ДОПОВІДІ
НАЦІОНАЛЬНОЇ
АКАДЕМІЇ НАУК
УКРАЇНИ

ІНФОРМАТИКА ТА КІБЕРНЕТИКА
INFORMATICS AND CYBERNETICS

https://doi.org/10.15407/dopovidi2026.02.012
УДК 004.056.5

О.О. Башук, https://orcid.org/0009-0002-6778-2943

Київський національний університет імені Тараса Шевченка, Київ, Україна
E-mail: a.bashuk@knu.ua

Вплив ступеня галуження дерев підписів, базованих на одноразових підписах, на ефективність їх використання

Представлена академіком НАН України А.В. Анісімовим

Комплексно досліджено вплив ступеня галуження N на продуктивність багаторазових деревоподібних цифрових підписів, побудованих на основі одноразових цифрових підписів. Розглянуто два основні типи структур: послідовні дерева, що потребують підтримки стану в пам'яті, та повні (безстанові) дерева, які відтворюють підпис у повному дереві динамічно. Теоретично обґрунтовано та емпірично підтверджено, що традиційні бінарні дерева (N = 2) не є оптимальними за більшістю показників, окрім швидкості первинного підписання в послідовних структурах. Встановлено, що для обох типів структур оптимальний баланс між часом відтворення, розміром підпису та швидкістю верифікації досягається при N = 3 та N = 4. Проте для послідовних дерев на досліджених проміжках ступінь галуження N = 3 демонструє дещо кращу ефективність щодо розміру підпису та часу його побудови на відмінну від теоретичних припущень. Доведено, що подальше збільшення значення N призводить до незначного пришвидшення верифікації, водночас спричиняючи значне лінійне зростання витрат на генерацію підпису. Отримані результати дають змогу вибирати архітектуру квантово-стійких систем автентифікації, оптимізуючи її залежно від пріоритетів швидкодії та ресурсних обмежень пристроїв.

Ключові слова: *геш-функція, цифрові підписи, одноразові цифрові підписи, багаторазові цифрові підписи, послідовні дерева, повні дерева.*

1. Вступ. З поточним розвитком технологій впровадження побутових квантових комп'ютерів є лише питанням часу, і забезпечення стійких до них постквантових протоколів у криптографії є надзвичайно актуальним. У випадку цифрових підписів досить популярними є одноразові цифрові підписи, що базуються на геш-функціях. Серед них можна виокремити підпис Лампорта (Lamport) [1], підпис Меркля (Merkle) [2], WOTS [2], підпис BiBa [3] та HORS [4]. Проте такі підписи мають очевидне обмеження на кількість використань. Для усунення цієї вади було розроблено підходи побудови багаторазових підписів на основі одноразових підписів. Більшість з них базуються на ланцюгових засадах [5], в

Цитування: Башук О.О. Вплив ступеня галуження дерев підписів, базованих на одноразових підписах, на ефективність їх використання. *Допов. Нац. акад. наук Укр.* 2026. № 2. С. 12—25. https://doi.org/10.15407/dopovidi2026.02.012

яких кожна "ланка", якій відповідає пара ключів одноразового підпису, використовується для підписання наступних "ланок" (у подальшому називатимемо їх вершинами). Зокрема, найпоширенішими є бінарні дерева підпису, де кожна вершина використовується для підписання двох наступних. Серед таких структур можна виокремити два основні підтипи: послідовні та повні (або безстанові).

Першим притаманна послідовна побудова дерева вершина за вершиною, з постійною підтримкою структури в пам'яті. Завдяки такій поведінці вони є досить швидкими порівняно з іншими, але з часом стають більшими, внаслідок чого збільшуються кількість необхідних обчислень, час побудови підпису та верифікації, що призводить до сповільнення продуктивності. Крім того, необхідна постійна підтримка структури в пам'яті, що може бути критичним для слабких пристроїв.

Повні ж структури, попри назву, практично не використовують пам'ять, окрім як для опрацювання самого запиту. Це можливо завдяки тому, що якщо зафіксувати основу псевдовипадкової функції, яка використовується для генерації нових пар ключів одноразових підписів, згенерована пара ключів буде завжди однаковою. І якщо під час побудови дерева підписувати лише наступні вершини без повідомлення, яке треба підписати, то все дерево буде однозначно відповідати заданій основі. Іншими словами, все згенероване дерево можна відтворити, якщо знати основу псевдовипадкової функції, з якої воно було побудоване, а тому й не вимагає постійної підтримки в пам'яті. Підписом повідомлення ж у такій структурі вважається шлях по цьому дереву від кореня, який однозначно визначається самим повідомленням. Проте через незалежність від пам'яті час, необхідний для підписання чи верифікації повідомлення, є значно довшим, ніж у послідовних структурах.

Порівнянню ефективності різних методів побудови багаторазових цифрових підписів присвячено окрему роботу [6], в якій явно продемонстровано різницю між різними підходами і розглянуто, чому вибір слід робити з огляду на конкретну ситуацію та її специфіку.

Проте чи можливо підвищити продуктивність того або іншого підходу, не змінюючи його основної ідеї? Як вже було зазначено, для побудови деревоподібних структур багаторазових підписів на основі одноразових зазвичай використовують саме бінарні дерева підпису. Але чи є бінарні дерева найбільш оптимальними, чи можливо з тернарними деревами досягти вищої продуктивності?

Мета дослідження — підвищення ефективності використання багаторазових цифрових підписів, базованих на одноразових підписах, шляхом аналізу впливу ступеня галуження дерева на ключові показники продуктивності для послідовних та повних структур, а також визначення оптимальних параметрів конфігурації таких систем.

2. Теоретичні розрахунки. На теоретичному рівні проаналізуємо вплив параметра ступеня галуження дерева підписів N, який визначає кількість дочірніх вершин у кожної вершини дерева, на різні показники. Спершу приділимо увагу деревам послідовної побудови, а потім — повної. Для кожного типу розглянемо час самого підписання, час створення підпису, час верифікації підпису та розмір підпису.

2.1. Послідовні дерева підпису. Спершу розглянемо послідовні дерева підпису та залежність їх показників від ступеня галуження дерева підписів N.

Час підписання. З часом підписання ситуація є досить простою. Для операції підписання чергового повідомлення необхідно взяти наступну в порядку обходу пошуком у ширину (BFS) вершину, створити N пар ключів одноразового підпису, якими в подальшому

ініціалізувати новостворені дочірні вершини до поточної, і підписати надане повідомлення разом з усіма N новоствореними публічними ключами. Оскільки поточна вершина може фігурувати в подальших підписах інших повідомлень, то у разі потреби можна створити N+1 пару ключів, підписати поточною вершиною лише публічні ключі цих N+1 пар, першими N парами ініціалізувати подальші дочірні вершини, а N+1 парою підписати саме повідомлення. Завдяки такій проміжній вершині, кожне повідомлення буде фігурувати лише у своєму підписі і ніде більше.

Проте в обох випадках, оскільки найскладнішими для обчислень є операції створення пари ключів одноразових підписів та підписання повідомлення за допомогою пари, часові витрати на підписання лінійно залежать від N і мають лишатися сталими під час подальших підписань. Відповідно, чим більша дочірність вершин дерева, тим пропорційно довший час підписання повідомлення в дереві.

Час побудови підпису та розмір підпису. Після самого підписання не менш важливим етапом є процес побудови підпису, який потрібно надати у відповідь на запит підписання повідомлення. Для верифікації того, що повідомлення було підписане деревом підписів, потрібно надавати не лише одноразовий підпис, яким було підписане саме повідомлення, а й усі одноразові підписи на шляху від відповідної вершини до кореня дерева. Для верифікації кожного з них треба також надати всі підписані елементи на цьому шляху, тобто публічні ключі дочірніх вершин і, можливо, самі повідомлення. Весь цей набір одноразових підписів, публічних ключів та, ймовірно, повідомлень і вважається підписом повідомлення в дереві підписів.

Щоб надати такий підпис у відповідь на запит, потрібно фактично продублювати всі перелічені дані. Тому час створення підпису має повністю відповідати його розміру, через що ці дві величини слід розглядати разом.

Розглядатимемо лише підписи, базовані на геш-функціях, зокрема на одноразових підписах Лампорта. Завдяки описаному в попередньому пункті підходу з N+1 дочірньою вершиною, розміром самого повідомлення можна знехтувати. Крім того, досить часто розмір одноразового підпису, що базується на геш-функціях, досить наближений до розміру відповідних ключів, а тому для простоти розрахунків його можна округлити.

Нехай S_0 — розмір однієї базової одиниці підпису в дереві (одноразовий підпис або публічний ключ), h — довжина шляху від кореня до вершини, якою було підписане повідомлення (висота). Тоді кількість даних, які треба продублювати для створення підпису в дереві, можна описати рівнянням

$$S(h, N) := (h+1)\,(N+2)\,S_0\,. \tag{1}$$

На перший погляд здається, що чим більше N, тим більший розмір підпису, а отже, і час його створення, а тому нема сенсу розглядати зростання N. Проте N впливає не тільки на розмір підпису, а й на життєдіяльність усього дерева підписів. Оскільки зі зростанням N збільшується ступінь галуження дерева, то й кількість вершин на кожному рівні дерева за висотою зростає. Відповідно, дерева з більшим N значно повільніше збільшують свою максимальну висоту, а отже, новостворені підписи в них довше залишаються коротшими, що впливає на показник h. Спробуємо дослідити цю залежність і простежимо, як з часом змінюється розмір підпису для різних значень N.

Для фіксованого N, кількість вершин у дереві на нульовому рівні буде 1, на першому — $1 \cdot N = N$, на другому — $N \cdot N = N^2$, …, на i-му — $N^{i-1} \cdot N = N^i$. Відповідно, кількість запитів на підписання повідомлень у дереві, після яких відбувається зростання довжини підпису, можна виразити такою послідовністю:

$$a_i := 1 + N + N^2 + \ldots + N^i = \frac{N^{i+1} - 1}{N - 1}. \tag{2}$$

Нехай в нас також є друге дерево підписів зі ступенем галуження M таке, що

$$1 < N < M, \tag{3}$$

$$C_1 := \frac{M}{N} > 1, \tag{4}$$

$$b_j := 1 + M + M^2 + \ldots + M^j = \frac{M^{j+1} - 1}{M - 1}. \tag{5}$$

Для довільних N і M досить важко знайти такі a_i та b_j, щоб можна було вдало порівняти розміри відповідних їм підписів. Натомість можна піти зворотним шляхом, прирівняти розміри самих підписів і порівняти елементи a_i та b_j, що їм відповідають, як максимальну кількість підписаних повідомлень на висоті не більше i та j відповідно.

Отже, нехай для деяких h_N та h_M маємо рівність

$$S(h_N, N) = (h_N + 1)(N + 2) S_0 = (h_M + 1)(M + 2) S_0 = S(h_M, M). \tag{6}$$

Тоді

$$C_2 := \frac{h_N + 1}{h_M + 1} = \frac{M + 2}{N + 2} > 1, \tag{7}$$

$$C_2 = \frac{M + 2}{N + 2} = \frac{C_1 N + 2}{N + 2} = C_1 - \frac{2(C_1 - 1)}{N + 2} < C_1. \tag{8}$$

Розглянемо тепер a_{h_N} та b_{h_M} кількості, що їм відповідають:

$$a_{h_N} = \frac{N^{h_N+1} + 1}{N + 1} = \frac{N^{C_2(h_M+1)} + 1}{N + 1} = \frac{(N^{C_2})^{h_M+1} + 1}{N + 1}, \tag{9}$$

$$b_{h_M} = \frac{M^{h_M+1} + 1}{M + 1} = \frac{(C_1 N)^{h_M+1} + 1}{C_1 N + 1}. \tag{10}$$

Позначимо співвідношення N^{C_2} до $C_1 N$ через K, зведемо до спільного знаменника і візьмемо різницю чисельників:

$$K := \frac{N^{C_2}}{C_1 N}, \tag{11}$$

$$(a_{h_N} - b_{h_M})(N+1)(C_1N+1) =$$
$$= (C_1N+1)(N^{C_2})^{h_M+1} + C_1N + 1 - (N+1)(C_1N)^{h_M+1} - N - 1 =$$
$$= (C_1N+1)(KC_1N)^{h_M+1} - (N+1)(C_1N)^{h_M+1} + (C_1-1)N =$$
$$= ((C_1N+1)K^{h_M+1} - N - 1)(KC_1N)^{h_M+1} + (C_1-1)N. \quad (12)$$

Оскільки $(C_1 - 1)N$ — це фіксоване позитивне значення, KC_1N та $C_1N + 1$ — фіксовані позитивні значення більші за 1, а з плином часу h_M зростає, то на довготривалій перспективі при $K < 1$ a_{h_N} буде меншим за b_{h_M}, інакше — навпаки. Але водночас, оскільки значення a_{h_N} та b_{h_M} — це максимальна можлива кількість повідомлень, що можуть бути підписані на висоті не більше ніж h_N та h_M відповідно, то кращим є більше з цих значень. Іншими словами, при $K < 1$ дерево зі ступенем галуження M є місткішим та кращим, інакше — дерево зі ступенем галуження N.

Розглянемо, як змінюється K за фіксованого N та зростання M:

$$K = \frac{N^{C_2}}{C_1 N} = \frac{N^{\frac{M+2}{N+2}}}{M} = \frac{\left(N^{\frac{1}{N+2}}\right)^{M+2}}{M}. \quad (13)$$

Нехай маємо таку функцію f:

$$f(x) := \frac{a^{x+2}}{x}, \quad (14)$$

$$f'(x) := \frac{d}{dx}\left(\frac{a^{x+2}}{x}\right) = \frac{a^{x+2}}{x^2}(x\ln(a) - 1). \quad (15)$$

Очевидно, що для $x > 1$ та $a > 1$ похідна функції f буде дорівнювати 0 тільки при $x_0 = 1/\ln(a)$ і додатною за більших значень x. Якщо ж підставити в a значення $N^{1/(N+2)} > 1$, матимемо

$$x_0 = \frac{1}{\ln(a)} = \frac{1}{\ln\left(N^{\frac{1}{N+2}}\right)} = \frac{N+2}{\ln(N)}. \quad (16)$$

Якщо порівнювати параметри x_0 та N, то N буде більшим за x_0 за умови $N\ln(N) - N - 2 > 0$, що внаслідок зростання цієї послідовності чисел при $N > 1$ буде вірним для всіх $N > 4$. Для випадків $N \le 4$ матимемо

$$N = 2 \Rightarrow x_0 \approx 5{,}77, \quad (17)$$

$$N = 3 \Rightarrow x_0 \approx 4{,}55, \quad (18)$$

$$N = 4 \Rightarrow x_0 \approx 4{,}32. \quad (19)$$

Водночас відомо, що експоненційна послідовність зростає швидше за лінійну:

$$a > 1 \Rightarrow \lim_{n\to\infty} \frac{a^n}{n} = \infty . \qquad (20)$$

На підставі цього, а також зростання похідної функції f' при $x > x_0$ можна дійти висновку, що зі збільшенням M і за фіксованого N коефіцієнт K рано чи пізно перевищить одиницю.

Розглянемо значення коефіцієнта K відносно одиниці для $2 \le N \le M \le 10$ (таблиця).

Таблиця наочно ілюструє правдивість отриманих властивостей та порогових значень (17)—(19). Крім того, з огляду на тенденцію зростання коефіцієнта K, наведені в таблиці результати і вплив коефіцієнта K на значення a_{h_N} та b_{h_M} можна дійти висновку, що найбільш містким деревом підписів є дерево зі ступенем галуження $N = 4$. За такого значення цього параметра розмір підпису на довгостроковій перспективі збільшуватиметься повільніше, а отже, й час створення підпису також зростатиме повільніше.

Час верифікації. Час верифікації, попри подібні залежності, має іншу поведінку. Він так само лінійно залежить від кількості вершин, за якими побудовано підпис у дереві, які, у свою чергу, логарифмічно залежать від кількості раніше підписаних повідомлень у дереві, та часу верифікації одноразового підпису в кожній з цих вершин. Для верифікації ж одноразових підписів у вершинах можна виокремити такі дві складові: побудова "повідомлення" для підпису і сама верифікація одноразового підпису для відповідного "повідомлення".

Побудова "повідомлення", яке насправді підписується одноразовим підписом — це знаходження загального гешу всіх підписуваних параметрів, а саме публічних ключів дочірніх вершин та, можливо, повідомлення, що відповідає цій вершині. Проте з урахуванням зазначеного раніше підходу з додатковою парою ключів одноразового підпису, не обмежуючи загальності, можна вважати, що підписується лише набір з публічних ключів. Водночас самі публічні ключі $N - 1$ дочірньої вершини не мають принципової важливості, а потрібні більше для побудови підписуваного "повідомлення", яке насправді підписується. Тому, щоб зайвий раз не рахувати геш кожного окремого публічного ключа, має сенс разом із самим публічним ключем у підписі надавати його геш, що, за бажанням перевіряльника, може помітно пришвидшити процес верифікації до обрахунку гешу одного публічного ключа та загального гешу $N + 1$ гешів як підписуваного "повідомлення".

Коефіцієнт *K*

$N \setminus M$	2	3	4	5	6	7	8	9	10
2	**1**	0,792	0,707	0,672	0,666	0,679	0,707	0,747	0,8
3	—	**1**	0,934	0,931	0,966	**1,032**	**1,125**	**1,245**	**1,396**
4	—	—	**1**	**1,007**	**1,058**	**1,142**	**1,259**	**1,411**	**1,6**
5	—	—	—	**1**	**1,048**	**1,131**	**1,245**	**1,393**	**1,578**
6	—	—	—	—	**1**	**1,072**	**1,173**	**1,305**	**1,469**
7	—	—	—	—	—	**1**	**1,086**	**1,198**	**1,339**
8	—	—	—	—	—	—	**1**	**1,094**	**1,212**
9	—	—	—	—	—	—	—	**1**	**1,098**
10	—	—	—	—	—	—	—	—	**1**

Верифікація ж "повідомлення" може різнитись залежно від обраного протоколу одноразових підписів. Здебільшого одноразові підписи, базовані на геш-функціях, потребують значної кількості гешувань для генерації ключів та верифікації повідомлень. До прикладу, підпис Лампорта, який узято за основу в цих дослідженнях, у стандартній імплементації на базі геш-функції SHA-256 [7] потребує 256 гешувань для верифікації.

Беручи це до уваги, за достатньо помірних значень N, а саме допоки N на порядок не перевищує кількість гешувань, необхідних для верифікації одноразового підпису, зміна значення N не має істотного впливу на час опрацювання однієї вершини підпису в дереві підписів протягом його верифікації. А такі великі значення N мають мало сенсу, особливо з огляду на отримані раніше результати.

Тоді маємо, що значення параметра N у межах розумного не впливає на час опрацювання однієї вершини в підписі, проте впливає на кількість вершин у ньому, оскільки зі збільшенням ступеня галуження дерева кількість вершин у підписі зростає повільніше. Отже, можна дійти висновку, що чим більше N, тим кращі показники часу верифікації демонструватиме відповідне дерево підписів.

2.2. Повні дерева підпису. Для повних дерев підписів діє дещо інша логіка. Насамперед з часом їхні показники не мають змінюватися, а тому достатньо розглядати лише безпосередній вплив зміни параметра N на них. Крім того, оскільки стан дерева не підтримується, підпис відтворюється в цьому дереві на ходу, а саме повідомлення, як таке, зазвичай не підписується жодним з одноразових підписів, а впливає лише на шлях у дереві, то в даному випадку немає такого поняття, як час підписання. Тому далі розглядатимемо лише час відтворення підпису, час верифікації та розмір підпису.

Час відтворення підпису. Для відтворення підпису в повному дереві необхідно згенерувати всі публічні ключі дочірніх вершин до вершин, що лежать на шляху від кореня до відповідної листової вершини, а також підписати дочірні вершини відповідними приватними ключами. Довжина ж цього шляху є сталою висотою H дерева підписів і визначається, як логарифм за основою N від кількості усіх можливих повідомлень, довжина яких має бути сталою, заокруглений вгору. Фіксованість довжини повідомлень зазвичай досягається шляхом попереднього їх гешування обраною геш-функцією. Так, якщо за геш-функцію взяти SHA256, а $N = 4$, то висота дерева H дорівнюватиме

$$H = [\log_4 2^{256}] = 128 . \tag{21}$$

Нехай B — кількість бітів, що повертає вибрана геш-функція, t_g — час генерації пари ключів одноразового підпису, t_s — час підписання одноразовим підписом, а t_h — час гешування повідомлення завдовжки B біт. Тоді загальний час, необхідний для відтворення одного підпису в повному дереві, становитиме

$$t = H \cdot (N \cdot t_g + N \cdot t_h + t_s) = [\log_N 2^B] \cdot (N \cdot t_g + N \cdot t_h + t_s) . \tag{22}$$

Для одноразових підписів, базованих на геш-функціях, здебільшого можна виокремити таку властивість:

$$t_g > t_s, t_h . \tag{23}$$

Час гешування сам по собі очікувано має бути меншим за час генерації пари ключів одноразового підпису, базованого на геш-функціях, а ось час підписання залежить від вибраного протоколу. Так, у випадку підпису Лампорта цей час достатньо малий, а у випадку WOTS може досягати часу генерації пари ключів. Тоді дещо спростимо вираз (22), прибравши з нього округлення:

$$t = [\log_N 2^B] \cdot (N \cdot t_g + N \cdot t_h + t_s) \approx t_g \ln(2^B) \cdot \frac{N\left(1 + \frac{t_h}{t_g}\right) + \frac{t_s}{t_g}}{\ln(N)} \approx$$

$$\approx t_g \ln(2^B) \cdot \frac{N + \Delta}{\ln(N)}, \quad 0 \leqslant \Delta \leqslant 1. \tag{24}$$

Знайдемо похідну останнього виразу за N:

$$\frac{d}{dN}\left(t_g \ln(2^B) \cdot \frac{N + \Delta}{\ln(N)}\right) = t_g \ln(2^B) \cdot \frac{N(\ln(N) - 1) - \Delta}{N(\ln(N))^2}. \tag{25}$$

Для $N = 4$ маємо вираз $N(\ln(N) - 1) = 1{,}5451 > 1$, а оскільки цей вираз зростає зі збільшенням N, то для всіх $N \geq 4$ отримана похідна в (25) буде додатною. Водночас досить очевидно, що при $N = 2$ отримана похідна в (25) буде від'ємною. Отже, мінімум (24), якого можна досягти в разі цілих значень $N \geq 2$, буде серед множини {2, 3, 4}, і цей вираз зростатиме з подальшим збільшенням N.

Розглянемо, що відбувається із залежною від N частиною в (24) за значень N з множини {2, 3, 4}:

$$N = 2 \Rightarrow \frac{N + \Delta}{\ln N} \approx 2{,}88 + 1{,}44 \cdot \Delta, \quad 0 \leqslant \Delta \leqslant 1, \tag{26}$$

$$N = 3 \Rightarrow \frac{N + \Delta}{\ln N} \approx 2{,}73 + 0{,}91 \cdot \Delta, \quad 0 \leqslant \Delta \leqslant 1, \tag{27}$$

$$N = 4 \Rightarrow \frac{N + \Delta}{\ln N} \approx 2{,}88 + 0{,}72 \cdot \Delta, \quad 0 \leqslant \Delta \leqslant 1. \tag{28}$$

Досить очевидно, що мінімум досягається, якщо N дорівнює 3 або 4, залежно від Δ, але різниця між ними не є істотною.

Розмір підпису. Для знаходження орієнтованого розміру підпису в повному дереві підписів можна скористатись тими ж міркуваннями, що і для часу відтворення підпису. Використовуючи позначення S_0 (див. п. 2.1) розмір підпису s можна виразити таким чином:

$$s = S_0 \cdot H \cdot (N + 1) \approx S_0 \ln 2^B \cdot \frac{N + 1}{\ln N}. \tag{29}$$

Оскільки в (29) бачимо аналогічний до (24) вираз, можемо скористатися попередніми висновками: при $N = 4$ ця функція досягатиме свого мінімуму на цілих значеннях $N \geq 2$, а при $N \geq 4$ вона зростатиме.

Час верифікації. Слідуючи аналогічним міркуванням до верифікації в послідовних деревах підпису, за не надто великих значень N під час верифікації підпису в повному дереві підписів на час верифікації однієї вершини впливатиме лише час верифікації відповідного одноразового підпису. Великі ж значення N нема сенсу розглядати, оскільки такі дерева підпису будуть не надто ефективними щодо інших показників. Водночас на загальний час верифікації впливатиме висота дерева H, яка залежить від N. Іншими словами, якщо t_v — час верифікації одноразового підпису, то загальний час верифікації орієнтовно дорівнює

$$t \approx \frac{t_g \ln 2^B}{\ln N}. \tag{30}$$

Обернений логарифм при $N > 1$ спадає до 0, але при $N \geq 3 > e$ він вже буде меншим за одиницю, а подальше спадання буде досить повільним. Тому, попри спадання часу верифікації зі збільшенням N, більші значення N можуть не давати відчутно кращих результатів порівняно з меншими. Враховуючи залежність інших показників та потенційний вплив часу гешування публічних ключів одноразових підписів за великих значень N, загалом найефективніші показники серед повних дерев підпису, ймовірно, матимуть дерева з відносно невеликими значеннями $N \geq 3$.

3. Заміри реалізованих дерев підписів. Код реалізовано мовою Python і розроблено узагальненим класом з параметризацією за такими характеристиками: ступінь галуження дерева arity, повне дерево full_tree, використання проміжної вершини use_proxy_node. Повний код реалізації можна знайти за посиланням: https://github.com/albashuk/Dissertation/tree/master/HashSignatures/Python/NaryTBS.

Для обох типів дерев підпису зроблено заміри усіх показників, що були розглянуті для них на теоретичному рівні, а саме час підписання, час побудови підпису, розмір підпису і час верифікації для послідовних дерев підпису та час відтворення підпису, розмір підпису і час верифікації для повних дерев підпису. Дані замірялись на MacBook Pro 2024 року з процесором Apple M4 Max та 64 ГБ оперативної пам'яті.

3.1. Послідовні дерева. Оскільки показники послідовних дерев підпису з часом змінюються, а теоретичні властивості розглядаються з точки зору довготривалих перспектив, заміри виконано впродовж тривалого часу окремо для кожного дерева з різним ступенем галуження. Так, було розглянуто дерева зі ступенем галуження 2, 3, 4, 5 та 8. Крім того, через малу різницю між випадками з використанням проміжної вершини та без її використання для отримання більш уніфікованих даних зроблено заміри саме послідовних дерев підпису з проміжними вершинами.

Також, у ході проведення замірів дерева очікувано зазнавали впливу інших сторонніх процесів, які паралельно відбувались на пристрої, що спричинило додаткові "шуми" в отриманих даних. Через це дані було попередньо оброблено для усунення цих "шумів".

Час підписання. Для часу підписання на графіку, зображеному на рис. 1, можна спостерігати практично константні значення, які пропорційні до ступеня галуження дерева.

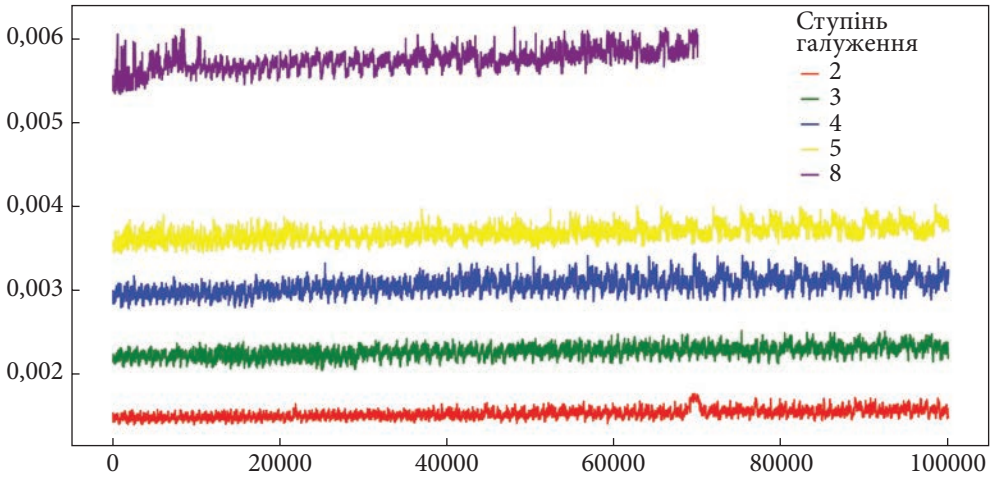

Рис. 1. Час підписання в послідовних деревах підписів (с)

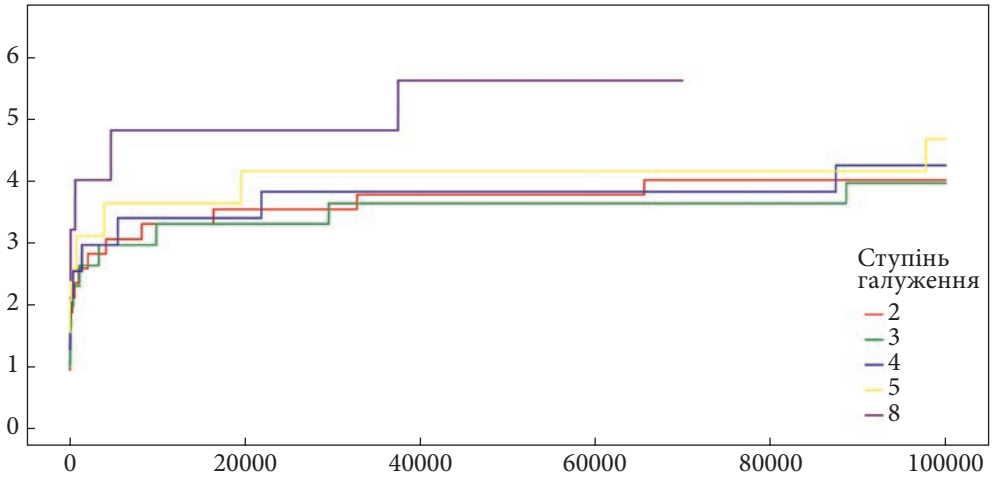

Рис. 2. Розмір підпису в послідовних деревах підписів (МБ)

Час побудови підпису та розмір підпису. У випадку розміру підпису "шумів" очікувано не спостерігалось і дані не потребували опрацювання (рис. 2). Розмір підпису при цьому очікувано логарифмічно зростає, і можна помітити, що попри близьку поведінку ступенів галуження 2, 3 та 4 у випадку галуження 4 і особливо 8 розмір підпису помітно більший. Якщо ж ступінь галуження 3, розмір підпису майже завжди найменший. Проте не виключено, що після подальших підписань і значно більшої кількості підписаних повідомлень тенденція зміниться в бік теоретичних результатів.

У випадку ж часу побудови підпису має відбуватись пропорційно аналогічна до розміру підпису тенденція, що ілюструє графік, зображений на рис. 3. Проте випадок зі ступенем галуження 4 дещо гірший, ніж для ступенів галуження 2 та 3, і ближче до 5.

Час верифікації. На графіку, наведеному на рис. 4, зображено очікувану логарифмічну залежність від кількості раніше підписаних повідомлень у дереві. Крім того, зі зростанням ступеня галуження дерева час верифікації очікувано спадає. Але водночас найбільш

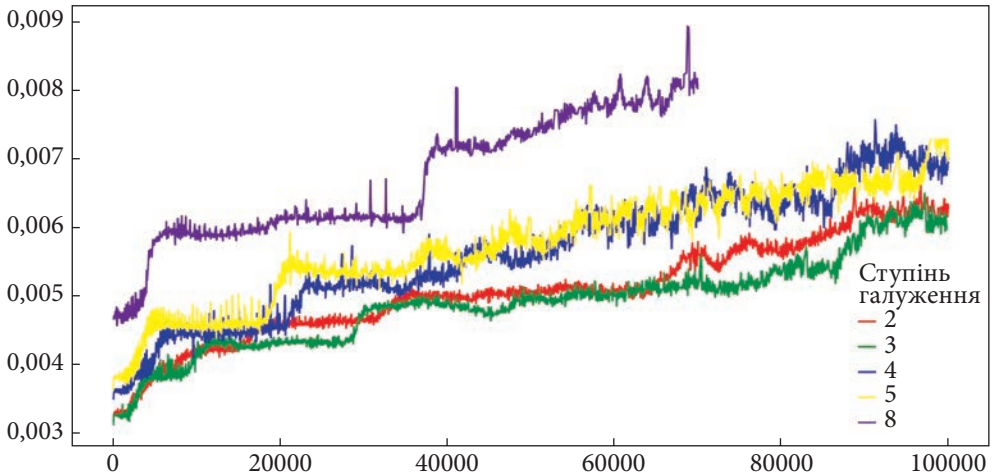

Рис. 3. Час побудови підпису в послідовних деревах підписів (с)

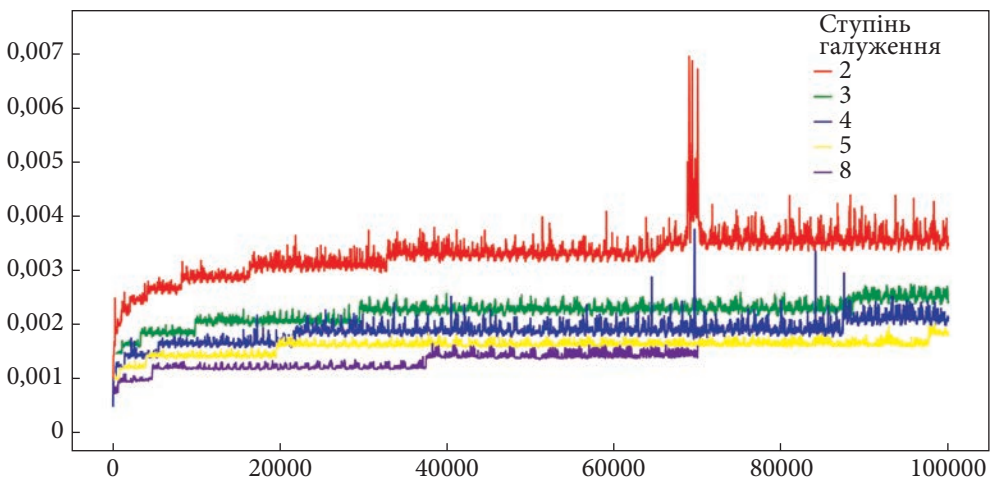

Рис. 4. Час верифікації в послідовних деревах підписів (с)

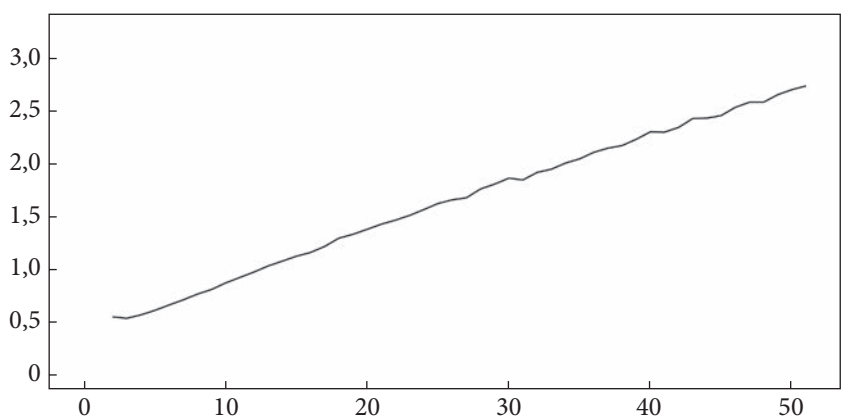

Рис. 5. Час відтворення підпису в повних деревах підписів (с)

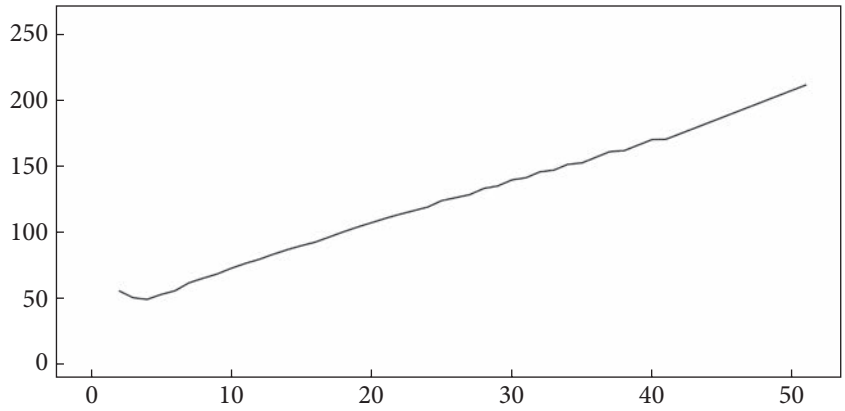

Рис. 6. Розмір підпису в повних деревах підписів (МБ)

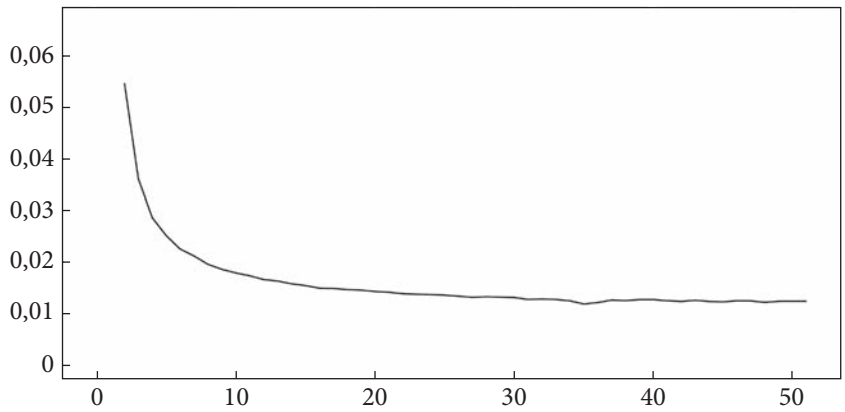

Рис. 7. Час верифікації в повних деревах підписів (с)

помітною різниця спостерігається за малих значень ступеня галуження, тоді як за подальшого зростання ступеня галуження різниця в часі стає менш помітною.

Підсумок. Розглянуті емпіричні дані здебільшого відповідають раніше запропонованим теоретичним припущенням, проте у випадку зі ступенем галуження 3 на дослідженому проміжку є більш ефективними, ніж для ступеня галуження 4.

3.2. Повні дерева. Для повних дерев підпису немає сенсу розглядати зміну їх показників з часом, оскільки всі вони мають лишатись орієнтовно сталими. Натомість має сенс узяти усереднені показники за невеликий проміжок часу, але для значно більшої кількості ступенів галуження дерева, що і було зроблено.

Час відтворення підпису. Оскільки час підписання підписом Лампорта значно менший за час, необхідний для генерації пари відповідних ключів, то можна теоретично припустити, що час відтворення підпису в повному дереві зі ступенем галуження дерева 3 менший за відповідний час у дереві зі ступенем галуження 4 і при цьому досягає мінімуму. З подальшим збільшенням ступеня галуження час очікувано лінійно зростає (рис. 5).

Розмір підпису. Розмір підпису поводить себе аналогічно до часу відтворення підпису, що підтверджує теоретичні припущення (рис. 6). Крім того, мінімум досягається у випадку ступеня галуження 4, хоч різниця з випадком зі ступенем галуження 3 і невелика.

Час верифікації. Для часу верифікації спостерігається очікувана обернено-логарифмічна тенденція впродовж усього графіка (рис. 7).

Підсумок. Розглянуті емпіричні дані повністю відповідають раніше запропонованим теоретичним припущенням.

Висновок. Під час дослідження виконано як теоретичні розрахунки та їх порівняння, так і порівняння на основі емпіричних даних для повних та послідовних дерев підписів різного ступеня галуження.

На підставі емпіричних даних, відображених на графіках, можна дійти висновку, що бінарні дерева не є найбільш ефективними у використанні, вони не домінують по жодному з показників, окрім часу підписання повідомлення в послідовному дереві підписів. Іншими словами, їх використання не є виправданим, попри зручність самої бінарної системи.

Водночас не можна надати перевагу якомусь одному ступеню галуження. У різних випадках і залежно від умов, таких як: завантаженість системи, розмір повідомлень, пріоритезація швидкодії підписання понад верифікацією підпису або навпаки тощо, можуть переважати ті чи інші ступені галуження дерева. Найбільш збалансованими серед них виглядають ступені галуження 3 та 4. За більших значень, хоч і зменшується час верифікації підпису, різниця в часі стає все менш і менш помітною, тоді як показники, пов'язані з підписанням, значно зростають, а тому, ймовірно, перевага у швидкодії верифікації того не варта.

ЦИТОВАНА ЛІТЕРАТУРА

1. Boneh D., Shoup V. A graduate course in applied cryptography. Version 0.6. 2023. P. 584—594. URL: https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_6.pdf. (Дата звернення: 02.02.2026).
2. Merkle R.C. A certified digital signature. *Advances in cryptology — CRYPTO' 89 Proceedings*. New York : Springer, 1990. P. 218—238. https://doi.org/10.1007/0-387-34805-0_21
3. Perrig A. The BiBa one-time signature and broadcast authentication protocol. *Proceedings of the 8th ACM conference on computer and communications security.* New York: Association for Computing Machinery, 2001. P. 28—37. https://doi.org/10.1145/501983.501988
4. Reyzin L., Reyzin N. Better than BiBa: Short one-time signatures with fast signing and verifying. *Information Security and Privacy (ACISP 2002).* Berlin, Heidelberg: Springer, 2002. P. 144—153. (Lecture Notes in Computer Science, Vol. 2384.). https://doi.org/10.1007/3-540-45450-0_11
5. Katz J., Lindell Y. Introduction to modern cryptography. 2nd ed. Boca Raton: CRC Press, 2015. P. 465—473. https://doi.org/10.1201/b17668
6. Anisimov A., Bashuk O. Implementation and comparison of hash function-based multi-time digital signature protocols. *Proceedings of the XI International Scientific Conference "Information Technology and Implementation"* (Kyiv, Ukraine, November 20-21, 2024). Kyiv, 2024. P. 500—506. URL: https://ceur-ws.org/Vol-3909/Short_1.pdf. (Дата звернення: 02.02.2026).
7. Secure Hash Standard (SHS): FIPS PUB 180-4. Gaithersburg: National Institute of Standards and Technology, 2015. https://doi.org/10.6028/NIST.FIPS.180-4

Надійшла до редакції 12.02.2026

REFERENCES

1. Boneh, D., & Shoup, V. (2023). A graduate course in applied cryptography. Version 0.6, pp. 584-594. Retrieved from https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_6.pdf
2. Merkle, R. C. (1990). A certified digital signature. In Brassard, G. (Ed.), Advances in cryptology — CRYPTO' 89 Proceedings (pp. 218-238). New York: Springer. https://doi.org/10.1007/0-387-34805-0_21
3. Perrig, A. (2001). The BiBa one-time signature and broadcast authentication protocol. In Proceedings of the 8th ACM conference on Computer and Communications Security (pp. 28-37). New York: Association for Computing Machinery. https://doi.org/10.1145/501983.501988

4. Reyzin, L., & Reyzin, N. (2002). Better than BiBa: Short one-time signatures with fast signing and verifying. In Batten, L. & Seberry, J. (Eds.), Information Security and Privacy. Lecture Notes in Computer Science,Vol. 2384 (pp. 144-153). Berlin, Heidelberg: Springer. https://doi.org/10.1007/3-540-45450-0_11
5. Katz, J., & Lindell, Y. (2015). Introduction to modern cryptography. 2nd ed. (pp. 465-473). Boca Raton: CRC Press. https://doi.org/10.1201/b17668
6. Anisimov, A., & Bashuk, O. (2024). Implementation and comparison of hash function-based multi-time digital signature protocols. Proceedings of the XI International Scientific Conference "Information Technology and Implementation", Vol. 3909 (pp. 500-506). Kyiv. Retrieved from https://ceur-ws.org/Vol-3909/Short_1.pdf
7. National Institute of Standards and Technology. (2015). Secure Hash Standard (SHS) (FIPS PUB 180-4). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.180-4

Received 12.02.2026

O.O. Bashuk, https://orcid.org/0009-0002-6778-2943

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

E-mail: a.bashuk@knu.ua

INFLUENCE OF BRANCHING DEGREE IN SIGNATURE TREES
BASED ON ONE-TIME SIGNATURES ON THE EFFICIENCY OF THEIR USE

The article provides a comprehensive study of the influence of the branching degree N on the performance of many-time tree-based digital signatures built on one-time digital signatures. Two main types of structures are considered: stateful sequential trees and full (stateless) trees that dynamically reconstruct the signature. It is theoretically substantiated and empirically confirmed that traditional binary trees ($N = 2$) are not optimal across most metrics, with the exception of initial signing speed in sequential structures. It was established that for both types of structures, the optimal balance between reconstruction time, signature size, and verification speed is achieved at $N = 3$ and $N = 4$. However, for sequential trees within the studied intervals, the branching degree $N = 3$ demonstrates slightly higher efficiency terms of signature size and construction time, contrary to theoretical assumptions. It is proved that a further increase in N leads to an insignificant acceleration of the verification process, while causing a significant linear increase in signature generation costs. The results of the work allow to select the architecture of quantum-resistant authentication systems with optimization based on performance priorities and device resource constraints.

Keywords: *hash function, digital signatures, one-time signatures, many-time signatures, sequential trees, full trees.*