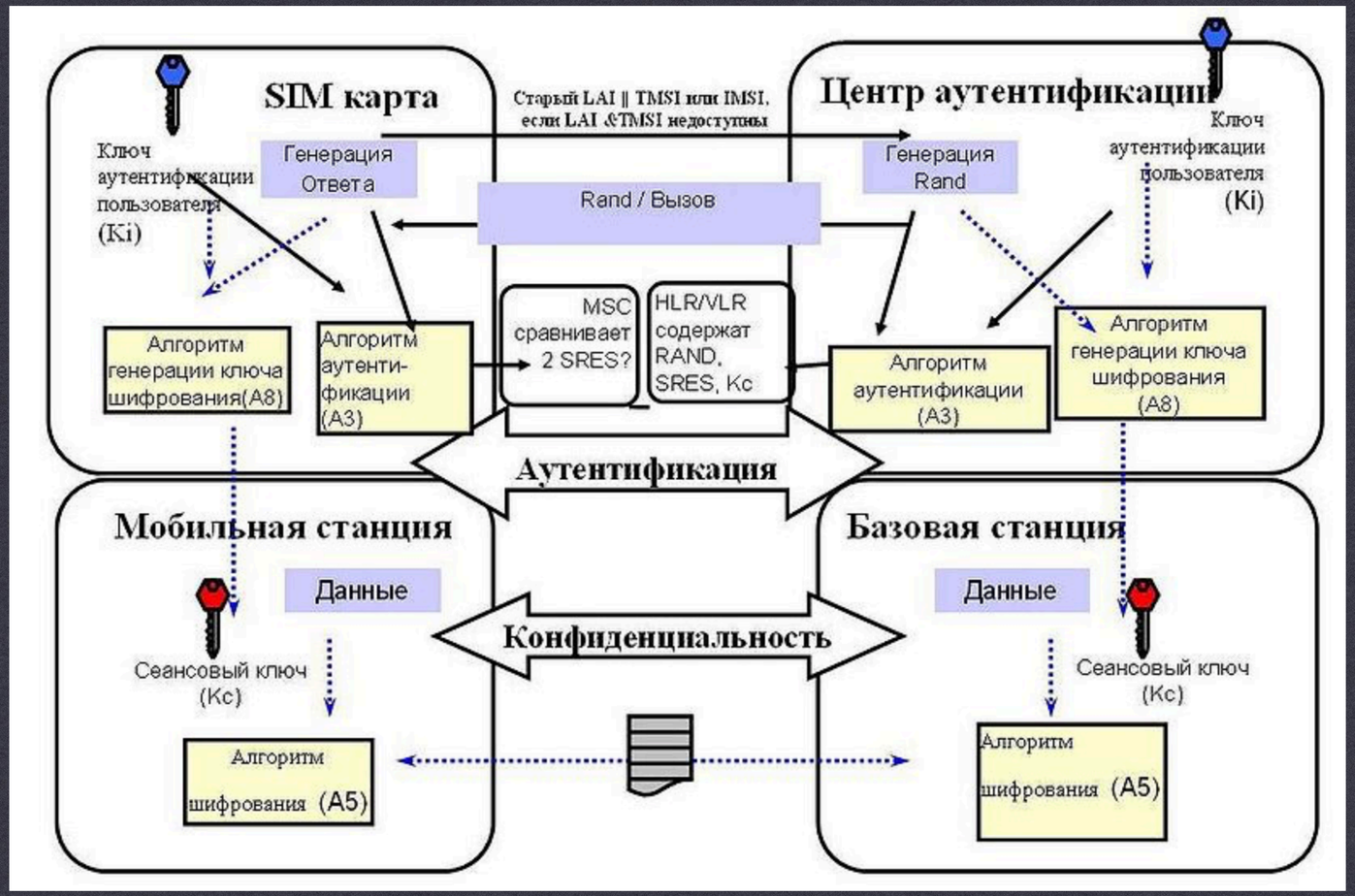
КРИПТОГРАФИЯ В СЕТЯХ GSM.
A5/1 VS A5/2

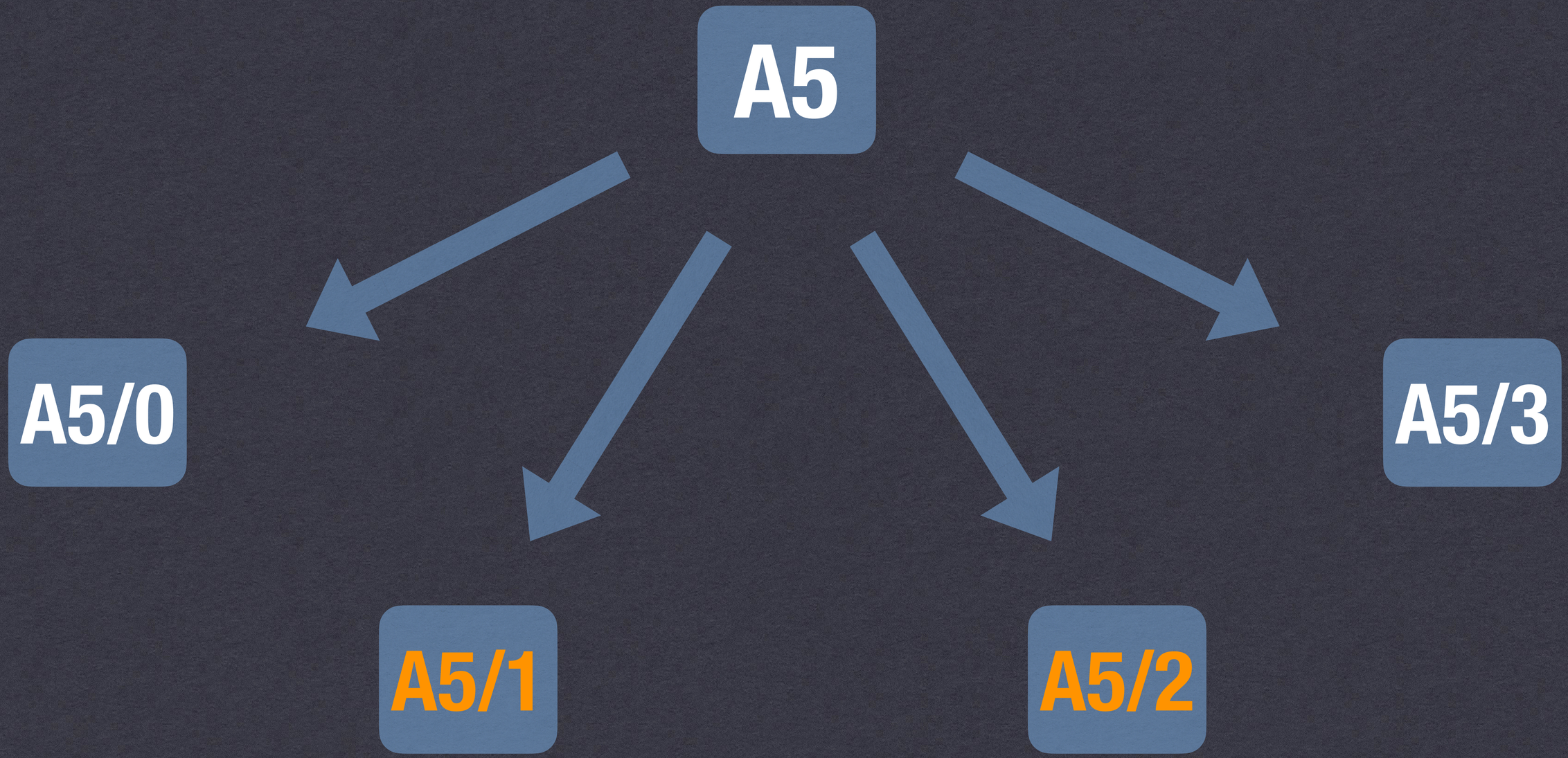
ПОДГОТОВИЛА ТРИФОНОВА НАДЕЖДА.

A5 — это поточный алгоритм шифрования, используемый для обеспечения конфиденциальности передаваемых данных между телефоном и базовой станцией в европейской системе мобильной цифровой связи GSM.

ИСТОРИЯ СОЗДАНИЯ И РАЗВИТИЯ

- A3 - аутентификации,
- A5 - шифрования потока,
- A8 - генерации сеансового ключа.



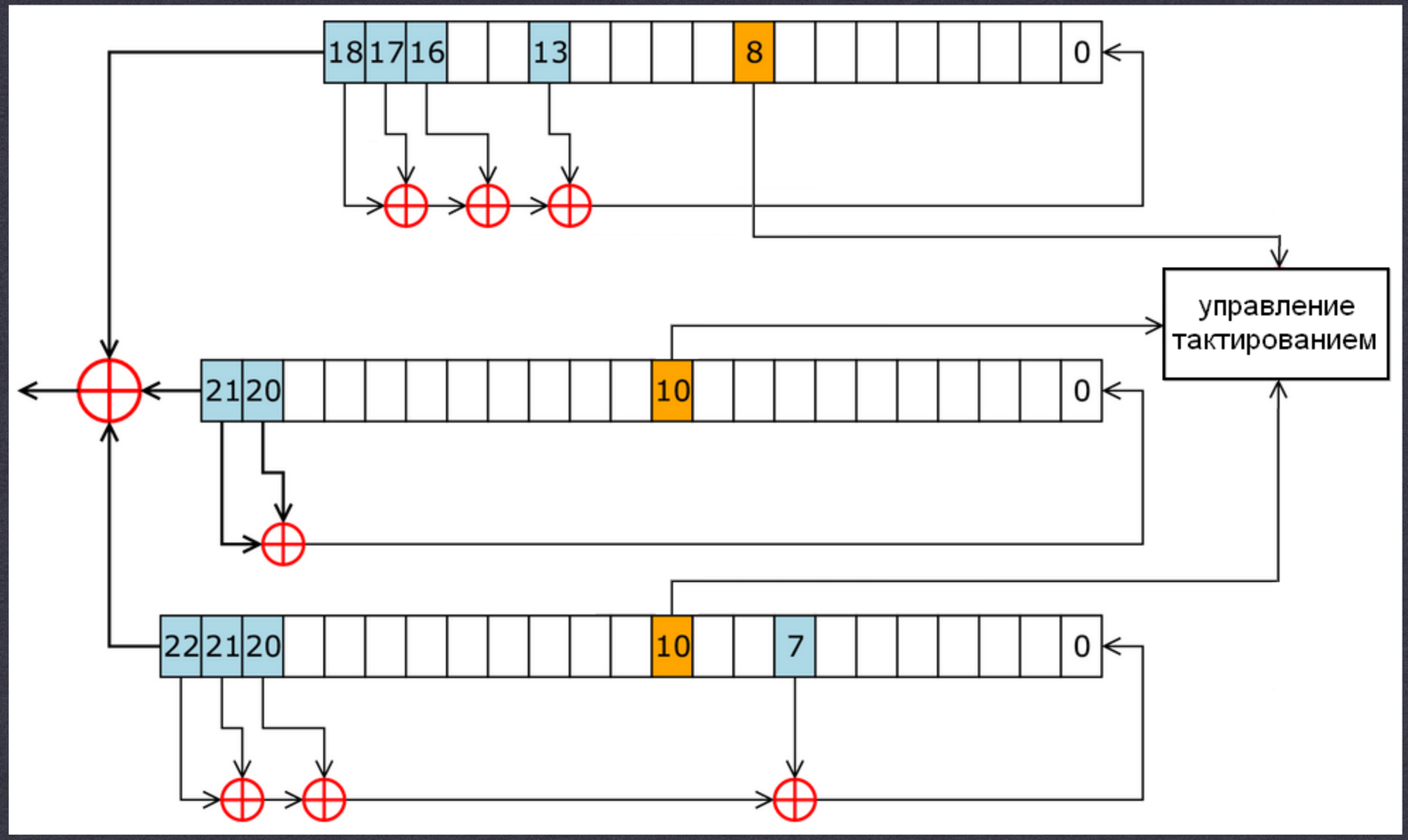

A5
A5/0
A5/1
A5/2
A5/3

АЛГОРИТМ ШИФРОВАНИЯ A5/1

$$x^{19} + x^{18} + x^{17} + x^{14} + 1$$

$$x^{22} + x^{21} + 1$$

$$x^{23} + x^{22} + x^{21} + x^{8} + 1$$



УПРАВЛЕНИЕ ТАКТИРОВАНИЕМ

- Биты синхронизации: 8 (R1), 10 (R2), 10 (R3),
- Вычисляется функция F = x&y|x&z|y&z,
- Сдвигаются только те регистры, у которых бит синхронизации равен F.

ФУНКЦИОНИРОВАНИЕ АЛГОРИТМА A5/1

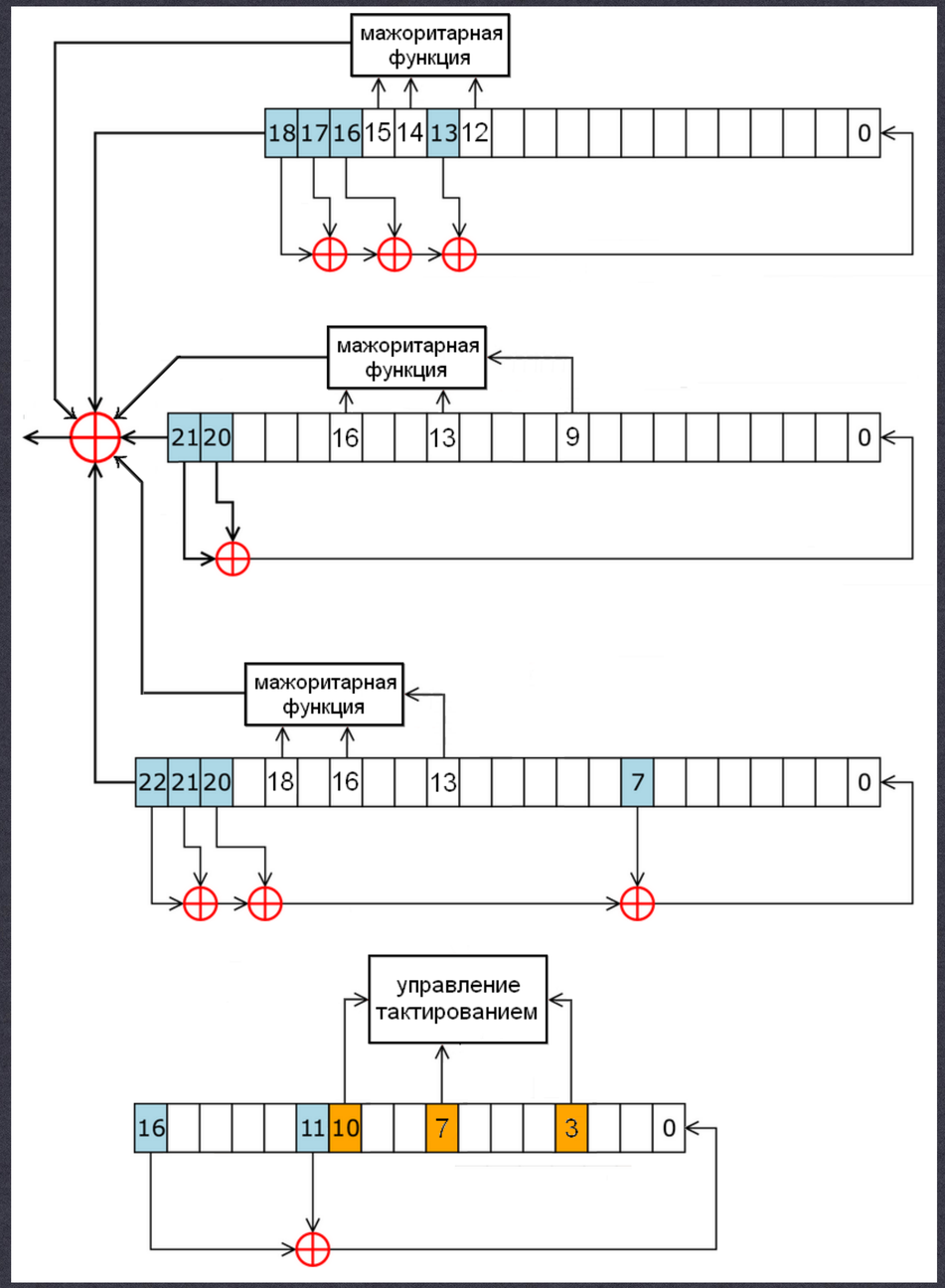
Инициализация

- 64 такта, при которых очередной бит ключа XOR-ится с младшим битом каждого регистра,
- аналогичные 22 такта, только операция XOR производится с номером кадра,
- 100 тактов с управлением сдвигами регистров, но без генерации последовательности.

АЛГОРИТМ A5/2

- Добавлен регистр R4 с длиной 17 бит
- Многочлен обратной связи для R4:

$$x^{17} + x^{12} + 1$$



УПРАВЛЕНИЕ ТАКТИРОВАНИЕМ

- В R4 биты 3, 7, 10 есть биты синхронизации,
- Вычисляется функция F = x&y|x&z|y&z,
- R1 сдвигается, если R4(10) = F,
- R2 сдвигается, если R4(3) = F,
- R3 сдвигается, если R4(7) = F.

Выходной бит системы — результат операции XOR над старшими битами регистров и функций от определённых битов регистров:

1. R1 — 12, 14, 15,
2. R2 — 9, 13, 16,
3. R3 — 13, 16, 18.

ИЗМЕНЕНИЯ В ФУНКЦИОНИРОВАНИИ

Инициализация

- 64 + 22 тактов заполняются сеансовым ключом и номером кадра,
- 1 такт R4(3), R4(7) и R4(10) заполняются 1,
- 99 тактов с управлением сдвигами регистров, но без генерации последовательности.

УЯЗВИМОСТИ

- 10 бит ключа занулены,
- отсутствие перекрестных связей между регистрами,
- шифрование служебной информации,
- свыше 40 % ключей приводит к длине периода $\frac{4}{3}(2^{23} - 1)$
- в начале сеанса осуществляется обмен нулевыми сообщениями,
- одинаковое дополнение (padding) для всех пакетов,
- в A5/2 движение осуществляется отдельным регистром.

АТАКИ

Прямой перебор

2^{64}

Зануление 10 бит

2^{45}

Нулевые сообщения

2^{40}

Начальное заполнение R4

2^{17}

СПАСИБО ЗА ВНИМАНИЕ!