УДК 004.056+511.176

Ю. Є. ЯРЕМЧУК[1]

АНАЛІЗ СТАТИСТИЧНОЇ БЕЗПЕКИ СХЕМИ АВТЕНТИФІКАЦІЇ НА ОСНОВІ VK-ПОСЛІДОВНОСТЕЙ

[1]*Вінницький національний технічний університет, м. Вінниця*

Анотація. У роботі проведено аналіз статистичної безпеки схеми автентифікації сторін взаємодії на основі рекурентних Vk-послідовностей у порівнянні з відомими схемами автентифікації Фейге-Фіата-Шаміра, Фіата-Шаміра та Шнорра для довжини ключа 1024 розряди. Результати аналізу показали, що схема на основі Vk-послідовностей у цілому має високі показники статистичної безпеки, не поступаючись відомим аналогам, однак у порівнянні з меншими довжинами ключів ці показники є вищими.
Ключові слова: криптографія, автентифікація сторін взаємодії, криптографічна стійкість, статистична безпека, рекурентні послідовності.
Аннотация. В работе проведен анализ статистической безопасности схемы аутентификации сторон взаимодействия на основе рекуррентных Vk-последовательностей по сравнению с известными схемами аутентификации Фейге-Фиата-Шамира, Фиата-Шамира и Шнорра для длины ключа 1024 разрядов. Результаты анализа показали, что схема на основе Vk-последовательностей в целом имеет высокие показатели статистической безопасности, не уступая известным аналогам, однако по сравнению с меньшими длинами ключей эти показатели выше.
Ключевые слова: криптография, аутентификация сторон взаимодействия, криптографическая стойкость, статистическая безопасность, рекуррентные последовательности.
Abstract. The paper analyzes the statistical security of authentication of the parties interaction schemes based on recurrent Vk-sequences compared to known authentication scheme Feige-Fiat-Shamir, Fiat-Shamir and Schnorr for key length 1024 bits. The results showed that the scheme on the basis of Vk-sequences as a whole has a high statistical security, not yielding to known peers, but compared with smaller key lengths, these indicators are higher.
Keywords: cryptography, authentication of the parties interaction, cryptographic resistance, statistical security, recurrent sequences.

ВСТУП

У схемі автентифікації з нульовим розголошенням знання [1] претендент має два ключа — загальнодоступний K_1 та секретний K_2 і довести свою автентичність він повинен таким чином, щоб можна було переконатись, що він знає K_2 і при цьому це можна було б перевірити, знаючи лише K_1. Найбільш відомими схемами автентифікації з нульовим розголошенням є схеми [1, 2] Фіата-Шаміра, Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра, які базуються на операціях піднесенні до степеня.

У роботі [3] представлено схему автентифікації сторін взаємодії, що базується на математичному апараті рекурентних V_k –послідовностей. У порівнянні з відомими схемами автентифікації запропонована схема є більш стійкою, оскільки в ній замість передавання з обох сторін автентифікації значень чисел-індексів, або чисел-степенів як у відомих схемах, передаються елементи V_k –послідовності, обчислені для цих значень індексів.

У роботі [4] проведено дослідження статистичної безпеки представленої у [3] схеми автентифікації сторін взаємодії, однак актуальним залишається питання більш детального аналізу статистичної безпеки цієї схеми для великих розмірів ключа, зокрема у 1024 розряди, 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 автентифікації на основі рекурентних V_k –послідовностей для розміру ключа 1024 розряди у порівнянні з відомими схемами Фейге-Фіата-Шаміра, Фіата-Шаміра та Шнорра.

ОЦІНЮВАННЯ СТАТИСТИЧНОЇ БЕЗПЕКИ СХЕМИ АВТЕНТИФІКАЦІЇ ДЛЯ ДОВЖИНИ КЛЮЧА 1024 РОЗРЯДИ

Для дослідження статистичної безпеки схем автентифікації використано пакет NIST STS [5], який включає у себе набір з 16 статистичних тестів. Однак для розміру ключа у 1024 біти 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 таблиці 1 наведено дані про проходження результуючих послідовностей схемами автентифікації на основі V_k –послідовностей та Фейге-Фіата-Шаміра, Фіата-Шаміра і Шнорра для довжини ключа 1024 біти.

Таблиця 1.

Кількість тестів, що пройшли успішне тестування для ключа у 1024 біти

Метод	для $\alpha = 0{,}01$		для $\alpha = 0{,}001$	
	більше 99 % послідовностей	більше 96 % послідовностей	більше 99 % послідовностей	більше 98 % послідовностей
V_k	3 (1,90 %)	49 (31,01 %)	50 (31,65 %)	100 (63,29 %)
Фейге-Фіата-Шаміра	25 (15,82 %)	131 (82,91 %)	107 (67,72 %)	152 (96,20 %)
Фіата-Шаміра	40 (25,32 %)	151 (95,57 %)	132 (83,54 %)	157 (99,37 %)
Шнорра	9 (5,70 %)	74 (46,84 %)	33 (20,89 %)	66 (41,77 %)

З таблиці 1 видно, що схема на основі V_k –послідовностей відстає від показників схем Фейге-Фіата-Шаміра та Фіата-Шаміра, а також схеми Шнорра $\alpha = 0{,}01$, але для $\alpha = 0{,}001$ схема на основі рекурентних послідовностей випереджає схему Шнорра. Отриманні результати значно різняться від тих, що отримані для менших розмірів ключа [4], де схема на основі V_k –послідовностей приблизно у 3 рази випереджає метод Шнорра, причому навіть для $\alpha = 0{,}01$.

У таблиці 2 наведено відсотки проходження кожного з 10 тестів для $\alpha = 0{,}001$ та $\alpha = 0{,}01$ для довжини ключа 1024 розряди.

Таблиця 2.

Відсотки проходження кожного з 10 тестів для довжини ключа 1024 біти

№ тесту	Назва статистичного тесту	для $\alpha = 0{,}001$				для $\alpha = 0{,}01$			
		V_k	Ф-Ф-Ш	Ф-Ш	Ш	V_k	Ф-Ф-Ш	Ф-Ш	Ш
1	Частотний (монобітний) тест	100 %	100 %	100 %	100 %	99 %	99 %	98 %	100 %
2	Частотний тест всередині блоку	100 %	100 %	100 %	99 %	99 %	98 %	100 %	98 %
3	Послідовний тест	100 %	100 %	99 %	100 %	98 %	100 %	99 %	100 %
4	Перевірка максим. довжини серії в блоці	99 %	100 %	100 %	100 %	98 %	99 %	99 %	99 %
5	Спектральний тест на основі дискретного перетворення Фур'є	100 %	100 %	100 %	100 %	99 %	100 %	98 %	99 %
6	Перевірка шаблонів, які не перекриваються	99 %	100 %	100 %	98 %	95 %	98 %	99 %	96 %
7	Перевірка серій	100 %	100 %	100 %	100 %	99 %	98 %	99 %	99 %
8	Ентропійний тест	100 %	100 %	100 %	100 %	99 %	100 %	98 %	100 %
9	Перевірка накоплених сум	100 %	100 %	100 %	100 %	100 %	99 %	99 %	100 %
10	Перевірка стиснення за алгоритмом Лемпеля-Зіва	100 %	100 %	100 %	100 %	99 %	99 %	98 %	100 %

Як видно з результатів наведених у таблиці 2, коли $\alpha = 0,001$ усі послідовності мають майже однакові показники за усіма видами тестів, найвищі показники має схема Фейге-Фіата-Шаміра (усі 100 %). Порівнюючи з результатами для менших довжин ключів представлених у роботі [4], схема на основі V_k –послідовностей має рівний результат з цим методом (99—100 %), що показує його високу стійкість, при довжині ключа у 768 біт найвищі результати отримав метод на основі V_k –послідовностей.

Коли $\alpha = 0,01$, схема на основі V_k –послідовностей у цілому має рівні показники з відомими схемами. У порівнянні з меншими довжинами ключів [4], зокрема при довжині ключа 512 бітів, схема на основі V_k –послідовностей має вищі показники (96—100 %).

На рисунках 1—4 представлено статистичні портрети схем автентифікації для довжини ключа 1024 біти.

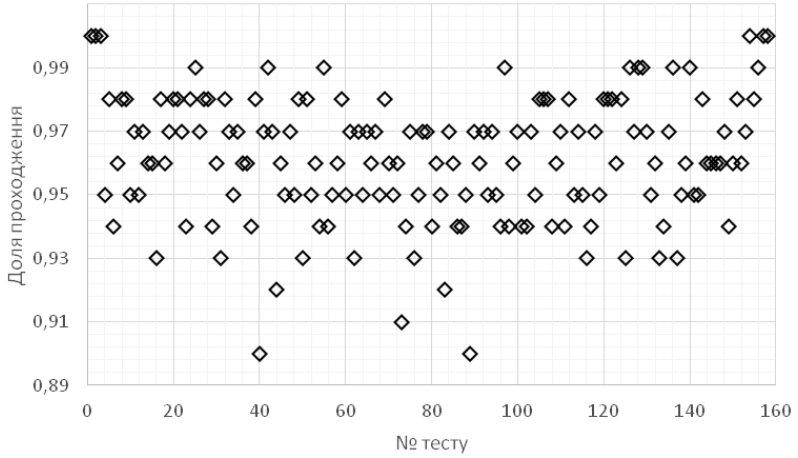

Рис. 1. Результати тестування схеми автентифікації на основі V_k –послідовностей з розміром ключа 1024 біти

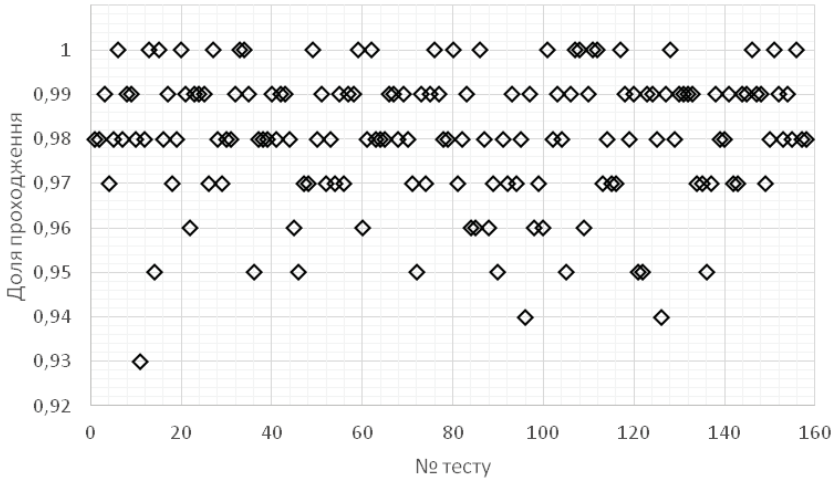

Рис. 2. Результати тестування схеми автентифікації Фейге-Фіата-Шаміра з розміром ключа 1024 біти

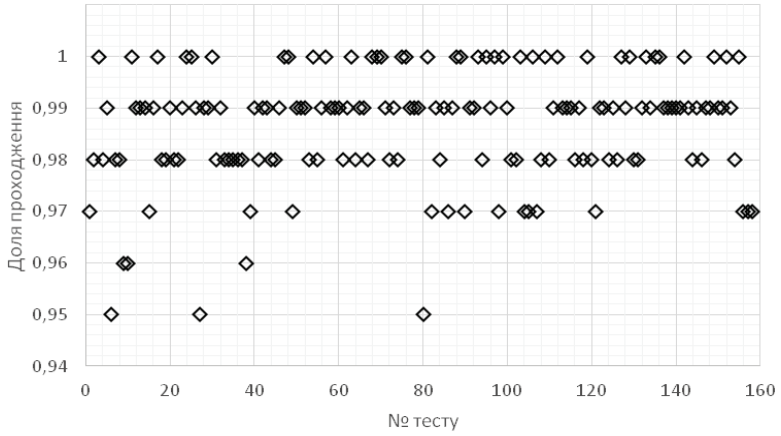

Рис. 3. Результати тестування схеми автентифікації Фіата-Шаміра з розміром ключа 1024 біти

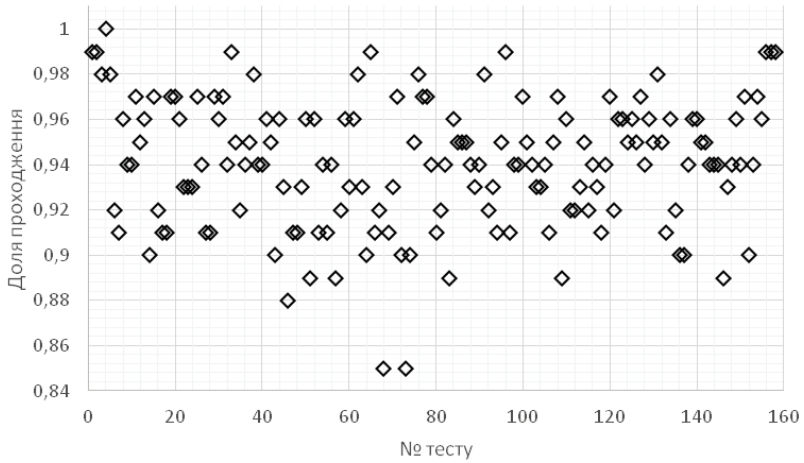

Рис. 4. Результати тестування схеми автентифікації Шнорра з розміром ключа 1024 біти

Результати тестування, що представлено статистичними портретами на рисунках 1–4, свідчать про високий рівень статистичної безпеки. З рисунків видно, що статистичні портрети тримаються у діапазоні від 0,9 до 1. Виключенням є схема Шнорра, у якого нижній поріг досягає 0,85. Найвищий нижній поріг спостерігається у схемі Фіата-Шаміра (0,95). Особливо варто відмітити схему на основі V_k –послідовностей, яка має рівномірний розкид показників проходження, що ускладнює виявив його слабких характеристик.

На рисунку 5 показано узагальнені графіки за кожним тестом для кожної схеми автентифікації для довжини ключа 1024 розрядів.

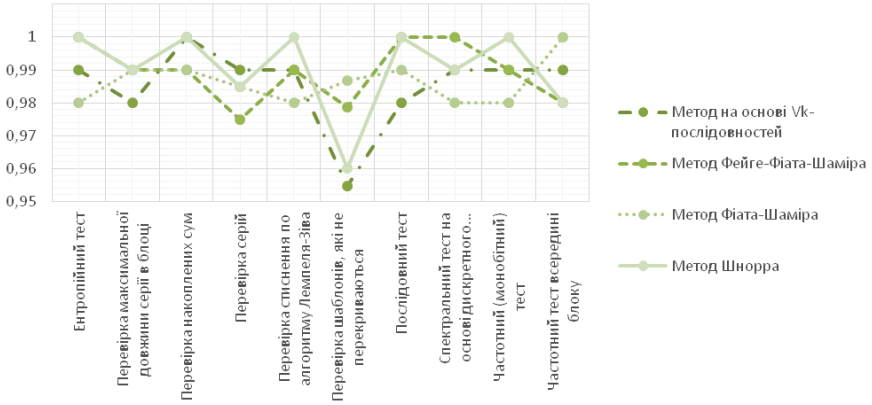

Рис. 5. Частка проходження тестів для схем автентифікації з розміром ключа 1024 біти

З рисунку 5 видно сильним провал у тесті на перевірку шаблонів, які не перекриваються (рівень до 0,955 порівняно з 0,98—1). Загалом вищі показники має схема Шнорра, проте в тестах на перевірку серій, перевірку шаблонів та спектральному тесті її випереджають інші схеми, а саме схема на основі V_k –послідовностей та схема Фейге-Фіата-Шаміра відповідно. Слід відзначити, що схема на основі V_k –послідовностей показує стабільно високі та середні результати, що характеризує його з гарного боку.

Порівнюючи з показниками при менших розмірах ключа, зокрема у 512 бітів [4], схема на основі V_k –послідовностей має у цілому вищі показники, загалом частки проходження за схемою на основі V_k –послідовностей знаходяться у межах 0,97—1, в той час як інші мають нижчий нижній поріг (0,93—0,96).

ВИСНОВКИ

Дослідження запропонованої у [3] схеми автентифікації на основі рекурентних V_k –послідовностей для розміру ключа 1024 розряди у порівнянні з відомими схемами Фейге-Фіата-Шаміра, Фіата-Шаміра та Шнорра показало, що схема у цілому має високий рівень стійкості порівняно з відомими схемами. Порівнюючи схему автентифікації на основі V_k –послідовностей для менших розмірів ключа, слід відзначити, що при менших значення ключів показники статистичної безпеки є кращими за відомі аналоги.

СПИСОК ЛІТЕРАТУРИ

1. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. — CRC Press, 2001. — 816 p.
2. Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. — М. : Горячая линия–Телеком, 2007. — 320 с.
3. Яремчук Ю. Є. Методи автентифікації на основі рекурентних послідовностей // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — Випуск 1(25), 2013. — С. 39—49.
4. Яремчук Ю. Є. Дослідження статистичної безпеки методу автентифікації сторін взаємодії на основі рекурентних послідовностей // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — Випуск 1(27), 2014. — С. 35—43.
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.

Надійшла до редакції 20.11.2014 р.

ЯРЕМЧУК Ю. Є. — к. т. н., доцент, директор Центру інформаційних технологій і захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету, м. Вінниця, Україна.