УДК 512.623.3

СИНТЕЗ І АНАЛІЗ УЗАГАЛЬНЕНИХ ПРИМІТИВНИХ ПОЛІНОМІВ

А. Я. Білецький, д-р техн. наук, проф.

Національний авіаційний університет

abelanu@ukr.net

Наведено алгоритм синтезу матриць Галуа і Фібоначчі над узагальненими примітивними поліномами та розглянуто прикладні аспекти їх застосування.

Ключові слова: узагальнені примітивні поліноми, поля Галуа, матриці Галуа і Фібоначчі.

Shown algorithm for synthesis of Galois and Fibonacci matrices over general primitive polynomials and applied aspects considered for their application.

Keywords: generalized primitive polynomials, Galois fields, Galois and Fibonacci matrix.

Вступ та постановка задачі

У теорії полів Галуа, яка складає основу алгебричної теорії завадостійкого кодування й сучасної теорії криптографії, ключовим є поняття незвідного полінома (НП). Виходячи з того, що в даній статті розглядатимемо змінні й функції, що належать двійковому простору, тобто полю Галуа $GF(2^n)$, наведено визначення НП, яке відповідає даному полю.

Поліном

$$\varphi_n(x) = \sum_{i=0}^{n} \alpha_{n-i} x^{n-i}, \quad \alpha_i \in \{0,1\}, \qquad (1)$$

ступеня n над полем $GF(2^n)$ називається *незвідним*, якщо він не ділиться ні на який поліном меншого ступеня над цим полем [1].

Поліном (1), що записаний в *алгебричній формі*, може бути однозначно представлений бінарним рядком (двійковим вектором) своїх коефіцієнтів (у *бінарній формі*)

$$\varphi_n = \{\alpha_n, \alpha_{n-1}, \ldots, \alpha_i, \ldots, \alpha_0\}, \ \alpha_i \in \{0,1\}.$$

Наприклад, бінарному вектору

$$\varphi_8 = 100011011$$

відповідає алгебрична форма полінома

$$\varphi_8(x) = x^8 + x^4 + x^3 + x + 1. \qquad (2)$$

Одна з головних характеристик НП є показник поліному.

Показник незвідного полінома дорівнює найменшому позитивному числу *e*, при якому НП $\varphi_n(x)$ ділить двочлен $x^e + 1$ без остачі [2].

Фізичний зміст такої характеристики полягає в тому, що він визначає *порядок* мультиплікативної групи, яка утворюється ступенями *примітивного елемента* θ групи по $\bmod \varphi_n$.

Множина незвідних поліномів $\{\varphi_n\}$ містить важливу (наприклад, для криптографічних застосувань) підмножину так званих примітивних поліномів (ПрП).

В алгебрі, теорії чисел і полів Галуа двійковий поліном $\varphi_n(x)$ ступеня n називається *примітивним*, якщо він є незвідним, а найменший показник e, при якому $\varphi_n(x)$ ділить двочлен $\Phi(x) = x^e + 1$ без остачі, визначається виразом $e = 2^n - 1$ [2].

У теорії поліномів стверджується, що всі примітивні поліноми є незвідними, тоді як зовсім не обов'язково, щоб кожний незвідний полином мав властивості примітивності.

Мета дослідження — доведення того, що, по-перше, будь-який НП φ_n ступеня n відповідним підбором утворювальних елементів ω приводиться до примітивного поліному $\varphi_n^{(\omega)}$; і, по-друге, число елементів ω, які додають довільному незвідному поліному φ_n властивості примітивності, є величина стала, зумовлена лише значенням n. Крім того, наводиться досить простий алгоритм синтезу двійкових утворюючих матриць n-го порядку, за допомогою яких формується m-послідовність ступенів ω по $\bmod \varphi_n$.

Основні співвідношення

Визначення примітивного полінома $\varphi_n(x)$, що наведене раніше, можна відобразити такими еквівалентними співвідношеннями:

$$\varphi_n(x) \mid x^e + 1; \qquad (3)$$

$$x^e \equiv 1 \,(\bmod \varphi_n(x)), \qquad (4)$$

за умови, що

$$\min e = 2^n - 1. \qquad (5)$$

Узагальнення поняття примітивного полінома, яке пропонується, зводиться до такого. Замінимо основу x одночлена x^e у формулах (3) і (4) довільним поліномом $\omega_m(x)$ ступеня m таким, що $1 \le m < n$. Тобто подамо дані вирази таким чином:

$$\varphi_n(x) \,|\, [\omega_m(x)]^e + 1; \qquad (6)$$

$$[\omega_m(x)]^e \equiv 1 \bmod \varphi_n(x), \qquad (7)$$

за дотримання умови (5).

Назвемо $\omega_m(x)$ *утворювальним елементом* (УЕ) примітивного полінома $\varphi_n(x)$.

Подальші пояснення спростяться, якщо від алгебричних форм поліномів $\varphi_n(x)$ і $\omega_m(x)$ перейти до їхніх бінарних форм.

У класичному варіанті (3) або (4) одночлен x^e можна записати у вигляді числового (бінарного) еквівалента $(10)^e$, оскільки x є поліном першого ступеня з мінімальною вагою, тобто $x = 10$.

Водночас УЕ ω_m може бути відмінним від полінома $x = 10$ і набувати значень 11, 110, 101 та ін.

Незвідний поліном (2) обраний розроблювачами криптографічного алгоритму *Rijndael* як базовий для побудови примітива нелінійної підстановки в шифрі AES [3].

Відносно НП (2) можна зауважити. По-перше, цей поліном не є примітивним; його показник дорівнює 51. По-друге, як справедливо відзначається в праці [4], поліном $\varphi_8(x)$, заданий співвідношенням (2), є першим НП восьмого ступеня, що згадується в більшості довідників, тобто його вибір досить довільний.

Як відомо, *S*-блоки подібні до тих, що обрані в шифрі AES, можуть бути реалізовані тільки на примітивних поліномах. Проблему непримітивності полінома автори алгоритму *Rijndael* вирішили простою заміною одночлена x двочленом $x+1$. Така заміна привела до того, що вихідний непримітивний поліном показника 51 набув властивість примітивності з показником 255.

Аналіз незвідних і примітивних поліномів підтверджує можливість і доцільність переходу від класичного подання примітивного полінома у вигляді співвідношень (3) або (4) до узагальненого подання виразами (6) або (7) відповідно.

Утворювальні елементи примітивних поліномів

Введемо ряд додаткових позначень. Нехай $L_n = 2^n - 1$ є загальне число *n*-бітних векторів, за винятком нульового вектора; $L_n^{(\omega)}$ — число утворювальних елементів ω, що додають НП φ_n властивість примітивності.

Число $L_n^{(\omega)}$ визначається функцією Ейлера φ аргументу L_n, тобто

$$L_n^{(\omega)} = \varphi(L_n). \qquad (8)$$

Справді, у будь-який комутативній групі порядку L_n число її елементів, взаємно простих з L_n (а саме такі елементи можуть бути обрані як утворювальні) становить величину, що є функцією Ейлера аргументу L_n. Тим самим приходимо до виразу (8).

Незвідний поліном φ_n, який стає примітивним, якщо утворюючим елементом мультиплікативної групи обраний деякий елемент ω, будемо називати *примітивним* над ω поліномом і позначати $\varphi_n^{(\omega)}$.

Матричні форми *m*-послідовностей

Мультиплікативну групу $\langle\omega\rangle$ можна сформувати послідовним піднесенням до ступеня утворювального елемента ω з подальшим приведенням ступеня УЕ до залишку за модулем $\varphi_n^{(\omega)}$.

Отже, *m*-послідовність $\langle\omega\rangle$ можна одержати на основі найпростіших модулярних матричних обчислень.

Нехай $G_n^{(\omega)}$ позначає матрицю, яка формує $\langle\omega\rangle$. Уведемо *n*-бітний вектор V_k, що зумовлений співвідношенням

$$V_k = \omega^k \bmod \varphi_n^{(\omega)}.$$

Необхідно знайти таку матрицю $G_n^{(\omega)}$, за допомогою якої можна було б реалізувати перетворення

$$V_{k+1} = V_k \otimes G_n^{(\omega)}, \quad k = \overline{0, L_n}, \quad V_0 = V_{L_n} = 1, \qquad (9)$$

і, тим самим одержати *m*-послідовність *n*-бітних чисел, що формуються ступенями УЕ ω за модулем ПрП $\varphi_n^{(\omega)}$.

Побудуємо матриці перетворення $G_n^{(\omega)}$ на прикладі примітивного над УЕ $\omega = 111$ поліному $\varphi_8 = 100101101$.

Процес синтезу матриці $G_n^{(\omega)}$ розбивається на два етапи.

На першому етапі складається так звана *стартова* таблиця, що містить *стартову* матрицю *n*-го порядку M. Для прикладу, що розглядається, $n = 8$, стартова матриця виділена затіненням у табл. 1 однозначно обумовлена її УЕ ω

Вектор V_1, що збігається з утворюючим поліномом ω, породжує діагональне заповнення елементів стартової матриці M.

Передбачається, що в незаповнених елементах матриці M перебувають нулі.

Для простоти сприйняття ці комірки залишені порожніми.

Таблиця 1

Стартова таблиця

φ →	1	0	0	1	0	1	1	0	1
	Позначки								
		8	7	6	5	4	3	2	1
8									
7									
6		1	1	1					
5			1	1	1				
4				1	1	1			
3					1	1	1		
2						1	1	1	
1	V_1						1	1	1

Перевіримо коректність запропонованого алгоритму побудови стартової матриці.

Для векторів V_k, у яких номер старшого розряду, що дорівнює 1, не перевищує $n-m$, де m-ступінь УЕ, ми можна двома способами обчислити вектор V_{k+1}.

При першому способі (назвемо його *аналітичним*) вектор V_{k+1} визначається співвідношенням

$$V_{k+1} = (V_k \otimes \omega) \bmod \varphi_n . \qquad (10)$$

Нехай $V_k = 110101$. Для обраних значень параметрів перетворення, а саме, $n = 8$, $\omega = 111$ і $\varphi_8 = 100101101$, за формулою (10) одержимо

$$V_{k+1} = 10001011 . \qquad (11)$$

Другий спосіб обчислення того ж самого вектора, який позначимо V^*_{k+1} (назвемо його *графічним*), зводиться до порозрядного додавання по $\bmod 2$ елементів тих рядків стартової матриці, номери яких збігаються з номерами розрядів вектора V_k, що містять 1.

Позначимо зірочками рядки стартової матриці, що відповідають вектору $V_k = 110101$, як це видно з табл. 2.

Виконавши порозрядне додавання елементів рядків, які виділені в табл. 2, одержимо кодову комбінацію 10001011, що збігається з раніше аналітично отриманим результатом (11).

Отже, можна переконатися в тому, що діагональне розміщення елементів стартової матриці, яке наведене в табл. 1, дає можливість правильно обчислити V_{k+1} для всіх вхідних векторів V_k, у яких номер старшого розряду, що містить 1, не перевищує 6.

Таблиця 2

Графічний спосіб обчислення добутку (10)

φ →	1	0	0	1	0	1	1	0	1
	Позначки								
		8	7	6	5	4	3	2	1
8									
7									
6	*	1	1	1					
5	*		1	1	1				
4				1	1	1			
3	*				1	1	1		
2						1	1	1	
1	*						1	1	1

У загальному випадку для ПрП ступеня n й УЕ ступеня m нижні $n-m$ рядки матриці M збігаються з відповідними рядками стартової матриці, а m — верхні рядки матриці, що залишилися, підлягають уточненню.

На другому етапі синтезу матриці $G_n^{(\omega)}$ для прикладу, що розглядається, нам залишається обчислити значення елементів у сьомому й восьмому рядках табл. 1. Із цією метою позначимо спочатку зірочками нижні сім рядків стартової матриці, сформувавши тим самим вхідний вектор V.

За формулою (10) одержимо вектор V_{k+1}, який дорівнює 01010000. Якщо ж порозрядно додати елементи рядків табл. 1 (тобто, скориставшись графічним методом) з першого до сьомого, то приходимо до вектора $V^*_{k+1} = 10111101$. Обчислимо нев'язку векторів V_{k+1} й V^*_{k+1}, яку розмістимо у сьомому рядку табл. 3.

Таблиця 3

До обчислення сьомого рядка матриці *M*

φ →	1	0	0	1	0	1	1	0	1
	Позначки								
		8	7	6	5	4	3	2	1
8									
7	*	1	1	1	0	1	1		1
6	*	1	1	1					
5	*		1	1	1				
4	*			1	1	1			
3	*				1	1	1		
2	*					1	1	1	
1	*						1	1	1

Виконавши аналогічне коригування восьмого рядка табл. 3, отримаємо остаточну форму матриці перетворення

$$G_n^{(\omega)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}. \qquad (12)$$

Легко переконатися в тому, що матриця (12) породжує послідовність восьмибітних кодів, що збігається з послідовністю, яка утворена ступенями $\omega = 111$ за модулем $\varphi_8 = 100101101$.

На цій підставі матрицю $G_n^{(\omega)}$ (і їй подібні) будемо називати *утворювальною* матрицею.

Матриці $G_n^{(\omega)}$ відповідає так звана *сполучена матриця Фібоначчі* $F_n^{(\omega)}$, яка пов'язана з $G_n^{(\omega)}$ оператором правобічного транспонування (тобто транспонування матриці щодо допоміжної діагоналі), що позначимо $\perp$. Маємо

$$G \xleftrightarrow{\perp} F, \qquad \text{инакше} \quad F = G^{\perp}, \quad \text{або} \quad G = F^{\perp}.$$

Матриця $F_n^{(\omega)}$, як і матриця $G_n^{(\omega)}$, також надає можливість формувати m-послідовність ступенів ω по $\bmod \varphi_n$. Алгоритм синтезу утворювальних матриць $G_n^{(\omega)}$ і $F_n^{(\omega)}$ досить простий і може бути застосований для довільних параметрів n, ω і φ_n.

Відзначимо області, у яких можуть бути використані матриці $G_n^{(\omega)}$ й $F_n^{(\omega)}$.

Це генератори псевдовипадкових послідовностей, криптографічні примітиви нелінійної підстановки (S-блоки) та ін.

Висновки

У праці введено поняття *узагальненого примітивного полінома*, що розширює класичний термін примітивного полінома.

Показано, по-перше, *всі* незвідні поліноми, у тому числі й ті, які в класичному розумінні не є примітивними, здобувають властивість примітивності відповідним вибором утворюючого елемента. По-друге, число утворювальних елементів, за допомогою яких *всі* незвідні поліноми ступеня n стають примітивними, визначається функцією Ейлера аргументу L_n. Крім того, запропонований досить простий алгоритм синтезу утворюючих матриць, за допомогою яких безпосередньо формуються мультиплікативні групи порядку L_n за обраними параметрами φ_n^* і ω.

ЛІТЕРАТУРА

1. *Лидл Р.* Конечные поля; пер. с англ. / Р. Лидл, Г. Нидеррайтер. — Т. 1. — М. : Мир, 1988. — 432 с.

2. *Иванов М. А.* Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. — М. : КУДИЦ-ОБРАЗ, 2001. — 368 с.

3. *Електронний* ресурс. Режим доступу: csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

4. З*ензин О. С.* Стандарт криптографической защиты AES. Конечные поля / О. С. Зензин, М. А. Иванов // под ред. М. А. Иванова. — М. : КУДИЦ-ОБРАЗ, 2002. — 176 с.

5. *Иванов М. А.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. — М. : КУДИЦ-ОБРАЗ, 2003. — 240 с.

Стаття надійшла до редакції 26.10.2011.