УДК 004.056.55:519.688

Палій О.М.

РЕКУРЕНТНІ ПОСЛІДОВНОСТІ НАД СКІНЧЕННИМИ ПОЛЯМИ ЯК МАТЕМАТИЧНИЙ АПАРАТ КРИПТОГРАФІЧНИХ ЗАДАЧ: ОГЛЯД ЗАСТОСУВАНЬ

Вінницький національний технічний університет

Анотація

У тезах представлено огляд застосувань рекурентних послідовностей над скінченними полями як єдиного математичного апарату для розв'язання криптографічних задач. Розглянуто класифікацію лінійних та нелінійних рекурентних структур (LFSR, m-послідовності, послідовності Голда і Касамі, NFSR-конструкції), окреслено їхню роль у потокових шифрах, генераторах псевдовипадкових чисел, завадостійких кодах і схемах розподілу секрету. Особливу увагу приділено малодослідженому напряму — застосуванню узагальнених послідовностей Фібоначчі у порогових схемах розподілу секрету. Виявлено наукову нішу та обґрунтовано перспективність побудови нового класу криптографічних протоколів на основі рекурентних структур над скінченними полями.

Ключові слова: рекурентні послідовності; скінченні поля; криптографія; потокові шифри; LFSR; розподіл секрету; узагальнені послідовності Фібоначчі.

Abstract

The theses present a review of applications of recurrent sequences over finite fields as a unified mathematical apparatus for cryptographic tasks. A classification of linear and nonlinear recurrent structures (LFSR, m-sequences, Gold and Kasami sequences, NFSR-based constructions) is considered, and their role in stream ciphers, pseudorandom number generators, error-correcting codes, and secret sharing schemes is outlined. Particular attention is paid to an underexplored direction — the use of generalized Fibonacci sequences in threshold secret sharing schemes. A scientific gap is identified, and the prospects for developing a new class of cryptographic protocols based on recurrent structures over finite fields are substantiated.

Keywords: recurrent sequences; finite fields; cryptography; stream ciphers; LFSR; secret sharing; generalized Fibonacci sequences.

Вступ

Сучасна криптографія значною мірою спирається на математичний апарат скінченних полів $GF(p)$ та $GF(p^m)$. Серед алгебраїчних об'єктів, побудованих над такими полями, особливе місце посідають рекурентні послідовності — детерміновані числові ряди, кожен наступний член яких визначається лінійною або нелінійною функцією попередніх. Лінійні рекурентні послідовності, реалізовані у формі регістрів зсуву зі зворотним зв'язком (LFSR), стали базовим примітивом для побудови потокових шифрів, генераторів псевдовипадкових чисел та завадостійких кодів [1]. Їх алгебраїчна структура — характеристичний поліном, матриця компаньйона, період та лінійна складність — описана у фундаментальних монографіях [1, 2] і є відправною точкою для аналізу стійкості відповідних криптосистем.

Незважаючи на те, що теорія рекурентних послідовностей є зрілою, її застосування у задачах розподілу секрету залишається малодослідженим. Класичні порогові схеми Шаміра та Блейклі [3] ґрунтуються на поліноміальній інтерполяції або геометрії гіперплощин, а не на рекурентних структурах. Лише окремі роботи [4] використали LFSR-послідовності для побудови верифікованих схем розподілу секрету. Метою цих тез є систематизація відомостей про рекурентні послідовності над скінченними полями як єдиний криптографічний апарат та обґрунтування доцільності їх застосування — зокрема, узагальнених послідовностей Фібоначчі — у схемах розподілу секрету.

Результати дослідження

Проведений аналіз дозволив побудувати таксономію рекурентних послідовностей над скінченними полями за критерієм типу зворотного зв'язку. До лінійних структур належать класичні LFSR, *m*-

послідовності з максимальним періодом $p^L - 1$, послідовності Голда і Касамі з регульованими кореляційними властивостями, а також послідовності Фібоначчі та їх узагальнення. До нелінійних — регістри зсуву з нелінійним зворотним зв'язком (NFSR), фільтрувальні та комбінаційні генератори, генератори зі стисканням і керованою тактовою частотою. Загальна форма лінійного рекурентного співвідношення порядку k над $GF(p)$ має вигляд:

$$F(n) = \sum_{i=1}^{k} C_i F(n-i) \bmod p, \tag{1}$$

де $C_i \in GF(p)$ — коефіцієнти рекурентного співвідношення; k — порядок рекурентності; $F(n-i)$ — попередні члени послідовності. Для криптографічного застосування ключовими властивостями є період, лінійна складність (за алгоритмом Берлекемпа–Мессі) та автокореляційна функція [1].

Класичні застосування рекурентних послідовностей охоплюють потокові шифри (A5/1 у GSM, E0 у Bluetooth, Trivium і Grain з портфоліо проєкту eSTREAM), генератори псевдовипадкових чисел, циклічні коди та коди Боуза–Чоудхурі–Хоквінгема (БЧХ), коди Ріда–Соломона, а також послідовності розширення спектра у системах CDMA [1, 2]. Сучасні застосування включають хеш-функції зі зворотним зв'язком, MAC-коди на базі поліноміального обчислення та постквантові схеми, що використовують рекурентні структури над поліноміальними кільцями (NTRU, ML-KEM).

Окремий науковий інтерес становить застосування рекурентних послідовностей у схемах розподілу секрету. Огляд літератури показав, що ця область є малодослідженою: у роботі [4] запропоновано верифіковану схему розподілу секрету з кількома секретами на основі LFSR-послідовностей; роботи [5] заклали матричний апарат узагальнених послідовностей Фібоначчі (матриця Q_p, тотожність типу Кассіні), однак запропоновані на їх основі шифрувальні алгоритми виявились вразливими до атак з обраним відкритим текстом. Водночас сам матрично-алгебраїчний апарат зберігає цінність як основа для побудови порогових та зважених схем розподілу секрету.

Узагальнена послідовність Фібоначчі порядку p над $GF(q)$ задається рекурентним співвідношенням:

$$F_p(n) = F_p(n-1) + F_p(n-p-1) \bmod q, \tag{2}$$

причому матриця компаньйона Q_p розміру $(p+1) \times (p+1)$ задовольняє тотожність $\det Q_p^n = (-1)^{pn}$. Ця властивість забезпечує природний механізм верифікації часток без використання обчислювально дорогих криптографічних зобов'язань.

Порівняльний аналіз існуючих підходів виявив наступні переваги схем на основі узагальнених послідовностей Фібоначчі:

- нижча обчислювальна складність на пристроях з обмеженими ресурсами завдяки заміні модульних інверсій додаваннями та зсувами;
- блочна структура матриці Q_p, що природно підтримує побудову ієрархічних та зважених схем;
- наявність вбудованих алгебраїчних інваріантів для верифікації;
- сумісність з апаратурою, що вже містить LFSR-блоки. Водночас виявлено принципове обмеження: відкриті члени послідовності піддаються атаці Берлекемпа–Мессі, якщо їх кількість перевищує $2k$, де k — лінійна складність. Це накладає обмеження на співвідношення між параметрами схеми.

Висновок

Проведений огляд підтверджує, що рекурентні послідовності над скінченними полями є універсальним математичним апаратом сучасної криптографії, об'єднуючи задачі побудови потокових шифрів, завадостійких кодів і схем розподілу секрету. Виявлено, що, попри зрілість цього апарату у класичних застосуваннях, його використання у порогових схемах розподілу секрету залишається малодослідженим. Узагальнені послідовності Фібоначчі, забезпечені матрично-алгебраїчним апаратом матриці компаньйона Q_p та тотожностями типу Кассіні, представляють перспективний напрям для побудови нового класу порогових, зважених та ієрархічних схем розподілу секрету з природною верифікованістю та низькою обчислювальною складністю. Подальші дослідження спрямовані на формалізацію конкретних схем розподілу та відновлення, аналіз їхньої стійкості з урахуванням обмежень Берлекемпа–Мессі, а також експериментальне порівняння з класичними схемами Шаміра та Асмута–Блума.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Golomb S. W. Shift Register Sequences / S. W. Golomb. – 3rd ed. – Singapore : World Scientific, 2017. – 624 p. – DOI: 10.1142/9361.
2. Lidl R. Finite Fields / R. Lidl, H. Niederreiter. – 2nd ed. – Cambridge : Cambridge University Press, 1997. – 755 p. – (Encyclopedia of Mathematics and its Applications ; vol. 20).
3. Beimel A. Secret-sharing schemes: a survey / A. Beimel // Coding and Cryptology : IWCC 2011 : Lecture Notes in Computer Science. – Berlin ; Heidelberg : Springer, 2011. – Vol. 6639. – P. 11–46. – DOI: 10.1007/978-3-642-20901-7_2.
4. Hu C. Verifiable multi-secret sharing based on LFSR sequences / C. Hu, X. Liao, X. Cheng // Theoretical Computer Science. – 2012. – Vol. 445. – P. 52–62. – DOI: 10.1016/j.tcs.2012.05.006.
5. Stakhov A. P. Fibonacci matrices, a generalization of the «Cassini formula», and a new coding theory / A. P. Stakhov // Chaos, Solitons & Fractals. – 2006. – Vol. 30, № 1. – P. 56–66. – DOI: 10.1016/j.chaos.2005.12.054.

Палій Олексій Миколайович — аспірант групи F5-25a, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: alexey.paliy1337@gmail.com

Oleksii Palii – Faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: alexey.paliy1337@gmail.com