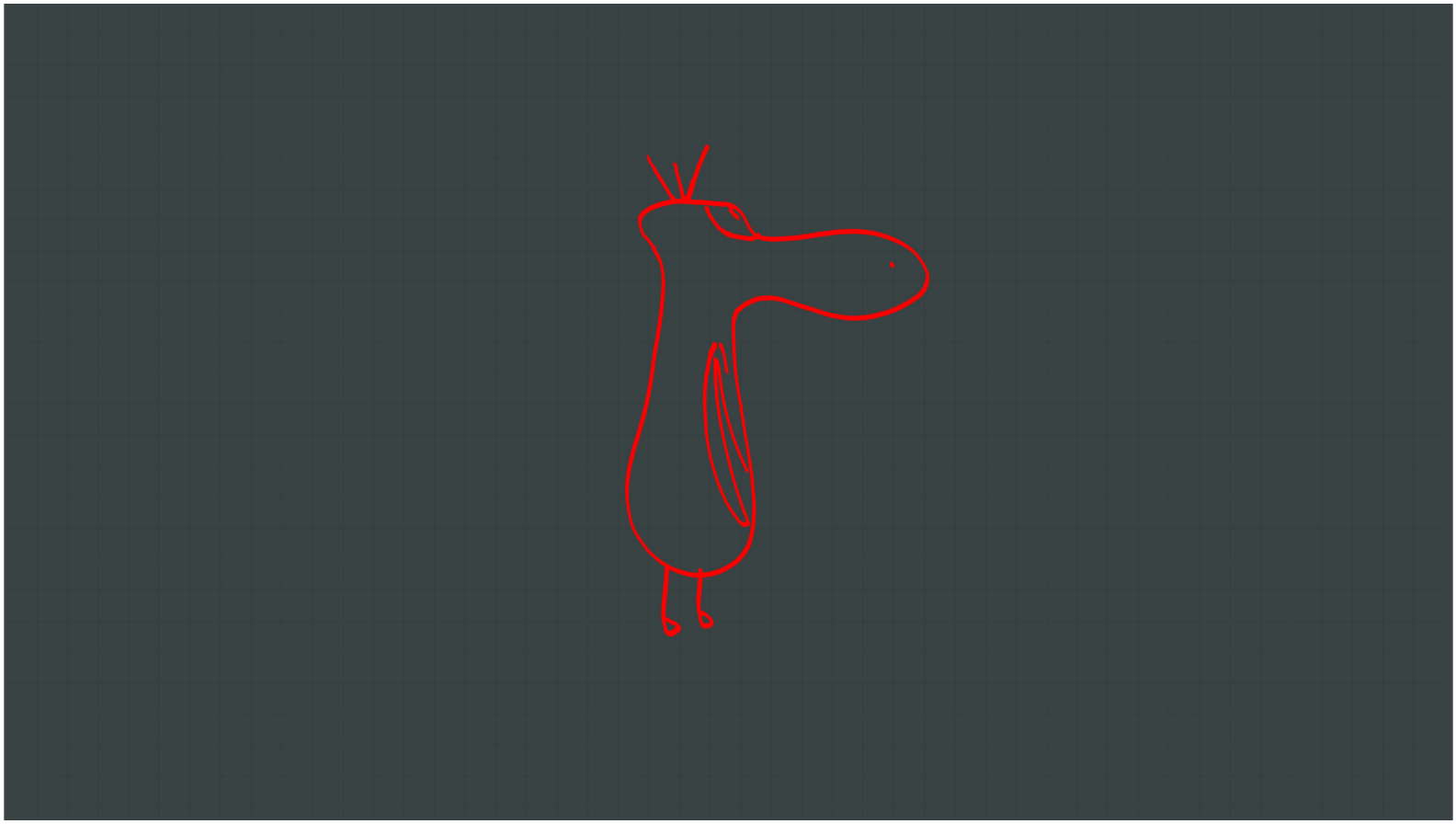


Алгоритм Фуллмера - Штерна

① Парадокс дней рождений

Дано множество A из n элементов

и мы выбираем из него (случ. и равн.) d элементов.

Тогда вер-ть выбора одного и того же элемента

дважды $\approx 1 - e^{\frac{-n^2}{2d}}$

Пример: $n = 23$, $d = 365$. Эти рождения совпадут с вероятностью > 0.5

Факт) Ожидаемое (среднее) число выборов до выборки двух элементов (повт.) равно $\approx \sqrt{\frac{\pi}{2} d}$

$$\sim \binom{n}{t} \to \sqrt{\binom{n}{t}}$$

сложность перебора

Алг.) Вход: H, y, t - кол-во ошибок

Выход: e т.ч. $He^T = y$, $\omega(e) = t$

$$He^T = y \to H_1 e_1^T + H_2 e_2^T = y$$

Строим два списка:

$$H_1 e_1^T = y - H_2 e_2^T$$

$$L_1 = \{ H_1 \cdot e_1^T \mid e_1 \in \mathbb{F}_2^{\frac{n}{2}}, \omega(e_1) = \tfrac{t}{2} \}$$

$$L_2 = \{ y - H_2 e_2^T \mid e_2 \in \mathbb{F}_2^{\frac{n}{2}}, \omega(e_2) = \tfrac{t}{2} \}$$

1. Вписываем L_1: $T[H_1 \cdot e_1^T] = e_1$, $\forall e_1 \in L_1$

2. Перебираем L_2:

$y_2 = L_2$: $y - H_2 e_2^T = y_2$

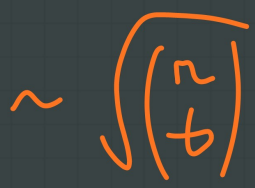
если $y_2 \in L_1 \Rightarrow e = e_1 \| e_2$.

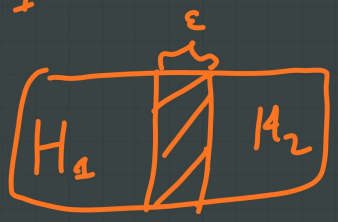
$T(x)$

$\tanh(x)$

$T_{\tanh}(x)$

$1 - e$





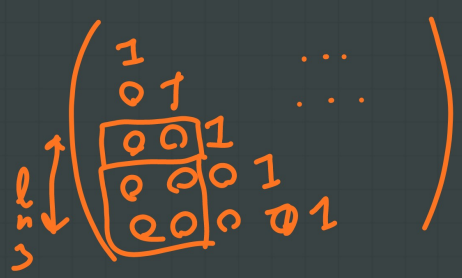
② Алг. Фуммера-Штерна

Вход: H, y, p (какой алг. Lee-Brickell), l

1) P – перест. сист. матр.

2) $\begin{matrix} n-k-l \\ l \end{matrix}\left(\begin{array}{c|c} I & M_1 \\ \square & M_2 \end{array}\right) = UHP = H'$

(частичный метод Гаусса)



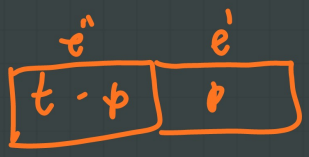
3) Решаем задачу SD для:

M_2 – проверочной матрицы.

y' – синдром: $\tilde{y} = Uy^T = H'\tilde{e}^T = \begin{pmatrix} y'' \\ y' \end{pmatrix}$

p – вес ошибки

} метод на основе парадокса дней рожд.

4) Выбираем решение. $\tilde{e} =$ 

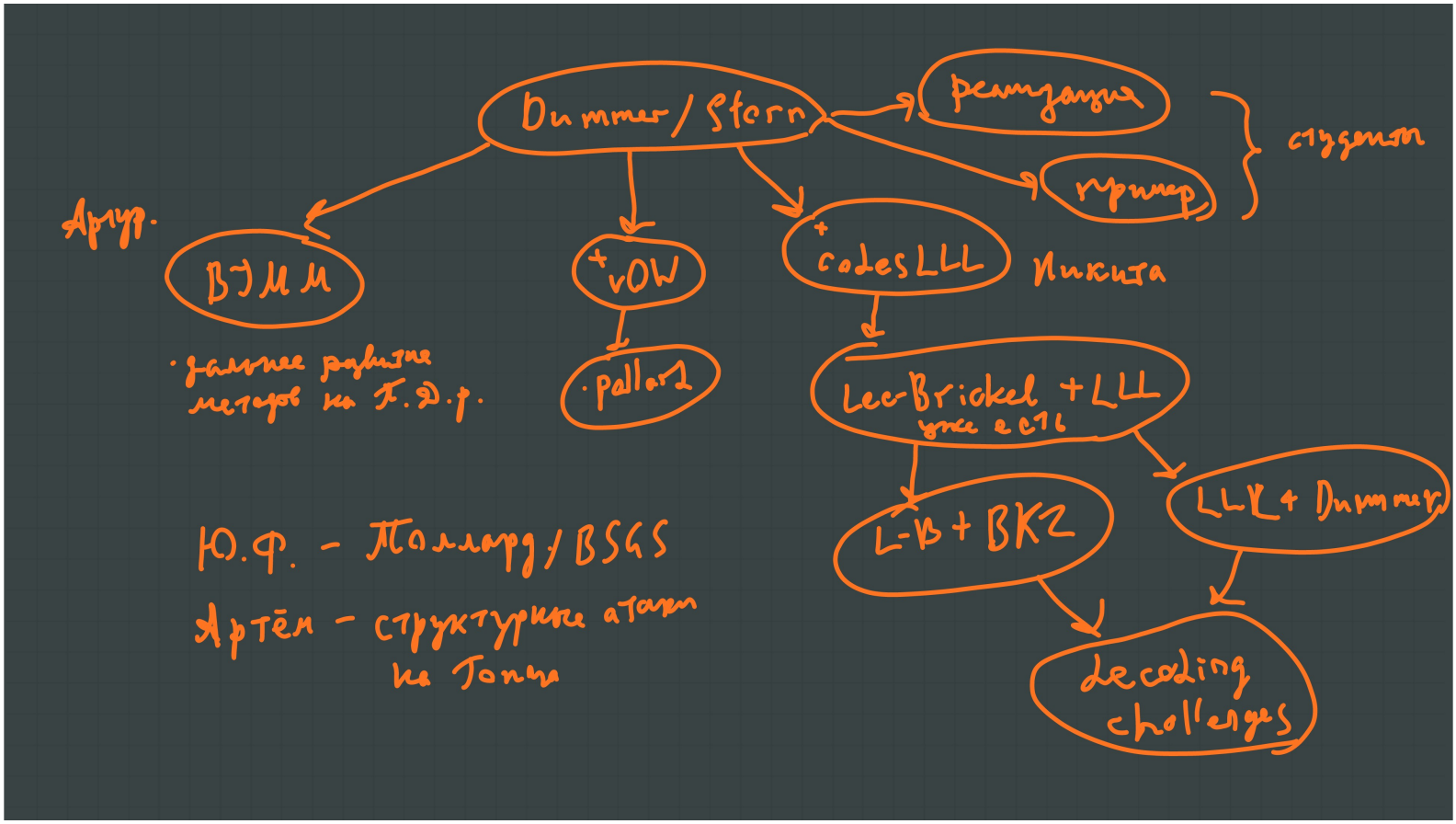
Имеем e' т.ч. $w(e') = p$

Тогда если $e'' = M_1 e'^T + y''$ т.ч.

$w(e'') = w - p$, то

вернуть: $e = (e'', e') P^{-1}$

5) Если нет решений → перейти к шагу 1.


Dumer / Stern
реализация
курсач
студенты
Артур.
BJMM
+ vOW
+ codesLLL
Никита
· дальнее развитие методов на Т.Э.Ф.
· pallard
Lee-Brickel + LLL
уже есть
L-B + BKZ
LLL + Дмитрий
decoding challenges
Ю.Ф. - Поллард / BSGS
Артём - структурные атаки на Гоппу