НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Криптография, основанная на помехоустойчивом кодировании.

Лекция 2. Различные конструкции кодовых криптосистем

Иванов Ф. И.
к.ф.-м.н., доцент

Национальный исследовательский университет
«Высшая школа экономики»

9 августа 2020 г.

Постановка задачи

- Основное достоинство кодовой криптографии - масштабируемость и стойкость (по крайней мере, пока) к квантовым вычислениям
- Основная проблема - очень длинные ключи, необходимость которых обуславливается требованиями криптографической стойкости
- Как уменьшить длину ключа?
  1. Искать коды, которые можно описать компактно
  2. Учиться декодировать за t хотя бы некоторые множества ошибок
  3. В идеале - хотелось бы построить систему, для которой атака по информационным совокупностям/атака Штерна неприменимы.

Конструкции

- 1978 McEliece: двоичные коды Гоппы
- 1986 Niederreiter: обобщенные коды Рида-Соломона
- 1991 Gabidulin, Paramonov, Tretjakov: коды Габидуллина
- 1994 Sidelnikov: коды Рида-Маллера
- 1996 Janwa-Moreno: алгебро-геометрические коды
- 199* множество конструкций на базе LDPC кодов
- 2005 Berger-Loidreau: подкоды обобщенных РС кодов
- 2006 Wieschebrink, обобщенные РС коды + случайные столбцы в порождающей матрице
- 2008 Baldi-Bodrato-Chiaraluce: MDPC коды, основанные на LDPC кодах

Конструкции

- 2010 Bernstein, Lange, Peters: недвоичные коды Гоппы
- 2012 Misoczki-Tillich-Barreto-Sendrier: MDPC коды
- 2012 Londahl-Johansson: сверточные коды
- 2013 Gaborit, Murat, Ruatta, Zemor: LRPC коды
- 2014 Shrestha, Kim: полярные коды
- 2014 Hooshmand, Shooshtari, Eghlidos, Aref: подкоды полярных кодов

Криптосистема Нидеррайтера

Основана на обобщенных кодах Рида-Соломона:
H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory, 15(2):159-166, 1986.
Параметры:

- (256,128,129) обобщенный код Рида-Соломона над полем F_{256}.
- Уровень защиты — 2^{95}

Атакована Сидельниковым и Шостаковым в 1992 году:
V. M. Sidelnikov and S. O. Shestakov. On the insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Math. Appl., 2:439-444, 1992.
Сложность атаки: $O(n^4)$, где n — длина кода.

Подкоды обобщенных РС кодов

T. Berger and P. Loidreau. How to mask the structure of codes for a cryptographic use. Des. Codes Cryptogr., 35:63-79, 2005.

Size of the key	Transmission rate	Bases enumeration
3850 bits	0.56	2^{71}
3750 bits	0.53	2^{92}
7680 bits	0.58	2^{95}

Идея - добавить к проверочной матрице ОРС кода линейно независимых строк (превратить код в подкод) и умножить на невырожденную матрицу слева.
Атака ($\approx O(n^5)$):
C. Wieschebrink. Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. In Post-Quantum Cryptography, volume 6061 of Lecture Notes in Comput. Sci., pages 61-72, 2010.

Коды Рида-Маллера

V. Sidelnikov. A public-key cryptosytem based on Reed-Muller codes. Discrete Math. Appl., 4(3):191-207, 1994.

Параметры:

- (1024,176,128) или $(2048, 232, 256)$ двоичный код Рида-Маллера.
- Уровень защиты — 2^{72} или 2^{93}

Атакована:

L. Minder and A. Shokrollahi. Cryptanalysis of the Sidelnikov cryptosystem. In EUROCRYPT 2007, pages 347-360, 2007.

Сложность атак: $O(poly(n)) \cdot \exp O(poly(\log(n)))$, где n — длина кода.

	$r = 2$	$r = 3$	$r = 4$
$m = 5$ $(n = 32)$	< 0.01s		
$m = 6$ $(n = 64)$	< 0.01s		
$m = 7$ $(n = 128)$	0.02s	5.261s	
$m = 8$ $(n = 256)$	0.081s	2.059s	
$m = 9$ $(n = 512)$	0.448s	3.462s	176.914s
$m = 10$ $(n = 1024)$	2.46s	26.6s	82197.4s
$m = 11$ $(n = 2048)$	18.34s	1192.71s	no try

Алгебро-геометрические коды

H. Janwa and O. Moreno. McEliece public crypto system using algebraic-geometric codes. Designs, Codes and Cryptography, 1996.
Параметры:

- (171,109,61) АГ-код над полем F_{128}.
- Уровень защиты — 2^{66}

Атакована: A. Couvreur, I. Márquez-Corbella and R. Pellikaan. A polynomial time attack against Algebraic Geometry code based Public-Key Cryptosystems. ISIT 2014, 1446-1450, 2014.

n	k	t	$\mathbf{w}$	key size	time
343	193	54	2^{84}	163 kbits	74 s
729	404	126	2^{182}	833 kbits	21 min
1331	885	168	2^{311}	2730 kbits	67 min

Криптосистема на базе каскадных кодов

H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory, 15(2):159-166, 1986.

Атакована

N. Sendrier. On the concatenated structure of a linear code. AAECC, 9(3):221-242, 1998

Показано, как для произвольного линейного кода найти разложение на каскадную структуру. Далее ищем слова малого веса у компонент.

"Уцелевшие"конструкции

1. На основе кодов Гоппы
2. На основе некоторых QC-LDPC
3. На основе некоторых QC-MDPC

2-3 конструкции имеют вероятностное декодирование. Кроме того, 2 конструкция подвержена атакам на дуальный код.

Квазициклический код

Определение

Линейный код C длины n называется квазициклическим, если сущетвует такое n_0, что любой циклический сдвиг слова $\mathbf{c} \in C$ на n_0 позиций снова является кодовым словом кода C: $x^{n_0 m}\mathbf{c} \mod (x^n - 1) \in C$ для любых $m \in \mathbb{N}$.

Если $n = n_0 p$ то матрицы $\mathbf{G}$ и $\mathbf{H}$ могут быть составлены из $p \times p$ циркулянтов.

Определение

Квадратная матрица $\mathbf{D}$ называется цикрулянтом, если все ее строки/столбцы $\mathbf{d}_i$, $i > 1$ являются различными циклическими сдвигами первой строки/столбца $\mathbf{d}_1$. Таким образом, циркулянт полностью определяется своей первой строкой/столбцом.

QC-LDPC

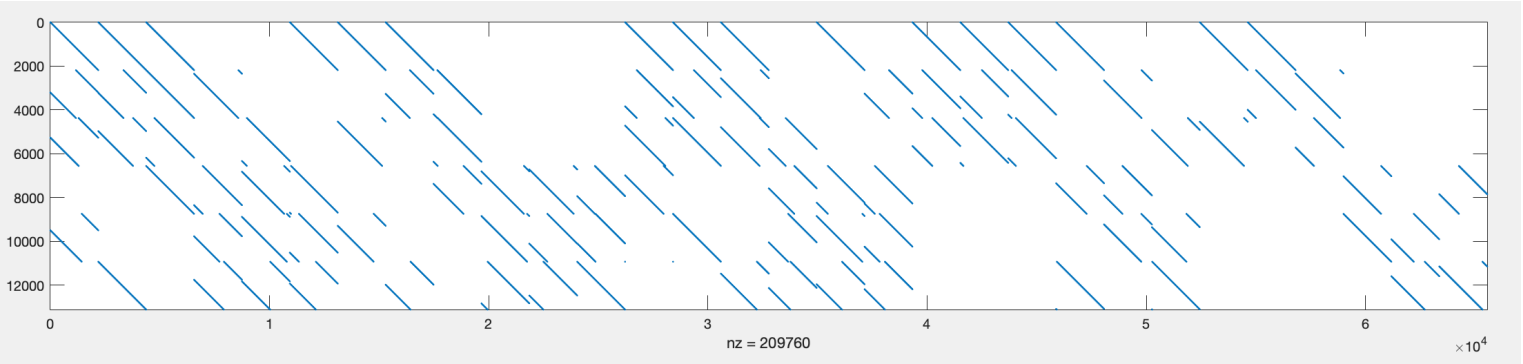
Определение

Линейный код C длины n назыается регулярным квазициклическим кодом с малой плотностью проверок (QC-LDPC), если:

- *Он квазициклический.*
- *Все строки его проверочной матрицы* $\mathbf{H}$ *имеют малый вес* w_r *по сравнению с длиной строки.*
- *Все столбцы его проверочной матрицы* $\mathbf{H}$ *имеют малый вес* w_c *по сравнению с высотой столбца.*

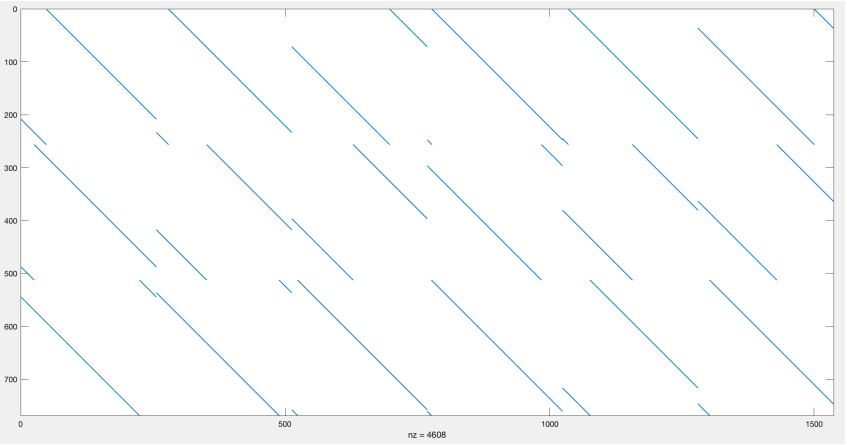
Если вес строки/столбца непостоянен, то такой код называется нерегулярным.

Пример проверочной матрицы нерегулярного кода



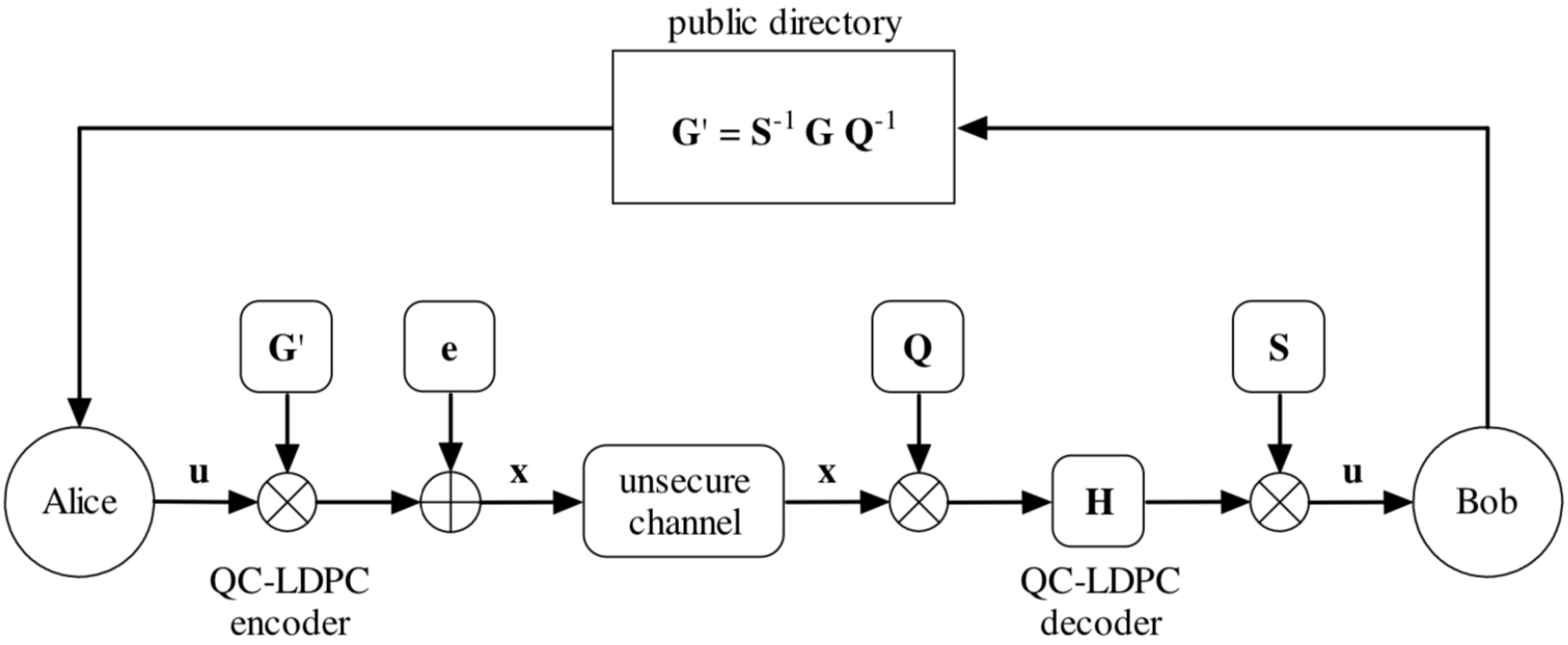
- Длина - 65550
- Число информационных символов - 52440
- Число проверочных символов - 13110
- Скорость кода - 0.8
- Число ненулевых элементов - 209760
- Плотность - $2.44 \cdot 10^{-4}$
- Размер циркулянта - 2185×2185
- Вес строки/столбца циркулянта - 1
- Вес строки - 16
- Веса столбцов - $\{2,3,4\}$
- Число ненулевых циркулянтов - 96

Пример проверочной матрицы регулярного кода



- Длина - 1536
- Число информационных символов - 768
- Число проверочных символов - 768
- Скорость кода - 0.5
- Число ненулевых элементов - 4608
- Плотность - $3.9 \cdot 10^{-3}$
- Размер циркулянта - 256×256
- Вес строки/столбца циркулянта - 1
- Вес строки - 6
- Веса столбца - 3
- Число ненулевых циркулянтов - 18

Общая схема криптосистемы на QC-LDPC



Генерация ключей - I

- Выбирают подходящие параметры d_v, n_0, k_0: $n_0 > k_0$ - малые числа и p - достаточно большое число. Для компактной записи часто берут $k_0 = n_0 - 1$.
- Секретный ключ - это разреженная проверочная матрица

$$\mathbf{H} = (\mathbf{H}_1\, \mathbf{H}_2\, \ldots\, \mathbf{H}_{n_0}),$$

  где $\mathbf{H}_i$ — циркулянты, вес каждой строки равен d_v
- Будем считать, что $\mathbf{H}_{n_0}$ не вырождена. Тогда построим порождающую матрицу $\mathbf{G}$ из $\mathbf{H}$:

$$\mathbf{G} = (\mathbf{I}\, \mathbf{R}),$$

  где $\mathbf{I}$ — $(n_0 - 1)p \times (n_0 - 1)p$ единичная матрица и $\mathbf{R}$ имеет вид:

$$\mathbf{R} = \left(\left(\mathbf{H}_{n_0}^{-1}\mathbf{H}_1\right)^T \left(\mathbf{H}_{n_0}^{-1}\mathbf{H}_2\right)^T \ldots \left(\mathbf{H}_{n_0}^{-1}\mathbf{H}_{n_0-1}\right)^T \right)^T.$$

Генерация ключей - II

- Строим еще 2 секретные матрицы: $k \times k$ невырожденную матрицу $\mathbf{S}$ и $n \times n$ невырожденную матрицу $\mathbf{Q}$ с весом строки/столбца m.
- Публичный ключ имеет вид:

$$\mathbf{G}' = \mathbf{S}^{-1}\mathbf{G}\mathbf{Q}^{-1}$$

- Секретный ключ - это тройка $(\mathbf{S},\mathbf{G},\mathbf{Q})$.

Шифрование/расшифрование

- Боб шифрует сообщение $\mathbf{m}$ длины k следующим образом: $\mathbf{x} = \mathbf{m}\mathbf{G}' + \mathbf{e}$, где $wt(\mathbf{e}) = t' \leq t/m$, где t - корректирующая способность QC-LDPC кода.
- Алиса принимает сообщение $\mathbf{x}$ от Боба, а затем:
  1. Умножает принятое сообщение на $\mathbf{Q}$:

$$\mathbf{x}' = \mathbf{x}\mathbf{Q} = \mathbf{m}\mathbf{S}^{-1}\mathbf{G} + \mathbf{e}\mathbf{Q}$$

  2. Алиса использует алгоритм декодирования принятого слова (предполагается, что $wt(\mathbf{e}\mathbf{Q}) \leq t$).
  3. Алиса получает $\mathbf{m}\mathbf{S}^{-1}$
  4. $\mathbf{m} = \mathbf{m}\mathbf{S}^{-1}\mathbf{S}$.

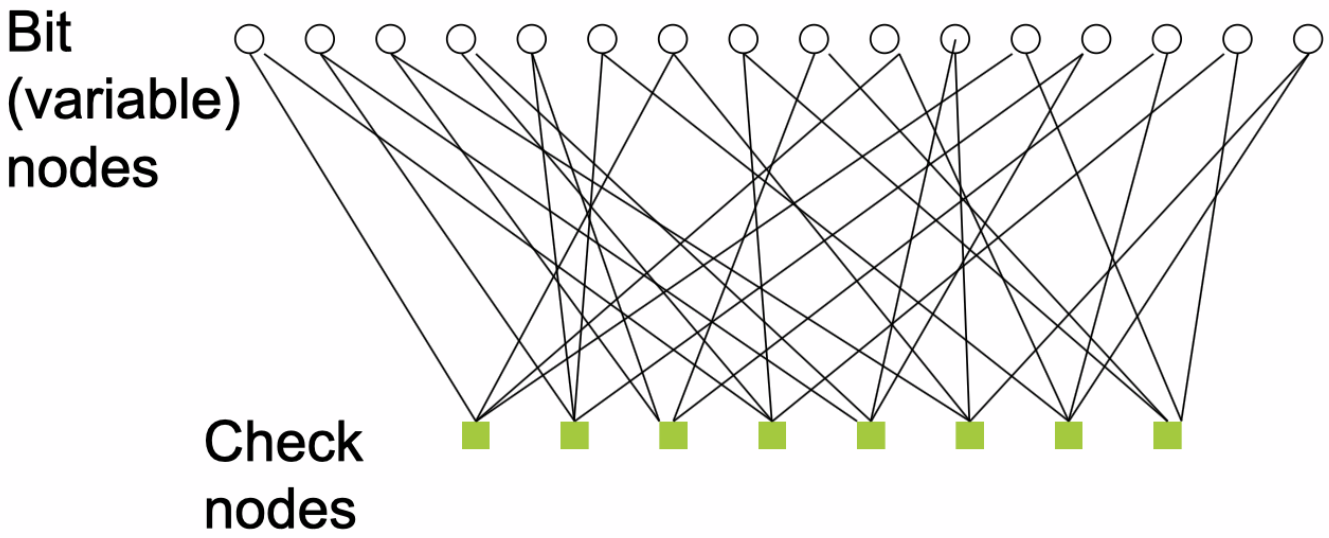
Длина открытых ключей

p [bits]	4096	5120	6144	7168	8192	9216	10240	11264	12288	13312	14336	15360	16384
$n_0 = 3$	1024	1280	1536	1792	2048	2304	2560	2816	3072	3328	3584	3840	4096
$n_0 = 4$	1536	1920	2304	2688	3072	3456	3840	4224	4608	4992	5376	5760	6144

- Публичный ключ - это матрица из $k_0 \times n_0 = (n_0 - 1)n_0$ циркулянтов размера $p \times p$
- Каждый циркулянт требует p бит для хранения
- Таким образом, размер публичного ключа - $n_0 k_0 p$ бит.
- В систематическом виде размер ключа можно снизить до $(n_0 - 1)p$ бит

Граф Таннера

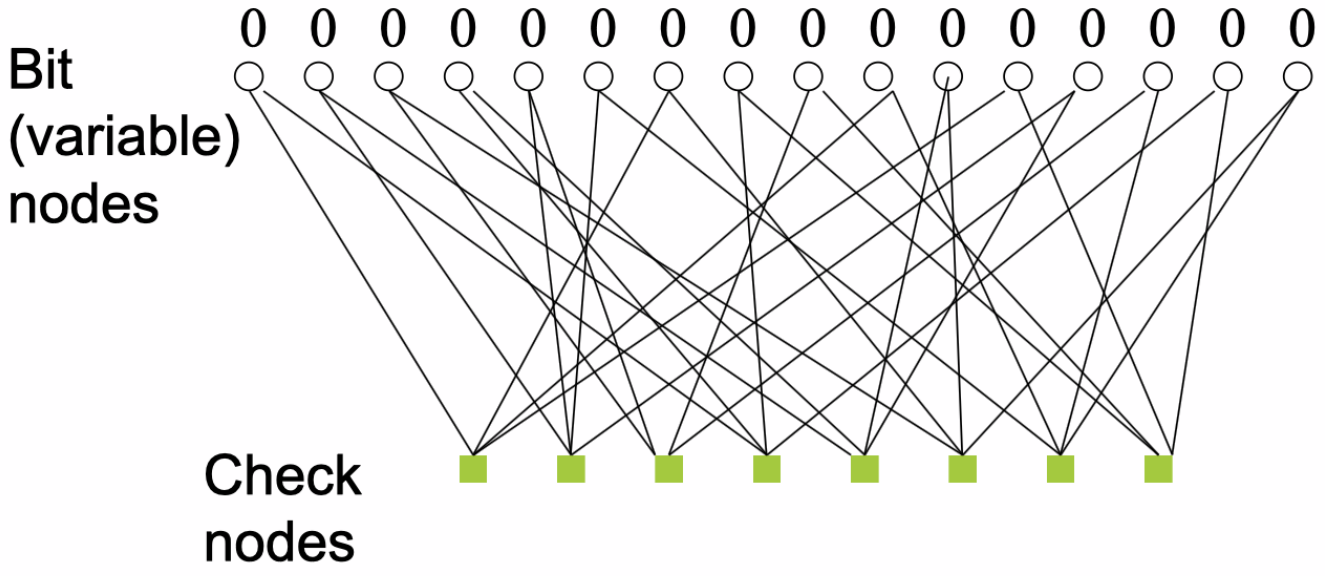
Любой код (не обязательно низкоплотностный) можно представить в виде графа Таннера. Это двудольный граф:



- Вершины-проверки (check nodes) - C_i
- Вершины-символы (variable nodes) - V_j
- Ребро соединяет C_i и V_j, если $h_{ij} = 1$

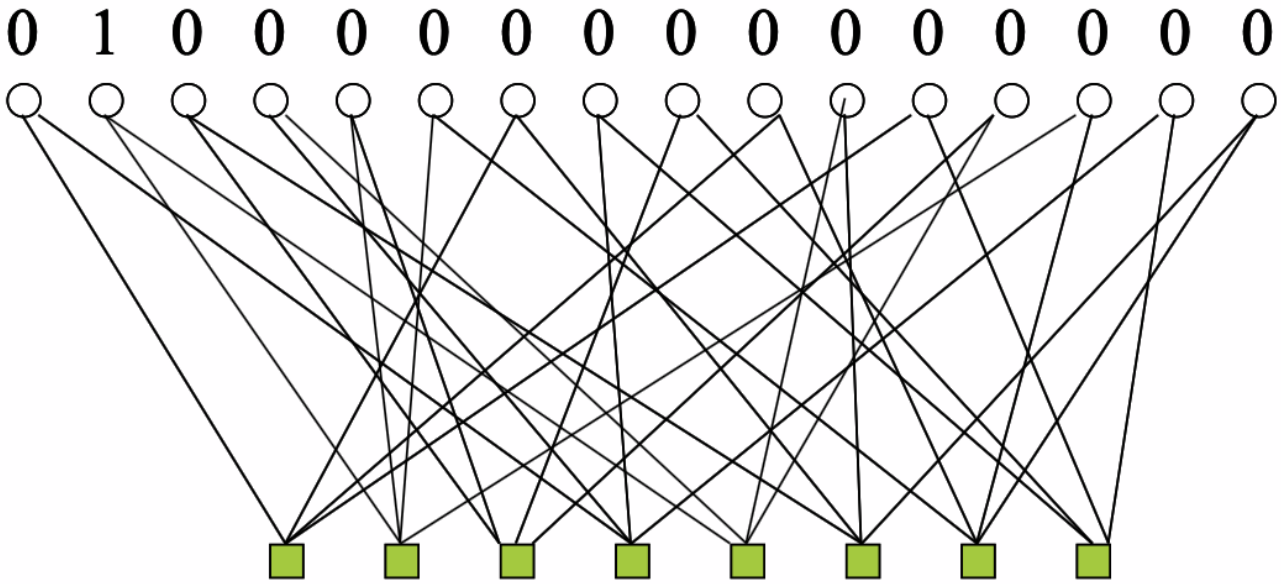
Пример декодирования

Предположим, что передавались нули:



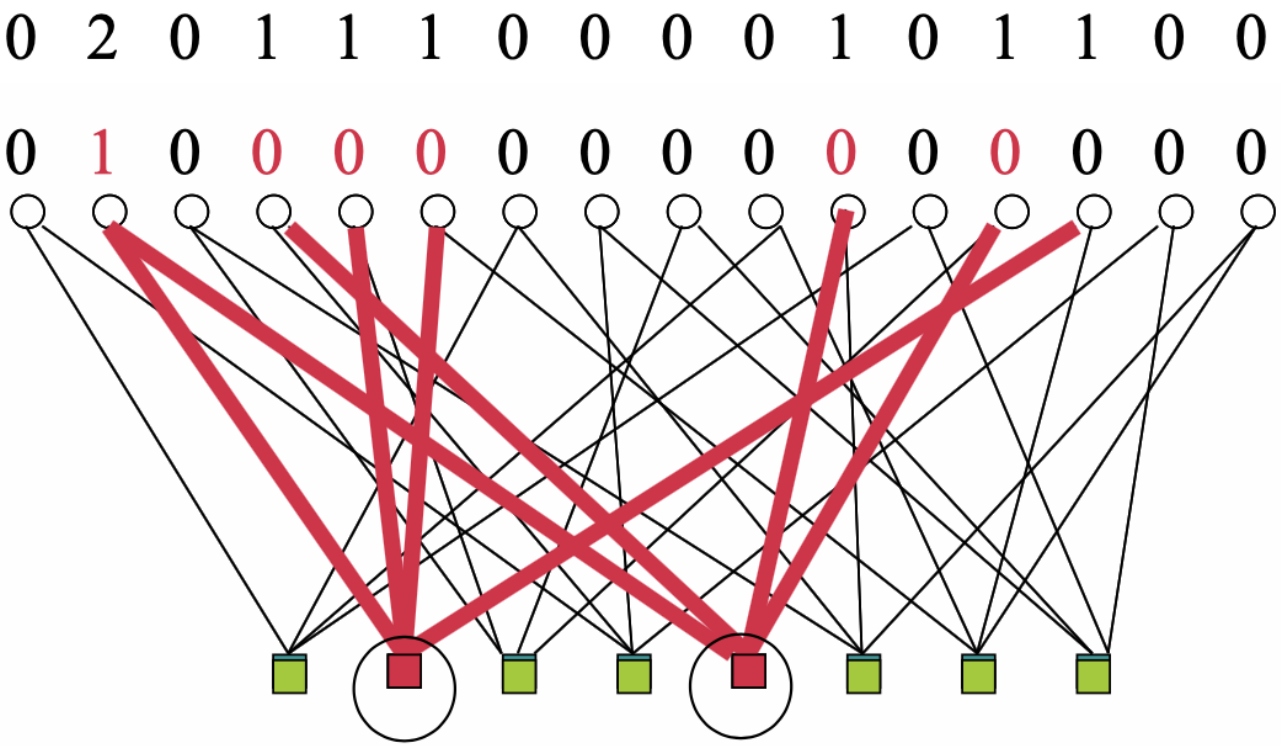
Пример декодирования - II

И произошла одна ошибка:



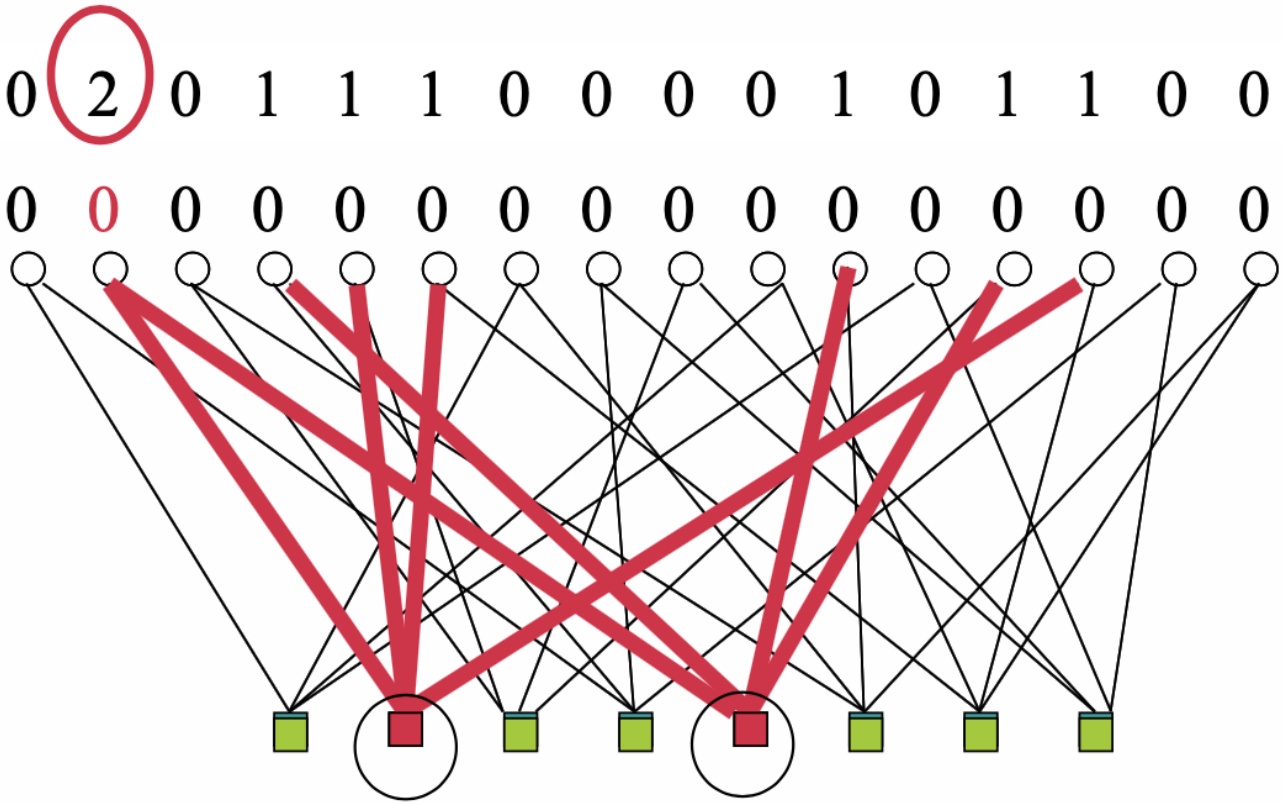
Пример декодирования - III

Для каждого символа вычислим число невыполненных проверок:



Пример декодирования - IV

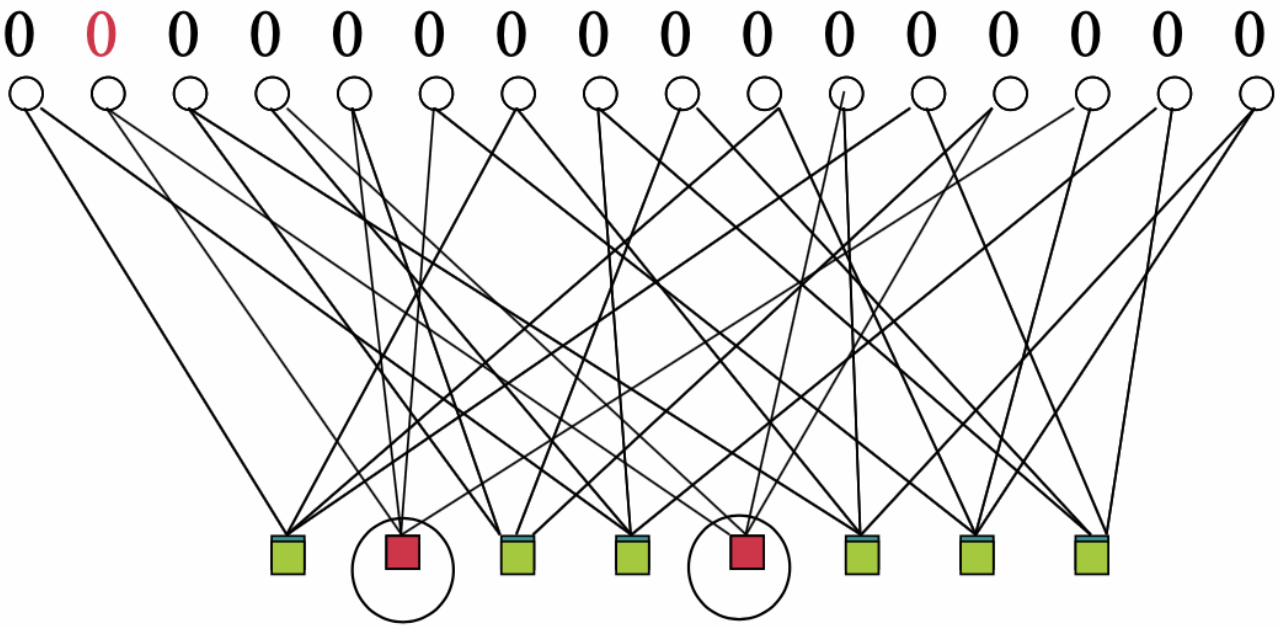
Если число невыполенных проверок превышает некоторый порог - то проинвертируем символ



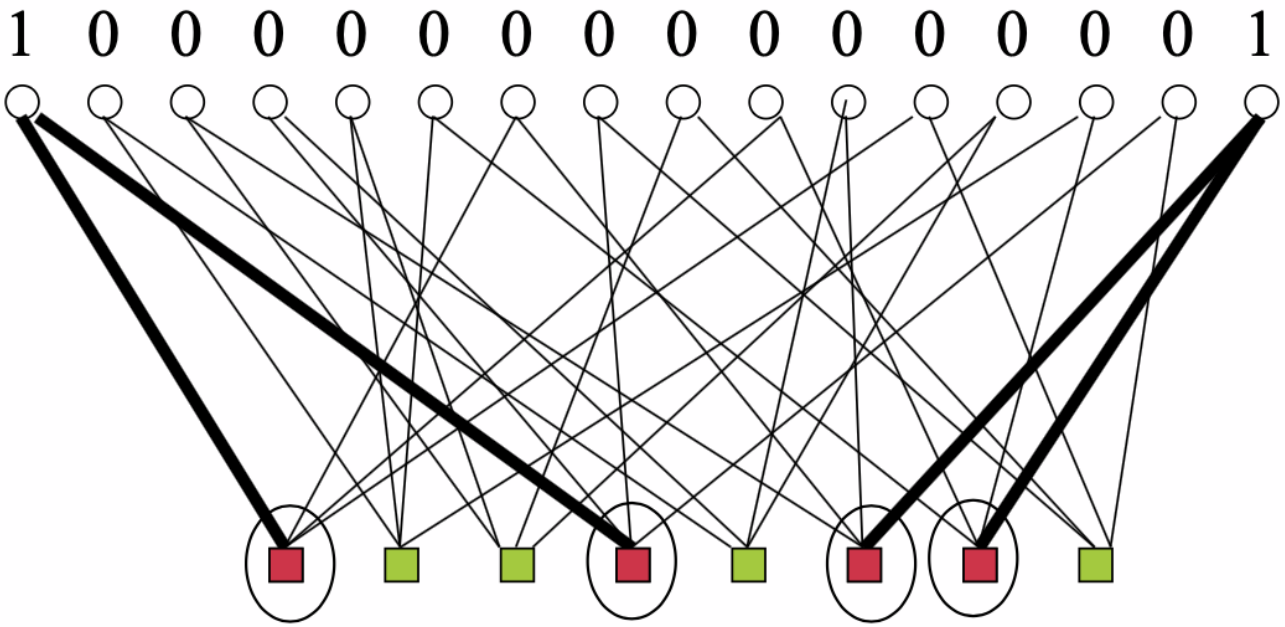
Порог = 1.

Пример декодирования - V

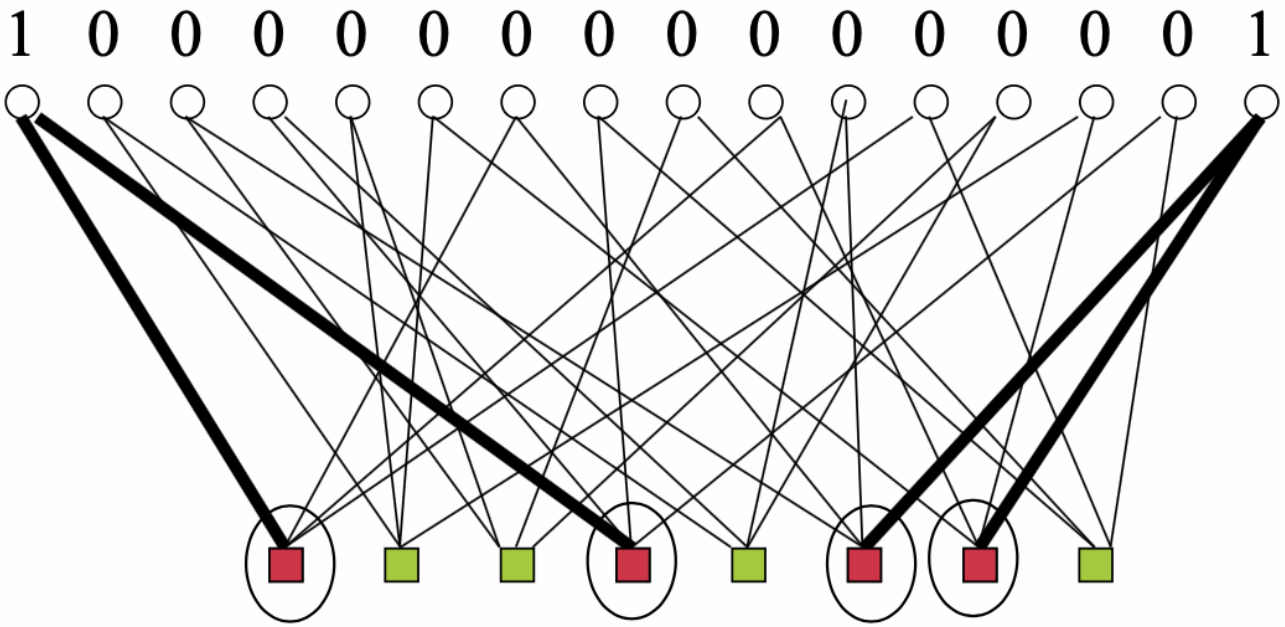
Теперь все проверки выполнены



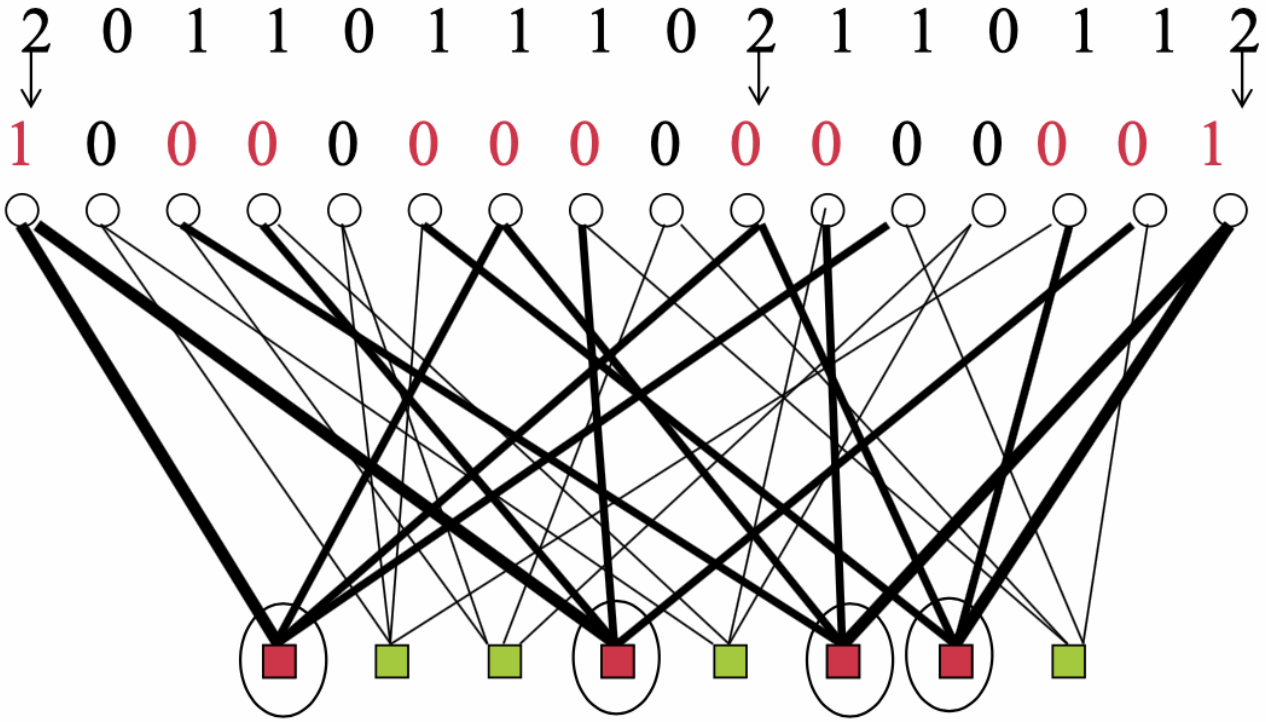
Случай двух ошибок - I



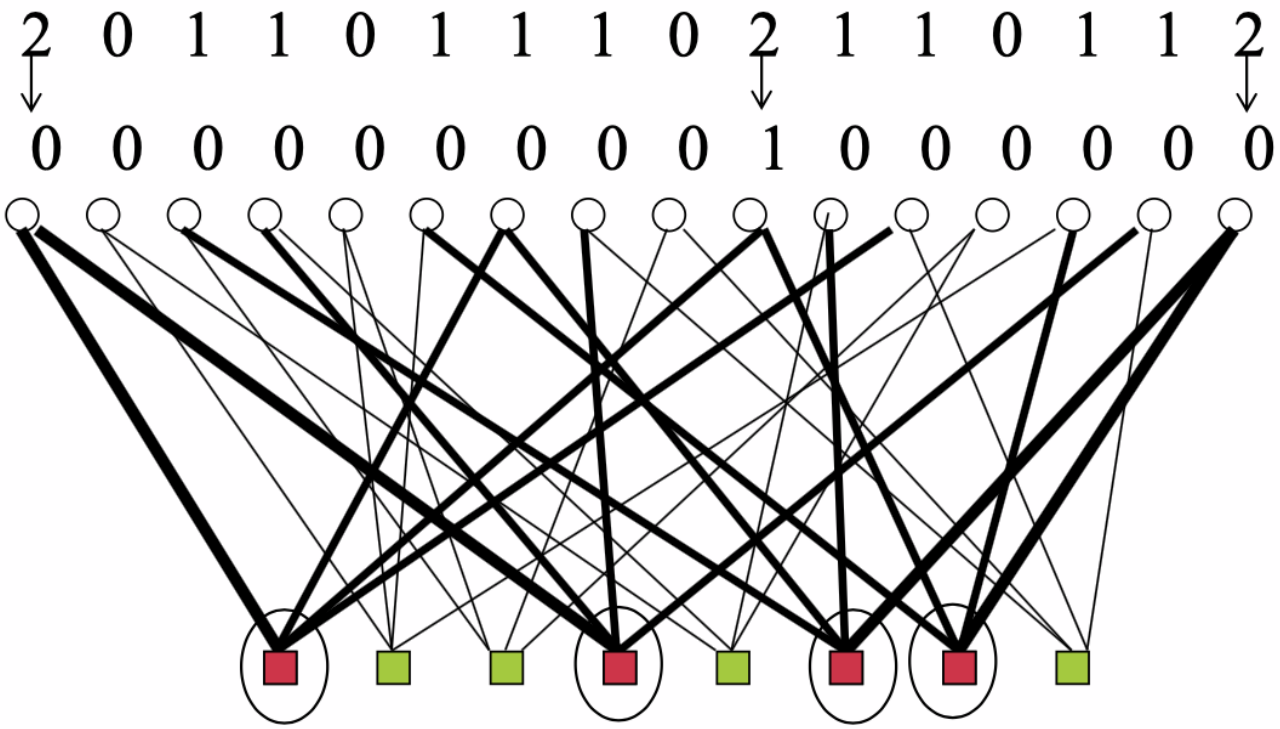
Случай двух ошибок - II



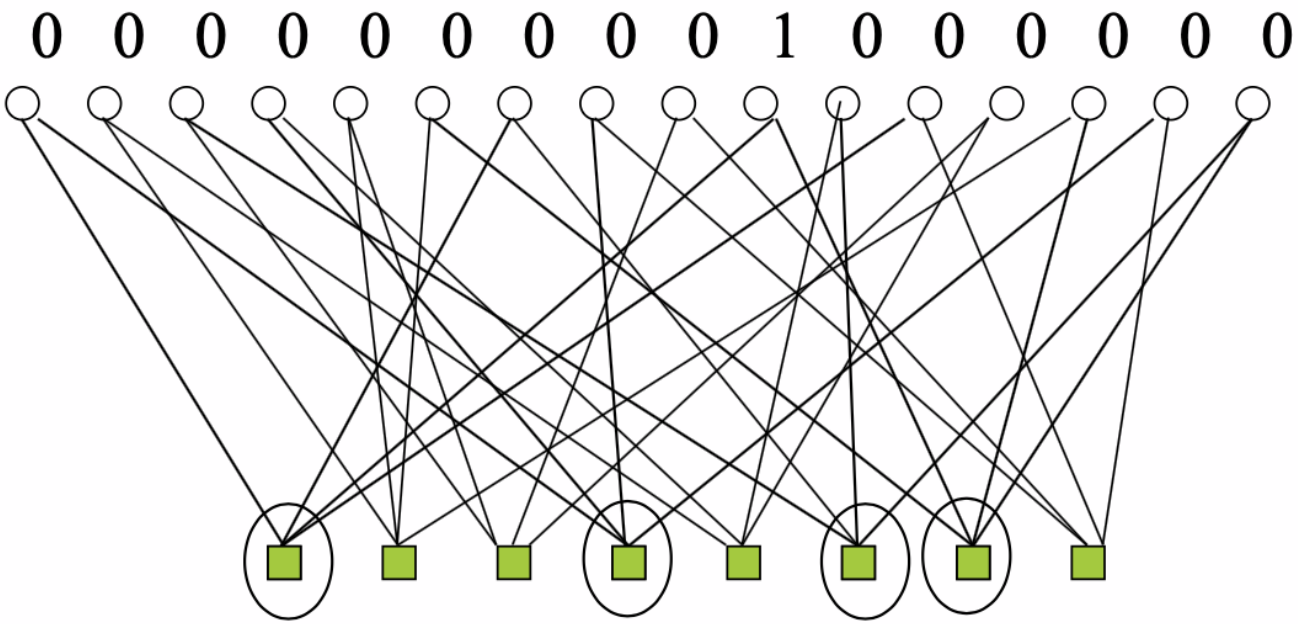
Случай двух ошибок - III



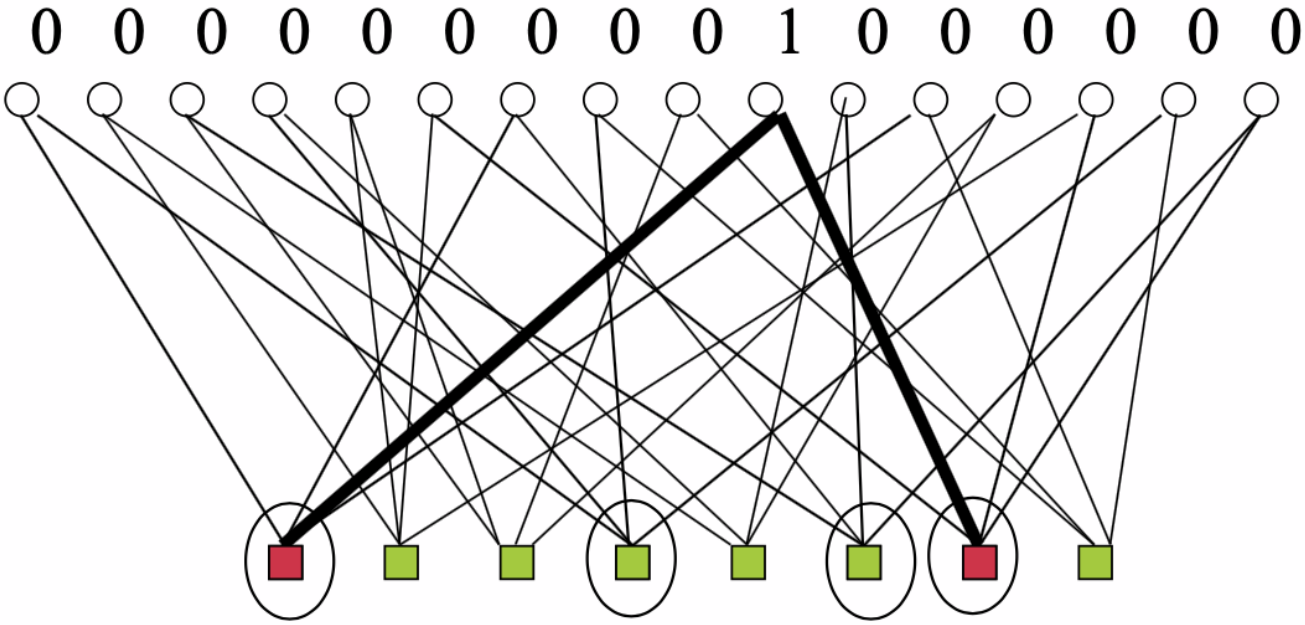
Случай двух ошибок - IV



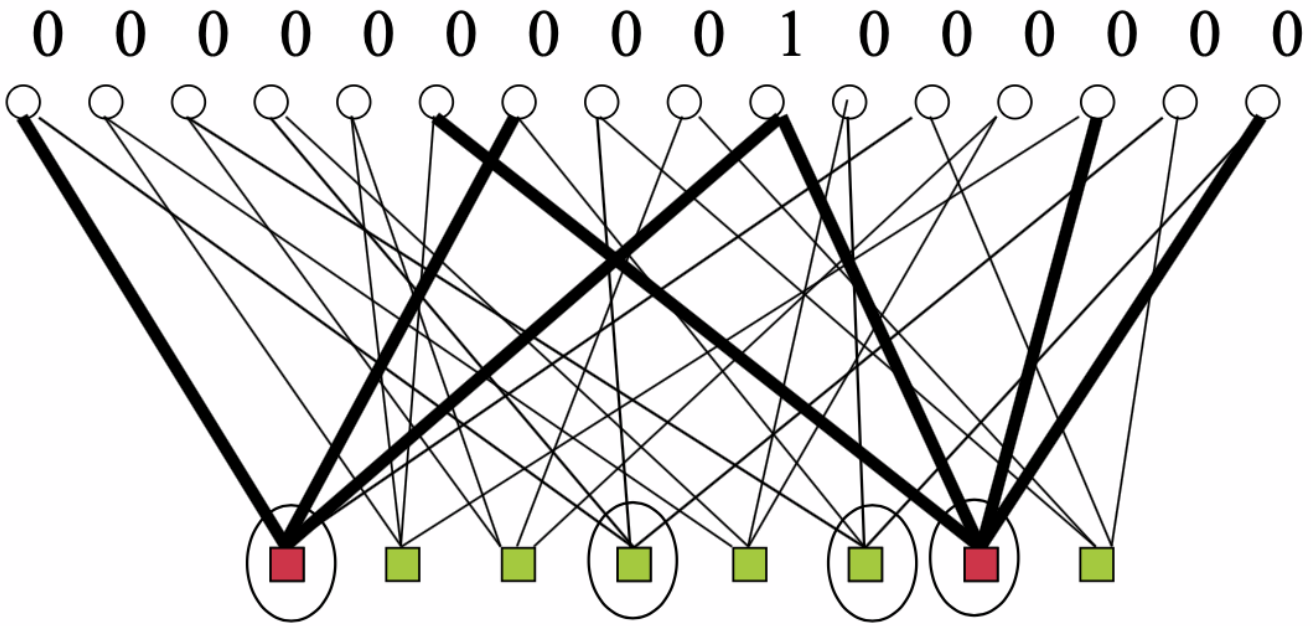
Случай двух ошибок - V



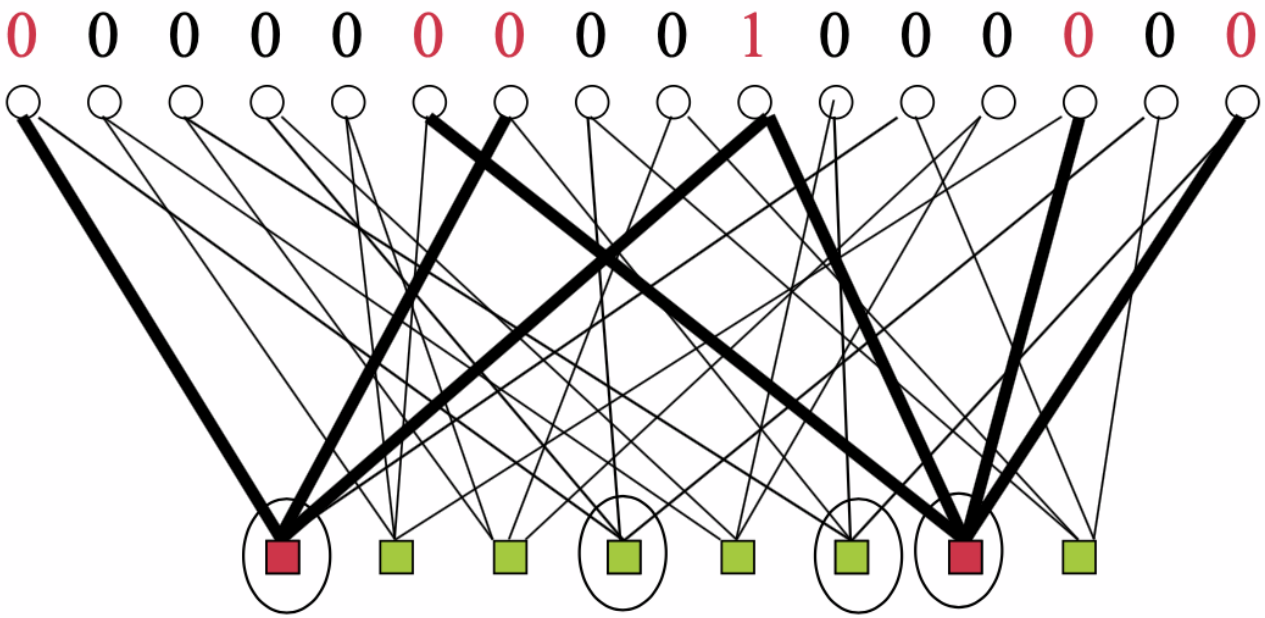
Случай двух ошибок - VI



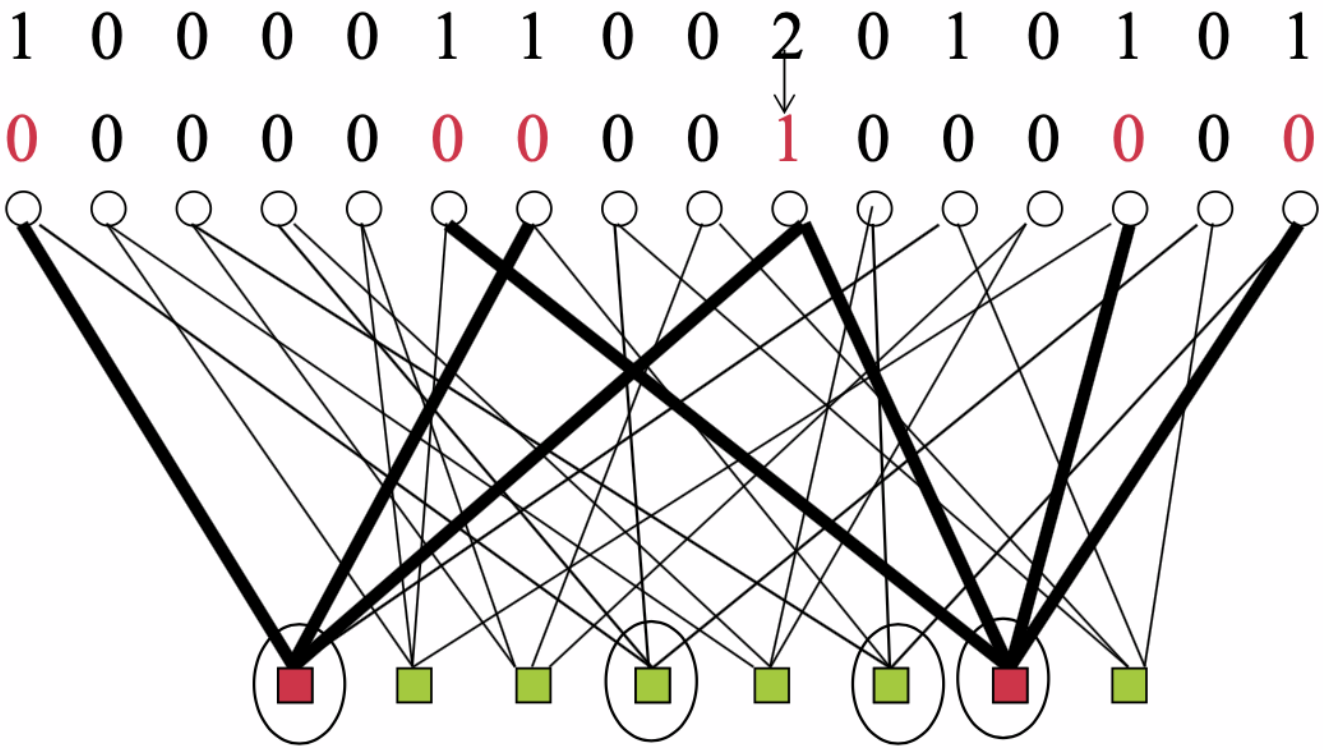
Случай двух ошибок - VII



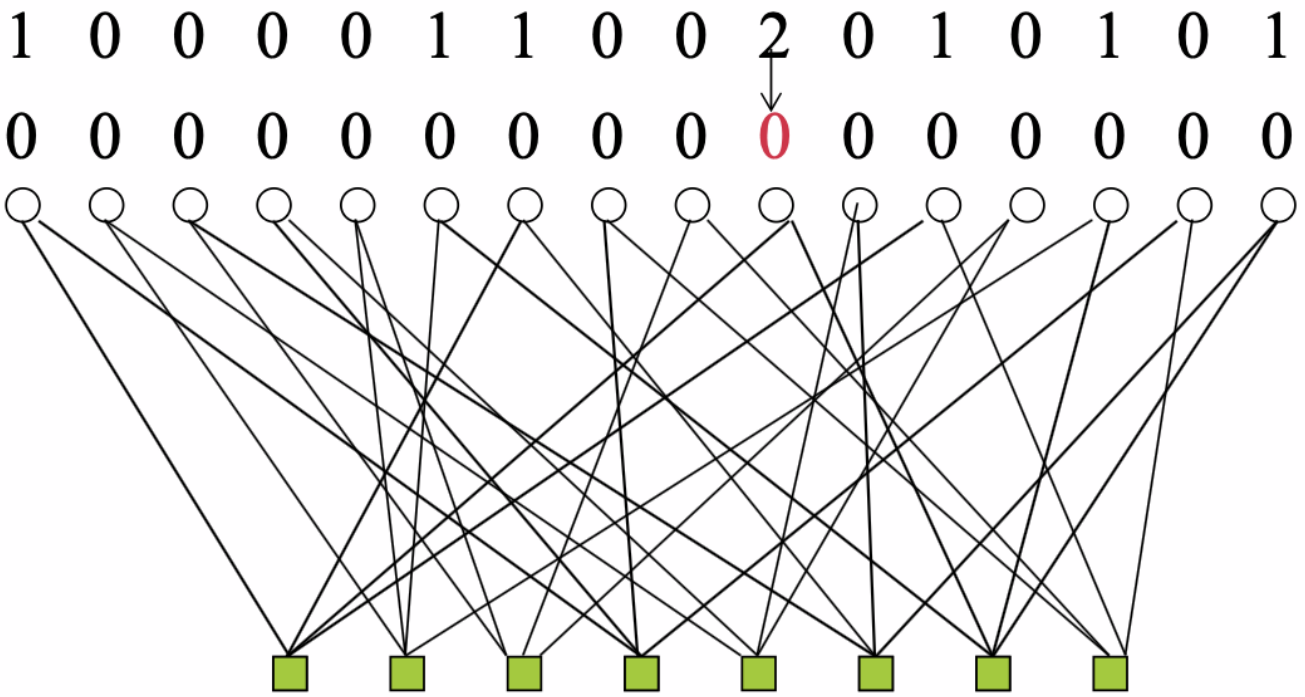
Случай двух ошибок - VIII



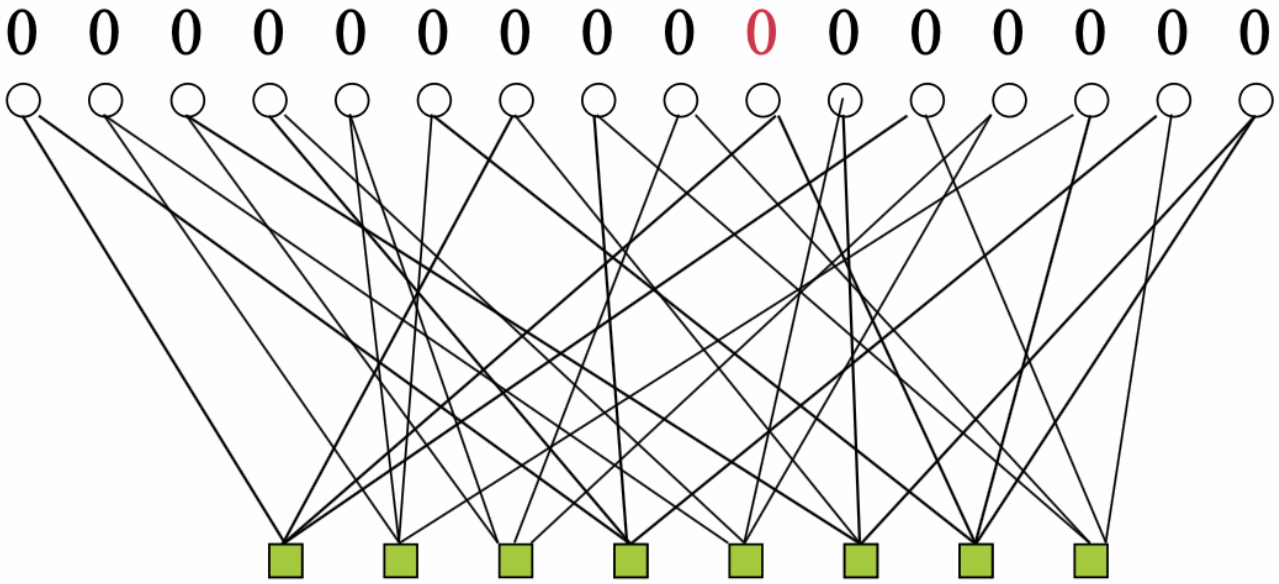
Случай двух ошибок - XI



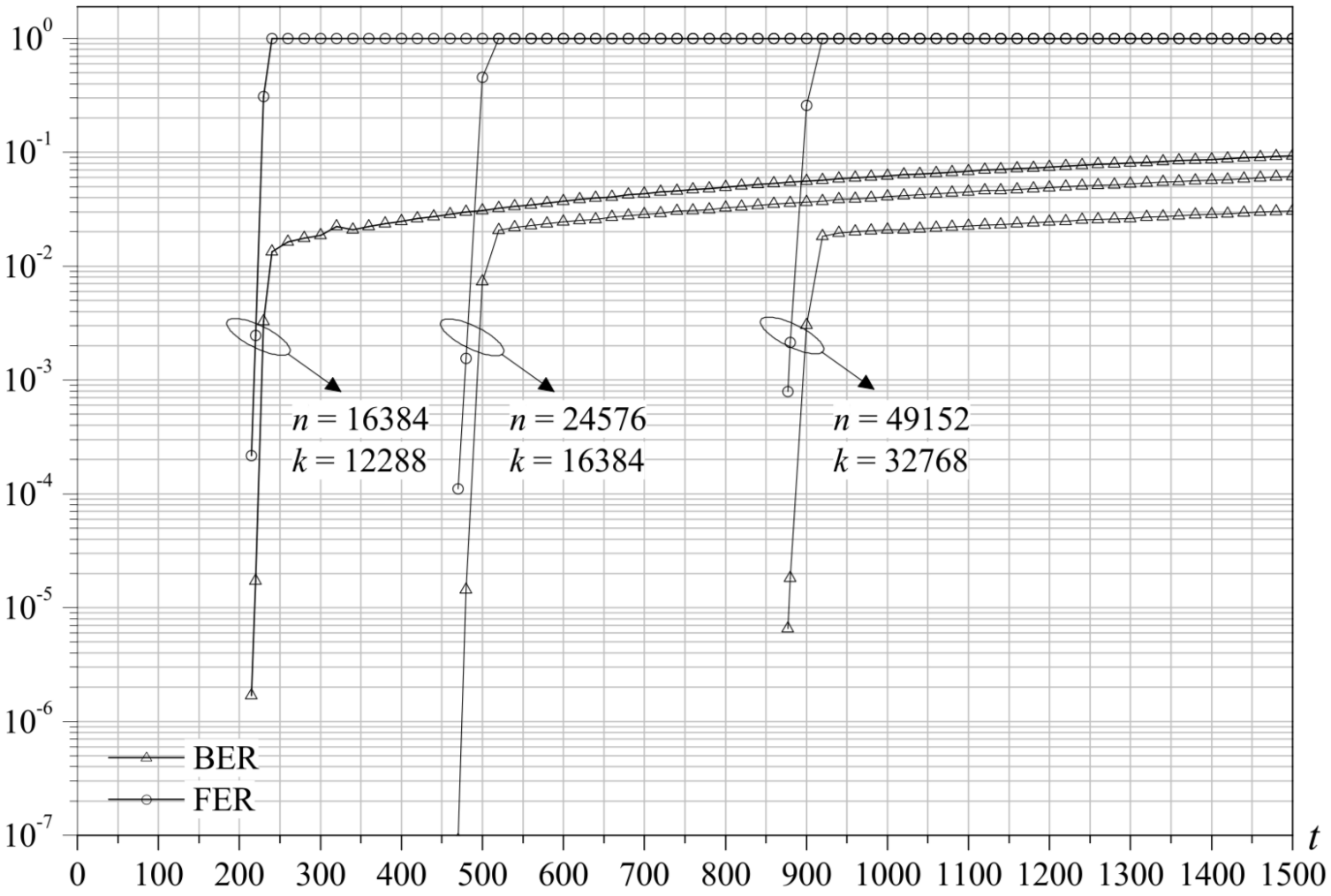
Случай двух ошибок - X



Случай двух ошибок - XI



Результаты моделирования



Оптимизация алгоритма декодирования

Оптимизация заключается в том, как требуется выбирать порог b, после достижения которого требуется инвертировать бит.
Порог - это число невыполенных проверок.
В оригинальной работе Галлагера предлагается 2 подхода:

1. $b = d_v - 1$
2. b может изменяться от $\frac{d_v}{2}$ до $d_v - 1$ в процессе декодирования

Оптимизация алгоритма декодирования

1. p^{cc} — вероятность того, что бит не искажен и проверка на четность для него выполнена
2. p^{ci} — вероятность того, что бит не искажен и проверка на четность для него не выполнена
3. p^{ic} — вероятность того, что бит искажен и проверка на четность для него выполнена
4. p^{ii} — вероятность того, что бит искажен и проверка на четность для него не выполнена

Можно показать, что

$$\begin{cases} p^{cc}(q_l) = \sum\limits_{\substack{j=0 \\ j \text{ even}}}^{\min\{d_c-1,q_l\}} \frac{\binom{d_c-1}{j}\binom{n-d_c}{q_l-j}}{\binom{n-1}{q_l}} \\ p^{ci}(q_l) = \sum\limits_{\substack{j=0 \\ j \text{ odd}}}^{\min\{d_c-1,q_l\}} \frac{\binom{d_c-1}{j}\binom{n-d_c}{q_l-j}}{\binom{n-1}{q_l}} \\ p^{ic}(q_l) = \sum\limits_{\substack{j=0 \\ j \text{ even}}}^{\min\{d_c-1,q_l\}} \frac{\binom{d_c-1}{j}\binom{n-d_c}{q_l-1-j}}{\binom{n-1}{q_l-1}} \\ p^{ii}(q_l) = \sum\limits_{\substack{j=0 \\ j \text{ odd}}}^{\min\{d_c-1,q_l\}} \frac{\binom{d_c-1}{j}\binom{n-d_c}{q_l-1-j}}{\binom{n-1}{q_l-1}} \end{cases}$$

Где $d_c = n_0 d_v$, q_l - среднее число ошибок после l-ой итерации, а $q_0 = t = t'm$.

Оптимизация алгоритма декодирования

Пусть после l-ой итерации бит искажен. Найдем вероятность того, что во время последующей итерации сообщение, исходящее из соответствующего узла переменных, будет правильным:

$$f^b(q_l) = \sum_{j=b}^{d_v-1} \binom{d_v-1}{j} \left[p^{ic}(q_l)\right]^j \left[p^{ii}(q_l)\right]^{d_v-1-j}$$

Точно так же вероятность неправильной оценки в одной итерации алгоритма того бита, который не является ошибочным, может быть выражена как:

$$g^b(q_l) = \sum_{j=b}^{d_v-1} \binom{d_v-1}{j} \left[p^{ci}(q_l)\right]^j \left[p^{cc}(q_l)\right]^{d_v-1-j}.$$

В идеальном предположении об отсутствии циклов в графе Таннера (что подразумевает рассмотрение кода бесконечной длины) среднее количество остаточных битовых ошибок на l-й итерации, q_l, приводит к:

$$q_l = t - t \cdot f^b(q_{l-1}) + (n-t) \cdot g^b(q_{l-1}).$$

Оптимизация алгоритма декодирования

Для уравнения

$$q_l = t - t \cdot f^b\left(q_{l-1}\right) + (n-t) \cdot g^b\left(q_{l-1}\right).$$

подбирается такой порог $t_{th} = t$, что $\lim\limits_{l \to \infty} q_l = 0$.

Это также позволяет оптимизировать порог b: для каждого b от $\frac{d_v}{2}$ до $d_v - 1$ решается задача оптимизации и выбирается максимальный $t_{th}(b')$ и соответствующее значение порога b'.

p [bits]		4096	5120	6144	7168	8192	9216	10240	11264	12288	13312	14336	15360	16384
$n_0 = 3$	$d_v = 13$	190	237	285	333	380	428	476	523	571	619	666	714	762
	$d_v = 15$	192	240	288	336	384	432	479	527	575	622	670	718	766
$n_0 = 4$	$d_v = 13$	181	225	270	315	360	405	450	495	540	585	630	675	720
	$d_v = 15$	187	233	280	327	374	421	468	515	561	608	655	702	749

Число вносимых Бобом ошибок ($m = 7$) и уровень защиты

p [bits]		4096	5120	6144	7168	8192	9216	10240	11264	12288	13312	14336	15360	16384
$n_0 = 3$	$d_v = 13$	27	33	40	47	54	61	68	74	81	88	95	102	108
	$d_v = 15$	27	34	41	48	54	61	68	75	82	88	95	102	109
$n_0 = 4$	$d_v = 13$	25	32	38	45	51	57	64	70	77	83	90	96	102
	$d_v = 15$	26	33	40	46	53	60	66	73	80	86	93	100	107

p [bits]		4096	5120	6144	7168	8192	9216	10240	11264	12288	13312	14336	15360	16384
$n_0 = 3$	$d_v = 13$	2^{54}	2^{63}	2^{73}	2^{84}	2^{94}	2^{105}	2^{116}	2^{125}	2^{135}	2^{146}	2^{157}	2^{161}	2^{161}
	$d_v = 15$	2^{54}	2^{64}	2^{75}	2^{85}	2^{94}	2^{105}	2^{116}	2^{126}	2^{137}	2^{146}	2^{157}	2^{168}	2^{179}
$n_0 = 4$	$d_v = 13$	2^{60}	2^{73}	2^{85}	2^{98}	2^{109}	2^{121}	2^{134}	2^{146}	2^{153}	2^{154}	2^{154}	2^{154}	2^{154}
	$d_v = 15$	2^{62}	2^{75}	2^{88}	2^{100}	2^{113}	2^{127}	2^{138}	2^{152}	2^{165}	2^{176}	2^{176}	2^{176}	2^{176}

Атака по дуальному коду

Одной из возможных уязвимостей криптосистемы является атака по дуальному коду в том случае, если этот код содержит слова малого веса (эти слова - это строки проверочной матрицы, получаемой из открытого ключа).
Известно, что проблема поиска слов малого веса и проблема декодирования кода связаны между собой. Более того, в работе *F. Chabaud, On the security of some cryptosystems based on error-correcting codes, Advances in Cryptology: Proceedings of EUROCRYPT'94, LNCS 950, Springer, 1995*
показано, что **любой алгоритм поиска слов с минимального веса может быть преобразован в алгоритм декодирования до половины кодового расстояния**
Достаточно вспомнить идею Штерна!

Алгоритм Штерна

1. Применить метод исключения Гаусса в следующем виде:
   1.1 Для $i = 1..n - k$ выбрать случайный столбец C матрицы **H** среди тех, которые не были ранее выбраны. Пусть m_i - это индекс столбца
   1.2 Выбрать, если это возможно, элемент, стоящий на пересечении столбца C и ранее не выбранной строки k_i и отметить эту строку
   1.3 Обнулить все остальные элементы столбца при помощи линейной комбинации строк
   1.4 Если строку выбрать нельзя, то исключить такой столбец C и выбрать другой
2. Произвольно разделить индексы столбцов **H**, которые не были выбраны на шаге 1, на два подмножества, обозначенных X и Y соответственно. Каждый индекс добавляется либо к X, либо к Y с вероятностью $1/2$, так что X и Y не обязательно имеют одинаковый размер.
3. Случайным образом выберите набор J, состоящий из l индексов $\leq (n - k)$, скажем, $j_l, \ldots, j_l$.
4. Для каждого подмножества A из X с p элементами вычислите l-битный вектор $\pi(A)$, полученный сложением столбцов матрицы

$$\left(H_{j,m}\right)_{j \in J, m \in A}$$

   и выполнить аналогичное вычисление для каждого подмножества B из Y с p элементами.
5. Перечислите все пары A, B такие, что $\pi(A) = \pi(B)$; для каждой такой пары найти сумму всех элементов в $A \cup B$; если один из только что вычисленных векторов, скажем V, имеет точно вес $w - 2p$, то строим решение x, определенное как:

$$x_m = 1 \ if \ m \in A \cup B \ or \ for \ some \ i \leq n - k \ m = m_i \ and \ V_{k_i} = 1$$

   если такого вектора V не найдено, то возврат к шагу 1

Атака по дуальному коду

Ясно, что проверочная матрица открытого ключа может быть представлена в виде:

$$\mathbf{H}' = \mathbf{H}\mathbf{Q}^T$$

Каждая строка этой матрицы это слово дуального кода и поэтому он имеет по крайней мере $A_w \geq n - k$ кодовых слов веса $w \leq n_0 d_v m$.
Алгоритм Штерна позволяет найти одно из A_w слов веса w в коде длины n_S и размерности k_S с вероятностью

$$P_{w,A_w} \leq A_w \cdot \frac{\binom{w}{g}\binom{n_S-w}{k_S/2-g}}{\binom{n_S}{k_S/2}} \cdot \frac{\binom{w-g}{g}\binom{n_S-k_S/2-w+g}{k_S/2-g}}{\binom{n_S-k_S/2}{k_S/2}} \cdot \frac{\binom{n_S-k_S-w+2g}{l}}{\binom{n_S-k_S}{l}},$$

где g и l - два параметра, значения которых должны быть оптимизированы как функции общего количества бинарных операций. Таким образом, среднее количество итераций, необходимых для поиска кодового слова с низким весом, составляет $c \geq P_{w,A_w}^{-1}$. Каждая итерация требует:

$$N = \frac{(n_S - k_S)^3}{2} + k_S(n_S - k_S)^2 + 2gl\binom{k_S/2}{g} + \frac{2g(n_S - k_S)\binom{k_S/2}{g}^2}{2^l}$$

Итоговое резюме

- Предложено достаточно много конструкций криптосистем на базе различных кодов, обеспечивающих компактную форму записи открытого ключа
- Обычно структурность кода / его "алгебраичность"позволяет записать открытый ключ компактно, однако структурность зачастую влечет за собой неустойчивость криптосистемы к структурным атакам
- Криптосистемы на базе кодов QC-LDPC и QC-MDPC при некоторых условиях пока остаются нераскрытыми
- Однако проблемой остается выбор параметров этих кодов, а особенно выбор векторов ошибок ввиду специфического алгоритма декодирования