UDC 004.8

Igor Boyarshin,
Oleksandr Markovskyi

METHOD OF HASH TRANSFORMATIONS CONSTRUCTION FOR STRICT USER IDENTIFICATION

Ігор Бояршин,
Олександр Марковський

МЕТОД ПОБУДОВИ ХЕШ-ПЕРЕТВОРЕНЬ ДЛЯ СТРОГОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ У СИСТЕМІ

The paper describes a new method of hash transformations construction for strict user identification. The key feature of this method is the utilization of a different algebraic basis, namely 41oolean functional transformers, which allows for a number of advantages compared to traditional approaches. The described method can generate for a given output key a range of unique input keys that satisfy the following rule: the given hash, once applied to such input key, yields the given output key.

Key words: cryptography, hash transformations, 41oolean functional transformers, strict identification.

Fig.: 1. Tabl.: 1. Bibl.: 5.

У статті описується новий метод побудови хеш-перетворень для строгої ідентифікації користувачів у системі. Особливістю методу є використання для його реалізації іншого алгебраїчного базису, а саме булевих функціональних перетворювачів, що дає ряд переваг у порівнянні з традиційними підходами. Метод дозволяє для заданого вихідного ключа згенерувати безліч унікальних вхідних ключів, що якщо до них застосувати задане хеш-перетворення, то буде отримано вихідний ключ.

Ключові слова: криптографія, хеш-перетворення, булеві функціональні перетворювачі, строга ідентифікація.

Рис.: 1. Табл.: 1. Бібл.: 5.

Target setting. With the rapid development of information technologies the demand for remote processing power and various services increased dramatically. As the majority of such systems is commercial, this requires for an efficient strict user identification algorithm to be developed. Such an algorithm must be both easy to use and provide sufficient security against attacks. The key question is thus to find a balance between the reliability of this algorithm and its ease of use.

Actual scientific researches and issues analysis. The analysis of known attacks on the identification systems showed that the most effective approach to withstand such attacks is to periodically re-identify the user in the system [1]. This implies that the method to be used for identification must have sufficient capabilities to provide enough sessions keys for the user to use when logging into the system [2].

Not investigated parts of the general subject. Although the matter of user identification in the system is not new, there have been few works addressing the usage of 42oolean functional transformations in it. The key advantage of such transformers is that they require much less computational power compared to other methods, and even more so with hardware implementation [3,4].

It is a known fact that 42oolean functional transformators are able to perform the computations in one third of the usual time. As a result, the choice of 42oolean functional transformations for the described task is obvious.

Research objective. The objective of this paper is to prove that the new method of hash transformations construction for strict user identification is viable and measure its performance, i.e. the amount of unique input keys x that the system can generate within the provided architecture for a given output key y [5].

As there are multiple ways to split the input vector into fragments, the resulting amount of generated vectors depends on it to some degree. That is why it is important to measure the performance for different splits of the key and find those that yield the most input keys.

Principal statements. The basic idea of the algorithm relies heavily on the underlying structure of the system, which is shown on Fig. 1 (for split of the key into 3 fragments). As can be seen from the figure, the system is comprised of multiple 42oolean functional transformers (each column corresponds to a single 42oolean functional transformer). An input key flows from top to bottom, layer by layer, resulting in an output key. The outputs of functional transformers are interconnected with each other by the means of XOR operator.

The essence of the algorithm is as follows: for a given output key y, keep filling the functional transformers with randomly-generated numbers from the bottom layer to the top layer, while meeting the rules of the underlying structure. Upon reaching the top layer a new input key is yielded. That concludes a single iteration I out of t total. Repeat the process until the 42oolean functional transformers become saturated. End by filling the remaining free slots of 42oolean functional transformers with randomly generated numbers.

If the algorithm is run for t iterations of the process, it results in t unique input keys x that all, once run through the system, yield the desired output key y. The proposed model structure provides sufficient non-linearity while keeping the overall performance of 42oolean functional transformators.

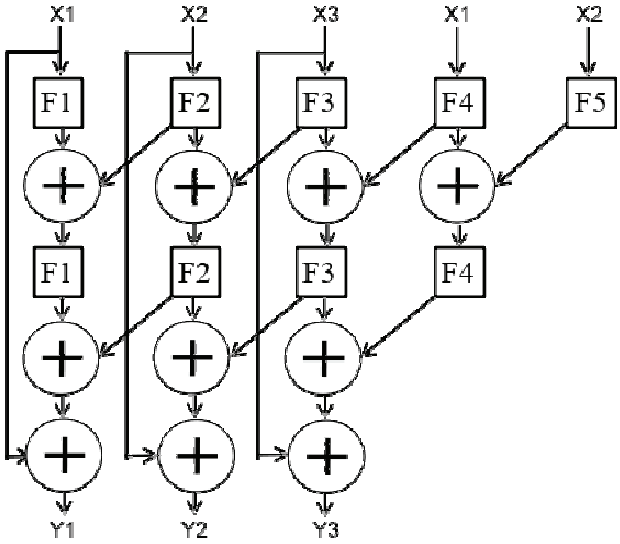

Fig. 1. The model structure for the split of key into 3 fragments

Testing. The purpose of testing is to find an approximate number of unique input keys *x* that the algorithm is able to generate for a given output key *y*. The testing was performed for different fragment size *k* and fragments amount *m*, so that *m*k=n*, where *n* is the size (bitness) of input and output keys. Table 1 gives the summary of the testing. As can be seen from the table, increasing the fragment size *k* by 1 results in doubled amount of generated keys.

Table 1

Amount of generated input keys for a given output key

Amount of fragments m	***Bitness of fragment k***			
	10	***11***	***12***	***13***
8	265	547	1102	2181
9	236	493	994	1988
10	221	452	909	1837
11	207	406	848	1702
12	193	379	789	1569

Conclusion. The study has proved that the new method based on 43oolean transformations is viable and can be used in user identification scenarios. It has been further shown that this method can generate sufficient number of unique input keys for a given output key. As the splitting of the key to be used inside the system can vary, a comprehensive testing was conducted to reveal dependencies between the amount of fragments and their bitness in regards to the amount of generated keys. The resulting performance of the method is a couple of magnitudes faster than that of other transformations based on a different underlying architecture, which confirms that the proposed solution can outperform existing solutions.

Future developments of the method could include experimenting with different system structures, as there are multiple ways functional transformers could be interconnected. Other variations of this structure could, for example, prove to be even more resilient to attacks or render even greater performance boost.

References

1. Широчин В. П., Мухин В. Е., Кулик А. В. Вопросы проектирования средств защиты информации в компьютерных системах и сетях. К.: 2000.- 111 с.

2. Захариудакис Лефтерис. Метод быстрой аутентификации удаленных пользователей на основе концепции “нулевых знаний” /Наукові записки Українського науково-дослідного інституту зв’язку. 2017.- № 1 (45).– С.109-117.

3. Захарченко Н. А., Топалова К. Н. Использование булевых преобразований для быстрой идентификации абонентов на основе концепции нулевых знаний. // Матеріали XII Міжнародної науково-технічної конференції ”Системний аналіз та інформаційні технології”.- К.:НТУУ ”КПІ”.-2010.- С.441.

4. Марковский А. П., Зюзя А. А., Шерстюк В. Д. Получение булевых преобразований специальных классов для построения эффективных алгоритмов защиты информации // Вісник Національного технічного університету України ”КПІ”. Інформатика, управління та обчислювальна техніка. К.,»ВЕК++»,- 2008.- № 49.- С.7-13.

5. Bardis N., Doukas N. Markovskyi O. A Method for strict remote user authentication using non-revesible Galois field transformations // Proceeding of IEEE Symposium on Computers and Communications. ISCC-2017. 3-6 July 2017. Heraclion, Crete, Greece. P.243-249.

Autors

Boyarshin Igor – student, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-Mail: igor.boyarshin@gmail.com

Бояршин Ігор Іванович – студент, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Markovskyi Oleksandr – associate professor, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: markovskyy@i.ua

Марковський Олександр Петрович – доцент, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

РОЗШИРЕНА АНОТАЦІЯ

І. І. Бояршин,
О. П. Марковський

МЕТОД ПОБУДОВИ ХЕШ-ПЕРЕТВОРЕНЬ ДЛЯ СТРОГОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ У СИСТЕМІ

Актуальність теми дослідження. З ростом популярності хмарних обчислень, що надають який-небудь сервіс або просто обчислювальні потужності, на передній план виходить проблема ідентифікації користувача у системі. Особливе місце серед можливих рішень посідає використання булевих нелінійних функціональних перетворень, що мають, по-перше, необхідну властивість незворотності, і по-друге, виконуються у декілька разів швидше за відомі аналоги. Ця робота присвячена опису нового методу побудови хеш-перетворень та його тестуванню.

Постановка проблеми. Завданням є надання такого методу ідентифікації користувача у системі, що був би водночас достатньо швидким, щоб система могла обробляти безліч користувачів за коротких проміжок часу, та з іншої сторони надавала можливість повторної ідентифікації користувача в цій системі для протистояння атакам.

Аналіз останніх досліджень і публікацій. Хоча проблема ідентифікації користувача в системі не є новою, використання в якості базису функціональних булевих перетворень є відносно новим. Основною перевагою такого базису у методах ідентифікації є швидкість їх роботи у порівнянні з іншими базисами, а також можливість зручної апаратної реалізації. Аналіз відомих атак на системи ідентифікації виявив, що найкращим способом протидії їм є повторна ідентифікація користувача в системі через деяких час.

Виділення недосліджених частин загальної проблеми. В цій статі описується новий метод побудови хеш-перетворень для строгої ідентифікації користувача в системі, що базується на булевих функціональних перетвореннях, а також тестування його роботи.

Постановка завдання. Для заданого вихідного ключа у необхідно згенерувати якомога більше унікальних вхідних ключів x, що якщо їх пропустити через систему (нелінійне булеве перетворення), то буде отримано заданий вихідний ключ y.

Викладення основного матеріалу. Побудована та проаналізована система, створена за описаним методом. Результати тестування показали, що побудована за цим методом система генерує достатньо велику кількість унікальних вхідних ключів користувача, а також виконується у декілька разів швидше за відомі аналоги на іншому алгебраїчному базисі.

Висновки. Новий метод строгої ідентифікації користувача в системі добре себе показує та дає задовільні результати з точки зору кількості згенерованих вхідних ключів та швидкості роботи. Таким чином, доведена можливість та доцільність його використання в системах ідентифікації користувачів.

Ключові слова: криптографія, хеш-перетворення, булеві функціональні перетворювачі, строга ідентифікація.