УДК 004.056.55:519.688

Палій О.М.

УЗАГАЛЬНЕНІ ПОСЛІДОВНОСТІ ФІБОНАЧЧІ ЯК ОСНОВА ПОБУДОВИ ПОРОГОВИХ СХЕМ РОЗПОДІЛУ СЕКРЕТУ

Вінницький національний технічний університет

Анотація

У тезах обґрунтовано доцільність застосування узагальнених послідовностей Фібоначчі (p-чисел Стахова) як математичної основи для побудови порогових схем розподілу секрету. Показано обмеженість класичних підходів (схема Шаміра) та запропоновано структуру схеми, у якій рекурентні співвідношення виду $F_p(n) = F_p(n-1) + F_p(n-p-1)$ визначають спосіб формування часток секрету. Встановлено, що варіювання порядку узагальнення p надає механізм гнучкої побудови (t, n)-порогових схем з додатковими властивостями: зваженим розподілом повноважень та компактністю часток. Результати відкривають перспективу для розроблення нового класу криптографічних протоколів розподілу секрету.

Ключові слова: розподіл секрету; порогова схема; узагальнені послідовності Фібоначчі; рекурентні послідовності; криптографія; схема Шаміра; скінченне поле.

Abstract

The theses substantiate the use of generalized Fibonacci sequences (Stakhov's p-numbers) as a mathematical foundation for constructing threshold secret sharing schemes. The limitations of classical approaches (Shamir's scheme) are demonstrated, and a scheme structure is proposed in which recurrent relations of the form $F_p(n) = F_p(n-1) + F_p(n-p-1)$ define the method of share generation. It is established that varying the generalization order p provides a mechanism for flexible construction of (t, n)-threshold schemes with additional properties: weighted authority distribution and share compactness. The results open prospects for developing a new class of cryptographic secret sharing protocols.

Keywords: secret sharing; threshold scheme; generalized Fibonacci sequences; recurrent sequences; cryptography; Shamir's scheme; finite field.

Вступ

Задача розподілу секрету полягає у розбитті конфіденційної інформації S на n часток таким чином, що будь-яка підмножина з t або більше часток дозволяє відновити секрет, тоді як будь-яка підмножина розміром менше t не дає жодної інформації про нього. Класична (t, n)-порогова схема Шаміра [1], запропонована у 1979 році, ґрунтується на інтерполяції поліномів над скінченним полем і залишається еталоном завдяки своїй інформаційно-теоретичній стійкості. Проте вона має конструктивні обмеження: розмір кожної частки дорівнює розміру самого секрету, а структура схеми не допускає природного розширення до зважених або ієрархічних схем без суттєвого ускладнення алгоритму [2]. Послідовності Фібоначчі та їх узагальнення давно відомі у комбінаториці та теорії чисел, проте їх систематичне застосування у криптографічних задачах залишається малодослідженою областю. Серед відомих узагальнень особливе місце посідають p-числа Фібоначчі, запропоновані А. Стаховим [3], які задаються рекурентним співвідношенням:

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

де $p \geq 1$ — порядок узагальнення; при $p = 1$ отримується класична послідовність Фібоначчі.

Послідовності F_p породжують детерміновані рекурентні структури з багатими алгебраїчними властивостями, описаними через матрицю компаньйона Q_p розміру $(p + 1) \times (p + 1)$ та тотожність типу Кассіні [3]. Це відкриває нову парадигму у проектуванні схем розподілу: замість поліноміальної інтерполяції — рекурентне розгортання над скінченним полем.

Результати дослідження

У рамках проведеного аналізу розглянуто конструкцію (t, n)-порогової схеми на основі p-чисел Фібоначчі над скінченним полем $GF(q)$:

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

де q — велике просте число або степінь простого числа.

Секрет S кодується у початкових умовах послідовності:

$$F_p(0) = S,\ F_p(1) = r_1, \dots, F_p(p) = r_p, \tag{3}$$

де r_1, ..., r_p — випадкові елементи поля $GF(q)$.

Частки $S_i = F_p(i)$ для $i = p + 1, \dots, p + n$ обчислюються дилером та передаються n учасникам. Відновлення секрету здійснюється за допомогою системи лінійних рівнянь над $GF(q)$, яка однозначно визначається за будь-якими $t = p + 1$ відомими членами послідовності [4]. Таким чином, параметр p безпосередньо визначає поріг схеми: $t = p + 1$.

Ключовою перевагою запропонованого підходу є те, що порядок p виступає як основний параметр проектування схеми. Зокрема, показано, що при $p = 1$ отримується схема на основі класичної послідовності Фібоначчі з порогом $t = 2$, тоді як зростання p природно збільшує пороговий параметр t без зміни алгоритмічної структури. Це принципово відрізняє запропонований підхід від схеми Шаміра, де зміна порога вимагає зміни степеня поліному.

Матрична форма рекурентного співвідношення (2) задається через матрицю компаньйона Q_p розміру $(p + 1) \times (p + 1)$:

$$Q_p = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \tag{4}$$

Така структура дозволяє виразити обчислення часток через піднесення матриці до степеня та використати апарат лінійної алгебри над $GF(q)$ для аналізу стійкості. Тотожність типу Кассіні, доведена А. Стаховим [3]:

$$\det Q_p^n = (-1)^{pn}, \tag{5}$$

забезпечує природний алгебраїчний інваріант, придатний для побудови верифікованих схем розподілу секрету без використання обчислювально дорогих криптографічних зобов'язань. Порівняльний аналіз із схемою Шаміра виявив наступне. По-перше, обидва підходи є інформаційно-теоретично стійкими за умови роботи над скінченним полем достатнього розміру. По-друге, варіювання порядку p дозволяє природно реалізувати зважені схеми, де вага учасника визначається позицією відповідного члена у послідовності [5]. По-третє, матрична форма через Q_p забезпечує ефективне обчислення часток та аналіз стійкості засобами лінійної алгебри.

Разом з тим, виявлено відкриті питання, що потребують подальшого дослідження: встановлення точних умов на параметр p та поле $GF(q)$ для максимізації ентропії часток, аналіз поведінки схеми при роботі з розширеннями полів Галуа $GF(p^m)$, а також дослідження можливості побудови верифікованих схем (Verifiable Secret Sharing) на основі рекурентних структур.

Висновок

Проведений теоретичний аналіз підтверджує перспективність застосування узагальнених послідовностей Фібоначчі (p-чисел Стахова) як основи для побудови порогових схем розподілу секрету. Визначено математичний апарат (рекурентні співвідношення над $GF(q)$, матриця компаньйона Q_p, тотожність типу Кассіні, система лінійних рівнянь) та окреслено переваги над класичною поліноміальною інтерполяцією: структурна гнучкість через єдиний параметр p, природне узагальнення на зважені схеми, наявність вбудованих алгебраїчних інваріантів. Подальші дослідження спрямовані на формалізацію умов стійкості, розроблення конкретних алгоритмів розподілу та відновлення, а також їх практичну реалізацію та порівняльне тестування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Shamir, A. How to share a secret. *Communications of the ACM.* 1979. Vol. 22, no. 11. P. 612–613. DOI: https://doi.org/10.1145/359168.359176.
2. Beimel A. Secret-sharing schemes: a survey. *Coding and Cryptology. IWCC 2011 : Lecture Notes in Computer Science.* Berlin ; Heidelberg : Springer, 2011, Vol. 6639. P. 11–46. DOI: https://doi.org/10.1007/978-3-642-20901-7_2
3. Stakhov, A. P. Fibonacci matrices, a generalization of the "Cassini formula", and a new coding theory. *Chaos, Solitons & Fractals.* 2006. Vol. 30, no. 1. P. 56–66. DOI: https://doi.org/10.1016/j.chaos.2005.12.054.
4. Blakley, G. R. Safeguarding cryptographic keys. *Proceedings of the AFIPS National Computer Conference.* New York : AFIPS Press, 1979. Vol. 48. P. 313–317.
5. Weighted threshold secret sharing schemes / P. Morillo, C. Padró, G. Sáez, J. L. Villar. *Information Processing Letters.* 1999. Vol. 70, no. 5. P. 211–216. DOI: https://doi.org/10.1016/S0020-0190(99)00068-4.

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