Estimating the QCMDPC decoding failure rate

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
- Promising code-based key exchange mechanism proposed to the NIST call for standardization of quantum safe cryptography
  - “BIKE”
  - “QC-MDPC KEM”

[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.

- For Public Key Encryption
  - [GJS16][2]: attack correlation between faulty error patterns and the secret key
  - $\rightarrow$ System is not IND-CCA
- For a Key Encapsulation Mechanism
  - Avoid a costly new exchange in case of failure
  - Misuse resilience

Objectives:

- Proven low Decoding Failure Rate (e.g. $2^{-\lambda}$ with λ the security parameter)
- Constant-time decoder

[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.

$H = (H_0|H_1) \leftarrow \mathbb{F}_2^{r\times n}$

- Sparse (Row weight: w)
- Quasi-cyclic

$G = (SH_1^T|SH_0^T) \in \mathbb{F}_2^{r\times n}$

- Dense
- Generator matrix of H
- S is a dense circulant block

$\xrightarrow{G}$

$m \leftarrow \{0,1\}^r$
$c = mG$
$e \in \{0,1\}^n$
$|e| = t$

$m = \mathrm{Decode}(y, H)$ $\xleftarrow{y = c + e}$

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

n	r	w	t	security
20 326	10 163	142	134	128
39 706	19 853	206	199	192
65 498	32 749	274	264	256

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

c: codeword
y: noisy codeword
e: error

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

s: syndrome

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

Input : y, H

Output : e

Idea : Write $\mathsf{H} = \left(\mathsf{h}_0, \mathsf{h}_1, \ldots \mathsf{h}_{n-1}\right)$ $\quad \mathsf{s} = \bigoplus_{j, e_j = 1} \mathsf{h}_j$

$$\mathsf{s} \star \mathsf{h}_j = \begin{cases} \mathsf{h}_j \oplus \text{Noise} & \text{if } e_j = 1 \\ \text{Noise} & \text{if } e_j = 0 \end{cases}$$

$$\Rightarrow |\mathsf{s} \star \mathsf{h}_j| = \begin{cases} \text{Big value} & \text{if } e_j = 1 \\ \text{Small value} & \text{if } e_j = 0 \end{cases}$$

(More rigourous analysis in [Cha17][3])

[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.

Classic

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**
    $T \leftarrow \mathrm{threshold}(context)$
    for $j \in \{0,\ldots,n-1\}$ **do**
      if $|\mathsf{s} \star \mathsf{h}_j| \geq T$ **then**
        $y_j \leftarrow 1 - y_j$
  return y

Step-by-step

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**
    $j \leftarrow \mathrm{sample}(context)$
    $T \leftarrow \mathrm{threshold}(context)$
    if $|\mathsf{s} \star \mathsf{h}_j| \geq T$ **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
  - $S = \left|eH^T\right|$: the syndrome weight
  - $t = |e|$: the error weight

Transitions:

- Defined by the algorithm

$$\mathrm{DFR}(S, t) = 1 - \Pr[(S, t) \xrightarrow{\infty} (0, 0)]$$

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**
    $j \leftarrow \mathrm{sample}(context)$
    $T \leftarrow \mathrm{threshold}(context)$
    if $|\mathsf{s} \star \mathsf{h}_j| \geq T$ **then**
      $y_j \leftarrow 1 - y_j$
  return y

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

Transitions:

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

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

$$(S, t) \circlearrowleft$$

[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

- Error positions are always independent
- Infinite number of iterations
- Counters distributions [Cha17][5]:
  - $\Pr\left[|\mathsf{s} \star \mathsf{h}_j| = \sigma | e_j = 0\right] = \binom{d}{\sigma}\pi_0^\sigma(1-\pi_0)^{d-\sigma}$ with

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

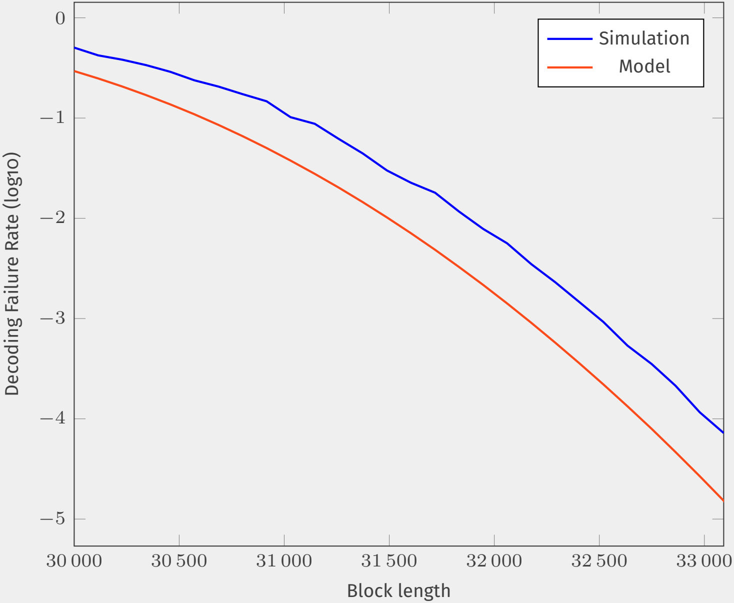
  - $\Pr\left[|\mathsf{s} \star \mathsf{h}_j| = \sigma | e_j = 1\right] = \binom{d}{\sigma}\pi_1^\sigma(1-\pi_1)^{d-\sigma}$ with

$$\pi_1 = \frac{\bar{\sigma}_{\text{err}}}{d} = \frac{|\mathsf{s}| + X}{d\,|\mathsf{e}|}$$

  - Additional term X is not dominant and is approximated by its expected value for a given $|\mathsf{s}|$ and $|\mathsf{e}|$

[5] 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.

Estimation for BIKE-1 Level 5: $d = 137$, $t = 264$



Achieving a DFR of 2^{-64}

security	Original r	Revised r	Ratio	DFR (log2)
128	10 163	13 109	1.29	-66.8
192	19 853	23 669	1.19	-66.2
256	32 749	37 781	1.15	-67.1

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

security	Original r	Revised r	Ratio	DFR (log2)
128	10 163	16 477	1.62	-130.3
192	19 853	31 357	1.58	-194.7
256	32 749	50 459	1.54	-258.0

Nonblocking heuristic:

- Store flipped positions in a queue
- If the algorithm is blocked, dequeue a position
- Reflip the dequeued position

$\rightarrow$ Surprisingly good results

- Step-by-step decoder
  - Not as good as the classical bitflipping
  - But its behavior can be estimated
- Nonblocking heuristic
  - Greatly lowers the Decoding Failure Rate
  - Harder to estimate