Математические и компьютерные основы защиты информации

Лекция 3

Антон Николаевич Гайдук | УНИВЕР

vk.com/gaidukedu

23 февраля 2023 г.

Содержание дисциплины

Раздел I Введение

- Тема 1. Введение. История. Основные понятия.

Раздел II Симметричная криптография

- Тема 2 Классические шифры.
- Тема 3 Поточные алгоритмы шифрования.
- Тема 4 Блочно-итерационные алгоритмы шифрования.
- Тема 5 Функции хэширования.
- Тема 6 Математические методы криптоанализа.

Раздел III Асимметричная криптография

- Тема 7 Протокол Диффи-Хэллмана.
- Тема 8 Криптосистемы с открытым ключом.
- Тема 9 Электронная цифровая подпись.

Раздел II Симметричная криптография

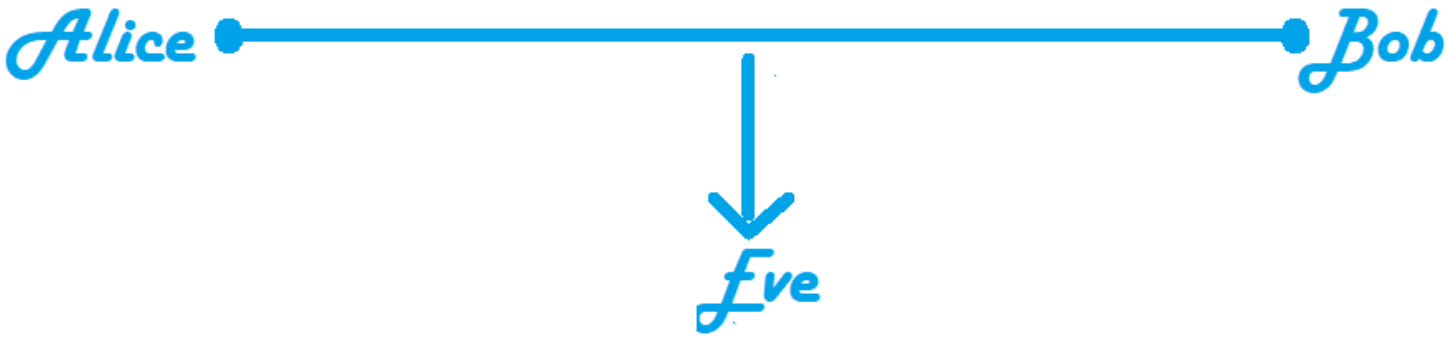
Тема 3 Поточные алгоритмы шифрования

- Теоретико-информационная стойкость
- Шифр Вернама
- Равномерно распределенная случайная последовательность и ее свойства
- Автоматная модель поточного алгоритма шифрования
- Рекуррентные последовательности
- РСЛОС
- Поточные алгоритмы шифрования на основе РСЛОС
- Тестирование случайных последовательностей


LAVOIE


LAVOIE

Общепринятые имена участников

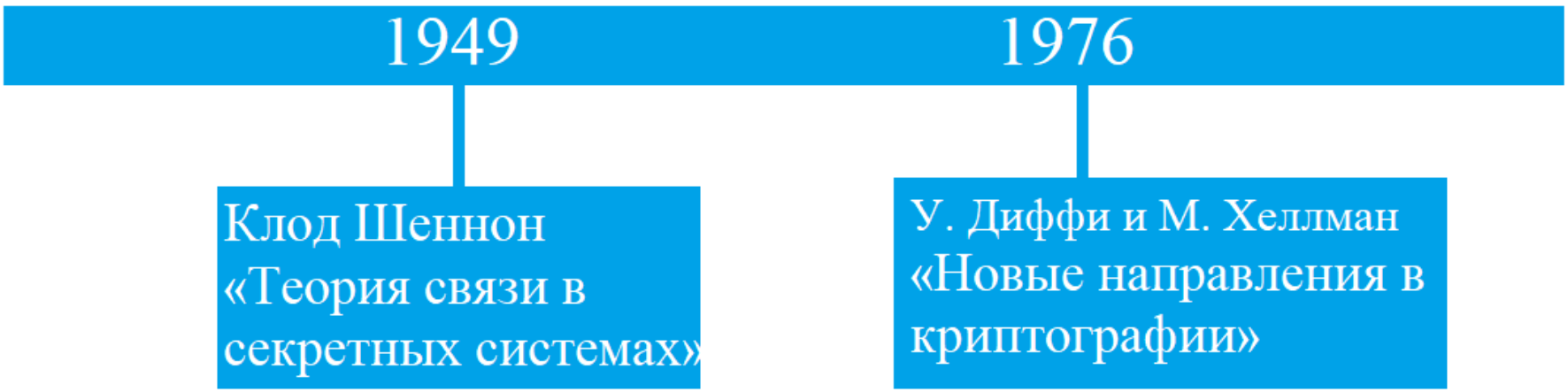


- Алиса и Боб обмениваются сообщениями
- Ева перехватывает сообщения (нарушение конфиденциальности)

Обеспечение конфиденциальности информации — защита информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней

Способность криптографического алгоритма противостоять атакам называется (крипто)стойкостью

История


1949
1976
Клод Шеннон «Теория связи в секретных системах»
У. Диффи и М. Хеллман «Новые направления в криптографии»

Модели

Для того, чтобы иметь возможность доказывать в криптографии точные результаты, нужны математические модели основных исследуемых объектов:

- модель шифрсистемы,
- модель противника.

Модели

Для того, чтобы иметь возможность доказывать в криптографии точные результаты, нужны математические модели основных исследуемых объектов:

- модель шифрсистемы,
- модель противника.

Определение

Шифрсистемой называется пятерка $\{\mathcal{K}, \mathcal{P}, \mathcal{C}, E, D\}$, где
$\mathcal{K}$ — множество ключей (секретных параметров),
$\mathcal{P}$ — множество открытых текстов,
$\mathcal{C}$ — множество шифртекстов,
E — семейство преобразований зашифрования $E = \{E_k : \mathcal{P} \to \mathcal{C} | k \in \mathcal{K}\}$
D — семейство преобразований расшифрования $D = \{D_k : \mathcal{C} \to \mathcal{P} | k \in \mathcal{K}\}$
с ограничениями

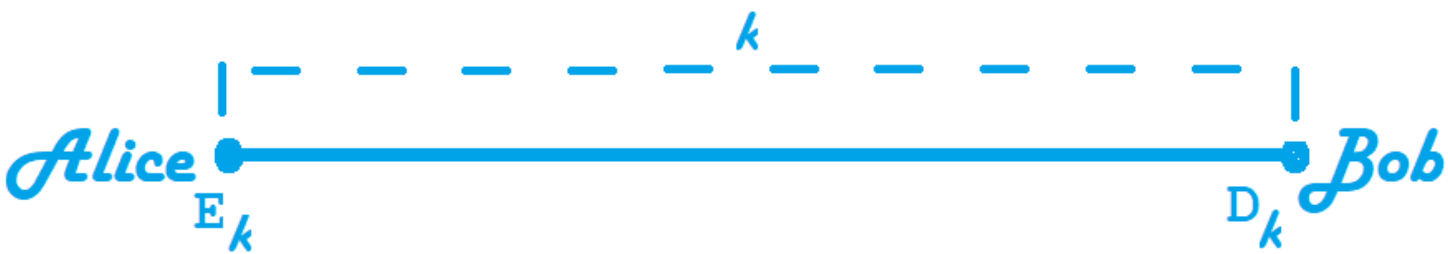
- однозначность расшифрования: $D_k(E_k(p)) = p$ для $\forall p \in \mathcal{P}$;
- реализуемость всех шифртекстов: $\bigcup\limits_{k \in \mathcal{K}} \bigcup\limits_{p \in \mathcal{P}} E_k(p) = \mathcal{C}$, т.е.

  $\forall c \in \mathcal{C} \qquad \exists p \in \mathcal{P}, k \in \mathcal{K}$ такие, что $E_k(p) = c$.

Модели

Для того, чтобы иметь возможность доказывать в криптографии точные результаты, нужны математические модели основных исследуемых объектов:

- модель шифрсистемы,
- модель противника.



Модель противника

- Шифрсистема $\Psi = \{\mathcal{K}, \mathcal{P}, \mathcal{C}, E, D\}$ — известна.
- Открытый текст X и ключ κ являются независимыми случайными величинами со следующими распределениями вероятностей:

$$\mathbb{P}\{X = x\} = p_X(x), x \in \mathcal{P}, \qquad \mathbb{P}\{\kappa = k\} = p_\kappa(k), k \in \mathcal{K},$$

- вычислительные ресурсы не ограничены.

Существуют ли шифрсистемы способные **противостоять** данной модели противника, который перехватывает шифртекст(ы)?

Шэннон (идея)

Шифрсистема совершенна, если из шифртекста нельзя получить никакой информации об открытом тексте.

Модели открытых текстов

Пусть A — некоторый конечный алфавит, например:
$A = \{0, 1\}, A = \{0, 1, \ldots, 25\}, A = \{0, 1, \ldots, 255\}$.
Пусть $x = (x_0, x_1, \ldots, x_{n-1}) \in A^n$ некоторое слово длины n.

Приближение

- 0 порядка: символы независимы и одинаково распределены:

$$\mathbb{P}\{X = x\} = \prod_{i=0}^{n-1} \mathbb{P}\{x_i\} = \left(\frac{1}{|A|}\right)^n.$$

- 1 порядка: символы независимы с дискретным распределением вероятностей:

$$\mathbb{P}\{X = x\} = \prod_{i=0}^{n-1} \mathbb{P}\{x_i\}.$$

- 2 порядка: распределение описывается моделью цепи Маркова первого порядка:

$$\mathbb{P}\{X = x\} = \mathbb{P}(x_0) \prod_{i=1}^{n-1} \mathbb{P}\{x_i | x_{i-1}\}.$$

- и т.д.

Совершенные шифрсистемы

Определение (Шеннон)

Симметричная криптосистема называется совершенно криптостойкой, если апостериорное распределение вероятностей исходного случайного сообщения X при регистрации случайного шифртекста $Y = E_k(X)$ совпадает с априорным распределением вероятностей:

$$\mathbb{P}\{X = x | Y = y\} = \mathbb{P}\{X = x\}, \qquad \forall x \in \mathcal{P}, y \in \mathcal{C}.$$

Совершенные шифрсистемы

Определение (Шеннон)

Симметричная криптосистема называется совершенно криптостойкой, если апостериорное распределение вероятностей исходного случайного сообщения X при регистрации случайного шифртекста $Y = E_k(X)$ совпадает с априорным распределением вероятностей:

$$\mathbb{P}\{X = x | Y = y\} = \mathbb{P}\{X = x\}, \qquad \forall x \in \mathcal{P}, y \in \mathcal{C}.$$

Используется шифр простой замены. Латинский алфавит.
Перехвачен шифр текст: abccd.

$$\mathbb{P}\{X = \text{after} | Y = \text{abccd}\} = 0, \qquad \mathbb{P}\{X = \text{catch} | Y = \text{abccd}\} = 0.$$

Совершенные шифрсистемы

Определение (Шеннон)

Симметричная криптосистема называется совершенно криптостойкой, если апостериорное распределение вероятностей исходного случайного сообщения X при регистрации случайного шифртекста $Y = E_k(X)$ совпадает с априорным распределением вероятностей:

$$\mathbb{P}\{X = x | Y = y\} = \mathbb{P}\{X = x\}, \qquad \forall x \in \mathcal{P}, y \in \mathcal{C}.$$

Теорема (Шеннон)

Необходимое и достаточное условие совершенной криптостойкости состоит в том, что условное распределение вероятностей шифртекста Y при фиксированном сообщении X не зависит от X:

$$\mathbb{P}\{Y = y | X = x\} = \mathbb{P}\{Y = y\}, \qquad \forall x \in \mathcal{P}, y \in \mathcal{C}.$$

Следует из формулы Байеса: $\mathbb{P}\{X = x | Y = y\} = \frac{\mathbb{P}\{X=x\}\mathbb{P}\{Y=y|X=x\}}{\mathbb{P}\{Y=y\}}$.

Совершенные шифрсистемы

Определение (Шеннон)

Симметричная криптосистема называется совершенно криптостойкой, если апостериорное распределение вероятностей исходного случайного сообщения X при регистрации случайного шифртекста $Y = E_k(X)$ совпадает с априорным распределением вероятностей:

$$\mathbb{P}\{X = x | Y = y\} = \mathbb{P}\{X = x\}, \qquad \forall x \in \mathcal{P}, y \in \mathcal{C}.$$

Следствие

Если выполняется условие совершенной криптостойкости, то количество информации по Шеннону, содержащейся в шифртексте Y об исходном сообщении X, равно нулю:

$$I(X, Y) = I(Y, X) = H(X) - H(X|Y) = H(Y) - H(Y|X) = 0.$$

Совершенные шифрсистемы

Теорема (Шеннон)

Если шифрсистема совершенна, то

$$|\mathcal{P}| \leqslant |\mathcal{C}| \leqslant |\mathcal{K}|$$

Теорема (Шеннон)

Если $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$, то шифрсистема совершенна тогда и только тогда, когда

1. Уравнение $E_k(x) = y$ однозначно разрешимо для любых $x \in \mathcal{P}, y \in \mathcal{C}$.
2. $p_\kappa(k) = \frac{1}{|\mathcal{K}|}, k \in \mathcal{K}$.

Шифр Вернама (одноразовый блокнот)

- шифр с абсолютной криптографической стойкостью
- секретный параметр шифра — ключ такой же длины, что и сообщение

$$A = \mathbb{Z}_2 = \{0, 1\}$$

$$E_\gamma(x) = D_\gamma(x) = x \oplus k, \qquad x, k \in A^n,$$

$$\mathbb{P}\{\kappa = k\} = p_\kappa(k) = \frac{1}{2^n}.$$

Пример

$$\begin{array}{cccccccc} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{array} \quad (\oplus)$$

Шифр Вернама: недостатки

- требуется истинно случайная последовательность (ключ),
- длина ключа должна совпадать с длиной открытого текста,
- ключ используется только один раз:

$$\begin{aligned} Y_1 &= X_1 \oplus k, \\ Y_2 &= X_2 \oplus k, \\ Y_1 \oplus Y_2 &= X_1 \oplus X_2. \end{aligned}$$

- отсутствует контроль целостности передаваемых данных.

Пример успешной атаки на реализацию шифра Вернама

Множество открытых текстов $\mathcal{P}$ состоит только из двух элементов:

$$X_1 = \text{yes}, X_2 = \text{no},$$

если используется шифр Вернама с переменной длинной ключа, то по длине шифртекста возможно восстановить открытый текст.

Поточные алгоритмы шифрования

Цель: придумать такой способ генерации последовательности γ, чтобы

1. Генерация была «быстрой».
2. Способ генерации γ задавался некоторым ключом $k \in \mathcal{K}$, зная который принимающая сторона могла бы сгенерировать идентичную последовательность.
3. Последовательность γ вела себя как последовательность независимых в совокупности равномерно распределенных случайных величин (псевдослучайная последовательность).

Поточные алгоритмы шифрования

Поточные алгоритмы шифрования

По ключу $k \in \mathcal{K}$ строится последовательность $\gamma = \gamma_1 \dots \gamma_n, \gamma_i \in \Gamma, i = \overline{1,n}$
шифрование открытого текста $p = p_1 \dots p_n$ осуществляется посимвольно:

$$p = p_1 \dots p_n \to E_{\gamma_1}(p_1) \dots E_{\gamma_n}(p_n) = c_1 \dots c_n = c,$$

$p_i \in A, c_i \in A, i = \overline{1,n}$.

На практике обычно используются $A = \{0,1\}^m$, $(m = 1, 8, 16)$,

$$\Gamma = \mathcal{P} = \mathcal{C} = A$$

$$E_\gamma(p) = p \oplus \gamma = c, \qquad D_\gamma(c) = c \oplus \gamma = p \oplus \gamma \oplus \gamma = p,$$

$$E_\gamma(x) = D_\gamma(x) = x \oplus \gamma, \qquad p, c, x, \gamma \in A^n.$$

Равномерно распределенная случайная последовательность

РРСП — это случайная последовательность $\gamma_1, \gamma_2, \ldots, \gamma_t, \gamma_{t+1}, \ldots$ со значениями в дискретном множестве $\mathcal{A} = \{0, 1, \ldots, N-1\}$ определенная на вероятностном пространстве $(\Omega, \mathcal{F}, \mathbb{P})$ и удовлетворяющая двум свойствам:

Свойство 1

Для любого $n \in \mathbb{N}$ и произвольных значений индексов $1 \leqslant t_1 < \cdots < t_n$ случайные величины $\gamma_{t_1}, \ldots, \gamma_{t_n} \in \mathcal{A}$ независимы в совокупности.

Свойство 2

Для любого номера $t \in \mathbb{N}$ случайная величина γ_t имеет дискретное равномерное на $\mathcal{A}$ распределение вероятностей:

$$\mathbb{P}\{\gamma_t = a\} = \frac{1}{N}, \qquad a \in \mathcal{A}.$$

Автоматная модель поточного алгоритма шифрования

Определение

Абстрактным конечным автоматом называется объект $\mathcal{U} = \{A, S, B, \varphi, \psi\}$, где
$A = \{a_1, \ldots, a_m\}$ — входной алфавит, множество входов,
$S = \{s_1, \ldots, s_n\}$ — множество состояний конечного автомата,
$B = \{b_1, \ldots, b_k\}$ — множество выходов конечного автомата (выходной алфавит),
$\varphi : S \times A \to S$ — функция переходов,
$\psi : S \times A \to B$ — функция выходов.

Для задания конечных автоматов необходимо определить множества A, S, B и задать функции φ, ψ.

Инициальный конечный автомат

Конечный автомат с фиксированным начальным состоянием называется инициальным конечным автоматом. Обозначается, инициальный конечный автомат следующим образом: $\mathcal{U}_{s_0} = \{A, S, B, \varphi, \psi, s_0\}$.

Алгоритм RC4

$n = 8, \mathcal{A} = \{0,1\}^8$.

Состояние алгоритма RC4

- Перестановка $S \in S(\mathbb{Z}_{256})$ из $N = 2^n = 256$ байт.
- Два индекса i, j.

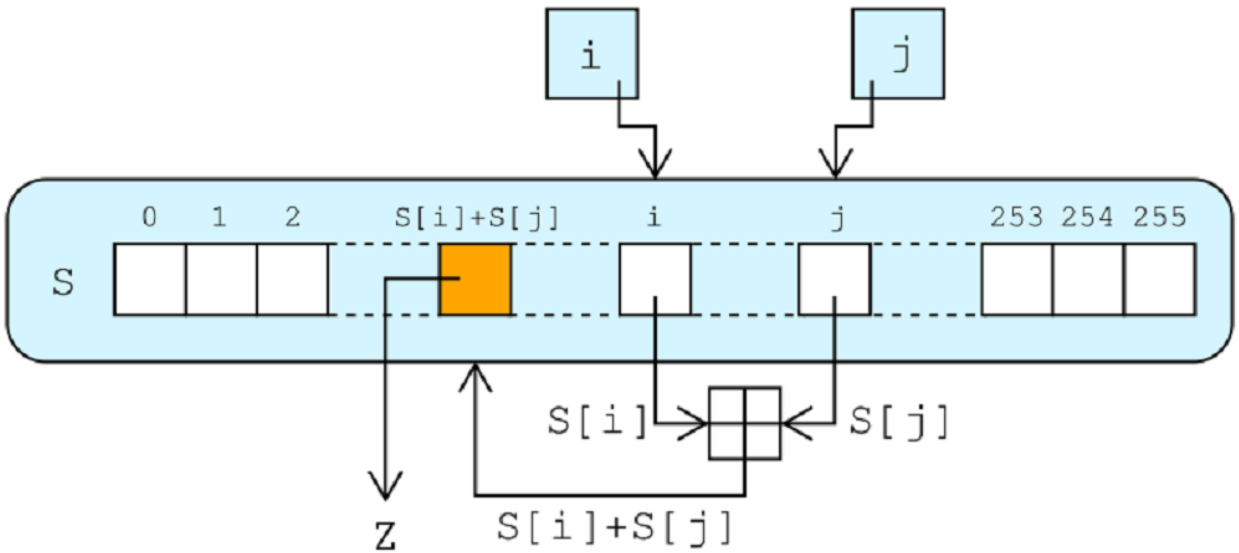
- Вход: секретный ключ K из l байт (5—32) с помощью процедуры загрузки ключа инициализирует состояние алгоритма RC4;
- Выход: гамма

Загрузка ключа	Выработка гаммы

`for i=0,...,N-1`
`  S[i]=i`
`j=0`
`for i=0,...,N-1`
`  j = j + S[i] + K [i mod l]`
`  Swap: S[i]<->S[j]`
`i=0 j=0`
	`i=i+1`
	`j = j + S[i]`
	`Swap: S[i]<->S[j]`
	`Output: Z=S[S[i]+S[j]]`

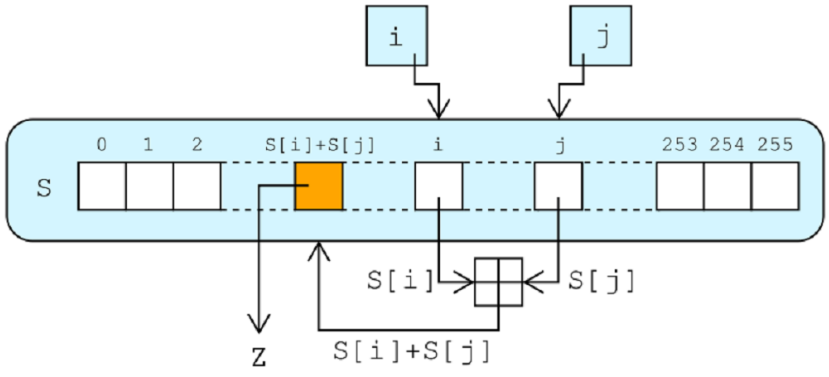
* сложение выполняется по модулю $N = 256$

Алгоритм RC4



Алгоритм RC4

Ключ:	K
Длина ключа (в байтах):	l
Открытый текст:	P
Гамма:	Z
Шифртекст:	C
Зашифрование:	$C = Z \bigoplus P$
Расшифрование:	$P = C \bigoplus Z$



- Размер внутреннего состояния алгоритма RC4: $\log_2(2^{16} \times 2^8!) \approx 1700$ бит.
- Процедура загрузки ключей не биективна: существуют разные ключи, которые приводят к одному и тому же состоянию алгоритма RC4.

Автоматная модель поточного алгоритма шифрования

Одним из важных результатов теории конечных автоматов является то, что вырабатываемая выходная последовательность является периодической (возможно с некоторым предпериодом).

Линейная рекуррентная последовательность

Последовательность $\{s_n\}_{n=0}^{\infty}$ над некоторым полем $\mathbb{K}$ называется линейной рекуррентной последовательностью (англ. constant-recursive sequence) порядка L, если её первые L членов заданы $(s_0, \dots s_{L-1})$, а для любого $n \geqslant L$ выполняется равенство:

$$s_n = c_1 s_{n-1} + \cdots + c_L s_{n-L} = \sum_{i=1}^{L} c_i s_{n-i}. \tag{1}$$

где коэффициенты $c_i \in \mathbb{K}, i = \overline{1, L}$.

Соотношение (1) также может быть представлено в виде:

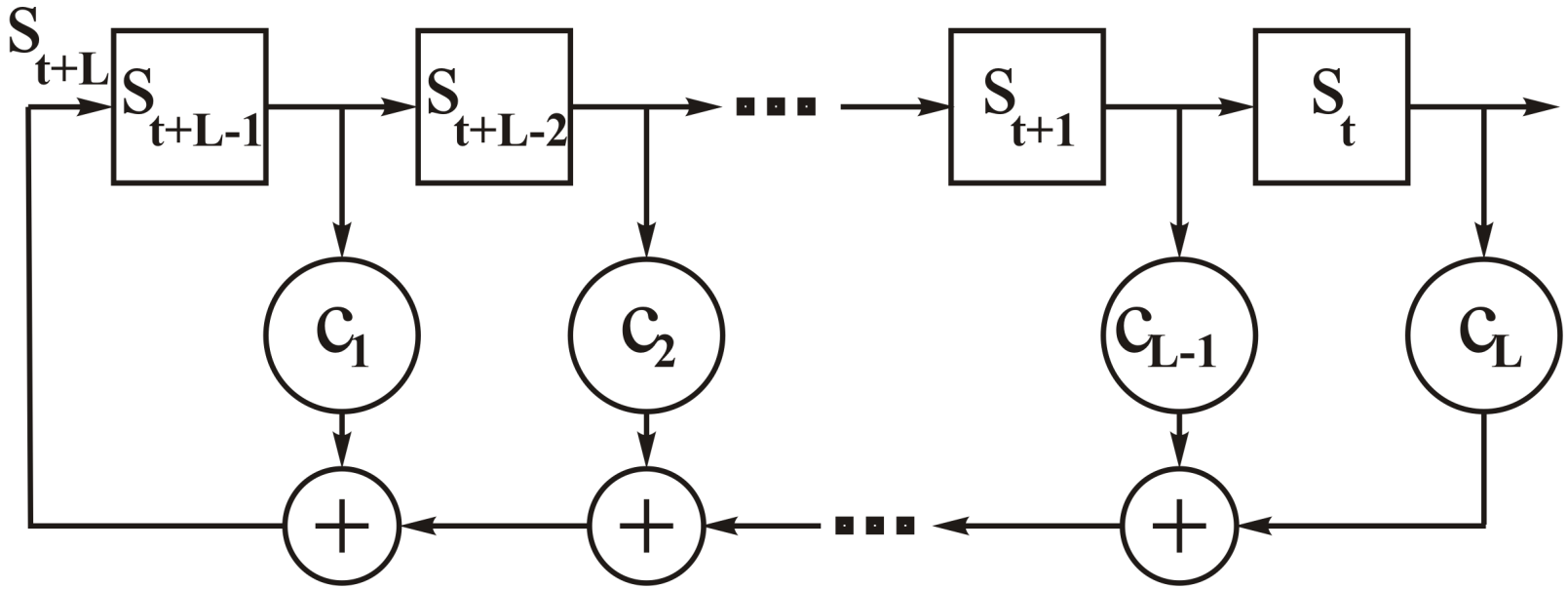
$$s_{n+L} = \sum_{i=1}^{L} c_i s_{n+L-i}, \qquad \forall n \geqslant 0. \tag{2}$$

РСЛОС

Регистром сдвига с линейной обратной связью (РСЛОС) длины L над полем $\mathbb{F}_q$ называют автономный КА, выходная последовательность ($S = \{s_t\}_{t=0}^{\infty}$) которого является линейной рекуррентой порядка L над полем $\mathbb{F}_q$:

$$s_{t+L} = \sum_{i=1}^{L} c_i s_{t+L-i}, \qquad \forall t \geqslant 0,$$

где коэффициенты $c_i \in \mathbb{F}_q, i = \overline{1, L}$ называются *коэффициентами обратной связи*.



РСЛОС

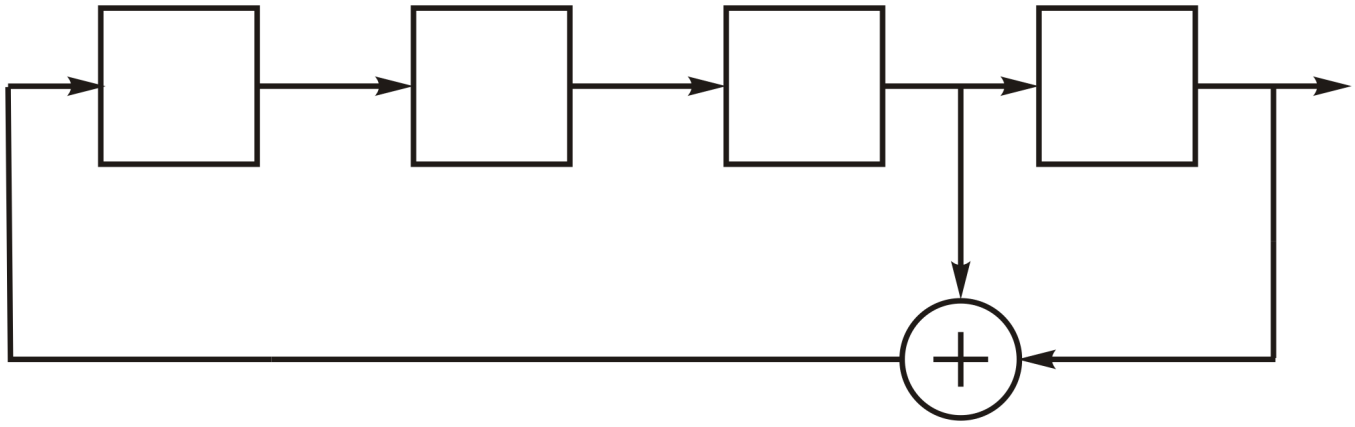
Обозначим $\mathbf{s_0} = (s_0, \dots s_{L-1}), \dots, \mathbf{s_n} = (s_n, \dots s_{n+L-1}), \dots$ — векторы составленных из L последовательных членов линейной рекуррентной последовательности.

Если $\{s_n\}_{n=0}^{\infty}$ — линейная рекуррентная последовательность над полем $\mathbb{F}_q$, удовлетворяющая соотношению (1), а $\mathcal{C}$ — матрица, связанная с этой последовательностью и задаваемая равенством (3), то для векторов состояний последовательности $\{s_n\}_{n=0}^{\infty}$ справедливо равенство

$$\mathbf{s_n} = \mathbf{s_0}\mathcal{C}^n, \qquad n \geqslant 0,$$

$$\mathcal{C} = \begin{vmatrix} 0 & 0 & 0 & \dots & 0 & c_L \\ 1 & 0 & 0 & \dots & 0 & c_{L-1} \\ 0 & 1 & 0 & \dots & 0 & c_{L-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & c_1 \end{vmatrix} \tag{3}$$

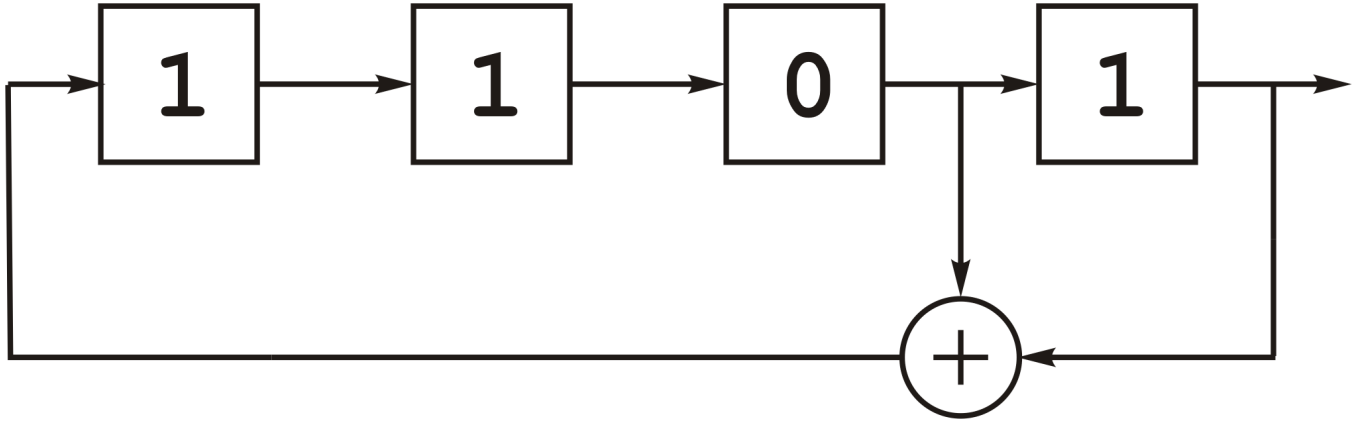
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

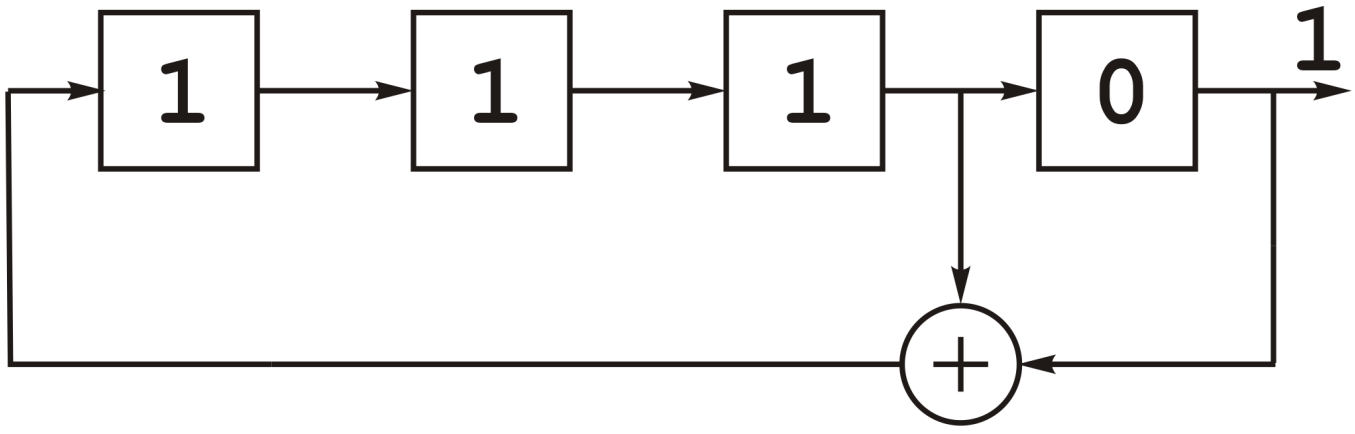
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

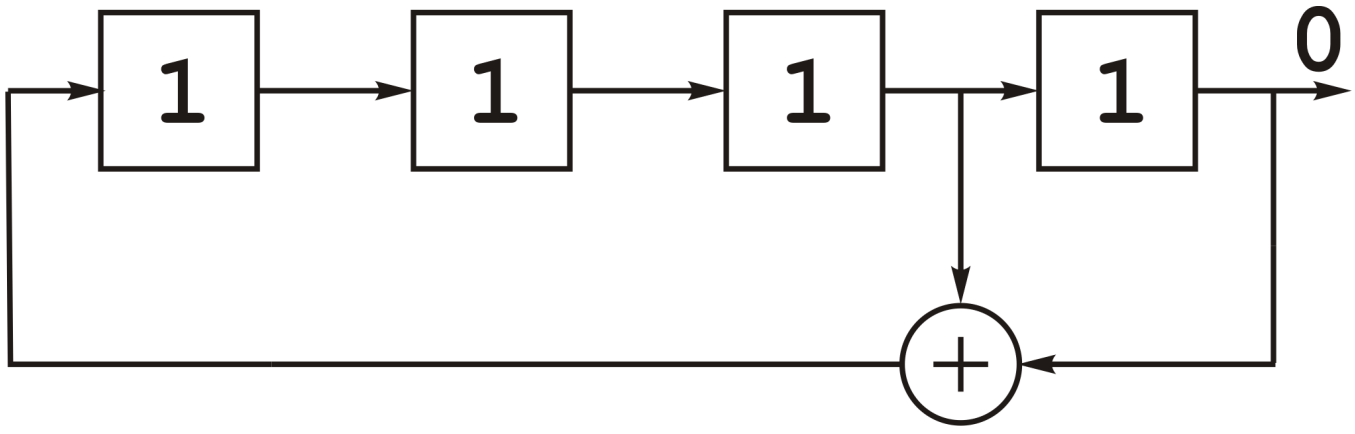
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

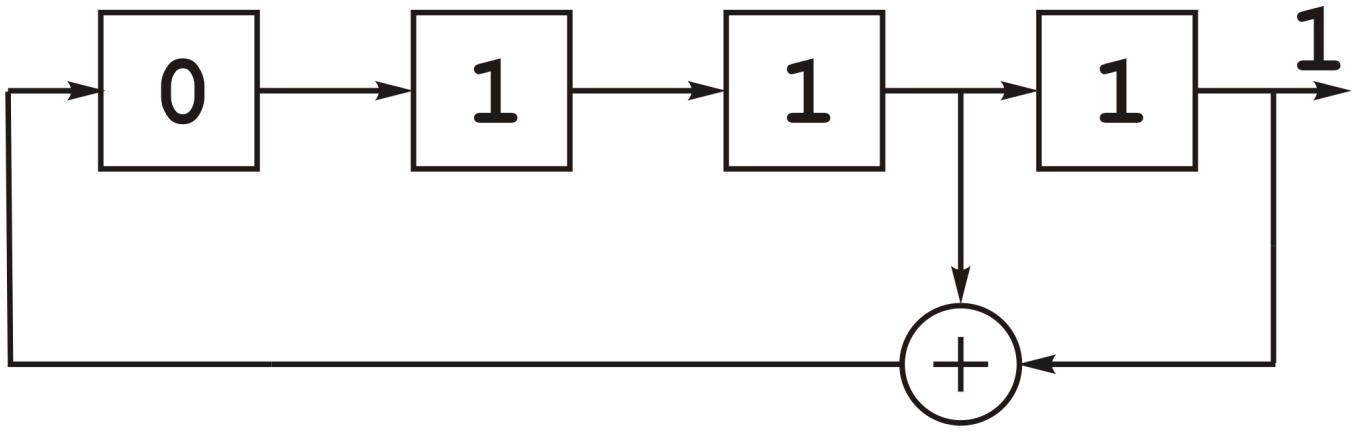
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

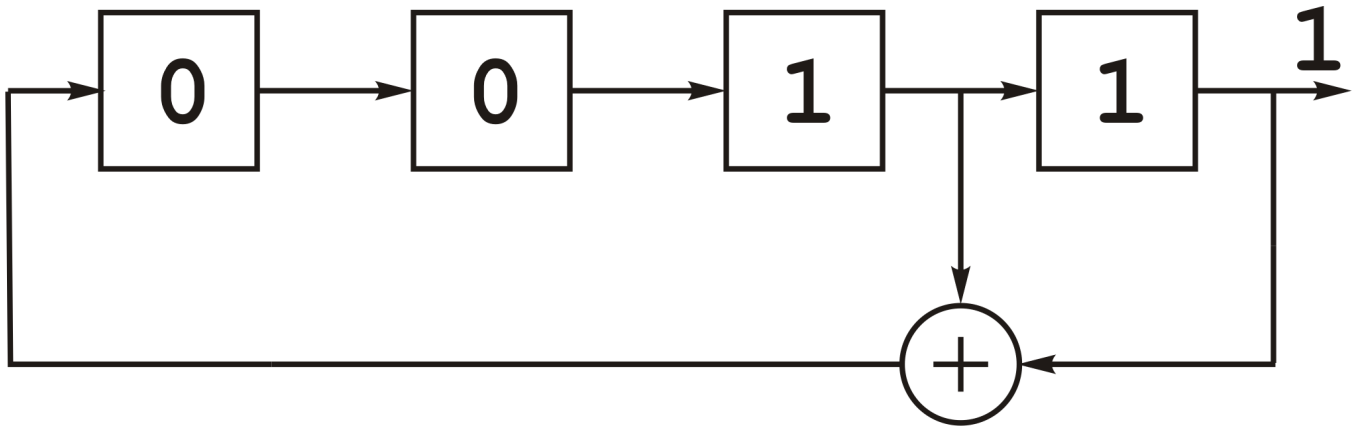
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

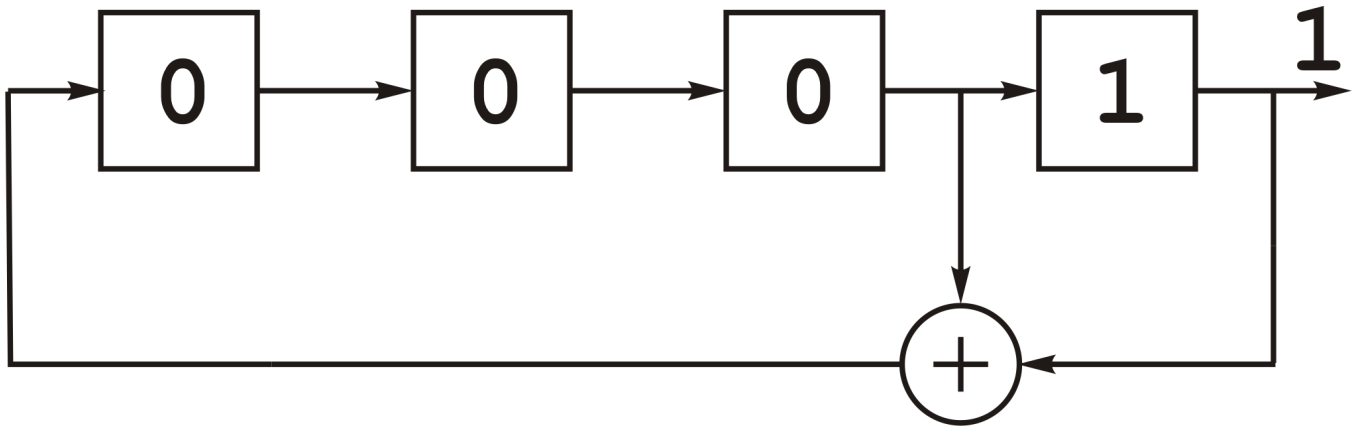
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

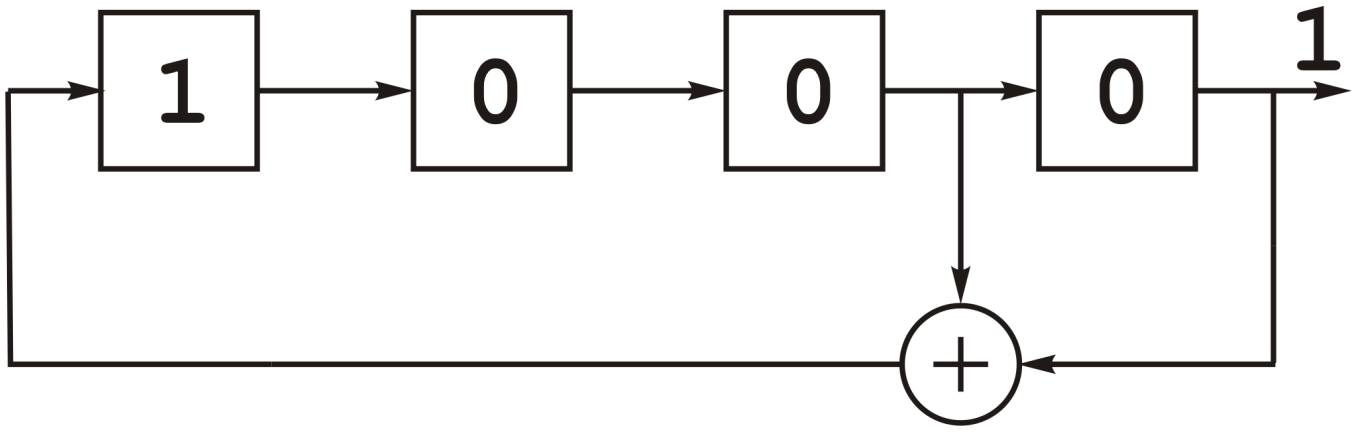
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

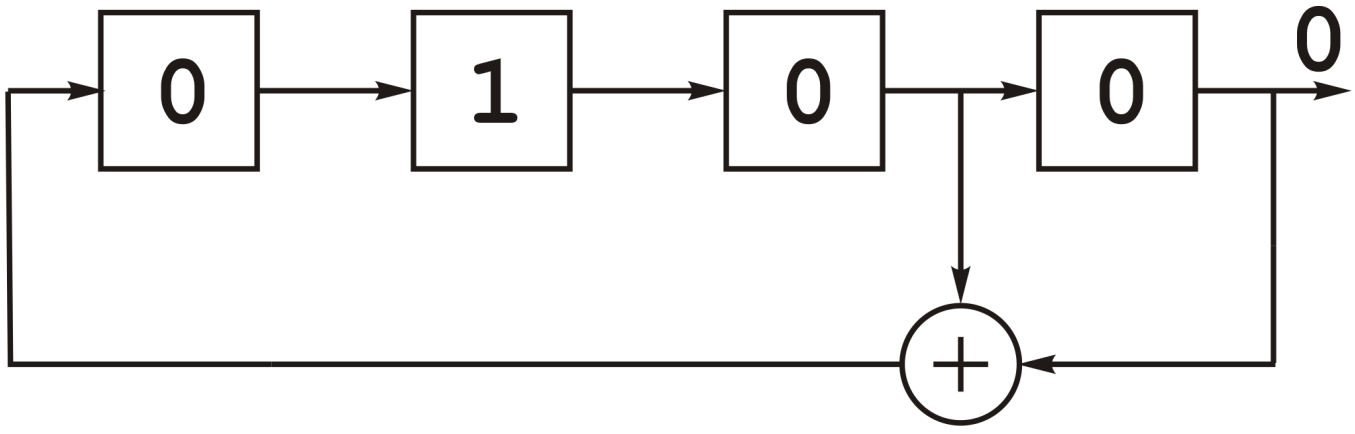
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

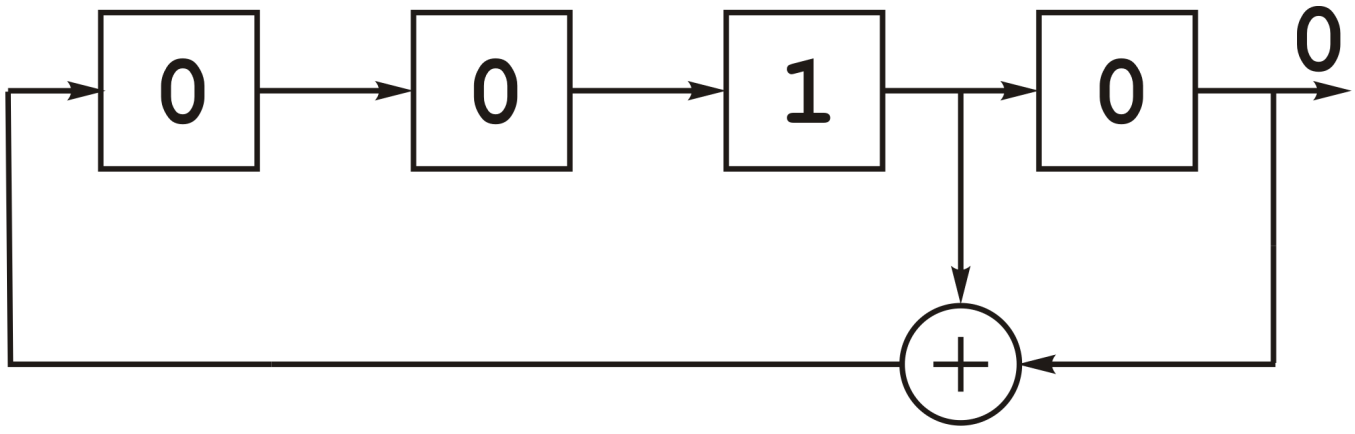
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

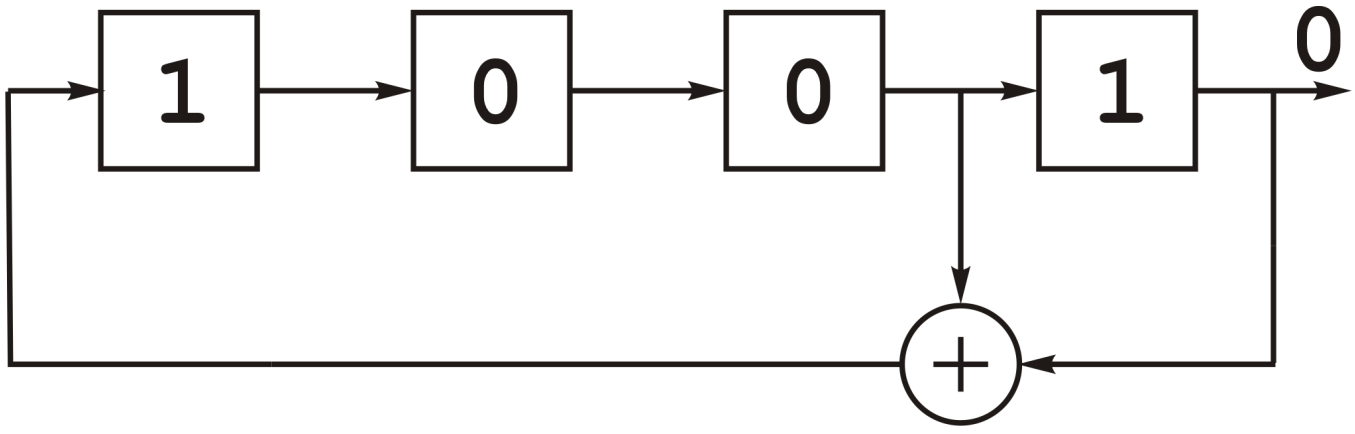
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

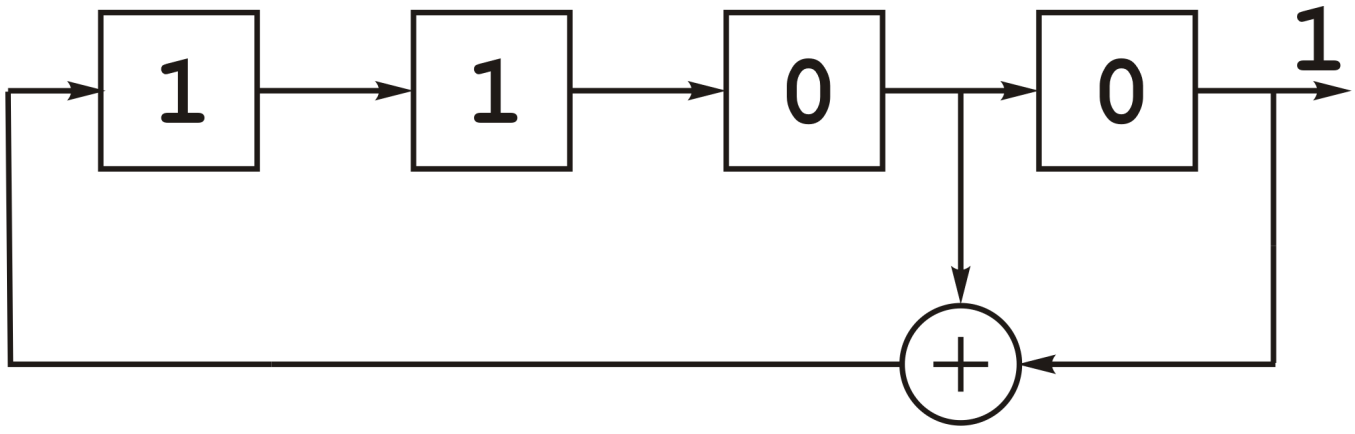
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

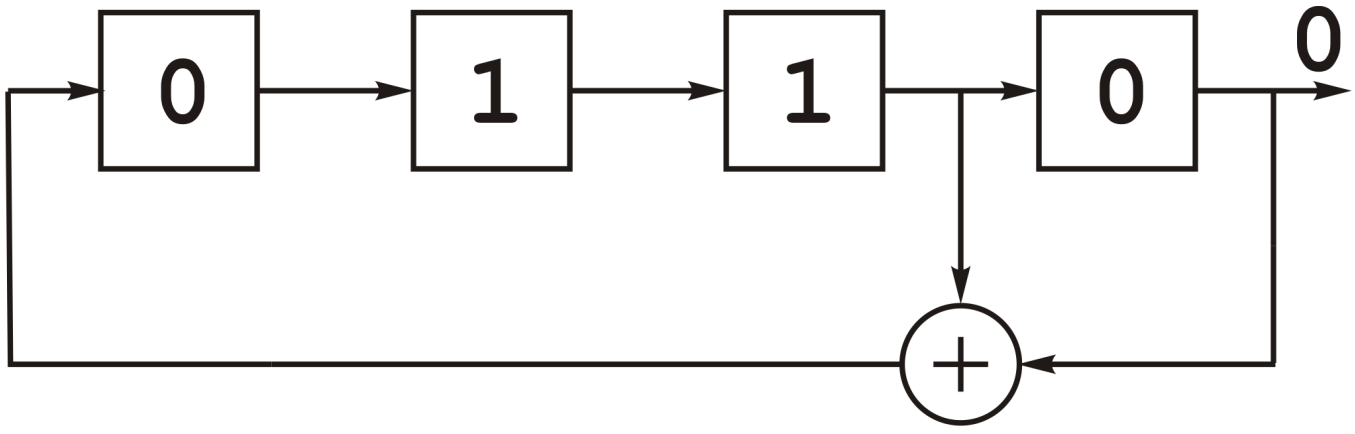
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

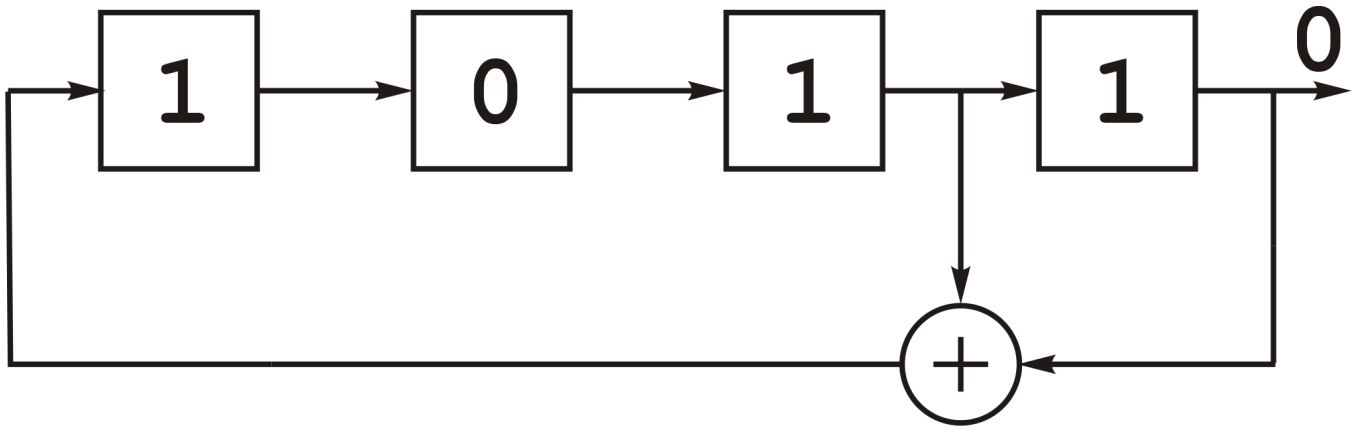
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

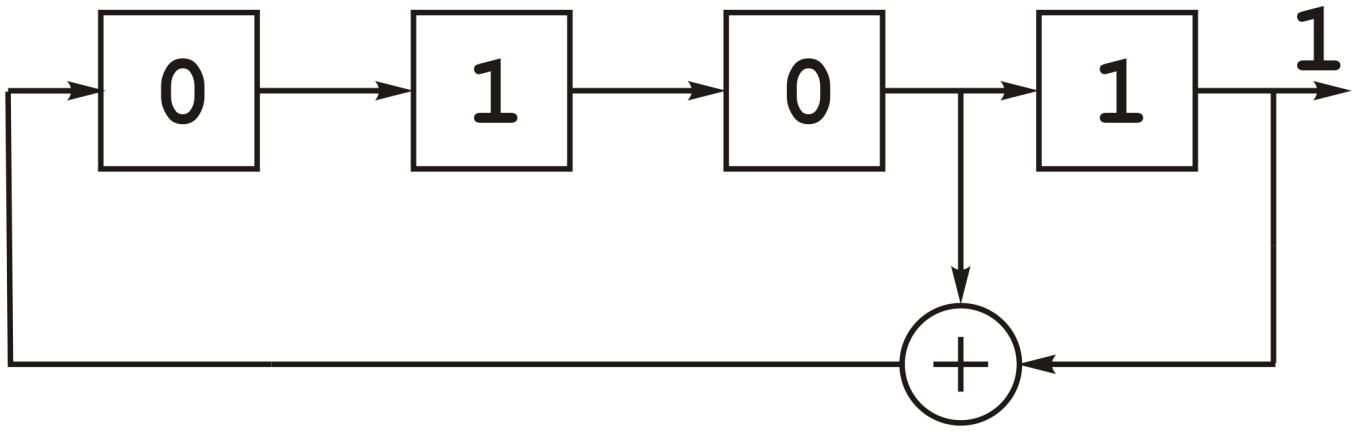
РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

РСЛОС



РСЛОС длины 4 с коэффициентами обратной связи $(c_1, c_2, c_3, c_4) = (0, 0, 1, 1)$ и начальным состоянием $(s_0, s_1, s_2, s_3) = (1, 0, 1, 1)$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_t	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
s_{t+1}	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0
s_{t+2}	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1
s_{t+3}	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1

Линейная сложность

Линейной сложностью последовательности $\{s_n\}_{n=0}^{\infty}$ называется длина L самого короткого регистра сдвига с линейной обратной связью, который может сгенерировать последовательность $\{s_n\}_{n=0}^{\infty}$, при этом первые L знаков последовательности $\{s_n\}_{n=0}^{\infty}$ являются начальным заполнением регистра.
Если последовательность состоит из нулей, то л.с. равняется 0.
Если последовательность не является периодической, то л. с. равна ∞.

Алгоритм Берлекампа-Мэсси

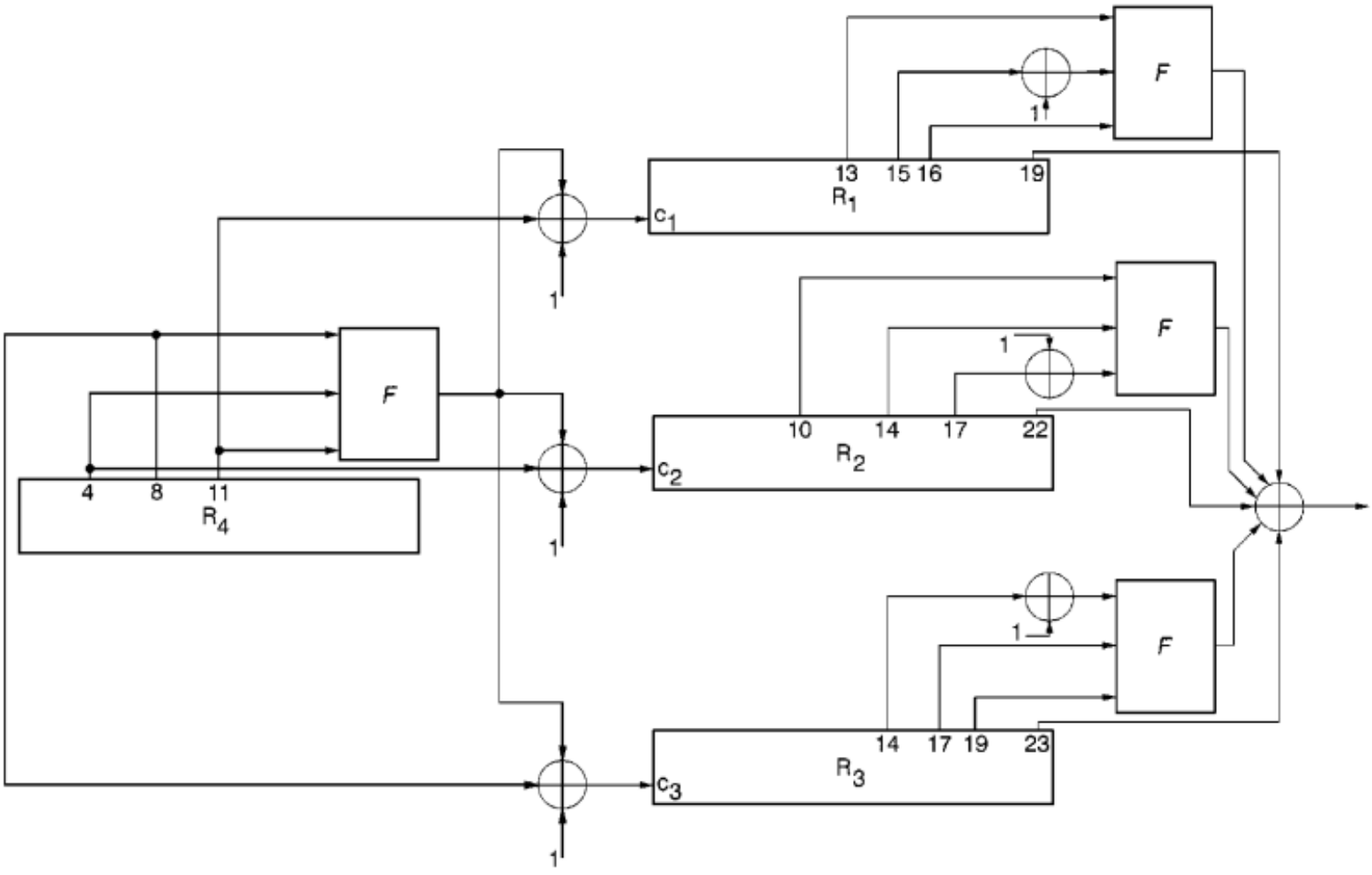
Находит минимальный РСЛОС по $2L$ значениям последовательности.

Решение: несколько РСЛОС-ов, на основе «комбинации» выходных последовательностей которых строится итоговая выходная последовательность.

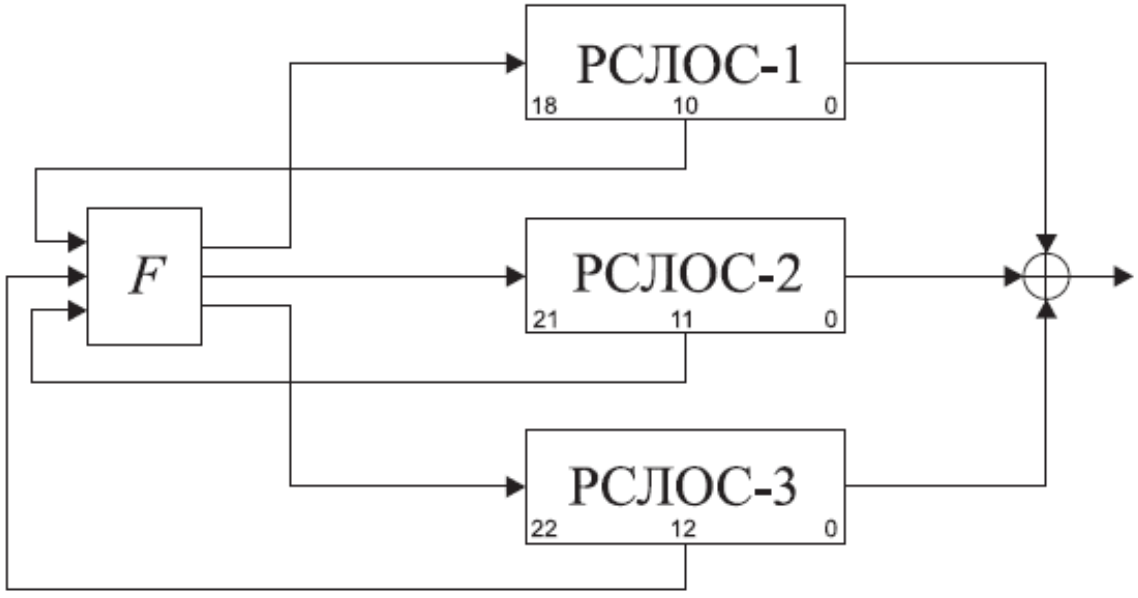
Поточные алгоритмы шифрования на основе РСЛОС

- CSS (Content Scramble System) — система защиты цифрового медиаконтента на DVD-носителяхб
- Алгоритм E0 (протокол bluetooth),
- Алгоритмы семейства A5: A5/1 и A5/2 (gsm 2g),
- Алгоритмы семейства SNOW: SNOW 3g (gsm 3g, LTE), SNOW-V (проект для 5g).

Алгоритм A5/2



Алгоритм A5/1



Неравномерное движение: на каждом такте, сдвигаются два или три регистра.

Постулаты Голомбо

1. Количество "1" в каждом периоде должно отличаться от количества "0" не более, чем на единицу.
2. В каждом периоде половина серий (из одинаковых символов) должна иметь длину один, одна четверть должна иметь длину два, одна восьмая должна иметь длину три и т.д. Более того, для каждой из этих длин должно быть одинаковое количество серий из "1" и "0".
3. Функция автокорреляции должна быть двузначной (это означает, что если последовательность на периоде сравнить с этой же последовательностью, но циклически сдвинутой на любое число битов (не равное нулю или периоду), то число несовпадений будет на единицу больше, чем число совпадений). Это необходимое условие независимости битов последовательности: совпадение последовательности и ее сдвинутых копий не дает информации о периоде.

Батареи статистических тестов

Батарея	Преимущества	Недостатки
Д. Кнут	первая разработанная батарея, является основой для проектирования других батарей	не используется плохие генераторы могут пройти тесты
Diehard	более строгие тесты, более полная, чем у Кнута	фиксированные параметры, ограниченный размер обрабатываемой выборки, фиксированный формат данных
Dieharder	более полная, чем предыдущие, Open source	фиксированные параметры, рекомендуется для проверки случайных чисел, а не битовых последовательностей
NIST	более полная, чем предыдущие, массовое использование	фиксированные параметры, есть зависимости между тестами
TESTU01	реализует большинство известных тестов, гибкость в выборе подмножества тестов	в зависимости от выбранного подмножества тестов, может потребоваться значительное время для вычислений