УДК 681.3.067

Ю. Є. Яремчук
Вінницький національний технічний університет
вул. Хмельницьке шосе 95, 21021 Вінниця, Україна

Дослідження статистичної безпеки методів цифрового підписування на основі рекурентних послідовностей

Проведено дослідження статистичної безпеки методу цифрового підписування на основі рекурентних V_k*-послідовностей і здійснено його порівняння з відомими методами Фейге-Фіата-Шаміра та Шнорра. Результати аналізу показали, що в цілому метод на основі* V_k*-послідовностей має високий рівень статистичної безпеки. Особливо це стосується малих довжин ключів, що рекомендує його для застосування, в першу чергу, в системах цифрового підписування, в яких використання великих ключів не так важливо.*

Ключові слова: *криптографія, цифрове підписування, криптостійкість, статистична безпека, рекурентні послідовності.*

Вступ

Цифрове підписування [1–3] використовується для автентифікації даних, що передаються телекомунікаційними каналами, функціонально є аналогом звичайного рукописного підпису і володіє такими його основними властивостями: посвідчує, що підписані дані надходять від особи, яка поставила підпис; не дає можливості підписанту відмовитися від зобов'язань, що пов'язані з підписаними даними; гарантує цілісність підписаних даних.

Цифровий підпис являє собою деяке число специфічної структури, яке допускає перевірку за допомогою відкритого ключа того факту, що воно було вироблено для деякого повідомлення з використанням секретного ключа.

У загальному вигляді в схемі цифрового підписування [3] існує два учасника — відправник-підписант та одержувач-перевіряльник. Відправник (або центр довіри) генерує два ключа — загальнодоступний відкритий ключ K_1 та відповідний йому секретний ключ K_2. При формуванні підпису для повідомлення M відправник обчислює цифровий підпис DS від M, використовуючи ключ K_2. При перевірці підпису одержувач перевіряє підпис DS від повідомлення M, використовуючи ключ K_1.

Цифрове підписування передбачає два етапи: формування та перевірку цифрового підпису, що реалізується за певним протоколом [1]. Серед існуючих протоколів цифрового підписування найбільшого поширення отримали ті, що реалізують рандомізовані схеми з додаванням повідомлення, зокрема це методи Шнорра [4], Фейге-Фіата-Шаміра [5], Ель-Гамаля [6], DSA [7]. Ці методи базуються на операції піднесення до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації. Крім того актуальним залишається підвищення стійкості схем цифрового підписування.

У цьому зв'язку певний інтерес викликає метод цифрового підписування [8, 9], що базується на математичному апараті рекурентних V_k-послідовностей, який, порівняно з відомими аналогами, є більш стійким і майже вдвічі забезпечує спрощення обчислень процедури перевірки підпису. Окрім того, метод має значно простішу процедуру завдання параметрів і дозволяє змінювати стійкість методу залежно від параметру k-порядку послідовності.

При цьому актуальним залишається визначення рівня практичної стійкості шляхом дослідження статистичної безпеки запропонованого в [8, 9] методу цифрового підписування та порівняння його з відомими аналогами.

Метою роботи є дослідження статистичної безпеки запропонованого в [8, 9] методу цифрового підписування на основі рекурентних V_k-послідовностей та порівняння його з відомими методами Фейге-Фіата-Шаміра та Шнорра.

Дослідження статистичної безпеки методу цифрового підписування на основі V_k-послідовностей

Для дослідження статистичної безпеки методів цифрового підписування використаємо пакет NIST STS (National Institute of Standard and Technologies Statistical Test Suite) [10], який на сьогодні є одним із кращих пакетів для статистичного тестування криптографічних схем і протоколів. Пакет NIST STS включає у себе набір з 16-ти статистичних тестів.

Дослідження методів цифрового підписування за допомогою цього пакету тестів будемо здійснювати за такою методикою [11]. Нехай задана двійкова послідовність S довжиною n бітів, тобто $S = \{S_1, S_2, \ldots, S_n\}$, $S_i \in \{0,1\}$. Для фіксованого значення n формуємо множину з m двійкових послідовностей. Сформована вибірка при цьому складатиме $N = m \times n$.

1. Далі будемо тестувати за допомогою пакету NIST STS кожну послідовність сформовану методом, у результаті якого отримаємо статистичний портрет сформованого цифрового підпису.

2. Статистичний портрет послідовності являє собою масив розмірністю $m \times q$, де m — кількість послідовностей, що тестуються; q — кількість статистичних тестів, які використовуються для тестування кожної послідовності. Елементи масиву $P_{i,j} \in [0,1]$, де $i = \overline{1,m}$, $j = \overline{1,q}$, являють собою значення ймовірності, що отримана в результаті тестування i-ї послідовності j-м тестом.

3. За отриманим статистичним портретом визначаємо долю послідовностей, які пройшли кожен статистичний тест. Для цього задають рівень значимості $\alpha \in [0{,}001; 0{,}01]$ і здійснюють підрахунок значень імовірності P, що перевищує заданий рівень α для кожного з q тестів. У результаті формується вектор коефіцієнтів $R = \{r_1, r_2, ..., r_q\}$, елементи якого характеризують у процентному співвідношенні проходження послідовності S_i усіх статистичних тестів. Після цього здійснюється статистичний аналіз статистичного портрету. Отримані значення ймовірностей P_{ij} повинні задовольняти рівномірному закону розподілу на інтервалі $[0,1]$.

Заключний висновок щодо методу цифрового підписування будемо приймати таким чином. Будемо вважати, що метод цифрового підписування G пройшов статистичне тестування пакетом NIST STS, якщо значення коефіцієнтів r_j для усіх $j = \overline{1,q}$ знаходяться всередині довірчого інтервалу $[r_{\min}, r_{\max}]$, де

$$r_{\max(\min)} = (1-\alpha) \pm 3\sqrt{\frac{\alpha(1-\alpha)}{m}}, \qquad (1)$$

і дотримується умова $\chi^2 > 0{,}0001$ для усіх $j = \overline{1,q}$, де χ^2 — критерій підкорення результатів рівномірному закону розподілу на інтервалі $[0,1]$.

Методи цифрового підписування вимагають використання різного роду однонаправлених хеш-функцій. На сьогодні методи хешування дозволяють створювати хеш-значення розміром до 512 бітів, а саме 128 бітів (MD5), 160 бітів (SHA1), 256 бітів (SHA256), 384 бітів (SHA384) та 512 бітів (SHA512). Тестування будемо проводити для усіх перерахованих довжин хеш-значень.

Довжина результуючих цифрових підписів, що відповідає даним розмірам ключів, дозволяє виконувати тестування лише для 10 тестів пакету NIST STS, що виключає тест на перевірку рангу двійкової матриці, тест на перевірку шаблонів, що перекриваються, універсальний тест Маурера, тест на перевірку лінійної складності, тест на перевірку випадкових відхилень і модифікований тест на перевірку випадкових відхилень, так як необхідна довжина послідовностей, що проходять тестування, є недостатньою для успішного проходження чи отримання достовірних результатів даних тестів.

Для виконання тестування було обрано такі параметри:

— довжина послідовності, яка тестується — від 128 до 1536 бітів залежно від довжини ключа та методу;

— кількість послідовностей, які тестуються, для кожної довжини ключа, $m = 100$;

— кількість тестів $q = 158$;

— рівень значимості $\alpha = 0{,}001$ та $\alpha = 0{,}01$ відповідно у першому та другому експериментах.

Таким чином, маємо: об’єм вибірки від 128 до 1536 бітів для тестування кожного методу цифрового підписування. Статистичний портрет коду для кожної довжини ключа буде вміщувати у собі від 12800 до 153600 значень імовірності P.

Вибір додаткових параметрів зроблено відповідно до рекомендацій, що описані в NIST STS [10].

На основі цих початкових даних проаналізуємо отримані результати тестування послідовностей. У табл. 1 і 2 наводяться дані про проходження результуючих послідовностей з розміром ключів 128–512 бітів відповідно усіма тестами згідно описаної методики.

Таблиця 1. Результати тестування методів цифрового підписування для $\alpha = 0{,}01$ та різних довжин ключів

Метод	Кількість тестів, які успішно пройшли тестування більше 99 % послідовностей					Кількість тестів, які успішно пройшли тестування більше 96 % послідовностей				
	128 бітів	160 бітів	256 бітів	384 бітів	512 бітів	128 бітів	160 бітів	256 бітів	384 бітів	512 бітів
V_k	5 (3,16 %)	2 (1,27%)	6 (3,80 %)	10 (6,33 %)	8 (5,06 %)	97 (61,39 %)	25 (15,82 %)	30 (18,99 %)	98 (62,03 %)	62 (39,24 %)
Фейге-Фіата-Шаміра	2 (1,27 %)	5 (3,16 %)	6 (3,80 %)	10 (6,33 %)	8 (5,06 %)	34 (21,52 %)	27 (17,09 %)	66 (41,77%)	100 (63,29 %)	91 (57,59 %)
Шнорра	7 (4,43 %)	5 (3,16 %)	5 (3,16%)	7 (4,43 %)	4 (2,53 %)	82 (51,90 %)	74 (46,84 %)	69 (43,67 %)	79 (50,00 %)	60 (37,97 %)

Таблиця 2. Результати тестування методів цифрового підписування для $\alpha = 0{,}01$ та різних довжин ключів

Метод	Кількість тестів, які успішно пройшли тестування більше 99 % послідовностей					Кількість тестів, які успішно пройшли тестування більше 98 % послідовностей				
	128 бітів	160 бітів	256 бітів	384 бітів	512 бітів	128 бітів	160 бітів	256 бітів	384 бітів	512 бітів
V_k	15 (9,49 %)	13 (8,23 %)	20 (12,66 %)	26 (16,46 %)	43 (27,22 %)	37 (23,42 %)	37 (23,42 %)	42 (26,58 %)	67 (42,41 %)	111 (70,25 %)
Фейге-Фіата-Шаміра	13 (8,23 %)	41 (25,95 %)	31 (19,62 %)	50 (31,65 %)	62 (39,24 %)	29 (18,35 %)	99 (62,66 %)	67 (42,41 %)	99 (62,66 %)	126 (79,75 %)
Шнорра	37 (23,42 %)	29 (18,35 %)	24 (15,19 %)	24 (15,19 %)	18 (11,39%)	83 (52,53 %)	64 (40,51 %)	66 (41,77 %)	73 (46,20 %)	61 (38,61 %)

З табл. 1 та 2 видно, що, якщо на початку послідовності Шнорра мали більші відсотки, то, починаючи з довжини ключа у 256 бітів, метод на основі V_k-послідовностей отримує значну перевагу, особливо при тестуванні в найжорсткіших умовах (5 % проти 2,5 %, 4 % проти 6 %). При рівні значимості $\alpha = 0{,}01$ різниця зменшується зі зростанням розміру ключа (від 30 % до 2 %). В усіх інших випадках зі зростанням розміру ключа зростає і різниця у кількості тестів, які метод на основі V_k-послідовностей проходить більше, порівняно з методом Шнорра. Метод Фейге-Фіата-Шаміра на малій довжині ключа (128 бітів) отримує значно менші результати (у 2,5 рази) з найжорсткішим порогом проходження, проте зі збільшенням ключа, метод починає показувати найвищі результати, отримуючи спочатку однаковий результат з методом Шнорра (довжина ключа 160 бітів), а потім з методом на основі V_k-послідовностей. При інших рівнях значимості метод тримає середні позиції.

Порівняємо результати з рівнем значимості $\alpha = 0{,}001$ за приведеною методикою. В табл. 3 наведено результати порівняння для різних довжин ключів.

Таблиця 3. Відсотки проходження кожного з 10 тестів для $\alpha = 0{,}01$ та різних довжин ключів

№ тесту	Назва статистичного тесту	128 бітів			160 бітів			256 бітів			384 бітів			512 бітів	
		V_k	**Ф-Ф-Ш**	**Ш**	V_k	**Ф-Ф-Ш**	**Ш**	V_k	**Ф-Ф-Ш**	**Ш**	V_k	**Ф-Ф-Ш**	**Ш**	V_k	**Ф-Ф-Ш**	**Ш**
1	Частотний (монобітний) тест	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	99 %	100 %
2	Частотний тест всередині блоку	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	99 %	100 %
3	Послідовний тест	100 %	99 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	99 %	100 %
4	Перевірка максимальної довжини серії в блоці	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %
5	Спектральний тест на основі дискретного перетворення Фур'є	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	99 %	100 %	100 %	99 %	100 %	99 %
6	Перевірка шаблонів, які не перекриваються	97 %	96 %	98 %	97 %	98 %	98 %	97 %	98 %	98 %	98 %	99 %	98 %	99 %	99 %	98 %
7	Перевірка серій	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %
8	Ентропійний тест	100 %	100 %	100 %	100 %	99 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %
9	Перевірка накоплених сум	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	99 %	100 %	100 %	100 %	99 %	100 %
10	Перевірка стиснення за алгоритмом Лемпеля-Зіва	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	99 %	100 %

Як видно з результатів, наведених у табл. 3, для ключів розміром 128, 160 та 256 бітів ми маємо однакову картину проходження тестів: майже в усіх тестах і метод на основі V_k-послідовностей, і метод Шнорра мають найвищі (100 %) показники. Метод Фейге-Фіата-Шаміра отримує трошки нижчі показники, проте все одно загальна картина залишається на високому рівні. Виключенням є тест на перевірку шаблонів, які не перекриваються, в якому метод на основі V_k-послідовностей та метод Фейге-Фіата-Шаміра має трошки гірші результати (98 % порівняно з 99 %) ніж метод Шнорра. Починаючи з довжини ключа 384 бітів, показники метода на основі V_k-послідовностей за спектральним тестом і тестом перевірки шаблонів погіршуються, і стають рівними показникам методу Шнорра і методу Фейге-Фіата-Шаміра, проте показник за тестом на перевірку шаблонів, які не перекриваються, зростає до показників інших методів.

Порівняємо коди, збільшивши рівень значимості $\alpha = 0{,}01$, що є більш жорстким підходом до оцінки за приведеною методикою. В табл. 4 наведено результати порівняння для різних довжин ключів.

Таблиця 4. Відсотки проходження кожного з 10 тестів для $\alpha = 0{,}01$ та різних довжин ключів

№ тесту	Назва статистичного тесту	128 бітів			160 бітів			256 бітів			384 бітів			512 бітів		
		V_k	Ф-Ф-Ш	Ш	V_k	Ф-Ф-Ш	Ш	V_k	Ф-Ф-Ш	Ш	V_k	Ф-Ф-Ш	Ш	V_k	Ф-Ф-Ш	Ш
1	Частотний (монобітний) тест	98 %	98 %	100 %	99 %	99 %	99 %	100 %	99 %	99 %	97 %	100 %	100 %	100 %	99 %	98 %
2	Частотний тест всередині блоку	98 %	98 %	99 %	99 %	98 %	100 %	99 %	100 %	100 %	99 %	98 %	98 %	100 %	97 %	100 %
3	Послідовний тест	97 %	97 %	97 %	100 %	99 %	100 %	99 %	100 %	99 %	99 %	99 %	99 %	100 %	99 %	100 %
4	Перевірка максимальної довжини серії в блоці	98 %	99 %	98 %	99 %	97 %	99 %	100 %	99 %	100 %	99 %	100 %	100 %	100 %	97 %	98 %
5	Спектральний тест на основі дискретного перетворення Фур'є	99 %	99 %	100 %	98 %	99 %	97 %	98 %	98 %	98 %	99 %	98 %	98 %	98 %	98 %	96 %
6	Перевірка шаблонів, які не перекриваються	97 %	94 %	96 %	94 %	93 %	96 %	94 %	96 %	96 %	97 %	97 %	96 %	96 %	97 %	96 %
7	Перевірка серій	99 %	100 %	100 %	99 %	99 %	99 %	99 %	100 %	99 %	100 %	99 %	99 %	99 %	99 %	97 %
8	Ентропійний тест	97 %	99 %	100 %	100 %	99 %	99 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %
9	Перевірка накоплених сум	98 %	97 %	100 %	99 %	99 %	99 %	100 %	100 %	99 %	97 %	100 %	100 %	97 %	99 %	98 %
10	Перевірка стиснення за алгоритмом Лемпеля-Зіва	98 %	98 %	100 %	99 %	99 %	99 %	100 %	99 %	99 %	97 %	100 %	100 %	100 %	99 %	98 %

З результатів, наведених у табл. 4 видно, що зі збільшенням рівня значимості, показники стають доволі різноманітними, і загалом при малих довжинах ключів виграє метод Шнорра, проте вже на довжині 256 бітів можна бачити майже однакові результати проходження, а починаючи з довжини 384 бітів, метод на основі V_k-послідовностей починає випереджати метод Шнорра, особливо це помітно при довжині ключа у 512 бітів, коли метод випереджає майже за усіма тестами, отримуючи високі відсотки проходження (96–100 %). Показники методу Фейге-Фіата-Шаміра постійно коливаються між методом Шнорра та методом на основі V_k-послідовностей, отримуючи схожі оцінки то з першим, то з другим методом. Виключенням є тільки тест перевірки накоплених сум, у якому метод на основі V_k-послідовностей отримав менший показник (97 % порівняно з 98 %) ніж метод Шнорра, а метод Фейге-Фіата-Шаміра отримав найвищий результат (99 %). Загалом можна зробити висновок, що запропонований метод цифрового підписування більш статистично стійкий і показує кращі показники для малих довжин ключів.

На рис. 1–3 представлено статистичні портрети методів цифрового підписування для довжини ключа 128 бітів з указанням їхніх параметрів і способів формування.

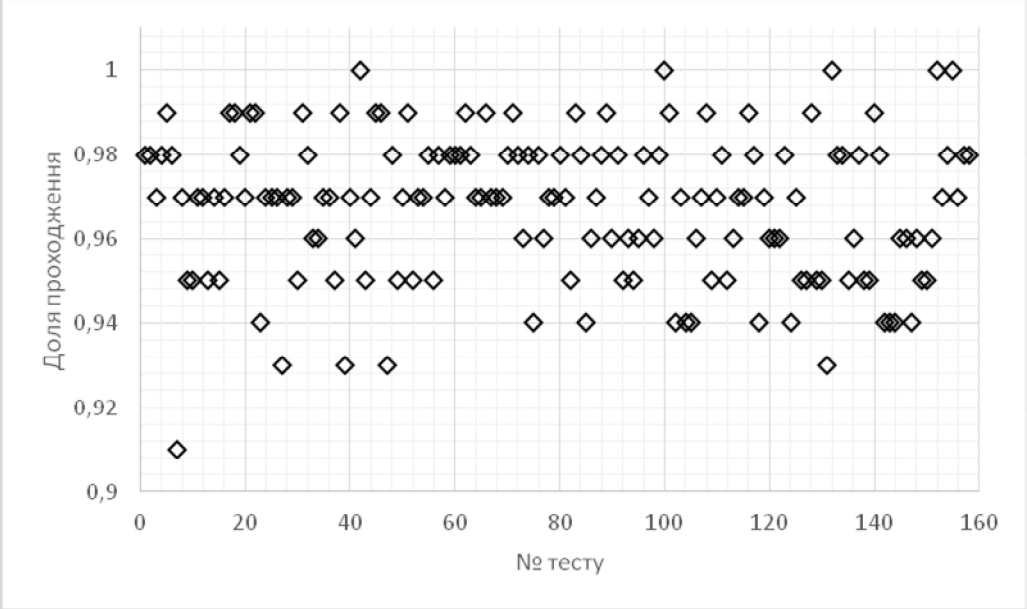

Рис. 1. Результати тестування методу цифрового підписування на основі V_k -послідовностей з розміром ключа 128 бітів

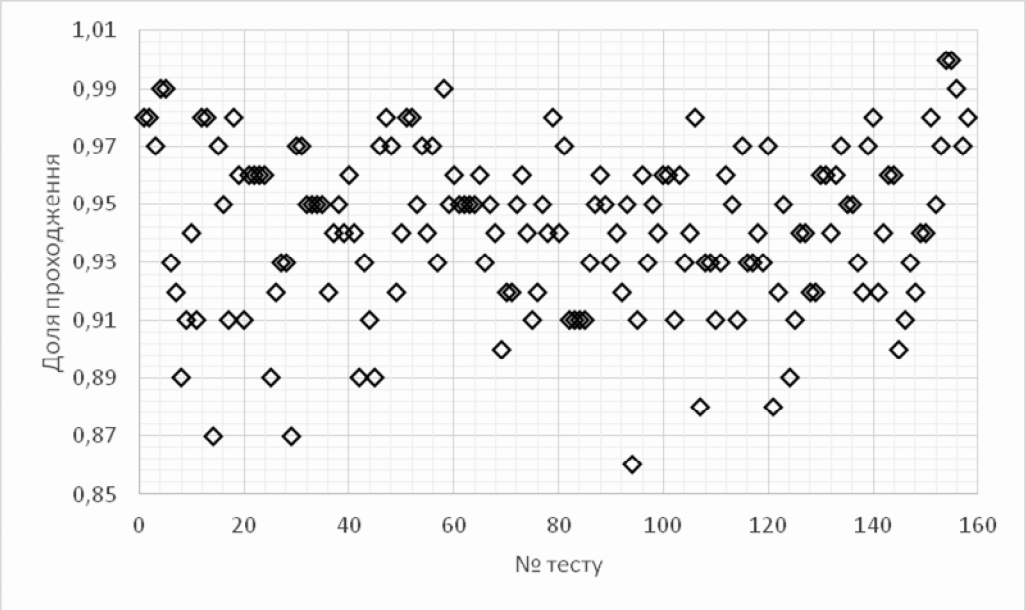

Рис. 2. Результати тестування методу цифрового підписування на основі Фейге-Фіата-Шаміра з розміром ключа 128 бітів

Також отримано статистичні портрети результатів тестування методів цифрового підписування для довжин ключа 160, 256, 384 та 512 бітів.

Як показують отримані статистичні портрети, методи загалом знаходяться на високому рівні (0,9 і вище). Менше 2 % послідовностей мають показники нижче 0,9, що є чудовим показником статистичної безпеки методів. У той же час метод на основі V_k -послідовностей виглядає більш скучкованим, що добре впливає на загальну властивість стійкості підпису до розшифрування криптоаналітиком.

Портрети показують, що при довжині ключа 128 бітів більшість тестів мають відсоток у діапазоні 0,94–0,99, у той час як метод Фейге-Фіата-Шаміра розмістився у діапазоні 0,89–0,97, а метод Шнорра має розріджену картину, яка знаходиться у діапазоні 0,92–0,99. При довжині ключа у 160 бітів найвижчий діапазон показав метод Шнорра (0,93–0,99), за ним іде метод на основі V_k-послідовностей (0,91–0,99), а найгірші показники отримав метод Фейге-Фіата-Шаміра (0,89–0,99). При довжині ключа у 256 бітів, показники методів розмістились у діапазоні 0,92–0,99, показуючи практично майже однакові нижні пороги діапазону (0,91, 0,93, 0,93 відповідно для методів на основі V_k-послідовностей, Фейге-Фіата-Шаміра та Шнорра). Для довжини ключа у 384 бітів більш нижні пороги отримали методи на основі V_k-послідовностей та Фейге-Фіата-Шаміра (0,94), за ними йде метод Шнорра (0,93). При довжині ключа у 512 бітів найкращий нижній поріг отримав метод на основі V_k-послідовностей (0,93), а методи Фейге-Фіата-Шаміра та Шнорра отримали нижчий результат (0,92). У цілому, аналізуючи портрети, можна зробити висновок, що метод на основі V_k-послідовностей найкраще себе показує при малій довжині ключа.

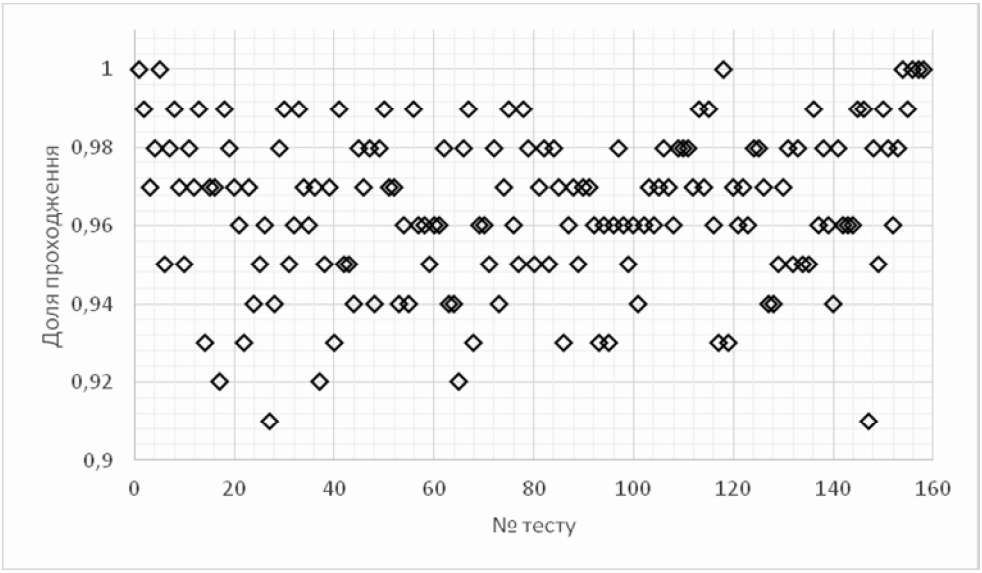

Рис. 3. Результати тестування методу цифрового підписування Шнорра з розміром ключа 128 бітів

Узагальнимо результати тестування, показавши частку проходження для кожного тесту з статистичного пакету NIST. На рис. 4–8 показано узагальнені графіки по кожному тесту для кожного методу цифрового підписування та довжини ключа.

Як видно з графіків (рис. 4), за певними тестами методи мають однакові показники. Зокрема, однакові оцінки методи отримали за тестом на перевірку максимальної довжини серії в блоці (0,98) та за тестом на послідовність (0,97). Метод Шнорра має вищі показники за такими тестами як ентропійний тест (на 0,03 більше), перевірка накоплених сум, перевірка стиснення за алгоритмом Лемпеля-Зіва та частотний тест (на 0,02 більший), перевірка серій (на 0,005 більший), спект-

ральний тест та частотний тест всередині блоку (на 0,01 більший). Метод Фейге-Фіата-Шаміра отримує середні показники, показуючи найгірші результати за тестом на перевірку шаблонів, які не перекриваються, отримуючи однакові результати з методом на основі V_k-послідовностей за спектральним, частотним тестами, а також за частотним тестом всередині блоку. В той же час останній метод має вищі показники за тестом на перевірку шаблонів, що не перекриваються.

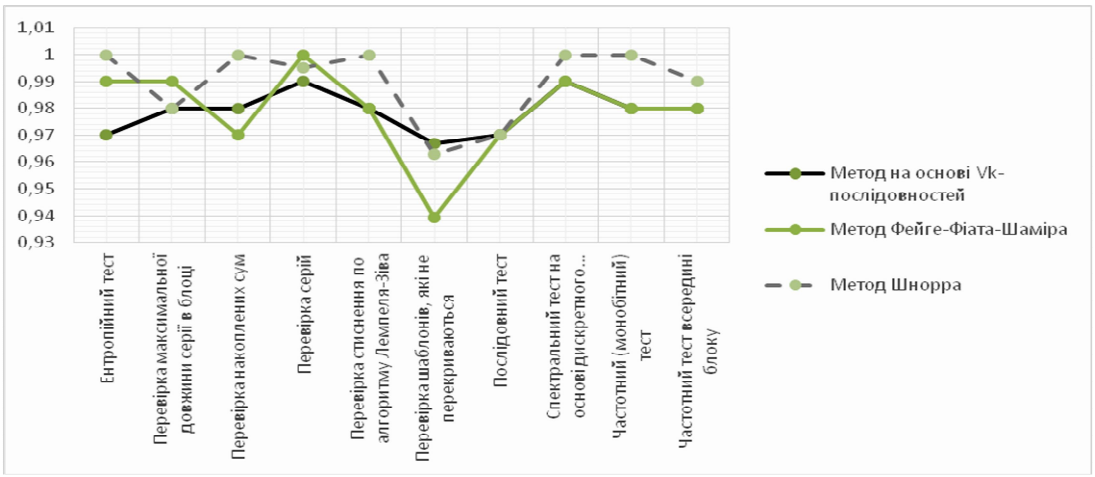

Рис. 4. Частка проходження тестів для послідовностей з розміром ключа 128 бітів

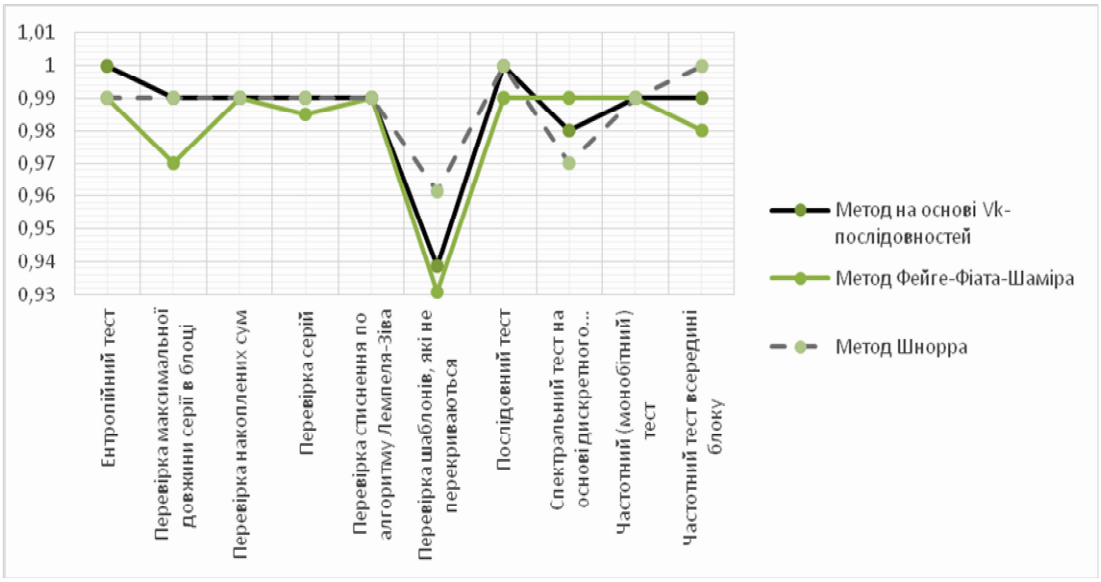

Рис. 5. Частка проходження тестів для послідовностей з розміром ключа 160 бітів

Як видно з рис. 5, при збільшені довжини ключа графіки починають йти до збігання. Так уже метод Шнорра випереджає лише в тесті на перевірку шаблонів, що не перекриваються (на 0,02), ентропійному та спектральному тесті (на 0,01). За всіма іншими тестами показники методу на основі V_k-послідовностей або рівні, або випереджають (на 0,01). Метод Фейге-Фіата-Шаміра має приблизно однакові

результати з методом Шнорра, отримуючи нижчий результат у тесті на перевірку максимальної довжини серії в блоці і вищу в спектральному тесті.

При довжині ключа у 256 бітів (рис. 6) все більше тестів за методом на основі V_k-послідовностей отримують вищі показники, ніж за методом Шнорра. Так метод Шнорра випереджає за тестом на перевірку шаблонів і за частотним тестом всередині блоку і має однакові результати за ентропійним, спектральним і послідовним тестами. В усіх випадках він відстає від методу на основі V_k-послідовностей (на 0,01 пункт). Метод Фейге-Фіата-Шаміра знову майже повторює результати метода Шнорра. Виключенням є послідовний тест і тести перевірки серій та накоплених сум, де метод отримав кращі результати та тест на перевірку максимальної довжини серії в блоці, де він отримав нижчий результат. Загалом видно, що метод на основі V_k-послідовностей лідирує за показниками.

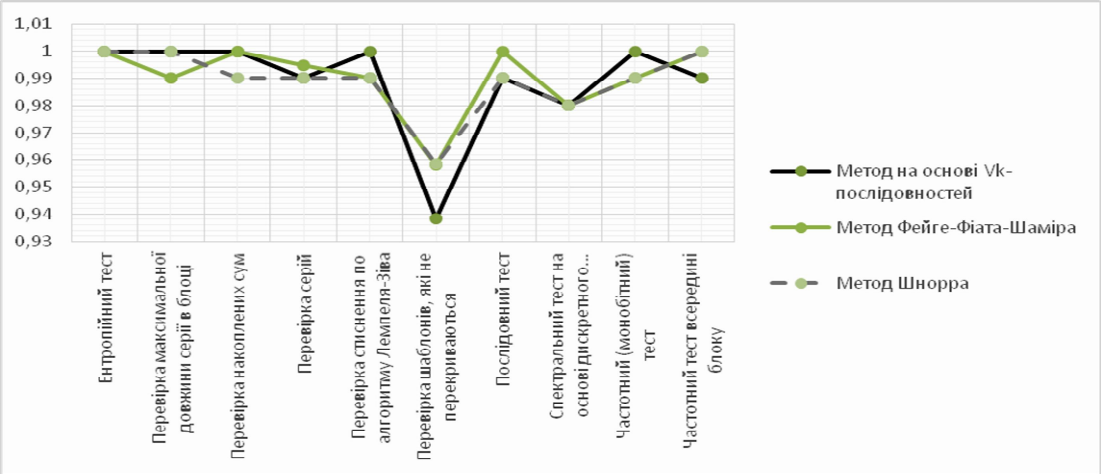

Рис. 6. Частка проходження тестів для послідовностей з розміром ключа 256 бітів

При довжині у 384 біти (рис. 7) пріоритет знову отримує метод Шнорра, хоча він отримує гірші показники, ніж метод на основі V_k-послідовностей, за тестами на перевірку серій, перевірку шаблонів, спектральному та частотному тестах, тесті всередині блоку в середньому на 0,01. Метод Фейге-Фіата-Шаміра практично повністю повторює показники методу Шнорра, отримуючи вищий показник (на 0,01) у тесті на перевірку шаблонів, які не перекриваються.

При найбільшій довжині ключа (рис. 8) «перемогу» знову отримує метод на основі V_k-послідовностей, випереджаючи метод Шнорра у 50 % тестів, ще 40 % мають однаковий результат, і лише тест на перевірку накоплених сум метод Шнорра пройшов на 0,01 краще, ніж метод на основі V_k-послідовностей. При цій довжині ключа, метод Фейге-Фіата-Шаміра отримав кращі результати порівняно з методом Шнорра за тестами на перевірку накоплених сум, перевірку серій, перевірку стиснення за алгоритмом Лемпеля-Зіва, перевірку шаблонів, які не перекриваються, спектральному та частотному тестах. Метод отримав однакові результа-

ти з методом на основі V_k-послідовностей у спектральному тесті, а з методом Шнорра в ентропійному тесті. В усіх інших він програє методу Шнорра.

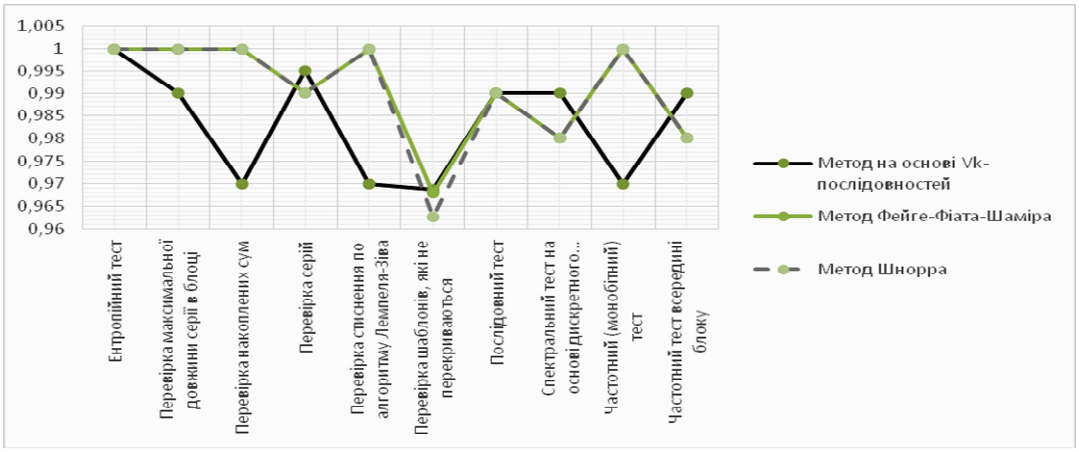

Рис. 7. Частка проходження тестів для послідовностей з розміром ключа 384 бітів

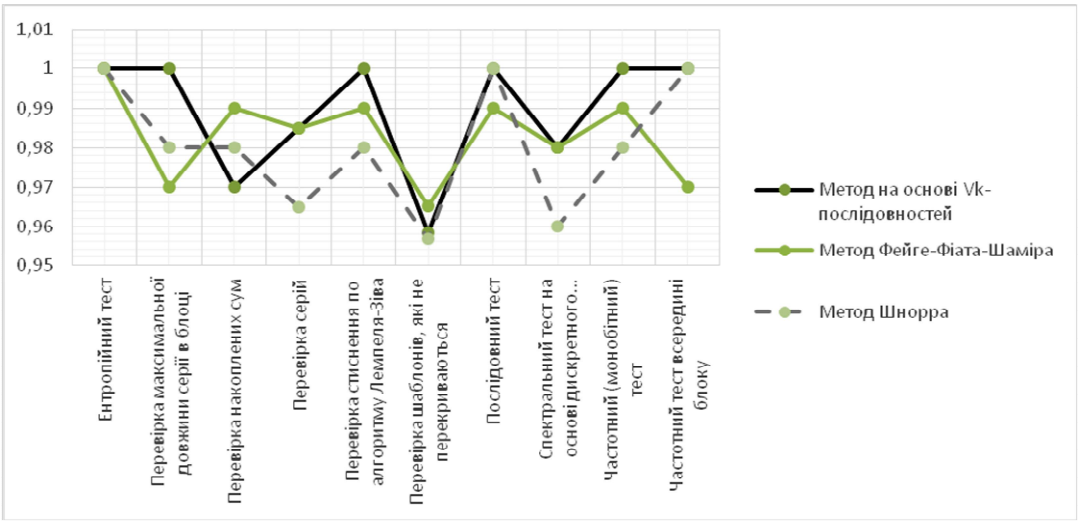

Рис. 8. Частка проходження тестів для послідовностей з розміром ключа 512 бітів

Висновки

Дослідження статистичної безпеки запропонованого в [8, 9] методу цифрового підписування на основі V_k-послідовностей порівняно з існуючими методами цифрового підписування Шнорра та Фейге-Фіата-Шаміра в цілому показало високий рівень його стійкості.

При довжині ключа у 128 бітів і найжорсткіших умовах тестування запропонований метод програє методу Шнорра на 0,73 %, проте випереджає метод Фейге-Фіата-Шаміра у 2,5 рази. Однак, починаючи з довжини ключа у 256 бітів, запропонований метод починає отримувати кращі показники і вже при довжині у 512 бітів він вдвічі випереджає існуючий аналог метод Шнорра.

При порівнянні за кожним тестом і рівнем значимості $\alpha = 0{,}001$ можна побачити, що метод на основі V_k-послідовностей має вищі показники вже з найменших довжин ключів, хоча при збільшенні довжини ключа ці показники вирівнюються, показуючи, що метод гарні можливості для використання при менших довжинах ключів.

При збільшенні рівня значимості до $\alpha = 0{,}01$ показники методу на основі V_k-послідовностей зменшуються і протягом збільшення ключа отримують однакові показники (97–100 %) з методами цифрового підписування Шнорра та Фейге-Фіата-Шаміра.

Отримано статистичні портрети, які у цілому виглядають однаково для методів, що досліджувались, і знаходяться на високому рівні (0,9 і вище), і лише менше 2 % послідовностей мають показники нижче 0,9. При цьому метод на основі V_k-послідовностей має більшу кучність частот, що є показовою складовою для статистичної безпеки. Загалом метод на основі V_k-послідовностей показує себе з кращого боку, так як діапазон його портретів вищий за діапазон інших методів (0,91–0,99 порівняно з 0,89–0,98 та 0,9–0,99).

Загальні графіки показуються, що кращим є метод на основі V_k-послідовностей при довжині ключа 384 бітів і 512 бітів. При цьому запропонований метод отримує або вищі, або приблизно однакові показники за усіма тестами. При інших довжинах ключів більшість тестів успішніше проходить саме метод Шнорра, проте цей виграш не є значним. Метод Фейге-Фіата-Шаміра майже повторює метод Шнорра, лише в деяких місцях випереджаючи чи відстаючи від нього на незначну дельту.

Загалом можна сказати, що запропонований метод цифрового підписування на основі V_k-послідовностей показує високий рівень статистичної безпеки і є чудовим замінником існуючих аналогів при довжинах ключів у 128–256 біт.

1. *Menezes A.J.* Handbook of Applied Cryptography [Текст] / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. — CRC Press, 2001. — 816 p.

2. *Молдавян Н.А.* Теоретический минимум и алгоритмы цифровой подписи [Текст] / Н.А. Молдавян. — СПб.: БХВ-Петербург, 2010. — 304 с.

3. *Введение* в криптографию [Текст] / под общ. ред. В.Б. Ященко. — М.: МЦНМО: «ЧеРо», 2000. — 236 с.

4. *Schnorr C.P.* Efficient Signature Generation for Smart Cards [Текст] / C.P. Schnorr // Advances CRYPTO '89 Proceedings. — Springer-Verlag, 1990. — P. 239–252.

5. *Feige U.* Zero Knowledge Proofs of Identity [Текст] / U. Feige, A. Fiat, A. Shamir // Proceedings of the lPth Annual ACM Symposium on the Theory of Computing, 1987. — P. 210–217.

6. *ElGamal T.* A Public-Key Cryptosystcm and a Signature Scheme Based on Discrete Logarithms [Текст] / T. ElGamal // Advances in Cryptology: Proceedings of CRYPTO 84. — Springer Verlag, 1985. — P. 1–18.

7. *National* Institute of Standards and Technology, NIST FIPS PUB 186, «Digital Signature Standard». — U.S. Department of Commerce, May 1994.

8. *Патент* України на корисну модель № 84274, (51) МПК (2013.01) H03M 13/00. Спосіб формування та перевіряння цифрового підпису у вигляді електронного коду на основі рекурентних послідовностей / Ю.Є. Яремчук: № u2013 06322; заявл. 22.05.2013; опубл. 10.10.2013, бюл. № 19.

9. *Яремчук Ю.Є.* Метод цифрового підписування на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Інформаційна безпека. — 2013. — № 1. — С. 165–175.

10. *NIST* SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo. — National Institute of Standards and Technology, 2010. — 131 p.

11. *Иванов, М.А.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей [Текст] / М.А. Иванов, И.В. Чугунков. — М.: КУДИЦ-ОБРАЗ, 2003. — 240 с.

Надійшла до редакції 11.06.2014