UDC 004.056

Vitaliy Kazmirevs'kiy

THE RESEARCH OF INFEASIBILITY TO LINEAR AND DIFFERENTIAL CRYPTOANALYSIS OF HASHING FUNCTIONS

Vinnytsia National Technical University

Abstract

Linear and differential cryptological analysis of hashing algorithms was considered and analyzed. The general structure of the hash code was considered. With the use of this structure, possible attacks on hash functions was considered. The infeasibility of a number of hashing algorithms has been studied.

Keywords: *hash function, cryptanalysis, prototype, algorithm, linear cryptanalysis, differential cryptanalysis.*

The introduction

The year 2022 in Ukraine is characterized by a number of mass cyberattacks. On January 14, twenty-two sites of public authorities suffered significant damage. Seventy sites were disabled on the instructions of the SBU and the State Special Service [1]. Subsequently, powerful DDoS-attacks were observed, interruptions were recorded in the work of the web services of PrivatBank and Oshkadbank and other information resources of Ukraine. The websites of the Armed Forces and the Ministry of Defense were also subjected to the cyberattacks [2]. In this manner, the task of protecting information and data follows. The events described above, which are related to the attacks on the various resources and services, have shown that the information security tools need to be improved or developed with a new approach. Such means of information protection include software modules of cryptographic data protection, in which it is necessary to implement the choice of hashing methods resistant to linear and differential cryptanalysis. The aim of this study is to improve the infeasibility of software libraries by cryptographic analysis of the hash functions they implement.

To achieve this goal, the following tasks were solved:

- a concept of hash function was analyzed;
- the cryptanalysis methods for their application to hash functions were analyzed;
- a tool was developed, which consists of a set of tests to analyze the infeasibility of hash functions;
- the test results were analyzed.

The cryptographic hash functions

The hash function (m) or hash function is a deterministic function, the input of which is a string of bits of arbitrary length, and the output is always a string of bits of fixed length n. The value of the hash function H (m) for the input m is called the hash value or abbreviated hash [3]. Other names can be widely used in the literature, namely: hash, hash image, hash code, convolution, message digest, cryptographic checksum, message authentication code, manipulation detection code.

The cryptanalysis of hashing functions is usually focused on the study of the internal structure of the compression algorithm and is based on attempts to find effective methods for detecting collisions in a single function [4].

If this problem is solved, the attacker has to consider a fixed initial value. The specific type of attack on the compression algorithm depends on the internal structure of this function. Usually, for example, when it comes to symmetric block ciphers, the compression algorithm involves several rounds of data processing, so it is best to analyze the change in the bit structure of the data from round to round [4].

It should be borne in mind that the collisions must exist in any hashing function, since the latter reflects at least a block of length b in the hash code of length n, where b> n [4].

All that is needed is the computational impossibility to detect such collisions [4, 5].

The linear cryptanalysis

In cryptography, linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. The attacks were designed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used block cipher attacks; the other is differential cryptanalysis. The discovery is attributed to Mitsuru Matsui, who first applied this technique to the FEAL cipher [6, 7].

Linear cryptanalysis consists of two parts. The first is to construct linear equations that connect plaintext, ciphertext, and key bits that have large offsets; that is, the retention probabilities (in the space of all possible values of their variables) are as close as possible to 0 or 1. Second, use these linear equations together with known pairs of plaintext and encrypted text to obtain key bits [6, 7].

The differential cryptanalysis

The differential cryptanalysis is a general form of cryptanalysis that applies primarily to block ciphers, as well as to stream ciphers and cryptographic hash functions. In the broadest sense, this is a study of how differences in the information entered can affect the resulting difference in output. The discovery of differential cryptanalysis is generally attributed to Eli Biham and Ada Shamir in the late 1980s, who published a series of attacks on various block ciphers and hash functions, including a theoretical weakness in the Data Encryption Standard (DES). Biham and Shamir noted that DES was surprisingly resistant to differential cryptanalysis, but small modifications of the algorithm would make it much more receptive [6, 7].

The differential cryptanalysis is usually an attack on the selected plaintext, which means that an attacker must be able to obtain encrypted texts for a certain set of plaintext of their choice. However, there are extensions that allow you to attack known plaintext or even attack only encrypted text. The main method uses plaintext pairs connected by a constant difference. The difference can be determined in several ways, but the exclusive OR (XOR) operation is common. Then the attacker calculates the differences of the corresponding encrypted texts, hoping to identify statistical patterns of their distribution [6, 7].

The cryptanalysis of hashing functions

The following hash functions were selected for cryptanalysis:

1) SHA-224,
2) SHA-256,
3) SHA-384,
4) SHA-512,
5) SHA3-224,
6) SHA3-256,
7) SHA3-384,
8) SHA3-512,
9) RIPEMD-128,
10) RIPEMD-160,
11) RIPEMD-256,
12) RIPEMD-320,
13) Scrypt.

The results of testing hashing algorithms are shown on the graph (Fig. 1), on the X axis - the points scored by the algorithms during the analysis, on the Y axis - the ordinal number of the hash function.

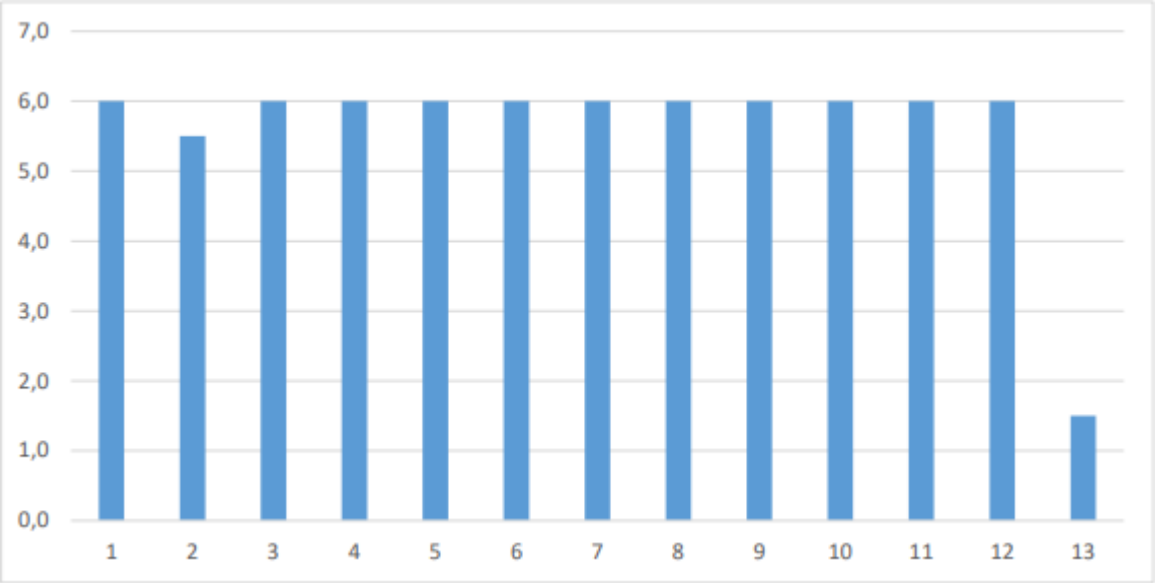

Figure 1 – Graphic comparison of hashing algorithms

The cryptanalysis of hashing algorithms showed that the most stable algorithms are SHA-224, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RIPEMD-128, RIPEMD-160, RIPEMD-256, RIPEMD-320. Less stable was the hash function SHA-256. The Scrypt algorithm showed the lowest result.

Conclusions

Thus, the main methods of linear and differential cryptographic analysis of hash functions are considered and analyzed. In this manner, the result of this study is the research of the infeasibility of a number of hash functions SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RIPEMD-128, RIPEMD- 160, RIPEMD-256, RIPEMD-320, Scrypt. Most hash functions have shown excellent results, but it must be remembered that there is no clear crypto-stable algorithm, crypto-stability of the algorithm is fleeting, so the algorithms are constantly in need of crypto-analysis and improvement. The mathematical probability of a system failure is always higher than the intuitive estimate of this probability. This conclusion is valid for all types of the cryptographic hash functions.

REFERENCES

1. Anton Kudin, Bogdan Kovalenko. Differential analysis of hashing functions and block ciphers: a generalized approach. URL: http://jrnl.nau.edu.ua/index.php/Infosecurity/ article/view/8734 (date of application: 18.05.2022).

2. Cabinet of Ministers of Ukraine - 22 state bodies were affected by the cyber attack on January 14, - State Special Service. (б.д.). b.d.). Home | Cabinet of Ministers of Ukraine. https://www.kmu.gov.ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnih-organi-derzhspeczvyazku (date of application: 18.05.2022)

3. Cabinet of Ministers of Ukraine - On cyber attacks on the sites of military structures and state banks. (b.d.). Home | cabinet of Ministers of Ukraine. https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv (date of application: 18.05.2022)

4. Gaetan Leurent. Improved Differential-Linear Cryptanalysis of 7-round Chaskey with Partitioning. URL: https://www.iacr.org/archive/eurocrypt2016 /96650217/96650217.pdf (date of application: 18.05.2022).

5. Howard M. Heys. A Tutorial on Linear and Differential Cryptanalysis. URL: https://ioactive.com/wp-content/uploads/2015/07/ldc_tutorial.pdf (date of application: 18.05.2022).

6. Vitaliy Kazmirevs'kiy Analysis of methods of cryptanalysis of hash functions: materials of the L scientific and technical conference of the Faculty of Information Technology and Computer Engineering, Vinnytsia, 2021. URL: https://conferences. vntu.edu.ua/index.php/all-fitki/all-fitki-2021/paper/ view/12543 (date of application: 18.05.2022).

7. Yurii Baryshev, Volodymyr Luzhetsky Methods and means of fast multichannel data hashing in computer systems: a monograph on the general. ed. Volodymyr Luzhetsky. Vinnytsia, VNTU, 2016. 144 p.

Vitaliy Kazmirevs'kiy — Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: kazmirevskiy1999@gmail.com

Scientific supervisor: ***Yurii Baryshev*** – PhD (Eng), Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia. email: yuriy.baryshev@vntu.edu.ua