УДК 004.056.55

І.Д. ГОРБЕНКО, д-р техн. наук, О.О. КУЗНЕЦОВ, д-р техн. наук, А.В. САМОЙЛОВА

СТАТИСТИЧНІ ВЛАСТИВОСТІ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ З МІЖНАРОДНОГО СТАНДАРТУ ISO/IEC 29192-2

Вступ

На нинішній час для забезпечення конфіденційності застосовуються криптографічні перетворення типу шифрування [1 – 5]. У зв'язку з тим, що конфіденційність згідно законодавства України повинна надаватись по запиту користувачів як обов'язкова послуга, таке перетворення уже сьогодні застосовується масово, тобто широким числом користувачів. В той же час засоби повинні бути як більш доступними для користувачів, повинні мати можливість простої експлуатації та невисокої вартості. У зв'язку з вказаними вимогами на міжнародному рівні були розроблені та прийняті в якості міжнародного стандарту такі блокові симетричні шифри (БСШ), що, як стверджують розробники, мають зменшену складність алгоритмів шифрування [1, 2]. В той же час, це полегшення викликає в свою чергу сумніви відносно рівнів стійкості цих шифрів та їх швидкодії, а також існують сумніви, щодо генерування такими шифрами «якісних» випадкових послідовностей. Порівняльний аналіз стійкості та швидкодії було вже розглянуто в попередній статті [3].

Метою цієї роботи є порівняльний аналіз статистичних властивостей перспективних шифрів полегшеного шифрування, що стандартизовані на міжнародному рівні як ISO/IEC 29192-2 [1], при застосуванні в різних режимах шифрування [6].

БСШ PRESENT та CLEFIA

Представлені в міжнародному стандарті ISO/IEC 29192-2 облегшені (Lightweight) БСШ PRESENT та CLEFIA були запропоновані для використання в спрощених застосуваннях, наприклад в смарт-картках.

БСШ CLEFIA (від фр. Clef «ключ») – алгоритм шифрування, який розроблений корпорацією Sony в якості безпечної альтернативи шифру AES для сфери захисту авторських прав і систем DRM (Digital rights management). Алгоритм складається з двох складових елементів: частини ключової обробки та частини обробки даних. Алгоритм відповідає вимогам до шифру AES:

- розмір блоку – 128 *біт* (16 *байт*);
- підтримувана довжина ключа – 128, 192 і 256 *біт*.

Алгоритм шифру побудовано на основі узагальненої структури Фейстеля, число раундів залежить від довжини ключа і становить відповідно 18, 22 або 26 раундів і 36, 44 і 52 використовуваних підключа. Раундова функція CLEFIA (рис. 1) складається з двох різних функцій F_0 та F_1, причому в першому та останньому раунді використовуються 4 забілені байти ключа. Функції F_0 та F_1 мають SP-структуру.

БСШ PRESENT це симетричний блочний шифр з 64 *бітами* блока даних та 80 (або 128) бітами блока ключа. Основне призначення цього шифру це використання у вузькоспеціалізованих приладах, наприклад, RFID міток або мереж сенсорів. Є одним з найбільш компактних криптоалгоритмів, бо за оцінкою складності в [2] для апаратної реалізації БСШ PRESENT потрібно приблизно в 2,5 рази менше логічних елементів ніж для БСШ AES або БСШ CLEFIA.

Основним критерієм при розробці БСШ PRESENT була простота реалізації при забезпеченні середніх показників захищеності. Алгоритм шифрування являє собою SP-мережу з 31 раундом перетворення (рис. 2).

Кожен раунд складається з операції XOR з раундовим ключем, що складається з 64 *біта*, які визначаються функцією оновлення ключа. Далі виконується нелінійне розсіювальне перетворення «sBoxLayer» – блок даних обробляється 16 однаковими 4-бітовими S-блоками. Потім блок даних підлягає лінійному перетворенню «pLayer» із перемішуванням (у вигляді перестановки біт).

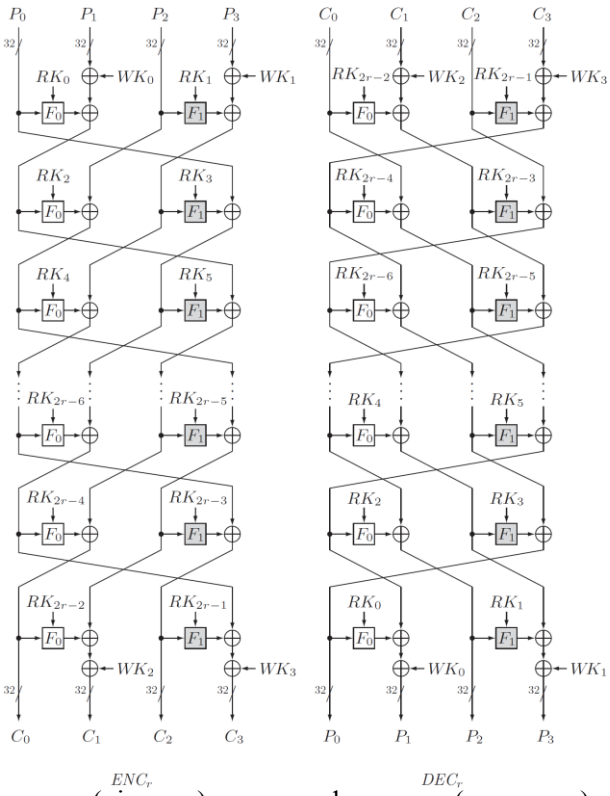

Рис. 1. Схема шифрування (ліворуч) та розшифрування (праворуч) алгоритмом CLEFIA

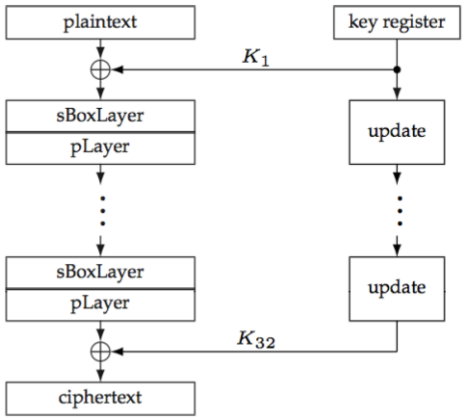

Рис. 2. Загальна схема шифрування алгоритмом PRESENT

На рис. 3 схематично наведено два раунди криптоперетворення алгоритмом PRESENT.

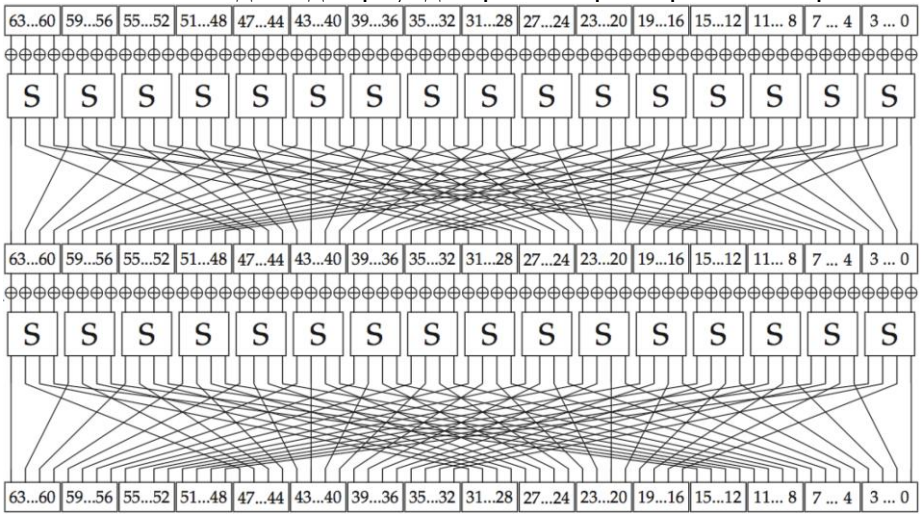

Рис. 3. Схема перетворення на двох раундах алгоритму PRESENT

Результати досліджень

Для оцінки статистичних властивостей був використаний стандартний пакет тестів NIST (188 тестів), програмні моделі шифрів PRESENT та CLEFIA в п'яти основних режимах роботи (ECB, CBC, CFB, CTR та OFB). Режими шифрування ретельно описані в міжнародному стандарті ISO/IEC 10116-2006 [6].

Сутність випробування полягала в генеруванні псевдовипадкової послідовності довжиною 10^8 бітів для кожного з шифрів та режимів, та перевірці її статистичних властивостей за допомогою тестів NIST STS. Параметри шифрів для генерування були такими:

а) для PRESENT: блок – 64 *біти*, ключ – 80 *бітів*;

б) для CLEFIA: блок – 128 *бітів*, ключ – 128 *бітів*.

Згідно [7] для оцінки результатів було прийняте наступне твердження: нехай рівень значимості α дорівнює 0.01. Послідовність буде визначена як випадкова за умови, що $P_v \geq \alpha$. Визначимо долю послідовностей, що пройшли випробування в кожному тесті, γ_i, як відношення числа послідовностей, визнаних «випадковими», до числа послідовностей, визнаних невипадковими. В нашому випадку цей показник $\gamma = 0.99$. Визначимо межі довірчого інтервалу: пропонується обмежити трьома середньоквадратичними відхиленнями, вважаючи, що розподіл результатів випробувань підпорядковується нормальному закону. Отже, $\gamma_{min\ max} = 0.99 \pm 0.0094392$.

Результати проведених статистичних досліджень наведено в табл. 1.

Таблиця 1

Результати статистичних досліджень БСШ PRESENT та CLEFIA

Кількість (доля) тестів	PRESENT				CLEFIA			
	CTR	CBC	CFB	OFB	CTR	CBC	CFB	OFB
в яких частка проходження тесту > 0,99	83 (44%)	83 (44%)	82 (44%)	83 (44%)	75 (40%)	79 (42%)	77 (40%)	76 (40%)
в яких частка проходження тесту > 0,96	185 (98%)	184 (97%)	185 (98%)	185 (98%)	181 (96%)	184 (97%)	183 (97%)	186 (98%)
в яких частка проходження тесту < 0,96	1 (0%)	1 (0%)	1 (0%)	0 (0%)	2 (1%)	0 (0%)	1 (0%)	0 (0%)
в яких значення ймовірності P<= 0,01	2 (1%)	1 (0%)	2 (1%)	1 (0%)	3 (2%)	3 (2%)	3 (2%)	3 (2%)
в яких значення ймовірності P<= 0,001	0 (0%)	0 (0%)	1 (0%)	0 (0%)	0 (0%)	1 (0%)	0 (0%)	0 (0%)
в яких значення ймовірності P<= 0,05	10 (5%)	11 (6%)	12 (6%)	10 (5%)	14 (7%)	13 (7%)	12 (6%)	12 (6%)

Для порівняння отриманих результатів із результатами проходження статистичних тестів вихідними послідовностями БСШ FIPS-197 (AES) та ГОСТ 28147-89 наведено відповідні статистичні портрети (рис. 4 – 7).

Проаналізувавши гістограми, можна зробити висновок, що послідовності, які були згенеровані спрощеними шифрами PRESENT та CLEFIA носять псевдовипадковий характер, через те, що один з тестів (Non-overlapping Template Matching Test) вони пройшли з ймовірністю 0,95 та 0,94 відповідно. Також можна зазначити, що отримані результати проходження тестів для послідовностей, які згенеровано в п'яти основних режимах застосування БСШ, є задовільними та мають також псевдовипадковий характер.

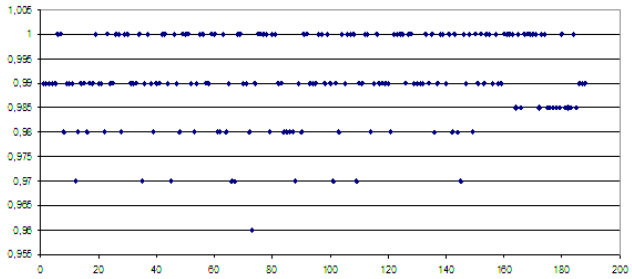

Рис. 4. Статистичний портрет БСШ FIPS-197

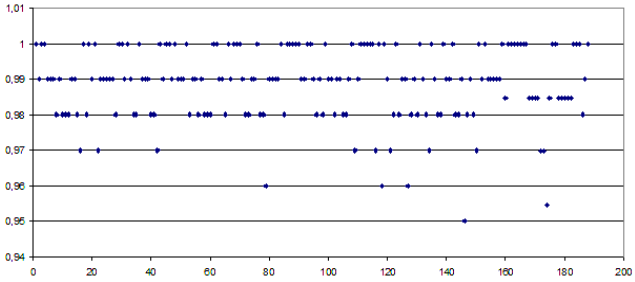

Рис. 5. Статистичний портрет БСШ ГОСТ 28147-89

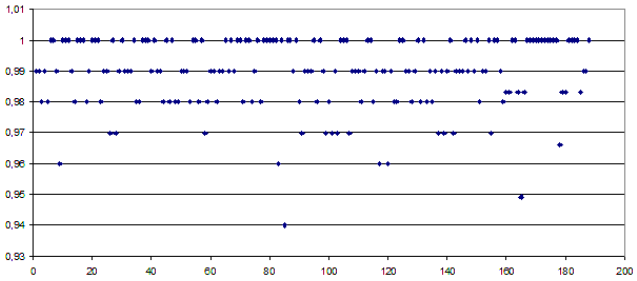

Рис. 6. Статистичний портрет БСШ CLEFIA

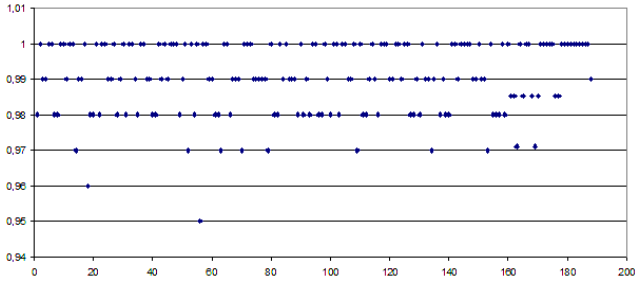

Рис. 7. Статистичний портрет БСШ PRESENT

Якщо обчислене значення ймовірності $P < 0{,}01$, тоді досліджувана двійкова послідовність не є істинно випадковою. Отже, можна відзначити, що в різних режимах шифрування для БСШ PRESENT-80 та CLEFIA-128 доля тестів, що пройшли таку характеристику дорівнює 2%. Для порівняння – шифри FIPS-197 та ГОСТ 28147-89 дають результат 0%.

Також програмно був проведений розрахунок швидкодії досліджуваних шифрів для підтвердження результатів випробувань [1]. Для дослідження були використані шифри з тими самими значеннями розмірів блоку та ключа, що й для попереднього випробування. Результати випробування наведені в табл. 2.

Таблиця 2

Результати випробування швидкодії

Шифри	FIPS-197 (enc/dec)	ГОСТ 28147 (enc/dec)	PRESENT (enc/dec)	CLEFIA (enc/dec)
Значення часу	23 (ms)	17 (ms)	7(ms)	7 (ms)

Отже, за результатами дослідження швидкодії можна зазначити, що спрощені (Lightweight) шифри реалізують процедури зашифрування та розшифрування в два рази швидше ніж визнані міжнародні стандарти (FIPS-197, ГОСТ 28147).

Таким чином, в результаті проведених досліджень статистичних властивостей та швидкодії БСШ з міжнародного стандарту ISO/IEC 29192-2 встановлено високі потенційні характеристики алгоритмів PRESENT-80 та CLEFIA-128, тобто ці шифри можуть застосовуватися в реальних криптосистемах та являють собою серйозну конкуренцію вже перевіреним рішенням.

Висновки

Аналізуючи отримані результати, можна дійти наступних висновків:

- вихідні послідовності, які сформовані за допомогою БСШ PRESENT та CLEFIA, в цілому за статистичними властивостями подібні випадковим послідовностям;
- застосування різних режимів шифрування з міжнародного стандарту ISO/IEC 10116 загалом не впливає на статистичні властивості формованих послідовностей;

- за показниками статистичної безпеки шифри з міжнародного стандарту ISO/IEC 29192-2 дещо поступаються алгоритмам FIPS-197 та ГОСТ 28147-89;
- спрощені (Lightweight) шифри реалізують процедури зашифрування та розшифрування в два рази швидше ніж визнані міжнародні стандарти (FIPS-197, ГОСТ 28147).

Перспективним напрямком подальших досліджень є розробка та теоретичне обґрунтування науково-технічних пропозицій щодо впровадження Lightweight-шифрів в національні системи захисту інформації, зокрема у вузькоспеціалізованих приладах, при використанні смарт-карток, тощо.

Список літератури: 1. *ISO/IEC 29192-2*, Information technology – Security techniques – Lightweight cryptography, Part 2: *Block* ciphers. Режим доступу: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56552**.** 2. PRESENT: An Ultra-Lightweight Block Cipher. Режим доступу: http://www.ist-ubisecsens.org/publications/present_ches2007.pdf**.** 3. *Горбенко І.Д.* Аналіз блокових симетричних шифрів міжнародного стандарту ISO/IEC 29192-2 / Горбенко І.Д., Самойлова А.В. // Прикладная радиоэлектроника. – Харьков, 2013. – Т. 12. №2. – С.247 – 249. 4. *National* Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard", November 2001. Режим доступу: http://csrc.nist.gov/publications/ fips/fips197/fips-197.pdf. 5. *ГОСТ 28147-89.* Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М. : Изд-во стандартов, 1989. – 20 с. 6. *ISO/IEC 10116*. Information technology – Security techniques – Modes of operation for an n-bit block cipher. Режим доступу: http://www.iso.org. 7. *Special* Publication 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 12.12.2013