Abstract. This article discusses the mathematical foundations of cryptography. The application of basic concepts of number theory such as the properties of primes and the difficulty of factorizing large numbers in RSA encryption. How algebraic structures such as groups, rings, and fields are used to build various cryptographic schemes, such as key exchange protocols. Use of non-associative algebraic systems – quasigroups in encryption. Polynomials in the construction of secret distribution schemes. As well as hash functions and hashing, which are an integral part of many data protection algorithms.
Keywords: algebra, quasigroup, cryptography, encryption, decryption.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Diffie W., Hellman M. E. New directions in cryptography. *IEEE Transactions on Information Theory.* 1976. Vol. 22(6). P. 644–654.
2. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM.* 1978. Vol. 21(2). P. 120–126.
3. Brassard G. Modern Cryptology, Lecture Notes in Computer Science 325, Berlin: Springer Verlag, 1988.
4. Smid M. E., Branstad D. K. The date encryption standard: past and future. *Contemporary Cryptology, The science of Information Integrity.* Piscataway: IEEE Press, 1992. P. 43–64.
5. D'enes J., Keedwell A. D. Some applications of non-associative algebraic systems in cryptology. *Pure Mathematics and Applications.* 2001. Vol. 12(2). P. 147–195.
6. Shcherbacov V. On some known possible applications of quasigroups in cryptology: manuscript, 2003.
7. Markovski S., Gligoroski D., Andova S. Using quasigroups for one-one secure encoding. *Proceedings of VIIIth Conference for Logic and Computing – LIRA'97.* September 1997, Novi Sad, 1997.
8. Markovski S., Gligoroski D., Bakeva V. Quasigroup String Processing: Part 1, Maced. Acad. of Sci. and Arts, Sc. Math. Tech. Scien. XX 1–2, 1999.
9. Gligoroski D., Markovski S. Cryptographic Potentials of Quasigroup Transformations, manuscript, 2003.
10. Mileva A. Cryptographic Primitives with Quasigroup Transformations: Ph.D. dissertation, University Ss. Cyril and Methodius, Skopje, Macedonia, 2010.

УДК 004.056.2:004.042:53.083.8:53.088.4

ПОРІВНЯННЯ СТАБІЛЬНОСТІ ДАТЧИКІВ ТЕМПЕРАТУРИ НА ОСНОВІ МЕТОДУ ДИСПЕРСІЇ АЛЛАНА В СИСТЕМАХ КЛІМАТИЧНОГО КОНТРОЛЮ

Д. А. Росолик, В. Г. Крижановський

Анотація. Дослідження спрямоване на оцінку стабільності і точності вимірювання залежностей температури середовища за допомогою сенсорів DHT22 та DS18B20, які широко використовуються в кліматичному обладнанні, за допомогою методів дисперсії Аллана. Проаналізовано три основні методи обчислення дисперсії Аллана: класичний, модифікований та перекриваючий. На основі експериментальних даних, отриманих з прототипу сенсорного вузла Інтернету речей, проведено порівняльний аналіз стабільності сенсорів. Результати дослідження надають цінну інформацію для вибору датчиків залежно від специфіки застосування в системах кліматичного контролю.
Ключові слова: сенсори, дисперсія Аллана, кліматичне обладнання, стабільність вимірювання.

У сучасному світі кліматичне обладнання відіграє критичну роль у забезпеченні комфорту та безпеки людей, а також у підтримці оптимальних умов для різноманітних технологічних процесів. Ключовим аспектом ефективності такого обладнання є точність і надійність сенсорних даних, які воно отримує та обробляє. Однак сенсори піддаються впливу різноманітних факторів, що можуть призвести до нестабільності вимірювань, дрейфу показників та накопичення похибок з часом. Обчислення дисперсії Аллана дає змогу окремо аналізувати впливи, які відрізняються часовим масштабом, що дає змогу розділяти похибки вимірювальної системи від характерних сторонніх впливів [1].

Актуальність дослідження методів обчислення дисперсії Аллана для аналізу сенсорних даних кліматичного обладнання зумовлена зростаючими вимогами до точності та надійності систем кліматичного контролю [2], неефективність роботи яких призводить до перевитрат енергії на опалення та кондиціонування приміщень.

Метою дослідження є провести оцінку стабільності та точності процесу вимірювання сенсорів DHT22 і DS18B20 через аналіз дисперсії Аллана, що надає цінну інформацію для вибору датчика залежно від специфіки застосування.

Проблема стабільності й точності сенсорів у кліматичному обладнанні є критичною для багатьох галузей. Наприклад:

• У серверних приміщеннях нестабільність температурних сенсорів може призвести до перегріву обладнання, що загрожує виходом з ладу дорогих систем.

• У фармацевтичній промисловості неточності у вимірюванні вологості можуть вплинути на якість ліків.

• У музеях неточний контроль кліматичних умов може призвести до пошкодження цінних експонатів.

Наявні дослідження [2; 3] вказують на ефективність методів дисперсії Аллана для оцінки стабільності різноманітних сенсорів, проте їх застосування до конкретних типів датчиків кліматичного обладнання залишається недостатньо вивченим.

Дисперсія Аллана є потужним інструментом для аналізу стабільності часових рядів, особливо в контексті сенсорних даних. У цьому дослідженні розглядаються три основні методи обчислення дисперсії Аллана:

1. Класичний метод дисперсії Аллана (ADEV);
2. Модифікована дисперсія Аллана (MDEV);
3. Перекриваюча дисперсія Аллана (OADEV).

Варто зазначити, що окрім класичних методів, існують інші підходи для обчислення дисперсії Аллана, які забезпечують різну точність і чутливість до шумів. Наприклад, Time Deviation (TDEV) аналізує часові зміни, Hadamard Deviation (HDEV) ефективно фільтрує дрейф, а Parabolic Deviation (PDEV) оцінює невизначеність даних та Groslambert Covariance (GCODEV) покращують точність для складних сигналів, що дає змогу дослідникам обирати методи, які найкраще відповідають специфіці їхніх даних [4].

Таблиця 1 представляє формули та короткий опис кожного методу:

Таблиця 1

Методи обчислення дисперсії Аллана

Метод	Формула	Короткий опис
Класичний метод дисперсії Аллана	$\sigma_y^2(\tau) = \frac{1}{2\tau^2}\langle(x_{i+2} - 2x_{i+1} + x_i)^2\rangle$	Базовий метод для оцінки стабільності часових рядів
Модифікована дисперсія Аллана	$\mathrm{Mod}\sigma_y^2 = \frac{1}{2m^4\tau_0^2(\mathrm{N} - 3\mathrm{m} + 1)} \sum_{j=0}^{N-3m} \left(\sum_{i=j}^{j+m-1} (x_{i+2m} - 2x_{i+m} + x_i) \right)^2$	Покращений метод з кращою здатністю розрізняти типи шумів
Перекриваюча дисперсія Аллана	$\sigma_y^2(\tau) = \frac{1}{2(\mathrm{N} - 2\mathrm{n} + 1)} \sum_{i=1}^{N-2n+1} (\bar{y}_{i+n}(\tau) - \bar{y}_i(\tau))^2$	Метод з більш ефективним використанням доступних даних

Кожен з цих методів має свої переваги та особливості застосування:

• Класичний метод (ADEV) відрізняється простотою реалізації та інтерпретації результатів, що робить його привабливим для швидкого аналізу. Він ефективно виявляє білий шум та випадкове блукання, які часто наявні в сигналах сенсорів температури та вологості.

• Модифікована дисперсія Аллана (MDEV) демонструє покращену здатність розрізняти різні типи шумів та підвищену чутливість до довгострокових нестабільностей. Це робить її особливо цінною для виявлення поступових змін у характеристиках сенсорів [1].

• Перекриваюча дисперсія Аллана (OADEV) пропонує більш ефективне використання доступних даних та покращену статистичну достовірність на довгих інтервалах вимірювань. Це робить її особливо цінною для аналізу систем кліматичного контролю з обмеженим набором вимірювань.

Для проведення експериментальних досліджень було створено прототип сенсорного вузла Інтернету речей на базі ESP32 з використанням двох датчиків температури: DHT22 та DS18B20. Система підключалася до комп'ютера з Windows 10, що дало змогу здійснювати збір даних за допомогою спеціалізованого програмного забезпечення.

Було зібрано по 265 вимірювань з інтервалом у 4 секунди для кожного сенсора. Зібрані дані були підготовлені для подальшого використання: видалення можливих аномальних значень.

Після цього дані були готові для обчислення дисперсії Аллана та подальшого аналізу. Такий підхід забезпечує високу якість отриманих результатів і мінімізує вплив перешкод на процес вимірювань.

Обробка та аналіз отриманих даних, включно з обчисленням дисперсії Аллана, проводилися з використанням мови програмування Python [5].

Важливо зазначити, що отримані значення ADEV, MDEV та OADEV представлені у безрозмірних одиницях і можна інтерпретувати як відхилення в °C. Порівняння з паспортною точністю сенсорів(±0.5°C для обох DS18B20 та DHT22) показує, що обидва сенсори працюють в межах заявленої точності.

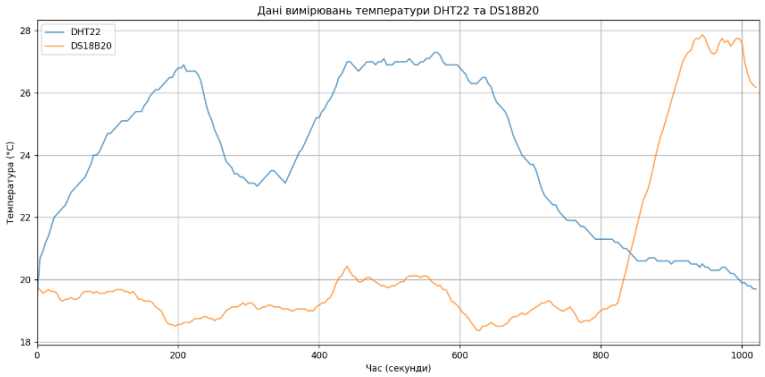

Рис. 1. Дані вимірювань температури, що використовувалися для обчислення дисперсії Аллана

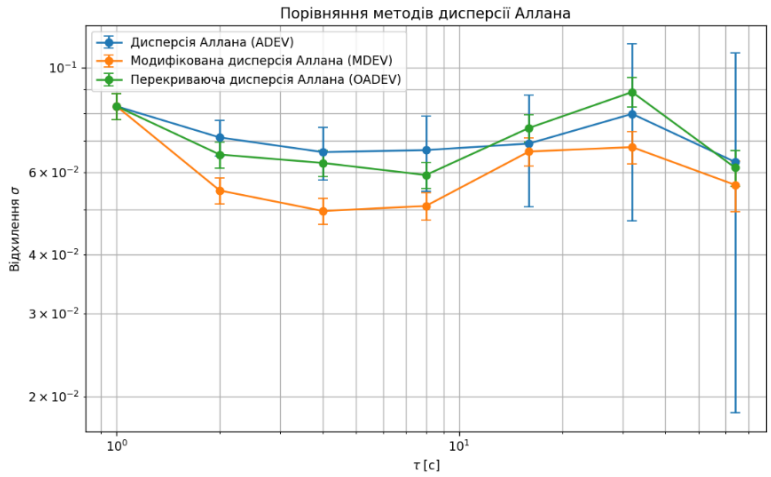

Рис. 2. Порівняння методів розрахунку дисперсії Аллана для даних з датчика DHT22

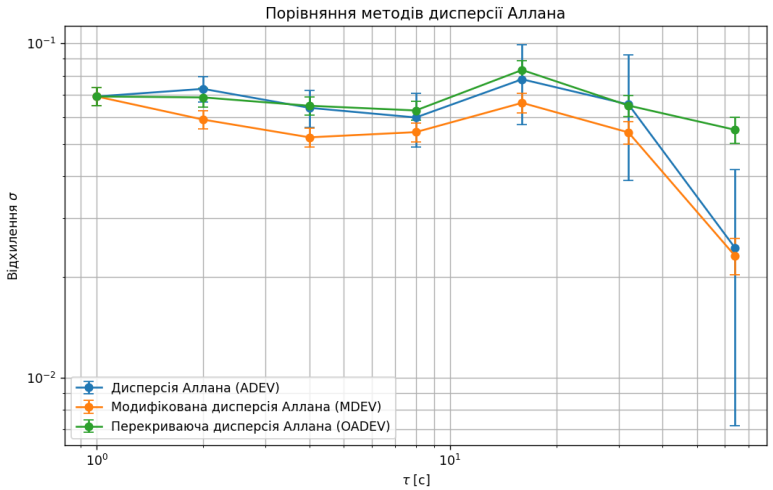

Рис. 3. Порівняння методів розрахунку дисперсії Аллана для даних з датчика DS18B20

Графіки рисунків 1, 2 демонструють, як різні методи розрахунку дисперсії Аллана (ADEV, MDEV, OADEV) оцінюють стабільність температурних вимірювань на різних часових інтервалах (τ). Часові інтервали представлені логарифмічному масштабі ступеня двійки. Результати

обчислення дисперсії Аллана різними методами для сенсорів DHT22 та DS18B20 представлені у таблиці 2 та 3 відповідно.

Таблиця 2

Обчислення дисперсії Аллана на основі даних сенсора DHT22

Метод	Taus	Відхилення	Помилки
ADEV	[1, 2, 4, 8, 16, 32, 64]	[0.0828, 0.0711, 0.0661, 0.0668, 0.0690, 0.0798, 0.0630]	[0.0052, 0.0063, 0.0084, 0.0122, 0.0184, 0.0326, 0.0446]
MDEV	[1, 2, 4, 8, 16, 32, 64]	[0.0828, 0.0548, 0.0496, 0.0508, 0.0663, 0.0678, 0.0563]	[0.0052, 0.0035, 0.0032, 0.0033, 0.0046, 0.0053, 0.0070]
OADEV	[1, 2, 4, 8, 16, 32, 64]	[0.0828, 0.0654, 0.0627, 0.0591, 0.0744, 0.0887, 0.0613]	[0.0052, 0.0041, 0.0040, 0.0038, 0.0050, 0.0064, 0.0054]

Таблиця 3

Обчислення дисперсії Аллана на основі даних сенсора DS18B20

Метод	Taus	Відхилення	Помилки
ADEV	[1, 2, 4, 8, 16, 32, 64]	[0.0693, 0.0731, 0.0641, 0.0600, 0.0780, 0.0656, 0.0245]	[0.0044, 0.0065, 0.0081, 0.0110, 0.0209, 0.0268, 0.0173]
MDEV	[1, 2, 4, 8, 16, 32, 64]	[0.0693, 0.0591, 0.0523, 0.0542, 0.0663, 0.0541, 0.0232]	[0.0044, 0.0037, 0.0033, 0.0036, 0.0046, 0.0043, 0.0029]
OADEV	[1, 2, 4, 8, 16, 32, 64]	[0.0693, 0.0689, 0.0650, 0.0630, 0.0832, 0.0651, 0.0551]	[0.0044, 0.0043, 0.0041, 0.0041, 0.0056, 0.0047, 0.0049]

Аналізуючи отримані результати, можна сказати, що:

- Датчик DHT22 під час використання ADEV демонструє значення, що варіюється від 0.0661 до 0.0828, що вказує на помірну наявність шуму. Помилки у вимірюваннях коливаються від 0.0052 до 0.0446.
- Датчик DS18B20 демонструє вищу стабільність з ADEV в межах 0.0245 до 0.0780 та меншими помилками, які варіюються від 0.0044 до 0.0268.
- Порівнюючи методи, у DHT22 модифікована дисперсія (MDEV) змінюється в діапазоні від 0.0496 до 0.0828, тоді як у DS18B20 MDEV коливається від 0.0523 до 0.0693. Це свідчить про те, що DS18B20 демонструє стабільніші показники, особливо на великих часових інтервалах.
- Використання методу OADEV для DHT22 показує відхилення в діапазоні від 0.0591 до 0.0887, тоді як для DS18B20 OADEV варіюється від 0.0551 до 0.0832. Це вказує на те, що сенсор DS18B20 має кращу стабільність, особливо при коротких часових інтервалах.

Висновки. Аналіз дисперсії на різних часових інтервалах має практичне значення, оскільки він дає змогу визначити, в яких умовах метрологічні (і фізичні) властивості сенсора мають вплив на вимірювану величину, відповідно оптимізувати використання сенсорів у реальних умовах, з вибором оптимального інтервалу вимірювань, оцінкою довгострокової стабільності результатів вимірювань.

На основі проведеного дослідження можна зробити висновок, що сенсор DS18B20 виявляється більш надійним для тривалих вимірювань завдяки меншим значенням ADEV (до 0.0780), MDEV (до 0.0693) і OADEV (до 0.0832). Натомість DHT22 показує вищі значення ADEV (до 0.0828) і OADEV (до 0.0887), що потребує більшого контролю на довгих інтервалах, аби забезпечити точність вимірювань у процесах моніторингу кліматичних умов.

Методи дисперсії Аллана виявилися ефективними для оцінки стабільності сенсорів кліматичного обладнання та можуть бути рекомендовані для використання під час розробки та оптимізації систем кліматичного контролю. Подальші дослідження можуть бути спрямовані на розширення спектра аналізованих сенсорів та розробку автоматизованих систем моніторингу стабільності датчиків на основі дисперсії Аллана.

Abstract. This study aims to evaluate the stability and accuracy of the DHT22 and DS18B20 sensors, which are widely used in climate equipment, using Allan variance methods. Three main methods for calculating Allan variance were analyzed: classical, modified, and overlapping. Based on experimental data obtained from a prototype Internet of Things sensor node, a comparative analysis of the sensors' stability was conducted. The research results provide valuable information for selecting sensors depending on the specific application in climate control systems.

Keywords: sensors, Allan variance, climate equipment, measurement stability.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Котелянець В. В. Інформаційна технологія моніторингу навколишнього середовища на базі концепції інтернету речей. МОН України, ЧДТУ. Черкаси, 2019.
2. Використання дисперсії Аллана для ідентифікації нормальної роботи сенсорних вузлів / В. Г. Крижановський, В. Ф. Комаров, С. П. Сергієнко, Л. В. Загоруйко. *Вісник Вінницького політехнічного інституту.* 2021. № 3.
3. Non-Stationary Noise Analysis of Magnetic Sensors using Allan Variance / K. Draganová, V. Moucha, T. Volcko, K. Semrád. *Acta Physica Polonica.* 2017. Vol. 131(4). P. 1126–1128.
4. Implemented statistics functions. URL: https://allantools.readthedocs.io/en/latest/functions.html
5. Python. URL: https://www.python.org/
6. Котелянець В. В. Інформаційна технологія моніторингу навколишнього середовища на базі концепції інтернету речей. МОН України, ЧДТУ. Черкаси, 2019.
7. Ємець К. Методи прогнозування часових рядів з вираженою сезонністю на основі трансформерів. *Herald of Khmelnytskyi National University. Technical Sciences.* 2024. Vol. 333(2). P. 131–134.
8. Marusenkova T. Analysis of the influence of sample rates on the allan variance. *Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі.* 2019. Вип. 5. С. 53–61.
9. Жураковський Б. Ю., Зенів І. О. Технології інтернету речей: навчальний посібник. Київ, 2021. 271 с.

УДК 004.437

ОПТИМІЗАЦІЇ РОБОТИ STD::LIST ШЛЯХОМ ВИБОРУ НАЙБІЛЬШ ЕФЕКТИВНОЇ СТРАТЕГІЇ ВИДІЛЕННЯ ПАМ'ЯТІ

М. В. Шевцов, О. С. Вєтров

Анотація. У роботі досліджується ефективність контейнера std::list з використанням різних алгоритмів виділення пам'яті. Проводиться порівняння між стандартним (std::allocator) та користувацьким аллокатором, що базується на принципах роботи stack-based allocator. Була детально розглянута теорія з цієї теми та проведене дослідження. Результати викладено у таблиці та візуалізовано у вигляді діаграми.

Ключові слова: C++, std::list, аллокатор пам'яті, StackAllocator, ефективність, оптимізація, зв'язний список.

Сучасний світ програмування визначається постійним прагненням до оптимізації та підвищення ефективності програмного забезпечення. Однією з ключових областей цього пошуку є вибір та оптимізація структур даних, які використовуються для зберігання і обробки інформації. Мова програмування C++ визначається своєю потужністю та широкими можливостями, що вона надає користувачу для роботи з пам'яттю. Водночас важливою залишається вимога до програміста контролювати всі процеси виділення пам'яті (аллокації), оскільки непродумана стратегія безпосередньої роботи з пам'яттю в C++ може привести до некоректного функціонування програмного додатка та всієї операційної системи загалом.

Аллокація – це процес виділення блоків пам'яті потрібного розміру.

Для роботи з масивами інформації має виділятися пам'ять для даних, що оброблюються комп'ютером. Для виділення пам'яті під масиви змінних використовуються відповідні оператори, функції тощо. Зокрема, у мові програмування C++ виділяють способи виділення пам'яті – статичний та динамічний.

Статичне (фіксоване) виділення пам'яті: пам'ять виділяється тільки один раз під час компіляції. Розмір виділеної пам'яті є фіксованим і незмінним до кінця виконання програми.

Динамічне виділення пам'яті: використовується комбінація операторів new і delete. Оператор new виділяє пам'ять для змінної (масиву) у спеціальній ділянці пам'яті, яка називається «купа» (heap). Оператор delete звільняє виділену пам'ять. Кожному оператору new має відповідати свій оператор delete.

Динамічно виділена пам'ять не має області видимості, тобто вона залишається виділеною доти, доки її не буде явно звільнено або доки ваша програма не завершить своє виконання (і операційна система очистить усі буфери пам'яті самостійно). Однак покажчики, що використовуються для зберігання динамічно виділених адрес пам'яті, дотримуються правил області видимості звичайних змінних.

У програмах, реалізованих на C++, доступні два види пам'яті: стек і купа (heap). Керування стеком відбувається автоматично. Під час виходу змінної з області видимості відповідна їй у