Криптография

Лекция 8. Шифрование файлов.

Дмитрий Яхонтов

“Кочерга”, 2018

Шифрование отдельных файлов

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

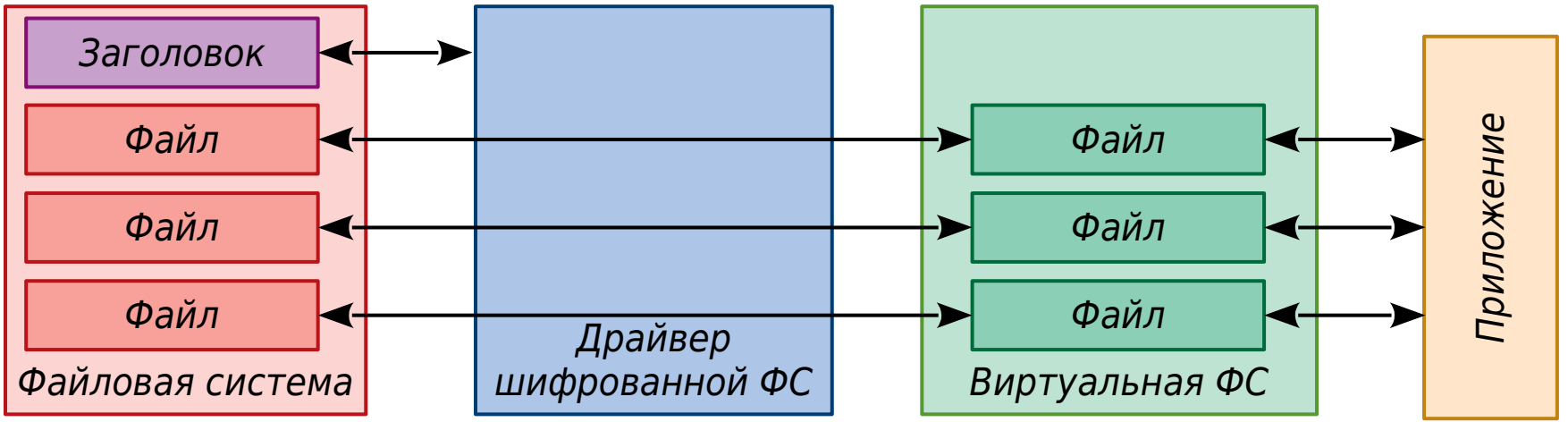
✔ удобно использовать для передачи файлов

✔ кроссплатформенно

✖ после изменения файла требуется вручную перешифровать его

✖ временные копии расшифрованных файлов хранятся на диске

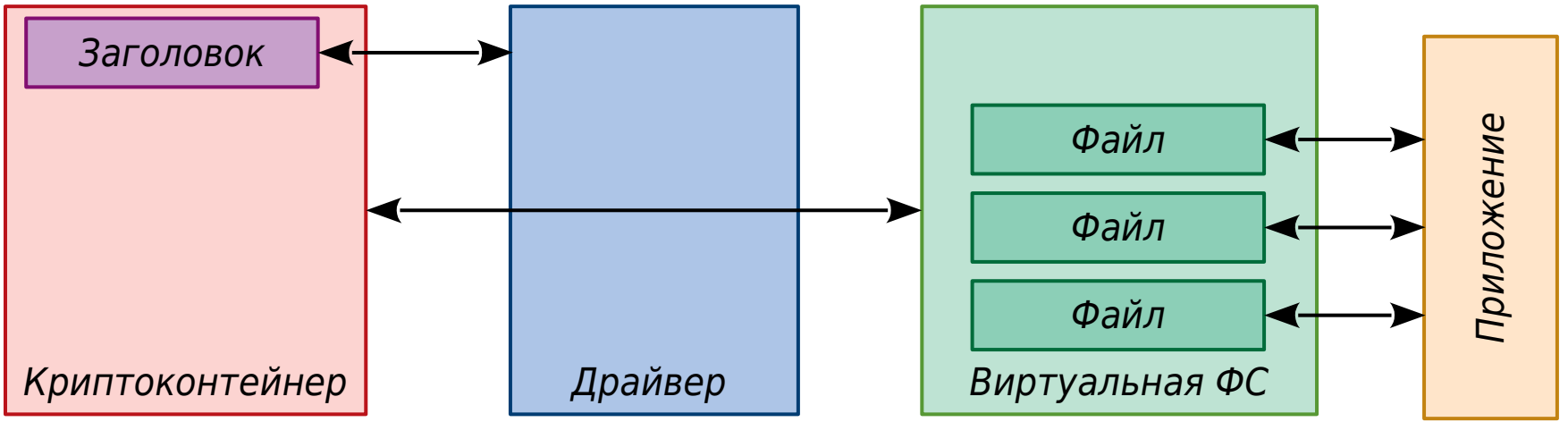
Шифрованные файловые системы



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

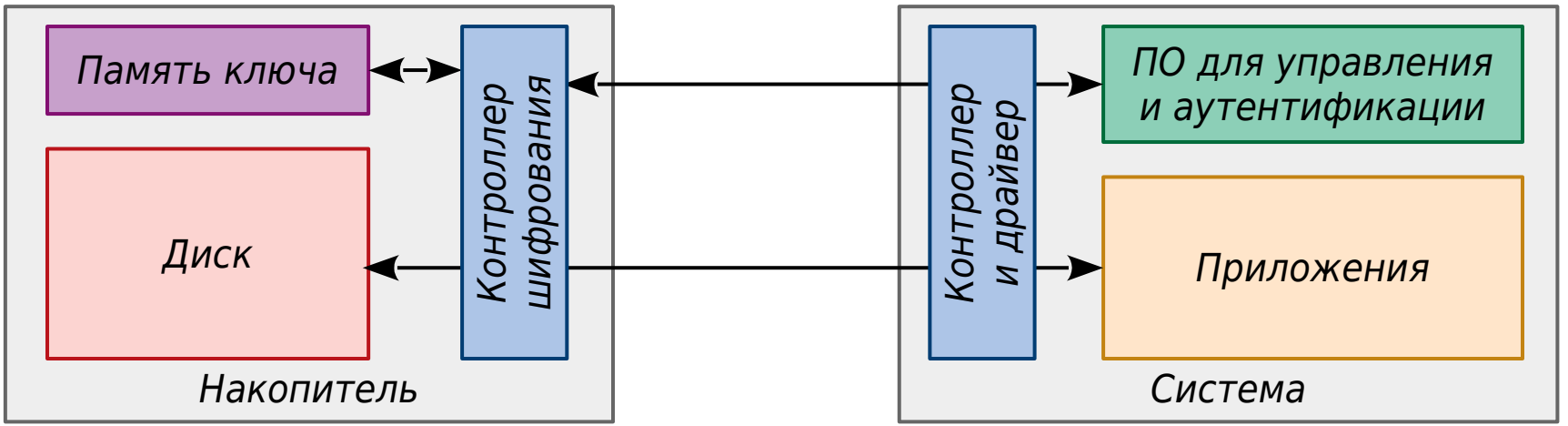
Шифрованные контейнеры / дисковые разделы



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

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

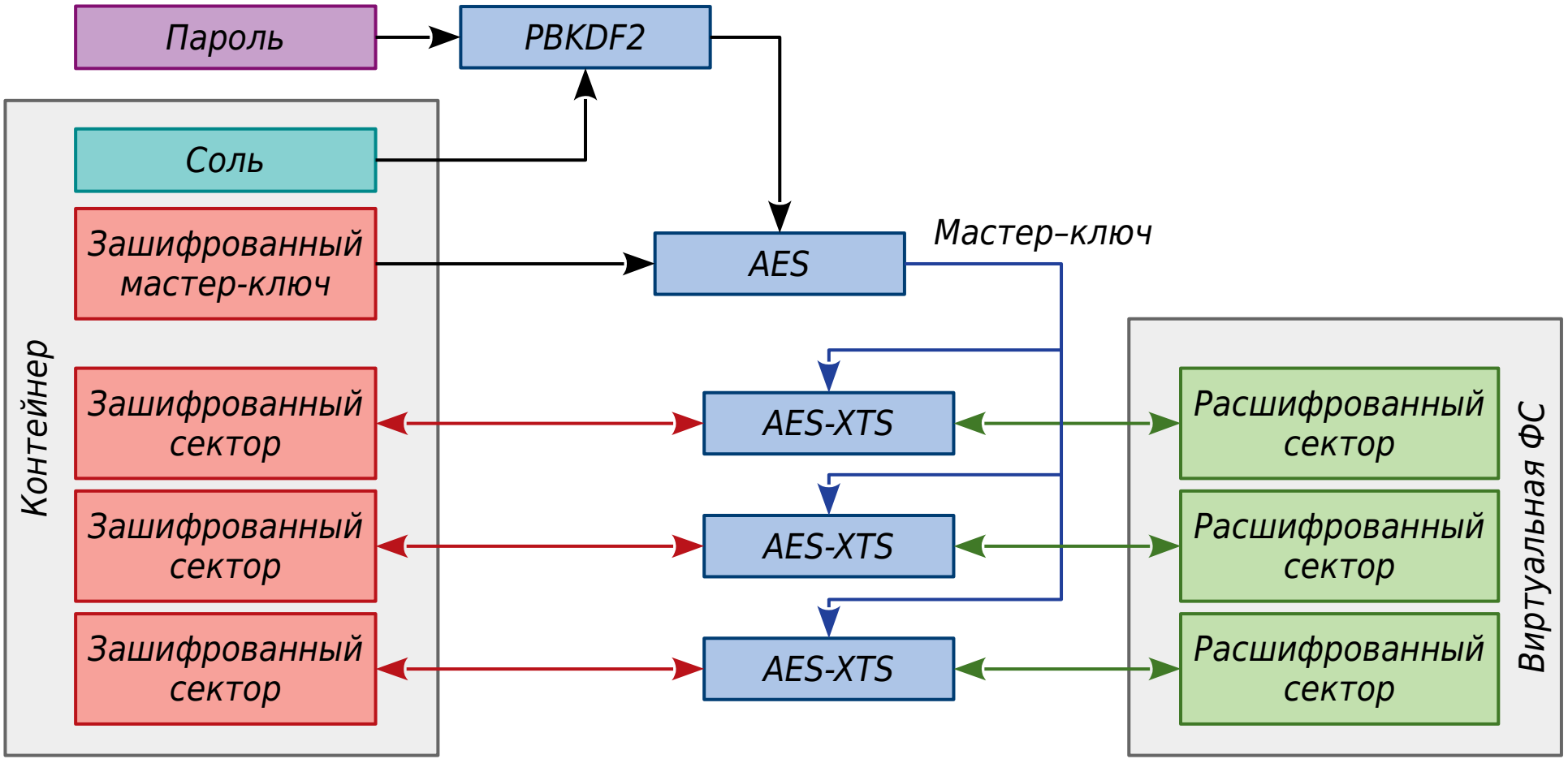
Аппаратно шифруемые диски

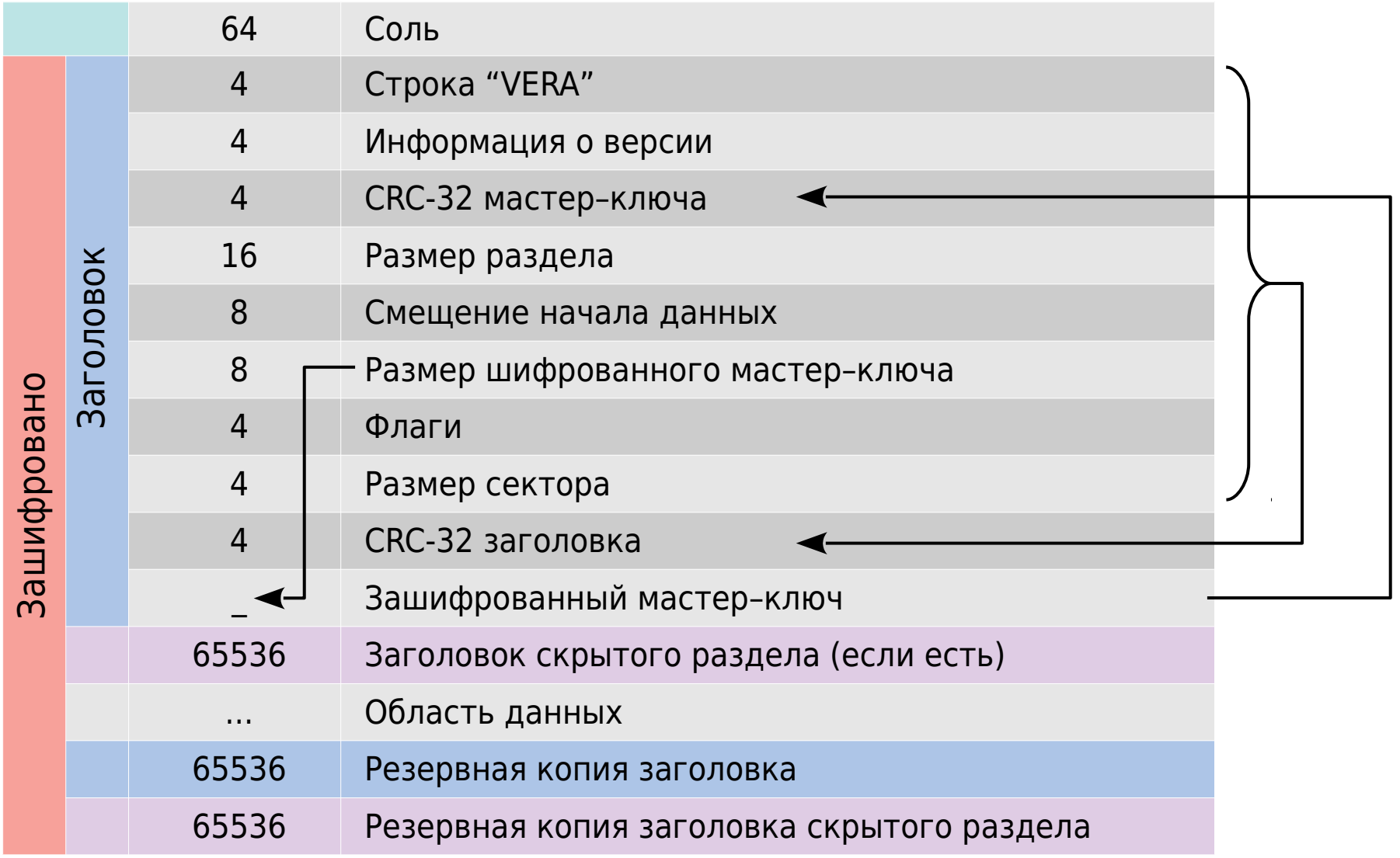


- ✔ работает независимо от ОС и приложений
- ✔ скрывает всю информацию на диске
- ✔ возможно уничтожение данных после N неудачных попыток разблокировки
- ✖ резервное копирование невозможно без расшифровки
- ✖ закрытая архитектура

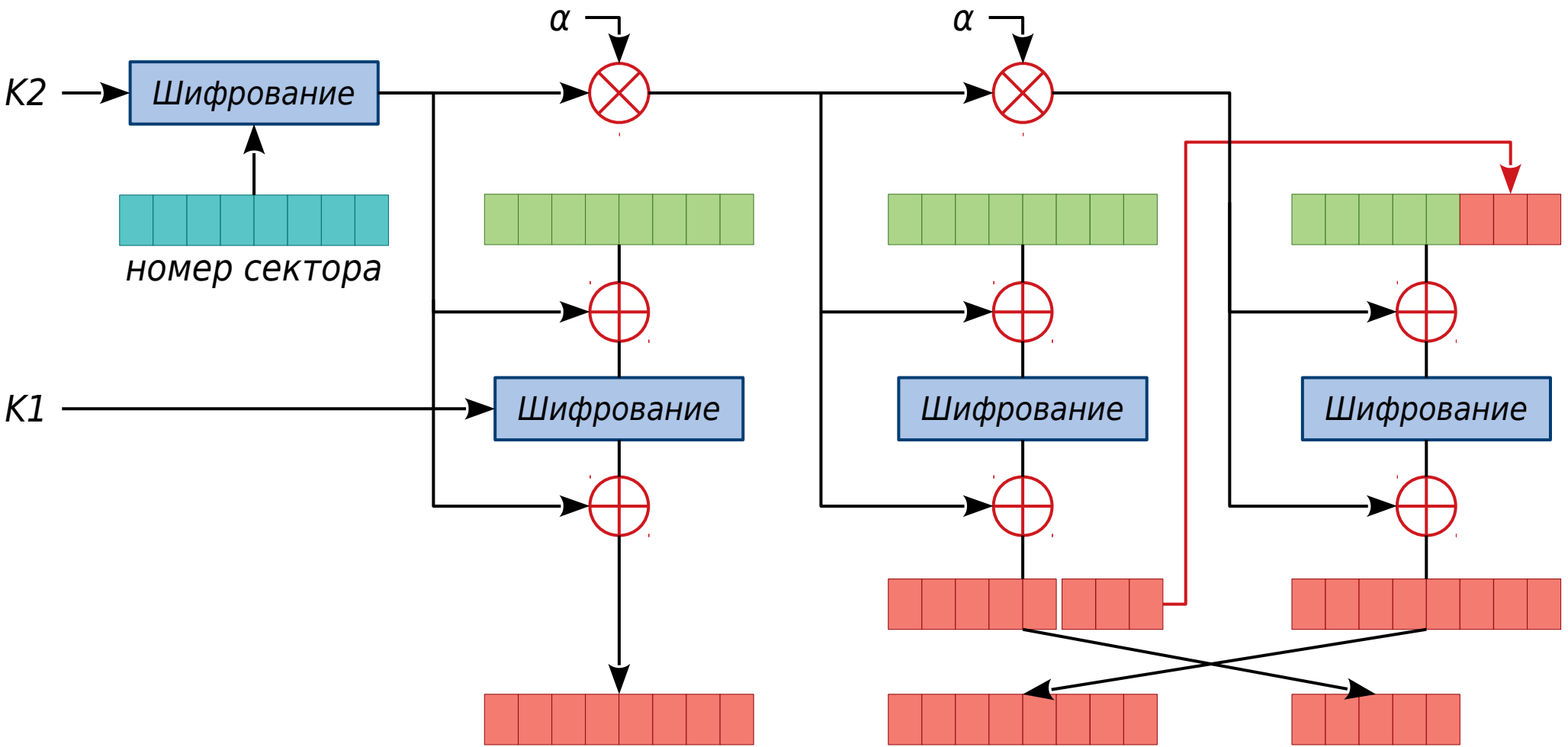
Аппаратно шифруемые диски

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

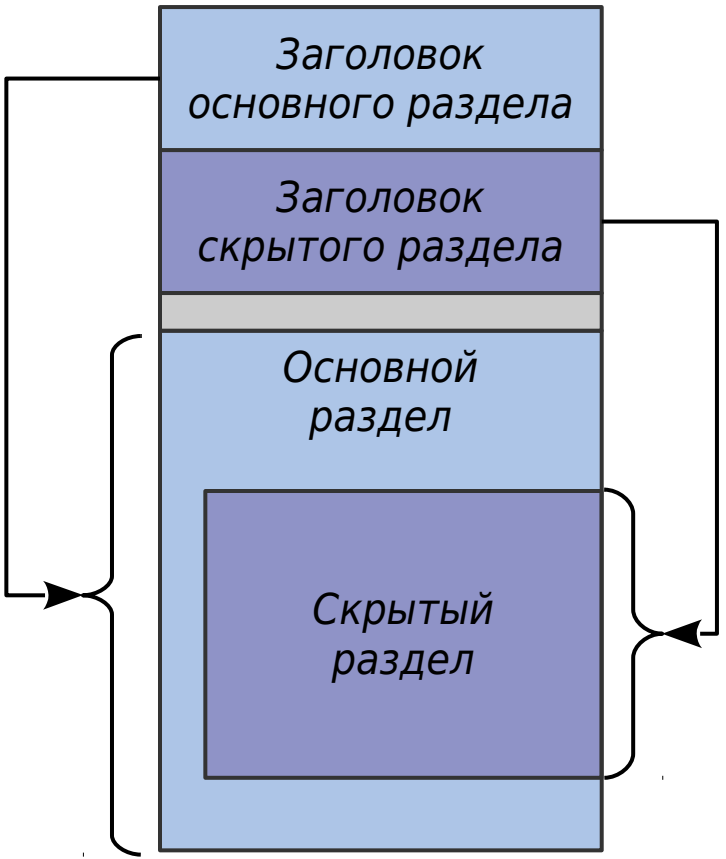
Режим шифрования XTS



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)

Задача

Боб написал программу для шифрования дисков. Алгоритм её работы:

1. Ключ шифрования формируется из пароля путем дополнения нулями до длины 32 байта.
2. Первые 16 байт дискового раздела содержат MD5-хеш ключа для проверки его корректности.
3. Шифрование/расшифровка данных выполняется блоками по 16 байт с использованием алгоритма AES-256 в режиме CTR (значение счетчика = номер блока). Данный режим обеспечивает произвольный доступ, а также то, что блоки с одинаковым содержимым шифруются в различающиеся шифроблоки.

Алиса говорит, что это — полное дно. Согласны ли вы с ней?
Какие ошибки и уязвимости есть в программе Боба?

Ссылки

- Обратная связь:
  - android.ruberoid@gmail.com
  - lesswrongru.slack.com @android_ruberoid
- 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