Reproducible Codes and Cryptographic Applications

Paolo Santini[1], Edoardo Persichetti[2] and Marco Baldi[1]

[1]Università Politecnica delle Marche, [2]Florida Atlantic University

Abstract. In this paper we study structured linear block codes, starting from well known examples and generalizing them to a wide class of codes that we call *reproducible codes*. These codes have the property that they can be entirely generated from a small number of signature vectors, and consequently admit matrices that can be described in a very compact way. We then show some cryptographic applications of this class of codes and explain why the general framework we introduce may pave the way for future developments of code-based cryptography.

Keywords: Linear block codes, code-based cryptography, post-quantum cryptography, reproducible codes

1 Introduction

Defining linear block codes that possess a certain inner structure and verify some regularity properties is a natural process in coding theory. Arguably, the most relevant example is represented by the class of *cyclic codes*, which includes several families of codes that proved to be important throughout the history of communications, such as BCH and Hamming codes, as well as the binary Golay codes, Reed-Solomon codes and many others. This class is defined by the property of having codewords that are invariant under the action of a specific permutation, namely the cyclic (circular) shift, i.e. the rotation of the vector to the right (equivalently, to the left). Other examples which are well-known in literature include *constacyclic* codes, *negacyclic* codes, *quasi-cyclic* codes and many others.

In recent times, this research direction has been investigated further: Misoczki and Barreto in 2009 introduced the family of *quasi-dyadic* codes [1], which contain codewords that are invariant under a different type of permutation. The work was motivated by its applications in the framework of the McEliece cryptosystem [2], and in particular by the necessity of having a family of codes which possess generator and parity-check matrices that can be represented in a compact way. The reason behind this is that, in code-based cryptography, the public key of an encryption (or signature) scheme usually consists precisely of a generator or parity-check matrix of a linear block code. With the size of the codes used in code-based cryptography (typical code length values are in the order of 10^3 to 10^4), describing a whole matrix results in a public key of several kilobytes, and this size increases quadratically in the code length. This has historically prevented the use of the original McEliece cryptosystem [2], which exploits random-looking public codes, in many applications. On the other hand, structured codes admit a generator and parity-check matrix which can be entirely described by one or few rows; this allows for a very important reduction in public-key size, and it is arguably a fundamental step towards making code-based cryptography truly practical. Previous efforts to reduce key size were centered on quasi-cyclic algebraic codes [3] and have been since then extended to codes of a different nature, namely the Low-Density Parity-Check (LDPC) codes and their recent generalization, Moderate-Density Parity-Check (MDPC). These codes are characterized by very sparse parity-check matrices with constant, low-weight rows, and trivially admit matrices in quasi-cyclic form, i.e. formed by circulant square blocks. Due to their efficient decoding algorithm and the lack of additional algebraic structure which could lead to structural attacks, schemes based on QC-LDPC codes [4] and QC-MDPC codes [5] are among the most promising solution in the area.

The importance of code-based cryptography has risen dramatically in modern times due to the work of Peter Shor [6], which shows how it will be possible to effectively break cryptography based on "classical" number theory problems by introducing polynomial-time algorithms for factoring and computing discrete logarithms on a quantum computer. This means that the cryptographic community has to devise primitives which rely on different hard problems, which will not be affected once quantum computers of an appropriate size will be available. Code-based cryptography is one of the most important areas in this scenario, and ever since McEliece's seminal work in 1978, has shown no vulnerabilities against quantum attackers. Together with schemes based on lattice problems, code-based cryptography represented the lion's share among all candidates for the Post-Quantum Standardization call recently launched by NIST [7].

Our Contribution In this paper we analyze in detail the nature of structured codes. First, we introduce the notion of *reproducible* codes, which captures the generic idea of a code admitting characteristic matrices that can be entirely described by a subset of their rows. To the best of our knowledge, it is the first time such a broad concept is introduced and studied in its entirety. We then show that all the existing constructions of structured codes (cyclic, quasi-cyclic, dyadic etc.) are in fact but a special case of our general formulation – in particular, corresponding to the simplest case where the codes are "reproduced" via a permutation. Finally, we propose a framework for constructing reproducible codes of any kind, and present concrete instantiations of non-trivial reproducible codes which have not appeared in literature before.

2 Preliminaries

We denote with $\mathbb{F}_q$ the finite field with q elements, where q is a prime power. For two sets X and Y we denote by X^Y the set of all functions from X to Y. For a set S we then denote by 2^S its power set, exploiting the well-known bijection between the power set of S and the set of functions from S to $\{0, 1\}$. We use bold letters to denote vectors and matrices. Given a vector $\mathbf{a}$, we refer to its element in position i as a_i. The size-k identity matrix is denoted as $\mathbf{I}_k$, while the $k \times n$ null matrix is denoted as $\mathbf{0}_{k\times n}$.

2.1 Coding Theory

A linear code $\mathcal{C}$ is a k-dimensional subspace of the n-dimensional vector space over the finite field $\mathbb{F}_q$. The parameters n (*length*) and k (*dimension*) are positive integers with $k \leq n$. The value $r = n - k$ is known as *codimension* of the code.

Definition 1 (Hamming metric). *The Hamming weight $\mathsf{wt}(\mathbf{x})$ of a vector $\mathbf{x} \in \mathbb{F}_q^n$ is the number of its non-zero entries. The Hamming distance $\mathsf{d}(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ is defined as the weight of their difference, i.e. $\mathsf{d}(\mathbf{x}, \mathbf{y}) = \mathsf{wt}(\mathbf{x} - \mathbf{y})$. The minimum distance d of a code $\mathcal{C}$ is defined as the minimum distance between any two different codewords of $\mathcal{C}$, or equivalently as the minimum weight over all non-zero codewords.*

A linear code of length n, dimension k, and minimum distance d is called an $[n, k, d]$-code.

The error-correcting capability of a linear code is connected to its minimum distance, and in particular it corresponds to $\lfloor (d - 1)/2 \rfloor$.

Definition 2 (Generator and Parity Check Matrices). *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. We call* generator matrix *of $\mathcal{C}$ a $k \times n$ matrix $\mathbf{G}$ whose rows form a basis for the vector space defined by $\mathcal{C}$, i.e.:*

$$\mathcal{C} = \{\mathbf{x}\mathbf{G} : \mathbf{x} \in \mathbb{F}_q^k\}.$$

For any matrix $\mathbf{H}$ and any vector $\mathbf{x}$, the vector $\mathbf{H}\mathbf{x}^T$ is called syndrome *of $\mathbf{x}$. We then call* parity-check matrix *of $\mathcal{C}$ an $r \times n$ matrix $\mathbf{H}$ such that every codeword has syndrome 0 with respect to $\mathbf{H}$, i.e.*

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{H}\mathbf{x}^T = 0\}.$$

Note that the parity-check matrix of a code $\mathcal{C}$ is also a generator matrix for the *dual* code $\mathcal{C}^\perp$, i.e. the linear code formed by all the words of $\mathbb{F}_q^n$ that are orthogonal to $\mathcal{C}$. It follows that for any generator matrix $\mathbf{G}$ and parity check matrix $\mathbf{H}$ of a code, we have $\mathbf{G}\mathbf{H}^T = \mathbf{0}_{k\times r}$.

Both matrices are required to always have to have full rank. Moreover, notice that, clearly, neither matrix is unique: for instance, given a generator matrix $\mathbf{G}$

it is always possible to obtain another generator matrix for the same code by a linear transformation, that is, the multiplication on the left by an invertible $k \times k$ matrix $\mathbf{S}$, so that $\mathbf{G}' = \mathbf{SG}$. This corresponds simply to a change of basis for the vector space. A similar property is verified by the parity-check matrix. Finally, two generator matrices generate *equivalent codes* if one is obtained from the other by a permutation of columns. These two facts are at the basis of the McEliece cryptosystem.

Joining these two properties, we can write any generator matrix $\mathbf{G}$ in *systematic form* as $\mathbf{G} = [\mathbf{I}_k|\mathbf{A}]$, where $\mathbf{I}_k$ is the identity matrix of size k and $|$ denotes concatenation. If $\mathcal{C}$ is generated by $\mathbf{G} = [\mathbf{I}_k|\mathbf{A}]$, then a parity check matrix for $\mathcal{C}$ is $\mathbf{H} = [-\mathbf{A}^T|\mathbf{I}_{n-k}]$ (up to permutation, $\mathbf{H}$ can be transformed so that the identity submatrix is on the left hand side).

2.2 The McEliece Cryptosystem

The McEliece public-key encryption scheme [2] was introduced by R. J. McEliece in 1978. The original scheme uses binary Goppa codes, with which it remains unbroken (with a proper choice of parameters), but the scheme can be used with any class of codes for which an efficient decoding algorithm is known.

Key Generation Let $\mathbf{G}$ be a generator matrix for a linear $[n, k, d]$-code over $\mathbb{F}_q$ with an efficient decoding algorithm $\mathcal{D}$ which can correct up to $t = \lfloor (d-1)/2 \rfloor$ errors. Let $\mathbf{S}$ be an invertible $k \times k$ matrix and P be a random $n \times n$ permutation matrix over $\mathbb{F}_q$. The private key is $(\mathbf{S}, \mathbf{G}, \mathbf{P})$ and the public key is $\mathbf{G}' := \mathbf{SGP}$.

Encryption To be able to encrypt a plaintext, it has to be represented as a vector $\mathbf{m}$ of length k over $\mathbb{F}_q$. The encryption algorithm chooses a random error vector $\mathbf{e}$ of weight t in $\mathbb{F}_q^n$, and computes the ciphertext $\mathbf{c} = \mathbf{mG}' + \mathbf{e}$.

Decryption The decryption algorithm first computes $\hat{\mathbf{c}} = \mathbf{cP}^{-1} = \mathbf{mSG} + \mathbf{eP}^{-1}$. As $\mathbf{P}$ is a permutation matrix, $\mathbf{eP}^{-1}$ has the same weight as $\mathbf{e}$. Therefore, $\mathcal{D}$ can be used to decode the errors: $\hat{\mathbf{m}} = \mathbf{mS} = \mathcal{D}(\hat{\mathbf{c}})$. Finally, the plaintext is retrieved as $\mathbf{m} = \hat{\mathbf{m}}\mathbf{S}^{-1}$.

In successive papers, the original McEliece cryptosystem was refined and tweaked many times; for example it is now common practice to replace the scrambling method given by $\mathbf{S}$ and $\mathbf{P}$ with the computation of the systematic form, i.e. $\mathbf{G}'$ is the systematic form of $\mathbf{G}$. This is possible when the McEliece cryptosystem is embedded into a larger framework to convert it into an IND-CCA2 secure PKE or KEM, and has the additional advantage (beyond the obvious simper formulation) of a smaller public key (since only the non-identity submatrix needs to be stored).

The (one-way) security of McEliece is largely based on the following hard problem.

Problem 1 (Syndrome Decoding Problem). Given an $(n-k) \times n$ full-rank matrix $\mathbf{H}$ and a vector $\mathbf{s}$, both with entries in $\mathbb{F}_q$, and a non-negative integer t; find a vector $\mathbf{e} \in \mathbb{F}_q^n$ of weight t such that $\mathbf{H}\mathbf{e}^T = \mathbf{s}^T$.

The Syndrome Decoding Problem (SDP) is a well-known problem in complexity theory, and it has been shown to be NP complete [8]. Note that, since the McEliece cryptosystem uses an $[n, k, d]$ code, the number of error vectors is $\binom{n}{t}(q-1)^t$, while the number of possible syndromes is q^r. Therefore, if

$$\binom{n}{t}(q-1)^t < q^r,$$

there is at most one solution to the problem, which guarantees the decoding process has a unique solution.

3 Sparse-Matrix Codes

One of the most delicate points about the McEliece cryptosystem is that, in order for the security to reduce to SDP, it is assumed that the matrix produced as the public key is indistinguishable from a uniformly random matrix of the same size. This is, as we just mentioned, an assumption, and while plausible, it has been shown to be false in several cases. For many variants of McEliece (e.g. [9]), in fact, this opened up avenues of attack which simply ruled out the variant altogether. Even the long-standing binary Goppa codes have been shown to be distinguishable [10] when the code rate is chosen carelessly (too high). This is arguably one of the main reasons that pushed researchers away from algebraic codes, and towards codes of a different nature.

Low-Density Parity-Check (LDPC) codes are defined by matrices whose only requirement is to be very sparse, with a very low, constant row weight. These codes are easy to generate, and moreover admit a variety of choices for the decoding algorithm $\mathcal{D}$, like the Bit Flipping (BF) decoder of Gallager [11], which is very efficient in practice. For these reasons, this class of codes is a natural candidates for the McEliece cryptosystem. In such a framework, the secret code $\mathcal{C}$ is represented through its parity check matrix $\mathbf{H}$; the public key corresponds to a generator matrix $\mathbf{G}$ for $\mathcal{C}$. It is important to note that, from the knowledge of $\mathbf{G}$, the opponent can compute several parity-check matrices $\mathbf{H}'$ for $\mathcal{C}$, but they will not lead to an efficient decoding, unless they are sparse. As explained in section 2.2, typically having $\mathbf{G}$ in systematic form is enough to guarantee such property. Indeed, we can always write $\mathbf{H} = [\mathbf{H}_0|\mathbf{H}_1]$, where $\mathbf{H}_0$ and $\mathbf{H}_1$ have dimensions, respectively, $r \times k$ and $r \times r$. Then, the corresponding generator matrix in systematic form is obtained as $\mathbf{G} = [\mathbf{I}_k|\mathbf{H}_0^T\mathbf{H}_1^{-T}]$. Typically (unless for specific choices of $\mathbf{H}$) the inverse of a sparse matrix is dense, and so $\mathbf{H}_1^{-T}$ is dense: in such a case, the multiplication of $\mathbf{H}_0^T$ by $\mathbf{H}_1^{-T}$ is enough to hide the structure of $\mathbf{H}$ into the one of $\mathbf{G}$.

It is important to note that, due to their probabilistic nature, decoding algorithms for LDPC codes are characterized by a non-trivial decoding failure rate (DFR). This means that, in the case of a decoding failure, Bob must ask Alice for a retransmission of the plaintext, encrypted with a different error vector. In order to avoid frequent retransmissions, which would obviously increase the latency of the system, the DFR must be kept sufficiently low; typically, values are in the range of 10^{-6} to 10^{-9}. As we will discuss later, this fact represents a crucial difference, with respect to the case of algebraic codes, since it leads to a new family of attacks, aimed at recovering the secret key.

3.1 Security

The advantage of using LDPC codes is that the indistinguishability issue boils down to recovering low-weight words, and specifically low-weight codewords in the dual code, which is again a decoding problem. In particular, let us denote by $\mathcal{C}^\perp$ the dual code of $\mathcal{C}$, which admits $\mathbf{H}$ as generator matrix. Since the rows of $\mathbf{H}$ are sparse, and have maximum weight $w \ll n$, with overwhelming probability they represent minimum-weight codewords in $\mathcal{C}^\perp$, and so can be searched with a generic algorithm for finding low-weight words.

At the current state of the art, the best procedure for this task is the information set decoding (ISD) algorithm, which was first introduced by Prange in 1962 [12], and has received many improvements during the years [13–16]. However, ISD and all its variants are characterized by an exponential complexity: the search for a weight-w codeword has asymptotic complexity equal to $2^{\alpha w}$, where the value of the constant α depends on the code parameters and on the particular algorithm we are analyzing. Even in a quantum setting, ISD algorithms are still characterized by exponential complexity: indeed, the only known application of a quantum algorithm to an ISD algorithm, which consists in using Grover's algorithm [17] to speed up the search, leads to a reduction in the complexity, with respect to the classical case, which cannot be larger than the square root of the exponent α [18]. This means that the adoption of Low-density parity-check (LDPC) and moderate-density parity-check (MDPC) codes does not reduce the security of the McEliece cryptosystem, since attacks deriving from the structure of the secret code can be easily avoided by fixing the minimum weight of the rows of $\mathbf{H}$.

Since the main threat to the use of LDPC codes is represented by a search for low-weight words, it makes sense to relax the notion of "Low-Density": the authors in [19] introduce the notion of "Moderate-Density" by increasing the allowed row weight in the parity-check matrix from $O(1)$ to $O(\sqrt{n})$. It is still possible to decode such codes (called MDPC by analogy) with the previously-mentioned algorithms; the error-correction capacity gets obviously worse, but the gain in security makes this tradeoff worth it.

3.2 Structured Codes

Using generic LDPC and MDPC without any structure is not a practical choice, since the resulting public-key sizes are significantly larger than the ones we can obtain with other families of codes, like Goppa codes. In fact, even if the private parity-check matrix can be compactly represented just by its non-null entries, together with their positions (and so, a row with Hamming weight equal to w can be stored just with $w \log_2 n \log_2 q$ bits), applying this technique to the public key is not possible, since a sparse $\mathbf{G}$ might compromise the security of the system. One way to avoid this issue is to add some structure to the code family. This idea was first introduced in the context of algebraic codes [3,20], and was therefore extended to sparse codes [5,21]. In all cases, the authors propose to use quasi-cyclic (QC) codes to reduce key size. A QC code is simply a code which admits parity-check and generator matrices made of *circulant* blocks. A circulant matrix is a matrix in which every row is obtained as the cyclic shift of the previous one; an example of a circulant matrix is depicted below.

$$\begin{bmatrix} a_0 & a_1 & \dots & a_{p-1} \\ a_{p-1} & a_0 & \dots & a_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix}$$

This means that, in the McEliece cryptosystem, we can describe the public key completely using just the first row of each circulant block; it is clear that this results in a significant reduction in the public key size. However, this additional structure presents some drawbacks, since it exposes the system to structural weaknesses. In particular, the QC structure summed to the algebraic structure of the underlying codes, provides a lot of information to the attacker, and opens up the possibility of structural attacks aimed at recovering the private code. The most famous structural attack of this type is known as FOPT [22], and works by solving a multivariate algebraic system with Gröbner bases techniques together with the QC property which greatly reduces the number of unknowns of the system. As a result, it seems very hard to provide secure schemes which involve QC algebraic codes (Goppa, GRS etc.), while still obtaining an effective key reduction: the recent NIST proposal BIG QUAKE [23] shows a reduction of about $1/4$ of the key size which would be obtained in a "classical" McEliece using unstructured binary Goppa codes.

Therefore, once again, it seems safer to deploy code-based schemes using sparse codes, since in this case there is no additional algebraic structure, and the QC property alone is not enough to provide a structural attack. However, some care is still necessary when using such systems. In particular, we can consider two main aspects which need to be addressed:

- ISD algorithms might exploit the QC structure, and thus obtain a speed up; this technique, consisting of analyzing multiple samples at once, is known as Decoding One Out of Many (DOOM) [24], and results in a reduction in the complexity of these attacks. Note that this speedup is valid not only for attacks aiming at recovering the secret key, but also for attacks aiming at decoding intercepted ciphertexts (one-way security). While the speedup is not dramatic (it is in the order of the circulant size), it still has an important impact, since it leads to an increase in the row weight of $\mathbf{H}$ and in the number of errors applied during encryption, which in turn results in an increase in the key length.
- It has been recently shown that the probability of a decoding failure depends on the number of overlapping ones between the error vector and rows of $\mathbf{H}$. In addition, in a circulant matrix, all the rows are characterized by the same set of cyclic distances between set symbols (given two ones at positions i and j, the corresponding cyclic distance is computed as $\min\{\pm(i-j) \mod p\}$, with p being the circulant size). As shown in [25], an adversary can mount a Chosen Ciphertext Attack (CCA) attack, in which he impersonates an honest user, producing ciphertexts and requesting their decryption. The adversary can then exploit the events of decoding failures, which are of public knowledge, in order to gather information about distances among ones. The set of all such distances is called *distance spectrum*, and can be used to reconstruct the secret parity-check matrix. This problem can be related to a graph problem, in which a row of $\mathbf{H}$ corresponds to a clique with maximum size. For a sparse QC matrix, such graph is sparse as well, and so it is typically characterized by a small number of cliques. This means that, once the distance spectrum is known, recovering the corresponding parity-check matrix is, in most of the cases, not a hard task.

Among the cited attacks, reaction attacks represent the main threat, since they can be fully avoided only with significant trade-offs. In fact, currently existing solutions are based on the use of ephemeral keys [26, 27], or on the use of particular families of codes which make the reconstruction of the secret key unfeasible [28]. However, as we mentioned, both these solutions come with a significant price to pay, since we must generate a new key-pair for each encryption (in the first case) or increase the size of the public key. Another solution could be that of reducing the DFR to a negligible value, in order to increase the number of ciphertexts that the opponent must produce to recover the secret distance spectrum [29]. In order to obtain this property, we need longer codes, and so we need to increase the public key size.

As we will see in the rest of this paper, the idea of using some structure to reduce the public key size can be strongly generalized. In particular, we will show that existing solutions are just very special cases of a wider framework, characterized by several different aspects. This generalization comes with no increase in the public key, while it might allow avoiding the attack of DOOM and/or reaction attacks, or at the very least reduce their efficiency.

4 Reproducibility

We are now ready to introduce the fundamental notions of this paper.

Definition 3. *Consider a matrix* $\mathbf{A} \in \mathbb{F}_q^{k \times n}$*. Let* $\mathcal{R}$ *be the set of the rows of* $\mathbf{A}$ *and let* $2^{\mathcal{R}}$ *be its power set. We say that* $\mathbf{A}$ *is* reproducible *if* $\mathbf{A}$ *can be entirely described as* $\mathcal{F}(\mathbf{a})$*, where* $\mathcal{F}$ *is a family of linear transformations on elements of* $\mathbb{F}_q^{m \times n}$ *and* $\mathbf{a}$ *is an element of* $2^{\mathcal{R}}$ *called the* signature set*.*

Definition 4. *Let* $\mathcal{C}$ *be a linear code over* $\mathbb{F}_q$*, described by a reproducible generator matrix* $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ *and/or a reproducible parity-check matrix* $\mathbf{H} \in \mathbb{F}_q^{r \times n}$*; then we say that* $\mathcal{C}$ *is in* reproducible form*.*

Thus, a reproducible matrix is described just by its signature set and by the corresponding family of linear functions. Consequently, having the generator matrix (and/or the parity-check matrix) in reproducible form leads to a compact representation of the code. Actually, the condition on the reproducibility of a matrix can be relaxed, in order to take into account also other structures that allow a compact representation.

Definition 5. *Let* $\mathbf{A}_{i,j} \in \mathbb{F}_q^{k_{i,j} \times n_{i,j}}$ *be reproducible matrices, each with its own dimensions, signature set* $\mathbf{a}_{i,j} \in \mathbb{F}_q^{m_{i,j} \times n_{i,j}}$ *and family of linear functions* $\mathcal{F}_{i,j}$*. Let* $\mathbf{A}$ *be a matrix obtained using as building blocks the matrices* $\mathbf{A}_{i,j}$*; then, we say that* $\mathbf{A}$ *is* quasi-reproducible*.*

Definition 6. *Let* $\mathcal{C}$ *be a linear code over* $\mathbb{F}_q$*, described by a quasi-reproducible generator matrix* $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ *and/or a quasi-reproducible parity-check matrix* $\mathbf{H} \in \mathbb{F}_q^{r \times n}$*; then we say that* $\mathcal{C}$ *is in* quasi-reproducible form*.*

It is clear that, in order to describe a quasi-reproducible matrix, we just need the ensemble of the signature sets of its building blocks, together with the corresponding families of linear functions. Quasi-reproducibility generalizes the concept of reproducibility, since each reproducible code can be seen as a particular quasi-reproducible code, with a generator matrix described just by one signature. A particular type of quasi-reproducible codes is the one in which the blocks $\mathbf{A}_{i,j}$ are square matrices, defined by the same family $\mathcal{F}$ and form a pseudo-ring (i.e. a ring without multiplicative identity).

Definition 7. *Consider a family* $\mathcal{F} = \left\{\boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \cdots, \boldsymbol{\sigma}_{\frac{p}{m}-1}\right\}$*, where each* $\boldsymbol{\sigma}_i$ *is a* $p \times p$ *matrix. We denote as* $\mathcal{M}_q^{\mathcal{F},m}$ *the ensemble of all reproducible matrices over* $\mathbb{F}_q$*, with signature of dimensions* $m \times p$ *and family of linear transformations* $\mathcal{F}$*, equipped with the usual operations of sum and multiplication between two matrices. If the following properties hold*

(a) *the set* $\mathcal{M}_q^{\mathcal{F},m}$*, equipped with the sum operation, is an abelian group;*
(b) *the set* $\mathcal{M}_q^{\mathcal{F},m}$*, equipped with the multiplication operation, is a semigroup;*
(c) *multiplication distributes over addition;*

then $\mathcal{M}_q^{\mathcal{F},m}$ *is a* pseudo-ring, *and we call it the* reproducible pseudo-ring *induced by* $\mathcal{F}$ *over* $\mathbb{F}_q$.

Showing that $\mathcal{M}_q^{\mathcal{F},m}$ is an additive abelian group is quite straightforward. In fact, the signature of the sum of two matrices corresponds to the sum of the original signatures; commutativity and associativity follow from the element-wise sum between two matrices. The identity is the null signature (i.e., the signature made of all zeros), while the inverse of a matrix with signature $\mathbf{a}$ is the matrix with signature $-\mathbf{a}$. On the other hand, the only requirement of a semigroup is being closed with respect to an associative operation (in our case the multiplication). While associativity easily follows from the properties of the multiplication between two matrices, in order to guarantee closure, we must make some further considerations.

Theorem 1. *Let* $\mathcal{F} = \left\{\boldsymbol{\sigma}_0 = \mathbf{I}_p, \boldsymbol{\sigma}_1, \cdots, \boldsymbol{\sigma}_{\frac{p}{m}-1}\right\}$ *be a family of linear transformations, and let* $\mathcal{M}_q^{\mathcal{F},m}$ *be the reproducible pseudo-ring induced by* $\mathcal{F}$ *over* $\mathbb{F}_q$. *Then, for every matrix* $\mathbf{B} \in \mathcal{M}_q^{\mathcal{F},m}$, *it must be*

$$\boldsymbol{\sigma}_i\mathbf{B} = \mathbf{B}\boldsymbol{\sigma}_i, \ \ \forall \ \ i \in \mathbb{N}, 0 \leq i \leq \frac{p}{m} - 1.$$

Proof. Let $\mathbf{A}$ and $\mathbf{B}$ be two matrices belonging to $\mathcal{M}_q^{\mathcal{F},m}$, with respective signatures $\mathbf{a}_0$, $\mathbf{b}_0$, that is

$$\mathbf{A} = \begin{bmatrix} \mathbf{a}_0 \\ \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\frac{p}{m}-1} \end{bmatrix} = \begin{bmatrix} \mathbf{a}_0 \\ \mathbf{a}_0\boldsymbol{\sigma}_1 \\ \vdots \\ \mathbf{a}_0\boldsymbol{\sigma}_{\frac{p}{m}-1} \end{bmatrix}, \ \ \mathbf{B} = \begin{bmatrix} \mathbf{b}_0 \\ \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_{\frac{p}{m}-1} \end{bmatrix} = \begin{bmatrix} \mathbf{b}_0 \\ \mathbf{b}_0\boldsymbol{\sigma}_1 \\ \vdots \\ \mathbf{b}_0\boldsymbol{\sigma}_{\frac{p}{m}-1} \end{bmatrix}.$$

Multiplying these two matrices yields to

$$\mathbf{C} = \begin{bmatrix} \mathbf{c}_0 \\ \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_{\frac{p}{m}-1} \end{bmatrix} = \mathbf{AB} = \begin{bmatrix} \mathbf{a}_0\mathbf{B} \\ \mathbf{a}_1\mathbf{B} \\ \vdots \\ \mathbf{a}_{\frac{p}{m}-1}\mathbf{B} \end{bmatrix} = \begin{bmatrix} \mathbf{a}_0\mathbf{B} \\ \mathbf{a}_0\boldsymbol{\sigma}_1\mathbf{B} \\ \vdots \\ \mathbf{a}_0\boldsymbol{\sigma}_{\frac{p}{m}-1}\mathbf{B} \end{bmatrix}. \tag{1}$$

Since we want $\mathbf{C}$ to be reproducible and defined by $\mathcal{F}$, it must be

$$\mathbf{a}_0\boldsymbol{\sigma}_i\mathbf{B} = \mathbf{c}_i = \mathbf{c}_0\boldsymbol{\sigma}_i = \mathbf{a}_0\mathbf{B}\boldsymbol{\sigma}_i, \tag{2}$$

for each integer $i \leq \frac{p}{m} - 1$. Since eq. (2) must be satisfied for every signature $\mathbf{a}_0 \in \mathbb{F}_q^{m\times p}$, then $\boldsymbol{\sigma}_i$ and $\mathbf{B} \in \mathcal{M}_q^{\mathcal{F},m}$ must commute, that is $\boldsymbol{\sigma}_i\mathbf{B} = \mathbf{B}\boldsymbol{\sigma}_i$. □

4.1 Pseudo-rings Induced by Families of Permutations

In the particular case of signatures made of just one row (i.e., $m = 1$) and the functions $\boldsymbol{\sigma}_i$ being permutations, Theorem 1 leads to a further result, which is described in Theorem 2. We point out that the results we present in this section can be generalized, in order to consider also the case of $m > 1$, but we will not go into further details. Since a $p \times p$ permutation corresponds to a matrix in which every row and column has weight equal to 1, it can equivalently be described as a bijection over $[0, p] \subset \mathbb{N}$. Given a permutation matrix $\boldsymbol{\sigma}_i$, we denote the corresponding bijection as $f_{\boldsymbol{\sigma}_i}$. If the element of $\boldsymbol{\sigma}_i$ in position (v, z) is equal to 1, then $f_{\boldsymbol{\sigma}_i}(v) = z$. The inverse of $f_{\boldsymbol{\sigma}_i}$ is denoted as $f_{\boldsymbol{\sigma}_i}^{-1}$, and is the bijection associated to the permutation matrix $\boldsymbol{\sigma}_i^{-1} = \boldsymbol{\sigma}_i^T$; if $f_{\boldsymbol{\sigma}_i}(v) = j$, then $f_{\boldsymbol{\sigma}_i}^{-1}(j) = v$. Let $\mathbf{a}$ and $\mathbf{a}'$ be two row vectors, such that $\mathbf{a}' = \mathbf{a}\boldsymbol{\sigma}_i$: then, $a'_j = a_{f_{\boldsymbol{\sigma}_i}^{-1}(j)}$. If $\mathbf{a}$ and $\mathbf{a}'$ are instead two column vectors, such that $\mathbf{a}' = \boldsymbol{\sigma}_i\mathbf{a}$, then $a'_j = a_{f_{\boldsymbol{\sigma}_i}(j)}$. We use $f_{\boldsymbol{\sigma}_i} \circ f_{\boldsymbol{\sigma}_j}$ to denote the bijection defined by the application of $f_{\boldsymbol{\sigma}_i}$ after $f_{\boldsymbol{\sigma}_j}$. In other words, $f_{\boldsymbol{\sigma}_i} \circ f_{\boldsymbol{\sigma}_j}$ corresponds to the permutation matrix $\boldsymbol{\sigma}_i\boldsymbol{\sigma}_j$, and $f_{\boldsymbol{\sigma}_i} \circ f_{\boldsymbol{\sigma}_j}(v) = f_{\boldsymbol{\sigma}_i}\left(f_{\boldsymbol{\sigma}_j}(v)\right)$. The identity $\mathbf{I}_p$ can be seen as the particular permutation that does not change the order of the elements; the corresponding bijection, which will be denoted as id, is such that each element is mapped into itself (in other words, $f_{\mathbf{I}_p}(v) = v$).

Theorem 2. *Let* $\mathcal{F} = \left\{\boldsymbol{\sigma}_0 = \mathbf{I}_p, \boldsymbol{\sigma}_1, \cdots, \boldsymbol{\sigma}_{\frac{p}{m}-1}\right\}$ *be a family of linear transformations, with each* $\boldsymbol{\sigma}_i$ *being a permutation, and suppose that* $\mathcal{F}$ *induces the reproducible pseudo-ring* $\mathcal{M}_q^{\mathcal{F},1}$ *over* $\mathbb{F}_q$*. Then, the following relation must be satisfied*

$$\boldsymbol{\sigma}_j\boldsymbol{\sigma}_i = \boldsymbol{\sigma}_{f_{\boldsymbol{\sigma}_i}(j)}, \quad \forall i, j \in \mathbb{N}, \ \ 0 \leq i \leq p-1, \ \ 0 \leq j \leq p-1.$$

Proof. We know from Theorem 1 that, for every matrix $\mathbf{B} \in \mathcal{M}_q^{\mathcal{F},1}$ and every function $\boldsymbol{\sigma}_i$, it must be $\boldsymbol{\sigma}_i\mathbf{B} = \mathbf{B}\boldsymbol{\sigma}_i$. In particular, the left-side multiplication of $\mathbf{B}$ by $\boldsymbol{\sigma}_i$ corresponds to a row-permutation, such that

$$\boldsymbol{\sigma}_i\mathbf{B} = \begin{bmatrix} \mathbf{b}_{f_{\boldsymbol{\sigma}_i}(0)} \\ \mathbf{b}_{f_{\boldsymbol{\sigma}_i}(1)} \\ \vdots \\ \mathbf{b}_{f_{\boldsymbol{\sigma}_i}(\frac{p}{m}-1)} = \end{bmatrix} = \begin{bmatrix} \mathbf{b}_0\boldsymbol{\sigma}_{f_{\boldsymbol{\sigma}_i}(0)} \\ \mathbf{b}_0\boldsymbol{\sigma}_{f_{\boldsymbol{\sigma}_i}(1)} \\ \vdots \\ \mathbf{b}_0\boldsymbol{\sigma}_{f_{\boldsymbol{\sigma}_i}(p-1)} \end{bmatrix}. \tag{3}$$

The product $\mathbf{B}\boldsymbol{\sigma}_i$ defines, instead, a column permutation of the elements in $\mathbf{B}$, and can be expressed as

$$\mathbf{B}\sigma_i = \begin{bmatrix} \mathbf{b}_0\boldsymbol{\sigma}_0 \\ \mathbf{b}_0\boldsymbol{\sigma}_1 \\ \vdots \\ \mathbf{b}_0\boldsymbol{\sigma}_{p-1} \end{bmatrix} \boldsymbol{\sigma}_i = \begin{bmatrix} \mathbf{b}_0\boldsymbol{\sigma}_0\boldsymbol{\sigma}_i \\ \mathbf{b}_0\boldsymbol{\sigma}_1\boldsymbol{\sigma}_i \\ \vdots \\ \mathbf{b}_0\boldsymbol{\sigma}_{p-1}\boldsymbol{\sigma}_i \end{bmatrix}. \tag{4}$$

Then, we can put together equations (3) and (4), and thus obtain

$$\boldsymbol{\sigma}_j\boldsymbol{\sigma}_i = \boldsymbol{\sigma}_{f_{\boldsymbol{\sigma}_i}(j)}, \tag{5}$$

which must be satisfied for every pair of indexes (i, j). $\square$

Starting from the result of Theorem 2, we can easily derive some other properties that $\mathcal{F}$ must satisfy.

Corollary 1. *Let $\mathcal{F}$ be a family of permutations satisfying Theorem 2. Then, $\mathcal{F}$ has the following properties*

(a) $f_{\boldsymbol{\sigma}_i}(0) = i, \ \ \forall i;$
(b) $\forall i \ \ \exists j \ \ s.t. \ \ f_{\boldsymbol{\sigma}_i} \circ f_{\boldsymbol{\sigma}_j} = id.$

Proof. According to Theorem 2, we have

$$\boldsymbol{\sigma}_i = \mathbf{I}_p \boldsymbol{\sigma}_i = \boldsymbol{\sigma}_0 \boldsymbol{\sigma}_i = \boldsymbol{\sigma}_{f_{\boldsymbol{\sigma}_i}(0)}, \tag{6}$$

which can be satisfied only if $f_{\boldsymbol{\sigma}_i}(0) = i$, and this proves property (a).
Since each $f_{\boldsymbol{\sigma}_i}$ is a bijection of the integers in $[0, p-1]$, we know that, for a fixed value of i, there is a value $j \in [0, p-1]$ such that $f_{\boldsymbol{\sigma}_i}(j) = 0$. Then, we have

$$\boldsymbol{\sigma}_j \boldsymbol{\sigma}_i = \boldsymbol{\sigma}_{f_{\sigma_i}(j)} = \boldsymbol{\sigma}_0 = \mathbf{I}_p. \tag{7}$$

In other words, the bijections corresponding to $f_{\boldsymbol{\sigma}_i}$ and $f_{\boldsymbol{\sigma}_j}$ are one the inverse of the other, and this proves property (b). □

Theorem 3. *Let $\mathcal{M}_q^{\mathcal{F},1}$ be a reproducible pseudo-ring, and let $\mathcal{F}$ be a family of permutations satisfying the hypothesis from Theorem 2. Then, the invertible elements of $\mathcal{M}_q^{\mathcal{F},1}$ constitute a multiplicative group.*

Proof. First of all, we show that $\mathcal{M}_q^{\mathcal{F},1}$ contains the multiplicative identity, i.e., the $p \times p$ identity matrix. In this case, $\mathcal{F}$ is formed by p permutations such that $f_{\boldsymbol{\sigma}_i}(0) = i$, because of Corollary 1. Then, it is straightforward to show that $\mathbf{I}_p \in \mathcal{M}_q^{\mathcal{F},1}$, with corresponding signature $\mathbf{u} = [1, 0, \cdots, 0]$. Now, we need to prove that any non-singular matrix in $\mathcal{M}_q^{\mathcal{F},1}$ admits inverse in $\mathcal{M}_q^{\mathcal{F},1}$. Let us consider a matrix $\mathbf{A} \in \mathcal{M}_q^{\mathcal{F},m}$, with signature $\mathbf{a}$, and let $\mathbf{B}$ be its inverse. Since $\mathbf{AB} = \mathbf{I}_p$, we have

$$\mathbf{AB} = \begin{bmatrix} \mathbf{a} \\ \mathbf{a}\boldsymbol{\sigma}_1 \\ \vdots \\ \mathbf{a}\boldsymbol{\sigma}_{p-1} \end{bmatrix} \mathbf{B} = \mathbf{I}_p = \begin{bmatrix} \mathbf{u} \\ \mathbf{u}\boldsymbol{\sigma}_1 \\ \vdots \\ \mathbf{u}\boldsymbol{\sigma}_{p-1} \end{bmatrix},$$

which yields to $\mathbf{a}\boldsymbol{\sigma}_i \mathbf{B} = \mathbf{u}\boldsymbol{\sigma}_i$. For $i = 0$ we have $\mathbf{aB} = \mathbf{u}$; for whichever value i, we obtain

$$\mathbf{a}\boldsymbol{\sigma}_i \mathbf{B} = \mathbf{u}\boldsymbol{\sigma}_i = \mathbf{aB}\boldsymbol{\sigma}_i,$$

which can be satisfied for whichever $\mathbf{a}$ only if $\boldsymbol{\sigma}_i$ and $\mathbf{B}$ commute. Because of Theorem 1, this means that $\mathbf{B} \in \mathcal{M}_q^{\mathcal{F},1}$. □

Sum and multiplication are not the only matrix operations we consider. In Theorem 4 we analyze how transposition acts on the matrices belonging to a reproducible pseudo-ring $\mathcal{M}_q^{\mathcal{F},1}$.

Theorem 4. *Let $\mathcal{M}_q^{\mathcal{F},1}$ be a reproducible pseudo-ring; if*

$$f_{\boldsymbol{\sigma}_j}^{-1}(i) = f_{\boldsymbol{\sigma}_v}^{-1}(0), \;\; v = f_{\boldsymbol{\sigma}_i}^{-1}(j), \;\; \forall i,j \;\; s.t. \;\; 0 \le i \le p-1, 0 \le j \le p-1$$

then $\mathcal{M}_q^{\mathcal{F},1}$ is closed under the transposition operation.

Proof. Let $\mathbf{A} \in \mathcal{M}_q^{\mathcal{F},1}$, with signature $\mathbf{a}$, and denote as $\mathbf{B} = \mathbf{A}^T$ its transpose. The i-th row of $\mathbf{B}$ corresponds to the i-th column of $\mathbf{A}$. In particular, the i-th column of $\mathbf{A}$ is defined as

$$\begin{bmatrix} a_i \\ a_{f_{\boldsymbol{\sigma}_1}^{-1}(i)} \\ a_{f_{\boldsymbol{\sigma}_2}^{-1}(i)} \\ \vdots \\ a_{f_{\boldsymbol{\sigma}_{p-1}}^{-1}(i)} \end{bmatrix}.$$

Because $\mathbf{B}$ is the transpose of $\mathbf{A}$, the i-th row of $\mathbf{B}$ corresponds to the i-th column of $\mathbf{A}$; let $\mathbf{b}_0$ denote the first row of $\mathbf{B}$, that is

$$\mathbf{b}_0 = [a_0, a_{f_{\boldsymbol{\sigma}_1}^{-1}(0)}, \cdots, a_{f_{\boldsymbol{\sigma}_{p-1}}^{-1}(0)}] = [a_{f_{\boldsymbol{\sigma}_0}^{-1}(0)}, a_{f_{\boldsymbol{\sigma}_1}^{-1}(0)}, \cdots, a_{f_{\boldsymbol{\sigma}_{p-1}}^{-1}(0)}]. \tag{8}$$

Let us consider the i-th row of $\mathbf{B}$, and denote it as $\mathbf{b}_i$; if transposition has closure in $\mathcal{M}_q^{\mathcal{F},1}$, then it must be

$$\begin{aligned} \mathbf{b}_i &= [a_i, a_{f_{\boldsymbol{\sigma}_1}^{-1}(i)}, \cdots, a_{f_{\boldsymbol{\sigma}_{p-1}}^{-1}(i)}] = \\ &= [a_{f_{\boldsymbol{\sigma}_0}^{-1}(i)}, a_{f_{\boldsymbol{\sigma}_1}^{-1}(i)}, \cdots, a_{f_{\boldsymbol{\sigma}_{p-1}}^{-1}(i)}] = \mathbf{b}_0 \boldsymbol{\sigma}_i. \end{aligned} \tag{9}$$

Now suppose that $f_{\boldsymbol{\sigma}_i}(v) = j$; then, the j-th entry in $\mathbf{b}_i$ corresponds to the v-th entry in $\mathbf{b}_0$, that is $a_{f_{\boldsymbol{\sigma}_v}^{-1}(0)}$. In other words we have $b_{i,j} = a_z$, with

$$z = f_{\boldsymbol{\sigma}_v}^{-1}(0), \;\; v = f_{\boldsymbol{\sigma}_i}^{-1}(j). \tag{10}$$

In order to satisfy eq. (9), a_z must be equal to the j-th entry of the i-th column of $\mathbf{A}$, that is $a_{f_{\boldsymbol{\sigma}_j}^{-1}(i)}$. Then, it must be $f_{\boldsymbol{\sigma}_j}^{-1}(i) = z$, that is

$$f_{\boldsymbol{\sigma}_j}^{-1}(i) = f_{\boldsymbol{\sigma}_v}^{-1}(0), \;\; v = f_{\boldsymbol{\sigma}_i}^{-1}(j). \tag{11}$$

□

Depending on the properties stated by the previous theorems, the family $\mathcal{F}$ might induce different algebraic structures over $\mathbb{F}_q^{p \times p}$. In particular, consider the case of $\mathcal{F}$, inducing $\mathcal{M}_q^{\mathcal{F},1}$, satisfying both Theorems 3 and 4. Let $\mathbf{A}$ be a square matrix whose elements are picked from $\mathcal{M}_q^{\mathcal{F},1}$. By definition, we have $\mathbf{A}^{-1} = \frac{1}{det(\mathbf{A})} adj(\mathbf{A})$, where $det(\mathbf{A})$ is the determinant of $\mathbf{A}$ and $adj(\mathbf{A})$ is the adjugate of $\mathbf{A}$. Computing $det(\mathbf{A})$ involves only sums and multiplications: this means that $det(\mathbf{A}) \in \mathcal{M}_q^{\mathcal{F},1}$; because of Theorem 3, $\frac{1}{det(\mathbf{A})} \in \mathcal{M}_q^{\mathcal{F},1}$. Computing $adj(\mathbf{A})$ involves sums, multiplications and transpositions: because of Theorem 4, we have that the entries of $adj(\mathbf{A})$ are again elements of $\mathcal{M}_q^{\mathcal{F},1}$. This means that $\mathbf{A}^{-1}$ is matrix whose elements are belong to $\mathcal{M}_q^{\mathcal{F},1}$, and so has the same quasi-reproducible structure of $\mathbf{A}$.

4.2 Known Examples of Reproducible Pseudo-Rings

In Section 4.1 we have described some properties that a family of permutations $\mathcal{F}$ must possess, in order to guarantee that it induces algebraic structures on $\mathbb{F}_q^{p\times p}$. Well-known cases of such objects, with common use in cryptography, are circulant matrices and dyadic matrices.

Circulant Matrices As we have seen before, a circulant matrix is a $p\times p$ matrix for which each row is obtained as the cyclic shift of the previous one. In particular, a circulant matrix can be seen as a square reproducible matrix, whose signature corresponds to the first row and the functions $\boldsymbol{\sigma}_i$ defining $\mathcal{F}$ correspond to $\boldsymbol{\pi}^i$, where the elements of $\boldsymbol{\pi}$ are defined as

$$\pi_{l,j} = \begin{cases} 1 & \text{if } l+1 \equiv j \mod p \\ 0 & \text{otherwise} \end{cases}. \tag{12}$$

Basically, the bijection representing $\boldsymbol{\pi}$ is defined as

$$f_{\boldsymbol{\pi}}(v) = v + 1 \mod p. \tag{13}$$

It can be easily shown that

$$f_{\boldsymbol{\sigma}_i}(v) = f_{\boldsymbol{\pi}^i}(v) = \underbrace{f_{\boldsymbol{\pi}} \circ f_{\boldsymbol{\pi}} \cdots \circ f_{\boldsymbol{\pi}}}_{i \text{ times}}(v) = v + i \mod p, \tag{14}$$

which leads to $\boldsymbol{\pi}^p = \mathbf{I}_p$ and $\boldsymbol{\pi}^i\boldsymbol{\pi}^j = \boldsymbol{\pi}^{i+j \mod p}$. Since permutation matrices are orthogonal, their inverse correspond to their transpose, and thus $(\boldsymbol{\pi}^i)^T = \boldsymbol{\pi}^{p-i}$. With these properties, we have

$$\boldsymbol{\sigma}_i\boldsymbol{\sigma}_j = \boldsymbol{\pi}^{i+j \mod p} = \tag{15}$$

$$= \boldsymbol{\sigma}_{i+j \mod p}, \tag{16}$$

which is compliant with Theorem 2, since $f_{\boldsymbol{\sigma}_i}(j) = i+j \mod p$. With some simple computations, it can be easily shown that circulant matrices satisfy Theorem 4 and that the multiplication between two circulants is commutative.

Dyadic Matrices A *dyadic* matrix is a $p \times p$ matrix, with p being a power of 2, whose signature is again its first row. The rows of a dyadic matrix are obtained by permuting the elements of the signature, such that the element in position (i,j) is the one in the signature in position $i \oplus j$, where $\oplus$ denotes the bitwise XOR between i and j. Then, a dyadic can be described in terms of reproducible matrices, for which each function $\boldsymbol{\sigma}_i$ is the dyadic matrix whose signature have all null entries, except for the one in position i. This means that $\boldsymbol{\sigma}_i$ can be described by the following bijection

$$f_{\boldsymbol{\sigma}_i}(v) = v \oplus i \mod p. \tag{17}$$

If we combine two transformations, we obtain

$$\begin{aligned} f_{\boldsymbol{\sigma}_i} \circ f_{\boldsymbol{\sigma}_j}(v) &= (v \oplus j) \oplus i = \\ &= v \oplus (i \oplus j) = \\ &= f_{\boldsymbol{\sigma}_{i \oplus j}}(v). \end{aligned} \tag{18}$$

Since $f_{\boldsymbol{\sigma}_i}(j) = i \oplus j$, this proves that the family of dyadics is compliant with Theorem 2. It can be straightforwardly proven that dyadics are symmetric (and so, satisfy Theorem 4), and that the multiplication between two dyadics is commutative.

Circulant and dyadic matrices are just two particular cases of reproducible groups, and can obviously be further generalized by considering signatures that are composed by more than one row. In addition, several more constructions can be obtained. For instance, for every permutation matrix $\boldsymbol{\psi}$ and every reproducible pseudo-ring $\mathcal{M}_q^{\mathcal{F},m}$, induced by $\mathcal{F} = \left\{\sigma_0 = \mathbf{I}_p, \sigma_1, \cdots, \sigma_{\frac{p}{m}-1}\right\}$, we can obtain a new pseudo-ring as

$$\mathcal{M}_q^{\mathcal{F}',m} = \left\{ \mathbf{M}' | \, \mathbf{M}' = \boldsymbol{\psi}\mathbf{M}\boldsymbol{\psi}^T, \;\; \mathbf{M} \in \mathcal{M}_q^{\mathcal{F},m} \right\}. \tag{19}$$

The corresponding family of transformations is $\mathcal{F}' = \left\{\sigma'_0, \sigma'_1, \cdots, \sigma'_{\frac{p}{m}-1}\right\}$, with $\boldsymbol{\sigma}'_i = \boldsymbol{\sigma}_{f_{\boldsymbol{\psi}}(i)}\boldsymbol{\psi}^T$. Proving that $\mathcal{F}'$ actually induces a pseudo-ring is quite simple; indeed, for any two matrices $\mathbf{A} = \boldsymbol{\psi}\mathbf{M}_A\boldsymbol{\psi}^T$ and $\mathbf{B} = \boldsymbol{\psi}\mathbf{M}_B\boldsymbol{\psi}^T$, with $\mathbf{M}_A, \mathbf{M}_B \in \mathcal{M}_{\mathcal{F},m}$, we have

$$\mathbf{A} + \mathbf{B} = \boldsymbol{\psi}\mathbf{M}_A\boldsymbol{\psi}^T + \boldsymbol{\psi}M_B\boldsymbol{\psi}^T = \boldsymbol{\psi}(\mathbf{M}_A + \mathbf{M}_B)\boldsymbol{\psi}^T, \tag{20}$$

$$\mathbf{AB} = \boldsymbol{\psi}\mathbf{M}_A\boldsymbol{\psi}^T\boldsymbol{\psi}\mathbf{M}_B\boldsymbol{\psi}^T = \boldsymbol{\psi}\mathbf{M}_A\mathbf{M}_B\boldsymbol{\psi}^T, \tag{21}$$

which return matrices belonging to the $\mathcal{M}_q^{\mathcal{F}',m}$, since $\mathbf{M}_A + \mathbf{M}_B, \mathbf{M}_A\mathbf{M}_B \in \mathcal{M}_q^{\mathcal{F},m}$. In addition, if multiplication is commutative in $\mathcal{M}_q^{\mathcal{F},m}$, then it will be commutative in $\mathcal{M}_q^{\mathcal{F}',m}$ too. To prove this fact, let us consider two matrices $\mathbf{M}_A, \mathbf{M}_B \in \mathcal{M}_q^{\mathcal{F},m}$, such that $\mathbf{M}_A\mathbf{M}_B = \mathbf{M}_B\mathbf{M}_A$. Then, for $\mathbf{A} = \boldsymbol{\psi}\mathbf{M}_A\boldsymbol{\psi}^T$ and $\mathbf{B} = \boldsymbol{\psi}\mathbf{M}_B\boldsymbol{\psi}^T$, we have

$$\begin{aligned} \mathbf{AB} &= \boldsymbol{\psi}\mathbf{M}_A\boldsymbol{\psi}^T\boldsymbol{\psi}\mathbf{M}_B\boldsymbol{\psi}^T = \\ &= \boldsymbol{\psi}\mathbf{M}_A\mathbf{M}_B\boldsymbol{\psi}^T = \\ &= \boldsymbol{\psi}\mathbf{M}_B\mathbf{M}_A\boldsymbol{\psi}^T = \\ &= \boldsymbol{\psi}\mathbf{M}_B\boldsymbol{\psi}^T\boldsymbol{\psi}\mathbf{M}_A\boldsymbol{\psi}^T = \\ &= \mathbf{BA}. \end{aligned} \tag{22}$$

With some straightforward computations, we can easily prove that, if $\mathcal{M}_q^{\mathcal{F},m}$ is closed under transposition, then $\mathcal{M}_q^{\mathcal{F}',m}$ will be closed as well.

5 Codes in Reproducible Form

In the previous section we have described the properties that a family of functions $\mathcal{F}$ must have, in order to induce objects with some reproducible structure. Our analysis has shown that there is a wide range of possibilities for obtaining a code with a compact representation. It is clear that the use of reproducible pseudo-rings allows to obtain codes that can be described efficiently. We remember that the use of such codes has a crucial meaning in code-based crypto, in which we are interested in obtaining public keys that can be compactly represented. In this section we describe how this whole construction can be further generalized. Indeed, we can obtain codes that are described by a generator matrix that is not made of reproducible square blocks. This fact offers a new wide range of possible constructions. Essentially, we remove the condition on reproducible groups and just consider the case of codes that can be described by a reproducible generator matrix. In addition, we provide simple methods that allow to obtain random codes in reproducible form, starting from their parity-check matrix.

The following theorem states some properties about the parity-check matrix that are sufficient conditions (but not necessary) for having a code in reproducible form.

Theorem 5. *Let $\mathcal{C}$ over $\mathbb{F}_q$ be a code with length n, dimension k and codimension r. Let $m \in \mathbb{N}$ be a factor of k, and consider a family of linear transformations $\mathcal{F} = \left\{\boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \cdots, \boldsymbol{\sigma}_{\frac{k}{m}-1}\right\}$, with $\boldsymbol{\sigma}_0 = \mathbf{I}_n$. Let $\mathbf{H} \in \mathbb{F}_q^{r\times n}$ be a parity-check matrix for $\mathcal{C}$, and $s \in \mathbb{N}$ be a factor of r. Let $\mathbf{h}_i$ denote the subset of rows of H in positions $\{is, is+1, \cdots, (i+1)s-1\}$. Let $\mathbf{g}_0 \in \mathbb{F}_q^{m\times n}$ be a matrix such that $\mathbf{g}_0\mathbf{H}^T = \mathbf{0}_{m\times r}$. If we can define a function $f(x_0, x_1) : [0, \frac{k}{m}-1] \times [0, \frac{r}{s}-1] \subset \mathbb{N}^2 \to [0, \frac{r}{s}-1] \subset \mathbb{N}$ with the following properties:*

(a) $\mathbf{h}_j\sigma_i^T = \mathbf{h}_{f(i,j)}$
(b) *for any three integers $x_0 \in [0, \frac{k}{m}-1]$ and $x_1', x_1'' \in [0, \frac{r}{s}-1]$ it must be $f(x_0, x_1') \neq f(x_0, x_1'')$*
(c) *for any three integers $x_0', x_0'' \in [0, \frac{k}{m}-1]$ and $x_1 \in [0, \frac{r}{s}-1]$ it must be $f(x_0', x_1) \neq f(x_0'', x_1)$*

then $\mathcal{C}$ admits a generator matrix in reproducible form which is defined by the family $\mathcal{F}$ and by the signature $\mathbf{g}_0$.

Proof. Since the generator matrix $\mathbf{G}$ is reproducible, with signature $\mathbf{g}_0$, we have

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{\frac{k}{m}-1} \end{bmatrix} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_0\sigma_1 \\ \vdots \\ \mathbf{g}_0\sigma_{\frac{k}{m}-1} \end{bmatrix}, \tag{23}$$

while for the parity-check matrix $\mathbf{H}$ we can write

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{\frac{r}{s}-1} \end{bmatrix}. \quad (24)$$

Because $\mathbf{G}\mathbf{H}^T = \mathbf{0}_{k\times r}$, it must be

$$\mathbf{g}_i\mathbf{h}_j^T = \mathbf{g}_0\boldsymbol{\sigma}_i\mathbf{h}_j^T = \mathbf{0}_{m\times s}, \quad \forall i,j \in \mathbb{N} \text{ s.t. } 0 \le i \le \frac{k}{m}-1, \quad 0 \le j \le \frac{r}{s}-1. \quad (25)$$

From the hypothesis, we have an $m \times n$ matrix $\mathbf{g}_0$ such that $\mathbf{g}_0\mathbf{H}^T = \mathbf{0}_{m\times r}$, which means

$$\mathbf{g}_0\mathbf{h}_j^T = \mathbf{0}_{m\times s}, \quad \forall j \in \mathbb{N} \text{ s.t. } 0 \le j \le \frac{r}{s}-1. \quad (26)$$

Consider now the product $\mathbf{g}_i\mathbf{h}_j^T = \mathbf{g}_0\boldsymbol{\sigma}_i\mathbf{h}_j^T$, for $i \ge 1$. If we can define a function $f(x_0,x_1) : [0,\frac{k}{m}-1] \times [0,\frac{r}{s}-1] \subset \mathbb{N}^2 \to [0,\frac{r}{s}-1] \subset \mathbb{N}$, and choose $x_0 = i$, $x_1 = j$, such that

$$\boldsymbol{\sigma}_i\mathbf{h}_j^T = \mathbf{h}_{f(i,j)}^T, \quad (27)$$

then equation (25) is surely satisfied, since

$$\mathbf{g}_i\mathbf{h}_j^T = \mathbf{g}_0\boldsymbol{\sigma}_i\mathbf{h}_j^T = \mathbf{g}_0\mathbf{h}_{f(i,j)}^T = \mathbf{0}_{m\times s}, \quad (28)$$

where $\mathbf{g}_0\mathbf{h}_{f(i,j)}^T$ because of (26). In particular, by transposing both sides of eq. (27), we obtain $\mathbf{h}_j\boldsymbol{\sigma}_i^T = \mathbf{h}_{f(i,j)}$, which proves property a).

For the other two properties, we must consider that we want $\mathbf{H}$ and $\mathbf{G}$ to have rank, respectively, equal to r and k. One necessary condition for having $\mathbf{H}$ with full rank (but obviously not a sufficient one) is that, for a fixed i, the function $f(i,j)$ spans over all the integers in $[0,\frac{r}{s}-1]$ for different input values j. Indeed, if for some integers i and $j' \neq j''$ we have $f(i,j') = f(i,j'')$, then this means that $\mathbf{h}_{j'}\boldsymbol{\sigma}_i^T = \mathbf{h}_{j''}\boldsymbol{\sigma}_i^T$, which implies $\mathbf{h}_{j'} = \mathbf{h}_{j''}$. In analogous way, there cannot exist three integers $i' \neq i''$ and j such that $\mathbf{h}_j\boldsymbol{\sigma}_{i'}^T = \mathbf{h}_j\boldsymbol{\sigma}_{i''}^T$, otherwise it must be $\boldsymbol{\sigma}_{i'} = \boldsymbol{\sigma}_{i''}$, which results in $\mathbf{G}$ having some identical rows. $\square$

Theorem 5 allows to obtain a code in reproducible form in a very simple way. Suppose that, given a family of transformations $\mathcal{F}$, we have found a matrix $\mathbf{H}$, with the characteristics required by the theorem. Then, for the code $\mathcal{C}$ having $\mathbf{H}$ as parity-check matrix we can obtain a variety of reproducible generator matrices. Indeed, let $\mathbf{G}$ be a generator matrix for $\mathcal{C}$: by definition, since $\mathbf{G}\mathbf{H}^T = \mathbf{0}_{k\times r}$, we know that whichever subset $\mathbf{g}_0$ formed by m rows of $\mathbf{G}$ is such that $\mathbf{g}_0\mathbf{H}^T = \mathbf{0}_{m\times r}$. Then, $\mathbf{g}_0$ is a valid signature for our reproducible generator matrix, defined by the family $\mathcal{F}$.

In some cases, a quasi-reproducible code can be seen as a particular case of a reproducible code (and viceversa). Indeed, consider a code $\mathcal{C}$ with length $n = n_0 p$, dimension $k = p$ and codimension $r = (n_0 - 1)p$, for some integer $n_0 \in \mathbb{N}$. We suppose that $\mathcal{C}$ is described by a generator matrix in quasi-reproducible form: in particular, we suppose that $\mathbf{G}$ is obtained as the concatenation of n_0 blocks with dimensions $p \times p$, that is

$$\mathbf{G} = [\mathbf{G}_0 | \mathbf{G}_1 | \cdots | \mathbf{G}_{n_0-1}], \tag{29}$$

where each $\mathbf{G}_i$ is an element of the reproducible pseudo-ring $\mathcal{M}_q^{\mathcal{F}_i, m_i}$, and has signature V_i. If the signatures have all the same number of rows (that is, $m_i = m$), then such a $\mathbf{G}$ can be characterized as a particular reproducible matrix. Indeed, let us denote as $\mathcal{F}_i = \left\{\sigma_0^{(i)}, \sigma_1^{(i)}, \cdots, \sigma_{\frac{p}{m}-1}^{(i)}\right\}$ the i-th family of transformations. It is then easy to see that a matrix of the form (29) can be described as a reproducible matrix, with signature

$$\mathbf{g}_0 = \left[\mathbf{g}_0^{(0)} \middle| \, \mathbf{g}_0^{(1)} \middle| \cdots \middle| \mathbf{g}_0^{(n_0-1)}\right], \tag{30}$$

and obtained by the unique family of transformations $\mathcal{F} = \left\{\boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \cdots, \boldsymbol{\sigma}_{\frac{p}{m}-1}\right\}$, such that

$$\boldsymbol{\sigma}_i = \begin{bmatrix} \boldsymbol{\sigma}_i^{(0)} & \mathbf{0}_{p\times p} & \mathbf{0}_{p\times p} & \cdots & \mathbf{0}_{p\times p} \\ \mathbf{0}_{p\times p} & \boldsymbol{\sigma}_i^{(1)} & \mathbf{0}_{p\times p} & \cdots & \mathbf{0}_{p\times p} \\ \mathbf{0}_{p\times p} & \mathbf{0}_{p\times p} & \boldsymbol{\sigma}_i^{(2)} & \cdots & \mathbf{0}_{p\times p} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_{p\times p} & \mathbf{0}_{p\times p} & \mathbf{0}_{p\times p} & \cdots & \boldsymbol{\sigma}_i^{(n_0-1)} \end{bmatrix}. \tag{31}$$

5.1 Reproducible Codes from Householder Matrices

A *Householder matrix* [30] is a matrix that is at the same time orthogonal and symmetric. Consider a set of Householder matrices $\boldsymbol{\psi}_0, \boldsymbol{\psi}_1, \cdots, \boldsymbol{\psi}_{v-1}$. We have that, for all $j = 0, \ldots, v-1$, it must be $\boldsymbol{\psi}_j^{-1} = \boldsymbol{\psi}_j^T = \boldsymbol{\psi}_j$. We would like these matrices to form a commutative group, that is

$$\boldsymbol{\psi}_i \boldsymbol{\psi}_j = \boldsymbol{\psi}_j \boldsymbol{\psi}_i, \; 0 \le i, j \le v-1. \tag{32}$$

Let us now take two sets of 2^v distinct binary v-tuples, that is

$$\begin{aligned} &\left\{\mathbf{a}^{(i)} \middle| \; 0 \le i \le 2^v - 1, \; \mathbf{a}^{(i)} \in \mathbb{F}_2^v, \; \forall i \; \nexists j \; \text{ s.t. } \; \mathbf{a}^{(i)} = \mathbf{a}^{(j)}\right\}, \\ &\left\{\mathbf{b}^{(i)} \middle| \; 0 \le i \le 2^v - 1, \; \mathbf{b}^{(i)} \in \mathbb{F}_2^v, \; \forall i \; \nexists j \; \text{ s.t. } \; \mathbf{b}^{(i)} = \mathbf{b}^{(j)}\right\}. \end{aligned} \tag{33}$$

For the sake of simplicity, set $\mathbf{a}^{(0)} = \mathbf{0}_{1\times v}$. It is clear that these two sets are identical, except for the order of their elements. We can now define a family of transformations $\mathcal{F}$, containing 2^v linear functions σ_i, defined as

$$\boldsymbol{\sigma}_i = \prod_{l=0}^{v-1} \boldsymbol{\psi}_l^{\mathbf{a}_l^{(i)}}. \tag{34}$$

Since we are considering Householder matrices, and $\boldsymbol{\sigma}_i^2 = \mathbf{I}_n$, it follows that each function is an involution.

The family $\mathcal{F}$ can be used to build a reproducible code. Consider a reproducible parity-check matrix defined by the $s \times n$ signature $\mathbf{h}_0$, whose rows are obtained as

$$\mathbf{h}_j = \mathbf{h}_0 \left(\prod_{l=0}^{v-1} \boldsymbol{\psi}_l^{\mathbf{b}_l^{(j)}} \right)^T. \tag{35}$$

The corresponding code has redundancy $r = s2^v$. We can now take m codewords, and put them in a matrix $\mathbf{g}_0$; it is clear that $\mathbf{H}\mathbf{g}_0^T = \mathbf{0}_{r\times n}$. A reproducible generator matrix for this code can be obtained using the signature $\mathbf{g}_0$ and the family of transformations $\mathcal{F}$. We have

$$\begin{aligned}
\mathbf{h}_j \boldsymbol{\sigma}_i^T &= \mathbf{h}_j \left(\prod_{l=0}^{v-1} \boldsymbol{\psi}_l^{\mathbf{a}^{(i)}} \right)^T = \\
&= \mathbf{h}_j \left(\prod_{l=0}^{v-1} \boldsymbol{\psi}_l^{\mathbf{b}^{(j)}} \right)^T \left(\prod_{l=0}^{v-1} \boldsymbol{\psi}_l^{\mathbf{a}_l^{(i)}} \right)^T = \\
&= \left(\prod_{l=0}^{v-1} \boldsymbol{\psi}_l^{\mathbf{a}_l^{(j)} \oplus \mathbf{b}_l^{(i)}} \right)^T = \\
&= \mathbf{h}_{f(i,j)},
\end{aligned} \tag{36}$$

where $\oplus$ denotes the modulo 2 sum and

$$f(i,j) = \mathbf{a}^{(i)} \oplus \mathbf{b}^{(j)}. \tag{37}$$

It is straightforward to show that such a function satisfies the properties required by Theorem 5. The corresponding code has length n, dimension $k = m2^v$ and redundancy $r = s2^v$. If desired, it is possible to obtain codes with rate close to $1/2$ or in fact equal to $1/2$, the latter corresponding to the case $n = 2^v$, where signatures are defined by a single row.

5.2 Reproducible Codes from Powers of a Single Function

In this section we present another construction which allows to obtain codes satisfying Theorem 5. Consider a $n \times n$ matrix $\boldsymbol{\pi}$ such that $\boldsymbol{\pi}^b = \mathbf{I}_n$, for some integer b. Let v be one of the divisors of b; obviously, if b is a prime, then $v = 1$. Then, we can use $\boldsymbol{\pi}$ to build a family $\mathcal{F}$ of linear transformations, made of $\frac{b}{v}$ matrices defined as $\boldsymbol{\sigma}_i = \boldsymbol{\pi}^{iv}$, for $i = 0, 1, \cdots, \frac{b}{v} - 1$. Then, given a $m \times n$ signature $\mathbf{g}_0$, we can use the family $\mathcal{F}$ to obtain a generator matrix $\mathbf{G}$ which defines a code $\mathcal{C}$ with length n and dimension $k = m\frac{b}{v}$.

A pair of generator/parity-check matrices for $\mathcal{C}$ can be easily obtained with the following procedure. Let us take an $s \times n$ matrix $\mathbf{h}_0$, and use it to generate the parity-check matrix $\mathbf{H}$ as

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \mathbf{h}_2 \\ \vdots \\ \mathbf{h}_{\frac{b}{v}-1} \end{bmatrix} = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_0(\boldsymbol{\pi}^{\frac{b}{v}-v})^T \\ \mathbf{h}_0(\boldsymbol{\pi}^{\frac{b}{v}-2v})^T \\ \vdots \\ \mathbf{h}_0(\boldsymbol{\pi}^1)^T \end{bmatrix}. \tag{38}$$

This matrix has $r = s\frac{b}{v}$ rows and the corresponding code has redundancy r. Then, it is enough to select m codewords and put them in a matrix $\mathbf{g}_0$.

It is quite easy to show that such a parity check matrix is compliant with property (a) from Theorem 5. In fact, we have

$$\begin{aligned} \mathbf{h}_j\boldsymbol{\sigma}_i^T &= \mathbf{h}_0(\boldsymbol{\pi}^{\frac{b}{v}-jv})^T(\boldsymbol{\pi}^{iv})^T = \\ &= \mathbf{h}_0\left[\boldsymbol{\pi}^{\frac{b}{v}+(i-j)v}\right]^T. \end{aligned} \tag{39}$$

If $i \geq j$, we have

$$\begin{aligned} \left[\boldsymbol{\pi}^{\frac{b}{v}+(i-j)v}\right]^T &= \left[\boldsymbol{\pi}^{2\frac{b}{v}-(\frac{b}{v}+j-i)v}\right]^T = \\ &= \left[\boldsymbol{\pi}^{\frac{b}{v}-(\frac{b}{v}+j-i)v}\right]^T\left[\boldsymbol{\pi}^{\frac{b}{v}}\right]^T = \\ &= \left[\boldsymbol{\pi}^{\frac{b}{v}-(\frac{b}{v}+j-i)v}\right]^T = \\ &= \left[\boldsymbol{\pi}^{\frac{b}{v}-(j-i \mod \frac{b}{v})v}\right]^T. \end{aligned} \tag{40}$$

In the case of $i < j$, we can write

$$\begin{aligned} \left[\boldsymbol{\pi}^{\frac{b}{v}+(i-j)v}\right]^T &= \left[\boldsymbol{\pi}^{\frac{b}{v}-(j-i)v}\right]^T = \\ &= \left[\boldsymbol{\pi}^{\frac{b}{v}-(j-i \mod \frac{b}{v})v}\right]^T. \end{aligned} \tag{41}$$

Thus, we have proven that

$$\begin{aligned} \mathbf{h}_j\boldsymbol{\sigma}_i^T &= \mathbf{h}_0\left[\boldsymbol{\pi}^{\frac{b}{v}-(j-i \mod \frac{b}{v})v}\right]^T = \\ &= \mathbf{h}_{(j-i \mod \frac{b}{v})}, \end{aligned} \tag{42}$$

so that the function $f(x_0, x_1)$ required by Theorem 5 is defined as

$$f(x_0, x_1) = x_1 - x_0 \mod \frac{b}{v}. \tag{43}$$

For what concerns property (b), we can consider the following equivalence

$$x_0 - x_1' \equiv x_0 - x_1'' \mod \frac{r}{s}, \tag{44}$$

which turns into

$$x_1'' - x_1' \equiv 0 \mod \frac{r}{s}. \tag{45}$$

Then, it is clear that it must be $x', x'' < \frac{r}{s}$: however, this condition is quite straightforward, since j denotes the row index of the matrix blocks in $\mathbf{H}$. In the same way, when considering the index of the transformation $\boldsymbol{\sigma}_i$, we have

$$x_0' - x_1 \equiv x_0'' - x_1 \mod \frac{r}{s}, \tag{46}$$

which turns into

$$x_0' - x_0'' \equiv 0 \mod \frac{r}{s}. \tag{47}$$

Again, in order to guarantee that the previous equivalence has no solution, it must be $x_0', x_0'' < \frac{r}{s}$. This basically means that we must have $k \leq m\frac{r}{s}$.

5.3 Code-Based Schemes from Quasi-Reproducible Codes

The algebraic structures we have introduced in the previous sections can be used to generate key-pairs in code-based cryptosystems. For instance, let us consider a parity-check matrix $\mathbf{H}$ made of $r_0 \times n_0$ matrices belonging to a pseudo-ring $\mathcal{M}_q^{\mathcal{F},m}$. In order to use $\mathbf{H}$ as the private key in a Niederreiter cryptosystem, we must guarantee that $\mathbf{H}$ is sufficiently sparse: this property can be easily achieved by choosing a family $\mathcal{F}$ of sparse matrices $\boldsymbol{\sigma}_i$. It is clear that a matrix defined by a sparse signature will be sparse as well. In such a case, we can obtain the public key as $\mathbf{H}' = \mathbf{SH}$, where $\mathbf{S}$ is a random dense matrix, whose elements are picked over $\mathcal{M}_q^{\mathcal{F},m}$. Because of Theorem 1, the entries of $\mathbf{H}'$ belong to $\mathcal{M}_q^{\mathcal{F},m}$, and so maintain the same reproducible structure defined by $\mathcal{F}$. If $m = 1$ and $\mathcal{F}$ is a family of permutations, then we can use a $1 \times n_0$ matrix $\mathbf{H} = [\mathbf{H}_0, \mathbf{H}_1, \cdots, \mathbf{H}_{n_0-1}]$, with $\mathbf{H}_i \in \mathcal{M}_q^{\mathcal{F},1}$, as the private key, and $\mathbf{H}' = \mathbf{H}_0^{-1}\mathbf{H}$ as the public key. Indeed, because of Theorem 3, we have $\mathbf{H}_0^{-1} \in \mathcal{M}_q^{\mathcal{F},1}$, and so $\mathbf{H}'$ is a matrix with entries over $\mathcal{M}_q^{\mathcal{F},1}$.

Suppose we have a family $\mathcal{F}$ satisfying Theorem 4, for which multiplication in $\mathcal{M}_q^{\mathcal{F},1}$ is commutative (see Section 4.2 for some examples). Then, we can use the reproducible pseudo-ring induced by $\mathcal{F}$ to obtain key-pairs for a McEliece cryptosystem. For instance, we can choose $\mathbf{H} = [\mathbf{H}_0, \mathbf{H}_1]$, with $\mathbf{H}_i \in \mathcal{M}_q^{\mathcal{F},1}$, as the secret parity-check matrix, and obtain a generator matrix as $\mathbf{G} = \mathbf{S}[\mathbf{H}_1^T, -\mathbf{H}_0^T]$, with $\mathbf{S} \in \mathcal{M}_q^{\mathcal{F},1}$. The pair of matrices $\mathbf{H}$ and $\mathbf{G}$ can be used as the private and public key, respectively, for a McEliece cryptosystem. Even if this case might seem quite specific, it is of significant interest since it is exactly the structure appearing in the first of the three variants (BIKE-1) of the BIKE proposal to the NIST competition.

When both Theorems 3 and 4 are satisfied, we can obtain a generator matrix in systematic form, which maintains a quasi-reproducible structure. In fact, starting from a $r_0 \times n_0$ parity-check matrix $\mathbf{H}$, where the elements are picked randomly from $\mathcal{M}_q^{\mathcal{F},1}$, we can use the corresponding parity-check matrix in systematic form as the public key for a Niederreiter cryptosystem. In the same way, we can compute the systematic generator matrix, and use it as the public key in a McEliece cryptosystem.

It is clear that having the public code described by a matrix in quasi-reproducible form leads to a very significant reduction in the public-key size. Indeed, once the structure of the matrix is fixed by the protocol (i.e. dimensions, family $\mathcal{F}$), the whole public-key can be efficiently represented using just the signatures of each building block. It is obvious that, when the public key is in systematic form, we have an even further reduction in the size of the public-key, since we do not need to publish the identity matrix, but just the non-trivial portion of the matrix.

References

1. R. Misoczki and P. S. L. M. Barreto, "Compact McEliece keys from Goppa codes," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science. Springer Verlag, 2009, vol. 5867, pp. 376–392.
2. R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory." *DSN Progress Report*, pp. 114–116, 1978.
3. P. Gaborit, "Shorter keys for code based cryptography," in *Proc. Int. Workshop on Coding and Cryptography (WCC 2005)*, Bergen, Norway, Mar. 2005, pp. 81–90.
4. M. Baldi, *LDPC codes in the McEliece cryptosystem: attacks and countermeasures*, ser. NATO Science for Peace and Security Series - D: Information and Communication Security. IOS Press, 2009, vol. 23, pp. 160–174.
5. R. Misoczki, J. P. Tillich, N. Sendrier, and P. S. L. M. Barreto, "MDPC-McEliece: New McEliece variants from moderate density parity-check codes," in *2013 IEEE International Symposium on Information Theory*, Jul. 2013, pp. 2069–2073.
6. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.
7. "https://csrc.nist.gov/projects/post-quantum-cryptography."
8. E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 384–386, May 1978.
9. V. M. Sidelnikov and S. O. Shestakov, "On insecurity of cryptosystems based on generalized reed-solomon codes," *Discrete Mathematics and Applications*, vol. 2, no. 4, pp. 439–444, 1992.
10. J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich, "A distinguisher for high rate McEliece cryptosystems," in *Proc. IEEE Information Theory Workshop (ITW)*, Paraty, Brazil, Oct. 2011, pp. 282–286.
11. R. G. Gallager, *Low-density parity-check codes.* M.I.T. Press, 1963.
12. E. Prange, "The use of information sets in decoding cyclic codes," *IRE Transactions on Information Theory*, vol. 8, no. 5, pp. 5–9, Sep. 1962.
13. J. Leon, "A probabilistic algorithm for computing minimum weights of large error-correcting codes," *IEEE Trans. Inform. Theory*, vol. 34, no. 5, pp. 1354–1359, Sep. 1988.

14. J. Stern, "A method for finding codewords of small weight," in *Coding Theory and Applications*, ser. Lecture Notes in Computer Science, G. Cohen and J. Wolfmann, Eds. Springer Verlag, 1989, vol. 388, pp. 106–113.
15. A. May, A. Meurer, and E. Thomae, "Decoding random linear codes in $O(2^{0.054n})$," in *ASIACRYPT*, ser. LNCS. Springer, 2011, vol. 7073, pp. 107–124.
16. A. Becker, A. Joux, A. May, and A. Meurer, "Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding," in *Advances in Cryptology - EUROCRYPT 2012*, ser. Lecture Notes in Computer Science, D. Pointcheval and T. Johansson, Eds. Springer Verlag, 2012, vol. 7237, pp. 520–536.
17. L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annual ACM Symposium on the Theory of Computing*, Philadephia, PA, May 1996, pp. 212–219.
18. D. J. Bernstein, "Grover vs. mceliece," in *PQCrypto*, 2010.
19. R. Misoczki, J.-P. Tillich, N. Sendrier, and P. S. L. M. Barreto. (2012) MDPC-McEliece: New McEliece variants from moderate density parity-check codes. [Online]. Available: http://eprint.iacr.org/2012/409
20. T. P. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani, "Reducing key length of the McEliece cryptosystem," in *Progress in Cryptology - AFRICACRYPT 2009*, ser. Lecture Notes in Computer Science. Springer Verlag, 2009, vol. 5580, pp. 77–97.
21. M. Baldi, M. Bodrato, and F. Chiaraluce, "A new analysis of the McEliece cryptosystem based on QC-LDPC codes," in *Security and Cryptography for Networks*, ser. Lecture Notes in Computer Science. Springer Verlag, 2008, vol. 5229, pp. 246–262.
22. J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich, "Algebraic cryptanalysis of McEliece variants with compact keys," in *EUROCRYPT 2010*, ser. Lecture Notes in Computer Science, vol. 6110. Springer Verlag, 2010, pp. 279–298.
23. "https://bigquake.inria.fr/."
24. N. Sendrier, "Decoding one out of many," in *Post-Quantum Cryptography*, ser. Lecture Notes in Computer Science, B.-Y. Yang, Ed. Springer Verlag, 2011, vol. 7071, pp. 51–67.
25. Q. Guo, T. Johansson, and P. Stankovski, "A key recovery attack on MDPC with CCA security using decoding errors," in *ASIACRYPT*, ser. LNCS. Springer, 2016, vol. 10031, pp. 789–815.
26. M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, "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*, 2018, pp. 3–24. [Online]. Available: https://doi.org/10.1007/978-3-319-79063-3_1
27. P. S. Barreto, S. Gueron, T. Gueneysu, R. Misoczki, E. Persichetti, N. Sendrier, and J.-P. Tillich, "Cake: code-based algorithm for key encapsulation," in *IMA International Conference on Cryptography and Coding*. Springer, 2017, pp. 207–226.
28.
29. J.-P. Tillich, "The decoding failure probability of mdpc codes," *CoRR*, vol. abs/1801.04668, 2018.
30. A. S. Householder, "Unitary triangularization of a nonsymmetric matrix," *J. ACM*, vol. 5, pp. 339–342, 1958.