UDC 004.8

Anna Doroshenko,
Oleksandr Markovskyi

ACCELERATION OF BOOLEAN TRANSFORMATIONS NONLINEARITY TESTING FOR CRYPTOGRAPHIC ALGORITHMS

Анна Дорошенко,
Олександр Марковський

ПРИСКОРЕННЯ ТЕСТУВАННЯ НЕЛІНІЙНОСТІ БУЛЕВИХ ПЕРЕТВОРЕНЬ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

The method proposed in this article allows to significantly accelerate the testing of balanced 35oolean transformations nonlinearity by successive reconstruction of the nearest by Hamming distance linear function to a given nonlinear function. The results of experimental simulation, which prove the effectiveness of the proposed method, are presented.

Key words: Boolean transformations nonlinearity, linear cryptanalysis, cryptographic algorithms testing, cryptoresisting measuring.

Fig.: 1. Tabl. 0. Bibl.: 4.

Запропонований у статті метод дозволяє значно прискорити тестування нелінійності балансних булевих перетворень шляхом послідовного відновлення найближчої за відстанню Геммінга лінійної функції до заданої нелінійної функції. Наведено результати експериментального моделювання, що доводять ефективність запропонованого методу.

Ключові слова: нелінійність булевих перетворень, лінійний криптоаналіз, тестування криптографічних алгоритмів, вимірювання криптостійкості.

Рис.: 1. Табл. 0. Бібл.: 4.

Target setting. The automatic construction of cryptographic algorithms systems, the stages of which are the Boolean transformations generation and the determination of their cryptostability, are becoming increasingly popular in recent years. Cloud technologies make the large amount of information processing and complex calculations performing possible. Therefore, development of new cryptographic algorithms with increased cryptoresistance has become a current topic [1, 2].

Actual scientific researches and issues analysis. Currently only for the narrow class of Boolean functions there are nonlinearity evaluation methods which do not use a brute force. Thus, the problem of the nonlinearity evaluation has an

exponential complexity, depending on the number of variables n. Majority of existing methods designed for arbitrary Boolean functions achieved the acceleration of nonlinearity evaluation by either narrowing the problem or defining a nonlinearity with a predetermined error [3].

Not investigated parts of general subject. Existing methods do not take into account such features of Boolean transformations, which are used in cryptographic protection algorithms in practice, as balancedness. And as a result, these methods cannot meet the current requirements for testing cryptographic algorithms.

Research objective. The objective of this paper is to propose and investigate a new method that will allow to organise more effective cryptostability testing of data protection algorithms based on Boolean transformations by accelerating the nonlinearity determination.

Principal statements. Nonlinearity is the mandatory property of irreversible Boolean transformations [4]. Such Boolean transformation is represented by a system of nonlinear balanced Boolean functions $f_1(x_1,x_2,\ldots x_n)$, $f_2(x_1,x_2,\ldots x_n)$, … $f_k(x_1,x_2,\ldots x_n)$ from n variables, $\forall i \in \{1,2,...n\} : x_i \in \{0,1\}$. Testing the Boolean transformation nonlinearity consists in the nonlinearity evaluation of each of these nonlinear Boolean functions. Nonlinearity testing of Boolean function $f(x_1,x_2,\ldots x_n)$ is based on its Hamming distance $HD(f, g)$ to a linear function $g(x_1,x_2,\ldots x_n)$: $g(x_1, x_2,...x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n$, where $\forall j \in \{1,2,...n\} : a_j \in \{0,1\}$. The Hamming distance $HD(f, g)$ is determined by the number of input sets $x_1,x_2,\ldots x_n$ on which the function $f(x_1,x_2,\ldots x_n)$ and the linear function $g(x_1,x_2,\ldots x_n)$ take different values (Hamming weight of the functions exclusive disjunction), namely, the Hamming distance $HD(f, g)$ can be determined by the formula:

$$HD(f, g) = \sum (f(x_1, x_2,...x_n) \oplus g(x_1, x_2,...x_n)). \quad (1)$$

Balanced Boolean function $f(x_1,x_2,\ldots x_n)$ from n variables is a function whose weight is equal to:

$$HW(f) = 2^{n-1} \quad (2)$$

Linear Boolean function is a function that does not contain the product of variables in Zhegalkin polynomial form.

In turn, the nonlinearity $NL(f)$ of the Boolean function $f(x_1,x_2,\ldots x_n)$ is the minimal Hamming distance, namely, the Hamming distance to the nearest linear function. The nonlinearity $NL(f)$ can be determined by the formula:

$$NL(f) = \min HD(f, g). \quad (3)$$

To ensure the cryptoresistance of Boolean transformations against cracks using linear cryptanalysis, they must have the most possible nonlinearity.

General structure. The linear approximation constructing principle, which is basic for the proposed method, is the use of the probability p_i of changing the function value while the inverting of the i-th variable x_i of the Boolean function $f(x_1,x_2,\ldots x_n)$. The probability p_i can be determined by the formula:

$$p_i = \frac{1}{2^n} \cdot \sum_{X \in \Omega} f(X) \oplus f(X \oplus C_i), \quad (4)$$

where Ω is the set of all 2^n possible vectors X, $C_i=\{c_{i1},c_{i2},\ldots,c_{in}\}$ is an n-bit binary vector whose i-th component is equal to 1 and all others are 0: $\forall l \in \{1,..,i\text{-}1,i\text{+}1,\ldots,n\}$: $c_{il}=0$, $c_{ii}=1$.

Analysing the vector $P=\{p_1, p_2,..., p_n\}$ of probability values, which of the coefficients $a_1,a_2,\ldots,a_n$ in the linear equation will have the value of 1 can be assumed. In the process of analysis the values of the vector P in descending order in n steps, a set $\Theta_n(x_1, x_2,..., x_n)$ of all possible linear functions from $x_1,x_2,\ldots x_n$ which have the smallest Hamming distance to a given nonlinear Boolean function $f(x_1,x_2,\ldots x_n)$ is obtained.

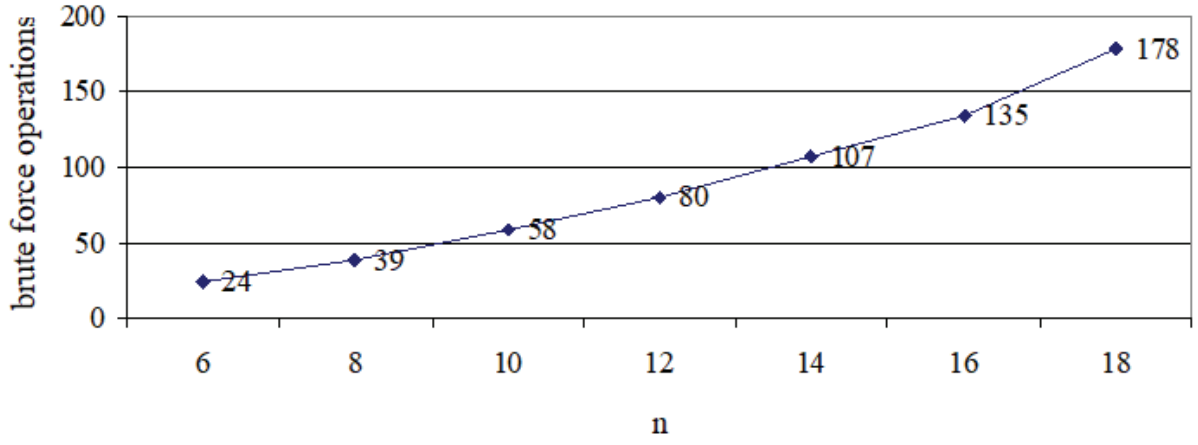
Testing. The purpose of experimental modelling was to analyse how the proposed method is effective in terms of the brute force operations number and how accurate the evaluated nonlinearity is.

In the experiments nonlinear Boolean functions with different number of variables have been tested. The graphs of the results are shown in Fig. 1 a) and b).

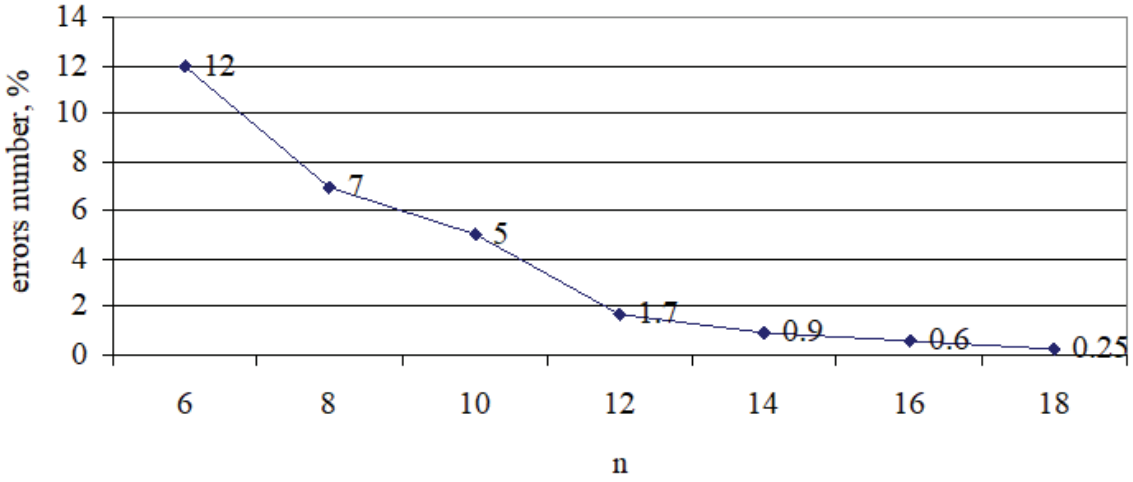
Received results illustrate that the proposed method, for example, for functions from 14 variables allows to accelerate computation approximately by $\frac{2^{14}}{107} \approx 153$ times.

Such an acceleration is achieved by the admissibility of the error in the nonlinearity evaluation.

As can be seen from Fig. 1 b), the proposed method extremely efficient for functions from a large number of variables, which is an advantage, since such functions are used in practice.



a)



b)

Fig. 1. The dependencies of a) the brute force operations number to evaluate the nonlinearity and b) the error magnitude from the variables number

Conclusion. The conducted experimental and theoretical studies have shown the effectiveness of the proposed method in testing modern algorithms of cryptographic data protection, functional basis of which is Boolean transformations.

To accelerate the construction of linear approximation, probabilities of changing the function values while the inverting of a particular variable of the Boolean function $f(x_1,x_2,\ldots x_n)$ are used, which is a peculiarity of the proposed method.

Application of the proposed method allows to provide better reliability and testing speed of wide class cryptographic algorithms.

References

5. Давиденко А.Н. Вероятностная оценка надежности реализации функций защиты информации // Моделювання та інформаційні технології: Зб.наук. праць.-Львів:НВМ ПТ УАТ.-2002.-Вип.14.-С.64-70.

6. Марковський О.П. Комбиаторный анализ булевых функций специальных классов для систем криптографической защиты информации // А.П. Марковский, Э.Р. Искаков, Г.В. Гарасимович // Збірник доповідей міжнародної науково-технічної конференції “The International Conference on Security, Fault Tolerance, Intelligence” (ICSFTI2018). – Київ, 10-11 травня 2018. – С.42-50.

7. Mesnager S. Bent Function: Fundamentals and Results / S. Mesnager // IEEE Trans. On Information Theory.-2016.- Vol.62, No. 7, , pp. 1825-1834.

8. Xiang C. A construction of linear codes from Boolean functions / C. Xiang, K.Feng, C.Taug // IEEE Trans. Inform.Theory, 2017.-Vol.63, № 1. – P. 167-176.

Autors

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

E-mail: annadoroshenko03@gmail.com

Дорошенко Анна Юріївна – студентка, 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

А. Ю. Дорошенко,
О. П. Марковський

ПРИСКОРЕННЯ ТЕСТУВАННЯ НЕЛІНІЙНОСТІ БУЛЕВИХ ПЕРЕТВОРЕНЬ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Актуальність теми дослідження. З появою хмарних технологій з’явилася можливість обробляти великий об’єм інформації та виконувати складні обчислення. Проте окрім очевидних переваг цих технологій існує вагомий недолік, пов’язаний із сумнівною безпекою даних та імовірністю їх пошкодження, викрадення або навіть знищення. Тому актуальним є розробка нових криптографічних алгоритмів з підвищеною криптостійкістю.

Постановка проблеми. Наразі існує тенденція збільшення кількості змінних булевих перетворень, які лежать в основі значної частини криптографічних алгоритмів. У зв’язку з цим постає проблема зростання часу та необхідних об’ємів ресурсів для тестування цих алгоритмів. Тому виникає нагальна потреба прискорення оцінювання криптостійкості алгоритмів захисту даних.

Аналіз останніх досліджень і публікацій. У більшості існуючих методів прискорення визначення нелінійності булевих перетворень досягається шляхом

звуженням поставленої задачі або визначенням нелінійності з наперед заданою похибкою.

Виділення недосліджених частин загальної проблеми. Існуючі методи не враховують такої особливості булевих перетворень, які використовуються в алгоритмах криптографічного захисту на практиці, як балансність. І як результат, ці методи не можуть задовольнити сучасні вимоги тестування криптографічних алгоритмів.

Постановка завдання. Завданням є запропонувати та дослідити метод, який дасть змогу більш ефективно проводити тестування криптостійкості алгоритмів захисту інформації, що мають за основу булеві перетворення, шляхом прискорення визначення їх нелінійності.

Викладення основного матеріалу. Проаналізовано недоліки існуючих методів визначення нелінійності. В основу запропонованого методу покладено концепції динамічного програмування, які дозволяють послідовно реконструювати лінійну апроксимацію за показниками імовірностей зміни значення заданої нелінійної булевої функції при інвертуванні конкретної змінної. Експериментальне моделювання показало високу ефективність запропонованого методу.

Висновки. Розроблено, теоретично обґрунтовано та досліджено метод підвищення ефективності тестування криптографічних алгоритмів шляхом пришвидшення визначення нелінійності булевих перетворень, які є основою цих алгоритмів. Наведено результати експериментального моделювання.

Ключові слова: нелінійність булевих перетворень, лінійний криптоаналіз, тестування криптографічних алгоритмів, вимірювання криптостійкості.