On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders

Nicolas Sendrier — Inria

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

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 et al. 'MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes'. In: *Proc. IEEE Int. Symposium Inf. Theory - ISIT*. 2013, pp. 2069–2073.

Methodology:

- Prove that the Decoding Failure Rate is negligible in an ideal model
- Study the validity of the model

Motivations:

- Security reasons
  - [GJS16][2]: correlation between faulty error patterns and the secret key

  → Scheme is not IND-CCA
- Engineering reasons
  - Avoid re-execution of the protocol in case of failure
  - Misuse resilience

[2] 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*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Vol. 10031. LNCS. 2016, pp. 789–815. ISBN: 978-3-662-53886-9. DOI: 10.1007/978-3-662-53887-6_29. URL: http://dx.doi.org/10.1007/978-3-662-53887-6_29.

Original

Input
 $\mathsf{H} \in \{0,1\}^{r \times n}$
 $\mathsf{y} \in \{0,1\}^{n}$
Output
 $\mathsf{c} \in \{0,1\}^{n}$
while $\mathsf{y}\mathsf{H}^{T} \neq 0$ **do**
 $\mathsf{s} \leftarrow \mathsf{y}\mathsf{H}^{T}$
 $T \leftarrow \text{threshold}(\textit{context})$
 for $j \in \{0, \dots, n-1\}$ **do**
  if $|\mathsf{s} \cap \mathsf{h}_j| \geq T$ **then**
   $y_j \leftarrow 1 - y_j$
return y

H: moderately sparse parity check matrix

$\mathsf{y} = \mathsf{c} + \mathsf{e}$

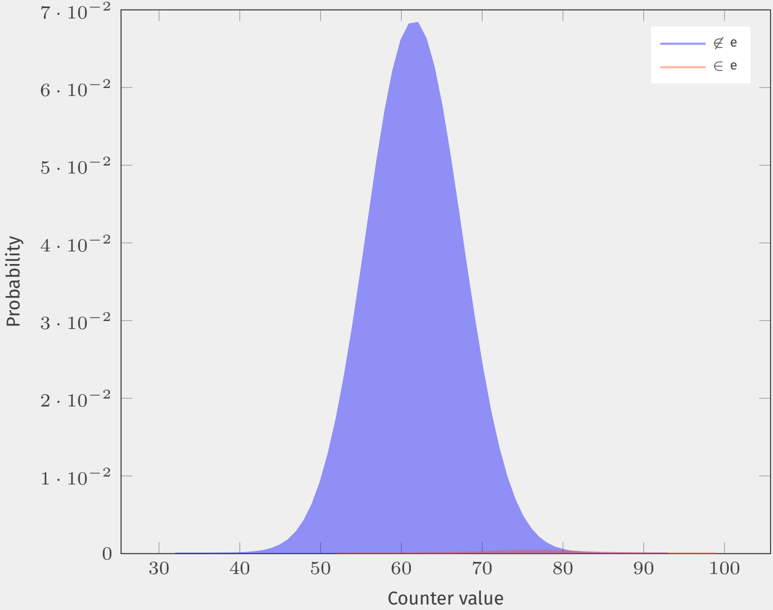
y: noisy codeword
c: codeword
e: error

$\mathsf{s} = \mathsf{y}\mathsf{H}^{T} = \underbrace{\mathsf{c}\mathsf{H}^{T}}_{=0} + \mathsf{e}\mathsf{H}^{T}$

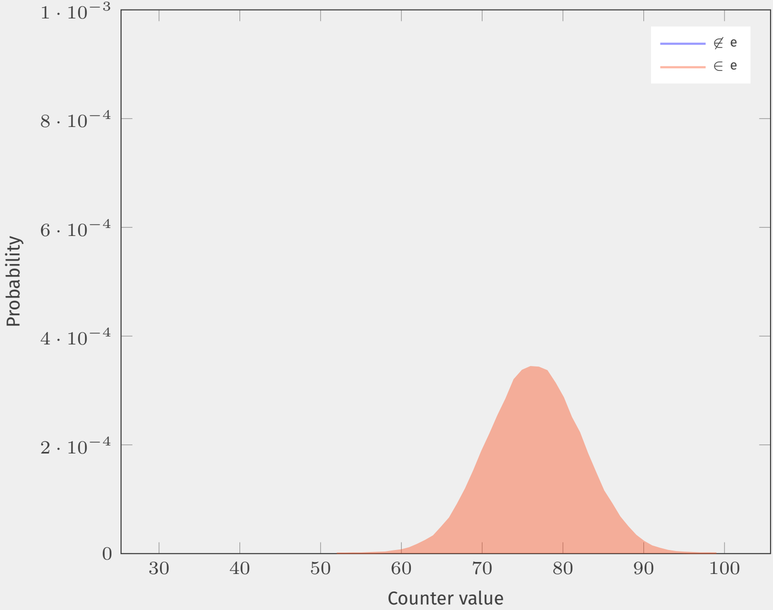
s: syndrome

$|\mathsf{s} \cap \mathsf{h}_j|$: counter

Counters distributions: $|S| = 14\,608$, $|E| = 264$



Counters distributions: $|\mathsf{S}| = 14\,608$, $|\mathsf{E}| = 264$



DECODING ALGORITHM (*BIT-FLIPPING*)

Original

Input
  $\mathsf{H} \in \{0,1\}^{r \times n}$
  $\mathsf{y} \in \{0,1\}^{n}$
Output
  $\mathsf{c} \in \{0,1\}^{n}$
while $\mathsf{yH}^T \neq 0$ **do**
  $\mathsf{s} \leftarrow \mathsf{yH}^T$
  $T \leftarrow \text{threshold}(\textit{context})$
  for $j \in \{0, \ldots, n-1\}$ **do**
    if $|\mathsf{s} \cap \mathsf{h}_j| \geq T$ **then**
      $y_j \leftarrow 1 - y_j$
return y

Step-by-step

Input
  $\mathsf{H} \in \{0,1\}^{r \times n}$
  $\mathsf{y} \in \{0,1\}^{n}$
Output
  $\mathsf{c} \in \{0,1\}^{n}$
while $\mathsf{yH}^T \neq 0$ **do**
  $\mathsf{s} \leftarrow \mathsf{yH}^T$
  $j \leftarrow \text{sample}(\textit{context})$
  $T \leftarrow \text{threshold}(\textit{context})$
  if $|\mathsf{s} \cap \mathsf{h}_j| \geq T$ **then**
    $y_j \leftarrow 1 - y_j$
return y

- Finite State Machine
- Stochastic process
- Suppose it is a memoryless process

$\rightarrow$ Markov chain

State space:

- all the possible combinations of (S, t) with
  - $S = \left|\mathsf{e}\mathsf{H}^T\right|$: the syndrome weight
  - $t = |\mathsf{e}|$: the error weight

Transitions:

- Defined by the algorithm

For a specific starting syndrome weight $|\mathsf{s}| = S$ and error weight $|\mathsf{e}| = t$:

$$\mathsf{P}_{\text{success}}(S, t) = \Pr[(S, t) \xrightarrow{\infty} (0, 0)] \qquad \mathsf{P}_{\text{failure}}(S, t) = 1 - \mathsf{P}_{\text{success}}(S, t)$$

Finally

$$\mathsf{DFR}(t) = \sum_S \Pr\left(|\mathsf{s}| = S \middle| \, |\mathsf{e}| = t\right) \cdot \mathsf{P}_{\text{failure}}(S, t)$$

- Error positions are always independent
- Infinite number of iterations
- Counters distributions [Cha17][3]:
  - $\Pr\left[\left|\mathsf{s} \cap \mathsf{h}_j\right| = \sigma | e_j = 0\right] = \binom{d}{\sigma}\pi_0^\sigma(1-\pi_0)^{d-\sigma}$ with
$$\pi_0 = \frac{\bar{\sigma}_{\text{corr}}}{d} = \frac{(w-1)\left|\mathsf{s}\right| - X}{d(n - |\mathsf{e}|)}$$
  - $\Pr\left[\left|\mathsf{s} \cap \mathsf{h}_j\right| = \sigma | e_j = 1\right] = \binom{d}{\sigma}\pi_1^\sigma(1-\pi_1)^{d-\sigma}$ with
$$\pi_1 = \frac{\bar{\sigma}_{\text{err}}}{d} = \frac{|\mathsf{s}| + X}{d\,|\mathsf{e}|}$$
  - Additional term X is not dominant and is approximated by its expected value for a given $|\mathsf{s}|$ and $|\mathsf{e}|$
$E_\ell = |\{\text{equations with } \ell \text{ errors}\}| \quad X = 2E_3 + 4E_5 + \cdots$

[3] 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.

Transitions

Require: $\mathsf{H} \in \{0,1\}^{r\times n}$, $\mathsf{y} \in \{0,1\}^n$
  while $(s \leftarrow \mathsf{y}\mathsf{H}^T) \neq 0$ **do**
    $j \leftarrow \mathsf{sample}(\mathit{context})$
    $T \leftarrow \mathsf{threshold}(\mathit{context})$
    if $|\mathsf{s} \cap \mathsf{h}_j| \geq T$ **then**
      $y_j \leftarrow 1 - y_j$
  return y

- Thresholds defined by the algorithm
- Distributions known from [Cha17][4]

Transitions:

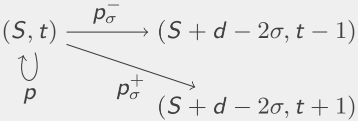
$(S, t) \circlearrowleft$

$(S, t) \longrightarrow (S + |\mathsf{h}_j| - 2\,|\mathsf{s} \cap \mathsf{h}_j|\,, t - 1)$

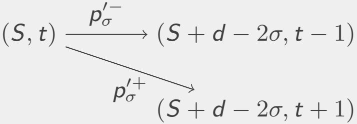
$(S, t) \longrightarrow (S + |\mathsf{h}_j| - 2\,|\mathsf{s} \cap \mathsf{h}_j|\,, t + 1)$

[4]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

- Finite number of iterations



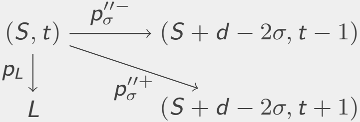
- Infinite number of iterations



$$p_\sigma'^- = \frac{p_\sigma^-}{1 - p}$$

$$p_\sigma'^+ = \frac{p_\sigma^+}{1 - p}$$

- Infinite number of iterations considering the possibility of locking



$$p_\sigma''^- = p_\sigma'^-(1 - p_L)$$

$$p_\sigma''^+ = p_\sigma'^+(1 - p_L)$$

For a fixed rate R:

- cost of an attack on the key:
  $\sim 2^{cw}$
- cost of an attack on the message:
  $\sim 2^{ct}$

for some constant c

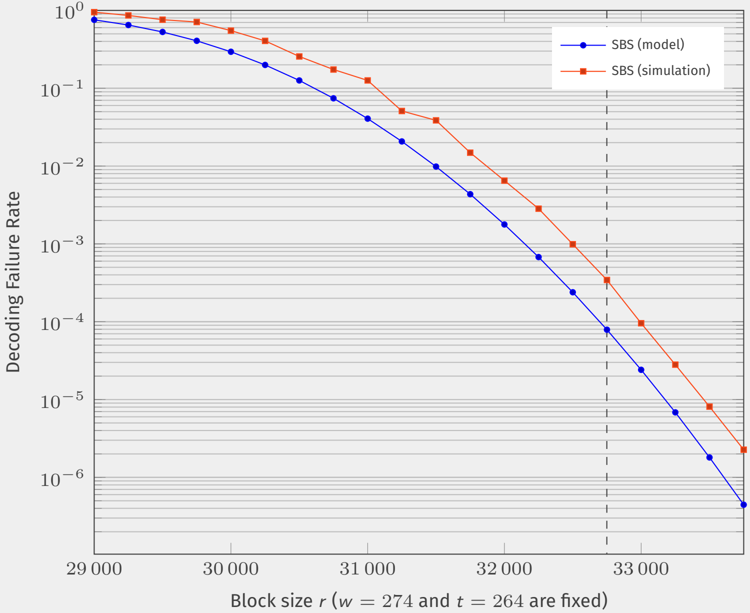
r: block size
n: code length
R: code rate
w: row weight
t: error weight

Changing r:

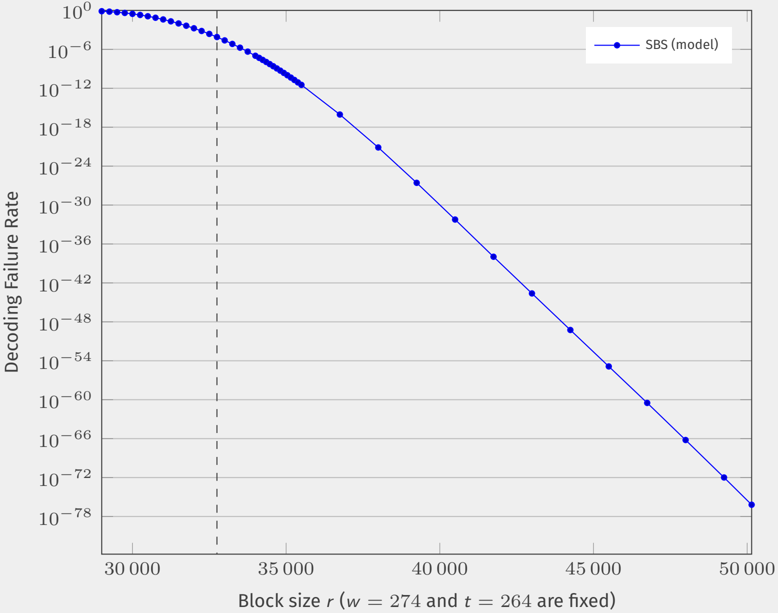
$\rightarrow$ same costs for these attacks

$\rightarrow$ different DFR

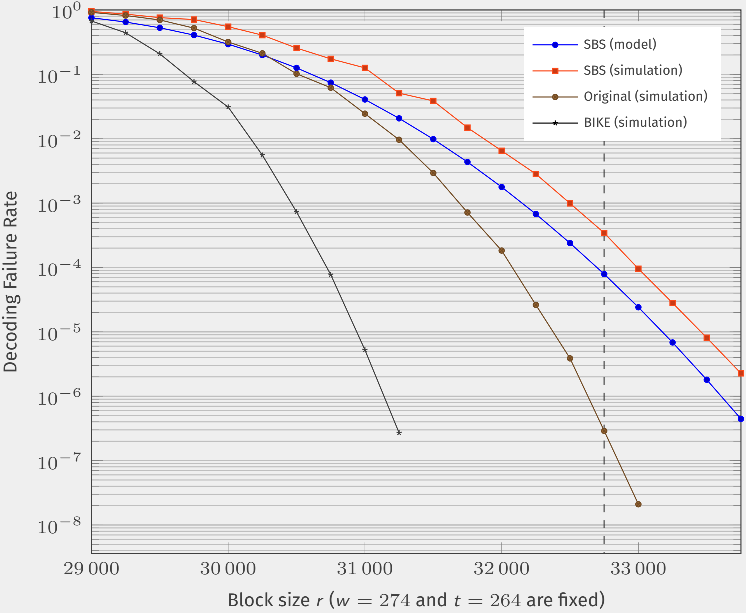
DFR of the step-by-step algorithm (∞ iterations)



DFR OF THE STEP-BY-STEP ALGORITHM (∞ ITERATIONS)



DFR of other algorithms



	$r = 32749$		2^{-128}		2^{-256}	
	(a)	(b)	(c)	(d)	(e)	(f)
SBS (model)	-13.6		$41\,872$		$50\,333$	
SBS (simulation)	-11.5		$40\,952$	$48\,610$	$45\,772$	$66\,020$
Original	-21.7		$36\,950$	$39\,766$	$39\,837$	$48\,215$
BIKE	-47.5	-57.0	$34\,712$	$37\,450$	$37\,159$	$44\,924$

(a): linearly extrapolated value for $\log_2(p_{\text{fail}}(32\,749))$;
(b): quadratically extrapolated value for $\log_2(p_{\text{fail}}(32\,749))$;
(c): minimal r such that $p_{\text{fail}}(r) < 2^{-128}$ assuming a quadratic evolution;
(d): minimal r such that $p_{\text{fail}}(r) < 2^{-128}$ assuming a linear evolution;
(e): minimal r such that $p_{\text{fail}}(r) < 2^{-256}$ assuming a quadratic evolution;
(f): minimal r such that $p_{\text{fail}}(r) < 2^{-256}$ assuming a linear evolution.

- Defined a simpler decoding algorithm
- Modeled this algorithm
- Derived a theoretical DFR from that model
- Assumed a similar behavior for other bitflipping algorithms

$\rightarrow$ Framework to estimate the DFR of other bitflipping algorithms for MDPC