Алгоритмы декодирования

1. Восстановление сообщ. (ISD)
2. Восстановление структуры кода (секр ключ)
3. Атаки на побочных каналах
4. Гибридные атаки (структурные атаки на расс. сообщ)

I Предв. сведения

В Маке – Элиса

1) $y = m \cdot G + e$
(m – сообщ., e – ошибки/шум)

G – открытый ключ

2) $y' = H e^T$, $e := e(m)$, $w(e) \leqslant t$
(y' – синдром)

Замеч.: · Гоппы · квазициклич. · самодуальные } интересные классы кодов

3) Маскировка
$G \mapsto U \cdot G \cdot P$, U – обр., P – перестановочная

Пример: $G' = (\, I \mid \dots \,)$

4) $(y, G) \to m$ – декодирование (общее)

② Brute-force

Теорема $y = H \cdot e^T = \{$ сумма столбцов H, в которых имеются ошибки $\}$

(для бинарных кодов)

Док-во $h_{j_1} + h_{j_2} + \dots + h_{j_t} = y$. Сложность $O\left(\binom{n}{t}\right)$, $t = 64$

(мин. набор параметров Classic McEliece

③ Алгоритм Prange (Прендж)

Вход: H — проверочная матрица,
y — синдром, $t = w(e)$

Выход: e — вектор ошибок, т.ч. $H \cdot e^T = y$

1. Выбрать случ. перестановочную матр. P

2. Привести $H \cdot P$ в систематическую форму:

$$\Big(\underbrace{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}_{n-k} \Big| \underbrace{M}_{k}\Big) = U H P = H'$$

(при ошибке переходим к шагу 1)

3. $w(Uy) \overset{?}{=} t \Rightarrow e = (Uy, \square) \cdot P^{-1}$

переходим к шагу 1 в противном случае

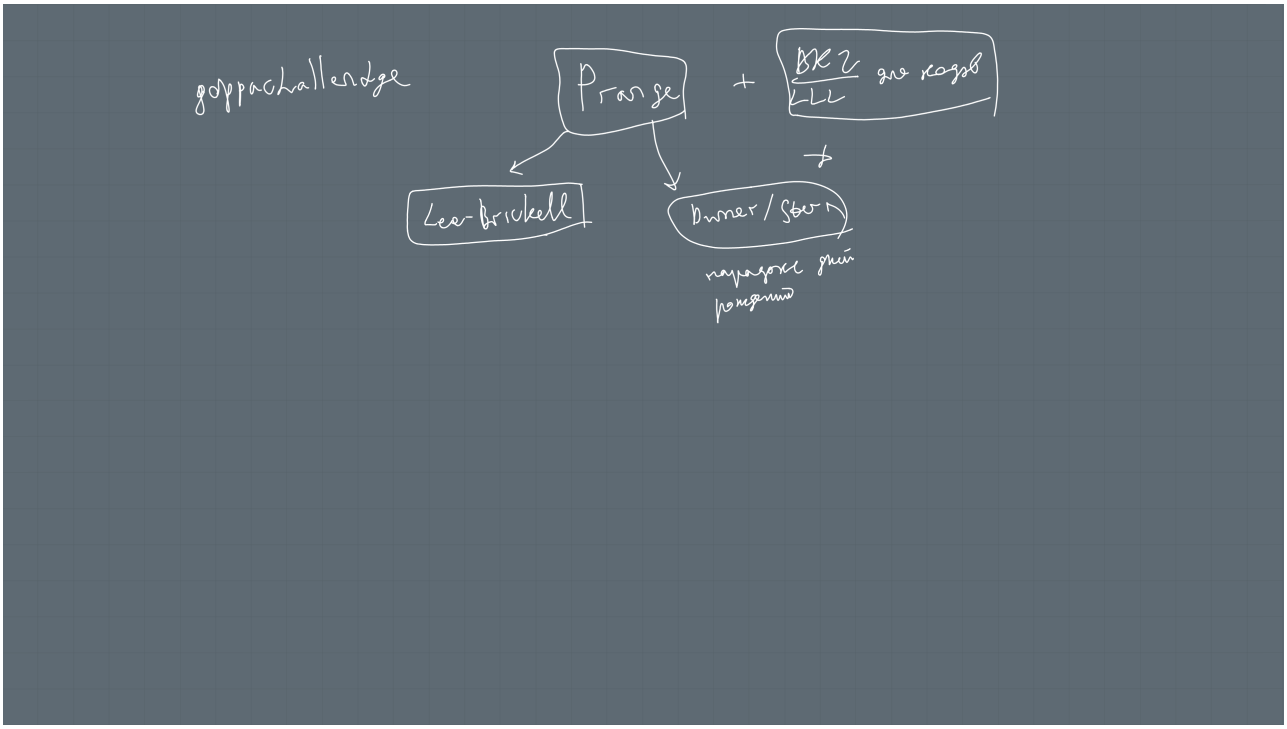
$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$y = He^T$$
$$\Updownarrow$$
$$y' = H'e'^T$$

$y' = Uy, \quad e' = eP$

$w(e') = w(e)$

▲ $y' = UHP(eP)^T = UHPP^Te^T = UHe^T = Uy$ ■


gopparchallenge
Prompt
+
BIRCH
KLL
для кодов
Lee-Brickell
Dumer / Stern
параллельный
режим