ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056+511.176

Ю.Є. ЯРЕМЧУК, канд. техн. наук

АНАЛІЗ СТАТИСТИЧНОЇ БЕЗПЕКИ СХЕМИ ЦИФРОВОГО ПІДПИСУВАННЯ НА ОСНОВІ Vk-ПОСЛІДОВНОСТЕЙ

Вступ

У схемі цифрового підписування [1] 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. Серед схем цифрового підписування найбільшого поширення отримали рандомізовані схеми з додаванням повідомлення, зокрема Ель-Гамаля, Шнорра, DSA, ГОСТ 34.10 [1, 2]

У роботі [3] представлено схему цифрового підписування, що базується на математичному апараті рекурентних V_k-послідовностей. У порівнянні з відомими схемами цифрового підписування запропонований метод є більш стійким, оскільки в ньому обчислення і передавання одержувачу частин s цифрового підпису здійснюється не як чисел-індексів або чисел-степенів, а як елементи рекурентної V_k-послідовності для значень цих індексів.

У роботі [4] проведено дослідження статистичної безпеки представленої у [3] схеми цифрового підписування, однак актуальним залишається питання більш детального аналізу статистичної безпеки цієї схеми для великих розмірів ключа, зокрема у 512 розрядів, оскільки розвиток обчислювальної техніки для збільшення стійкості вимагає постійного збільшення розміру чисел, над якими виконуються криптографічні перетворення.

Метою роботи є проведення аналізу статистичної безпеки представленої у [3] схеми цифрового підписування на основі рекурентних V_k-послідовностей для розміру ключа 512 розрядів у порівнянні з відомими схемами Фейге – Фіата – Шаміра та Шнорра.

Оцінювання статистичної безпеки схеми цифрового підписування для довжини ключа 512 розрядів

Для дослідження статистичної безпеки асиметричних криптоалгоритмів використано пакет NIST STS [5], який включає у себе набір з 16 статистичних тестів. Однак для розміру ключа у 512 бітів можливим є виконання тестування лише для 10 тестів, 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 та 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.

У табл. 1 наведено дані про проходження результуючих послідовностей схемами цифрового підписування на основі V_k-послідовностей та Фейге – Фіата – Шаміра і Шнорра для довжини ключа 512 бітів.

З табл. 1 видно, що схема на основі V_k –послідовностей дещо відстає від показників схеми Фейге – Фіата – Шаміра, однак при цьому схема отримує значну перевагу перед схемою Шнорра.

Таблиця 1

Кількість тестів, що пройшли успішне тестування для ключа у 512 бітів

Метод	для $\alpha = 0{,}01$		для $\alpha = 0{,}001$	
	більше 99% послідовностей	більше 96% послідовностей	більше 99% послідовностей	більше 98% послідовностей
V_k	8 (5,06%)	62 (39,24%)	43 (27,22%)	111 (70,25%)
Фейге – Фіата – Шаміра	8 (5,06%)	91 (57,59%)	62 (39,24%)	126 (79,75%)
Шнорра	4 (2,53%)	60 (37,97%)	18 (11,39%)	61 (38,61%)

У табл. 2 наведено відсотки проходження кожного з 10 тестів для $\alpha = 0{,}001$ та $\alpha = 0{,}01$ для довжини ключа 512 розрядів.

Таблиця 2

Відсотки проходження кожного з 10 тестів для довжини ключа 512 бітів

Номер тесту	Назва статистичного тесту	для $\alpha = 0{,}001$			для $\alpha = 0{,}01$		
		V_k	Ф-Ф-Ш	Ш	V_k	Ф-Ф-Ш	Ш
1	Частотний (монобітний) тест	100%	99%	100%	100%	99%	98%
2	Частотний тест всередині блоку	100%	99%	100%	100%	97%	100%
3	Послідовний тест	100%	99%	100%	100%	99%	100%
4	Перевірка максимальної довжини серії в блоці	100%	100%	100%	100%	97%	98%
5	Спектральний тест на основі дискр. перетв. Фур'є	99%	100%	99%	98%	98%	96%
6	Перевірка шаблонів, які не перекриваються	99%	99%	98%	96%	97%	96%
7	Перевірка серій	100%	100%	100%	99%	99%	97%
8	Ентропійний тест	100%	100%	100%	100%	100%	100%
9	Перевірка накоплених сум	100%	99%	100%	97%	99%	98%
10	Перевірка стиснення за алгоритмом Лемпеля – Зіва	100%	99%	100%	100%	99%	98%

Як видно з результатів, наведених у табл. 2, схема на основі V_k -послідовностей має вищі показники статистичної безпеки майже за усіма тестами, отримуючи високі відсотки проходження (96 – 100 %). Особливо це спостерігається для рівня значимості $\alpha = 0{,}01$, де схема на основі рекурентних послідовностей програє відомим методам за тестом на перевірку накоплених сум, причому лише на 1 – 2 %, і ще 1 % схема програє схемі Фейге – Фіата – Шаміра за тестом перевірки шаблонів, які не перекриваються.

На рис. 1 – 3 представлено статистичні портрети схем цифрового підписування для довжини ключа 512 бітів.

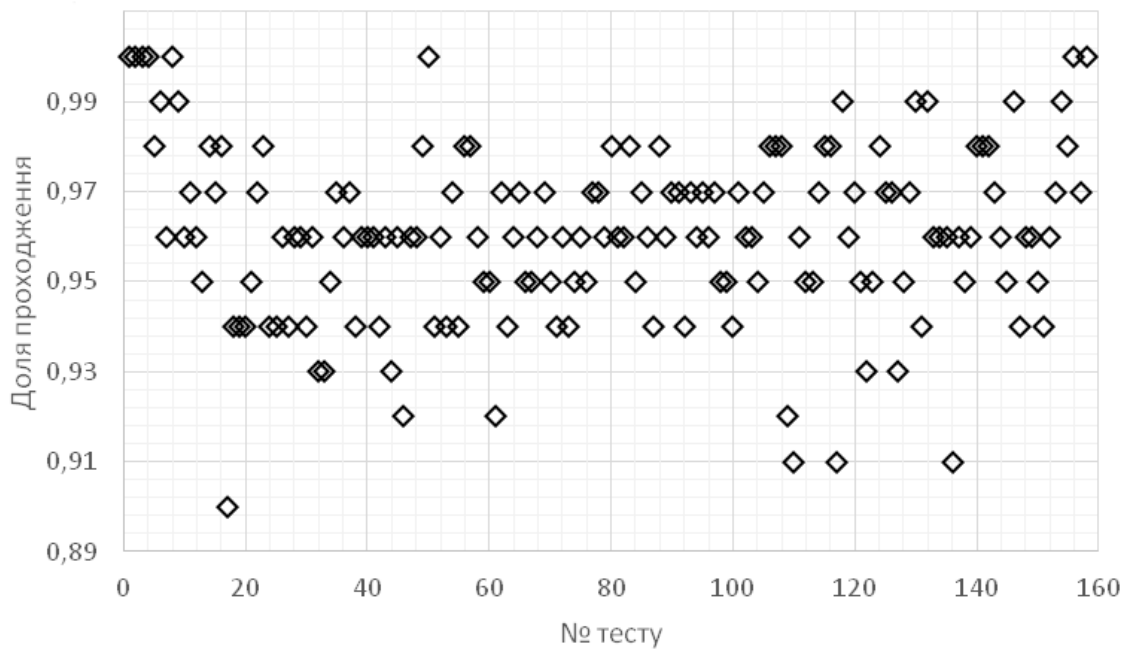

Рис. 1. Результати тестування схеми цифрового підписування на основі V_k -послідовностей з розміром ключа 512 бітів

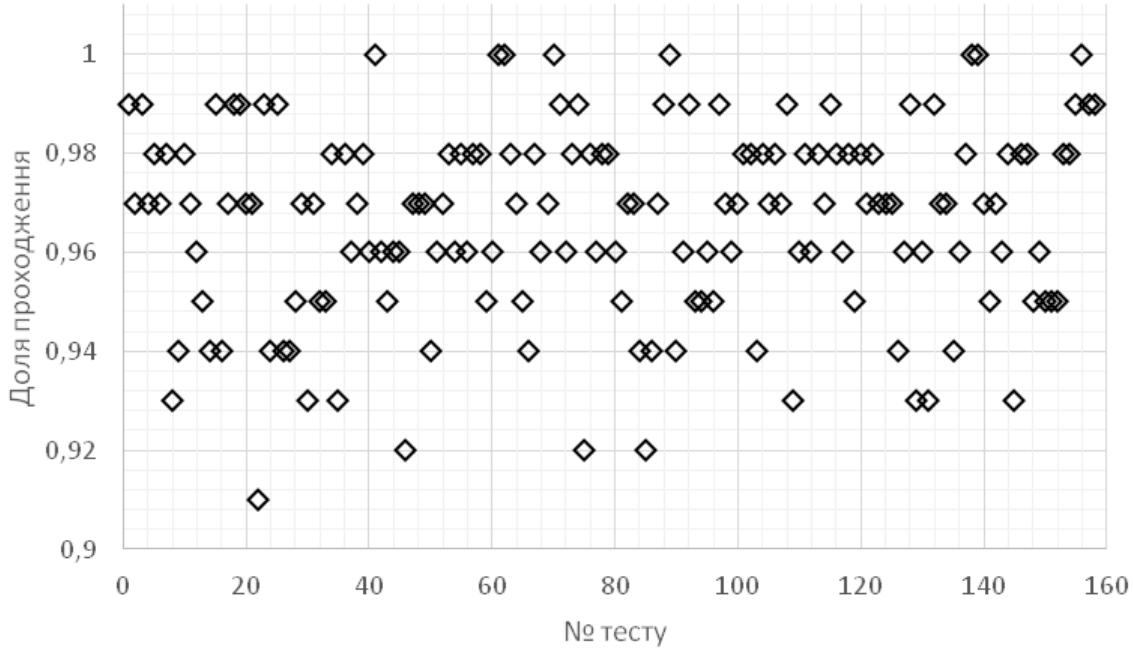

Рис. 2. Результати тестування схеми цифрового підписування на основі Фейге – Фіата – Шаміра з розміром ключа 512 бітів

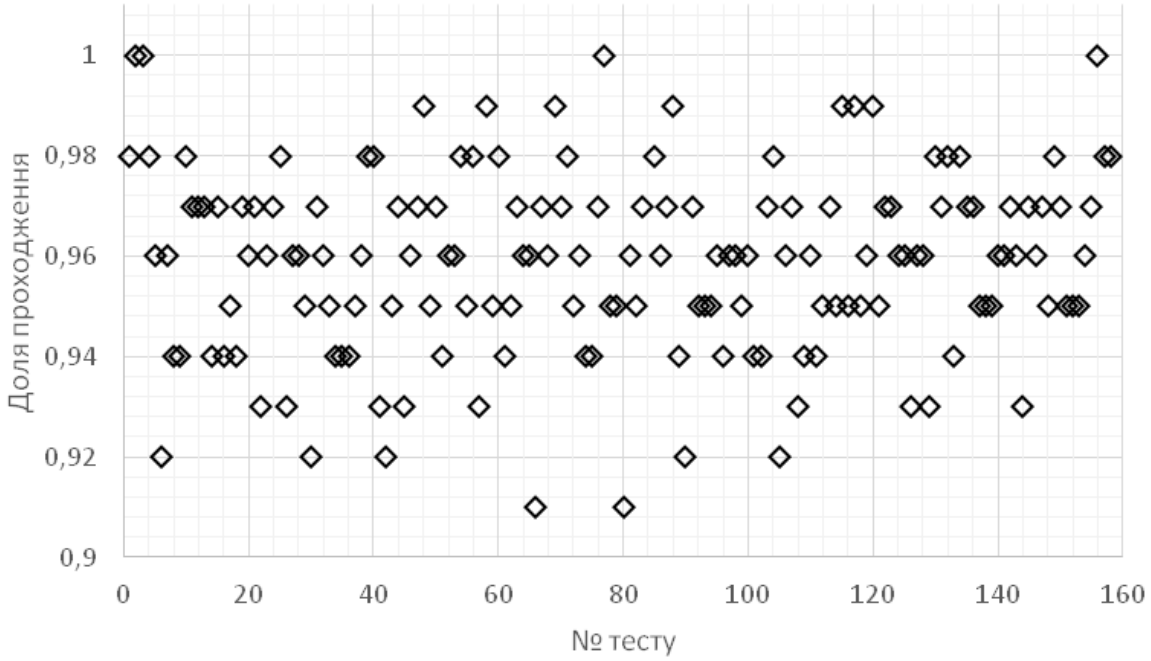

Рис. 3. Результати тестування схеми цифрового підписування Шнорра з розміром ключа 512 бітів

Результати тестування, що представлено статистичними портретами на рис. 1 – 3, свідчать про високий рівень статистичної безпеки. З рисунків видно, що схеми загалом знаходяться на високому рівні (0,9 і вище). Менше 2 % послідовностей мають показники нижче 0,9, що є гарним показником статистичної безпеки схем. У той же час схема на основі V_k -послідовностей виглядає більш скучкованою, що добре впливає на загальну властивість стійкості підпису до зламу криптоаналітиком.

На рис. 4 показано узагальнені графіки за кожним тестом для кожної схеми цифрового підписування для довжини ключа 512 розрядів.

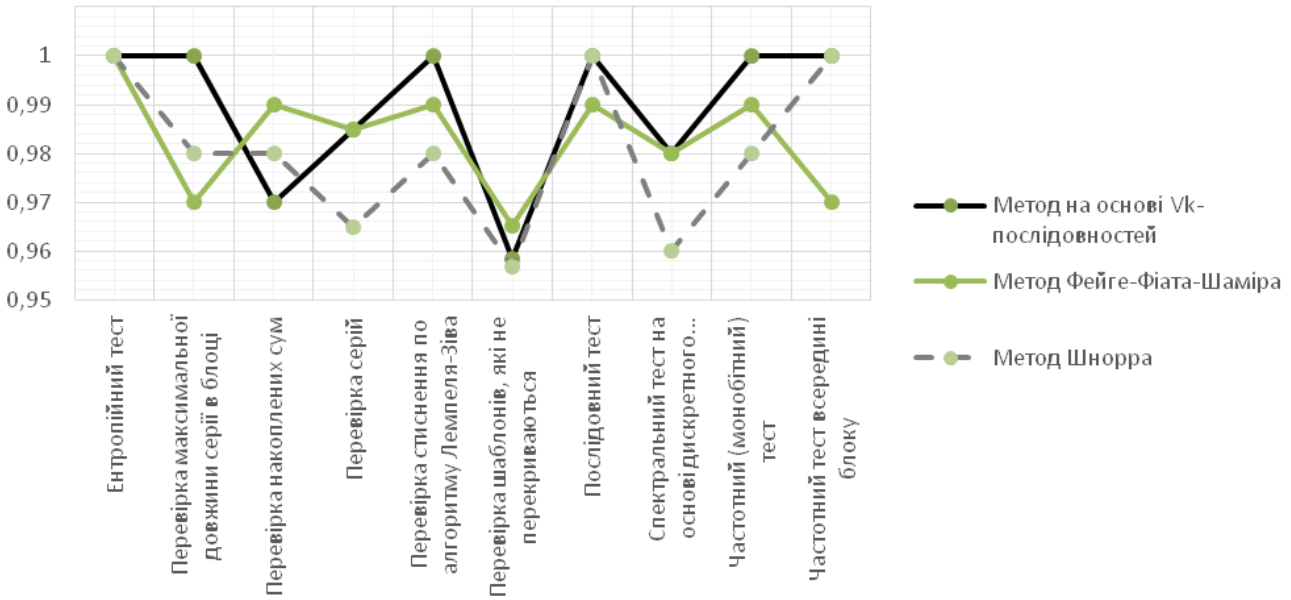

Рис. 4. Частка проходження тестів для схем ЦП з розміром ключа 512 бітів

З рис. 4 видно, що кращим у цілому щодо статистичної безпеки є схема на основі V_k-послідовностей, яка випереджає схему Шнорра у 50 % тестів, ще 40 % мають однаковий результат і лише тест на перевірку накоплених сум схема Шнорра пройшла на 0,01 краще, ніж схема на основі V_k-послідовностей. При цій довжині ключа, схема Фейге – Фіата – Шаміра отримала кращі результати порівняно зі схемою Шнорра за тестами на перевірку накоплених сум, перевірку серій, перевірку стиснення за алгоритмом Лемпеля – Зіва, перевірку шаблонів, які не перекриваються, спектральному та частотному тестах. Схема ЦП отримала однакові результати зі схемою на основі V_k-послідовностей у спектральному тесті, а зі схемою Шнорра у ентропійному тесті. В усіх інших тестах вона програє схемі Шнорра.

Висновки

Дослідження запропонованої у [3] схеми цифрового підписування на основі рекурентних V_k-послідовностей для розміру ключа 512 розрядів у порівнянні з відомими схемами Фейге – Фіата – Шаміра та Шнорра показало, що схема має високий рівень стійкості порівняно з відомими схемами. Схема на основі V_k-послідовностей має у цілому більшу кучність частот, має вищий діапазон показників портретів та має вищі показники за усіма тестами.

Список літератури: 1. *Menezes A.J., van Oorschot P.C., Vanstone S.A.* Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p. 2. *Молдавян Н.А.* Теоретический минимум и алгоритмы цифровой подписи. – СПб. : БХВ-Петербург, 2010. – 304 с. 3. *Яремчук Ю.Є.* Метод цифрового підписування на основі рекурентних послідовностей // Інформаційна безпека. –2013. – №1. – С. 165–175. 4. *Яремчук Ю.Є.* Дослідження статистичної безпеки методів цифрового підписування на основі рекурентних послідовностей // Реєстрація, зберігання і обробка даних. – 2014. – Т. 16, №2. – С. 74 – 86. 5. *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.

Вінницький національний технічний університет *Надійшла до редколегії 11.11.2014*