The Method of Building a Quaternary Tree

Volodymyr Luzhetskyi
Department of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine
v.luzhetskyi@vntu.edu.ua

Dmytro Rohachevskyi
Department of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine
dimonrogach@gmail.com

Volodymyr Kozyra
Department of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine
vovakozira@gmail.com

Метод Побудови Кватернарного Дерева

Володимир Лужецький
Кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
v.luzhetskyi@vntu.edu.ua

Дмитро Рогачевський
Кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
dimonrogach@gmail.com

Володимир Козира
Кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
vovakozira@gmail.com

Abstract — A method for constructing a quaternary hash tree based on the convolution of four previous hash values is proposed. The reduction of the volume of intermediate hash values by about 1,5 times compared to binary Merkle trees is theoretically substantiated.

***Анотація* — Запропоновано метод побудови кватернарного геш-дерева на основі згортання чотирьох попередніх геш-значень. Теоретично обгрунтовано зменшення обсягу проміжних геш-значень приблизно в 1,5 рази порівняно з бінарними деревами Меркля.**

Keywords — hash value, binary hash tree, quaternary hash tree.

Ключові слова — геш-значення, бінарне геш-дерево, кватернарне геш-дерево.

I. Вступ

Будучи основним типом геш-дерева, дерева Меркля незамінні в блокчейні, розподілених системах і будь-якій програмі, яка вимагає цілісності даних. За своєю суттю, дерево Меркля є спеціалізованим видом геш-дерева.

Геш-дерево – це дерево, у якому кожен листовий вузол позначено криптографічним гешем даних, а кожен нелистовий вузол позначено гешем своїх дочірніх вузлів.

Хоча дерева Меркля є поняттям, яке застосовується в криптографії, їх застосування охоплює різні галузі:

Блокчейн: такі криптовалюти, як біткойн, використовують дерева Меркля для забезпечення узгоджених і непідроблених даних транзакцій у межах блоків [1].

Розподілені системи: дерева Меркля допомагають перевіряти дані в розподілених базах даних або файлових системах, гарантуючи, що репліки мають узгоджені дані [2].

Перевірки цілісності даних: програмні додатки або контентні мережі можуть використовувати дерева Меркля, щоб переконатися, що завантажені файли або фрагменти даних справжні та не підроблені [3].

Часто геш-дерева будують як збалансовані бінарні дерева, що забезпечують постійну глибину та

передбачувану продуктивність. Однак основною метою є не баланс, а надійна криптографічна перевірка даних.

Безумовно, такий метод є ефективним, але він вимагає зберігання багатьох даних для багатьох елементів. Тому запропоновано для обчислення проміжних значень брати не по 2 елементи, як в класичному дереві, а по 4 елементи. Таке дерево будемо називати *кватернарним* [4].

Метою роботи є зменшення обсягу геш-значень, що складають геш-дерево.

II. ГЕШ-ДЕРЕВА МЕРКЛЯ

Дерево Меркля або, іншими словами, геш-дерево, має структуру бінарного дерева, де геші даних у нижньому рядку називаються «листовими вузлами», проміжні геші — «нелистовими вузлами», а геш у верхній частині — «коренем». Попри те, що більшість реалізацій геш-дерева мають бінарний характер (кожен вузол має два дочірні вузли), дочірніх вузлів може бути набагато більше [5].

Приклад дерева Меркля для чотирьох даних m_1, m_2, m_3 і m_4 наведено на рис.1.

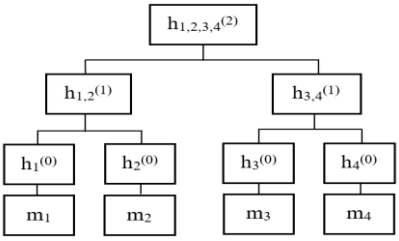

Рис. 1.Геш-дерево Меркля

Обсяг геш-значень дерева Меркля для n даних дорівнює:

$$C_2 = n + \sum_{i=0}^{k} 2^i,$$

де $k =]log_2 n[- 1.$

1. МЕТОД ПОБУДОВИ КВАТЕРНАРНОГО ДЕРЕВА

Для побудови кватернарного геш-дерева спочатку для всіх n даних формуються геш-значення. Після цього здійснюється згортання цих геш-значень за схемою кватернарного дерева до одного остаточного геш-значення. Приклад геш-дерева для 16 даних наведено на рис. 2.

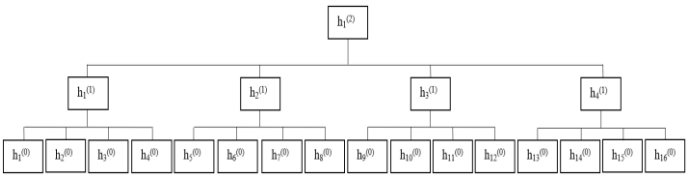

Рис. 2.Приклад кватернарного геш-дерева

Обсяг геш-значень кватернарного дерева для n даних дорівнює:

$$C_4 = n + \sum_{i=0}^{k} 4^i,$$

де $k =]log_4 n[- 1.$

Деякі обсяги геш-значень для бінарного і кватернарного дерев наведено в таб.1.

ТАБЛИЦЯ І. – ОБСЯГИ ГЕШ-ЗНАЧЕНЬ

Тип дерева	**Кількість даних**				
	256	1024	4096	16384	65536
Бінарне	511	2047	8191	32767	131071
Кватернарне	341	1365	5461	21845	87381

Аналіз цієї таблиці показує, що обсяг геш-значень кватернарного дерева в 1,5 рази менше, ніж для бінарного геш-дерева.

Особливість кватернарного дерева полягає в тому, що одночасно згортаються 4 попередні геш-значення. Схему цієї процедури наведено на рис. 3.

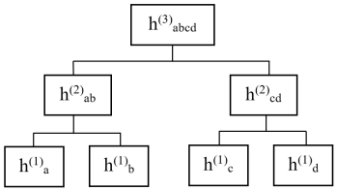

Рис. 3.Схема формування геш-значення з 4 елементів

III. ВИСНОВКИ

Теоретично в деревах кожен вузол може мати певну кількість дочірніх вузлів, однак найпоширенішими є бінарні дерева, в яких кожен вузол має два дочірні вузли.

Існують задачі, що вимагають побудови бінарних дерев для великої кількості даних і тому виникає потреба у зменшенні обсягу пам’яті для зберігання таких дерев.

Запропонований метод побудови кватернарного дерева забезпечує зменшення обсягу пам’яті для зберігання геш-дерева в 1,5 рази порівняно з використанням бінарного дерева.

ЛІТЕРАТУРА REFERENCES

[1] Дерево Меркля та його роль у блокчейні [Online]. Available: https://learn.bybit.com/uk/blockchain/what-is-merkle-tree/ [Accessed: 08-May-2024].

[2] Merkle Tree [Online]. Available: https://brilliant.org/wiki/merkle-tree/ [Accessed: 08-May-2024].

[3] Data verification & error detection with Merkle trees [Online]. Available: https://www.educative.io/answers/data-verification-error-detection-with-merkle-trees [Accessed: 08-May-2024].

[4] В. А. Лужецький та Ю. В. Баришев, “ПІДХІД ДО ПАРАЛЕЛЬНОГО ГЕШУВАННЯ ДАНИХ НА ОСНОВІ МОДЕЛІ КВАТЕРНІОНА”, у ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА ІНФОРМ. СИСТЕМ, Львів, Україна, 25–26 трав. 2023. Львів: Вид-во Львів. політехніки, 2023, с. 81–82.

[5] How Do Merkle Trees Work ? [Online]. Available: https://www.baeldung.com/cs/merkle-trees [Accessed: 09-May-2024].