УДК 004.056.55

Н. Р. Григорук

АНАЛІЗ КОНСТРУКЦІЙ ГЕШУВАННЯ

Вінницький національний технічний університет

Анотація

У роботі розглянуто різні конструкції криптографічних геш-функцій, зокрема деревоподібні, графові та ітеративні підходи. Проаналізовано принципи побудови дерев Меркля, спрямованих ациклічних графів та класичних послідовних схем гешування. Розглянуто альтернативні конструкції, зокрема «губку» та HAIFA, а також гібридні та паралельні схеми. Проведено порівняльний аналіз їх стійкості до колізій, мультиколізій та атак подовження повідомлення. Показано особливості застосування різних конструкцій у системах електронного цифрового підпису, блокчейн-технологіях і постквантових криптографічних рішеннях.

Ключові слова: геш-функції, дерево Меркля, Merkle DAG, губка, HAIFA, колізії, електронний підпис, блокчейн, криптографія.

Abstract

The paper examines various constructions of cryptographic hash functions, including tree-based, graph-based, and iterative approaches. The principles of Merkle trees, directed acyclic graphs, and classical sequential hashing schemes are analyzed. Alternative constructions, such as the sponge and HAIFA, as well as hybrid and parallel hashing schemes, are considered. A comparative analysis of their resistance to collisions, multicollisions, and length-extension attacks is provided. The applicability of different constructions in digital signature systems, blockchain technologies, and post-quantum cryptographic solutions is discussed.

Keywords: hash functions, Merkle tree, Merkle DAG, sponge, HAIFA, collisions, digital signature, blockchain, cryptography.

Вступ

Сучасна криптографія стикається з критичною проблемою вразливості класичних геш-функцій до нових типів атак, таких як колізійні атаки та атаки на знаходження мультиколізій. Геш-функції є фундаментальним компонентом забезпечення цілісності даних у файлових системах, функціонування технологій блокчейн та електронних цифрових підписах, де вони дозволяють підписувати стислий відбиток повідомлення замість усього обсягу даних [1]. Порівняння різних конструкцій гешування є актуальним для вибору найбільш стійких алгоритмів, що відповідають сучасним вимогам безпеки.

Метою роботи є удосконалення безпеки інформаційних систем, що використовують геш-функції шляхом проведення порівняльного аналізу деревоподібних структур гешування у зіставленні з альтернативними послідовними та графовими конструкціями.

Результати дослідження

Фундаментальна концепція дерев Меркля полягає у використанні бінарної деревної структури для швидкої верифікації цілісності великих наборів даних, де кінцеві вузли дерева містять геші блоків даних, а кожен батьківський вузол формується з гешу конкатенації своїх дочірніх вузлів. Залежно від коефіцієнта розгалуження виділяють кілька типів структур. Бінарні дерева з двома дочірніми вузлами є класичним стандартом, що забезпечує логарифмічну складність верифікації, проте при значній кількості листків глибина дерева може стати критичною для продуктивності [2]. Четвіркові дерева мають чотири дочірні вузли та дозволяють ефективніше розпаралелювати обчислення на сучасних архітектурах, що є особливо актуальним для обробки двовимірних масивів даних. Вісімкові дерева з вісьмома вузлами оптимізовані для тривимірного простору, суттєво зменшуючи глибину дерева, але збільшуючи обчислювальне навантаження на кожному окремому вузлі [3].

Нециклічні структури, до яких належать класичні дерева, є ациклічними графами, де шлях від кореня до листка завжди є унікальним, що спрощує процедуру перевірки. Натомість циклічні структури дозволяють створення зворотних посилань, утворюючи петлі в графі обчислень. Порівняння цих підходів демонструє суттєві відмінності у складності верифікації та ефективності

використання пам'яті. Нециклічні структури мають фіксовану складність перевірки та високу ефективність пам'яті, тоді як циклічні структури вимагають складних алгоритмів для уникнення зациклень та керування станом пам'яті. Саме через вразливість до атак, пов'язаних із пошуком циклів, та складність реалізації, нециклічні структури безальтернативно використовуються в системах блокчейн та алгоритмах електронного цифрового підпису [2].

Спрямований ациклічний граф Меркля (Merkle DAG) представляє собою еволюцію деревоподібних структур, де кожен вузол може мати декілька батьківських вузлів, на відміну від суворої ієрархії дерева. Ключовими властивостями такої структури є спрямованість ребер та відсутність циклів, що дозволяє різним гілкам спільно використовувати одні й ті самі дочірні вузли [3]. Ця особливість надає графовим конструкціям значні переваги у вигляді автоматичної дедуплікації даних, оскільки однакові блоки інформації представлені єдиним вузлом, що критично важливо для таких систем, як IPFS та Git. Проте ці переваги супроводжуються певними викликами, зокрема підвищеною складністю алгоритмів обходу графа порівняно з простими деревами.

Найбільш поширеною історично є конструкція Меркля-Дамгаарда, яка обробляє блоки даних ітеративно і лежить в основі багатьох класичних стандартів. Незважаючи на доведену стійкість до колізій при використанні ідеальної функції стиснення, ця конструкція має критичну вразливість до атак подовження повідомлення [1]. Альтернативою виступає конструкція "Губка" (Sponge), яка працює у фазах поглинання та витискання [1, 3]. Вона принципово відрізняється від Меркля-Дамгаарда відсутністю зовнішніх змінних ланцюжка, що робить її природно стійкою до атак подовження. Також існує конструкція HAIFA, яка є вдосконаленою версією Меркля-Дамгаарда з додаванням лічильників бітів та солі для кожного блоку, що нівелює недоліки попередника [4].

Гібридні підходи поєднують переваги деревоподібних структур для забезпечення необмеженого паралелізму та послідовного гешування для високої швидкості на малих обсягах даних. Іншим прикладом є стандартизована конструкція паралельного гешування (наприклад, ParallelHash), яка досягає високої продуктивності шляхом розбиття вхідних даних на незалежні блоки для паралельної обробки з подальшим об'єднанням результатів, що робить її ідеальною для сучасних багатоядерних процесорів [1].

Атака колізій має на меті пошук двох різних повідомлень з однаковим гешем, і для ідеальної функції її складність становить O(2^n/2). Деревоподібні та графові конструкції демонструють високу стійкість, успадковуючи властивості базової функції стиснення, тоді як класичні послідовні конструкції виявилися вразливими на практиці через алгоритмічні слабкості етапу стиснення [1]. Атака Жукса є специфічним вектором загрози для ітеративних геш-функцій, дозволяючи знаходити велику кількість повідомлень з однаковим гешем зі значно меншою складністю, ніж повний перебір. Класичні ітеративні конструкції є вразливими до цієї атаки. Найкращий захист демонструють конструкції HAIFA завдяки використанню лічильників та солі, а також конструкції з широким каналом, які збільшують внутрішній стан геш-функції [4]. Стійкість до знаходження першого та другого прообразів є базовою вимогою безпеки, де складність атаки має наближатися до O(2^n). Хоча більшість сучасних конструкцій є стійкими, довгі повідомлення в класичних ітеративних схемах можуть піддаватися специфічним атакам, що зменшують ефективну складність пошуку другого прообразу [4].

Узагальнені результати порівняльного аналізу основних конструкцій гешування за критеріями топології, можливостей дедуплікації, паралелізації та стійкості до атак наведено в таблиці 1.

Таблиця 1. Порівняльна характеристика структур гешування

Критерій порівняння	Деревоподібна (Merkle Tree)	Графова (Merkle DAG)	Ітеративна (Merkle-Damgård)	Губка (Sponge)
Топологія	Ієрархічне дерево	Ациклічний граф	Послідовний ланцюг	Стан перестановки
Дедуплікація	Відсутня	Вбудована	Відсутня	Відсутня
Паралелізація	Висока	Висока	Відсутня	Обмежена
Стійкість до подовження	Висока	Висока	Низька	Висока
Стійкість до мультиколізій	Середня	Висока	Низька	Висока

Використання геш-функцій є критично важливим етапом формування електронного цифрового підпису, оскільки підписується саме геш, а не вихідний документ. Для класичних схем ЕЦП рекомендується перехід від застарілих ітеративних конструкцій, вразливих до атак подовження, до конструкцій типу "Губка". Ці структури забезпечують вищий рівень криптографічної гнучкості та безпеки, дозволяючи генерувати дайджести довільної довжини без загрози компрометації внутрішнього стану [5]. У контексті постквантової криптографії, де використовуються геш-базовані підписи, критично важливими стають саме деревоподібні структури. Вони дозволяють ефективно керувати станом підпису та верифікувати окремі гілки без розкриття всього дерева, що є фундаментом для схем одноразових та багаторазових підписів нового покоління. Модифіковані ітеративні конструкції з посиленням (наприклад, HAIFA) також залишаються актуальними для національних стандартів завдяки стійкості до мультиколізій.

Висновок

Проведений аналіз дозволяє стверджувати, що вибір конструкції гешування має базуватися на конкретних вимогах системи до продуктивності та безпеки. Ітеративні конструкції, хоча й є перевіреними часом, поступаються новітнім розробкам у стійкості до специфічних атак. Для завдань електронного цифрового підпису найбільш перспективними є конструкції типу "Губка" та спеціалізовані паралельні схеми. Деревоподібні конструкції демонструють найкращий потенціал для систем розподіленого зберігання даних та технологій блокчейн завдяки можливості верифікації частини даних без необхідності обробки всього масиву. Подальші дослідження мають бути спрямовані на вдосконалення графових структур для забезпечення балансу між ефективністю дедуплікації та швидкістю криптографічних перетворень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Al-Kuwari S., Davenport J. H., Bradford R. J. Cryptographic Hash Functions: Recent Design Trends and Security Notions / Department of Computer Science, University of Bath. Bath, 2011. 37 p. URL: https://eprint.iacr.org/2011/565.pdf (last access: 25.01.2026).
2. Preneel B. Analysis and Design of Cryptographic Hash Functions. February 2003. 338 p. URL: https://homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf (last access: 25.01.2026).
3. Sefid-Dashti B., Salimi Sartakhti J., Daghigh H. Brand New Categories of Cryptographic Hash Functions: A Survey. Electr. Comput. Eng. Innovations. 2023. Vol. 11, No 2. P. 335–354. URL: https://jecei.sru.ac.ir/article_1840.html (last access: 25.01.2026).
4. Лужецький В. А., Баришев Ю. В. Конструкції гешування стійкі до мультиколізій. Наукові праці ВНТУ. 2010. № 1. 8 с.
5. Ginting F. S. O., Zainal V. R., Hakim A. Digital Signature Standard Implementation Strategy by Optimizing Hash Functions Through Performance Optimization. Journal of Accounting and Finance Management. 2023. Vol. 3, No 6. P. 362–371. URL: https://www.researchgate.net/publication/370740247_Digital_Signature_Standard_Implementation_Strategy_by_Optimizing_Hash_Functions_Through_Performance_Optimization (last access: 25.01.2026).

Григорук Надія Романівна – студентка групи 2БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: grigoruknadia15@gmail.com

Науковий керівник: ***Баришев Юрій Володимирович*** – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua

Nadiia Hryhoruk – student of group 2BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: grigoruknadia15@gmail.com

Scientific supervisor: ***Yurii Baryshev*** – PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, yuriy.baryshev@vntu.edu.ua