $P_{\partial} = P(|\widetilde{m}(n_3) - m(n_3)| < 0.1) = 0.97$ for fixed precision (confidence interval is 0.31 ± 0.1).

The explanation for this behavior of the modular transformations in the MASH-1 and MASH-2 schemes lies in the chosen parameters of the modular exponent. Thus, for the MASH-1 algorithm cyclic function (4.3) assumes the value of the modular exponent e = 2 that always breaks the condition (4.5). In the algorithm MASH-2 exponent is set e = 2^8+1 = 257 that for the chosen parameters $p = 17$, $q = 19$, $N = 323$ satisfies the constraint (4.5): $\gcd(e, \varphi(N)) = \gcd(257, 288) = 1$. Therefore, the key hashing built on the basis of modular transformations in some cases allows to provide for the universal properties and strictly universal hashing. To perform these properties condition (3.5) is necessary to be performed which a scheme for the selected parameters on the basis of the algorithm MASH-2 shows.

CONCLUSIONS

In this paper were obtained the theoretical generalization and new solution of scientific-applied problem, which is to develop and research of models and methods of effective mechanisms for monitoring the integrity and authenticity of data packets while minimizing the number of CPU cycles per byte of information to process to provide the necessary reliability and data security in telecommunications networks.

Scientific novelty of the work is following.

1. For the first time to analyze the collision properties of the codes monitoring the integrity and authenticity an approach is suggested based on the creation of scale models (mini version) algorithms of UMAC, which allows them to retain the algebraic structure.

2. For the first time mathematical apparatus and methods for the analysis of statistical studies of collisional properties are suggested which allows to determine the distribution of codes formed on the entire set of key data and obtain estimates of collisional properties with the required accuracy.

3. For the first time model and method of forming codes of integrity and authenticity of data using at the final stage cryptographically strong strictly universal hash function based on modular transformations. The proposed solution provides high collision properties of strictly universal hashing, low computational complexity and high security performance at the level of modern means of cryptographic protection with provable security.

Practical advice on building a cascade formation schemes of MAC based on modular hashing was justified the implementation of which will ensure the delivery time information packet to 0.5 sec; safe time more than 200 years; the probability of imposing a false message is not more than 10^{-25}; the probability of message modification message is not more than 10^{-25}. The usage of the developed models and methods of forming the MAC to control the integrity and authenticity of data packets in security protocols of telecommunication networks and internal payment banking systems.

ACKNOWLEDGEMENTS

The work is supported by the scientific research project «Prospective study of methods and mechanisms to ensure the integrity and authenticity of data circulating in the internal payment system of commercial bank» № 58/2008 and scientific research project «Development of methods of expediting the transfer and protection of information in telecommunication systems» № 36B113.

REFERENCES

1. Stinson D. R. Some constructions and bounds for authentication codes / D. R. Stinson // J. Cryptology. – 1988. – № 1. – P. 37–51.
2. Stinson D. R. The combinatorics of authentication and secrecy codes / D. R. Stinson // J. Cryptology. – 1990. – № 2. – P. 23–49.
3. Кузнецов А. А. Исследование коллизионных свойств кодов аутентификации сообщений UMAC / А. А. Кузнецов, О. Г. Король, С. П. Евсеев // Прикладная радиоэлектроника. – Харьков : Изд-во ХНУРЭ, 2012. – Т. 11, № 2. – С. 171–183.
4. Hoholdt T. An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound / T. Hoholdt // The first steps, IEEE Trans. Info. Theory. – 1997. – 135 p.
5. Maitra S. Further constructions of resilient Boolean functions with very high nonlinearity / S. Maitra, E. Pasalic // Accepted in SETA. – May, 2001.
6. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 504 с.
7. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag.
8. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. / В. Столлингс : пер. с англ. – М. : Вильям, 2001. – 672 с.
9. Король О. Г. Исследование методов обеспечения аутентичности и целостности данных на основе односторонних хеш-функций / О. Г. Король, С. П. Евсеев // Науково-технічний журнал «Захист інформації». – 2008. – Спецвипуск (40). – С. 50–55.
10. Bierbrauer J. Authentification via algebraic-geometric codes [Electronic resource] / J. Bierbrauer. – Access mode : http:// www.math.mtu.edu/~jbierbra/ potpap.ps.
11. Bierbrauer J. On families of hash function via geometric codes and concatenation / J. Bierbrauer, T. Johansson, G. Kabatianskii // Advances in Cryptology – CRYPTO 93. Lecture Notes in Computer Science. – 1994 – № 773. – P. 331–342.
12. Bierbrauer J. Universal hashing and geometric codes [Electronic resource] / J. Bierbrauer. – Access mode : http://www.math.mtu.edu/ ~jbierbra/ hashco1.ps.

13. Black J. «UMAC: Fast and provably secure message authentication», Advances in Cryptology. / J. Black, S. Halevi, H. Krawczyk, T. Krovetz, P. Rogaway // CRYPTO '99, LNCS, Springer-Verlag, 1999. – Vol. 1666 – P. 216–233.
14. Carter J. L. Universal classes of hash functions / J. L. Carter, M. N. Wegman // Computer and System Scince. – 1979. – № 18. – P. 143–154.
15. Krovetz T. UMAC – Message authentication code using universal hashing. IETF Internet Draft, draft-krovetz-umac-02.txt [Electronic resource]. – Access mode: www.cs.ucdavis.edu/~rogaway/umac, 2004.
16. NESSIE consortium «NESSIE Security report» Deliverable report D20 – NESSIE, 2002. – NES/DOC/ENS/WP5/D20 [Electronic resource]. – Access mode: http://www.cryptonessie.org/.

Article was submitted 07.11.2014.
After revision 21.11.2014.

Король О. Г.

Преподаватель кафедры информационных систем, Харьковский национальный экономический университет им. С. Кузнеца, Харьков, Украина

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ МАС, ОСНОВАННЫЙ НА ИСПОЛЬЗОВАНИИ МОДУЛЯРНЫХ ПРЕОБРАЗОВАНИЙ

Обосновывается выбор цикловых функций в схеме доказуемо стойкого ключевого универсального хеширования, предлагается модель и метод формирования кодов контроля целостности и аутентичности данных на основе модулярных преобразований, алгоритм снижения вычислительной сложности реализации схем хеширования с использованием цикловых функций. Объектом исследования является процесс повышения целостности и аутентичности пакетов данных в протоколах безопасности телекоммуникационных сетей. Предметом исследования являются модели, методы и алгоритмы контроля целостности и аутентичности пакетов данных в протоколах безопасности телекоммуникационных сетей. Целью работы является повышение целостности и аутентичности пакетов данных в протоколах безопасности телекоммуникационных сетей. Разработанный усовершенствованный метод каскадного формирования МАС-кодов отличается от известного (алгоритм UMAC) применением модулярного хеширования на последнем этапе формирования МАС, что позволяет обеспечить высокие коллизионные свойства строго универсального хеширования и показатели безопасности на уровне современных средств защиты доказуемой стойкости. Получены оценки вычислительной сложности формирования МАС с использованием модулярного хеширования, установлено, что при сравнимых показателях стойкости сложность модулярного хеширования превышает на 1–2 порядка известные схемы на основе блочных симметричных шифров. Тем не менее, применение модулярных преобразований обеспечивает доказуемый уровень безопасности и высокие коллизионные свойства строго универсального хеширования.

Ключевые слова: коды контроля целостности и аутентичности данных, модулярные преобразования, универсальные классы хеширующих функций.

Король О. Г.

Викладач кафедри інформаційних систем, Харківський національний економічний університет ім. С. Кузнеця, Харків, Україна

ВДОСКОНАЛЕНИЙ АЛГОРИТМ МАС, ЗАСНОВАНИЙ НА ВИКОРИСТАННІ МОДУЛЯРНИХ ПЕРЕТВОРЕНЬ

Обґрунтовується вибір циклових функцій у схемі доказово стійкого ключового універсального хешування, пропонується модель і метод формування кодів контролю цілісності та автентичності даних на основі модулярних перетворень, алгоритм зниження обчислювальної складності реалізації схем хешування з використанням циклових функцій. Об'єктом дослідження є процес підвищення цілісності та автентичності пакетів даних у протоколах безпеки телекомунікаційних мереж. Предметом дослідження є моделі, методи та алгоритми контролю цілісності та автентичності пакетів даних у протоколах безпеки телекомунікаційних мереж. Метою роботи є підвищення цілісності та автентичності пакетів даних у протоколах безпеки телекомунікаційних мереж. Розроблений удосконалений метод каскадного формування МАС-кодів відрізняється від відомого (алгоритм UMAC) застосуванням модулярного хешування на останньому етапі формування МАС, що дозволяє забезпечити високі колізійні властивості суворо універсального хешування і показники безпеки на рівні сучасних засобів захисту доказової стійкості. Отримано оцінки обчислювальної складності формування МАС з використанням модулярного хешування, встановлено, що при порівнянних показниках стійкості складність модулярного хешування перевищує на 1–2 порядки відомі схеми на основі блокових симетричних шифрів. Проте, застосування модулярних перетворень забезпечує доказовий рівень безпеки і високі колізійні властивості суворо універсального хешування.

Ключові слова: коди контролю цілісності та автентичності даних, модулярні перетворення, універсальні класи хешуючих функцій.

REFERENCES

1. Stinson D. R. Some constructions and bounds for authentication codes, *J. Cryptology,* 1988, No. 1, pp. 37–51.
2. Stinson D. R., The combinatorics of authentication and secrecy codes, *J. Cryptology,* 1990, No. 2, pp. 23–49.
3. Kuznecov A. A., Korol' O. G., Evseev S. P. Issledovanie kolliziionnyx svojstv kodov autentifikacii soobshhenij UMAC, *Prikladnaya radioe'lektronika.* Xar'kov, Izd-vo XNURE', 2012, Vol. 11, No. 2, pp. 171–183.
4. Hoholdt T. An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps, *IEEE Trans. Info. Theory*, 1997, 135 p.
5. Maitra S., Pasalic E. Further constructions of resilient Boolean functions with very high nonlinearity, *Accepted in SETA,* May, 2001.
6. Kuznecov O. O. Evseev S. P., Korol' O. G. Zaxist informacії v informacijnix sistemax. Xar'kov, Vid. XNEU, 2011, 504 p.
7. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004, Version 0.15 (beta), Springer-Verlag.
8. Stollings V. per. s angl. Kriptografiya i zashhita setej: principy i praktika, 2-e izd. Moscow, izdatel'skij dom «Vil'yam», 2001, 672 p.
9. Korol' O. G., Evseev S. P. Issledovanie metodov obespecheniya autentichnosti i celostnosti dannyx na osnove odnostoronnix xesh-funkcij, *Naukovo-texnichnij zhurnal «Zaxist informacії»*, Specvipusk (40), 2008, pp. 50–55.
10. Bierbrauer J. Authentification via algebraic-geometric codes [Electronic resource], Access mode : http://www.math.mtu.edu/~jbierbra/ potpap.ps.
11. Bierbrauer J., Johansson T., Kabatianskii G. On families of hash function via geometric codes and concatenation, *Advances in Cryptology – CRYPTO 93. Lecture Notes in Computer Science*, 1994, No. 773, pp. 331–342.
12. Bierbrauer J. Universal hashing and geometric codes [Electronic resource], Access mode : http://www.math.mtu.edu/~jbierbra/ hashco1.ps.
13. Black J., Halevi S., Krawczyk H., Krovetz T., Rogaway P. «UMAC: Fast and provably secure message authentication», Advances in Cryptology, CRYPTO '99, LNCS, Springer-Verlag, 1999, vol. 1666, pp. 216–233.
14. Carter J. L., Wegman M. N. Universal classes of hash functions, *Computer and System Science,* 1979, No. 18, pp. 143–154.
15. Krovetz T. UMAC – Message authentication code using universal hashing. IETF Internet Draft, draft-krovetz-umac-02.txt [Electronic resource]. Access mode: www.cs.ucdavis.edu/~rogaway/ umac, 2004.
16. NESSIE consortium «NESSIE Security report». Deliverable report D20. NESSIE, 2002. NES/DOC/ENS/WP5/D20 [Electronic resource]. Access mode: http://www.cryptonessie.org/.