УДК 004.738.5:004.722]:004.056

ПОЛІНОМІАЛЬНІ КРИПТОГРАФІЧНІ МЕТОДИ АВТЕНТИФІКАЦІЇ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Соколов О.К.
e-mail: oleksandr.sokolov1@nure.ua
Науковий керівник – д.т.н., доц. Чала О.В.
Харківський національний університет радіоелектроніки, каф. ІСТ
м. Харків, Україна

The rapid development of the Internet of Things (IoT) requires lightweight security mechanisms for device authentication. This paper considers polynomial-based cryptographic methods for IoT systems. Symmetric, quadratic, Chebyshev, and Dickson polynomials are analyzed in the context of authentication protocols. The results show that polynomial methods can provide sufficient security with relatively low computational overhead, making them suitable for resource-constrained IoT devices.

Стрімкий розвиток технологій інтернету речей (Internet of Things, IoT) призводить до зростання кількості пристроїв, що взаємодіють у мережевому середовищі та обмінюються даними в режимі реального часу. До таких пристроїв належать сенсорні вузли, промислові контролери, безпілотні системи, елементи «розумної» інфраструктури та інші компоненти кіберфізичних систем. Водночас обмежені обчислювальні ресурси, невеликий обсяг пам’яті та низьке енергоспоживання таких пристроїв створюють суттєві труднощі для використання класичних криптографічних механізмів захисту. У зв’язку з цим особливої актуальності набуває розробка легковагових криптографічних методів, здатних забезпечити надійну автентифікацію пристроїв при мінімальних витратах ресурсів.

Одним із перспективних напрямів у цій сфері є використання поліноміальних криптографічних конструкцій. Поліноміальні методи базуються на властивостях математичних функцій, що дозволяють будувати ефективні схеми узгодження ключів, автентифікації та розподілу секретів. Завдяки відносно простим обчисленням такі методи добре підходять для реалізації у середовищі IoT, де критичними є швидкість виконання операцій і мінімізація енергоспоживання [1].

Одним із базових підходів до побудови криптографічних схем у сенсорних мережах є використання симетричних поліномів для попереднього розподілу ключів. Нехай

$$f(x,y) = \sum_{i=0}^{t} \sum_{j=0}^{t} a_{ij} x^i y^j, \qquad (1)$$

де t – степінь полінома, а коефіцієнти задовольняють умову симетрії $a_{ij} = a_{ji}$. У такому випадку виконується властивість $f(x, y) = f(y, x)$.

Якщо вузли мережі мають унікальні ідентифікатори u та v, кожен із них може обчислити спільний секретний ключ $K_{uv} = f(u, v) = f(v, u)$.

Таким чином, обидва пристрої незалежно формують однаковий ключ без необхідності передавання секретних параметрів мережею. Такий механізм значно зменшує комунікаційні витрати та підвищує стійкість системи до атак перехоплення даних [2].

Подальший розвиток поліноміальних криптографічних схем пов'язаний із використанням квадратичних форм. У цьому випадку ключова функція може бути представлена у вигляді $Q(x) = x^T Ax$, де x – вектор параметрів вузла, а A – симетрична матриця коефіцієнтів. Для взаємодії двох вузлів може використовуватися узагальнена функція $Q(x, y) = x^T Ay$.

Застосування квадратичних поліномів дозволяє підвищити криптографічну стійкість схеми, оскільки визначення секретних параметрів потребує розв'язання системи нелінійних рівнянь. Крім того, такі конструкції можуть забезпечувати генерацію унікальних сеансових ключів для різних пар вузлів мережі [3].

Іншим перспективним підходом є використання поліномів Чебишова, які широко застосовуються у легковагових криптографічних протоколах. Поліноми першого роду визначаються рекурентним співвідношенням $T_0(x) = 1, T_1(x) = x, T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$. Важливою властивістю цих поліномів є композиційна залежність

$$T_{mn}(x) = T_m\big(T_n(x)\big). \qquad (2)$$

Завдяки цій властивості можна реалізувати механізм узгодження ключів між пристроями. Нехай один пристрій обирає секретне число a, а інший – b, тоді вони обчислюють $A = T_a(x), B = T_b(x)$, після чого можуть сформувати спільний ключ $K = T_a(B) = T_b(A) = T_{ab}(x)$. Такий підхід нагадує принцип роботи протоколу Діффі–Хеллмана, однак використовує поліноміальні перетворення, що можуть виконуватися з меншими обчислювальними витратами [4].

У системах, де необхідно автентифікувати одночасно групу пристроїв, можуть застосовуватися поліноми Діксона. Ці поліноми задаються параметрами n та a і мають важливу властивість композиції

$$D_{mn}(x, a) = D_m(D_n(x, a), a). \qquad (3)$$

Завдяки цьому вони можуть використовуватися для побудови групових криптографічних протоколів, у яких кілька пристроїв проходять процедуру автентифікації через перевірку відповідності значень поліноміальних функцій. Це особливо актуально для промислових IoT-систем, де велика кількість вузлів повинна взаємодіяти в єдиній мережі [1].

Застосування поліноміальних криптографічних методів дозволяє забезпечити ефективний баланс між рівнем безпеки та витратами ресурсів.

Такі методи характеризуються відносно невеликою обчислювальною складністю, що робить їх придатними для використання на пристроях з обмеженими апаратними можливостями. Крім того, поліноміальні схеми можуть забезпечувати стійкість до типових атак у середовищі IoT, зокрема атак повтору (replay attack), підміни повідомлень, перехоплення ключів та захоплення вузлів мережі [1, 3].

Для оцінювання ефективності поліноміальних підходів до автентифікації пристроїв інтернету речей враховують обчислювальну складність алгоритмів, обсяг передаваних даних, вимоги до пам'яті та стійкість до типових криптографічних атак.

Симетричні поліноми характеризуються низькою складністю та простотою реалізації, що дозволяє застосовувати їх для розподілу ключів між вузлами мережі, однак вони можуть бути вразливими при компрометації значної кількості пристроїв. Квадратичні поліноміальні конструкції забезпечують вищу криптографічну стійкість і формування унікальних ключів, але потребують більших ресурсів. Поліноми Чебишова використовуються у легковагових криптографічних протоколах, тоді як поліноми Діксона застосовуються для групової автентифікації в масштабних IoT-мережах.

Таким чином, поліноміальні криптографічні методи є перспективним напрямом забезпечення безпеки IoT, оскільки поєднують достатній рівень захисту з відносно невеликими обчислювальними витратами.

Список використаних джерел:

1. Liu Z., Luo Y. Dynamic coefficient symmetric polynomial-based secure key management scheme for Internet of Things (IoT) networks. PeerJ computer science. 2023. Vol. 9. P. e1726. URL: https://doi.org/10.7717/peerj-cs.1726 (дата звернення: 11.03.2026).

2. Wang Q., Li H. Application of IoT authentication key management algorithm to personnel information management. Computational intelligence and neuroscience. 2022. Vol. 2022. P. 1–11. URL: https://doi.org/10.1155/2022/4584072 (дата звернення: 11.03.2026).

3. Dickson polynomial-based secure group authentication scheme for Internet of Things / S. A. Syed et al. Scientific reports. 2024. Vol. 14, no. 1. URL: https://doi.org/10.1038/s41598-024-55044-2 (дата звернення: 12.03.2026).

4. ChebIoD: a Chebyshev polynomial-based lightweight authentication scheme for internet of drones environments / Z. G. Al-Mekhlafi et al. Scientific reports. 2025. Vol. 15, no. 1. URL: https://doi.org/10.1038/s41598-025-18387-y (дата звернення: 12.03.2026).