УДК 004.056.55:004.421.5 DOI: 10.31673/2409-7292.2026.026904

Горячий Олег Ярославович
доктор філософії, старший викладач кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0000-0003-4948-458X
E-mail: oleh.y.horiachyi@lpnu.ua

Юрченко Артем Олександрович
студент 4-го курсу кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0009-0000-3007-1430
E-mail: artem.yurchenko.kb.2022@lpnu.ua

АНАЛІЗ ЕФЕКТИВНОСТІ АТАКИ ТИПУ «ВГАДАЙ ТА ВИЗНАЧ» НА ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ГОЛЬДРАЙХА З МОДИФІКОВАНИМ ПРЕДИКАТОМ P_5

У даній статті досліджено стійкість генератора псевдовипадкових послідовностей Гольдрайха класу складності NC^0 з різними предикатами локальності 5 до атаки типу “вгадай та визнач” (guess-and-determine). Генератор належить до локальних, у яких кожен вихідний біт залежить лише від фіксованої кількості вхідних бітів, що забезпечує високу швидкодію та паралельність обчислень. Розглянуто п’ять варіантів предиката P_5, що відрізняються позицією нелінійного елемента (AND): на початку, всередині та в кінці булевої функції, а також, для порівняння, лінійний предикат. Метою роботи є визначення впливу розташування елемента AND та інших параметрів генератора на ефективність атаки, зокрема на відсоток успішності, час її проведення, кількість необхідних вгадувань та кількість колізій. Проведено експериментальні дослідження для розмірів початкових значень n = 16, 32, 48, 64 та різних коефіцієнтів розтягу s = 1,15; 1,20; 1,25; 1,30; 1,35. Встановлено, що позиція операції AND та параметри n і s суттєво впливають на стійкість генератора. Методом Гаусса можна відновити початкове значення з ймовірністю понад 90%, що підтверджує необхідність використання нелінійних елементів для забезпечення криптографічної стійкості. Предикати з AND на початку або в кінці забезпечують найвищу успішність атаки для малих значень n та s, однак характеризуються більшою тривалістю виконання. Натомість запропоновані предикати з AND всередині виявилися стійкішими при малих s, особливо зі збільшенням розміру n. Виявлено, що збільшення коефіцієнта розтягу s спрощує атаку через зростання кількості колізій, тоді як збільшення розміру насіння n, навпаки, знижує її ефективність внаслідок експоненційного зростання простору станів. Отримані результати уточнюють вплив структури предиката та параметрів генератора Гольдрайха на його стійкість і можуть слугувати теоретичною основою для прогнозування їхньої поведінки при збільшенні n та проєктування безпечніших криптографічних генераторів.

Ключові слова: генератор псевдовипадкових послідовностей, генератор Гольдрайха, криптоаналіз, атака типу “guess-and-determine”, низька локальність, нелінійність, колізії.

Вступ

Генератори псевдовипадкових бітових послідовностей (ГПВБП) є фундаментальними компонентами сучасних криптографічних систем [1-9]. Згідно з класичним визначенням, ГПВБП – це детермінований алгоритм, який за коротким рівномірно випадковим початковим значенням (англ. seed, тобто “насіння”) формує довшу бітову послідовність, що є обчислювально нерозрізнюваною (computationally indistinguishable) від істинно випадкової. Вони використовуються для формування ключів шифрування, векторів ініціалізації, одноразових кодів, а також у протоколах аутентифікації, розділення секрету та багатосторонніх обчисленнях [1, 2, 5, 7-9]. Особливий інтерес становлять локальні генератори, що належать до класу складності NC^0, де кожен вихідний біт залежить лише від константної кількості вхідних бітів, що забезпечує високу паралельність обчислень та ефективність апаратної реалізації [12-14].

Одним з найвідоміших локальних генераторів є генератор, запропонований О. Гольдрайхом у 2000 році [10]. Він базується на застосуванні простого предиката до випадково вибраних підмножин бітів початкового значення. Найбільш дослідженим варіантом є предикат P_5: $x_1 \oplus x_2 \oplus x_3 \oplus (x_4 \wedge x_5)$, який має локальність 5 та забезпечує поліноміальне розтягнення $m = n^s$, де $s > 1$ [11, 12]. У роботах [16, 18] досліджено стійкість цього генератора

до різних типів атак та запропоновано конкретні параметри для досягнення 80-бітного та 128-бітного рівнів безпеки. Важливо зазначити, що атака типу “вгадай та визнач” (англ. guess-and-determine) належить до класу атак відновлення стану (state recovery attacks), де метою є безпосереднє відновлення початкового значення. Успішне відновлення насіння є достатньою умовою для розрізнення (distinguishing attack), оскільки дозволяє детерміністично відтворити вихід ГПВБП та порівняти його з аналізованою послідовністю.

Модель безпеки

У межах даного дослідження під “зламом” генератора розуміється обчислювально успішне відновлення його насіння за відомою парою (гіперграф, вихідна послідовність). Така атака є сильнішою за просте розрізнення, оскільки дозволяє повністю компрометувати генератор. Прийнято припущення, що зловмиснику відомі всі публічні параметри (алгоритм, гіперграф, розмір насіння n, коефіцієнт розтягу s), але невідоме саме початкове значення.

Проте в літературі недостатньо уваги приділено впливу структури предиката, зокрема позиції в ньому нелінійного елемента (AND), на стійкість генератора [15, 17, 19]. Інтуїтивно зрозуміло, що розміщення нелінійного члена AND на початку, в середині чи в кінці предиката формі P_5 серед інших лінійних елементів може впливати на стійкість генератора Гольдрайха до атак. Проте, кількісні оцінки цього впливу все ще не досліджені. Крім того, більшість досліджень зосереджені на великих розмірах початкових значень (зокрема, $n \geq 256$) [11, 14, 16, 18, 20], що робить їх важкими для тестування та попереднього аналізу їх ефективності.

Метою даної роботи є дослідження впливу позиції нелінійного елемента предиката на стійкість генератора Гольдрайха з локальністю 5 до атаки типу “вгадай та визнач” для різних розмірів початкових значень (n = 16, 32, 48, 64) та різних коефіцієнтів розтягу (s = 1,15; 1,20; 1,25; 1,30; 1,35).

Для досягнення поставленої мети необхідно вирішити наступні **завдання**:

1. Реалізувати програмну модель генератора Гольдрайха для п'яти різних варіацій предиката локальності 5.
2. Реалізувати атаку типу “вгадай та визнач” для кожного з варіантів позицій нелінійного елемента.
3. Провести експериментальне дослідження ГПВБП для всіх п'яти предикатів.
4. Проаналізувати залежність успішності та часу атаки від позиції AND, розміру початкового значення n та коефіцієнта розтягу s.
5. Сформулювати рекомендації щодо вибору структури предиката P_5 ГПВБП Гольдрайха для підвищення його стійкості.

Об'єкт дослідження – генератори псевдовипадкових послідовностей на основі локальних функцій.

Предмет дослідження – стійкість генератора Гольдрайха до атак типу “вгадай та визнач” залежно від позиції нелінійного елемента в предикаті локальності 5.

Огляд літератури

Генератор Гольдрайха був вперше запропонований як кандидат для побудови односторонньої функції [10]. Пізніше Е. Моссель зі співавторами [11] показали, що при використанні предиката P_5 ця функція може слугувати псевдовипадковим генератором з поліноміальним розтягом. Вони довели, що такий генератор обманює лінійні тести навіть при $m = poly(n)$. Подальші дослідження Б. Епплбаума та співавторів [12, 13] підтвердили можливість існування криптографічно стійких локальних генераторів у класі NC^0.

Р. О'Доннелл та Д. Вітмер [14] надали докази того, що ГПВБП Гольдрайха може досягати майже оптимального поліноміального розтягу, встановивши теоретичні межі для параметра s. Б. Епплбаум та Ш. Ловетт [15] дослідили алгебраїчні атаки на локальні функції та показали важливість таких критеріїв, як алгебраїчний імунітет та стійкість. Автори запропонували використовувати предикати XOR-MAJ як перспективні кандидати для побудови стійких генераторів.

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

У роботі [16] Ж. Куто зі співавторами вперше дослідили конкретну безпеку генератора Гольдрайха, запропонувавши атаку типу “вгадай та визнач” та визначивши параметри, які забезпечують 80-бітний та 128-бітний рівні безпеки. Вони також вказали на важливість дослідження інших предикатів, відмінних від класичного P_5. Презентація результатів цієї роботи доступна в [17].

Ц. Ян зі співавторами [18] значно покращили атаку “вгадай та визнач”, запропонувавши нову стратегію вибору змінних для вгадування та використавши ітеративне декодування. Їм вдалося зламати всі параметри, запропоновані в [16], та отримати ще нижчі оцінки складності атаки.

Сучасні дослідження продовжують розвивати методи криптоаналізу локальних генераторів. Б. Епплбаум зі співавторами [19] дослідили узагальнення локальних ГПВБП зі структурованим насінням. С. Фу зі співавторами [20] запропонували нові атаки на генератори Гольдрайха, засновані на групуванні рівнянь та їх розв'язанні.

Проте жодна з цих робіт не досліджує систематично вплив позиції нелінійного елемента на стійкість генератора саме для локальності 5 та для невеликих розмірів початкових значень, що і становить наукову новизну даної роботи.

Генератор Гольдрайха

Нехай n – розмір початкового значення (секретного ключа), а s – коефіцієнт розтягу, тоді довжина виходу m визначається як $m = n^s$.

Генератор використовує предикат P локальності 5 (наприклад, P_5) та випадковий гіперграф $G = (\sigma^1, \ldots, \sigma^m)$, де кожне σ^i є підмножиною з п’яти різних індексів з діапазону $[0; n-1]$. Вихідний біт y_i обчислюється як $y_i = P(x[\sigma^i])$, де $x[\sigma^i]$ – значення бітів початкового значення за індексами з підмножини σ^i.

Усі підмножини генеруються випадково та незалежно, при цьому гарантується їх унікальність (відсутність дублікатів).

Досліджувані предикати локальності 5

Для дослідження впливу позиції нелінійного елемента AND обрано наступні предикати (табл. 1).

Таблиця 1

Позначення досліджуваних предикатів локальності 5

Позначення	Позиція AND	Формула
P_5 – оригінальний	в кінці (між x_4 та x_5)	$x_1 \oplus x_2 \oplus x_3 \oplus (x_4 \wedge x_5)$
Q_5	на початку (між x_1 та x_2)	$(x_1 \wedge x_2) \oplus x_3 \oplus x_4 \oplus x_5$
W_5	в середині (між x_2 та x_3)	$x_1 \oplus (x_2 \wedge x_3) \oplus x_4 \oplus x_5$
E_5	в середині (між x_3 та x_4)	$x_1 \oplus x_2 \oplus (x_3 \wedge x_4) \oplus x_5$
L_5 – лінійний	немає	$x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5$

Атака “вгадай та визнач”

Атака типу “вгадай та визнач” для генератора Гольдрайха базується на наступних принципах:

1. Пошук колізій. Якщо два булеві рівняння мають однакову пару змінних у квадратичному члені (AND), то їх XOR дає лінійне рівняння, що не залежить від значень цих змінних. Такі лінійні рівняння отримуються “безкоштовно”. Важливо, що в різних предикатів позиція AND різна, тому пошук колізій виконується для різних пар індексів;

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

2. Вибір змінних для вгадування. Аналізується частота появи змінних у квадратичних членах. Залежно від предиката, це будуть різні пари індексів:

- для P_5: індекси 4 та 5;
- для Q_5: індекси 1 та 2;
- для W_5: індекси 2 та 3;
- для E_5: індекси 3 та 4;

3. Перебір варіантів. Для вибраних l булевих змінних перебирають всі 2^l можливих комбінацій значень. Для кожної комбінації будується система лінійних рівнянь (з урахуванням колізій та вгаданих значень), яка розв'язується методом Гаусса над полем GF(2);

4. Перевірка. Якщо знайдений розв'язок збігається зі справжнім початковим значенням (тобто забезпечує той самий вихід ГПВБП), атака вважається успішною;

Зв'язок атаки з формальними моделями криптографічної безпеки

Описана атака належить до класу атак відновлення стану генератора Гольдрайха та водночас є достатньою умовою для здійснення атаки на розрізнення. Розрізнення (distinguishing attack) – це криптографічна задача, в якій супротивник має розрізнити вихідну послідовність досліджуваного ГПВБП від істинно випадкової послідовності з імовірністю, помітно вищою за випадкове вгадування. У контексті даної роботи, якщо зловмисник за виходом ГПВБП здатний відновити початкове значення та детерміністично відновити вихідну послідовність, він може порівняти її з аналізованою. Таким чином, успішне відновлення стану автоматично забезпечує можливість розрізнення виходу ГПВБП від істинно випадкової послідовності. Оскільки задача відновлення насіння є складнішою за безпосереднє розрізнення, її аналіз дає більш консервативну оцінку криптостійкості генератора.

Методика дослідження

Для проведення експериментальних досліджень розроблено програмне забезпечення мовою Python з використанням бібліотеки NumPy для ефективних обчислень над GF(2). Програма реалізує:

- генерацію випадкового початкового значення заданого розміру n;
- генерацію унікального гіперграфа з $m = n^s$ ребрами (з гарантією відсутності дублікатів);
- обчислення виходу ГПВБП Гольдрайха для кожного з п'яти предикатів з табл. 1;
- проведення атаки "вгадай та визнач" з можливістю налаштування максимальної кількості вгадувань l_{max};

Крім того, для забезпечення відтворюваності результатів використано фіксовані початкові значення генераторів псевдовипадкових чисел у Python (random.seed(42) та np.random.seed(42)).

Параметри проведення експериментів

Під час досліджень будемо використовувати наступні параметри алгоритмів:

- розмір початкового значення n = 16, 32, 48, 64;
- коефіцієнт розтягу s = 1,15; 1,20; 1,25; 1,30; 1,35;
- максимальна кількість вгадувань l_{max} визначається динамічно за формулою (8) з роботи [18]:

$$l_{max} = [\frac{n-c}{4n^{s-1}+2} + 1],$$

де c – кількість лінійних рівнянь, отриманих з колізій;

- кількість тестів для кожного набору досліджуваних параметрів: 1000.

Для кожного проведеного тесту фіксувалися: успішність (true/false), кількість вгадувань $l \leq l_{max}$ (якщо атака успішна), час проведення атаки, кількість колізій, вгадувань та отриманих лінійних рівнянь.

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

Окрім аналізу стійкості до атак відновлення стану, було проведено оцінку статистичних властивостей згенерованих бітових послідовностей на відповідність вимогам стандарту FIPS 140-1. Для тестування використовувалася вихідна послідовність об'ємом 2500 байт (20 000 біт), сформована генератором Гольдрайха з практично значущими параметрами: розмір початкового значення n = 512 біт, коефіцієнт розтягу s = 1,6 та предикатом P_5. Тестування включало чотири базові статистичні перевірки: монобітний тест, покер-тест, тест довжин серій та тест максимальної довжини серії.

Приклад проведення атаки

Для ілюстрації виконання атаки типу "вгадай та визнач" розглянемо конкретний приклад генератора Гольдрайха з предикатом $P_5 = x_1 \oplus x_2 \oplus x_3 \oplus (x_4 \wedge x_5)$, розміром початкового значення n = 8 та коефіцієнтом розтягу s = 1,2 ($m = 8^{1,2} \approx 12$).

Крок 1. Генерація вхідних даних

Генератор отримує випадкове 8-бітове початкове значення x (секретний ключ). Нехай x = [1, 0, 1, 0, 1, 0, 1, 0] (діапазон індексів 0…7). Потім для отримання 12 вихідних бітів ГПВБП випадково обираються 12 різних підмножин індексів розміру 5. Для кожної підмножини обчислюється значення предиката P_5. У табл. 2 наведено всі 12 отриманих рівнянь та обчислені вихідні біти.

Таблиця 2

Процедура генерації вихідної послідовності ГПВБП та формування повної системи рівнянь

№	Індекси σ^i	Біти x[σ^i]	Обчислення P_5	y_i
1	[0, 1, 2, 5, 7]	[1, 0, 1, 0, 0]	$1 \oplus 0 \oplus 1 \oplus (0 \wedge 0)$	0
2	[0, 1, 3, 4, 5]	[1, 0, 0, 1, 0]	$1 \oplus 0 \oplus 0 \oplus (1 \wedge 0)$	1
3	[0, 1, 5, 6, 7]	[1, 0, 0, 1, 0]	$1 \oplus 0 \oplus 0 \oplus (1 \wedge 0)$	1
4	[0, 1, 3, 4, 6]	[1, 0, 0, 1, 1]	$1 \oplus 0 \oplus 0 \oplus (1 \wedge 1)$	0
5	[1, 2, 3, 4, 6]	[0, 1, 0, 1, 1]	$0 \oplus 1 \oplus 0 \oplus (1 \wedge 1)$	0
6	[0, 1, 2, 3, 6]	[1, 0, 1, 0, 1]	$1 \oplus 0 \oplus 1 \oplus (0 \wedge 1)$	0
7	[0, 1, 2, 4, 6]	[1, 0, 1, 1, 1]	$1 \oplus 0 \oplus 1 \oplus (1 \wedge 1)$	1
8	[0, 1, 2, 3, 4]	[1, 0, 1, 0, 1]	$1 \oplus 0 \oplus 1 \oplus (0 \wedge 1)$	0
9	[0, 3, 4, 5, 6]	[1, 0, 1, 0, 1]	$1 \oplus 0 \oplus 1 \oplus (0 \wedge 1)$	0
10	[0, 2, 4, 5, 6]	[1, 1, 1, 0, 1]	$1 \oplus 1 \oplus 1 \oplus (0 \wedge 1)$	1
11	[0, 1, 3, 5, 6]	[1, 0, 0, 0, 1]	$1 \oplus 0 \oplus 0 \oplus (0 \wedge 1)$	1
12	[0, 1, 2, 5, 6]	[1, 0, 1, 0, 1]	$1 \oplus 0 \oplus 1 \oplus (0 \wedge 1)$	0

Отже, y = [0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0] – вихід ГПВБП.

Крок 2. Пошук колізій

Колізія виникає, коли два рівняння мають однакову пару в квадратичному члені $(x_4 \wedge x_5)$. На основі табл. 2 побудуємо систему рівнянь із вісьмома невідомими, в якій виділяємо рівняння, що містять колізію:

- пара індексів (4, 6): рівняння №4, №5 та №7 (позначимо їх як A_4, A_5 та A_7);
- пара індексів (5, 6): рівняння № 9, №10, №11 та №12 (серед них достатньо розглянути лише рівняння A_9, A_{10} та A_{11}, оскільки вони мають унікальні значення бітів).

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

Для кожної пари індексів виконуємо XOR відповідних рівнянь, що дозволяє позбутися квадратичного члена та отримати лінійні рівняння.

Для пари (4, 6):

$$\begin{cases} x_0 \oplus x_1 \oplus x_3 \oplus (x_4 \wedge x_6) = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus (x_4 \wedge x_6) = 0 \\ x_0 \oplus x_1 \oplus x_2 \oplus (x_4 \wedge x_6) = 1 \end{cases}.$$

Виконуємо операцію XOR між A_4 та A_5:

$$A_4 \oplus A_5 = (x_0 \oplus x_1 \oplus x_3) \oplus (x_1 \oplus x_2 \oplus x_3) = 0 \oplus 0 .$$

Звідси отримуємо рівняння $x_0 \oplus x_2 = 0$. Аналогічно для A_4 та A_7:

$$A_4 \oplus A_7 = (x_0 \oplus x_1 \oplus x_3) \oplus (x_0 \oplus x_1 \oplus x_2) = 0 \oplus 1 \quad \Rightarrow \quad x_2 \oplus x_3 = 1 .$$

Для пари (5, 6):

$$\begin{cases} x_0 \oplus x_3 \oplus x_4 \oplus (x_5 \wedge x_6) = 0 \\ x_0 \oplus x_2 \oplus x_4 \oplus (x_5 \wedge x_6) = 1 \\ x_0 \oplus x_1 \oplus x_3 \oplus (x_5 \wedge x_6) = 1 \end{cases},$$

$$A_9 \oplus A_{10} = (x_0 \oplus x_3 \oplus x_4) \oplus (x_0 \oplus x_2 \oplus x_4) = 0 \oplus 1 \quad \Rightarrow \quad x_2 \oplus x_3 = 1 \text{ (дублікат)},$$

$$A_9 \oplus A_{11} = (x_0 \oplus x_3 \oplus x_4) \oplus (x_0 \oplus x_1 \oplus x_3) = 0 \oplus 1 \quad \Rightarrow \quad x_1 \oplus x_4 = 1,$$

$$A_{10} \oplus A_{11} = (x_0 \oplus x_2 \oplus x_4) \oplus (x_0 \oplus x_1 \oplus x_3) = 1 \oplus 1 \quad \Rightarrow \quad x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 .$$

Таким чином ми отримали 4 унікальні лінійні рівняння, які можна представити у вигляді:

$$\begin{cases} x_0 \oplus x_2 = 0 \\ x_2 \oplus x_3 = 1 \\ x_1 \oplus x_4 = 1 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \end{cases}.$$

Крок 3. Аналіз частоти появи змінних у квадратичних членах

Для подальшого вгадування змінних визначаємо, скільки разів кожна змінна з'являється у квадратичних членах (позиції 3 та 4 в індексах, тобто четвертий і п'ятий елементи підмножини), як наведено у табл. 3.

Таблиця 3

Аналіз частоти змінних у квадратичних членах

Змінна	Частота появи
x_0	0
x_1	0
x_2	0
x_3	2 (у рівняннях A_6 та A_8)
x_4	5 (у рівняннях A_2, A_4, A_5, A_7 та A_8)
x_5	6 (у рівняннях A_1, A_2, A_9, A_{10}, A_{11} та A_{12})
x_6	9 (у рівняннях A_3, A_4, A_5, A_6, A_7, A_9, A_{10}, A_{11} та A_{12})
x_7	2 (у рівняннях A_1 та A_3)

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

Отже, найчастішими змінними є x_6 (9 разів), x_5 (6 разів) та x_4 (5 разів). Саме їх обираємо для вгадування.

Крок 4. Перебір варіантів

Для трьох вибраних змінних (x_4, x_5, x_6) існує $2^3 = 8$ можливих комбінацій двійкових значень. Для кожної комбінації підставляємо вгадані значення у вихідні рівняння, що перетворює їх на лінійні. Додаємо до цього 4 лінійні рівняння, отримані з колізій, та будуємо лінійну систему рівнянь, що розв'язується методом Гаусса. Тоді перевіряємо, чи отриманий розв'язок відповідає вихідній послідовності генератора.

У даному прикладі розглянемо лише комбінацію (x_4, x_5, x_6), що відповідає оригінальному початковому значенню ГПВБП: $x_4 = 1$, $x_5 = 0$ та $x_6 = 1$. Підставивши їх в останні два рівняння з колізіями (які вже є лінійними), отримаємо:

$$x_1 \oplus x_4 = x_1 \oplus 1 = 1 \quad \Rightarrow \quad x_1 = 0\,,$$

$$x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \oplus x_2 \oplus x_3 \oplus 1 = 0 \quad \Rightarrow \quad x_2 \oplus x_3 = 1 \text{ (дублікат).}$$

Тепер підставляємо $x_1 = 0$, $x_4 = 1$, $x_5 = 0$ та $x_6 = 1$ в кожне з 12 рівнянь, завдяки чому багато з них стають лінійними:

$$A_1\colon x_0 \oplus x_1 \oplus x_2 \oplus (x_5 \wedge x_7) = 0 \quad \Rightarrow \quad x_0 \oplus 0 \oplus x_2 \oplus (0 \wedge x_7) = 0 \quad \Rightarrow \quad x_0 \oplus x_2 = 0 \text{ (дублікат)}\,,$$

$$A_2\colon x_0 \oplus x_1 \oplus x_3 \oplus (x_4 \wedge x_5) = 1 \quad \Rightarrow \quad x_0 \oplus 0 \oplus x_3 \oplus (1 \wedge 0) = 1 \quad \Rightarrow \quad x_0 \oplus x_3 = 1\,,$$

$$A_3\colon x_0 \oplus x_1 \oplus x_5 \oplus (x_6 \wedge x_7) = 1 \quad \Rightarrow \quad x_0 \oplus 0 \oplus 0 \oplus (1 \wedge x_7) = 1 \quad \Rightarrow \quad x_0 \oplus x_7 = 1\,,$$

$$A_4\colon x_0 \oplus x_1 \oplus x_3 \oplus (x_4 \wedge x_6) = 0 \quad \Rightarrow \quad x_0 \oplus 0 \oplus x_3 \oplus (1 \wedge 1) = 0 \quad \Rightarrow$$
$$\Rightarrow \quad x_0 \oplus x_3 \oplus 1 = 0 \quad \Rightarrow \quad x_0 \oplus x_3 = 1 \text{ (дублікат)}\,,$$

$$A_5\colon x_1 \oplus x_2 \oplus x_3 \oplus (x_4 \wedge x_6) = 0 \quad \Rightarrow \quad 0 \oplus x_2 \oplus x_3 \oplus (1 \wedge 1) = 0 \quad \Rightarrow$$
$$\Rightarrow \quad x_2 \oplus x_3 \oplus 1 = 0 \quad \Rightarrow \quad x_2 \oplus x_3 = 1 \text{ (дублікат)}\,,$$

$$A_6\colon x_0 \oplus x_1 \oplus x_2 \oplus (x_3 \wedge x_6) = 0 \quad \Rightarrow \quad x_0 \oplus 0 \oplus x_2 \oplus (x_3 \wedge 1) = 0 \quad \Rightarrow \quad x_0 \oplus x_2 \oplus x_3 = 0.$$

Як можна побачити далі, опрацювання наступних шести рівнянь дозволить отримати лише дублікати з попередніх:

$$A_7\colon x_0 \oplus x_1 \oplus x_2 \oplus (x_4 \wedge x_6) = 1 \quad \Rightarrow \quad x_0 \oplus 0 \oplus x_2 \oplus (1 \wedge 1) = 1 \quad \Rightarrow$$
$$\Rightarrow \quad x_0 \oplus x_2 \oplus 1 = 1 \quad \Rightarrow \quad x_0 \oplus x_2 = 0\,,$$

$$A_8\colon x_0 \oplus x_1 \oplus x_2 \oplus (x_3 \wedge x_4) = 0 \quad \Rightarrow \quad x_0 \oplus 0 \oplus x_2 \oplus (x_3 \wedge 1) = 0 \quad \Rightarrow \quad x_0 \oplus x_2 \oplus x_3 = 0\,,$$

$$A_9\colon x_0 \oplus x_3 \oplus x_4 \oplus (x_5 \wedge x_6) = 0 \quad \Rightarrow \quad x_0 \oplus x_3 \oplus 1 \oplus (0 \wedge 1) = 0 \quad \Rightarrow \quad x_0 \oplus x_3 = 1\,,$$

$$A_{10}\colon x_0 \oplus x_2 \oplus x_4 \oplus (x_5 \wedge x_6) = 1 \quad \Rightarrow \quad x_0 \oplus x_2 \oplus 1 \oplus (0 \wedge 1) = 1 \quad \Rightarrow \quad x_0 \oplus x_2 = 0\,,$$

$$A_{11}\colon x_0 \oplus x_1 \oplus x_3 \oplus (x_5 \wedge x_6) = 1 \quad \Rightarrow \quad x_0 \oplus 0 \oplus x_3 \oplus (0 \wedge 1) = 1 \quad \Rightarrow \quad x_0 \oplus x_3 = 1\,,$$

$$A_{12}\colon x_0 \oplus x_1 \oplus x_2 \oplus (x_5 \wedge x_6) = 0 \quad \Rightarrow \quad x_0 \oplus 0 \oplus x_2 \oplus (0 \wedge 1) = 0 \quad \Rightarrow \quad x_0 \oplus x_2 = 0\,.$$

Після підстановки ми отримали наступні унікальні рівняння (без дублікатів):

$$\begin{cases} x_0 \oplus x_2 = 0 \\ x_2 \oplus x_3 = 1 \\ x_1 = 0 \\ x_0 \oplus x_3 = 1 \\ x_0 \oplus x_7 = 1 \\ x_0 \oplus x_2 \oplus x_3 = 0 \end{cases}.$$

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

Крок 5. Розв'язання системи лінійних рівнянь

Ми отримали 6 рівнянь для 8 змінних. Ця система недовизначена, але в поєднанні з вгаданими змінними ($x_4 = 1$, $x_5 = 0$ та $x_6 = 1$) дає єдиний розв'язок.

$$\begin{cases} x_0 = x_2 \\ x_3 = x_2 \oplus 1 \\ x_1 = 0 \\ x_0 \oplus x_3 = x_2 \oplus (x_2 \oplus 1) = 1 \\ x_7 = x_0 \oplus 1 \\ x_0 \oplus x_2 \oplus x_3 = x_2 \oplus x_2 \oplus (x_2 \oplus 1) = 0 \end{cases} \Rightarrow \begin{cases} x_2 = 1 \\ x_0 = x_2 = 1 \\ x_3 = x_2 \oplus 1 = 1 \oplus 1 = 0 \\ x_1 = 0 \\ x_7 = x_0 \oplus 1 = 1 \oplus 1 = 0 \end{cases}.$$

Таким чином, разом з вгаданими змінними, ми отримуємо наступний розв'язок x = [1, 0, 1, 0, 1, 0, 1, 0].

Крок 6. Перевірка

Знайдений розв'язок повністю збігається з оригінальним початковим значенням. Підстановка x у вихідні рівняння дає той самий вихід y ГПВБП, що підтверджує успішність атаки.

Результати проведених експериментів

Оскільки при використанні лінійного предиката L_5 у системі рівнянь відсутні нелінійні елементи, у цьому випадку для атаки на генератор Гольдрайха використовується метод Гаусса, що забезпечує значно вищу ефективність, ніж атака типу "вгадай та визнач".

Результати статистичного тестування за стандартом FIPS 140-1

Для перевірки якості генерації та підтвердження практичної придатності досліджуваного ГПВБП було згенеровано послідовність довжиною більше 20 000 біт із розміром початкового значення n = 512 біт (розтяг s = 1,6). Отримані псевдовипадкові бінарні дані було піддано статистичним тестам пакета FIPS 140-1. Результати експериментальної перевірки наведено у табл. 4.

Таблиця 4

Результати статистичного тестування FIPS 140-1 згенерованої ГПВБП Гольдрайха послідовності розміру 20 000 біт

Назва тесту	**Відповідність умовам тесту**		**Результат**
Монобітний тест	9654 ≤ 9803 (одиниць) ≤ 10346		Пройдено
Покер-тест	1,03 ≤ 23,60 ≤ 57,4		Пройдено
Тест довжин серій	Довжина серії 1	2267 ≤ 2488 (нулів), 2582 (одиниць) ≤ 2733	Пройдено
	Довжина серії 2	1079 ≤ 1282 (нулів), 1266 (одиниць) ≤ 1421	
	Довжина серії 3	502 ≤ 628 (нулів), 632 (одиниць) ≤ 748	
	Довжина серії 4	223≤ 332 (нулів), 315 (одиниць) ≤ 402	
	Довжина серії 5	90 ≤ 168 (нулів), 138 (одиниць) ≤ 223	
	Довжина серії 6+	90≤ 157 (нулів), 123 (одиниць) ≤ 223	
Тест максимальної довжини серії	12 ≤ 34 біт		Пройдено

Аналіз даних табл. 4 свідчить, що кількість одиниць (9803) знаходиться в межах норми, показник покер-тесту (23,6) демонструє хорошу рівномірність розподілу 4-бітових блоків, а

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

довжини послідовних серій нулів та одиниць повністю задовольняють теоретичним критеріям. Максимальна зафіксована серія однакових бітів становила 12, що суттєво менше критичного порогу в 34 біти. Таким чином, бітова послідовність успішно пройшла всі чотири статистичні перевірки, що дозволяє зробити висновок: генератор Гольдрайха з предикатом P_5. при великому розміру початкового значення (n = 512 біт) та коефіцієнті розтягу s = 1,6 забезпечує належну якість випадковості вихідного потоку.

Результати дослідження успішності атак

Для лінійного предиката L_5 успішність проведення атаки методом Гаусса складає 99-100% для всіх досліджуваних параметрів (для прикладу показано лише для параметрів s = 1,15 та для n = 16; 32 та 64) (див. рис. 1). Цей показник не досягає 100% лише в окремих випадках через можливу виродженість матриць при відносно невеликій кількості рівнянь m, що підтверджує непридатність лінійного предиката для криптографічних застосувань.

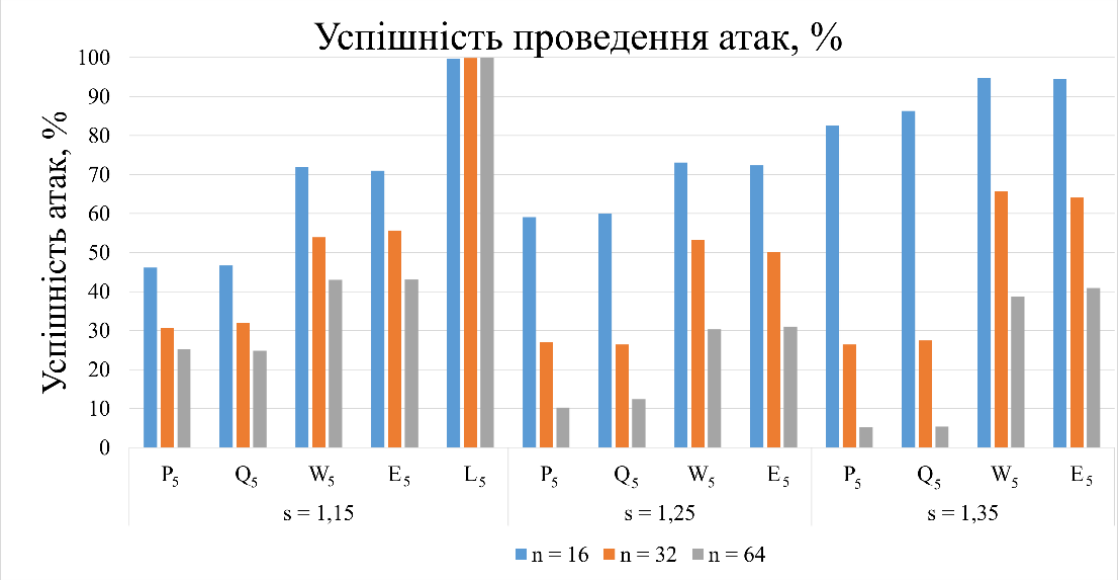


Рис. 1. Результати визначення успішності проведення атак

Як видно з рис.1, для s = 1,15 успішність атаки для всіх нелінійних предикатів очікувано знижується зі збільшенням розміру початкового значення n. Для n = 16 найвищу успішність демонструють предикати W_5 та E_5 (72% та 71% відповідно), тоді як P_5 та Q_5 мають значно нижчі показники (46% та 47 %).

Для n = 32 та n = 64 ця різниця зберігається: W_5 та E_5 залишаються більш вразливими (54 % та 56 % для n = 32; 43% та 44% для n = 64), ніж P_5 та Q_5 (31% та 33% для n = 32; 25% та 24% для n = 64). Лінійний предикат L_5 очікувано демонстує 100% успішності для всіх n та s.

Для s = 1,35 спостерігається суттєво вища успішність атаки для всіх предикатів порівняно з s = 1,15, що пояснюється більшою кількістю рівнянь та, відповідно, колізій. Для n = 16 успішність P_5 досягає 84%, Q_5 – 87%, W_5 – 95%, E_5 – 96%. Для n = 64 успішність P_5 знижується до 6%, Q_5 – до 7%, тоді як W_5 та E_5 демонструють значно вищі показники (40% та 41% успішності). Це підтверджує, що предикати з AND всередині (W_5, E_5) є більш вразливими до атаки типу “вгадай та визнач”, особливо при великих значеннях коефіцієнта розтягу s.

Таким чином, отримані результати чітко демонструють, що позиція нелінійного елемента AND суттєво впливає на стійкість генератора: розташування AND в середині предиката (W_5, E_5) робить генератор значно більш вразливим порівняно з розташуванням на початку (Q_5) або в кінці (P_5).

Зі збільшенням n успішність атаки для всіх предикатів знижується, що узгоджується з теоретичними очікуваннями щодо експоненційного зростання простору станів.

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

Результати дослідження тривалості атак

Дослідження тривалості виконання атаки (див. рис. 2) показало, що час атаки суттєво залежить від розміру початкового значення n та коефіцієнта розтягу s. Лінійний предикат L_5 очікувано демонструє найменший час (від 3 до 20 мс) через відсутність нелінійних елементів.

Для коефіцієнта розтягу s = 1,25 при n = 64 спостерігається різке зростання часу атаки для предикатів W_5 (92 мс) та E_5(93 мс), що значно перевищує час для P_5 (59 мс) та Q_5(57 мс). Для n = 48 час атаки для всіх предикатів є близьким (24-33 мс), а для n = 32 – практично однаковим (8-10 мс).

Для коефіцієнта розтягу s = 1,35 час атаки є загалом нижчим. При n = 64 W_5 та E_5 мають 34 та 36 мс, P_5 та Q_5 – 26 та 24 мс. Для n = 48 час атаки становить 11-18 мс, для n = 32 – 5-10 мс.

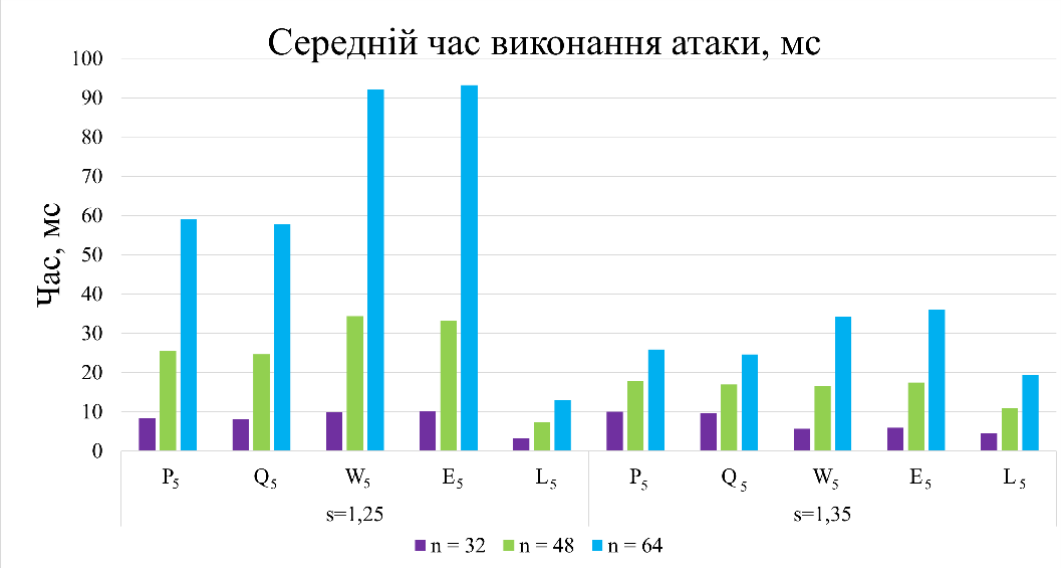


Рис. 2. Дослідження середнього часу виконання атаки

Більший коефіцієнт розтягу s призводить до збільшення кількості рівнянь та колізій, що зменшує потребу у вгадуваннях та, відповідно, знижує час атаки.

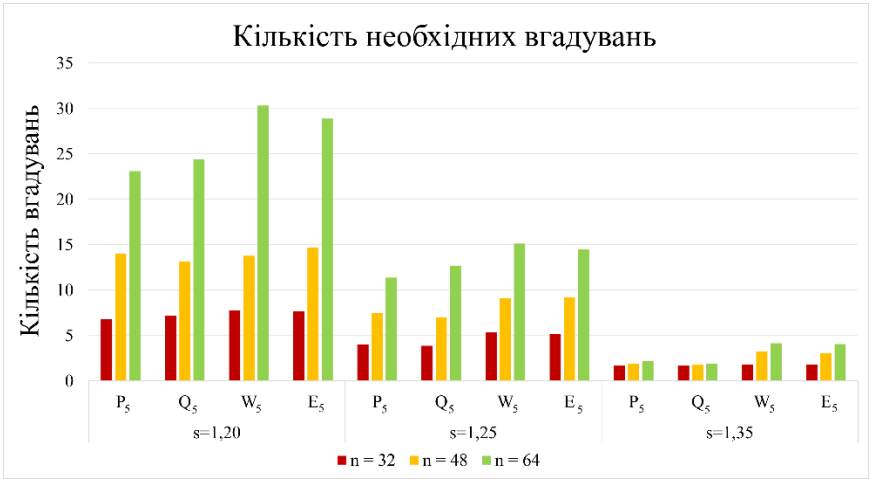
Інтерпретація результатів: роль колізій та нелінійності

Як видно з рис. 3а, середня кількість необхідних вгадувань l суттєво залежить від коефіцієнта розтягу s та розміру початкового значення n. Для s = 1,20 при n = 64 l = 23 для P_5 та l = 24 для Q_5, тоді як для W_5 та E_5 – l = 30 та l = 29 відповідно. При збільшення s до 1,25 l знижується до 11-15, а при s = 1,35 – до 2-4. Це підтверджує, що більший коефіцієнт розтягу полегшує атаку.

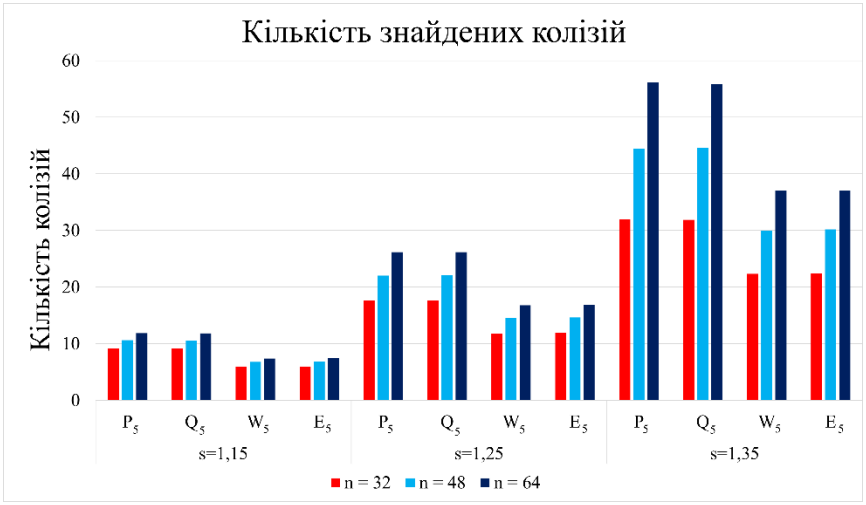
На рис. 3б наведено залежність кількості знайдених колізій c від параметрів n та s. Для P_5 при n = 64 кількість колізій зростає з 12 (s = 1,15) до 56 (s = 1,35). Для W_5 цей показник є значно нижчим (від 7 до 37). Очевидно, що збільшення кількості колізій безпосередньо зменшує кількість необхідних вгадувань, оскільки кожна колізія дає “безкоштовне” лінійне рівняння. Лінійний предикат L_5 позбавлений операції AND, не створює колізій, тому атака типу “вгадай та визнач” до нього не застосовна. Однак він тривіально зламується методом Гаусса (успішність 99-100%). Це підтверджує, що нелінійність є необхідною умовою криптографічної стійкості локальних генераторів.

Отримані результати узгоджуються з теоретичними оцінками [16, 18]. Збільшення розміру насіння n експоненційно ускладнює атаку, тоді як збільшення коефіцієнта розтягу s полегшує її за рахунок зростання кількості колізій. Правильний вибір позиції AND є критичним: розташування в кінці та на початку забезпечує найкращий баланс.

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904



а



б

Рис. 3. Результати дослідження впливу розміру початкового насіння та розтягу на: а - середньої кількості вгадувань; б - середньої кількості колізій

Обговорення результатів

Аналіз отриманих результатів (рис. 1-4) дозволяє зробити кілька ключових висновків щодо стійкості генератора Гольдрайха до атака типу “вгадай та визнач”.

Вплив позиції AND. Предикати з AND всередині є значно більш вразливими, ніж з AND на початку або в кінці. При $s = 1{,}35$ та $n = 64$ успішність атаки для W_5 та E_5 становить 40% та 41%, тоді як для P_5 та Q_5 – лише 6-7% (рис. 1). Це пояснюється меншою кількістю колізій для W_5 та E_5 (рис. 4) та, відповідно, більшою кількістю необхідних вгадувань (рис. 3).

Вплив коефіцієнта розтягу s. Збільшення s призводить до зростання кількості колізій (рис. 4). Наприклад, для P_5 при $n = 64$ колізії збільшуються з 12 ($s = 1{,}15$) до 56 ($s = 1{,}35$). Відповідно, успішність атаки зростає (рис. 1), а кількість вгадувань зменшується (рис. 3). Однак при $s = 1{,}35$ час атаки для W_5 та E_5 значно нижчий (35-36 мс), ніж при $s = 1{,}25$ (92-93 мс), що свідчить про нелінійний характер залежності.

Вплив розміру початкового значення n. Збільшення n очікувано знижує успішність атаки для всіх предикатів (рис. 1). Наприклад, для P_5 при $s = 1{,}15$ успішність падає з 46% ($n = 16$) до 25% ($n = 64$). Час атаки також зростає зі збільшенням n (рис. 2).

Лінійний предикат. Як і очікувалося, він демонструє 100% успішності при атаці методом Гаусса (рис. 1) та мінімальний час виконання (рис. 2), що підтверджує необхідність нелінійності для криптографічної стійкості.

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

Масштабованість та застосовність до більших параметрів

Отримані експериментальні дані для розміру початкового насіння меншого або рівного за 64 біт демонструють чітку закономірність: успішність атаки знижується зі збільшенням n, а час атаки зростає. Згідно з теоретичними оцінками [16, 18], складність атаки масштабується як 2^l, де $l = n^{2-s}$. Виявлена залежність дозволяє припустити, що для практичних розмірів псевдовипадкових послідовностей, які більші за 128 бітів, атака типу "вгадай та визнач" залишається обчислювально складною. Кількісна оцінка ефективності методів для таких параметрів потребує застосування високопродуктивних обчислень.

Висновки

У роботі досліджено вплив позиції нелінійного елемента AND на стійкість генератора Гольдрайха до атаки типу "вгадай та визнач" для різних довжин початкових значень n (16, 32, 48, 64) та коефіцієнту розтягу s (1,15; 1,20; 1,25; 1,30; 1,35). Встановлено, що предикати з AND всередині є значно більш вразливими, ніж з AND на початку або в кінці. Збільшення коефіцієнта розтягу підвищує успішність атаки за рахунок зростання кількості колізій, тоді як збільшення розміру початкового значення знижує її внаслідок експоненційного зростання простору станів. Лінійний предикат є криптографічно нестійким, що підтверджує необхідність нелінійності. Найкращий баланс між стійкість та обчислювальною складність атаки забезпечують предикати з AND в кінці та на початку.

Експериментально перевірено статистичні властивості вихідних послідовностей генератора Гольдрайха для криптографічно стійких параметрів (n = 512, s = 1,6). За результатами тестування за стандартом FIPS 140-1 (монобітний, покер-тест, аналіз серій та максимальних довжин) встановлено, що згенерована послідовність об'ємом 20 000 біт задовольняє вимогам випадковості та є придатною для використання в криптографічних цілях.

Отримані результати можуть бути використані при проєктуванні безпечніших криптографічних генераторів, а також для прогнозування їхньої поведінки при збільшенні розміру насіння.

Перелік посилань

1. Röck A. Pseudorandom number generators for cryptographic applications [Electronic resource]: Master's thesis / A. Röck, Paris-Lodron-Universität Salzburg, 2005. 131 p. Mode of access: https://www-roc.inria.fr/secret/Andrea.Roeck/pdfs/dipl.pdf.

2. Кіх М. Комплексне криптографічне оцінювання гібридного генератора псевдовипадкових послідовностей на основі аудіоентропії та нелінійних булевих функцій / М. Кіх, О. Нємкова // Кібербезпека: освіта, наука, техніка. 2025. Том 31, № 3. P. 270–282. https://doi.org/10.28925/2663-4023.2025.31.1020.

3. Мандрона М. Атаки на генератори псевдовипадкових чисел / М. Мандрона, О. Гарасимчук // Вісник Національного університету "Львівська політехніка". Серія: Автоматика, вимірювання та керування. 2012. № 741. P. 251–256. Mode of access: https://ena.lpnu.ua/items/f0830f09-b7b1-4750-b462-6d9c0006e9f1.

4. Цебак О. Методи оцінки якості та криптостійкості послідовностей, згенерованих генераторами псевдовипадкових чисел / О. Цебак, С. Войтусік // Сучасний захист інформації. 2025. Том 64, № 4. P. 164–171. https://doi.org/10.31673/2409-7292.2025.041218.

5. Горячий О. Дослідження множини початкових значень генераторів псевдовипадкових чисел на основі арифметики з рухомою комою / О. Горячий, В. Максимович, М. Шабатура // Сучасний захист інформації. 2024. Том 58, № 2. P. 91–102. https://doi.org/10.31673/2409-7292.2024.020011.

6. Kelsey J. Cryptanalytic attacks on pseudorandom number generators / J. Kelsey, B. Schneier, D. Wagner, C. Hall // Fast Software Encryption Workshop (FSE 1998). Lecture Notes in Computer Science, Springer, Vol. 1372, 1998. P. 168–188. https://doi.org/10.1007/3-540-69710-1_12.

7. Горячий О. Розроблення генераторів псевдовипадкових чисел на основі покращених методів обчислення елементарних функцій для задач кібербезпеки [Електронний ресурс] : Дисертація доктора філософії / О. Горячий Національний університет "Львівська політехніка", Львів, 2025. 288 р. Режим доступу: https://lpnu.ua/sites/default/files/2025/radaphd/32585/disertaciya-goryachogo-o-ya.pdf.

8. Almaraz Luengo E. Cryptographically secured pseudo-random number generators: analysis and testing with NIST statistical test suite / E. Almaraz Luengo, J. Román Villaizán // Mathematics. 2023. Vol. 11, no. 23. 4812. https://doi.org/10.3390/math11234812.

9. Ruhault S. Security analysis for pseudo-random number generators [Electronic resource] : Doctoral thesis / S. Ruhault, Ecole normale supérieure, 2015. 156 p. Mode of access: https://theses.hal.science/tel-01236602v2.

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

10. Goldreich O. Candidate one-way functions based on expander graphs / O. Goldreich // IACR Cryptology ePrint Archive. 2000. Report 2000/063. Mode of access: https://www.wisdom.weizmann.ac.il/~oded/COL/ow-cand.pdf.

11. Mossel E. On ε-biased generators in NC⁰ / E. Mossel, A. Shpilka, L. Trevisan // 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2003). IEEE, 2003. P. 136–145. Mode of access: https://faculty.wharton.upenn.edu/wp-content/uploads/2014/07/On_Biased_Generators_in_NC0_1.pdf.

12. Applebaum B. Cryptography in NC⁰ / B. Applebaum, Y. Ishai, E. Kushilevitz // SIAM Journal on Computing. 2006. Vol. 36, no. 4. P. 845–888. Mode of access: https://www.wisdom.weizmann.ac.il/~bennyap/pubs/nc0.pdf.

13. Applebaum B. Pseudorandom generators with long stretch and low locality from random local one-way functions / B. Applebaum // SIAM Journal on Computing. 2013. Vol. 42, no. 5. P. 2008–2037. Mode of access: https://eccc.weizmann.ac.il/report/2011/007/download/.

14. O'Donnell R. Goldreich's PRG: Evidence for near-optimal polynomial stretch / R. O'Donnell, D. Witmer // IEEE 29th Conference on Computational Complexity (CCC 2014). IEEE, 2014. P. 1–12. Mode of access: https://www.cs.cmu.edu/~dwitmer/papers/csp-prg.pdf.

15. Applebaum B. Algebraic attacks against random local functions and their countermeasures / B. Applebaum, S. Lovett // 48th Annual ACM Symposium on Theory of Computing (STOC 2016). ACM, 2016. P. 1087–1100. Mode of access: https://dl.acm.org/doi/epdf/10.1145/2897518.2897554.

16. Couteau G. On the concrete security of Goldreich's pseudorandom generator / G. Couteau, A. Dupin, P. Méaux, M. Rossi, Y. Rotella // International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018). – Springer, 2018. P. 96–124. Mode of access: https://eprint.iacr.org/2018/1162.pdf.

17. Couteau G. On the concrete security of Goldreich's pseudorandom generator [Electronic resource] / G. Couteau, A. Dupin, P. Méaux, M. Rossi, Y. Rotella // ASIACRYPT 2018. 2018. Mode of access: https://asiacrypt.iacr.org/2018/files/SLIDES/TUESDAY/421/slides_PRG.pdf.

18. Yang J. Revisiting the concrete security of Goldreich's pseudorandom generator / J. Yang, Q. Guo, T. Johansson, M. Lentmaier // IEEE Transactions on Information Theory. 2020. Mode of access: https://ieeexplore.ieee.org/document/9615074.

19. Applebaum B. Structured-seed local pseudorandom generators and their applications / B. Applebaum, D. Bui, G. Couteau, N. Melissaris // IACR Cryptology ePrint Archive. 2024. Report 2024/1027. Mode of access: https://eprint.iacr.org/2024/1027.pdf.

20. Fu X. Attacks on Goldreich's pseudorandom generators by grouping and solving / X. Fu, M. Li, S. Lyu, C. Liu // IACR Cryptology ePrint Archive. 2024. Report 2024/1594. Mode of access: https://eprint.iacr.org/2024/1594.pdf.

Oleh Horyachyi
PhD, Senior Lecturer, Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0003-4948-458X
E-mail: oleh.y.horiachyi@lpnu.ua

Artem Yurchenko
4th year student of the Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0000-3007-1430
E-mail: artem.yurchenko.kb.2022@lpnu.ua

ANALYSIS OF THE EFFECTIVENESS OF THE "GUESS AND DETERMINE" ATTACK ON THE GOLDREICH PSEUDORANDO SEQUENCE GENERATOR WITH THE MODIFIED P_5 PREDICT

This article investigates the stability of a Goldreich pseudorandom sequence generator of complexity class NC⁰ with different locality 5 predicates to a "guess-and-determine" attack. The generator is a local one, in which each output bit depends only on a fixed number of input bits, which ensures high performance and parallelism of calculations. Five variants of the P_5 predicate are considered, differing in the position of the nonlinear element (AND): at the beginning, inside, and at the end of the Boolean function, as well as, for comparison, a linear predicate. The aim of the work is to determine the influence of the location of the AND element and other generator parameters on the effectiveness of the attack, in particular, on the success rate, execution time, number of necessary guesses, and number of collisions. Experimental studies have been conducted for the sizes of the initial values n = 16, 32, 48, 64 and different stretch coefficients s = 1.15; 1.20; 1.25; 1.30; 1.35. It was found that the position of the AND operation and the parameters n and s significantly affect the stability of the generator. The Gaussian method can restore the initial value with a probability of more than 90%, which confirms the need to use nonlinear elements to ensure cryptographic stability. Predicates with AND at the beginning or end provide the highest attack success for small values of n and s, but are characterized by a longer execution time. In contrast, the proposed predicates with AND inside turned out to be more stable for small s,

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

especially with increasing size n. It was found that increasing the stretch factor s simplifies the attack due to the increase in the number of collisions, while increasing the seed size n, on the contrary, reduces its effectiveness due to the exponential growth of the state space. The results obtained clarify the influence of the predicate structure and parameters of the Goldreich generator on its stability and can serve as a theoretical basis for predicting their behavior with increasing n and designing more secure cryptographic generators.

Keywords: pseudorandom sequence generator, Goldreich generator, cryptanalysis, “guess-and-determine” attack, low locality, nonlinearity, collisions.

Надійшла до редакції (Received): 13.04.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

УДК 004.8:004.056:004.75 DOI: 10.31673/2409-7292.2026.024106

Костюк Юлія Володимирівна
доктор філософії, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-5423-0985
E-mail: y.kostiuk@kubg.edu.ua

Складанний Павло Миколайович
кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-7775-6039
E-mail: p.skladannyi@kubg.edu.ua

Кучаковська Галина Андріївна
кандидат педагогічних наук, старший викладач кафедри комп’ютерних наук
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-4555-896X
E-mail: h.kuchakovska@kubg.edu.ua

ІНТЕЛЕКТУАЛЬНА ІНФОРМАЦІЙНА СИСТЕМА АДАПТИВНОГО ВИЯВЛЕННЯ АНОМАЛІЙ У РОЗПОДІЛЕНИХ СЕРЕДОВИЩАХ НА ОСНОВІ ГІБРИДНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ

У статті розглянуто проблему виявлення аномалій у розподілених інформаційних середовищах, що функціонують в умовах динамічних навантажень, високої інтенсивності інформаційних потоків, неоднорідності даних та зростання кіберзагроз. Актуальність дослідження зумовлена розвитком хмарних технологій, Internet of Things (IoT) та систем обробки великих даних, що ускладнює моніторинг стану інформаційних систем і потребує застосування інтелектуальних методів аналізу. Встановлено, що традиційні підходи, засновані на статичних правилах і порогових значеннях, не забезпечують достатньої точності та адаптивності, що призводить до помилкових спрацьовувань або пропуску критичних подій. Метою дослідження є розроблення інтелектуальної інформаційної системи адаптивного виявлення аномалій на основі гібридних моделей штучного інтелекту. Для її досягнення використано нейронні мережі, методи машинного навчання та нечітку логіку. Запропоновано архітектуру системи з модулями збору даних, прогнозування, виявлення аномалій та прийняття рішень. Розроблено математичну модель оцінювання аномалій на основі відхилення між фактичними та прогнозованими параметрами, а також інтегральний показник з урахуванням вразливості та критичності. Реалізовано механізм нечіткого логічного виведення для формування керуючих впливів. Проведено імітаційне моделювання для різних сценаріїв, що підтвердило підвищення точності виявлення аномалій, зменшення помилкових спрацьовувань і скорочення часу реагування системи.

Ключові слова: інтелектуальна інформаційна система; хмарні технології; розподілені системи; виявлення аномалій; машинне навчання; нейронні мережі; нечітка логіка; адаптивні системи; штучний інтелект.

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904