Порівнювальні дослідження нелінійних вузлів заміни сучасних блокових симетричних шифрів

Білозерцев І.М.[1], Андрушкевич А.В.[2], Луценко М.С.[3]

[1]Студент факультету комп'ютерних наук, Харківський національний університет ім. В.Н. Каразіна
пл. Свободи 4, м. Харків, Україна, ivanbelozersevv.jw@gmail.com
[2]Аспірантка, інженер 1 кат. кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки
пр. Науки 14, м. Харків, Україна, alina.samoilova@nure.ua
[3]Студентка факультету комп'ютерних наук, Харківський національний університет ім. В.Н. Каразіна
пл. Свободи 4, м. Харків, Україна, maria-lutsenko@mail.ru

***Анотація* – Розглянуто сучасні блокові симетричні шифри та нелінійні вузли замін, що в них застосовуються. Проаналізовано показники та критерії ефективності нелінійних вузлів замін: збалансованість, нелінійність, кореляційний імунітет, критерії розповсюдження, автокореляція та інші. Проведено порівняльні дослідження ефективності нелінійних вузлів заміни сучасних блокових симетричних шифрів.**

Ключові слова: нелінійний вузол заміни, блоковий симетричний шифр, критерії ефективності.

Comparative research of non-linear substitution components of modern block ciphers

Bilozertsev I.M.[1], Andrushkevych A.V. [2], Lutsenko M. S.[3]

[1]Student of Faculty of Computer Sciences, V. N. Karazin Kharkiv National University
Svobody Sq. 4, Kharkiv, Ukraine, ivanbelozersevv.jw@gmail.com
[2]Graduate student, Engineer of 1 category of Department of Security of Information Technologies, Kharkiv National University of Radio Electronics
Nauka ave 14, Kharkiv, Ukraine, alina.samoilova@nure.ua
[3]Student of Faculty of Computer Sciences, V. N. Karazin Kharkiv National University
Svobody Sq. 4, Kharkiv, Ukraine, maria-lutsenko@mail.ru

***Abstract* – The paper examines modern block ciphers and non-linear substitution components(S-blocks), which were used in them. Properties and criteria of S-block effectiveness such as balancedness, correlation immunity, propagation criteria, autocorrelation et cetera are analyzed. A comparative research of the effectiveness of non-linear substitution components of modern block ciphers is conducted.**

Keywords: non-linear substitution components, symmetric block cipher, efficiency criteria.

ВСТУП

Розвиток сучасних комп'ютерних систем та технологій, застосування хмарних обчислень, використання мобільних пристроїв віддаленого підключення до інформаційно-телекомунікаційних систем (ІТС) призводять до значного ускладнення процедур захисту інформації, що оброблюється та передається. Необхідною умовою виконання основних послуг безпеки є застосування криптографічних засобів захисту інформації [1].

Найбільш поширене використання в ІТС для забезпечення послуги конфіденціальності інформації отримали блокові симетричні шифри (БСШ) [3-7]. Важливість розробки, дослідження і обгрунтування умов застосування сучасних БСШ підтверджується кількістю та масштабністю міжнародних криптографічних конкурсів, проведених в останні роки. Так, наприклад, міжнародні проекти AES, NESSIE, CRYPTREC тощо, були орієнтовані на розробку БСШ, які відповідають високим вимогам криптографічної стійкості і ефективності програмної і апаратної реалізації. Результатами проведення цих та багатьох інших дослідницьких проектів є прийняті в останні роки міжнародні та національні стандарти криптографічного перетворення [3 - 7].

Належний високий рівень стійкості БСШ забезпечується ефективністю складових, що до нього входять: схема розгортання секретного ключа (розклад ключів), базова структура алгоритму, лінійні та нелінійні перетворення, та інші. В роботі увагу буде акцентовано на нелінійних вузлах замін, критеріях та показниках їх ефективності [2]. Планується провести порівняльні дослідження деяких властивостей нелінійних вузлів замін (S-боксів) сучасних БСШ, що стандартизовані на міжнародному та національному рівнях [3-6].

ОСНОВНІ ВЛАСТИВОСТІ СУЧАСНИХ БСШ

Розглянемо основні властивості сучасних БСШ та нелінійних вузлів замін, що в них використовуються (таблиця 1). В таблиці зазначено назву сучасного шифру, країну, в якій було розроблено шифр, стандарт (національний або міжнародний). Розмір блоку шифру позначається як N_b біт, розмір ключа – N_k біт, кількість циклів перетворення – K

.

Таблиця 1 – Основні властивості сучасних БСШ [3-7]

№ п/п	Назва БСШ	Країна Стандарт	N_b	N_k	K	Основні перетворення	Вид S-блоку
1	БСШ «Калина»	Україна, ДСТУ 7624:2014	128	128	10	Square-подібна SPN-структура. Циклове перетворення побудовано на базі таблиць підстановки (S-блоків) на множення на МДР-матрицю над кінцевим полем.	Використовує 4 таблиці підстановки байт в байт.
			128	256	14		
			256				
			256	512	18		
			512				
2	БСШ «Кузнечик»	Росія ГОСТ 34.12-2015	128	256	10	Square-подібна SPN-структура. Циклове перетворення побудовано на базі таблиць підстановки (S-блоків) на множення на МДР-матрицю над кінцевим полем.	Використовує одну таблицю підстановки байт в байт.
3	БСШ «BelT»	Республіка Беларусь СТБ 34.101.31-2011	128	256	8	В основі схеми ланцюг Фейстеля, що оперує 32-бітними блоками. Циклове перетворення побудовано на базі таблиці підстановки (S-блоків), блоці лінійного розсіювання.	Використовує одну таблицю підстановки байт в байт.
4	БСШ «AES»	США FIPS-197 ISO/IEC 18033-3	128	128	10	Square-подібна SPN-структура. Циклове перетворення побудовано на базі таблиць підстановки (S-блоків) на множення на МДР-матрицю над кінцевим полем.	Використовує одну таблицю підстановки байт в байт.
				192	12		
				256	14		
5	БСШ «Camellia»	Японія ISO/IEC 18033-3	128	128	18	Класичний ланцюг Фейстеля с попереднім та фінальним забілюванням. Циклова функція використовує нелінійне перетворення (S-блок), блок лінійного розсіювання кожні 16 циклів (побайтова операція XOR) та байтова перестановка.	Використовує одну таблицю підстановки байт в байт.
				192	24		
				256			
6	БСШ «SEED»	Корея, ISO/IEC 18033-3	128	128	16	В основі схеми ланцюг Фейстеля Циклове перетворення побудовано на базі таблиць підстановок (S-блоків), блоці лінійного розсіювання.	Використовує дві таблиці підстановки байт в байт.

КРИТЕРІЇ ТА ПОКАЗНИКИ ЕФЕКТИВНОСТІ НЕЛІНІЙНИХ ВУЗЛІВ ЗАМІНИ

Розглянемо критерії та показники ефективності нелінійних вузлів заміни, що безпосередньо впливають на рівень стійкості сучасних БСШ до різних криптоаналітичних атак.

Під ефективністю функціонування будь-якої технічної системи розуміють відповідність отриманих результатів функціонування необхідним. Очевидно, що нелінійний вузол вважатається ефективним, якщо він забезпечує стійкість до відомих на сьогоднішній день методів криптографічного аналізу.

У більшості відомих робіт в області аналізу і синтезу нелінійних вузлів заміни сучасних БСШ використовується математичний апарат криптографічних булевих функцій [7 - 13]. При цьому кожен S-блок представляється сукупністю компонентних булевих функцій, властивості яких характеризують ефективність нелінійного вузла замін.

В роботі були розглянуті такі основні показники ефективності нелінійних вузлів заміни, як збалансованість, нелінійність, автокореляція, алгебраїчна ступінь, ступінь критерію поширення і кореляційного імунітету криптографічних булевих функцій. Розглянуті критерії та показники ефективності S-блоків відображають здатність нелінійного вузла протистояти атакам певного типу. Нелінійність, критерій поширення і кореляційний імунітет характеризують здатність протистояти кореляційним атакам, алгебраїчна ступінь і автокорреляция – аналітичним атакам, збалансованість - статистичним.

РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ

Для проведення експериментальних досліджень ефективності різних S-блоків у середі IntelliJ IDEA 15 Community edition на мові Java був розроблений програмний обчислювальний комплекс.

Результати експериментальних досліджень зведені в таблиці 2-4. Використано наступні позначення: B - збалансованість; N - нелінійність; A - автокорреляція; AD - алгебраїчна ступінь; PC - критерій поширення; CI - кореляційний імунітет; f_n - функція, відповідна n-му виходу S-блоку; S-box -

показники ефективності S-блоку по критерію мінімального ризику (гірший випадок серед усіх компонентних булевих функцій); Linear combinations (LC) - показники ефективності S-блоку по критерію мінімального ризику (гірший випадок серед усіх лінійних комбінацій булевих функцій).

Таблиця 2 – Показники ефективності таблиць підстановок шифру «Калина»

	S_1-блок						**S_2-блок**						**S_3-блок**						**S_4-блок**					
	B	**N**	**A**	**AD**	**PC**	**CI**	**B**	**N**	**A**	**AD**	**PC**	**CI**	**B**	**N**	**A**	**AD**	**PC**	**CI**	**B**	**N**	**A**	**AD**	**PC**	**CI**
f_1	+	106	48	7	0	0	+	106	48	7	0	0	+	106	56	7	0	0	+	108	56	7	0	0
f_2	+	106	64	7	0	0	+	106	64	7	0	0	+	104	64	7	0	0	+	104	56	7	0	0
f_3	+	106	56	7	0	0	+	106	56	7	0	0	+	106	56	7	0	0	+	108	64	7	0	0
f_4	+	104	72	7	0	0	+	104	72	7	0	0	+	106	56	7	0	0	+	108	48	7	0	0
f_5	+	104	56	7	0	0	+	104	56	7	0	0	+	108	48	7	0	0	+	104	64	7	0	0
f_6	+	106	56	7	0	0	+	106	56	7	0	0	+	104	56	7	0	0	+	108	56	7	0	0
f_7	+	106	64	7	0	0	+	106	64	7	0	0	+	106	56	7	0	0	+	104	64	7	0	0
f_8	+	106	64	7	0	0	+	106	64	7	0	0	+	104	56	7	0	0	+	108	48	7	0	0
S-box	+	104	72	7	0	0	+	104	72	7	0	0	+	104	64	7	0	0	+	104	64	7	0	0
LC	+	104	72	7	0	0	+	104	72	7	0	0	+	104	72	7	0	0	+	104	72	7	0	0

Таблиця 3 – Показники ефективності таблиць підстановок шифрів «Кузнечик», «BelT», «AES», «Camellia»

	S-блок «Кузнечик»						**S-блок «BelT»**						**S-блок «AES»**						**S-блок «Camellia»**					
	B	N	A	**AD**	**PC**	**CI**	**B**	**N**	**A**	**AD**	**PC**	**CI**	**B**	**N**	**A**	**AD**	**PC**	**CI**	**B**	**N**	**A**	**AD**	**PC**	**CI**
f1	+	104	64	7	0	0	+	106	56	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f2	+	106	56	7	0	0	+	106	72	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f3	+	116	24	7	0	0	+	106	56	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f4	+	104	64	7	0	0	+	104	72	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f5	+	110	48	7	0	0	+	108	56	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f6	+	106	64	7	0	0	+	106	72	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f7	+	102	72	7	0	0	+	108	56	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
f8	+	104	64	7	0	0	+	108	64	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
S-box	+	102	72	7	0	0	+	104	72	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0
LC	+	102	80	7	0	0	+	102	72	7	0	0	+	112	32	7	0	0	+	112	32	7	0	0

Таблиця 4 – Показники ефективності таблиць підстановок шифру «SEED»

S_1-блок	**B**	**N**	**A**	**AD**	**PC**	**CI**	**S_2-блок**	**B**	**N**	**A**	**AD**	**PC**	**CI**
f_1	+	110	40	7	0	0	f_1	+	112	32	7	0	0
f_2	-	111	36	8	0	0	f_2	+	112	32	7	0	0
f_3	+	112	32	7	0	0	f_3	+	112	32	7	0	0
f_4	+	112	40	7	0	0	f_4	+	112	32	7	0	0
f_5	+	110	40	7	0	0	f_5	+	111	36	8	0	0
f_6	-	111	36	8	0	0	f_6	-	113	36	8	0	0
f_7	-	111	36	8	0	0	f_7	+	112	32	7	0	0
f_8	+	111	36	8	0	0	f_8	+	111	36	8	0	0
S-box	-	110	40	7	0	0	S-box	-	111	36	7	0	0
LC	-	109	44	7	0	0	LC	+	111	36	7	0	0

Отримані результати показали різноманітність думок розробників досліджуваних шифрів щодо концепцій формування S-блоків. Розробники БСШ «SEED» також наголошували на збільшення ефективності таблиці підстановки за рахунок зниження автокорреляции. Однак S-блок, що використовується, має менше значення нелінійності, а також є незбалансованим. Таблиця підстановки БСШ «AES» має високу алгебраїчну ступінь, хороші показники по нелінійності і автокореляції, однак має нульовий критерій поширення. Крім того, S-блок БСШ «AES» сформований на основі алгебраїчної конструкції Нібер-Дінга, що створює передумови для можливої реалізації алгебраїчного криптоанализа. БСШ «Camellia» показав однакові з «AES» результати. Решта проаналізованих S-блоків не є алгебраїчними, але при цьому втрачають в нелінійності і автокореляції.

Таблиці підстановки шифрів, затверджених в якості державних стандартів України, Російської Федерації та Білорусі є найбільш збалансованим, компромісним рішенням. Серед них найкращими показниками володіє S-блок українського шифру «Калина», слідом за ним йде білоруський «BelT» і російський «Кузнечик».

ВИСНОВКИ

Отримані результати дозволяють судити про основні концепції формування нелінійних вузлів замін сучасних БСШ. Як правило, нелінійні вузли розробляються з урахуванням найбільш ймовірних загроз і особлива увага приділяється специфічним показникам ефективності. Перспективні шифри повинні протистояти всім найбільш поширеним існуючим атакам.

Вибрані показники ефективності нелінійних вузлів замін характеризують першочергові вимоги до забезпечення їх стійкості. Отримані результати не дозволяють однозначно визначити кращий S-бокс, через різні концептуальні особливості в проектуванні кожного з них. Однак серед шифрів, які стандартизовані в пострадянських країнах, найкращим за показниками ефективності нелінійних вузлів замін слід зазначити S-блок шифру «Калина».

Перспективним напрямком подальших досліджень є аналіз властивостей нелінійних вузлів ускладнення поточних криптоалгоритмів, обґрунтування рекомендацій і пропозицій щодо розроблення національного стандарту поточного шифрування України.

ЛІТЕРАТУРА REFERENCES

[1] Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: Підручник для вищих навч. закладів. – Харків: Вид-во «Форт», 2013. – 880 с.

[2] Аналіз та порівняльні дослідження нелінійних вузлів замін сучасних блокових симетричних ши-фрів / Кузнецов О.О., Білозерцев І.М., Андрушкевич А.В. // Прикладна радіоелектроніка: наук.-техн. журнал. – 2015. – Том 14. – №4. – с. 343-350.

[3] Information technology – Security techniques – Encryption algorithms, Part 3: Block ciphers (ISO/IEC 18033-3), 80 с.

[4] ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015г. – 25с.

[5] СТБ 34.101.31-2011 Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности. – Минск: Госстандарт, 2011г. – 35с.

[6] Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Мінекономрозвитку України, 2015. – 238 с.

[7] Розробка нового блокового симетричного шифру: звіт за перший етап НДР «Алгоритм» (проміжний) / АТ «ІІТ»; кер. І.Д. Горбенко – Харків, 2014, Том 4. – 304 с.

[8] Bart Preneel. Analysis and Design of Cryptographic Hash Functions. [Электронный ресурс] – Режим доступа: homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf

[9] Carlet C. Vectorial Boolean functions for // Cambridge Univ. Press, Cambridge. – 95 p. [Электронный ресурс] – Режим доступа: www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf

[10] Carlet C. Boolean functions for cryptography and error correcting codes // Cambridge Univ. Press, Cambridge. – 2007. – 148 p. [Электронный ресурс] – Режим доступа: www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf

[11] Zhuo Zepeng, Zhang Weiguo On correlation properties of Boolean functions // Chinese Journal of Electronics. Jan, Vol.20, 2011, №1, 143-146 pp.

[12] O'Connor L. An analysis of a class of algorithms for S-box construction // J. Cryptology. -1994. – p. 133-151.

[13] Clark J.A., Jacob J.L., Stepney S. The Design of S-Boxes by Simulated Annealing // New Generation Computing. – 2005. – 23(3). – p.219–231.