

## К ВОПРОСУ О ПОЛУЧЕНИИ НЕРАЗЛОЖИМЫХ ПОЛИНОМОВ НА ПОЛЯХ ГАЛУА ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В статье рассматривается проблема получения неразложимых полиномов на полях Галуа для использования в системах криптографической защиты информации, генерации псевдослучайных чисел и последовательностей, сжатия данных, а также исправления ошибок при их передаче. На основе теоретических и экспериментальных исследований выявлены новые свойства полиномов на конечных полях. Предложен подход к ускорению поиска неразложимых полиномов за счет оптимизации процедуры их селекции и тестирования на основе выявленных свойств.

The article is dedicated to the problem of generating the indecomposable polynomials over Galois fields used in cryptographic information security, generation of pseudo random numbers and sequences, data compression and error-correction during data transmission. New properties of polynomials over finite fields was discovered after theoretical and experimental research. The approach to increase speed of searching indecomposable polynomials is proposed and relies on the optimization of the procedure of their selection and testing using discovered features.

### Введение

Теория конечных полей, начатая работами французского математика Э.Галуа в начале 19-века получила широкое практическое применение только в конце следующего, 20-го века с развитием компьютерных и информационных технологий. В настоящее время теоретические положения полей Галуа лежат в основе большинства поточных шифров [1], широко используемых для защиты данных в мобильной связи, компьютерных системах и сетях. Преобразования на полях Галуа используются и в криптографических средствах блочного шифрования, в том числе и алгоритме Rijndael, ставшим победителем всемирного конкурса блочных шифров AES [2].

Кроме систем защиты информации теоретические положения полей Галуа с 50-х широко используются в компьютерных технологиях для генерации псевдослучайных последовательностей и чисел [3]. Значительная часть широко используемых на практике технологий обнаружения и исправления ошибок передачи данных базируется на математических принципах конечных полей. К их числу относятся циклические коды, коды Рида-Соломона, коды Файра, а также часть взвешенных контрольных сумм [4]. Кроме того, поля Галуа активно используются в системах кодирования результатов измерений и архивировании данных. Новый мощный импульс развитию теории полей Галуа стало их

применение в современных системах мобильной связи [5].

Практически во всех перечисленных применениях полей Галуа решается задача выбора образующего полинома  $P(x)$ , который представляет собой неразложимый полином (неприводимый многочлен) то есть такой, который не может быть представлен в виде произведения двух других полиномов. В алгебре конечных полей образующему полиному поля Галуа можно однозначно сопоставить двоичное число  $P$ , которое является простым в этой алгебре, то есть не может быть представлено в виде произведения без переносов других чисел. Задача получения простого в алгебре конечных полей числа  $P$  является достаточно сложной и к настоящему времени не существует алгоритмов ее решения, которые бы не предполагали определенного перебора. Для большей части перечисленных выше применений полей Галуа, кроме приложений связанных с защитой информации, образующий полином  $P(x)$  выбирается один раз из специальных таблиц [5].

Для применений полей Галуа, связанных с защитой информации, необходимо решать задачу генерации неразложимых полиномов. С ростом степени полинома (разрядности простого в алгебре конечных полей числа  $P$ ) сложность задачи его генерации растет экспоненциально [6], поэтому необходимым представляется разработка методов, направленных на

уменьшение вычислительной сложности получения неразложимых полиномов полей Галуа.

Таким образом, задача совершенствования технологии получения неразложимых многочленов, необходимых для использования в качестве образующих полиномов полей Галуа является актуальной для широкого круга практически важных задач современных информационных и компьютерных технологий.

### **Анализ существующих технологий получения неразложимых многочленов**

Задача получения неразложимых многочленов в определенном плане является схожей с задачей получения простых чисел в обычной арифметике [6].

Для обеих задач к настоящему времени не существует метода или алгоритма решения без перебора. Возникновение в 1978 г. криптографии с открытым числом и ее широкое использование стимулировали развитие технология получения простых чисел в обычной арифметике.

К настоящему времени методика получения как простых чисел, так и неразложимых полиномов, в общем виде схожа и состоит в следующем: генерируется случайное число и над ним выполняется последовательность тестов, каждый из которых подтверждает или опровергает гипотезу о том, что число простое. Чем более эффективны тесты и чем большее число их проводится – тем больше вероятность того, что тестируемое число является простым. Даже для чисел, которые успешно прошли все тесты существует низкая вероятность того, что они могут быть разложены на множители. В этой связи для таких чисел принят термин “промышленно простые числа” (ППЧ) [6], чтобы отличить их от истинно простых чисел.

Из сказанного явствует, что эффективность технологий получения ППЧ определяется эффективностью тестов, которая характеризуется:

- вероятностью того, что после прохождения теста число окажется не простым;
- временем выполнения теста.

Оптимизация тестирования состоит в выборе такого набора тестов  $T_1, T_2, \dots, T_k$ , которые позволяют решить одну из двух задач оптимизации тестирования:

1) достижение минимальной вероятности того, что после прохождения тестов  $T_1, T_2, \dots, T_k$ , тестируемое число окажется не простым при

заданном ограничении  $G$  на суммарное время тестирования  $t(T_1) + t(T_2) + \dots + t(T_k) \leq G$ , где  $t(T_j)$  – время выполнения  $j$ -го теста ( $j \in \{1, \dots, k\}$ );

2) достижение минимального времени тестирования  $\min(t(T_1) + t(T_2) + \dots + t(T_k))$  для достижения заданной вероятности  $q$  того, что после прохождения выбранного набора тестов  $T_1, T_2, \dots, T_k$ , тестируемое число окажется не простым.

Для тестирования простых в арифметическом смысле чисел разработано ряд тестов, наиболее известными из которых являются тест Соловея-Штрассера, тест Лемана, тест Рабина-Миллера [6].

Вполне очевидным, что для повышения эффективности генерации неразложимых полиномов для использования в качестве образующих полей Галуа необходимо разработать эффективные независимые тесты на неразложимость и определить характеристики их эффективности. Для этого, теоретически и экспериментально надо изучить свойства неразложимых полиномов.

Целью исследований является теоретическое и экспериментальное исследование свойств неразложимых полиномов и разработка на этой основе эффективной системы тестов для проверки возможности разложения многочлена на множители.

### **Исследование свойств неразложимых полиномов**

Для создания эффективной системы тестов на неразложимость необходимо с теоретических позиций исследовать специфические свойства, использование которых позволяет сократить время тестирования.

Базовыми операциями над многочленами являются: сложение многочленов, соответствующее логической операции XOR, обозначаемое далее символом  $\oplus$ , умножение многочленов, соответствующее операции умножения двоичных чисел без переносов, обозначаемое далее символом  $\otimes$ , операция

Далее в тексте статьи символом операцию «/» будет считаться операцией деления без переносов. Ниже представлено доказательства ряда лемм и теорем, которые могут быть использованы для эффективного тестирования многочленов на предмет их неразложимости.

**Лемма 1.** Если многочлен  $P(a) = a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \dots + a_1 \cdot x + a_0$  делится без остатка на много-

член  $P(b)=b_{m-1}\cdot x^{m-1}+b_{m-2}\cdot x^{m-2}+\dots+b_1\cdot x+b_0$ , то на этот многочлен делится также многочлен  $P(c)=a_{n-1}\cdot x^{n+k-1}+a_{n-2}\cdot x^{n+k-2}+\dots+a_1\cdot x^{k+1}+a_0\cdot x^k$ .

**Доказательство:** Согласно правилам выполнения операции деления многочленов [2] многочлен-делитель  $P(b)$  степени  $m-1$ , умноженный на  $x^{n+k-m}$  суммируется с  $P(c)$  с образованием остатка  $P_1=P(c)+P(b)\cdot x^{n+k-m}$ . Аналогично, при делении многочлена  $P(a)$  на  $P(b)$  на первом шаге выполняется суммирование  $P(a)$  с произведением  $P(b)\cdot x^{n-m}$  с образованием остатка  $P'_1=P(a)+P(b)\cdot x^{n-m}$ . В силу того, что  $P(c)=P(a)\cdot x^k$ , то  $P_1=P'_1\cdot x^k$ . Аналогичные рассуждения полностью справедливы и для вторых остатков:  $P_2=P'_2\cdot x^k$ , и для третьих, четвертых и всех остальных остатков, включая последний  $l$ -тый:  $P_l=P'_l\cdot x^k$ . Так как последний остаток  $P'_l$ , возникающий в процессе деления многочлена  $P(a)$  на многочлен  $P(b)$  равен нулю, то равен нулю и остаток  $P_l$  от деления многочлена  $P(c)$  на многочлен  $P(b)$ , что и требовалось доказать.

**Теорема 2.** Если многочлен  $P(a)=a_{n-1}\cdot x^{n-1}+a_{n-2}\cdot x^{n-2}+\dots+a_1\cdot x+a_0$  и многочлен  $P(b)=b_{k-1}\cdot x^{k-1}+b_{k-2}\cdot x^{k-2}+\dots+b_1\cdot x+b_0$  делятся на многочлен  $P(c)=c_{m-1}\cdot x^{m-1}+c_{m-2}\cdot x^{m-2}+\dots+c_1\cdot x+c_0$ , то многочлен  $P(d)=P(a)\cdot x^{k+q}+P(b)=a_{n-1}\cdot x^{n+q+k-1}+\dots+a_1\cdot x^{q+k+1}+a_0\cdot x^{q+k}+b_{k-1}\cdot x^{k-1}+b_{k-2}\cdot x^{k-2}+\dots+b_1\cdot x+b_0$  также делится без остатка на полином  $P(c)$ .

**Доказательство:** многочлен  $P(d)$  можно записать в виде  $P(d)=P(a)\cdot x^{k+q}+P(b)$ . Выше леммой 1 было доказано, что, если  $P(a)$  делится без остатка на  $P(c)$ , то и  $P(a)\cdot x^{k+q}$  также без остатка делится на  $P(c)$ . По условиям теоремы и  $P(b)$  делится без остатка на  $P(c)$ . Поскольку операция полиномиального деления обладает свойством дистрибутивности [2], то остаток от деления полинома  $P(d)$  на полином  $P(c)$  равен сумме остатков от деления полиномов  $P(a)\cdot x^{k+q}$  и  $P(b)$ , то есть равен нулю, что и требовалось доказать.

**Лемма 2.** Если многочлен  $P_1$  является двучленом, то есть может быть представлен в виде  $P_1=x^n+x^k$ , то он делится без остатка на многочлен  $P_3=x+1$ .

**Доказательство:** на основании леммы 1 можно утверждать, что многочлен  $P_1=x^n+x^k$  делится без остатка на многочлен  $P_3$ , если таким свойством обладает многочлен  $P_2=x^{n-k}+1$ . В процессе полиномиального деления многочлена  $P_2$  последовательно образуются остатки:  $x^{n-k-l}+1, x^{n-k-2}+1, x^{n-k-3}+1, \dots, x+1$ . Поскольку последний из остатков совпадает с  $P_3$ , то  $P_2$  делится

без остатка на  $P_3$ , а, значит, согласно лемме 1 и многочлен  $P_1$  делится без остатка на  $P_3$ , что и требовалось доказать.

**Теорема 3.** Если многочлен  $P_e$  содержит четное число членов, то он делится без остатка на многочлен  $P_3=x+1$ .

**Доказательство.** Поскольку полином  $P_e$  содержит четное число  $h$  членов, то он может быть представлен в виде суммы  $h/2$  многочленов, каждый из которых содержит в точности два члена. Леммой 2 доказано, что каждый из этих двучленов делится без остатка на многочлен  $P_3=x+1$ . Согласно свойству дистрибутивности [2] остаток от деления многочлена  $P_e$  на  $P_3$  равен сумме остатков от деления двучленов составляющих  $P_e$  на  $P_3$ , то есть нулю, что и требовалось доказать.

Симметричным по отношению к многочлену  $P(a)=a_{n-1}\cdot x^{n-1}+a_{n-2}\cdot x^{n-2}+\dots+a_1\cdot x+a_0$  является многочлен  $P(\hat{a})=a_0\cdot x^{n-1}+a_1\cdot x^{n-2}+\dots+a_{n-2}\cdot x+a_{n-1}$ . Симметричными называются двоичные числа  $a$  и  $\hat{a}$ , соответствующие приведенным многочленам. Например, если  $a=1101_2$ , то  $\hat{a}=1011_2$ .

**Теорема 4.** Если  $a\otimes b=c$ , то  $\hat{a}\otimes\hat{b}=\hat{c}$ . Произведение симметрических двух чисел является собой симметричное число к произведению этих чисел.

Например, если  $a=1101_2, b=5=0101_2$ , то  $\hat{a}=1011_2=11_{10}$ , а  $\hat{b}=1010_2=10_2$ . Произведение без переносов  $a\otimes b=13\otimes 5=c=57_{10}=0111001_2$ , а произведение симметрических  $\hat{a}\otimes\hat{b}=11\otimes 10=78_{10}=1001110=\hat{c}$ .

**Доказательство:**

Пусть  $a$  –  $n$ -разрядное двоичное число  $a=2^{n-1}\cdot a_{n-1}+2^{n-2}\cdot a_{n-2}+\dots+2\cdot a_1+a_0$ , причем для всех  $q\in\{0,\dots,n-1\}$ :  $a_q\in\{0,1\}$ , соответственно, симметрическое числу  $a$  число  $\hat{a}$  можно представить в следующем виде:  $\hat{a}=2^{n-1}\cdot a_0+2^{n-2}\cdot a_1+\dots+2\cdot a_{n-2}+a_{n-1}$ .

Аналогически, если  $b$  –  $m$ -разрядное число  $b=2^{m-1}\cdot b_{m-1}+2^{m-2}\cdot b_{m-2}+\dots+2\cdot b_1+b_0, g\in\{0,\dots,m-1\}$ :  $b_g\in\{0,1\}$ , то симметрическое ему число  $\hat{b}=2^{m-1}\cdot b_0+2^{m-2}\cdot b_1+\dots+2\cdot b_{m-2}+b_{m-1}$ . Тогда произведение без переносов этих чисел является собой число  $c$ , разрядностью  $l=n+m-1$ :  $c=2^{l-1}\cdot c_{l-1}+2^{l-2}\cdot c_{l-2}+\dots+2\cdot c_1+c_0$ , причем,  $h\in\{0,1,\dots,l\}$ :  $c_h\in\{0,1\}$ . Соответственно симметричное  $\hat{c}=2^{l-1}\cdot c_0+2^{l-2}\cdot c_1+\dots+2\cdot c_{l-2}+c_{l-1}$ .

Если  $d = 2^{l-1} \cdot d_{l-1} + 2^{l-2} \cdot d_{l-2} + \dots + 2 \cdot d_1 + d_0$  –  $l$ -разрядное произведение без переносов  $\hat{a} \otimes \hat{b}$ , то для того, что бы доказать теорему не обязательно показать, что для каждого  $h \in \{0, 1, \dots, l\}$ :  $c_h = d_{l-h-1}$ .

Как биномиальный коэффициент при  $2^h$ ,  $c_u$  являет собой сумму по модулю два произведений  $a_i \cdot b_j$  двоичных разрядов  $a$  и  $b$ , для которых сумма индексов равняется  $h$ :  $i+j=h$ :

$$c_h = \bigoplus_{i+j=h} a_i \cdot b_j \quad (1)$$

Выражение (1) может быть преобразовано следующим образом:

$$\begin{aligned} c_h &= \bigoplus_{i+j=h} a_i \cdot b_j = \bigoplus_{i+j=h} \hat{a}_{n-i-1} \cdot \hat{b}_{m-j-1} = \\ &= \bigoplus_{r+v=m+n-(i+j)-2} \hat{a}_r \cdot \hat{b}_v = \bigoplus_{r+v=l-h-1} \hat{a}_r \cdot \hat{b}_v = d_{l-h-1} \end{aligned}$$

Таким образом, доказано, что  $c = \hat{d}$ .

*Следствие:*

Если  $c \bmod a = b$ , то  $\hat{c} \bmod \hat{a} = \hat{b}$ .

**Теорема 5.** Если  $c$  – непростое, то и  $\hat{c}$  – тоже непростое.

*Доказательство:* Если  $c$  – непростое, то его можно представить в виде произведения:  $c = a \otimes b$ . Тогда, согласно теореме 4 существуют  $\hat{a}$  и  $\hat{b}$  такие, что  $\hat{a} \otimes \hat{b} = \hat{c}$ , таким образом  $\hat{c}$  можно представить в виде произведения двух чисел. А из этого следует, что  $\hat{c}$  непростое.

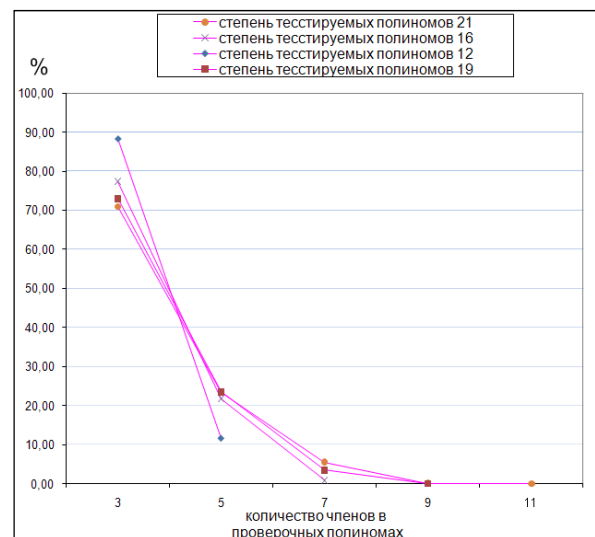
**Теорема 6.** Если  $c$  – простое, то и  $\hat{c}$  – также простое.

*Доказательство:* Если  $\hat{c}$  – непростое, то его можно представить в виде произведения  $\hat{c} = a \oplus b$ . Тогда, в соответствии с теоремой 4 существуют  $\hat{a}$  и  $\hat{b}$  такие, что  $\hat{a} \otimes \hat{b} = c$ , таким образом  $c$  также можно представить в виде произведения двух чисел. Это противоречит условию теоремы, согласно которому  $c$  – простое. Таким образом, доказано, что если  $c$  – простое, то и  $\hat{c}$  также простое.

Кроме теоретических, были проведены широкие экспериментальные исследования, направленные на выявления свойств неразложимых многочленов, которые могли бы быть использованы для построения эффективной системы тестов.

Исследовались свойства проверочных многочленов, которые могли бы быть исполь-

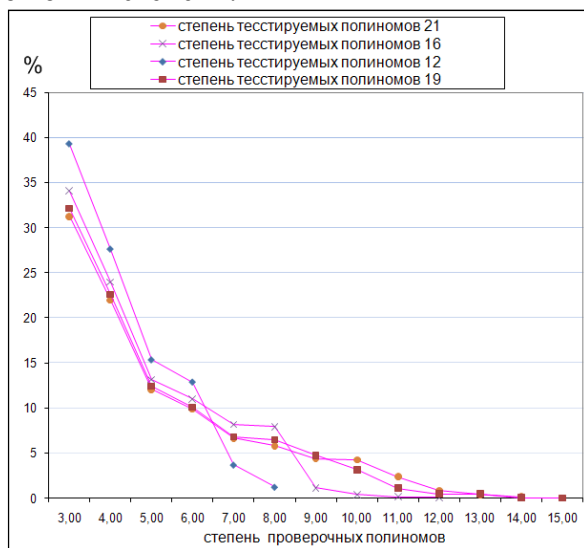
зованы в качестве тестирующих делителей исследуемого многочлена. Проверочные многочлены выбирались только с нечетным количеством членов, и также, обязательным условием было наличие в них члена нулевой степени. В начале эксперимента количество членов проверочных полиномов равнялось трем. При проведении проверок степень проверочных полиномов постепенно повышалась до  $n-2$  (где  $n$  – степень тестируемых полиномов). Если были выполнены проверки всех возможных комбинаций для текущего количества членов в проверочных полиномах, то выполнялось увеличение количества членов в проверочных полиномах на два и снова выполнялись проверки с новым количеством членов и с постепенным повышением степени проверочных полиномов. Максимальное количество членов в проверочных полиномах равняется  $n-2$ . В случае нахождения полинома результат редукции с тестируемым полиномом, для которого равнялся нулю, тестирование текущего тестируемого полинома прекращалось и констатировался тот факт, что тестируемый полином не принадлежит к множеству неразложимых многочленов. В ходе эксперимента выполнялся подсчет характеристик таких проверочных полиномов, которые указывали на непринадлежность текущего тестируемого полинома к множеству неразложимых, а именно запоминалась их степень и количество членов, поскольку именно эти параметры определяют вычислительную сложность тестирования. Результаты исследований показали, что вероятность отнесения проверяемого многочлена к разряду разложимых при использовании проверочных полиномов зависит от количества их членов.



**Рис.1.** Зависимость количества проверочных полиномов от количества членов в них

На рис.1 показано, что наибольшее количество проверочных полиномов имело три члена, затем их количество постепенно спадает к нулю относительно количества их членов. Поскольку максимальное значение членов в полиноме меньше чем  $n/2$ , то при проведении эксперимента имела место большая избыточность проверок по количеству членов в проверочных полиномах.

Анализ экспериментальных исследований также показал избыточность проверок по степени проверочных полиномов. На рис.2 показана зависимость количества проверочных полиномов от их степени.



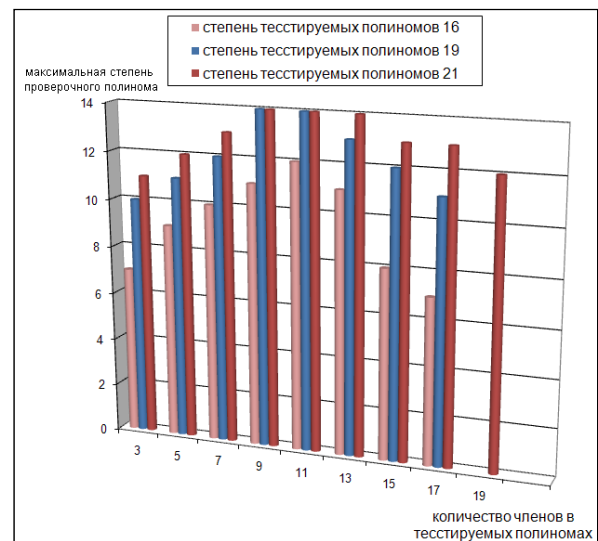
**Рис.2. Зависимость количества проверочных полиномов от их степени**

Кроме того, в результате проведенных экспериментальных исследований был установлен тот факт, что сложность проверок зависит от количества членов в тестируемом полиноме, а именно количество членов и степень проверочных полиномов возрастает с приближением количества членов в тестируемых полиномах к  $n/2$ , а на промежутке от  $n/2$  до  $n$  постепенно спадает. Результаты этих исследований представлены на рис. 3 и рис.4.

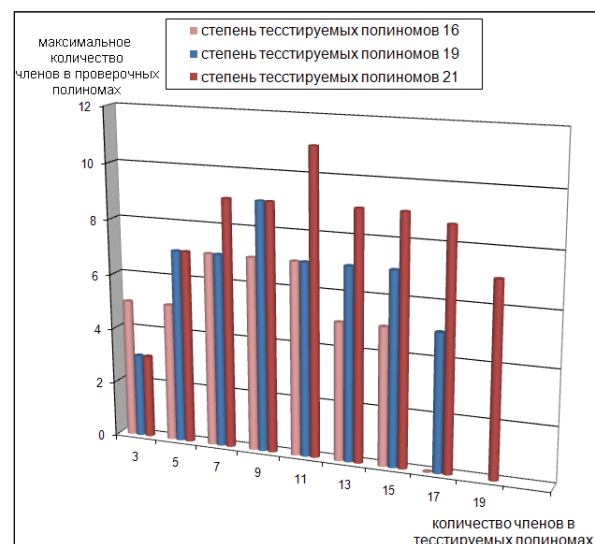
Из рисунка 3 видно, что при выполнении полного перебора проверочных полиномов значение максимальной степени проверочных полиномов зависит от количества членов в тестируемом полиноме. Это значит что при выборе максимального значения степени проверочных полиномов, надо учитывать количество членов в тестируемом полиноме.

Из рисунка 4 видно, что при выполнении проверок значение максимального количества

членов в проверочных полиномах зависят от количества членов в тестируемом полиноме.



**Рис.3. Зависимость максимального значения степени проверочных полиномов от количества членов в тестируемых полиномах**



**Рис.4. Зависимость максимального количества членов в проверочных полиномах от количества членов в тестируемых полиномах**

Из этого следует, что при формировании тестов надо выбирать проверочные полиномы начиная с меньших степеней, причем наиболее эффективными из них являются полиномы, число членов которых близко к половине от их степени.

### Организация выбора оптимального плана тестирования

Проведенные теоретические и экспериментальные исследования свойств неразложи-

мых многочленов и проверочных полиномов позволяют сформулировать порядок организации тестирования, позволяющий уменьшить время тестирования и вероятность того, что многочлен, прошедший тесты окажется разложимым.

Критерии к нижнему уровню вероятности ошибки тестирования определяются спецификой использования многочлена. Как, если многочлен используется для построения генератора псевдослучайных последовательностей, то ошибка тестирования будет иметь следствием разделение одного цикла повторения на  $k$  локальных, период повторения которых соответственно в  $k$  раз меньше.

При использовании формируемого многочлена в криптографических системах цифровой подписи, ошибка теста не является критической – она сказывается только на этапе нахождения мультипликативной инверсии [6]: если многочлен не является простым, то операция нахождения мультипликативной инверсии для небольшого числа чисел не может быть выполнена. Поскольку эта операция осуществляется лицом, подписывающим документ, то необходимо оперативно прервать процесс подписи и выбрать другой многочлен.

При организации процесса тестирования многочлена степени  $n$  на предмет его неразложимости рекомендуется выполнять следующее:

1) Выбрать случайное нечетное число, содержащее нечетное число единиц, близкое к  $n/4$ . Соответствующий этому числу полином использовать в качестве тестируемого.

2) Сформировать список проверочных многочленов, причем их порядок должен соответствовать увеличению их степени, причем степень проверочных полиномов должна не превышать  $n/3$  плюс количество членов в тестируемом полиноме. Согласно выше представленным исследованиям количество членов проверочных полиномов не должно превышать  $n/4$  плюс количество членов в тестируемом полиноме.

3) С процессе тестирования выполняется деление тестируемого многочлена на проверочный. Каждый тест целесообразно выполнять два раза: по отношению к тестируемому многочлену и по отношению к многочлену, симметричному к тестируемому.

### Выводы

В результате проведенных исследований, направленных на повышение эффективности генерации неразложимых полиномов полей Галуа для систем защиты информации определены стратегии тестирования. Теоретически и экспериментально исследованы специфические свойства неразложимых многочленов, использование которых позволяет существенно сократить время тестирования и повысить его достоверность. На основе изучения свойств проверочных многочленов разработаны рекомендации.

Полученные в работе результаты могут быть использованы для сокращения времени генерации криптографических систем защиты информации с открытым ключом, а также систем точного шифрования данных.

### Список литературы

1. Асосков А.В., Иванов М.А., Мирский А.А., Рузин А.В., Сланин А.В., Тютвин А.Н. Поточные шифры. – М.:Кудиц-образ.-2003.– 334 с.
2. Зенин О.С., Иванов М.А. Стандарт криптографической защиты AES. Конечные поля. – М.:Кудиц-образ.-2002.– 174 с.
3. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ.– 2003 – 260 с.
4. Марковский А.П., Турченко Ю.А., Саидреза Мехмали, Сакун В.М. Использование взвешенных контрольных сумм для исправления “пачек” ошибок передачи данных // Вісник Національного технічного університету України “КПІ”. Інформатика, управління та обчислювальна техніка. К., “БЕК++”, – 2009. – № 51. – С.90-96.
5. Peterson R.L., Ziemer R.E., Borth D.E. Introduction to Spread Spectrum Communication. Prentice Hall.– 1995.– 695 p.
6. Шнайер Б. Прикладная криптография. Протоколы и алгоритмы. М.:Триумф.-2003.-816 с.