On weak keys in QC-MDPC schemes

Nicolas Sendrier — Inria

Valentin Vasseur — Inria, Université de Paris

QC-MDPC [MTSB13][1]

- McEliece-like public-key encryption scheme with a quasi-cyclic structure
  - Reasonable key sizes
  - Reduction to generic hard problems over quasi-cyclic codes
- 2nd round candidate to the NIST post-quantum cryptography standardization process
  - BIKE

[1] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier and Paulo S. L. M. Barreto. 'MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes'. In: *Proc. IEEE Int. Symposium Inf. Theory - ISIT*. 2013.

$H = (H_0 | H_1) \leftarrow \mathbb{F}_2^{r \times n}$
$H_{pub} = (I_r | H_0^{-1} H_1) \in \mathbb{F}_2^{r \times n}$
H_0, H_1 circulant matrices with row weight d

$\xrightarrow{H_{pub}}$

$e \leftarrow \{0,1\}^n$
$|e| = t$

$\xleftarrow{c = H_{pub} e^\intercal}$

$e = \text{Decode}(H_0 c, H)$

Parameters: $r, d, t \in \mathbb{N}$, $n = 2r$, $w = 2d \sim t \sim \sqrt{n}$

λ	r_{CPA}	r_{CCA}	d	t
128	10163	**11779**	**71**	**134**
192	19853	24821	103	199
256	32749	40597	137	264

[2] https://bikesuite.org/

Circulant matrix

A circulant matrix is a matrix where each row vector is rotated one element to the right relative to the preceding row vector

$$H = \begin{pmatrix} h_0 & h_{r-1} & \dots & h_2 & h_1 \\ h_1 & h_0 & h_{r-1} & & h_2 \\ \vdots & h_1 & h_0 & \ddots & \vdots \\ h_{r-2} & & \ddots & \ddots & h_{r-1} \\ h_{r-1} & h_{r-2} & \dots & h_1 & h_0 \end{pmatrix}.$$

Truncated polynomial

$$H \mapsto h_0 + h_1 x + \cdots + h_{r-2} x^{r-2} + h_{r-1} x^{r-1}$$

is an isomorphism between the circulant $r \times r$ matrices and the quotient $\mathbb{F}_2[x]/(x^r - 1)$.

$\mathsf{h}_0, \mathsf{h}_1 \leftarrow \mathbb{F}_2[x]/(x^r - 1)$

$\mathsf{h}_{\mathsf{pub}} = \mathsf{h}_0^{-1}\mathsf{h}_1 \in \mathbb{F}_2[x]/(x^r - 1)$

$|\mathsf{h}_0| = |\mathsf{h}_1| = d$

$\xrightarrow{\mathsf{h}_{\mathsf{pub}}}$

$\mathsf{e}_0, \mathsf{e}_1 \leftarrow \mathbb{F}_2[x]/(x^r - 1)$

$|\mathsf{e}_0| + |\mathsf{e}_1| = t$

$\xleftarrow{\mathsf{c} = \mathsf{e}_0 + \mathsf{h}_{\mathsf{pub}}\mathsf{e}_1}$

$\mathsf{e} = \mathrm{Decode}(\mathsf{h}_0\mathsf{c}, \mathsf{h}_0, \mathsf{h}_1)$

Parameters: $r, d, t \in \mathbb{N}$, $n = 2r$, $w = 2d \sim t \sim \sqrt{n}$

λ	r_{CPA}	r_{CCA}	d	t
128	10163	**11779**	**71**	**134**
192	19853	24821	103	199
256	32749	40597	137	264

[3] https://bikesuite.org/

e_0, e_1: error pattern

s: syndrome

$\left|x^j h_i \star s\right|$: counter

$$\begin{aligned} s = h_0 c &= h_0(e_0 + h_{pub} e_1) \\ &= h_0 e_0 + h_1 e_1 \end{aligned}$$

Input : s, h_0, h_1

Output : e_0, e_1

Idea : $s = \sum_{j, e_{0j}=1} x^j h_0 + \sum_{j, e_{1j}=1} x^j h_1$

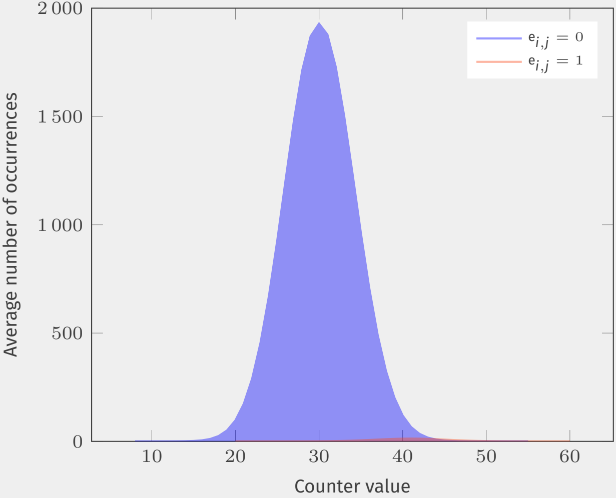
$$x^j h_i \star s \approx \begin{cases} x^j h_i + \text{Noise} & \text{if } e_{ij} = 1 \\ \text{Noise} & \text{if } e_{ij} = 0 \end{cases}$$

$$\Rightarrow \left|x^j h_i \star s\right| \approx \begin{cases} \text{Big value} & \text{if } e_{ij} = 1 \\ \text{Small value} & \text{if } e_{ij} = 0 \end{cases}$$

$x^{j'} h_{i'} \star x^j h_i$ is small if $(i, j) \neq (i', j')$

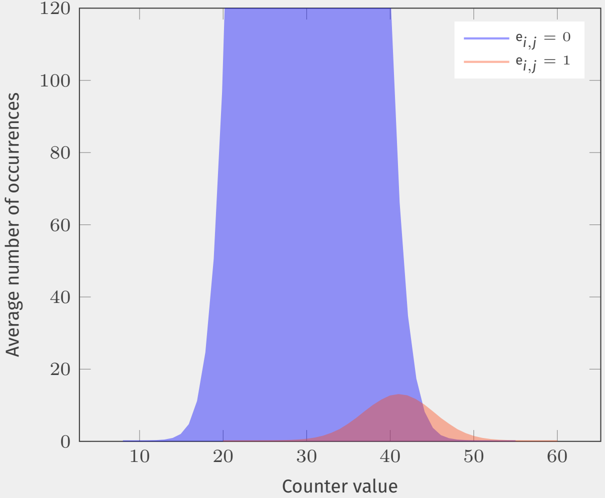
Counters

$$\forall i \in \{0,1\}, \forall j \in \{0,\ldots,r-1\}, \sigma_{i,j} = \left| x^j \mathsf{h}_i \star \mathsf{s} \right|$$



Counters

$$\forall i \in \{0,1\}, \forall j \in \{0,\dots,r-1\}, \sigma_{i,j} = \left| x^j \mathrm{h}_i \star \mathrm{s} \right|$$



Goal:

- Show that the DFR is less than $2^{-\lambda}$ (λ security parameter)

Motivations:

- Security reasons
  - Needed for the IND-CCA proof [HHK17][4]
  - [GJS16][5] shows a practical attack using decoding failures

[4]Dennis Hofheinz, Kathrin Hövelmanns and Eike Kiltz. 'A modular analysis of the Fujisaki-Okamoto transformation'. In: *Theory of Cryptography Conference*. Springer. 2017.

[5]Qian Guo, Thomas Johansson and Paul Stankovski. 'A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors'. In: *Advances in Cryptology - ASIACRYPT 2016*. 2016. URL: http://dx.doi.org/10.1007/978-3-662-53887-6_29.

δ-correctness [HHK17][6]

A public-key encryption scheme is δ-correct if:

$$\mathbf{E}_{(\mathsf{sk},\mathsf{pk})}\left[\underbrace{\max_{m\in\mathcal{M}} \Pr(\mathrm{Dec}(\mathrm{Enc}(m,\mathsf{pk}),\mathsf{sk}) \neq m)}_{\mathsf{DFR}_{(\mathsf{sk},\mathsf{pk})}}\right] < \delta\,.$$

For λ bits of security, we want $\delta < 2^{-\lambda}$.

Weak keys

We say that $\mathcal{W}$ is a set of weak keys if $\mathbf{E}_{(\mathsf{sk},\mathsf{pk})\in\mathcal{W}}\left[\mathsf{DFR}_{(\mathsf{sk},\mathsf{pk})}\right]$ is high.

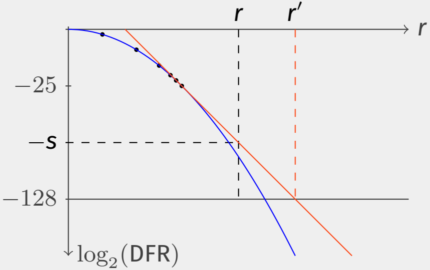
We want to make sure that

$$\mathbf{E}_{(\mathsf{sk},\mathsf{pk})\in\mathcal{W}}\left[\mathsf{DFR}_{(\mathsf{sk},\mathsf{pk})}\right] \times \Pr((\mathsf{sk},\mathsf{pk}) \in \mathcal{W}) < 2^{-\lambda}\,.$$

[6] Dennis Hofheinz, Kathrin Hövelmanns and Eike Kiltz. ‘A modular analysis of the Fujisaki-Okamoto transformation’. In: *Theory of Cryptography Conference*. Springer. 2017.

Assumption

For a given decoder $\mathcal{D}$, and a given security level λ, the function $r \mapsto \log(\mathrm{DFR}_{\mathcal{D},\lambda}(r))$ is decreasing and is concave if $\mathrm{DFR}_{\mathcal{D},\lambda}(r) \geq 2^{-\lambda}$.

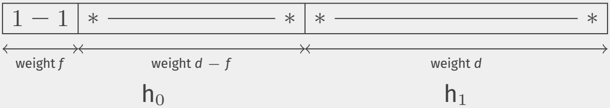


This assumption is backed by [Til18][7] and [SV19][8].

[7] Jean-Pierre Tillich. 'The Decoding Failure Probability of MDPC Codes'. In: *2018 IEEE International Symposium on Information Theory, ISIT 2018, Vail, CO, USA, June 17-22, 2018*. 2018. URL: https://doi.org/10.1109/ISIT.2018.8437843.

[8] Nicolas Sendrier and Valentin Vasseur. 'On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders'. In: *Post-Quantum Cryptography 2019*. May 2019.

[DGK19][9]: “Instead of generating a random h_0, we start by setting the first $f = 0, 20, 30, 40$ bits, and then select randomly the positions of the additional $(d{-}f)$ bits.”



[9] Nir Drucker, Shay Gueron and Dusan Kostic. *On constant-time QC-MDPC decoding with negligible failure rate.* Cryptology ePrint Archive, Report 2019/1289. 2019.

Counting Type I weak keys ($r = 11\,779$)

$$N_f^{\mathrm{I}} = \frac{\binom{r-f}{d-f}}{\binom{r}{d}}$$

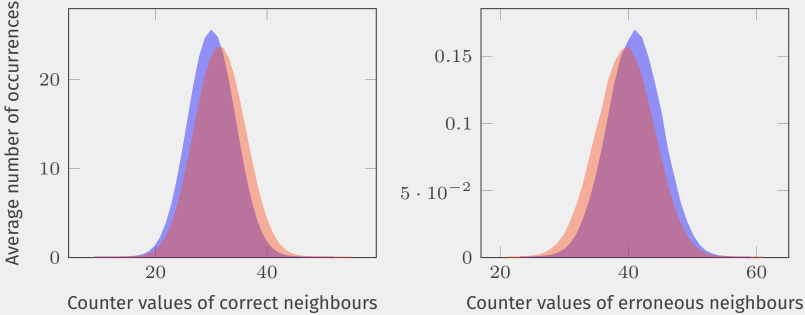
f	$\log_2 N_f^I$
4	-29.620
5	-37.077
6	-44.556
7	-52.057
8	-59.580
9	-67.126
10	-74.694
11	-82.286
12	-89.902
13	-97.542
14	-105.206
15	-112.896
16	-120.610
17	-128.351
18	-136.118
19	-143.912
20	-151.733
21	-159.582

f	$\log_2 N_f^l$	$\log_2$ DFR	$\log_2(N_f^l \times \text{DFR})$
Random		-83.300	
6	-44.556	-83.363	-127.919
8	-59.580	-84.245	-143.825
10	-74.694	-85.535	-160.229
12	-89.902	-83.547	-173.449
14	-105.206	-83.267	-188.473
16	-120.610	-81.392	-202.002
18	-136.118	-78.701	-214.819
20	-151.733	-75.291	-227.024
22	-167.459	-67.365	-234.824

A weak key of Type I has a parity check matrix as follows:

$$
\begin{bmatrix}
\ddots & & & & & & & & \\
& 1 & 1 & 1 & 0 & * & * & * & \\
& 1 & 1 & 1 & 1 & 0 & * & * & \\
& 0 & 1 & 1 & 1 & 1 & 0 & * & \\
& * & 0 & 1 & 1 & 1 & 1 & 0 & \\
& * & * & 0 & 1 & 1 & 1 & 1 & \\
& * & * & * & 0 & 1 & 1 & 1 & \\
& & & & & & & & \ddots
\end{bmatrix}.
$$

- In blue, average case
- In red, $f = 20$



Cyclic distance

$$\forall i,j, \quad 0 \leq i < j < r, \quad \mathrm{d}(i,j) = \min(j-i, r+i-j)\,.$$

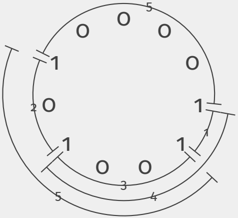
Spectrum

$$\text{Define } S_\delta(\mathsf{h}) = \left\{(i,j) \;\middle|\; 0 \leq i < j < r, h_i = h_j = 1 \text{ and } \mathrm{d}(i,j) = \delta\right\}.$$

$$\mathrm{Sp}(\mathsf{h}) = \left\{(\delta, |S_\delta(\mathsf{h})|) \;\middle|\; \delta \in \{1,\dots,\lfloor r/2 \rfloor\}\right\}$$

$$\mathsf{h} = (0,0,0,1,1,0,0,1,0,1,0)$$

$$\mathrm{Sp}(\mathsf{h}) = \{(1,1),(2,1),(3,1),(4,1),(5,2)\}$$



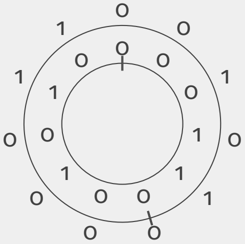
Neighbours

$(\delta, m) \in \mathrm{Sp}(\mathsf{h})$ if and only if h and its δ-shift $x^\delta \mathsf{h}$ intersect in m equations.

$$\left| \mathsf{h} \star x^\delta \mathsf{h} \right| = m$$

$$\begin{aligned} \mathsf{h} &= (0,0,0,1,1,0,0,1,0,1,0) \\ x^5 \mathsf{h} &= (0,0,1,0,1,0,0,0,0,1,1) \end{aligned}$$

$$\mathrm{Sp}(\mathsf{h}) = \{(1,1),(2,1),(3,1),(4,1),(5,2)\}$$



Weak keys of Type I (rev.)

Fix a number of bits f.

- Choose a starting point $i_0 \in \{0, \ldots, r-1\}$.
- Choose a distance $\delta \in \{1, \ldots, \lfloor r/2 \rfloor\}$.
- Set f bits regularly spaced by a distance δ.

$$\boxed{0 - 0\;1\;0 \;\text{————}\; 0\;1\;0 \quad \cdots \quad 0\;1\;0 \;\text{————}\; 0\;1\;0 - 0}$$
$$\xleftrightarrow[i_0]{\quad}\xleftrightarrow[\delta]{\qquad\qquad}\xleftrightarrow[(f-3)\delta]{\qquad\qquad}\xleftrightarrow[\delta]{\qquad\qquad}$$

- Complete the error pattern to obtain a vector of weight d.

(Previous construction corresponds to $i_0 = 0$ and $\delta = 1$.)

Counting Type I weak keys (rev.) ($r = 11\,779$)

$$N_f^{\mathrm{I}} = \frac{r(r-1)}{2} \frac{\binom{r-f}{d-f}}{\binom{r}{d}}$$

f	$\log_2 N_f^I$	was
6	-18.509	-44.556
7	-26.009	-52.057
8	-33.532	-59.580
9	-41.078	-67.126
10	-48.647	-74.694
11	-56.239	-82.286
12	-63.854	-89.902
13	-71.494	-97.542
14	-79.159	-105.206
15	-86.848	-112.896
16	-94.563	-120.610
17	-102.303	-128.351
18	-110.070	-136.118
19	-117.864	-143.912
20	-125.685	-151.733
21	-133.534	-159.582

Effect on the DFR (Backflip with 15 iterations) (rev.)

f	$\log_2 N_f^l$	$\log_2$ DFR	$\log_2(N_f^l \times \text{DFR})$
Random		-83.300	
6	-18.509	-83.363	-101.872
8	-33.532	-84.245	-117.777
10	-48.647	-85.535	-134.182
12	-63.854	-83.547	-147.401
14	-79.159	-83.267	-162.426
16	-94.563	-81.392	-175.955
18	-110.070	-78.701	-188.771
20	-125.685	-75.291	-200.976
22	-141.412	-67.365	-208.777

Idea

Generate h such that $\max\{m \mid (\delta, m) \in \mathrm{Sp}(\mathsf{h})\}$ is high ($\gtrsim 10$).

Fix a multiplicity m.

- Choose a distance $\delta \in \{1, \ldots, \lfloor r/2 \rfloor\}$.
- Generate a pattern h of weight d such that $(\delta, m) \in \mathrm{Sp}(\mathsf{h})$.

Isomorphism

If $\delta \in \mathbb{Z}_r^\times$, then

$$\phi_\delta \colon (\mathbb{F}_2[x]/(x^r - 1), +, \times) \to (\mathbb{F}_2[x]/(x^r - 1), +, \times)$$
$$\mathsf{h} = \sum_{i \in \mathrm{Supp}(\mathsf{h})} x^i \mapsto \sum_{i \in \mathrm{Supp}(\mathsf{h})} x^{\delta \cdot i}$$

is an ring isomorphism.

In BIKE, by construction r is always a prime number and the decoder is such that

$$\mathsf{Decode}(\phi_\delta(\mathsf{s}), \phi_\delta(\mathsf{h}_0), \phi_\delta(\mathsf{h}_1)) = \phi_\delta(\mathsf{Decode}(\mathsf{s}, \mathsf{h}_0, \mathsf{h}_1))\ .$$

Reduction to $\delta = 1$

$(\delta, m) \in \mathrm{Sp}(\mathsf{h})$ if and only if $(1, m) \in \mathrm{Sp}(\phi_{\delta^{-1}}(\mathsf{h}))$.

Idea

Generate h such that $\max\{m \mid (\delta, m) \in \mathrm{Sp}(\mathsf{h})\}$ is high ($\gtrsim 10$).

Fix a multiplicity m.

- Choose a distance $\delta \in \{1, \ldots, \lfloor r/2 \rfloor\}$.
- Generate a pattern h' of weight d such that $(1, m) \in \mathrm{Sp}(\mathsf{h}')$.
- Take $\mathsf{h} = \phi_\delta(\mathsf{h}')$.

DECOMPOSING A PATTERN h′

First, suppose h′ starts with a 0 and ends with a 1.

$$\boxed{\underbrace{0 - 0}_{z_1}\underbrace{1 - 1}_{o_1} \;\cdots\; \underbrace{0 - 0}_{z_{s-1}}\underbrace{1 - 1}_{o_{s-1}}\underbrace{0 - 0}_{z_s}\underbrace{1 - 1}_{o_s}}$$

We have

$$\begin{cases} o_1 + o_2 + \cdots + o_s = d \; ; \\ z_1 + z_2 + \cdots + z_s = r - d \; . \end{cases}$$

A block of k successive 1 adds $(k-1)$ to the multiplicity of $\delta = 1$.

So h′ has multiplicity $m = \sum_{i=1}^{s} o_i - 1 = d - s$.

Fix $s = d - m$.

- There are $\binom{d-1}{s-1}$ tuples $(o_1, o_2, \ldots, o_s)$ such that $o_1 + o_2 + \cdots + o_s = d$.
- There are $\binom{r-d-1}{s-1}$ tuples $(z_1, z_2, \ldots, z_s)$ such that $z_1 + z_2 + \cdots + z_s = r - d$.

$\Rightarrow$ There are $\binom{d-1}{s-1}\binom{r-d-1}{s-1}$ patterns h′ that start with a 0 and end with a 1.

Let ℓ be the smallest integer such that $x^{-\ell}\mathrm{h}'$ starts with a 0 and ends with a 1.
$x^{-\ell}\mathrm{h}'$ follows a pattern $(z_1, o_1, \ldots, z_{s-1}, o_{s-1}, z_s, o_s)$

Bijection

For all $s \in \{1, \ldots, d\}$, there is a bijection between the pairs $(\ell, (z_1, o_1, \ldots, z_{s-1}, o_{s-1}, z_s, o_s))$ such that

$$\begin{cases} \ell \in \{0, \ldots, z_1 + o_1 - 1\} ; \\ o_1 + o_2 + \cdots + o_s = d ; \\ z_1 + z_2 + \cdots + z_s = r - d \end{cases}$$

and the patterns h' of weight d and length r where 1 has multiplicity $m = d - s$.

- If $m = d - 1$, r patterns possible.
- If $m < d - 1 \Rightarrow s > 1$

  Fix z_1 and o_1, then
  - there are $\binom{d-1-o_1}{s-2}$ tuples $(o_2, \dots, o_s)$ such that $o_1 + o_2 + \cdots + o_s = d$;
  - there are $\binom{r-d-1-z_1}{s-2}$ tuples $(z_2, \dots, z_s)$ such that $z_1 + z_2 + \cdots + z_s = r - d$.

  $\rightarrow$ In general, there are

$$\sum_{z_1=1}^{r-d-s+1} \sum_{o_1=1}^{d-s+1} (z_1 + o_1) \binom{d - o_1 - 1}{s-2} \binom{r - d - z_1 - 1}{s-2}$$

  patterns.

Considering all the values for $\delta \in \{1, \ldots, \lfloor r/2 \rfloor\}$.

- If $m = d - 1$,

$$N_m^{II} = \frac{r(r-1)}{2} \ .$$

- If $m < d - 1 \Rightarrow s > 1$,

$$N_m^{II} = \frac{r-1}{2} \sum_{z_1=1}^{r-d-s+1} \sum_{o_1=1}^{d-s+1} (z_1 + o_1) \binom{d - o_1 - 1}{s-2} \binom{r - d - z_1 - 1}{s-2} \ .$$

Comparing Type I and Type II weak keys frequencies ($r = 11\,779$)

f	$\log_2 N^I_f$
8	-33.532
9	-41.078
10	-48.647
11	-56.239
12	-63.854
13	-71.494
14	-79.159
15	-86.848
16	-94.563
17	-102.303
18	-110.070
19	-117.864
20	-125.685
21	-133.534
22	-141.412
23	-149.318

Type I

m	$\log_2 N^{II}_m$
12	-34.524
13	-39.992
14	-45.617
15	-51.392
16	-57.311
17	-63.371
18	-69.567
19	-75.895
20	-82.353
21	-88.938
22	-95.648
23	-102.481
24	-109.436
25	-116.511
26	-123.706
27	-131.019

Type II

m	$\log_2 N_f^{II}$	$\log_2$ DFR	$\log_2(N_f^{II} \times \text{DFR})$
Random		-83.300	
8	-13.677	-84.210	-97.887
10	-23.411	-83.790	-107.201
12	-33.886	-83.665	-117.551
14	-45.020	-83.749	-128.769
16	-56.753	-83.600	-140.353
18	-69.047	-83.086	-152.133
20	-81.869	-82.437	-164.306
22	-95.199	-81.466	-176.665
24	-109.020	-80.218	-189.238
26	-123.322	-79.186	-202.508
28	-138.097	-77.643	-215.740

Type III: Intersections between two different blocks in a QC-MDPC

Column intersection

The block h_0 and $x^j h_1$ for any $j \in \{0, \ldots, r-1\}$ intersect on m equations with probability

$$N_m^{III} = r \frac{\binom{d}{m}\binom{r-d}{d-m}}{\binom{r}{d}} .$$

m	$\log_2 N_m^{II}$	$\log_2 N_m^{III}$
6	-5.578	-4.459
7	-9.870	-8.729
8	-14.400	-13.237
9	-19.146	-17.960
10	-24.091	-22.881
11	-29.221	-27.986
12	-34.524	-33.266
13	-39.992	-38.709
14	-45.617	-44.308
15	-51.392	-50.058
16	-57.311	-55.951
17	-63.371	-61.985
18	-69.567	-68.154
19	-75.895	-74.454

m	$\log_2 N_f^{III}$	$\log_2$ DFR	$\log_2(N_f^{III} \times \text{DFR})$
Random		-83.300	
8	-13.237	-84.014	-97.251
10	-22.881	-84.146	-107.027
12	-33.266	-84.198	-117.464
14	-44.308	-83.988	-128.296
18	-68.154	-82.938	-151.092
20	-80.884	-82.982	-163.866
24	-107.850	-81.333	-189.183
26	-122.057	-79.567	-201.624
28	-136.736	-76.028	-212.764

- Type I keys are weak because they increase a multiplicity in a block
- Type II keys generalize the construction as much as possible
- Type III considers the two blocks of the QC-MDPC
- Simulation show that these keys have small contribution in the DFR

$\rightarrow$ These weak keys do not break the decoder properties needed for the IND-CCA conversion

(Filtering keys is also a possibility)