УДК 621.374.2

МЕТОДИКА ВЫЧИСЛЕНИЯ ДИСКРЕТНОГО ЛОГАРИФМА

Мурашко И.А., Малашенко В.С.

Гомельский политехнический институт им.П.О.Сухого

Наиболее часто при организации встроенного самотестирования (ВСТ) цифровых устройств на основе СБИС в качестве источника тестов используют генератор псевдослучайных тестовых наборов (ГПТН), выполненный на основе так называемого LFSR (Linear Feedback Shift Register) [1]. Это связано с простотой его использования и небольшими аппаратными затратами на реализацию. Кроме того, его достаточно просто преобразовать в устройство сжатия реакций тестируемой схемы (ТС), как правило это одно- или многоканальный сигнатурный анализатор, что позволяет минимизировать аппаратные затраты на ВСТ [1]. Однако в случаях, когда ТС содержит элементы памяти или при организации ВСТ на основе STUMPS-архитектуры (Self-Test Using a Multiple input signature register and a Parallel Shift register sequence generator) [1], применение LFSR неэффективно из-за наличия структурной зависимости между ГПТН и ТС. Для устранения этого недостатка применяют различные структуры генераторов, такие как модифицированный LFSR [2], генератор на основе клеточных автоматов (КА) [2,3], генератор на основе децимации М-последовательности [4]. Основным достоинством этих генераторов является то, что они позволяют формировать на своих разрядах копии псевдослучайной последовательности, сдвинутые друг относительно друга на достаточно большое количество тактов, что устраняет эффект структурной зависимости.

При анализе и проектировании генераторов данного типа возникает ряд проблем, одной из которых является вычисление дискретных логариф-

мов по модулю порождающего полинома. Так, например, для анализа генератора на КА, функционирование которого определяется примитивным неприводимым полиномом **φ(x)** степени **n**, в общем случае необходимо знать значения дискретных логарифмов по модулю **φ(x)** для всех примитивных полиномов степени меньше, чем **n**. Для анализа генераторов на основе модифицированного LFSR необходимо знать значения всех дискретных логарифмов вида $(X^i \oplus 1)$ для **i=1..n-1, где n=deg φ(x) [2].** В настоящее время для организации ВСТ применяются полиномы, старшая степень которых достигает 100. Соответственно, анализ генераторов на основе таких полиномов представляет собой достаточно трудоемкую задачу.

В работе предлагается методика вычисления дискретных логарифмов по модулю порождающего полинома, основанная на применении свойства децимации М-последовательности [5].

Рассмотрим работу методики. Пусть требуется вычислить значение дискретного логарифма **ψ(x)** по модулю порождающего полинома **φ(x),** то есть необходимо найти такое **k**, для которого истинно соотношение

$$x^k \bmod \varphi(x) = \psi(x) \qquad (1)$$

Для вычисления значения **k** выполним следующие действия.

1) Запишем полином **φ(x)** в следующем виде

$$\varphi(x) = \beta_0 X^0 \oplus \beta_1 X^1 \oplus \beta_2 X^2 \oplus \ldots \oplus \beta_n X^n \qquad (2)$$

и сформируем вектор-строку **M** из коэффициентов при соответствующих степенях X, за исключением X^0

$$M = | \beta_1 \beta_2 \beta_3 \ldots \beta_n |$$

2) По аналогии запишем полином **φ(x)** в следующем виде

$$\psi(x) = \alpha_0 X^0 \oplus \alpha_1 X^1 \oplus \alpha_2 X^2 \oplus \ldots \oplus \alpha_{n-1} X^{n-1} \qquad (3)$$

и сформируем вектор-строку A_0 из коэффициентов полинома

$$A_0 = | \alpha_0 \alpha_1 \alpha_2 \ldots \alpha_{n-1} |$$

3) Сдвигаем вектор A_0 влево до тех пор, пока не получим код вида

$$A_k = | 1\ 0\ 0\ \ldots\ 0 |$$

Количество сдвигов **k**, необходимое для достижения данного кода, является значением искомого дискретного логарифма. Сдвиг осуществляется по следующему правилу

а) Формируется промежуточное значение

$$A_1' = | \alpha_1\alpha_2\alpha_2...\alpha_{n-2}\ 0 |$$

b) Проверяется значение выдвинутого символа α_0.

$$\text{Если } \alpha_0 = 0, \text{ то } A_1 = A_1';$$

$$\text{если } \alpha_0 = 1, \text{ то } A_1 = A_1' \oplus M$$

Рассмотрим работу методики на примере. Пусть требуется вычислить значение **k**, для которого справедливо соотношение (1), если $\varphi(x) = 1 \oplus X^2 \oplus X^5$, $\psi(x) = 1 \oplus X$. Соответственно формируем $M = |0\ 1\ 0\ 0\ 1|$ и $A_0 = |1\ 1\ 0\ 0\ 0|$. Сдвигаем A_0 до тех пор, пока не получим код $|1\ 0\ 0\ 0\ 0|$. Процедура сдвига представлена в таблице. В результате получили, что искомое значение **k=18.** В терминах дискретного логарифма это можно записать

$$\log (X \oplus 1) = 18 \bmod X^5 \oplus X^2 \oplus 1$$

Таблица

Такт	Результат сдвига Начальное состояние - 1 1 0 0 0	Такт	Результат сдвига
1	1 1 0 0 1	10	1 0 1 1 0
2	1 1 0 1 1	11	0 0 1 0 1
3	1 1 1 1 1	12	0 1 0 1 0
4	1 0 1 1 1	13	1 0 1 0 0
5	0 0 1 1 1	14	0 0 0 0 1
6	0 1 1 1 0	15	0 0 0 1 0
7	1 1 1 0 0	16	0 0 1 0 0
8	1 0 0 0 1	17	0 1 0 0 0
9	0 1 0 1 1	18	1 0 0 0 0

На основании данной методики разработана программа вычисления дискретных логарифмов по модулю примитивных неприводимых порождающих полиномов, старшая степень которых не превышает 126.

Литература

1. Savir J.,Bardell P.H. «Built-in Self-Test: Milestones and Challengers», VLSI Design, vol.1, N1, pp.23-44
2. Bardell P.H. «Discrete Logarithms A Parallel Pseudorandom Pattern Generator Analysis Method», Journal of Electronic Testing: Theory and Applications, 1992, N3, pp.17-31
3. Ярмолик В.Н., Мурашко И.А. «Реализация генератора псевдослучайной последовательности на клеточных автоматах», Автоматика и вычислительная техника, 1993, N3, с.9-13
4. Ярмолик В.Н., Мурашко И.А. «Методика проектирования генератора тестовых воздействий, основанного на свойстве децимации М-последовательности», Автоматика и вычислительная техника, 1997, N1, с.13-20
5. Golomb S.W. “Shift Register Sequences” , Holden Day, San-Francisko, 1967