

ТЕМА № 2.

«Системы шифрования.»

ЗАНЯТИЕ 2/1.

«ПОТОЧНЫЕ СИСТЕМЫ ШИФРОВАНИЯ.»

Учебные вопросы.

1. Синхронизация поточных шифрсистем.
2. Принципы построения поточных шифрсистем.
3. Примеры поточных шифрсистем

1-й учебный вопрос:

**«Синхронизация поточных
шифрсистем»**

При использовании **поточных шифров**
простой замены потеря (или искажение)
отдельных знаков шифрованного текста при
передаче по каналу связи **приводит лишь к**
локальным потерям: все знаки шифртекста,
принятые без искажений, будут
расшифрованы правильно.

Это объясняется тем, что алгоритм
шифрования не зависит ни от расположения
знаков в тексте, ни от их конкретного вида.

По способу решения проблемы
синхронизации процедур зашифрования
и расшифрования, поточные
шифрсистемы делят на:

-синхронные;

- системы с салюсинхронизацией.

Для **синхронных** поточных шифрсистем выбор применяемых шифрующих преобразований **однозначно определяется** **распределителем** и зависит только от **номера такта** шифрования. Каждый знак шифртекста зависит только от соответствующего знака открытого текста и номера такта шифрования и не зависит от того, какие знаки были зашифрованы до или после него. Поэтому применяемое при расшифровании преобразование не зависит от последовательности принятых знаков шифртекста.

В этом случае ***размножение ошибки полностью отсутствует:*** каждый знак, искаженный при передаче, приведет к появлению только одного ошибочно расшифрованного знака.

Обычно *синхронизация достигается* вставкой в передаваемое сообщение *специальных маркеров*. В результате этого знак шифртекста, пропущенный в процессе передачи, приводит к неверному расшифрованию лишь до тех пор, *пока не будет принят один из маркеров*.

Другое решение состоит в *реинициализации состояний*, как шифратора отправителя, так и шифратора получателя при некотором *предварительно согласованном условии*.

Примерами синхронных систем являются регистры сдвига с обратной связью, дисковые шифраторы или шифрмашинка Б. Хагелина С-36.

Наиболее распространенный режим использования шифрсистем с самосинхронизацией — это (уже знакомый нам) режим обратной связи по шифртексту, при котором *текущее состояние системы зависит от некоторого числа N предыдущих знаков шифртекста.*

В этом режиме потерянный в канале знак влияет на N последовательных состояний

После приема N правильных последовательных знаков из канала связи ***состояние приемного шифратора становится идентичным состоянию передающего шифратора.***

2-й учебный вопрос:

**«Принципы построения
поточных шифрсистем»**

Для построения *многоалфавитного
поточного шифра замены* необходимо
указать его *распределитель*,
определяющий порядок использования
шифрующих преобразований, и сами эти
преобразования, то есть *простые
замены, составляющие данный шифр
замены.*

Поточная шифрсистема представляется в виде *двух основных блоков*, отвечающих за выработку распределителя и собственно зашифрование очередного знака открытого текста.

Первый блок вырабатывает *последовательность номеров шифрующих преобразований*, то есть фактически управляет порядком процедуры шифрования. Поэтому этот блок называют *управляющим блоком*, а вырабатываемую им последовательность номеров преобразований — *управляющей последовательностью* (или *управляющей гаммой*).

Второй блок в соответствии со знаком управляющей последовательности *реализует собственно алгоритм зашифрования текущего знака.*

В связи с этим этот блок называют **шифрующим блоком.**

Требования к управляющему блоку:

- период управляющей гаммы должен превышать максимально возможную длину открытых сообщений, подлежащих шифрованию;
- статистические свойства управляющей гаммы должны приближаться к свойствам случайной равновероятной последовательности;
- в управляющей гамме должны отсутствовать простые аналитические зависимости между близко расположенными знаками;
- криптографический алгоритм получения знаков управляющей гаммы должен обеспечивать высокую сложность определения секретного ключа.

Требование к шифрующему блоку:

- применение алгоритма шифрования должно носить универсальный характер, не зависеть от вида шифруемой информации.

Иногда выдвигается *дополнительное требование:*

- способ построения шифрующего блока должен обеспечивать криптографическую стойкость шифра при перекрытиях управляющей гаммы, в частности при повторном использовании ключей.

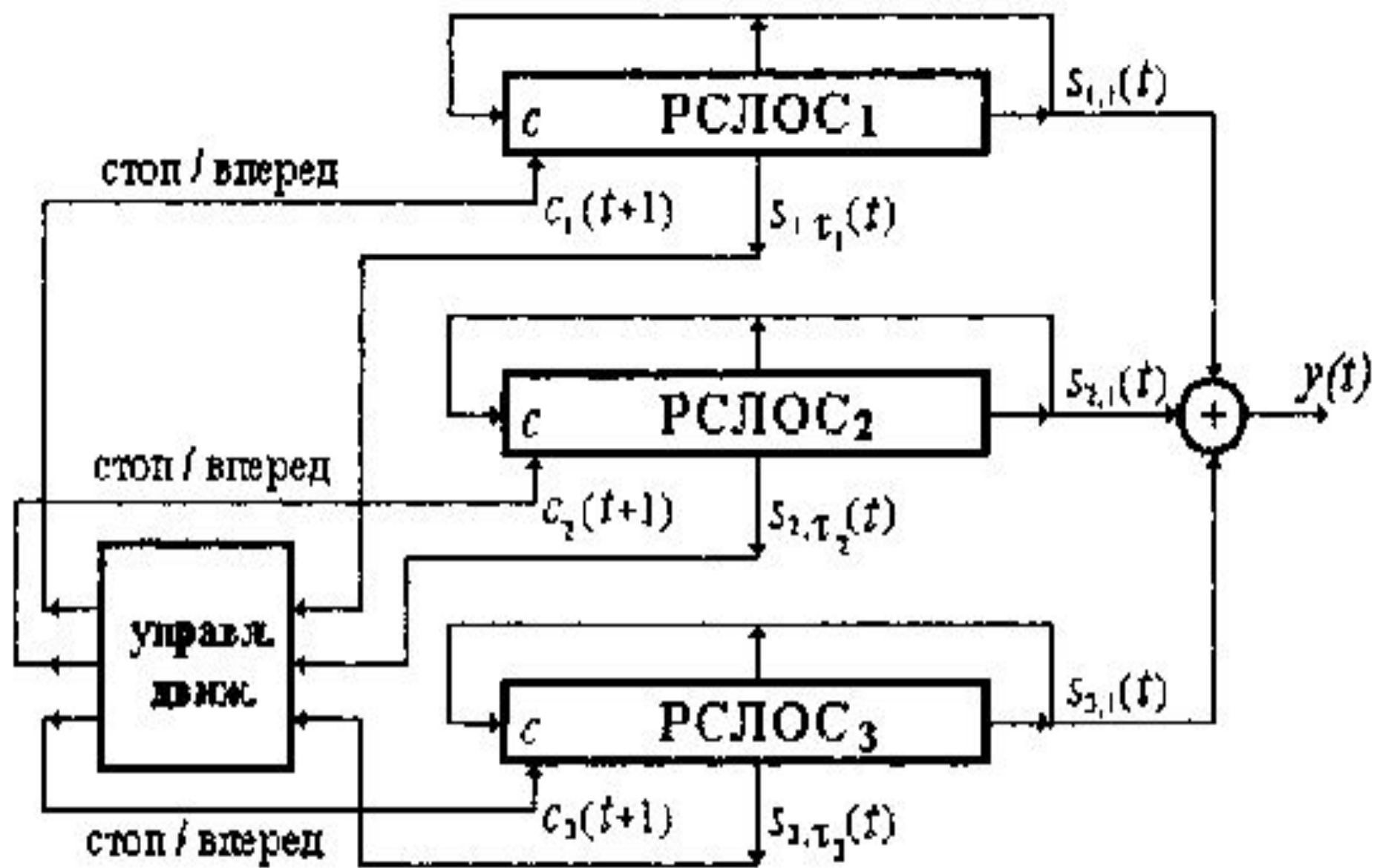
3-й учебный вопрос:

**«Примеры поточных
шифрсистем»**

A5 — шифрсистема гаммирования,
применяемая для шифрования
телефонных сеансов в европейской
системе мобильной цифровой связи *GSM*
(*Group Special Mobile*).

В открытой печати криптосхема A5
официально не публиковалась.

Британская телефонная компания
передала всю техническую
документацию Брэдфордскому
университету.



Криптосхема А5

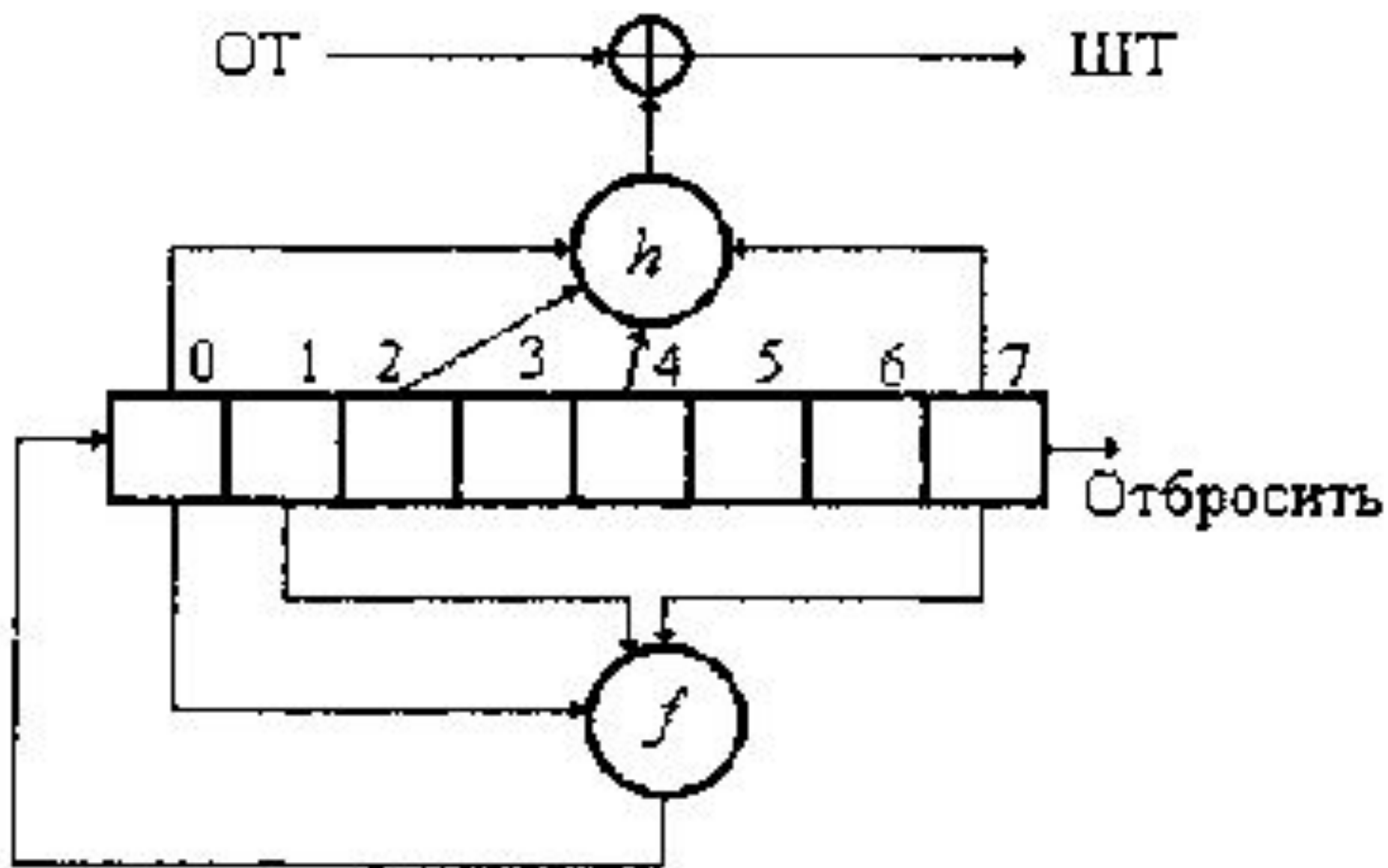
Знаки управляющей движением последовательности $C(t)$ определяют, какие регистры сдвигаются в t -м такте работы схемы. Ясно, что в каждом такте сдвигаются, по меньшей мере, два регистра.

Выходной бит гаммы $y(t)$ вычисляется как сумма $y(t) = s_{1,1}(t) + s_{2,1}(t) + s_{3,1}(t), t \geq 1$.

Д. Гиффорд предложил схему *поточного шифра*, которая использовалась с 1984 по 1988 г. агентством Associated Press.

Криптосхема генератора представляет собой 8- байтовый регистр сдвига с линейной функцией обратной связи f и нелинейной функцией выхода h . Ключом являются 64 бита начального заполнения регистра.

Схема реализует шифр гаммирования.

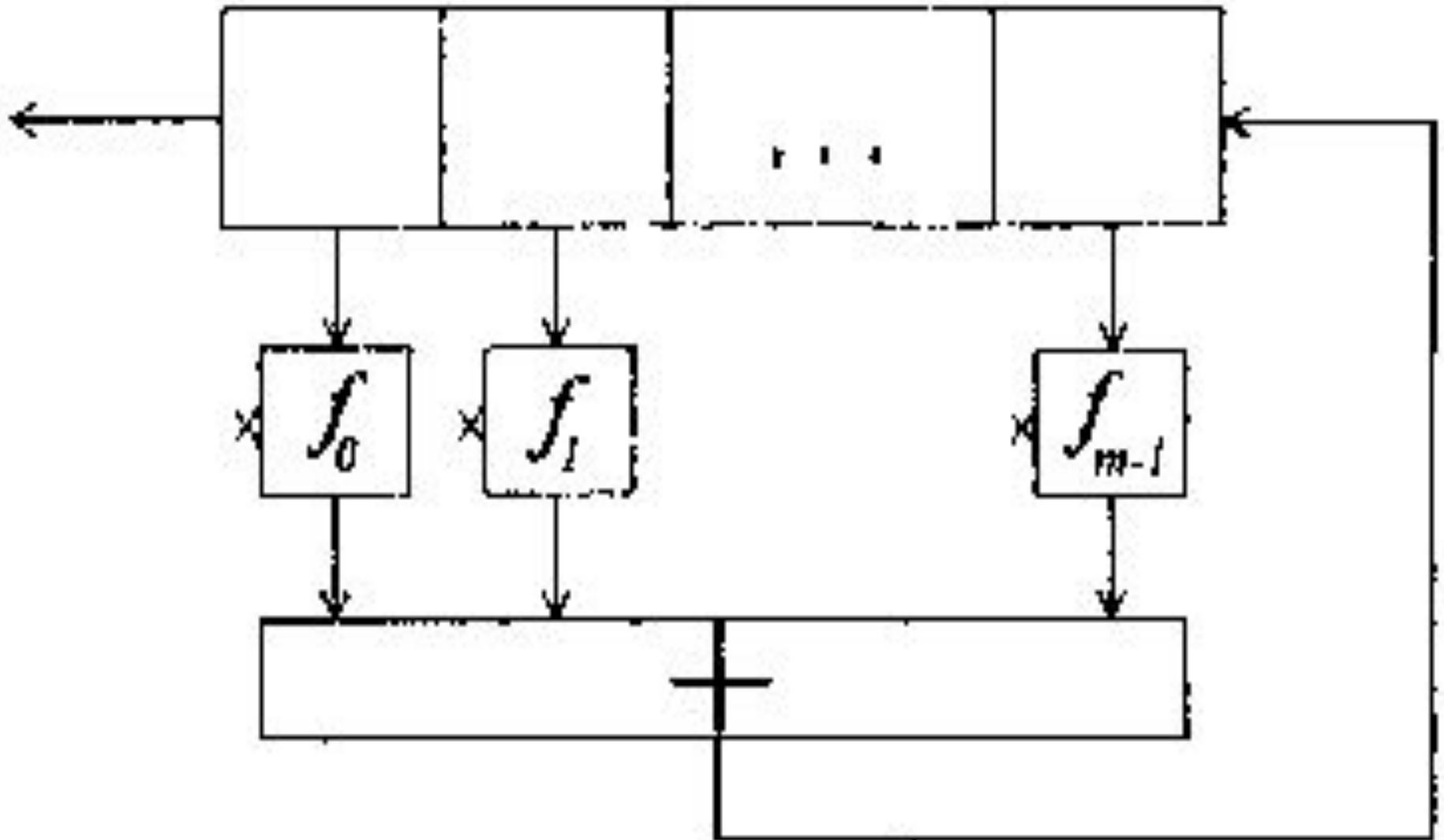


Генератор Гиффорда

Широкое распространение в криптографических приложениях линейных регистров сдвига над конечными полями и кольцами обусловлено целым рядом факторов. Среди них можно отметить:

- использование только простейших операций сложения и умножения, аппаратно реализованных практически на всех вычислительных средствах;
- высокое быстродействие создаваемых на их основе криптографических алгоритмов;
- большое количество теоретических исследований свойств линейных рекуррентных последовательностей (ЛРП), свидетельствующих об их удовлетворительных криптографических свойствах.

Схема линейного регистра сдвига



В очередном такте работы регистра значения, содержащиеся в ячейках его накопителя, умножаются на соответствующие коэффициенты (f_j) и суммируются, после чего происходит (левый) сдвиг информации в регистре, а в освободившуюся крайнюю ячейку записывается вычисленное значение суммы. Заметим при этом, что операции сложения и умножения выполняются в поле P .

Последовательности, в которых каждый член, начиная с некоторого, выражается через предыдущие, часто встречаются в математике и

*называются **рекуррентными** (от латинского recurrere – возвращаться)* или **возвратными**.*

*Процесс вычисления членов этих последовательностей называется **рекуррентным процессом**.*