

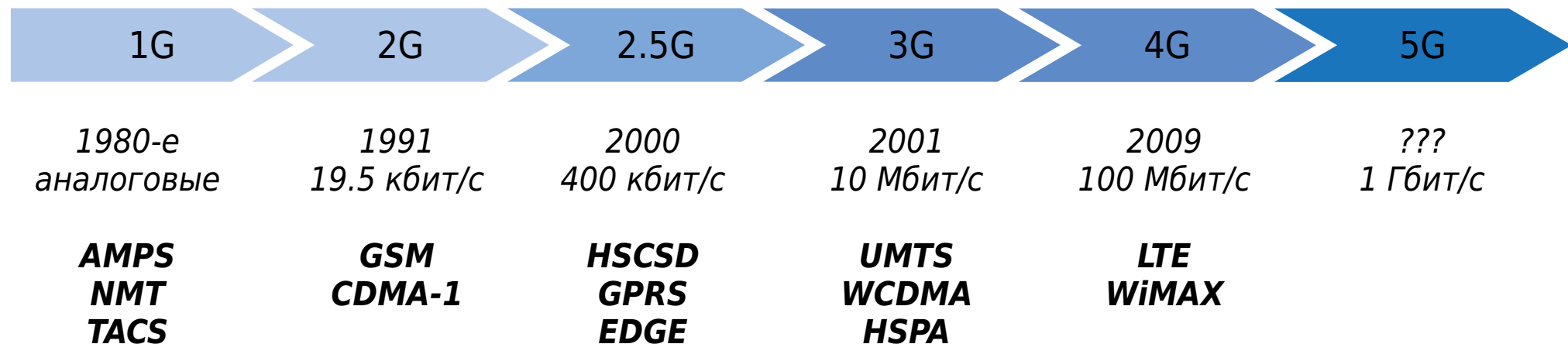
Криптография

Лекция 10. Мобильная связь.

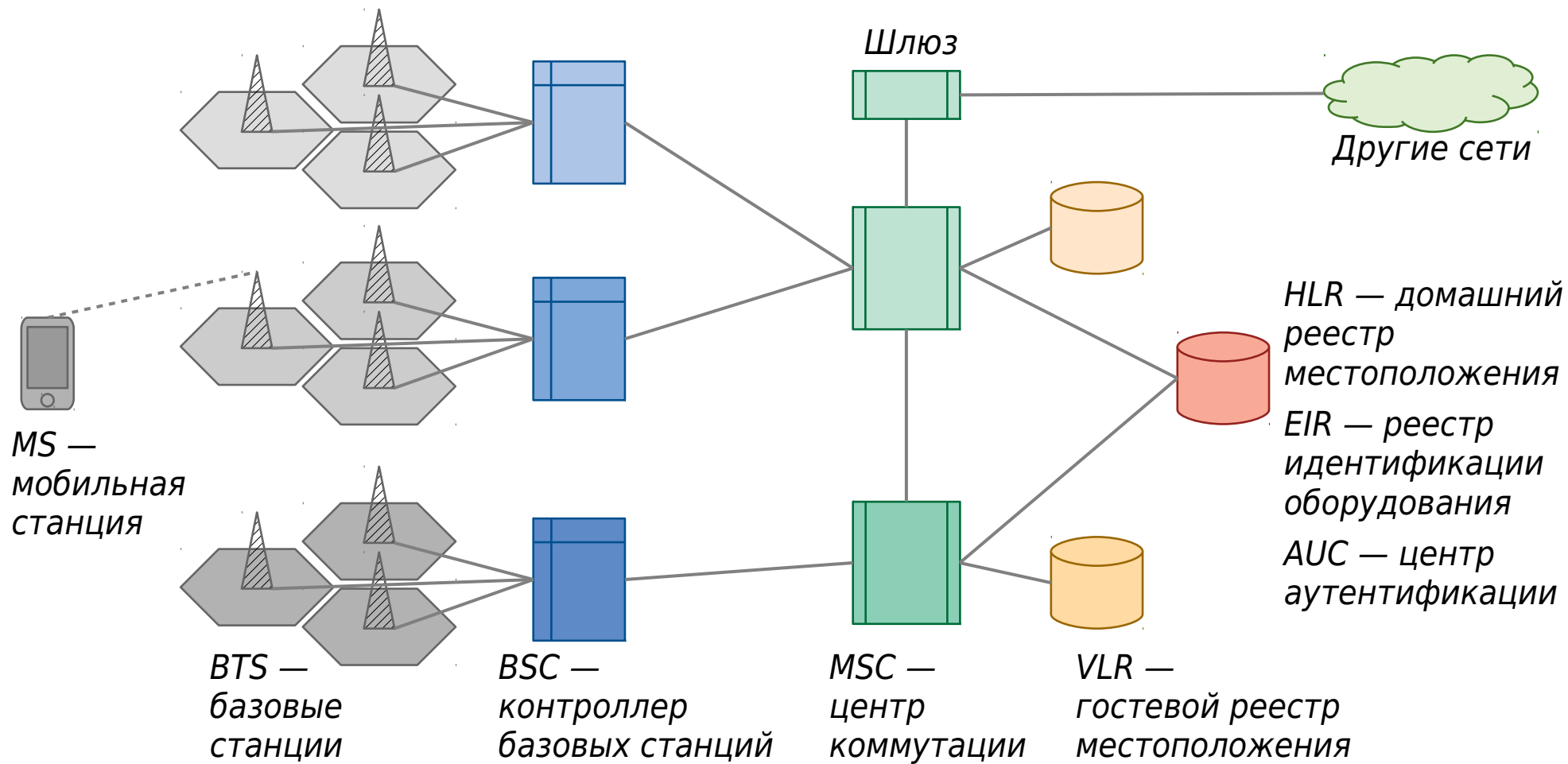
Дмитрий Яхонтов

“Кочерга”, 2018

Поколения сотовой связи



Структура сети GSM



Идентификация абонента

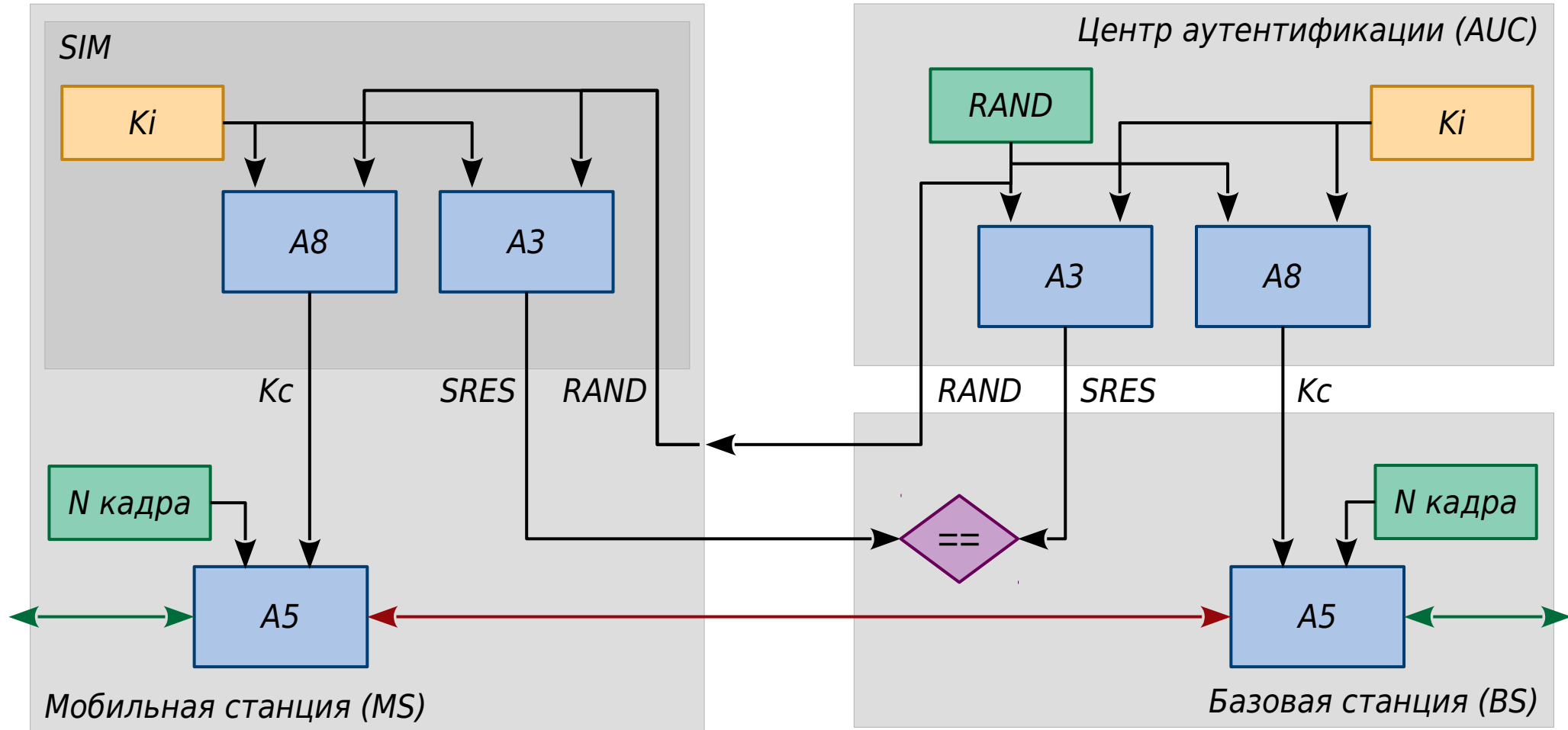
IMEI (International Mobile Equipment Identity) — международный идентификатор мобильного оборудования. Уникальный номер мобильного устройства.

MSISDN (Mobile Subscriber Integrated Services Digital Number) — телефонный номер вида 7-916-1234567. Ассоциирован с IMSI.

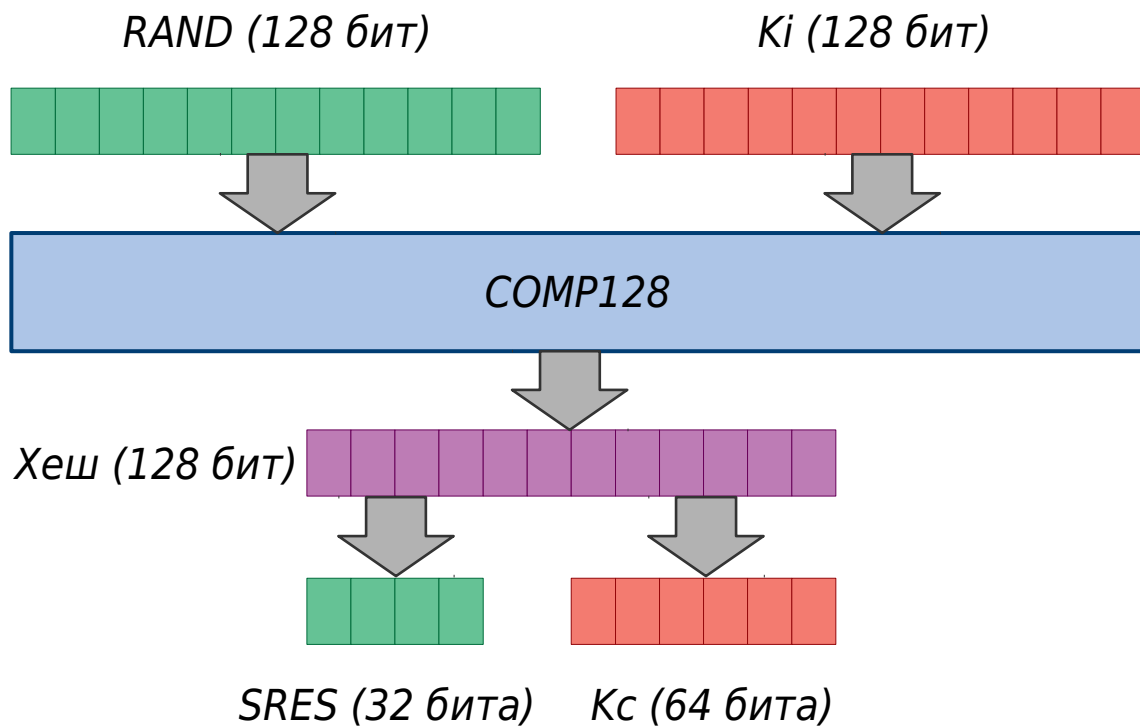
IMSI (International Mobile Subscriber Identity) — международный идентификатор мобильного абонента. Включает в себя код страны, код мобильной сети и собственно ID пользователя. Хранится на SIM. Передается при первой регистрации в сети.

TMSI (Temporary Mobile Subscriber Identity) — временный идентификатор мобильного абонента. Назначается случайно после успешной аутентификации абонента. Действует в пределах зоны обслуживания данного VLR.

Аутентификация и шифрование в GSM



Алгоритмы А3 и А8 (COMP128)



Функции А3 и А8 одновременно выполняет один алгоритм. Старшие 32 бита результата используются как SRES, младшие 64 бита — как Kc.

COMP128 v1 — хеш-функция разрядностью 128 бит, 8 раундов.

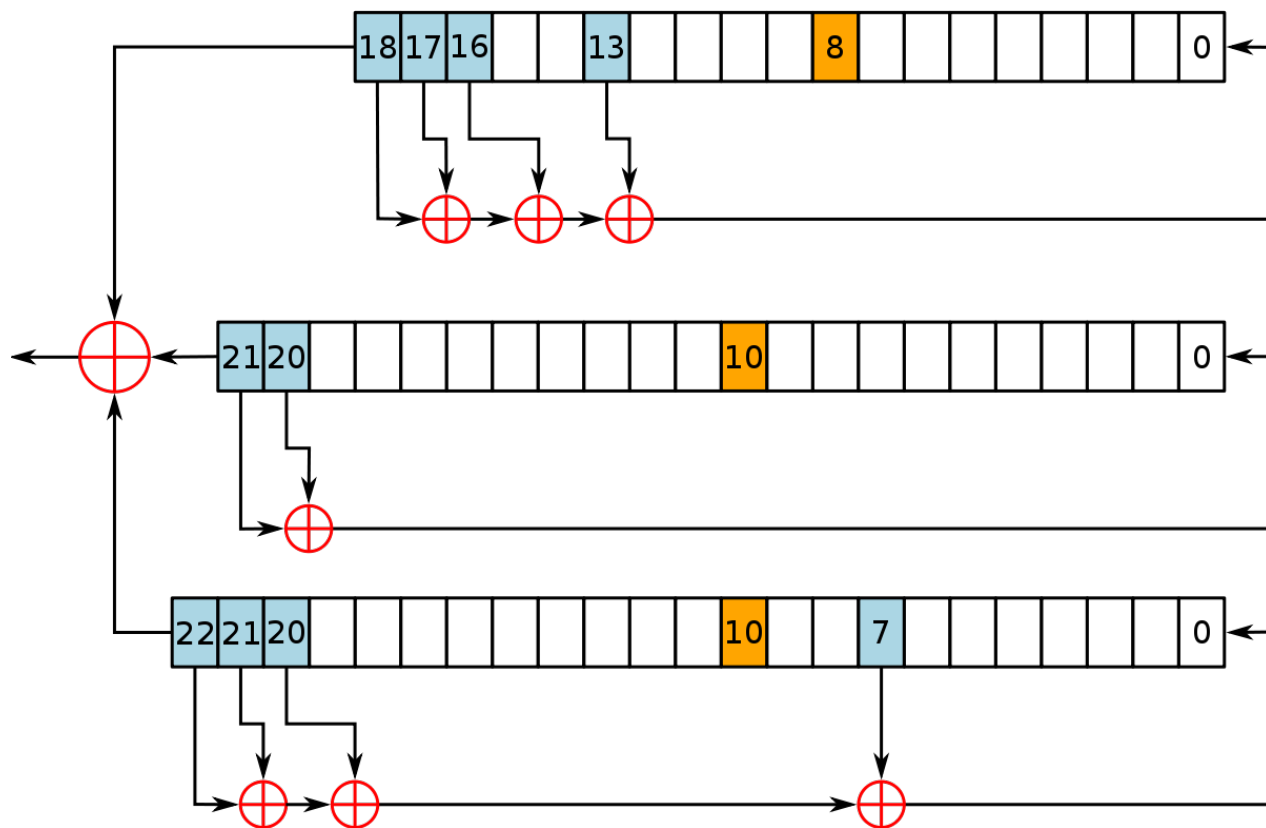
COMP128 v2
COMP128 v3 —
усиленные версии.

COMP128 v4 (Milenage) —
основан на алгоритме AES

Уязвимости COMP128 v1

- Недостаточный лавинный эффект
- Наличие коллизий
- Уязвимость к дифференциальному криптоанализу
- 1998 г, вскрытие Ki за примерно 150 000 запросов к SIM (8 часов)
- 2002 г, атака с использованием побочного канала (анализ потребляемого тока SIM),
вскрытие Ki за 250–1000 запросов (секунды)

Алгоритм А5/1

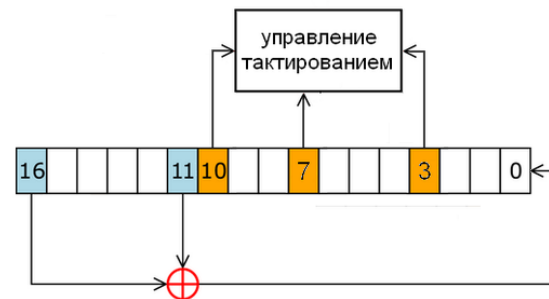
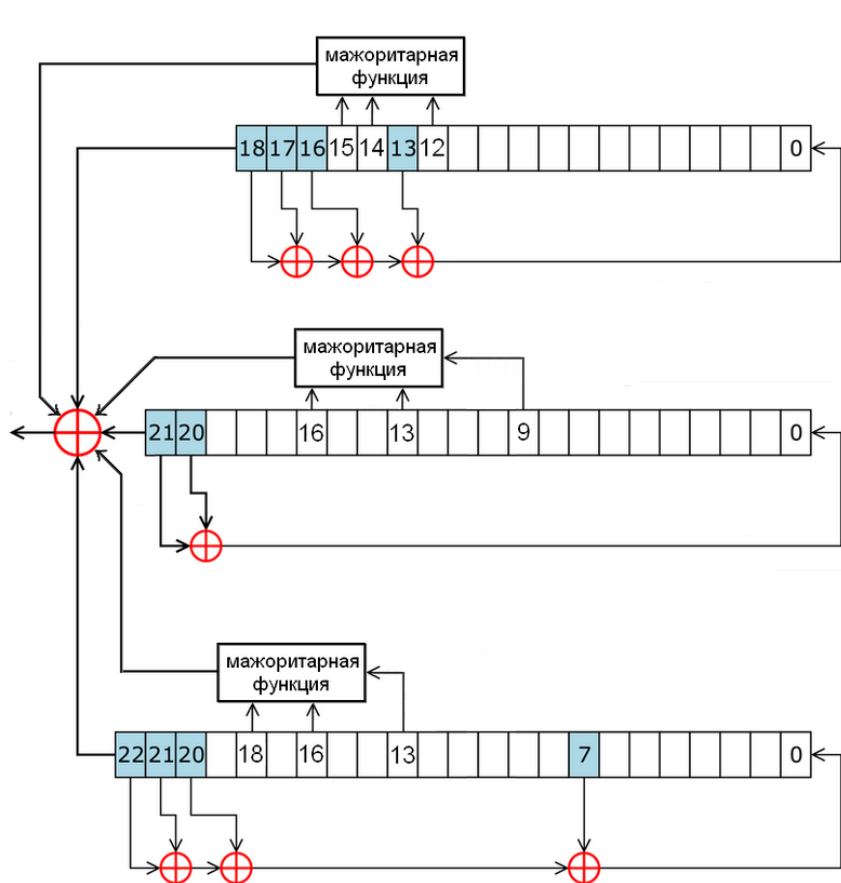


Три сдвиговых регистра
с длинами 19, 22 и 23.

Каждый регистр
(биты 8, 10 и 10) управляет
тактированием двух
остальных регистров

Инициализация:
XOR младшего бита
каждого регистра с битом
ключа (64 такта), затем
аналогично с номером
кадра (22 такта)

Алгоритм А5/2 (ослабленная версия)



Добавлен четвертый регистр
для управления тактированием

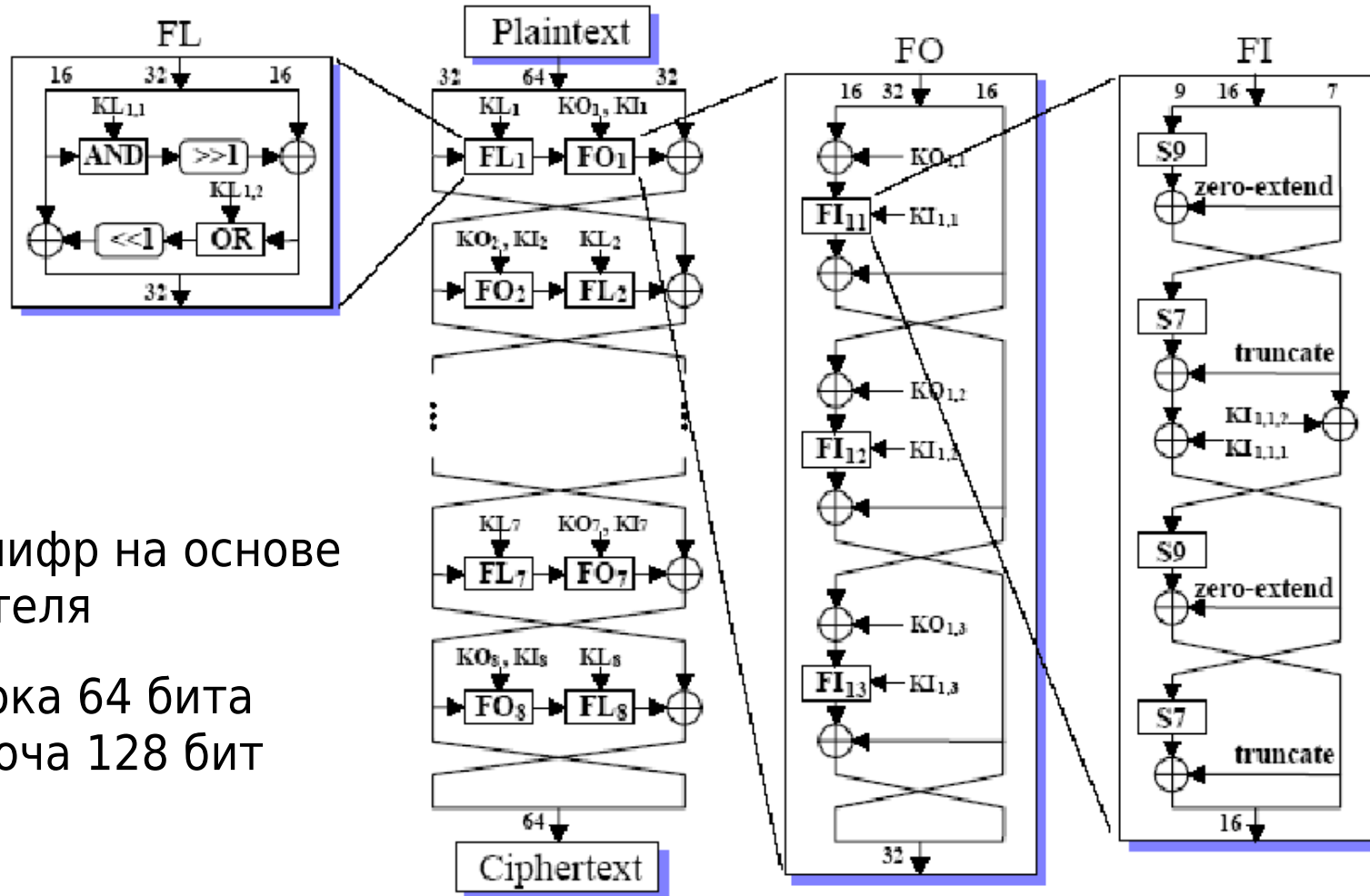
Изменена формула подсчета
выходного значения

Изменена процедура
инициализации

Уязвимости A5/1

- Малая длина ключа — 64 бита
- 10 бит ключа принудительно занулены
- Наличие слабых ключей, дающих малую длину гаммы
- Передача нулевых кадров в начале сеанса связи (возможна атака по открытому тексту)
- 1997 г, атака по 64 битам гаммы, сложность 2^{40} (десятки минут – часы)
- 1999 г, атака по 64 битам гаммы, сложность 2^{17} (секунды), 2 ТБ памяти
- 2002 г, корреляционная атака по 2000 кадрам, без предвычислений
- 2008 г, первая практическая демонстрация атаки

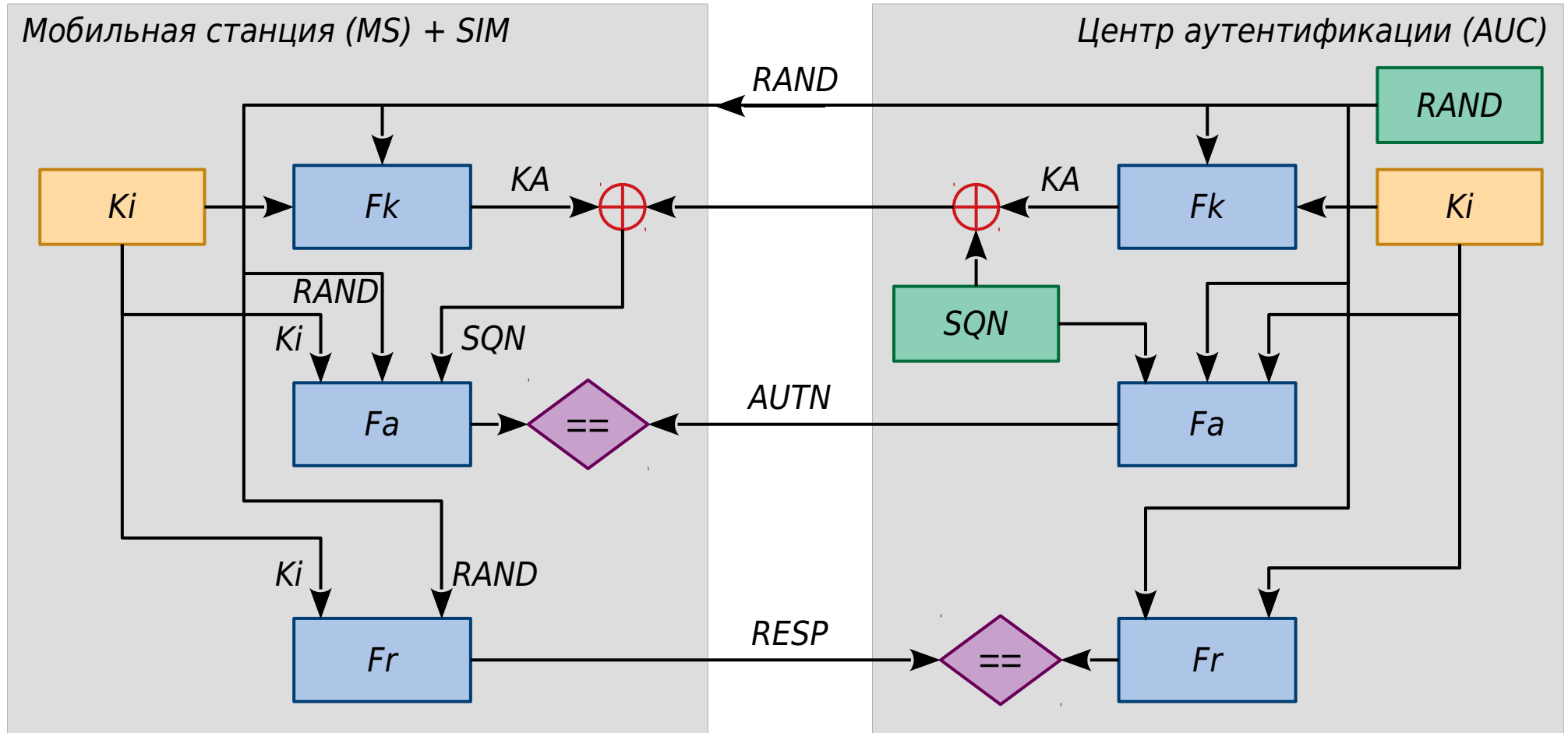
Алгоритм А5/3 (KASUMI)



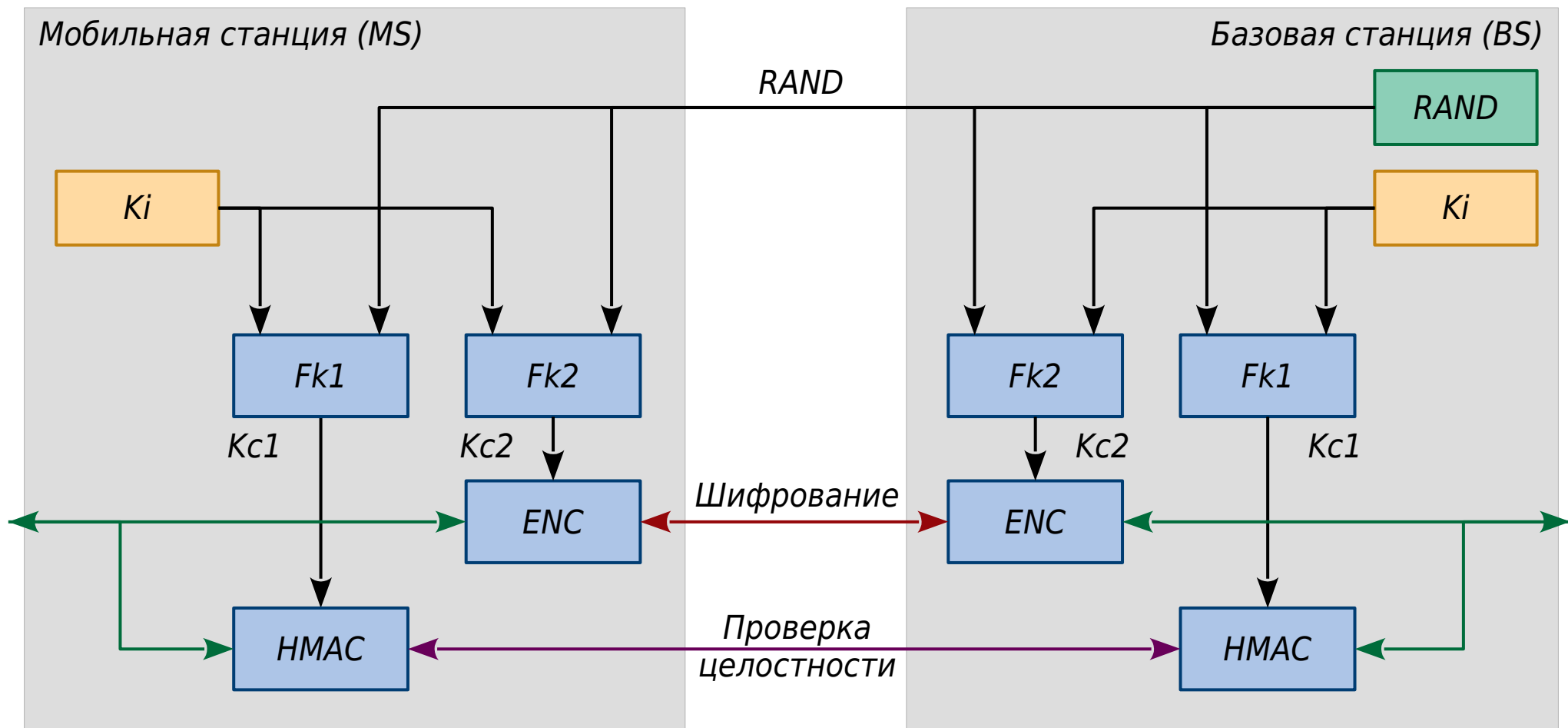
Блочный шифр на основе
сети Фейстеля

Размер блока 64 бита
Размер ключа 128 бит
8 раундов

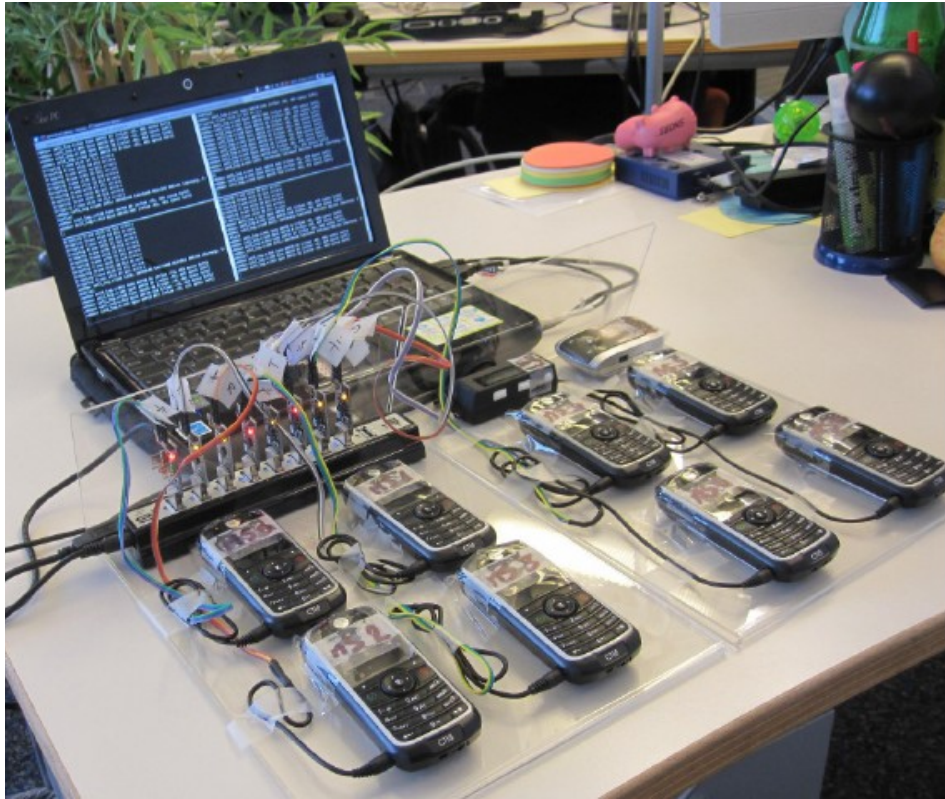
Аутентификация в 3G-сетях



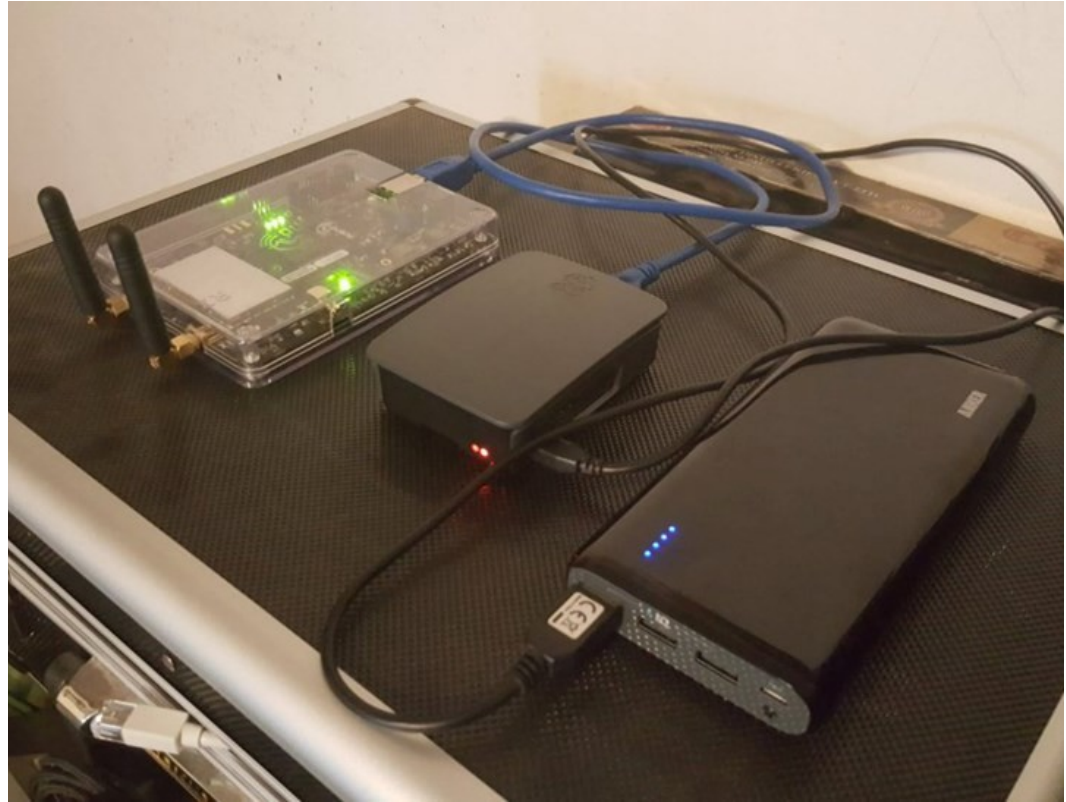
Шифрование в 3G-сетях



Поддельные базовые станции



На основе телефонов Motorola C123



На основе SDR (Software Defined Radio) bladeRF

Ссылки

- Обратная связь:

 android.ruberoi@gmail.com

 [@android_ruberoi](https://lesswrongru.slack.com)

- Анонсы:

 facebook.com/kocherga.club

 vk.com/kocherga_club

 vk.com/kocherga_prog

- Материалы лекций:

 github.com/notOcelot/Kocherga_crypto

- Видео:

 youtube.com/channel/UCeLSDFOndI4eKFutg3oowHg

