ММРО
математические методы распознавания образов

Метод встраивания криптографического ключа в биометрический эталон радужной оболочки глаза

Матвеев И.А.

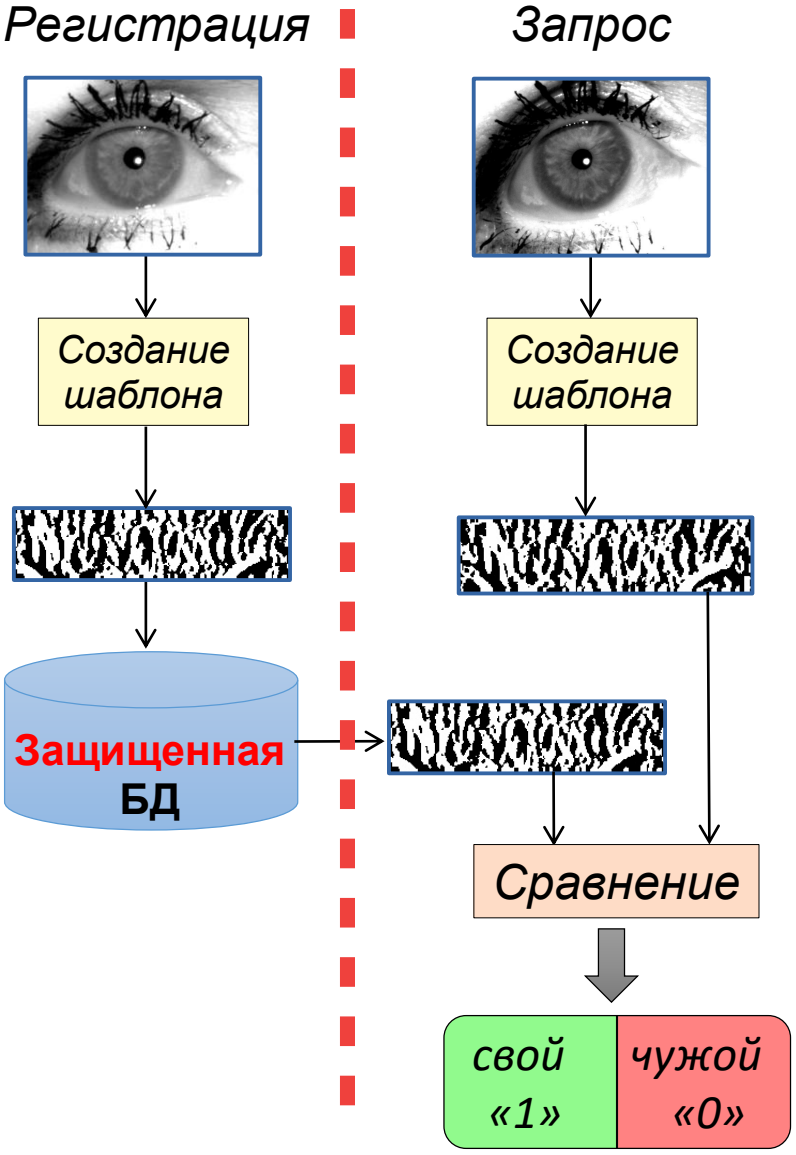
Вычислительный центр Российской академии наук

Зайнулина Э.Т.

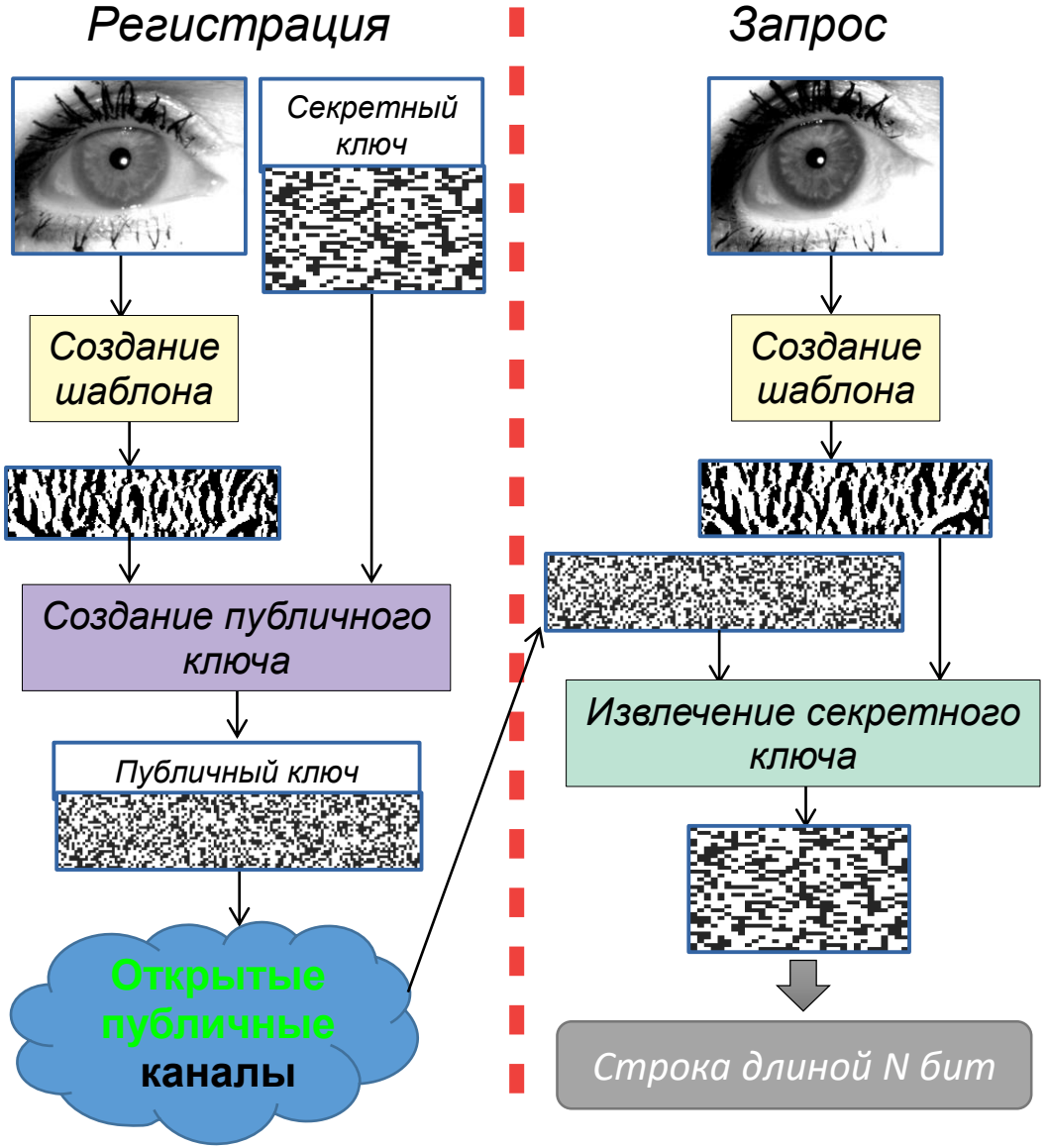
Московский физико-технический институт

Сравнение биометрической аутенцикации и бометрической криптографии

BioID (аутентификация)

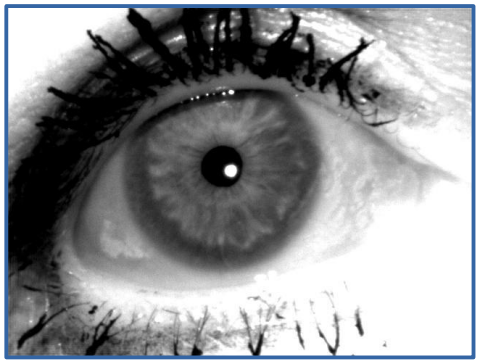


BioEC (нечёткий экстрактор)



Исходные компоненты

Биометрические данные



- Длинные

  ~ 10 000 бит

- Неточные

  Образцы данных одного человека различаются, но число отличных битов не превышает определённого порога

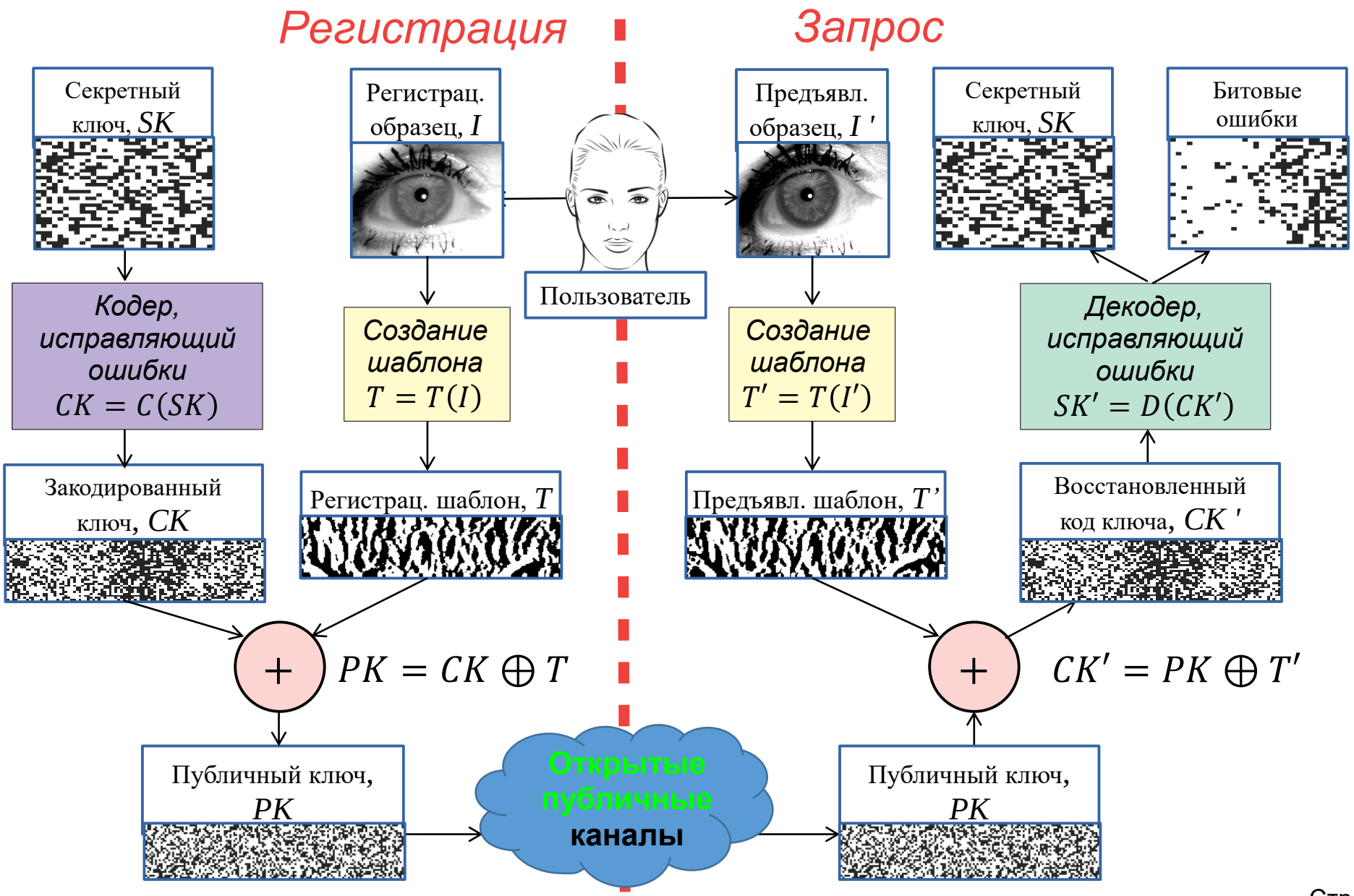
Секретный (криптографический) ключ

- Короткий
  - 256 бит для таких алгоритмов, как ГОСТ-28147, AES-256
  - 64 бита достаточно для обычных паролей, DES, RC5
- Точный

  Ни один бит не может быть изменён

Схема экстрактора на данных радужной оболочки глаза

Предложена Hao F., Anderson R., Daugman J. (2006)



Необходимые компоненты BioEC

Создание шаблона

- Преобразование исходного изображения в строку битов.
- Доля различных битов (нормализованное расстояние Хэмминга) не превышает порог соответствия θ для «истинных» сравнений (шаблонов одного человека) и выше этого порога для «чужих» (сравнений с обазцом самозванца).
- Может быть немедленно взят или адаптирован из хорошо разработанных проектов BioID.

Кодер, корректирующий ошибки

- Добавляет избыточные биты в код, позволяя исправить определенную долю ошибок (количество ошибок не должно превышать порог допустимого числа ошибок для успешного восстановления закодированного сообщения).
- - Криптографический ключ (размер ~ 100 бит) может быть увеличен до размера шаблона (~ 10000 бит).

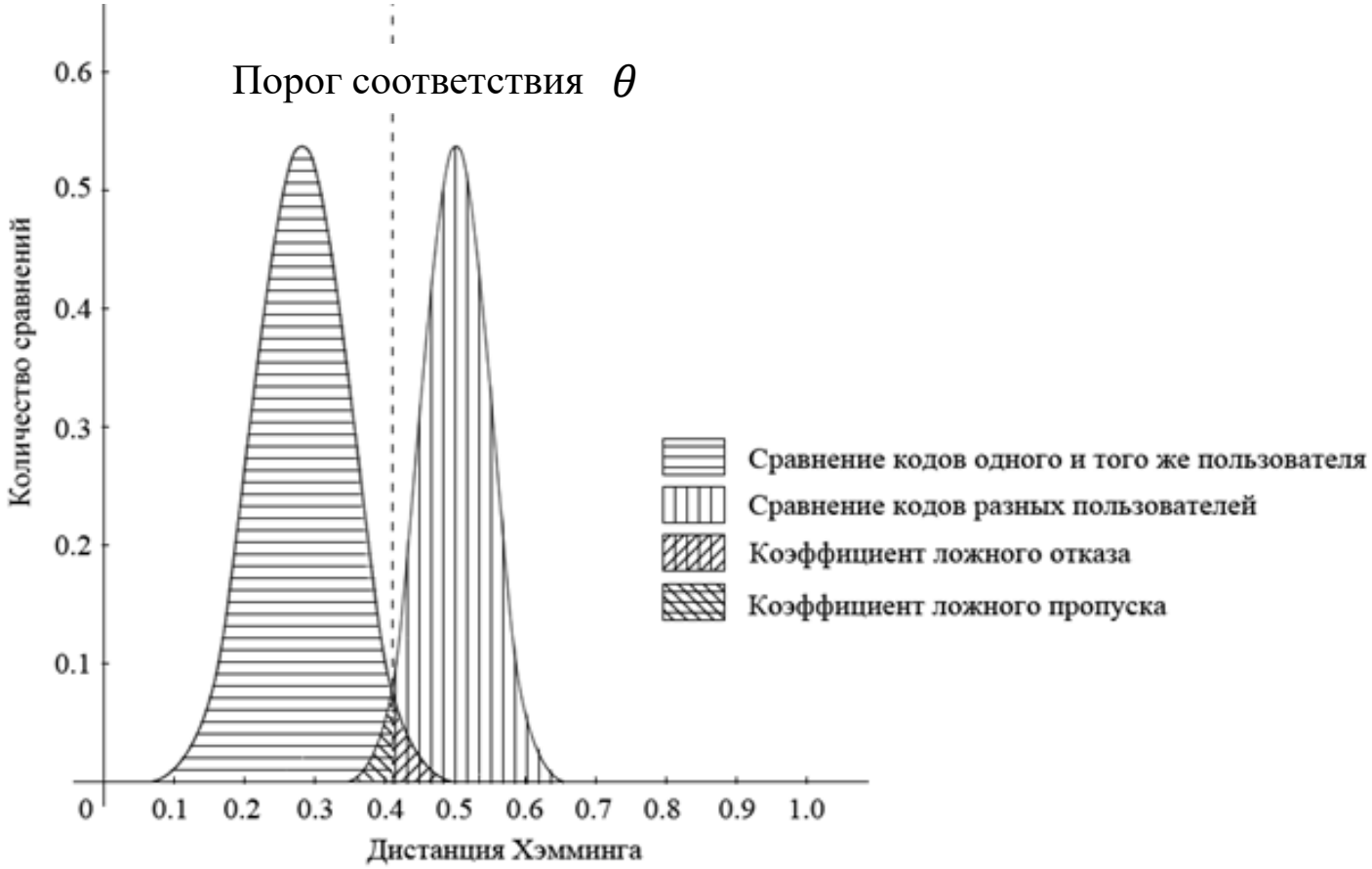
Объединение шаблона и закодированного ключа

- Тривиальное побитовое суммирование по модулю 2 (XOR)

Декодер, корректирующий ошибки

- Дуален энкодеру.
- Декодирование – более сложная задача, чем кодирование.
- Может потребоваться запустить несколько раз из-за сдвига радужной оболочки.

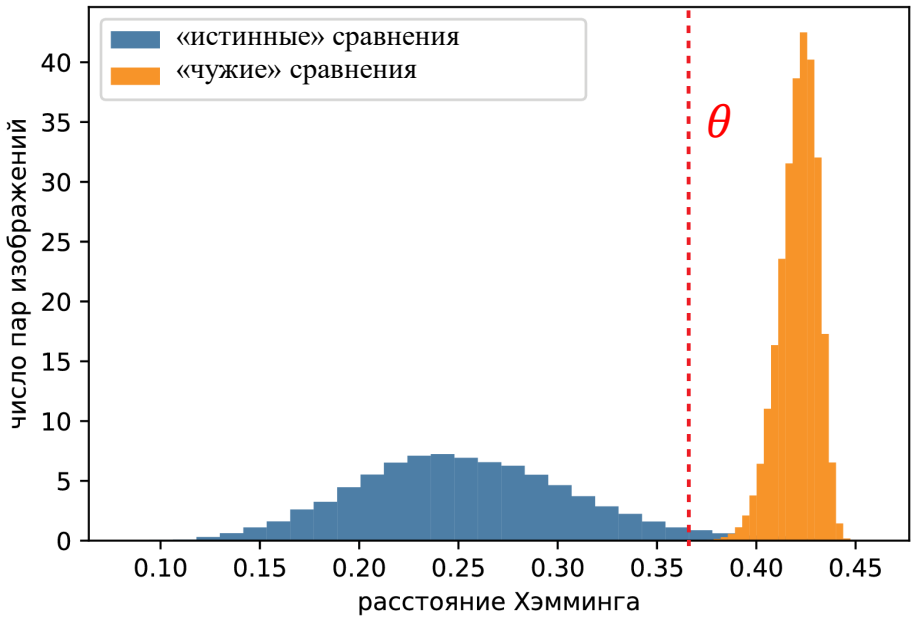
Связь между порогом соответствия и порогом допустимого числа ошибок



$$CK' = T' \oplus (T \oplus CK) = (T' \oplus T) \oplus CK$$

Порог допустимого числа ошибок кодека должен совпадать с порогом соответствия

Выбор порога



Название БД	Число радужек	Число образцов	θ при $FAR=10^{-4}$	FAR при $\theta=0.35$, $.\times10^{-4}$
BATH	1600	31988	0,402	0,03
CASIA-4-Thousand	2000	20000	0,351	0,97
ES	426	22954	0,356	0,79
ICE	242	2953	0,395	0,011
LG-3000	265	2864	0,386	0,07
Panasonic	277	2890	0,389	0,2
UBIRIS-1	240	1207	0,401	0,001

Коэффициент ложного допуска (FAR) должен быть меньше 10^{-4}

Для всех баз данных это вполняется при $\theta \geq 0.35$

Слишком высокий порог

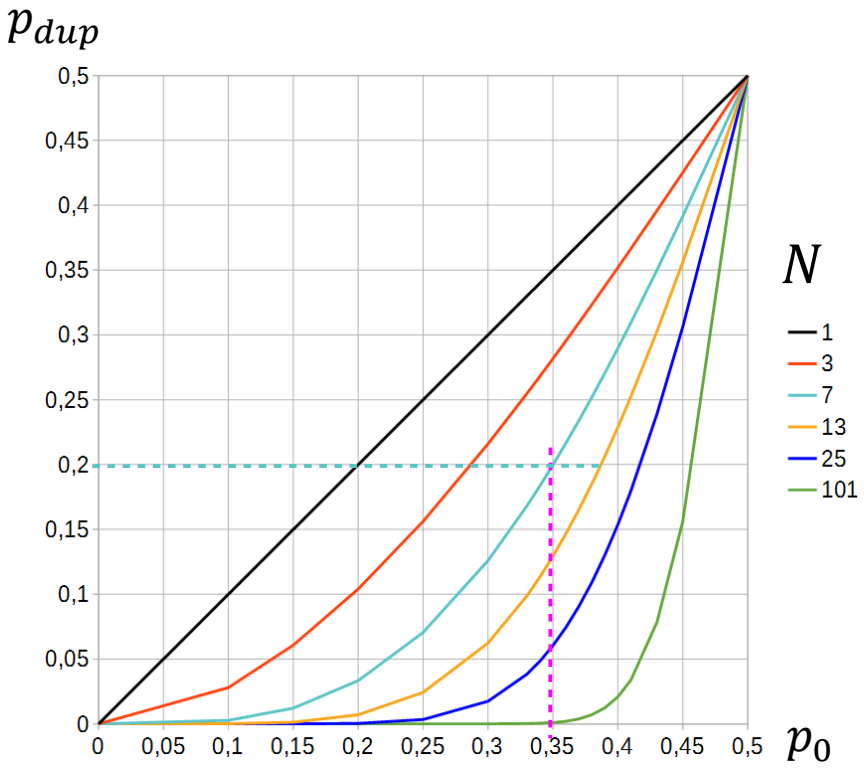
$\theta = 0.35$ – довольно высокий порог

Hao, F., Anderson, R., and Daugman, J. (2006). Combining crypto with biometrics effectively. IEEE Transactions on Computers, 55(9):1081–1088.

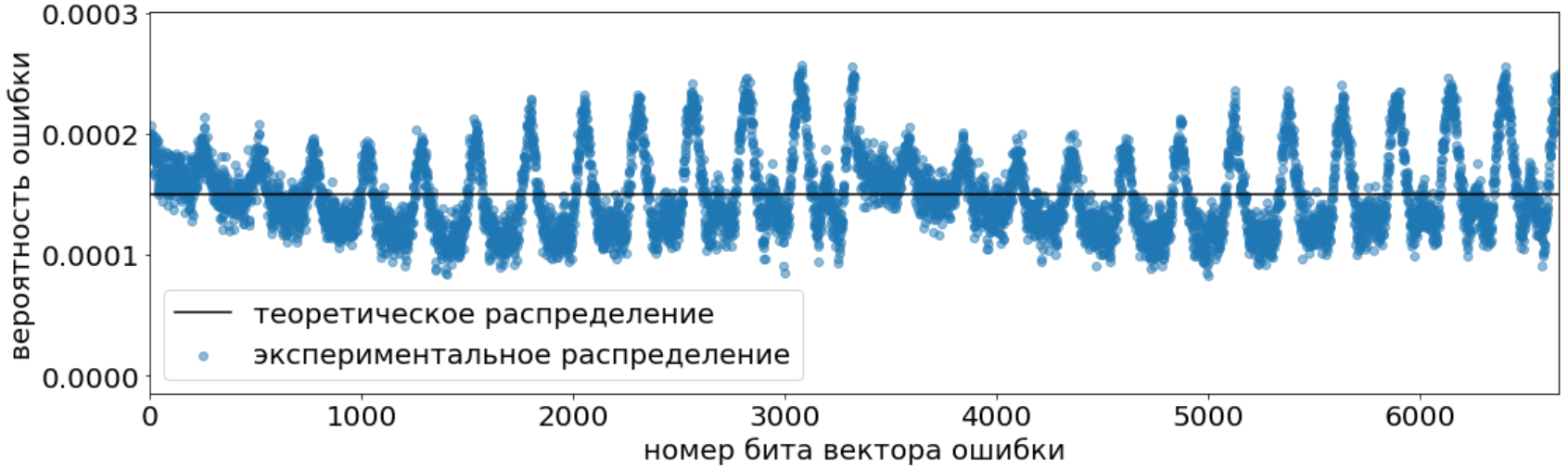
Предложенная схема: RS-HAD

Коды Адамара успешно восстанавливают сообщение только при θ<0.25.

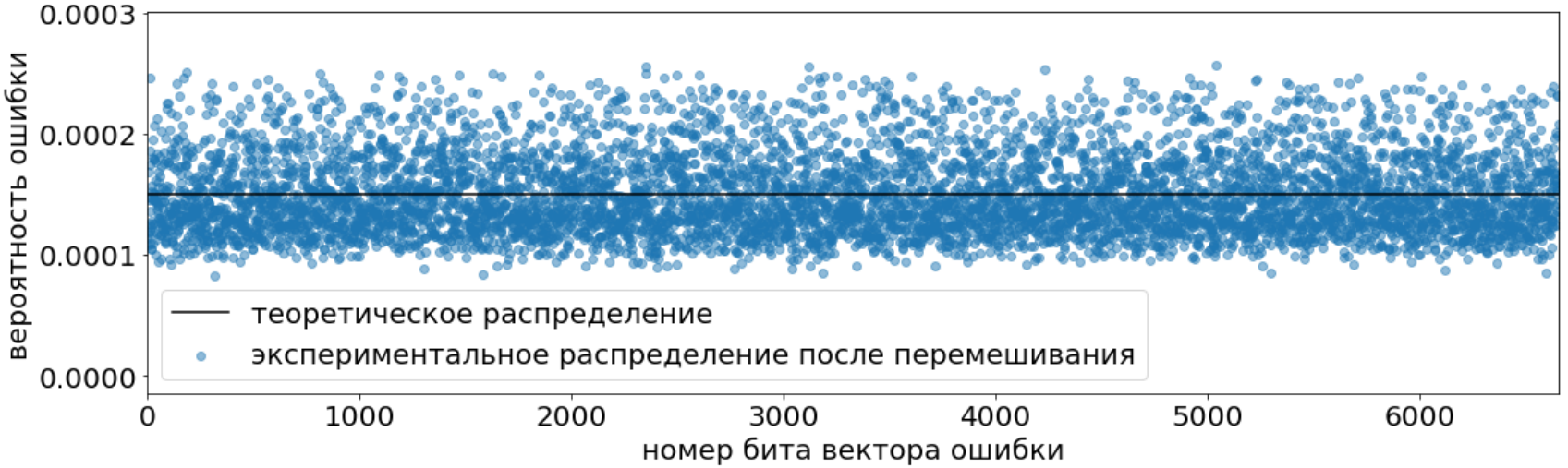
Решение: добавить этап кодирования дублированием битов



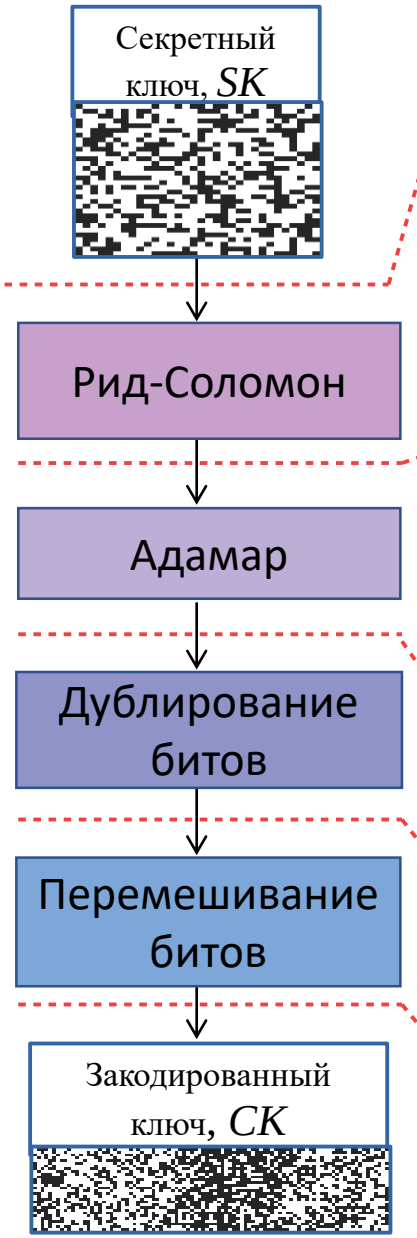
Неравномерность распределения ошибки



Решение: добавить этап перемешивания битов



Кодер



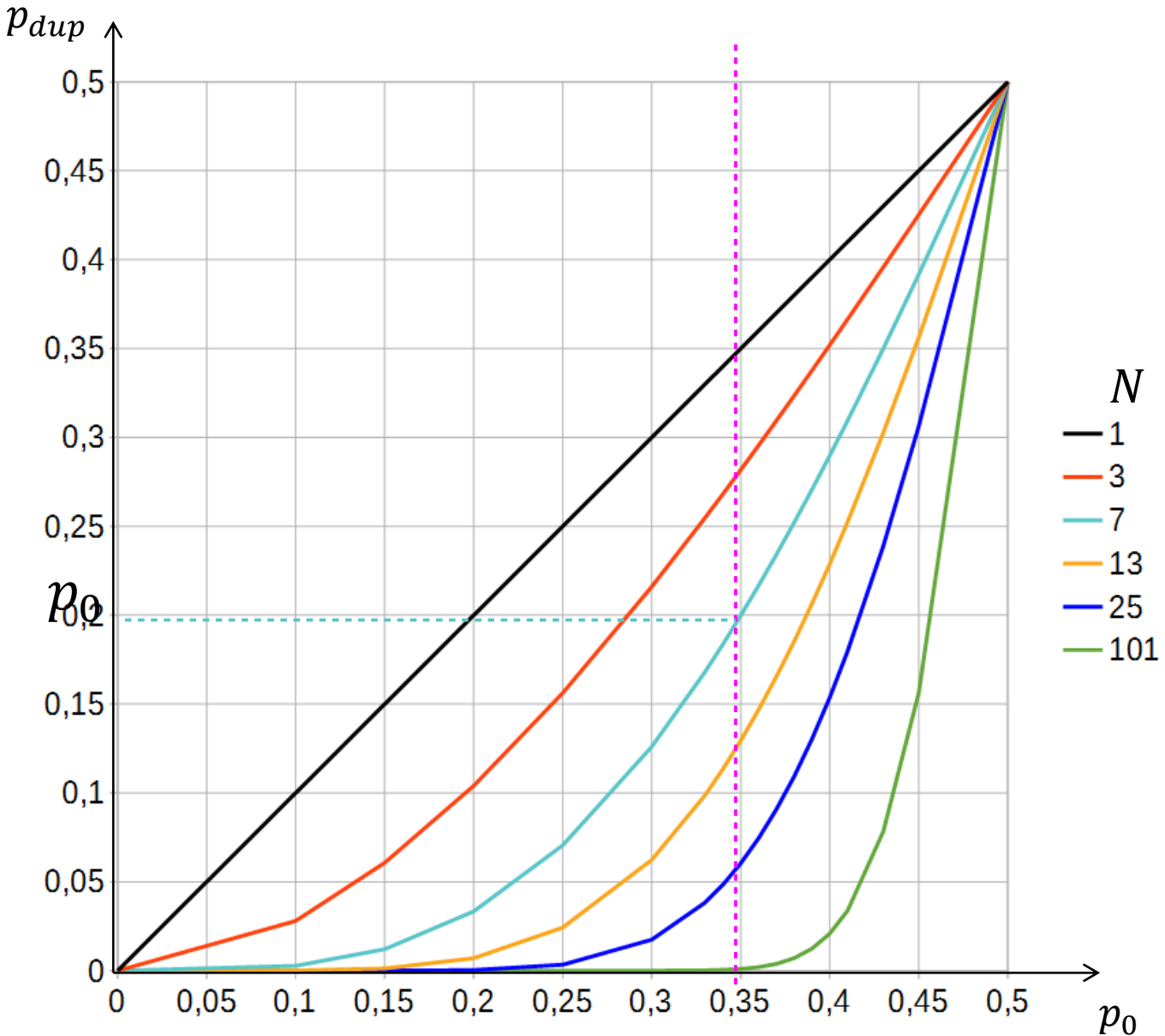
Кодирует всё сообщение.
Разделяет сообщение на слова (несколько битов).
Слово верное, если ВСЕ биты правильные.
Размер кода $C=M+2T$ (в словах), где T – это число ошибочных слов
Восстанавливает долю ошибок $s = T/C = 0.5(1-M/C)$.
Параметры: s, M

Кодирует слово размером $w=3\sim8$ бит (больше неоптимально).
Размер кодового слова $c=2^w$.
Восстанваливает до 0.25 доли ошибочных бит.
Параметры: w

Повторяет каждый бит N раз. N - нечётное.
Параметры: N

Псевдослучайно перемешивает биты.
Параметры: нет

Trade-offs (на примере кодирования дублированием битов)



Избыточность:

$N \to min$

Итоговая ошибка декодирования:

$p_{dup} \to min$

Начальная ошибка:

определяется из предыдущих этапов

Выбор параметров

Параметры кодера:

s — доляя ошибочных слов, исправляемых кодами Рида-Солмона,
w — размер слова, кодируемым Адамаром,
N — число дублирования битов.

Ограничения:

- доля ошибочных битов в декодируемом сообщении *p_0* = 0.35
- размер сообщения (секретного ключа): 64, 128, 256 бит.
- размер шаблона радужки: 26*256=6656 бит (Iritech шаблон).

Оптимальное решение для 64 битов:

$$s = 9/31 \approx 0.29$$
$$w = 5$$
$$N = 13$$

Тесты показали

$$FAR < 10^{-5}$$
$$FRR = 4.2\,\%$$

Для 128 и 256 битов решения не удовлетворяют ограничениям.

Заключения

- На данных рудажной оболочки глаза был построен нечёткий экстрактор и показал хорошие результаты на реальных данных.
- Выяснилось, что реальным данным соответствует доля ошибочных битов выше 1/3, поэтому требуется более высокая избыточность.
- Всё ещё требуются исследования схемы в области криптографии.

Приложения

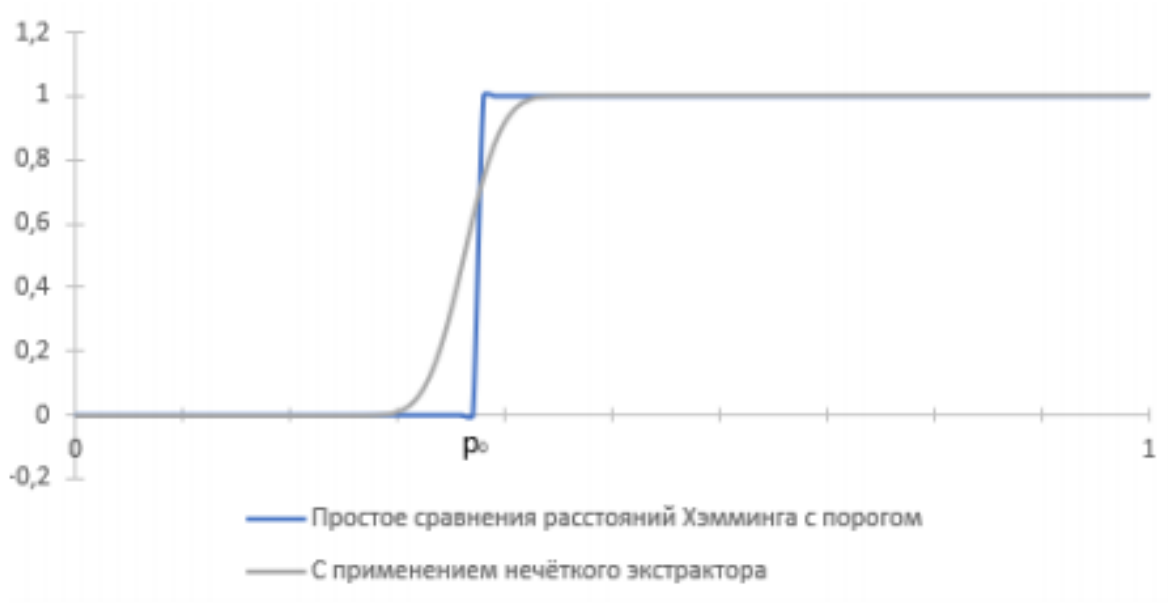


График зависимости вероятности отказа в доступе от расстояния Хэмминга между изображениями оригинальной и предоставляемой радужных оболочек глаза.

$$\max_{N,K,k,t} \quad p_{gen}(N, K, k, t, p_0 + \varepsilon_1) - p_{gen}(N, K, k, t, p_0 - \varepsilon_2)$$

Приложения

$$\mathrm{FRR} = \frac{FN}{FN + TP} = \frac{\sum_{p \in P_{in}} C(p) p_{gen}(p)}{FN + TP},$$

$$\mathrm{FAR} = \frac{FP}{FP + TN} = \frac{\sum_{p \in P_{out}} C(p)(1 - p_{gen}(p))}{FP + TN},$$

$C(p)$ — число попыток авторизации с помощью изображения радужки, где расстояние Хэмминга между ним и оригинальным составляет p,

$p \in P_{in}$ соответствует попыткам аутентификации истинного пользователя,

$p \in P_{out}$ соответствует попыткам аутентификации “чужого”

Приложения

$$\min_{N,K,k,t} \quad \sum_{p \in P_{in}} C(p) p_{gen}(p, N, K, k, t)$$

$$\text{subject to} \quad \sum_{p \in P_{out}} C(p)(1 - p_{gen}(p)) \leq (FP + TN) \times 10^{-4},$$

$$\|\kappa\| \geq k_{th}, \ \|\theta_{lock}\| \leq s_{th}.$$