УДК 621. 3.06

АНАЛІЗ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ МІЖНАРОДНОГО СТАНДАРТУ ISO/IEC 29192-2

І.Д. ГОРБЕНКО, А.В. САМОЙЛОВА

Виконується оцінка та порівняльний аналіз блокових симетричних шифрів перспективного міжнародного стандарту ISO/IEC 29192-2. Метою порівняння є оцінка стійкості та швидкодії за умови їх застосування в спрощених застосуваннях (смарт-картках).

Ключові слова: блоковий симетричний шифр, спрощені застосування, міжнародний стандарт, диференційний та лінійний криптоаналіз.

Сьогодні розроблено, стандартизовано та використовуються блокові симетричні шифри (БСШ), які забезпечують високий (гарантований) рівень стійкості та знайшли широке розповсюдження та застосування [1]. В процесі їх впровадження на практиці виявилось, що для деяких додатків вони є складними в реалізації і не забезпечують психологічного сприйняття під час застосування користувачами, наприклад, у ході використання в смарт-картках. Зважаючи на це, розроблено та стандартизовано новітні версії БСШ, які отримали назву полегшених. Зміст полегшеності в тому, що в них зменшена складність криптографічних перетворень. Водночас, це полегшення викликає в свою чергу сумніви відносно рівнів стійкості таких шифрів та їх швидкодії. Метою цієї статті є вивчення сутностей та порівняльний аналіз криптографічної стійкості і швидкодії перспективних БСШ згідно з ISO/IEC 29192-2 [2].

У міжнародному стандарті ISO/IEC 29192-2 представлені два БСШ – PRESENT та CLEFIA. Вони, на наш погляд, складають серйозну конкуренцію вже перевіреним міжнародним стандартам БСШ – AES, Camellia та SEED [1] для використання у смарт картках.

БСШ PRESENT – це симетричний БСШ з 64-ма бітами блока даних та 80 або 128-ма бітами ключа. Він є ітераційним і базується на схемі підстановки-перестановки та складається з 31 раунду.

БСШ CLEFIA має довжину блоків даних у 128 біт та довжину ключа 128, 192 або 256 бітів. Алгоритм шифру побудовано на основі узагальненої структури ланцюга Фейстеля та вимагає виконання 18, 22, 26 раундів відповідно для 128, 192, 256 бітних ключів. Раундова функція CLEFIA ґрунтується на двох різних функціях – F_0 та F_1. N-раунд CLEFIA повторює раундову функцію N разів, причому в першому та останньому раундах використовуються 4 забілені байти ключа. Функції F_0 та F_1 мають SP-структуру.

1. ОЦІНКА СТІЙКОСТІ

Оцінка стійкості БСШ здійснювалась на основі, по-перше, аналізу існуючих джерел та стандартів, відносно цих БСШ, по-друге, на основі самостійних досліджень з використанням програмних моделей.

З'ясовано, що на БСШ PRESENT існують такі види атак: «груба сила», диференційний та лінійний криптоаналіз, алгебраїчна атака, структурна атака та атака на розгортання ключів. Результати аналізу стійкості цього БСШ PRESENT зведено в таблиці 1 [3].

Відносно БСШ CLEFIA існують такі види атак: лінійний та диференційний криптоаналіз, атака нездійсненних диференціалів, та square - атака, з яких атака нездійсненних диференціалів є найбільш ефективною. В таблиці 2 наведено дані щодо стійкості БСШ CLEFIA до певних атак [4].

Результати порівняння БСШ PRESENT та CLEFIA зводяться до наступного. Відносно них не було виявлено криптоаналітичних атак, складність яких була б менше, ніж атака «груба сила». В цілому можна зробити висновок, що БСШ PRESENT та CLEFIA відповідають як мінімум мінімальним вимогам, і можуть бути рекомендованими до застосування для шифрування інформації з використанням малопотужних засобів (смарт-карток). Водночас, на наш погляд, необхідно також провести аналіз стійкості цих шифрів відносно структурної та атаки на схему розгортання ключів, а також square-атаки.

Таблиця 1

Аналіз стійкості шифру PRESENT

Атака	Кількість раундів	Складність реалізації
Атака «груба сила»	Полягає в переборі ключів	На пошук ключів у просторі з 2^{80} ключів знадобиться приблизно $1.596*10^6$ років
Диференційний криптоаналіз	15 раундів	$2^{35,6}$ пар «відкритий текст – шифр - текст»
Лінійний криптоаналіз	26 раундів	2^{64} пар «відкритий текст – шифр - текст»
Алгебраїчна атака	Полягає у вирішенні квадратичних рівнянь	Вирішення 11067 квадратичних рівнянь з 4216 перемінними

Таблиця 2

Аналіз стійкості шифру CLEFIA

Атака	Кількість раундів	Обсяг даних	Час	Сутність атаки
Інтегральна атака на CLEFIA-128/192/256	12	2^{113}	$2^{116.7}$	Метою цієї атаки є прогнозування значень в сумах від обраного байта після певної кількості раундів шифрування
Інтегральна атака на CLEFIA-192/256	13	2^{113}	$2^{180.5}$	
Інтегральна атака на CLEFIA-256	14	2^{113}	$2^{244.5}$	
Атака нездійсненних диференціалів на CLEFIA-128	12	$2^{118,9}$	2^{119}	Атака, реалізована з використанням 9-раундового нездійсненного диференціала
Атака нездійсненних диференціалів на CLEFIA-192	13	$2^{119,8}$	2^{147}	
Атака нездійсненних диференціалів на CLEFIA-256	14	$2^{120,3}$	2^{211}	

2. ОЦІНКА ШВИДКОДІЇ

Оцінка швидкодії здійснювалась на основі програмного моделювання процедур зашифрування та розшифрування для БСШ PRESENT та CLEFIA. Сутність методики порівняння в тому, що алгоритм зашифрування та розшифрування реалізується програмно мовою C++. Далі блоки інформації з довжиною для PRESENT 64 біти, та для CLEFIA 128 бітів зашифровуються багаторазово, і вимірюється число тактів (час зашифрування на блок). Були використані програмні моделі зашифрування – розшифрування: Для БСШ PRESENT з довжинами ключів 80 та 128 бітів, та для БСШ CLEFIA з довжиною ключа 128 бітів.

Результати оцінки швидкодії порівнювались з БСШ міжнародного стандарту ISO/IEC 18033-3 [1].

На основі аналізу даних таблиць 3 та 4, можна зробити висновок, що показники найвищої швидкодії мають БСШ стандарту ISO/IEC 29192-2.

Додатково, аналіз швидкодії здійснюють за вхідною ефективністю. При цьому ефективність устаткування визначається як відношення пропускної здатності до розмірів входу. На рис. 1 зображена площа, яка вказує на більш високу продуктивність, що призводить до більш низького споживання енергії [5]. На рис. 1 БСШ CLEFIA порівнюється з БСШ AES (FIPS197), Camellia (RFC3713), та SEED (RFC4269). Із аналізу графіків можна зробити висновок, що перевагу серед останніх у продуктивності відносно апаратного входу, має БСШ CLEFIA. Отже, можна зазначити, що БСШ стандарту ISO/IEC 29192-2, через свою властивість полегшеності, мають вищі показники швидкодії відносно інших міжнародних стандартів шифрування, та можуть використовуватись ефективно в малопотужних засобах (смарт-картках).

Вказані БСШ можуть використовуватися у вбудованих та безконтактних системах, для конструкцій яких необхідні лише невелика площа кристалу та низьке споживання енергії. Стосовно питань швидкодії та стійкості шифри

Таблиця 3

Аналіз реалізації БСШ (оптимізація площі)

	Режим	Розмір блоку (біти)	Розмір ключа (біти)	Цикл	Площа (GE)	Частота (МГц)	Пропускна здатність (Мбіт/с)	Технологія (μm)
PRESENT	enc	64	80	547	1075	0.1	0.0117	0.18
PRESENT	enc	64	128	559	1391	0.1	0.0115	0.18
CLEFIA	enc	128	128	176	2893	67	49	0.13
CLEFIA	enc/dec	128	128	176	2996	61	44	0.13
AES	enc	128	128	177	3100	152	110	0.13
AES	enc/dec	128	128	1032	3400	80	10	0.35

Таблиця 4

Аналіз реалізації БСШ(оптимізація продуктивності)

	Режим	Розмір блоку (біти)	Розмір ключа (біти)	Цикл	Площа (GE)	Частота (МГц)	Пропускна здатність (Мбіт/с)	Технологія (μm)
PRESENT	enc	64	80	32	1570	0,1	0,20	0,18
PRESENT	enc	64	128	32	1884	0,1	0,20	0,18
CLEFIA	enc/dec	128	128	36	4950	201,3	716,69	0,09
CLEFIA	enc/dec	128	128	18	5979	225,8	1605,94	0,09
AES	enc/dec	128	128	11	12454	145,4	1691,35	0,13
AES	enc/dec	128	128	54	5398	131,2	311,09	0,13

міжнародного стандарту ISO/IEC 29192-2 не поступаються БСШ AES, Camellia, SEED.

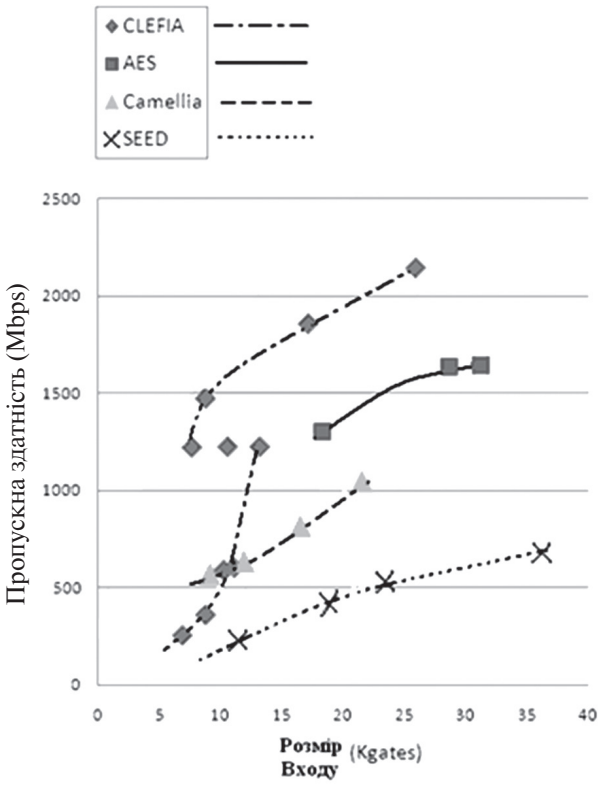

Рис. 1. Графік залежності пропускної здатності від розміру входу

Література

[1] ISO/IEC 18033-3:2005, Information technology – Security techniques – Encryption algorithms, Part 3: Block ciphers.

[2] ISO/IEC 29192-2, Information technology — Security techniques — Lightweight cryptography, Part 2: Block ciphers.

[3] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher.

[4] Yukiyasu Tsunoo, Impossible Differential Cryptanalysis of CLEFIA.

[5] Masanobu Katagi, Lightweight Cryptography for the Internet of Things.

Надійшла до редколегії 4.04.2013

Горбенко Іван Дмитрович, фото та відомості про автора див. на с. 201.

Самойлова Аліна Вадимівна, студентка 4-го курсу спеціальності БІКС ХНУРЕ. Наукові інтереси: аналіз стійкості блокових симетричних шифрів, симетрична криптографія.

УДК 621. 3.06

Анализ блочных симметричных шифров международного стандарта ISO/IEC 29192-2 / И.Д. Горбенко, А.В. Самойлова // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 247–249.

Выполняется оценка и сравнительный анализ блочных симметричных шифров перспективного международного стандарта ISO / IEC 29192-2. Целью сравнения является оценка устойчивости и быстродействия при условии их применения в упрощенных приложениях (смарт-картах).

Ключевые слова: блочный симметричний шифр, упрощенные применения, международный стандарт, дифференциальный и линейный криптоанализ.

Табл.: 4. Ил.: 1. Библиогр.: 5 назв.

UDC 621. 3.06

Analysis of block symmetric ciphers of international standard ISO/IEC 29192-2 / I.D. Gorbenko, A.V. Samoilova // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. –№ 2. – P. 247–249.

This paper gives assessment and comparative analysis of block symmetric ciphers of the perspective standard ISO/IEC 29192-2. The aim of comparison is assessing security and speed of response under conditions of their use in simplified applications (smart cards).

Keywords: block symmetric cipher, lightweight application, international standard, differential and linear cryptanalysis.

Tab.: 4. Fig.: 1. Ref.: 5 items.