On the Hardness of Decoding Quasi-Cyclic Codes and the Security of Code-Based Public-Key Cryptosystems

Alessandro Annechini[1][a], Alessandro Barenghi[1][b] and Gerardo Pelosi[1][c]
[1]*Department of Electronics, Information and Bioengineering - DEIB, Politecnico di Milano, Milano, Italy*
{alessandro_annechini, alessandro_barenghi, gerardo_pelosi}@polimi.it

Keywords: Post-quantum Cryptography, Code-based Cryptography, Quasi-Cyclic Codes

Abstract: Post-quantum public key encryption (PKE) schemes employing Quasi-Cyclic (QC) sparse parity-check matrix codes are enjoying significant success, thanks to their good performance profile and significant reduction in the keypair size. However, there is no formal proof that the hardness of decoding random QC codes is related to the decoding hardness of random codes, which is known to be NP-hard, nor that changing the (constant in the length) rate of the employed QC codes does not change the nature of the underlying hard problem. In this work, we address and solve these challenges, answering both of them in the affirmative. First, we prove computational equivalences among hard problems from coding theory and the corresponding problems for QC codes. Then, we provide a systematization of hard problems and security assumptions underlying QC-MDPC-based cryptosystems, proving that fixing the rate of the QC codes does not change the hardness of key recovery attacks. These results allow the design of Niederreiter-style QC-MDPC PKEs, with the additional flexibility granted by freely choosing the code rate, leading to code-based public key encryption schemes which are both secure and can be fit in very demanding scenarios, such as embedded systems.

1 INTRODUCTION

Designing post-quantum cryptosystems and digital signature schemes has seen a significant amount of interest in recent years, as a consequence of a steady intellectual and economic investment in the advancement of quantum computing technologies. A further spur to the interest in the topic was the public international contest by the US National Institute of Standards and Technology (NIST) for the selection of a portfolio of post-quantum cryptosystems and signatures. Indeed, the US NIST has selected, after a five years long public scrutiny process, two candidate Key Encapsulation Methods (KEMs), i.e. Public Key Encryption (PKE) schemes augmented with a construction fit to encrypting a small random bitstring to be used as a symmetric key to encrypt long messages and three signature schemes, with an on-going further call for other standardization candidates.

The most promising computationally hard problems on which to build post quantum cryptosystems, in terms of both confidence in their computational intractability, and efficiency of the derived cryptosystems come from either discrete lattices or the theory of linear error correction codes. The reason for the selection of two candidate KEMs by NIST, CRYSTALS-Kyber (Bos et al., 2018; Kevin M. Stine, 2024) and HQC (Melchor et al., 2025), was to avoid relying on a single computationally hard problem (CRYSTALS-Kyber is built on lattices, while HQC on hard problems from coding theory).

The work of Berlekamp, McEliece and Van Tilborg (Berlekamp et al., 1978) proving that decoding errors through a randomly chosen error correction code, or finding one of its codewords given the Hamming weight, are NP-hard problems, (as their decision version are NP-complete), acted as the starting points to build public key cryptosystems relying on hard problems in coding theory. Three templates to build a cryptosystem out of coding-theory based problems were proposed by McEliece (McEliece, 1978), Niederreiter (Niederreiter, 1986) and, later by Alekhnovich (Alekhnovich, 2003). While the latter relies only on the computational hardness of decoding random codes, the former two templates require choosing an efficiently decodable code, and transform its representation to hide its structure, making it indistinguishable from a randomly sampled code. The

[a] https://orcid.org/0009-0009-4452-802X
[b] https://orcid.org/0000-0003-0840-6358
[c] https://orcid.org/0000-0002-3812-5429

McEliece and Niederreiter cryptosystem templates were proven to provide equivalent security if the same structured code is chosen in both cases; Niederreiter's template is usually chosen, as it provides shorter ciphertexts. Unfortunately, choosing an efficiently decodable code whose structure can be hidden is significantly challenging, with proposals such as the original one by Niederreiter (Niederreiter, 1986) (employing Reed-Solomon codes) being broken. Currently, the choice of only two code families survived cryptanalytic attacks: the original binary Goppa codes selected by McEliece, which gave rise to the NIST contest participant Classic McEliece (Albrecht et al., 2022), and the sparse Quasi-Cyclic (QC) parity-check matrix codes, resulting in the design of the NIST contest participants LEDAcrypt-KEM (Baldi et al., 2025) and BIKE (Aragon et al., 2025), which employ the low/medium density parity check codes (LDPC/MDPC) as sparse codes.

Employing QC (random) codes was also the intuition which allowed to make Alekhnovich's template practically viable, resulting in the design of HQC (Melchor et al., 2018). Indeed, using QC codes allows representing the matrices describing a code with a row single vector of a matrix instead of the full matrix, significantly reducing the key sizes. Employing a QC structure with an algebraic code was shown to add too much structure to the code itself, facilitating the removal of the hiding required by Niederreiter's template (Sidelnikov and Shestakov, 1992). Classic McEliece, adopting Goppa codes, accepts the tradeoff of having a full matrix as its significantly large public key (256–1024 KiB, for the recommended parameter choices (Albrecht et al., 2022)). By contrast, using sparse Quasi-Cyclic (QC) parity-check matrix codes such as QC-MDPC/QC-LDPC, which are random QC codes characterized uniquely by the sparsity of one of their parity-check matrices, in Niederreiter's template is maintained to be secure, with only a small known polynomial loss in the (exponential) security margin. Furthermore, such an approach is known to attain smaller public keys and ciphertexts with respect to the use of random QC codes in Alekhnovich's template.

This strategy has been implemented in two cryptosystems, BIKE (Aragon et al., 2025) and LEDAcrypt-KEM (Baldi et al., 2025), with BIKE relying on QC-MDPC codes with rate $\frac{1}{2}$, and LEDAcrypt-KEM relying on QC-LDPC codes with rate $\in \left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}\right\}$. While the original LEDAcrypt-KEM design has been proven insecure due to weak keys coming from the QC-LDPC design (Apon et al., 2020), instantiating LEDAcrypt-KEM with QC-MDPC codes, as in BIKE, is secure, and provides the additional flexibility of choosing the code rate, enabling a tradeoff between public key and ciphertext sizes. Indeed, QC-MDPC codes with rate greater than $\frac{1}{2}$ yield smaller ciphertexts.

Despite the widespread use of QC codes in post-quantum cryptography, no formal proof exists relating the hardness of decoding QC codes to the decoding hardness of random codes, in a similar fashion to what takes place with lattice and cyclic lattice problems. Moreover, it is yet to be proven that that fixing the rate of the QC codes employed in the cryptosystem to any value $\frac{n_0-1}{n_0}$ does not modify the nature of the underlying hard problem.

Contributions. In this work, we provide a proof that employing QC random codes has essentially the same complexity of considering fully random codes, as decoding them is still NP-hard, paving the way for a complete proof of the hardness of structural attacks on QC-MDPC based cryptosystems. Our second contribution is the systematization of the relations between computationally hard problems underpinning QC-MDPC based cryptosystems, highlighting that proving the hardness of a single remaining assumption would make the exact cryptographically hard problem employed NP-hard. Our third contribution is to prove that considering rates $\neq \frac{1}{2}$ does not constitute a vulnerability for QC-MDPC cryptosystem, thus providing sound security guarantees which enable a secure tradeoff between public key and ciphertext sizes, as in LEDAcrypt-KEM (Baldi et al., 2025).

2 RELATED WORK

The following two computationally hard problems, stated and proven to be NP-complete in (Berlekamp et al., 1978) have since then been the mainstay for building code-based cryptosystems.

Definition 1 (Decisional Syndrome Decoding Problem (D-SDP$_{n,k,t}(\mathbf{H},\mathbf{s})$))**.** *Given a generic parity-check matrix* $\mathbf{H} \in \mathbb{F}_2^{r\times n}$*, a binary vector* $\mathbf{s} \in \mathbb{F}_2^r$ *and an integer* $t > 0$ *determine if there is a (column) binary vector* $\mathbf{e}$*, with* $\mathtt{wt}(e) \leq t$ *s.t.* $\mathbf{s}$ *is the syndrome of* $\mathbf{e}$ *through* $\mathbf{H}$*, i.e.,* $\mathbf{s} = \mathbf{He}$*.*

Definition 2 (Decisional Codeword Finding Problem (D-CFP$_{n,k,w}(\mathbf{H})$))**.** *Given a generic parity-check matrix* $\mathbf{H} \in \mathbb{F}_2^{r\times n}$ *and an integer* $w > 0$*, determine if there is a binary vector* $\mathbf{e} \in \mathbb{F}_2^n$*, with* $\mathtt{wt}(\mathbf{e}) = w$ *s.t.* $\mathbf{s} = \mathbf{He} = \mathbf{0}$*, i.e.,* $\mathbf{e}$ *is a codeword.*

The question on whether the variant of the D-CFP$_{n,k,w}$ considering a lesser-or-equal match on the weight of the binary vector $\mathbf{e}$, i.e., $0 < \mathtt{wt}(\mathbf{e}) \leq w$,

denoted as D-CFPLE$_{n,k,w}(\mathbf{H})$, is NP-complete or not was left open in (Berlekamp et al., 1978), and mentioned to be interesting as it would imply that computing the minimum distance of a random code, given its parity-check matrix, denoted as MINDIST$_{n,k,w}(\mathbf{H})$, is also NP-complete. The question was solved in the affirmative by Vardy in (Vardy, 1997), where it is shown that the decision problem is effectively NP-complete, and thus its search version is NP-hard.

In 1986, Harald Niederreiter (Niederreiter, 1986) proposed a PKE scheme based on the hardness of the D-CFP$_{n,k,w}$, and on the impossibility of retrieving the error (equiv., the information word) employing a code admitting an efficient decoding, when provided only with the systematic form of its scrambled parity-check matrix. The first proposal of the Niederreiter cryptosystem was described employing Generalized Reed-Solomon codes, which in turn were subsequently proven to fail the second aforementioned assumption (Sidelnikov and Shestakov, 1992). The Niederreiter design yields a PKE with more compact ciphertexts than the alternative code-based PKE proposed by McEliece (McEliece, 1978), while retaining the same security guarantees, if the hidden codes are of the same kind (Li et al., 2006).

Choosing a sparse code as the hidden decodable code in a Niederreiter PKE was first proposed in (Monico et al., 2000) exploiting the intuition that sparse random codes lack algebraic structure and should therefore be easier to hide. The combination of this choice with QC codes to reduce the key size was proposed in (Baldi et al., 2008; Misoczki et al., 2012), and lead, after improvements, to the design of the "Bit Flipping Key Encapsulation" scheme, known as BIKE (Aragon et al., 2025), and to the key encapsulation scheme included in the "Low-dEnsity parity-check coDe-bAsed cryptographic systems", known as LEDAcrypt-KEM (Baldi et al., 2025), both proposed as code-based post-quantum KEMs. Following Niederreiter's construction, BIKE and LEDAcrypt-KEM rely on the hardness of distinguishing QC codes admitting a sparse parity-check matrix from random QC codes, and on the hardness of decoding QC codes.

It is currently unknown whether hard problems involving random codes, such as the D-CFP$_{n,k,w}$ and the D-CFPLE$_{n,k,w}$, are NP-complete when constrained on random QC codes. In a related work, the authors of (Berger et al., 2009, Proposition 4) report a proof sketch for the NP-hardness of a variant of D-SDP for quasi-cyclic codes. However, the definition of QC codes in the proof considers a parity-check matrix different from the one employed in BIKE and LEDAcrypt-KEM, and limited to a 2×1 circulant tiling of blocks. In its current form, the result, while correct, is not applicable to the instances of hard problems which we will employ in the design of the cryptosystems of interest.

3 BACKGROUND

In this section we summarize notions and definitions from coding theory, and we describe the code-based Niederreiter-style public key encryption (PKE) schemes LEDAcrypt-KEM (Baldi et al., 2025) and BIKE (Aragon et al., 2025).

Notation. A vector $\mathbf{v} \in \mathbb{F}_2^n$ represents a column vector with $n \geq 1$ entries in $\mathbb{F}_2$. The notation $\mathbf{v}_{n\times 1}$ denotes a column vector of size n, while $\mathbf{v}_{1\times n}$ a row vector of size n. We denote as $\mathtt{wt}(\mathbf{v})$ the Hamming weight of $\mathbf{v}$, i.e., the number of non-zero elements in it, while the null vector is denoted as $\mathbf{0}$. A matrix $\mathbf{M} \in \mathbb{F}_2^{n_1\times n_2}$ has n_1 rows and n_2 columns. The identity matrix is denoted by $\mathbf{I}$. The element at row i and column j of a matrix $\mathbf{M}$ is written as $m_{i,j}$, with $0 \leq i < n_1$ and $0 \leq j < n_2$. If $\mathbf{M}$ is defined as a block matrix, $\mathbf{M}_{i,j}$ indicates the submatrix at row i and column j. Given a binary polynomial $\mathtt{a}(x) \in \mathbb{F}_2[x]$ of degree $p \geq 1$, we denote by $\mathbf{A} = \mathbf{circ}(\mathtt{a}(x))$ the associated $p \times p$ circulant matrix. The first row of $\mathbf{A}$ consists of the coefficients of $\mathtt{a}(x)$, ordered from least to most significant. Each subsequent row is a one-bit circular right shift of the previous one.

Given two computational problems P and Q, we will denote as P $\leq_P$ Q the fact that it is possible to reduce polynomially P to Q (Cook reduction), i.e., it is possible to solve P in polynomial time given a solver for Q. A stronger notion of reduction, of which we will make use for decision problems, is the *many-to-one*, polynomial time reduction (Karp reduction). We say that P Karp-reduces to Q, denoted as P $\leq_p$ Q iff, given a solver for Q, it is possible to transform an instance of P in an input for a solver for Q and return the solution obtained from the latter as a solution for the instance of P. The complexity classes NP and P are closed under Karp reduction, and this enables to prove that P $\in$ NP, knowing that Q $\in$ NP, by proving that P $\leq_p$ Q and Q $\leq_p$ P. We will denote computational equivalence under Karp reductions as P $=_p$ Q, while equivalence under Cook reductions will be denoted as P $=_P$ Q.

3.1 Preliminaries on Coding Theory

Binary error correcting codes rely on a redundant representation of information as binary strings to detect and correct errors which may occur during transmission. In the following, we consider binary codes

known as *block codes* acting on a finite binary sequence at once known as the *information word*.

Binary Linear Codes. A binary linear code is a subspace of $\mathbb{F}_2^n$ obtained as the image of a bijective linear map $\mathcal{C}[n,k]:\mathbb{F}_2^k\to\mathbb{F}_2^n$, $n,k\in\mathbb{N}^+$, with $k\leq n$, between any binary k-tuple, a.k.a. *information word* and a binary n-tuple, a.k.a. *codeword*. The values n and k are known as the length and the dimension of the code, respectively, and their ratio $\frac{k}{n}$ defines the code rate. Encoding in $\mathcal{C}[n,k]$ means converting an information word $\mathbf{u}\in\mathbb{F}_2^k$ into its corresponding codeword $\mathbf{c}\in\mathbb{F}_2^n$. Given a codeword $\widetilde{\mathbf{c}}$ corrupted by an unknown error vector $\mathbf{e}\in\mathbb{F}_2^n$, with $\mathtt{wt}(\mathbf{e})\leq t$, i.e.: $\widetilde{\mathbf{c}}=\mathbf{c}\oplus\mathbf{e}$, recovering the original information word $\mathbf{u}$ and the error vector $\mathbf{e}$ requires the application of a *decoding procedure*, which is able to correct up to t bit-flips occurred to the coordinates of the original codeword. The parameter $t>0$ denotes the error correcting power of the code $\mathcal{C}[n,k]$ in a chosen metric. In this work, we consider only the Hamming metric, which defines the distance between two $n\times 1$ binary vectors $\mathbf{u},\mathbf{v}\in\mathbb{F}_2^n$, as the number of their components that have distinct values in corresponding positions. In this metric, decoding associates each corrupted codeword $\widetilde{\mathbf{c}}\in\mathbb{F}_2^n$ to its closest codeword $\mathbf{c}\in\mathcal{C}[n,k]$, where $\mathcal{C}$ is s.t. the Hamming ball of radius t around any codeword, defined as $\mathcal{B}(\mathbf{c},t)=\{\mathbf{v}\in\mathbb{F}_2^n:\mathtt{dist}(\mathbf{v},\mathbf{c})\leq t\}$, contains no other codeword of $\mathcal{C}$. In this regard, it is easy to infer that the (minimum) distance of the code, d, which is defined as the minimum distance between two codewords, i.e., $d=\min_{\mathbf{c}_1,\mathbf{c}_2\in\mathcal{C}}\{\mathtt{dist}(\mathbf{c}_1,\mathbf{c}_2)\}=\min_{\mathbf{c}\in\mathcal{C}}\{\mathtt{dist}(\mathbf{c},\mathbf{0})\}=\min_{\mathbf{c}\in\mathcal{C}}\{\mathtt{wt}(\mathbf{c})\}$, must be such that $d\geq 2t+1$ to guarantee the existence of a decoding procedure.

The linear error correcting code $\mathcal{C}[n,k]$ can be described by any set of k linearly independent codewords $\{\mathbf{g_0},\mathbf{g_1},\ldots,\mathbf{g_{k-1}}\}\in\mathbb{F}_2^n$, i.e., by a *basis* of $\mathcal{C}$. As a consequence, any codeword $\mathbf{c}\in\mathcal{C}$ can be computed also as $\mathbf{c}^\mathtt{T}=\mathbf{u}^\mathtt{T}\mathbf{G}$, where $\mathtt{T}$ denotes a transposition, while the $k\times n$ binary matrix $\mathbf{G}$ is obtained by stacking the basis vectors $\mathbf{g_i}^\mathtt{T}$, with $0\leq i<k$, in such a way that $\mathbf{g_0}^\mathtt{T}$ is on top of $\mathbf{g_1}^\mathtt{T}$, $\mathbf{g_1}^\mathtt{T}$ is on top of $\mathbf{g_2}^\mathtt{T}$, and so on. The $k\times n$ matrix $\mathbf{G}$ is called *generator matrix* of the code $\mathcal{C}[n,k]$. Note that the same code $\mathcal{C}[n,k]$ admits multiple generator matrices $\mathbf{G}$ up to a pre-multiplication of $\mathbf{G}$ by a $k\times k$ non-singular matrix over $\mathbb{F}_2$, corresponding to a change of the basis defining $\mathbf{G}$. To indicate the code $\mathcal{C}[n,k]$ described by a given generator matrix $\mathbf{G}$, we will write $\mathcal{C}(\mathbf{G})$.

Definition 3 (Systematic Form of a Generator Matrix)**.** *A generator matrix is said to be in systematic form if it is expressed as* $\mathbf{G}=[\mathbf{Q}\mid\mathbf{I}]$*, where* $\mathbf{Q}$ *is a* $k\times r$ *matrix and* $\mathbf{I}$ *is a* $k\times k$ *identity matrix. The systematic form of* $\mathbf{G}$ *is unique.*

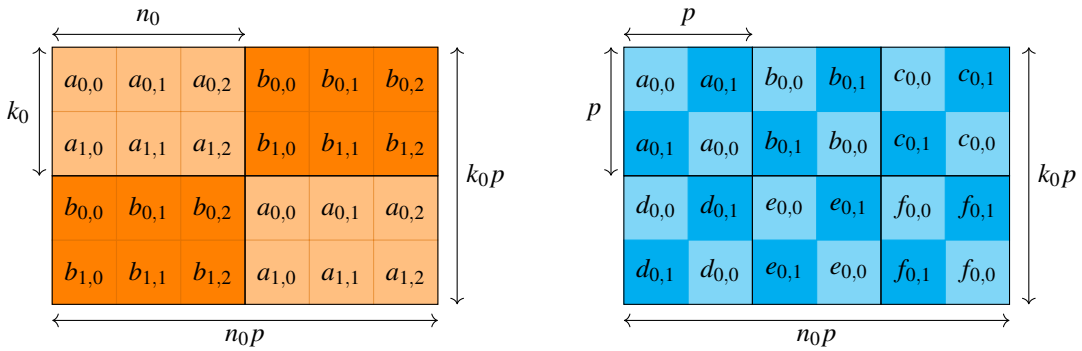
Definition 4 (Permutation Equivalent Codes)**.** *Given two linear codes* $\mathcal{C}[n,k]$*,* $\mathcal{C}'[n,k]$*, they are said to be permutation equivalent if there is a permutation of coordinates mapping each codeword of* $\mathcal{C}[n,k]$ *bijectively into a codeword of* $\mathcal{C}'[n,k]$*. Analogously, given a generator matrix* $\mathbf{G}$ *for* $\mathcal{C}[n,k]$*, a generator matrix* $\mathbf{G}'$ *for a permutation equivalent code* $\mathcal{C}'[n,k]$ *is obtained by permuting the columns of* $\mathbf{G}$*.*

Note that permutation equivalent codes have the same minimum distance. Since the (row) rank of a generator $\mathbf{G}$ of a code $\mathcal{C}[n,k]$ is k, even if $\mathcal{C}[n,k]$ does not admit a systematic form, there is a permutation equivalent code $\mathcal{C}'[n,k]$ that does: it is the one described by a $\mathbf{G}'$ obtained by permuting the columns of $\mathbf{G}$ s.t. the rightmost $k\times k$ submatrix has full rank.

Consider the dual space of $\mathcal{C}[n,k]$, $\mathcal{C}[n,k]^\perp$, i.e., the subspace of $\mathbb{F}_2^n$ containing all and only the vectors orthogonal to any codeword in $\mathcal{C}[n,k]$, with dimension $\dim\left(\mathcal{C}[n,k]^\perp\right)=n-\dim(\mathcal{C}[n,k])=n-k=r$. A basis for $\mathcal{C}[n,k]^\perp$, which is known as the *dual code* of $\mathcal{C}[n,k]$ is obtained by choosing r linearly independent (column) vectors $\mathbf{h}_i\in\mathcal{C}[n,k]^\perp\subseteq\mathbb{F}_2^r$, $0\leq i<r$. Subsequently, an $r\times n$ matrix $\mathbf{H}$ can be obtained by stacking $\mathbf{h_0}^\mathtt{T}$ on top of $\mathbf{h_1}^\mathtt{T}$, $\mathbf{h_1}^\mathtt{T}$ on top of $\mathbf{h_2}^\mathtt{T}\ldots$, to the end of exhibiting a generator matrix for the so-called dual code of $\mathcal{C}[n,k]$, i.e., $\mathcal{C}[n,r]^\perp$. The $r\times n$ matrix $\mathbf{H}$ is also called *parity-check matrix* of the code $\mathcal{C}[n,k]$. For any n-bit vector $\mathbf{x}\in\mathbb{F}_2^n$, the $r\times 1$ vector $\mathbf{s}=\mathbf{H}\mathbf{x}\in\mathbb{F}_2^r$, is known as the syndrome of $\mathbf{x}$ through $\mathbf{H}$. Being $\mathbf{H}$ a basis of $\mathcal{C}[n,k]^\perp$, every $\mathbf{c}\in\mathcal{C}[n,k]$ is s.t. $\mathbf{H}\mathbf{c}=\mathbf{0}_{r\times 1}$, i.e., any codeword in $\mathcal{C}[n,k]$ has a null syndrome through $\mathbf{H}$. It is also easy to show that a code admitting a systematic form generator matrix will also admit a systematic form parity-check matrix $\mathbf{H}=[\mathbf{V}\mid\mathbf{I}]$, where $\mathbf{V}\in\mathbb{F}_2^{r\times k}$. Note that a parity-check matrix also fully describes a code $\mathcal{C}[n,k]$. We will denote the code admitting $\mathbf{H}$ as a parity-check matrix as $\mathcal{C}(\mathbf{H})$, whenever no ambiguities ensue on the fact that $\mathbf{H}$ is a parity-check matrix.

Quasi-cyclic Sparse Linear Codes. Quasi-cyclic (QC) codes (QCCs) constitute an important category of codes, that is interesting because the generator matrix or the parity-check matrix of its elements can be fully described by a few row vectors. There are two commonplace definitions for what constitutes QCCs, for which we provide a visualization of the structure of a generic generator matrix in Figure 1.

Definition 5 (QCCs - Circulant Tiling of Blocks Generator Matrix (CToB))**.** *A linear code* $\mathcal{C}[n,k]$*, with* $n=pn_0$*,* $k=pk_0$ *(and redundancy* $r=n-k=pr_0$*,* $r_0=n_0-k_0$*) is said to be quasi-cyclic (QC) with basic block* n_0 *if every cyclic shift of a codeword by* n_0



(a) Circulant Tiling of Blocks (CToB)

(b) Tiling of Circulant Blocks (ToCB)

Figure 1: A visualization of the two different definitions of QCCs in terms of CToB (a) and ToCB (b) generator matrices for $p = 2$, $k_0 = 2$ and $n_0 = 3$. Matrix (a) is built by tiling two $k_0 \times n_0$ matrices $\mathbf{A}$, $\mathbf{B}$, in a $p \times p$ circulant pattern. Matrix (b) is built by tiling six $p \times p$ circulant matrices $\mathbf{A}$, $\mathbf{B}$, ..., $\mathbf{F}$ in a $k_0 \times n_0$ pattern.

digits yields another codeword. These codes are described by a Circulant Tiling of Blocks (CToB) generator matrix (Figure 1.a) built as a rank-k matrix split into $p \times p$ blocks. Each block is a $k_0 \times n_0$ binary matrix, and each consecutive row of blocks is obtained performing a circular shift, by one block, of the row of blocks immediately above it.

Definition 6 (QCCs - Tiling of Circulant Blocks Generator Matrix (ToCB))**.** *A linear code $\mathcal{C}[n,k]$, with $n = pn_0$, $k = pk_0$ (and redundancy $r = n-k = pr_0$, $r_0 = n_0 - k_0$) is said to be quasi-cyclic with Tiling of Circulant Blocks (ToCB) generator matrix, if such a matrix is obtained as a tiling of circulant matrices, each one $p \times p$ elements big, on a $k_0 \times n_0$ grid.*

Each code in one of the families of QC codes defined above has a corresponding *permutation equivalent* code in the other family. Furthermore, there exist a one-to-one correspondence between a $p \times p$ circulant matrix and the elements of the polynomial ring $\mathbb{F}_2[x]/(x^p - 1)$. Hinging on such mapping, in the following sections we are going to denote any circulant block $\mathbf{H}_i \in \mathbb{F}_2^{p \times p}$ also as $\mathbf{circ}(\mathtt{h}_i(x))$, where $\mathtt{h}_i(x) = \mathtt{h}_{i,0} + \mathtt{h}_{i,1}x + \mathtt{h}_{i,2}x^2 + \cdots + \mathtt{h}_{i,p-1}x^{p-1} \in \mathbb{F}_2[x]$ is a polynomial having the values of its coefficients in one-to-one correspondence with the binary digits in the first row of $\mathbf{H}_i$, scanning them from left to right. An additional equivalent representation for the circulant matrix or its associated polynomial will be also a binary tuple coinciding with the first row of the matrix or with the sequence of binary coefficient of the polynomial: $(\mathtt{h}_{i,0}, \mathtt{h}_{i,1}, \cdots, \mathtt{h}_{i,p-1})$.

Definition 7 (Binary Regular Codes)**.** *A binary linear code $\mathcal{C}[n,k]$ admitting a (v, w)-regular parity-check matrix, where v and w are the weights of each column and each row, respectively, is defined as (v, w)-regular code, with regularity condition $\frac{n-k}{n} = \frac{v}{w}$.*

It is customary to distinguish between regular Low Density Parity-Check (LDPC) codes when the code admits at least one sparse parity-check matrix with $v \in O(\log(n))$ (Alrabiah et al., 2025), and regular Medium Density Parity-Check (MDPC) codes when the code admits at least one sparse parity-check matrix with $v \in O(\sqrt{n})$ (Tillich, 2018). It is worth noting that left-multiplying a parity-check matrix by a full rank random matrix allows exhibiting another parity-check instance of the same code that possibly does not have low weight columns. Binary LDPC and/or MDPC codes admitting a (v,w)-regular QC $(pr_0) \times (pn_0)$ parity-check matrix are known as QC-LDPC and QC-MDPC codes, respectively. Their distance is upper bounded by $\leq 2v$ (Baldi et al., 2021).

An efficient and effective decoder for LDPC/MDPC codes, given access to the defining sparse parity-check matrix, is the (parallel) bit flipping decoding procedure introduced by Gallager in (Gallager, 1962). Such decoder, employed when $\mathbf{H}$ is sparse, will fail to decode with overwhelming probability as the weight of the columns of $\mathbf{H}$ rises above $O(\sqrt{n})$ (Annechini et al., 2024).

3.2 QC-MDPC based Post-quantum Cryptosystems

The code-based post-quantum cryptosystems BIKE (Aragon et al., 2025) and LEDAcrypt-KEM (Baldi et al., 2025) are based on the template proposed by Niederreiter in (Niederreiter, 1986). The inner workings of both schemes follow the operations of the PKE reported in Figure 2. In particular BIKE can be seen as a special parametrization of the LEDAcrypt-KEM scheme, which fixes the code rate to $\frac{1}{2}$, while still ensuring a prescribed level λ of com-

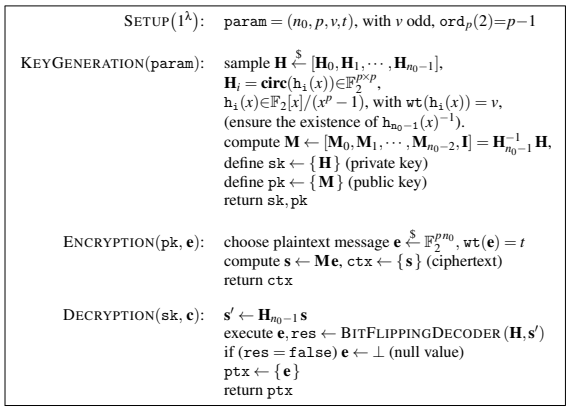


Figure 2: Niederreiter based QC-MDPC PKE scheme matching the BIKE-PKE ($n_0 = 2$) (Aragon et al., 2025; Misoczki et al., 2013), and the PKE in LEDAcrypt-KEM (Baldi et al., 2025; Baldi et al., 2018) ($n_0 \in \{2,3,4\}$).

putational security (typically, $\lambda \in \{128,192,256\}$) as LEDAcrypt-KEM does. Indeed, each of the underlying QC regular codes $\mathcal{C}[n,k]$, $n = pn_0$, $k = p(n_0-1)$, with p a prime number, exhibits a code rate $\frac{k}{n} = \frac{n_0-1}{n_0}$, and a $1\times n_0$ $(p\times p)$-block matrix $\mathbf{H}$ as parity-check matrix, with v (odd) asserted bits in each column (and row) of a circulant block, and $w = n_0 v$ asserted bits in each row of the whole matrix. Being v odd, the constraint that $\mathtt{ord}_p(2)=p-1$ ensures that each circulant block is invertible. Such a condition is important because, $\mathbf{H} = [\mathbf{H}_0,\cdots,\mathbf{H}_{n_0-1}]$ is used as a private key, while the corresponding public key $\mathbf{M}$ is scrambled as per Niederreiter's template, as $\mathbf{M} = \mathbf{H}_{n_0-1}^{-1}\mathbf{H}$, i.e., it is block matrix built as the concatenation of (n_0-1) $p\times p$ random looking blocks and a $p\times p$ identity matrix, i.e., $\mathbf{M} = [\mathbf{M}_0,\cdots,\mathbf{M}_{n_0-2},\mathbf{I}]$.

Being the PKE at hand the inner primitive of a KEM, the binary string defining a plaintext message is identified with a randomly and uniformly chosen error vector $\mathbf{e} \in \mathbb{F}_2^n$ with $\mathtt{wt}(\mathbf{e}) = t$; the ciphertext is obtained as its associated syndrome $\mathbf{s} = \mathbf{M}\mathbf{e}$, which has size p. Given a ciphertext $\mathbf{s}$ and the corresponding public key $\mathbf{M}$, the keypair owner multiplies the last circulant block of her own private key $\mathbf{H}$ by the received syndrome, and obtains a QC-MDPC/QC-LDPC syndrome that can be subsequently fed into the bit-flipping decoder to obtain the original error vector.

The security of the PKE scheme in Fig. 2, and consequently also the one of the PKE schemes adopted by LEDAcrypt-KEM (Baldi et al., 2025) and BIKE (Aragon et al., 2025), depends on the computational hardness of the following problems.

Definition 8 (LEDA Public Key Distinguisher (LEDA-PK-DIST$_{n_0,p,v}(\mathbf{H})$))**.** *Given a $p\times n_0 p$ QC-MDPC parity-check matrix in systematic form, distinguish if it is a uniformly randomly sampled matrix from a QC code in systematic form or a LEDAcrypt-KEM public key, for the same choice of the parameters n_0, p, v.*

Definition 9 (LEDA Message Recovery Attack (LEDA-MRA$_{n_0,p,t}(\mathbf{M},\mathbf{s})$))**.** *Given a LEDAcrypt-KEM public key, i.e., a binary QC-MDPC parity-check matrix $\mathbf{M} \in \mathbb{F}_2^{p\times pn_0}$ in systematic form, and the syndrome $\mathbf{s} = \mathbf{M}\mathbf{e} \in \mathbb{F}_2^p$ of a weight t unknown error vector $\mathbf{e} \in \mathbb{F}_2^{pn_0}$ through $\mathbf{M} \in \mathbb{F}_2^{p\times pn_0}$, compute $\mathbf{e}$.*

Definition 10 (LEDA Key Recovery Attack (LEDA-KRA$_{n_0,p,v}(\mathbf{M})$))**.** *Given a LEDAcrypt-KEM public key, i.e., a binary QC-MDPC parity-check matrix $\mathbf{M} \in \mathbb{F}_2^{p\times pn_0}$ in systematic form, compute the corresponding private key $\mathbf{H} \in \mathbb{F}_2^{p\times pn_0}$, having column and row weight of its n_0 circulant blocks equal to v.*

The hard problems for the BIKE cryptosystem, D-BIKE-PK$_{p,v}$, BIKE-MRA$_{p,t}$, and BIKE-KRA$_{p,v}$, are specializations of D-LEDA-PK$_{n_0,p,v}$, LEDA-MRA$_{n_0,p,t}$, and LEDA-KRA$_{n_0,p,v}$, for $n_0 = 2$.

4 COMPUTATIONAL HARDNESS OF QC-MDPC BASED PKEs

We now provide a systematization of the hard problems underlying QC-MDPC based cryptosystems; a diagram of the computational reductions is provided in Figure 3. In the depicted graph, nodes are computational problems, a D- prefix indicates a decision problem, while a S- prefix a search problem. Our goal is to relate the hardness of the problems constituting a Message Recovery Attack (MRA) or a Key Recovery Attack (KRA) for the LEDAcrypt-KEM and BIKE cryptosystems (blue squares) to the hardness of D-SDP$_{n,k,t}$and D-CFPLE$_{n,k,w}$. In doing so, we prove the computational reductions denoted by blue arrows in Figure 3, and make use of a single hardness assumption (marked by the red arrow tip).

4.1 Hard Problems for QC Codes

In the following, we prove that the problem of decoding a random code and determining its minimum distance, described in the previous section, are NP-complete even when restricted to random QC codes. We start by proving the equivalence of the D-SDP$_{n,k,t}$ to the Decision Quasi-Cyclic Syndrome Decoding Problem, defined as follows:

Definition 11 (Decision Quasi-Cyclic Syndrome Decoding Problem (D-QCSDP$_{n_0,k_0,p,t}(\mathbf{H},\mathbf{s})$))**.** *Given a randomly sampled QC parity-check matrix $\mathbf{H} \in$*

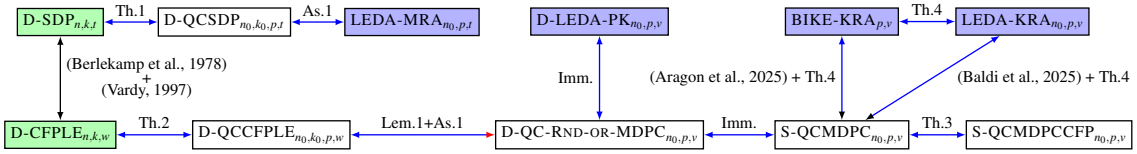


Figure 3: Summary of the relations between computational problems and key or message recovery attacks. Blue arrows denote results in Section 4, red arrows denote security assumptions.

$\mathbb{F}_2^{p(n_0-k_0)\times pn_0}$ *provided as a* $(n_0-k_0)\times n_0$ *tiling of circulant blocks (ToCB), with length* $p>1$ *each, a binary vector* $\mathbf{s}\in\mathbb{F}_2^{pr_0}$*, and an integer* $t>0$*, determine if there is a binary vector* $\mathbf{e}\in\mathbb{F}_2^{pn_0}$*, with* $\mathtt{wt}(\mathbf{e})\leq t$ *s.t.* $\mathbf{s}$ *is the syndrome of* $\mathbf{e}$ *through* $\mathbf{H}$*, i.e.,* $\mathbf{s}=\mathbf{He}$*.*

Theorem 1. D-QCSDP$_{n_0,k_0,p,t}$ *is* NP-complete.

Proof. We prove how an oracle for the D-QCSDP$_{n,k,p,pt}$ can solve the D-SDP$_{n,k,t}$, thus reducing the latter to the former (i.e., D-SDP$_{n,k,t}$ $\leq_p$D-QCSDP$_{n,k,p,pt}$), and then that also an oracle for the D-SDP$_{n_0p,k_0p,pt}$ can solve the D-QCSDP$_{n_0,k_0,p,t}$, that is D-QCSDP$_{n_0,k_0,p,t}$ $\leq_p$D-SDP$_{n_0p,k_0p,pt}$.

Reduction of D-SDP$_{n,k,t}$ **to** D-QCSDP$_{n,k,p,pt}$.

To prove this fact, we employ a procedure which allows to construct efficiently a QC code with a parity-check matrix in ToCB form from a QC code with a parity-check matrix in CToB form and viceversa. We provide an operational description of the procedure, as its correctness is proven in (Baldi, 2014, Lemma 3.4). Let us consider a QC code with a parity-check matrix in CToB form, $\mathbf{H}_{\text{CToB}}$, then we first apply a column permutation which maps the column in position $(i+pj)$, with $j\in\{0,\ldots,n_0-1\}$ and $i\in\{0,\ldots,p-1\}$ to the $(j+n_0i)$-th position. In the following, we will denote with $\mathbf{P}_{\text{col}}$ the $n\times n$ permutation matrix describing the aforementioned column permutation. Subsequently, we apply to the resulting parity-check matrix, a row permutation that maps the row in position $(i+pj)$, with $j\in\{0,\ldots,r_0-1\}$ and $i\in\{0,\ldots,p-1\}$ to the $(j+r_0i)$-th position. In the following, we will denote with $\mathbf{P}_{\text{row}}$ the $r\times r$ permutation matrix describing the aforementioned row permutation. This transformation, which we denote as CToB-to-ToCB$(\cdot)$ produces the parity-check matrix $\mathbf{H}_{\text{ToCB}}=\mathbf{P}_{\text{row}}(\mathbf{H}_{\text{CToB}}\mathbf{P}_{\text{col}})$ describing a code which is *permutation equivalent* to the one described by $\mathbf{H}_{\text{CToB}}$. Indeed, the row permutation applied by CToB-to-ToCB has no effect on the code $\mathcal{C}(\mathbf{H}_{\text{CToB}}\mathbf{P}_{\text{col}})$ represented by $(\mathbf{H}_{\text{CToB}}\mathbf{P}_{\text{col}})$, while the $\mathbf{P}_{\text{col}}$ permutes the coordinates of $\mathcal{C}(\mathbf{H}_{\text{CToB}})$.

The CToB-to-ToCB procedure can be used together with a solver for the D-QCSDP$_{n,k,p,pt}$ where p is a positive integer (denoted as $\mathcal{A}_{\text{D-QCSDP}_{n,k,p,pt}}(\mathbf{H},\mathbf{s})$), to build a polynomial steps solver for D-SDP$_{n,k,t}$ (denoted as $\mathcal{A}_{\text{D-SDP}_{n,k,t}}(\mathbf{H},\mathbf{s})$) as reported in Algorithm 1.

Input: $\mathbf{H}\in\mathbb{F}_2^{r\times n}$ (parity-check matrix), $r=n-k$; $\mathbf{s}\in\mathbb{F}_2^r$ (binary vector)

Output: $b\in\{\mathtt{true},\mathtt{false}\}$: `true` if there is $\mathbf{e}$ s.t. $\mathbf{He}=\mathbf{s}$ and $\mathtt{wt}(\mathbf{e})\leq t$

`// CToB` $\mathbf{H}'$, $p\times p$ `blocks of size` $r\times n$

$$\mathbf{H}'\leftarrow\begin{bmatrix}\mathbf{H} & \mathbf{0}_{r\times n} & \mathbf{0}_{r\times n} & \ldots & \mathbf{0}_{r\times n}\\ \mathbf{0}_{r\times n} & \mathbf{H} & \mathbf{0}_{r\times n} & \ldots & \mathbf{0}_{r\times n}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ \mathbf{0}_{r\times n} & \mathbf{0}_{r\times n} & \mathbf{0}_{r\times n} & \ldots & \mathbf{H}\end{bmatrix}$$

`//` $\mathbf{s}'$ `is a column vector with` p `replicas of` $\mathbf{s}$

$\mathbf{s}'\leftarrow[\mathbf{s}^{\mathrm{T}}\cdots\mathbf{s}^{\mathrm{T}}]^{\mathrm{T}}$

$\mathbf{H}'',\mathbf{P}_{\text{row}}\leftarrow$ CToB-to-ToCB$(\mathbf{H}')$ `//` $\mathbf{H}''=\mathbf{P}_{\text{row}}(\mathbf{H}'\mathbf{P}_{\text{col}})$

$\mathbf{s}''\leftarrow\mathbf{P}_{\text{row}}\mathbf{s}'$

$b\leftarrow\mathcal{A}_{\text{D-QCSDP}_{n,k,p,pt}}(\mathbf{H}'',\mathbf{s}'')$

return b

Algorithm 1: Description of the D-SDP solver for $\mathcal{A}_{\text{D-SDP}_{n,k,t}}(\mathbf{H},\mathbf{s})$, given a solver for $\mathcal{A}_{\text{D-QCSDP}_{n,k,p,pt}}(\mathbf{H}'',\mathbf{s}'')$

The procedure starts by obtaining a CToB parity-check matrix $\mathbf{H}'\in\mathbb{F}^{pr\times pn}, r=n-k$ by placing replicas of $\mathbf{H}$ along the diagonal of the $p\times p$ pattern. Similarly, the procedure obtains a syndrome vector $\mathbf{s}'$ is obtained concatenating p replicas of $\mathbf{s}$ vertically. Note that, if the D-SDP$_{n,k,t}$ instance has positive solution, i.e., an $\mathbf{e}\in\mathbb{F}_2^n$ with $\mathtt{wt}(\mathbf{e})\leq t$ s.t. $\mathbf{He}=\mathbf{s}$ exists, then the D-SDP$_{n,k,t}$ problem instance having parity-check matrix $\mathbf{H}'$ and syndrome $\mathbf{s}'$ admits $\mathbf{e}'=[\mathbf{e}^{\mathrm{T}}\mathbf{e}^{\mathrm{T}}\ldots\mathbf{e}^{\mathrm{T}}]^{\mathrm{T}}$ as a solution, and $\mathtt{wt}(\mathbf{e}')\leq pt$. Furthermore, if D-SDP$_{n,k,t}(\mathbf{H}',\mathbf{s}')$ has a positive solution, there is at least an error vector $\mathbf{e}'=[\mathbf{e}_0^{\mathrm{T}}\mathbf{e}_1^{\mathrm{T}}\ldots\mathbf{e}_{p-1}^{\mathrm{T}}]$, with weight $\leq pt$ which satisfies $\mathbf{s}'=\mathbf{H}'\mathbf{e}'$. This in turn implies that at least one of the vectors $\mathbf{e}_i, i\in\{0,\ldots,p-1\}$ has weight lesser or equal to t (as the sum of their weight is $\leq pt$ and there are p of them). It is also worth noting that the QC-CToB problem instance obtained, while being on a larger code, is still characterized by the same error density $\frac{t}{n}=\frac{pt}{pn}$. The parity-check matrix $\mathbf{H}'$ is then transformed in the one of the permutation equivalent code represented by the result of the CToB-to-ToCB procedure. The syndrome $\mathbf{s}'$ is mapped onto the syndrome $\mathbf{s}''=\mathbf{P}_{\text{row}}\mathbf{s}'$ which, if and only if the original D-SDP$_{n,k,t}$ instance admits a solution, is the syndrome of an error vector $\mathbf{e}''=(\mathbf{e}'^{\mathrm{T}}\mathbf{P}_{\text{col}})^{\mathrm{T}}$. Since the matrix $\mathbf{H}''$ is in ToCB

form, with $p \times p$ sized circulant blocks, it is possible to employ the available $\mathcal{A}_{\text{D-QCSDP}_{n,k,p,t}}$ to solve the decision problem on $(\mathbf{H}'', \mathbf{s}'')$. The decision computed by $\mathcal{A}_{\text{D-QCSDP}_{n,k,p,t}}$ is therefore the same that the procedure solving the D-SDP$_{n,k,t}$ should return.

Reduction of D-QCSDP$_{n_0,k_0,p,t}$ **to** D-SDP$_{n_0 p,k_0 p,pt}$. Given a solver $\mathcal{A}_{\text{D-SDP}}(\mathbf{H}, \mathbf{s})$, and an instance of the D-QCSDP with input $(\mathbf{H}, \mathbf{s})$ to be solved, it suffices to invoke $\mathcal{A}_{\text{D-SDP}}$ on $(\mathbf{H}, \mathbf{s})$. Regardless of the QC structure of $\mathbf{H}$, $\mathcal{A}_{\text{D-SDP}}$ will return the correct answer. □

We now move on to proving the equivalence of the D-CFPLE$_{n,k,w}$ to the Decision Quasi-Cyclic Lesser-or-Equal Codeword Finding Problem, D-QCCFPLE$_{n_0,k_0,p,w}$, defined as follows:

Definition 12 (Decision Quasi-Cyclic Lesser-or-Equal Codeword Finding Problem (D-QCCFPLE$_{n_0,k_0,p,w}(\mathbf{H})$))**.** *Given a randomly sampled QC parity-check matrix* $\mathbf{H} \in \mathbb{F}_2^{p(n_0-k_0)\times pn_0}$ *provided as a tiling of* $(n_0-k_0)\times n_0$ *circulant blocks (ToCB), with length* $p>1$ *each, and an integer* $w > 0$*, determine if there is a binary vector* $\mathbf{e} \in \mathbb{F}_2^{pn_0}$*, with* $0 < \mathtt{wt}(\mathbf{e}) \leq w$ *s.t.* $\mathbf{e}$ *is a codeword, i.e.,* $\mathbf{s} = \mathbf{H}\mathbf{e} = \mathbf{0}$.

Note that D-QCCFPLE$_{n_0,k_0,p,w}$ is equivalent to the problem of computing the minimum distance of a QC code. We now prove the following statement:

Theorem 2. D-QCCFPLE$_{n_0,k_0,p,w}$ *is* NP-complete.

Proof. We exhibit a procedure that with an oracle for D-QCCFPLE$_{n,k,p,w}$ can solve the D-CFPLE$_{n,k,w}$ (i.e. D-CFPLE$_{n,k,w}$ $\leq_p$ D-QCCFPLE$_{n_0,k_0,p,w}$), and then a procedure that with an oracle for the D-CFPLE$_{n,k,w}$ can solve D-QCCFPLE$_{n,k,p,w}$ (i.e. D-QCCFPLE$_{n_0,k_0,p,w}$ $\leq_p$ D-CFPLE$_{n,k,w}$).

Reduction of D-CFPLE$_{n,k,w}$ **to** D-QCCFPLE$_{n,k,p,w}$**.** We use the procedure CToB-to-ToCB$(\cdot)$ described before, to construct efficiently a QC code with a parity-check matrix in ToCB form from a QC code with a parity check matrix in CToB form. The CToB-to-ToCB$(\cdot)$ procedure together with a solver for the D-QCCFPLE$_{n,k,p,w}$, where p is a positive integer, yields a polynomial steps D-CFPLE$_{n,k,w}$ solver.

Following the same structure as Algorithm 1, the procedure starts by constructing a CToB parity-check matrix $\mathbf{H}' \in \mathbb{F}^{pr\times pn}$, placing p replicas of $\mathbf{M}$ along the diagonal of the $p \times p$ pattern, while the remaining blocks are set to $\mathbf{0}_{r\times n}$. Note that, if $\mathcal{C}(\mathbf{H})$ has a codeword $\mathbf{c}$ of weight $\mathtt{wt}(\mathbf{c}) \leq w$, then $\mathbf{H}'$ has p codewords of the form $\mathbf{c}'_i = [\mathbf{0}^{\mathsf{T}}\ \mathbf{0}^{\mathsf{T}}\ \ldots\ \mathbf{c}_i^{\mathsf{T}} \ldots\ \mathbf{0}^{\mathsf{T}}]^{\mathsf{T}}$, $0 \leq i \leq p-1$, where $\mathtt{wt}(\mathbf{c}'_i) \leq w$. Moreover, if $\mathbf{H}'$ admits a codeword $\mathbf{c}' = [\mathbf{c}_0^{\mathsf{T}}\ \mathbf{c}_1^{\mathsf{T}}\ \ldots\ \mathbf{c}_{p-1}^{\mathsf{T}}]^{\mathsf{T}}$ with Hamming weight $\mathtt{wt}(\mathbf{c}) \leq w$, then each $\mathbf{c}_i$ is a (possibly null) codeword of $\mathcal{C}(\mathbf{H})$, i.e., $\mathbf{H}\mathbf{c}_i = \mathbf{0}$, and at least one of such codewords is non null with weight $\leq w$, meaning that also D-CFPLE$_{n,k,w}(\mathbf{H})$ admits a solution. The parity-check matrix $\mathbf{H}'$ is then transformed in the one of the permutation equivalent code represented by the result of the CToB-to-ToCB procedure, $\mathbf{H}''$. Since $\mathcal{C}(\mathbf{H}')$ and $\mathcal{C}(\mathbf{H}'')$ are permutation equivalent, D-CFPLE$_{n,k,w}(\mathbf{H})$ admits a solution if and only if $\mathcal{C}(\mathbf{H}'')$ exhibits a non-zero codeword with weight $\leq w$. The matrix $\mathbf{H}''$ is in ToCB form, thus it is possible to query $\mathcal{A}_{\text{D-QCCFPLE}_{n,k,p,w}}(\mathbf{H}'')$, and the decision computed by $\mathcal{A}_{\text{D-QCCFPLE}_{n,k,p,w}}(\mathbf{H}'')$ is the same that $\mathcal{A}_{\text{D-CFPLE}_{n,k,w}}(\mathbf{H})$ should return.

Reduction of D-QCCFPLE$_{n_0,k_0,p,w}$ **to** D-CFPLE$_{n,k,w}$. Given a solver for D-CFPLE$_{n,k,w}$ and a QC parity-check matrix $\mathbf{H}$ in ToCB form, invoking the solver for D-CFPLE$_{n,k,w}(\mathbf{H})$ will yield the correct answer for D-QCCFPLE$_{n_0,k_0,p,w}(\mathbf{H})$. □

This result implies that computing the minimum distance of a QC code is as hard as computing the minimum distance of a random code.

4.2 Security of QC-MDPC Based PKEs

We now move onto considering computationally hard problems regarding QC-MDPC codes. To this end, we consider codes which admit a $pr_0 \times pn_0$ QC parity-check matrix with $r_0{=}n_0{-}k_0{=}1$, i.e., $\mathbf{H} = [\mathbf{H}_0, \cdots, \mathbf{H}_{n_0-1}]$ where each $\mathbf{H}_i$, $i{\in}\{0, \ldots, n_0{-}1\}$ is a $p \times p$ circulant block. The restriction on r_0 is due to an engineering reason: as we are willing to design a Niederreiter-like cryptosystem, we aim at obtaining a flexible tradeoff between the public key size (i.e., the size of $\mathbf{H}$) and the ciphertext size (i.e., the size of $\mathbf{s}$). We consider the following problem:

Definition 13 (D-QC-Rnd-or-MDPC$_{n_0,p,v}$)**.** *Given an* $p \times pn_0$ *QC parity-check in systematic form* $\mathbf{H} = [\mathbf{H}_0, \cdots, \mathbf{H}_{n_0-2}, \mathbf{I}]$*, decide with probability at least* $1 - \mathsf{negl}(n)$ *if it is obtained:* i) *as a random sample from the uniform distribution over all* $p \times pn_0$ *QC parity-check matrices admitting systematic form, or* ii) *as the systematic form of a regular QC-MDPC parity-check matrix having row weight* $w = n_0 v$*, and column weight* $v \in O(\sqrt{n})$.

The hardness of specific instances of the D-QC-Rnd-or-MDPC$_{n_0,p,v}$ problem is known to depend on the choice of p. Indeed, while there are no known general (w.r.t. the choice of p) solvers faster than $O(2^{cw}), 0 < c \leq 1$, for the case of p having as a factor a power of two, the authors of (Löndahl et al., 2016) have shown that it is possible to reduce the complexity of finding a weight-w codeword of a QC-MDPC code given its parity-check matrix $\mathbf{H}$ in systematic form (and thus solve D-QC-Rnd-or-MDPC$_{n_0,p,v}$) translating it a set of

codeword finding instances for codeword weights and code lengths significantly smaller thant n, w, plus an appropriate polynomial square root extraction algorithm (Löndahl and Johansson, 2014). To avoid these attacks, a popular choice is to take p to be a prime.

In addition to p being a prime, LEDAcrypt-KEM, and BIKE also choose p s.t. 2 generates the multiplicative subgroup of $\mathbb{F}_p$, i.e., $\mathtt{ord}_p(2) = p-1$. The choice is very convenient, as it provides a straightforward way to sample QC codes admitting a systematic form: it is sufficient to pick the side of the block to be p prime and such that 2 generates $\mathbb{F}_p^*$ and choose an odd-weight block except for the one constituted of all ones to obtain an invertible block (Baldi et al., 2017). We note that such a choice also allows us to relate the hardness of D-QC-RND-OR-MDPC$_{n_0,p,v}$ to the one of D-QCCFPLE$_{n_0,k_0,p,w}$, and in particular, that D-QC-RND-OR-MDPC$_{n_0,p,v} \leq_p$ D-QCCFPLE$_{n_0,k_0,p,w}$.

Lemma 1. D-QC-RND-OR-MDPC$_{n_0,p,v} \leq_p$ D-QCCFPLE$_{n_0,k_0,p,w}$

Proof. To prove this, we recall a fact from (Chen et al., 1969), i.e., that a randomly sampled QC code with code rate either $\frac{n_0-1}{n_0}$ or $\frac{1}{n_0}$ and p s.t. $\mathtt{ord}_p(2) = p-1$ achieves the distance described by the so-called Gilbert–Varshamov bound with probability $1-\mathsf{negl}(n)$. This fact implies that, for a constant (in n) rate, the distance of a random QC code is a constant fraction of $\frac{n}{c}$, where c depends on the code rate. By contrast, a QC-MDPC code has a distance which is upper-bounded by $2v \in O(\sqrt{n})$ (Baldi et al., 2021). Therefore, to solve D-QC-RND-OR-MDPC$_{n_0,p,v}(\mathbf{H})$ with probability $1-\mathsf{negl}(n)$ it is sufficient to invoke the solver for D-QCCFPLE$_{n_0,k_0,p,w}(\mathbf{H})$, where $k_0 = n_0-1$ and $w = 2v$, and in case the solver for D-QCCFPLE$_{n_0,k_0,p,w}(\mathbf{H})$ returns an affirmative answer, provide as answer to D-QC-RND-OR-MDPC$_{n_0,p,v}(\mathbf{H})$ that the code is QC-MDPC, and a random QC code otherwise. □

While D-QC-RND-OR-MDPC$_{n_0,p,v}$ can be solved by solving of D-QCCFPLE$_{n_0,k_0,p,w}$ (D-QC-RND-OR-MDPC$_{n_0,p,v} \leq_p$ D-QCCFPLE$_{n_0,k_0,p,w}$), it is not currently known if D-QCCFPLE$_{n_0,k_0,p,w} \leq_p$ D-QC-RND-OR-MDPC$_{n_0,p,v}$, that is, if the problem of distinguishing a QC code with rate $\frac{n_0-1}{n_0}$ admitting a regular MDPC parity check matrix, and minimum distance $\leq 2v$, from a random QC code is at least as hard as the problem of distinguishing whether a QC code has minimum distance $\leq w$ or not. If D-QCCFPLE$_{n_0,k_0,p,w} \leq_p$ D-QC-RND-OR-MDPC$_{n_0,p,v}$ were to hold, the computational problems would be equally difficult and therefore the problem D-QC-RND-OR-MDPC$_{n_0,p,v}$ would be NP-complete itself. We observe that the computational intractability of breaking a generic instance of both LEDAcrypt-KEM and BIKE, either by message or private key recovery, can be shown to depend on the following assumption alone.

Assumption 1. D-QC-RND-OR-MDPC$_{n_0,p,v}$ *is* NP-complete.

Given the said assumption, it is indeed immediate to observe that solving the problem D-LEDA-PK$_{n_0,p,v}(\mathbf{H})$ of deciding if a QC parity-check matrix $\mathbf{H}$ is a public key of the LEDAcrypt-KEM cryptosystem or a randomly sampled QC parity-check matrix in systematic form is indeed an instance of the problem D-QC-RND-OR-MDPC$_{n_0,p,v}$. Assuming that D-LEDA-PK$_{n_0,p,v}$ is computationally intractable also leads to the intractability of LEDA-MRA$_{n_0,p,t}$, as the attacker will be required to solve a D-QCSDP$_{n_0,k_0,p,t}$ instance, since he will not be able to distinguish LEDAcrypt-KEM public keys from random QC parity-check matrices admitting systematic form.

The problem D-QC-RND-OR-MDPC$_{n_0,p,v}(\mathbf{H})$ being NP-complete implies that the corresponding search problem, defined as follows, is NP-hard:

Definition 14 (S-QCMDPC$_{n_0,p,v}(\mathbf{M})$)**.** *Given a $p \times n_0 p$ QC parity-check matrix in systematic form, i.e., $\mathbf{M} = [\mathbf{M}_0, \mathbf{M}_1, \ldots, \mathbf{M}_{n_0-2}, \mathbf{I}]$, find the $(v, n_0 v)$-regular, $p \times n_0 p$ QC-MDPC matrix $\mathbf{H}$ such that $\mathbf{M}$ is the systematic form of $\mathbf{H}$.*

Under the same assumption, the decision problem D-QC-RND-OR-MDPC$_{n_0,p,v}$ has the same computational complexity as the corresponding search problem, as all NP-complete problems enjoy a search-to-decision reduction (Arora and Barak, 2009).

We now show that S-QCMDPC$_{n_0,p,v}(\mathbf{M})$ i.e., finding the definitory low weight parity-check matrix defining the same code $\mathcal{C}(\mathbf{M})$, is equivalent to finding low-weight codewords in $\mathcal{C}(\mathbf{M})$ itself. We start by defining the codeword finding problem as follows:

Definition 15 (S-QCMDPCCFP$_{n_0,p,v}(\mathbf{M})$)**.** *Given a $p \times pn_0$ QC-MDPC parity-check matrix $\mathbf{M}$ in systematic form, find a vector $\mathbf{e} \in \mathbb{F}_2^{n_0 p}$ such that $\mathbf{s} = \mathbf{M}\mathbf{e} = \mathbf{0}$ (i.e., $\mathbf{e}$ is a codeword of $\mathcal{C}(\mathbf{M})$) with $\mathtt{wt}(\mathbf{c}) = 2v$.*

Theorem 3. S-QCMDPC$_{n_0,p,v} =_P$ S-QCMDPCCFP$_{n_0,p,v}$

Proof. We now show how an oracle for S-QCMDPCCFP$_{n_0,p,v}$ can solve S-QCMDPC$_{n_0,p,v}$, and how an oracle for S-QCMDPC$_{n_0,p,v}$ can solve the S-QCMDPCCFP$_{n_0,p,v}$.

Reduction of S-QCMDPC$_{n_0,p,v}$ **to** S-QCMDPCCFP$_{n_0,p,v}$ Solving S-QCMDPC$_{n_0,p,v}$ amounts to deriving a $(v, n_0 v)$-regular QC-MDPC matrix

$\mathbf{H} = [\mathbf{H}_0, \mathbf{H}_1, \ldots \mathbf{H}_{n_0-1}]$, given a $p \times pn_0$ QC-MDPC code parity-check matrix in systematic form $\mathbf{M} = [\mathbf{M}_0, \mathbf{M}_1, \ldots, \mathbf{M}_{n_0-2}, \mathbf{I}]$. To do so, consider the code described by puncturing (i.e., removing coordinates from) $\mathcal{C}(\mathbf{M})$, to obtain a code $\mathcal{C}(\mathbf{M}'_i)$ described by $\mathbf{M}'_i = [\mathbf{M}_i, \mathbf{I}], i \in \{0, \ldots, n_0-2\}$. Repeat the following procedure for each value $i \in \{0, \ldots, n_0-2\}$.

Consider that $\mathcal{C}(\mathbf{M}'_i)$ is, by construction, a $2, p, v$ QC-MDPC code: indeed, $\mathbf{M}'_i$ is the systematic form of the QC-MDPC matrix $\mathbf{H}'_i = [\mathbf{H}_i, \mathbf{H}_{n_0-1}]$. Consequently, $\mathcal{C}(\mathbf{M}'_i)$ is also described by the generator matrix $\mathbf{G}'_i = [\mathbf{H}^{\mathsf{T}}_{n_0-1}, \mathbf{H}^{\mathsf{T}}_i]$, where each row (i.e., codeword) of $\mathbf{G}'_i$ has weight $2v$. Computing the parity-check matrix $\mathbf{H}'_i$ thus amounts to deriving a $(v, 2v)$-regular QC generator matrix $\mathbf{G}'_i$ of $\mathcal{C}(\mathbf{M}'_i)$. To do so, start by invoking S-QCMDPCCFP$_{n_0,p,v}(\mathbf{M}'_i)$ and get $\mathbf{c}_i = [\mathbf{c}^{\mathsf{T}}_{i,0} \ \mathbf{c}^{\mathsf{T}}_{i,1}]^{\mathsf{T}}$, where $\mathbf{c}_{i,0}, \mathbf{c}_{i,1} \in \mathbb{F}_2^p$ and $\mathtt{wt}(\mathbf{c}_{i,0}) = \mathtt{wt}(\mathbf{c}_{i,1}) = v$. Since $\mathbf{c}_i$ is a codeword of $\mathcal{C}(\mathbf{M}'_i) = \mathcal{C}(\mathbf{H}'_i)$, and $\mathcal{C}(\mathbf{H}'_i)$ is a QC-MDPC code in ToCB form, also the p block-wise circular shifts of $\mathbf{c}_i$ will be codewords of $\mathcal{C}(\mathbf{H}'_i)$. The matrix obtained as $\mathbf{G}'_i = [\mathbf{circ}(\mathbf{c}_{i,0}), \mathbf{circ}(\mathbf{c}_{i,1})]$ is thus a generator matrix for $\mathcal{C}(\mathbf{H}'_i)$, meaning that $\mathbf{H}'_i$ can be computed as $\mathbf{H}'_i = [\mathbf{circ}(\mathbf{c}_{i,1})^{\mathsf{T}}, \mathbf{circ}(\mathbf{c}_{i,0})^{\mathsf{T}}]$. This implies that $\mathbf{H}_i = \mathbf{circ}(\mathbf{c}_{i,1})^{\mathsf{T}}$, and $\mathbf{H}_{n_0-1} = \mathbf{circ}(\mathbf{c}_{i,0})^{\mathsf{T}}$.

Repeating the computation for each value of $i \in \{0, \ldots, n_0-2\}$, observe that the value $\mathbf{H}_{n_0-1}$ returned at each computation is the same (up to a cyclic shift, which we will discuss later), while the values $\mathbf{H}_i$ correspond to the missing $p \times p$ circulant blocks of $\mathbf{H}$. Computing $\mathbf{H} = [\mathbf{H}_0, \ldots, \mathbf{H}_{n_0-1}]$ thus solves S-QCMDPC$_{n_0,p,v}(\mathbf{M})$.

As a final note, the weight-$2v$ codewords $\mathbf{c}'_i, \mathbf{c}'_j$ returned by S-QCMDPCCFP$_{n_0,p,v}(\mathbf{M}'_i)$ and S-QCMDPCCFP$_{n_0,p,v}(\mathbf{M}'_j)$, $i, j \in \{0, \ldots, n_0-2\}$, $i \neq j$, may have $\mathbf{c}'_{i,0} \neq \mathbf{c}'_{j,0}$, with $\mathbf{c}'_{j,0}$ being a cyclic shift of $\mathbf{c}'_{i,0}$. To account for this fact, it is sufficient to perform block-wise cyclic shifts on $\mathbf{c}'_0$ (i.e., the result of S-QCMDPCCFP$_{n_0,p,v}(\mathbf{M}'_0)$) until the systematic form of the resulting matrix $\mathbf{H}'_0$ matches $\mathbf{M}'_0$, and then to perform block-wise cyclic shifts on each $\mathbf{c}'_j$, $j \in \{1, \ldots, n_0-2\}$ until $\mathbf{c}'_{j,0} = \mathbf{c}'_{0,0}$. All these steps can be performed in polynomial time, therefore S-QCMDPC$_{n_0,p,v} \leq_P$ S-QCMDPCCFP$_{n_0,p,v}$.

Reduction of S-QCMDPCCFP$_{n_0,p,v}$ **to** S-QCMDPC$_{n_0,p,v}$ This reduction amounts to the fact that, given a QC-MDPC matrix $\mathbf{H} = [\mathbf{H}_0, \mathbf{H}_1, \ldots, \mathbf{H}_{n_0-1}]$, the code $\mathcal{C}(\mathbf{H})$ admits the following generator matrix $\mathbf{G}$, where each row (which is also a codeword of $\mathcal{C}(\mathbf{G})$) has Hamming weight $2v$:

$$\mathbf{G} = \begin{bmatrix} \mathbf{H}^{\mathsf{T}}_{n_0-1} & \mathbf{0}_{p\times p} & \cdots & \mathbf{0}_{p\times p} & \mathbf{H}^{\mathsf{T}}_0 \\ \mathbf{0}_{p\times p} & \mathbf{H}^{\mathsf{T}}_{n_0-1} & \cdots & \mathbf{0}_{p\times p} & \mathbf{H}^{\mathsf{T}}_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0}_{p\times p} & \mathbf{0}_{p\times p} & \cdots & \mathbf{H}^{\mathsf{T}}_{n_0-1} & \mathbf{H}^{\mathsf{T}}_{n_0-2} \end{bmatrix}$$

To solve S-QCMDPCCFP$_{n_0,p,v}(\mathbf{M})$, it is sufficient invoke the solver for S-QCMDPC$_{n_0,p,v}(\mathbf{M})$ that computes the QC-MDPC matrix $\mathbf{H}$, and then return as solution to S-QCMDPCCFP$_{n_0,p,v}(\mathbf{M})$ one of the weight-$2v$ codewords in the corresponding generator matrix $\mathbf{G}$. □

BIKE authors (Aragon et al., 2025) relate the key recovery attack (BIKE-KRA$_{p,v}$) to specific instances of S-QCMDPCCFP$_{n_0,p,v}(\mathbf{H})$ with $n_0 = 2$, while the key recovery attack against an instance of LEDAcrypt-KEM (LEDA-KRA$_{n_0,p,v}$) corresponds to solving an instance of S-QCMDPCCFP$_{n_0,p,v}(\mathbf{H})$ with $n_0 \in \{2,3,4\}$ (Baldi et al., 2025) No proof exists on whether the codeword finding problem (i.e., S-QCMDPCCFP$_{n_0,p,v}$), or the key recovery attack (i.e., S-QCMDPC$_{n_0,p,v}$, that by Theorem 3 is $=_P$ S-QCMDPCCFP$_{n_0,p,v}$), is equivalently hard for any fixed rate $\frac{n_0-1}{n_0}$. We now prove the aforementioned fact, systematizing the relation between S-QCMDPCCFP$_{n_0,p,v}$, S-QCMDPC$_{n_0,p,v}$, BIKE-KRA$_{p,v}$ and LEDA-KRA$_{n_0,p,v}$, by showing their equivalence.

Theorem 4. S-QCMDPC$_{n_0,p,v} =_P$ S-QCMDPC$_{\overline{n_0},p,v}$ *for any fixed* $\overline{n_0} \geq 2$.

Proof. We begin by noting that S-QCMDPC$_{\overline{n_0},p,v} \leq_P$ S-QCMDPC$_{n_0,p,v}$, since S-QCMDPC$_{\overline{n_0},p,v}$ is a particular instance of S-QCMDPC$_{n_0,p,v}$. To prove that S-QCMDPC$_{n_0,p,v} \leq_P$ S-QCMDPC$_{\overline{n_0},p,v}$, we show that S-QCMDPC$_{n_0,p,v} \leq_P$ S-QCMDPC$_{2,p,v}$ and S-QCMDPC$_{2,p,v} \leq_P$ S-QCMDPC$_{\overline{n_0},p,v}$ for any fixed $\overline{n_0} \geq 2$.

Reduction of S-QCMDPC$_{n_0,p,v}$ **to** S-QCMDPC$_{2,p,v}$**.** Solving S-QCMDPC$_{n_0,p,v}$ amounts to deriving a $(v, n_0 v)$-regular QC-MDPC matrix $\mathbf{H} = [\mathbf{H}_0, \mathbf{H}_1, \ldots \mathbf{H}_{n_0-1}]$, given a $p \times pn_0$ QC-MDPC code parity-check matrix in systematic form $\mathbf{M} = [\mathbf{M}_0, \mathbf{M}_1, \ldots, \mathbf{M}_{n_0-2}, \mathbf{I}]$. To do so, consider the code described by puncturing $\mathcal{C}(\mathbf{M})$, to obtain a code $\mathcal{C}(\mathbf{M}'_i)$ described by $\mathbf{M}'_i = [\mathbf{M}_i, \mathbf{I}], i \in \{0, \ldots, n_0-2\}$. $\mathcal{C}(\mathbf{M}'_i)$ is a $2, p, v$ QC-MDPC code, as $\mathbf{M}'_i$ is the systematic form of the QC-MDPC matrix $\mathbf{H}'_i = [\mathbf{H}_i, \mathbf{H}_{n_0-1}]$. Invoking S-QCMDPC$_{2,p,v}(\mathbf{M}'_i)$ will therefore yield the QC-MDPC matrix $\mathbf{H}'_i$, which can be used to retrieve two blocks of the target QC-MDPC parity-check matrix $\mathbf{H} = [\mathbf{H}_0, \mathbf{H}_1, \ldots \mathbf{H}_{n_0-1}]$, namely, $\mathbf{H}_i$ and $\mathbf{H}_{n_0-1}$. Performing $n_0 - 1$ calls to

Input: $\mathbf{M} \in \mathbb{F}_2^{p \times n_0 p}$ parity-check matrix in systematic form
Output: $\mathbf{H} \in \mathbb{F}_2^{p \times n_0 p}$ $(v, n_0 v)$-regular QC-MDPC parity-check matrix such that $\mathbf{M}$ is the systematic form of $\mathbf{H}$.

$i \leftarrow 0$
while $i \leq n_0 - 2$ **do**
  $\overline{\mathbf{M}}_i \leftarrow [\mathbf{M}_i, \mathbf{I}, \ldots, \mathbf{I}]$
  $\overline{\mathbf{H}}_i \leftarrow \mathcal{A}_{\text{S-QCMDPC}_{\overline{n_0},p,v}}(\overline{\mathbf{M}}_i)$
    // $\overline{\mathbf{H}}_i = [\overline{\mathbf{H}}_{i,0}, \overline{\mathbf{H}}_{i,1}, \ldots, \overline{\mathbf{H}}_{i,\overline{n_0}-1}]$
  $\mathbf{H}_i \leftarrow \overline{\mathbf{H}}_{i,0}$
  $\mathbf{H}_{n_0-1} \leftarrow \overline{\mathbf{H}}_{i,1}$
  $i \leftarrow i+1$
end
$\mathbf{H} \leftarrow [\mathbf{H}_0, \ldots, \mathbf{H}_{n_0-1}]$
return H

Algorithm 2: Description of the S-QCMDPC solver $\mathcal{A}_{\text{S-QCMDPC}_{n_0,p,v}}(\mathbf{M})$, given a solver for $\mathcal{A}_{\text{S-QCMDPC}_{\overline{n_0},p,v}}(\overline{\mathbf{M}})$ (with fixed $\overline{n_0} \geq 2$).

S-QCMDPC$_{2,p,v}(\mathbf{M}'_i)$, for $i \in \{0, \ldots, n_0 - 2\}$ is sufficient to compute all the circulant blocks of $\mathbf{H}$, solving S-QCMDPC$_{n_0,p,v}$.

Reduction of S-QCMDPC$_{2,p,v}$ **to** S-QCMDPC$_{\overline{n_0},p,v}$**.** Solving S-QCMDPC$_{2,p,v}$ amounts to deriving a $(v, 2v)$-regular QC-MDPC matrix $\mathbf{H} = [\mathbf{H}_0, \mathbf{H}_1]$, given a $p \times 2p$ QC-MDPC code parity-check matrix in systematic form $\mathbf{M} = [\mathbf{M}_0, \mathbf{I}]$.

If $\overline{n_0} = 2$, then the two problems coincide. For $\overline{n_0} > 2$, consider the augmented $p \times \overline{n_0} p$ parity-check matrix $\overline{\mathbf{M}} = [\mathbf{M}_0, \mathbf{I}, \mathbf{I}, \ldots, \mathbf{I}]$. $\overline{\mathbf{M}}$ describes a QC-MDPC code, admitting as parity-check matrix $\overline{\mathbf{H}} = [\mathbf{H}_0, \mathbf{H}_1, \mathbf{H}_1, \ldots, \mathbf{H}_1]$. To solve S-QCMDPC$_{2,p,v}(\mathbf{M})$, it is sufficient to invoke the solver for S-QCMDPC$_{\overline{n_0},p,v}(\overline{\mathbf{M}})$ and retaining the first two circulant blocks of the result (i.e., the first two circulant blocks of $\overline{\mathbf{H}}$).

Reduction of S-QCMDPC$_{n_0,p,v}$ **to** S-QCMDPC$_{\overline{n_0},p,v}$**.** A naïve solver for S-QCMDPC$_{n_0,p,v}$ given a solver for S-QCMDPC$_{\overline{n_0},p,v}$ (with $\overline{n_0} \geq 2$ fixed) is shown in Algorithm 2. The S-QCMDPC$_{n_0,p,v}(\mathbf{M})$ instance can be solved with $n_0 - 1$ calls to $\mathcal{A}_{\text{S-QCMDPC}_{\overline{n_0},p,v}}(\overline{\mathbf{M}_i})$, $i \in \{0, \ldots, n_0 - 2\}$, each computing the circulant blocks $\mathbf{H}_i$ and $\mathbf{H}_{n_0-1}$ composing the solution $\mathbf{H}$=$[\mathbf{H}_0, \ldots, \mathbf{H}_{n_0-1}]$. □

Since BIKE-KRA$_{p,v}$ coincides with S-QCMDPC$_{2,p,v}$, and LEDA-KRA$_{n_0,p,v}$ coincides with S-QCMDPC$_{\overline{n_0},p,v}$ for $\overline{n_0} \in \{2,3,4\}$, a direct consequence of Theorem 4 is that BIKE-KRA$_{p,v} =_P$ LEDA-KRA$_{n_0,p,v}$.

5 CONCLUSION

Quasi-Cyclic codes employed in post-quantum cryptosystem offer desirable performances and security guarantees, as the complexity of attacking such cryptosystems is related to well-established hard problems in coding theory. In this work, we prove that decoding random QC codes and computing the minimum distance of a random QC code are NP-complete problems, providing strong evidence that quasi-cyclicity does not damage security. We provide a systematization of the hard problem underlying the Niederreiter-style QC-MDPC based cryptosystems BIKE (Aragon et al., 2025) and LEDAcrypt-KEM (Baldi et al., 2025), highlighting the single hardness assumption on which they rely. Finally, we prove that the security of BIKE and LEDAcrypt-KEM is equivalent, showing that the rate of the QC-MDPC codes employed in the cryptosystems does not change the nature of the underlying hard problem. This contribution also allows to pick any $\frac{n_0-1}{n_0}$ rate for QC-MDPC codes in a Niederreiter design , enabling tradeoffs between public key and ciphertext size which are crucial in practical scenarios such as, e.g., the Wireguard VPN protocol (Lafourcade et al., 2025) where the ciphertexts should be fitting into a single packed data unit due to lack of fragmentation support.

REFERENCES

Albrecht, M. R., Bernstein, D. J., Chou, T., Cid, C., Gilcher, J., Lange, T., Maram, V., von Maurich, I., Misoczki, R., Niederhagen, R., Paterson, K. G., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Tjhai, C. J., Tomlinson, M., and Wang, W. (2022). Classic McEliece. https://csrc.nist.gov/projects/post-quantumcryptography/round-4-submissions.

Alekhnovich, M. (2003). More on Average Case vs Approximation Complexity. In *44th Symposium on Foundations of Computer Science (FOCS 2003), 11-14 October 2003, Cambridge, MA, USA, Proceedings*, pages 298–307. IEEE Computer Society.

Alrabiah, O., Ananth, P., Christ, M., Dodis, Y., and Gunn, S. (2025). Ideal pseudorandom codes. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025*, pages 1638–1647. ACM.

Annechini, A., Barenghi, A., and Pelosi, G. (2024). Bit-Flipping Decoder Failure Rate Estimation for (v, w)-Regular Codes. In *IEEE International Symposium on Information Theory, ISIT 2024, Athens, Greece, July 7-12, 2024*, pages 3374–3379. IEEE.

Apon, D., Perlner, R. A., Robinson, A., and Santini, P. (2020). Cryptanalysis of ledacrypt. In *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*, volume 12172 of *Lecture Notes in Computer Science*, pages 389–418. Springer.

Aragon, N., Barreto, P. S. L. M., Bettaieb, S., Bidoux,

L., Blazy, O., Deneuville, J.-C., Gaborit, P., Ghosh, S., Gueron, S., Güneysu, T., Melchor, C. A., Misoczki, R., Persichetti, E., Richter-Brockmann, J., Sendrier, N., Tillich, J.-P., Vasseur, V., and Zémor, G. (2025). BIKE: Bit Flipping Key Encapsulation. Round 4 Submission - Version 5.2 - 10/10/2024. [Online] Available: https://bikesuite.org/files/v5.2/BIKE_Spec.2024.10.10.1.pdf.

Arora, S. and Barak, B. (2009). Computational complexity - A modern approach.

Baldi, M. (2014). *QC-LDPC Code-Based Cryptography*. Springer Briefs in Electrical and Computer Engineering. Springer.

Baldi, M., Barenghi, A., Chiaraluce, F., Pelosi, G., and Santini, P. (2017). LEDAcrypt-KEM submission bundle. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/LEDAkem.zip.

Baldi, M., Barenghi, A., Chiaraluce, F., Pelosi, G., and Santini, P. (2018). LEDAkem: A Post-quantum Key Encapsulation Mechanism Based on QC-LDPC Codes. In *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, volume 10786 of *Lecture Notes in Computer Science*, pages 3–24. Springer.

Baldi, M., Barenghi, A., Chiaraluce, F., Pelosi, G., and Santini, P. (2021). Performance Bounds for QC-MDPC Codes Decoders. In *9th International Workshop, CBCrypto 2021, Munich, Germany, June 21-22,*, volume 13150 of *Lecture Notes in Computer Science*, pages 95–122. Springer.

Baldi, M., Barenghi, A., Chiaraluce, F., Pelosi, G., and Santini, P. (2025). LEDAcrypt - version 3.0 Specification (2020). [Online] Available: https://www.ledacrypt.org/documents/LEDAcrypt_v3.pdf.

Baldi, M., Bodrato, M., and Chiaraluce, F. (2008). A New Analysis of the McEliece Cryptosystem Based on QC-LDPC Codes. In *Security and Cryptography for Networks, 6th International Conference, SCN 2008, Amalfi, Italy, September 10-12, 2008. Proceedings*, volume 5229 of *Lecture Notes in Computer Science*, pages 246–262. Springer.

Berger, T. P., Cayrel, P., Gaborit, P., and Otmani, A. (2009). Reducing Key Length of the McEliece Cryptosystem. In *AFRICACRYPT 2009, Second International Conference on Cryptology in Africa, Gammarth, Tunisia, June 21-25, 2009. Proceedings*, volume 5580 of *Lecture Notes in Computer Science*, pages 77–97. Springer.

Berlekamp, E. R., McEliece, R. J., and van Tilborg, H. C. A. (1978). On the inherent intractability of certain coding problems (Corresp.). *IEEE Trans. Inf. Theory*, 24(3):384–386.

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., and Stehle, D. (2018). CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367.

Chen, C. L., Peterson, W. W., and Weldon Jr., E. J. (1969). Some Results on Quasi-Cyclic Codes. *Inf. Control.*, 15(5):407–423.

Gallager, R. G. (1962). Low-density parity-check codes. *IRE Trans. Inf. Theory*, 8(1):21–28.

Kevin M. Stine (2024). FIPS 2023 Federal Information Processing Standards Publication - Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). https://doi.org/10.6028/NIST.FIPS.203. U.S. National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, USA.

Lafourcade, P., Mahmoud, D., Ruhault, S., and Taleb, A. R. (2025). A Tale of Two Worlds, a Formal Story of WireGuard Hybridization. *IACR Cryptol. ePrint Arch.*, page 1179.

Li, Y. X., Deng, R. H., and Wang, X. M. (2006). On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Trans. Inf. Theor.*, 40(1):271–273.

Löndahl, C. and Johansson, T. (2014). Improved algorithms for finding low-weight polynomial multiples in $\mathbb{F}_2[x]$ and some cryptographic applications. *Des. Codes Cryptogr.*, 73(2):625–640.

Löndahl, C., Johansson, T., Shooshtari, M. K., Ahmadian-Attari, M., and Aref, M. R. (2016). Squaring attacks on McEliece public-key cryptosystems using quasi-cyclic codes of even dimension. *Des. Codes Cryptogr.*, 80(2):359–377.

McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. *Deep Space Network Progress Report 42-44*, pages 114–116.

Melchor, C. A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Bos, J., Deneuville, J.-C., Dion, A., Gaborit, P., Lacan, J., Persichetti, E., Robert, J.-M., Véron, P., and Zémor, G. (2025). Hamming Quasi-Cyclic (HQC) - Fourth round version. https://pqc-hqc.org/doc/hqc-specification_2024-02-23.pdf.

Melchor, C. A., Blazy, O., Deneuville, J., Gaborit, P., and Zémor, G. (2018). Efficient Encryption From Random Quasi-Cyclic Codes. *IEEE Trans. Inf. Theory*, 64(5):3927–3943.

Misoczki, R., Tillich, J., Sendrier, N., and Barreto, P. S. L. M. (2012). MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes. *IACR Cryptol. ePrint Arch.*, page 409.

Misoczki, R., Tillich, J., Sendrier, N., and Barreto, P. S. L. M. (2013). MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. In *Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013*, pages 2069–2073. IEEE.

Monico, C., Rosenthal, J., and Shokrollahi, A. (2000). Using low density parity check codes in the McEliece cryptosystem. In *IEEE International Symposium on Information Theory*, volume -, page 215. IEEE.

Niederreiter, H. (1986). Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15:159–166.

Sidelnikov, V. and Shestakov, S. (1992). On insecurity

of cryptosystems based on generalized Reed-Solomon codes. *Discrete Math. and Appl.*, 2:439–444.

Tillich, J. (2018). The Decoding Failure Probability of MDPC Codes. In *2018 IEEE International Symposium on Information Theory, ISIT 2018, Vail, CO, USA, June 17-22, 2018*, pages 941–945. IEEE.

Vardy, A. (1997). The intractability of computing the minimum distance of a code. *IEEE Trans. Inf. Theory*, 43(6):1757–1766.