UDC 004.056.55 DOI https://doi.org/10.35546/kntu2078-4481.2025.4.3.24

V. I. RUZHENTSEV
Doctor of Technical Sciences, Associate Professor,
Professor at the Department of Secure Information Technologies
Kharkiv National University of Radioelectronics
ORCID: 0000-0002-1007-6530

ANALYSIS OF CRYPTOGRAPHIC RESISTANCE OF ITERATIVE ALGORITHMS BASED ON CONSIDERATION OF ITERATIVE DIFFERENTIAL CHARACTERISTICS

The experiments on searching for the best (with maximum probability) differential characteristics (DC) for the well-known DES algorithm is performed. It was demonstrated for the DES algorithm that in the best DCs with a large number of rounds (more than 10), about 70% of the rounds are covered by the iterative DC. Based on these facts, an improved method for estimating the probability of the best DCs for the DES algorithm was proposed. Estimation was performed using various methods. It was assumed that for other iterative algorithms in the best multi-round DCs a significant percentage of rounds will also be covered by iterative DCs.

A review of the existing results of estimating the differential properties of the Ascon algorithm (NIST SP 800-232 standard) was made.

Information about the minimum number of active substitutions is known: for 2 rounds, the minimum number is at least 4, for 3 rounds – at least 15.

The results of the search for DHs for the p-transformation of the Ascon algorithm for 5 or more rounds are also known: no DH with the number of active S-blocks less than 64 was found. It is also noted that the search was carried out by selecting a small number of active S-blocks in the middle rounds, and then moving to the initial and final rounds, where, of course, the number of active S-boxes will grow rapidly. It is clear that such an approach and the resulting estimate cannot be considered accurate and final.

In our opinion, a smaller total number of active S-boxes can be obtained by preliminary searching for iterative DHs and their subsequent use.

The possibility of performing a search for the best DHs for Ascon algorithm based on consideration of iterative differential characteristics is discussed. An algorithm for searching for iterative differential characteristics for modern ciphers is proposed.

Key words: *Symmetric ciphers, Differential cryptanalysis, Differential characteristic, Iterative differential characteristic, DES, Ascon.*

В. І. РУЖЕНЦЕВ
доктор технічних наук, доцент,
професор кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-1007-6530

АНАЛІЗ КРІПТОГРАФІЧНОЇ СТІЙКОСТІ ІТЕРАТИВНИХ АЛГОРИТМІВ, ОСНОВАНИЙ НА РОЗГЛЯДІ ІТЕРАТИВНИХ ДИФЕРЕНЦІАЛЬНИХ ХАРАКТЕРИСТИК

Проведено експерименти з пошуку найкращих (з максимальною ймовірністю) диференціальних характеристик (ДХ) для відомого алгоритму DES. Представлено аналіз структури цих ДХ з метою визначення загальних принципів побудови таких ДХ для інших, більш сучасних алгоритмів. Для алгоритму DES продемонстровано, що у найкращих ДХ при великій кількості циклів (більше 10), близько 70 % відсотків циклів закриває саме ітеративна ДХ. На основі цих даних запропоновано вдосконалений метод оцінювання ймовірності найкращих ДХ для алгоритму DES та виконане порівняння оцінок, які надають інші методи. Зроблено припущення, що для інших ітеративних алгоритмів у кращих багатоциклових ДХ значний відсоток циклів теж буде накриватися ітеративними ДХ.

Зроблено огляд існуючих результатів оцінювання диференційних властивостей алгоритму Ascon (стандарт NIST SP 800-232).

Відома інформація про мінімальну кількість активних підстановок: для 2 раундів мінімальна кількість не менше 4, для 3 раундів – не менше 15.

Також відомі результати пошуку ДХ для p-перетворення алгоритму Ascon для 5 або більше раундів: не було знайдено жодної ДХ з кількістю активних S-блоків менше 64. Також зазначається, що пошук здійснювався шляхом вибору невеликої кількості активних S-блоків у середніх раундах, а потім переходу до початкового та фінального раундів, де, звичайно, кількість активних S-боксів швидко зростатиме. Зрозуміло, що такий підхід та отриману оцінку не можна вважати точними та остаточними.

На нашу думку, меншу загальну кількість активних S-боксів можна отримати шляхом попереднього пошуку ІДХ та їх подальшого використання.

Обговорюється можливість виконання пошуку найкращих ДХ для цього алгоритму на основі розгляду ітераційних диференціальних характеристик. Запропоновано алгоритм пошуку ітераційних диференціальних характеристик для сучасних шифрів.

Ключові слова: *Симетричні шифри, диференціальний криптоаналіз, диференціальна характеристика, ітеративна диференціальна характеристика, DES, Ascon.*

Introduction

The symmetric cryptography is the main tool for ensuring cybersecurity. The evolution of symmetric cryptology, like the evolution of many other areas of science, partially occurs in a spiral. Those algorithms that were considered obsolete and out of use 10 years ago can today be attributed to an actively developing area of symmetric cryptography – lightweight cryptography. Such algorithms include DSTU GOST 28147 – 2009, DES, TEA, IDEA, etc. The attention paid to these algorithms is confirmed by the fact that lightweight versions of these algorithms are appearing: for example, for the DES algorithm [1] – the DESL [2] and DESXL [3] algorithms, for the TEA algorithm – the XTEA [4] and XXTEA [5] algorithms.

More modern lightweight algorithms, as a rule, are used larger block size and key, however, main principles and ideas related to the analysis of cryptanalytic properties for long-known algorithms are also applicable to more modern ones. The above said is fully applies to one of the most powerful and universal cryptanalytic attacks – differential cryptanalysis. And for the analysis of resistance to this attack it is usually necessary to estimate the upper bound of the (r-1)-round differential characteristic (DC) for the r-round cipher`s transformation. The existence of DC with high probability leads to effective differential attack [6].

Statement of the problem

Assessing the strength of iterative crypto-transformations with a large block (for example, the Ascon algorithm with block size 320 bits) to differential attacks.

Known research and publications analysis. Results of differential characteristic search for algorithm Ascon

The process of finding the best DCs is problematic for modern lightweight cryptographic algorithms with a block size significantly larger than 64 bits.

In [15] were presented information about the minimum number of active substitutions: for 2 rounds minimum number is not less than 4, for 3 rounds – not less than 15.

Known results of DC search for the p transformation of the Ascon algorithm are presented in [13]. It is said that for 5 or more rounds, no DC with a number of active S-boxes less than 64 was found. It is also said that the search was carried out by selecting a small number of active S-boxes in the middle rounds and then moving to the initial and final rounds, where, of course, the number of active S-boxes will increase rapidly. It is clear that such an approach and the obtained assessment cannot be considered as accurate and final.

In our opinion, a smaller total number of active S-boxes can be obtained by preliminary search for iterative DC and their subsequent use.

The aim of work

The aim of this work is to perform and discuss experiments on searching for the best (having the maximum probability) differential characteristics (DC) for the well-known DES algorithm, as well as to analyze the structure of these DCs to identify general principles for constructing such DCs for other, more modern algorithms [7] including the relatively new lightweight standardized Ascon algorithm [13,14].

Methods for searching for DCs with maximum probability

Method of Matsui

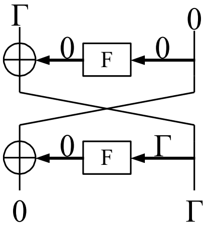
In the work [8] M. Matsui proposed an algorithm for searching for multi-round differential characteristics with maximum probabilities for DES-like ciphers. The method is based on the fastest possible sifting out of DCs that cannot be better than the best known DCs for a given number of transformation rounds.

This method is applicable to ciphers with a small block size (not more than 64 bits), for example, DES, FEAL, and requires significant computing resources. For ciphers with a large block size, this algorithm will require too much computational resources that are unrealistic in practice.

Method of Knudsen

One of the methods for finding multi-round differential characteristics with high probabilities was proposed by L. R. Knudsen in [9] and is based on the consideration of iterative differential characteristics (IDC). The method requires significantly fewer computing resources than Matsui method, since it operates more selectively. To assess the security of the DES [1] and s2-DES [10] ciphers, Knudsen considered several types of IDC (see Fig. 1) and then construct multi-round DC from these IDCs.

$(\Gamma,0)$
$0 \leftarrow 0$
$0 \leftarrow \Gamma$
$(0,\Gamma)$



a)

$(\Gamma, 0)$
$0 \leftarrow 0$
$\Phi \leftarrow \Gamma$
$\Gamma \leftarrow \Phi$
$0 \leftarrow 0$
$\Gamma \leftarrow \Phi$
$\Phi \leftarrow \Gamma$
$(0, \Gamma)$

b)

$(\mathrm{P}, 0)$
$0 \leftarrow 0$
$\Phi \leftarrow \mathrm{P}$
$\Gamma \leftarrow \Phi$
$\Phi \leftarrow \mathrm{P}\oplus\Gamma$
$0 \leftarrow 0$
$\Phi \leftarrow \mathrm{P}\oplus\Gamma$
$\Gamma \leftarrow \Phi$
$\Phi \leftarrow \mathrm{P}$
$(0, \mathrm{P})$

c)

Fig. 1. Types of IDCs from Knudsen's method

In this figure and further, the IDCs are presented in the notation of the work [9], for the first type of IDC in Fig. 1, a) an explanatory scheme for the Feistel chain is also given. In the works [11-12], an extended set of IDCs was presented (Fig. 2).

1
$0_x \leftarrow \Gamma$
$0_x \leftarrow 0_x$
2-round iterative characteristic

2
$\Phi \leftarrow \Gamma$
$0_x \leftarrow \Phi$
$\Phi \leftarrow \Gamma$
$0_x \leftarrow 0_x$
4-round iterative characteristic

3
$\Phi \leftarrow \Gamma$
$\Gamma\oplus\Psi \leftarrow \Theta$
$\Phi \leftarrow \Psi$
$\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$
4-round iterative characteristic

4
$\Phi \leftarrow \Gamma$
$\Gamma \leftarrow \Phi$
$0_x \leftarrow 0_x$
$\Gamma \leftarrow \Phi$
$\Phi \leftarrow \Gamma$
$0_x \leftarrow 0_x$
6-round iterative characteristic

5
$\Phi \leftarrow \Gamma$
$\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$
$\Theta \leftarrow \Psi$
$\Gamma \leftarrow \Phi$
$\Phi\oplus\Theta \leftarrow \Gamma\oplus\Psi$
$\Psi \leftarrow \Theta$
6-round iterative characteristic

6
$\Phi \leftarrow \Gamma$
$\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$
$\Theta \leftarrow \Psi$
$\Gamma\oplus\Psi \leftarrow \Phi$
$\Theta \leftarrow \Gamma$
$\Psi \leftarrow \Phi\oplus\Theta$
$\Phi \leftarrow \Gamma\oplus\Psi$
$\Psi \leftarrow \Theta$
8-round iterative characteristic

7
$\Phi \leftarrow \Gamma$
$\Psi \leftarrow \Phi$
$\Phi \leftarrow \Gamma\oplus\Psi$
$0_x \leftarrow 0_x$
$\Phi \leftarrow \Gamma\oplus\Psi$
$\Psi \leftarrow \Phi$
$\Phi \leftarrow \Gamma$
$0_x \leftarrow 0_x$
8-round iterative characteristic

8
$\Phi \leftarrow \Gamma$
$\Psi \leftarrow \Phi$
$\Theta \leftarrow \Gamma\oplus\Psi$
$\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$
$0_x \leftarrow 0_x$
$\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$
$\Theta \leftarrow \Gamma\oplus\Psi$
$\Psi \leftarrow \Phi$
$\Phi \leftarrow \Gamma$
$0_x \leftarrow 0_x$
10-round iterative characteristic

9
$\Phi \leftarrow \Gamma$
$\Psi \leftarrow \Phi\oplus\Theta$
$\Theta \leftarrow \Gamma\oplus\Psi$
$\Gamma \leftarrow \Phi$
$\Phi\oplus\Theta \leftarrow \Psi$
$\Gamma\oplus\Psi \leftarrow \Theta$
$\Phi \leftarrow \Gamma$
$\Psi \leftarrow \Phi\oplus\Theta$
$\Phi \leftarrow \Gamma\oplus\Psi$
$\Psi \leftarrow \Theta$

10-round iterative characteristic

Fig. 2. Extended set of iterative differential characteristics

Iterative characteristics differ in the number of groups of active substitutions, between which transitions occur in the process of performed transformations.

By going through various values of Г, Ф, Р for the schemes in Fig. 1, Knudsen found IDCs of various types. Repeating the found IDC the required number of times, he covered the number of rounds necessary for organizing an attack, as shown in scheme a) in Fig. 3.

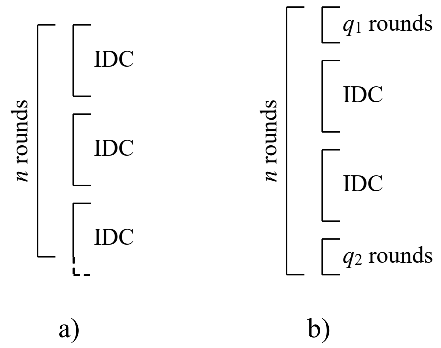


Fig. 3. Schemes of using IDCs in building best DCs

Proposed modified method

However, our computational experiments on finding the best DC for Feistel-like ciphers indicate that the general form of the best multi-round DC can be represented as in Fig. 3, b). Due to this discrepancy with scheme in Fig. 3, a), the probability of a multi-round DC obtained using the Knudsen method will be lower than the actual value, i.e. the cipher may be more vulnerable to differential cryptanalysis than would be expected after using the Knudsen method.

Thus, one of the main drawbacks of the Knudsen method is possible underestimation of the DC probabilities. In addition, the types of IDC considered by Knudsen (Fig. 1) are far from exhausting the entire set of IDC. Additional types of IDH were considered in the works [11-12] and presented on Fig. 2.

Computational experiments to find the best DC using the algorithm proposed by Matsui [8] was performed for a number of DES-like ciphers that differ in substitution tables: the original DES [1], s3DES [10], s5DES, DES variants with substitution tables constructed in accordance with additional requirements [11,12]. The best multi-round (up to 16 rounds) DCs were found. The design features of the best multi-round DCs for some DES-like ciphers are presented in Table 1.

The column "IDC type" indicates the type of IDC and the number of rounds that the extended IDC of this type covers in the best DC. Based on the analysis of these data, as well as similar indicators for other considered ciphers, the following statement can be formulated:

Statement 1. For a DES-like cipher, in the best *n*-round DC (*n*>10), at least *n*–6 rounds are covered by a multiple-extended IDC.

Unfortunately, it was not possible to prove statement 1 theoretically at this stage, therefore the validity of the presented statement is confirmed by the results of computational experiments on constructing multi-round DC for DES-like ciphers (in total, about seven variants of DES-like ciphers were considered). The presented statement allows us to propose a method for estimating the maximum probability of DC.

Method for estimating the maximum probability of an n-round (n> 10) DC of a Feistel-like cipher:

1) using the Matsui algorithm or in some other way, the maximum probability of a 6-round DC is determined;

2) using the modified Knudsen method with an increased set of considered types of IDC, the maximum probability of an (n-6)-round DC is determined;

3) the maximum probability of an n-round DC is calculated as the product of the values obtained in the first two steps.

According to Statement 1, the probability of DC found using the given method will not be lower than the actual value, therefore, the proposed method can be used to check the practical criterion for the resistance of ciphers of the considered type to differential cryptanalysis.

We believe that the general structure of the best DCs will correspond to the scheme in Fig. 3,b) for many other iterative ciphers with a sufficiently large number of rounds. Then, to estimate the maximum probability of a DC, we need to find the IDC and determine the number of rounds that the IDC will cover.

Results of using modified method for DES-like ciphers

The results of considered methods using for DES-like ciphers is presented in Table 2.

First of all, practical feasibility is important. Next, it is bad when the probability of DC is underestimated, since the real algorithm will be more vulnerable to attack than the results of analysis show (Knudsen's method in the table 2). It is also bad when the probability of DC is greatly overestimated (standard method in table 2). In this case, the algorithm may be too slow due to the using of larger number of rounds than it is needed.

Table 1

The design features of the best multi-round DCs for some DES-like ciphers

Cipher	Number of rounds	IDC type (number of rounds covered by IDC)	Probability with using Matsui's method (exact value)	Probability with using Knudsen's method	Probability with using classical method	Probability with using our method
DES	7	2-rounds (7)	$2^{-23,6}$	$2^{-23,6}$		
	8	2-rounds (8)	$2^{-30,48}$	$2^{-31,48}$	$2^{-11,74}$	
	9	2-rounds (9)	$2^{-31,48}$	$2^{-31,48}$		
	10	2-rounds (10)	$2^{-38,35}$	$2^{-39,35}$		$2^{-35,71}$
	11	2-rounds (11)	$2^{-39,35}$	$2^{-39,35}$		$2^{-35,71}$
	12	2-rounds (12)	$2^{-46,22}$	$2^{-47,22}$	$2^{-18,46}$	$2^{-43,58}$
	13	2-rounds (13)	$2^{-47,22}$	$2^{-47,22}$		$2^{-43,58}$
	14	2-rounds (14)	$2^{-55,1}$	$2^{-55,1}$		$2^{-51,45}$
	15	2-rounds (15)	$2^{-56,1}$	$2^{-55,1}$		$2^{-51,45}$
	16	2-rounds (16)	$2^{-61,97}$	$2^{-62,97}$	$2^{-23,5}$	$2^{-59,32}$
S3DES	7		$2^{-26,03}$	$2^{-34,48}$		
	8		$2^{-35,22}$	$2^{-42,9}$	$2^{-11,74}$	
	9	6-rounds (9)	$2^{-41,07}$	$2^{-42,9}$		
	10	6-rounds (10)	$2^{-45,42}$	$2^{-50,93}$		$2^{-40,97}$
	11	6-rounds (10)	$2^{-47,84}$	$2^{-55,93}$		$2^{-40,97}$
	12	6-rounds (10)	$2^{-53,1}$	$2^{-64,35}$	$2^{-18,46}$	$2^{-49,00}$
	13	6-rounds (10)	$2^{-55,52}$	$2^{-64,35}$		2^{-54}
	14	6-rounds (10)	$2^{-64,61}$	$2^{-72,38}$		$2^{-62,4}$
	15	6-rounds (11)	$2^{-69,85}$	$2^{-77,38}$		$2^{-62,4}$
	16	4-rounds (14)	$2^{-78,03}$	$2^{-85,8}$	$2^{-23,5}$	$2^{-70,45}$
S5DES	7	8-rounds (5)	$2^{-27,15}$	$2^{-28,52}$		
	8		$2^{-35,62}$	$2^{-38,56}$	$2^{-11,74}$	
	9	8-rounds (9)	$2^{-38,56}$	$2^{-38,56}$		
	10	8-rounds (9)	$2^{-43,24}$	$2^{-43,56}$		$2^{-40,05}$
	11	8-rounds (9)	$2^{-46,43}$	$2^{-47,81}$		$2^{-40,05}$
	12	8-rounds (9)	$2^{-51,11}$	$2^{-57,84}$	$2^{-18,46}$	$2^{-45,05}$
	13	8-rounds (9)	$2^{-54,3}$	$2^{-57,84}$		$2^{-49,3}$
	14	8-rounds (13)	$2^{-62,52}$	$2^{-62,84}$		$2^{-59,33}$
	15	8-rounds (13)	$2^{-65,71}$	$2^{-67,09}$		$2^{-59,33}$
	16	8-rounds (13)	$2^{-75,42}$	$2^{-77,12}$	$2^{-23,5}$	$2^{-68,58}$

Table 2

The results of considered methods using for DES-like ciphers

	Standard classical method	Knudsen's method	Proposed method	Matsui's method
Working time (computational complexity)	—	15 minutes	25 minutes	4-5 days
The maximum deviation of the result from the exact value	Overestimation by $2^{54,53}$ times (deviation increases with increasing number of rounds)	Underestimation by $2^{11,25}$ times	Overestimation by $2^{7,58}$ times	Exact value

It can be seen that the proposed method makes it possible to obtain a sufficiently accurate value with low computational complexity. Therefore, we believe that this method will also be useful in the analysis of more modern algorithms.

Algorithm for Iterative differential characteristics search for Ascon

According to the results presented in sections 5, 6, in our opinion, the refinement of the known results of the resistance of the Ascon algorithm to differential attacks (presented in section 3) can be connected with the analysis of iterative DCs.

For organizing the IDC search, at the first stage it is needed to identify two or more groups of S-boxes that can be alternately activated in accordance with the linear dispersion transformations used in the cipher. In this case, the search will consist of performing the following steps:

a) building of difference distribution tables for the S-substitutions of the algorithm;

b) all possible variants of the number of groups g and the number of active S-boxes in each of the groups are considered: m_1, m_2, ..., m_g;

c) for each variant of the numbers m_1, m_2, ..., m_g all possible combinations of S-boxes are considered. If such groups of S-boxes are found for which cyclic movement is possible: from group m_1 of active S-boxes to group m_2, from group m_2 of active S-boxes to group m_3, etc. until the transition from group m_g of active S-boxes to group m_1, then proceed to the next step d;

d) all possible values of differences are analyzed within the selected groups of active S-boxes;

e) for each variant, in accordance with the differential difference tables, the possibility of transitions between different groups is checked; if there is such possibility, then an iterative characteristic found.

The presented algorithm will be difficult to implement for a large number of groups and a large number of active S-boxes in groups, but for limited variants (2-4 groups of 2-5 S-boxes in each groups), computational experiments are planned for the Ascon algorithm.

Conclusions

1 Evaluation of resistance to Differential Cryptanalysis based on consideration of IDC (iterative differential characteristics) allows to obtain a more accurate estimation of resistance than the Knudsen method [9] with significantly fewer computational costs than the Matsui method [8].

2 Using the example of the DES algorithm, it was demonstrated that the best differential characteristics with a sufficiently large number of rounds contain most of the rounds that are covered by the iterative differential characteristic (according to the results of experiments for DES with 10 or more rounds, the iterative differential characteristic covers at least 70% of the rounds). We believe that the such structure of the best DCs will correspond and for many other iterative ciphers with a sufficiently large number of rounds.

3 The main steps of the algorithm for searching for iterative differential characteristics for iterative symmetric cryptographic algorithms were developed. It is planned to implement this algorithm for the Ascon cipher [13, 14].

Bibliography

1. Data encryption standard. Federal Information Processing Standards Publication 46, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977 (revised as FIPS 46-1:1988; FIPS 46-2:1993).

2. A. Poschmann, G. Leander, K. Schramm, and C. Paar. New light-weight crypto algorithms for RFID, Proceedings in 2007 IEEE International Symposium on Circuits and Systems. IEEE, 2007, pp. 1843–1846. https://doi.org/10.1109/ISCAS.2007.378273

3. P. K. Kushwaha, M. Singh, and P. Kumar. A survey on lightweight block ciphers. *International Journal of Computer Applications*, vol. 96, no. 17, 2014. https://doi.org/10.1109/MDT.2007.178.

4. J.-P. Kaps. Chai-tea, cryptographic hardware implementations of XTEA. International Conference on Cryptology in India. Springer, 2008, pp. 363–375. https://doi.org/10.1007/978-3-540-89754-5_28

5. E. Yarrkov. Cryptanalysis of XXTEA [Electronic resource]. IACR Cryptology ePrint Archive, Report 2010/254, 2010. http:// https://eprint.iacr.org/2010/254.pdf.

6. Biham, E., Shamir, A. Differential Cryptanalysis of the Full 16-Round DES. In: Differential Cryptanalysis of the Data Encryption Standard. Springer, New York, NY. https://doi.org/10.1007/978-1-4613-9314-6_5

7. Lightweight cryptography project of the American National Institute of Standards and Technology [Electronic resource], 2015. https://csrc.nist.gov/projects/ lightweight-cryptography.

8. Matsui, M. On correlation between the order of S-boxes and the strength of DES. In: EUROCRYPT 1994, Perugia, Italy, 9-12 May. pp. 366–375. Springer, Heidelberg. https://dx.doi.org/10.1007/BFb0053451

9. L. Knudsen. Iterative characteristics of DES and s2-DES. Advances in Cryptology – Crypto'92. Springer Verlag, LNCS 746, pp. 497-511, Berlin Heidelberg 1993. https://dx.doi.org/10.1007/3-540-48071-4_35

10. K. Kim. Construction of DES-like S-boxes Based on Boolean Function Satisfying the SAK. Proceedings Of Asiacrypt'91, pp. 59-72, Fujiyoshida, Japan, 1991. https://dx.doi.org/10.1007/3-540-57332-1_5

11. В. І. Долгов, І. В. Лисицька, В. І. Руженцев. Забезпечення стійкости шифра DES до атак диференціального криптоаналіза. Перекриття характеристик обнуляючого типа и чотирициклових ітеративних характеристик. *Радіотехника* : Всеукр. межвід. наук.–техн. зб. 2001. Вип. 120. С. 192–198.

12. В.І. Долгов, І. В. Лисицька, В. І. Руженцев. Забезпечення стійкости шифра DES до атак диференціального криптоаналіза перекриття шести-, восьми- і десятициклових ітеративних характеристик. *Радіотехніка* : Всеукр. межвід. наук.–техн. зб. 2002. Вип. 124. С. 182–189.

13. Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2. [Electronic resource] Submission to NIST, 2019. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ascon-spec-round2.pdf.

14. Ascon-Based Lightweight Cryptography Standards for Constrained Devices. Authenticated Encryption, Hash, and Extendable Output Functions [Electronic resource]. National Institute of Standards and Technology, 2025 (NIST Special Publication 800 NIST SP 800-232). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-232.pdf

15. Christoph Dobraunig, Maria Eichlseder, Florian Mendel and Martin Schlaffer. Cryptanalysis of Ascon [Electronic resource]. Cryptology ePrint Archive, Report 2015/030, 2015. https://eprint.iacr.org/2015/030.pdf.

References

1. Data encryption standard (1988). Federal Information Processing Standards Publication 46, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977 (revised as FIPS 46-1:1988; FIPS 46-2:1993).

2. A. Poschmann, G. Leander, K. Schramm, and C. Paar (2007). New light-weight crypto algorithms for RFID, Proceedings in 2007 IEEE International Symposium on Circuits and Systems. IEEE, 2007, pp. 1843–1846. https://doi.org/10.1109/ISCAS.2007.378273

3. P. K. Kushwaha, M. Singh, and P. Kumar (2014). A survey on lightweight block ciphers. International Journal of Computer Applications, vol. 96, no. 17, 2014. https://doi.org/10.1109/MDT.2007.178.

4. J.-P. Kaps (2008). Chai-tea, cryptographic hardware implementations of XTEA. International Conference on Cryptology in India. Springer, 2008, pp. 363–375. https://doi.org/10.1007/978-3-540-89754-5_28

5. E. Yarrkov (2010). Cryptanalysis of XXTEA. IACR Cryptology ePrint Archive, Report 2010/254, 2010. http://https://eprint.iacr.org/2010/254.pdf.

6. Biham, E., Shamir, A. (1993). Differential Cryptanalysis of the Full 16-Round DES. In: Differential Cryptanalysis of the Data Encryption Standard. Springer, New York, NY. https://doi.org/10.1007/978-1-4613-9314-6_5

7. Lightweight cryptography project of the American National Institute of Standards and Technology, 2015. https://csrc.nist.gov/projects/ lightweight-cryptography.

8. Matsui, M. (1994). On correlation between the order of S-boxes and the strength of DES. In: EUROCRYPT 1994, Perugia, Italy, 9-12 May. pp. 366–375. Springer, Heidelberg. https://dx.doi.org/10.1007/BFb0053451

9. L. Knudsen (1992). Iterative characteristics of DES and s2-DES. Advances in Cryptology – Crypto'92. Springer Verlag, LNCS 746, pp. 497-511, Berlin Heidelberg 1993. https://dx.doi.org/10.1007/3-540-48071-4_35

10. K. Kim (1991). Construction of DES-like S-boxes Based on Boolean Function Satisfying the SAK. Proceedings Of Asiacrypt'91, pp. 59-72, Fujiyoshida, Japan, 1991. https://dx.doi.org/10.1007/3-540-57332-1_5

11. V. I. Dolgov, I. V. Lisitska, V. I. Ruzhentsev (2001). Zabezpechennya stiykosti shifra DES do atak diferenciynogo kryptoanaliza. Perekryttya harakterystyk obnulyauchogo typu i chotyryciklovyh iteratyvnyh harakterystyk. *Radiotechnics* Vyp. 120. C. 192–198. (in Ukrainian)

12. V. I. Dolgov, I. V. Lisitska, V. I. Ruzhentsev (2002). Zabezpechennya stiykosti shifra DES do atak diferenciynogo kryptoanaliza. Perekryttya shosty-, vosmy- i desyatyciklovih iteratyvnyh harakterystyk. *Radiotechnics*. Vyp. 124. C. 182–189. (in Ukrainian)

13. Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer (2019). Ascon v1.2. Submission to NIST, 2019. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ascon-spec-round2.pdf.

14. Ascon-Based Lightweight Cryptography Standards for Constrained Devices. Authenticated Encryption, Hash, and Extendable Output Functions (2025). National Institute of Standards and Technology, 2025 (NIST Special Publication 800 NIST SP 800-232). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-232.pdf

15. Christoph Dobraunig, Maria Eichlseder, Florian Mendel and Martin Schlaffer (2015). Cryptanalysis of Ascon. Cryptology ePrint Archive, Report 2015/030, 2015. https://eprint.iacr.org/2015/030.pdf.

Дата першого надходження рукопису до видання: 21.11.2025
Дата прийнятого до друку рукопису після рецензування: 19.12.2025
Дата публікації: 31.12.2025