УДК 004.056.55

І.Д. ГОРБЕНКО, д-р техн. наук, Р.І. МОРДВІНОВ

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТІЙКОСТІ СУЧАСНИХ АЛГОРИТМІВ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУВАННЯ

На сучасному етапі розвитку інформаційних технологій все більш важливими постають питання з захисту інформації в ІТС. Останні події у світі підтвердили особливу важливість протидії порушникам та спробам ведення інформаційної боротьби з метою нанесення втрат. При правильному виборі та застосуванні, згідно з вимогами криптографічних перетворень, досягається високий рівень безпеки та відповідно основні послуги – конфіденційність, цілісність, захист від НСД, доступність, неспростовність тощо. При криптографічному захисті інформації висуваються та мають бути забезпечені криптографічна стійкість, цілісність, швидкодія криптографічних перетворень та вимоги, що висуваються додатками.

Однією з важливих властивостей шифрів є нерозрізнюваність вихідної послідовності, тобто шифргама повинна мати властивості випадкової послідовності. Найбільш поширеним методом статистичного тестування є NIST STS [1]. Накопичений досвід проведення статистичного тестування показує, що кількість пройдених тестів досліджуваним генератором безпосередньо залежить від обраної вихідної послідовності криптоалгоритму. При цьому різні вихідні послідовності заданої довжини можуть давати і різні значення числа пройдених тестів, при цьому відмінності можуть бути суттєвими.

Таким чином, оцінка числа пройдених тестів може носити суб'єктивний характер, тобто результат тестування може істотно залежати від обраної вхідної послідовності і не давати об'єктивну оцінку статистичної безпеки. Для забезпечення заданої достовірності результатів статистичного тестування в даній роботі пропонується оцінювати математичне сподівання числа пройдених тестів досліджуваним генератором (криптоалгоритмом), розглядаючи при цьому кожне друге тестування як одне спостереження (досвід), тобто як конкретну реалізацію деякої випадкової величини.

Для емпіричної оцінки математичного сподівання m випадкової величини скористаємося методами теорії ймовірності та математичної статистики. Закон великих чисел у теорії ймовірностей стверджує, що вибіркове середнє (середнє арифметичне) досить великої кінцевої вибірки з фіксованого розподілу близьке до теоретичного середнього (математичного сподівання) цього розподілу. Іншими словами, завжди знайдеться така кількість випробувань, при якій з будь-якою наперед заданою ймовірністю відносна частота появи деякої події буде як завгодно мало відрізнятися від його ймовірності.

Таким чином, природною оцінкою для математичного сподівання m випадкової величини X є середнє арифметичне її спостережуваних значень (або статистичне середнє) :

$$\tilde{m} = \frac{1}{N}\sum_{i=1}^{N} X_i ,$$

де N – кількість реалізацій випадкової величини X.

Оцінка дисперсії випадкової величини X визначається виразом

$$\tilde{D} = \frac{1}{N-1}\sum_{i=1}^{N} (X_i - \tilde{m})^2 . \qquad (1)$$

Значення з (1) визначатимемо за результатами 188 статистичних тестів. Вважатимемо, що результат *j*-го тесту на *i*-му тестуванні носить імовірнісний характер, тобто результат кожного тесту є реалізація деякої випадкової величини. Згідно з центральною граничною теоремою в теорії ймовірностей [2, 3], сума досить великої кількості слабкозалежних випадкових величин, що мають приблизно однакові масштаби (жодне з доданків не домінує, не вносить в суму визначального вкладу), має розподіл, близький до нормального[4].

Беручи припущення про незалежність результатів статистичного тестування і при достатній їх кількості, при великих значеннях кількості реалізацій N середнє арифметичне $\tilde{m}$ випадкової величини X матиме розподіл, близький до нормального з математичним очікуванням:

$$m[\tilde{m}] \approx m$$

і середнім квадратичним відхиленням:

$$\sigma[\tilde{m}] \approx \frac{\sigma}{\sqrt{N}},$$

де σ – середньоквадратичне відхилення оцінюваного параметра.

При цьому імовірність того, що оцінка $\tilde{m}$ відхилиться від свого математичного очікування менше, ніж на ε (довірча ймовірність), дорівнює

$$P_\partial(|\tilde{m} - m| < \varepsilon) \approx 2\Phi\left(\frac{\varepsilon}{\sigma[\tilde{m}]}\right),$$

де $\Phi(x)$ – функція Лапласа, що визначається виразом

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt.$$

І навпаки, зафіксувавши значення довірчої ймовірності P_∂, можемо побудувати довірчий інтервал з відповідними межами:

$$\tilde{m} - t_\rho \cdot \sigma[\tilde{m}] < m < \tilde{m} + t_\rho \cdot \sigma[\tilde{m}],$$

де t_ρ – корінь рівняння $2\Phi(t_\rho) = P_\partial$.

Величина ε задає точність експериментальних даних, величину максимального відхилення отриманої оцінки від істинного значення, тобто ε є абсолютним значенням помилки у визначенні значення шуканої характеристики. При цьому довірча ймовірність P_∂ вказує на те, з якою ймовірністю задана точність ε досягається.

За допомогою описаного методу було проведено загальне тестування п'яти обраних шифрів – ДСТУ 7624:2014 (в подальшому «Калина»), ДСТУ ГОСТ 28147:2009, американського стандарту блокового симетричного шифрування (БСШ) AES, білоруського стандарту шифрування Belt та шифру Camellia. Кожен з цих шифрів проходив тестування у 10 режимах роботи, перелік яких наведено у табл. 1. Результати тестування для «Калини», ГОСТ 28147, AES, Belt та Camellia наведено у табл. 2 – 6 відповідно.

Таблиця 1

Номер режиму	Назва режиму	Позначення	Послуга безпеки
1	Проста заміна (базове перетворення)	ECB	Конфіденційність
2	Гамування	CTR	Конфіденційність
3	Гамування зі зворотним зв’язком по шифртексту	CFB	Конфіденційність
4	Вироблення імітовставки	CMAC	Цілісність
5	Зчеплення шифрблоків	CBC	Конфіденційність
6	Гамування зі зворотним зв’язком по шифргамі	OFB	Конфіденційність
7	Вибіркове гамування із прискореним виробленням імітовставки	GCM, GMAC	Конфіденційність і цілісність (GCM), тільки цілісність (GMAC)
8	Вироблення імітовставки і гамування	CCM	Цілісність і конфіденційність
9	Індексованої заміни	XTS	Конфіденційність
10	Захисту ключових даних	KW	Конфіденційність і цілісність

Для можливості порівняння отриманих оцінок було прийнято рішення використовувати найбільш близькі розміри блоків та ключів. Таким чином для ГОСТ 28147:2009 це єдино можливі параметри, а саме розмір блоку 64 біти та розмір ключа – 256 біт. Для останніх чотирьох шифрів було обрано розмір блоку, що дорівнює 128 біт та розмір ключа 256 біт.

Таблиця 2

Назва алгоритму	M099	D099	S099	P099	M096	D096	S096	P096	MIN
Kalyna_ECB	132.47	35.73	5.98	1.00	186.73	0.13	0.36	1.00	184
Kalyna_CTR	132.09	22.79	4.77	1.00	186.74	0.83	0.91	1.00	181
Kalyna_CBC	132.53	20.17	4.49	1.00	186.63	1.06	1.03	1.00	179
Kalyna_CFB	132.50	25.79	5.08	1.00	186.50	0.44	0.66	1.00	182
Kalyna_OFB	132.35	20.53	4.53	1.00	186.63	0.57	0.76	1.00	181
Kalyna_CMAC	131.62	24.72	4.97	1.00	186.79	0.51	0.71	1.00	182
Kalyna_GCM	132.35	27.86	5.28	1.00	186.81	0.51	0.72	1.00	182
Kalyna_CCM	132.09	22.79	4.77	1.00	186.74	0.83	0.91	1.00	181
Kalyna_KW	131.34	29.03	5.39	1.00	186.77	0.74	0.86	1.00	180
Kalyna_XTS	132.71	30.35	5.51	1.00	186.72	0.82	0.91	1.00	181

Таблиця 3

Назва алгоритму	M099	D099	S099	P099	M096	D096	S096	P096	MIN
GOST_ECB	131.72	34.17	5.85	1.00	186.77	1.28	1.13	1.00	178
GOST_CTR	130.62	23.71	4.87	1.00	186.88	0.88	0.94	1.00	181
GOST_CBC	131.76	21.74	4.66	1.00	186.67	0.34	0.59	1.00	182
GOST_CFB	132.07	28.30	5.32	1.00	187.02	0.15	0.39	1.00	184
GOST_OFB	131.71	31.68	5.63	1.00	186.64	2.38	1.54	1.00	176
GOST_CMAC	132.69	24.18	4.92	1.00	186.92	0.30	0.55	1.00	183
GOST_GCM	132.30	21.88	4.68	1.00	186.77	1.05	1.03	1.00	178
GOST_CCM	133.56	34.31	5.86	1.00	186.74	0.83	0.91	1.00	181
GOST_KW	133.02	26.82	5.18	1.00	186.69	0.48	0.70	1.00	182
GOST_XTS	133.77	30.64	5.54	1.00	186.82	0.48	0.69	1.00	181

Таблиця 4

Назва алгоритму	M099	D099	S099	P099	M096	D096	S096	P096	MIN
AES_ECB	132.06	19.34	4.40	1.00	186.62	0.66	0.81	1.00	181
AES_CTR	132.73	30.31	5.51	1.00	186.83	1.70	1.31	1.00	176
AES_CBC	132.31	32.30	5.68	1.00	186.89	0.29	0.54	1.00	183
AES_CFB	133.63	18.23	4.27	1.00	186.72	0.60	0.77	1.00	181
AES_OFB	131.98	29.01	5.39	1.00	186.89	0.29	0.54	1.00	183
AES_CMAC	132.82	21.35	4.62	1.00	186.78	0.84	0.92	1.00	181
AES_GCM	133.26	38.43	6.20	1.00	186.74	1.44	1.20	1.00	176
AES_CCM	131.97	15.65	3.96	1.00	186.59	0.46	0.68	1.00	182
AES_KW	133.20	30.17	5.49	1.00	186.76	0.50	0.71	1.00	182
AES_XTS	132.09	22.28	4.72	1.00	186.58	0.46	0.68	1.00	182

Таблиця 5

Назва алгоритму	M099	D099	S099	P099	M096	D096	S096	P096	MIN
Belt_ECB	132.05	31.77	5.64	1.00	186.77	0.50	0.71	1.00	182
Belt_CTR	132.20	36.18	6.02	1.00	186.63	0.47	0.69	1.00	182
Belt_CBC	133.14	21.90	4.68	1.00	186.91	0.30	0.55	1.00	183
Belt_CFB	132.53	23.73	4.87	1.00	187.07	0.16	0.40	1.00	184
Belt_OFB	131.95	22.52	4.75	1.00	186.62	0.91	0.95	1.00	180
Belt_CMAC	133.66	27.45	5.24	1.00	186.80	0.51	0.72	1.00	182
Belt_GCM	131.78	32.90	5.74	1.00	186.86	0.38	0.61	1.00	182
Belt_CCM	131.99	25.81	5.08	1.00	186.64	0.79	0.89	1.00	181
Belt_KW	132.69	27.31	5.23	1.00	186.92	0.30	0.55	1.00	183
Belt_XTS	132.15	25.93	5.09	1.00	186.71	0.49	0.70	1.00	182

Таблиця 6

Назва алгоритму	M099	D099	S099	P099	M096	D096	S096	P096	MIN
Camellia_ECB	134.05	28.96	5.38	1.00	186.78	0.47	0.68	1.00	181
Camellia_CTR	130.88	26.78	5.17	1.00	186.64	0.47	0.69	1.00	182
Camellia_CBC	131.34	36.18	6.02	1.00	186.64	0.85	0.92	1.00	179
Camellia_CFB	132.17	33.33	5.77	1.00	186.49	1.17	1.08	1.00	180
Camellia_OFB	132.12	20.79	4.56	1.00	186.74	0.46	0.68	1.00	181
Camellia_CMAC	133.57	29.55	5.44	1.00	186.78	0.47	0.68	1.00	181
Camellia_GCM	132.73	24.82	4.98	1.00	186.75	0.27	0.52	1.00	183
Camellia_CCM	132.49	31.09	5.58	1.00	186.81	0.28	0.53	1.00	183
Camellia_KW	132.99	19.79	4.45	1.00	186.72	1.28	1.13	1.00	180
Camellia_XTS	132.85	31.22	5.59	1.00	186.83	0.37	0.61	1.00	182

Значення, що описані в табл. 2 – 6:

– «Назва алгоритму» – отримані результати статистичних досліджень в ході реалізації режиму роботи БСШ у відповідному режимі з використанням розміру блоку 128 біт (64 для ГОСТ 28147) та розміру ключа 256 біт;

– «M096», «M099» – оцінки математичного сподівання (вибіркові середні) числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$ і за критерієм $P_j \geq 0{,}99$ відповідно;

– «D096», «D099» («S096», «S099») – оцінки дисперсії (середньоквадратичного відхилення) результатів тестування числа пройдених статистичних тестів за критеріями $P_j \geq 0{,}96$ і $P_j \geq 0{,}99$ відповідно;

– «P099» – розраховане значення довірчої ймовірності для числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}99$ і точності $\varepsilon = 2$;

– «P096» – розраховане значення довірчої ймовірності для числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$ і точності ε = 1;

– «MIN» – наведені мінімальні значення числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$.

Як видно з табл. 2 – 6, результати статистичних тестів, а саме математичне очікування, є приблизно однаковим для обраних БСШ, що говорить про високі показники захищеності з точки зору статистичних властивостей вихідних послідовностей, але оцінки «Калини» є кращими через те, що значення мінімального числа проходження тестів за критерієм 0.96 є вищим за інші і складає 184 проти 181 у AES та Camellia, 182 у Belt, та 178 у ГОСТ. Також значення дисперсії у «Калини» має кращі показники, що показує більшу щільність отриманих оцінок.

Список літератури: 1. *A Statistical* Test Suite for Random and Pseudorandom Number Generators for Cryptgraphic Applications : NIST SP 800-22. – [Чинний від 2011-08-01]. – Gaithersburg : Natl. Inst. Stand. Technol. 131 p. 2. *Вентцель Е.С.* Теория вероятностей : учеб. для вузов / Вентцель Е.С. – 6-е изд. стер. – М. : Высш. шк., 1999. – 576 с. 3. *Гнеденко Б.В.* Курс теории вероятностей / Гнеденко Б.В. – 8-е изд., испр. и доп. – М. : Едиториал УРСС, 2005 р. – 448 с. 4. *Чистяков В.П.* Курс теории вероятности / Чистяков В.П. – М. : Наука, 1978. – 224 с.

Харківський національний університет
імені В.Н. Каразіна

Надійшла до редколегії 14.04.2015