**УДК 623.647, 681.325.5-181.4**

**В.С. Глухов**
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

# ВИБІР БАГАТОЯДЕРНИХ СТРУКТУР ДЛЯ ПРИСТРОЇВ ОБРОБКИ ЦИФРОВИХ ПІДПИСІВ



**Проведене порівняння паралельних та ієрархічних структур з використанням законів Амдаля і Густафсона.**

**Comparison of parallel and hierarchical structures with use of Amdahl and Gustafson laws is described in this article.**

**Вступ**. Сучасні комп’ютерні системи є багатоядерними. Багатоядерні системи можуть бути лінійними або ієрархічними (багатовимірними, багаторівневими). У роботі доводиться, що для багатоядерних систем обробки цифрових підписів ієрархічні структури мають переваги над паралельними.

**Аналіз публікацій і окреслення проблеми.** Збільшення в n разів апаратних ресурсів одноядерної системи збільшує її продуктивність у $\sqrt{n}$ разів (так званий закон Поллака [1]). Якщо ж збільшити кількість ядер в n разів, то збільшення продуктивності буде більшим за визначений законом Поллака. Тому сучасні комп’ютерні системи є багатоядерними. Але із збільшенням кількості рівноправних ядер збільшується кількість зв’язків між ними, ця залежність приблизно квадратична. Впровадження ієрархічного підходу і методів декомпозиції замінює квадратичну залежність на лінійну [1].

Згідно з законом Амдаля для паралельних систем [2] коефіцієнт збільшення продуктивності

$$P_N = \frac{1}{S + \frac{1-S}{N}} = \frac{N}{(N-1)S+1},$$

де $S$ – частка послідовного коду у програмі; $N$ – кількість пристроїв (програм), що працюють паралельно.

Згідно з законом Густафсона для паралельних систем [3]

$$P_N = \frac{T(1)}{T(N)} = \frac{S \times T(N) + N \times (1-S) \times T(N)}{S \times T(N) + (1-S) \times T(N)} = S + N(1-S) = N + (1-N) \times S = N - S(N-1),$$

де *T(i)* – час виконання програми на *i* процесорах.

Ієрархічні багатовимірні системи у [2, 3] не розглядаються. Водночас в складі гарантоздатних систем [10, 11] присутні пристрої, які забезпечують їхню конфіденційність. Одним з таких пристроїв є пристрій обробки цифрових підписів, який реалізує криптографічні алгоритми [4], що мають саме ієрархічну структуру (рис. 1). Це змушує аналізувати можливість використання для їх реалізації ієрархічних комп’ютерних систем. Дворівневі ієрархічні системи з обмеженою кількістю елементів розглянуті у [5], де доведена їхня перевага перед лінійними паралельними. Використання при проектуванні багаторівневих систем моделі взаємозв’язку відкритих систем [6**Ошибка! Источник ссылки не найден.**] обґрунтовується в [6]. Підхід до оцінювання апаратних витрат на реалізацію багаторівневих систем наведений у [7]. Найкращий спосіб декомпозиції цифрового автомата на два ієрархічно зв’язані пропонується в [8]. Методика використання ієрархічних систем у програмуванні (підпрограм, процедур, функцій) описана в [9, 12, 13].

Зараз актуальною є задача порівняння багатоелементних багаторівневих ієрархічних структур з паралельними з метою вибору для реалізації пристроїв обробки цифрових підписів системи з більшою продуктивністю.

**Мета роботи.** Метою роботи є обґрунтування переваги ієрархічної структури над паралельною для пристроїв обробки цифрових підписів.

**Вимоги до паралельних систем.** Для виграшу порівняно із одноядерною системою багатоядерна повинна забезпечувати виконання умови $P_N > \sqrt{N}$, звідки випливає $S < \frac{1}{\sqrt{N}+1}$. Граничні значення S показує (рис. 2).

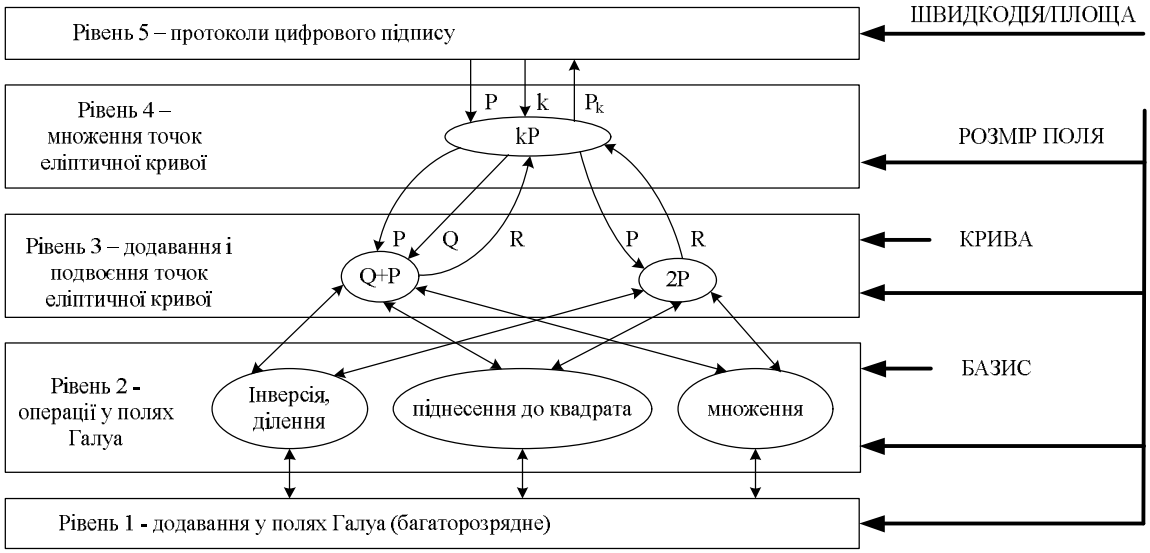


*Рис. 1. Ієрархічні рівні алгоритмів*

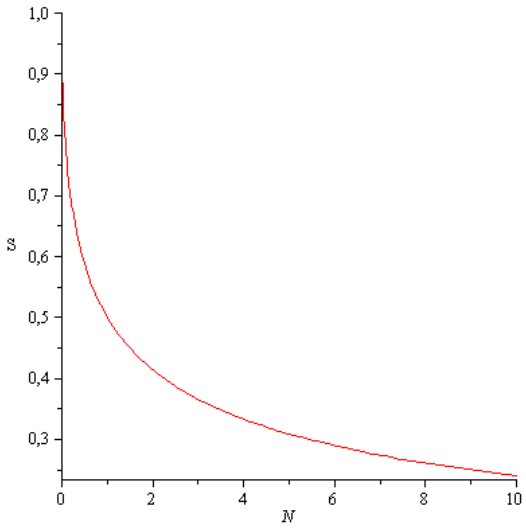


*Рис. 2. Граничні значення S*

**Порівняння структур за законом Амдаля.** Переваги ієрархічної структури за законом Амдаля можна показати на прикладі структур, що складаються з $n^2$ ядер (вузлів). Можна порівняти зростання продуктивності системи для двох варіантів її структури:

паралельна одновимірна система $P_N$ (рис. 3): $n^2$ ($N=n^2$) вузлів, що працюють паралельно, зростання продуктивності системи позначено також як $P_N$;

ієрархічна двовимірна система $P_{n^2}$ (рис. 4): $n$ вузлів 1-го рівня, що працюють паралельно, кожний вузол 1-го рівня складається з $n$ вузлів 2-го рівня, що так само працюють паралельно. Зростання продуктивності системи також позначено як $P_{n^2}$, внесок кожної сукупності n вузлів у зростання продуктивності та самі вузли 1-го рівня – як $P_n$. Рис. 1–5 лінії зображають не зв'язки між вузлами, а належність вузлів до одного рівня.

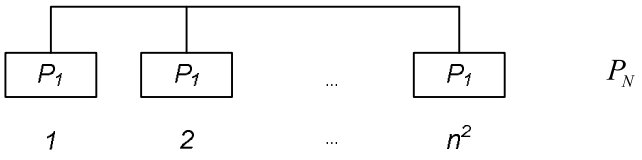


*Рис. 3. Одновимірна система* $P_N$

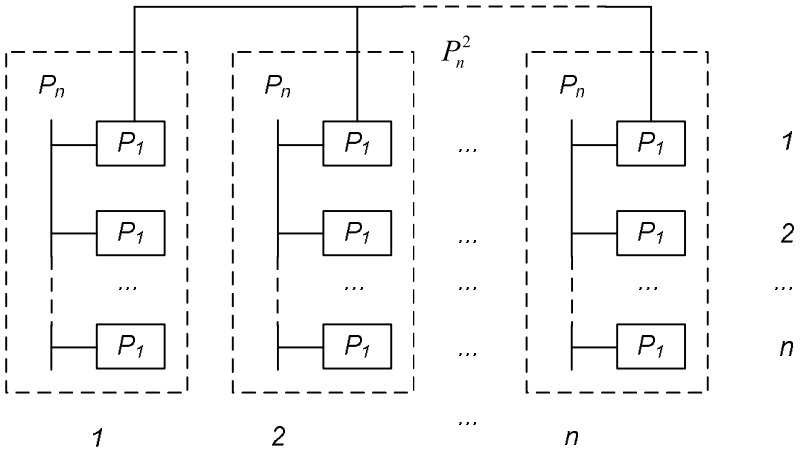


*Рис. 4. Двовимірна ієрархічна система* $P_{n^2}$

Позначимо $N=n^2$, $m=n-1$; $n=m+1$;

$$P_N = \frac{N}{(N-1)S+1} = \frac{n^2}{(n^2-1)S+1} = \frac{(m+1)^2}{m(m+2)S+1}.$$

Кожний вузол $P_n$ розглядається як $n$-ядерна паралельна система. Тоді

$$P_{n^2} = P_n^2 = (\frac{n}{(n-1)S+1})^2 = \frac{n^2}{((n-1)S+1)^2} = \frac{(m+1)^2}{(mS+1)^2}.$$

$$\frac{P_N}{P_{n^2}} = \frac{(m+1)^2}{m(m+2)S+1} : \frac{(m+1)^2}{(mS+1)^2} = \frac{(mS+1)^2}{m(m+2)S+1} = \frac{m^2S^2+2mS+1}{m^2S+2mS+1}.$$

$$0 \le S \le 1, S^2 \le S, \frac{P_N}{P_{n^2}} \le 1.$$

Як видно, зростання продуктивності ієрархічної системи більше за зростання продуктивності паралельної системи для всіх значень $S$ за винятком тривіальних значень $S$=0 (повністю паралельна система) та $S$=1 (система без можливості паралельної роботи). За законом Амдаля двовимірна ієрархічна система забезпечує більше зростання продуктивності, ніж паралельна одновимірна незалежно від властивостей програм, які виконують її вузли.

**Порівняння структур за законом Густафсона**

За законом Густафсона:

$$P_N = N + (1-N)S = n^2 + (1-n^2)S;$$

$$P_{n^2} = (n + (1-n)S)^2 = n^2 + 2n(1-n)S + (1-n)^2 S^2;$$

$$P_N - P_{n^2} = (n^2 + (1-n^2)S) - (n^2 + 2n(1-n)S + (1-n)^2 S^2);$$

$$P_N - P_{n^2} = S(1-S)(1-n)^2 \geq 0 \cdot$$

За законом Густафсона двовимірна ієрархічна система забезпечує менше зростання продуктивності, ніж паралельна одновимірна незалежно від властивостей програм, які виконують її вузли.

**Найкращі за законом Амдаля багатовимірні структури**

Як було показано, двовимірна система (рис. 4) має за законом Амдаля більшу продуктивність, ніж одновимірна (рис. 3). Якщо розглядати кожний вузол 2-го рівня як паралельну систему вузлів 3-го рівня, можна за аналогією показати, що тривимірна ієрархічна система (рис. 5) є більш продуктивною за законом Амдаля, ніж двовимірна. Загалом $n$-вимірна ієрархічна система є більш продуктивною, ніж $m$-вимірна ($n > m$).

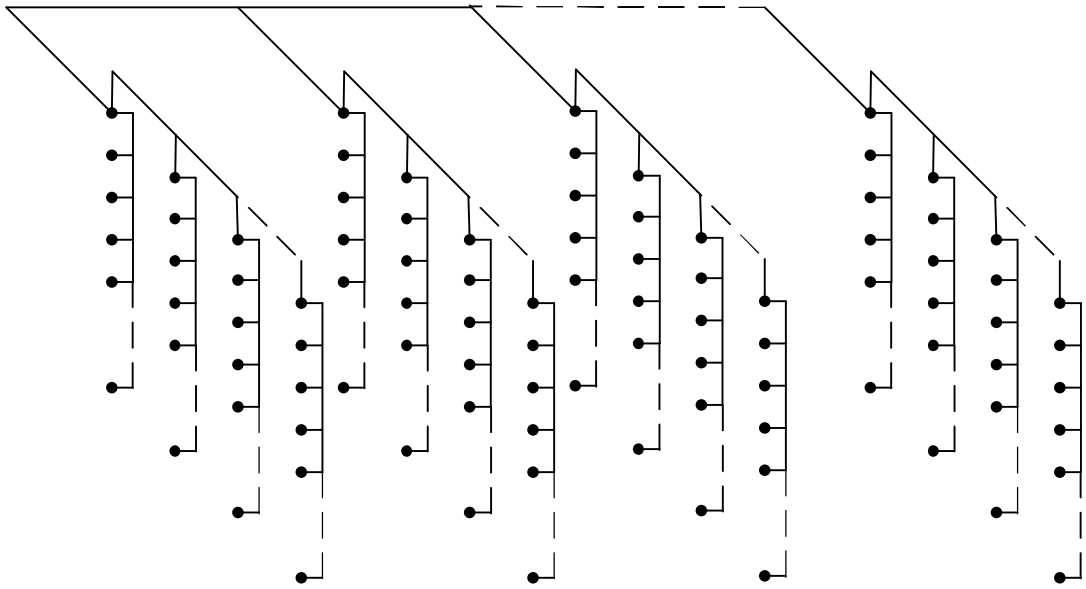

*Рис. 5. Тривимірна система*

У наведених прикладах передбачалось для спрощення, що всі вузли порівнюваних систем мають однакові характеристики. Але до складу ієрархічних систем входять вузли з різними характеристиками. Деякі з вузлів ієрархічних систем (протокольні процесори) виконують специфічні функції забезпечення зв'язку між ієрархічними рівнями (на наведених рисунках до них підходять декілька ліній зв'язку). Відмінність характеристик вузлів слід враховувати при точнішому оцінюванні ієрархічних систем.

**Апаратні і програмні багаторівневі системи**

Аналогією апаратних багаторівневих структур у програмуванні є програми з підпрограмами (процедурами, функціями). Така аналогія дає змогу адаптувати для проектування спеціалізованих багаторівневих процесорів рішення (процедурну абстракцію і наступну декомпозицію), знайдені для програмування [9]. Перевагами процедурної абстракції є модифікованість і локальність. І вони ж є визначальними рисами гарантоздатних [10, 11] систем, так само, як і конфіденційність. Одним із засобів забезпечення конфіденційності є використання цифрових підписів та пристроїв, які їх обробляють.

При створенні процедур (функцій) програмісти дотримуються таких загальних рекомендацій [12, 13]:

– процедура (функція) повинна містити не більше ніж 60 рядків тексту;
– процедура (функція) повинна викликатися не менше двох разів (більше одного разу);

– функція повинна робити тільки одне справу;
– мати дуже багато рівнів абстракції або інкапсуляції так само погано, як і дуже мало;
– код, використовуваний більше одного разу, має бути поміщений у функцію;
– функція повинна мати лише одну точку виходу.

Ці самі рекомендації можуть бути цінними і при виділенні рівнів у багаторівневій системі під час її проектування.

Отже, використовувати багаторівневі системи у пристроях обробки цифрових підписів змушує не тільки їхня більша (порівняно з паралельними системами) продуктивність, але і їхня локальність і можливість модифікації (менша, своєю чергою, ніж у паралельних систем).

**Висновки.** У складі гарантоздатних систем присутні пристрої, які забезпечують їхню конфіденційність. Одним з таких пристроїв є пристрій обробки цифрових підписів, який реалізує криптографічні алгоритми, що мають ієрархічну структуру.

Перевага ієрархічних структур за законом Амдаля підтверджує доцільність обрання таких структур на етапі проектування ієрархічних багаторівневих пристроїв обробки цифрових підписів.

Менша продуктивність ієрархічних структур за законом Густафсона свідчить про їхню меншу гнучкість, модифікація таких систем здійснюється складніше за модифікацію паралельних систем.

Можна вважати ієрархічні структури більш спеціалізованими, ніж паралельні.

*1. Cees Jan Koomen. Multicore demands communications. EE Times Europe. September 22-October 5. 2008. p. 6. 2. Shekhar Borkar. Thousand Core Chips – A Technology Perspective. DAC 2007, June 4–8, 2007, San Diego, California, USA. Copyright 2007 ACM 978-1-59593-627-1/07/0006. 3. Кудин А.В., Линёв А.В. Архитектура и операционные системы параллельных вычислительных систем: Учебно-методические материалы по программе повышения квалификации «Технологии высокопроизводительных вычислений для обеспечения учебного процесса и научных исследований». – Нижний Новгород, 2007. – 73 с. 4. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003. 5. Глухов В.С., Еліас Р. Багаторівневі системи і закон Амдаля / Материалы международной научно-практической конференции «Информационные технологии и информационная безопасность в науке, технике и образовании. Инфотех-2009», г. Севастополь. – С. 252–255, 7–12 вересня 2009. 6. ДСТУ ISO/IEC 7498-1:2004. Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Ч. 1. Базова модель (ISO/IEC 7498-1:1994, IDT). 6. Глухов В.С., Бондарук А.Б., Євтушенко К.С., Заіченко Н.В., Калінічев В.А., Оліярник Б.О. Гарантоздатна система оброблення навігаційних і картографічних даних: Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення захисту інформації в Україні». – К., 2008. – Вип. 1 (16). 7. Глухов В.С. Оцінка апаратних витрат на реалізацію багаторівневої комп'ютерної системи // Вісник Національного університету «Львівська політехніка» «Комп'ютерні науки та інформаційні технології». – 2008. – № 629. – С.13–20. 8. Глухов В., Еліас Р. Вибір варіанту декомпозиції цифрових автоматів. Матеріали 4$^{oї}$ міжнародної науково-технічної конференції CSIT'2009 «Комп'ютерні науки та інформаційні технології 2009». – Львів. – С. 202–205, 15–17 жовтня 2009 р. 9. Лисков Б., Гатэг Дж. Использование абстракций и спецификаций при разработке программ. – М.: Мир, 1989. – 424 с. 10. Avizienis, J.-C. Laprie and B. Randell. Fundamental Concepts of Dependability. Research Report No 1145, LAAS-CNRS, April 2001. 11. A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, pp. 11-33, 2004. 12. Anderson Paul. Trends in safety-critical coding and testing practices. In Boards & Solutions (the european embedded computing magazine), June 2009, pp. 32-33. 13. Ален И. Голуб. Правила программирования на С и С++. –М.: БИНОМ, 1996.*