

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

**ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ
УКРАЇНИ В УМОВАХ ВІЙНИ
ТА ГЛОБАЛЬНИХ ВИКЛИКІВ ХХІ СТОЛІТТЯ:
СИНЕРГІЯ НАУКОВИХ, ОСВІТНІХ
ТА ТЕХНОЛОГІЧНИХ РІШЕНЬ**

МАТЕРІАЛИ
Міжнародної науково-практичної
конференції

19 травня 2023 року

У двох томах

Том 1



Видавництво
«Юридика»
2023

УДК 005.332.2(4):316.42(477)"364""20"(062.552)
Є24

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16.06.2023 р.)

За загальною редакцією **С. В. Ківалова**.

Відповідальний за випуск **М. Р. Аракелян**.
Матеріали видано в авторській редакції.

Європейські орієнтири розвитку України в умовах війни та
Є24 глобальних викликів XXI століття: синергія наукових, освітніх
та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-
практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редак-
цією С. В. Ківалова. – Одеса : Видавництво «Юридика», 2023. –
Т. 1. – 790 с.

ISBN 978-617-8263-39-3

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень». У першому томі збірника містяться наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині в умовах повномасштабного військового вторгнення у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології. Висвітлено питання загроз національній безпеці в їхньому конституційному вимірі, у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики.

Збірник розраховано на наукових та науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)"364""20"(062.552)

ISBN 978-617-8263-37-9 (у 2 т.)
ISBN 978-617-8263-39-3 (т. 1)

© Національний університет
«Одеська юридична академія», 2023

Чикунів Павло Олександрович Застосування патернів проектування у процесі конструювання програмного забезпечення	606
Щербина Юрій Володимирович, Казакова Надія Феліксівна Проблеми захисту великих даних	609

СЕКЦІЯ 13

КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Горбаченко Станіслав Анатолійович Інформаційно-геометричні підходи в менеджменті кібербезпеки . . .	612
Василенко Микола Дмитрович, Слатвінська Валерія Миколаївна Забезпечення кіберзахисту кіберрозвідки	614
Ахматметьєва Ганна Валеріївна Використання хмарних ресурсів при викладанні спеціальних дисциплін в галузі інформаційних технологій в умовах військового стану.	616
Бойко Віктор Дмитрович Інструменти моделювання та аналізу даних у навчальному та дослідному процесі	618
Кухаренко Сергій Вікторович, Стаднік Денис Андрійович Забезпечення безпеки вебсерверів	622
Чепурна Олена Євгенівна, Кулешова Євгенія Романівна Сучасні математичні методи оптимізації заходів кібербезпеки	625
Баландіна Наталія Миколаївна Алгебраїчна нелінійність S-блоків конструкції Ніберг при їх представленні функціями багатозначної логіки	627
Слатвінська Валерія Миколаївна Цифровізація суспільства за допомогою gpt4	631
Drobchak Alla, Kovalchuk Kostyantyn Methods of information hygiene of citizens of Ukraine for the purpose of preventing cybercrime activities.	633
Слатвінська Валерія Миколаївна, Дрига Артем Вадимович Організація змагань по типу Capture The Flag з напрямку Web В НУ «ОЮА».	637

2. Результати Глобального дослідження ЕУ. URL: <https://eba.com.ua/rezultaty-globalnogo-doslidzhennya-ey-z-informatsijnoyi-bezpeky-pokazuyut-shho-kiberbezpeka-zalyshayetsya-vazhlyvym-pytannam-poryadku-dennogo-organizatsij/>
3. Моделі та методи кібернетичного захисту інформаційно-комунікаційних систем на основі логіко-ймовірнісного підходу / О. М. Новіков, А. М. Родіонов, А. О. Тимошенко. – Київ : НТУУ «КПІ» Вид-во «Політехніка», 2015. – 276 с.
4. Fighting Cyber Attacks with Game Theory. URL: <https://www.sciencedirect.com/science/article/abs/pii/B9780128205433000134?via%3DihubShun-ichiA-mari>
5. Information Geometry and Its Applications. Applied Mathematical Sciences, Springer, 2016.

Ключові слова: кібербезпека, теорія ймовірностей, математичне моделювання, інформаційна геометрія.

Key words: cyber security, probability theory, mathematical modeling, information geometry.

БАЛАНДІНА НАТАЛІЯ МИКОЛАЇВНА

*Національний університет «Одеська юридична академія»,
старший викладач кафедри кібербезпеки*

АЛГЕБРАЇЧНА НЕЛІНІЙНІСТЬ S-БЛОКІВ КОНСТРУКЦІЇ НІБЕРГ ПРИ ЇХ ПРЕДСТАВЛЕННІ ФУНКЦІЯМИ БАГАТОЗНАЧНОЇ ЛОГІКИ

Криптографічний S-блок є основним компонентом сучасних шифрів, який визначає їх ефективність. На сьогоднішній день в літературі відомо чимало методів синтезу S-блоків, які відповідають критеріям криптографічної якості. При цьому серед основних критеріїв криптографічної якості дослідники виділяють алгебраїчну нелінійність, відстань нелінійності, критерій розповсюдження помилки і критерій кореляційного імунітету. Зважаючи на останні наукові дослідження, зазначені критерії криптографічної якості мають застосовуватися не тільки до компонентних булевих функцій S-блоків [1], але і до їх компонентних функцій багатозначної логіки [2].

На сьогоднішній день, однією з найбільш затребуваних та застосовуваних конструкцій побудови S-блоків є конструкція Ніберг [3], що пропонує побудову елементів S-блока за допомогою мультиплікативного обернення над розширеним полем Галуа.

Дослідженню відповідності S-блоків конструкції Ніберг критеріям криптографічної якості як при її представленні булевими функціями, так і функціями багатозначної логіки присвячено чимало досліджень, наприклад [4, 5]. Тим не менш, алгебраїчна нелінійність S-блоків конструкції Ніберг при їх можливому представленні 4-функціями та 16-функціями лишається недослідженою.

Метою цієї роботи є оцінка алгебраїчної степені нелінійності S-блоків конструкції Ніберг при їх представленні компонентними функціями багатозначної логіки.

Відомо [3], що S-блоки конструкції Ніберг визначаються за допомогою наступного співвідношення

$$y_i = x_i^{-1} \bmod [f(z), p], y_p, x_i \in GF(2^k), i = 0, 1, \dots, 2^k - 1, \quad (1)$$

де y_i – вихідний елемент S-блока, x_i – вхідний елемент S-блока, $f(z)$ – незвідний поліном (кількість яких для найбільш затребуваної на сьогодні довжини S-блоків $N = 256$ складає $J = 30$).

На сьогодні добре відомо [2], що будь-який S-блок довжини $N = 256$ може бути представлений у вигляді своїх компонентних булевих функцій, 4-функцій та 16-функцій, які, у свою чергу, із застосуванням методів [6] можуть бути представлені за допомогою алгебраїчної нормальної форми. При цьому одним з показників якості реалізації концепції конфузії та стійкості до атак алгебраїчного криптоаналізу конструкцій шифру є їх алгебраїчний степінь нелінійності. Алгебраїчний степінь нелінійності функції багатозначної логіки визначається найбільшим алгебраїчним степенем доданку в поліномі АНФ.

Важливим є проведення дослідження алгебраїчних степенів нелінійності компонентних функцій багатозначної логіки S-блоків конструкції Ніберг, яке будемо виконувати відповідно до наступного алгоритму:

Крок 1. Для обраного незвідного поліному побудувати S-блок конструкції Ніберг відповідно до (1).

Крок 2. Представити побудований S-блок за допомогою восьми компонентних булевих функцій, для кожної з яких знайти АНФ. Оцінити алгебраїчний степінь нелінійності S-блока як мінімум серед алгебраїчних степенів АНФ побудованих компонентних булевих функцій.

Крок 3. Представити побудований S-блок за допомогою чотирьох компонентних 4-функцій, для кожної з яких знайти АНФ над полем $GF(4)$, що побудовано на основі первісного незвідного поліному $g_{41} = x^2 + x + 1$. Оцінити алгебраїчний степінь нелінійності S-блока.

Крок 4. Представити побудований S-блок за допомогою двох компонентних 16-функцій, для кожної з яких знайти АНФ над полем $GF(16)$: розглянути два можливі ізоморфізми, на основі первісного незвідного поліному $g_{161} = x^4 + x + 1$ та первісного незвідного поліному $g_{162} = x^4 + x^3 + 1$. Оцінити алгебраїчний степінь нелінійності S-блока для кожного з ізоморфізмів.

Алгебраїчні степені нелінійності компонентних q -функцій для кожного з $J = 30$ незвідних над полем $GF(2^8)$ поліномів показані у таблиці.

Відзначимо, що максимальний алгебраїчний степінь нелінійності для булевих функцій восьми змінних становить 8, для 4-функцій чотирьох змінних – 12, для 16-функцій двох змінних – 30.

Отже, алгебраїчний степінь нелінійності для уявлення S-блоків конструкції Ніберг за допомогою компонентних булевих функцій є стабільним і складає 87,5 % від максимального значення.

Таблиця – Алгебраїчні степені нелінійності компонентних q -функцій S-блоків конструкції Ніберг

№	Поліном	Двійковий випадок, $\{N_{f_{20}}, \dots, N_{f_{27}}\}$	Четвірковий випадок, $\{N_{f_{40}}, \dots, N_{f_{43}}\}$	Шістнадцятковий випадок, ізоморфізм $g_1(x)$, $\{N_{f_{160}}, \dots, N_{f_{161}}\}$	Шістнадцятковий випадок, ізоморфізм $g_2(x)$, $\{N_{f_{160}}, N_{f_{161}}\}$
1	283	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{28,29}
2	285	{7,7,7,7,7,7,7}	{11,10,11,11}	{30,30}	{28,29}
3	299	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
4	301	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
5	313	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
6	319	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
7	333	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{28,29}
8	351	{7,7,7,7,7,7,7}	{11,10,11,11}	{30,30}	{28,29}
9	355	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
10	357	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{28,29}
11	361	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
12	369	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
13	375	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
14	379	{7,7,7,7,7,7,7}	{11,11,11,11}	{28,30}	{29,29}
15	391	{7,7,7,7,7,7,7}	{11,10,10,11}	{30,30}	{29,29}
16	395	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
17	397	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
18	415	{7,7,7,7,7,7,7}	{11,10,11,11}	{30,29}	{29,29}
19	419	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
20	425	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
21	433	{7,7,7,7,7,7,7}	{10,10,10,11}	{29,30}	{29,29}
22	445	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
23	451	{7,7,7,7,7,7,7}	{11,11,10,11}	{30,30}	{29,29}
24	463	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
25	471	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
26	477	{7,7,7,7,7,7,7}	{10,10,10,11}	{29,30}	{29,29}
27	487	{7,7,7,7,7,7,7}	{11,11,10,11}	{30,30}	{29,29}
28	499	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{28,29}
29	501	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,30}	{29,29}
30	505	{7,7,7,7,7,7,7}	{11,11,11,11}	{30,29}	{29,29}

У разі представлення S-блоків конструкції Ніберг 4-функціями, алгебраїчний степінь нелінійності лежить у діапазоні від 83,3 % до 91,67 %.

У разі представлення S-блоків конструкції Ніберг 16-функціями над ізоморфним представленням поля $GF(16)$ на основі первісного

незвідного полінома $g_{161} = x^4 + x + 1$, алгебраїчний степінь нелінійності лежить у діапазоні від 96,67 % до 100 %.

У разі представлення S-блоків конструкції Ніберг 16-функціями над ізоморфним представленням поля $GF(16)$ на основі первісного незвідного полінома $g_{162} = x^4 + x^3 + 1$, алгебраїчний степінь нелінійності лежить у діапазоні від 93,33 % до 96,67 %.

Таким чином, в цілому конструкція Ніберг характеризується високими алгебраїчними степенями нелінійності компонентних функцій багатозначної логіки, що є її безсумнівною перевагою. При цьому, спостерігається навіть зростання алгебраїчного степеню нелінійності із зростанням значення основи уявлення q .

Відзначимо основні результати проведених досліджень:

1. Проведено дослідження алгебраїчних степенів нелінійності S-блоків конструкції Ніберг довжини $N = 256$, побудованих на основі повної множини незвідних поліномів при всіх можливих їх представленнях за допомогою функцій багатозначної логіки.

2. Для представлення S-блоків конструкції Ніберг за допомогою двох компонентних 16-функцій, для оцінки їх алгебраїчного степеню нелінійності розглянуто два можливі ізоморфізми поля $GF(16)$, які можуть бути застосовані криптоаналітиком для опису криптографічної конструкції.

3. Проведені експерименти показали, що S-блоки конструкції Ніберг, незалежно від виду обраного для їх побудови незвідного поліному, характеризуються високим рівнем алгебраїчного степеню нелінійності, при цьому, його значення відносно максимально можливого значення нелінійності навіть зростають із зростанням основи уявлення q .

Список використаних джерел:

1. Waheed A. et al. An analytical review of current S-box design methodologies, performance evaluation criteria, and major challenges. Multimedia Tools and Applications. 2023. P. 1–24.
2. Соколов А. В., Жданов О. Н. Криптографические конструкции на основе функций многозначной логики. Монография. Научная мысль, 2020. 192 с.
3. Nyberg K. Differentially uniform mappings for cryptography. In Advances in cryptology. Proc. of EUROCRYPT'93. 1994. Vol. 765. P. 55–65.
4. Мазурков М. И., Соколов А. В. Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов. Труды Одесского политехнического университета. 2012. № 2 (39). С. 183–189.
5. Sokolov A. V., Djiofack T. V. N. Nonlinear Properties of Rijndael S-boxes Represented by the Many-Valued Logic Functions. Proceedings of the International Workshop on Cyber Hygiene, Kyiv, Ukraine, Nov. 30, 2019. P. 96–106.
6. Stankovic R. S., Astola J. T., Moraga C. Representations of Multiple-Valued Logic Functions. Morgan and Claypool Publishers, 2012. 160 p.

Ключові слова: криптографія, S-блок, АНФ, алгебраїчний степінь нелінійності.

Key words: cryptography, S-box, ANF, algebraic degree of nonlinearity.