

Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна

О. О. Кузнецов
М. О. Полуяненко
О. О. Полуяненко

ОГЛЯД СУЧАСНИХ АЛГОРИТМІВ ГЕШУВАННЯ У БЛОКЧЕЙН-СИСТЕМАХ

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни
«Технології блокчейн»

для студентів
спеціальності 125 «Кібербезпека»

Харків – 2021

Рецензенти:

О. В. Лемешко – доктор технічних наук, професор, завідувач кафедри інфокомунікаційної інженерії імені В. В. Поповського Харківського національного університету радіоелектроніки;

О. Г. Толстолузька – доктор технічних наук, старший науковий співробітник, професор кафедри теоретичної та прикладної системотехніки факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна.

*Затверджено до друку рішенням Науково-методичної ради
Харківського національного університету імені В. Н. Каразіна
(протокол № 5 від 10 червня 2021 року)*

Кузнецов О. О.

К 89 Огляд сучасних алгоритмів гешування у блокчейн-системах : конспект лекцій з дисципліни «Технології блокчейн» для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 140 с.

Важливою складовою сучасних інформаційних технологій та комп'ютерних систем є криптографічні методи та засоби захисту інформації. П'ята частина «Огляд сучасних алгоритмів гешування у блокчейн-системах» конспектів лекцій для студентів факультету комп'ютерних наук за спеціальністю «Кібербезпека» присвячена дослідженню сучасних криптографічних примітивів для їх застосування в децентралізованих системах блокчейн. Зокрема досліджуються властивості різних сімейств криптографічних геш-функцій, аналізуються різні шляхи їхньої побудови та вивчається сучасний стан у галузі стандартизації та практичного застосування криптографічних функцій гешування для побудови розподілених інформаційних систем типу блокчейн. Розглянуті у даній частині конспекту лекції алгоритми криптографічного гешування застосовуються у понад 90 % існуючих проєктів децентралізованих систем за технологією блокчейн. До цього опису долучено також національний алгоритм криптографічного гешування «Купина», який стандартизовано у національному стандарті.

УДК 004.031.43

© Харківський національний університет імені В. Н. Каразіна, 2021

© Кузнецов О. О., Полуяненко М. О.,
Полуяненко О. О., 2021

© Дончик І. М., макет обкладинки, 2021

Навчальне видання

Кузнецов Олександр Олександрович

Полуяненко Микола Олександрович

Полуяненко Ольга Олександрівна

**ОГЛЯД СУЧАСНИХ АЛГОРИТМІВ
ГЕШУВАННЯ У БЛОКЧЕЙН-СИСТЕМАХ**

Конспект лекцій з дисципліни «Технології блокчейн»
для студентів спеціальності 125 «Кібербезпека»

Коректор *О. В. Анцибора*

Комп'ютерне верстання *В. В. Савінкова*

Макет обкладинки *І. М. Дончик*

Формат 60 x 84/16. Ум. друк. арк. 8,30. Наклад 50 пр. Зам. № 211/21.

Видавець і виготовлювач

Харківський національний університет імені В. Н. Каразіна,
61022, м. Харків, майдан Свободи, 4.

Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.2009

Видавництво ХНУ імені В. Н. Каразіна

Тел. 705-24-32

ЗМІСТ

Скорочення та умовні позначення.....	6
Вступ.....	7
1. Класифікація та загальні відомості щодо сучасних функцій гешування в децентралізованих системах Blockchain.....	10
2. Огляд сучасних алгоритмів гешування, які застосовуються або можуть застосовуватися в різних блокчейн-системах.....	16
2.1. Алгоритм криптографічного гешування ARGON2 та його опис.....	16
2.1.1. Безпека алгоритму.....	18
2.1.2. Практичне застосування алгоритму.....	18
2.2. Алгоритм криптографічного гешування BALLOON та специфікація ...	19
2.2.1. Функція Balloon.....	20
2.3. Алгоритм криптографічного гешування BLAKE.....	21
2.3.1. Очікувана стійкість.....	22
2.3.2. Функції стискання.....	23
2.3.3. Ініціалізація.....	23
2.3.4. Раундова функція.....	23
2.3.5. Останній крок.....	24
2.3.6. Гешування повідомлення.....	24
2.3.7. Оцінка алгоритму.....	25
2.4. BLAKE-512.....	25
2.4.1. Гешування повідомлення.....	27
2.5. Алгоритм криптографічного гешування BMW.....	28
2.6. Алгоритм криптографічного гешування CUBHASH та специфікація.....	30
2.6.1. Особливості реалізації, криптографічна стійкість та впровадження алгоритму.....	31
2.7. Алгоритм криптографічного гешування DJB-2.....	32
2.8. Алгоритм криптографічного гешування ECHO та його специфікація...	33
2.8.1. Безпека алгоритму.....	33
2.9. Алгоритм криптографічного гешування ED2K.....	34
2.10. Алгоритм криптографічного гешування EDONR та специфікація.....	35
2.10.1. Параметри, змінні та константи.....	35
2.10.2. Загальні конструктивні властивості EDON-R.....	36
2.10.3. Попередня обробка та заповнення повідомлення.....	37
2.10.4. Розбір повідомлення.....	38
2.10.5. Встановлення початкового значення подвійної труби $P^{(0)}$	38
2.10.6. Безпека алгоритму та його швидкодія.....	39
2.11. Алгоритм криптографічного гешування DAGGER-HASHIMOTO та його варіації.....	39
2.11.1. Ethash – остання версія Dagger-Hashimoto.....	40
2.11.2. Алгоритм криптографічного гешування ETHASH.....	42

2.12. Алгоритм криптографічного гешування FUGUE та специфікація.....	42
2.12.1. Оцінки швидкості.....	44
2.13. Алгоритм криптографічного гешування GOST34.11-94.....	44
2.14. Алгоритм криптографічного гешування GROESTL та специфікація ..	46
2.15. Алгоритм криптографічного гешування HAMSI.....	48
2.15.1. Загальна будова	49
2.15.2. Початкові значення	50
2.15.3. Заповнення повідомлень.....	50
2.15.4. Розширення повідомлень	51
2.15.5. Зчеплення	51
2.15.6. Додавання сталих і лічильника	52
2.15.7. Шар підстановки	52
2.15.8. Шар дифузії.....	53
2.15.9. Усічення	54
2.16. Алгоритм криптографічного гешування Has160 та специфікація	54
2.17. Алгоритм криптографічного гешування J-H.....	56
2.18. Алгоритм криптографічного гешування KECCAK	58
2.19. Алгоритм криптографічного гешування Курупа.....	59
2.20. Алгоритм криптографічного гешування LOSELOSE	62
2.21. Алгоритм криптографічного гешування LUFFA та специфікація.....	62
2.22. Алгоритм криптографічного гешування LYRA2RE	64
2.22.1. Оцінка алгоритму і його використання	66
2.23. Алгоритм криптографічного гешування LYRA2REV2 та специфікація	66
2.23.1. Особливості роботи та застосування алгоритму криптографічного гешування Lyra2Rev2.....	67
2.24. Алгоритм криптографічного гешування MD4.....	68
2.25. Алгоритм криптографічного гешування MD5.....	68
2.26. Алгоритм криптографічного гешування PANAMA256.....	69
2.26.1. «Panama» як геш-функція.....	70
2.26.2. Безпека алгоритму.....	70
2.27. Алгоритм криптографічного гешування PROGPOW	70
2.28. Алгоритм криптографічного гешування EQUHASH та специфікація.....	72
2.28.1. Особливості реалізації	74
2.28.2. Оцінка алгоритму та його використання	75
2.29. Алгоритм криптографічного гешування RANDOMX.....	75
2.29.1. Параметри налаштування	76
2.29.2. Опис алгоритму	77
2.29.3. Безпечність, продуктивність і застосування алгоритму	78
2.30. Алгоритм криптографічного гешування RIPEMD160	79
2.31. RIPEMD-128.....	83
2.31.1. Булеві функції.....	83

2.31.2. Вибіркові розширення до 256- та 320-бітних результатів гешування	83
2.31.3. Оцінювання продуктивності	84
2.32. Алгоритм криптографічного гешування SCRYPT	84
2.32.1. Опис алгоритму	86
2.32.2. Оцінка алгоритму та його використання	87
2.33. Алгоритм криптографічного гешування SHA1	87
2.33.1. Опис алгоритму	88
2.33.2. Порівняння SHA-1 з іншими алгоритмами	88
2.34. Алгоритм криптографічного гешування SHA2	88
2.35. Алгоритм криптографічного гешування SHABAL	91
2.35.1. Стійкість алгоритму та його застосування	93
2.36. Алгоритм криптографічного гешування SHAVITE	93
2.36.1. Специфікація SHAvite-3	94
2.36.2. Специфікація SHAvite-3 ₂₅₆	94
2.36.3. Специфікація SHAvite-3 ₅₁₂	97
2.36.4. Безпека SHAvite-3 та продуктивність	100
2.37. Алгоритм криптографічного гешування SIMD	101
2.37.1. Математичні перетворення в алгоритмі SIMD	101
2.37.2. Опис алгоритму	102
2.37.3. Результати конкурсу SHA-3 для SIMD	113
2.38. Алгоритм криптографічного гешування SKEIN та специфікація	113
2.38.1. Відомості щодо стійкості, швидкості та використання алгоритму гешування	117
2.38.2. Алгоритм криптографічного гешування SNEFRU256	118
2.39. Алгоритм криптографічного гешування STREEBOG	119
2.40. Алгоритм криптографічного гешування та специфікація TIGER	122
2.41. Алгоритм криптографічного гешування WHIRLPOOL	125
2.41.1. Опис алгоритму	125
2.41.2. Криптостійкість алгоритму та його застосування	129
2.42. Алгоритми криптографічного гешування сімейства «X»	130
Перелік джерел посилання	132