Palo Alto Networks	Cortex XDR	Автоматизація від виявлення до усунення загрози. LLM для інтерпретації логів у контексті бізнес-процесів. Динамічні шаблони - групування подій на основі поведінкових моделей UEBA.
ServiceNow	Security Operations - SecOps	Аналіз інцидентів (пріоритезація і виявлення аналогів), автоматизація, резюмування, запити і звітування природною мовою, рекомендації дій.

1. George, D. A. S., George, A. H., Baskar, T., Pandey, D. XDR: the evolution of endpoint security solutions-superior extensibility and analytics to satisfy the organizational needs of the future. *International Journal of Advanced Research in Science, Communication and Technology* . 2021. Vol. 8. No. 1. P. 493–501.
2. Kern, M., Landauer, M., Skopik, F., Weippl, E. A logging maturity and decision model for the selection of intrusion detection cyber security solutions. *Computers & Security*. 2024. Vol. 141. (10384).
3. Vielberth, M. Security information and event management (SIEM). In: *Encyclopedia of Cryptography, Security and Privacy*. Cham: Springer Nature Switzerland, 2025. P. 2304–2306.

Оптимізація адитивних генераторів Фібоначчі на основі примітивних поліномів для усунення слабких ключів

УДК 004.056

Олег Гарасимчук[1], Іван Опірський[2]
Національний університет "Львівська політехніка",
[1]oleh.i.harasymchuk@lpnu.ua, [2]ivan.r.opirskyi@lpnu.ua

Адитивні генератори Фібоначчі є різновидом генераторів псевдовипадкових чисел, що базуються на послідовності Фібоначчі та операції додавання. Завдяки своїй простоті та ефективності, вони знаходять широке застосування, зокрема в галузі кібербезпеки [1–2]. З огляду на зростаючий інтерес до таких генераторів, актуальним залишається завдання вдосконалення методів генерації псевдовипадкових послідовностей.

Встановлено, що адитивні генератори Фібоначчі (АГФ), реалізовані на основі примітивних поліномів у полі GF(p), формують псевдовипадкову послідовність з періодом повторення $p^k–1$, де k — ступінь полінома, для довільного початкового стану генератора (seed) [3]. Проте при непарних значеннях p вихідна бітова послідовність не відповідає статистичним вимогам, що зумовлено асиметрією у формуванні розрядів, внаслідок чого середнє співвідношення між 0 та 1 є нерівномірним.

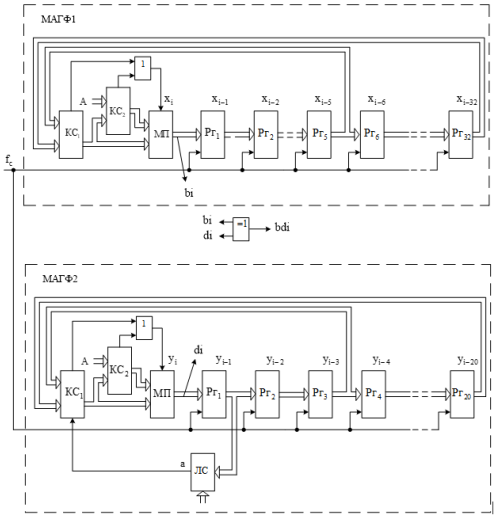
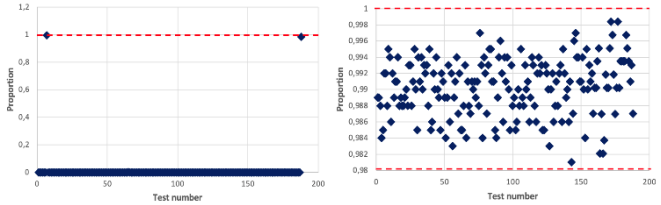


Рис. 1. Апаратна схема комбінованого генератора

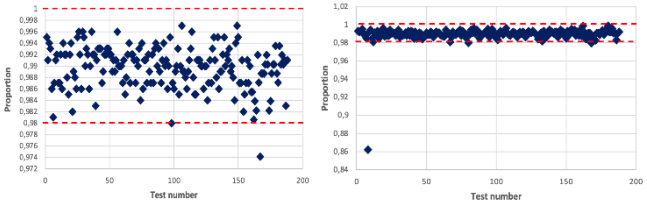
На рис. 1 наведена схема комбінованого генератора реалізованого на двох МАГФ: МАГФ1 – на основі примітивного поліному x32+x5+2 в полі GF(3) і МАГФ2 – на основі поліному y20+y3+1 з додатковою ЛС. Вихідна бітова послідовність формується на виході логічного елемента XOR.

Оцінювання проводилось за методикою NIST. Результати тестування комбінованого генератора наведено на рис. 2–3.



а б

Рис. 2. Статистичні портрети комбіновано генератора при z = 4:
а – без використання ЛС (hhh = 0), б – з ЛС (hhh = h0 xor h1)



а б

Рис. 3. Статистичні портрети комбіновано генератора при z = 10:
а – без використання ЛС (hhh = 0), б – з ЛС (hhh = h0 xor h3)

Результати дослідження показали, що додавання логічної схеми до комбінованого генератора суттєво покращує статистичні характеристики послідовності та забезпечує усунення слабких ключів завдяки збереженню максимального періоду повторення для всього діапазону початкових значень у MAFG на основі примітивних поліномів у полі GF(p).

1. Agarwal P., Agarwal N., Saxena R. Data encryption through fibonacci sequence and unicode characters, MIT International Journal of Computer Science and Information Technology, Vol. 5, No. 2, (August 2015), pp. 79-82 79 ISSN 2230-7621©MIT Publications.
2. Maksymovych, V.; Shabatura, M.; Harasymchuk, O.; Karpinski, M.; Jancarczyk, D.; Sawicki, P. Development of Additive Fibonacci Generators with Improved Characteristics for Cybersecurity Needs. Appl. Sci. (2022), 12(3), 1519.
3. Schneier, B. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C; John Wiley & Sons, Inc.: Indianapolis, Indiana, 2015; ISBN 9781119183471.

Дослідження методів аналізу для вивчення різних аспектів ринку криптовалют

УДК 004 (519.8) Олександр Корченко[1], Антон Герасименко[2]
ДУІКТ, [1]o.korchenko@duikt.edu.ua, [2]a.herasymenko@stud.duikt.edu.ua

Розвиток методів аналізу для вивчення різних аспектів ринку криптовалют спрямовано на допомогу трейдерам та інвесторам приймати обґрунтовані рішення. До основних видів аналітики можна віднести [1]:

Технічний аналіз: вивчення історичних графіків цін та обсягів торгів для виявлення тенденцій та закономірностей, які можуть передбачити майбутні рухи цін. Використання різних індикаторів, таких як ковзні середні, RSI (індекс відносної сили), MACD (сходження/розбіжність ковзних середніх), смуги Боллінджера та рівні Фібоначчі. Використання графічних патернів для інтерпретації ринкової ситуації.

Фундаментальний аналіз: Оцінка внутрішньої вартості криптовалюти на основі різних факторів, таких як технологія, команда розробників, рівень