Development of hashing algorithms based on iterative block ciphers and study of their cryptographic strength

by

Kairat Sakanuly Sakan

Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy (Ph.D.) in the doctoral program "8D06301- Information Security Systems"

ABSTRACT

The relevance of the research topic. In the era of the rapid development of modern electronic devices, communications, and Internet technologies, cryptographic methods, that is, encryption and hashing systems, are mainly used to ensure the security of information.

Hash functions are widely used in electronic systems, ranging from password and key protection, integrity checking, and authentication to blockchain technology, as well as in the field of post-quantum cryptography.

Currently, many new data protection systems and models are being developed with the help of new constructions and design methods. However, the expansion of information technology capabilities and the rapid development of computing power leads to the emergence of new specialized attacks and modified versions of existing attacks. In this regard, there is a need to constantly develop and update information security systems, including existing models and hashing systems, that is, the developed hash functions must undergo strict checks on security properties.

The main advantage of hash functions based on block ciphers is the use of well-studied cryptographic primitives and constructs. Also, in a block cipher, it is possible to adjust the required level of security and performance of hash functions by making changes to such parameters as the length of the block and key and the number of rounds. The use of a strong block cipher in the hashing algorithm makes it difficult to use the methods of linear and differential cryptanalysis to search for collisions, as well as the first and second preimages. An in-depth analysis of the block cipher components used in the development of hash functions, and also the role of hash functions in modern technologies, require continuous and focused scientific research.

The main direction of the dissertation work is the development of a new hashing algorithm based on a block cipher that provides a high level of security and computational performance.

Taking into account the fact that now international standards, cryptographic tools, and foreign-made software are mainly used to protect the information in the electronic systems of the Republic of Kazakhstan, the creation of domestic data hashing systems is certainly an urgent and necessary issue.

The purpose of the dissertation work. Development of a secure and high-performance hashing algorithm based on a block cipher adapted to software and

hardware implementation and parallel computing, as well as the study of its security and efficiency properties.

Research objectives:

– Conduct a review of modern hash functions, analysis of collision research methods in hash functions, a study of types of attacks and cryptanalysis methods;

– Develop a new block cipher algorithm used as a compression function;

– Develop a new hashing algorithm based on the block cipher;

– Investigate the security properties of the developed hashing algorithm using sets of statistical tests, the avalanche effect criterion, cryptanalysis methods, and "close collisions";

– Implement software and hardware-software implementation of the developed hashing algorithm and evaluate its effectiveness.

The object of study. Encryption systems and cryptographic hash functions.

The subject of study.

– Developed block cipher algorithm with a special architecture of substitution tables, using S-boxes of small dimensions;

– Developed hashing algorithm based on block cipher used as compression function.

Research methods. The paper uses methods of the theory of Boolean functions, linear algebra, probability theory and mathematical statistics, various cryptographic methods and types of attacks on hash functions, and the avalanche effect.

The scientific novelty of the research:

– A new symmetric block cipher algorithm has been developed;

– A new hashing algorithm based on a block cipher has been developed, adapted for parallel computing and software and hardware implementation;

– A new scheme for the conjugated use of four 4-bit S-boxes to matrix element indices is proposed, the use of which makes it possible to increase the security of the algorithm and more efficiently use the chip memory in hardware implementation;

– A new scheme for applying a nonlinear transformation to the compression function is proposed, which helps to reduce the number of rounds;

– The possibility of choosing k parts of a hashing block relative to the size of the initial hashed message is proposed, which in turn increases the performance of calculations (k=3,…, 8, k is the number of parts).

The theoretical and practical significance of the work. The theoretical and practical value of the results obtained in the course of scientific research increases the possibility of using cryptographic information protection facilities in electronic devices and special data transmission and storage systems, which in the future opens up new opportunities for the development of domestic information systems.

The developed hashing algorithm HBC-256 was included as a separate section in the monograph "Development and research of hashing algorithms of arbitrary length" by the Guppyprint publishing house, Almaty (ISBN 978-601-08-2549-9, p. 95).

The results of the research work are published in international scientific journals indexed in the SCOPUS and Web of Science databases, as well as in publications recommended by the Committee for Control in the Sphere of Education and Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Appendix A, in the dissertation work).

The results of studies of this hashing algorithm, obtained by foreign scientists, were included in the collection of works of the summer school-conference "Cryptography and Information Security", organized by the Novosibirsk State University and "Cryptographic Center" (Novosibirsk) on the topic "Investigation of the cryptographic properties of the new HBC and HAS01 hash functions."

The National Institute of Intellectual Property of the Ministry of Justice of the Republic of Kazakhstan issued 1 copyright certificate for proprietary research content and 3 copyright certificates for the HBC-256 hashing algorithm software (Appendix Ә in the dissertation work).

The main conclusion of the defense. Based on a block cipher, a new hashing algorithm has been developed, adapted to software and hardware implementation and parallel computing. The security and efficiency of the developed hashing algorithm are substantiated using sets of statistical tests, the avalanche effect criterion, the "close collisions" method, as well as the methods of differential, linear, and algebraic cryptanalysis.

Confidence level and results of approbation. The reliability of the conducted research and the results of the dissertation is shown in the third section of the dissertation. The results of the study are presented at the following scientific and practical conferences, as well as at scientific seminars of domestic and foreign research institutes and higher educational institutions (Appendix B in the dissertation work):

- V, VI, and VII International scientific-practical Conferences “Computer Science and Applied Mathematics” (Almaty, October 20-21, 2020-2022);
- International scientific-practical Conference “Actual problems of information security in Kazakhstan” (APISK-2021, Almaty, June 11, 2021);
- International scientific conference in the field of Information technologies dedicated to the 75th anniversary of Professor U. Tukeyev (Almaty, October 8, 2021);
- IV International Scientific and Technical Conference “Minsk Scientific Readings 2023. Advanced technologies and materials of the future” (Minsk, Belarus, December, 9-10, 2021);
- International Conference "Computer Data Analysis and Modeling: Stochastics & Data Science» (CDAM-2022, Minsk, Belarus, September, 6-9, 2022);
- Scientific seminar of the Faculty of Cybersecurity and Software Engineering of the National Aviation University (Kyiv, Ukraine, December 3, 2021);
- Scientific seminar of the "Research Institute for Applied Problems of Mathematics and Informatics" at Belarusian State University (Minsk, Belarus, September 6, 2022);
- Scientific seminar of the Electrical Engineering and Computer Science Department of Khalifa University (Abu Dhabi, UAE, December 13, 2022);

– Scientific seminars of the Institute of Information and Computational Technologies and the Faculty of Information Technology of al-Farabi KazNU (2020-2023, Almaty).

Connection of the topic of the dissertation with the plans of research works. The dissertation work was carried out under the doctoral dissertation plan approved by the Institute of Information and Computational Technologies of the RK MSHE CS and with the work plan of the PTF project OR11465439 "Development and study of hashing algorithms of arbitrary length for digital signatures and assessment of their strength". The results of this research work are included in the reports of this PTF project for 2021-2022 and an implementation certificate has been received (Appendix B in the dissertation).

The volume and structure of the work. The dissertation consists of an introduction, four sections, a conclusion, a list of references, and appendices. The total volume of the dissertation is 103 pages of written text including 30 figures, 28 tables, a bibliography from 99 sources, and 6 appendices.

Publication of results.

The main results of the research on the topic of the dissertation are presented in 24 publications including 7 in scientific journals recommended by the Committee for Quality Assurance in the Sphere of Education of the Ministry of Science and Higher Education of the Republic of Kazakhstan, 1 monograph, 7 in international scientific journals indexed in the Scopus and Web of Science databases, and 10 in collections of international and domestic scientific-practical conferences and other scientific journals.

The introduction provides a rationale for the relevance of the dissertation topic. It also formulates the purpose, object, and subject of the research work, as well as presents information on scientific novelty, practical significance, publications of works, and approbation of the results of the work.

The first section provides information about the basic concepts, terms, and varieties of hash functions. The requirements for hash functions are described and their main properties are highlighted. At the end of the section, criteria for assessing the quality of hash functions and classifying attacks on them are listed.

The second section describes the hashing algorithm HBC-256, which is based on a block cipher and satisfies all the requirements for hash functions. As a block cipher, a new encryption algorithm CF, designed on the SP network, is considered. This section details the cryptographic primitives and transformations used in the development of the CF encryption algorithm. In order to improve computational efficiency, a new scheme is presented that minimizes the number of rounds. To save chip memory, four 4-bit S-box replacement tables are used and the principle of their efficient use is shown.

The third section presents the results of the work carried out to assess the security of the developed hashing algorithm HBC-256. Estimates of the complexity of attacks on this algorithm and the level of statistical security of the algorithm based on sets of statistical tests by NIST and D. Knuth are given. The avalanche and strict avalanche effects are considered, which describe the relationship between the original message and the hash value. The possibilities of finding collisions by

methods of "close collisions," and differential, linear, and algebraic cryptanalysis are also evaluated.

The fourth section provides information about the software and hardware-software implementation of the developed hashing algorithm. The main characteristics of the HBC-256 algorithm by implementation types are given, their computational performance is evaluated, and comparative analysis data are presented relative to other hashing algorithms.

The conclusion reflects the results of the research work and gives a brief assessment of them.