Lublin, 13 April 2023

REVIEW

The foreign scientific adviser for the dissertation work of doctoral student **Sakan Kairat Sakanuly** on " Development of hashing algorithms based on iterative block ciphers and research of their cryptographic strength", presented for the degree of PhD in educational program "8D06301 - Information Security Systems

Cryptographic protection of information is one of the approaches to ensure information security, which includes the protection of confidentiality, integrity and availability of data using various cryptographic algorithms of encryption, hashing and digital signature. Robust cryptographic data protection involves not only the use of strong information security algorithms, but also the secure storage, transmission, integrity and validity control of data. Hashing is one of the important types of cryptographic transformation. The task of designing a quality hash function is more complex than that of designing a quality encryption algorithm.

Building hash functions based on block ciphers is one of the most popular and well-established design approaches. In this approach, the compression function is a block cipher with two inputs to which a message block and a key are fed. The advantage of using block ciphers to create hash functions is their high resistance to attack and the ability to use keys for additional security.

In the course of research work on the thesis topic, a new hashing algorithm HBC-256 based on the CF block cipher was developed by candidate. Algorithm HBC-256 provides an opportunity to choose different block lengths of 128 * k bits, where the value of k can vary from 3 to 8 depending on the amount of information to be hashed. A modified version of Merkle-Damgard's Wide-pipe design was used for iterative data processing, and a Davis-Meier scheme was used to ensure irreversibility. The applicant also proposed a symmetric CF block cipher algorithm used as a compression function in HBC-256. In the design of the CF algorithm, a new scheme has been used to improve security by providing a high degree of nonlinearity even with a small number of encryption rounds.

In this paper, much attention is paid to the security analysis of the developed hashing algorithm HBC-256 using cryptographic analysis techniques as well as NIST and D. Knuth statistical test suites. In addition, the degree of avalanche and strict avalanche effect is evaluated and a practical evaluation of "close collisions" search in hash values is made.

The results of statistical tests confirm the absence of defects in the sequences obtained with the hashing algorithm under consideration, and hence the high level of statistical safety of the algorithm under consideration.

The avalanche effect parameter, which is one of the most important properties in hash functions, corresponds to the required level of input bits dispersion.

Based on the security analysis of the HBC-256 algorithm, it is found that it has a high ability to resist the differential, linear, and algebraic types of cryptographic attacks, carried out to find collisions and first- and second-order prototypes.

Results of research work have scientific and practical value, which use promotes the decision of problems of protection of the information, having great value for maintenance of information safety of the country.

Sakan K.S. published 20 scientific papers on the topic of research, including 7 articles published in journals indexed in the database Scopus and Web of Science, including co-authorship with staff of the Laboratory of Information Security Institute of Information and Computer Technology, Ministry of Science and Higher Education of Kazakhstan.

A doctoral student in 2022 did research internship at Lublin University of Technology in Lublin, Poland. During the internship spoke at scientific seminars, including on the topic of his dissertation, as well as familiarized himself with the materials from the international database of the university library.

On the whole, the thesis is a completed research work, carried out on a high technical level. The results comply with the criteria established by the Regulations for the awarding of the academic degree of PhD in the educational program "8D06301 - Information Security Systems". Based on the above, I believe that the applicant **Sakan Kairat Sakanuly merits to be admitted to defend his thesis for the degree of Doctor of Philosophy** (PhD).

Foreign Scientific Advisor:
PhD DSc. Andrzej Smolarz,
Professor at Lublin University of Technology

POLITECHNIKA LUBELSKA
Katedra Elektroniki i Technik Informacyjnych
ul. Nadbystrzycka 38A, 20-618 Lublin
tel. 81 538 43 00, fax 81 538 43 12

Люблин, 13 апреля 2023 г.

ОТЗЫВ

зарубежного научного консультанта на диссертационную работу докторанта **Сакан Кайрат Саканулы** на тему «Разработка алгоритмов хеширования на основе итеративных блочных шифров и исследование их криптостойкости», представленную на соискание ученой степени PhD по образовательной программе «8D06301 – Системы информационной безопасности»

Криптографическая защита информации является одним из подходов обеспечения информационной безопасности, включающим в себя защиту конфиденциальности, целостности и доступности данных с использованием различных криптографических алгоритмов шифрования, хеширования и цифровой подписи. Надежная криптографическая защита данных включает в себя не только использование надежных алгоритмов защиты информации, но и безопасное хранение, передачу, контроль целостности и достоверности данных. Хеширование является одним из важных видов криптографического преобразования. Задача проектирования качественной хеш-функции более сложная, чем задача проектирования качественного алгоритма шифрования.

Построение хеш-функций на основе блочных шифров один из самых популярных и устоявшихся подходов проектирования. В этом подходе функция сжатия представляет собой блочный шифр с двумя входами, на которые подаются блок сообщения и ключ. Преимуществом использования блочных шифров для создания хеш-функций является их высокая стойкость к атакам и возможность использования ключей для дополнительной безопасности.

В ходе исследовательской работы по теме диссертации соискателем разработан новый алгоритм хеширования HBC-256 на основе блочного шифра CF. Алгоритм HBC-256 предоставляет возможность выбирать различную длину блока, составляющую $128*k$ бит, где значение k может меняться от 3 до 8 в зависимости от объема хешируемой информации. Для итеративной обработки данных использовалась модифицированная версия конструкции Меркла-Дамгарда – Wide-pipe, а для обеспечения необратимости – схема Девиса-Мейера. Соискателем также был предложен симметричный алгоритм блочного шифрования CF, применяемый в качестве функции сжатия в HBC-256. При проектировании алгоритма CF с целью повышения безопасности была использована новая схема, обеспечивающая высокую степень нелинейности даже при небольшом количестве раундов шифрования.

В работе большое внимание уделено проведению анализа безопасности разработанного алгоритма хеширования HBC-256 с применением методов криптографического анализа, а также наборов статистических тестов NIST и

Д. Кнута. Кроме того, оценена степень лавинного и строго лавинного эффекта и произведена практическая оценка поиска «близких коллизиий» в хеш-значениях.

Результаты статистических тестов подтверждают отсутствие дефектов в последовательностях, полученных с помощью рассматриваемого алгоритма хеширования, а следовательно и высокий уровень статистической безопасности рассматриваемого алгоритма.

Параметр лавинного эффекта, который является одним из важнейших свойств в хеш-функциях, соответствует требуемому уровню рассеивания входных битов.

По результатам анализа безопасности алгоритма HBC-256 установлено, что он обладает высокой способностью противостоять криптографическим атакам дифференциального, линейного и алгебраического типа, проведенным с целью нахождения коллизий и прообразов первого и второго рода.

Результаты исследовательской работы имеют научное и практическое значение, использование которых способствует решению задач по защите информации, имеющих большое значение для обеспечения информационной безопасности страны.

Сакан К.С. опубликовал 20 научных статей по теме исследования, из них 7 статей, опубликованных в журналах, индексируемых в базе данных Scopus и Web of Science, в том числе и в сооавторстве с сотрудниками Лаборатории информационной безопасности Института информационных и вычислительных технологий Министерства науки и высшего образования Республики Казахстан.

Докторант в 2022 году прошел научно-исследовательскую стажировку в Люблинском техническом университете в г. Люблин, Польша. В период прохождения стажировки выступал на научных семинарах, в том числе и по теме его диссертации, а также ознакомился с материалами из международной базы данных библиотеки университета.

В целом, диссертационная работа представляет собой завершенную исследовательскую работу, выполненную на высоком техническом уровне. Полученные результаты соответствуют критериям, установленном Положением о присуждении ученой степени PhD по образовательной программе «8D06301 – Системы информационной безопасности». На основаниях вышеизложенного считаю, что соискатель **Сакан К.С. заслуживает допуска к защите диссертации на соискание ученой степени доктора философии** (PhD).

Зарубежный научный консультант:
Д.т.н., профессор Люблинского
технического университета

Анджей Смолаж

POLITECHNIKA LUBELSKA
Katedra Elektroniki i Technik Informacyjnych
ul. Nadbystrzycka 38A, 20-618 Lublin
tel. 81 538 43 09, fax 81 538 43 12