Cryptographie post-quantique : étude du décodage des codes QC-MDPC

Soutenance de thèse

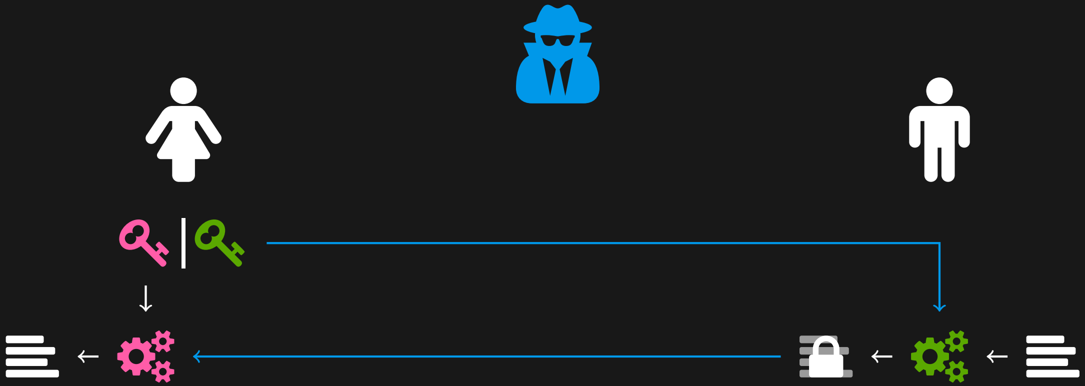
Valentin Vasseur

Université de Paris
Inria

Monday 29th March, 2021

Introduction

Public key cryptography



Post-quantum cryptography

Quantum algorithm for cryptography

[Sho99]: Factorization & Discrete logarithm.

Post-quantum cryptography

Aims at being secure against an adversary with a quantum computer.

NIST Post-Quantum Cryptography Standardization Process — Round 3

	PKE/KEM	Signature
Code	3	0
Lattice	5	2
Hash	0	1
Isogeny	1	0
Multivariate	0	2
Zero-knoweldge	0	1

Classic McEliece
BIKE
HQC

Peter W Shor. 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer'. In: *SIAM Review* 2 (Jan. 1999).

Coding theory

(Binary) Linear code

$\mathbb{F}_2$-*linear code* $\mathcal{C}$ of *length* n and *dimension* k: linear subspace of $\mathbb{F}_2^n$ of dimension k.

Generator matrix

Generator matrix $\mathbf{G} \in \mathbb{F}_2^{k \times n}$: rows form a basis of $\mathcal{C}$.

Parity check matrix

Parity check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k) \times n}$: $\mathcal{C} = \{\mathrm{c} \in \mathbb{F}_2^n \mid \mathbf{H}\mathrm{c}^\mathsf{T} = 0\}$.

Syndrome

Syndrome of $\mathrm{x} \in \mathbb{F}_2^n$: $\mathbf{H}\mathrm{x}^\mathsf{T} \in \mathbb{F}_2^{n-k}$.

Hard problems in code-based cryptography

Syndrome Decoding – SD

Instance: A parity check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$, a syndrome $\mathrm{s} \in \mathbb{F}_2^{n-k}$, a target weight t.
Property: There exists $\mathrm{e} \in \mathbb{F}_2^n$ such that $|\mathrm{e}| = t$ and $\mathbf{H}\mathrm{e}^\intercal = \mathrm{s}$.

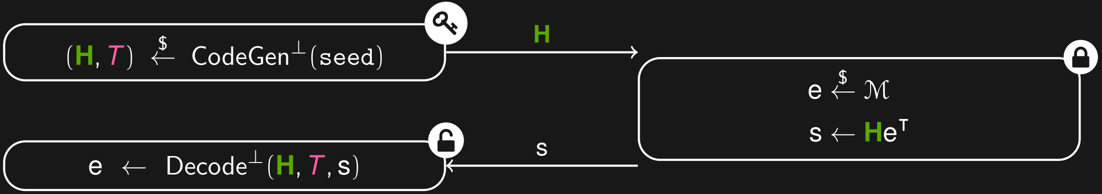
Codeword Finding – CF

Instance: A parity check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$, a target weight $w > 0$.
Property: There exists $\mathrm{e} \in \mathbb{F}_2^n$ such that $|\mathrm{e}| = w$ and $\mathbf{H}\mathrm{e}^\intercal = 0$.

They were proven to be NP-complete in [BMT78].

Elwyn Berlekamp, Robert McEliece and Henk van Tilborg. 'On the inherent intractability of certain coding problems'. In: *IEEE Transactions on Information Theory* 3 (May 1978).

Niederreiter cryptosystem [Nie86]



- $\mathsf{CodeGen}^{\perp}$: Generates a public parity check matrix and a private trapdoor.
- $\mathsf{Decode}^{\perp}$: Polynomial time decoder for any syndrome constructed from $\mathcal{M}$.

Security relies on the difficulty of SD and the difficulty of finding the trapdoor.

Harald Niederreiter. 'Knapsack-type cryptosystems and algebraic coding theory'. In: *Problems of Control and Information Theory* 2 (1986).

Quasi-cyclic code

Circulant matrix

A circulant matrix is a matrix of the form

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

Quasi-cyclic code

A quasi-cyclic code has a parity check matrix consisting of circulant blocks.

Double-circulant code

A double-circulant code has a parity check matrix consisting of two circulant blocks

$$\mathbf{H} = \begin{pmatrix} \underset{\circlearrowright}{\mathrm{h}_0} & \underset{\circlearrowright}{\mathrm{h}_1} \end{pmatrix}.$$

Polynomial representation

Polynomial $\leftrightarrow$ Circulant matrix

$$\mathbf{H} = \begin{pmatrix} h_0 & h_1 & \dots & h_{r-2} & h_{r-1} \\ h_{r-1} & h_0 & h_1 & & h_{r-2} \\ \vdots & h_{r-1} & h_0 & \ddots & \vdots \\ h_2 & & \ddots & \ddots & h_1 \\ h_1 & h_2 & \dots & h_{r-1} & h_0 \end{pmatrix} \xrightarrow{\sim} h_0 + h_1 x + \cdots + h_{r-2}x^{r-2} + h_{r-1}x^{r-1} =: \mathrm{h}$$

$$r \times r \text{ circulant matrices} \quad \simeq \quad \mathbb{F}_2[x]/(x^r - 1) =: \mathcal{R}$$

Underlying problems and best known attacks

QC Syndrome Decoding – QCSD

Instance: $(\mathrm{h}, \mathrm{s}) \in \mathcal{R}^2$, an integer $t > 0$.
Property: There exists $(\mathrm{e}_0, \mathrm{e}_1) \in \mathcal{R}^2$ such that $\mathrm{e}_0 + \mathrm{e}_1 h = \mathrm{s}$ and $|\mathrm{e}_0| + |\mathrm{e}_1| = t$.

QC Codeword Finding – QCCF

Instance: $\mathrm{h} \in \mathcal{R}$, an even integer $w > 0$.
Property: There exists $(\mathrm{h}_0, \mathrm{h}_1) \in \mathcal{R}^2$ such that $\mathrm{h}_1 + \mathrm{h}_0\mathrm{h} = 0$ and $|\mathrm{h}_0| + |\mathrm{h}_1| = w$.

Asymptotically [CS15] best known attacks still cost the same as [Pra62], and with [Sen11]:

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

Rodolfo Canto Torres and Nicolas Sendrier. 'Analysis of Information Set Decoding for a Sub-linear Error Weight'. In: *Post-Quantum Cryptography (PQCrypto)*. 2015.
Eugene Prange. 'The use of information sets in decoding cyclic codes'. In: *IRE Transactions on Information Theory* 5 (Sept. 1962).
Nicolas Sendrier. 'Decoding One Out of Many'. In: *Post-Quantum Cryptography (PQCrypto)*. 2011.

Low / Moderate Density Parity Check codes

	LDPC	MDPC
Row weight	$w = \Theta(1)$	$w = \Theta(\sqrt{n})$
Decoding capability	$t = \Theta(n)$	$t = \Theta(\sqrt{n})$

LDPC decoding algorithms can decode t errors with $t \cdot w < c \cdot n$ for some constant $c < 1$.

Tradeoff between security and code length achieved for $t = \Theta(\sqrt{n})$ and $w = \Theta(\sqrt{n})$.

Quasi-Cyclic Moderate Density Parity Check [MTSB13]

A $[n = 2r, r]$ *QC-MDPC code* has a quasi-cyclic parity check matrix $\begin{pmatrix} \mathrm{h}_0 & \mathrm{h}_1 \\ \circlearrowright & \circlearrowright \end{pmatrix}$ of row weight $w = \Theta(\sqrt{n})$.

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: *IEEE International Symposium on Information Theory (ISIT)*. 2013.

BIKE

Parameters

- r: block size,
- w: row weight,
- t: error weight.

Decoding

Decoding done with an efficient iterative probabilstic algorithm.
It has a Decoding Failure Rate (DFR).

$(h_0, h_1) \xleftarrow{\$} \mathcal{R}$ s.t. $|h_0| = |h_1| = w/2$

$h \leftarrow {h_0}^{-1} h_1$

h →

$(e_0, e_1) \xleftarrow{\$} \mathcal{R}$ s.t. $|e_0| + |e_1| = t$

$c \leftarrow e_0 + e_1 h$

← c

$(e_0, e_1) \leftarrow \text{Decode}(c, h_0, h_1)$

Shared key: $K(e_0, e_1)$

Needs a semantic security conversion to meet IND-CPA or IND-CCA requirements.

Summary on security

Requirements for λ bits of security [FO99; HHK17]

$$\left.\begin{array}{l}\left.\begin{array}{l}\text{1. QCSD costs } 2^{\lambda} \text{ operations,}\\ \text{2. QCCF costs } 2^{\lambda} \text{ operations,}\end{array}\right\}\text{IND-CPA}\\ \text{3. DFR} \leqslant 2^{-\lambda}.\end{array}\right\}\text{IND-CCA}$$

- [GJS16] attack costs in the order of $\frac{1}{\text{DFR}}$ operations.

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

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

[BIKE] IND-CCA parameters

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

λ	r	n	w	t
128	**12 323**	**24 646**	**142**	**134**
192	24 659	49 318	206	199
256	40 973	81 946	274	264

Carlos Aguilar Melchor, Nicolas Aragon, Paulo S L M Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Ghosh Santosh, Shay Gueron, Tim Güneysu, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur and Gilles Zémor. *BIKE*. Aug. 2020.

NIST about BIKE

- “BIKE as one of the most promising code-based candidates”
- “serious questions about side-channel protections and CCA security”
- “need to be resolved before BIKE can be considered for standardization”
- “more time will be needed to address the security concerns listed”
- “not chosen to be a finalist but will advance to the third round for more study”

Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson and Daniel Smith-Tone. ‘Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process’. In: (July 2020).

Goal

Reducing & Proving Decoding Failure Rate.

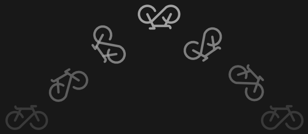
Reducing ↓ better parameters

Proving ↓ security reduction (IND-CCA)

→ Improve performance and confidence in the system.

Contributions

- New decoders with low complexity and high performance
  - Backflip
  - Grey decoders
- Design statistical models
  - Precise model of one iteration accounting for the regularity of the code
  - Full Markovian model of a sequential decoder
- Estimate DFR
  - Extrapolation framework with confidence intervals based on decoding assumption
  - Analysis of weak keys with combinatorial properties that hinder decoding
  - Analysis of error floors



New decoding algorithm: Backflip

Nicolas Sendrier and Valentin Vasseur. 'About Low DFR for QC-MDPC Decoding'. In: *Post-Quantum Cryptography (PQCrypto)*. Paris, France, Apr. 2020

Original bitflipping algorithm

input : $\mathbf{H} \in \mathbb{F}_2^{r\times n}$, $\mathrm{s} = \mathbf{H}\mathrm{e}^\intercal \in \mathbb{F}_2^r$ with $|\mathrm{e}| \leqslant t$
output : $\mathrm{e}' \in \mathbb{F}_2^n$ s.t. $\mathbf{H}\mathrm{e}'^\intercal = \mathrm{s}$
$\mathrm{e}' \leftarrow 0$; $\mathrm{s}' \leftarrow \mathrm{s} - \mathbf{H}\mathrm{e}'^\intercal$;
while $\mathrm{s}' \neq 0$ **do**
  $T \leftarrow \mathtt{threshold}(context)$;
  for $j \in \{0, \ldots, n-1\}$ **do**
    if $|\mathrm{s}' \star \mathbf{h}_j| \geqslant T$ **then**
      $e'_j \leftarrow 1 - e'_j$;
  $\mathrm{s}' \leftarrow \mathrm{s} - \mathbf{H}\mathrm{e}'^\intercal$;
return e';

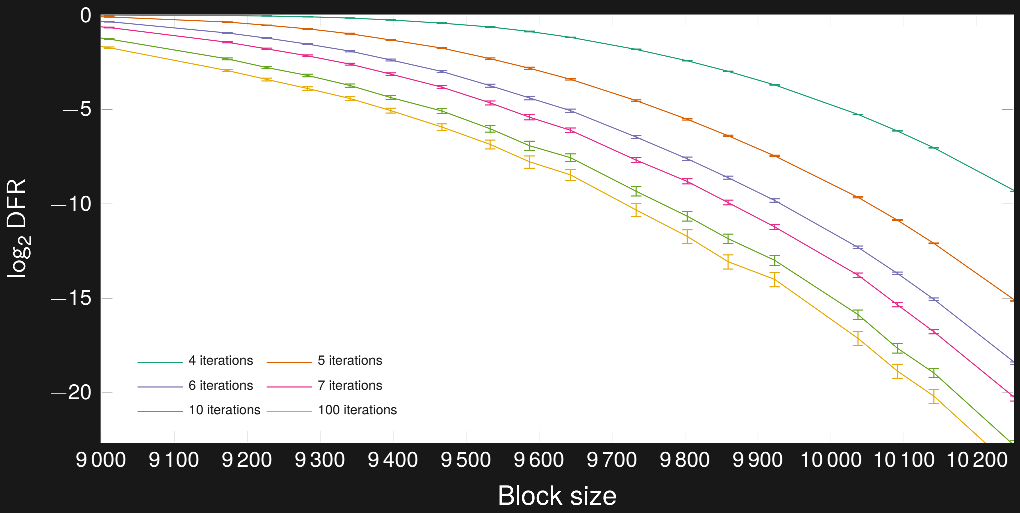
$\mathbf{H}$	:	Parity check matrix
$\mathbf{h}_j$	:	j-th column of $\mathbf{H}$
$\lvert\mathrm{s}' \star \mathbf{h}_j\rvert$	:	counter of position j
i.e.		# unsatisfied equations

Problem of the original algorithm

Algorithm takes bad decisions (adds errors):

- hard to detect,
- hinder progress when too many.

Classic bitflipping



$(w, t) = (142, 134)$

Backflip ideas

Soft decision decoder

A soft decision decoder handles probabilities rather than bits

$\Rightarrow$ better decoding performance,

$\Rightarrow$ not as computationally efficient.

Backflip

- Approach soft decision decoding:
  - limit the impact of a flip based on reliability,
  - counters give a reliability information.
- Each flip has a time-to-live (a few iterations):
  - for each flip, a `ttl` is computed,
  - most reliable flips live longer,
  - at each iteration revert expired flips.

Backflip algorithm

input : $\mathbf{H} \in \mathbb{F}_2^{r \times n}$, $\mathrm{s} = \mathbf{H}\mathrm{e}^\mathsf{T} \in \mathbb{F}_2^r$ with $|\mathrm{e}| \leqslant t$
output : $\mathrm{e}' \in \mathbb{F}_2^n$ s.t. $\mathbf{H}\mathrm{e}'^\mathsf{T} = \mathrm{s}$
$\mathrm{e}' \leftarrow 0$; $\mathrm{s}' \leftarrow \mathrm{s} - \mathbf{H}\mathrm{e}'^\mathsf{T}$; $\mathrm{D} \leftarrow 0$;
while $\mathrm{s}' \neq 0$ **do**
  for $j \in \{0, \ldots, n-1\}$ **do**
    $D_j \leftarrow D_j - 1$;
    if $D_j = 0$ **then** $e'_j \leftarrow 0$;
  $\mathrm{s}' \leftarrow \mathrm{s} - \mathbf{H}\mathrm{e}'^\mathsf{T}$; $T \leftarrow \mathtt{threshold}(context)$;
  for $j \in \{0, \ldots, n-1\}$ **do**
    if $|\mathrm{s}' \star \mathbf{h}_j| \geqslant T$ **then**
      $e'_j \leftarrow 1 - e'_j$;
      $D_j \leftarrow \mathtt{ttl}(|\mathrm{s}' \star \mathrm{h}_j|)$
  $\mathrm{s}' \leftarrow \mathrm{s} - \mathbf{H}\mathrm{e}'^\mathsf{T}$;
return e';

$\mathbf{H}$	:	parity check matrix
$\mathbf{h}_j$	:	j-th column of $\mathbf{H}$
$\lvert\mathrm{s}' \star \mathbf{h}_j\rvert$	:	counter of position j
i.e.		# unsatisfied equations
D	:	time-to-live of flips

Low additional cost of our variant

- each flip has a time-to-live,
- need extra memory to store,
- obsolete flips are reverted first at each iteration.

Thresholds and time-to-live function

Idea

`ttl` is an increasing function of the counter value σ.

Implementation

Thresholds $T_1, T_2, \ldots, T_\ell$: A flip survives i iterations if its counter is above T_i.

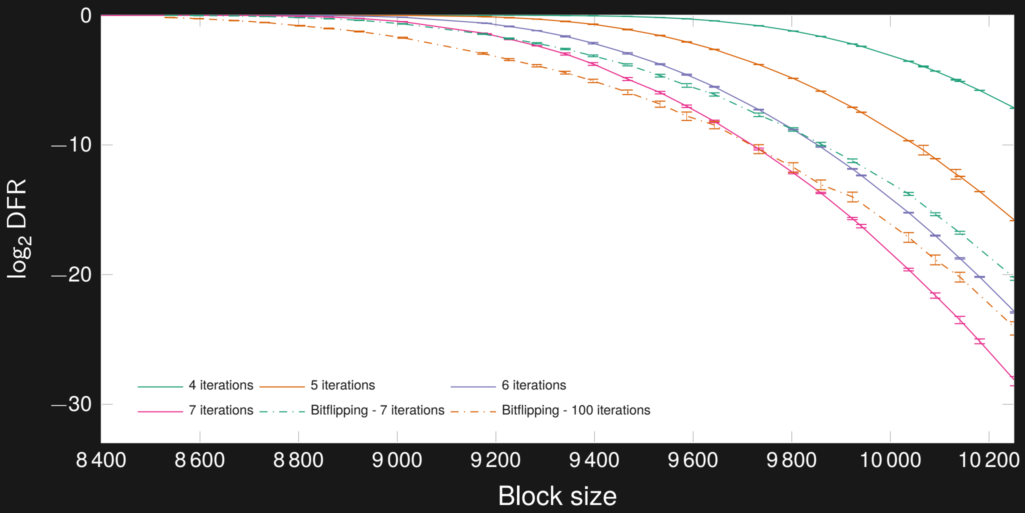
$$n \binom{w/2}{T_i} \pi_0^{T_i} (1 - \pi_0)^{w/2 - T_i} < \alpha_i$$

for some chosen constants $\alpha_1 > \alpha_2 > \cdots > \alpha_\ell > 0$ decreasing exponentially.

π_0:

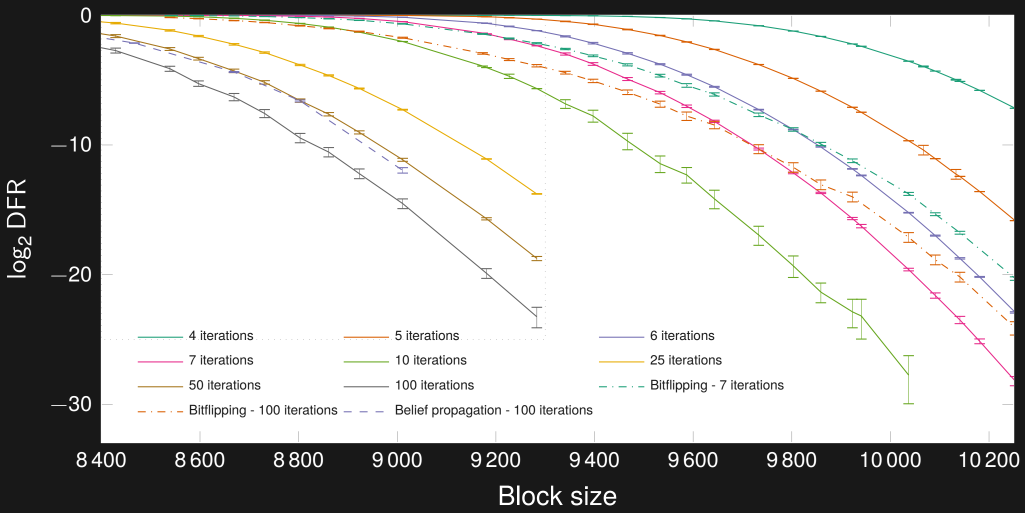
- for a correct position, probability that an equation in which it is involved is unsatisfied,
- well estimated in a statistical model.

Backflip



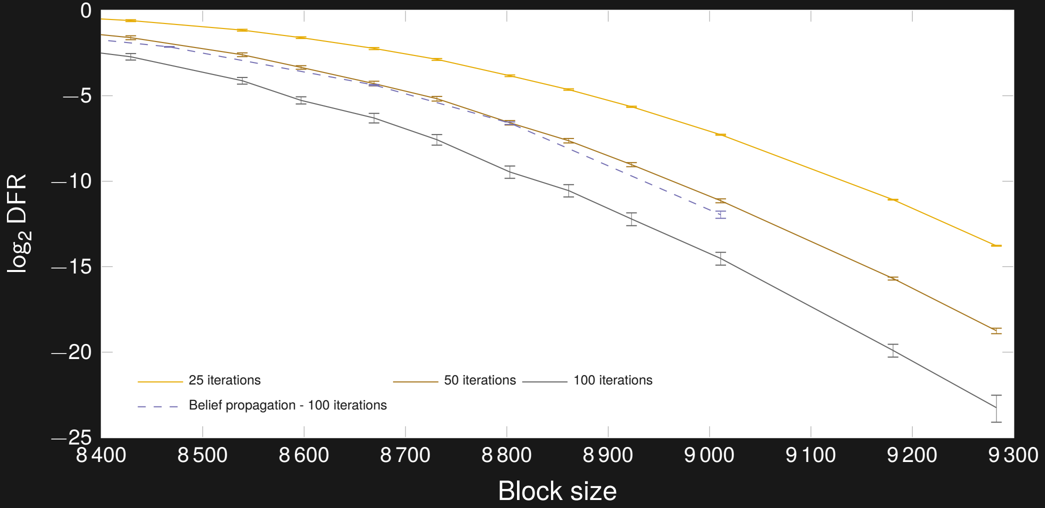
With $\alpha_1 = 8$, $\alpha_2 = 2$, $\alpha_3 = 1/2$, $\alpha_4 = 1/8$, $\alpha_5 = 1/32$. $(w, t) = (142, 134)$

Backflip

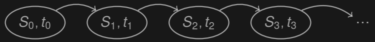


With $\alpha_1 = 8$, $\alpha_2 = 2$, $\alpha_3 = 1/2$, $\alpha_4 = 1/8$, $\alpha_5 = 1/32$. $(w, t) = (142, 134)$

Backflip



With $\alpha_1 = 8$, $\alpha_2 = 2$, $\alpha_3 = 1/2$, $\alpha_4 = 1/8$, $\alpha_5 = 1/32$. $(w, t) = (142, 134)$



Statistical modeling of the bitflipping

Nicolas Sendrier and Valentin Vasseur. 'On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders'. In: *Post-Quantum Cryptography (PQCrypto)*. Chongqing, China, May 2019

Step-by-step algorithm

input : $\mathbf{H} \in \mathbb{F}_2^{r \times n}$, $\mathsf{s} = \mathbf{H}\mathsf{e}^\intercal \in \mathbb{F}_2^r$ with $|\mathsf{e}| \leqslant t$
output : $\mathsf{e}' \in \mathbb{F}_2^n$ s.t. $\mathbf{H}\mathsf{e}'^\intercal = \mathsf{s}$
$\mathsf{e}' \leftarrow 0$; $\mathsf{s}' \leftarrow \mathsf{s} - \mathbf{H}\mathsf{e}'^\intercal$;
while $\mathsf{s}' \neq 0$ **do**
  $T \leftarrow \mathtt{threshold}(\mathit{context})$;
  $j \leftarrow \mathtt{sample}(\mathit{context})$;
  if $|\mathsf{s}' \star \mathbf{h}_j| \geqslant T$ **then**
    $e'_j \leftarrow 1 - e'_j$;
    $\mathsf{s}' \leftarrow \mathsf{s} - \mathbf{H}\mathsf{e}'^\intercal$;
return e';

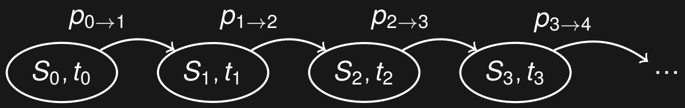
$\mathbf{H}$: Parity check matrix
$\mathbf{h}_j$: j-th column of $\mathbf{H}$
$|\mathsf{s}' \star \mathbf{h}_j|$: counter of position j
i.e. # unsatisfied equations

We write, at iteration i:

$$S_i := |\mathsf{s}'| = \left|\mathbf{H}(\mathsf{e} - \mathsf{e}')^\intercal\right|$$

$$t_i := |\mathsf{e} - \mathsf{e}'|$$

Assumptions: Markov chain



- The step-by-step algorithm is a time-homogeneous Markov chain.

Assumptions: Counters

- Counters are independent
- Numbers of errors per equation are independent

Counters

The counters σ_j follow binomial distributions [Cha17]:

$$\sigma_j \sim \mathrm{Bin}(w/2, \pi_1) \text{ if } j \in \mathrm{e} - \mathrm{e}', \qquad \sigma_j \sim \mathrm{Bin}(w/2, \pi_0) \text{ if } j \notin \mathrm{e} - \mathrm{e}'.$$

with

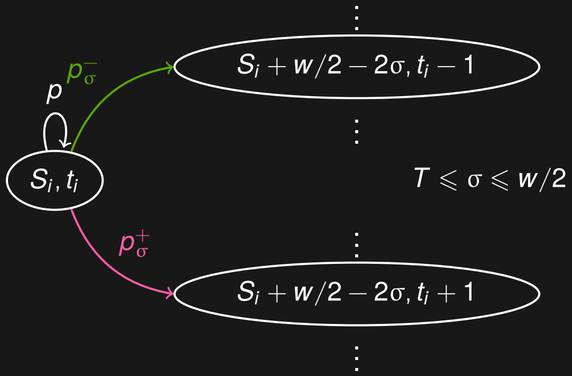
$$\pi_1 = \frac{S_i + \overline{X}}{t_i w/2}, \qquad \pi_0 = \frac{(w-1)S_i - \overline{X}}{(n - t_i)w/2}$$

and $\overline{X} = \xi \, \mathrm{E}[X \mid S_i, t_i]$ for some constant ξ,

$$X = \left(\sum_{j \in \mathrm{e}} \left| \mathrm{s}' \star \mathbf{h}_j \right| \right) - |\mathrm{s}'| .$$

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

Transition diagram



When we flip the column $\mathbf{h}_j$, $s' \leftarrow s' + \mathbf{h}_j$

$$\underbrace{\left|s' + \mathbf{h}_j\right|}_{S_{i+1}} = \underbrace{\left|s'\right|}_{S_i} + \underbrace{\left|\mathbf{h}_j\right|}_{w/2} - 2\underbrace{\left|s' \star \mathbf{h}_j\right|}_{\sigma}$$

Transitions

Transition probabilities are derived from the counters distributions

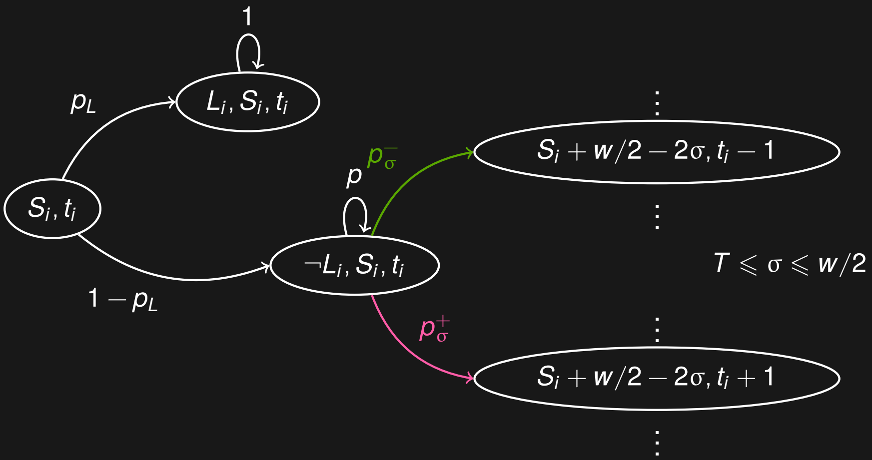
Problem

Model does not account for the situation where all the counters are below the threshold.

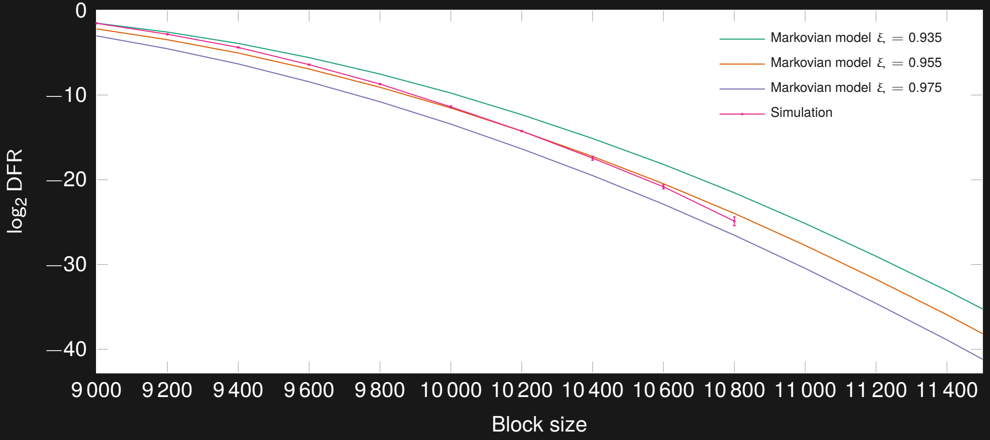
Solution

Add a special state in the FSM for this blocked decoder state.

Transition diagram

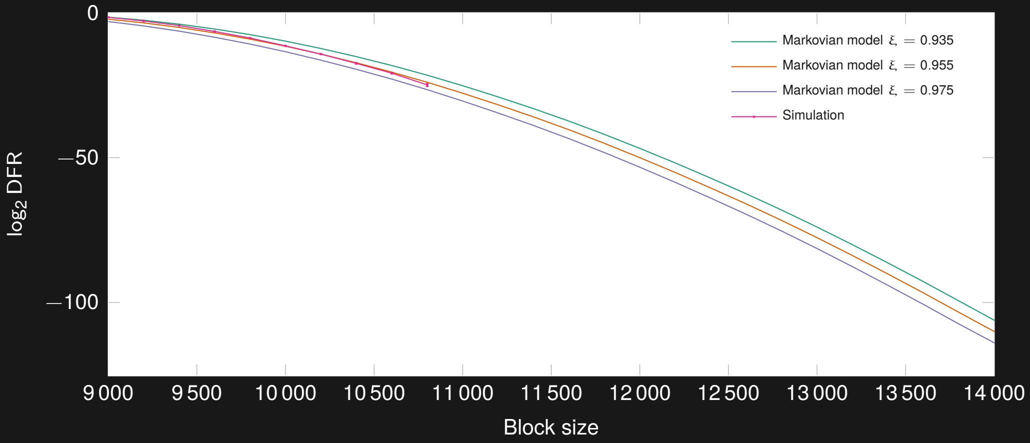


Results

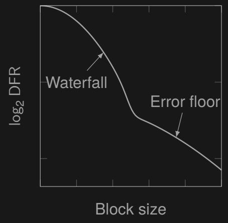


$(w, t) = (142, 134)$

Results



$(w, t) = (142, 134)$



Decoding assumption and validation

Nicolas Sendrier and Valentin Vasseur. ‘On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders’. In: *Post-Quantum Cryptography (PQCrypto)*. Chongqing, China, May 2019

DFR curve behavior

- Step-by-step algorithm — 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, for large r, $\log \mathrm{DFR}$ is an affine function
- Simulation of several variants of decoding algorithm — fixed (w, t), varying r
  - $r \mapsto \log \mathrm{DFR}(r, \mathcal{D})$ is a concave function
- Asymptotic result [Til18] — $w = \Theta(\sqrt{n})$, $t = \Theta(\sqrt{n})$
  - $r \mapsto \log \mathrm{DFR}(r, \mathcal{D})$ is upper bounded by a concave function of r

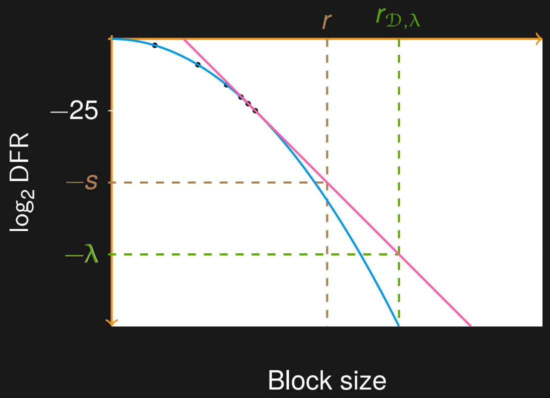
---

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

Decoding assumption

Assumption

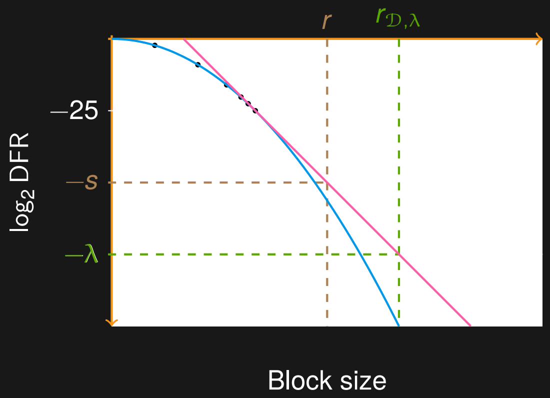
For a given decoder $\mathcal{D}$, and a given security level λ, the function $r \mapsto \log \mathrm{DFR}(r, \mathcal{D})$ is concave.



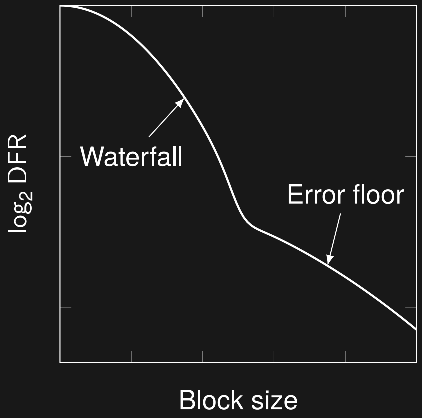
Decoding assumption

Assumption

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



Error floor



Source of error floors [Ric03]

- Low weight codewords
- “Near codewords”

Tom Richardson. ‘Error Floors of LDPC Codes’. In: *41st Annual Allerton Conference on Communication, Control, and Computing*. 2003.

In a QC-MDPC code

Near-codeword

A (u, v) near-codeword is an error pattern of (small) weight u that produces a syndrome of (small) weight v.

$$\mathrm{s} = \mathrm{h}_0\mathrm{e}_0 + \mathrm{h}_1\mathrm{e}_1$$

e_0	e_1	s	$\lvert\mathrm{e}_0\rvert + \lvert\mathrm{e}_1\rvert$	$\lvert\mathrm{s}\rvert$
$\mathcal{C}$: low weight codewords				$\#\mathcal{C} = r$
$x^i\mathrm{h}_1$	$x^i\mathrm{h}_0$	0	w	0
$\mathcal{N}$: $(w/2, w/2)$ near-codewords				$\#\mathcal{N} = 2r$
$x^i\mathrm{h}_0$	0	$x^i\mathrm{h}_0^2$	$w/2$	$w/2$
0	$x^i\mathrm{h}_1$	$x^i\mathrm{h}_1^2$	$w/2$	$w/2$
$2\mathcal{N}$: $(w, \approx w)$ near-codewords				$\#2\mathcal{N} = r^2$
$x^i\mathrm{h}_0$	$x^j\mathrm{h}_1$	$x^i\mathrm{h}_0^2 + x^j\mathrm{h}_1^2$	w	$\approx w$

Impact of near-codewords on DFR

$\mathcal{S}$: either $\mathcal{C}$ or $\mathcal{N}$ or $2\mathcal{N}$

$\mathcal{E}$: set of all the error patterns

Problem

Decoding is impaired when the error pattern is close to an element of $\mathcal{S}$

Experiment

Define $\mathcal{A}_{\delta,\mathcal{S}}$: set of vectors at distance exactly δ of $\mathcal{S}$
For any $\delta > 0$, generate error patterns of $\mathcal{A}_{\delta,\mathcal{S}}$ and evaluate

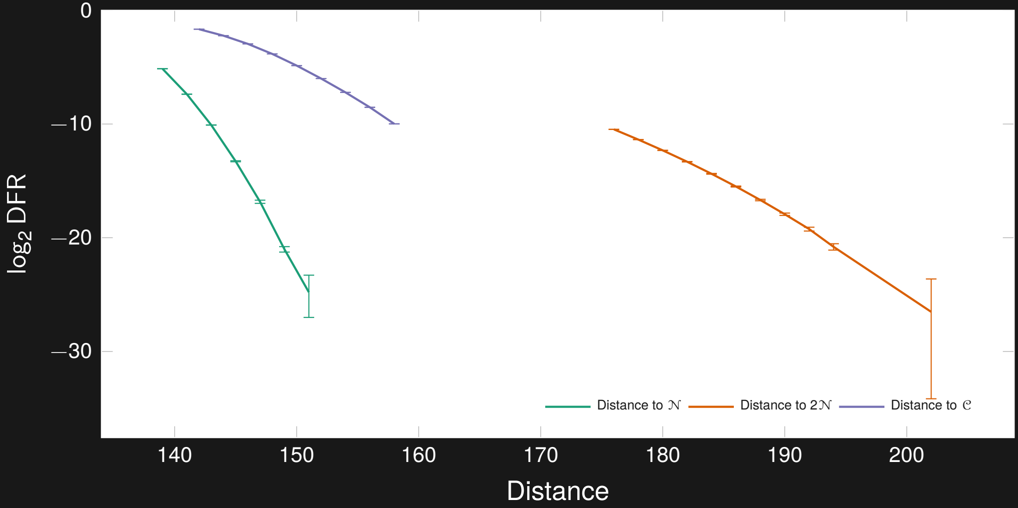
$$\mathrm{DFR}_{\mathcal{A}_{\delta,\mathcal{S}}}$$

Decoding assumption

The decoding assumption is wrong if there exists a δ such that

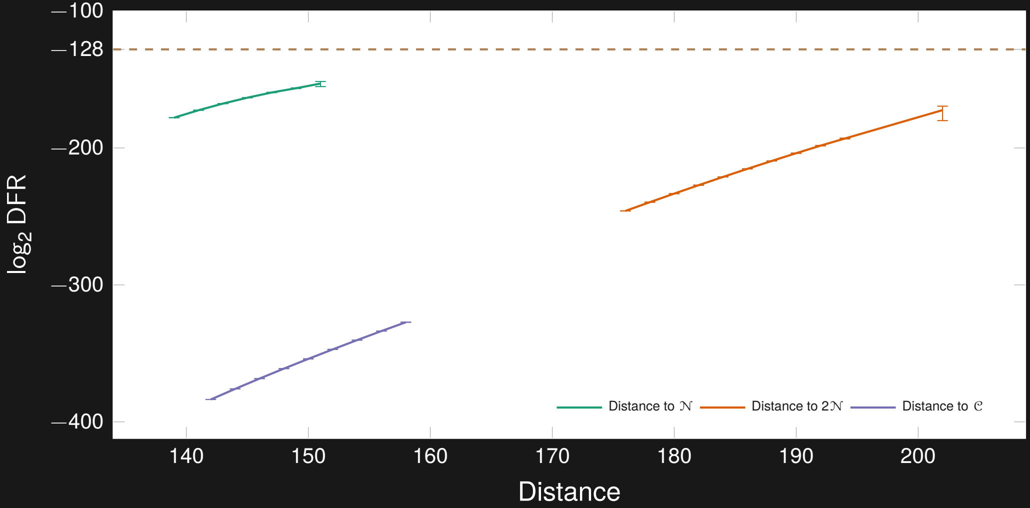
$$2^{-\lambda} < \frac{\#\mathcal{A}_{\delta,\mathcal{S}}}{\#\mathcal{E}} \mathrm{DFR}_{\mathcal{A}_{\delta,\mathcal{S}}} < \mathrm{DFR}$$

DFR *vs.* distance with Backflip (7 iterations) - raw data



$$(r, w, t) = (12\,323, 142, 134)$$

DFR *vs.* distance with Backflip (7 iterations) - weighted by density



$(r, w, t) = (12\,323, 142, 134)$

Conclusion and perspectives

- New decoders with low complexity and high performance
  - Backflip
  - Grey decoders
- Design statistical models
  - Precise model of one iteration accounting for the regularity of the code
  - Full Markovian model of a sequential decoder
- Estimate DFR
  - Extrapolation framework with confidence intervals based on decoding assumption
  - Analysis of weak keys with combinatorial properties that hinder decoding
  - Analysis of error floors

Perspectives:

- Better understand the mechanics behind Backflip to have a better `ttl` function
- Improve model to estimate the syndrome weight distribution
- Understand the link between weak keys/near-codeword and counters correlations