Высокопроизводительная схемотехническая реализация криптографического многоскоростного генератора скалярного произведения

А.Б. Сизоненко
Краснодарский университет МВД России, Краснодар

Введение

Эффективным способом защиты информации, передаваемой по линиям связи всех типов, является шифрование передаваемых сообщений [0, 0]. Линейные рекуррентные регистры сдвига (ЛРРС) являются базовыми блоками для построения многих генераторов гаммы, однако сами по себе имеют достаточно низкую криптографическую стойкость. [0-0]. Одним из способов достижения нелинейной зависимости знаков гаммы от ключевых элементов генератора, является неравномерное движение информации в определенных узлах генератора, определяемое ключом [0, 0]. Изменение закона движения приводит к изменению исходной гаммы, увеличивая ее сложность. Необходимость сдвига регистров на разное количество шагов приводит к тому, что увеличивается количество тактов синхронизирующего генератора, необходимое для получения одного элемента гаммы. В данной статье, с использованием алгоритма параллельной реализации линейного рекуррентного регистра сдвига за счет переопределения булевой функции обратной связи, дающего возможность получать состояние рекуррентного регистра сдвига через произвольное количество тактов функционирования, приводится пример реализации одного из генераторов гаммы с неравномерным движением – генератора скалярного произведения.

1. Понятие генератора скалярного произведения

В генераторе скалярного произведения (рис. 1) используется два ЛРРС с разными тактовыми частотами и, возможно, разной длины [0]. ЛРРС 1 имеет длину $n^{(1)}$ и показатель скорости $d^{(1)}$, ЛРРС 2 соответственно – $n^{(2)}$ и $d^{(2)}$. Ключом является начальное состояние ЛРРС – $X_0^{(1)}$ и $X_0^{(2)}$. Отдельные биты этих ЛРРС объединены операцией логического умножения (AND), а затем, для получения выходного бита они объединяются посредством сумматора по модулю два, т. е. вычисление каждого *i*-ого бита гаммы осуществляется по алгоритму:

1. Сдвинуть ЛРРС 1 на $d^{(1)}$ шагов.
2. Сдвинуть ЛРРС 2 на $d^{(2)}$ шага.
3. Вычислить знак гаммы: $y_i = \bigoplus_{k=0}^{\min(n^{(1)},n^{(2)})} = x_k^{(1)} \& x_k^{(2)}$.

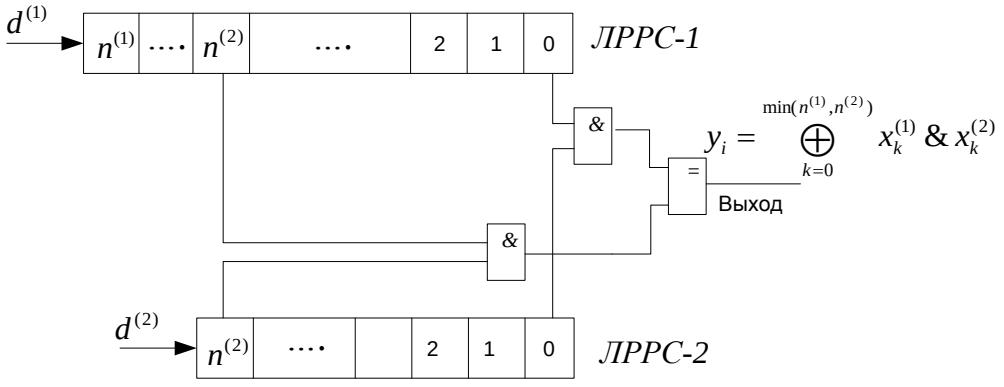


Рис. 1. Генератор скалярного произведения

2. Сдвиг рекуррентного регистра сдвига на произвольное количество шагов за один такт функционирования

Рекуррентный регистр сдвига с обратными связями состоит из регистра сдвига и схемы, реализующей функцию обратной связи. К простейшему типу устройств данного класса относится рекуррентный регистр с линейной обратной связью (рис. 2, а). Функция обратной связи в таких регистрах задается операцией «сумма по модулю два» над некоторыми битами регист-

ра. Номера этих битов определяются на основе полинома степени n [0]:

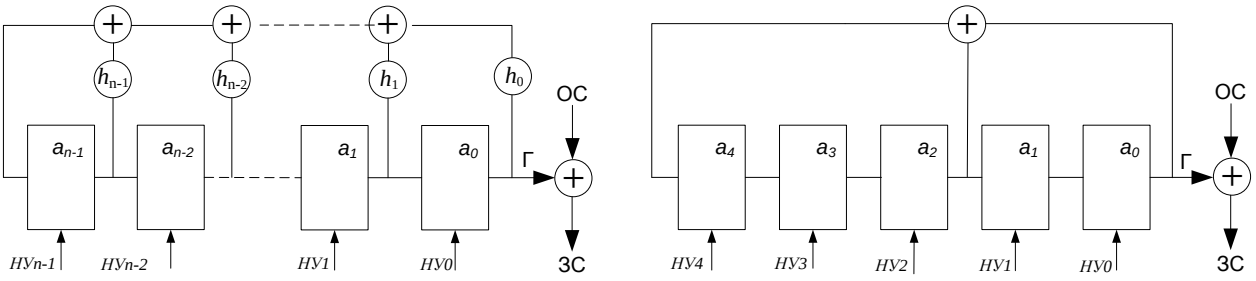
$h(x)=x^n+h_{n-1}\,x^{n-1}+h_{n-2}\,x^{n-2}+\ldots+h_2\,x^2+h_1\,x+h_0$,

где $h_i \in \{0,1\}$ – коэффициент связей.

Для обеспечения максимального периода псевдослучайной последовательности, генерируемой ЛРРС, образующий полином должен быть неприводимым и примитивным. На его основе строится линейное рекуррентное уравнение, которое при выполнении вычислений в $GF(2)$ имеет следующий вид [0]:

$$x_{(n-1)(t+1)}=h_{n-1}\,x_{n-1}\oplus\ldots\oplus h_1\,x_1\oplus h_0\,x_0. \quad (1)$$

Пример 1. ЛРРС, построенный на основе образующего полинома $h(x)=x^5\oplus x^2\oplus 1$, показан на рис. 2, б.



а) *б*)

Рис. 2 Линейный рекуррентный регистр сдвига

(НУ – сигналы начальной установки, ОС – открытое сообщение, ЗС – зашифрованное сообщение, *а* – разряды ЛРРС)

Для увеличения производительности возможно произвести переопределение булевой функции, описывающей функционирование ЛРРС, таким образом, чтобы за один такт функционирования получить несколько значений последовательности. Исходными данными для построения такой схемы будут: длина ЛРРС – n; начальное состояние ЛРРС – $X=(x_{n-1},\ldots,x_1,x_0)$; линейное рекуррентное уравнение $f(\mathbf{X},\mathbf{H})$, построенное по образующему полиному $h(x)$; количество моделируемых шагов работы – d.

Необходимо найти такую систему булевых функций $F(X)$, задающую обратные связи при приведении ЛРРС к виду (рис. 3), позволяющему за один такт сдвинуть ЛРРС на d шагов.

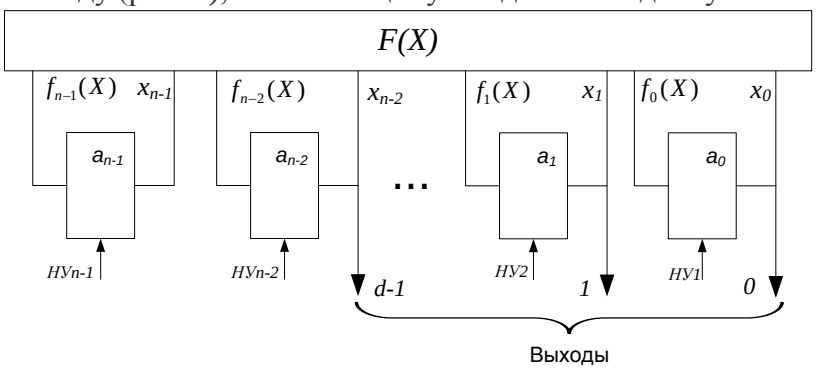


Рис. 3 Приведение ЛРРС к параллельному виду

Каждое последующее состояние ЛРРС можно выразить через предыдущее. При этом значение самого старшего разряда вычисляется с помощью линейного рекуррентного уравнения (1), значения остальных разрядов вычисляются сдвигом вправо предыдущих значений ячеек РРС.

Зависимость состояния РРС $\mathbf{X}_{t+1}=[x_{(n-1)(t+1)}\ldots x_{0(t+1)}]$ в определенный момент времени от предыдущего заполнения $\mathbf{X}_t=[x_{(n-1)t}\ldots x_{0t}]$ можно задать системой логических выражений:

$$\mathbf{X}_{t+1}=\begin{cases} x_{(n-1)(t+1)} = f(\mathbf{X},\mathbf{H}) = h_{(n-1)}x_{(n-1)t} \oplus .... \oplus h_0 x_{0t}, \\ x_{(n-2)(t+1)} = x_{(n-1)t}, \\ x_{(n-3)(t+1)} = x_{(n-2)t}, \\ \vdots \\ x_{1(t+1)} = x_{2t}, \\ x_{0(t+1)} = x_{1t}, \end{cases} \quad (2)$$

где: t – предыдущее состояние ЛРРС, t+1 – последующее состояние РРС.

Вычисляя последовательно каждое последующее состояние РРС через предыдущее по системе логических выражений (2), можно построить зависимость состояния РРС через определенное число тактов функционирования $\mathbf{X}_{t+d}$ от начального заполнения $\mathbf{X}$:

$$\mathbf{X}_{t+d}=\begin{cases} x_{(n-1)(t+d)} = f_{n-1}(\mathbf{X}), \\ \vdots \\ x_{1(t+d)} = f_1(\mathbf{X}), \\ x_{0(t+d)} = f_0(\mathbf{X}). \end{cases}$$

Каждое выражение, составляющее систему, является линейным полиномом Жегалкина. Каждое выражение будет полностью задано, если определены коэффициенты при переменных. Для формализации алгоритма определения выражений, описывающих состояние ЛРРС в определенный момент времени, коэффициенты при логических переменных удобно представить в виде матрицы, в которой строки будут соответствовать состоянию РРС в определенный момент времени, а столбцы — соответствовать начальному состоянию РРС:

$$\mathbf{W}=\begin{bmatrix} w_{00} & w_{01} & \dots & w_{0n-1} \\ w_{10} & w_{11} & \dots & w_{1n-1} \\ \vdots & \vdots & & \vdots \\ w_{(n-1)0} & w_{(n-1)1} & \dots & w_{(n-1)(n-1)} \end{bmatrix},$$

где $w_{ij} \in \{0,1\}$.

В начальный момент времени матрица коэффициентов будет иметь вид:

$$\mathbf{W}_t=\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Для нахождения коэффициентов в следующий момент времени необходимо умножить матрицу на вектор коэффициентов линейного рекуррентного уравнения:

$$\mathbf{W}_{t+1}=\mathbf{W}_t \cdot \mathbf{H}, \quad (3)$$

полученный вектор подставить в первую строку матрицы, а остальные строки сдвинуть на одну вниз.

3. Демонстрационный пример реализации генератора скалярного произведения

Исходные данные:

Для ЛРРС 1 – $n^{(1)}$=4, $x^{(1)}{}_{3(t+1)} = x^{(1)}{}_{1t} \oplus x^{(1)}{}_{0t}$, $d^{(1)}$=2.

Для ЛРРС 2 – $n^{(2)}$=3, $x^{(2)}{}_{2(t+1)} = x^{(2)}{}_{2t} \oplus x^{(2)}{}_{0t}$, $d^{(1)}$=1.

Для ЛРРС 1 найдем функцию обратной связи, осуществляющую сдвиг на 2 шага за один такт функционирования.

$$F\left(X_t^{(1)}\right)=\begin{cases} x_{3(t+2)}^{(1)} = x_{2t}^{(1)} \oplus x_{1t}^{(1)} \\ x_{2(t+2)}^{(1)} = x_{1t}^{(1)} \oplus x_{0t}^{(1)} \\ x_{1(t+2)}^{(1)} = x_{3t}^{(1)} \\ x_{0(t+2)}^{(1)} = x_{2t}^{(1)} \end{cases} \quad (4)$$

Схемотехническая реализация данного примера показана на (рис. 4).

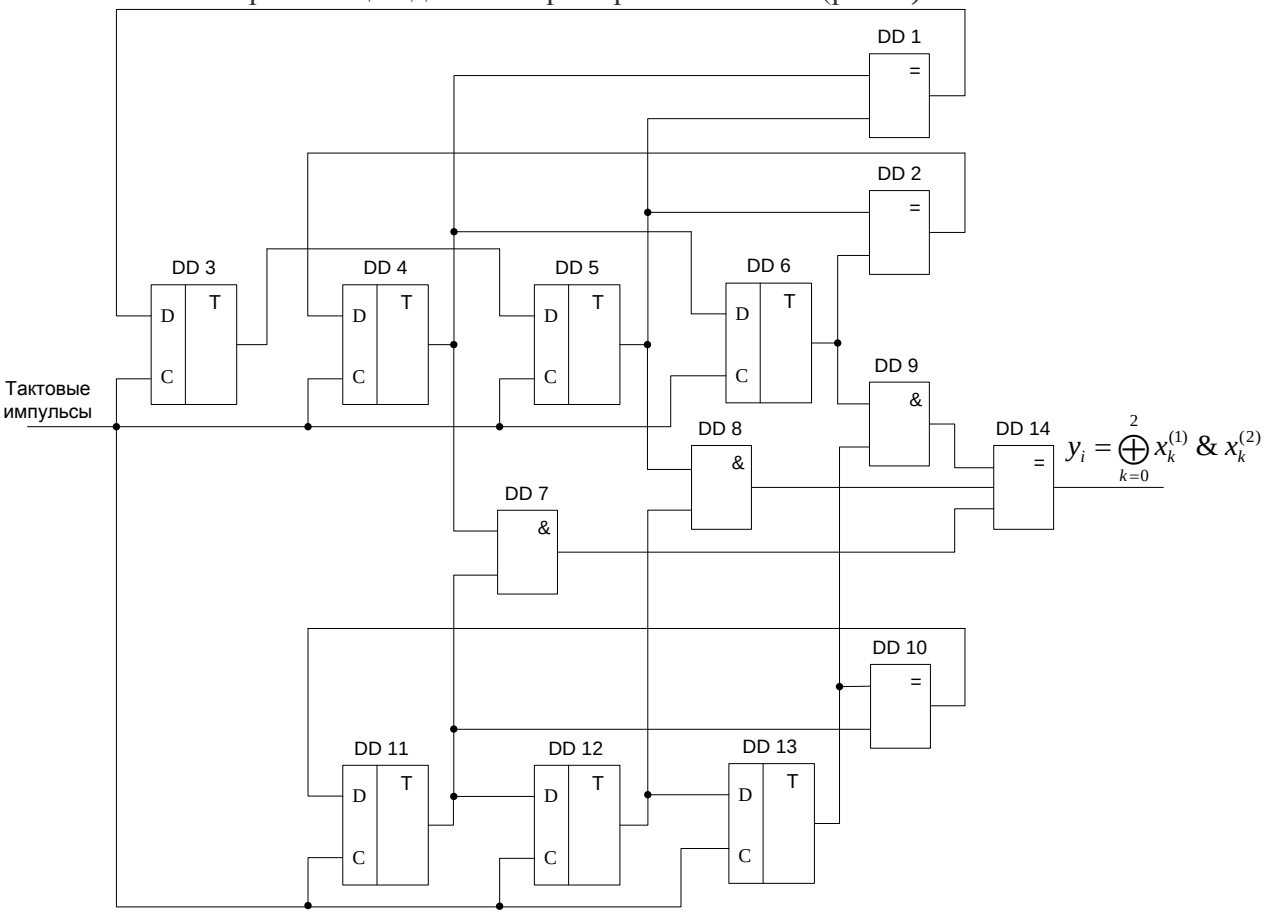


Рис. 4. Модель генератора скалярного произведения

Описание схемы. ЛРРС 1 собран на триггерах D-триггерах DD3-DD6, функция обратной связи (4) реализована на элементах DD1, DD2. ЛРРС 2 собран на триггерах DD11-DD13 и сумматоре по модулю два DD10. Побитная конъюнкция соответствующих разрядов ЛРРС 1 и ЛРРС 2 осуществляется элементами DD7-DD9, DD14 – результирующий сумматор по модулю два.

Первые девять значений гаммы при начальном заполнении 1000 и 100 для ЛРРС 1 и ЛРРС 2 соответственно показаны в табл. 1. В таблице невыделенными остались строки, в которых записаны пропускаемые состояния ЛРРС 1. Запустив схему на выполнение, получаем гамму на выходе генератора скалярного произведения, соответствующую теоретическим вычислениям, причем каждый знак гаммы получает за один такт функционирования.

Таблица 1

Смена состояний генератора скалярного произведения

N такт	$x_3^{(1)}$	$x_2^{(1)}$	$x_1^{(1)}$	$x_0^{(1)}$		$x_2^{(2)}$	$x_1^{(2)}$	$x_0^{(2)}$		Г
0	1	0	0	0		1	0	0		0
	0	1	0	0						
1	0	0	1	0		1	1	0		1

	1	0	0	1						
2	1	1	0	0		1	1	1		1
	0	1	1	0						
3	1	0	1	1		0	1	1		0
	0	1	0	1						
4	1	0	1	0		1	0	1		0
	1	1	0	1						
5	1	1	1	0		0	1	0		1
	1	1	1	1						
6	0	1	1	1		0	0	1		1
	0	0	1	1						
7	0	0	0	1		1	0	0		0
	1	0	0	0						
8	0	1	0	0		1	1	0		1
	0	0	1	0						
9	1	0	0	1		1	1	1		1

Таким образом, при незначительном усложнении схемы (в данном примере на один двухвходовый сумматор по модулю два) получили схемотехническую реализацию генератора скалярного произведения, в котором для получения знака гаммы необходим всего один такт функционирования вместо двух при классическом способе реализации. Описанный алгоритм переопределения функции обратной связи ЛРРС может использоваться для построения схем более сложных генераторов гаммы скалярного произведения при произвольных значениях длин регистров $n^{(1)}$ и $n^{(2)}$ и показателях скоростей $d^{(1)}$ и $d^{(2)}$.

Литература:

1.Основы криптографии: Учебное пособие/ Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. — М.: Гелиос АРВ, 2001. — 480 с.

2. Фомичев В. М. Дискретная математика и криптология: Курс лекций/ Под общ ред. Н. Д. Подуфалова. — М.: Диалог-МИФИ, 2003. — 400 с.

3.Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.