Поточные шифры (потоковые)

Введение

- Потоковые шифры на базе сдвиговых регистров активно использовались в годы войны, ещё задолго до появления электроники. Они были просты в проектировании и реализации.

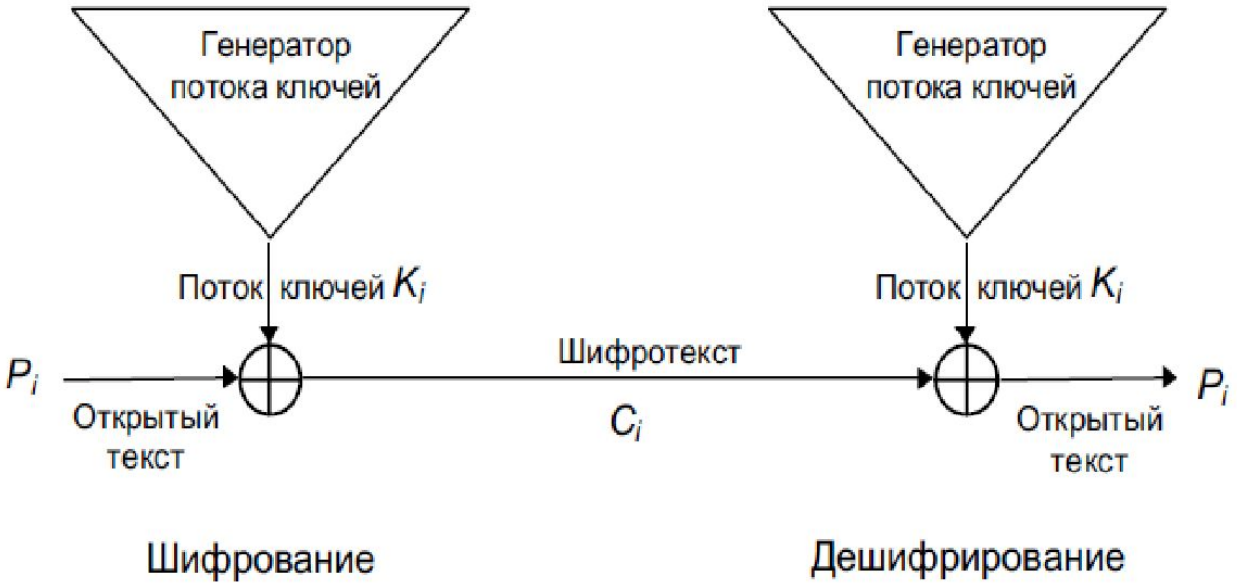
- В 1965 году Эрнст Селмер, главный криптограф норвежского правительства, разработал теорию последовательности сдвиговых регистров. Позже Соломон Голомб, математик Агентства Национальной Безопасности США, написал книгу под названием «Shift Register Sequences»(« Последовательности сдвиговых регистров»), в которой изложил свои основные достижения в этой области, а также достижения Селмера.

- Большую популярность потоковым шифрам принесла работа Клода Шеннона, опубликованная в 1949 году, в которой Шеннон доказал абсолютную стойкость шифра Вернама (также известного, как одноразовый блокнот). В шифре Вернама ключ имеет длину, равную длине самого передаваемого сообщения. Ключ используется в качестве гаммы, и если каждый бит ключа выбирается случайно, то вскрыть шифр невозможно (т.к. все возможные открытые тексты будут равновероятны). До настоящего времени было придумано немало алгоритмов потокового шифрования. Такие как: A3, A5, A8, RC4,PIKE, SEAL, eSTREAM.

Введение

- *Шифр Вернама –шифр-блокнот*

Введение


Генератор потока ключей
Поток ключей K_i
P_i
Открытый текст
Шифротекст
C_i
Генератор потока ключей
Поток ключей K_i
P_i
Открытый текст
Шифрование
Дешифрирование

Введение

- Шифротекст

$$c_i = p_i \oplus k_i$$

- Дешифрование

При дешифрировании операция XOR выполняется над битами шифротекста и тем же самым потоком ключей для восстановления битов открытого текста.

$$p_i = c_i \oplus k_i$$

Так как

$$p_i \oplus k_i \oplus k_i = p_i$$

это работает правильно.

Введение

- Взлом

$$C_1 \oplus C_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2.$$

- Свойства генератора ключевого
  - Иметь большой период. Поскольку ключевой поток получается в результате детерминированного процесса из основного ключа, найдется такое число n, что $k_i = k_i + n$ для всех значений i. Число n называется периодом последовательности, и для обеспечения стойкости шифра выбирается достаточно большим.

Введение

- Иметь псевдо-случайные свойства. Генератор должен производить последовательность, которая кажется случайной. Другими словами, генерируемая последовательность должна выдержать определенное число статистических тестов на случайность.
- Обладать линейной сложностью.

Определение 5.2. *Линейной сложностью* бесконечной последовательности битов

$$s = s_0, s_1, s_2, s_3, \ldots ,$$

называется величина $L(s)$, равная

- 0, если s — последовательность нулей,
- ∞, если s нельзя получить с помощью какого-нибудь $РСЛОС$,
- длине наименьшего $РСЛОС$, выдающего последовательность s в остальных случаях.

Введение

- Потеря бита (опасно)
- Искажения бита (безопасно)

Синхронные поточные шифры

- *Синхронные поточные шифры (СПШ) — шифры, в которых поток ключей генерируется независимо от открытого текста и шифротекста.*

- При шифровании генератор потока ключей выдаёт биты потока ключей, которые идентичны битам потока ключей при дешифровании. Потеря знака шифротекста приведёт к нарушению синхронизации между этими двумя генераторами и невозможности расшифрования оставшейся части сообщения. Очевидно, что в этой ситуации отправитель и получатель должны повторно синхронизоваться для продолжения работы.

Плюсы СПШ:

- отсутствие эффекта распространения ошибок (только искажённый бит будет расшифрован неверно);
- предохраняют от любых вставок и удалений шифротекста, так как они приведут к потере синхронизации и будут обнаружены.

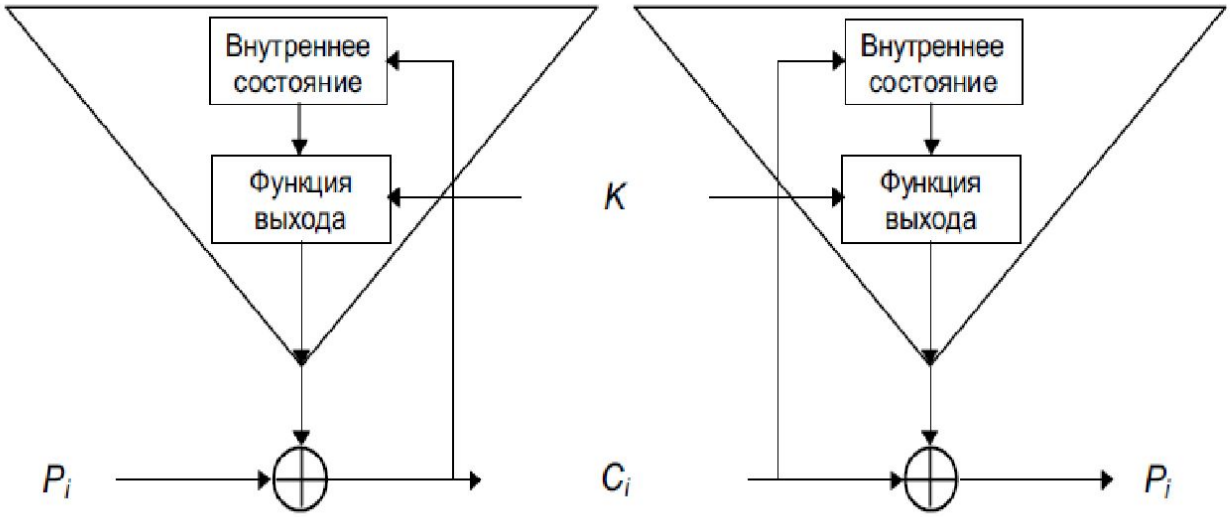
Минусы СПШ:

- уязвимы к изменению отдельных бит шифрованного текста. Если злоумышленнику известен открытый текст, он может изменить эти биты так, чтобы они расшифровывались, как ему надо.

Самосинхронизирующиеся поточные шифры

- *Самосинхронизирующиеся поточные шифры (асинхронные поточные шифры (АПШ)) – шифры, в которых поток ключей создаётся функцией ключа и фиксированного числа знаков шифротекста.*

Военные называют этот шифр **автоключом шифротек-**
ста (ciphertext auto key, CTAK). Основная идея была запатентована в 1946



Самосинхронизирующиеся поточные шифры

Так как внутреннее состояние полностью зависит от предыдущих *n* шифротекста, дешифрирующий генератор потока ключей автоматически синхронизируется с шифрующим генератором потока ключей, приняв *n* битов шифротекста.

В интеллектуальных реализациях этого режима каждое сообщение начинается случайным заголовком дл иной *n* битов. Этот заголовок шифруется, передается и затем расшифровывается . Расшифровка будет неправильной, но после этих *n* битов оба генератора потока ключей будут синхронизированы .

Слабой стороной самосинхронизирующегося потокового шифра является распространение ошибки . Для каждого бита шифротекста, испорченного при передаче, дешифрирующий генератор потока ключей выдает *n* неправильных битов потока ключей. Следовательно, каждому неправильному биту шифротекста соответствуют *n* ошибок в открытом тексте, пока испорченный бит не перестанет влиять на внутреннее состояние .

Самосинхронизирующиеся поточные шифры

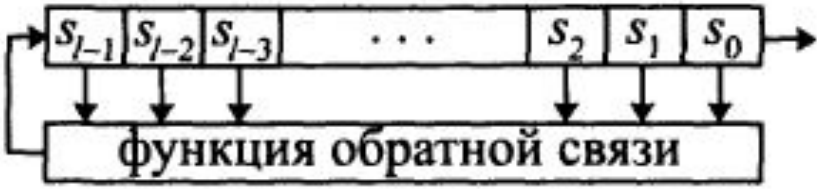
Плюсы АПШ:

- Размешивание статистики открытого текста. Так как каждый знак открытого текста влияет на следующий шифротекст, статистические свойства открытого текста распространяются на весь шифротекст. Следовательно, АПШ может быть более устойчивым к атакам на основе избыточности открытого текста, чем СПШ.

Минусы АПШ:

- распространение ошибки (каждому неправильному биту шифротекста соответствуют N ошибок в открытом тексте);
- чувствительны к вскрытию повторной передачей.

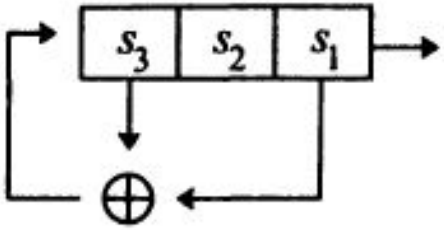
РСЛОС



Свойства выдаваемой *РСЛОС* последовательности тесно связаны со свойствами двоичного многочлена

$$C(X) = 1 + c_1 X + c_2 X^2 + \cdots + c_l X^l \in \mathbb{F}_2[X],$$

РСЛОС



$$X^3+X+1,$$

$$[0, 0, 1]$$

РСЛОС

Номер шага	состояние	генерируемый бит
0	[0,0,1]	-
1	[1,0,0]	1
2	[1,1,0]	0
3	[1,1,1]	0
4	[0,1,1]	1
5	[1,0,1]	1
6	[0,1,0]	1
7	[0,0,1]	0

Комбинирование РСЛОС

$$f(x_1, x_2, x_3, x_4, x_5) = 1 \oplus x_2 \oplus x_3 \oplus x_4 \cdot x_5 \oplus x_1 \cdot x_2 \cdot x_3 \cdot x_5.$$

RC4

Используется S-блок размером 8*8: $S_0, S_1, \ldots, S_{255}$. Элементы представляют собой перестановку чисел от 0 до 255, а перестановка является функцией ключа переменной длины. В алгоритме применяются два счетчика, i и j, с нулевыми начальными значениями.

Для генерации случайного байта выполняется следующее:

$i = (i + 1) \bmod 256$

$j = (j + S_i) \bmod 256$

поменять местами S_i и Sj

$t = (S_i + S_j) \bmod 256$

$K = S_t$

Байт K используется в операции XOR с открытым текстом для получения шифротекста или в операции XOR с шифротекстом для получения открытого текста. Шифрование выполняется примерно в 10 раз быстрее, чем DES.

RC4

Также несложна и инициализация S-блока. Сначала заполним его линейно: $S_0 = 0, S_1 = 1, \ldots, S_{255} = 255$. Затем заполним ключом другой 256-байтовый массив, при необходимости для заполнения всего массива повторяя ключ: $K_0, K_1, \ldots, K_{255}$. Установим значение индекса j равным 0. Затем:

for $i = 0$ to 255:

$j = (j + S_i + K_i) \bmod 256$

поменять местами S_i и S_j

A5

- Основные детали алгоритма A5 известны. Британская телефонная компания передала всю техническую документацию Брэдфордскому университету, забыв заключить соглашение о неразглашении информации. Поэтому детали о конструкции A5 понемногу стали просачиваться в печать, и в конце концов кто-то опубликовал схему в INTERNET

- Аутентификация – процедура входа в систему с предоставлением идентификационных данных. Является необходимым условием обеспечения секретности обмена данными. Пользователи должны иметь возможность подтвердить свою подлинность и проверить идентификацию других пользователей, с которым они общаются. Цифровой сертификат является распространенным средством

  идентификации

- Аутентифика́ция (англ. Authentication) — процедура проверки подлинности

Аутентификацию не следует путать с авторизацией (процедурой предоставления субъекту определённых прав) и идентификацией (процедурой распознавания субъекта по его идентификатору).

A5

2 РАЗВИТИЕ GSM

Стандарт является одним из первых цифровых систем цифровой мобильной связи, пришедший на смену аналоговым.

Развитие GSM началось в 1982 году, когда была создана Groupe Speciale Mobile, организация прогнозирования и исследования систем сотовой связи в Европе. В 1987 проведены испытания ряда систем, которые включили проверки спектральной эффективности, качества речи и радио-интерфейса, а в январе 1992 года с запуском первой сети GSM в Финляндии аббревиатура получила современную расшифровку. К концу года число сетей выросло до 14. На следующий год сеть была запущена неевропейской компанией. Такое бурное развитие послужило к закреплению за стандартом нового диапазона 1800МГц (изначально был тока 900МГц).

С 2002 году поддержку стандарта осуществляет 3GPP (3rd Generation Partnership Project).

Аутентификация

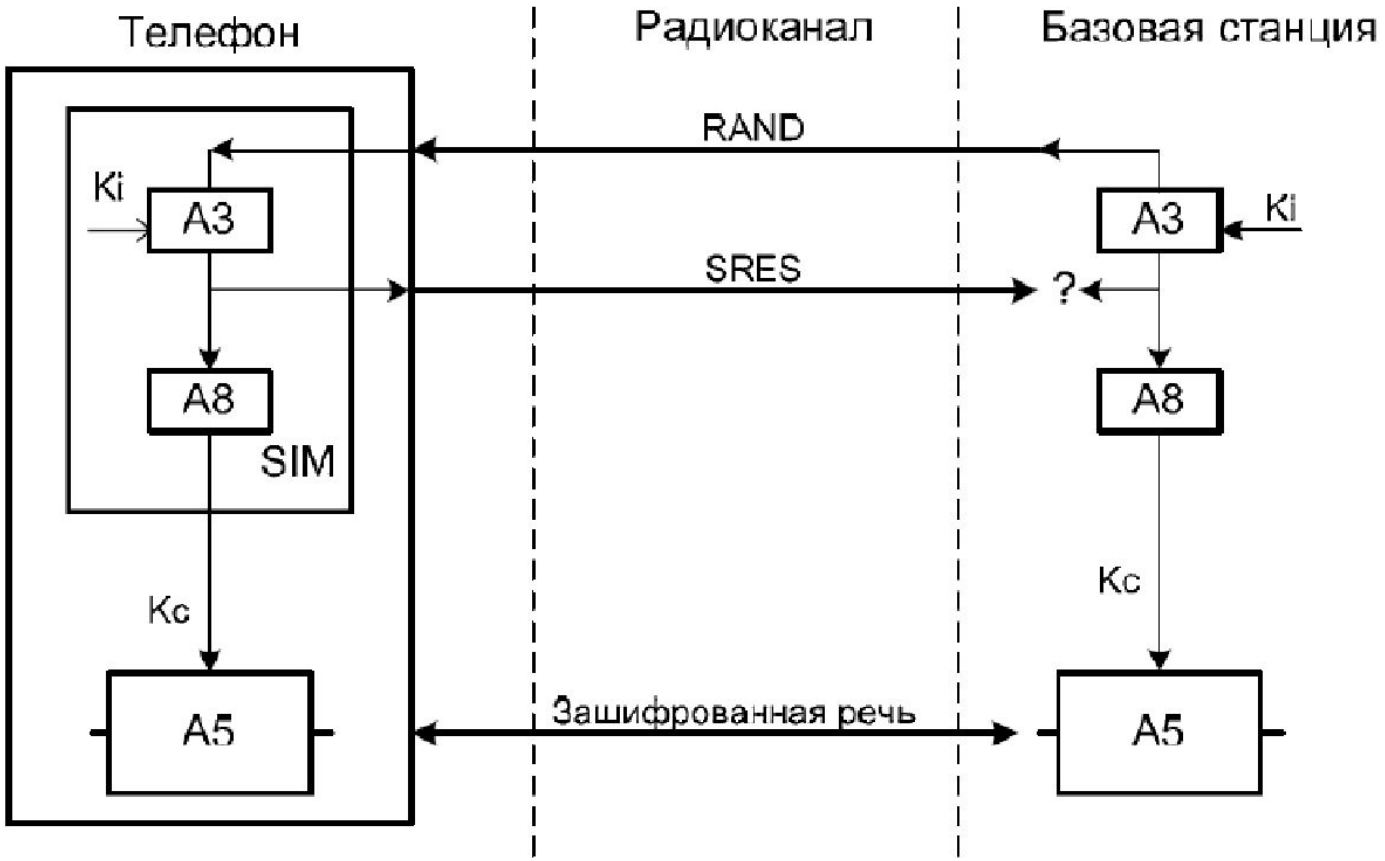
Позволяет избежать клонирования мобильного телефона абонента. Для этого абоненту выдается временный международный ид-й номер пользователя IMSI, который действителен только в пределах зоны расположения а так же индивидуальный 128-битный ключ авторизации Ki. Схемы спроектированы так, что ни одно из этих значений напрямую через радио канал не передается.

Ключ Ki известен обоим сторонам.

В аутентификации используется SIM-карта и Центр Авторизации (Authentication Center AuC).

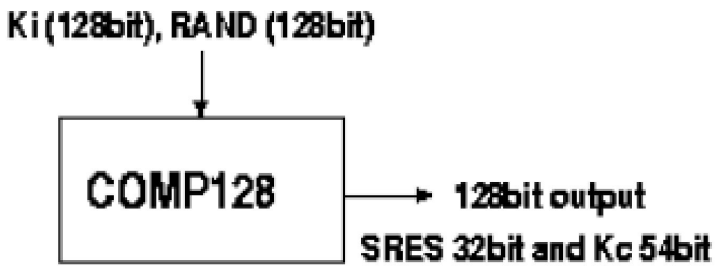
Auc генерирует 128 битовое значение RAND и посылает мобильной станции, в ответ получает 32-битное значение SRES=A3(RAND, Ki) которое сравнивает с вычисленным самостоятельно тем же алгоритмом A3. В мобильной станции A3 прошит в SIM-карте.

A5


Телефон
Радиоканал
Базовая станция
RAND
Ki
A3
A3
Ki
SRES
?
A8
A8
SIM
Kc
Kc
A5
Зашифрованная речь
A5

Сеансовый ключ

На мобильной станции производится алгоритмом A8, вновь используя полученный RAND и имеющийся Ki. Сеансовый ключ Kc вычисляется и в AuC.
С этого момента радиоканал считает шифрованным.
Сегодня реализация A3\A8 в основном использует алгоритм COMP128, который сразу вычисляет и SRES и Kc значение(см рис). Ключ Kc имеет длину 64 бит, образуется добавлением к 54 битам, полученным данным алгоритмом, десяти нулевых битов – это значение и является входом для алгоритма шифрования A5 разговора.
В мобильной станции A8 также как и A3 прошит в SIM-карте.



Осуществляется алгоритмом A5 по кадрам, который в качестве параметров шифрования получает сеансовый ключ Kc и 22-битный номер кадра Frame, а на выходе каждому кадру соответствует 114-битовая кодовая последовательность. Сеансовый ключ может использоваться несколько дней, т.к. аутентификация является необязательным действием при звонке по телефону.
Т.о. для дешифрации аналитик должен знать номер кадра и Kc.

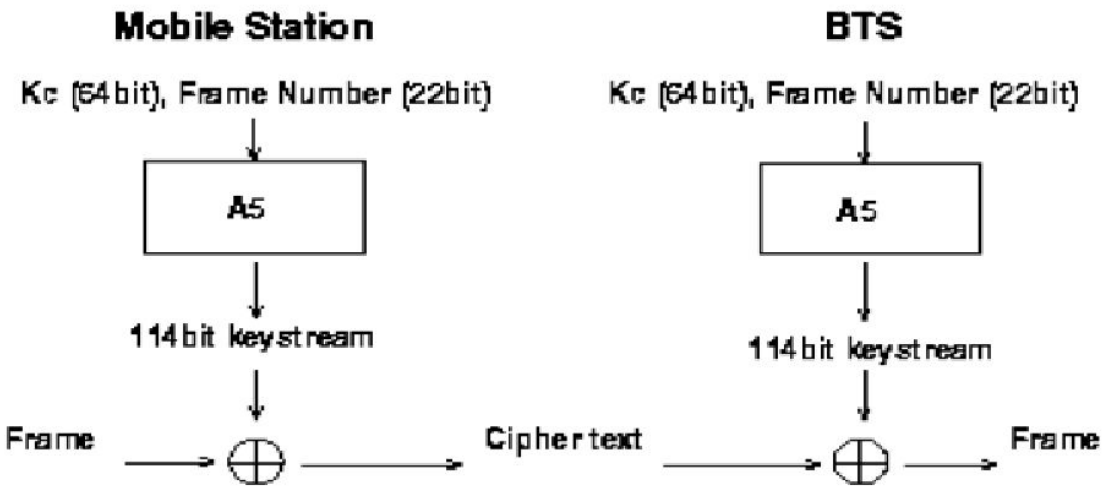
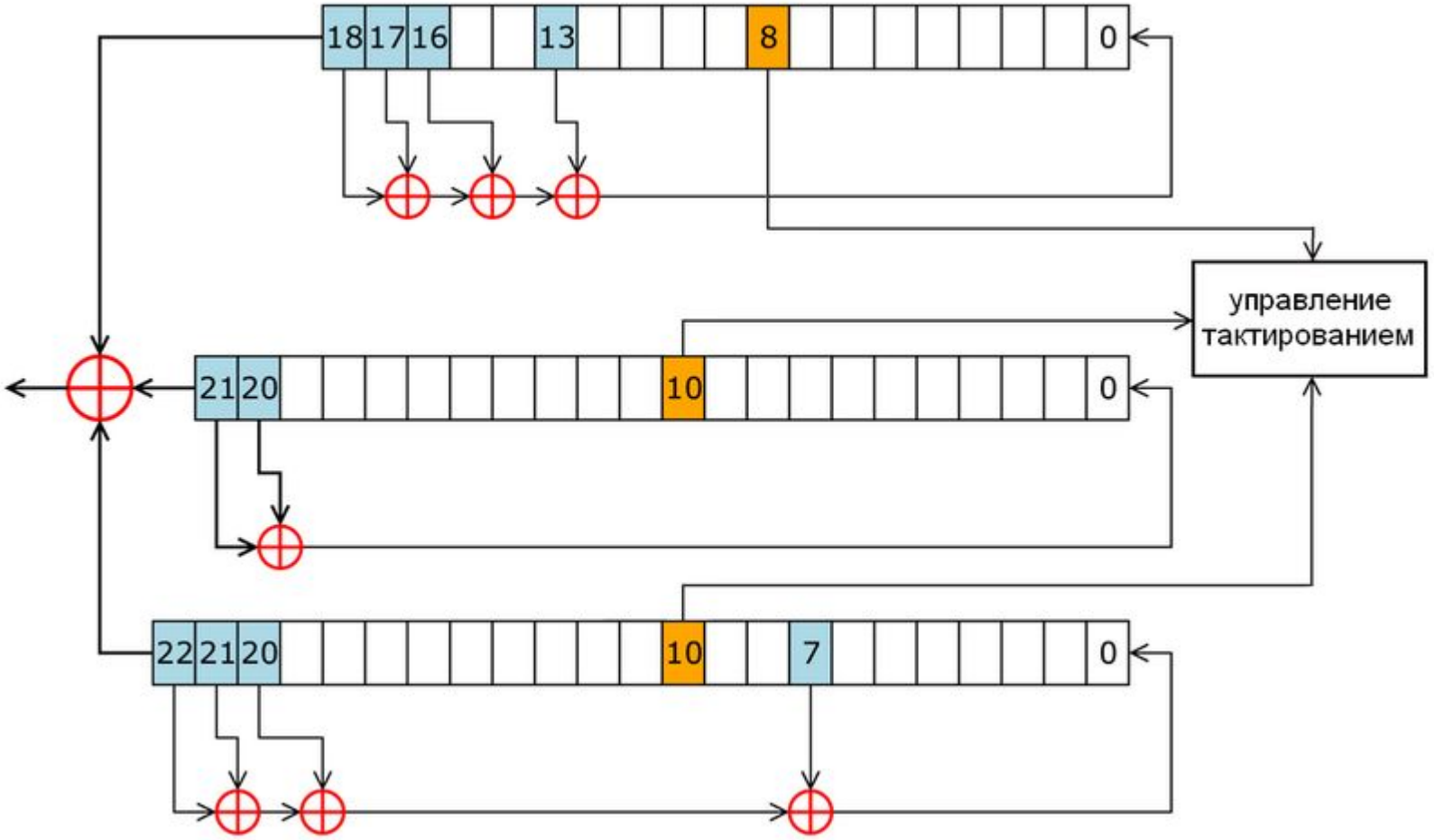


Схема алгоритма A5 используемого в европейских странах содержит 3 LSFR различной длины (19, 22, 23 бита), суммарной длиной в 64 бита. Для получения очередного бита ключевой последовательности, выходы всех регистров складываются по модулю 2. Все 3 регистра имеют управление сдвигом, т.е. можно запретить сдвиг по очередному сигналу тактового генератора.


18
17
16
13
8
0
управление
тактированием
21
20
10
0
22
21
20
10
7
0

- Структура алгоритма A5 выглядит следующим образом:
- три регистра(R1, R2, R3) имеют длины 19, 22 и 23 бита,
- многочлены обратных связей:
  - X19 + X18 + X17 + X14 + 1 для R1,
  - X22 + X21 + 1 для R2 и
  - X23 + X22 + X21 + X8 + 1 для R3,
- управление тактированием осуществляется специальным механизмом:
  - в каждом регистре есть биты синхронизации: 8 (R1), 10 (R2), 10 (R3),
  - вычисляется функция F = x&y|x&z|y&z, где & — булево AND, | - булево OR, а x, y и z — биты синхронизации R1, R2 и R3 соответственно,
  - сдвигаются только те регистры, у которых бит синхронизации равен F,
  - фактически, сдвигаются регистры, синхробит которых принадлежит большинству,
- выходной бит системы — результат операции XOR над выходными битами регистров.

$\mathbb{P}$ — множество возможных открытых текстов, т. е. пространство сообщений;

$\mathbb{K}$ — совокупность возможных ключей;

$\mathbb{C}$ — множество шифротекстов.

Теорема 4.4. (Шеннон.) Пусть набор

$$(\mathbb{P}, \mathbb{C}, \mathbb{K}, e_k(\cdot), d_k(\cdot))$$

обозначает симметричную криптосистему, в которой $\#\mathbb{P} = \#\mathbb{C} = \#\mathbb{K}$. Она обладает абсолютной стойкостью тогда и только тогда, когда

- использование всех ключей равновероятно, т. е. $p(K = k) = \frac{1}{\#\mathbb{K}}$ $\forall k \in \mathbb{K}$;
- для каждой пары $m \in \mathbb{P}$ и $c \in \mathbb{C}$ существует единственный ключ k, такой что $e_k(m) = c$.