Development of a pseudo-random substrate for the UMAC algorithm on crypto-code constructions

Alla Havrylova [1], Andrii Tkachov[1],
Alexander Shmatko[2]

1. Department of Cybersecurity and Information Technologies, Kharkiv National Economic University named after Semyon Kuznets, UKRAINE, Kharkiv, Nauki str., 9-A,
E-mail: alla.gavrylova@hneu.net
E-mail: snsncps@gmail.com

2. Department of Software Engineering and Management Information Technologies, National Technical University "Kharkov Polytechnic Institute", UKRAINE, Kharkov, st. Kirpicheva, 2,
E-mail: asu.spios@gmail.com

Abstract – an analysis of the options for the formation of hash-codes has been carried out, modifications of the codes for controlling the integrity and authenticity of data have been proposed.

Keywords – hash-code, UMAC, AES, RSA, MASH-2, crypto-code constructions.

I. Introduction

When transmitting information over telecommunication channels, hashing of transmitted messages is used, which is usually carried out using manipulation detection codes (to control data integrity) and message authentication codes (to confirm the authenticity of data). When using a reliable hash function, it is computationally difficult to create a fake message with the same hash value as the genuine one. However, these threats can be realized due to the weaknesses of specific hashing algorithms, signatures, or errors in their implementations.

The existing hashing algorithms for verifying the authenticity of received messages when working in the post-quantum period do not have the necessary cryptographic resistance to hacking [1], so the problem arises of creating new algorithms or modifying existing ones. These cryptographic algorithms must have not only a higher degree of cryptographic strength, but also sufficient efficiency. Also, hashing algorithms that are resistant to hacking from quantum computers require large enough power resources and a large number of operations to calculate the hash code. Consequently, the purpose of this work is to analyze the proposed approaches to the creation of hash codes and to propose a way to increase their cryptographic properties by modifying the codes for controlling the integrity and authenticity of data.

II. Analysis of algorithms for the formation of a pseudo-random substrate

In their work [2], the authors proposed a method for constructing multilayer hashing functions using the UMAC algorithm as an example. This algorithm is required to form a pseudo-random substrate. It is based on a combination of multi-step key universal hashing and the use of a symmetric block cipher. Thus, universal hashing in a multi-layered UMAC design allows providing the same probability of generating hash images for the entire set of key data used. In works [3, 4] it is indicated that the obtained property ensures the safety of the algorithm.

Let us consider the features of the formation of a pseudo-random substrate with cryptographically strong algorithms: 1) the AES block symmetric cipher algorithm; 2) RSA algorithm on modular transformations using cycle functions; 3) keyless algorithm MASH-2 using modular transformations (Table 1).

TABLE 1

ANALYSIS OF ALGORITHMS FOR FORMATION OF PSEUDO-RANDOM SUBSTRATE

Algorithm	Algorithm properties
AES	+ high performance indicators; - there is no guarantee of preservation of properties of universality
RSA	+ burglary resistance in existing conditions is high; - does not provide efficiency; - low post-quantum cryptographic strength
MASH-2	+ provides universality and cryptographic strength; - low speed of hash-code generation

III. The use of modified codes on elliptic curves of McEliece in crypto-code constructions

Thus, to eliminate the identified shortage, it is proposed to use crypto-code constructions on McEliece elliptic curves and hybrid crypto-code constructions on defective codes as a mechanism for forming a pseudo-random substrate for the third layer of the cascade hashing algorithm UMAC (Figure 1).

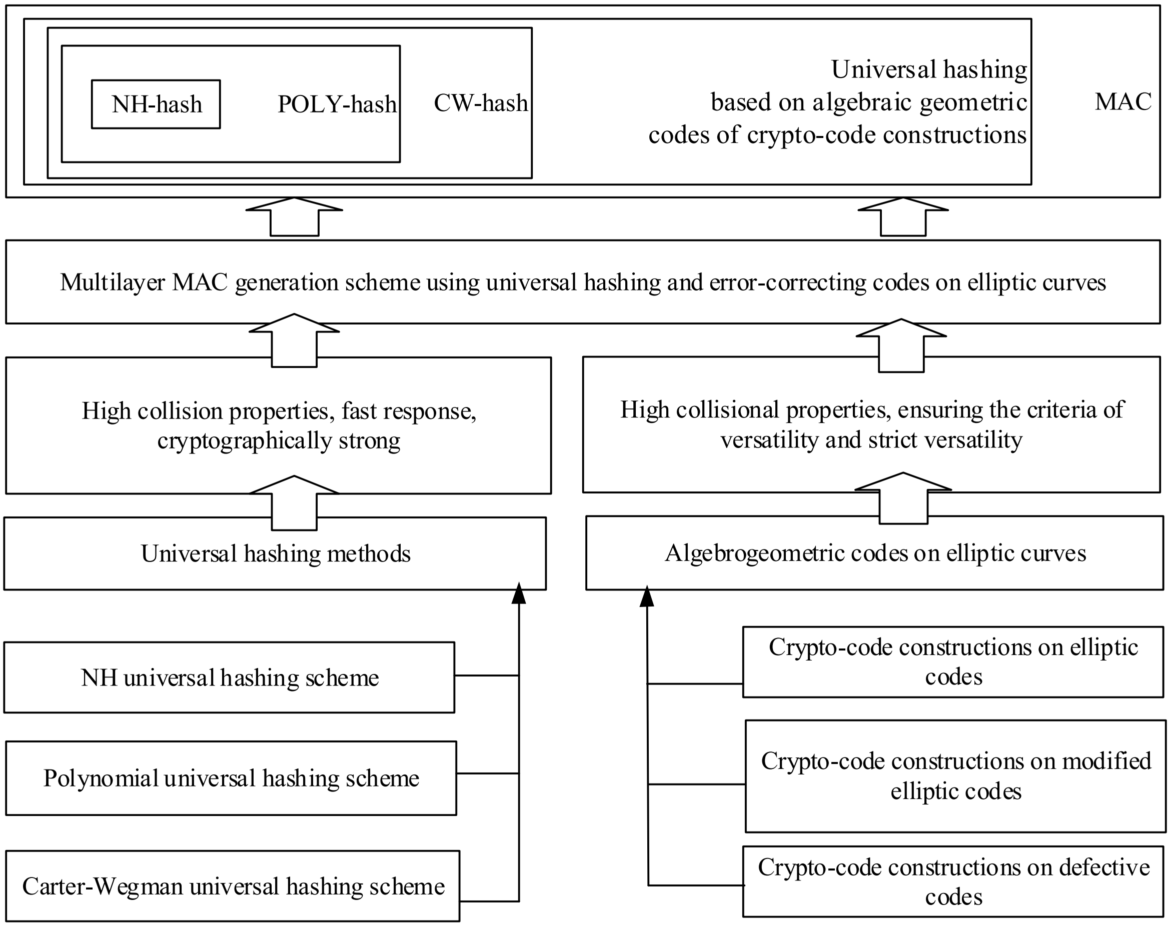
NH-hash
POLY-hash
CW-hash
Universal hashing based on algebraic geometric codes of crypto-code constructions
MAC
Multilayer MAC generation scheme using universal hashing and error-correcting codes on elliptic curves
High collision properties, fast response, cryptographically strong
High collisional properties, ensuring the criteria of versatility and strict versatility
Universal hashing methods
Algebrogeometric codes on elliptic curves
NH universal hashing scheme
Polynomial universal hashing scheme
Carter-Wegman universal hashing scheme
Crypto-code constructions on elliptic codes
Crypto-code constructions on modified elliptic codes
Crypto-code constructions on defective codes

Fig. 1 – Scheme of the formation of a pseudo-random substrate of the UMAC algorithm on crypto-code constructions

In the proposed method for generating data integrity and authenticity control codes, the first transformation layers are proposed to be implemented with high-speed, but cryptographically weak universal hashing schemes, traditional for the UMAC algorithm-code constructions. The pseudo-random substrate can be represented by varieties that should equally ensure the implementation of the necessary transformations and the preservation of the properties of universality by the UMAC algorithm.

Conclusions

As a result of the analysis of the existing algorithms for the formation of a pseudo-random substrate, the advantages and disadvantages accompanying the formation of a hash code were highlighted, and it was also proposed to use varieties of McEliece elliptic codes on crypto-code constructions.

References

[1] Gavrilova A. and other. Development of a modified UMAC Algorithm based on crypto-code constructions / A. Gavrilova, I. Volkov, Yu. Kozhedub, R. Korolev, O. Lezik, V. Medvediev, O. Milov, B. Tomashevsky, A. Trystan, O. Chekunova // Eastern-European Journal of Enterprise Technologies. – 2020. – № 4/9 (106). – C. 45 – 63.

[2] Korol Olha, Havrylova Alla. Mathematical models of hybrid crypto-code constructions in the UMAC algorithm / Olha Korol, Alla Havrylova // Przetwarzanie, transmisja i bezpieczenstwo informacji, 2020, Vol. 12. – Bielsko-Biala : Wydawnictwo naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej. – S. 125-134.

[3] Korol Olga, Parhuts Lubomir, Evseev Sergey. Method of concatenated transformation of MAC-codes using modular transformations / Olga Korol, Lyubomir Parkhuts, Sergey Evseev // Nauchnye vedomosti. Series History. Political science. Economy. Computer science. – 2013. – No. 15 (158). – Issue. 27/1. – S. 147 – 157.

[4] Yevseiev Serhii, Havrylova Alla. Improved UMAC algorithm with crypto-code McEliece's scheme / Serhii Yevseiev, Alla Havrylova // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko].– Vienna : Premier Publishing s.r.o., 2020.– P. 79 – 92..