v. 2.0

Криптография

Лекция 8. Шифрование файлов.

Дмитрий Яхонтов

“Кочерга”, 2019

Шифрование отдельных файлов

- Архиваторы (Zip, Rar)
  - Симметричные алгоритмы: RC4, AES
- PGP / GnuPG
  - Симметричные алгоритмы: 3DES, AES, Blowfish, Twofish, Camellia
  - Асимметричные алгоритмы: ElGamal, RSA

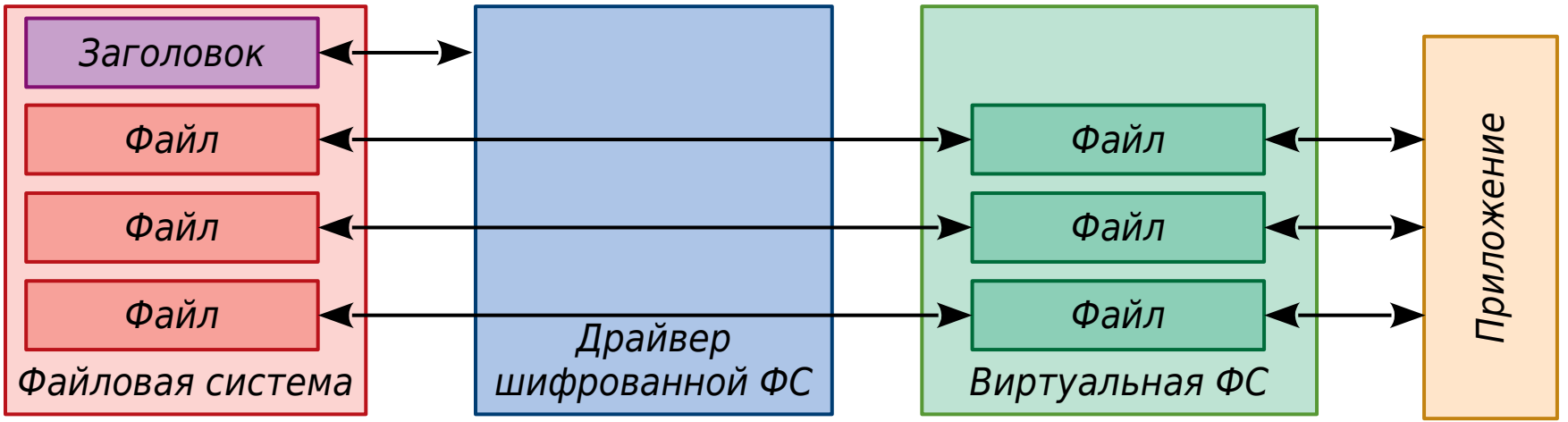
✔ удобно использовать для передачи файлов

✔ кроссплатформенно

✖ после изменения файла требуется вручную перешифровать его

✖ временные копии расшифрованных файлов хранятся на диске

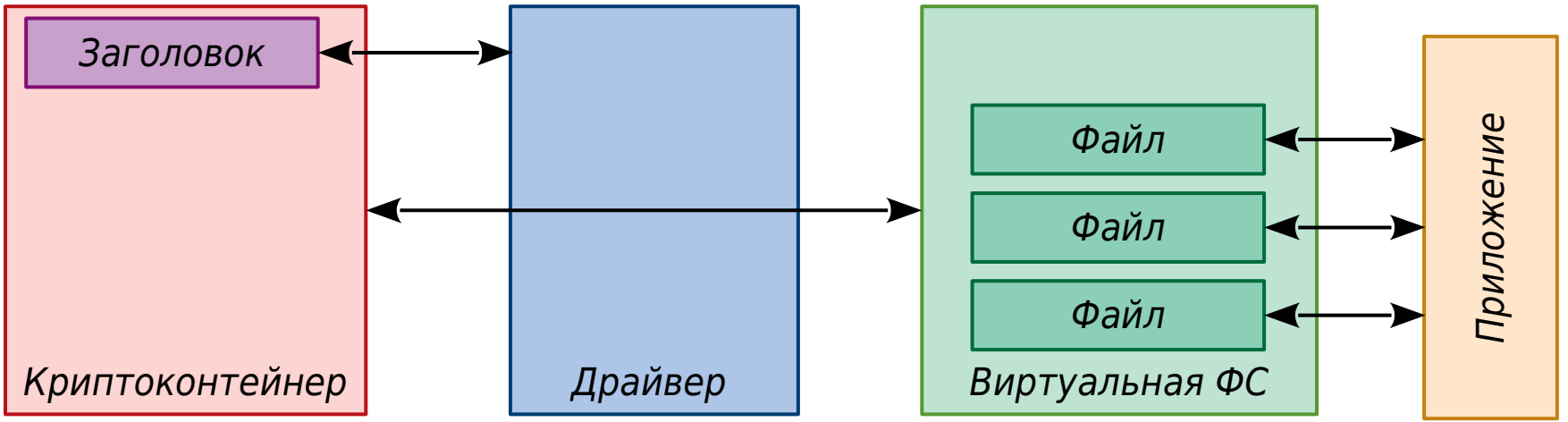
Шифрованные файловые системы



EFS (Windows), EncFS, eCryptfs (Linux)

- ✔ “прозрачная” работа
- ✔ позволяет выполнять инкрементное резервное копирование
- ✖ не скрывает количество файлов и их размер
- ✖ сохраняет все ограничения файловой системы–источника

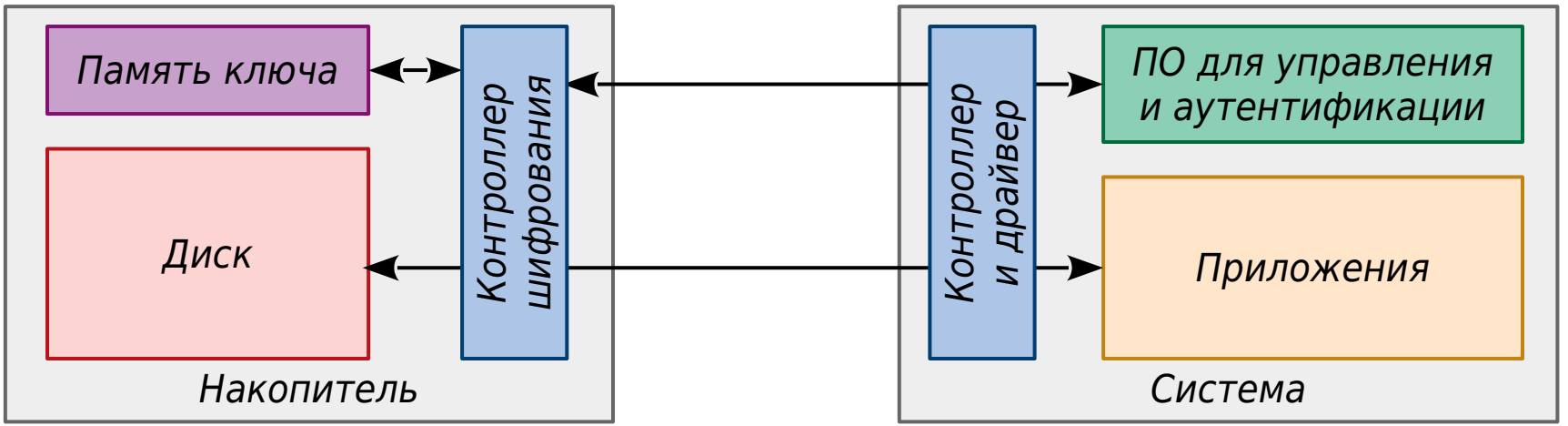
Шифрованные контейнеры / дисковые разделы



BitLocker (Windows), BestCrypt, DiskCryptor, ~~TrueCrypt~~, VeraCrypt

- ✔ “прозрачная” работа
- ✔ скрывает всю информацию о файловой системе
- ✖ затруднено резервное копирование: только контейнер целиком
- ✖ фиксированный размер контейнера

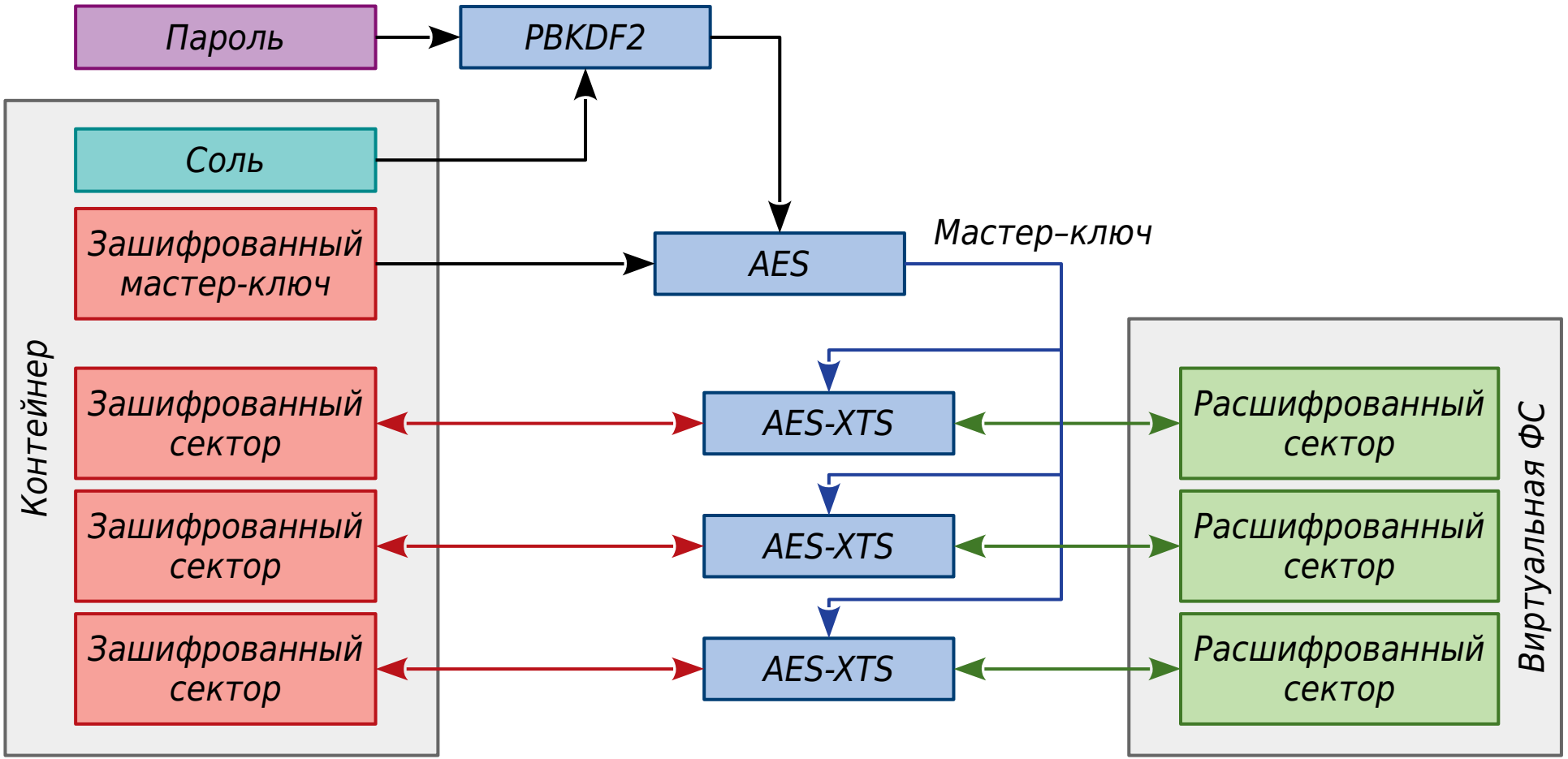
Аппаратно шифруемые диски

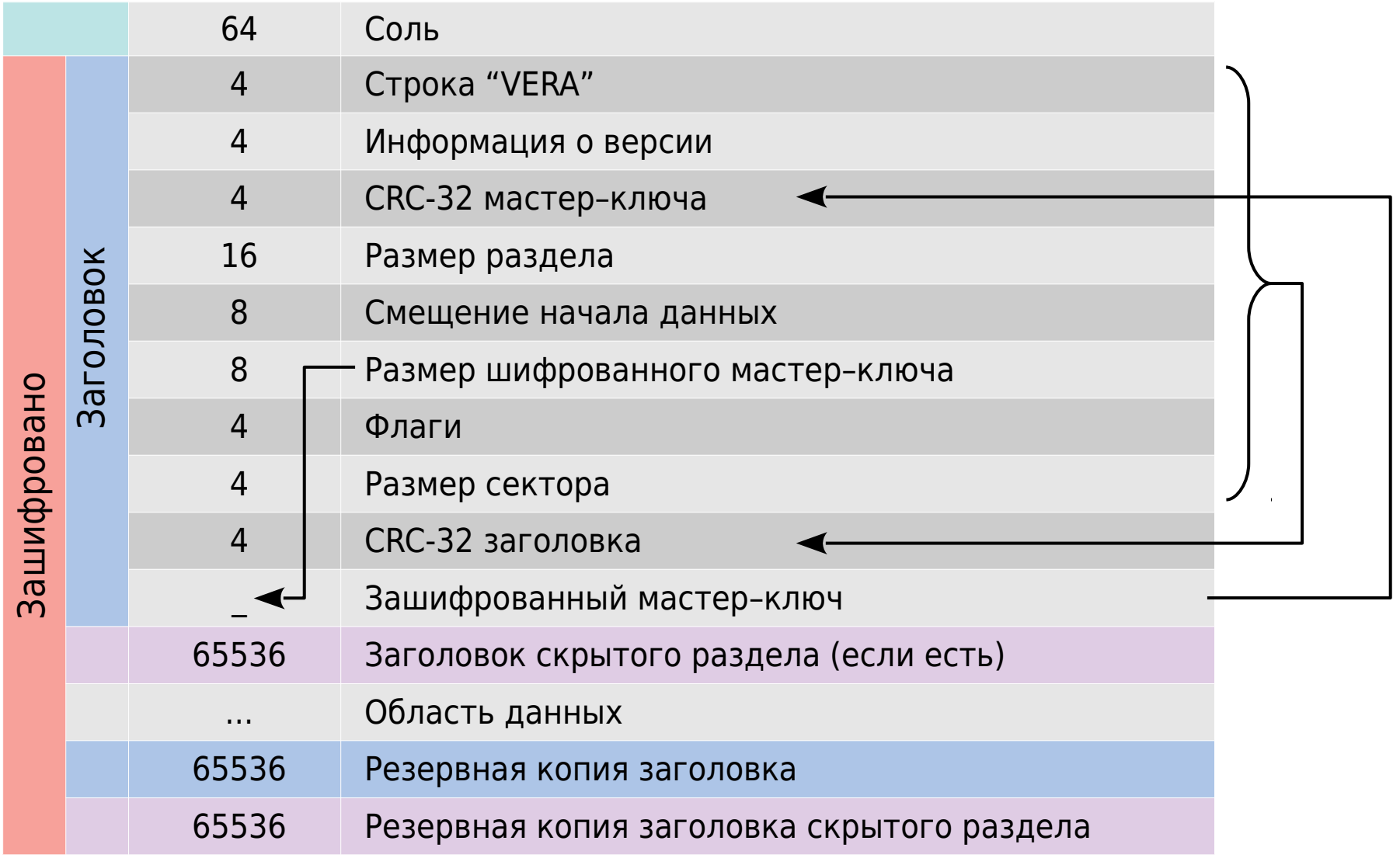


- ✔ работает независимо от ОС и приложений
- ✔ скрывает всю информацию на диске
- ✔ возможно уничтожение данных после N неудачных попыток разблокировки
- ✖ резервное копирование невозможно без расшифровки
- ✖ закрытая архитектура

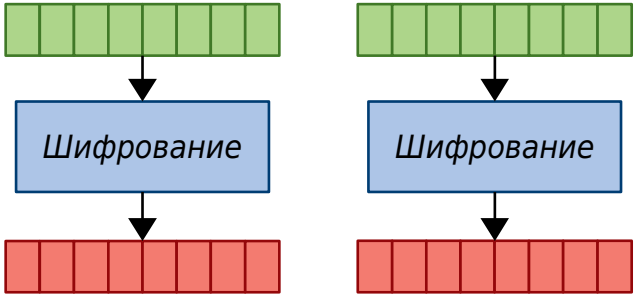
Аппаратно шифруемые диски

Схема работы VeraCrypt

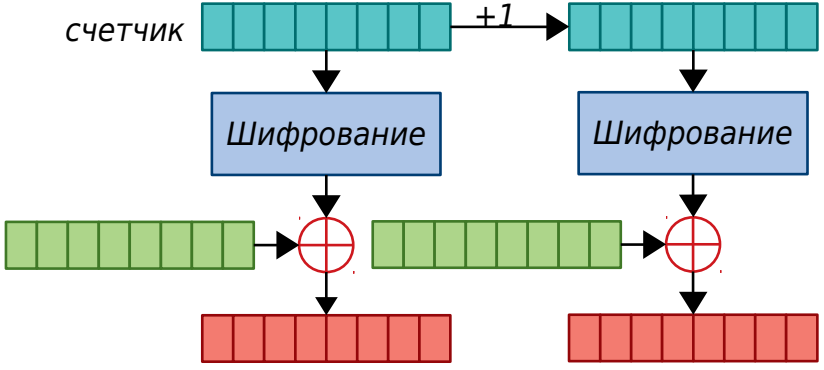



Зашифровано
Заголовок
64
Соль
4
Строка “VERA”
4
Информация о версии
4
CRC-32 мастер–ключа
16
Размер раздела
8
Смещение начала данных
8
Размер шифрованного мастер–ключа
4
Флаги
4
Размер сектора
4
CRC-32 заголовка
_
Зашифрованный мастер–ключ
65536
Заголовок скрытого раздела (если есть)
...
Область данных
65536
Резервная копия заголовка
65536
Резервная копия заголовка скрытого раздела

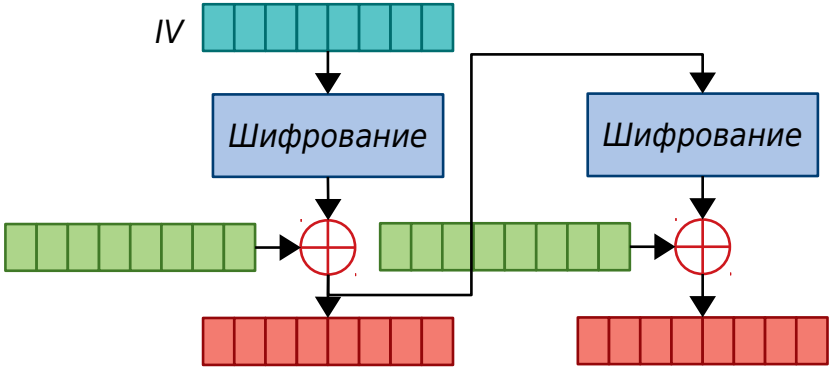
Режимы блочного шифрования
(и почему они не подходят для файловых систем)



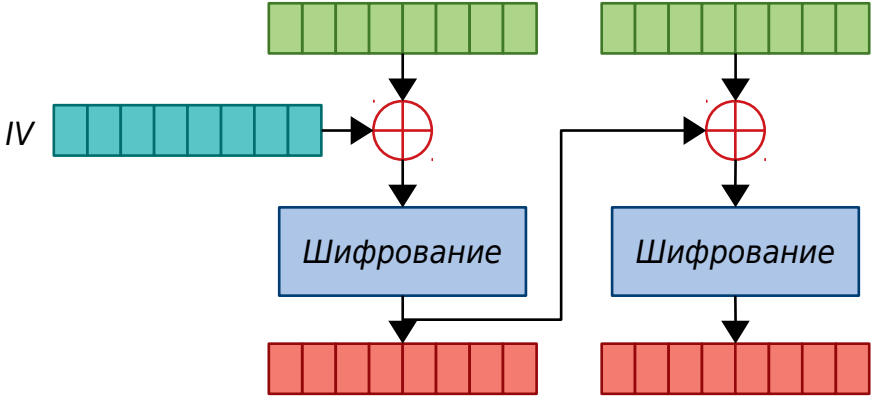
- Простая замена (ECB)
  - нет уникальности блоков



- Со счетчиком (CTR)
  - уязвим к повторной записи других данных в тот же блок

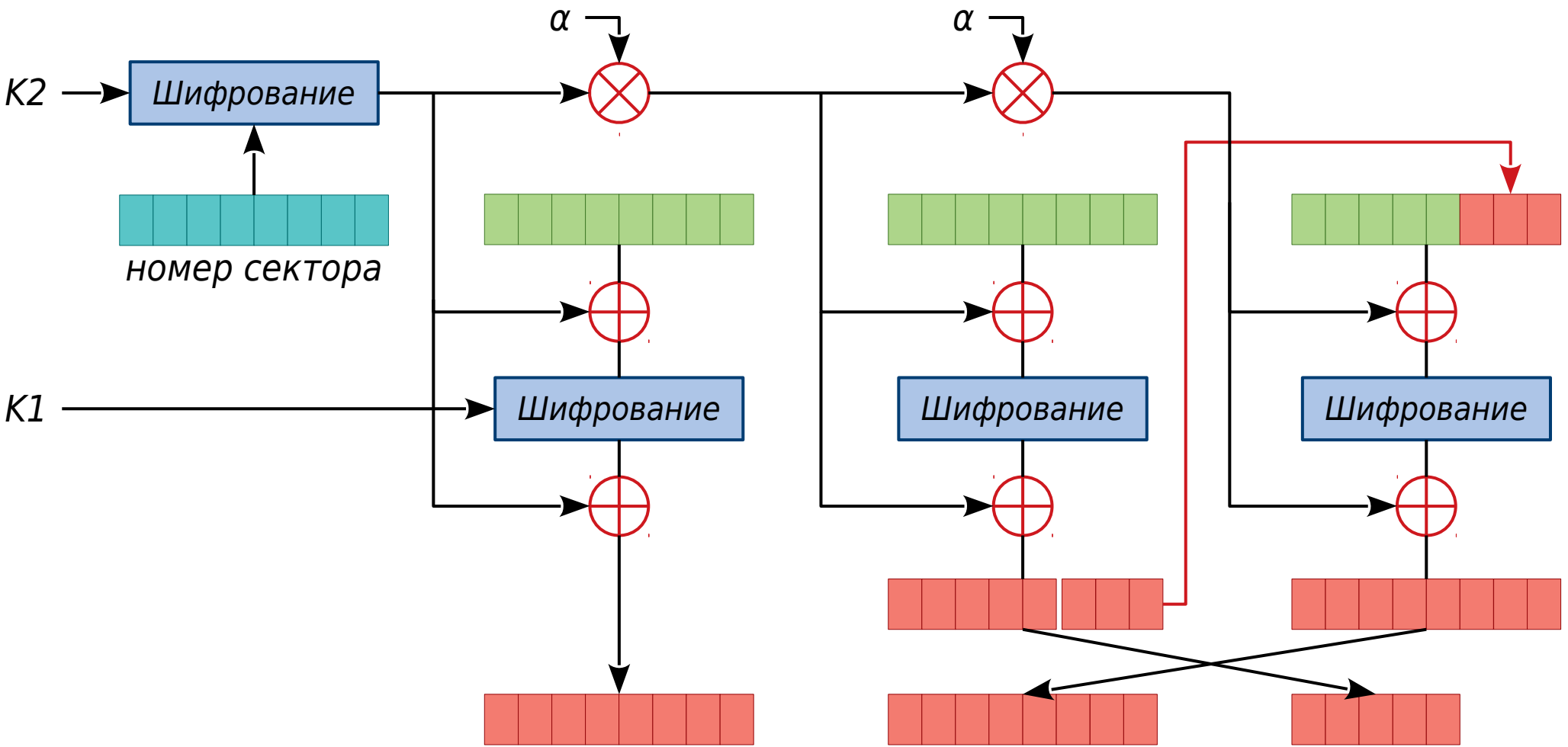


- С обратной связью (CFB и OFB)
  - нет произвольного доступа
  - уязвим к повторной записи других данных в тот же блок
    (CFB — первый блок, OFB — полностью)



- Со сцеплением блоков (CBC)
  - опять нет произвольного доступа
  - если известен открытый текст,
    можно подменить каждый второй блок
  - если IV предсказуемый,
    можно создавать блоки,
    обнаружимые после шифрования

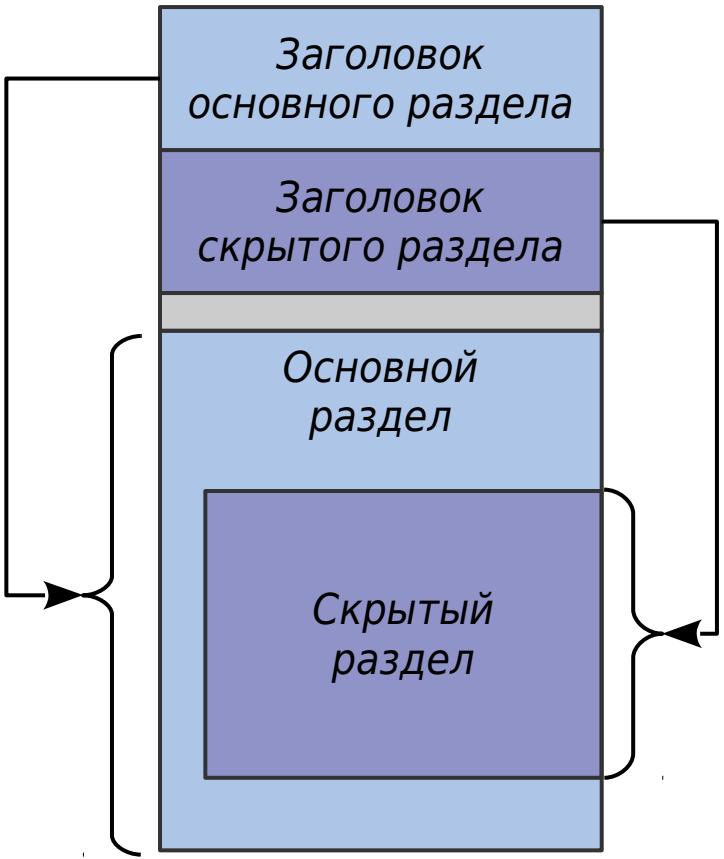
Режим шифрования XTS



Правдоподобное отрицание

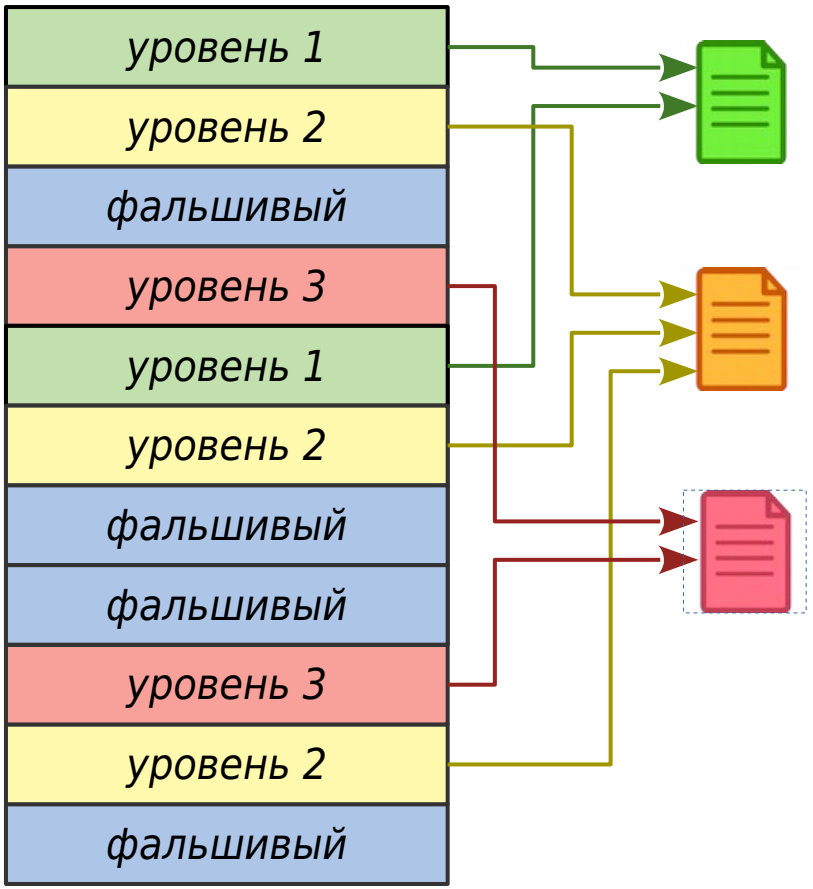
- Цель — отрицать наличие секрета, причем так, чтобы у атакующего не было возможности доказать обратное.
- Уровень 0: контейнер выглядит как случайные данные
  - нет открытых заголовков и сигнатур
  - нет узнаваемой структуры данных
  - нет статистических особенностей (кроме высокой энтропии)
- Уровень 1, 2 … N: скрытые разделы
  - позволяет раскрыть часть секретов, сохранив остальные

Скрытые разделы



- Скрытый раздел расположен внутри основного в случайном месте
- Скрытый раздел имеет собственный заголовок и шифруется собственными ключами
- Без знания ключа скрытый раздел выглядит как свободная часть основного
(случайные данные)
- Запись в основной раздел может повредить информацию в скрытом. Этого можно избежать, используя режим защиты
(требует ключ скрытого раздела)
- VeraCrypt — один скрытый раздел,
LibreCrypt, BestCrypt — несколько разделов

Файловые системы с множеством уровней



- Файловая система разбита на фрагменты, каждый из которых может принадлежать к одному из уровней
- Для доступа к каждому уровню необходим свой ключ
- Присутствуют фальшивые (chaff) уровни, заполненые случайными данными
- Без знания ключа невозможно отличить настоящий уровень от фальшивого
- Rubberhose, StegFS *(разработка прекращена)*

Ссылки

- Обратная связь:
  - android.ruberoid@gmail.com
  - @androidruberoid
- Анонсы:
  - facebook.com/kocherga.club
  - vk.com/kocherga_club
  - vk.com/kocherga_prog
- Материалы лекций:
  - github.com/notOcelot/Kocherga_crypto
- Видео:
  - youtube.com/channel/UCeLSDFOndl4eKFutg3oowHg