Backflip: An Improved QC-MDPC Bit-Flipping Decoder

Nicolas Sendrier — Inria

Valentin Vasseur — Inria, Université Paris Descartes, Sorbonne Paris Cité

Input

$H \in \{0,1\}^{r \times n}$
$s = eH^T \in \{0,1\}^r$
$|e| \leq t$

Output

$e \in \{0,1\}^r$

$e \leftarrow 0$
while $\left|s - eH^T\right| \neq 0$ **do**
  $s' \leftarrow s - eH^T$
  $T \leftarrow \text{threshold}(\mathit{context})$
  for $j \in \{0, \ldots, n-1\}$ **do**
    if $|s' \cap h_j| \geq T$ **then**
      $e_j \leftarrow 1 - e_j$
return e

H: moderately sparse parity check matrix

e: error pattern

$s = eH^T$

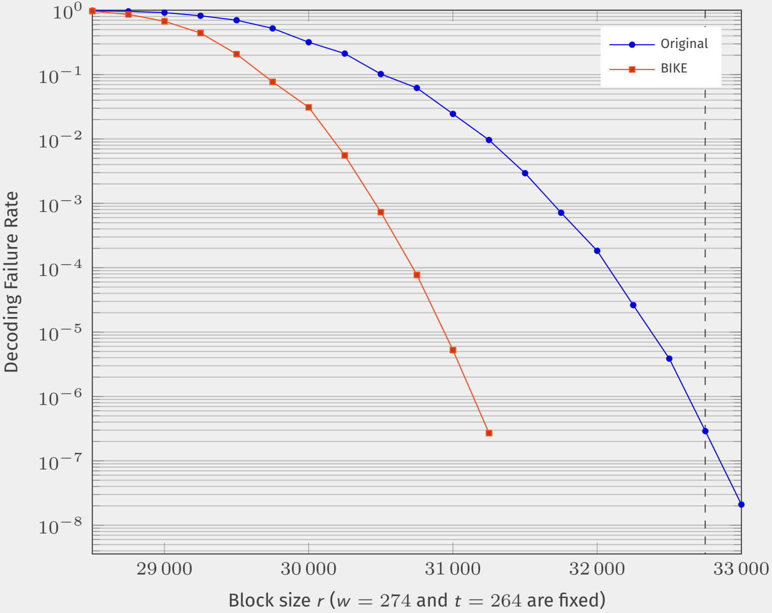
s: syndrome

$|s \cap h_j|$: counter

Main idea:

If $j \notin e$, $|s \cap h_j|$ is small
If $j \in e$, $|s \cap h_j|$ is big

State of the art of MDPC decoders



	(a)	(b_{128})	(b_{256})
Original	-21.7	39 766	48 215
BIKE	-47.5	37 450	44 924

(a): linearly extrapolated value for $\log_2(p_{\mathrm{fail}}(32\,749))$
(b_λ): minimal r such that $p_{\mathrm{fail}}(r) < 2^{-\lambda}$ assuming a linear evolution

[1] Nicolas Sendrier and Valentin Vasseur. *On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders*. Cryptology ePrint Archive, Report 2018/1207. `https://eprint.iacr.org/2018/1207` - To appear in PQCrypto 2019. 2018.

Input
$\mathsf{H} \in \{0,1\}^{r \times n}$
$\mathsf{s} = \mathsf{e}\mathsf{H}^T \in \{0,1\}^r$
$|\mathsf{e}| \leq t$

Output
$\mathsf{e} \in \{0,1\}^r$

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

return e

Problem: algorithm sometimes takes bad decisions

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

- Regularly and systematically cancel oldest flips to avoid locking

- Each flip has a time-to-live (from 1 to 5 iterations)
- Most reliable flips (higher counters) live longer

- Threshold selection rule should be adapted

Input

$H \in \{0,1\}^{r \times n}$; $s = eH^T \in \{0,1\}^r$

$|e| \leq t$

Output

$e \in \{0,1\}^r$

$e \leftarrow 0$; $F \leftarrow 0$; $\text{now} \leftarrow 1$

while $\left|s - eH^T\right| \neq 0$ **do**

  for each j **such that** $F_j = \text{now}$ **do**

    $e_j \leftarrow 1 - e_j$; $F_j \leftarrow 0$

  $\text{now} \leftarrow \text{now} + 1$

  $s' \leftarrow s - eH^T$

  $T \leftarrow \text{threshold}(\mathit{context})$

  for $j \in \{0, \ldots, n-1\}$ **do**

    if $|s' \cap h_j| \geq T$ **then**

      $e_j \leftarrow 1 - e_j$

      if $F_j \geq \text{now}$ **then**

        $F_j \leftarrow 0$

      else

        $F_j \leftarrow \text{now} + \text{ttl}(\mathit{context})$

return e

- To each flip, a time-to-live is computed
- F is a vector storing the time-of-death of each position
- At the beginning of every iteration, obsolete flips are canceled

Input

$H \in \{0,1\}^{r \times n}$; $s = eH^T \in \{0,1\}^r$

$|e| \leq t$

Output

$e \in \{0,1\}^r$

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

- To each flip, a time-to-live is computed
- F is a vector storing the time-of-death of each position
- At the beginning of every iteration, obsolete flips are canceled

Time-to-live: ttl(δ)

δ: difference between the counter and the threshold
ttl: saturating affine function in δ

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

Using optimization methods to minimize the DFR:

security level	max_ttl	A	B
1	5	0.45	1.1
3	5	0.36	1.41
5	5	0.45	1

BIKE-1 and BIKE-2

From [Cha17][2], a good threshold is the smallest T such that

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

with

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

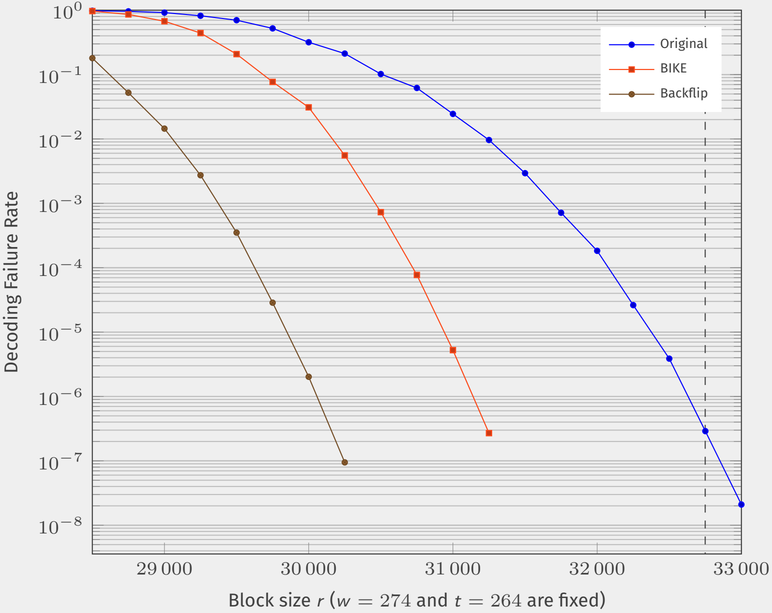
π_0 and π_1 depend on

- $|\mathsf{s}|$ which we can know,
- $|\mathsf{e}|$ which we cannot.

Assume that $|\mathsf{e}| = t - |F|$

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

[2] Julia Chaulet. 'Étude de cryptosystèmes à clé publique basés sur les codes MDPC quasi-cycliques'. PhD thesis. University Pierre et Marie Curie, Mar. 2017. URL: `https://tel.archives-ouvertes.fr/tel-01599347`.


10^{0}
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
Decoding Failure Rate
Original
BIKE
Backflip
29 000
30 000
31 000
32 000
33 000
Block size r ($w = 274$ and $t = 264$ are fixed)

	(a)	(b_{128})	(b_{256})
Original	-21.7	39 766	48 215
BIKE	-47.5	37 450	44 924
Backflip	-75.9	34 939	40 597

(a): linearly extrapolated value for $\log_2(p_{\text{fail}}(32\,749))$
(b_λ): minimal r such that $p_{\text{fail}}(r) < 2^{-\lambda}$ assuming a linear evolution

[1] Nicolas Sendrier and Valentin Vasseur. *On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders*. Cryptology ePrint Archive, Report 2018/1207. `https://eprint.iacr.org/2018/1207` - To appear in PQCrypto 2019. 2018.

Achieving a DFR of $2^{-\lambda/2}$ where λ is the security parameter

security	Original r	Revised r	Ratio
128	10 163	10 253	1.009
192	19 853	21 059	1.061
256	32 749	34 939	1.067

Achieving a DFR of $2^{-\lambda}$ where λ is the security parameter

security	Original r	Revised r	Ratio
128	10 163	11 779	1.159
192	19 853	24 821	1.250
256	32 749	40 597	1.240

- We propose an improved decoding algorithm for MDPC
  - Slighly higher complexity
  - Order of magnitude lower DFR

- We extrapolate the DFR for BIKE parameters needed to reach IND-CCA security
  - $<$ 25 % increase in blocksize