About Low DFR for QC-MDPC Decoding

Nicolas Sendrier — Inria

Valentin Vasseur — Inria, Université de Paris

Wednesday 23rd September, 2020

- Code-based Key Encapsulation Mechanism (KEM)
- Niederreiter framework (BIKE-2)
  - ⇒ Half bandwidth compared to a McEliece scheme
- Quasi-cyclic structure
  - ⇒ Reduced key sizes
- Moderate Density Parity Check (MDPC) codes [MTSB13]
  - ⇒ Reduction to generic hard problems over quasi-cyclic codes
- Efficient implementation
  - Fast encapsulation/decapsulation [DG19]
  - Fast key generation [DGK20]
- NIST post-quantum cryptography standardization process
  - 3rd round alternate candidate

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.

Nir Drucker and Shay Gueron. 'A toolbox for software optimization of QC-MDPC code-based cryptosystems'. In: *Journal of Cryptographic Engineering* 4 (Nov. 2019).

Nir Drucker, Shay Gueron and Dusan Kostic. 'Fast Polynomial Inversion for Post Quantum QC-MDPC Cryptography'. In: *CSCML*. 2020.

`https://bikesuite.org`

$\mathsf{h}_0, \mathsf{h}_1 \leftarrow \mathcal{H}_w$
$\mathsf{h}_{\text{pub}} = \mathsf{h}_0^{-1}\mathsf{h}_1 \in \mathcal{R}$

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

$(\mathsf{e}_0, \mathsf{e}_1) \leftarrow \mathcal{E}_t$

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

$(\mathsf{e}_0, \mathsf{e}_1) = \text{Decode}(\mathsf{h}_0\mathsf{s}, (\mathsf{h}_0, \mathsf{h}_1))$

- $\mathcal{R}$: Cyclic polynomial ring $\mathbb{F}_2[X]/(X^r - 1)$.
- $\mathcal{H}_w$: Private key space $\{(h_0, h_1) \in \mathcal{R}^2 \mid |h_0| = |h_1| = w/2\}$
- $\mathcal{E}_t$: Error space $\{(e_0, e_1) \in \mathcal{R}^2 \mid |e_0| + |e_1| = t\}$

Parameters: $n = 2r$, $w \sim t \sim \sqrt{n}$

λ	r_{CPA}	w	t
128	10 163	142	134
192	19 853	206	199
256	32 749	274	264

https://bikesuite.org/

QC Syndrome Decoding – QCSD

Instance: $(h, s) \in \mathcal{R} \times \mathcal{R}$, an integer $t > 0$.
Property: There exists $(e_0, e_1) \in \mathcal{E}_t$ such that $e_0 + e_1 h = s$.

QC Codeword Finding – QCCF

Instance: $h \in \mathcal{R}$, an even integer $w > 0$, with $w/2$ odd.
Property: There exists $(h_0, h_1) \in \mathcal{H}_w$ such that $h_1 + h_0 h = 0$.

Asymptotically [CS16] with the multi-target variant [Sen11], the best know attacks cost:

- for QCSD, $\dfrac{2^{t(1+o(1))}}{\sqrt{r}}$ operations ,
- for QCCF, $\dfrac{2^{w(1+o(1))}}{r}$ operations .

Rodolfo Canto-Torres and Nicolas Sendrier. 'Analysis of Information Set Decoding for a Sub-linear Error Weight'. In: *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016*. 2016.

Nicolas Sendrier. 'Decoding One Out of Many'. In: *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011*. Nov. 2011.

IND-CCA security and Decoding Failure Rate (DFR)

δ-correctness [HHK17]

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

$$\mathbf{E}_{\substack{(\mathsf{h}_0,\mathsf{h}_1)\in\mathcal{H}_w,\\ \mathsf{h}_{\mathsf{pub}}\in\mathcal{R}}}\left[\underbrace{\max_{(\mathsf{e}_0,\mathsf{e}_1)\in\mathcal{M}} \Pr(\mathrm{Dec}(\mathrm{Enc}((\mathsf{e}_0,\mathsf{e}_1),\mathsf{h}_{\mathsf{pub}}),(\mathsf{h}_0,\mathsf{h}_1)) \neq (\mathsf{e}_0,\mathsf{e}_1))}_{\mathsf{DFR}_{(\mathsf{h}_0,\mathsf{h}_1),\mathsf{h}_{\mathsf{pub}}}(\mathcal{D})}\right] < \delta\,.$$

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

Dennis Hofheinz, Kathrin Hövelmanns and Eike Kiltz. ‘A Modular Analysis of the Fujisaki-Okamoto Transformation’. In: *TCC 2017, Part I*. Nov. 2017.

Summary on security

Requirements [FO99; HHK17]

$$\left.\begin{array}{l}\left.\begin{array}{l}\text{1. QCSD offers } \lambda \text{ bits of security}\\ \text{2. QCCF offers } \lambda \text{ bits of security}\end{array}\right\}\text{IND-CPA}\\ \text{3. } \mathrm{DFR}_r(\mathcal{D}) \le 2^{-\lambda}.\end{array}\right\}\text{IND-CCA}$$

- 1, 2 marginally depend on r,
- 3 depends mainly on r,
- [GJS16] shows a practical attack if 3 is not true.

Eiichiro Fujisaki and Tatsuaki Okamoto. 'Secure Integration of Asymmetric and Symmetric Encryption Schemes'. In: *CRYPTO'99*. Aug. 1999.

Dennis Hofheinz, Kathrin Hövelmanns and Eike Kiltz. 'A Modular Analysis of the Fujisaki-Okamoto Transformation'. In: *TCC 2017, Part I*. Nov. 2017.

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.

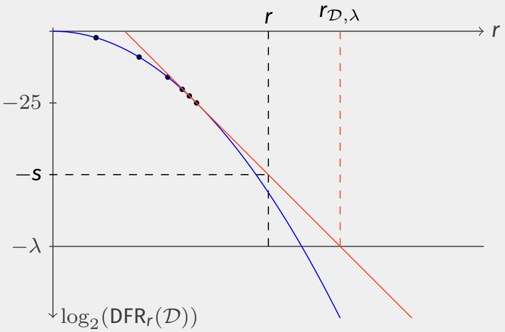
- Step-by-step algorithm [SV19] — fixed (w, t), varying r
  - Simple sequential bitflipping algoritm
  - Modeled with a Markov chain allowing to predict its DFR
  - Small difference between the DFR predicted and with simulation
  - In the model, at worst $r \mapsto \log(\mathsf{DFR}_r(\mathcal{D}))$ is an affine function
- Simulation of several variants of decoding algorithm — fixed (w, t), varying r
  - $r \mapsto \log(\mathsf{DFR}_r(\mathcal{D}))$ is a concave function
- Asymptotic result [Til18] — $w = \Theta(\sqrt{n})$, $t = \Theta(\sqrt{n})$
  - $r \mapsto \log(\mathsf{DFR}_r(\mathcal{D}))$ is upper bounded by a concave function of r

Nicolas Sendrier and Valentin Vasseur. ‘On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders’. In: *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019*. 2019.

Jean-Pierre Tillich. *The decoding failure probability of MDPC codes*. preprint. Sept. 2018.

Assumption

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



Error floors from low weight codewords

For a given error e of weight t, and two codewords c_0 and c_1 at distance w from one another, the decoding will fail if $|c_0 + e - c_1| \leq |e|$

$$P_w(r) = \sum_{i=w/2}^{w} \frac{\binom{w}{i}\binom{2r-w}{t-i}}{\binom{2r}{t}}.$$

For BIKE,

$$\begin{array}{llll} \lambda = 128, & \log_2 P_w(r_{\mathrm{CPA}}) = -396.8, & \text{and} & \log_2 P_w(r) \approx 535.0 - 70\log_2 r \\ \lambda = 192, & \log_2 P_w(r_{\mathrm{CPA}}) = -618.5, & \text{and} & \log_2 P_w(r) \approx 837.8 - 102\log_2 r \\ \lambda = 256, & \log_2 P_w(r_{\mathrm{CPA}}) = -868.7, & \text{and} & \log_2 P_w(r) \approx 1171.2 - 136\log_2 r \end{array}$$

Further ongoing work on error floors and weak keys do not invalidate the assumption

Input

$\mathrm{H} \in \mathbb{F}_2^{r \times n}$

$\mathrm{s} = \mathrm{eH}^T \in \mathbb{F}_2^r$ with $|\mathrm{e}| \leq t$

Output

$\mathrm{e} \in \mathbb{F}_2^n$

$\mathrm{e} \leftarrow 0$
while $\left|\mathrm{s} - \mathrm{e}H^T\right| \neq 0$ **do**
$\quad \mathrm{s}' \leftarrow \mathrm{s} - \mathrm{eH}^T$
$\quad T \leftarrow \mathrm{threshold}(context)$
$\quad$ **for** $j \in \{0, \ldots, n-1\}$ **do**
$\quad\quad$ **if** $\left|\mathrm{s}' \star \mathrm{h}_j\right| \geq T$ **then**
$\quad\quad\quad e_j \leftarrow 1 - e_j$
return e

H : QC matrix whose first row is $\mathrm{h}_0, \mathrm{h}_1$
h_j : j-th column of H
$\left|\mathrm{s}' \star \mathrm{h}_j\right|$: counter of position j
i.e. # unverified equations involving j

Problem of the original algorithm

Algorithm sometimes takes **bad decisions** (adding errors instead of removing them)

- Bad flips are not always easy to detect
- Too many bad flips hinder progress of the algorithm and can block it

Soft decision decoder

A **soft decision decoder** handles probabilities rather than bits

$\Rightarrow$ better decoding performance,

$\Rightarrow$ not computationally efficient.

Ideas of our variant

- Approach **soft decoding**
  - counters give a reliability information for each position
  - use this reliability information to limit the duration of a flip
- Each flip has a **time-to-live** (from 1 to 5 iterations)
  - regularly and systematically revert least reliable flips to avoid locking
  - most reliable flips (higher counters) live longer
- Threshold selection rule should be adapted

Input
  $H \in \mathbb{F}_2^{r \times n}$
  $s = eH^T \in \mathbb{F}_2^r$ with $|e| \le t$
Output
  $e \in \mathbb{F}_2^n$

$e \leftarrow 0$; $F \leftarrow 0$; $\mathrm{now} \leftarrow 1$
while $\left|s - eH^T\right| \neq 0$ **do**
  for each j **such that** $F_j = \mathrm{now}$ **do**
    $e_j \leftarrow 1 - e_j$; $F_j \leftarrow 0$
  $\mathrm{now} \leftarrow \mathrm{now} + 1$
  $s' \leftarrow s - eH^T$
  $T \leftarrow \mathrm{threshold}(context)$
  for $j \in \{0, \ldots, n-1\}$ **do**
    if $\left|s' \star h_j\right| \ge T$ **then**
      $e_j \leftarrow 1 - e_j$
      if $F_j \ge \mathrm{now}$ **then**
        $F_j \leftarrow 0$
      else
        $F_j \leftarrow \mathrm{now} + \mathrm{ttl}(\left|s' \star h_j\right| - T)$
return e

H	: QC matrix whose first row is h_0, h_1
h_j	: j-th column of H
$\left\|s' \star h_j\right\|$	: counter of position j
i.e.	# unverified equations involving j

Low additional cost of our variant

- For each flip, a time-to-live is computed
- Need some memory to store the time-of-death of each flipped position
- At the beginning of every iteration, obsolete flips are reverted

Time-to-live: ttl(δ)

- δ is the difference between the counter and the threshold
- ttl(δ) is an increasing function of δ

Empirical choices

- ttl(δ) is a saturating affine function in δ :

$$\mathrm{ttl}(\delta) = \max(1, \min(\mathrm{max\_ttl}, \lfloor A\,\delta + B \rfloor))$$

- Determine A and B with an optimization method on the DFR obtained by simulation

Obtained values

security	max_ttl	A	B
128	5	0.45	1.1
192	5	0.36	1.41
256	5	0.45	1

Threshold: threshold(|s| , |e|) (see [Cha17])

Smallest T such that

$$|e|\, f_{d,\pi_1}(T) \geq (n - |e|) f_{d,\pi_0}(T) \, .$$

with

$$\pi_0 = \frac{\bar{\sigma}_{\text{corr}}}{d} = \frac{(w-1)\,|s| - X}{d(n - |e|)} \quad \text{and} \quad \pi_1 = \frac{\bar{\sigma}_{\text{err}}}{d} = \frac{|s| + X}{d\,|e|}$$

and $f_{d,\pi}$ is the binomial distribution probability mass function for parameters d and π

π_0 and π_1 depend on

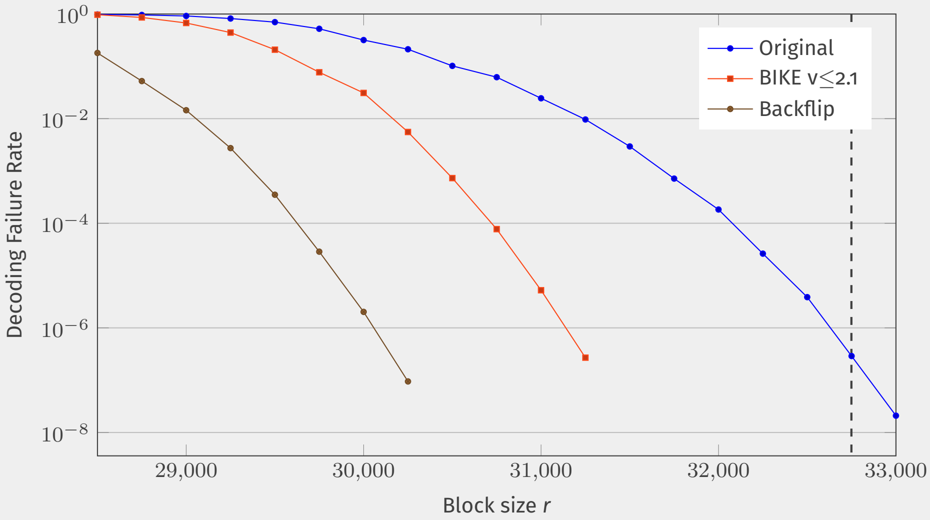
- $|s|$ which is known,
- $|e|$ which is not known.

Assume that $|e| = t - \#\text{flips}$

- true if no error was added,
- otherwise, gives a more conservative threshold.

Julia Chaulet. 'Étude de cryptosystèmes à clé publique basés sur les codes MDPC quasi-cycliques'. PhD thesis. University Pierre et Marie Curie, Mar. 2017.

Decoding performance comparison $(w, t) = (274, 264)$



#iter	λ	r_1	r_2	$\log_2 \mathsf{DFR}_{r_1}(\mathcal{D})$	$\log_2 \mathsf{DFR}_{r_2}(\mathcal{D})$	$r_{\mathcal{D},\lambda}$	r_{CPA}	$r_{\mathcal{D},\lambda}/r_{\mathsf{CPA}}$
100	128	9200	9350	-21.4	-27.7	11717	10163	1.15
	192	18200	18300	-23.0	-25.6	24665	19853	1.24
	256	30250	30400	-23.3	-26.2	42418	32749	1.30
10	128	10000	10050	-22.7	-24.6	12816	10163	1.26
	192	19550	19650	-23.5	-25.7	26939	19853	1.36
	256	32250	32450	-22.9	-26.6	44638	32749	1.36
11	128	10000	10050	-25.1	-27.1	12573	10163	1.24
	192	19550	19650	-25.9	-28.6	25580	19853	1.29
	256	32250	32450	-25.1	-29.5	42706	32749	1.30

Conclusion

- Explain the status of the DFR in the security analysis
- Justify the DFR extrapolation technique with previous works
- Introduce a new security assumption related to the decoder
- Explain the rationale of the Backflip decoder
- Show the decoding performance of the Backflip decoder