

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРАВИЛ ЕЛЕМЕНТАРНИХ КЛІТИННИХ АВТОМАТІВ ДЛЯ МОДИФІКАЦІЇ ДЕРЕВОПОДІБНОЇ ГЕШ-ФУНКЦІЇ

¹ Вінницький національний технічний університет

Анотація

У роботі розглянуто правила елементарних клітинних автоматів як інструмент формування складної бітової динаміки, що може бути використана для модифікації деревоподібних геш-функцій. Увагу дослідження зосереджено на порівнянні правил елементарних клітинних автоматів як дискретних динамічних систем. Аналіз здійснюється з урахуванням таких властивостей, як схильність до виродження або періодичності, швидкість поширення локальних збурень, баланс нулів та одиниць, ентропійні характеристики, наявність просторово-часових кореляцій і загальна складність поведінки. Особливий інтерес становлять правила, що демонструють хаотичну або близьку до хаотичної динаміку, оскільки саме вони можуть бути найбільш придатними для використання як додатковий шар перетворення в ієрархічних структурах обробки даних. Порівняльний підхід дає змогу встановити, які з правил мають найкраще поєднання нелінійності, дифузії та статистичної збалансованості, а отже можуть розглядатися як найбільш перспективні для подальшого застосування в модифікації деревоподібних геш-функцій.

Ключові слова: елементарний клітинний автомат, правила клітинних автоматів, деревоподібна геш-функція, дерево Merkle, нелінійне змішування, хаотична динаміка, ентропія.

Abstract

The paper examines the rules of elementary cellular automata as a tool for generating complex bit dynamics that can be used to modify tree-based hash functions. The study focuses on comparing elementary cellular automaton rules as discrete dynamical systems. The analysis is carried out with regard to such properties as the tendency toward degeneration or periodicity, the rate of propagation of local perturbations, the balance of zeros and ones, entropy characteristics, the presence of spatiotemporal correlations, and the overall complexity of behavior. Particular interest is devoted to rules that demonstrate chaotic or near-chaotic dynamics, since they may be the most suitable for use as an additional transformation layer in hierarchical data processing structures. The comparative approach makes it possible to determine which rules provide the best combination of nonlinearity, diffusion, and statistical balance and therefore can be considered the most promising for further application in the modification of tree-based hash functions.

Keywords: elementary cellular automaton, cellular automaton rules, tree-based hash function, Merkle tree, nonlinear mixing, chaotic dynamics, entropy.

Вступ

У сучасних інформаційних системах криптографічні геш-функції є одним із базових засобів забезпечення цілісності даних, автентифікації та захисту інформації. Особливе місце в цій сфері посідають деревоподібні геш-функції, зокрема структури типу дерева Merkle, які дають змогу ефективно працювати з великими обсягами даних завдяки ієрархічній організації обчислень [1]. Водночас зростання вимог до криптографічної стійкості таких конструкцій стимулює пошук додаткових механізмів нелінійного змішування, здатних посилити дифузійні властивості та ускладнити структуру перетворення.

Одним із перспективних підходів до розв'язання цієї задачі є використання елементарних клітинних автоматів. Клітинні автомати розглядаються як дискретні обчислювальні моделі, у яких глобальна поведінка системи формується на основі простих локальних правил взаємодії клітин [1]. Дослідження показують, що навіть найпростіші одновимірні автомати можуть демонструвати самоорганізацію, складну просторово-часову динаміку та хаотичні режими еволюції [1-2]. Саме ці властивості роблять їх привабливими для застосування в задачах криптографічного перетворення даних.

Суттєвою особливістю елементарних клітинних автоматів є те, що різні правила породжують принципово різні типи поведінки: від швидкого переходу до однорідних або періодичних конфігура-

цій до формування складних, нестійких і статистично насичених структур [1-2]. Тому використання клітинних автоматів у модифікації деревоподібної геш-функції потребує попереднього порівняльного аналізу правил, їхніх динамічних характеристик і придатності до реалізації функції нелінійного змішування. З огляду на це, актуальним є встановлення тих правил елементарних клітинних автоматів, які найкраще поєднують складність поведінки, чутливість до початкових умов, добру дифузію та відсутність очевидного виродження [2-4].

Результати дослідження

Клітинні автомати є дискретними обчислювальними моделями, що складаються з множини клітин, кожна з яких у певний момент часу перебуває в одному зі скінченних станів, а перехід до нового стану визначається локальним правилом залежно від стану самої клітини та її сусідів [1-2]. Для таких систем простір, час і множина станів є дискретними, тоді як складна глобальна поведінка формується внаслідок багаторазового застосування простих локальних правил. Саме ця властивість робить клітинні автомати зручним інструментом для дослідження самоорганізації, складної динаміки та механізмів породження структур із простих обчислювальних схем.

Найпростішим і водночас одним із найважливіших класів є елементарні клітинні автомати, які являють собою одновимірний масив двійкових клітин, де новий стан кожної клітини визначається її власним станом і станами двох найближчих сусідів. Для такої моделі існує 256 можливих правил еволюції. Попри простоту побудови, елементарні клітинні автомати здатні демонструвати широкий спектр поведінки – від швидкого переходу до однорідних або періодичних конфігурацій до складної хаотичної та локалізовано-складної динаміки [1-2]. У дослідженнях клітинних автоматів поширеним є поділ правил за характером еволюції на такі, що ведуть до стабільного стану, до періодичних структур, до хаотичної поведінки або до складної динаміки з локальними структурами. Для задач, пов'язаних із нелінійним змішуванням, найбільший інтерес становлять саме ті правила, які не вироджуються в простий цикл або стабільну конфігурацію, а забезпечують високу чутливість до початкових умов, добру дифузію локальних змін і складну просторово-часову поведінку.

У межах даного дослідження доцільно зосередитися саме на елементарних одновимірних двійкових клітинних автоматах, оскільки вони є достатньо простими для формального опису, мають чітко визначений набір правил і водночас дозволяють отримати репрезентативне порівняння різних типів динаміки. З огляду на це, для подальшого аналізу доцільно обрати правила 30, 90, 105 і 150. Такий вибір дає змогу зіставити правила з різною природою еволюції: правило 30 традиційно розглядається як приклад правила зі складною та хаотичною поведінкою, тоді як правило 90 і правило 150 є показовими прикладами адитивних правил, а правило 105 доцільно включити як проміжний варіант для порівняння різних режимів формування бітової динаміки [4-6].

Аналіз виконувався для різних ширин решітки та різних крайових умов. Основними критеріями оцінювання були середня відстань Хеммінга між двома траєкторіями, що відрізнялися одним бітом у початковому стані, частка одиниць, бінарна ентропія, автокореляція та наявність циклічної поведінки.

Для прикладного етапу було змодельовано вузол деревоподібної геш-функції, у якому вхід формувалася з двох 256-бітових дочірніх значень. Початковий 512-бітовий стан задавався асиметричним перетворенням лівої та правої гілок із використанням циклічних зсувів і фіксованих бітових масок. Після цього стан еволюціонував за вибраним правилом клітинного автомата протягом 16, 32, 64, 96, 128, 160, 192 та 256 раундів, а потім стискався до 256-бітового виходу. Оцінювання виконувалося за лавинним ефектом, чутливістю до перестановки дочірніх значень, балансом вихідних бітів, середньою ентропією бітових позицій, середнім бітовим зміщенням та автокореляцією. Для кожної конфігурації виконувалося 500 незалежних запусків. В табл. 1 зображено найкращі результати тестів для кожного із правил.

Таблиця 1. Найкращі результати для досліджених правил

Правило	Оптимальна кількість раундів	Середній лавинний ефект, %	Чутливість до перестановки гілок, %	Частка одиниць, %	Середня ентропія бітових позицій	Середнє бітове зміщення
30	256	49,89	50,00	49,91	0,9987	0,0169
90	160	7,32	49,98	49,93	0,9986	0,0174
105	160	15,20	50,28	50,22	0,9986	0,0165
150	160	15,20	50,28	50,22	0,9986	0,0165

Отримані результати показали, що правило 30 суттєво переважає інші досліджені правила з погляду придатності до використання у вузлі деревоподібної геш-функції. На відміну від правил 90, 105 і 150, правило 30 демонструє стабільне зростання лавинного ефекту зі збільшенням кількості раундів і вже в діапазоні 96-128 кроків досягає значень, близьких до теоретично бажаних 50 %. Зокрема, при 128 раундах середній лавинний ефект для правила 30 становив 49,70 %, а при 160-256 раундах залишався на рівні 49,9-50,1 %. При цьому різниця між впливом змін у лівій та правій гілках була практично відсутня, а чутливість до перестановки дочірніх значень також наближалася до 50 %, що свідчить про належну асиметричність вузла та добру дифузію змін у внутрішньому стані.

Натомість правила 105 і 150 продемонстрували лише помірну здатність до поширення локальних збурень: їх максимальний середній лавинний ефект становив близько 15,2 % при 160 раундах, після чого знову знижувався. Правило 90 виявилось найменш придатним до поставленої задачі: в усіх конфігураціях воно демонструвало низькі значення лавинного ефекту, а при 256 раундах вироджувалося у тривіальний стан із нульовою ентропією та повною кореляцією. Водночас показники балансу нулів та одиниць, ентропії бітових позицій і автокореляції для більшості правил залишалися близькими до оптимальних, тому основним чинником вибору правила стала саме швидкість і повнота досягнення лавинного ефекту. Детальні результати для правила 30 залежно від кількості раундів наведено в табл. 2.

Таблиця 2. Залежність характеристик правила 30 від кількості раундів

Кількість раундів	Середній лавинний ефект, %	Чутливість до перестановки гілок, %	Частка одиниць, %
16	19,54	49,89	50,08
32	31,36	50,22	49,58
64	44,44	50,06	50,00
96	48,61	49,98	49,98
128	49,70	49,89	50,17
160	49,97	50,22	49,97
192	50,09	49,85	50,10
256	49,89	50,00	49,91

Як видно з табл. 2, зростання кількості раундів для правила 30 приводить до швидкого підвищення лавинного ефекту, який уже при 128 раундах досягає майже оптимального значення. Подальше збільшення кількості раундів не дає суттєвого покращення результату, тому діапазон 128–160 раундів можна вважати практично доцільним. Для наочності результату на рис.1 відображено залежність лавинного ефекту від кількості раундів для правила 30 в порівнянні з ідеальним лавинним ефектом 50,00.



Рис. 1. Залежність лавинного ефекту від кількості раундів для правила 30

З урахуванням отриманих результатів правило 30 слід розглядати як найперспективніше для подальшого використання в механізмі бітового змішування деревоподібної геш-функції. Практично доці-

льним компромісом між якістю змішування та обчислювальною вартістю можна вважати використання близько 128 раундів, оскільки подальше збільшення їх кількості вже не дає суттєвого приросту якості.

Висновки

У роботі проведено порівняльний аналіз правил 30, 90, 105 і 150 елементарних клітинних автоматів з метою вибору найбільш придатного правила для використання як механізму бітового змішування у вузлі деревоподібної геш-функції. Показано, що серед досліджених правил саме правило 30 демонструє найкраще поєднання динамічної складності, чутливості до локальних змін, статистичної збалансованості та дифузійних властивостей.

У межах прикладно-орієнтованої моделі вузла дерева встановлено, що правило 30 забезпечує стійке зростання лавинного ефекту зі збільшенням кількості раундів і вже при 128 раундах досягає значення 49,70 %, тобто практично оптимального рівня. Подальше збільшення кількості раундів до 160-256 не дає суттєвого покращення результату, що дозволяє розглядати діапазон 128-160 раундів як доцільний компроміс між якістю змішування та обчислювальною вартістю.

Показано, що правила 105 і 150 мають близькі між собою характеристики, однак поступаються правилу 30 за повнотою поширення локальних збурень і не досягають необхідного рівня лавинного ефекту. Правило 90 виявилось найменш придатним до поставленої задачі, оскільки демонструє низькі значення лавинного ефекту, а в окремих конфігураціях вироджується у тривіальний стан. Отже, правило 30 доцільно розглядати як найбільш перспективну основу для подальшої модифікації деревоподібної геш-функції.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Wolfram S. Statistical mechanics of cellular automata // Reviews of Modern Physics. 1983. Vol. 55, № 3. P. 601-644.
2. Wolfram S. A New Kind of Science. Champaign, IL : Wolfram Media, 2002. 1197 p.
3. Merkle R. C. Protocols for public key cryptosystems // Proceedings of the 1980 IEEE Symposium on Security and Privacy. Oakland, CA, 1980. P. 122-134.
4. ElRakaiby M. M. Cryptographic hash function using cellular automata // International Journal of Computer Applications Technology and Research. 2016. Vol. 5, Issue 5. P. 238-240.
5. Belfedhal A. E., Faraoun K. M. Building secure and fast cryptographic hash functions based on cellular automata // Information Sciences. 2015. Vol. 290. P. 283-297.
6. Vaughn R., Borowczak M. Strict Avalanche Criterion of SHA-256 and sub-function-removed variants // Cryptography. 2024. Vol. 8, № 3. Article 40.

Баришев Юрій Володимирович — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Казміревський Віталій Віталійович — аспірант групи 125-23а, інститут докторантури та аспірантури, Вінницький національний технічний університет, Вінниця, e-mail: kazmirevskiy1999@gmail.com

Baryshev Yuri V. — Cand. Sc. (Eng), Associate Professor of Information Security, Vinnytsia National Technical University, Vinnytsia

Kazmirevskiy Vitalii V. — PhD student, group 125-23a, Institute of Doctoral and Postgraduate Studies, Vinnytsia National Technical University, Vinnytsia, email: kazmirevskiy1999@gmail.com